RSA Authentication Manager 6.1
管理者ガイド

商標

ACE/Agent、ACE/Server、Because Knowledge is Security、BSAFE、ClearTrust、Confidence Inspired、e-Titlement、IntelliAccess、Keon、RC2、RC4、RC5、RSA、RSA ロゴ、RSA Secured、RSA Secured ロゴ、RSA Security、SecurCare、SecurID、SecurWorld、Smart Rules、The Most Trusted Name in e-Security、Transaction Authority、および Virtual Business Units は米国およびその他の国における RSA Security Inc. の登録商標または商標です。本書に記載したその他の会社名および商品名は各社の商標または登録商標です。

ライセンス契約

本ソフトウェアと関連ドキュメンテーションは、米 RSA Security 社が著作権を保有しており、ライセンス契約に従って提供されます。本ソフトウェアおよび関連ドキュメンテーションの使用と複製は、ライセンス契約の条項に従い、添付の著作権を侵害しない場合のみ許諾されます。本ソフトウェアとその複製物を他人に提供することは一切認められません。

本ソフトウェアとその複製物を第三者に提供することは一切認められません。このライセンス契約によって、本ソフトウェアの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアを不正に使用または複製した場合、民事および刑事責任が課せられることがあります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

暗号技術に関するご注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を輸出する場合は、各国の輸出入に関する法律に従わなければなりません。

配布に関するご注意

本マニュアルは信頼できる人にだけ配布するように制限してください。

RSA セキュリティからのお知らせ

本ソフトウェアは米国特許 #4,720,860、#4,885,778、#4,856,062、およびその他の国の特許によって保護されています。

「RC5™ Block Encryption Algorithm With Data-Dependent Rotations」は、米国特許番号 #5,724,428 および #5,835,600 によって保護されています。

本書は英語マニュアル『RSA Authentication Manager 6.1 Administrator’s Guide』の内容を日本語に翻訳したものです。

© 2005 RSA Security Inc. All rights reserved.
第 1 版 日本語版：2005 年 9 月

P/N JS-ACE-6101

目次

はじめに 11
対象となる読者 11
マニュアル 11
サポートとサービス 11
正規販売代理店に電話をかける前に 11

第 1 章 : 概要 13
RSA SecurID トークンと二要素認証 14
RSA SecurID ソフトウェア トークン 15
RSA SecurID Authenticator SID800 15
ユーザ パスワード トークン 15
トークンの割り当ての制限 15
RSA SecurID コードの生成とタイム シンクロナイゼーション 16
正確なシステム時刻の維持 16
RSA Authentication Manager のその他のセキュリティ機能 17
アカウンタビリティとセキュリティ監査 17
攻撃者からの防御 17
データの暗号化 19
エマージェンシー アクセス 19
RSA Authentication Manager アーキテクチャ 20
RSA Authentication Manager データベース 20
プライマリ / レプリカ モデル 21
エージェント ホスト /Authentication Manager アーキテクチャ 23
レルム間モデル 25
RSA Authentication Manager 6.1 の新機能 27
RSA Authentication Manager Control Panel 27
グループ認証設定 27
Funk Software が提供する機能を備えた RSA RADIUS Server 6.1 27
RSA Authentication Manager ライセンス 28

第 2 章 : RSA Authentication Manager Administration アプリケーションの使用 29
アドミニストレーション権限 29
アドミニストレーション スコープ 30
タスク リスト 30
アドミニストレーション スコープとタスク リストの組み合わせ 31
重要な管理ツール 32
システム デザイン ツール 32
アドミニストレーション支援ツール 33
RSA Authentication Manager Host Mode の概要 34
RSA Authentication Manager Host Mode の終了 35
言語サポート (Windows) 35
英語以外の言語を入力できるデータ フィールド 36
MS-IME による日本語の入力 36
ひらがなとカタカナ 37

1 バイト フィールドへの文字の入力 38
Remote Administration 38
Remote Administration 接続のリダイレクト 38
リモート アドミニストレーション用のシステムの構成 39
リモート管理者の認証 40
認証の要求 (チャレンジ) 40
通常のログオンと PASSCODE 入力要求 41
トークンがネクスト トークンコード モードの場合の認証 41
トークンが New PIN モードの場合の認証 42
Quick Admin を使用した Web ベースのアドミニストレーション 44
Quick Admin アーキテクチャ 44
Quick Admin のアドミニストレーション権限 45
タスク リストの設定 46
Quick Admin 管理者の認証 48
検索とレポートのガイドライン 49
Quick Admin の再構成 49
トラブルシューティング 51
Quick Admin の次のステップ 51
第 3 章 : エージェントとエージェント ホスト上でのアクティブ化 53
各プラットフォーム向けの最新のエージェントのダウンロード 54
エージェント ホストの作成と変更 54
自動登録されるエージェント ホスト 54
エージェント ホストのデフォルト設定 54
エージェント ホスト拡張データの変更 55
エージェント構成レコードの作成と編集 55
オフライン認証およびパスワードの統合の設定 57
システム レベルでのオフライン認証の設定 57
システム レベルでのパスワードの統合の設定 59
エージェントごとのオフライン認証とパスワードの統合の設定 59
保護されたドメインでリモート アクセス エージェント ホストが機能するための設定 59
フロントエンド / バックエンド環境での Web アプリケーションのサポート 60
オフライン認証ユーザに対するエマージェンシー アクセスの設定 60
不正な PASSCODE を処理するエージェントの設定 61
オープン エージェント ホスト 63
オープン エージェント ホストの指定 63
オープン エージェント ホストへのアクセスの制限 63
エージェント ホストの自動登録 / 更新 64
DHCP (Dynamic Host Configuration Protocol) のサポート 66
エージェント ホストによる負荷分散 67
sdopts.rec ファイルによる手動負荷分散 68
エージェント ホストの最優先 IP アドレスの設定 72
Client_IP キーワードの使用 73
旧バージョンのエージェント ホスト 74
Configuration Record Editor 77
マスタおよびスレーブのデータの編集 (GUI バージョン) 77

マスタおよびスレーブのデータの編集 (コマンド ライン バージョン)..... 77
第 4 章 : レルム アドミニストレーション 79
レルム間認証..... 79
他のレルムのユーザのレコードの自動作成 79
リモート ユーザ レコードの手動作成 79
レルム間認証でのデフォルト ログイン 80
一部のレルムが RSA ACE/Server 5.0.1 以降にアップグレードされていない場合..... 81
レルム間認証の計画..... 81
レルムの作成と変更..... 83
第 5 章 : データベースのメンテナンス (Windows)..... 85
適切なディスク容量の確保..... 85
データベース圧縮ユーティリティによるディスク領域の再利用 85
RSA Authentication Manager データのバックアップと復元..... 86
RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ..... 87
RSA Authentication Manager プログラムが実行されているときのデータのバックアップ..... 88
データベース バックアップ コマンドで作成されたデータベースの復元 89
オフライン バックアップまたはサーバからのデータの復元 90
データベース レコードのインポートとエクスポート..... 91
データベース ダンプ ユーティリティとロード ユーティリティの使用 92
復元手順..... 92
最新のデータベースの特定 92
レプリカのデータベースの交換 93
レプリカのハードウェアの交換 93
プライマリのデータベースの交換 94
レプリカの指名によるプライマリのハードウェアの交換 96
カスタム定義データ (拡張レコード) のメンテナンス..... 98
ログ拡張データの管理 99
外部 4GL プロシージャの実行 100
第 6 章 : 認証のためのユーザの登録 103
PIN に関するオプション 103
英数字 PIN または数字 PIN の選択..... 103
固定長 PIN または可変長 PIN の選択..... 104
ユーザ作成 PIN またはシステム生成 PIN の選択..... 104
PIN を必要としないトークン 105
ユーザ レコードの作成と変更..... 105
LDAP ユーザ レコードの同期化 106
sdldapsync ユーティリティ 107
コマンド ラインからの LDAP ユーザ データのインポート 107
ライブラリ パスの設定 108
LDAP マップ ファイル 108
sdaceldap ユーティリティ 108
構文 109

SSL の使用 111
LDAP ユーザの管理 112
ユーザ レコードの内容 113
他のインストレーションとのトークン レコード データの共有 113
トークンの割り当て 114
RSA SecurID ソフトウェア トークン 114
トークン レコードの内容 115
グループの作成と変更 117
エージェント ホストでユーザをアクティブ化するためのグループの使用例 118
グループ メンバーシップ リストの作成と変更 118
グループ拡張データの変更 118
エージェント ホスト上でのアクティブ化 119
ユーザのアクティブ化と非アクティブ化 119
グループのアクティブ化と非アクティブ化 120
ユーザおよびグループのアクセス時間の変更 120
ユーザへのハードウェア トークンの配布 120
ユーザの認証に関する問題の回避と処理 121
セキュリティ上の責任に関するユーザの教育 121
トークンの割り当ての解除 121
トークンの無効化 122
トークンが盗まれたり、紛失した場合 122
PIN が盗まれたり、他人に知られた場合 125
New PIN モードの設定 127
New PIN 手順でのユーザ支援 127
トークンの同期のとり直し 128
サイトの作成と変更 130
サイト拡張データの編集 131

第 7 章 : データベースのメンテナンス (UNIX) 133

適切なディスク容量の確保 133
データベース圧縮ユーティリティによるディスク領域の再利用 133
RSA Authentication Manager データのバックアップと復元 134
RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ 135
RSA Authentication Manager プログラムが実行されているときのデータのバックアップ 136
データベース バックアップ コマンドで作成されたデータベースの復元 137
オフライン バックアップまたはサーバからのデータの復元 137
データベース レコードのインポートとエクスポート 139
データベース ダンプ ユーティリティとロード ユーティリティの使用 140
復元手順 140
最新のデータベースの特定 140
レプリカのデータベースの交換 141
レプリカのハードウェアの交換 142
プライマリのデータベースの交換 143
レプリカの指名によるプライマリのハードウェアの交換 144
カスタム定義データ (拡張レコード) のメンテナンス 146

ログ拡張データの管理 147
外部 4GL プロシージャの実行 148
第 8 章 : ログ データベースのメンテナンス 151
[Log] メニュー 151
ログ データベース統計情報の表示 151
ログ レコードの削除 152
ログ データベースの自動メンテナンスのスケジュール 153
アーカイブ ファイル 153
ログ フィルタリング 154
第 9 章 : レポート 155
監査証跡レポート 155
ログ レコードの内容 155
レポートの種類 156
レポートの作成 158
ファイルへのレポートの出力 162
拡張データ レポート 163
ログ モニタとレポート作成 164
ログ モニタ オプション 165
sdlogmon コマンドの使い方 165
システム ログ内の Authentication Manager イベントの監視 166
ログ アーカイブ ファイルの使い方 167
RSA Authentication Manager レポート作成ユーティリティ (Windows) 169
レポート作成ユーティリティのインストール 169
レポート作成ユーティリティの起動と停止 169
実行するレポートの選択 170
レポートの [Run List] の保存 170
標準レポートの種類 171
レポート出力ファイル 171
カスタム レポートの作成と管理 172
ユーザ情報の表示 176
コマンド ラインからのレポートの実行 177
RSA Authentication Manager レポート作成ユーティリティ (UNIX) 178
UNIX インタフェースの基本操作 178
レポート作成ユーティリティのインストール 179
レポート作成ユーティリティの起動と停止 179
実行するレポートの選択 180
標準レポートの種類 181
レポート出力ファイル 182
カスタム レポートの作成と管理 182
ユーザ情報の表示 186
コマンド ラインからのレポートの実行 187
カスタム SQL クエリの作成と実行 187
カスタム クエリ ツールの基本的な使い方 188
カスタム クエリの作成と編集 190
カスタム クエリの SQL 構文と記述方法 191

カスタム クエリに関する高度なアプリケーション ノート 200
第 10 章 : その他の管理タスク 207
システム パラメータの変更 207
システム拡張データの変更 209
承認手順のカスタマイズ 209
External Authorization オプションの選択 211
External Authorization の停止と再起動 211
第 11 章 : プログラム ファイルとデータ ファイル 213
RSA Authentication Manager ソフトウェア 213
Configuration Management 213
ユーザの認証 213
データベースの管理 214
アクティビティのリアルタイム監視 214
レルム ステータスの判断 214
RSA Authentication Agent ソフトウェア 216
ユーザ認証ダイアログ 216
構成情報の表示 217
エージェント ホストの自動登録と更新 217
通信の暗号化と復号化 217
RSA Authentication Manager データ 218
Authentication Manager データベース 218
ログ データベース 219
sdconf.rec ファイル 220
license.rec ファイル 221
ノード シークレット ファイル 222
データベースの調整 223
RSA Authentication Manager インストール情報およびパッチ情報の表示 225
第 12 章 : RSA Authentication Manager の構成 (Windows) 227
[License Information] (ライセンス情報) 229
RSA Authentication Manager でのライセンス レコードの更新 229
[Configuration Information] (構成情報) 230
[Enable Features] (有効にする機能) 231
[Agent Host Communication] (エージェント ホストの通信) 231
[Primary/Replica Communication] (プライマリとレプリカ間の通信) 232
[Services] (サービスの構成) 232
[Legacy Agent Server Identification] (旧バージョンのエージェントをサポートするサーバの指定) 234
[RSA Authentication Manager Identification] (プライマリとレプリカの指定) 234
エージェント ホストの PASSCODE の設定 235
更新した構成ファイルの配布 236
複数のネットワーク インタフェース間の認証 237
第 13 章 : レプリカ管理ユーティリティ (Windows) 239
レプリカ Authentication Manager 情報の表示 240

第 14 章 : RSA Authentication Manager の構成 (UNIX) 243
RSA Authentication Manager for UNIX でのライセンス レコードの更新 243
RSA Authentication Manager の構成の概要 244
構成の変更 247
更新した構成ファイルの配布 251
エージェント ホストの名前または IP アドレスの変更 253
エージェント ホストの複数の IP アドレス 253
第 15 章 : レプリカ管理ユーティリティ (UNIX) 255
レプリカ管理ユーティリティの起動 255
対話モードとコマンド ライン モード 255
レプリカの追加 256
Name of the Replica (レプリカの名前) 256
IP Address (IP アドレス) 256
Alias IP Addresses (エイリアス IP アドレス) 256
Service Name (サービス名) 256
Service Port (サービス ポート) 256
Delay (遅延) 256
Interval (間隔) 256
レプリカの変更 257
レプリカの交換 257
レプリカの削除 257
Authentication Manager 情報の表示 258
プライマリの名前または IP アドレスの変更 259
複数のネットワーク インタフェース間の認証 261
コマンド ラインでの操作 263
構文 263
レプリカの追加 (コマンド ライン) 265
エイリアス IP アドレスの割り当て 265
レプリカ情報の変更 (コマンド ライン) 266
付録 A : ライセンス 271
アクティブ ユーザ 271
ライセンスの種類 271
ライセンスの制限の管理 272
インストール時のライセンスの管理 272
日常操作および管理作業でのライセンスの管理 273
レルム間環境 274
ライセンスのアップグレードまたは変換 274
付録 B : サービスとプロセス 275
サービスとネットワーク ポート (Windows および UNIX) 275
RSA Authentication Manager プロセス (Windows および UNIX) 278
サービス コントロール マネージャ サービス (Windows のみ) 279
付録 C : トラブルシューティング 281
イベント ログまたはシステム ログへの監査ログ メッセージの送信 281
イベント ログとシステム ログの例 284

SNMP によるメッセージのフィルタリング 286
エラー状況 286
認証に関連するエラー状況 286
アドミニストレーションに関連するエラー状況 290
問題の解決方法 291
ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合 291
LDAP 同期に関連するエラー メッセージ 291
External Authorization のタイムアウトに関連するメッセージ 292
プライマリとレプリカ間の通信の開始に関連する問題の解決 292
メッセージ 293
メッセージの ID 番号 401
用語集 443
索引 447

はじめに

対象となる読者

本書は、システム管理者とその他の信任された人だけを対象としています。セキュリティ上の理由から、本書を一般ユーザに公開しないでください。

マニュアル

RSA Authentication Manager 6.1 CD-ROM には、RSA Authentication Manager のすべてのマニュアルとヘルプが収録されており、インストール、構成、アドミニストレーション、およびトラブルシューティングに関する詳細な情報が提供されています。RSA Authentication Manager 6.1 で提供されるすべての資料に関しては、RSA Authentication Manager パッケージに付属している印刷物『Getting Started』を参照してください。

メモ：セキュリティ上の理由から、ご使用のプラットフォーム用の Adobe Reader の最新バージョンは、**www.adobe.com** で入手してください。

サポートとサービス

RSA SecurCare Online	**https://knowledge.rsasecurity.com**

正規販売代理店に電話をかける前に

メモ：有効なソフトウェア年間保守契約が締結されていない限り、保証期間内でもテクニカル サポートを受けることはできません。

RSA Authentication Manager ソフトウェアを実行しているコンピュータに直接アクセスできることを確認し、次の情報を準備してください。

- RSA セキュリティ社のカスタマ / ライセンス ID。この番号は、ライセンス配布メディアに記載されています。Windows で Configuration Management アプリケーションを実行するか、UNIX で **sdinfo** を実行して確認することもできます。
- RSA Authentication Manager ソフトウェア バージョン番号。
- 問題が発生したマシンのメーカとモデル。
- 問題が発生したオペレーティング システムの名前とバージョン。

1 概要

RSA Authentication Manager は RSA Authentication Agent と連携して動作し、時間ベースの RSA SecurID トークンの強力な二要素認証機能により、Windows 環境のセキュリティを強化します。このソフトウェア リリースで提供される RSA SecurID for Microsoft Windows ソリューションは、次の機能を備えています。

- **RSA Authentication Manager 6.1** は、アドミニストレーション、ユーザ認証、パスワードの統合、および監査を行います。
- **RSA Authentication Agent 6.0 または 6.1** は、ローカル コンピュータ、ドメイン サーバ、およびターミナル サーバを保護し、Microsoft RRAS (ルーティングとリモート アクセス サービス) および Microsoft ワイヤレス LAN を介したリモート ログオンも保護します。
- **RSA Authentication Agent 5.3 for Web** は、Web サーバを保護し、Microsoft Outlook Web Access も保護します。

RSA Authentication Manager 6.0 または 6.1、RSA Authentication Agent 6.0 または 6.1、および RSA SecurID を組み合わせて使用することで、コンピュータおよびネットワークで Windows パスワードのセキュリティを向上することができます。保護されたシステムでは、RSA Authentication Agent はユーザに対してログオン名と PASSCODE の入力を求め、RSA Authentication Manager認証サービスに入力内容を転送します。Authentication Manager の応答に応じて、ユーザのログオンは許可される場合と、拒否される場合があります。

RSA Authentication Agentソフトウェアの各バージョンは他のプラットフォームでも実行でき、さまざまなネットワーク リソースを RSA SecurID で保護することができます。サポートされるプラットフォームの一覧については、216 ページの「RSA Authentication Agent ソフトウェア」を参照してください。

RSA Authentication Manager は、Progress Software 社で開発された商用リレーショナル データベースを統合して、数多くのユーザやトークンをサポートするための拡張機能を実現しています。

RSA Authentication Manager データベースの読み書きを行うためのカスタム アドミニストレーション アプリケーションを作成するには、RSA Authentication Manager 製品セットに付属しているアドミニストレーション ツールキットを使用します。詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリまたはソフトウェア CD-ROM の **authmgr_admin_toolkit.pdf**) を参照してください。

この章では、RSA Authentication Manager および SecurID ソリューションのセキュリティ機能、システム アーキテクチャ、新機能などについて説明します。

RSA SecurID トークンと二要素認証

RSA SecurID が導入されている組織では、ユーザは正しい PASSCODE を入力しなければ、保護されているシステムにアクセスできません。PASSCODE は次のもので構成されます。

- 個人識別番号、PIN (ユーザだけが**知っている**もの)
- ユーザのトークンに現在表示されているトークンコード (ユーザが**保有**しているもの)

RSA SecurID ソリューションによるユーザ認証ではこれらの 2 つの要素が必要であるため、従来のパスワード (一要素認証) より強力なセキュリティを実現できます。

ほとんどの RSA SecurID トークンは携帯型のデバイスであり、ランダムなコード (トークンコード) を計算して表示するマイクロプロセッサを搭載しています。

SID800 トークン

PINPAD

キーホルダ

トークンコードは、指定された間隔(通常は60秒おき)で変化します。RSA Authentication Manager 6.1 では、次のトークン アルゴリズムがサポートされます。

- **従来型 SID** (64 ビット アルゴリズム) トークンは、SID アルゴリズムを使用して時間ベースの認証機能を提供します。SID シード レコードは、ASCII 形式または XML 形式で提供されます。
- **AES** (128 ビット アルゴリズム) トークンは、AES (Advanced Encryption Standard) 暗号化アルゴリズムを使用して時間ベースの認証機能を提供します。AES シード レコードは、XML 形式で提供されます。

トークン アルゴリズムは、RSA Authentication Manager Host Mode の多くのアドミニストレーション タスクにフィールドまたは検索条件として含まれています。たとえば、データベース内のトークン レコードを表示する場合は、アルゴリズムで表示することも、SID または AES アルゴリズムだけで表示することもできます。

認証手順のテンプレートが提供されます (**authmgr_authentication.doc** および **authmgr_authentication.pdf**)。このファイルは必要に応じて変更し、ユーザに渡すことができます。

RSA SecurID Authenticator SID800 を導入する場合、ユーザ向けの認証手順については、RSA Security Center のヘルプおよび『RSA Authenticator Utility 1.0 ユーザーズ クイック リファレンス』を参照してください。いずれも RSA Authenticator Utility 1.0 に同梱されています。

メモ : RSA Authentication Manager では、PIN を必要としないハードウェア トークンによる認証もサポートされます。詳細については、105 ページの「PIN を必要としないトークン」を参照してください。

RSA SecurID ソフトウェア トークン

ソフトウェア トークンとは、クライアント ワークステーション、RSA SecurID スマート カード、PDA (personal digital assistant)、携帯電話にインストールされるソフトウェア ファイルです。

RSA Authentication Manager Host Mode では、サポートされているデバイスに対して RSA SecurID ソフトウェア トークンを発行するための集中管理インタフェースを提供しています。トークン拡張フィールドを使用すると、デバイスの種類、デバイスのシリアル番号、トークンのニックネームなどの情報をソフトウェア トークンに追加できます。

ソフトウェア トークンの詳細については、114 ページの「RSA SecurID ソフトウェア トークン」、および各 RSA SecurID ソフトウェア トークン製品に付属しているマニュアルを参照してください。

RSA SecurID Authenticator SID800

RSA SecurID Authenticator SID800 は、RSA SecurID トークンであり、同時にリーダを搭載した USB スマート カード (USB トークン) でもあります。2 組の電子部品は相互に独立して動作します。

コンピュータに非接続の場合、SID800 は RSA SecurID 認証で使用されるトークンコードを生成し、表示します。コンピュータに接続した状態では、トークンは次の 2 つの機能を実行します。

- RSA SecurID 認証では、デスクトップ上のサポートされるソフトウェアからトークンコードを取得できるので、トークンに表示される数字を読み取る必要がありません。
- トークンのスマート カード機能を使用すると、Windows へのログオンに必要なデジタル証明書や Windows ログオン アカウントなどのクレデンシャルを保存できます。

詳細については、RSA Authenticator Utility 1.0 のマニュアルを参照してください。

ユーザ パスワード トークン

ユーザ パスワード トークンは、PIN とトークンコードの代わりにユーザが入力する 1 つのパスワードです。ユーザ パスワードは他のトークンほど安全ではありませんが、ユーザ パスワードを使用すれば、セキュリティ レベルの異なるユーザを管理できます。たとえば、物理的に安全な施設で作業しているユーザには、ユーザ パスワードを割り当ててもよいでしょう (ユーザ パスワードは 1 つのトークンとして扱われ、管理者が作成または変更してから 3 年間有効です)。

重要：しかし、ユーザ パスワード トークンは他の種類のトークンほど安全ではないため、長期的に使用するセキュリティ ソリューションとして使用することはお勧めできません。

トークンの割り当ての制限

保護されたシステムへのアクセスが承認されている各ユーザには、RSA SecurID トークンを最大 3 個まで割り当てることができます。たとえば、使用する場所に応じて、適切な種類のトークンを使用できます。自宅で通信するときはハードウェア トークンを使用し、オフィスでは RSA SecurID ソフトウェア トークンを使用することなどが可能です。

RSA SecurID コードの生成とタイム シンクロナイゼーション

RSA Authentication Manager ソフトウェアと RSA SecurID トークンは連携動作して、ユーザの身元を認証します。米 RSA Security 社が特許を保有しているタイム シンクロナイゼーション方式では、ユーザのトークンに表示される擬似乱数コードは、RSA Authentication Manager ソフトウェアがその瞬間に生成するコードと同じコードであることを保証しています。

RSA SecurID トークンは次の情報にもとづいて計算し、トークンコードを生成します。

- トークンに格納されているトークン固有の識別子 (「シード」とも呼びます)。
- トークンの内部クロックから生成される現在の時刻。世界協定時 (Coordinated Universal Time) で表します。

RSA Authentication Manager は次の情報を使用して、トークンのトークンコードを生成します。

- RSA Authentication Manager データベースのトークン レコードに格納されているトークン固有の識別子。
- トークン レコードに格納されたオフセットを現在の RSA Authentication Manager 時刻に加算して算出し、世界協定時 (UTC) で表した時刻。

アクセスが正当なユーザによるものかどうか判断するために、RSA Authentication Manager が生成したトークンコードと、ユーザが入力したトークンコードとが比較されます。2 つのトークンコードが一致しない場合や、誤った PIN が入力された場合には、ユーザのアクセスは拒否されます。

RSA Security 社のタイム シンクロナイゼーション方式の詳細と、トークン レコードに格納される時刻オフセットの詳細については、128 ページの「同期」を参照してください。

正確なシステム時刻の維持

RSA Authentication Manager は、世界協定時 (UTC) と呼ばれる標準時をベースにして動作します。RSA Authentication Manager ソフトウェアが稼動するコンピュータの時刻、日付、タイム ゾーンは、常に UTC を基準にして正しく設定されている必要があります。

RSA Authentication Manager をインストールするコンピュータの時刻がローカル時刻に設定され、世界協定時 (UTC) に対応していることを確認してください。たとえば、UTC が 11:43 a.m. のときに、日本時間 (UTC+9:00) に設定されているコンピュータに RSA Authentication Manager をインストールする場合は、コンピュータの時刻が 8:43 p.m. に設定されている必要があります。

日本時間は時報で確認してください。117 に電話して確認できます。

メモ : NTP (ネットワーク タイム プロトコル) を使用して正確な時刻を維持する場合は、プライマリ Authentication Manager でのみ有効にしてください。プライマリは、レプリカのタイム シンクロナイゼーションを自動的に維持します。しかし、例外が 1 つあります。UNIX 環境では、セキュリティ上の理由から、root ユーザが Authentication Manager を起動することが認められていない場合があります。この場合、プライマリはレプリカで正確な時刻を**維持しない**ので、プライマリとレプリカで NTP を使用してもかまいません。

RSA Authentication Manager のその他のセキュリティ機能

RSA Authentication Manager で提供されるその他のセキュリティ機能としては、監査機能、攻撃者からの防御機能、データの暗号化機能があります。

アカウンタビリティとセキュリティ監査

ユーザのアカウンタビリティ (責任) は、システム セキュリティの重要な部分であるため、RSA Authentication Manager では監査証跡を作成します。この監査証跡はすべてのログオン要求と、RSA Authentication Manager Host Mode で実行されたすべての操作を追跡します。

RSA Authentication Manager が正しく実装されている場合は、監査証跡を使用することで、ログに記録された各アクションを実行したユーザを正しく判別できます。記録されたアクションを誰が実行したかが問題になる場合、二要素認証をベースとするユーザ情報は、パスワード単独による認証方式よりも、法的に強力な証拠となります。

自分の ID やシステムが不正に使用されないように、厳重にユーザ教育をしてください。詳細については、121 ページの「セキュリティ上の責任に関するユーザの教育」を参照してください。

監査証跡は次の方法で確認できます。

- RSA Authentication Manager Host Mode のレポート
- レポート作成ユーティリテイ (169 ページの「RSA Authentication Manager レポート作成ユーティリティ (Windows)」を参照)
- 自動ログ メンテナンス機能によって生成されたファイルを使用して、サードパーティ ソフトウェアで作成されるレポート (153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照)

また、レコードが作成されるのと同時に画面にも表示されるように指定すると、活動 (アクティビティ) をリアルタイムに監視できます。詳細については、214 ページの「アクティビティのリアルタイム監視」を参照してください。

攻撃者からの防御

盗んだ PIN や RSA SecurID トークンを使用して、不正なユーザがシステムに侵入しようとすると、RSA Authentication Manager の**攻撃回避**機能が不正な攻撃を検出し、アクセスを拒否します。どんなに強力な攻撃回避機能があっても、製品の適切な実装と使用が不要になるわけではなく、ユーザの PIN と RSA SecurID トークンの両方を攻撃者に盗まれてしまうと、システムを**保護することはできません**。

したがって、次の指針を遵守することが**重要**になります。

- すべてのユーザが自分の PIN を他人に知られないようにし、トークンを安全な場所に保管しなければなりません。
- PIN が盗まれたり、トークンを紛失した場合は、管理者はただちにこれらを無効にしなければなりません。
- プライマリ マシンとレプリカ マシンは、RSA Authentication Manager の専用マシンとして設定する必要があります。これらのコンピュータを Web サーバやファイル サーバ、ファイアウォール、その他のアプリケーション用に使用することは避けてください。
- RSA Authentication Manager プライマリ マシンとレプリカ マシンは物理的に安全な場所に設置しなければなりません。

重要：管理者はユーザに対して、認証手順マニュアルの「User Responsibilities」の指示に従うように注意してください。

攻撃回避機能

不正なユーザが PIN を盗み、最終的に正しいトークンコードを推測することができたとしても、アクセスがただちに許可されるわけではありません。ログオンの試行に連続して失敗すると、次に表示されるトークンコードが Authentication Manager から要求されます。次に表示されるトークンコードを正しく入力しない限り、アクセスは許可されません。一定の回数連続してログオンに失敗すると、そのログオン試行に使用されたトークンは自動的に無効になります。詳細については、126 ページの「攻撃回避機能の要約」を参照してください。

不正な PASSCODE の入力が許容される回数は、Configuration Management アプリケーション (Windows) または ***ACEPROG*/sdsetup -config** コマンド (UNIX) を使用して設定できます。詳細については、第 12 章「RSA Authentication Manager の構成 (Windows)」または第 14 章「RSA Authentication Manager の構成 (UNIX)」を参照してください。

ロック マネージャ

ロック マネージャは、すでに使用された PASSCODE を攻撃者が再利用しようとしたり、トークンの現在の PASSCODE を取得しようとするリプレイ アタックから RSA Authentication Manager を防御します。ロック マネージャのサービス名は **sdlockmgr** で、デフォルトのサービス ポートは **5560/tcp** です。

ロック マネージャは、これまで RSA Authentication Manager のワーク キュー (work queue) で管理されていたデータを統合します。ワーク キューは、**レスポンス遅延時間** Response Delay) と呼ばれる時間内に、同じ認証機器 (RSA SecurID トークン) に対して 2 つの認証が同時に発生した場合に、その認証を検出するために使用されます。さらに、RSA Authentication Manager はトークンの**ハイ ウォータ マーク**を使用することで、認証時間枠内に (したがって、RSA Authentication Manager で受け付けられる) 過去のトークンコードのリプレイが行われるのを防止します。RSA Authentication Manager プロセスをレプリケートする場合は、1 つのレルム内のすべての RSA Authentication Managerからのワーク キュー データを統合するメカニズムが必要です。ロック マネージャは、次の操作により、この役割を果たします。

- RSA Authentication Agentが名前ロック要求をRSA Authentication Managerに送信すると、ユーザのデフォルト ログオン名をロックします。Authentication Manager が 2 つ目の名前ロック要求を受信すると、2 つ目の要求は拒否されます。
- **ハイ ウォータ マーク**を追跡します。ハイ ウォータ マークとは、トークンで最後に使用された正しい PASSCODE の記録です。Authentication Manager は、最後に使用された正しい PASSCODE の**後**に計算される PASSCODE は受け付けます。このトークン レコードには今後もハイ ウォータ マークを格納できますが(前のリリースと同様)、現在はこのタスクをすべて、ロック マネージャで行うことができるようになりました。トークン レコードにハイ ウォータ マークが記録されないように Authentication Manager を設定するには、[System] > [System Configuration] > [Edit Token, PIN and Password Parameters] の順にクリックし、[Store time of last login in token records] チェックボックスをオフにします。

リプレイ アタックの検出

リプレイ アタックでは、攻撃者はサーバのシステム クロックを戻し、適切なシステム時刻になったら、不正に取得した PASSCODE を再利用してシステムにアクセスします。リプレイ アタックの可能性を示すシステム時刻の変化が検出されると、RSA Authentication Manager ソフトウェアは管理者にそのことを警告します。

サーバのシステム クロックが戻されていることを RSA Authentication Manager ソフトウェアが検出すると、「*** System clock setback detected (システム クロックの巻き戻しが検出されました)」という警告メッセージがログ データベースに記録されます。このメッセージは、RSA Authentication Manager Host Mode の Activity レポートまたは Exception レポートで確認できます。また、このメッセージはデフォルト設定でイベント ログにも記録されるので、市販のネットワーク管理ツールを使用して追跡し、識別することができます。

メモ：このメッセージは重大なセキュリティ侵害の可能性を示します。したがって、イベント ログに送信するメッセージ タイプ リストからこのメッセージを**削除しないでください**。

データの暗号化

RSA Authentication Manager 6.1 では、システムのセキュリティ確保のために数種類のデータ暗号化を使用します。

- プライマリとレプリカの間で交換されるメッセージとデータはすべて、送信中に暗号化されます。機密性の高いデータは安全な RC5 ブロック暗号で暗号化され、それほど機密性の高くないデータは、10 分おきに変化する DES 暗号鍵で暗号化されます。
- エージェントとプライマリまたはレプリカの間の通信は、特定のエージェントと Authentication Manager だけが知っている固有の鍵 (**ノード シークレット**) を使用して暗号化されます。この機能により、承認されていないマシンがエージェント、プライマリ、またはレプリカになりすますのを防止できます。詳細については、222 ページの「ノード シークレット ファイル」を参照してください。
- 同様に、個別の RSA Authentication Manager システム (レルム) 間の通信は、情報交換に関係する 2 台の Authentication Manager だけが知っている固有の**レルム シークレット**にもとづいて暗号化されます。レルム シークレットの詳細については、83 ページの「レルムの作成と変更」を参照してください。
- ユーザの PIN などの重要なトークン データは暗号化されており、システム管理者も含めて、誰もそのデータを表示できません。一方、トークン シリアル番号は暗号化されないので、管理者は管理のためにシリアル番号でトークンを指定できます。

エマージェンシー アクセス

どんなに責任感の強いユーザでも、トークンを紛失する可能性があります。紛失したトークンは無効にしてください。ただし、組織のセキュリティ ポリシーで認められている場合は、紛失したトークンが見つかるまで、または紛失したトークンを無効にしなければならないと管理者が判断するまで、認証のために**テンポラリ** パスワード (1 つの固定パスワードまたは一連のワンタイム パスワード) を割り当てることができます。詳細については、124 ページの「紛失したトークンの代わりに使用するテンポラリ パスワード」を参照してください。

テンポラリ パスワードは、トークンと同じように注意深く保管するようにユーザに指示してください。テンポラリ パスワードの使用の詳細については、日本語 CD-ROM の『RSA SecurID トークンによる認証』(英語版は **authmgr_authentication.pdf**) を参照してください。

RSA Authentication Manager アーキテクチャ

このセクションでは、RSA Authentication Manager データベース、プライマリ / レプリカ モデル、レルム間モデル、エージェント ホスト アーキテクチャなど、システムのアーキテクチャの概要を示します。

RSA Authentication Manager データベース

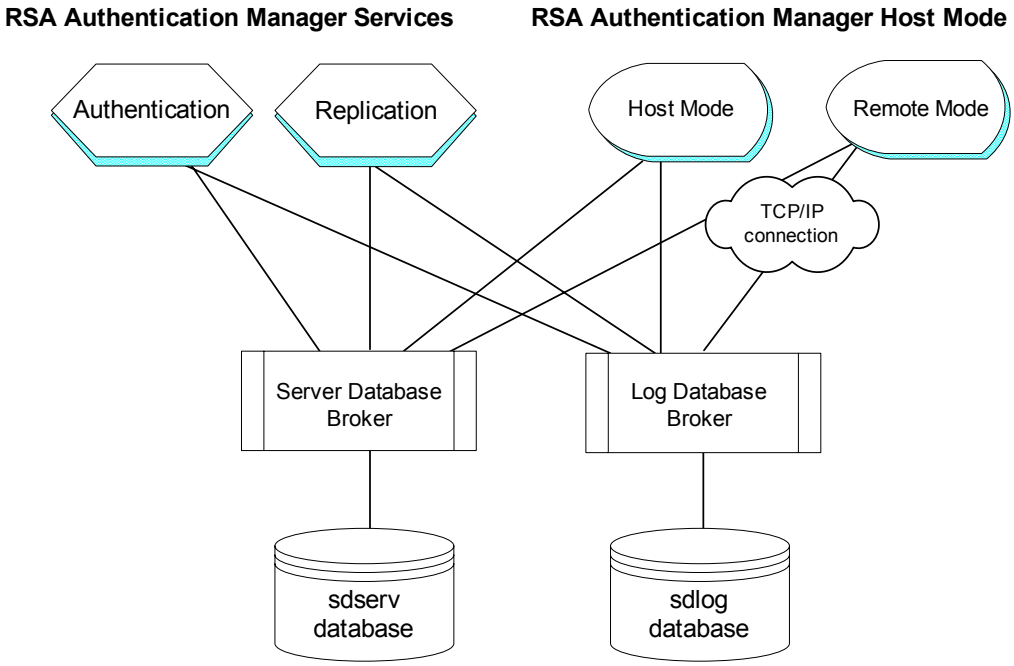
RSA Authentication Manager データは、Progress Software 社で開発されたリレーショナル データベース管理システム (RDBMS) に格納されます。このソフトウェアは RSA Authentication Manager ソフトウェアに統合されています。

Authentication Manager では、**sdserv** (ユーザ データベース) と **sdlog** (監査ログ データベース) の 2 つのデータベースが管理されます。Authentication Manager データベースには次の情報が格納されます。

- RSA SecurID 認証で保護されるリソースのリスト
- すべてのトークンのレコード
- ユーザの登録情報
- レルム間認証とリモート アドミニストレーションで使用するレルムの登録情報
- 認証アクティビティと管理アクティビティの監査証跡

次の図は、2 つのデータベース (**sdserv** と **sdlog**)、RSA Authentication Manager 認証サービスおよびレプリケーション サービス、およびホスト モードとリモート モードの RSA Authentication Manager Host Mode の関係を示しています。

ブローカは、これらのサービスおよび RSA Authentication Manager Host Mode セッションをデータベースに接続します。RSA Authentication Manager サービスまたは RSA Authentication Manager Host Mode をホスト モードで起動した場合、Authentication Manager ソフトウェアはブローカが動作しているかどうか確認し、必要に応じてブローカを起動します。この時点で、Remote Administration サービス (**sdadmind**) も起動されるので、RSA Authentication Manager Host Mode をリモートから実行できるようになります。



すべての RSA Authentication Manager サービスを停止すると、Authentication Manager ソフトウェアはデータベース ブローカを自動的に停止します。ブローカをシャットダウンすると、データベースとアクティブなアドミニストレーション セッションの間の必要な接続が切断されます。

RSA Authentication Manager Host Mode セッションを終了した場合、RSA Authentication Manager サービスが動作していない場合でも、ブローカは動作を続行します。

Windows を使用している場合は、[RSA Authentication Manager Control Panel] からサービスの起動と停止を行うことができます。

UNIX を使用している場合は、コマンド プロンプトで次のコマンドを入力することでブローカを停止できます。

```
ACEPROG/sdconnect stop
```

ACEPROG は **ace/prog** ディレクトリの場所を表します。

メモ：External Authorization (**sdxauthd**) という RSA Authentication Manager サービスについては、Authentication Manager アーキテクチャの中核となるものではないため、ここでは詳しく説明しません。

プライマリ / レプリカ モデル

RSA Authentication Manager 6.1 では、1 台のプライマリと最大 10 台のレプリカを使用できます。プライマリはアドミニストレーション Authentication Manager として機能し、データベースの変更を各レプリカに複製し、ユーザを認証し、すべてのレプリカから受信したログ メッセージを統合ログ データベースに記録します。レプリカは認証サーバとして機能し、データベースに対して読み取りアクセスだけが許可されています。

メモ：複数のレプリカをインストールするには、RSA Authentication Manager アドバンスド ライセンスが必要です。RSA Authentication Manager ベース ライセンスでは、プライマリとレプリカはそれぞれ 1 台ずつに制限されます。ライセンスの詳細については、付録 A「ライセンス」を参照してください。

データベースのレプリケーション (複製)

プライマリは、システム内の各レプリカに対して、レプリケーション サービス (UNIX では **acesyncd**、Windows では **syncserv**) を個別に実行します。各レプリカは、レプリケーション サービスを実行します。レプリケーション サービスを使用すると、プライマリ サーバとレプリカ サーバが通信し、データベースの変更に関する情報を定期的に交換できます。プライマリとレプリカの間のデルタ レコードの交換は、レプリケーション パス (replication pass) と呼ばれます。

最初のレプリケーション プロセスは、プライマリが起動してから特定の秒数が経過した後で開始されます。2 回目のレプリケーション プロセスは、最初のプロセスから同じ秒数が経過してから開始されます。3 回目以降も同様に行われます。起動遅延によってレプリケーション プロセスの開始時刻を遅らせるのは、レルム内のすべてのレプリカがプライマリに変更内容を同時に送信しないようにするためです。

起動後、プライマリとレプリカは、レプリケーション間隔と呼ばれる指定された頻度で、デルタ レコードを交換します。起動遅延とレプリケーション間隔は両方とも、**sdsetup -repmgmt**ツール(UNIX)またはReplica Managementアプリケーション(Windows)で定義できます。

プライマリ データベースの変更のほとんどは、管理操作によって発生します。たとえば、管理者がデータベースにユーザを追加し、そのユーザに RSA SecurID トークンを割り当てた場合などに発生します。レプリカ データベースが変更されるのは、ユーザが認証を受けるときと (成功または失敗)、その認証試行との接続時にログ メッセージが生成されたときです。たとえば、新しいユーザがトークンを使用して初めてログインし、新しい PIN を選択したと仮定します。その認証要求を受信したレプリカは新しい PIN を受け付け、ユーザを認証し、レプリカ データベースのそのユーザのレコードを変更します。レプリカはこの変更内容をプライマリに送信し、プライマリはレルム内の他のすべてのレプリカにその情報を送信します。また、レプリカは、プライマリの変更結果としてログに記録されたメッセージもすべて送信しますが、プライマリはこのログ メッセージを他のレプリカには送信しません。

レプリカ パッケージ

レプリカ パッケージには、1 台以上のレプリカをインストールするのに必要なデータベース ファイルとライセンス ファイルが含まれています。レプリカ パッケージはプライマリで作成し、レプリカに RSA Security ソフトウェアをインストールする前にレプリカ マシンにコピーします。

レプリカ パッケージの作成時に複数のレプリカ マシンを指定すると、これらのマシンのすべてに対して同じパッケージを使用できます。このため、レプリカ パッケージを作成する前に、すべてのレプリカ マシンを特定するようにしてください。後で、元のパッケージに指定されていないレプリカを追加する必要がある場合は、まずレプリカを追加し、そのレプリカに対して新しいレプリカ パッケージを作成します。

データベース プッシュ (Push DB Assisted Recovery) 機能

Push DB (データベース プッシュ) 機能はシステム パラメータで設定するオプションです。有効にすると、ネットワークを通じて最新のデータベース ファイルがレプリカにコピーされます。

Push DB 機能は、インストール時に使用したり、Authentication Manager や Authentication Manager 上のデータベースで問題が発生した後の復元プロセスの一部として指定できます。インストールでは、今後も初期レプリカ パッケージを作成し、レプリカ パッケージからレプリカにライセンス ファイルをコピーし、ソフトウェアをインストールする必要があります。データベース プッシュ機能 (Push DB) を使用すると、レプリカを初めて起動した時点で、データベース ファイルがプライマリからレプリカに自動的にコピーされます。

大規模なデータベース ファイルをコピーすると、ネットワークの帯域幅、必要とされる転送速度、ネットワークの速度などが許容できないレベルまで低下する可能性があります。Push DB 機能を使用してデータベースをプライマリからレプリカにコピーするか、ネットワークを使用しないコピー方式を使用するかは、状況に応じて判断してください。

レプリカ指名 (Nominate) 機能

元のプライマリ マシンを修復または交換している間も、RSA Authentication Manager システムの実行を続行するには、レプリカ管理ユーティリティの**レプリカ指名**機能を使用します。

レプリカから、使用しているプラットフォーム (Windows または UNIX) に適したレプリカ管理ユーティリテイを実行し、このレプリカを新しいプライマリ サーバとして指名することができます。

Authentication Manager で Windows 2000 または Windows 2003 が稼動している場合は、詳細について、96 ページの「レプリカの指名によるプライマリのハードウェアの交換」を参照してください。UNIX の場合は、144 ページの「レプリカの指名によるプライマリのハードウェアの交換」を参照してください。

エージェント ホスト /Authentication Manager アーキテクチャ

RSA Authentication Manager ソフトウェアを Windows システムで実行すると、TCP/IP ネットワーク上のさまざまなリソースを RSA SecurID で保護することができます。たとえば、ローカル マシン、ドメイン コントローラ、ファイアウォール、ルータ、VPN (virtual private network)、Web サーバなどを保護できます。

RSA SecurID 認証の保護を受けるには、RSA Authentication Agent ソフトウェアを実行するコンピュータや他のデバイスを、RSA Authentication Manager データベースにエージェント ホストとして登録しなければなりません。

Authentication Manager データベースに登録される各エージェント ホストには、そのエージェント ホストへのアクセスが承認されているRSA SecurIDユーザのリストを割り当てることができます。このリストを作成するには、エージェント ホストでユーザをアクティブ化するか、ユーザをエージェント ホストでアクティブ化されたグループのメンバにします。また**オープン** エージェント ホストを指定することもできます。オープン エージェント ホストでは、特定のユーザやグループをアクティブ化する必要はありません。

次の表は、エージェント ホストの設定に応じて、どのカテゴリのユーザがアクセスできるかを示しています。オープン エージェント ホストでは、必要に応じて、ローカルで認識されないユーザを他のレルムで検索するように設定できることに注意してください。ただし、これらのユーザは、RSA Authentication Manager データベースに登録されているレルムに属していなければなりません。

エージェント ホストの設定	ローカル データベースの登録ユーザ	外部ユーザ
アクティブ化されたユーザとグループのリストを使用する場合	アクティブ化されている有効なユーザ、およびアクティブ化されているグループのメンバに対してオープンです。	ユーザのレルムがローカルに登録されている場合、アクティブ化されている有効なユーザ、およびアクティブ化されているグループの有効なメンバに対してオープンです。
オープンであり、登録されているレルムでユーザを検索するように設定されている場合	有効なすべてのユーザに対してオープンです。	ユーザのレルムがローカルに登録されている場合は、有効なすべてのユーザに対してオープンです。
オープンのみの場合	有効なすべてのユーザに対してオープンです。	どのユーザもアクセスできません。

エージェントとエージェント ホスト上でのアクティブ化については、第 3 章「エージェントとエージェント ホスト上でのアクティブ化」を参照してください。

RSA Authentication Agent ソフトウェアがエージェント ホストにインストールされているか、またはルータ、コミュニケーション サーバ、VPN サーバ、およびファイアウォールに統合されている場合には、認証プロセスの一部として次の機能を実行します。

- ログオン試行に対して、RSA SecurID PASSCODE を要求します。
- ユーザのコンピュータがオンライン (ネットワークに接続された状態) の場合は、ユーザがエージェント ホストのリソースを使用することを承認されているかどうか確認するために、ユーザの応答を Authentication Manager に送信します。
- ユーザのコンピュータがオフライン (ネットワークから切断された状態) の場合は、ユーザのマシンにインストールされている他の RSA Security ソフトウェアと連携して、オフライン認証を実行します (RSA Authentication Agent 6.1 のみ)。
- ユーザのマシンがネットワークに再接続されると、ログ データベースの統合のために、オフライン認証ログ データを RSA Authentication Manager に送信します。
- 他のマシンがAuthentication Managerになりすましてセキュリティ データを取得できないようにするために、RSA Authentication Manager が本物であるかどうか確認します。
- エージェント ホストとAuthentication Managerの間で送信されるメッセージを暗号化 / 復号化します。

RSA Authentication Manager は次の機能を提供します。

- エージェント ホストに認証サービスを継続的に提供します。
- ネットワークから頻繁に切断されるコンピュータにオフライン認証データを提供します(RSA Authentication Agent 6.1がインストールされているコンピュータのみ)
- 他のレルムのユーザに対してレルム間認証サービスを提供します。
- Authentication Manager システムに対して管理機能を提供します (プライマリのみ、レプリカでの管理機能は制限されています)。
- RSA SecurID 認証および管理アクティビティをリアルタイムに監視します。

自動負荷分散機能

RSA Authentication Agent v5.0 以降では、Authentication Manager をポーリングし、認証要求にもっとも速く応答する Authentication Manager を選ぶことで、自動的に負荷を分散できます。エージェントが特定の Authentication Manager に高い優先順位を割り当てるように設定することで、手動で負荷分散することもできます。詳細については、67 ページの「エージェント ホストによる負荷分散」を参照してください。

ファイアウォールを介した Authentication Manager とエージェント ホストの通信

RSA Authentication Agent ホストは、Authentication Manager のエイリアス IP アドレスを最大 3 つ使用して、1 つ以上のファイアウォールの反対側にある RSA Authentication Manager と通信できます。これらのファイアウォールのいずれかが認証要求を受信すると、Authentication Manager のエイリアス IP アドレスのいずれかを認識し、確立されたプロトコルを使用して、そのエイリアスと有効な IP アドレスを照合します。エイリアス Authentication Manager IP アドレスの詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』を参照してください。

ファイアウォールによって Authentication Manager から分離されたエージェント ホストの構成ファイルには、使用できるエイリアスのリストが登録されていなければなりません。ファイアウォールを介して旧バージョンのエージェント ホストを認証する際に、データベースに使用可能なエイリアスとして登録されていないエイリアス IP アドレスを使用する場合は、Configuration Record Editor を使用して、*sdconf.rec* ファイルのアクティング マスタ Authentication Manager とアクティング スレーブ Authentication Manager のフィールドを編集してください。詳細については、74 ページの「旧バージョンのエージェント ホスト」を参照してください。

旧バージョンのエージェントのサポート

RSA Authentication Manager 5.0 (およびそれ以降) アーキテクチャでは、以下の 2 つの変更を行ったことにより、以前のメジャー バージョンより認証速度が向上しています。1 つは複数の認証レプリカの使用であり、もう 1 つは、認証要求にもっとも速く応答するレプリカを選択する RSA Authentication Agent ソフトウェアの新機能です。新しいエージェント ソフトウェアはレルム内のすべてのレプリカを認識するので、認証要求をその中のどのレプリカにでも送信できます。

v5.0 より前の RSA ACE/Agent ソフトウェアを実行するエージェント ホストにはこの機能がなく、ユーザが認証を受けることができるのはマスタまたはスレーブでだけです。これは、エージェント ホストの構成ファイル(**sdconf.rec**)でこれらの2つのAuthentication Manager だけが識別されるからです。

旧バージョンのエージェントの問題点の詳細については、74 ページの「旧バージョンのエージェント ホスト」を参照してください。

レルム間モデル

RSA Authentication Manager では、プライマリとそのレプリカの各インスタンスをレルムと呼んでいます。1 つのシステム構成に複数のレルムを持つことができ、各レルムは、他のレルムのユーザを認証し、アクセスを許可するように設定できます。これを**レルム間**認証と呼びます。

重要：ここでは、複数のレルムがある環境に関して説明します。この説明は、RSA Authentication Manager アドバンスド ライセンスを購入されたお客様だけを対象としています。ライセンス オプションの詳細については、付録 A「ライセンス」を参照してください。

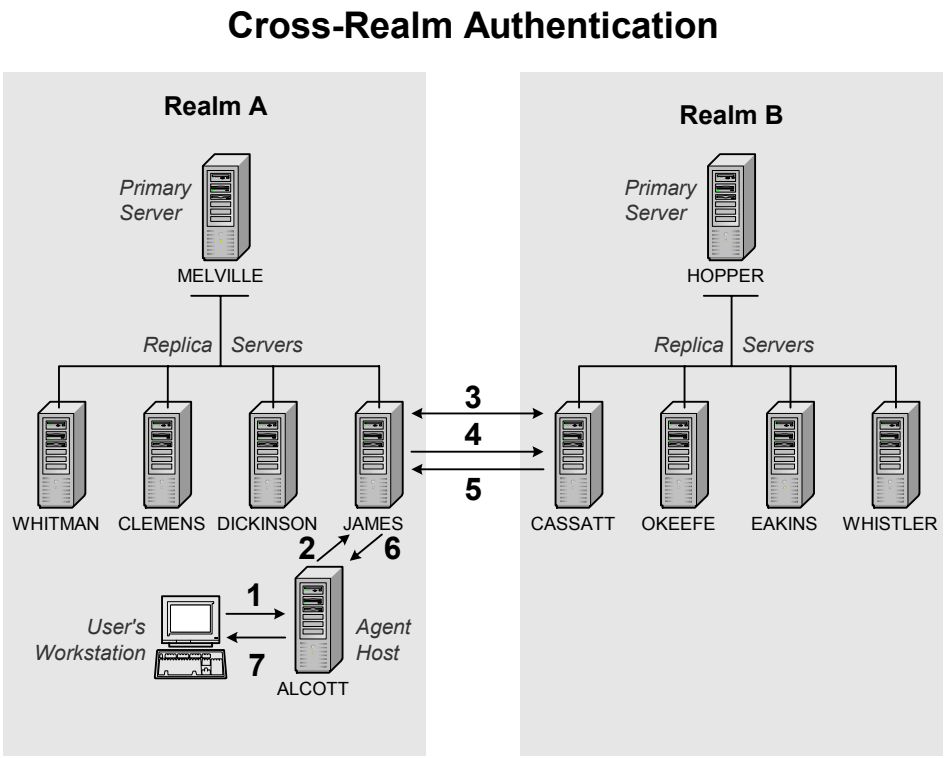
導入環境によっては、複数のレルムが必要でないこともあります。RSA Authentication Manager 6.1 では、各プライマリに対してレプリカを最大 10 台使用でき、1 つのレルムで処理できる負荷を大幅に増大できます。最初は 1 台のプライマリと 2 台のレプリカだけを使用し、ユーザが増加したら、必要に応じて複数の場所にレプリカを追加することができます。

ユーザ数が非常に多い場合や、遠く離れたサイトにプライマリ Authentication Manager をインストールする場合は、複数のレルムを使用するとよいでしょう。この場合は、他のレルムのユーザの受け付けと認証を実行できるように、各レルムを構成する必要があります。

ユーザの**ホーム** レルムとは、ユーザがデータベースに追加され、そのユーザのユーザ レコードが格納されているレルムのことです。**リモート** レルムとは、そのレルムのデータベースにレコードが格納されていないユーザを認証する任意のレルムを指します。

データベースにレルムを追加する場合、リモート レルムのプライマリと、そのレルムからのユーザが認証を受けるリモート レルム内の Authentication Manager を 1 台または 2 台指定しなければなりません。また、ローカル レルムのユーザがリモート レルムにアクセスしたときに、認証を受けるローカル レルム内の Authentication Manager を 1 台または 2 台指定する必要があります。レルム間認証用に各レルムに 2 台の Authentication Manager を指定する場合、1 台は優先 Authentication Manager として設定し、もう 1 台は、優先 Authentication Manager が利用できなくなった場合に使用されるフェールオーバ Authentication Manager として設定してください。

次の図は、レルム間認証の手順を示しています。



1. レルム B のユーザが、レルム A のエージェント ホスト ALCOTT にログオンしようとしました。
2. エージェント ホストはレプリカ JAMES に要求を渡し、そこで RSA Authentication Manager 6.1 ソフトウェアがデータベースをチェックしましたが、ユーザが見つかりません。
3. Authentication Manager JAMES はレルム A のデータベースに登録されている各レルムの優先 Authentication Manager (優先 Authentication Manager を利用できない場合はフェールオーバ Authentication Manager) をポーリングして、目的のユーザのユーザ レコードが格納されている Authentication Manager (レルム B の CASSATT) を検索します。
4. Authentication Manager JAMES は認証要求を CASSATT に送信します (CASSATT を利用できない場合、その要求は OKEEFE に送られます。OKEEFE はレルム レコードにフェールオーバ Authentication Manager として登録されています)。
5. レルム B の CASSATT の RSA Authentication Manager 6.1 ソフトウェアはユーザを認証し、この情報をレルム A の JAMES に戻します。

6. JAMES はユーザが認証を受けたことをエージェント ホスト ALCOTT に通知します。
7. ALCOTT の RSA Authentication Agent は、ユーザにネットワークへのアクセスを許可します。

操作手順：[Realm] > [Add Realm] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

RSA Authentication Manager 6.1 の新機能

RSA Authentication Manager Control Panel

展開した [RSA Authentication Manager Control Panel] では、インストールの種類に応じて、RSA Authentication Manager サービスの起動と停止、インストール情報の表示、さまざまなメンテナンス作業などを行うことができます。

[RSA Authentication Manager Control Panel] にアクセスするには、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。

各操作の詳細については、本書および各プラットフォーム用の『インストール ガイド』、ヘルプの対応する箇所を参照してください。

グループ認証設定

グループを追加または編集するときに、そのグループのすべてのメンバに対して [Offline Authentication and Windows Password Integration] を有効に設定できます。これらの機能を使用するには、そのエージェントに RSA Authentication Agent 6.1 for Microsoft Windows をインストールし、グループをアクティブ化する必要があります。

Funk Software が提供する機能を備えた RSA RADIUS Server 6.1

RSA Authentication Manager 6.1 には、Funk Software が提供する新しい RSA RADIUS サーバが搭載されており、次のような拡張機能を提供します。

- RSA SecurID 二要素認証の使用による従来の認証およびワイヤレス認証のサポート
- PAP、EAP-PEAP-GTC、EAP-TTLS-PAP、および EAP-TTLS-GTC プロトコルのサポート
- RSA Authentication Manager プライマリ / レプリカ モデルを反映したアーキテクチャ

RSA RADIUS サーバ 6.1 の管理作業の大部分は、独自のアドミニストレーション アプリケーションから実行します。アドミニストレーション アプリケーションを起動するには、RSA Authentication Manager Host Mode で [RADIUS] > [Manage RADIUS Server] の順にクリックします。RSA Authentication Manager を通じて、ユーザとグループにプロファイルを割り当てます。RSA RADIUS サーバ アプリケーションを起動するには、RSA Authentication Manager データベースでトークンまたは PASSCODE を割り当てておく必要があります。

メモ：RSA RADIUS サーバ内のプロファイルの名前はすべて、RSA Authentication Manager 内のプロファイル名と対応している必要があります。

プロファイルの詳細については、ヘルプを参照してください。

RSA Authentication Manager 6.1 へのアップグレードの一部として RSA RADIUS 6.1 にアップグレードする操作については、ご使用のプラットフォームの『インストール ガイド』を参照してください。RSA RADIUS 6.1 のインストールと管理については、『RSA RADIUS Server 6.1 Administrator's Guide』を参照してください。

RSA Authentication Manager ライセンス

RSA Authentication Manager には、ベース ライセンスとアドバンスド ライセンスの 2 種類のパーマネント ライセンスがあり、インストール時、および日常の一般的な操作やアドミニストレーションにライセンスの制限が適用されます (RSA Authentication Manager には、評価用ライセンスというテンポラリのトライアル ライセンスも用意されています)。

RSA Authentication Manager ベース ライセンスでは、次の条件で RSA Authentication Manager ソフトウェアを使用する権利が与えられます。

- RSA Authentication Manager データベースには、購入した「ユーザ数の範囲」で指定される数まで、ユーザを登録できます。アクティブ ユーザの詳細については、付録 A「ライセンス」を参照してください。
- 1 台のプライマリと 1 台のレプリカ構成を 1 つ (1 レルム) 稼動できます。

  レプリカを 2 台以上導入する場合やプライマリを 2 台以上導入する場合 (レルムが複数の場合など) は、アドバンスド ライセンスをご購入ください。

RSA Authentication Manager アドバンスド ライセンスでは、次の条件で RSA Authentication Manager ソフトウェアを使用する権利が与えられます。

- RSA Authentication Manager データベースには、購入した「ユーザ数の範囲」で指定される数まで、ユーザを登録できます。
- 1台のプライマリに対して最大10台のレプリカ構成を6つ(6レルム)稼動できます。

  7 つ以上のレルムにソフトウェアをインストールする場合は、複数のアドバンスド ライセンスをご購入ください。
- 正常に動作することが確認されている高可用性ハードウェア　システムにインストールできます。現在、高可用性を実現するために、Sun Solaris 9.0 で Veritas Cluster Server がサポートされています。

ライセンスとアクティブ ユーザの詳細については、付録 A「ライセンス」を参照してください。

2 RSA Authentication Manager Administration アプリケーションの使用

この章では、RSA Authentication Manager をセットアップするための作業について説明し、RSA Authentication Manager Host Mode についても簡単に説明します。

Windows では、すべてのサブディレクトリ、データベース、およびプログラム ファイルは、インストール時に指定したディレクトリにインストールされます。デフォルトのインストール ディレクトリは**c:¥ace**です。プログラム ファイルを格納するサブディレクトリは **prog** であり、データ ファイルを格納するサブディレクトリは **data** です。

UNIX では、すべてのディレクトリ、データベース、およびプログラム ファイルは、インストール時に指定した最上位のディレクトリにインストールされます。プログラム ファイルを格納するサブディレクトリは **ace/prog** であり、データを格納するサブディレクトリは **ace/data** でなければなりません。

本書では、次の表記規則を使用します。

- ***ACEPROG*** は、Authentication Manager プログラム ファイルを格納するディレクトリへのフルパス名を表します。
- ***ACEDATA*** は、Authentication Manager データベースを格納するディレクトリへのフルパス名を表します。

RSA Authentication Manager の管理者は、インストール後にこの章で説明するセットアップ作業を実行する必要があります。これらの作業が正しく終了すると、ネットワーク リソースは RSA SecurID 認証によって保護されるようになります。

アドミニストレーション権限

アドミニストレーション権限とは、ユーザが特定のレルム、サイト、またはグループに対して実行できる一連のタスクを定義するテンプレートです。アドミニストレーション権限を割り当てると、管理者の権限が、特定の種類のアクション、および RSA Authentication Manager データベースの特定領域に制限されます。権限を定義した後、選択した複数の管理者に権限を割り当てることができます。管理者の各ユーザ レコードに同じタスクや制限を何度も指定する必要はありません。

注意：アドミニストレーション権限の定義または割り当ての権限が悪用されると、ネットワークのセキュリティに重大な問題が発生する可能性があります。この権限は、信頼のおけるスタッフのみに与えるようにしてください。

アドミニストレーション権限は、次の 2 つの要素で構成されます。

アドミニストレーション スコープ。権限が割り当てられた管理者が管理できるサイト、エージェント ホスト、グループ、ユーザ、およびトークンを指定します。詳細については、次の「アドミニストレーション スコープ」を参照してください。

アドミニストレーション タスク リスト。特定の権限が割り当てられた管理者が、アドミニストレーション スコープ内で実行できる名前付きのタスク セットです。詳細については、31 ページの「タスク リスト」を参照してください。

特定のアドミニストレーション スコープを特定のタスク リストと組み合わせると、管理者が RSA Authentication Manager データを制御できる権限が的確に制限されます。

アドミニストレーション スコープ

アドミニストレーション スコープは、アドミニストレーション権限の 2 つの構成要素の 1 つであり、権限が割り当てられた管理者が管理できるサイト、エージェント ホスト、グループ、ユーザ、およびトークンを指定します。

アドミニストレーション スコープには 3 つのカテゴリがあります。それは、レルム、サイト、およびグループです。各カテゴリは、システム内の 1 つ以上のレベルで管理者の権限を定義します。これらのカテゴリの内部でも、アドミニストレーション スコープの適用対象のレルム、サイト、またはグループを指定することで、スコープを変更できます。たとえば、レルム管理者は 1 つ以上のレルムを制御でき、サイト管理者やグループ管理者についても同様の原則が適用されます。

アドミニストレーション スコープのカテゴリは階層構造になっており、レベルの高い権限の下に、それよりレベルの低い権限が含まれます。たとえば、レルム管理者はレルム内のサイトとグループを管理できますが、グループ管理者の権限は、自分のグループ内に限定されます。しかし、レルム管理者であっても、割り当てられたアドミニストレーション スコープに含まれていないレルム内のサイトやグループに対する権限はありません。RSA Authentication Manager は、このスコープ定義に従って、管理者の画面上に表示されるサイト名、グループ名、ユーザ名、エージェント ホスト名、トークン名を制限するので、その管理者に割り当てられているスコープの範囲内のデータにしかアクセスできません。

アドミニストレーション スコープの 3 つの基本カテゴリは、割り当てれらた特定のレルム、サイト、またはグループ内で、次のようにアドミニストレーション権限を分配します。

- **レルム管理者**は、管理しているレルム内のすべてのサイト、グループ、ユーザ、エージェント ホスト、およびトークン (割り当てられているかどうかとは無関係) を表示し、編集できます。
- **サイト管理者**は、サイトの追加および削除を行うことができません。管理しているサイトをはじめ、そのサイトに属するグループ、ユーザ、エージェント ホスト、および割り当て済みのトークンの表示と編集は可能です。また、サイト管理者は、Authentication Manager データベースでまだ割り当てられていないすべてのトークンを表示し、編集することもできます。どのグループまたはサイトにも属さないすべてのエージェント ホスト、ユーザ、およびトークンの表示と編集もできます。
- **グループ管理者**は、グループの追加および削除を行うことができません。管理しているグループをはじめ、そのグループに属するユーザ、エージェント ホスト、および割り当てられたトークンを表示し、編集することはできます。また、グループ管理者は、そのグループ内のユーザに割り当てられているすべてのトークン、および Authentication Manager データベースでまだ割り当てられていないすべてのトークンの表示と編集も可能です。どのグループまたはサイトにも属さないすべてのエージェント ホスト、ユーザ、およびトークンの表示と編集もできます。

タスク リスト

タスク リストとは、アドミニストレーション権限の 2 つ目の構成要素です。タスク リストは、特定の権限が割り当てられた管理者が、アドミニストレーション スコープ内で実行できる名前付きのタスク セットです。タスクはユーザ インタフェースのコマンドに対応します。管理者に割り当てられている権限のタスク リストに含まれていないコマンドは、その管理者に表示されるメニューでは灰色表示になります。

RSA Authentication Manager では、3 つのタスク リストがあらかじめ定義されています。それは Realm (レルム)、Site (サイト)、および Group (グループ) です。これらのタスク リストには、レルム管理者、サイト管理者、またはグループ管理者にとって必要なタスクが含まれています。

また、この定義済みのタスク リストの修正版を作成したり、まったく新しいタスク リストを作成して、レルム内の管理者に割り当てることもできます。このように権限をカスタマイズできるので、管理者の権限を的確に制御できます。ただし、割り当てられたアドミニストレーション スコープで禁止されているタスクを管理者に許可することはできません。管理者の権限は、割り当てられたアドミニストレーション スコープに従って制限され、タスク リストの内容に関係なく、スコープの定義で許可されたタスクだけが実行可能であることに注意してください。

アドミニストレーション スコープとタスク リストの組み合わせ

アドミニストレーション権限とは、ユーザに割り当てるアドミニストレーション スコープとタスク リストの組み合わせです。たとえば、複数のサイトを所有する大規模な企業で、New York サイトの管理者のアドミニストレーション権限を割り当てる場合について考えてみましょう。

- まず、New York サイトに制限されるサイト管理者のアドミニストレーション スコープを割り当てます。このように割り当てると、ユーザには、New York サイトに関連付けられているグループ、ユーザ、エージェント ホスト、およびトークンを管理する権限が与えられますが、他のサイトに関連付けられている同様のリソースを管理することはできません。
- 次に、あらかじめ定義されているサイト管理者のタスク リストをユーザに割り当てます。このようにすると、ユーザはサイト管理者にとって必要なタスクを実行できます。たとえば、アドミニストレーション権限の割り当て、トークンのインポートとエクスポート、グループの追加と削除、およびサイトの編集などを実行できます。

さらに、もう 1 人別のアシスタント管理者を New York サイトに割り当てるとします。しかし、この管理者には、プライマリ管理者より制限の厳しいタスク リストを割り当てます。たとえば、あらかじめ定義されている Group Administrator タスク リストやカスタム タスク リストを割り当てることができます。このように割り当てると、アシスタント管理者は、New York サイトに関連付けられたすべてのリソースに対して、特定のタスクだけを実行できるようになります。たとえばユーザ、トークン、およびグループを編集することはできますが、プライマリ サイト管理者に許可されているすべてのタスクを実行できるわけではありません。

タスク リストの作成と、ユーザにタスク リストを割り当てる方法の詳細については、ヘルプの「Creating a Task List」と「Assigning Administrative Roles」を参照してください。アドミニストレーション タスクとそのサブタスクの一覧については、ヘルプの「Categories of Tasks」を参照してください。

操作手順：[User] > [Edit User] の順に選択し、ユーザを選択してから [OK] をクリックします。[Edit User] ダイアログボックスで [Administrative Roles] をクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

重要な管理ツール

次の機能は、RSA Authentication Manager エージェント ホスト、トークン、およびユーザを効率よく管理するのに役立ちます。

システム デザイン ツール

オープン エージェント ホスト

オープン エージェント ホストは、すべてのエージェント タイプでサポートされます。エージェント ホストが**オープン**の場合は、ユーザをエージェント ホストで直接アクティブ化する必要がなく、エージェント ホストでアクティブ化されるグループのメンバにする必要もありません。Authentication Manager データベースに登録されているユーザであれば、どのユーザでもオープン エージェント ホストで認証を受けることができます。詳細については、23 ページの「エージェント ホスト /Authentication Manager アーキテクチャ」を参照してください。

メモ：RSA Authentication Agent 6.0 または 6.1 でオフライン認証を有効に設定し、しかも一部のユーザだけがこの機能を利用できるように設定する場合は、エージェント ホスト単位でこの機能を制御できます。この場合、オープン エージェント ホストを使用する必要はありません。オフライン認証 (および関連) 機能の詳細については、57 ページの「オフライン認証およびパスワードの統合の設定」を参照してください。

エージェント ホストの自動登録と更新

自動化されたエージェント ホストの登録機能と更新機能を使用すると、新規エージェント ホストは自分自身を Authentication Manager に対して登録することができ、既存のエージェント ホストは自分の IP アドレスや *sdconf.rec* ファイルを自動的に更新できるため、管理作業を削減できます。64 ページの「エージェント ホストの自動登録 / 更新」を参照してください。

統合されたログの記録

すべてのログ メッセージは、プライマリに統合されます。レプリカでのアクティビティによってログ メッセージが生成されると、メッセージは最終的にプライマリに送られ、プライマリ ログ データベースに記録されます。認証が混みあっている時間帯は、これらの**デルタ レコード**をプライマリ データベースへ統合する処理の優先順位が低くなりますが、最終的には統合されます。

External Authorization

External Authorization を使用すると、ユーザにネットワーク リソースへのアクセスを許可する前に、追加条件を適用できます。External Authorization による条件は、RSA Authentication Managerによる認証を補足しますが、それに代わるものではありません。209 ページの「承認手順のカスタマイズ」を参照してください。

レポート作成ユーティリティ

標準レポート (変更も削除もできないレポート) の実行、およびカスタム レポートの作成と実行が可能です。監査証跡レポートは **sdlog** データベースに対して実行されます。トークン統計レポートは **sdserv** データベースに対して実行されます。詳細については、169 ページの「RSA Authentication Manager レポート作成ユーティリティ (Windows)」、または 178 ページの「RSA Authentication Manager レポート作成ユーティリティ (UNIX)」を参照してください。

カスタム クエリ

カスタム クエリ機能を使用すると、提供されるサンプル SQL クエリを利用するか、または独自のクエリを作成して、RSA Authentication Manager ログおよびユーザ データベースからデータを収集して表示できます。詳細については、187 ページの「カスタム SQL クエリの作成と実行」を参照してください。

アドミニストレーション支援ツール

RSA Authentication Manager Control Panel

[RSA Authentication Manager Control Panel] では、インストールの種類に応じて、RSA Authentication Manager サービスの起動と停止、インストール情報の表示、さまざまなメンテナンス作業などを行うことができます。[RSA Authentication Manager Control Panel] にアクセスするには、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。各操作の詳細については、『RSA Authentication Manager 管理者ガイド』、『RSA Authentication Manager 6.1 for Windows インストール ガイド』、およびヘルプを参照してください。

トークンの一括交換

トークンの一括交換機能を使用すると、大量のユーザ (たとえば、間もなく有効期限が切れるトークンを保有しているユーザ) のトークンを効率よく交換できます。詳細については、ヘルプの「Replacing Many Tokens Using a Batch Procedure」を参照してください。

RSA SecurID ソフトウェア トークンの管理

RSA SecurID ソフトウェア トークンを発行したり、失効にしたりするには、[Token] メニューを使用します。ソフトウェア トークンはソフトウェア ベースのセキュリティ トークンであり、ユーザのコンピュータや PDA、携帯電話などにインストールします。詳細については、ヘルプの「Issuing Software Tokens」を参照してください。

ログ データベースの自動メンテナンス

スケジューリングと定義のオプションを使用して、ログ レコードの削除やアーカイブして保存するように RSA Authentication Manager を構成できます。設定したスケジュールと方法で、定期的なバックアップとメンテナンスが自動的に行われます。詳細については、153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください。

テンポラリ パスワード

ユーザがトークンを紛失した場合は、テンポラリ パスワードを割り当てることができます。このパスワードは、新しいトークンがユーザに与えられるまで使用できます。詳細については、124 ページの「紛失したトークンの代わりに使用するテンポラリ パスワード」を参照してください。

Remote Administration

Remote Administration を使用すると、直接接続していなくても、RSA Authentication Managerデータベースを管理できます。Remote Administration ソフトウェアは、Windows Server 2003、Windows XP Professional、および Windows 2000 (Advanced、Server、Professional) マシンで動作します。

Remote Administration 機能を使用すると、ローカル レルムや登録されているリモート レルムの Windows データベースや UNIX データベースを管理できます。詳細については、38 ページの「Remote Administration」を参照してください。

Quick Admin

RSA Authentication Manager Quick Admin アプリケーションを使用すると、ヘルプ デスク管理者は Web ブラウザを利用して、RSA Authentication Manager データベース内のユーザ、トークン、および拡張レコード データを表示および変更できます。詳細については、44 ページの「Quick Admin を使用した Web ベースのアドミニストレーション」を参照してください。

イベント ログ内の監査ログ メッセージ

現在のログオン、ユーザ名、影響を受けるトークン、エージェント ホスト名、Authentication Manager の名前などの選択条件をもとに、特定の監査ログ メッセージがイベント ログに記録されるように指定できます。詳細については、166 ページの「システム ログ内の Authentication Manager イベントの監視」を参照してください。

カスタム定義拡張レコード

RSA Authentication Manager システムの要素 (トークン、ユーザ、グループ、エージェント ホスト、ログ) を定義するデータベース レコードには、管理者が定義したい追加情報を含む拡張レコードを追加できます。たとえば、ユーザの自宅の電話番号や社員番号のレコードを登録できます。詳細については、98 ページの「カスタム定義データ (拡張レコード) のメンテナンス」を参照してください。

RSA Authentication Manager Host Mode の概要

RSA Authentication Manager Host Mode を使用すると、さまざまな管理作業を実行できます。たとえば、ユーザ、エージェント ホスト、レルム、サイト、グループの追加や編集、オフライン認証、ドメイン サーバ認証、およびターミナル サービス認証の有効化、ログイン パスワードの統合の有効化、RSA Authentication Manager のアクティビティに関するレポートの生成などを実行できます。このアプリケーションはホスト モード (Windows のみ) またはリモート モードで動作します。

メモ：UNIX プラットフォームでは、**sdadmin** プログラムを使用することで、RSA Authentication Manager ソフトウェアの多くの機能にアクセスできますが、Remote Administration を使用すると、グラフィカル ユーザ インタフェースを介して RSA Authentication Manager データベースを管理できます。さらに、Remote Administration はすべての管理機能にアクセスできる唯一の方法です。詳細については、38 ページの「Remote Administration」を参照してください。

ホスト モードの場合、RSA Authentication Manager データベースへの直接接続が必要なので、RSA Authentication Manager Host Mode はプライマリで実行する必要があります。リモート モードの場合は、Remote Administration サービスを通じて、Windows 2000、Windows XP、および Windows 2003 マシンから実行できます。このアプリケーションでは、複数のセッションを取り扱うことができるようにするために、使用中のレコードをロックして、複数のセッションからレコードが変更されないようにしています。

データベースをリモートから管理するには、その前にプライマリで特定の作業を直接実行する必要があります。詳細については、ご使用のプラットフォームの『インストール ガイド』を参照してください。

リモートからの RSA Authentication Manager Host Mode 実行の詳細および手順については、38 ページの「Remote Administration」を参照してください。

RSA Authentication Manager Host Mode をホスト モードで実行するには

Windows マシンで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Host Mode] の順にクリックします。

RSA Authentication Manager Host Mode のメイン メニューが表示されます。

RSA Authentication Manager Host Mode の終了

RSA Authentication Manager Host Mode を終了するには、[File] メニューの [Exit] をクリックします。

重要：ホスト モードまたはリモート モードで RSA Authentication Manager Host Mode を実行している間は、絶対にマシンから離れないでください。マシンから離れるときは、RSA Authentication Manager Host Mode を終了して、ログオフしてください。RSA Authentication Manager Host Mode を実行したまま放置しておくと、マシンにアクセスできる人なら誰でも、管理者になりすまして、Authentication Manager データを変更することができてしまいます。

言語サポート (Windows)

RSA Authentication Manager ソフトウェアでは、多くの ISO Latin-1 言語および日本語を含むアジア言語の文字セットがサポートされています。特定の言語をサポートするには、Windows システムの設定が必要です。また、RSA Authentication Manager データベースには、英語の文字しかサポートされていないフィールドがいくつかあります。

ISO Latin-1 言語

- 英語
- フィンランド語
- フランス語
- ドイツ語
- ノルウェー語
- スペイン語
- スウェーデン語

アジア言語

- 中国語 (簡体字および繁体字)
- 日本語 (カタカナ、ひらがな、および漢字)
- 韓国語

Authentication Managerデータベースで英語以外の ISO Latin-1 言語のいずれかをサポートするには、RSA Authentication Manager ソフトウェアをインストールする前に、目的の言語を使用するように Windows 2000 または Windows 2003 システムを設定しなければなりません。Authentication Manager データベースで、中国語、日本語、または韓国語をサポートするには、システムで適切なバージョンの Windows を実行しなければなりません。

英語以外のシステムに RSA Authentication Manager をインストールした後、英語版に戻すことはできません。このような変更を試みた場合、RSA Authentication Manager データベースには、英語システムで表示できない英語以外の文字がそのまま残されます。

サポートされている Latin-1 言語のいずれかを使用するためのシステムの設定の詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』を参照してください。

重要 : 言語のサポートと使用は、RSA Authentication Manager システム全体で統一しておかなければなりません。すべてのレルムのすべてのプライマリ Authentication Manager、レプリカ Authentication Manager、およびリモート アドミニストレーション マシンで、同じ言語をサポートしなければなりません。各レプリカ データベースの言語は、そのプライマリ データベースの言語と同じでなければなりません。また、Authentication Manager データベースの言語と異なる言語をサポートするリモート アドミニストレーション マシンから、Authentication Manager データベースを管理することはできません。英語以外の言語が使用されているレルムのユーザを英語レルムで認証することはできません。

英語以外の言語を入力できるデータ フィールド

RSA Authentication Manager データベースのほとんどのテキスト フィールドは、英語以外の言語の入力に対応しています。しかし、次に示すテキスト フィールドでは、1 バイトの英字しか使用できません (入力できたとしてもサポートしていません)。

ダイアログ ボックス	テキスト フィールド
[Add User]、[Edit User]	[Default Login]
[Add Agent Host]、[Edit Agent Host]	[Name]
[Add Realm]、[Edit Realm]	[Primary Name]
[Add Realm]、[Edit Realm]	[Replica Name]

数値フィールドにはアラビア数字 (1 バイト) しか入力できません。

MS-IME による日本語の入力

RSA Authentication Manager Host Mode では、Authentication Manager データベースのほとんどのテキスト フィールドに日本語 (カタカナ、ひらがな、および漢字) を入力できます。ただし、前のセクション「英語以外の言語を入力できるデータ フィールド」の一覧に示したフィールドには日本語を入力できません。

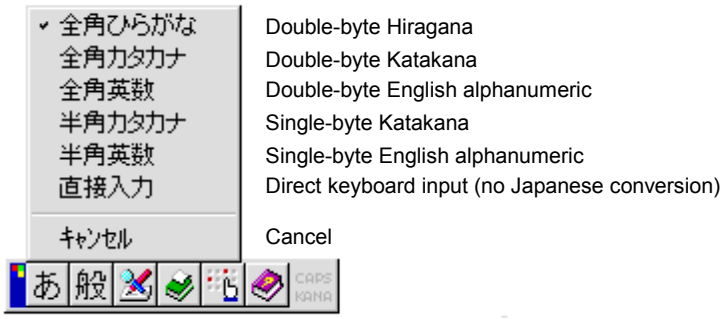
日本語を入力するには、Windows 2000、Windows XP、または Windows Server 2003 の日本語版を実行しているマシンを使用する必要があります。

このセクションでは、MS-IME (Microsoft Input Method Editor) を使用して日本語を入力する方法について説明します。MS-IME の使い方の詳細については、MS-IME 日本語入力システムのヘルプを参照してください。

ひらがなとカタカナ

サポートされている日本語版 Windows を実行するワークステーションから RSA Authentication Manager Host Mode のテキスト フィールドに日本語を入力するには、MS-IME を起動し、入力モードを「ひらがな」または「カタカナ」に設定します。MS-IME を起動するには (まだ起動されていない場合)、標準 101 キーボードで Alt + ~ を押すか、日本語 106 キーボードで Alt + [半角 / 全角] を押します。MS-IME が起動されると、次の図に示すフローティング ツールバーが画面に表示されます。

MS-IME ツールバーの左端のボタンをクリックすると、ドロップダウン メニューが表示されます。このメニューには、MS-IME でサポートされるすべての入力モードが表示されます。次の図を参照してください。



日本語を入力するには、入力カーソルをテキスト フィールドに置いて、[全角ひらがな]、[全角カタカナ]、[半角カタカナ] のいずれかを選択します。入力モードには、「かな」入力モードと「ローマ字」入力モードの 2 種類があります。

- かな入力モードでは、ひらがな / カタカナ文字はキーボードのキーに対応します。キーを押すと、入力モードに応じて、ひらがなまたはカタカナが画面に表示されます。
- ローマ字入力の場合は、日本語文字の読みをローマ字で入力します。MS-IME は入力されたローマ字を 1 文字のひらがなまたはカタカナに変換します。

かな入力またはローマ字入力を選択するには、ツールバーの 5 番目のボタンをクリックし、最初のタブを選択して、MS-IME の基本設定を変更します。プルダウン リストの 2 番目のフィールドで入力モードを適切なモードに設定します。106 キーの日本語キーボードを使用している場合には、Alt + [カタカナ ひらがな] を押すことにより、入力モードを切り替えることができます。かな入力モードを選択すると、ツールバーの KANA ステータスが有効になり、次の図に示すフローティング ツールバーが画面に表示されます。

ひらがなとカタカナから漢字への変換

漢字を入力するには、漢字の読みをカタカナまたはひらがなで入力します。カタカナまたはひらがなの音節を入力すると、それが点線の下線付きで画面に表示されます。漢字に変換するときは、適切な漢字が表示されるまで、101 キーボードではスペースバーを押し、106 日本語キーボードではスペースバーまたは [前候補 変換 (次候補)] キーを押します。ENTER を押すと、変換が確定して入力フィールドに入力されます。

漢字に変換するときに、4 つ以上の候補があるときは、すべての候補を示す選択リストが表示されます。上向き矢印または下向き矢印キーを使用して、適切な候補を反転表示します。ENTER を押すと、選択した漢字が入力フィールドに入力されます。

1 バイト フィールドへの文字の入力

メモ:2バイト文字に対応していないテキスト フィールドにテキストを入力する際も、RSA Authentication Manager Host Mode で MS-IME の使用を禁止するような措置は取られません。つまり、入力フォーカスがこれらのフィールドにある場合でも、入力モードを全角ひらがな、全角カタカナ、全角英数、半角カタカナのいずれかに切り替えることができます。しかし、2 バイト入力に対応していないフィールドに 2 バイト文字や半角カタカナを入力すると、このフィールドの入力を終了したときに、エラー メッセージが表示されます。したがって、2 バイト入力に対応していないテキスト フィールドでは、直接入力モードに設定しなければなりません。

他のモードから直接入力モードに設定するには、101 キーボードでは Alt + ~、日本語 106 キーボードでは Alt + [半角 / 全角] を押します。ツールバーの左端のボタンが直接入力モードを示すように変化します。次の図を参照してください。

MS-IME の他の機能の使い方については、ツールバーの右端のボタンを押して、MS-IME 日本語入力システムのヘルプを開き、表示される情報を参照してください。

Remote Administration

Remote Administration アプリケーションを使用すると、Windows リモート ホストから RSA Authentication Manager データベースに接続して管理できます。リモート ホストの **¥ace¥data¥realms¥[プライマリ サーバ名]** ディレクトリに **sdconf.rec** のコピーが必要です。このディレクトリは、Remote Administration のインストール時にホストに作成されます。

プライマリへの Remote Administration 接続では読み取りと書き込みが可能なので、データベースのレコードを変更できます。レプリカへの接続は読み取り専用となります。レポートを実行し、ログおよびアクティビティ モニタを表示することはできますが、レコードを変更することはできません。

認証を受け、管理するレルムを選択すると、Remote Administration は、**sdconf.rec** に登録されている名前と IP アドレスを使用して、プライマリに接続します。管理しているレルム内の各 Authentication Manager が、RSA Authentication Manager Host Mode のメイン メニューの左上に表示されます。別の Authentication Manager に接続するには、その Authentication Manager の名前および IP アドレスの横のボタンをクリックします。

プライマリまたはレプリカに接続すると、Authentication Manager からリモート ホストのレルム ディレクトリに **failover.dat** というファイルが送信されます。このファイルには、Authentication Manager の IP アドレスに加えて、1 つのエイリアス IP アドレスも登録されています。次回、リモート ホストがその Authentication Manager に接続する場合は、**failover.dat** に指定されている IP アドレスを使用します。

Remote Administration 接続のリダイレクト

Remote Administration の接続は、次の場合にレプリカにリダイレクトされます。

- プライマリの IP アドレスが変更された場合。

- レプリカがプラマリとして指名された場合。
- プライマリが使用できない状態になった場合。

これらの状況では、**failover.dat** に指定されている元のプライマリの IP アドレスを使用して接続を確立できないことを説明するメッセージが表示されます。その後、Remote Administration は、**failover.dat** に指定されている、次に使用可能なレプリカに接続します。

Authentication Manager の IP エイリアスの管理

failover.dat に登録されている Authentication Manager のエイリアス IP アドレス情報は、Remote Administration のメイン メニューで目的の Authentication Manager を選択し、[Manage Server IP Address Aliases] をクリックすることで更新できます。[Manage Server IP Address Aliases] ダイアログ ボックスには、レルム内のすべての Authentication Manager が表示されます。Authentication Manager を選択した後、次のいずれかのボタンをクリックします。

- **[Auto Select]**。選んだ Authentication Manager のエイリアス IP アドレスが自動的に選択されます。
- **[Select Manually]**。選んだ Authentication Manager の対応するすべての IP アドレスの一覧から、エイリアスを選択できます。

メモ：名前によってホストとサービスの解決が許可されるように構成されている Authentication Manager に接続した場合は、RSA Authentication Manager Host Mode のメイン メニューに [Manage Server IP Address Aliases] ボタンは表示されません。詳細については、231 ページの「[Enable Features] (有効にする機能)」を参照してください。

Remote Administration は、次のどの状況でも使用できます。

- RSA Authentication Manager が Windows 2000 または Windows Server 2003 で動作している場合は、Windows 2000、Windows XP Professional、または Windows Server 2003 が稼動しているリモート ホストから、データベースを管理できます。
- RSA Authentication Manager が UNIX で動作している場合は、Windows 2000、Windows XP Professional、または Windows Server 2003 を稼動しているリモート ホストから、データベースを管理できます。

  メモ：UNIX プラットフォームでは、**sdadmin** プログラムを使用することで、RSA Authentication Manager ソフトウェアの多くの機能にアクセスできますが、Remote Administration を使用すると、グラフィカル ユーザ インタフェースを介して RSA Authentication Manager データベースを管理できます。さらに、Remote Administration はすべての管理機能にアクセスできる唯一の方法です。

Remote Administration セッションのアイドル時間が 12 時間以上続くと、エラー メッセージ「Encryption Error: -1 (暗号化エラー : -1)」が表示されることがあります。このメッセージは、セッションがタイムアウトしたことを示します。Remote Administration では、同時に 32 のセッションを稼動することができます。

リモート アドミニストレーション用のシステムの構成

UNIX システムでは、デフォルトでリモート アドミニストレーションが**許可されていません**。リモート アドミニストレーション用に UNIX システムを設定するには、Remote Administration アプリケーションのキャラクタベースのバージョンを使用する必要があります。UNIX プライマリで次のコマンドを入力します。

```
./sdadmin
```

リモート アドミニストレーション用に RSA Authentication Manager システムをセットアップするには

1. プライマリで、[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。
   [System Parameter] ダイアログ ボックスが表示されます。
2. [Allow remote administration] チェックボックスをオンにします。
3. RSA Authentication Manager が受け付ける認証方式を選択します。選択できる方式については、次のセクションで説明します。
4. ダイアログ ボックスを閉じ、変更を保存します。
5. トークンをリモート管理者に割り当てます。
6. 割り当てたトークンを配布します。

メモ : リモートから管理または使用する RSA Authentication Manager (プライマリまたはレプリカ) は、それぞれ、リモート アドミニストレーションに使用するマシン上にレコードが登録されている必要があります。リモートから管理または使用する Authentication Manager またはレルムに対して Remote Administration ソフトウェアをインストールする手順、およびレコードを追加する手順については、ご使用のプラットフォームの『インストール ガイド』を参照してください。

リモート管理者の認証

RSA Authentication Manager データベースをリモートから管理するには、管理者が Authentication Manager で認証を受けなければなりません。つまり、管理者はデータベースにトークン レコードを登録しておかなければなりません。

管理者はレルムごとに異なるトークンを使用するようにしてください。管理者が複数のレルムで同じトークンを使用すると、あるレルムで管理者がトークンコードを入力したときに、侵入者がそのコードを検出し、そのコードを使用して他のレルムで RSA Authentication Manager Host Mode にアクセスしたり、他のネットワーク リソースにアクセスできる危険性があります。

メモ : 管理者が認証時にデータベースを企業ファイアウォールの外側の任意の場所から管理することが**絶対ない**場合は、複数のレルムで 1 つのトークンを使用しても、危険性はそれほど高くなりません。しかし、このような使い方は望ましくありません。

認証方式の選択

各レルムのセキュリティ管理者は、レルム内でどの管理者認証方式を採用するかを決定します。

リモート管理者の認証のために使用できるトークンとパスワードの種類は、RSA Authentication Manager Host Mode の [Edit System Parameters] ダイアログ ボックスで設定します。

どの種類のトークンあるいはパスワードでも選択できますが、管理者はできるだけハードウェア トークンを使用してください。これは、ハードウェア トークンがもっとも安全だからです。ハードウェア トークンとしては、RSA SecurID PINPAD、スタンダード カード、およびキーホルダが提供されています。

認証の要求 (チャレンジ)

リモート管理者は他のユーザと同様に、認証プロセスを実行しなければなりません。異なるのは表示される画面だけです。そのため、認証についてすでに十分理解している場合には、次の手順を実行する必要はありません。

次の「通常のログオンと PASSCODE 入力要求」の操作手順は、RSA SecurID スタンダード カードまたはキーホルダを使用していることが前提となっています。PINPAD を使用している場合は、PASSCODE が要求されたときに、次の手順を実行してください (ただし、New PIN 手順のときは**例外**です)。

1. PINPAD に PIN を入力し、カードの下部にある菱形を押します。
2. トークンに表示されたトークンコードをキーボードから入力し、[OK] をクリックします。

通常のログオンと PASSCODE 入力要求

通常、認証ダイアログ ボックスは 1 つだけ表示され、その中に 2 つの入力要求が表示されます。トークンが New PIN モードの場合は、42 ページの「トークンが New PIN モードの場合の認証」を参照してください。

認証を受けるには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Remote Mode] の順にクリックします。

   [Select Server to Administer] ダイアログ ボックスが表示されます。
2. 管理するサーバを選択し、[OK] をクリックします。

   [Administrator Authentication] ダイアログ ボックスが表示されます。
3. ユーザ名を [Login] フィールドに入力し、PASSCODE を [PASSCODE] フィールドに入力します。

   PASSCODE とは、PIN と、トークンに表示されるトークンコードを組み合わせたものです。
4. [OK] をクリックします。

   PASSCODE が受け付けられると、RSA Authentication Manager Host Mode のメイン メニューが表示されます。ヘッダには、データベースが存在するプライマリの名前が表示されます。

   ネクスト トークンコードを要求するプロンプトが表示された場合は、次の「トークンがネクスト トークンコード モードの場合の認証」を参照してください。

トークンがネクスト トークンコード モードの場合の認証

PASSCODE を正しく入力しても、入力した人が正当なトークン保有者であることを確認するために、トークンに次に表示されるコード (ネクスト トークンコード) を要求するプロンプトが表示されることがあります。このプロンプトは、トークンがネクスト トークンコード モードであることを示します。

トークンがネクスト トークンコード モードのときに認証を受けるには

1. RSA SecurID トークンで、次のトークンコードが表示されるのを待ちます。
2. トークンコード**だけ**を入力してください。

   トークンコードが正しい場合は、最初に入力した PASSCODE が受け付けられ、RSA Authentication Manager Host Mode のメイン メニューが表示されます。

トークンが New PIN モードの場合の認証

特定のトークンで初めてログインするときには、トークンは New PIN モードになっています。システムの設定に応じて、次のいずれかの操作を行う必要があります。

- 自分で PIN を作成するのか、システム生成 PIN を使用するのかを選択します (次に示す操作手順を参照してください)。
- システム生成 PIN を使用します (43 ページの操作手順を参照してください)。
- 自分で PIN を作成します (44 ページの操作手順を参照してください)。

PIN のタイプを選択できる場合に、New PIN モードで認証を受けるには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Remote Mode] の順にクリックします。

   [Select Server to Administer] ダイアログ ボックスが表示されます。
2. サーバを選択して [OK] をクリックします。
3. 次に表示される [Administrator Authentication] ダイアログ ボックスで、トークンコードを入力し、[OK] をクリックします。

   システムで新しい PIN を生成するかどうかを確認するメッセージが表示されます。
4. 次のいずれかの操作を実行します。
   - システムが PIN を生成するように設定するには、「y」と入力し、[OK] をクリックします。システムで PIN を生成するための準備ができているかどうかを確認するメッセージが表示されます。

     準備ができているというのは、手順を続行する準備ができていることと、PIN が画面に表示されたときに他人に見られないようになっていることの両方を示します。
   - 自分で PIN を作成するには、「n」と入力し、[OK] をクリックします。その後、ステップ 8 に進みます。

   メモ：自分の PIN はメモに書き留めずに、記憶するようにしてください。
5. ステップ 4 で「y」と入力した場合は、PIN を生成する準備ができていることを確認してください。「y」と入力し、[OK] をクリックします。

   次のダイアログ ボックスに PIN が表示されます。さらに、トークンコードが変化するのを待ち、変化したら新しい PASSCODE を入力するように指示するメッセージも表示されます。
6. ダイアログ ボックスに表示される指示に従って、新しい PASSCODE を入力し、[OK] をクリックします。

   重要：このダイアログ ボックスは、認証手順が終了するまで表示されています。したがって、PIN を保護するために、認証手順をただちに終了してください。
7. 画面に表示される指示に従って、システム生成 PIN を使用して認証手順を終了します。
8. ステップ 4 で「n」と入力した場合は、新しい PIN の入力を求めるメッセージが表示されます。
9. 条件を満たす PIN を入力して、[OK] をクリックします。

10. 確認のために PIN を再入力して、[OK] をクリックします。
11. 画面に表示される指示に従って、作成した PIN を使用して認証手順を完了してください。

システム生成 PIN を使用しなければならない場合に、New PIN モードで認証を受けるには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Remote Mode] の順にクリックします。

   [Select Server to Administer] ダイアログ ボックスが表示されます。
2. サーバを選択して [OK] をクリックします。
3. 表示される [Administrator Authentication] ダイアログ ボックスで、トークンコードを入力し、[OK] をクリックします。

   システム生成 PIN を使用しなければならないことを知らせ、生成する準備ができたかどうかを確認するメッセージが表示されます。

   準備ができているというのは、手順を続行する準備ができるていることと、新しい PIN が画面に表示されたときに他人に見られないようになっていることの両方を示します。
4. 次のいずれかの手順を実行します。
   - システムが新しい PIN をすぐに生成するように設定するには、「y」と入力し、[OK] をクリックします。

     次のダイアログ ボックスに PIN が表示されます。さらに、トークンコードが変化するのを待ち、変化したら新しい PASSCODE を入力するように指示するメッセージも表示されます。ステップ 5 に進んでください。
   - この時点でシステム生成 PIN が不要な場合には、「n」と入力し、[OK] をクリックします。Remote Administration アプリケーションが終了します。

   メモ：自分の PIN はメモに書き留めずに、記憶するようにしてください。
5. ダイアログ ボックスに表示される指示に従って、新しい PASSCODE を入力し、[OK] をクリックします。

   重要：認証手順が終了するまで、この画面は表示されています。PIN を保護するために、認証手順をただちに終了してください。
6. 画面に表示される指示に従って、認証手順を終了します。

自分で PIN を作成しなければならない場合に、New PIN モードで認証を受けるには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Remote Mode] の順にクリックします。

   [Select Server to Administer] ダイアログ ボックスが表示されます。
2. サーバを選択して [OK] をクリックします。
3. 表示される [Administrator Authentication] ダイアログ ボックスで、トークンコードを入力し、[OK] をクリックします。

   新しい PIN の入力を求めるメッセージが表示されます。

4. 条件を満たす PIN を入力し、[OK] をクリックします。

メモ：自分の PIN はメモに書き留めずに、記憶するようにしてください。

5. 確認のために PIN を再入力して、[OK] をクリックします。
6. ダイアログ ボックスに表示される指示に従って、作成した PIN を使用して認証手順を完了してください。

Quick Admin を使用した Web ベースのアドミニストレーション

Quick Admin を使用すると、管理者は Web ブラウザを利用して、RSA Authentication Manager データベース内のユーザ、トークン、および拡張レコード データを表示および変更できます。Quick Admin ではデータベースへのアクセスが制限されるので、ヘルプ デスク、およびヘルプ デスク業務をサードパーティに委託する組織に適しています。

Quick Admin 管理者は、次のような一般的な操作を実行できます。

- ユーザ情報およびトークン情報の編集
- ユーザの削除
- ユーザへのテンポラリ パスワードの割り当て
- トークンの紛失処理
- トークンの再設定
- ユーザとトークンの拡張データの編集
- ユーザ レポートまたはトークン レポートの生成

Quick Admin 管理者は、レルム、サイト、グループ、またはエージェント ホスト レコードの編集、新規ユーザ レコードの作成、RSA Authentication Manager データベースへのトークン レコードのインポートを**実行できません**。

さらに、Quick Admin 管理者がアクセスできるのは、ユーザ レポートとトークン レポートだけであり、ユーザ拡張データ機能とトークン拡張データ機能についても、その一部にしかアクセスできません。

メモ：Quick Admin で実行できる作業の一覧については、ヘルプの「Categories of Tasks」を参照してください。アスタリスク (*) の付いた操作は、Quick Admin を使用して実行できます。

Quick Admin アーキテクチャ

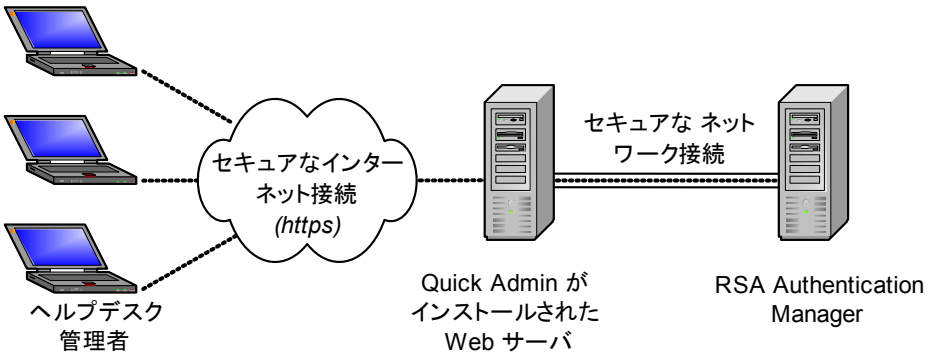
Quick Admin は以下で構成されています。

- Web サーバを通じてアクセス可能な Java サーブレット。これらのサーブレットは Apache Jakarta Tomcat 5.5.7 サーブレット エンジンを使用しています。
- RSA Authentication Manager プライマリ サーバで実行されるバックエンド プロセス。このプロセスは RSA Authentication Manager Quick Admin Daemon という名前であり、サーブレットとプライマリ データベースの間の暗号化された通信を管理します。

RSA Authentication Manager と同じマシンに Web サーバをインストールしないでください。インストールと構成の詳細については、ご使用のプラットフォームの『インストール ガイド』を参照してください。

重要：セキュリティ上の理由から、Apache Software Foundation が提供する最新のガイドラインに従ってください。詳細については、**http://jakarta.apache.org/tomcat** を参照してください。

次の図は、Quick Admin アーキテクチャを示しています。



Quick Admin のアドミニストレーション権限

Quick Admin 6.1 では、RSA Authentication Manager で定義したアドミニストレーション権限を適用します。アドミニストレーション権限とは、ユーザが特定のレルム、サイト、またはグループに対して実行できる一連のタスクを定義するテンプレートです。アドミニストレーション権限を割り当てると、管理者の権限が、特定の種類のアクション、および RSA Authentication Manager データベースの特定領域に制限されます。

アドミニストレーション権限は、次の 2 つの要素で構成されます。

アドミニストレーション スコープ。権限を割り当てる対象の管理者が管理できるサイトおよびグループ (したがって、ユーザとそのトークン) を指定します。Quick Admin のアドミニストレーション スコープを無効にすることもできます。手順については、46 ページの「Quick Admin アドミニストレーション スコープの無効化」を参照してください。

アドミニストレーション タスク リスト。特定の権限が割り当てられた管理者が、アドミニストレーション スコープ内で実行できる名前付きのタスク セットです。Quick Admin では、Quick Admin 管理者の定義されたタスク リストに**含まれていない**タスクは実行できません。詳細については、47 ページの「タスク リストの設定」を参照してください。

Quick Admin アドミニストレーション スコープの無効化

Quick Admin でアドミニストレーション スコープを適用しない場合は、アドミニストレーション タスク リストだけが適用されるように Quick Admin を設定できます。つまり、Quick Admin を使用する管理者は、割り当てられているスコープ以外のレコードに対しても、割り当てられているタスクを実行できます。

Quick Admin スコープを無効にするには

1. Quick Admin 管理者全員が Quick Admin セッションからログオフしたことを確認します。
2. Windows マシンの場合は、プライマリの ***%SystemRoot%*¥system32¥** ディレクトリにある **apidemon.ini** ファイルを開きます。

UNIX マシンの場合は、プライマリの ***ACEPROG*** ディレクトリにある **apidemon.ini** ファイルを開きます。

apidemon.ini ファイルには、1 行以上のテキスト行が記述されており、それぞれが 1 つのキーを定義しています。SCOPE は、Quick Admin がアドミニストレーション スコープを適用するかしないかを指定するキーです。

apidemon.ini ファイルの詳細については、『Administration Toolkit Reference Guide』(**authmgr_admin_toolkit.pdf**) の「Configuring the apidemon」を参照してください。

3. **apidemon.ini** で、次の行を見つけます。

   ```
   SCOPE=TRUE
   ```

4. Quick Admin のスコープ適用を無効にするには、次の行のように “TRUE” を “FALSE” に変更します。

   ```
   SCOPE=FALSE
   ```

5. **apidemon.ini** ファイルを保存して、閉じます。

6. ブラウザをいったん閉じて再起動して、Quick Admin を再起動します。

これで、Quick Admin のアドミニストレーション スコープは適用されなくなります。

タスク リストの設定

操作手順：

- タスク リストを追加するには、プライマリで、[System] > [Task Lists] > [Add Task List] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。
- タスク リストを Quick Admin 管理者に割り当てるには、[User] > [Edit User] > [Administrative Role] の順にクリックし、[Task List] オプションから、Quick Admin 管理者に対して設定するタスク リストを選択します。詳細については、[Help] をクリックして表示される情報を参照してください。

Quick Admin にアクセスするには、管理者のタスク リストに List User (ユーザのリスト表示) タスクと List Tokens (トークンのリスト表示) タスクの**いずれか一方または両方**が含まれている必要があります。次の表は、Quick Admin 管理者のタスク リストに設定できるタスクを示しています。

メモ：次の表の「補助タスク」列は、Quick Admin 管理者に対して許可できる追加アクションを示しています。ただし、これらのタスクはユーザ データベースを変更するので、Quick Admin 管理者のタスク リストに追加するときは十分注意してください。

情報の種類	必須タスク	補助タスク
ユーザ情報の編集	• List User (ユーザのリスト表示) • Edit User (ユーザの編集)	• Edit Token - User Assignment (トークンの編集 - ユーザの割り当て) **メモ：**Quick Admin では、このタスクは Unassign Token (トークンの割り当ての解除) 操作を制御します。 • Set/Change User Password (ユーザ パスワードの設定 / 変更) • Remove User Password (ユーザ パスワードの削除) • Delete User (ユーザの削除) • Replace Token (トークンの交換) • Edit User - Group Assignment (ユーザの編集 - グループの割り当て) **メモ：**Quick Admin では、このタスクは管理者にグループ メンバーシップの**表示**のみを許可します。グループ メンバーシップの**編集**は許可しません。 • Edit User Extension Data (ユーザ拡張データの編集)
ユーザ レポート	List User (ユーザのリスト表示)	なし

情報の種類	必須タスク	補助タスク
トークン情報の編集	• List Tokens (トークンのリスト表示) • List User (ユーザのリスト表示) • Edit Token (トークンの編集)	• Edit Token Extension Data (トークン拡張データの編集) • Edit Lost Status (紛失ステータスの編集) • Edit Token - User Assignment (トークンの編集 - ユーザの割り当て) **メモ：**Quick Admin では、このタスクは Unassign Token (トークンの割り当ての解除) 操作を制御します。 • Enable/Disable Token (トークンの有効化 / 無効化) • Clear PIN (PIN のクリア) **メモ：**Quick Admin では、このタスクは Reset Token (トークンの再設定) 操作を制御します。 • Resynchronize Token (トークンの同期のとり直し) • Set New PIN Mode (New PIN モードに設定) • Replace Token (トークンの交換)
トークン レポート	List Tokens (トークンのリスト表示)	なし

Quick Admin 管理者の認証

Quick Admin にアクセスするには、管理者は Authentication Manager の認証を受ける必要があります。したがって、各管理者は RSA Authentication Manager データベースにユーザ レコードを登録し、割り当てられたトークンを保有している必要があります。

Quick Admin 管理者はレルムごとに異なるトークンを使用するようにしてください。管理者が複数のレルムで同じトークンを使用すると、あるレルムで管理者がトークンコードを入力したときに侵入者がそのコードを検出し、そのコードを使用して他のレルムで Quick Admin にアクセスしてしまう危険性があります。

メモ：Quick Admin にアクセスするには、管理者のタスク リストに List User (ユーザのリスト表示) タスクと List Tokens (トークンのリスト表示) タスクのいずれか一方または両方が含まれている必要があります。

管理者の認証方式の選択

各レルムのセキュリティ管理者は、レルム内の管理者に対してどの認証方式を採用するかを決定します。リモート管理者の認証のために使用できるトークンの種類は、RSA Authentication Manager Host Mode の [Edit System Parameters] ダイアログ ボックスで設定します。デフォルト設定は、[SecurID Cards and Fobs] です。

どの種類のトークンあるいはパスワードでも選択できますが、管理者はできるだけハードウェア トークンを使用してください。これは、ハードウェア トークンがもっとも安全だからです。ハードウェア トークンとしては、RSA SecurID PINPAD、スタンダード カード、およびキーホルダが提供されています。

管理者の認証方式でもっとも安全性が低いのはユーザ パスワードです。ユーザ パスワードを使用する場合、二要素認証は実行されません。

Quick Admin 管理者は他のユーザと同様に、基本的な認証プロセスを使用します。操作手順については、Quick Admin のヘルプ「Logging On and Off」を参照してください。

検索とレポートのガイドライン

検索

Quick Admin 管理者は、特定のユーザおよび割り当て済みトークンを検索できます。検索クエリを限定的にする (絞り込む) ほど、情報取得までの所要時間が短くなります。Authentication Manager データベースの規模が大きいと、検索完了までの時間が長くなります。**quickadminconfig.properties** 構成ファイルで **Max_Search** 変数を設定すると、検索結果を少なくすることができます。このファイルは、***Quick Admin installation directory*¥Tomcat¥webapps¥ quickadmin¥WEB-INF¥ properties** ディレクトリにあります。

メモ：ユーザを検索するには、管理者のタスク リストに List User (ユーザのリスト表示) タスクが含まれている必要があります。割り当て済みトークンを検索するには、管理者のタスク リストに List Tokens (トークンのリスト表示) タスクが含まれている必要があります。

レポート

Quick Admin 管理者は、ユーザ レポートおよびトークン レポートを生成できます。レポートは、Quick Admin Web サーバの ***Quick Admin installation directory*¥Tomcat¥webapps¥ quickadmin¥WEB-INF¥reports** ディレクトリにあるテキスト ファイルに格納されます。ディスク容量を確保するために、このディレクトリの内容は定期的に削除してください。

Quick Admin 管理者に対して、できるだけレポートの作成を限定するようにアドバイスしてください。取得するレコード数が多くなれば、レポートの生成時間も長くなります。大きなレポートを生成する必要がある場合は、Quick Admin のログ記録をオフにすることをお勧めします。ログへの記録をオフにするには、***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥ WEB-INF¥ properties¥quickadminconfig.properties** をテキスト エディタで開き、**Verbose** パラメータを **no** に設定します。

メモ：ユーザ レポートを作成するには、管理者のタスク リストに List User (ユーザのリスト表示) タスクが含まれている必要があります。トークン レポートを作成するには、管理者のタスク リストに List Tokens (トークンのリスト表示) タスクが含まれている必要があります。

Quick Admin の再構成

レプリカをプライマリに指名する場合など、状況によっては、機能を維持するために Quick Admin の設定を再構成する必要があります。その場合は、ここで説明する操作を実行してください。

まず、Quick Admin ソフトウェアがインストールされているマシンで、**quickadminconfig.properties** ファイルの情報を再構成する必要があります。デフォルトでは、このファイルは、***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥WEB-INF¥properties** ディレクトリにあります。

quickadminconfig.properties ファイルを再構成するには

1. **ACE_SERVER**パラメータを、新しいプライマリの完全修飾DNS名に変更します。

   たとえば、新しいプライマリの名前が **oxygen** の場合、完全修飾 DNS 名は **oxygen**.*yourdomainname* となります。

2. **ACE_IP** パラメータを、新しいプライマリの IP アドレスに変更します。

次に、***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥WEB-INF¥certs** ディレクトリにあるプライマリ ディレクトリを再構成する必要があります。

プライマリ ディレクトリを再構成するには

1. ***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥ WEB-INF¥certs** ディレクトリに移動します。
2. 元のプライマリの名前と一致するサブディレクトリを削除します。
3. サブディレクトリを作成して、新しいプライマリの名前を付けます。
4. 新しいプライマリの ***ACEDATA*** ディレクトリから新しいプライマリの名前の付いたサブディレクトリに、**sdti.cer** および **server.cer** ファイルをコピーします。

変更が有効になるように、Quick Admin がインストールされているマシンで、Tomcat サーバをいったん停止して再起動します。

最後に、新しいプライマリの ***ACEPROG*¥hosts.conf** ファイルにいくつか変更を加える必要があります。

hosts.conf ファイルを変更するには

1. ***ACEPROG*¥hosts.conf** ファイルを開きます。
2. Quick Admin マシンの完全修飾 DNS 名と IP アドレスを追加します。
3. RSA Authentication Manager をいったん停止し、再起動します。

   Windows では、次の手順を実行します。

   - プライマリで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。
   - [RSA Authentication Manager Control Panel] ウィンドウの左側のパネルで、[Start & Stop RSA Auth Mgr Services] を選択します。
   - 右パネルで、[Stop All] をクリックします。警告メッセージが表示された場合は、[OK] をクリックします。
   - RSA Authentication Manager が完全に停止したら、[Start All] をクリックします。
   - [Close] をクリックします。

   UNIX マシンの場合は、次のように入力します。

   ```
   sdconnect stop
   aceserver stop
   ```

```
sdconnect start
aceserver start
```

トラブルシューティング

Quick Admin の特定のエラー メッセージのトラブルシューティングについては、付録 C「トラブルシューティング」を参照してください。

Quick Admin へのログオンに問題がある場合、Quick Admin 管理者は次のことを確認してください。

- 管理者がログオン時に入力した UserID に、正しいトークン パスワードまたはユーザ パスワードが割り当てられているかどうか。
- その UserID が割り当てられている管理者が十分な RSA Authentication Manager アドミニストレーション権限を保有しているかどうか。
- プライマリの **sdti.cer** および **server.cer** ファイルの有効なコピーが、Web サーバ ホストの ***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥WEB-INF¥certs¥***servername*** サブディレクトリに格納されているかどうか。

RSA Authentication Manager Activity ログ ファイルおよび Tomcat ログ ファイルも確認してください (Web サーバ ホストの ***Quick Admin installation directory*¥Tomcat¥logs** サブディレクトリにあります)。

メモ : Web サーバにインストールされている Quick Admin ソフトウェアは、すべてのトランザクションを ***Quick Admin installation directory*¥Tomcat¥logs¥**ディレクトリのログ ファイル (Windows の場合は **stdout_*date*.log**、Solaris の場合は **catalina.out**) に記録します。ログ ファイルは拡大するので、Web サーバのディスク空間が満杯になる可能性があります。ログ ファイルの拡大状況を監視し、定期的にアーカイブして、Web サーバから削除するようにしてください。

Quick Admin の次のステップ

- Quick Admin のインストールまたはアップグレードの詳細については、ご使用のプラットフォームの『インストール ガイド』の「RSA Authentication Manager Quick Admin ソフトウェアのインストール」の章を参照してください。
- Quick Admin の操作手順については、Quick Admin に付属のヘルプを参照してください。
- Quick Admin の特定のエラー メッセージのトラブルシューティングについては、付録 C「トラブルシューティング」の「メッセージ」を参照してください。
- RSA SecurID Web Express を Quick Admin と同じ Web サーバにインストールする手順については、ご使用のプラットフォームの『インストール ガイド』を参照してください。

3 エージェントとエージェント ホスト上でのアクティブ化

この章では、RSA Authentication Agent ソフトウェアと、エージェント ホスト上でのアクティブ化について説明します。RSA SecurID 認証による保護では、RSA Authentication Agent ソフトウェアを実行するコンピュータや他のデバイスは、RSA Authentication Manager データベースにエージェント ホストとして登録するか、登録されているエージェント ホストのクライアントになる必要があります。

RSA Authentication Manager Host Mode を使用すると、承認された管理者はいつでも、エージェント ホスト レコードを Authentication Manager データベースに追加したり、変更したりすることができます。

典型的なユーザ認証では、ユーザがパーソナル コンピュータやその他の保護されたリソースにアクセスしようとすると、RSA Authentication Agent がその要求を受け取り、ユーザに PASSCODE の入力を求め、入力された PASSCODE を RSA Authentication Manager に送信します。Authentication Manager はユーザの認証要求を検証し、アクセスの許可または拒否を RSA Authentication Agent に返します。エージェントは、ユーザがアクセスしようとしている保護対象のデバイスに、認証結果 (アクセスの許可または拒否) を返します。

Microsoft Windows 環境で RSA SecurID を使用するための新機能が、このリリースで提供されるようになりました。RSA Authentication Manager 6.1 および RSA Authentication Agent 6.0 または 6.1 を使用して、次の機能を有効にすることができます。

オフライン認証。ネットワークに接続している場合もオフラインの場合も、ユーザは RSA SecurID トークンを使用して保護されているリソースにログオンできます。外出先や自宅だけでなく、RSA Authentication Manager へのネットワーク接続が一時的に使用できなくなった場合も、ユーザのコンピュータ、ドメイン サーバ、またはターミナル サーバに格納されているオフライン認証データにより、ユーザは RSA SecurID で認証を受けることができます。ユーザがトークンを紛失したり、PIN を忘れたりした場合には、管理者はエマージェンシー トークンコードおよび PASSCODE を提供することで、ユーザがオフライン コンピュータにログオンできるように設定できます。

Windows パスワードの統合。このオプションを使用すると、ユーザが RSA SecurID PASSCODE を入力して、保護されているリソースにログオンするときに、ログオン パスワードが Windows 認証サービスに自動的に送信されます。ユーザが手動でパスワードを入力する必要はありません。この機能を利用すると、組織のパスワード セキュリティ ポリシーを単純化して向上することができ、パスワードの管理に必要なコストを削減できます。

これらの機能の管理の詳細については、57 ページの「オフライン認証およびパスワードの統合の設定」を参照してください。

これらの機能に関連するシステム アーキテクチャのオプションの概要と、RSA SecurID for Microsoft Windows ソリューションを実装するのに必要な情報については、『RSA SecurID for Microsoft Windows Planning Guide』を参照してください。

ネットワーク環境で保護されているさまざまなリソースにエージェントをインストールして構成する方法については、『RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide』を参照してください。

各プラットフォーム向けの最新のエージェントのダウンロード

各プラットフォーム向けの最新の RSA Authentication Agent ソフトウェアは、**http://www.rsasecurity.com/node.asp?id=1174** で提供されます。エージェントのダウンロード パッケージには、インストール ガイドとアドミニストレーション ガイド、および『Readme』が付属しています。エージェントをインストールする前に、これらのマニュアルをお読みください。

エージェント ホストの作成と変更

Authentication Manager 管理者またはエージェント管理者がエージェント ソフトウェアをインストールして構成した後、レルム内の各エージェント ホストのエージェント ホスト レコードを Authentication Manager データベースに追加する必要があります。エージェント ホストの自動登録機能が設定されている場合は、レコードはデータベースに自動的に追加されます。詳細については、64 ページの「エージェント ホストの自動登録 / 更新」、および次の「自動登録されるエージェント ホスト」を参照してください。

エージェント ホストの自動登録機能を使用しない場合は、RSA Authentication Agent ソフトウェアを実行し、RSA SecurID 認証による保護の必要なローカル リソースを Authentication Manager データベースに指定する必要があります。

操作手順：[Agent Host] > [Add Agent Host] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

メモ：エージェント ホスト レコードを RSA Authentication Manager データベースに登録した後に編集するには、[Agent Host] > [Edit Agent Host] の順にクリックします。

自動登録されるエージェント ホスト

新しいエージェント ホストが自動的に登録され、RSA Authentication Manager データベースのレコードが更新されるように、システムを構成することができます。Windows、HP-UX、AIX、および Solaris エージェント ホストの自動登録機能の使用方法の詳細については、64 ページの「エージェント ホストの自動登録 / 更新」を参照してください。

メモ：標準の自動登録手順では、エージェント ホストがアドレス / 名前解決のために DNS 方式をサポートすることを前提にしています。追加するエージェント ホストでこの方式がサポートされない場合は、Configuration Management プログラムを実行し、[Resolve Hosts and Services By Name] チェックボックス ([Enable Features] パネル) がオンになって**いない**ことを確認してください。どのエージェント ホストでも DNS 方式の解決がサポートされない場合は、このチェックボックスを再びオンにする必要はありませんが、DNS をサポートするエージェント ホストとサポートしないエージェント ホストが混在する場合は、必要に応じてチェックボックスのオンとオフを切り替えてください。

エージェント ホストのデフォルト設定

新たにインストールした未登録のエージェント ホストで自動登録プログラムを実行すると、Authentication Manager データベースにそのエージェント ホストのレコードが作成されます。デフォルトでは、エージェント ホストの設定は次のようになります。

- オープン アクセスが可能です。

- ローカルで認識されないユーザを他のレルムから検索するように設定されます。
- タイプは UNIX エージェント ホストになります。
- DES 暗号方式を使用します。
- アクティング マスタは設定されません。
- アクティング スレーブは設定されません。

これらのデフォルト設定が新しいエージェント ホストにとって不適切な場合には、必要に応じて、レコードを編集して設定を変更します。[Agent Host] > [Edit Agent Host] の順にクリックし、変更するレコードを選択します。[Edit Agent Host] ダイアログ ボックスが表示されます。

エージェント ホスト拡張データの変更

エージェント ホスト拡張レコードの情報を変更するには、[Add Agent Host] または [Edit Agent Host] ダイアログ ボックスの [Edit Agent Host Extension Data] ボタンを使用します。これらのレコードには、カスタム アドミニストレーション プログラムからアクセスできる情報 (組織で定義された情報) が格納されます。

RSA Authentication Manager Administration Toolkit を使用してカスタム アドミニストレーション プログラムを作成する方法については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

エージェント構成レコードの作成と編集

RSA Authentication Agent ホストとして定義されている各デバイスには、***%SYSTEMROOT%¥system32*** ディレクトリ (Windows マシン) または ***ACEDATA*** ディレクトリ (UNIX マシン) に RSA Authentication Manager 構成ファイル (**sdconf.rec**) が格納されています。RSA Authentication Manager は、プライマリのインストール時に初期構成ファイルを作成し、プライマリの ***ACEDATA*** ディレクトリに格納します。

ほとんどの場合、RSA Authentication Agent ソフトウェアをインストールする前に、この **sdconf.rec** をエージェント ホストにコピーできます。

メモ：多くのデバイス メーカは、RSA Authentication Agent ツールキットを使用して独自にエージェントを作成しています。これらのサードパーティ製のエージェントの中には、**sdconf.rec** ファイルを使用しないものもあります。

一部のエージェント ホストでは、**sdconf.rec** ファイルを作成しなければならないことがあります。構成ファイルの作成プロセスでは、エージェント ホストに必要な構成データが構成ファイルに登録されているかどうかが確認されます。たとえば、次のデータが必要です。

- アクティング マスタとアクティング スレーブの識別子。旧バージョンのエージェント ホストをサポートするために必要です (74 ページの「旧バージョンのエージェント ホスト」を参照)。
- プライマリのエイリアス IP アドレス。ファイアウォールを介した認証をサポートするために必要です (24 ページの「ファイアウォールを介した Authentication Manager とエージェント ホストの通信」を参照)。

エージェント ホストの構成ファイルを作成するには、RSA Authentication Manager Host Mode を起動し (第 2 章「RSA Authentication Manager Administration アプリケーションの使用」を参照)、[Agent Host] > [Add Agent Host] > [Assign Acting Servers] > [Generate Configuration File] の順にクリックします。詳細については、ヘルプを参照してください。

構成ファイルを編集するには、Windows システムで Configuration Management アプリケーションを実行するか、UNIX システムで ***ACEPROG*/sdsetup -config** を実行します。詳細については、第 12 章「RSA Authentication Manager の構成 (Windows)」または第 14 章「RSA Authentication Manager の構成 (UNIX)」を参照してください。

メモ: RSA Authentication Manager 6.1 をインストールした後、旧バージョンのエージェント ホストを追加する場合は、アクティング マスタおよびアクティング スレーブの識別子を手動で入力する必要があります。67 ページの「エージェント ホストによる負荷分散」を参照してください。

Configuration Record Editor (***ACEPROG*** ディレクトリの **sdcfgedit_ui.exe**) を使用すると、任意の **sdconf.rec** ファイル内のアクティング マスタとアクティング スレーブの設定を編集できます。手順については、74 ページの「旧バージョンのエージェント ホスト」を参照してください。

システムをエージェント ホストの自動登録用に構成している場合は、新しいエージェント ホストで自動登録 / 更新ユーティリティを実行すると、そのエージェント ホストはデータベースに登録されるので、管理者がエージェント ホスト レコードを作成する必要はありません。

また、エージェント ホストの IP アドレスが変更されたときは、いつでもこのユーティリティを実行して、Authentication Manager データベースのエージェント ホスト レコードの IP アドレス フィールドを更新できます。この更新機能は、エージェント ホスト リソースへの IP アドレスの割り当てに DHCP (Dynamic Host Configuration Protocol) を使用するシステムでは特に便利です。詳細については、64 ページの「エージェント ホストの自動登録 / 更新」を参照してください。

エージェント ホストは、制限されたエージェント ホストまたはオープン エージェント ホストとして構成できます。制限されたエージェント ホストでは、エージェント ホストでアクティブ化されているユーザ、またはエージェント ホストでアクティブ化されているグループに所属するユーザにのみアクセスが許可されます。

制限されたエージェント ホストとして保護されたリソースの場合、RSA Authentication Manager データベース内のどのユーザでもアクセスが許可されるのではなく、個別にアクティブ化されるか、またはグループに所属するユーザとしてアクティブ化された場合にのみアクセスが許可されるので、より安全であると考えられます。

特定のリソースへのアクセスを制限する場合は、そのリソースを制限されたエージェント ホストで保護する必要があります。オープン エージェント ホストは、次のカテゴリのユーザにアクセスを許可するように構成できます。

- データベース内で RSA SecurID によって認証を受けるすべてのユーザ。ただし、現在の時刻にアクセスが禁止されるようなアクセス時刻の制限が設定されたエージェント ホストでアクティブ化されていない場合、または同様のアクセス時刻の制限を持つグループに属していない場合に限ります (63 ページの「オープン エージェント ホストへのアクセスの制限」を参照してください)。
- RSA SecurID によって認証を受けるユーザとしてデータベースに登録されているユーザのうち、その他の制限が設定されていないすべてのユーザ。

別の設定が有効な場合は、エージェント ホストは、ホーム レルムのデータベースに登録されている他のレルムから不明なユーザを検索するようになり、エージェント ホストはレルム間認証の対象になります。その設定が無効な場合は、エージェント ホストのホーム レルムのユーザにだけアクセスが許可されます。

制限されているのかオープンであるのかに関係なく、エージェント ホストは承認されたユーザの独自のリストを保有できます。このリストを作成するには、エージェント ホストでユーザをアクティブ化するか、ユーザをエージェント ホストでアクティブ化されたグループのメンバにします。119 ページの「エージェント ホスト上でのアクティブ化」を参照してください(オープン エージェント ホストでユーザおよびグループをアクティブ化するのは、アクセス時刻の制限を設定するためだけです)。

オフライン認証およびパスワードの統合の設定

RSA Authentication Manager 6.1 と RSA Authentication Agent 6.1 は連携して動作して、ローカル認証、ドメイン サーバ認証、およびターミナル サーバ認証を可能にし、ログイン パスワードの統合も可能にします。これらの機能のインストールと構成の大部分はエージェント側で行われます。詳細については、『RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide』を参照してください。

Authentication Manager では RSA Authentication Manager Host Mode を使用して、システム全体でオフライン認証機能と Windows パスワードの統合機能を有効に設定した後、エージェント ホストごとに個別にこれらの機能を有効または無効に設定することができます。

メモ：オフライン認証とパスワードの統合が正常に動作するには、ユーザは Windows 環境と正確に同じログイン名を RSA Authentication Manager データベースに登録する必要があります。サポートされる LDAP サーバでユーザが定義されている場合は、RSA Authentication Manager の LDAP 同期機能を使用して、ユーザを RSA Authentication Manager データベースにインポートできます。詳細については、106 ページの「LDAP ユーザ レコードの同期化」を参照してください。

システム レベルでのオフライン認証の設定

多くのオフライン認証パラメータはシステム レベルで設定できます。これらのパラメータはエージェントのデフォルトになります。さらに、個々のエージェントに対して、オフライン認証とパスワードの統合を設定することができます。詳細については、59 ページの「エージェントごとのオフライン認証とパスワードの統合の設定」を参照してください。

次の表は、システム レベルで設定できるパラメータを示しています。

パラメータ	説明
オフライン認証をシステム レベルで有効にします。	オフライン認証が許可されるかどうかを指定します。

パラメータ	説明
オフライン認証のセキュリティ設定： • 有効に設定されているエージェントに、最大 *nn* 日のオフラインデータを提供します。 • PIN + トークンコードの長さを *nn* 文字以上に設定します。 • 代替トークン タイプ (PINPAD、トークンコードのみが表示されるトークン、固定パスワード) によるオフライン認証を許可します。	ユーザがシステムに保有できるオフライン日数 (*nn*)、要求される PASSCODE の長さ、オフライン認証で使用できる代替トークン タイプを設定します。 ユーザがオフライン認証データをダウンロードした後で、データの最大日数の設定を小さくしても、オフライン データが残されている間、ユーザは認証を受けることができます。ダウンロードされるオフライン日数の新しい設定 (削減された値) は、ユーザがネットワークに接続した後、初めて適用されます。 PASSCODE は 12 文字以上に設定することを推奨します。 代替トークン タイプを有効にした結果、オフライン認証に対して組織で要求されるセキュリティ レベルが低下しないかどうかを考慮してください。たとえば、トークンコードのみが表示されるトークンの場合、ユーザのコンピュータとトークンが盗まれると、侵入者によって無制限のアクセスが可能になってしまいます。
オフライン エマージェンシー コード： • オフライン エマージェンシー コードを作成します。 • コードの種類： – オフライン エマージェンシー トークンコード – オフライン エマージェンシー PASSCODE – 両方 • コードに含まれるもの： – 数字 – 文字 – 句読点記号 • オフライン認証に *nn* 回失敗した後、エマージェンシー コードを要求します。 • エマージェンシー コードは、*nn* 日後に有効期限が切れます。	ユーザのコンピュータがロックされて使用できなくなった場合 (たとえば、不正な PASSCODE を何度も入力した場合など)、RSA Authentication Manager 管理者はエマージェンシー コードを提供して、ユーザがコンピュータにアクセスできるようにすることができます。これらのパラメータは、エマージェンシー コードの使用が許可されるかどうか、許可されるコードの種類、要求される状況、有効期限などを設定します。 通常、ユーザのコンピュータがロックされて使用できなくなると、管理者に連絡して、コンピュータにアクセスするためのエマージェンシー コードを提供してもらいます。エマージェンシー コードの詳細については、60 ページの「オフライン認証ユーザに対するエマージェンシー アクセスの設定」を参照してください。
オフライン認証データの残りが *nn* 日になったときに、そのことをユーザに警告します。	オフライン認証データの残りが特定の日数になったときに、ユーザに自動的に警告を出すように設定できます。
ユーザが再接続したときに、オフライン認証ログ エントリをアップロードします。	ユーザがネットワークに再接続したときに、ユーザ コンピュータで実行されたオフライン認証ログ アクティビティを Authentication Manager のログ データベースに必ず送信します。

パラメータ	説明
詳細なオフライン認証ログ機能を有効にします。	オフライン認証アクティビティおよび障害に関する詳細なログ (たとえば、ユーザの PIN とトークンコードの組み合わせ (PASSCODE) が要求されている長さでないなど) を提供します。

操作手順：RSA Authentication Manager Host Mode で、[System] > [System Configuration] > [Edit Offline Authentication] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

システム レベルでのパスワードの統合の設定

オフライン認証と同様に、パスワードの統合もシステム レベルで設定できます。ただし、次の「エージェントごとのオフライン認証とパスワードの統合の設定」で説明しているように、このパラメータはエージェントごとに無効に設定できます。

操作手順：RSA Authentication Manager Host Mode で、[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。[Enable Windows password integration at system level] をクリックします。

エージェントごとのオフライン認証とパスワードの統合の設定

デフォルト設定では、RSA Authentication Agent 6.1 を実行しているコンピュータは、オフライン認証とパスワードの統合に関してシステム レベルのパラメータを使用します。しかし、RSA Authentication Manager Host Mode では、エージェントごとにこれらのパラメータを無効にすることができます。

たとえば、一部のエージェント ホストをオープン エージェント ホストとして設定している場合、これらの機能のいずれか一方または両方を無効に設定しなければならないことがあります。

操作手順：[Agent Host] > [Add Agent Host] (または [Edit Agent Host]) をクリックします。詳細については、ヘルプの「Adding an Agent Host」または「Editing an Agent Host」を参照してください。

保護されたドメインでリモート アクセス エージェント ホストが機能するための設定

ドメインが RSA Authentication Agent 6.1 for Microsoft Windows で保護されていて、リモート アクセス アプリケーションを使用している場合、ドメイン認証とリモート認証とは互換性がありません。この問題を解決するには、Authentication Agent 管理者はドメイン コントローラのエージェントに対して、認証時にリモート アクセス アプリケーション ホストのアドレスを指定する方法を指示する必要があります。リモート アクセス アプリケーションに別のRSA SecurIDアプリケーションがインストールされている場合は、エージェント管理者は、リモート アクセス アプリケーション ホストが最近、有効な認証要求を RSA Authentication Manager に対して作成したかどうかを確認するよう、ドメイン コントローラのエージェントに対して指示します。リモート アクセス アプリケーション ホストが有効な要求を作成した場合は、エージェントはドメインへのアクセスを許可します。詳細については、『RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide』の「Using Domain Authentication With Remote Authentication」を参照してください。

確認作業を行うには、RSA Authentication Manager がリモート アクセス アプリケーション ホストに対して検証可能な認証を作成できるように設定する必要があります。

操作手順：RSA Authentication Manager Host Mode で、[Agent Host] > [Edit Agent Host] の順にクリックしてエージェント ホストを選択し [OK] をクリックします。次に、[Create Verifiable Authentications] を選択します。詳細については、ヘルプの「Editing an Agent Host」を参照してください。

重要：エージェント ホストに対して [Create Verifiable Authentications] を選択し、変更を保存した後、構成を有効にするには、RSA Authentication Manager を再起動する必要があります。多くのエージェント ホストに対してこの設定を指定する場合は、すべての設定を行った後で Authentication Manager を再起動してください。

フロントエンド / バックエンド環境での Web アプリケーションのサポート

保護されたフロントエンド/バックエンド環境では、フロントエンド Web サーバは RSA SecurID チャレンジ (認証要求) を行い、バックエンドは Windows チャレンジ (認証要求) を行います。

この種の環境をサポートするには、フロントエンドのエージェント ホスト レコードを RSA Authentication Manager に作成し、バックエンドのエージェント ホスト レコードをコピーし、両方のエージェント ホストが検証可能な認証を作成するように設定されたことを確認する必要があります。両方のエージェント ホストで、ユーザのアクティブ化とグループのアクティブ化が同一の設定になっていなければなりません。

操作手順：RSA Authentication Manager Host Mode で、フロントエンド コンポーネントに対して、[Agent Host] > [Add Agent Host] の順にクリックします。ユーザとグループのアクティブ化も含めて、エージェント ホストの設定を完全に定義し、[Create Verifiable Authentications] が選択されていることを確認します。バックエンド コンポーネントに対して、[Agent Host] > [Copy Agent Host] の順にクリックして、フロントエンド コンポーネントのコピーを作成します。バックエンド コンポーネントのコピーに名前を付け、[Create Verifiable Authentications] が選択されていることを確認します。詳細については、ヘルプの「Adding an Agent Host」または「Copying an Agent Host」を参照してください。

構成を完了するには、フロントエンド エージェント ホストとバックエンド エージェント ホストの両方を、ドメイン コントローラで動作しているドメイン エージェント ホストの [Verify Group] グループに追加します。詳細については、『RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide』の「Configuring Web Servers for RSA SecurID Authentication」を参照してください。

オフライン認証ユーザに対するエマージェンシー アクセスの設定

次のような状況が発生すると、ユーザは自分のコンピュータを使用できなくなります。

- ユーザのシステムが長期にわたってネットワークから切断されたため、データの有効期限が切れた場合。
- ユーザが不正な PASSCODE を認められている回数より多く入力した場合。
- ユーザが自分の PIN を忘れた場合。
- ユーザがトークンを紛失した場合。

このような状況になったら、ユーザは RSA Authentication Manager 管理者に連絡し、エマージェンシー コードを発行してもらう必要があります。

メモ：セキュリティを確保するために、管理者がエマージェンシー コードを表示すると、RSA Authentication Manager はそのイベントをログに記録します。

エマージェンシー コードには、オフライン エマージェンシー トークンコードとオフライン エマージェンシー PASSCODE の 2 種類があります。

オフライン エマージェンシー トークンコード

オフライン認証のユーザが RSA SecurID トークンを紛失した場合は、RSA Authentication Manager 管理者に連絡して、エマージェンシー トークンコードを提供してもらう必要があります。ユーザは自分の PIN の後に続けてオフライン エマージェンシー トークンコードを入力することで、認証を受けてオフライン コンピュータにアクセスできます。

メモ：紛失したトークンが後で見つかった場合には、ユーザがネットワークに接続して認証を受けようとすると、トークンは New PIN モードになります。

ユーザに提供するためにオフライン エマージェンシー トークンコードを表示するには、まず、RSA Authentication Manager Host Mode からトークンを編集する必要があります。

操作手順：[Token] > [Edit Token] の順にクリックします。操作手順については、ヘルプの「Editing a Token」を参照してください。

オフライン エマージェンシー PASSCODE

オフライン認証のユーザが PIN を忘れてしまった場合、オフライン コンピュータで認証を受けるには、オフライン エマージェンシー PASSCODE が必要です。ユーザに提供するためにオフライン エマージェンシー PASSCODE を表示するには、まず、RSA Authentication Manager Host Mode からユーザを編集する必要があります。

操作手順：[User] > [Edit User] の順にクリックします。操作手順については、ヘルプの「Editing a User」を参照してください。

メモ：オフライン エマージェンシー PASSCODE を使用する場合、PIN が必要ないので、ユーザの身元を必ず確認してください。

不正な PASSCODE を処理するエージェントの設定

RSA Authentication Manager システムでは、誤った PASSCODE の入力をある程度は認める必要があります。一方、システムのセキュリティについて考えると、攻撃する意図を持った人が、偶然に認証が成功するまで入力を次々と試行するのを防ぐ必要があります。次の各処理を実行する前に、誤った認証試行を受け付ける回数を RSA Authentication Manager で設定することができます。

- トークンをネクスト トークンコード モードにする。
- トークンを無効にする。

たとえば、RSA Authentication Manager システムが、登録されているユーザであるように見える人から認証要求を受け取ったとします。ユーザは、PASSCODE の要求に対して、不正な値を入力します。このエラーが通知されても、ユーザは誤った PASSCODE の入力を続行します。不正な PASSCODE を入力した回数が、エージェントに対して設定されている回数を超えると、トークンは無効になります。無効になったトークンは、管理者が有効にしなければ、再び使用できません。

しかし、不正な PASSCODE を数回入力した後に、偶然正しい PASSCODE を入力したとします。Authentication Manager はその入力を受け付けることができますが、一連の不正な PASSCODE の後の偶然の当たりである可能性もあります。トークンをネクスト トークンコード モードにすると、PASSCODE を実際に入力した人物が正当なトークン保有者であるかどうかを検証できます。このモードでは、エージェントはユーザに 2 つの連続して表示される PASSCODE を入力することを要求します。正しく入力できず、入力の失敗が繰り返されると、Authentication Manager は失敗試行回数の上限に達し次第、すぐにトークンを無効にします。

ユーザが有効な PASSCODE を入力しない限り、ネクスト トークンコード モードは解消されません。RSA Authentication Manager のデフォルト設定では、トークンをネクスト トークンコード モードにするまでに、(正しい入力の前に) 不正な入力が 3 回まで許容され、トークンを無効にするまでに、不正な入力が 10 回まで許容されます。

Windows サーバで不正な PASSCODE を管理するエージェントを構成するには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Configuration Management] の順にクリックします。
2. [Edit] をクリックし [OK] をクリックしてから、[Agent Host] をクリックします。
3. エージェントの種類ごとに、構成値を入力します。
4. [OK] をクリックします。
5. [OK] をクリックします。
6. この情報は複製されないので、レルム内のすべてのサーバでこの手順を繰り返します。

詳細については、235 ページの「エージェント ホストの PASSCODE の設定」を参照してください。

UNIX サーバで不正な PASSCODE を管理するエージェントを構成するには

1. ***ACEPROG*/sdsetup -config** を実行します。
2. プロンプトが表示されたら RETURN を押します。次のプロンプトが表示されるまで、この操作を繰り返します。
3. 次のプロンプトが表示されたら、構成値を入力します。

   ```
   How many wrong PASSCODEs before a token is set to next
   tokencode? ( ネクスト トークンコードに設定されるまでに不正な PASSCODE の
   入力を許容する回数を指定してください )

   How many wrong PASSCODEs before a token is set to disabled?
   ( トークンが使用不可となるまでに不正な PASSCODE の入力を許容する回数を指定
   してください )
   ```

RSA Authentication Manager for UNIX の構成の詳細については、第 14 章「RSA Authentication Manager の構成 (UNIX)」を参照してください。

オープン エージェント ホスト

オープン エージェント ホスト機能を使用すると、エージェント ホスト上で個々のユーザをアクティブ化したり、エージェント ホストでアクティブ化されるグループにユーザを追加したりする必要がないため、管理作業を削減できます。Authentication Manager データベースに登録されているユーザであれば、どのユーザでもオープン エージェント ホストで認証を受けることができます。この場合、ユーザを直接アクティブ化したり、グループを通じてアクティブ化する必要はありません。ただし、ユーザまたはグループのアクセス時刻を制限する目的で、オープン エージェント ホスト上でもユーザまたはグループをアクティブ化することはできます。詳細については、「オープン エージェント ホストへのアクセスの制限」を参照してください。

オープン エージェント ホストの指定

エージェント ホストをオープン エージェント ホストとして設定するには、[Add Agent Host] または [Edit Agent Host] ダイアログ ボックスで [Open to All Locally Known Users]チェックボックスをオンにします。また、[Search Other Realms for Unknown Users] チェックボックスをオンにすることもできます。このチェックボックスをオンにした場合、ローカル データベースに登録されていない他のレルムのユーザから認証要求が送信されると、エージェント ホストはレルム間認証でオープン エージェント ホストとして設定されます。

エージェント ホスト自動登録機能を使用すると、新規エージェント ホストはデフォルト設定でオープン エージェント ホストとして登録されます。詳細については、67 ページの「エージェント ホストによる負荷分散」を参照してください。

オープン エージェント ホストへのアクセスの制限

ユーザとグループは、制限付きエージェント ホストの場合と同様に、オープン エージェント ホスト上でもアクティブ化できます。ユーザがエージェント ホスト上で直接アクティブ化された場合も、エージェント ホスト上でアクティブ化されたグループのメンバである場合も、アクセス時刻が制限されているときは、オープン エージェント ホストであっても、このユーザに対してオープンにならないことがあります。

ユーザが認証を受けるときに、Authentication Manager は、そのユーザがエージェント ホスト上で直接アクティブ化されたかどうかを確認します。直接アクティブ化されている場合は、Authentication Manager はユーザのアクセス時刻が制限されていないかどうかを確認します。アクセス時刻が制限されていない場合や、(制限されていても) 許可されている時刻に認証を受けている場合は、ユーザはエージェント ホストへのアクセスを許可されます。

ユーザがエージェント ホスト上で直接アクティブ化されていない場合は、Authentication Manager はユーザのグループ アクティブ化情報を確認します。ユーザが 1 つ以上のグループを介してエージェント ホスト上でアクティブ化されている場合は、Authentication Manager はグループのアクセス時刻の制限を確認します。たとえば、ユーザが Group 1 のメンバであり、午前 8 時から午後 5 時までの間、グループのログオンが許可されている場合には、ユーザもこの時間だけログオンできます。このユーザが Group 2 のメンバでもあり、午後 8 時から午前 8 時までの間、グループのログインが許可されている場合は、ユーザは午後 5 時から午後 8 時までの間だけ、アクセスを拒否されます。

エージェント ホストの自動登録 / 更新

RSA Authentication Manager のエージェント ホスト自動登録 / 更新機能を使用すると、次の理由により、管理作業が削減されます。

- 新規エージェント ホストはAuthentication Managerデータベースに自動的に登録されるので、管理者がエージェント ホスト レコードを作成する必要はありません。
- アドレスが変更された場合 (たとえば DHCP によって)、既存のエージェント ホストは Authentication Manager データベースでその IP アドレスを更新できます。

  メモ : エージェント ホストの名前は同じままでなければなりません。名前と IP アドレスの両方が変更されると、Authentication Manager で新しいエントリが作成されます。

- Authentication Manager 構成ファイルが変更された場合、既存のエージェント ホストは **sdconf.rec** ファイルを更新できます。アクティング Authentication Manager およびエイリアス IP アドレス情報の変更は送信されません。

これらの機能は、Windows、HP-UX、AIX、および Solaris のサポートされているバージョンで使用できます。詳細については、ご使用のプラットフォームの『インストール ガイド』を参照してください。自動登録機能は、v5.0 (およびそれ以降) のエージェント ホストで完全にサポートされています。複数のネットワーク インタフェースが搭載されたマシンでは、自動登録機能はサポートされません。自動登録機能を使用するように既存のエージェント ホストを構成した場合は、76 ページの「旧バージョンのエージェント ホストの自動登録機能のサポート」を参照してください。

新しいエージェント ホストから登録情報を受け取るには、既存のエージェント ホストに自動登録 / 更新プログラムをインストールし、自動登録を許可するように RSA Authentication Manager を設定する必要があります。各エージェント ホストの管理者に対して、自動登録 / 更新プログラムのインストールおよび使用方法に関して、次の中から適切な操作手順を通知してください。

- エージェント ホスト自動登録機能 (Automated Agent Host Registration) を使用するエージェント ホストは、プライマリに登録する必要があります。プライマリのエージェント ホスト レコード、およびエージェント ホストの **sdconf.rec** ファイルの両方で、プライマリをアクティング マスタとして指定していなければなりません。

  プライマリのエージェント ホスト レコードで、プライマリをアクティング マスタとして設定します。次に、新しい構成ファイルを作成し、エージェント ホストに配布します。
- マスタをプライマリにアップグレードした場合は、既存のエージェント ホストはプライマリに登録するように既に構成されています。既存の他のエージェント ホストや新しいエージェント ホストに自動登録機能を追加する場合は、自動登録機能を使用するエージェント ホストごとに、プライマリをアクティング マスタとして割り当て、新しい **sdconf.rec** ファイルを作成し、そのファイルをエージェント ホストに配布します。
- マスタをプライマリにアップグレードせずに、新しいマシンをプライマリとして使用する場合は、自動登録機能を使用するエージェント ホストごとに、プライマリをアクティング マスタとして割り当て、新しい **sdconf.rec** ファイルを作成し、そのファイルをエージェント ホストに配布します。

- 複数のレルムをマージ (結合) している場合は、マージされたレルム内で自動登録を使用するエージェント ホストごとに、プライマリをアクティング マスタとして割り当て、新しい **sdconf.rec** ファイルを作成し、そのファイルをエージェント ホストに配布します。

アクティング Authentication Manager の割り当てと **sdconf.rec** ファイルの作成については、ヘルプの「Assign Acting Authentication Managers」を参照してください。

Microsoft Windows エージェント ホストの管理者は次の手順に従ってください。

1. プライマリの **sdconf.rec** ファイルと **server.cer** ファイルをターゲット エージェント ホストのテンポラリ ディレクトリにコピーします。
2. RSA Authentication Manager 6.1 CD-ROM の **acesupp¥sdadmreg¥windows** ディレクトリから、**sdconf.rec** ファイルと **server.cer** ファイルを格納しているテンポラリ ディレクトリに、**sdadmreg_install.exe** をコピーします。
3. インストール先の Windows エージェント ホストの Windows エクスプローラで、**sdadmreg_install.exe** をダブルクリックし、画面に表示される指示に従います。

   sdadmreg_installユーティリティは、エージェント ホストの ***%SYSTEMROOT%¥system32*** ディレクトリ (たとえば **winnt¥system32**) に **sdconf.rec**、**server.cer**、および **sdadmreg.exe** をインストールします。
4. プライマリでデータベース ブローカを起動してから、**sdadmreg** を実行します。

   Windows を使用している場合、RSA Authentication Manager Host Mode などの RSA Authentication Manager プログラムを起動すると、データベース ブローカが自動的に起動します。

   UNIX を使用している場合は、Authentication Manager で ***ACEPROG*/sdconnect start** コマンドを実行してデータベース ブローカを起動します。
5. エージェント ホストを再起動するたびに、自動登録プログラムが実行されます。自動登録プログラムを手動で実行するには、**sdadmreg.exe** をダブルクリックします。

   メモ : コマンド プロンプトを使用して **sdadmreg** を実行した場合は、結果が出力されません。この場合は、イベント ログで関連メッセージを表示する必要があります。イベント ログを表示するには、[スタート] > [プログラム] > [管理ツール] > [イベント ビューア] の順にクリックします。

   このプログラムは次の場合に実行できます。

   - 新しい Windows エージェント ホストに RSA Authentication Agent ソフトウェアをインストールする前、またはインストールした直後。エージェント ホスト レコードが存在しない場合や、Authentication Manager で自動登録が有効に設定されている場合は、エージェント ホスト レコードが Authentication Manager データベースに追加されます。
   - エージェント ホストに新しい IP アドレスを割り当てた場合。このエージェント ホストのノード シークレットがすでに作成されている場合は、新しいエージェント ホスト IP アドレスが Authentication Manager データベースのエージェント ホスト レコードに書き込まれます。
   - Authentication Manager の現在の **sdconf.rec** でエージェント ホストの **sdconf.rec** を更新しなければならない場合。更新した **sdconf.rec** は、エージェント ホストを再起動するまで有効になりません。

UNIX エージェント ホストの管理者は次の手順に従ってください。

1. プライマリの **sdconf.rec** ファイルと **server.cer** ファイルをターゲット エージェント ホストのテンポラリ ディレクトリにコピーします。
2. RSA Authentication Manager 6.1 CD-ROM の **acesupp¥sdadmreg¥*platform*** ディレクトリから、**sdconf.rec** ファイルと **server.cer** ファイルを格納しているテンポラリ ディレクトリに、**sdadmreg_install** と **sdadmreg** をコピーします。
3. ステップ 1 とステップ 2 で使用したテンポラリ ディレクトリに移動します。
4. UNIX コマンド ライン プロンプトで次のように入力して、インストール スクリプトを実行します。

   ```
   sdadmreg_install
   ```

   画面に表示される指示に従います。

   sdadmreg_install ユーティリティは、エージェント ホストの ***ACEDATA*** ディレクトリに**sdconf.rec**と**server.cer**をインストールし、エージェント ホストの***ACEPROG*** ディレクトリに **sdadmreg** プログラムをインストールします。
5. プライマリでデータベース ブローカを起動してから、**sdadmreg** を実行します。

   Windows を使用している場合、RSA Authentication Manager Host Mode などの RSA Authentication Manager プログラムを起動すると、データベース ブローカが自動的に起動します。

   UNIX を使用している場合は、Authentication Manager で ***ACEPROG*/sdconnect start** コマンドを実行してデータベース ブローカを起動します。
6. UNIX コマンド ライン プロンプトで次のように入力して、自動登録 / 更新プログラムをエージェント ホストで実行します。

   ```
   ACEPROG/sdadmreg
   ```

   このプログラムは次の場合に実行できます。

   - 新しい Windows エージェント ホストに RSA Authentication Agent ソフトウェアをインストールする前、またはインストールした直後。エージェント ホスト レコードが存在しない場合や、Authentication Manager で自動登録が有効に設定されている場合は、エージェント ホスト レコードが Authentication Manager データベースに追加されます。
   - エージェント ホストに新しい IP アドレスを割り当てた場合。このエージェント ホストのノード シークレットがすでに作成されている場合は、新しいエージェント ホスト IP アドレスが Authentication Manager データベースのエージェント ホスト レコードに書き込まれます。
   - Authentication Manager の現在の **sdconf.rec** でエージェント ホストの **sdconf.rec** を更新しなければならない場合。更新した **sdconf.rec** は、エージェント ホストを再起動するまで有効になりません。**sdadmreg** はこの目的で定期的に実行しなければならない可能性があります (たとえば、エージェント ホストを再起動するたびに、などです)。

DHCP (Dynamic Host Configuration Protocol) のサポート

メモ：RSA Authentication Manager DHCP サポートを使用するエージェント ホストは、スタートアップ ファイルに **sdadmreg** プログラムを組み込んでおく必要があります。

sdadmreg プログラムは、DHCP (Dynamic Host Configuration Protocol) によるアドレスの変更を反映するために、Authentication Manager データベース内のエージェント ホストのレコードの IP アドレス フィールドを自動的にチェックし、更新します。

メモ：エージェント ホストの名前は同じままでなければなりません。名前と IP アドレスの両方が変更されると、Authentication Managerで新しいエントリが作成されます。

セキュリティ上の理由から、新しい RSA Authentication Manager エージェント ホストは、エージェント ホストからの最初の認証が成功するまで、競合しない IP アドレスを使用する必要があります。DHCP によって制御されない IP アドレスを新しいエージェント ホストに一時的に割り当てるようにすれば、IP アドレスが競合することはありません。初めて認証が成功した後、エージェント ホストを再起動すると、IP アドレスをエージェント ホストに割り当てる作業は DHCP に引き継がれます。次の例を参照してください。

- エージェント ホスト **hopper** は RSA Authentication Agent ソフトウェアを実行していて、IP アドレス 192.168.10.23 で RSA Authentication Manager データベースに登録されています。
- エージェント ホスト **hopper** がシャットダウンされ、IP アドレス 192.168.10.23 を解放しました。
- エージェント ホスト **eakins** がネットワークに参加し、DHCP サーバから IP アドレス 192.168.10.23 (**hopper** の以前のアドレス) を割り当てられました。**hopper** のエージェント ホスト レコードの IP アドレス エントリは “DHCP_UNASSIGNED *Agent Host number*” になります。
- エージェント ホスト **hopper** が再起動され、ネットワークに再度参加することを要求しました。
- DHCP サーバは **hopper** に IP アドレス 192.168.10.26 を割り当てました。
- **sdadmreg** プログラムが自動的に実行され、IP アドレスの変更を **hopper** のデータベース レコードに書き込みます。

エージェント ホストによる負荷分散

RSA ACE/Agent ソフトウェア 5.1 および 5.2 では、認証要求の負荷を自動的に分散できます。負荷を分散するには、レルム内の各 Authentication Manager にタイム リクエストを送信し、各 Authentication Manager の応答時間をもとに優先順位を判断します。もっとも応答の速い Authentication Manager にはもっとも高い優先順位が与えられ、エージェント ホストからもっとも多くの要求が送信されます。他の Authentication Manager の優先順位はそれよりも低くなり、送信される要求の数も少なくなります。この設定は、エージェント ソフトウェアが別のタイム リクエストを送信するまで有効です。Authentication Manager が次のタイム リクエストに異なる順番で応答すると、エージェント ホストは応答の順番に従って優先順位を変更します。

さらに、エージェント ホストは、Authentication Manager の代替 IP アドレス (エイリアス) がエージェント ホストの構成レコード ファイル (**sdconf.rec**) に指定されているか、またはエージェント ホストからの要求時に 6.1 の Authentication Manager から提供される場合、ファイアウォールを介して Authentication Manager に接続できます。RSA Authentication Agent ソフトウェアは、このエイリアス IP アドレスを使用して Authentication Manager に認証要求を送信する前に、エイリアス IP アドレス情報を自動的にチェックします。

この自動負荷分散処理の代わりに、各エージェント ホストが要求の処理に使用する Authentication Manager を指定することで、エージェント管理者が手動で負荷分散を定義することもできます。このとき、各 Authentication Manager に優先順位も割り当てて、エージェント ホストが認証要求を送信する頻度に関して、Authentication Manager 間で差を付けます。このオプションを使用するには、エージェント管理者が **sdopts.rec** という名前のテキスト ファイルに優先順位を定義します。**sdopts.rec** ファイルはエージェント ホストに作成します。

また、Authentication Manager にアクセスするために使用する追加のファイアウォール IP アドレスを定義することもできます。最後に、ホストがマルチホーム サーバーである場合は、エージェント ホストに対して最優先 IP アドレス (overriding IP address) を指定できます。これらは、オプションのテキスト ファイル **sdopts.rec** に定義した設定に依存します。

RSA Authentication Manager 管理者は、エージェント ホストが行う負荷分散に直接関わる必要はありません。しかし、管理しているレルム内のエージェント管理者が負荷分散をどのように管理しているのかについては把握しておく必要があります。

エージェント管理者が **sdopts.rec** ファイルを使用する場合は、Authentication Manager に対して設定した優先順位を把握することが特に重要です。これらのファイルで設定された優先順位が自動的に調整されることはないので、同じ Authentication Manager に要求を送信するエージェント ホストが多すぎて、パフォーマンスに悪影響を与える場合があり、最初は効果的な優先順位でも、状況が変化すると効果がなくなることも考えられます。RSA Authentication Manager 管理者はエージェント管理者と絶えず連絡を取り、できる限りシステムが円滑かつ効率的に実行されるように協力してください。

次のセクション「sdopts.rec ファイルによる手動負荷分散」は、エージェント管理者を対象としています。**sdopts.rec** ファイルを使用して、手動で負荷を分散させる手順について説明しています。

sdopts.rec ファイルによる手動負荷分散

手動負荷分散を指定するには、**sdopts.rec** ファイルを作成します。**sdopts.rec** ファイルの作成と編集には、任意のテキスト エディタを使用できます。

sdopts.rec ファイルを作成したら、エージェント ホスト プラットフォームの適切なディレクトリに保存してください。Windows の場合は ***%SYSTEMROOT%*¥System32** に保存します。UNIX の場合は、**/var/ace** ディレクトリ (または **$VAR_ACE** システム変数で指定されたディレクトリ) に保存します。

ファイルが誤って変更されないように保護するには、管理者だけが変更できるように、**sdopts.rec** ファイルでアクセス権の設定を変更します。

重要：sdopts.rec ファイルを変更したら、必ずエージェントを再起動して、変更を登録する必要があります。

このファイルには、次の種類の行を指定できます。

- コメント。各コメント行の先頭にはセミコロンを付けます。
- キーワード値ペア。次のいずれかの値を指定できます。

  CLIENT_IP=<*ip_address*>。エージェント ホストの最優先 IP アドレスを指定します。**Client_IP** キーワードは、ファイルで一度だけ使用できます。最優先 IP アドレスについては、72 ページの「エージェント ホストの最優先 IP アドレスの設定」を参照してください。

USESERVER=<*ip_address*>, <*priority*>。指定された優先順位に従ってエージェント ホストから認証要求を受信する (または受信できる) Authentication Manager を指定します。エージェント ホストが使用する Authentication Manager ごとに 1 つの設定を使用します各 **Useserver** キーワードの値には、Authentication Manager の実際の IP アドレスと、Authentication Manager に割り当てられた ***priority*** (優先順位) をカンマで区切って指定します。優先順位によって、Authentication Manager が認証要求を受信するかどうか、およびその頻度を定義します。

重要：sdopts.rec ファイルおよび **sdconf.rec** ファイルに指定できる Authentication Manager の最大数は**合計** 11 個です。

優先順位の値は、次の表に示す値のいずれかである必要があります。

優先順位	説明
2 ～ 10	Authentication Manager に割り当てられた優先順位に従って重みが付けられたランダム選択を行って、この Authentication Manager に認証要求を送信します。範囲は 2 ～ 10 です。値が大きいほど、Authentication Manager が受信する要求は多くなります。優先順位 10 の Authentication Manager は、優先順位 2 の Authentication Manager の約 24 倍の要求を受信します。
1	この Authentication Manager を最後の手段として使用します。優先順位 1 の Authentication Manager は、優先順位の高い Authentication Manager を利用できない場合にのみ使用されます。
0	この Authentication Manager を無視します。優先順位 0 は特別な状況でのみ使用できます。まず、**sdconf.rec** ファイルに登録されている 4 台の Authentication Manager のいずれかである必要があります。その条件が満たされる場合、優先順位 0 の Authentication Manager はエージェントの最初の認証にのみ使用できます。ただし、**sdopts.rec** ファイルに登録されている優先順位 1 ～ 10 のすべての Authentication Manager がエージェント ホストによって使用不可として認識されている場合は、優先順位 0 の Authentication Manager は使用されません。一般に、優先順位 0 を使用すると、Authentication Manager を使用せずにその Authentication Manager のファイルにエントリを追加できます。後で使用することになった場合は、その Authentication Manager の優先順位の値を変更できます。

USESERVER キーワードを付けて **sdopts.rec** ファイルに追加した各 Authentication Manager に、優先順位を割り当てる必要があります。そうしないと、そのエントリは無効と見なされます。ファイル内の IP アドレスは、エージェントが 6.1 の Authentication Manager との最初の認証の一部として受信する有効な Authentication Manager のリストに対してチェックされます。

ALIAS=*ip_address*, *alias_ip_address_1*[, *alias_ip_address_2*, *alias_ip_address_3*]。1 台の Authentication Manager に対して 1 つ以上の代替 IP アドレス (**エイリアス**) を指定します。Authentication Manager のエイリアスは、エージェントの **sdconf.rec** ファイルに指定できます。**ALIAS** キーワードを使用すると、追加ファイアウォールの IP アドレスを最大 3 つ指定できます。ファイアウォールを介してエージェントからアクセスできるのは、指定された Authentication Manager だけです。

ALIAS キーワードの値には、Authentication Manager の実際の IP アドレスと、その Authentication Manager のエイリアス IP アドレスを最大 3 つ指定します。エージェントは、実際の IP アドレスとエイリアス IP アドレスの両方にタイム リクエストを送信します。

ALIAS キーワードで指定された実際の IP アドレスだけは、指定される Authentication Manager から認識される必要があります。さらに、エージェントが受信するどの **Authentication Manager リスト**にも実際の IP アドレスが含まれている必要があります。Authentication Manager リストでは、レルム内で認識されるすべての Authentication Manager の実際の IP アドレスとエイリアス IP アドレスが提供され、エージェントは Authentication Manager が認証要求を確認した後、6.1 の Authentication Manager からこの Authentication Manager リストを受信します。

ALIASES_ONLY[=*ip_address*]。このキーワードを使用する場合は、少なくとも 1 台の Authentication Manager に対して、**sdconf.rec** ファイルまたは **sdopts.rec** ファイルでエイリアス IP アドレスが指定されていることを確認してください。

値を指定せずに、**ALIASES_ONLY** キーワードを使用すると、エイリアス IP アドレスが割り当てられている Authentication Manager に対してのみ、エージェントが要求を送信するように設定されます。**sdopts.rec** ファイルに **IGNORE_ALIASES** キーワードを最大 10 個指定することで、例外を設定することもできます。**IGNORE_ALIASES** キーワードは、アクセスするために実際の IP アドレスを使用する必要のある Authentication Manager を指定します。この例外のサンプルについては、71 ページの「ALIAS、ALIASES_ONLY、および IGNORE_ALIASES キーワードの使用例」を参照してください。

ALIASES_ONLY の値として、Authentication Manager の実際の IP アドレスを指定すると、このキーワードは、Authentication Manager へのアクセスにエイリアス IP アドレスだけが使用されることを指定します。

IGNORE_ALIASES[=*ip_address*]。値を指定せずに **IGNORE_ALIASES** キーワードを使用すると、**sdopts.rec** ファイル、**sdconf.rec** ファイル、または 6.1 の Authentication Manager が提供する Authentication Manager リストに登録されているすべてのエイリアス IP アドレスは無視されます。**sdopts.rec** ファイルに **ALIASES_ONLY** キーワードを最大 10 個指定することで、例外を設定することもできます。**ALIASES_ONLY** キーワードは、アクセスするためにエイリアス IP アドレスを使用する必要のある Authentication Manager を指定します。この例外のサンプルについては、71 ページの「ALIAS、ALIASES_ONLY、および IGNORE_ALIASES キーワードの使用例」を参照してください。

IGNORE_ALIASES の値として、Authentication Manager の実際の IP アドレスを指定すると、このキーワードは、Authentication Manager へのアクセスに Authentication Manager の実際の IP アドレスだけが使用されることを指定します。

USESERVER キーワードの使用例

ファイルに設定を指定する場合、どのような順序で指定してもかまいません。ただし、設定は 1 行に 1 つずつ個別に登録する必要があります。次の例は、**USESERVER** キーワードだけを使用した場合を示しています。

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign.Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.
USESERVER=192.168.10.23, 10
```

```
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
```

実際の IP アドレス 192.168.10.23 で識別される Authentication Manager は、Authentication Manager 192.168.10.22 よりも多くの認証要求を受信します。Authentication Manager 192.168.10.20 は、より優先順位の高い Authentication Manager を使用できない場合にのみ使用され、Authentication Manager 192.168.10.21 は、**USESERVER** キーワードの説明の優先順位 0 の定義で示したような、ごく稀な状況を除いて無視されます。

メモ：sdopts.rec ファイルでは、定義されているキーワードであれば、どのキーワードでも自由な組み合わせで指定できます。このため、**USESERVER** キーワードと **ALIAS** キーワードもこのファイルで一緒に使用できます。ただし、**USESERVER** キーワードは Authentication Manager への接続に使用されるエイリアス アドレスには影響を与えず、**ALIAS** キーワードは使用する Authentication Manager の指定には影響を与えません。

ALIAS、ALIASES_ONLY、および IGNORE_ALIASES キーワードの使用例

ファイルに設定を指定する場合、どのような順序で指定してもかまいません。ただし、設定は 1 行に 1 つずつ個別に登録する必要があります。次の例は、Authentication Managerエイリアス アドレスに関連するキーワードを使用したサンプルを示しています。

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign.Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from other IP
;addresses.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
ALIAS=192.168.10.23, 192.168.4.1, 192.168.4.2, 192.168.4.3
ALIAS=192.168.10.22, 192.168.5.2, 192.168.5.3
ALIAS=192.168.10.20, 192.168.5.2
ALIAS=192.168.10.21, 192.168.1.1
ALIASES_ONLY=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

この例では、デフォルト設定により、エイリアス IP アドレスまたは実際の IP アドレスが使用されます。ただし、2 つの例外があります。実際の IP アドレスが 192.168.10.23 である Authentication Manager には、3 つのエイリアス アドレスが指定されています。Authentication Manager 192.168.10.20 および 192.168.10.21 には、それぞれエイリアスが 1 つずつ指定されており、Authentication Manager 192.168.10.22 には 2 つのエイリアス アドレスが指定されています。**ALIAS** キーワードで指定されるエイリアスは、**sdconf.rec** または Authentication Manager リストで指定される任意のエイリアスに加えて提供されるエイリアスです。

メモ：sdopts.rec ファイルでは、定義されているキーワードであれば、どのキーワードでも自由な組み合わせで指定できます。このため、**USESERVER** キーワードと **ALIAS** キーワードもこのファイルで一緒に使用できます。ただし、**USESERVER** キーワードは Authentication Manager への接続に使用されるエイリアス アドレスには影響を与えず、**ALIAS** キーワードは使用する Authentication Manager の指定には影響を与えません。

例外として、**ALIASES_ONLY** キーワードの指定に従って、Authentication Manager 192.168.10.23 にエージェントからアクセスするには、Authentication Manager のエイリアス IP アドレスを使用しなければなりません。一方、**IGNORE_ALIASES** キーワードの指定に従って、Authentication Manager 192.168.10.22 にエージェントからアクセスするには、Authentication Manager の実際の IP アドレスを使用します。

次の例では、デフォルト設定により、エイリアスが無視されます。ただし、2 つの例外があります。

```
IGNORE_ALIASES
ALIASES_ONLY=192.168.10.23
ALIASES_ONLY=192.168.10.22
```

ALIASES_ONLY によって指定される例外では、エージェントはエイリアス IP アドレスのみを使用して、Authentication Manager 192.168.10.23 および Authentication Manager 192.168.10.22 に要求を送信することを指定しています。

次の例では、デフォルト設定により、エイリアスが使用されます。ただし、2 つの例外があります。

```
ALIASES_ONLY
IGNORE_ALIASES=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

IGNORE_ALIASES によって指定される例外では、エージェントは実際の IP アドレスのみを使用して、Authentication Manager 192.168.10.23 および Authentication Manager 192.168.10.22 に要求を送信することを指定しています。

エージェント ホストの最優先 IP アドレスの設定

複数のネットワーク インタフェース カードが搭載された (したがって複数の IP アドレスを使用する) エージェント ホストで RSA Authentication Agent を実行する場合、エージェント管理者はエージェント ホストと RSA Authentication Manager の間の暗号化された通信に、プライマリ エージェント ホスト IP アドレスを指定する必要があります。

通常、エージェント ホストは自分の IP アドレスを検出しようとします。アドレスの選択はエージェント ホスト自体が行うため、複数のアドレスを持つエージェント ホストが、Authentication Manager で認識されないアドレスを選択した結果、エージェントと Authentication Manager の間の通信が不能になることがあります。エージェント管理者は **sdopts.rec** ファイルで **Client_IP=** キーワードを使用することで、キーワードの値として指定したプライマリ IP アドレスが常に Authentication Manager との通信に使用されるように設定できます。

エージェント ホストの各プライマリ IP アドレスは、Authentication Manager データベースのエージェント ホスト レコードに指定する必要があります。エージェント ホストの他の IP アドレスも、フェールオーバ用に (**セカンダリ ノード**として) 登録できます。

RSA Authentication Manager システムでエージェント ホストの自動登録機能を使用している場合 (詳細については 64 ページの「エージェント ホストの自動登録 / 更新」を参照)、各エージェント ホストのプライマリ IP アドレスは、エージェント ホストのレコードに自動的に入力され、IP アドレスが変更されると、レコードも必ず更新されます。

エージェント ホストを手動で登録する場合、Authentication Manager 管理者は、Authentication Manager データベースのエージェント ホスト レコードのエージェントのプライマリ IP アドレスが、エージェント ホストの構成レコードまたは **sdopts.rec** ファイルに指定されているプライマリ IP アドレスと同一になるようにしなければなりません。これらの2つの設定が一致しない場合、エージェント ホストと Authentication Manager の間の通信は失敗します。エージェント ホストに対してセカンダリ IP アドレスも指定する場合は、これらのアドレスもレコードに入力し、変更されたらすべてのアドレスを更新する必要があります。

次の「Client_IP キーワードの使用」の説明は、RSA Authentication Agent 管理者を対象としています。**sdopts.rec** ファイルで **Client_IP** キーワードを使用して、エージェント ホストのプライマリ IP アドレスを指定することで、エージェント ホストが Authentication Manager と通信するときに、常にこのアドレスが使用されるようにする方法について説明します。

RSA Authentication Agent for Microsoft Windows の管理者は、[RSA Authentication Agent Control Panel] でエージェント ホストの最優先 IP アドレスを指定することができます。Control Panel を使用してエージェント ホストのプライマリ IP アドレスを指定するには、『RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide』を参照してください。

Client_IP キーワードの使用

エージェント ホストの既存の **sdopts.rec** ファイルに **Client_IP** キーワードを追加することができます。**sdopts.rec** ファイルが存在しない場合は、このファイルを作成することもできます。詳細については、68 ページの「sdopts.rec ファイルによる手動負荷分散」を参照してください。

メモ：DHCP (Dynamic Host Configuration Protocol) は、エージェント ホストに動的に IP アドレスを割り当てます (詳細については、66 ページの「DHCP (Dynamic Host Configuration Protocol) のサポート」を参照してください)。アドレスの競合を回避するには、複数の IP アドレスを持つエージェント ホストに対して、DHCP を有効にしないようにしてください。逆に、単一の IP アドレスを持つエージェント ホストに対して、**Client_IP** キーワードを使用する必要はありません。このようなエージェント ホストには、優先する代替アドレスがないからです。

sdopts.rec ファイルで最優先する IP アドレスを指定するには、次の例に示すように **Client_IP** キーワードを使用します。

```
CLIENT_IP=192.168.10.19
```

sdopts.rec ファイルでこのように記述すると、エージェント ホストは常に RSA Authentication Manager との通信で、指定された IP アドレスを使用します。

エージェント ホストの自動登録機能を使用しない場合は、RSA Authentication Agent 管理者として、エージェント ホストを RSA Authentication Manager システムで最初に構成するときに、エージェント ホストのプライマリおよびセカンダリ IP アドレスを Authentication Manager 管理者に必ず知らせる必要があります。エージェント ホストのアドレスが変わったら、Authentication Manager 管理者にすぐに知らせて、Authentication Manager データベースのエージェント ホスト レコードを更新してもらいます。

旧バージョンのエージェント ホスト

RSA Authentication Manager 6.1 では、旧バージョンのエージェント ホスト (v 5.0 より前のバージョンの RSA ACE/Agent ソフトウェアを実行しているエージェント ホスト) を引き続きサポートします。このセクションでは、旧バージョンのエージェント ホストに関連する問題点について説明します。

旧バージョンのエージェント ソフトウェアで必要とされる Authentication Manager の定義

RSA Authentication Manager 6.1 は、v5.0 で導入されたアーキテクチャを基礎にしています。RSA ACE/Server 5.0 のアーキテクチャでは、以下の 2 つの変更を行ったことにより、以前のメジャー バージョンより認証速度が向上しています。1 つは複数の認証レプリカの使用であり、もう 1 つは、認証要求にもっとも速く応答するレプリカを選択する RSA Authentication Agent ソフトウェアの新機能です。v5.0 のアーキテクチャを基礎にしたエージェント ソフトウェアはレルム内のすべてのレプリカを認識するので、認証要求をその中のどのレプリカにでも送信できます。

旧バージョンのエージェント ホストには負荷分散機能がなく、エージェント ホストの構成ファイル (**sdconf.rec**) が識別できるのはマスタとスレーブだけなので、ユーザの認証はこれらの 2 つの Authentication Manager に対してだけ要求できます。

旧バージョンのエージェント　ホストがシステムに含まれている場合は、RSA Authentication Manager 6.1 のインストール ソフトウェアは、Authentication Manager 構成ファイル (**sdconf.rec**) を変更するときに、元のマスタとスレーブの識別子を保存します。この情報は旧バージョンの各エージェント ホストの構成ファイルに記録されており、この情報によって、元のマスタとスレーブ (6.1 環境ではレプリカとして構成) は、新しい環境内で旧バージョンのエージェント ホストに対するアクティング マスタおよびアクティング スレーブとして割り当てられます。

メモ：インストール後に、旧バージョンのエージェント ホスト (つまり、5.0 より前の RSA ACE/Agent ソフトウェアを実行するエージェント ホスト) を追加する場合は、エージェント ホスト構成レコードにアクティング マスタおよびアクティブ スレーブの名前を手動で入力しなければなりません。この作業は、エージェント ホスト レコードを自動登録プロセスで作成した場合にも行う必要があります。エージェント ホスト レコードの変更の詳細については、74 ページの「旧バージョンのエージェント ホスト」を参照してください。

旧バージョンのエージェント ホストを含むレルムのマージ

RSA Authentication Manager 6.1 をインストールした後、旧バージョンのエージェント ホストを含む別のレルムとデータベースをマージすることができます。マージする場合は、これらの**インポート**された旧バージョンのエージェント ホストが、その後も確実に認証要求を元のマスタおよびスレーブに送信するようにしなければなりません。

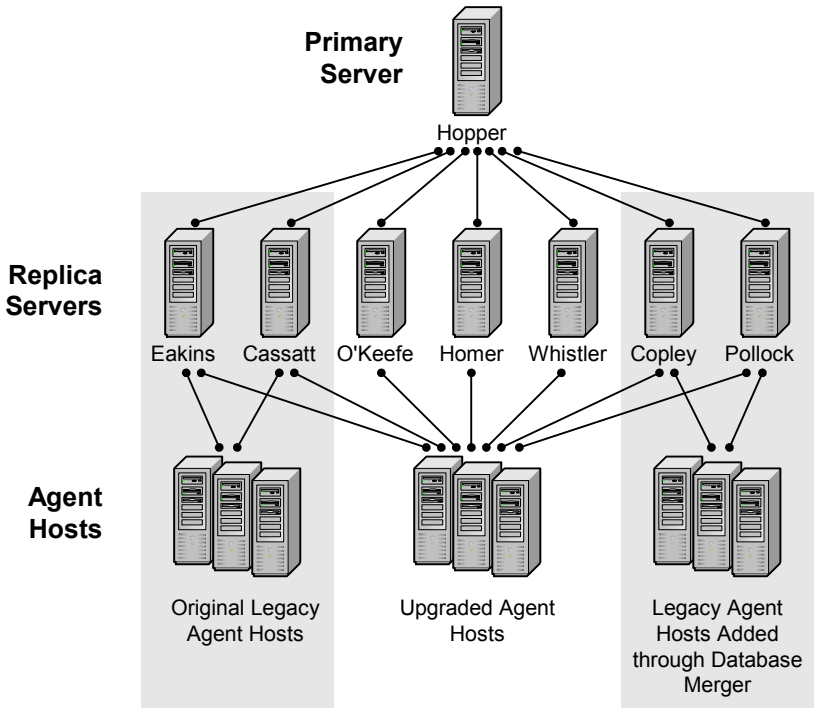
マージ手順を実行する前に、プライマリで **sdconf.rec** を編集して、自分のレルムの以前のマスタおよびスレーブではなく、インポートするレルムのマスタおよびスレーブを指定するようにしてください。

この変更によって、レルム内の既存の旧バージョンのエージェント ホストの動作が影響を受けることはなく、その後も構成ファイルで指定されたアクティング マスタおよびアクティング スレーブに認証要求を送信します。ただし、データベースのマージ手順で、新しいアクティング マスタとアクティング スレーブの情報は、プライマリの **sdconf.rec** から新しい旧バージョンの各エージェント ホストのエージェント ホスト レコードにコピーされます。**sdconf.rec** の指定を変更していなければ、レルムに追加されたばかりのエージェント ホストも含めて、すべての旧バージョンのエージェント ホストからの認証要求は、以前と同じ Authentication Manager のペアに送信されます。

操作手順：ご使用のプラットフォームの『インストール ガイド』に記載されているデータベース マージ手順を参照してください。

次の図は、このセクションで説明するシナリオを示しています。

Servers and Agent Host Connections in an Upgraded RSA ACE/Server 5.2 Realm



左側の灰色の領域は、サンプル レルムを RSA Authentication Manager 6.1 にアップグレードした時点でレルムに属していたエージェント ホストです。アップグレードする前は、“Eakins” および “Cassatt” という Authentication Manager はマスタとスレーブだったため、旧バージョンの各エージェント ホスト レコードで、旧バージョンのエージェント ホストのアクティング マスタおよびアクティング スレーブとして識別されています。各エージェント ホストの構成ファイルは、RSA Authentication Manager のアップグレード プロセスでは変更されず、Eakins をマスタ、Cassatt をスレーブとして指定しています。したがって、エージェント ホストはすべての認証要求をこれらの 2 台の Authentication Manager にのみ送信しなければなりません。

中央の領域は、RSA ACE/Agent 5.0 またはそれ以降のバージョンにアップグレードされたエージェント ホストです。これらのエージェント ホストは、レルム内のどのレプリカにも認証要求を送信できます。

右側の灰色の領域は、データベースを別のレルムのデータベースとマージすることで、レルムに追加された旧バージョンのエージェント ホスト群を示しています。新しく追加されたエージェント ホストはすべての認証要求をこれらの Authentication Manager に送信しなければならないので、そのレルムの前のマスタとスレーブ (“Copley” と “Pollock”) は、アクティング マスタおよびアクティング スレーブとして指定してください。Copley と Pollock は、構成ファイルで指定されたマスタとスレーブであるため、エージェント ホスト レコードでこれらの権限に Copley と Pollock が指定されていない場合、旧バージョンのエージェント ホストは機能できません。

メモ：図に示したシステムでは、RSA Authentication Manager アドバンスド ライセンスが必要です。RSA Authentication Manager ベース ライセンスでは、プライマリとレプリカをそれぞれ 1 台ずつしか使用できません。

旧バージョンのエージェント ホストの自動登録機能のサポート

旧バージョンのエージェント ホストでは、自動登録機能が完全にはサポートされていません。旧バージョンのエージェント ホストの **sdconf.rec** ファイルには、データベースのエージェント ホスト レコードで割り当てられているアクティング マスタとアクティング スレーブに一致するマスタとスレーブが登録されている必要があります。エージェント ホストの **sdconf.rec** ファイルとデータベースが一致しない場合、旧バージョンのエージェント ホストを介してユーザが認証を受けることはできません。

このような状況は自動登録の際に問題となります。自動登録機能では、Authentication Manager の **sdconf.rec** ファイルが使用されますが、このファイルが、エージェント ホストの **sdconf.rec** ファイル内のマスタおよびスレーブの情報、およびデータベース内のアクティング マスタおよびアクティング スレーブの情報と一致する場合と、一致しない場合があるためです。旧バージョンのエージェント ホストが自動登録機能を使用して **sdconf.rec** ファイルを更新すると、データベースで割り当てられているアクティング マスタおよびアクティング スレーブとは異なるものが登録されている **sdconf.rec** ファイルを受け取る可能性があります。旧バージョンのエージェント ホストが、更新された **sdconf.rec** ファイル内のアクティング マスタおよびアクティング スレーブに対して認証を試みると、その認証は失敗します。

このため、自動登録機能を使用する旧バージョンのエージェント ホストがある場合は、これらのすべてのエージェント ホストで同じアクティング マスタおよびアクティング スレーブを使用する必要があります。さらに、Authentication Manager の **sdconf.rec** ファイルには、エージェント ホストの **sdconf.rec** ファイルと同じアクティング マスタおよびアクティング スレーブが登録されている必要があります。

インストール後に、v5.0 より前の同じエージェント ソフトウェアを実行するエージェント ホストを追加する場合、そのエージェント ホストが認証を正しく処理するには、エージェント ホスト レコードにアクティング マスタ (および必要に応じてアクティング スレーブ)の名前とIPアドレスを入力する必要があります。Authentication Manager データベースのエージェント ホスト レコードが自動登録機能で自動的に作成されたのか、管理者によって手動で作成されたのかに関係なく、この作業が必要です。エージェント ホスト レコードを編集して、アクティング マスタの ID を指定するまで、エージェントは認証要求をどこにも送付できません。

操作手順：[Agent Hosts] > [Edit Agent Host] の順にクリックします。レコードを編集するエージェント ホストを選択し、[OK] をクリックして、[Edit Agent Host] ダイアログ ボックスを表示します。[Assign Acting Servers] をクリックします。必要に応じて [Help] をクリックして、表示される情報を参照してください。

Configuration Record Editor

Configuration Record Editor を使用すると、任意の Authentication Manager 構成ファイルのアクティング マスタおよびアクティング スレーブのフィールドを変更できます。この操作が必要になる理由については、74 ページの「旧バージョンのエージェント ソフトウェアで必要とされる Authentication Manager の定義」を参照してください。

ACEPROG ディレクトリには 2 つのバージョンの Configuration Record Editor があります。それは、Windows 用の GUI バージョン (**sdcfgedit_ui.exe**) と UNIX 用のコマンド ライン バージョン (**sdcfgedit**) です。コマンド ライン バージョンは、Windows プラットフォームでも使用できます。

マスタおよびスレーブのデータの編集 (GUI バージョン)

既存の構成ファイルでアクティング マスタおよびアクティング スレーブを編集するには

1. Authentication Manager で ***ACEPROG*** ディレクトリに移動し、**sdcfgedit_ui.exe** をダブルクリックします。
2. [Select Configuration File] をクリックします。
3. [ファイルを開く] ダイアログ ボックスで、編集する構成ファイルを選択し、[開く] をクリックします。
4. 各アクティング Authentication Manager の名前と IP アドレスを [Name] ボックスおよび [IP Address] ボックスに入力します。

   DNS を使用していて、[Resolve host name and addresses] チェックボックスがオンになっている場合は、[Name] ボックスの入力を終了した後に TAB を押すと、Authentication Manager の IP アドレスが自動的に挿入されます。
5. [OK] をクリックして構成ファイルを保存します。

マスタおよびスレーブのデータの編集 (コマンド ライン バージョン)

コマンド ライン バージョンの Configuration Record Editor では、**sdconf.rec** ファイルの場所を指定し、新しいアクティング マスタとアクティング スレーブの名前または IP アドレスを指定する必要があります。

UNIX で既存の構成ファイル内のアクティング マスタおよびアクティング スレーブを編集するには

ACEPROG ディレクトリに移動し、次のコマンドを入力します。

```
sdcfgedit -ffilename -mname,IPAddress
-sname,IPaddress
```

このコマンドには、次のオプション スイッチがあります。

- **-f*filename*** は、構成ファイルのフルパスとファイル名を指定します。
- **-m*name, IP address*** は、アクティング マスタの名前と IP アドレスを指定します。
- **-s*name, IP address*** は、アクティング スレーブの名前と IP アドレスを指定します。

メモ：構成ファイルからアクティング マスタまたはアクティング スレーブの指定を削除するには、名前の場所にダッシュを使用します。たとえば、アクティング スレーブの指定を削除するには、**-s-** を使用します。

Authentication Manager の名前は完全修飾名で解決されます。ただし、オプションの *-p* スイッチを使用した場合は、入力したままの名前が使用されます (**-p** スイッチはコマンド ラインの **-m** スイッチの直前に入力する必要があります)。Authentication Manager の IP アドレスを指定しなかった場合は、システムの標準のアドレス解決方法を使用して、アドレスが解決されます。

4 レルム アドミニストレーション

この章では、RSA Authentication Manager システムでレルムの計画、作成、および変更を行う方法について説明します。

レルムという用語は、プライマリ Authentication Manager とレプリカ Authentication Manager、データベース、ユーザ、トークン、およびエージェント ホストを指します。レルムはレルム間認証のために、メッセージの交換をサポートします。この章では、複数のレルムが含まれる環境に関して説明しており、RSA Authentication Manager アドバンスド ライセンスを購入されたお客様だけを対象としています。詳細については、付録 A「ライセンス」を参照してください。

レルムがレルム間認証に参加するには、参加するレルムのリストをプライマリで作成する必要があります。

レルム間認証

必要最低限の管理作業を実行するだけで、他のレルムのユーザが RSA SecurID による認証を受けた後、エージェント ホストにアクセスできるように設定できます。レルム間認証を有効にするには、次のセクション「他のレルムのユーザのレコードの自動作成」または 79 ページの「リモート ユーザ レコードの手動作成」を参照してください。

他のレルムのユーザのレコードの自動作成

次の 2 つの条件が満たされる場合、他のレルムのユーザは認証を受け、エージェント ホストにアクセスできます。

- 認識されるすべてのユーザに対してエージェント ホストがオープンであること。
- エージェント ホストで認証を受けようとしたユーザが不明なときに、エージェントが他のレルムを検索するように構成されていること。

エージェント ホストでこれらの設定を行っておけば、認証を受けようとするユーザのログイン名がローカル RSA Authentication Manager データベースから見つからない場合、その認証の問い合わせは、データベースに登録されているすべてのレルムにブロードキャストされます。ユーザのホーム レルムが検索され、ユーザが入力した認証情報が正しいことが確認されると、Authentication Manager はそのユーザのリモート ユーザ レコードを作成し、格納します。そのユーザが後で再度認証を受ける場合は、登録されているすべてのレルムに対して問い合わせを行う必要がなく、ユーザのホーム レルムで直接確認されます。詳細については、80 ページの「レルム間認証でのデフォルト ログイン」を参照してください。

リモート ユーザ レコードの手動作成

リモート ユーザ レコードは自動処理で作成することも、手動で作成することもできます。リモート ユーザ レコードを使用すると、ローカル レルムの制限されたエージェント ホストで、他のレルムのユーザをローカル ユーザであるかのようにアクティブ化できます。ローカル レルムのオープン エージェント ホストの場合は、このように明示的にアクティブ化する必要がありません。オープン エージェント ホストの場合、レコードに登録されているユーザは認証を受けることができ、登録されているすべてのレルムに要求をブロードキャストする必要はありません。

レルム内の制限されたエージェント ホストでリモート ユーザをアクティブ化するには、リモート ユーザのユーザ レコードを Authentication Manager データベースに作成し、制限されたエージェント ホストでそのユーザをアクティブ化します。

RSA Authentication Manager システムはリモート エイリアスを使用して、ログインの競合を防止します。詳細については、次のセクション「レルム間認証でのデフォルト ログイン」を参照してください。

レルム間認証でのデフォルト ログイン

同じレルム内の各ユーザは固有のデフォルト ログインを使用しなければなりませんが、レルム間認証環境の異なるレルムのユーザが同じデフォルト ログインを使用してもかまいません。異なるレルムに所属するユーザが同じデフォルト ログインを使用した結果、問題が発生するのは、次のような状況です。

- ユーザが自分のレルム以外で認証を受け、RSA Authentication Manager で保護されているリソースを使用する必要がある場合。
- 複数の既存のレルムを 1 つにマージ (結合) する場合。

  データベース ダンプ / ロード ユーティリティ (各プラットフォームの『インストール ガイド』を参照) を使用すると、複数のレルムのデータベースを v6.1 データベースにロードでき、その結果、すべてのデータがマージされます。重複するデフォルト ログインがあると、マージ操作中にエラーが発生します。

ユーザがリモート レルムの保護されているリソースにアクセスしようとすると、リモート レルムの Authentication Manager はまず、そのレルムのデータベースから対応するログインを検索します。Authentication Manager が一致するログイン名を見つけても、ユーザが入力した PASSCODE が異なる場合には、そのリモート ユーザのアクセスを拒否し、認証要求を他のレルムに通知しません。他のレルムのユーザがアクセス試行を続行すると、同じログインを使用しているローカル ユーザのトークンが最終的に無効に設定されます。

この状況では、他のレルムのユーザはリモート レルムで他のデフォルト ログインを使用する必要がありますが、認証が実際に行われる、ユーザのホーム レルムの Authentication Manager では、そのレルムに登録されているデフォルト ログインが必要とされます。このような競合を解決するには、リモート レルムの管理者は、他のレルムのユーザのリモート ユーザ レコードを作成することで、リモート デフォルト ログイン名をそのユーザのホーム デフォルト ログイン名の代わりに使用するようにしなければなりません。2 つのデフォルト ログイン名は同一でなく、それぞれが使用されるレルム内で固有のログイン名である必要があります。つまり、リモート デフォルト ログイン名は、ホーム デフォルト ログイン名のエイリアスとして設定されます。

たとえば、**Joshua Abrams** というユーザがレルム *okeefe* からレルム *cassatt* にアクセスしたとしましょう。*okeefe* でのこのユーザのデフォルト ログインは **jba** です。*cassatt* では、**Jane Anderson** というユーザがすでに **jba** を使用しています。*cassatt* の管理者は **Joshua Abrams** をリモート ユーザとして追加し、リモート レルムでこのユーザが使用するデフォルト ログインとして **jba1** を追加し、リモート エイリアスとして「jba」と入力しました。*cassatt* の Authentication Manager が **Joshua Abrams** の認証の試みを *okeefe* に送信する場合は、リモート ユーザ レコードのデフォルト ログインを無視し、リモート エイリアス **(jba)** を送信します。これは、*okeefe* の Authentication Manager が期待しているログインです。

メモ: [Remote Alias] フィールドにエントリが必要です。このエントリは [Default Login] フィールドのエントリと同じでもかまいません。

一部のレルムが RSA ACE/Server 5.0.1 以降にアップグレードされていない場合

レルム間認証環境のすべてのレルムが RSA ACE/Server 5.0.1 またはそれ以降のバージョンにアップグレードされるまで、レルム間認証をサポートするために追加管理作業が必要になります。詳細については、RSA セキュリティ正規販売代理店にお問い合わせください。

レルム間認証の計画

レルム間認証の計画を立てるには、次のことを考慮してください。

- レルム間認証には、レルムを 6 つまでサポートする RSA Authentication Manager アドバンスド ライセンスが必要です。
- レルム間認証では、レルム管理者間の密接な協力が必要です。たとえば、レルム間で信頼関係を確立するために、レルム管理者はトークンのシリアル番号とトークンコードを共有しなければなりません。レルム管理者は複数のレルム間レベルの問題に協力して対処しなければなりません。
- ログイン名はすべてのレルムで一意になるように設定する必要があります。一意でない場合は、他のレルムのユーザはリモート ログインのエイリアスを自分のホーム レルムのログイン名に設定する必要があります。
- RSA Authentication Manager マシンのアドレスが変更された場合、セキュリティ管理者はすべてのレルムにそのことを通知しなければなりません。リモート レルムの管理者は、[Edit Realm] ダイアログ ボックスを使用してアドレスを更新しなければなりません。ネットワーク構成を変更すると、管理コストが一時的に増加します。
- 認証要求に対して、各レルムで同じ UDP ポートを使用するように設定しなければなりません。
- エージェントのタイムアウトの時間は、リモート認証要求の場合もローカル要求と同じです (デフォルトは 5 秒)。ネットワークが低速の場合は、Authentication Manager が肯定応答を返す前に、エージェント ホストがタイムアウトになることがあります。このような場合は、エージェントのタイムアウト値を大きくしなければなりません。
- 認証に参加するすべてのレルムで、External Authorization を有効にするか、External Authorization を無効にするか、どちらかに統一する必要があります。External Authorization が有効なレルムと無効なレルムとが混在していると、レルム間認証は失敗します。External Authorization の詳細については、209 ページの「承認手順のカスタマイズ」を参照してください。

メモ：レルム間認証の概要については、25 ページの「レルム間モデル」を参照してください。

レルム間認証には、動的に割り当てられる UDP ポートが必要です。UDP ポートはリモート レルムとユーザのホーム レルムの間の通信、および RSA Authentication Manager 上の特定の種類の内部通信に使用されます。RSA Authentication Manager で実行されるそれぞれのプロセス (Windows プラットフォームの **acesrvc_be.exe** または UNIX プラットフォームの **aceserver_be**) に対して、利用可能な UDP ポートが 1 つずつ必要です。

レルム間にファイアウォールがある場合は、レルム間認証中に必要なポートが割り当てられるように、少なくとも 11 個の範囲の UDP ポートがオープンされている必要があります。RSA Authentication Manager for Windows では Windows レジストリで、RSA Authentication Manager for UNIX では環境変数として、ポート番号の最大値と最小値を設定して、Authentication Manager で同じ範囲のポート番号を使用するように構成する必要があります。最大ポート番号は、最小ポート番号より 10 だけ大きい値でなければなりません。デフォルト設定では、最小ポート番号は 0 に設定されています。これは、最初に利用可能なポートが通信に使用されることを意味します。最大ポート番号は 65,535 に設定されています。レルム間にファイアウォールがない場合は、RSA Authentication Managerがレルム間の通信に使用するポート番号の範囲を制限する必要はありません。

重要：必要な範囲のポート番号が常に利用可能であるようにしてください。RSA Authentication Managerがポートをバインドできないと、致命的なエラーが発生します。正しい範囲のポート番号を設定し、Authentication Manager を再起動してください。

RSA Authentication Manager for Windows でポート番号の範囲を制限するには

1. プライマリで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。
2. [Start & Stop RSA Authentication Manager Services]パネルで、[Stop Auth Service Only] をクリックします。
3. [Configure Authentication Processes] で、ポート範囲を指定し、[OK] をクリックします。
4. [Start & Stop RSA Authentication Manager Services] パネルで、[Start All] をクリックします。

RSA Authentication Manager for UNIX でポート番号の範囲を制限するには

1. Authentication Manager プロセスが実行されていないことを確認します。
2. **MINIMUM_BE_PORT** 環境変数に、使用するオープン状態の UDP ポートの最小ポート番号を設定します。
3. **MAXIMUM_BE_PORT** に、使用するオープン状態の UDP ポートの最大ポート番号を設定します。

Authentication Manager スタートアップ スクリプト (**/ace/prog/aceserver**) に、環境変数を設定する行を記述することもできます。VAR_ACE、USR_ACE、および DLC の値を設定するスタートアップ スクリプトのセクションに、行を記述します。たとえば、最小ポート番号を 10,000、最大ポート番号を 10,011 にする場合は、次の行を記述します。

```
MINIMUM_BE_PORT=10000
export MINIMUM_BE_PORT
MAXIMUM_BE_PORT=10011
export MAXIMUM_BE_PORT
```

これらの変数を設定しないと、デフォルト値 (1024 ～ 9999) が使用されます。

メモ：RSA Authentication Manager 6.1 を再インストールした場合、最小ポート番号と最大ポート番号はデフォルト値に設定されます。最小値と最大値を再設定して、使用するポートの範囲を反映してください。

レルムの作成と変更

ローカル レルム以外で認証を受けるように設定するには、リモート レルムをローカル Authentication Manager データベースに登録し、ローカル レルムをリモート Authentication Manager データベースに登録しなければなりません。レルムを追加および変更するには、レルム管理者であるか、またはレルム管理者の権限を含むカスタムの役割が設定されている必要があります。

この後の説明では、**ローカル レルム**は自分が管理している RSA Authentication Manager を指し、**リモート レルム**は自分のデータベースに追加するレルムを指します。

レルム レコードを追加するには、組織内の他のレルム管理者との密接な協力が必要です。Authentication Manager データベースにリモート レルムを登録するには、そのレルムに関する次の情報が必要です。

- プライマリの名前と IP アドレス。
- ローカル レルムにアクセスしているリモート ユーザを認証するための1つまたは 2 つのリモート Authentication Manager の名前と IP アドレス。2 つある場合は、リモート レルム管理者が指定したとおりに、優先 Authentication Manager とフェールオーバ Authentication Manager を区別しなければなりません。

  メモ : レルム シークレットは、最初はプライマリを優先 Authentication Manager として使用して確立する必要があります。レルム シークレットを確立した後、優先 Authentication Manager とフェールオーバ Authentication Manager を更新できます。また、優先 Authentication Manager とフェールオーバ Authentication Manager を更新する場合は、他のレルムの情報も同様に更新する必要があります。

  リモート ユーザがローカル レルムからエージェント ホストにログオンしようとすると、エージェント ホストはローカル レルムの Authentication Manager に認証要求を送信し、ローカル Authentication Manager はリモート レルムの優先 Authentication Manager に要求を転送します。優先 Authentication Manager が応答しない場合、ローカル Authentication Manager は次にフェールオーバ Authentication Manager に要求を送信します。フェールオーバ Authentication Manager も応答しない場合は、レルム間認証は失敗します。レルム間の認証要求が成功するには、いずれかの Authentication Manager が**動作していなければなりません**。
- 認証サービスのポート番号 (ローカル Authentication Manager の認証ポート番号と一致する必要があります)。
- リモート レルム管理者のトークンのシリアル番号。
- リモート レルム管理者のトークンに表示される一連のトークンコード。

リモート レルムに関するこれらの情報の他に、リモート レルムにアクセスするローカル ユーザを認証する 1 つまたは 2 つのローカル Authentication Manager の名前と IP アドレスも用意しておく必要があります。2 つのローカル Authentication Manager を使用する場合は、一方を優先 Authentication Manager、もう一方をフェールオーバ Authentication Manager として指定してください。この情報は、リモート レルム管理者に渡してください。

ローカル レルムでのこれらのサーバの機能は、リモート レルムでの優先 Authentication Manager およびフェールオーバ Authentication Manager の機能と同じです。ローカル ユーザがリモート レルムのエージェント ホストにログオンしようとすると、認証要求はまずローカル レルムの優先 Authentication Manager に転送され、優先 Authentication Manager が応答しない場合は、フェールオーバ Authentication Manager に転送されます。レルム間認証が成功するには、いずれかの Authentication Manager が応答しなければなりません。

操作手順 : [Realm] メニューの [Add Realm] をクリックしてレルムを追加します。詳細については、[Help] をクリックして表示される情報を参照してください。

リモート レルム管理者のトークンに表示される一連のトークンコードを入力すると、初期認証トランザクションで 2 つの重要な作業が行われます。

- ローカル レルム (ローカル Authentication Manager) とリモート レルムの間でレルム シークレットが確立されます。レルム シークレットとは、ローカル レルムとリモート レルムだけが知っているランダムな文字列です。レルム シークレットは、2 台のマシン間で送信されるパケットの暗号化に使用される鍵の一部です。ローカル レルムとリモート レルムの間で認証要求を交換するには、その前にレルム シークレットを確立しておかなければなりません。
- ローカル レルム レコードがリモート レルム データベースに自動的に追加されます。ローカル レルム レコードをリモート レルム データベースに追加するために、リモート レルムの管理者が何らかの操作を実行する必要はありません。ローカル レルム レコードがリモート レルム データベースにすでに存在する場合は、「Remote error inserting realm (レルムの追加でリモート エラーが発生しました)」というエラー メッセージが表示されます。この場合は、レルム シークレットを確立する前に、ローカル レルム レコードをリモート データベースから削除しなければなりません。

5 データベースのメンテナンス (Windows)

この章では、RSA Authentication Manager データのバックアップ、復元、オフライン ストレージの作成方法、および拡張データ レコードの情報を更新する方法について説明します。また、RSA Authentication Manager Host Mode から外部プロシージャを直接実行する手順についても説明します。

適切なディスク容量の確保

ファイル システムに空きがなくなり、RSA Authentication Manager データベースに書き込むことができなくなると、Authentication Manager プログラムは中断されます。必要最低限の空きディスク領域を確保できるように、必要な処置をとってください。

重要：プライマリまたはレプリカ Authentication Manager のディスクの空き領域は、ディスク容量の 10% 未満にならないようにしてください。

必要なディスク容量は各システムで異なるため、次の表に示すデータベース サイズの例は、単なるガイドラインとして参考にしてください。

ユーザ数	エージェント ホスト数	1 日の監査証跡エントリ数	Authentication Manager データベースのサイズ	ログ データベースが毎日拡大するサイズ	イベント ログが拡大するサイズ
100	50	1000	1.8 MB	1 MB	0.1 MB
1000	500	10000	2.2 MB	5 MB	0.5 MB
10000	5000	25000	19.2 MB	11 MB	1.1 MB

データベース圧縮ユーティリティによるディスク領域の再利用

ディスク領域を効率よく利用するために、Authentication Manager データベースとログ データベースは定期的に圧縮しなければなりません。このため、RSA Authentication Manager には RSA Authentication Manager データベースで使用されていたディスク領域を再利用できるようにする圧縮ユーティリティが用意されています。たとえば、古いログ レコードの消去など、大量の削除操作を実行した後、圧縮ユーティリティを使用して、ログ データベースで使用されていないディスク領域を解放できます。

圧縮中にプライマリでデータベース ブローカを実行しないでください。圧縮ユーティリティは、プライマリで認証サービスやその他の RSA Authentication Manager プログラムをシャットダウンした後で使用してください。

データベース ファイルを圧縮するには

1. Windows Administrator としてログオンします。
2. すべての Authentication Manager プログラムとデータベース ブローカを終了します。

3. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Database Tools] > [Compress] の順にクリックします。

   [RSA Authentication Manager Database Compression] ダイアログ ボックスが表示されます。このダイアログ ボックスには、使用できるディスク容量とデータベースへのパス名が表示されます。

4. [Compress Log Database] チェックボックスと [Compress Server Database] チェックボックスのいずれか一方または両方をオンにします。

   圧縮に必要なディスク容量と、使用できるディスク容量が表示されます。プライマリがインストールされているドライブに十分な容量がない場合は、圧縮を開始する前に空き領域を確保する必要があります。また、別のドライブやパーティションに利用できる領域がある場合は、そのドライブまたはパーティション上のディレクトリの場所と名前を [Path] ボックスに入力してください。

   重要：[Do not load delta records] チェックボックスは、欠陥のあるレコードによってデータベースに発生する問題に対処するためのものです。RSA セキュリティ正規販売代理店から指示がない限り、このチェックボックスをオンにしないでください。

5. [OK] をクリックします。

   データベースが圧縮されている間、圧縮の進行状況が画面に表示されます。最後の 2 行には、データベースの圧縮前のサイズと、圧縮後のサイズが表示されます。

6. 表示される情報のすべてをファイルに保存するには、[Save As] をクリックします。保存しない場合は、[Close] をクリックします。

RSA Authentication Manager データのバックアップと復元

信頼性の高い完全なバックアップ ファイルを作成するには、このセクションの手順に従ってください。

- ***ACEDATA***
  - ログ データベースと Authentication Manager データベースのバックアップは毎日作成してください (管理者が選択したスケジュールと方法に従って、ログ データベースをアーカイブ ファイルに保存するように、RSA Authentication Manager を設定できます。153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください)。
  - **sdconf.rec** ファイルを変更する場合は、必ずバックアップを作成してください。
  - 製品を初めてインストールした後や、何らかの理由でライセンス レコードをアップグレードした後は、**license.rec** ファイルのバックアップを作成してください。
  - リモート アドミニストレーション、RADIUS リモート アドミニストレーション、および LDAP 同期に使用される SSL ファイルのバックアップを作成してください (**sdti.cer**、**server.cer**、**server.key**、**radius.key**、**radius.cer**、**key3.db**、および **cert7.db**)。
  - カスタム クエリのバックアップを作成してください (**queries¥***)。
- ***ACEPROG***
  - 構成ファイル **hosts.conf** のバックアップを作成してください。

– 構成ファイル **sdcommdConfig.txt** のバックアップを作成してください。

メモ : データベースのバックアップは、RSA Authentication Manager プログラムが**実行されていない**ときに行ってください。プログラムの実行中ににバックアップを**作成する必要がある**場合は、88 ページの「RSA Authentication Manager プログラムが実行されているときのデータのバックアップ」を参照してください。

RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ

複数のレプリカがある場合は、認証サービスを中断せずに、Authentication Manager ですべての RSA Authentication Manager プログラムを停止してデータをバックアップできます。

データベースをバックアップするには

1. Windows Administrator としてログオンします。
2. バックアップを作成する Authentication Manager で RSA Authentication Manager プログラムが実行されていないことを確認します。
3. データベース ブローカが実行されている場合は、[RSA Authentication Manager Control Panel] を使用して停止します。
4. バックアップを作成するデータ ファイルの場所を確認します。

   データベース ファイルは、***ACEDATA*** ディレクトリ (...**¥ace¥data** など) に格納されています。

   ログ データベースのバックアップを作成するには、すべての **sdlog** ファイルをコピーします。

   sdlog.b1
   sdlog.d1
   sdlog.db
   sdlog.lg
   sdlog.st
   sdlog.vrs

   Authentication Manager データベースのバックアップを作成するには、すべての **sdserv** ファイルをコピーします。

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

RSA Authentication Manager プログラムが実行されているときのデータのバックアップ

このセクションで説明するデータベース バックアップ コマンドを使用すると、プライマリとレプリカの両方でデータベースのバックアップを作成できます。できるだけ 86 ページの「RSA Authentication Manager データのバックアップと復元」の最初に示したバックアップ手順に従ってください。

メモ：この方法では、RSA Authentication Manager プログラムの実行中にバックアップを作成することができ、そのためにデータベースの整合性が損なわれることはありません。ただし、不完全なバックアップが作成される可能性があります。これは、レルム内の各レプリカからの**デルタ レコード**（たとえば、直前に行った認証など）がプライマリのデータベースに反映されていない可能性があるためです。バックアップを開始する前に、他の人が同時にデータベースのバックアップ操作を実行していないことを確認してください。同時に複数のバックアップを作成すると、システムのパフォーマンスが大幅に低下します。

構文

sdbkup コマンドの構文は次のとおりです。

```
sdbkup [noprompt|prompt] [online] databasefile backupfile
```

次の表は、**sdbkup** コマンドのオプションを示しています。

オプション	説明
noprompt	指定した場所にある既存のバックアップ ファイルを *backupfile* で上書きします。
prompt	バックアップ ファイルが存在する場合は、メッセージが表示されます。バックアップ ファイルを上書きするかどうかを選択できます。これはデフォルトの動作です。
online	RSA Authentication Manager プログラムの実行中にバックアップを実行することを指定します。
databasefile	バックアップするデータベース ファイルのフルパス名（通常は ***ACEDATA*** ディレクトリのファイル）を指定します。
backupfile	バックアップ ファイルのフルパス名（またはファイル名のみ）を指定します。

たとえば、Authentication Manager データベースのバックアップを **sdserv1** という名前のファイルに作成する場合のコマンドは次のとおりです。

```
sdbkup online ¥ace¥data¥sdserv sdserv1
```

sdserv1 という名前のファイルがすでに存在する場合、次のメッセージが表示されます。

```
*** <backup-file> already exists *** （バックアップ ファイルはすでに存在します）
Press "Enter" to continue; <backup-file> will be overwritten. （続行するには Enter キーを押してください。バックアップ ファイルは上書きされます）
-- または --
Press CTRL_C to abort. （中断するには CTRL + C キーを押してください）
```

```
Press any key to continue . . . (続行するには、いずれかのキーを押してください...)
```

次のコマンドを使用すると、メッセージを表示せずに **sdserv1** ファイルを上書きできます。

```
sdbkup noprompt online ¥ace¥data¥sdserv sdserv1
```

メモ：バックアップ ファイルのターゲット ディレクトリをコマンドに指定しないと、ファイルはコマンドを実行したディレクトリに作成されます。このため、***ACEDATA*** ディレクトリにバックアップ ディレクトリを作成すると便利です (**¥ace¥data¥backups** など)。このディレクトリのパスを **sdbkup** コマンドに指定するか、または、このディレクトリからコマンドを実行してください。

データベース バックアップ コマンドで作成されたデータベースの復元

データベース バックアップ コマンドで作成されたデータベースを復元するには、このセクションで説明する手順を実行します。前のセクション「RSA Authentication Manager プログラムが実行されているときのデータのバックアップ」を参照してください。

メモ：sdrest コマンドは、**sdbackup online** コマンドで作成されたデータベース**だけ**を復元します。

RSA Authentication Manager プログラムが実行されていないときにプライマリのバックアップを作成した場合は、次のセクション「オフライン バックアップまたはサーバからのデータの復元」を参照してください。

sdrest を使用してデータベースを復元するには

1. Windows Administrator としてログオンします。
2. [RSA Authentication Manager Control Panel] ですべてのサービスを停止します。
3. データベースを復元するには、次のコマンドを使用します。

   ```
   sdrest ACEDATA¥filename pathname¥backup_filename
   ```

   たとえば、**ace¥data** ディレクトリ内の **backups** ディレクトリにある **sdserv1** というファイルからサーバ データベースを復元するには、次のコマンドを使用します。

   ```
   sdrest ¥ace¥data¥sdserv ¥ace¥data¥backups¥sdserv1
   ```

   ace¥data ディレクトリ内の **backups** ディレクトリにある **sdlog1** というファイルからログ データベースを復元するには、次のコマンドを使用します。

   ```
   sdrest ¥ace¥data¥sdlog ¥ace¥data¥backups¥sdlog1
   ```

4. すべてのレプリカのレプリカ パッケージを作成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリを再起動したときに、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーし、[RSA Authentication Manager Control Panel] を使用してレプリカ パッケージを適用します。

5. プライマリを再起動します。

オフライン バックアップまたはサーバからのデータの復元

sdbkup コマンド (88 ページの「RSA Authentication Manager プログラムが実行されているときのデータのバックアップ」を参照) を使用してバックアップを作成していないデータを復元する場合は、最新のデータベースが格納されている場所に応じて最適な手順が異なります。

- 87 ページの「RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ」の手順で作成したデータベースが最新である場合は、このセクションの最初の手順に従ってデータを復元します。
- レプリカのいずれかのデータベースが最新である場合は、このセクションの 2 番目の手順に従ってデータを復元します。
- プライマリのデータベースが最新である場合は、このセクションの 3 番目の手順に従ってデータを復元します。

オフライン バックアップからデータを復元するには

1. プライマリに Windows Administrator としてログオンします。
2. [RSA Authentication Manager Control Panel] ですべてのサービスを停止します。
3. オフライン バックアップ ファイルが格納されているディレクトリから、**sdserv** データベースと **sdlog** データベースを ***ACEDATA*** ディレクトリにコピーします。

   コピーする **sdserv** ファイルは、**sdserv.d1**、**sdserv.b1**、**sdserv.db**、**sdserv.lg**、**sdserv.st**、および **sdserv.vrs** です。コピーする **sdlog** ファイルは、**sdlog.d1**、**sdlog.b1**、**sdlog.db**、**sdlog.lg**、**sdlog.st**、および **sdlog.vrs** です。
4. すべてのレプリカのレプリカ パッケージを作成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーし、[RSA Authentication Manager Control Panel] を使用してレプリカ パッケージを適用します。
5. プライマリで RSA Authentication Manager 認証サービスを起動します。

レプリカのデータをプライマリで復元するには

1. プライマリに Windows Administrator としてログオンします。
2. [RSA Authentication Manager Control Panel] ですべてのサービスを停止します。
3. レプリカでステップ 1 とステップ 2 を繰り返します。
4. レプリカの **sdserv** データベースをプライマリにコピーします。

   レプリカからプライマリにコピーするファイルは、**sdserv.db**、**sdserv.lg**、**sdserv.lic**、および **sdserv.vrs** です。
5. すべてのレプリカのレプリカ パッケージを作成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーし、[RSA Authentication Manager Control Panel] を使用してレプリカ パッケージを適用します。

6. プライマリで RSA Authentication Manager 認証サービスを起動します。
7. レプリカで RSA Authentication Manager 認証サービスを起動します。

プライマリのデータをレプリカで復元するには

1. レプリカに Windows Administrator としてログオンします。
2. レプリカの [RSA Authentication Manager Control Panel] ですべてのサービスを停止します。
3. プライマリでステップ 1 とステップ 2 を繰り返します。
4. すべてのレプリカのレプリカ パッケージを作成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーし、[RSA Authentication Manager Control Panel] を使用してレプリカ パッケージを適用します。
5. プライマリで RSA Authentication Manager 認証サービスを起動します。
6. レプリカで RSA Authentication Manager 認証サービスを起動します。

データベース レコードのインポートとエクスポート

一部の RSA Authentication Manager データは、エクスポートして ASCII テキスト ファイル形式で保存できます。これらのファイルはバックアップ用ではなく、オフラインで表示または処理するためのものです。データベースに復元して、Authentication Manager で使用することはできません。

RSA Authentication Manager Host Mode を使用して、次のデータが格納されたテキスト ファイルを作成できます。

- ユーザ名やログインなどの特定のユーザ データ。

  詳細については、[User] > [List Users] > [Help] の順にクリックして、表示される情報を参照してください。
- RSA Authentication Manager レポート形式のログ レコード。

  詳細については、162 ページの「ファイルへのレポートの出力」を参照してください。
- Microsoft Excel などのサード パーティ ソフトウェアで使用できるカンマ区切り (CSV) 形式のログ レコード。

  詳細については、153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください。

これらのファイルは安全な場所に保管してください。ファイルに格納されているデータが不正なユーザのアクセスを受けると、システム セキュリティが重大な危険にさらされる可能性があります。

データベース ダンプ ユーティリティとロード ユーティリティの使用

ダンプ ユーティリティとロード ユーティリティを使用すると、テキスト ファイルとは異なり、データベースに**インポートできる**形式でデータベース レコードをエクスポートできます。詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』を参照してください。

復元手順

Authentication Manager でハードウェア障害が発生したり、データベースで問題が発生した場合は、次の手順に従って問題のハードウェアやデータベースを復元または交換できます。

この手順の一部は、システムで Push DB Assisted Recovery 機能を使用するかどうかに応じて異なります。この機能は有効にしておくことをお勧めします。詳細については、22 ページの「データベース プッシュ (Push DB Assisted Recovery) 機能」を参照してください。

システムで Push DB Assisted Recovery 機能を使用するには、RSA Authentication Manager Host Mode を起動し、[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。次に、[Allow Push DB Assisted Recovery] チェックボックスをオンにします。

最新のデータベースの特定

RSA Authentication Manager アドバンスド ライセンスを保有し、複数のレプリカを使用している場合、最新のデータベースを使用するには、使用するデータベースを次の手順で決定します。プライマリのハードウェアが機能している場合は、プライマリのイベント ログを確認します。プライマリのハードウェアが機能していない場合は、各レプリカのイベント ログを確認します。

最新のデータベースを特定するには

1. [スタート] > [プログラム] > [管理ツール] > [イベント ビューア] の順にクリックします。
2. [ログ] > [アプリケーション ログ] の順にクリックします。
3. プライマリで次のメッセージを検索します。

   ```
   Primary Successfully Received Replica Records
   ```

   このメッセージには、日付、時刻、およびレプリカの IP アドレスが含まれます。最新のデータベースは、最新のメッセージに IP アドレスで示されているレプリカにあります。

   レプリカで次のメッセージを検索します。

   ```
   Replica Successfully Reconciled Databases
   ```

   このメッセージには、日付、時刻、およびプライマリの IP アドレスが含まれます。各レプリカのイベント ログを確認します。最新のデータベースは、最新のメッセージが保存されたレプリカにあります。

レプリカのデータベースの交換

レプリカのデータベースを交換する必要がある場合は、プライマリに新しいレプリカ パッケージを作成し、レプリカで新しいデータベースが必要であることを指定しなければなりません。

レプリカのデータベースを交換するには

1. プライマリに Windows Administrator としてログオンします。
2. レプリカの [RSA Authentication Manager Control Panel] で RSA Authentication Manager のみを停止します。

   すべての管理セッションが切断されます。
3. データベースを交換するレプリカでステップ 1 とステップ 2 を繰り返し、プライマリにもう一度ログオンします。
4. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックします。

   メモ：アクティブなコマンド ボタンが [Details] だけの場合は、レプリカで操作しているか、またはデータベース ブローカがシャットダウンされていません。
5. [Servers in This Realm] リストからレプリカを選択します。
6. [Generate Replica Package] をクリックします。

   選択したレプリカをデータベース プッシュの対象としてマークするかどうか質問されます。
7. 選択したレプリカのレプリカ　パッケージを作成するという旨のメッセージが表示されたら、[OK] をクリックします。
8. レプリカがデータベース プッシュの対象としてマークされたら、[OK] をクリックします。

   各レプリカについて、マークを確認するメッセージが表示されます。レプリカをプッシュの対象としてマークするかどうかの確認が求められるたびに、[OK] をクリックします。
9. 正常終了を示すメッセージが表示されたら、[OK] をクリックします。

   レプリカ パッケージは、***ACEDATA*** ディレクトリ内の **replica_package** ディレクトリに作成されます。
10. プライマリの ***ACEDATA*¥replica_package¥database** ディレクトリと ***ACEDATA*¥replica_package¥license** ディレクトリのファイルをレプリカの ***ACEDATA*** 以外のディレクトリにコピーします。
11. レプリカで [RSA Authentication Manager Control Panel] を使用してレプリカ パッケージを適用します。

レプリカのハードウェアの交換

レプリカにハードウェア障害が発生して機能しなくなった場合は、レプリカ管理ユーティリティの [Replace] ボタンを使用して交換することをお勧めします。まず、新しいレプリカとして使用するネットワーク マシンを選択する必要があります。

レプリカのハードウェアを交換するには

1. [Servers in This Realm] リストからレプリカを選択し、[Replace] をクリックします。
2. 新しいレプリカの名前を [Name] ボックスに入力します。
3. カーソルを [IP Address] ボックスに置きます。
4. 新しいレプリカの IP アドレスが [IP Address] ボックスに表示されます。
5. [OK] をクリックします。
6. 表示されるメッセージに対して、[OK] をクリックします。
7. レプリカ パッケージを作成し、レプリカ パッケージを使用して新しいレプリカをインストールします。
8. レプリカのインストールの詳細については、各プラットフォームの『インストール ガイド』を参照してください。
9. レプリカを交換した後、必要に応じて次の操作を実行します。
   - 古いレプリカがレルム間認証のローカル レルム Authentication Manager またはリモート レルム Authentication Manager として指定されている場合は、ローカル レルムおよびリモート レルムのデータベースのレルム レコードを編集して、新しいレプリカの名前と IP アドレスを反映します。詳細については、ヘルプの「Edit Realm」を参照してください。
   - レプリカが RADIUS サーバとして指定されている場合は、RADIUS サーバをインストールし、新しいレプリカを使用するようにすべての RADIUS クライアントを構成します。

     RADIUS サーバのインストールの詳細については、『RSA RADIUS Server 6.1 Administrator's Guide』を参照してください。
   - レプリカを旧バージョンのエージェント ホストのアクティング Authentication Manager として定義する場合は、この Authentication Manager をアクティング マスタまたはアクティング スレーブとして使用する旧バージョンのすべてのエージェント ホストに対して、新しい **sdconf.rec** ファイルを作成し、その **sdconf.rec** ファイルをエージェント ホストに配布します。詳細については、ヘルプの「Assign Acting Servers」を参照してください。
   - レプリカが v5.0 以降のエージェント ホストの **sdopts.rec** ファイルで指定されている場合は、エージェント ホストの **sdopts.rec** ファイルを編集して新しいレプリカの名前と IP アドレスを反映します。

プライマリのデータベースの交換

プライマリのデータベースが壊れた場合は、レプリカの最新のデータベースのコピーと交換し、新しくレプリカ パッケージを作成して他のすべてのレプリカに配布する必要があります。

プライマリのデータベースを交換するには

1. [RSA Authentication Manager Control Panel] で RSA Authentication Manager のみを停止します。

   すべての管理セッションが切断されます。
2. レプリカからデータベースのダンプを取得します。レプリカで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Database Tools] > [Dump] の順にクリックします。

3. [Database Dump] ダイアログ ボックスで、[Dump Server Database] チェックボックスだけをオンにして、[OK] をクリックします。

   ダンプ ユーティリティは ***ACEDATA*** ディレクトリに **sdserv.dmp** ファイルを作成します。既存のダンプ ファイルは上書きされます。ダンプの取得が完了したら、[Done] と表示されるので、[Close] をクリックします。

4. **sdserv.dmp** ファイルをプライマリにコピーします。

5. プライマリの [RSA Authentication Manager Control Panel] ですべてのサービスを停止します。

6. プライマリに新しい空のデータベースを作成します。***ACEPROG*** ディレクトリの **sdnewdb.exe** をダブルクリックします。

7. 新しいデータベースにダンプ ファイルをロードします。[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Database Tools] > [Load] の順にクリックします。

8. [Server Database] を選択します。

9. **sdserv.dmp** ファイルのパス名を [Server dump filename] ボックスに入力するか、または [Browse] ボタンをクリックして該当するディレクトリに移動し、ファイルを選択します。次に、[OK] をクリックします。

10. データベースのロードが完了したら、[Close] をクリックします。

11. プライマリでレプリカ パッケージを作成します。[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックします。

    メモ：アクティブなコマンド ボタンが [Details] だけの場合は、レプリカで操作しているか、またはデータベース ブローカがシャットダウンされていません。

12. [Servers in This Realm] リストからすべてのレプリカを選択します。

13. [Generate Replica Package] をクリックします。

    選択したレプリカをデータベース プッシュの対象としてマークするかどうか質問されます。

14. 選択したレプリカのレプリカ　パッケージを作成するというメッセージが表示されたら、[OK] をクリックします。

15. レプリカがデータベース プッシュの対象としてマークされたら、[OK] をクリックします。

    各レプリカについて、マークを確認するメッセージが表示されます。レプリカをプッシュの対象としてマークするかどうかの確認が求められるたびに、[OK] をクリックします。

16. 正常終了を示すメッセージが表示されたら、[OK] をクリックします。

    レプリカ パッケージは、***ACEDATA*** ディレクトリ内の **replica_package** ディレクトリに作成されます。

    RSA Authentication Manager のシステム パラメータが Push DB Assisted Recovery 機能を有効にするように設定されている場合は、プライマリとレプリカを再起動したときに、プライマリによってデータベース ファイルがレプリカにプッシュされ、処理が完了します。

システム パラメータが Push DB Assisted Recovery 機能を有効にするように**設定されていない**場合は、ステップ 17 に進みます。

17. プライマリの ***ACEDATA*¥replica_package¥database** ディレクトリのファイルをレプリカの ***ACEDATA*** 以外のディレクトリにコピーします。

18. レプリカで [RSA Authentication Manager Control Panel] を使用してレプリカ パッケージを適用します。

レプリカの指名によるプライマリのハードウェアの交換

プライマリでハードウェア障害が発生した場合は、既存のレプリカをプライマリとして指名できます。まず、指名するレプリカを選択します。選択したレプリカで、レプリカ管理ユーティリティの [Nominate] ボタンをクリックすると、レプリカがプライマリに自動的に変換されます。更新されたレプリカ パッケージが新しいプライマリの ***ACEDATA*¥replica_package** ディレクトリに作成されます。

メモ：機能しているプライマリのハードウェアをより新しいハードウェアに交換する場合は、新しいハードウェアをレプリカとして追加してから、プライマリとして指名することもできます。その後、古いプライマリをオフラインにします。ただし、この場合は一定の手順に従って操作する必要があります。まず、プライマリを停止し、新しいマシンをレプリカとして追加して、新しいマシンのレプリカ パッケージを作成します。現在のプライマリのバックアップを再起動し、レプリカを調整します。次に、以下に示すように、新しいレプリカを指名する手順を実行します。

レプリカ指名の準備

レプリカを指名する前に、障害が発生したプライマリのハードウェアの状態を確認する必要があります。障害が発生したプライマリが長期にわたって使用できない場合は、レプリカを指名する必要があります。必要な修復が短期間で終了する場合は、レプリカを**指名せず**、元のプライマリを修復して使用することもできます。いずれの場合も、プライマリが動作していない間は各レプリカが認証要求の処理を続行します。元のプライマリを修復する場合、すべての Quick Admin 管理者およびリモート管理者に状況を通知し、プライマリが復元されるまで、レルム内のマシンの Quick Admin または Remote Administration を実行できないことを説明してください。

レプリカを指名するには

1. 障害が発生したプライマリの代わりに使用するレプリカを選択します。

   メモ：最新のデータベースが格納されているレプリカを選択することをお勧めします。詳細については、92 ページの「最新のデータベースの特定」を参照してください。

2. レプリカの [RSA Authentication Manager Control Panel] で RSA Authentication Manager のみを停止します。

   すべての管理セッションが切断されます。

3. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックします。

4. [Nominate] をクリックします。

5. [OK] をクリックしてこのレプリカを指名します。

6. 新しいプライマリで、RSA Authentication Manager サービスとデータベース ブローカを起動します。

   RSA Authentication Manager のシステム パラメータが Push DB Assisted Recovery 機能を有効にするように設定されている場合は、レプリカ パッケージが各レプリカに自動的に配布され、反映されます。

   システム パラメータが Push DB Assisted Recovery 機能を有効にするように**設定されていない**場合は、各レプリカでステップ 7 ～ 13 を繰り返します。

7. レプリカのすべてのサービスを停止します。

8. 新しいプライマリの ***ACEDATA*¥replica_package¥database** ディレクトリと ***ACEDATA*¥replica_package¥license** ディレクトリのファイルをレプリカの ***ACEDATA*** 以外のディレクトリにコピーします。

9. レプリカで [RSA Authentication Manager Contol Panel] を使用してレプリカ パッケージを適用します。

メモ：古いプライマリを修復してネットワークに再接続すると、自動的にレプリカとして追加されます。プライマリとして復元するには、指名する必要があります。

レプリカを指名するか、新しいマシンにプライマリをインストールすることによって、障害が発生したプライマリのハードウェアを交換する場合、Quick Admin、RADIUS サーバ、エージェント ホスト、LDAP 同期、および Remote Administration も影響を受けることに注意してください。これらが新しいプライマリで正しく機能するように、対応する指示を参照して、次の操作を重要なものから実行してください。

1. Quick Admin がインストールされている場合は、新しいプライマリの名前と IP アドレスで Quick Admin の設定を再構成する必要があります。操作手順については、49 ページの「Quick Admin の再構成」を参照してください。

2. Authentication Manager がレルム間認証のローカル レルム Authentication Manager またはリモート レルム Authentication Manager として指定されている場合は、ローカル レルムおよびリモート レルムのデータベースのレルム レコードを編集して新しい名前または IP アドレスを反映します。詳細については、ヘルプの「Edit Realm」を参照してください。

3. 障害が発生したプライマリが RADIUS サーバに指定されていた場合は、RADIUS サーバを新しいプライマリ、他のレプリカ、別のホスト マシンのいずれかにインストールできます。新しいプライマリの管理機能に悪影響を与えないように、他のレプリカ上で RADIUS を有効にすることをお勧めします。必ず次の操作を実行してください。
   - RADIUS サーバとして使用する Authentication Manager をデータベースにエージェント ホストとして追加します。詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』の「サーバをエージェント ホストとしてプライマリ データベースへ追加」を参照してください。
   - 新しいプライマリを RADIUS サーバとして使用する場合は、RADIUS サーバの構成設定を更新して古いプライマリの構成設定と同じにします。
   - 指定された RSA RADIUS サーバの正しい名前と IP アドレスを使用するようにすべての RADIUS クライアントを構成します。デバイス固有の構成手順については、NAS デバイスのマニュアルを参照してください。

4. Authentication Manager を旧バージョンのエージェント ホストのアクティング Authentication Manager として定義する場合は、この Authentication Manager をアクティング マスタまたはアクティング スレーブとして使用する旧バージョンのすべてのエージェント ホストに対して、新しい **sdconf.rec** ファイルを作成し、その **sdconf.rec** ファイルをエージェント ホストに配布します。詳細については、ヘルプの「Assign Acting Servers」を参照してください。

5. Authentication Manager が v5 のエージェント ホストの **sdopts.rec** ファイルで指定されている場合は、エージェント ホストの **sdopts.rec** ファイルを編集して Authentication Manager の新しい名前または IP アドレスを反映します。

6. SSL を使用して LDAP サーバに接続する LDAP 同期ジョブが設定されていた Authentication Manager の場合、新しいプライマリで ***ACEDATA*/ldapjobs/sslcerts** ディレクトリに必要な **cert7.db** ファイルがあることを確認する必要があります。このファイルがない場合、LDAP 同期が実行されると次のエラー メッセージが表示されます。

   ```
   LDAP connection error - Failed to initialize LDAP session (LDAP 接続エラー - LDAP セッションを初期化できません)
   ```

   cert7.db ファイルの設定については、111 ページの「SSL の使用」を参照してください。

7. すべてのリモート アドミニストレーション マシンに対して、プライマリの ***ACEDATA*** ディレクトリから **sdconf.rec** ファイルと **server.cer** ファイルをコピーし、リモート アドミニストレーション マシンからプライマリを削除します。次に、新しい **sdconf.rec** ファイルを使用してプライマリを追加します。詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』を参照してください。

カスタム定義データ (拡張レコード) のメンテナンス

RSA Authentication Manager 拡張レコードを使用すると、RSA Authentication Manager プログラムの実行に必要な情報の他に、組織で必要とされるデータベース情報などを定義して管理できます。このカスタム定義情報を**拡張データ**と呼びます。

RSA Authentication Manager Host Mode では、拡張レコードにアクセスし、処理するためのメニュー オプションが提供されています。次の表は、処理対象の拡張データの種類、データが格納されているデータベース テーブル、データを処理するために使用するメニュー、および詳細情報が示されている場所を示しています。

拡張データ	データベース テーブル	メニュー	参照ページ
RSA Authentication Manager システム関連	CustSystemExtension	[System]	209
エージェント ホスト関連	CustClientExtension	[Agent Host]	55
グループ関連	CustGroupExtension	[Group]	118
ログ エントリ関連	CustLogExtension	[Log]	99
サイト関連	CustSiteExtension	[Site]	131
トークン関連	CustTokenExtension	[Token]	117

拡張データ	データベース テーブル	メニュー	参照ページ
ユーザ関連	CustUserExtension	[User]	ヘルプを参照

カスタム定義データにもとづくレポートを作成するには、[Report] メニューの [Extension Data] をクリックします。

メモ：拡張フィールドとカスタム アドミニストレーション プログラムの作成の詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

ログ拡張データの管理

このセクションでは、ログ関連の拡張データを作成、編集、および削除する方法について説明します。その他の種類の拡張データの管理方法については、前のセクション「カスタム定義データ (拡張レコード) のメンテナンス」の表を参照してください。

ログ エントリ拡張フィールドを使用すると、既存のログ エントリに情報を追加できます。この情報を使用して、後でレポートで使用するログ エントリを選択できます。

ログ拡張データを編集するには

1. [Log] > [Edit Log Extension Data] の順にクリックします。
2. 拡張データが関連付けられているログ メッセージの種類を選択します。[Activity]、[Exception]、[Incident] のいずれかを選択してください。

   [Log Entry Selection Criteria] ダイアログ ボックスが表示されます。
3. [Log Entry Selection Criteria] ダイアログ ボックスの 1 つまたは複数のフィールドに選択条件を入力します。フィールドの説明については、159 ページの「レポートの内容の選択条件」を参照してください。

   すべての選択条件をデフォルト値にリセットするには、[Clear] をクリックします。
4. 選択条件を指定したら、[OK] をクリックします。

   [Select Log Entry] ダイアログ ボックスが表示され、入力したすべての条件を満たすログ レコードだけが表示されます。

   ダイアログ ボックスでは、エントリごとに時刻 (世界協定時とローカル時刻)、動作が記録されたユーザ、およびログ メッセージが表示されます。管理者が選択値を変更するか、または現在のアドミニストレーション セッションを終了するまで、選択されている値は有効です。
5. 拡張データが関連付けられているログ エントリを選択し、[Edit Log Extension Data] をクリックします。

   [Edit Log Extension Data] ダイアログ ボックスに、ログ エントリと、このエントリに対して定義されているレコードが表示されます。各レコードはセカンダリ キー (48 文字以内) とデータ (80 文字以内) で構成されます。
6. これらのレコードは追加、変更、削除できます。同じキーを使用して複数のレコードを作成できますが、1 つの拡張データベース テーブルに重複するレコード (キーとデータ値の**両方**が同一のレコード) を作成することはできません。
   - 既存のレコードを変更するには、レコードを選択し、[Key] フィールドまたは [Data] フィールドに表示された情報を変更し、[Save] をクリックします (これらのフィールドのいずれかに入力するまで、[Save] ボタンは使用できません)。

レコードを変更せずにフィールドをクリアするには、[Clear] をクリックします。

- 新規レコードを作成するには、必要に応じて [Clear] をクリックして、[Key] フィールドと [Data] フィールドをクリアします。新規レコードの情報を入力し、[Save] をクリックします。
- レコードを削除するには、レコードを選択し、[Delete] をクリックします。確認のために [OK] をクリックします。

7. [Exit] をクリックして、[Edit Log Extension Data] ダイアログ ボックスを閉じます。

外部 4GL プロシージャの実行

4GL によるプログラミングに習熟している場合は、RSA Authentication Manager Host Mode から独自の 4GL プロシージャを直接実行して、RSA Authentication Manager データを処理できます。RSA Authentication Manager データを更新するプロシージャを実行できるのは、レルム管理者か、または **Run Custom 4GL** タスクが割り当てられているユーザだけです。

注意 : 4GL プロシージャを実行すると、ログ レコードや拡張データなどの有効なデータが上書きまたは削除されたり、データベースが壊れる可能性もあります。Administration Toolkit を使用して、RSA Authentication Manager データベースに対して使用するカスタム アプリケーションを作成することを**強くお勧めします**。詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

フィールドの中には、カスタム アドミニストレーション プログラムで変更できないものが数多くあります。これらのフィールドとカスタム アドミニストレーション プログラムの作成の詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

RSA Authentication Manager Host Mode から 4GL プロシージャを実行するには

1. [RSA Authentication Manager Host Mode] > [File] > [Run Custom 4GL] の順にクリックします。

   [Run External Procedure] ダイアログ ボックスが表示されます。

2. 実行するプロシージャのファイル名を [Procedure Name] フィールドに入力するか、または [Browse] をクリックし、リストからファイル名を選択します。

3. [Automatically Connect to RSA Database] チェックボックスを使用して、RSA Authentication Manager データベースに対して選択したプロシージャを実行するかどうかを指定します。

   このチェックボックスは便宜上提供されています。このチェックボックスをオンにしておくと、管理者権限を示すコード行や、対象となる RSA Authentication Manager データベースを指定するコード行を 4GL プロシージャに指定する必要がありません。これらの指定は RSA Authentication Manager Host Mode が行います。

   RSA Authentication Manager データベース以外のデータベースにアクセスするプロシージャを実行している場合は、このチェックボックスをオンにしないでください。その場合は、対象のデータベースに接続するためのコードを 4GL プロシージャに指定します。

4. 基本的にはすべてのデータベース　レコードに対してプロシージャを実行できますが、『Administration Toolkit Reference Guide』のデータベースに関する説明で、アスタリスクがついているデータベース レコードに対してはプロシージャを実行できません。また、[Object Type] フィールドを使用して、プロシージャの実行対象を特定の種類のレコード (ユーザ レコードやトークン レコードなど) に制限することもできます。

   すべての種類のレコードに対してプロシージャを実行するには、デフォルト オブジェクト タイプ ([None]) を使用します。特定の種類のレコードに対してプロシージャを実行するには、[Object Type] の下のデータの種類 ([User]、[Token]、[Group]、[Agent Host]、[Site]、[Realm] のいずれか) を選択します。その後表示される [Select] ダイアログボックスから特定のレコードを選択し、[OK] をクリックします。

   選択したレコードのフィールドが [Argument List] に表示されます。プロシージャは、これらのフィールドの値を使用します。RSA Authentication Manager Host Mode は、各フィールドの値を抽出し、一続きのデータとして表示順に連結します。それぞれの値は、シャープ記号 (#) で区切られます。一続きのデータを解析し、フィールドの値ごとにレコードを処理するようにアプリケーションを作成できます。

   次の表は、[Object Type] フィールドで各オブジェクト タイプを選択したときに、RSA Authentication Manager Host Mode が抽出し、連結するレコードのフィールドを示しています。

オブジェクト タイプ	[Argument List] の内容
[User]	First name (ファースト ネーム)、Last name (ラスト ネーム)、Default login (デフォルト ログイン)、Default shell (デフォルト シェル)
[Token]	Token serial number (トークンのシリアル番号)、Last login date (最終ログイン日)、Last login time (最終ログイン時刻)
[Group]	Site name (サイト名)、Group name (グループ名)
[Agent Host]	Agent Host name (エージェント ホスト名)、Network address (ネットワーク アドレス)、Protocol (プロトコル)
[Site]	Site name (サイト名)
[Realm]	Primary name (プライマリ名)、Primary address (プライマリ アドレス)、Replica name (レプリカ名)、Replica address (レプリカ アドレス)

5. [OK] をクリックします。

6 認証のためのユーザの登録

この章では、ユーザに関連する管理タスクについて説明します。この章のセクションは、操作の実行順に構成されています。すべての操作を完了すると、RSA Authentication Manager システムはユーザを認証するように設定され、ユーザは割り当てられた RSA SecurID トークンを使用してログオンできるようになります。

RSA Authentication Manager 管理者は、次の操作を行う責任があります。

- ユーザ情報を更新する。
- ユーザからトークンの盗難または紛失の報告があった場合に、ただちにトークンを無効にする。
- ユーザから PIN を他人に知られたという報告があった場合に、ただちにそのトークンを New PIN モードにする。
- Authentication Manager データベースのバックアップを定期的に行う。
- トークンの有効期限が切れたか、またはトークンが破損した場合に、交換用トークンを入手し、インストールする。

PIN に関するオプション

トークンの割り当てや配布を行う前に、次に示すユーザの PIN の属性を定義します。

- 英数字なのか、数字のみか
- 固定長であるのか、可変長であるのか
- ユーザが作成するのか、システムで生成するのか

システムにとって最適な PIN オプションを判断した後、[System Parameters] ダイアログ ボックスでこれらのオプションを設定します。

操作手順：[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

英数字 PIN または数字 PIN の選択

RSA SecurID スタンダード カードとキーホルダでは、なるべく英数字 PIN を使用してください。PIN に数字と英字の両方が含まれていれば、PIN を推測するのがより困難になるため、セキュリティを向上できます。

一方、英数字 PIN の欠点として、通常、システム生成の長い英数字 PIN は覚えにくいということがあげられます。たとえば、**kh8n4wo** のような PIN がユーザに割り当てられた場合、ユーザはなかなか覚えられないので、それをメモに書き留める可能性があり、セキュリティの弱点になります。

メモ：PIN を割り当てるか、または作成した後に、システム パラメータを英数字から数字に変更した場合、以前の PIN に英字が含まれていたトークンはそれぞれ New PIN モードに設定されます。このため、そのトークンのユーザは、次回の認証試行時に新しい PIN を入力する必要があります。

RSA SecurID PINPAD、およびソフトウェア トークンの PIN は数字でなければなりません。PINPAD カードの保有者は PASSCODE を生成するために、自分の PIN をカードに入力する必要があります。しかし、PINPAD には英字キーがないため、New PIN 操作でこれらのユーザが英数字 PIN を作成したり、受け取ることはできません。

固定長 PIN または可変長 PIN の選択

RSA Authentication Manager システムでは、PIN の長さをすべて同じにするか、または 4 ～ 8 文字の範囲で可変長にするかを設定できます。

システム管理者の中には、既存のシステムとの互換性の維持や、管理の単純化のために、固定長 PIN を選択する人がいます。ユーザが自分で PIN を作成する場合は、可変長 PIN の方が柔軟性が高くなります。これは、システム管理者が指定した最小長と最大長の範囲から適切な PIN を選択できるからです。

最適な PIN の長さ

RSA Authentication Manager PIN の長さは、4 ～ 8 文字でなければなりません。できるだけ、6 文字以上の PIN を使用してください。PIN の長さが長くなるほど、セキュリティは向上しますが、ユーザにとっては短い PIN の方が便利です。6 文字という長さは、ユーザが記憶しやすく、またセキュリティも保てる長さです。

RSA Authentication Manager の制限内で、可能な長さの範囲を指定します (要求する PIN の長さを統一するには、最小長と最大長に同じ値を設定します)。New PIN 操作で、設定した範囲外の PIN を作成したり、受け付けることはできません。

ユーザ作成 PIN またはシステム生成 PIN の選択

PIN の割り当てには次の 3 種類のモードがあり、そのうちのいずれかを指定しなければなりません。

- すべてのユーザがシステムで生成された PIN を使用するモード
- すべてのユーザが自分で PIN を作成しなければならないモード
- ユーザが自分で PIN を作成でき、システムで生成された PIN を使用することも可能なモード

RSA Authentication Manager システムでは、ユーザ作成 PIN とシステム生成 PIN の両方を使用できるように設定されています([Edit System Parameters]ダイアログ ボックスで、[User-created PINs allowed] チェックボックスがオンに設定され、[User-created PINs required] チェックボックスがオフに設定されています)。この設定では、ユーザは PIN を作成できますが、必ずしも自分で作成しなければならないというわけではありません。ユーザをデータベースに追加するときに、ユーザごとに、ユーザが自分で PIN を作成できるのか、システム生成 PIN を使用しなければならないのかを指定します。

システム生成 PIN を使用するように設定すると、ユーザがたとえば **1234** のような簡単な数字の組み合わせ、自分の内線番号など、簡単に推測できる PIN を選択するのを防止することができます。また、PIN をシステムで生成するようにしておけば、他人に PIN を知られてしまったために、New PIN モードに設定されたトークンを保有しているユーザが、他人に知られてしまった PIN と同じ PIN を選択するのも防止できます。

システム生成 PIN を使用する方が安全ですが、ユーザが自分で PIN を作成する方法にも利点はあります。複数のトークンを保有しているユーザは、両方で同じ PIN を使用してもかまいません。システム生成 PIN を使用すると、このような重複を防止できますが、ユーザに自分の PIN の作成を許可する方が安全な場合もあります。ユーザが複数の PIN を記憶することは困難であり、PIN を覚えられずにメモに書き留める可能性があるからです。

また、すべてのユーザが自分で PIN を作成しなければならないように、RSA Authentication Manager システムを設定することもできます。その場合、New PIN プロンプトで、システムが PIN を生成するオプションは選択できません。

PIN を必要としないトークン

RSA Authentication Manager では、PIN を必要としないトークンによる認証がサポートされています。ユーザは認証を受けるときに、PIN の後にトークンコードを入力するのではなく、トークンに現在表示されているトークンコードのみを入力します。

トークンコードのみによる認証は、ユーザが PIN でロックを解除する必要があるスマート カード上のトークンや、ユーザがパスワードでロックを解除する必要があるデスクトップ上のトークンなどの場合に適しています。このような場合、ユーザが 2 つの異なる PIN を入力しなくても、リソースは二要素認証によって保護されます。

従来型トークンとソフトウェア トークンのどちらも、PIN を必要としないように設定できます。

操作手順：[Token] > [Change Tokens to Authenticate With] の順にクリックします。操作手順については、ヘルプを参照してください。PIN を必要としないようにソフトウェア トークンを設定する方法については、115 ページの「ソフトウェア トークンの発行 (Issue Software Token)」を参照してください。

ユーザ レコードの作成と変更

各 RSA SecurID トークン保有者は、ユーザ レコードを RSA Authentication Manager データベースに登録しておかなければなりません。ユーザ レコードを作成する方法は 4 つあります。

- [Add User] ダイアログ ボックスで個々のユーザのデータを追加する方法。

  [User] > [Add User] の順にクリックして [Add User] ダイアログ ボックスを表示します。詳細については、[Help] をクリックして表示される情報を参照してください。

- 既存のユーザ レコードをコピーし、編集して、グループ メンバーシップとエージェント ホストのアクティブ化リストを含むテンプレートを作成し、そのテンプレートを使用して多くの新規ユーザを作成する方法。

  [User] > [Copy User] の順にクリックして、モデルとなるユーザ レコードを選択し、[Add User] ダイアログ ボックスを表示します。詳細については、[Help] をクリックして表示される情報を参照してください。

- SAM データベースからユーザ データをインポートする方法。

  詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』(英語版は ***ACEDOC*** ディレクトリの **authmgr_install_windows.pdf**) の「SAM データベースからのユーザ レコードの作成」を参照してください。

- LDAP ディレクトリからユーザ データをインポートする方法。

  既存の LDAP ディレクトリにあるデータから RSA Authentication Manager データベースにユーザ レコードを作成できます。LDAP 比較ユーティリティ (***ACEUTILS*** ディレクトリの **sdaceldap**) を実行して、LDAP ユーザのリストを含むカンマ区切り (.csv) ファイルを作成し、[User] メニューから [LDAP Users] を選択し、[Manage LDAP Users] オプションを使用して、このファイルをデータベースにインポートします。詳細については、次のセクション「コマンド ラインからの LDAP ユーザ データのインポート」を参照してください。

ユーザ レコードのデータは、レコードに入力したか、テンプレートから継承したか、またはファイルにインポートしたかに関係なく、[Edit User] オプションで変更できます。

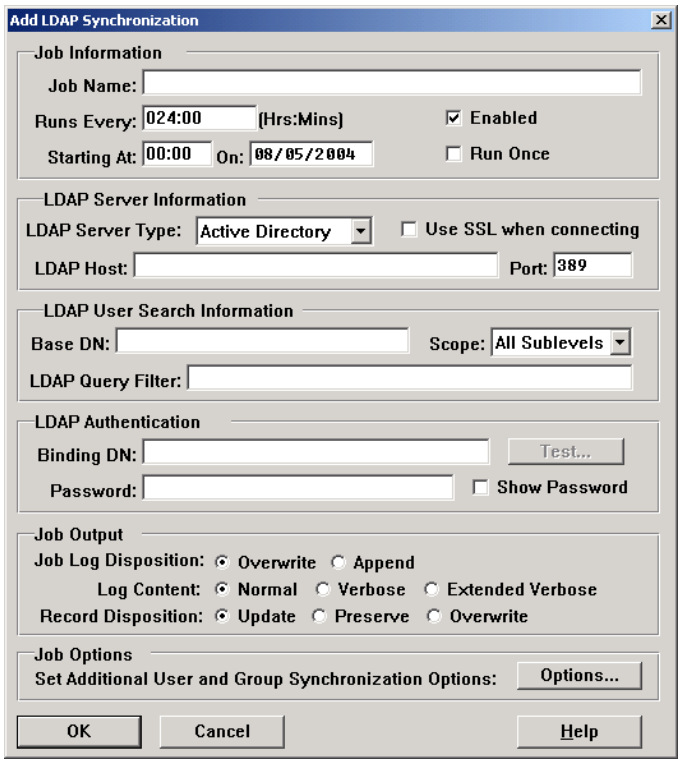
LDAP ユーザ レコードの同期化

RSA Authentication Manager Host Mode が提供する LDAP 同期ツールを使用すると、Authentication Manager ユーザ データベースを設定し、LDAP ディレクトリ サーバと同期をとることができます。

RSA Authentication Manager でサポートされる LDAP ディレクトリ サーバは、Microsoft Active Directory、Sun ONE Directory Server と Novell NDS eDirectory です。

RSA Authentication Manager Host Mode を使用すると、同期ジョブを追加、編集、コピー、リスト、削除、および実行して、RSA Authentication Manager データベース内の LDAP ユーザ レコードのメンテナンスを自動的に行うことができます。

操作手順：プライマリ Authentication Manager で、[User] > [LDAP Users] の順にクリックし、[Add Synchronization] を選択します。詳細については、[Help] をクリックして表示される情報を参照してください。



同期ジョブは必要に応じて実行するか、または特定の時間に実行されるようにスケジュールすることができます。同期ジョブの実行時に、RSA Authentication Manager は、指定された LDAP ディレクトリとの接続を確立し、ディレクトリ内のユーザ データを確認します。同期ジョブは次の操作を実行できます。

- LDAP に存在しなくなったユーザを削除する。
- Authentication Manager 内で、LDAP で有効になったユーザを有効にし、無効になったユーザを無効にする。
- LDAP ユーザを既存の Authentication Manager グループに割り当てる。

また、Authentication Manager データベースに新規 LDAP ユーザのグループおよびサイトが作成されるように、同期ジョブを設定できます。同期ジョブが Authentication Manager データベースに作成するグループには、新規ユーザが登録されている LDAP グループの名前が使用されます。新規ユーザが LDAP のグループに属していない場合、同期ジョブは Authentication Manager データベースにグループを作成しません。また、新規グループのサイトも作成できます。同期ジョブによって作成されたサイトには、LDAP 内の対応する OU レベルと同じ名前が使用されます。

メモ：同期ジョブは、プライマリで**のみ**、ローカルまたはリモートで設定できます。

同期ジョブを追加すると、そのジョブの名前の付いたサブディレクトリが ***ACEDATA*** の **/ldapjobs** ディレクトリに作成されます。ジョブが完了すると、出力ファイル (**ldapsync.log**) が生成され、**/ldapjobs** ディレクトリに保存されます。このファイルには、Authentication Manager データベースで行われた LDAP ユーザに関係する変更の要約が記録されています。

メモ：sdaceldap import を使用して**以前にデータベースに追加された LDAP ユーザを管理する場合**、まず、**sdaceldap compare** を実行して、LDAP に存在しなくなったユーザを削除します。その後、同期ジョブを実行して、LDAP に残っているユーザを更新できます。詳細については、108 ページの「sdaceldap ユーティリティ」を参照してください。

sdldapsync ユーティリティ

sdldapsync ユーティリティを使用すると、コマンド ラインから同期ジョブを実行できます。**sdldapsync** を使用すると、データベースで有効になっている同期ジョブを実行できます。このユーティリティを使用する場合は、RSA Authentication Manager Host Mode の [Edit Synchronization] コマンドを使用して、前もって [Starting At] フィールドの日付を過去の日付に変更します。このように変更することで、RSA Authentication Manager によるジョブの実行と、**sdldapsync** を使用したジョブの実行が誤って同時に行われるのを防ぐことができます。**sdldapsync** のみを使用して実行する新しいジョブを追加し、実行時間として過去の時間をスケジュールしておくとよいでしょう。次のコマンドを入力してください。

```
sdldapsync -j jobnumber
```

job number は、データベース内のジョブの番号です。

コマンド ラインからの LDAP ユーザ データのインポート

以前のリリースと同様に、ユーザ レコードを作成し、インポートと比較ユーティリティを使用してそのユーザ レコードを LDAP ディレクトリ エントリからインポートすることもできます。この既存のユーティリティは、LDAP 同期インタフェースと同じ LDAP ディレクトリ サーバでサポートされます。

ライブラリ パスの設定

LDAP 比較ユーティリティは、RSA Authentication Manager Administration Toolkit の共有オブジェクト ライブラリを使用します。比較ユーティリティを実行する場合、共有オブジェクト ライブラリが保存されているディレクトリがユーザのライブラリ パス環境変数に指定されている必要があります。この環境変数が正しく設定されるように、UNIX 版には **admenv** ユーティリティが提供されています。このユーティリティは、システムにとって適切な環境変数の設定を表示します。**/ace/utils** ディレクトリで **admenv** を実行し、表示された情報に従って環境変数を設定します。

LDAP マップ ファイル

RSA Authentication Manager では、サポートされる LDAP ディレクトリ サーバごとに、マップ ファイルが提供されます。**sdaceldap** ユーティリティはこれらのファイルを使用して、LDAP ディレクトリのエントリを RSA Authentication Manager データベースのフィールドにマップします。このマップ ファイル (**active.map**、**sunone.map**、および **novell.map**) は ***ACEUTILS*** ディレクトリの **toolkit** ディレクトリにあります。

このマップ ファイルを編集すると、LDAP ディレクトリの追加エントリを最大 4 つ、RSA Authentication Manager データベースの拡張フィールドにマップできます。少なくとも、RSA Authentication Manager データベースの Default Login フィールドを LDAP フィールドにマップしなければなりません。

メモ：LDAP マップ ファイルの編集は、プライマリで行う必要があります。

操作手順：プライマリで、[System] > [LDAP Maps] の順にクリックし、使用する LDAP ディレクトリ サービスに対応するマップ ファイルの名前をクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

sdaceldap ユーティリティ

sdaceldap ユーティリティは、Windows では **¥ace¥utils¥toolkit** ディレクトリに、UNIX システムでは **/ace/utils/toolkit** ディレクトリにあります。このユーティリティは、LDAP ディレクトリを RSA Authentication Manager データベースと比較し、カンマ区切り形式 (**.csv**) のファイルを生成します。このファイルには、[Manage LDAP Users] メニュー項目を使用してデータベースにインポートできるユーザ情報が保存されます (LDAP ユーザの情報のみをインポートすることができ、電子メール アドレスや電話番号など、特定のユーザ拡張情報を追加することも選択できます)。

このユーティリティはプライマリでもレプリカでも実行できますが、.csv ファイルのインポートはプライマリで行わなければなりません。

import と **compare** の 2 つのオプションを使用することで、**sdaceldap** ユーティリティが作成するファイルの内容を指定できます。**import** オプションを使用すると、次の情報を格納したファイルが作成されます。

- デフォルト ログインが LDAP ディレクトリに登録されていて、RSA Authentication Manager データベースには登録されていないユーザ。データベースに .csv ファイルをインポートすると、LDAP ユーザとして指定された各ユーザのユーザ レコードが作成されます。
- デフォルト ログインが両方の場所に登録されているが、Authentication Manager データベースのレコードでは LDAP ユーザとして識別されないユーザ。このような**競合**するユーザは、個別に処理することも、一括して処理することもできます。次のような一括オプションを使用できます。
  - RSA Authentication Manager データベースにユーザをインポートしない

- 現在のユーザ レコードのすべての情報を上書きして、インポートする
- 現在のユーザ データを残したまま、[LDAP User] フィールド (およびインポート用に指定した拡張データ フィールド) のみを更新して、インポートする

compare オプションを使用すると、データベースで LDAP ユーザとして指定されているものの、LDAP ディレクトリのエントリが何らかの方法で変更された (そのユーザの LDAP エントリの情報が変更されたか、またはエントリが削除された) ユーザを格納したファイルが作成されます。RSA Authentication Manager データベースに登録されているレコードで LDAP ユーザとして識別されるユーザだけが、LDAP ディレクトリのユーザと比較されます。

ユーティリティを初めて実行するときは、**import** オプションを使用します (**compare** オプションは、RSA Authentication Manager データベースに LDAP ユーザが定義されていない場合は無効です)。2回目以降は、目的に応じて**import**オプションまたは**compare**オプションを選択します。

- 前回のインポート操作の後に LDAP ディレクトリに新しくエントリが追加されたユーザを Authentication Manager データベースに追加するには、**import** を選択します。
- LDAP ディレクトリから以前にインポートしたことのあるユーザのレコードを更新するには、**compare** を選択します。

  このオプションで作成した .csv ファイルをインポートするときに、LDAP エントリからもともとインポートされていたユーザ拡張情報が変更されていた場合は、更新されます。LDAP ディレクトリに登録されていないユーザについては、Authentication Manager データベースのユーザ レコードから LDAP ユーザの定義を削除するか、またはレコードを完全に削除するかを (個々のユーザに対して、またはこのカテゴリ内のすべてのユーザに対して) 選択できます。

構文

次の表は、**sdaceldap** ユーティリティのオプションと引数について説明しています。

オプション	引数	説明
-b	*basedn*	比較に使用する識別ユーザ名が格納されているベース レベルの LDAP ディレクトリを指定します。
-D	*binddn*	指定した LDAP サーバ ディレクトリに登録されている識別ユーザ名。これは、承認された管理者の名前である必要があります。Microsoft Active Directory では、Windows ドメインで認識されたユーザに対して、**-D** オプションを使用する必要があります。そうしないと、0 個のエラー、0 個のユーザが返されます。

オプション	引数	説明
-d	*import* *compare*	Authentication Manager データベースのエントリを、対応する LDAP ディレクトリのエントリと比較し、出力ファイルを作成します。 • **import** オプションを指定すると、LDAP ディレクトリにはエントリがあるものの、RSA Authentication Manager データベースにはユーザ レコードがないユーザのリストを格納したファイルが作成されます。 • **compare** オプションを指定すると、RSA Authentication Manager データベースで LDAP ユーザとして指定されているものの、LDAP ディレクトリのエントリが変更されているユーザのリストを格納したファイルが作成されます。
-h	*hostname* または *IP Address*	LDAP サーバ名または IP アドレス。
-m	*mapfile*	比較時に必要となるマップ ファイル。このファイルは LDAP ディレクトリのエントリを RSA Authentication Manager データベースのフィールドにマップするために使用されます。RSA セキュリティ社は以下の LDAP サーバのマップ ファイルを提供しています。 Sun ONE Directory Server (**sunone.map**) Novell NDS eDirectory (**novell.map**) Microsoft Active Directory (**active.map**)
-o	*filename*	CSV 出力ファイルの名前。
-P	*pathname*	SSL 接続で使用する証明書が格納されている証明書データベースへのパス名。
-p	*ldap port*	**sdaceldap** が LDAP ディレクトリ サーバへの接続に使用する TCP ポート番号。デフォルト設定は 389 です。
-s	*base* *one* *sub*	検索する LDAP ディレクトリのレベルを指定します。 **base** -- ベース DN を検索します。 **one** -- ベースの 1 つ下のレベルを検索します。 **sub** -- ベースの下のすべてのレベルを検索します。
-w	*password*	識別名と一緒に使用するパスワードを指定します。
-Z	なし	LDAP ディレクトリに対する接続 (SSL で暗号化された接続) を指定します。SSL 接続を確立する場合は、証明書データベースにアクセスするために **-P** 引数を指定する必要があります。

例

次の例では、LDAP ディレクトリに登録されているユーザのうち、Authentication Managerデータベースにユーザ レコードが登録されていないすべてのユーザのリストが格納されているファイルを作成します。

この例は、SSL (Secure Socket Layer)接続を使用して、AIXプラットフォームでMicrosoft Active Directory サーバに対して実行されています。Microsoft Active Directory サーバからの証明書は Netscape ブラウザにインポートされ、**-P** オプションに指定されたディレクトリ パスに **cert7.db** と **key3.db** がコピーされました。

```
sdaceldap -h active -p 636 -Z -P "/ace/data/ldapjobs/sslcerts"
-D "user@rsa.com" -w passwd -b "cn=Users,DC=hixville,DC=com"
-d import -m active.map -s sub -o aixact.csv "objectclass=user"
```

メモ : この例は、実際には 1 行のコマンド ラインです。ただし、ここではオプションと引数の組み合わせをわかりやすく示すために、改行を挿入しています。

このコマンドを RSA Authentication Manager で実行すると、**active** という LDAP ディレクトリ サーバが指定され、ポート番号 **636** を使用して接続されます。**-Z** オプションは、SSL 接続を使用することと、SSL 接続に必要な **cert7.db** および **key3.db** ファイルが **/ace/data/ldapjobs/sslcerts** ディレクトリにあることを示しています。LDAP ディレクトリ サーバへの接続を試みているユーザは **user@rsa.com** で、パスワードは **passwd** です。このユーティリティは、ベース レベル **cn=Users,DC=hixville,DC=com** の下のサブレベル **(-s sub)** をすべて検索します。このユーティリティはMicrosoft Active Directory サーバ用のマップ ファイル **(-m active.map)** を使用して **aixact.csv** という名前のファイルを生成します。フィルタ **objectclass=user** を使用すると、ファイルの内容は、LDAP ディレクトリに登録されているユーザのうち、RSA Authentication Manager データベースにユーザ レコードが登録されていないすべてのユーザに制限されます。

メモ : フィルタは、インポート **(-d import** オプションを使用) 時にのみ適用されます。**-d compare** オプションを使用する場合は適用されません。サポートされているフィルタについては、LDAP ディレクトリのマニュアルを参照してください。

SSL の使用

使用している LDAP ディレクトリ サーバへの SSL 接続を確立するには、**sdaceldap** および **sdldapsync** ユーティリティで、適切に構成された **cert7.db** (証明書データベース) が必要です。これを可能にするために、RSA Authentication Manager 6.1 には **www.mozilla.org** から提供されているオープン ソース ユーティリティ **certutil.exe** が含まれています。このユーティリティを使用すると、**cert7.db** ファイルを作成し、使用している LDAP ディレクトリ サーバの証明書 (.cer または .crt) ファイルをインポートできます。

certutil.exe ユーティリティは ***ACEUTILS*/toolkit** ディレクトリにあります。Microsoft Active Directory、Sun ONE Directory、および Novell NDS eDirectory の証明書をインポートできます。次のサンプル コマンドは、**cert7.db** ファイルを作成し、Microsoft Active Directory 証明書ファイルを証明書データベースにインポートします。

```
certutil.exe -A -n ace_ads -t P -i /data/LDAP/ADS_1.cer -d
/top/ace/data/ldapjobs/sslcerts
```

次の表は、このサンプル コマンドで使用されているオプションを示しています。**certutil.exe** ユーティリティの詳細については、**http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html** を参照してください。

オプション	引数	説明
-A	なし	証明書が証明書データベースに追加されることを指定します。**cert7.db** が存在しない場合は作成されます。
-n	*name*	LDAP サーバ証明書のニックネーム (この場合は “ace_ads”) を指定します。このニックネームが実際の証明書ファイルの名前と一致する必要はありませんが、証明書データベース内で固有の名前である必要があります。
-t	*trustedargs*	証明書の作成時に証明書に適用される信頼属性を指定します。RSA Authentication Manager で使用する場合は、**P** オプション (有効なピア / 信頼されるピア) のみを指定する必要があります。
-i	*pathname*	証明書データベースに追加する LDAP ディレクトリ サーバの証明書ファイルのフルパス名を指定します。
-d	*path*	**cert7.db** および関連ファイルを作成するディレクトリを指定します。RSA Authentication Manager で使用する場合は、***ACEDATA*/ldapjobs/sslcerts** を指定してください。

証明書データベースを作成し、サーバの証明書をその証明書データベースにインポートしたら、**sdaceldap** または **sdldapsync** ユーティリティを実行する RSA Authentication Manager プライマリまたはレプリカに **cert7.db** をコピーできます。

LDAP ユーザの管理

[User] > [LDAP Users] > [Manage LDAP Users] を使用すると、**sdaceldap** ユーティリティで作成したファイルを Authentication Manager データベースにインポートできます。比較ユーティリティはどの Authentication Manager (プライマリまたはレプリカ) でも実行できますが、ファイルをインポートできるのはプライマリだけです。作成されたファイルを処理すると、データベースには、処理した各ユーザのユーザ レコードが登録されます。ユーザにグループを割り当てた後、このファイルを処理すると、データベースには、処理したユーザが所属しているグループが登録されます。

操作手順 : [User] メニューから [LDAP Users] を選択し、[Manage LDAP Users] をクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

ユーザ レコードの内容

各ユーザ レコードには、RSA SecurID トークン保有者に関して、次の情報が格納されます (Default Shell など、一部の情報はオプションです)。

- ユーザ名
- デフォルト ログイン
- Default Shell (AIX 以外の UNIX エージェント ホストの場合)
- ユーザがローカル ユーザの場合は、トークン タイプ、ユーザが PASSCODE とトークンコードのみのどちらで認証を受けるかどうか、トークン ステータス、およびユーザに割り当てられているトークンのシリアル番号
- アドミニストレーション権限のレベル
- ユーザが自分の PIN を作成できるかどうか
- ユーザが認証を受けることができる期間の最初の日と最後の日
- ユーザが 1 つ以上のエージェント ホスト上で直接アクティブ化される場合は、ユーザが各エージェント ホストで認証を受けることができる時間

操作手順：[User] > [Add User] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。ユーザ情報を変更するには、[User] > [Edit User] の順にクリックします。

他のインストレーションとのトークン レコード データの共有

RSA Authentication Manager のエクスポート オプションを使用すると、異なる Authentication Manager 間でトークン レコードを移動できます。このエクスポート オプションによって、トークン レコードのダンプ ファイル (.dmp) が作成されます。必要に応じて、そのトークンに関連付けられているユーザ情報をエクスポートできます。

メモ：RSA Authentication Manager 6.1 では、トークンを ASCII(.asc) 形式にエクスポートできなくなりました。v5.0 より前の RSA ACE/Server ソフトウェアでは、ASCII 形式のファイル**だけ**がインポートできます

別のシステムでトークン レコードを使用するには、[Token] メニューの [Export Token] のオプションを使用します。その後、[Token] メニューの [Import Tokens] のオプションを使用して、トークン レコードを別のシステムにインポートします。

トークンの割り当て

RSA Authentication Manager データベースを初めてインストールした時点では、このデータベースは空で、RSA セキュリティから納品されたトークン レコードは割り当てられていません。トークンをユーザに割り当てるには、その前にトークン レコードをデータベースにインポートし、承認された各ユーザのレコードを作成しなければなりません。

ユーザにトークンを割り当てると、ユーザはアクティブ化されます。1 つ以上のトークン (またはユーザ パスワード) をユーザに割り当てると、そのユーザはアクティブ ユーザとみなされます。アクティブ ユーザの数が、ライセンスで許諾されているアクティブ ユーザ数を超えないかどうかを確認してください。つまり、アクティブ ユーザ数が 900 のライセンスを持っている場合、900 人のユーザにそれぞれ最大 3 個のトークン (またはユーザ パスワード) を割り当てることができます。

ライセンスとアクティブ ユーザの詳細については、付録 A「ライセンス」を参照してください。

重要 : Authentication Manager は入力情報をチェックするときに、各トークンを順に照合するため、1 人のユーザに割り当てられるトークンの数が多くなると、認証要求の処理時間が長くなります。一致するトークンが見つからない場合は、ユーザの**すべて**のトークンの不正ログイン カウントが更新されるため、トークンが無効になったり、ネクスト トークンコード モードに設定される可能性が高くなります。例については、123 ページの「トークンによる攻撃の回避」を参照してください。

RSA SecurID ソフトウェア トークン

RSA SecurID ソフトウェア トークンは、ユーザのコンピュータ、RSA SecurID スマート カード、またはその他のデバイス (Palm Pilots、Pocket PC、携帯電話など) に常駐するソフトウェア ベースのセキュリティ トークンです。このソフトウェアは、ユーザが RSA Authentication Manager で保護されたネットワークまたはスタンドアロン リソースにアクセスするときに、二要素認証方式を使用します。

ソフトウェア トークンには、SID (64 ビット) アルゴリズムまたは AES (128 ビット) アルゴリズムを実行するものがあります (携帯電話用は SID アルゴリズムのみです)。RSA Authentication Manager が発行するソフトウェア トークン レコードはすべて .sdtid ファイルです。このソフトウェア トークン アプリケーションは、配布されたトークンのタイプを判別し、それに従ってファイルを読み取ります。

AES (128 ビット) ソフトウェア トークンの発行では、定義済みの **DeviceSerialNumber** という名前の拡張フィールドが含まれるため、トークンをインストールするデバイスを 1 つのみに限定できます。**DeviceSerialNumber** フィールドにシリアル番号を入力すると、その番号はエンド ユーザがソフトウェア トークン アプリケーションを使用してインストールするトークン ファイルに含まれるようになります。ユーザが入力したシリアル番号がファイル内の番号と一致しない場合、トークンはインストールされません。

重要 : ソフトウェア トークンが格納されている XML ファイルに対しては、パスワードで保護する機能を利用してください。また、すべてのソフトウェア トークン ファイルを、安全なマシンの安全なディレクトリに保管してください。

ソフトウェア トークンの発行 (Issue Software Token)

ソフトウェア トークンを発行すると、そのトークンは自動的に有効になり、[RSA SecurID Issue Software Tokens] ダイアログ ボックスで選択したユーザまたはユーザ グループに割り当てられます。この処理中にソフトウェア トークンを含むファイルが生成され、ファイルのネットワーク上の位置を指定できます。この後で管理者は RSA Security ソフトウェア トークン アプリケーションを使用して、サポートされているデバイスにソフトウェア トークンをインストールできます。ソフトウェア トークンの詳細については、製品に付属のマニュアルを参照してください。

操作手順：[Token] > [Issue Software Tokens] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

ソフトウェア トークンの失効 (Revoke Software Token)

ソフトウェア トークンを失効にすると、そのトークンは自動的に無効になり、ユーザへの割り当てが解除されます。

操作手順：[Token] > [Revoke Software Tokens] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

ソフトウェア トークンの再発行 (Reissue Software Token)

ソフトウェア トークンを再発行しなければならないことがあります。トークンを再発行すると、前に発行したトークンは正しいコードを生成しなくなり、機能しなくなります。同一のトークンを同一のユーザに再発行する場合は、トークンを最初に発行するときに [Issue Software Token] ダイアログ ボックスの [Retain token information] を選択する必要があります。

トークン レコードの内容

[Edit Token] ダイアログ ボックスには、指定されたトークンのトークン レコードの情報が表示されます。[Edit Token] ダイアログ ボックスを表示するには、[Token] > [Edit Token] の順にクリックします。

ここでは、[Edit Token] ダイアログ ボックスの各フィールドについて説明します。

[Serial Number] …ハードウェア トークンの背面に記載されているか、またはソフトウェア トークンの GUI に表示されるシリアル番号。

[Algorithm is] … SID トークンは独自の SID アルゴリズムを使用して時間ベースの認証機能を提供し、AES トークンは AES (Advanced Encryption Standard) 暗号化アルゴリズムを使用して時間ベースの認証機能を提供します。

[Assigned to] …トークンが割り当てられている場合は、このフィールドにはトークンが割り当てられているユーザの名前が表示されます。この名前は、ユーザの名前またはログインです。

[Next Tokencode Mode] …この値が On の場合は、このトークンの PIN とコードを認証で次回使用するときに、システムへのアクセスが許可される前に、トークンに表示される次のコード (ネクスト トークンコード) を入力するように要求されます。

[Replacement Serial Number] … このフィールドは、編集の対象として選択したトークンに交換用トークンが割り当てられている場合にだけ表示されます。このフィールドには、割り当てられている交換用トークンのシリアル番号と種類が表示されます。

[Lost Status] … トークンを紛失したかどうかを示す状態。Lost ステータスのトークンにだけ、テンポラリ パスワードを割り当てることができます。トークンを紛失した場合は、次のテンポラリ パスワード情報が表示されます。

- パスワードのタイプ (固定またはワンタイム パスワード セット)

- 有効期限の日時

固定パスワードの場合、“AUTO” は固定パスワードの有効期限が切れたときにトークン ステータスが **Not Lost** に変更されることを示します。RSA Authentication Manager では、[Enter Lost Token Password] ダイアログ ボックスで [When lost status expires, mark token as Not Lost] が選択されている場合に、この変更を実行します。

[Software Token] … トークンが発行されたソフトウェア トークンの場合、次の情報が表示されます。

- トークン ファイルを保護するために割り当てられているパスワード
- トークンのコピー保護の状態
- トークンの発行回数
- トークンが現在発行されているかどうか

[Last Login Date] …このトークンを使用して最後に正しく認証を受けた日時、または同期をとり直すことができた日時。世界協定時 (Coordinated Universal Time) で表示されます。トークンが割り当てられていない場合や、新たに割り当てられた場合は、このフィールドは意味がないので、01/01/1986 という初期値が表示されます。

[Enabled Status] …[Enabled] チェックボックスがオンの場合、トークンは有効な状態です。トークンが無効の場合は、認証のためにそのトークンを使用できません。この値は、管理者が [Enabled] チェックボックスを使用して設定するか、または不正な認証の試みが連続して行われたときに設定されます。後者の場合は、トークンが自動的に無効になります。詳細については、122 ページの「トークンが盗まれたり、紛失した場合」を参照してください。

[Token Start Date] と [Token Shutdown Date] …トークンがコードの表示を開始した日付と終了する日付 (*mm/dd/yyyy* 形式) と時刻。シャットダウン日が過ぎると、トークンは機能しなくなります。

メモ：トークン レポートではローカル時刻ではなく世界協定時が使用されるので、トークンのシャットダウン日時が、[Edit Token] ダイアログ ボックスに表示されるトークンのシャットダウン日時と数時間ずれることがあります。

[New PIN mode] …[New PIN mode] チェックボックスがオンの場合には、管理者はトークンを New PIN モードに設定しています。この場合、RSA SecurID で保護されたリソースにアクセスする前に、ユーザは New PIN 操作を実行しなければなりません。

[Token Assignment Date] …トークンがユーザに割り当てられた日付。トークンが割り当てられていない場合は、日付の位置に「NONE (なし)」と表示されます。割り当てられたトークンが以前のバージョンの RSA Authentication Manager の .asc ファイルまたは .dmp ファイルからインポートされたものであるか、5.2 より前のバージョンからアップグレードされたものである場合は、日付の位置に「UNDEFINED (未定義)」と表示されます。

[User Authenticates With] …ユーザが PASSCODE とトークンコードのみのどちらで認証を受けるかを指定します。詳細については、105 ページの「PIN を必要としないトークン」を参照してください。

トークン レコードには次の情報も格納されていますが、これらの情報は絶対に表示されません。

- 同期オフセット値。128 ページの「同期」を参照してください。
- トークンの擬似乱数コードを生成するために使用される固有のキー。
- 割り当てられているユーザだけが知っているトークンの PIN。
- トークンを使用して認証要求に連続して失敗した回数。

不正な認証要求が一定回数連続して実行されると、使用されていたトークンは無効になります。

不正な PIN と有効なトークンコードを使用して認証を受けようとした場合、不正な認証の試みが、あらかじめ設定されている回数に到達する前に、スタンダードカードまたはキーホルダは無効になります。このような場合は、承認されていないユーザがトークンを取得し、そのトークンと推測した PIN を使用していると解釈されます。この種の認証の試みが 3 回連続して行われると、そのトークンは無効になります。

次の場合は、この数が 0 にリセットされます。1) トークンを使用してユーザが正しく認証を受けることができた場合、2) 管理者がトークンの同期をとり直すか、トークンの割り当てを解除した場合、3) 誤った PASSCODE が一定回数連続して入力され、トークンが無効になった後、管理者がそのトークンを再び有効にした場合。

メモ：1 人のユーザに複数のトークンが割り当てられている場合、不正な認証要求は、そのユーザに割り当てられているすべてのトークンに影響します。つまり、不正な認証試行を行っていないトークンが無効になったり、ネクスト トークンコード モードになることがあります。

トークン拡張データの変更

トークン拡張レコードの情報を変更するには、[Edit Token]ダイアログ ボックスの[Edit Token Extension Data] をクリックします。トークン拡張レコードには、カスタム アドミニストレーション プログラムからアクセスできるユーザ定義トークン情報が格納されています。

グループの作成と変更

このセクションでは、制限されたエージェント ホストでユーザ グループをアクティブ化するための管理ツールについて説明します。

メモ：システムのすべてのエージェント ホストがオープン エージェント ホストである場合は、このセクションの情報を参照する必要はありません。グループ機能は、特定のユーザとユーザ グループのリストに制限されているエージェント ホストの場合にだけ有効です。

ユーザをグループにまとめておくと、管理に必要な時間を短縮し、便利な方法でユーザを管理できます。ユーザをグループに登録しておけば、グループ全体を 1 回の操作でアクティブ化することができ、多数のユーザを個別にエージェント ホストで直接アクティブ化する必要がありません。このようにしておけば、グループに対して行った変更は、グループがアクティブ化されたすべてのエージェント ホストで有効になります。たとえば、メンバをグループに追加したり、グループから削除すると、対応するグループがアクティブ化されているすべてのエージェント ホストで、そのメンバのアクセスが一度に許可または拒否されます。1 つのグループを複数のエージェント ホストでアクティブ化することができます。

また、グループをサイトに関連付けることもできます。1 つのサイトにグループをいくつでも登録できます。サイトの詳細については、130 ページの「サイトの作成と変更」を参照してください。

操作手順：グループを作成するには、[Group] メニューの [Add Group] をクリックして [Add Group] ダイアログ ボックスを表示します。詳細については、[Help] をクリックして表示される情報を参照してください。

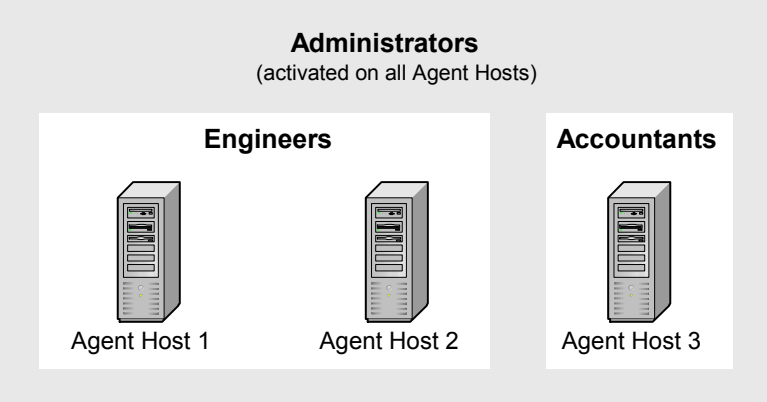
エージェント ホストでユーザをアクティブ化するためのグループの使用例

部署ごと、ビルのフロアごと、または類似した状況のユーザごとなどに、グループを作成できます。

例：権限のレベルによってユーザをグループに分類すると、便利な場合があります。たとえば、レルム管理者で構成される **Administrators** というグループを作成し、プライマリおよびレプリカを含めて (保護のために RSA Authentication Agent ホストとして設定しておかなければなりません)、すべてのマシンでこのグループをアクティブ化することができます。

Authentication Manager にアクセスする必要のない他のユーザは、部署や他の何らかの基準によってグループに分類できます。たとえば、エンジニアリング部門は 2 つのエージェント ホストにアクセスする必要があり、経理部門は 1 つのエージェント ホストにだけアクセスする必要があるとしましょう。このような場合は、**Engineers** というグループを作成し、エンジニアリング部門のすべてのメンバをこのグループに登録し、2 つのエージェント ホストでグループをアクティブ化します。次に **Accountants** という別のグループを作成し、経理部門のすべてのメンバをこのグループに登録し、そのグループを 1 つのエージェント ホストでアクティブ化します。

次の図は、上記のグループのアクティブ化の例を示しています。



グループ メンバーシップ リストの作成と変更

メンバをグループに追加するには、[Add User] または [Edit User] ダイアログ ボックスの [Group Memberships] ボタンを使用します。105 ページの「ユーザ レコードの作成と変更」を参照してください。また、[Add Group] または [Edit Group] ダイアログ ボックスの [Members] ボタンを使用することもできます。

グループ拡張データの変更

グループ拡張レコードの情報を変更するには、[Add Group] または [Edit Group] ダイアログ ボックスの [Edit Group Extension Data] ボタンを使用します。これらのレコードには、カスタム アドミニストレーション プログラムからアクセスできる情報 (組織で定義された情報) が格納されます。

RSA Authentication Manager Administration Toolkit を使用してカスタム アドミニストレーション プログラムを作成する方法については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

エージェント ホスト上でのアクティブ化

エージェント ホストの設定によっては、ユーザ レコードまたはグループ レコードにエントリを追加して、エージェント ホストにユーザまたはグループを明示的に関連付けなければならないことがあります。このようにすると、そのユーザまたはグループはエージェント ホストでアクティブ化されたとみなされます。この操作が必要かどうかは、エージェント ホストの設定によって決まります。

エージェント ホストは特定のユーザおよびグループに**制限**したり、ローカルで認識されるすべてのユーザに**オープン**にすることができます。オープン エージェント ホストの場合は、ローカル RSA Authentication Manager データベースに登録されている他のレルムのユーザのアクセスも許可されるように設定できます。オープン エージェント ホストおよび制限されたエージェント ホストの詳細については、56 ページを参照してください。

すべてが適切にインストールされていれば、エージェント ホストはユーザに正しい PASSCODE の入力を要求して、ログイン試行に応答します。PASSCODE が正しいというだけでアクセスが許可されるかどうかは、次の表に示すように、エージェント ホストの設定によって異なります (すべてのユーザが正しい PASSCODE を入力したものとします)。

エージェント ホストの設定	アクセスが許可されるローカル ユーザ	アクセスが許可される外部ユーザ
直接アクティブ化されたユーザおよびグループに**制限**されている。	直接アクティブ化されたユーザ、または直接アクティブ化されたグループのメンバであるユーザのみ。	直接アクティブ化されたユーザ、または直接アクティブ化されたグループのメンバであるユーザで、ホーム レルムがローカルに登録されているユーザのみ。
オープンであり、登録されたレルムでユーザを検索するように設定されている。	すべてのユーザ。	ホーム レルムがローカルに登録されているすべてのユーザ。
オープンであるが、検索されないように設定されている。	すべてのユーザ。	どのユーザも許可されない。

メモ：上の表には記載されていませんが、オープン エージェント ホストではユーザおよびグループのアクセス時間を制限できます。それには、制限されたエージェント ホストの場合と同様に、ユーザおよびグループを直接アクティブ化し、アクセス時間を定義します。120 ページの「ユーザおよびグループのアクセス時間の変更」を参照してください。

ユーザのアクティブ化と非アクティブ化

エージェント ホストでユーザをアクティブ化したり、非アクティブ化するには、[Add User] または [Edit User] ダイアログ ボックスの [Agent Host Activations] をクリックするか、[Add Agent Host] または [Edit Agent Host] ダイアログ ボックスの [User Activations] をクリックします。

グループのアクティブ化と非アクティブ化

ユーザをエージェント ホストで個別に直接アクティブ化することもできますが、ユーザをグループに登録し、エージェント ホストでそのグループのすべてのメンバを同時にアクティブ化すると、管理上さらに便利です。

グループについてと、グループの作成およびメンバの追加手順については、117 ページの「グループの作成と変更」および 118 ページの「グループ メンバーシップ リストの作成と変更」を参照してください。

エージェント ホストでグループをアクティブ化または非アクティブ化するには、次のいずれかの操作を実行します。

- [Add Group] または [Edit Group] ダイアログ ボックスの [Agent Host Activations] をクリックします。
- [Add Agent Host] または [Edit Agent Host] ダイアログ ボックスの [Group Activations] をクリックします。

ユーザおよびグループのアクセス時間の変更

デフォルト設定では、ユーザは、自分がアクティブ化されている、保護されたエージェント ホストでいつでも認証を受けることができます。アクティブ化されたグループのメンバについても同様です。ただし、[Edit Access Times] 機能を使用すれば、管理者はユーザまたはグループが認証を受けることができる時間を制限できます (たとえば、8 a.m. ～ 5 p.m. や月～金曜日、あるいは週末のみなど)。

[Edit Access Times] 機能で制限されるのは**認証**だけです。指定の時間になるまでに認証を受けたユーザは、ユーザ側の何らかの動作で PASSCODE プロンプトが新たに表示されるまで (たとえば、ユーザがいったんログアウトして再度ログインするなど)、そのままアクセスを続行できます。

操作手順：

- 個々のユーザの場合は、[User] > [Add User] > [Edit Access Times] または [User] > [Edit User] > [Edit Access Times] の順にクリックします。
- グループの場合は、[Group] > [Add Group] > [Edit Access Times] または [Group] > [Edit Group] > [Edit Access Times] の順にクリックします。

詳細については、[Help] をクリックして表示される情報を参照してください。

ユーザへのハードウェア トークンの配布

ハードウェア トークンをユーザに配布する場合は、次に示すように安全な手段を使用してください。

- 割り当てられているだけで、まだ無効のトークンを配布します。
- トークンを割り当てられたユーザがそのトークンを保有していること、およびそのユーザがトークンを使用してログインできる状態になったという通知を受けてから、トークンを有効にします。
- 有効に設定したトークンをユーザに配布するときは、信頼できる人が直接納品するなど、安全な方法で配布します。

各ユーザに割り当てたトークンを配布するときは、トークンの使い方を説明した認証手順マニュアルのコピーも渡してください。認証手順マニュアルが格納されている場所とその印刷方法については、11 ページの「マニュアル」を参照してください。RSA SecurID ハードウェア トークンのメンテナンスについての説明は、各トークンに添付されています。トークンの配布計画の詳細については、『RSA Authentication Manager 6.1 Deployment Guide』を参照してください。

メモ: RSA SecurID ソフトウェア トークンの配布と使用の手順については、『RSA SecurID Software Token 3.0 for Windows® Workstations Administrator's Guide』および『RSA SecurID Software Token 3.0 for Windows® Workstations User's Guide』を参照してください。

ユーザの認証に関する問題の回避と処理

RSA SecurID 認証がユーザの日常業務で定期的に行われるようになると、トークンと認証に関する問題が発生することがあります。このセクションでは、RSA Authentication Manager の管理中に実行する必要のある対処作業について説明します。その前に、問題を最小限に抑えるためのユーザ教育について説明します。

セキュリティ上の責任に関するユーザの教育

安全なシステムを実現するために重要なことは、セキュリティの保護責任について、ユーザを教育することです。承認されたユーザがセキュリティに関して各自の義務を果たさず、その責任を深刻に受け止めなければ、どんなに強力なセキュリティ製品でもシステムを完全に保護することはできません。

侵入者がユーザの PIN と RSA SecurID トークンの両方を取得してしまうと、RSA Authentication Manager はシステムを**保護できません**。ユーザと管理者はそのことを十分理解しておく必要があります。そのため、次のユーザ側の責任について、すべてのユーザが確実に認識することが重要です。

- ユーザは自分の PIN を他人に知られないようにしなければなりません。
- ユーザは自分のトークンを物理的に安全に管理しなければなりません。
- PIN が他人に知られた可能性があるときは、そのことをただちに管理者に報告してください。
- トークンを紛失したときは、そのことをただちに管理者に報告してください。
- トークンが破損しないように、物理的に保護してください。
- 侵入者がシステムに不正に侵入する隙がないように、必ず標準ログオフ手順に従ってください。
- 自分のアカウントは自分だけが使用するようにし、他人に使わせないようにしてください。

トークンの割り当ての解除

トークンの割り当てを解除すると、ユーザ レコードとトークン レコードの間のリンクが解除され、PIN がクリアされます。割り当てられていないトークンは認証に使用できません。

通常、ユーザが会社を辞めるときは、トークンの割り当てを解除します。その場合、トークンを削除するのではなく、単に割り当てを解除します。このようにしておけば、トークン レコードはデータベースに残り、後で別のユーザにトークンを再割り当てすることができます。トークンを削除すると、トークン レコードがデータベースから永久に削除されます。

操作手順: [Token] > [Edit Token] の順にクリックします。トークンを選択して [Edit Token] ダイアログ ボックスを表示し、[Unassign Token] をクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

メモ：ユーザに割り当てた RSA SecurID ソフトウェア トークンを失効にするには、[Token] メニューの [Revoke Software Tokens] オプションを選択します。ソフトウェア トークンを失効にすると、そのトークンは自動的に割り当てが解除されます。

ユーザがトークンを紛失した場合は、割り当てを解除するのではなく、単に無効にしてください。次のセクション「トークンの無効化」を参照してください。

トークンの無効化

トークンを無効にしても、トークン レコードに格納されているすべての情報 (ユーザの PIN など) はそのまま保存されます。承認されたユーザが紛失したトークンを後で発見した場合には、トークンを再度有効にして、使用することができます。無効にしたトークンは認証に使用できませんが、ユーザ レコードとトークン レコードの間の関連付けはそのまま保持されています。管理者はいつでもトークンを有効にできます。

承認されたユーザがトークンを紛失したことを報告してきた場合は、そのトークンを無効にしてください。紛失したトークンが後で見つかった場合、管理者がそのトークンを再度有効にすると、トークンは再び使用できるようになります。その際に、管理者やユーザが他の処置をとる必要はありません。

操作手順：[Token] > [Edit Token] の順にクリックします。トークンを選択して [Edit Token] ダイアログ ボックスを表示し、[Enabled] チェックボックスをオフにします。詳細については、[Help] をクリックして表示される情報を参照してください。

トークンが RSA Authentication Manager によって無効に設定される場合

管理者がトークンを無効にするのではなく、Authentication Manager がトークンを無効にする場合があります。RSA SecurID スタンダード カードまたはキーホルダに表示された正しいコードと間違った PIN の組み合わせを使用して認証を受けようとした場合、3 回数連続して誤った組み合わせを入力すると、Authentication Manager はトークンを無効にします。この場合、承認されていない人物がトークンを不正に取得して、そのトークンと推測した PIN を使用してアクセスしようとしているものと解釈されます。

また、一定回数、連続して認証要求に失敗した場合も、Authentication Manager はユーザのトークンを無効にします。トークンが無効になるまでに認められる認証失敗の連続回数は設定可能です。詳細については、61 ページの「不正な PASSCODE を処理するエージェントの設定」を参照してください。

トークンが盗まれたり、紛失した場合

重要：紛失したトークンや盗まれたトークンは**ただちに**無効にしなければなりません。RSA SecurID トークンと PIN が盗まれると、承認されていないユーザがシステムにアクセスできるようになります。

トークンを盗まれたり、紛失した場合は、ただちに管理者に報告するように、すべてのユーザに指示してください。**そのような報告を受けた場合、管理者はただちにトークンを無効にしなければなりません** (安全性は低下しますが、ユーザにテンポラリ パスワードを割り当てることもできます。この機能を使用するかどうかは、セキュリティ ポリシーに応じて異なります。詳細については、124 ページの「紛失したトークンの代わりに使用するテンポラリ パスワード」を参照してください)。

しかし、承認されたユーザがトークンの紛失を報告する前に、承認されていない人物がトークンを取得し、そのトークンを使用してしまう可能性があります。RSA Authentication Manager の攻撃回避機能は、このような場合にセキュリティを維持するのに役立ちます。

盗んだトークンを使用してシステムに侵入しようとすると、Authentication Manager はこのような攻撃を検出し、アクセスを拒否し、トークンを無効にすることができます。しかし、ユーザの PIN と RSA SecurID トークンの両方を攻撃者が取得した場合は、この機能があっても、システムを**保護することはできません**。

したがって、次の対策をとることが**重要**です。

- すべてのユーザは、自分のトークンを物理的に安全に保護し、PIN を他人に知られないようにしなければなりません。
- トークンを紛失したり、PIN が他人に知られた可能性があるという報告を受けた場合は、ただちにトークンを無効にしなければなりません。

操作手順：[Token] > [Edit Token] の順にクリックします。トークンを選択して [Edit Token] ダイアログ ボックスを表示します。

- トークンを無効にするには、[Enabled] チェックボックスをオフにします。
- PIN を無効にするには、[Clear PIN] をクリックします (詳細については、125 ページの「PIN が盗まれたり、他人に知られた場合」を参照してください)。

詳細については、[Help] をクリックして表示される情報を参照してください。

トークンによる攻撃の回避

次のように、認証試行が連続して失敗すると、その認証で使用されたトークンは RSA Authentication Manager によって無効にされます。

- トークンコードと PIN を別々に入力する必要のあるトークン (RSA SecurID スタンダード カードとキーホルダ) は、認証要求で正しいトークンコードと不正な PIN の組み合わせが 3 回連続して入力されると、無効になります (3 回という回数は変更できません)。
- トークンの種類に関係なく、**どの**トークンも、認証要求が一定回数連続して失敗すると無効になります。この回数は、どの種類のエージェント ホストでも設定できますが、4 回以上の値に設定した場合でも、前の項目で説明した規則は変わりません。

メモ：これらの機能は、旧バージョンのエージェント ホストではサポートされていません。

ユーザが複数のトークンを使用している場合は、Authentication Manager は不正に使用されたトークンと他のトークンとを区別しません。認証が失敗した場合は、失敗したトークンだけでなく、すべてのトークンの不正ログイン カウントが加算されます。認証が成功すると、その認証で使用されたトークンに**対してだけ**、不正ログイン カウントがクリアされます。このように、認証要求の失敗は累積され、ユーザが保有しているすべてのトークンまたはほとんどすべてのトークンを同時に無効にします。

ここでは、複数のトークンがある場合の 2 つの例について考えてみましょう。どちらの例でも、認証要求が連続して 4 回失敗するとトークンが無効になるように、Authentication Manager を設定しています。また、ユーザは 3 つのトークン A、B、C を保有しており、認証要求が 3 回連続して失敗したために、各トークンの不正ログイン カウントが累積されているものとします。

- ユーザがトークン A を使用してログオンしようとし、誤った PASSCODE を入力しました。認証要求の失敗によって、各トークンの不正ログイン カウントが 3 から 4 に増加したため、Authentication Manager は 3 つのすべてのトークン (A、B、および C) を無効にします。

- ユーザがトークン C を使用してログオンし、正しく認証を受けることができました。この場合、システムはトークン C の不正ログイン カウントをクリアしますが、トークン A とトークン B にはまだ 3 回の不正ログイン カウントが累積されています。

  次回の認証で、ユーザは再びトークン C を使用してログオンを試みましたが、誤った PASSCODE を入力しました。その結果、トークン C の不正ログイン カウントは 1 になりますが、トークン A とトークン B の不正ログイン カウントは 4 になります。したがって、Authentication Manager はトークン A とトークン B を無効にします。

紛失したトークンの代わりに使用するテンポラリ パスワード

ユーザがトークンを紛失した場合は、トークンを無効にしてください。しかし、各組織のセキュリティ ポリシーと、ユーザのセキュリティ要件によっては、ユーザが紛失したトークンを探している間、ユーザにテンポラリ パスワードを割り当てることにより、その後もユーザがシステムにアクセスできるように設定できます。テンポラリ パスワードには次の 2 種類があります。

- 単一の**固定**テンポラリ　パスワード。有効期限が切れるまで何度でも使用できます。
- 複数の**ワンタイム** テンポラリ パスワードのセット。それぞれ 1 回だけ使用でき、指定した日付にすべてのパスワードの有効期限が切れます。

ユーザがテンポラリ パスワードを使用して認証を受けるには、「Enter PASSCODE (PASSCODE を入力してください)」プロンプトに対して PIN とテンポラリ パスワードを入力します。その場合、PIN を使用するときと同じ手順および必要条件が適用されます。

テンポラリ パスワードを使用したアクセスに失敗すると、紛失したトークンに対して記録されている連続した不正ログオンのカウントが更新されます。認証が成功すると、このカウントは 0 にリセットされます。他のトークンと同様に、一定回数連続して認証に失敗すると、紛失したトークンは自動的に無効になります。

テンポラリ パスワードを割り当てるには、その前にトークン ステータスを **Lost** として定義しなければなりません。トークンが見つかったら、トークンステータスを **Not Lost** に変更します。ステータスを変更することにより、そのトークンを使用して再び認証を受けることができるようになります。トークンを **Not Lost** に変更すると、それまでそのトークンに対して作成したテンポラリ パスワードは無効になります。トークン ステータスを **Lost** から **Not Lost** に変更すると、削除されたワンタイム パスワード情報が Authentication Manager から通知されます。

操作手順：[Token] メニューの [Edit Token] をクリックしてトークンを選択し、[Edit Token] ダイアログ ボックスを表示します。詳細については、[Help] をクリックして表示される情報を参照してください。

- トークン ステータスを変更するには、[Edit Lost Status] をクリックします。
- パスワードを割り当てるには、認証方式として [Fixed Password] または [One-Time Password Set] を選択します。次に、[Set up Passwords] をクリックします。

紛失したトークンはトークン統計情報の一部としてカウントされ、別のレポートにリストできます。紛失したトークンをエクスポートすることはできますが、**Lost** というステータスは保存されません。

メモ：テンポラリ パスワードはユーザ パスワードと異なります。Authentication Manager はユーザ パスワードを一種のトークンとして扱います。ユーザの標準的な認証手段として、ユーザ パスワードを割り当てることができます。詳細については、15 ページの「ユーザ パスワード トークン」を参照してください。

オフライン認証ユーザのエマージェンシー アクセス

使用しているコンピュータが会社のネットワークに接続されていないオフサイト ユーザ (オフィスの外部にいるユーザ) に対して、オフライン認証を導入している場合は、さまざまな状況でエマージェンシー アクセスを提供できます。詳細については、60 ページの「オフライン認証ユーザに対するエマージェンシー アクセスの設定」を参照してください。

PIN が盗まれたり、他人に知られた場合

割り当てられたトークンの PIN が他人に知られた場合、そのことをただちに管理者に報告するように、ユーザを教育してください。管理者はそのトークンをただちに New PIN モードに設定しなければなりません。

PINを知られたことを承認されたユーザが報告する前に、承認されていない人物がPINを取得し、使用する可能性があります。RSA Authentication Manager の攻撃回避機能は、このような場合にセキュリティを維持するのに役立ちます。

誰かが承認されたユーザの PIN を使用してシステムに侵入しようとした場合、Authentication Manager は攻撃を検出し、アクセスを拒否できます。ただし、侵入者が PIN とそれに割り当てられている RSA SecurID トークンの両方を取得した場合は、この機能でシステムを保護することはできません。

システムのセキュリティを維持するには、次の対策をとることが**重要**です。

- すべてのユーザが自分の PIN を他人に知られないようにし、トークンを安全な場所に保管しなければなりません。
- PIN が他人に知られたり、トークンを紛失したことが報告された場合は、ただちに (トークンを New PIN モードにして) その PIN を無効にするか、または紛失したトークンを無効にしなければなりません。

操作手順：[Token] > [Edit Token] の順にクリックしてトークンを選択し、[Edit Token] ダイアログ ボックスを表示します。詳細については、[Help] をクリックして表示される情報を参照してください。

- PIN を無効にし、トークンを New PIN モードにするには、[New PIN mode] チェックボックスをオンにし、[Clear PIN] をクリックします。

  メモ：オフライン認証ユーザの PIN を New PIN モードに設定すると、トークン レコードからエマージェンシー アクセス データがクリアされます。オフライン ユーザがエマージェンシー アクセス上の理由で問い合わせてきた場合は、エマージェンシー アクセス用の PASSCODE を提供する必要があります。

- トークンを無効にするには、[Enabled] チェックボックスをオフにします。

盗まれた PIN による攻撃の回避

承認されていない人物が PIN を盗み、何回かの認証の試行の結果、たまたまトークンコードを推測できた場合でも、アクセスは許可されません。認証が連続して失敗すると、その後で正しいコードが入力されても、Authentication Manager は次に表示されるコードを要求します。ユーザがトークンに表示される次のコードを入力しないと、アクセスは拒否されます。

トークンがネクスト トークンコード モードになるまでに認証に失敗できる回数は設定できます。回数を設定するには、Configuration Management アプリケーション (Windows) または ***ACEPROG*/sdsetup** (UNIX) を使用します。詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』または『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

攻撃回避機能の要約

次の表は、攻撃回避機能の要約を示しています。

RSA SecurID PINPAD

検出されたイベント	RSA Authentication Manager の処置
推測された PASSCODE を使用したログイン試行が検出されました。	認証要求が一定回数失敗した後、トークンをネクスト トークンコード モードに設定します。
トークン保有者が誤った PASSCODE を使用して連続して認証に失敗し、失敗回数が許容される回数を超えました。	トークンをただちに無効にします。

RSA SecurID スタンダード カードとキーホルダ

検出されたイベント	RSA Authentication Manager の処置
不正な PIN と正しい SecurID トークンコードで構成される不正な PASSCODE が 3 回検出されました。	承認されていない人物がトークンを取得し、PIN を推測していると考えられるため、トークンをただちに無効にします。
推測された PASSCODE を使用したログオン試行が検出されました。	認証要求が一定回数失敗した後、トークンをネクスト トークンコード モードに設定します。
トークン保有者が誤った PASSCODE を使用して連続して認証に失敗し、失敗回数が許容される回数を超えました。	トークンをただちに無効にします。

RSA SecurID ソフトウェア トークン

検出されたイベント	RSA Authentication Manager の処置
不正な PASSCODE が 1 回入力されました。	トークンをネクスト トークンコード モードにします。
トークン保有者が誤った PASSCODE を使用して連続して認証に失敗し、失敗回数が許容される回数を超えました。	トークンをただちに無効にします。

メモ：トークンのクロックとシステム クロックの同期がとれていないために、Authentication Manager がトークンをネクスト トークンコード モードに設定することもあります。詳細については、128 ページの「同期」を参照してください。

New PIN モードの設定

RSA SecurID 認証では、定期的に PIN を変更する必要はありません。しかし、次のいずれかの場合は、トークンに関連付けられている PIN を変更する必要があります。

- 承認されたユーザが PIN を忘れた場合
- 他人が PIN を不正に取得した場合
- 「PASSCODE REUSE ATTACK DETECTED (PASSCODEの再利用による攻撃を検出しました)」または「Simultaneous Login Detected (同時ログインを検出しました)」というログ メッセージを確認した場合

重要：承認されていない人物がユーザの PIN を取得した可能性がある場合や、上記のログ メッセージのいずれかを確認した場合は (ネットワークへの侵入が試みられたことを示します)、**ただちに**トークンを New PIN モードに設定してください。その後、トークン ステータスが変更されたことを承認されたユーザに通知します。

New PIN 手順でのユーザ支援

システムを設定した後に、ユーザは New PIN 手順を完了する必要があります。この手順は、ユーザのトークンが New PIN モードに設定された場合にも必ず実行する必要があります。

メモ：すでに PIN が含まれているトークン レコードをインポートまたは変換した場合や、ユーザのトークンをトークンコードのみで認証するように設定した場合は、New PIN 手順は必要ありません。

新規ユーザの場合

新規ユーザが初めて RSA SecurID PASSCODE プロンプトに対して入力する場合は、割り当てられたトークンに現在表示されているトークンコードのみを入力します。

New PIN モードに設定され、PIN がクリアされている場合

PIN がクリアされたユーザは、認証プロセスで新規ユーザとして処理されます。PASSCODE を求めるプロンプトが表示されたら、新規ユーザはトークンに表示されたトークンコードのみを入力します。PIN がクリアされたユーザが元の PIN とトークンコードを入力すると、Authentication Manager は「Access denied (アクセスは拒否されました)」というメッセージを応答します。

New PIN モードで以前の PIN がクリアされていないトークンの場合

ユーザのトークンが New PIN モードに設定されているのに、以前の PIN をクリアしていない場合には、ユーザは元の PIN と、トークンに現在表示されているトークンコードを入力しなければなりません。

すべてのユーザ

ユーザが自分で PIN を作成する場合は、特に次のことに注意してください。

- PIN を他人に知られた場合、ユーザは新しい PIN を作成しなければなりません。
- 数字のみの PIN を使用するより、英字と数字の両方を含む PIN を使用する方が安全です。システムでは英数字 PIN を使用できるため、スタンダード カードやキーホルダのユーザはできるだけ英数字 PIN を使用するようにしてください。

トークンの同期のとり直し

米 RSA Security が特許を保有しているタイム シンクロナイゼーション方式では、ユーザの RSA SecurID トークンに表示される擬似乱数トークンコードは、ある一定の間隔で RSA Authentication Manager ソフトウェアが生成するコードと同じであることが保証されます。

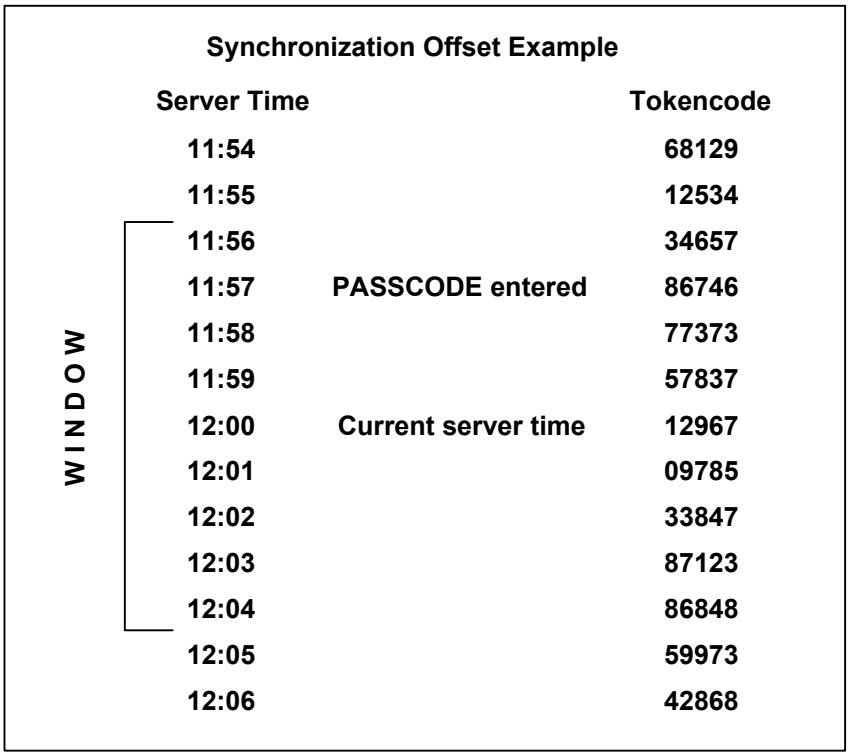
ユーザが正しい PASSCODE を入力しているのに、連続してアクセスが拒否される場合は、トークンのクロックとシステム クロックの同期がとれていない可能性があります。システム時刻が正しいにもかかわらず、ユーザのアクセスが拒否された場合は、**Resynchronize Token** 操作 (トークンの同期のとり直し) を実行します。詳細については、ヘルプを参照してください。この操作を実行すると、Authentication Manager は生成するトークンコードの数を一時的に拡大し、一致する値を見つけようとします。一致する値が見つかると、トークンとシステム クロックの同期がとり直されます。

次のセクション「同期」では、同期機能がどのように動作するかについて説明し、システムがより範囲の広い正しいトークンコードを計算する場合の例を示します。

同期

ユーザが認証を受けようとすると、Authentication Manager は一定の時間の範囲でユーザのトークンの PASSCODE を計算します。ユーザが初めて認証を受ける場合は、この時間の範囲 (**時間枠**) は Authentication Manager のシステム時刻を中心として設定されます。入力された PASSCODE と、計算した値が一致する場合は、Authentication Manager システムの時刻と、この PASSCODE に対応する時刻の差 (**同期オフセット**と呼びます) は、Authentication Manager データベースのトークン レコードに格納されます。Authentication Manager システム時刻は、前回のログオン時刻としてもトークン レコードに格納されます。

次の例では、同期オフセットの計算方法を示しています。このトークンはサーバ時刻より 3 分遅れているため、トークンの同期オフセットは -180 です。-180 が現在の Authentication Manager の時刻に加算されると、コードは一致するはずです。



この後の認証試行では、トークンの同期オフセットが RSA Authentication Manager のシステム時刻に加算され、計算する PASSCODE の範囲の中心として、加算した合計が使用されます。たとえば、ユーザが同じトークンを使用して 12 時 20 分に別の認証要求を実行した場合、範囲の中心は次のように決定されます。

12:20 + (-180) = 12:17

時間枠のサイズは通常、3 つのコードが表示される間隔と同じです (コードが表示される間隔は通常 60 秒ですが、それより長い間隔または短い間隔に設定されたトークンも提供されています)。場合によっては、システムが時間枠を拡大することもあります。

メモ:RSA SecurID ソフトウェア トークンの時間枠は、スタンダード カード、PINPAD、キーホルダの時間枠よりも拡大されています。詳細については、ソフトウェア トークンのマニュアルを参照してください。

時間枠は、次のいずれかの場合に拡大されます。

- 前回ログオンしてから長い時間が経過した場合

  時間枠のサイズは、RSA Authentication Manager システム時刻と前回のログオン時刻の差に比例します (つまり、前回ログオンしてから長い時間が経過しているほど、時間枠は広くなります)。このため、トークンのクロックと Authentication Manager のクロックの同期がとれていない場合でも、アクセスが可能です。
- 連続してログオンに失敗した結果、トークンがネクスト トークンコード モードに設定された場合

この場合は、Authentication Manager は不正と判断したコードが時間の遅れや進みによって発生しただけであり、実際には正しいコードであるかどうかを確認します。

- トークンが New PIN モードの場合

  このモードのトークンの場合、トークンとシステム クロックとの同期がとられていなかったり、トークンがしばらく使用されていなかったために、システム クロックとの同期がとれていない場合に備えて、Authentication Manager によって時間枠が広げられます。

- コミュニケーション サーバであるエージェント ホストを通じて、ユーザがログオンしている場合

  この種のエージェント ホストで認証手順を実行するには、通常より長い時間がかかる可能性があります。したがって、Authentication Manager は時間枠を広げて、コードを照合します。

トークンのコードが拡大した時間枠にも収まらないほど、RSA Authentication Manager システム クロックとの同期がずれている場合、そのトークンは使用できません。トークンの交換については、RSA セキュリティ正規販売代理店にお問い合わせください。

一致する PASSCODE が見つかると、同期オフセットと前回のログイン時刻の両方がトークン レコードで更新されます。この後の認証サービス プロセスでは、標準の時間枠 (つまり、プラス マイナス 1 つのコード表示間隔) だけが使用されるようになります。

時間枠が拡大されるのは、承認されたユーザが正しい PASSCODE を入力したのに、アクセスが拒否されることがないようにするためです。しかし、時間枠を拡大して照合できるようにした結果、セキュリティが低下しては困ります。そのため、ユーザに対して第 2 のトークンコードを要求するプロンプトが表示されます。

ネクスト トークン コード プロンプトが表示されるのは、連続して不正なログインが実行されたために、トークンがネクスト トークンコード モードに設定されたか、または拡大した時間枠でコードの照合が行われた場合です。使用しているエージェント ホスト デバイスにネクスト トークンコード プロンプトが表示されない場合、ユーザはこのモードを終了するための支援を必要とします。

操作手順：[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

サイトの作成と変更

ユーザの数や保護されているエージェント ホストの数が増えた場合、サイトを使ってエージェント ホストやグループを編成することを検討してください。すべての承認されたユーザに対して必ずしもオープンではないエージェント ホストでグループをアクティブ化する場合、サイトを使ってエージェント ホストやグループが編成されていると便利です。

1 つまたは複数のサイトを作成し、エージェント ホストとグループをサイトに関連付けることができます。サイトに関連付けたからといって、グループをアクティブ化できるエージェント ホストが制限されるわけではありません。どのグループもすべてのエージェント ホストでアクティブ化できます。

エージェント ホスト名の場合とは違って、グループ名は、サイトが異なれば同じ名前でもかまいません。サイト名はグループ識別子の一部になるため、**Saitama** サイトで **Operations** というグループを作成し、**Kyoto** サイトで **Operations** という別のグループを作成してもかまいません。

サイトを使用する場合は、サイト名によって選択したレポートを作成でき、次のアクティビティがログに記録されているかどうかを確認できます。

- サイト名の変更
- サイトの削除
- グループまたはエージェント ホストとサイトの関連付け
- サイトからのグループまたはエージェント ホストの削除
- サイトに関連付けられたグループまたはエージェント ホストの削除

操作手順：サイトを作成するには、[Site] メニューの [Add Site] をクリックして [Add Sites] ダイアログ ボックスを表示します。詳細については、[Help] をクリックして表示される情報を参照してください。

メモ：サイトごとのレポートには、サイトに関連付けられたエージェント ホストへのログオンも含めて、ログオン アクティビティは一切**記録されません**。選択条件によってレポートを作成する方法については、第 9 章「レポート」を参照してください。

サイト拡張データの編集

サイト拡張レコードの情報を変更するには、[Add Site] または [Edit Site] ダイアログ ボックスで [Edit Site Extension Data] ボタンを使用します。これらのレコードには、カスタム アドミニストレーション プログラムからアクセスできるユーザ定義情報が格納されています。

RSA Authentication Manager Administration Toolkit を使用してカスタム アドミニストレーション プログラムを作成する方法については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

7 データベースのメンテナンス (UNIX)

この章では、RSA Authentication Manager データのバックアップ、復元、オフライン ストレージの作成方法について説明します。また、古いログ レコードの削除やアーカイブによる監査証跡データベースの管理方法と、拡張データ レコードの情報を更新する方法についても説明します。最後に、RSA Authentication Manager Host Mode から外部プロシージャを直接実行する手順について説明します。

この章では、UNIX RSA Authentication Manager マシン上でコマンド ライン プロンプトに UNIX コマンドを入力して実行する操作について説明します。また、RSA Authentication Manager Host Mode を必要とするその他の操作についても説明します。このアプリケーションは、リモート アドミニストレーション マシンで実行します。

実際に操作を開始する前に、次のセクション「適切なディスク容量の確保」を参照して、RSA Authentication Manager で適切なディスク容量を確保してください。

適切なディスク容量の確保

ファイル システムに空きがなくなり、RSA Authentication Manager データベースに書き込むことができなくなると、Authentication Manager プログラムは中断されます。必要最低限の空きディスク領域を確保できるように、必要な処置をとってください。

重要：プライマリまたはレプリカ Authentication Manager のディスクの空き領域は、ディスク容量の 10% 未満にならないようにしてください。

必要なディスク容量は各システムで異なるため、次の表に示すデータベース サイズの例は、単なるガイドラインとして参考にしてください。

ユーザ数	エージェント ホスト数	1 日の監査証跡エントリ数	Authentication Manager データベースのサイズ	ログ データベースが毎日拡大するサイズ	syslog が拡大するサイズ
100	50	1000	1.8 MB	1 MB	0.1 MB
1000	500	10000	2.2 MB	5 MB	0.5 MB
10000	5000	25000	19.2 MB	11 MB	1.1 MB

データベース圧縮ユーティリティによるディスク領域の再利用

ディスク領域を効率よく利用するために、Authentication Manager データベースとログ データベースは定期的に圧縮しなければなりません。RSA セキュリティが提供するデータベース圧縮ユーティリティを使用すると、RSA Authentication Manager データベースで使用されていたディスク領域を再利用できます。たとえば、古いログ レコードの消去など、大量の削除操作を実行した後、圧縮ユーティリティを使用して、ログ データベースで使用されていないディスク領域を解放できます。

また、データベース圧縮ユーティリティを使用すると、**sdserv.bi** ファイルと **sdlog.bi** ファイルも圧縮できます。これらのファイルは、一連のトランザクションが正常に終了しなかった場合に、トランザクションをロールバックするために作成されます。これらのファイルが自動的に消去されることはないので、非常に大きいサイズになることがあります。特に、データベースに対して大量の変更を行う操作 (トークンのインポートなど) の後では、このファイルのサイズが非常に大きくなります。

圧縮操作を実行している間、RSA Authentication Manager プログラムやデータベース ブローカを実行することはできません。このため、毎日のバックアップを実行するために、**aceserver** プロセスとブローカを停止したときに、このユーティリティを使用すると便利です。

複数のレプリカを使用している場合は、データのバックアップやファイルの圧縮のためにプライマリをシャットダウンしている間も、認証サービスを続行できます。

プライマリまたはレプリカでデータベース ファイルを圧縮するには

1. **root** または RSA Authentication Manager ファイルのオーナとしてログインしていない場合は、そのいずれかのアカウントに対して **su** を実行します。

   ファイル オーナが不明の場合は、***ACEPROG*/sdinfo** を実行して、設定値を確認してください。

2. **aceserver** プロセスも含めて、すべての RSA Authentication Manager プログラムを終了します。

3. 次のコマンドを使用して、データベース ブローカを停止します。

   ```
   sdconnect stop
   ```

4. どのデータベースを圧縮するかを指定して、**sdcompress** を実行します。

   ```
   ACEPROG/sdcompress -l | -s
   ```

   このコマンドで、**-s** (“server”) を使用すると **sdserv** が圧縮され、**-l** (“log”) を使用すると **sdlog** が圧縮されます。

   sdcompress スクリプトは、自動的にデータベースのバックアップを作成し、圧縮操作が正常に終了するまで、そのバックバックを保存します。空きディスク領域が非常に少なく、この一時的なバックアップを格納するための十分な容量がない場合は、**-n** オプションを指定して **sdcompress** を実行できます。**このコマンドではバックアップが作成されないため、どうしても必要な場合にだけ使用してください**。このオプションを使用する必要がある場合は、あらかじめ、データベースのバックアップ テープを作成しておいてください。

   ```
   ACEPROG/sdcompress -db -n
   ```

RSA Authentication Manager データのバックアップと復元

信頼性の高い完全なバックアップ ファイルを作成するには、このセクションの手順に従ってください。

- ***ACEDATA***
  - ログ データベースと Authentication Manager データベースのバックアップは、毎日作成してください (管理者が選択したスケジュールと方法に従って、ログ データベースをアーカイブ ファイルに保存するように、RSA Authentication Manager を設定できます。詳細については、153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください)。

- **sdconf.rec** ファイルを変更する場合は、必ずバックアップを作成してください。
- 製品を初めてインストールした後や、何らかの理由でライセンス レコードをアップグレードした後は、**license.rec** ファイルのバックアップを作成してください。
- リモート アドミニストレーションおよびLDAP同期に使用されるSSLファイルのバックアップを作成してください (**sdti.cer**、**server.cer**、**server.key**、**key3.db**、および **cert7.db**)。
- カスタム クエリのバックアップを作成してください (**queries¥***)。
- TACACS+ を使用する場合は、**sdtacplus.cfg** のバックアップを作成してください。

- ***ACEPROG***
  - 構成ファイル **hosts.conf** のバックアップを作成してください。
  - 構成ファイル **sdcommdConfig.txt** のバックアップを作成してください。

メモ : データベースのバックアップは、RSA Authentication Manager プログラムが**実行されていない**ときに行ってください。プログラムの実行中にバックアップを**作成する必要がある**場合は、136 ページのセクション「RSA Authentication Manager プログラムが実行されているときのデータのバックアップ」を参照してください。

RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ

複数のレプリカがある場合は、認証を中断せずに、Authentication Manager ですべての RSA Authentication Manager プログラムを停止してデータをバックアップできます。

プログラムを使用していないときにデータベースのバックアップを作成するには

1. RSA Authentication Manager プログラムが実行されていないことを確認します。
2. コマンド プロンプトで次のように入力します。

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

   sdconnect stop を実行しないと、バックアップにはロック ファイル (**sdserv.lk** および **sdlog.lk**) が含まれます。ロック ファイルを含むデータベースのバックアップを作成し、そのバックアップを復元すると、**sdconnect start** はエラーになります。
3. バックアップを作成するデータ ファイルの場所を確認します。

   データベース ファイルは、***ACEDATA*** ディレクトリ (**/top/ace/data** など) に格納されています。

   次のファイルはログ データベース (**sdlog**) ファイルです。

   sdlog.b1
   sdlog.d1
   sdlog.db
   sdlog.lg
   sdlog.st
   sdlog.vrs

次のファイルは Authentication Manager データベース (**sdserv**) ファイルです。

sdserv.b1
sdserv.d1
sdserv.db
sdserv.lg
sdserv.st
sdserv.vrs

4. UNIX コマンドの **tar -p** または **cp -p** を使用して、ログ データベース ファイルと Authentication Manager データベース ファイルをコピーします。

   ファイルをテープにコピーするには **tar** コマンドを使用し、ファイルを別のディレクトリにコピーするには **cp** コマンドを使用します。**-p** オプションを使用して、ファイル アクセス権を保存します。

RSA Authentication Manager プログラムが実行されているときのデータのバックアップ

このセクションで説明するデータベース バックアップ コマンドを使用すると、プライマリとレプリカの両方でデータベースのバックアップを作成できます。ただし、できるだけ前のセクション「RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ」で説明したバックアップ手順に従ってください。

メモ：シングル ユーザ モードの場合は、このバックアップ方法を絶対に使用しないでください。この方法では、RSA Authentication Manager プログラムの実行中にバックアップを作成することができ、そのためにデータベースの整合性が損なわれることはありません。ただし、作成したバックアップが完全であるとは限りません。バックアップを開始する前に、他の人が同時にデータベースのバックアップ操作を実行していないことを確認してください。同時に複数のバックアップを作成すると、システムのパフォーマンスが大幅に低下します。

構文

sdbkup コマンドの構文は次のとおりです。

```
sdbkup [online] databasefile backupfile
```

次の表は、**sdbkup** コマンドのオプションを示しています。

オプション	説明
online	RSA Authentication Manager プログラムの実行中にバックアップを実行することを指定します。
databasefile	バックアップするデータベース ファイルのフルパス名 (通常は ***ACEDATA*** ディレクトリのファイル) を指定します。
backupfile	バックアップ ファイルのフルパス名 (またはファイル名のみ) を指定します。

たとえば、Authentication Manager データベースのバックアップを **sdserv1** という名前のファイルに作成する場合、コマンド ラインに次のように入力します。

```
sdbkup online /ace/data/sdserv /dev/rst0/sdserv1
```

sdserv1 という名前のファイルがすでに存在する場合、メッセージは表示されずにバックアップ ファイルは上書きされます。

データベース バックアップ コマンドで作成されたデータベースの復元

データベース バックアップ コマンドで作成されたデータベースを復元するには、このセクションで説明する手順を実行します。

データベースを復元するには

1. RSA Authentication Manager プログラムが実行されていないことを確認します。
2. 次のコマンドを実行して、レポート作成ユーティリティ (実行している場合)、**aceserver** プロセス、およびデータベース ブローカを停止します。

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. Authentication Manager データベースを復元するには、次のコマンドを実行します。

   ```
   sdrest /top/ace/data/sdserv /dev/rst0
   ```

4. ログ データベースを復元するには、次のコマンドを実行します。

   ```
   sdrest /top/ace/data/sdlog /dev/rst0
   ```

5. すべてのレプリカのレプリカ パッケージを生成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリを再起動したときに、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーします。

6. プライマリを再起動します。

オフライン バックアップまたはサーバからのデータの復元

sdbkup コマンド (詳細については 136 ページの「RSA Authentication Manager プログラムが実行されているときのデータのバックアップ」を参照) を使用してバックアップを作成していないデータを復元する場合は、最新のデータベースが格納されている場所に応じて最適な手順が異なります。

- 135 ページの「RSA Authentication Manager プログラムが実行されていないときのデータのバックアップ」の手順で作成したデータベースが最新である場合は、このセクションの最初の手順に従ってデータを復元します。
- レプリカのいずれかのデータベースが最新である場合は、このセクションの 2 番目の手順に従ってデータを復元します。
- プライマリのデータベースが最新である場合は、このセクションの 3 番目の手順に従ってデータを復元します。

オフライン バックアップからデータを復元するには

1. **root** または RSA Authentication Manager ファイルのオーナとしてログインしていない場合は、そのいずれかのアカウントに対して **su** を実行します。
2. プライマリで実行されているすべての RSA Authentication Manager プログラムを停止します。

コマンド プロンプトで次のコマンドを入力して、レポート作成ユーティリティ (実行している場合)、**aceserver** プロセス、およびデータベース ブローカを停止します。

```
rptconnect stop
aceserver stop
sdconnect stop
```

3. バックアップ ファイルの形式に適したコマンドを使用して、バックアップの **sdlog** データベースおよび **sdserv** データベースを ***ACEDATA*** ディレクトリにコピーします。

   次のファイルはログ データベース (**sdlog**) ファイルです。

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

   次のファイルは Authentication Manager データベース (**sdserv**) ファイルです。

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

4. すべてのレプリカのレプリカ パッケージを生成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーします。

5. プライマリで **aceserver** を起動します。

レプリカのデータをプライマリで復元するには

1. **root** または RSA Authentication Manager ファイルのオーナとしてログオンしていない場合は、そのいずれかのアカウントに対して **su** を実行します。

2. プライマリで実行されているすべての RSA Authentication Manager プログラムを停止します。

   コマンド プロンプトで次のコマンドを入力して、レポート作成ユーティリティ (実行している場合)、**aceserver** プロセス、およびデータベース ブローカを停止します。

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. レプリカでステップ 1 とステップ 2 を繰り返します。

4. バックアップ　ファイルの形式に適したコマンドを使用して、レプリカのデータベースをプライマリにコピーします。

   レプリカからプライマリにコピーするファイルは、**sdserv.bi**、**sdserv.db**、**sdserv.lg**、**sdserv.lic**、および **sdserv.vrs** です。

5. すべてのレプリカのレプリカ パッケージを生成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーします。

6. プライマリで **aceserver** を起動します。

7. レプリカで **aceserver** を起動します。

プライマリのデータをレプリカで復元するには

1. **root** または RSA Authentication Manager ファイルのオーナとしてログオンしていない場合は、そのいずれかのアカウントに対して **su** を実行します。

2. レプリカで RSA Authentication Manager プログラムが実行されていないことを確認します。

   コマンド プロンプトで次のコマンドを入力して、レポート作成ユーティリティ (実行している場合)、**aceserver** プロセス、およびデータベース ブローカを停止します。

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. プライマリでステップ 1 とステップ 2 を繰り返します。

4. すべてのレプリカのレプリカ パッケージを生成し、レプリカ パッケージ内の新しいデータベース ファイルをすべてのレプリカに配布します。

   Push DB Assisted Recovery 機能が有効になっている場合は、プライマリによって新しいデータベース ファイルがレプリカにプッシュされます。有効になっていない場合は、レプリカにデータベース ファイルを手動でコピーします。

5. プライマリで **aceserver** を起動します。

6. レプリカで **aceserver** を起動します。

データベース レコードのインポートとエクスポート

一部の RSA Authentication Manager データは、エクスポートして ASCII テキスト ファイル形式で保存できます。これらのファイルはバックアップ用ではなく、オフラインで表示または処理するためのものです。データベースに復元して、Authentication Manager で使用することはできません。

リモート アドミニストレーション マシンで RSA Authentication Manager Host Mode を使用して、次のデータが格納されたテキスト ファイルを作成できます。

- ユーザ名やログインなどの特定のユーザ データ。詳細については、[User] > [List Users] > [Help] の順にクリックして、表示される情報を参照してください。
- RSA Authentication Manager レポート形式のログ レコード。

  詳細については、162 ページの「ファイルへのレポートの出力」を参照してください。
- Microsoft Excel などのサード パーティ ソフトウェアで使用できるカンマ区切り (CSV) 形式のログ レコード。

詳細については、153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください。

これらのファイルは安全な場所に保管してください。ファイルに格納されているデータが不正なユーザのアクセスを受けると、システム セキュリティが重大な危険にさらされる可能性があります。

データベース ダンプ ユーティリティとロード ユーティリティの使用

ダンプ ユーティリティとロード ユーティリティを使用すると、テキスト ファイルとは異なり、データベースに**インポートできる**形式でデータベース レコードをエクスポートできます。詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

復元手順

Authentication Manager でハードウェア障害が発生したり、データベースで問題が発生した場合は、次の手順に従って問題のハードウェアやデータベースを復元または交換できます。

この手順の一部は、システムで Push DB Assisted Recovery 機能を使用するかどうかに応じて異なります。この機能は有効にしておくことをお勧めします。詳細については、22 ページの「データベース プッシュ (Push DB Assisted Recovery) 機能」を参照してください。

システムでPush DB Assisted Recovery機能を使用するには、RSA Authentication Manager Host Mode を起動し、[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。次に、[Allow Push DB Assisted Recovery] チェックボックスをオンにします。

最新のデータベースの特定

RSA Authentication Manager アドバンスド ライセンスを保有し、複数のレプリカを使用している場合、最新のデータベースを使用するには、使用するデータベースを次の手順で決定します。プライマリのハードウェアが機能している場合は、プライマリの syslog を確認します。プライマリのハードウェアが機能していない場合は、各レプリカの syslog を確認します。

最新のデータベースを特定するには

Authentication Manager で syslog を確認し、正常な最新の複製を見つけます。

- プライマリで次のメッセージを探します。

  `Primary Successfully Received Replica Records`（プライマリでレプリカ レコードを正しく受信しました）

  このメッセージには、日付、時刻、およびレプリカの IP アドレスが含まれます。最新のデータベースは、最新のメッセージに IP アドレスで示されているレプリカにあります。

- レプリカで次のメッセージを探します。

  `Replica Successfully Reconciled Databases`（レプリカでデータベースの調整に成功しました）

  このメッセージには、日付、時刻、およびプライマリの IP アドレスが含まれます。各レプリカの syslog を確認します。最新のデータベースは、最新のメッセージが保存されたレプリカにあります。

レプリカのデータベースの交換

レプリカのデータベースを交換する必要がある場合は、プライマリに新しいレプリカパッケージを作成し、レプリカで新しいデータベースが必要であることを指定しなければなりません。

レプリカのデータベースを交換するには

1. プライマリに **root** または RSA Authentication Manager ファイルのオーナとしてログオンします。
2. レプリカとプライマリで実行されているすべてのRSA Authentication Managerプログラムとデータベース ブローカを停止します。***ACEPROG***ディレクトリに移動し、コマンド プロンプトで次のコマンドを入力します。

   ```
   aceserver stop
   sdconnect stop
   ```

3. プライマリでレプリカ パッケージを作成します。次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -package
   ```

4. [Name of replica] プロンプトで、同じレプリカの完全な名前を入力し、RETURN キーを押します。
5. [Confirm] プロンプトで「y」と入力し、もう一度 RETURN キーを押します。
6. 交換する各データベースについて、ステップ 4 とステップ 5 を繰り返します。すべてのレプリカの名前を入力したら、[Name of replica] プロンプトで RETURN キーを押します。[Have you entered all the Replicas you would like included in this package (y/n/q) [y]:] (このパッケージに含めるすべてのレプリカの名前を入力しましたか (y/n/q) [y]:) というプロンプトが表示されたら、もう一度 RETURN キーを押します。

   RSA Authentication Manager のシステム パラメータが Push DB Assisted Recovery 機能を有効にするように設定されている場合は、次のステップでプライマリとレプリカを再起動したときに、プライマリによってデータベース ファイルがレプリカにプッシュされます。

   システム パラメータが Push DB Assisted Recovery 機能を有効にするように**設定されていない**場合は、プライマリの ***ACEDATA*/replica_package/database** ディレクトリのファイルを、レプリカの ***ACEDATA*** ディレクトリにコピーします。
7. プライマリとレプリカで、RSA Authentication Manager とデータベース ブローカを起動します。各システムで、コマンド プロンプトで次のコマンドを入力します。

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

   Push DB Assisted Recovery 機能が有効になっている場合、プライマリは新しいデータベースをレプリカにプッシュすることにより、復元支援 (Push DB) プロセスを開始します。

   Push DB Assisted Recovery 機能が有効になっていない場合、復元プロセスはこれで完了です。

レプリカのハードウェアの交換

レプリカにハードウェア障害が発生して機能しなくなった場合は、データベースに登録されているレプリカを別のマシンと交換します。レプリカのハードウェアを交換するには、レプリカ管理ユーティリティを使用します。ユーティリティの指示に従って操作すると、まず、交換するレプリカの名前と IP アドレスを指定するように求められます。次に、新しいレプリカの名前と IP アドレスを指定するように求められます。

レプリカのハードウェアを交換するには

1. 新しいレプリカとして使用するネットワーク マシンを選択します。
2. プライマリに **root** または RSA Authentication Manager ファイルのオーナとしてログオンします。
3. プライマリで実行されているすべての RSA Authentication Manager プログラムとデータベース ブローカを停止します。***ACEPROG*** ディレクトリに移動し、コマンド プロンプトで次のコマンドを入力します。

   ```
   aceserver stop
   sdconnect stop
   ```

4. プライマリでレプリカ管理ユーティリティを実行し、障害が発生したレプリカを交換します。次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -repmgmt replace
   ```

5. プロンプトで、交換するレプリカの完全な名前を入力し、RETURN キーを押します。
6. プロンプトで、新しいシステム名と IP アドレスを入力し、RETURN キーを押します。

   プライマリの***ACEDATA/*replica_package**ディレクトリにレプリカ パッケージが生成されます。
7. コマンド プロンプトで次のコマンドを入力して、プライマリで RSA Authentication Manager とデータベース ブローカを起動します。

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

8. レプリカ パッケージのディレクトリを新しいレプリカにコピーします。システム パラメータが Push DB Assisted Recovery 機能を有効にするように設定されている場合は、ライセンス ディレクトリのみをコピーします。システム パラメータが Push DB Assisted Recovery 機能を有効にするように**設定されていない**場合は、ライセンス ディレクトリとデータベース ディレクトリの両方をコピーする必要があります。
9. 新しいレプリカ パッケージを使用して、新しいレプリカでレプリカ ソフトウェアの新規インストールを実行します。レプリカのインストールの詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

   Push DB Assisted Recovery 機能が有効になっている場合、プライマリは新しいデータベースをレプリカにプッシュすることにより、復元支援 (Push DB) プロセスを開始します。

   Push DB Assisted Recovery 機能が有効になっていない場合は、レプリカで RSA Authentication Manager サービスとデータベース ブローカを再起動します。

交換するレプリカごとに、この手順を繰り返してください。

プライマリのデータベースの交換

プライマリのデータベースが壊れた場合は、レプリカ上の最新のデータベースのコピーと交換し、新しくレプリカ パッケージを作成して他のすべてのレプリカに配布する必要があります。

プライマリのデータベースを交換するには

1. プライマリに **root** または RSA Authentication Manager ファイルのオーナとしてログオンします。
2. いずれかのレプリカからデータベースのダンプを取得します。レプリカで ***ACEPROG*** ディレクトリに移動し、次のように入力します。

   ```
   sddump -s
   ```

   ダンプ ユーティリティは ***ACEDATA*** ディレクトリに **sdserv.dmp** ファイルを作成します。既存のダンプ ファイルは上書きされます。
3. **sdserv.dmp** ファイルをプライマリにコピーします。
4. プライマリで実行されているすべての RSA Authentication Manager プログラムとデータベース ブローカを停止します。***ACEPROG*** ディレクトリに移動し、次のように入力します。

   ```
   aceserver stop
   sdconnect stop
   ```
5. プライマリに新しい空のデータベースを作成します。次のコマンドを入力します。

   ```
   sdnewdb server
   ```
6. 新しいデータベースにダンプ ファイルをロードします。次のコマンドを入力します。

   ```
   sdload -s -f pathname/sdserv.dmp
   ```

   pathname には、ダンプ ファイルの場所を入力します。
7. プライマリでレプリカ パッケージを作成します。次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -package
   ```
8. [Name of replica] プロンプトで、レプリカの完全な名前を入力し、RETURN キーを押します。
9. [Confirm] プロンプトで「y」と入力し、もう一度 RETURN キーを押します。
10. 各レプリカについて、ステップ 7 とステップ 8 を繰り返します。すべてのレプリカの名前を入力したら、[Name of replica] プロンプトで RETURN キーを押します。[Have you entered all the Replicas you would like included in this package (y/n/q) [y]:] (このパッケージに含めるすべてのレプリカの名前を入力しましたか (y/n/q) [y]:) というプロンプトが表示されたら、もう一度 RETURN キーを押します。
11. プライマリで RSA Authentication Manager とデータベース ブローカを起動します。次のコマンドを入力します。

    ```
    ACEPROG/sdconnect start
    ACEPROG/aceserver start
    ```

    Push DB Assisted Recovery 機能が有効になっている場合、プライマリは新しいデータベースをレプリカにプッシュすることにより、復元支援 (Push DB) プロセスを開始します。

Push DB Assisted Recovery 機能が有効になっていない場合は、***ACEDATA*/replica_package/database** ディレクトリのファイルを各レプリカにコピーします。レプリカで、すべての RSA Authentication Manager プログラムとデータベース ブローカを停止し、データベース ファイルを ***ACEDATA*** ディレクトリに移動します。次に、RSA Authentication Manager とデータベース ブローカを再起動します。

レプリカの指名によるプライマリのハードウェアの交換

プライマリでハードウェア障害が発生した場合は、既存のレプリカをプライマリとして指名できます。まず、指名するレプリカを選択します。選択したレプリカで、レプリカ管理ユーティリティの [Nominate] ボタンをクリックすると、レプリカがプライマリに自動的に変換されます。更新されたレプリカ パッケージが新しいプライマリの ***ACEDATA*¥replica_package** ディレクトリに作成されます。

メモ：機能しているプライマリのハードウェアをより新しいハードウェアに交換する場合は、新しいハードウェアをレプリカとして追加してから、プライマリとして指名することもできます。その後、古いプライマリをオフラインにします。ただし、この場合は一定の手順に従って操作する必要があります。まず、プライマリを停止し、新しいマシンをレプリカとして追加して、新しいマシンのレプリカ パッケージを作成します。現在のプライマリを再起動し、レプリカを調整します。次に、以下に示すように、新しいレプリカを指名する手順を実行します。

レプリカ指名の準備

レプリカを指名する前に、障害が発生したプライマリのハードウェアの状態を確認する必要があります。障害が発生したプライマリが長期にわたって使用できない場合は、レプリカを指名する必要があります。必要な修復が短期間で終了する場合は、レプリカを**指名せず**、元のプライマリを修復して使用することもできます。いずれの場合も、プライマリが機能していない間は各レプリカが認証要求の処理を続行します。元のプライマリを修復する場合、すべての Quick Admin 管理者およびリモート管理者に状況を通知し、プライマリが復元されるまで、レルム内のマシンの Quick Admin または Remote Administration を実行できないことを説明してください。

メモ：最新のデータベースが格納されているレプリカを選択することをお勧めします。詳細については、140 ページの「最新のデータベースの特定」を参照してください。

レプリカを指名するには

1. レプリカで次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -repmgmt nominate
   ```

2. 「y」と入力し、RETURN キーを押して、レプリカを新しいプライマリとして指名します。

3. 新しいプライマリで、RSA Authentication Manager サービスとデータベース ブローカを起動します。

   RSA Authentication Manager のシステム パラメータが Push DB Assisted Recovery 機能を有効にするように設定されている場合は、更新されたレプリカ パッケージが各レプリカに自動的に配布されます。新しいプライマリを再起動すると、復元プロセスが完了します。

   Push DB Assisted Recovery 機能が**有効になっていない**場合は、各レプリカでステップ 4 ～ 6 を繰り返します。

4. レプリカですべての RSA Authentication Manager サービスとデータベース ブローカを停止します。
5. 新しいプライマリの ***ACEDATA*/replica_package/database** ディレクトリと ***ACEDATA*/replica_package/license** ディレクトリのファイルをレプリカの ***ACEDATA*** 以外のディレクトリにコピーします。
6. レプリカ パッケージを適用します。レプリカで次のコマンドを入力します。

   ACEPROG/sdsetup -apply_package *pathname*

   次のメッセージが表示されます。

   Replica Package was successfully applied. (レプリカ パッケージが正しく適用されました)

メモ: 古いプライマリを修復してネットワークに再接続すると、自動的にレプリカとして追加されます。プライマリとして復元するには、指名する必要があります。

レプリカを指名するか、新しいマシンにプライマリをインストールすることによって、障害が発生したプライマリのハードウェアを交換する場合、Quick Admin、RADIUS サーバ、エージェント ホスト、および Remote Administration も影響を受けることに注意してください。これらが新しいプライマリで正しく機能するように、対応する指示を参照して次の操作を実行してください。

メモ: これらの操作を実行する場合は、必要に応じて関連ヘルプを表示できるように、Remote Administration を使用してください。Remote Administration を有効にするには、最初にプライマリで操作 1 を実行する必要があります。次に、リモート アドミニストレーション マシンで、操作 2 から操作 7 までを任意の順番で実行してください。

1. すべてのリモート アドミニストレーション マシンに対して、プライマリの ***ACEDATA*** ディレクトリから **sdconf.rec** ファイルと **server.cer** ファイルをコピーし、リモート アドミニストレーション マシンからプライマリを削除します。次に、新しい **sdconf.rec** ファイルを使用してプライマリを追加します。詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』を参照してください。
2. Quick Admin がインストールされている場合は、新しいプライマリの名前と IP アドレスで Quick Admin の設定を再構成する必要があります。操作手順については、49 ページの「Quick Admin の再構成」を参照してください。
3. Authentication Manager がレルム間認証のローカル レルム Authentication Manager またはリモート レルム Authentication Manager として指定されている場合は、ローカル レルムおよびリモート レルムのデータベースのレルム レコードを編集して新しい名前または IP アドレスを反映します。詳細については、ヘルプの「Edit Realm」を参照してください。
4. 障害が発生したプライマリが RADIUS サーバに指定されていた場合は、RADIUS サーバを新しいプライマリ、他のレプリカ、別のホスト マシンのいずれかにインストールできます。新しいプライマリの管理機能に悪影響を与えないように、他のレプリカ上で RADIUS を有効にすることをお勧めします。必ず次の操作を実行してください。
   - RADIUS サーバとして使用する Authentication Manager をデータベースにエージェント ホストとして追加します。詳細については、『RSA Authentication Manager 6.1 for Windows インストール ガイド』の「サーバをエージェント ホストとしてプライマリ データベースへ追加」を参照してください。

- 新しいプライマリを RADIUS サーバとして使用する場合は、RADIUS サーバの構成設定を更新して古いプライマリの構成設定と同じにします。
- 指定された RSA RADIUS サーバの正しい名前と IP アドレスを使用するようにすべての RADIUS クライアントを構成します。デバイス固有の構成手順については、NAS デバイスのマニュアルを参照してください。

5. Authentication Manager を旧バージョンのエージェント ホストのアクティング サーバとして定義する場合は、このサーバをアクティング マスタまたはアクティング スレーブとして使用する旧バージョンのすべてのエージェント ホストに対して、新しい **sdconf.rec** ファイルを作成し、その **sdconf.rec** ファイルをエージェント ホストに配布します。詳細については、ヘルプの「Assign Acting Servers」を参照してください。
6. SSL を使用して LDAP サーバに接続する LDAP 同期ジョブが設定されていた Authentication Manager の場合、新しいプライマリで ***ACEDATA*/ldapjobs/sslcerts** ディレクトリに必要な **cert7.db** ファイルがあることを確認する必要があります。このファイルがない場合、LDAP 同期が実行されると次のエラー メッセージが表示されます。

   ```
   LDAP connection error - Failed to initialize LDAP session (LDAP 接続エラー - LDAP セッションを初期化できません)
   ```

   cert7.db ファイルの設定については、111 ページの「SSL の使用」を参照してください。
7. Authentication Manager が v5.0 のエージェント ホストの **sdopts.rec** ファイルで指定されている場合は、エージェント ホストの **sdopts.rec** ファイルを編集して Authentication Manager の新しい名前または IP アドレスを反映します。

カスタム定義データ (拡張レコード) のメンテナンス

RSA Authentication Manager 拡張レコードを使用すると、RSA Authentication Manager プログラムの実行に必要な情報の他に、組織で必要とされるデータベース情報などを定義して管理できます。このカスタム定義情報を**拡張データ**と呼びます。

リモート アドミニストレーション マシンで実行される RSA Authentication Manager Host Mode アプリケーションでは、拡張レコードにアクセスし、処理するためのメニュー オプションが提供されています。

次の表は、処理対象の拡張データの種類、データが格納されているデータベース テーブル、データを処理するために使用するメニュー、および詳細情報が示されている場所を示しています。

拡張データ	データベース テーブル	メニュー	参照ページ
RSA Authentication Manager システム関連	CustSystemExtension	[System]	209
エージェント ホスト関連	CustClientExtension	[Agent Host]	55
グループ関連	CustGroupExtension	[Group]	118
ログ エントリ関連	CustLogExtension	[Log]	147
サイト関連	CustSiteExtension	[Site]	131

拡張データ	データベース テーブル	メニュー	参照ページ
トークン関連	CustTokenExtension	[Token]	117
ユーザ関連	CustUserExtension	[User]	ヘルプを参照

カスタム定義データにもとづくレポートを作成するには、[Report] メニューの [Extension Data] をクリックします。

メモ：拡張フィールドとカスタム アドミニストレーション プログラムの作成の詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

ログ拡張データの管理

このセクションでは、ログ関連の拡張データを作成、編集、および削除する方法について説明します。その他の種類の拡張データの管理方法については、前のセクション「カスタム定義データ (拡張レコード) のメンテナンス」の表を参照してください。

ログ エントリ拡張フィールドを使用すると、既存のログ エントリに情報を追加できます。この情報を使用して、レポートで使用するログ エントリを選択できます。

ログ拡張データを編集するには

1. リモート アドミニストレーション マシンでRSA Authentication Manager Host Mode を起動します。
2. [Log] > [Edit Log Extension Data] の順にポイントします。
3. 拡張データが関連付けられているログ　メッセージの種類を選択します。[Activity Log Extension]、[Exception Log Extension]、[Incident Log Extension] のいずれかを選択してください。

   [Log Entry Selection Criteria] ダイアログ ボックスが表示されます。
4. 1 つまたは複数のフィールドに選択条件を入力します。フィールドの説明については、159 ページの「レポートの内容の選択条件」を参照してください。

   すべての選択条件をデフォルト値にリセットするには、[Clear] をクリックします。
5. 選択条件を指定したら、[OK] をクリックします。

   [Select Log Entry] ダイアログ ボックスが表示され、入力したすべての条件を満たすログ レコードだけが表示されます。

   ダイアログ ボックスでは、エントリごとに時刻 (世界協定時とローカル時刻)、動作が記録されたユーザ、およびログ メッセージが表示されます。管理者が選択値を変更するか、または現在のアドミニストレーション セッションを終了するまで、選択されている値は有効です。
6. 拡張データが関連付けられているログ　エントリを選択し、[Edit Log Extension Data] をクリックします。

   [Edit Log Extension Data] ダイアログ ボックスが表示され、ログ エントリと、このエントリに対して定義されているレコードが表示されます。各レコードはセカンダリ キー (48 バイト以内) とデータ (80 バイト以内) で構成されます。

7. これらのレコードは追加、変更、削除できます。同じキーを使用して複数のレコードを作成できますが、1 つの拡張データベース テーブルに重複するレコード (キーとデータ値の**両方**が同一のレコード) を作成することはできません。
   - 既存のレコードを変更するには、レコードを選択し、[Key] フィールドまたは [Data] フィールドに表示された情報を変更し、[Save] をクリックします (これらのフィールドのいずれかに入力するまで、[Save] ボタンは使用できません)。

     レコードを変更せずにフィールドをクリアするには、[Clear] をクリックします。
   - 新規レコードを作成するには、必要に応じて [Clear] をクリックして [Key] フィールドと [Data] フィールドをクリアし、新規レコードの情報を入力し、[Save] をクリックします。
   - レコードを削除するには、レコードを選択し、[Delete] をクリックします。確認のために [OK] をクリックします。
8. [Exit] をクリックして、[Edit Log Extension Data] ダイアログ ボックスを閉じます。

外部 4GL プロシージャの実行

4GL によるプログラミングに習熟している場合は、RSA Authentication Manager Host Mode から独自の 4GL プロシージャを直接実行して、RSA Authentication Manager データを処理できます。RSA Authentication Manager データを更新するプロシージャを実行できるのは、レルム管理者か、または **Run Custom 4GL** タスクが割り当てられているユーザだけです。

注意 : 4GL プロシージャを実行すると、ログ レコードや拡張データなどの有効なデータが上書きまたは削除されたり、データベースが壊れる可能性もあります。Administration Toolkit を使用して、RSA Authentication Manager データベースに対して使用するカスタム アプリケーションを作成することを**強くお勧めします**。詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

Authentication Manager データベース フィールドの中には、カスタム アドミニストレーション プログラムで変更できないものが数多くあります。これらのフィールドとカスタム アドミニストレーション プログラムの作成の詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

RSA Authentication Manager Host Mode から 4GL プロシージャを実行するには

1. [RSA Authentication Manager Host Mode] の [File] を選択し、[Run Custom 4GL] をクリックします。

   [Run External Procedure] ダイアログ ボックスが表示されます。
2. 実行するプロシージャのファイル名を [Procedure Name] フィールドに入力するか、または [Browse] をクリックし、リストからファイル名を選択します。
3. [Automatically Connect to RSA Authentication Manager Database] チェックボックスを使用して、RSA Authentication Manager データベースに対して選択したプロシージャを実行するかどうかを指定します。

このチェックボックスは便宜上提供されています。このチェックボックスをオンにしておくと、管理者権限を示すコード行や、対象となる RSA Authentication Manager データベースを指定するコード行を 4GL プロシージャに指定する必要がありません。これらの指定は RSA Authentication Manager Host Mode が行います。

RSA Authentication Manager データベース以外のデータベースにアクセスするプロシージャを実行している場合は、このチェックボックスをオンにしないでください。その場合は、対象のデータベースに接続するためのコードを 4GL プロシージャに指定します。

4. 基本的にはすべてのデータベース　レコードに対してプロシージャを実行できますが、『Administration Toolkit Reference Guide』のデータベースに関する説明で、アスタリスクがついているデータベース レコードに対してはプロシージャを実行できません。また、[Object Type] フィールドを使用して、プロシージャの実行対象を特定の種類のレコード (ユーザ レコードやトークン レコードなど) に制限することもできます。

   すべての種類のレコードに対してプロシージャを実行するには、デフォルト オブジェクト タイプ ([None]) を使用します。特定の種類のレコードに対してプロシージャを実行するには、[Object Type] の下のデータの種類 ([User]、[Token]、[Group]、[Agent Host]、[Site]、[Realm] のいずれか) を選択します。その後表示される [Select] ダイアログ ボックスから特定のレコードを選択し、[OK] をクリックします。

   選択したレコードのフィールドが [Argument List] に表示されます。プロシージャは、これらのフィールドの値を使用します。RSA Authentication Manager Host Mode は、各フィールドの値を抽出し、一続きのデータとして表示順に連結します。それぞれの値は、シャープ記号 (#) で区切られます。一続きのデータを解析し、フィールドの値ごとにレコードを処理するようにアプリケーションを作成できます。

   次の表は、[Object Type] フィールドで各オブジェクト タイプを選択したときに、RSA Authentication Manager Host Mode が抽出し、連結するレコードのフィールドを示しています。

オブジェクト タイプ	[Argument List] の内容
[User]	First name (ファースト ネーム)、Last name (ラスト ネーム)、Default login (デフォルト ログイン)、Default shell (デフォルト シェル)
[Token]	Token serial number (トークンのシリアル番号)、Last login date (最終ログイン日)、Last login time (最終ログイン時刻)
[Group]	Site name (サイト名)、Group name (グループ名)
[Agent Host]	Agent Host name (エージェント ホスト名)、Network address (ネットワーク アドレス)、Protocol (プロトコル)
[Site]	Site name (サイト名)
[Realm]	Primary name (プライマリ名)、Primary address (プライマリ アドレス)、Replica name (レプリカ名)、Replica address (レプリカ アドレス)

5. [OK] をクリックします。

8 ログ データベースのメンテナンス

この章では、ログ データベースのメンテナンス ツールと使用手順について説明します。

この章の説明は、RSA Authentication Manager 監査証跡が格納されている**ログ データベース**にのみ適用されます。ユーザ、トークン、グループ、エージェント ホストなどのレコードが格納される **Authentication Manager データベース**には適用されません。

レプリカ Authentication Manager のアクティビティによってログ メッセージが生成されると、そのメッセージはプライマリ Authentication Manager に送信されます。プライマリは、すべてのレプリカから受信したログ メッセージをログ データベースに統合収集します。

[Log] メニュー

RSA Authentication Manager Host Mode の [Log] メニューには、RSA Authentication Managerログ データベースのメンテナンスと制御を行うためのコマンドが用意されています。このセクションでは、監査証跡に関係する [Log Statistics]、[Delete by Percentage]、[Delete Before a Date]、[Automate Log Maintenance]、および [Log Filtering] の 5 つのコマンドについて説明します。[Log] メニューのその他のコマンドについては、ヘルプを参照してください。

ログ データベース統計情報の表示

ログ レコード データベースに格納されているエントリの数を表示するには、[Log] メニューの [Log Statistics] をクリックします。[Audit Trail Statistics] ダイアログ ボックスが表示されます。

このダイアログ ボックスには、もっとも古いログ レコードのタイムスタンプも表示されます (24 時間形式の世界協定時で表示されます)。この情報は、日付をもとにログ レコードを削除するときに便利です。詳細については、次のセクション「ログ レコードの削除」を参照してください。

ログ レコードの削除

ログ データベースは、データベース レコードを削除するか、または Authentication Manager 内で使用できるディスク領域がなくなるまで絶えず拡大します。古いログ レコードを削除して、ログ レコード ファイルが拡大しすぎないように注意してください。ログ データベースが空きディスク領域をすべて使い切ってしまった場合、Authentication Managerは実行された操作をログに記録できず、ユーザを認証しません。このため、ユーザのアクセスは拒否されます。

データベース内のログ レコードを特定の割合だけ削除したり、特定の日付以前に作成されたすべてのログ レコードを削除することができます。また、スケジュールに従ってレコードを削除するように、Authentication Manager を設定することもできます。153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください。

ログ レコードを削除すると、ディスク領域が解放され、新しいログ レコードの格納に利用できるようになります。ただし、データベース圧縮ユーティリティを実行しないと、このディスク領域を他のユーザが**使用することはできません**。したがって、大量のログ レコードを削除した後に、データベースを圧縮してください。

一定の割合でログ レコードを削除するには

1. [Log] メニューの [Delete by Percentage] を選択します。
   ログ エントリの総数に対するパーセントを要求するプロンプトが表示されます。
2. データベース内のすべてのレコードを削除するときは、「100」と入力し、[OK] をクリックします。
   一部のレコードだけを削除するときは、データベースに現在格納されているログ レコードの総数に対するパーセントを入力します。このダイアログ ボックスには、ログ レコードの総数、もっとも古いログ レコードの日付とローカル時刻が表示されます。
3. [OK] をクリックします。
   1 ～ 100 の数値を入力すると、確認ボックスが表示され、削除の対象として選択したログ レコードの数が表示されます。ログ レコードはデータベース内で古い順に選択されます。
4. 選択したログ レコードを削除するには、[OK] をクリックします。

削除操作が完了すると、データベース内のログ レコードの総数が少なくなり、ダイアログ ボックスが閉じます。

日付と時刻でログ レコードを削除するには

1. [Log] メニューの [Delete Before a Date] を選択します。
   [Audit Trail Delete Before a Date] ダイアログ ボックスが表示されます。
   このダイアログ ボックスには、もっとも古いログ レコードの日付とローカル時刻、およびデータベースに現在格納されているログ レコードの総数が表示されます。
2. データベースに残すログ レコードの日付を月、日、年の形式 (***mm/dd/yyyy***) で入力します。
   時刻 (世界協定時ではなく、ローカル時刻) も指定できます。時刻を指定しなかった場合は、ローカル時刻の 00:00:00 (午前 0 時) であるものと解釈され、ログに記録されたレコードのうち、指定された日付より前のレコードが削除されます。

たとえば、「02/02/2001」と入力したときに、タイムスタンプが 02/01/2001 23:59:59 のレコードがあると、それが削除される最新のレコードになります。

正しい日付を入力すると、確認ボックスが表示され、削除の対象として選択されたログ レコードの数 (つまり、データベースに格納されているログ レコードのうち、入力した日時以前のタイムスタンプを持つログ レコードの数) が表示されます。

3. ログ レコードを削除するには、[OK] をクリックします。

削除操作が完了すると、データベース内のログ レコードの総数が少なくなり、ダイアログ ボックスが閉じます。詳細については、85 ページの「データベース圧縮ユーティリティによるディスク領域の再利用」(Windows)、または 133 ページの「データベース圧縮ユーティリティによるディスク領域の再利用」(UNIX) を参照してください。

ログ データベースの自動メンテナンスのスケジュール

監査ログ データベースの定期的なバックアップとメンテナンスをスケジュールするには、Automated Log Maintenance (ログの自動メンテナンス) 機能を使用します。Authentication Manager は、指定されたスケジュールと方法に従って、監査ログ レコードを削除し、アーカイブすることができます。

削除を実行すると、ログ レコードが監査ログから削除されます。アーカイブを実行すると、ログ レコードがカンマ区切り (CSV) 形式でファイルに保存されますが、元のレコードは削除されません。ログ レコードを削除したときに、ディスク領域をログ データベース以外の用途に使用できるようにするには、85 ページの「データベース圧縮ユーティリティによるディスク領域の再利用」(Windows)、または 133 ページの「データベース圧縮ユーティリティによるディスク領域の再利用」(UNIX) で説明したデータベース圧縮ユーティリティを使用する必要があります。

アーカイブ ファイル

アーカイブ ファイルは、ログ データベースのバックアップ コピーとは異なります。バックアップ コピーの場合は、ファイルを復元して Authentication Manager で使用できますが、アーカイブ ファイルをログ データベースに復元することはできません。ログ データベースのバックアップ コピーの作成方法については、86 ページの「RSA Authentication Manager データのバックアップと復元」(Windows)、または 134 ページの「RSA Authentication Manager データのバックアップと復元」(UNIX) を参照してください。

アーカイブ ファイルはカンマ区切り (CSV) 形式で保存されます。この形式のファイルでは、列はカンマで区切られ、行は EOL 記号で区切られます。Microsoft Excel やその他のサードパーティ製ソフトウェアで CSV 形式のファイルを使用すると、監査ログ レコードを表示したり、レポートを作成できます。

Automated Log Maintenance 機能でログ レコードがファイルにアーカイブされるたびに、ユーザ定義拡張データだけが格納された別のファイルも保存されます。このファイルはアーカイブ ファイルと同じ名前であり、**x** が最後に追加されます。このファイルは拡張データを定義したかどうかとは無関係に作成されます。

たとえば、アーカイブ ファイルにデフォルトの **logcsv** という名前を付けてログ レコードをアーカイブした場合、拡張データは **logcsvx** という名前のファイルに保存されます。拡張データの詳細については、98 ページの「カスタム定義データ (拡張レコード) のメンテナンス」(Windows)、または 146 ページの「カスタム定義データ (拡張レコード) のメンテナンス」(UNIX) を参照してください。

アーカイブ ファイルのバージョンはすべて、Authentication Manager の ***ACEDATA*** ディレクトリに格納されます。アーカイブ ファイルのバージョン数が [Cycle Through] フィールドに入力した値に等しくなると、Automated Log Maintenance 機能はもっとも古いバージョンを上書きします。どのバージョンが最新のバージョンであるかを判断するには、ファイルの日付を確認しなければなりません。

たとえば、[Cycle Through] フィールドに「3」と入力し、デフォルト アーカイブ ファイル名 **logcsv** を使用した場合には、Automated Log Maintenance 機能を 4 回目に実行したときに、**logcsv.1** ファイルが上書きされます。

操作手順：[Log] > [Automate Log Maintenance] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

ログ フィルタリング

ログ フィルタリングを使用すると、RSA Authentication Manager ログ データベースに保存されるログ メッセージを選択できます。特定のメッセージをフィルタ条件で除外すると、ログ データベースのサイズの増大を緩和でき、RSA Authentication Manager のレプリケーション、認証、管理のパフォーマンスを向上できます。次の例を参照してください。

- Authentication Managerがユーザを認証するたびにデータベースに記録される「PASSCODE Accepted (PASSCODE が受け付けられました)」というメッセージをフィルタで除外すると、認証速度を向上できます。
- レルム間認証の場合は、レルム間の認証要求を受け付ける Authentication Manager でのみ、レルム間メッセージ (XR で始まるメッセージ) をログに記録できます。

  詳細については、第 4 章「レルム アドミニストレーション」を参照してください。

プライマリで特定のログ メッセージをフィルタリングするように設定した場合は、設定をファイルに保存し、設定をレプリカにインポートすることができます。

注意：フィルタで除外されたログ メッセージを復元することはできません。記録する必要がないと確信できるメッセージだけを除外するようにしてください。

操作手順：[Log] > [Log Filtering] > [Configure] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

9 レポート

この章では、RSA Authentication Manager のアクティビティとデータに関するレポートの作成について説明します。また、ユーザ データベースおよびログ データベースからデータを取得するための SQL ベースのカスタム クエリ ツールについても説明します。この章は次のセクションで構成されています。

監査証跡レポート。RSA Authentication Manager は、各ログイン試行と、RSA Authentication Manager Host Mode を通じて実行されたアクションのレコードをログに記録します。管理者はさまざまなレポートを実行して、この監査証跡を表示できます。このセクションでは、RSA Authentication Manager Host Mode の監査証跡レポートと、その書式設定や作成方法について説明します。

拡張データ レポート。このセクションでは、Authentication Manager 拡張レコードのユーザ定義情報に関するレポートの作成方法について説明します。

ログ モニタとレポート作成。このセクションでは、RSA Authentication Manager Host Mode のログ モニタについて説明します。ログ モニタを使用すると、ログ エントリが監査証跡に書き込まれたときに、ただちにそのエントリを表示できます。また、ログ アーカイブ ファイルの形式と、ログ モニタおよびレポート作成のオプションについても説明します。

レポート作成ユーティリティ。2 つのセクションで、カスタム レポートの作成と実行、既製レポートの実行のために使用できるユーティリティについて説明します。レポート作成ユーティリティには、Windows プラットフォーム用と UNIX プラットフォーム用の 2 つのバージョンがあります。レポート作成ユーティリティは、プログラミングに関する知識がなくても使用できます。

カスタム SQL クエリの作成と実行。このセクションでは、RSA Authentication Manager Host Mode に組み込まれているクエリ ツールについて説明します。これらのツールを使用すると、ユーザ データベースおよびログ データベースに対する SQL ベースのクエリを作成および管理できます。実行結果のデータは、一般に使用されている各種のテキスト形式で出力および表示できます。

監査証跡レポート

ログ レコードの内容

このセクションでは、各ログ レコードのフィールドに記録される情報について説明します。ログ レポートのカラムは、これらのフィールドに対応しています。各イベントやアクションは 2 ～ 3 行のデータとしてレコードに記録されます。

ログ レコードの 1 行目

Date と **Time** (日時)。記録されたイベントが発生した日時を世界協定時で表します。

Current User (現在のユーザ)。アクションを実行したユーザのログインです。自動的に発生するシステム イベントの場合 (たとえば、ログイン試行が連続して失敗した後、トークンがネクスト トークンコード モードに設定された場合) には、ユーザは記録されません。認証ログ レコードはユーザのレコードを変更するイベントを記録するので、ログインしているユーザの名前は **Affected User** フィールドに示され、**Current User** フィールドは空白になります。

Agent Host (エージェント ホスト)。イベントが発生したエージェント ホストの名前です。すべての Authentication Manager はエージェント ホストとして定義されているため、アクションが Authentication Manager で実行された場合もエージェント ホスト名が記録されます。

(Group (グループ))。アクションがグループ情報 (メンバーシップ データなど) に影響する場合は、エージェント ホスト名の後にかっこで囲まれたグループ名が記録されます。ユーザのグループ名は、認証ログ レコードには記録されません。

Affected User (影響を受けるユーザ)。トークンが何らかの操作によって直接影響を受けた場合は、シリアル番号が右側のカラムに示されます。トークンが割り当てられている場合は、シリアル番号の代わりに (またはシリアル番号に加えて)、ユーザのログイン名が示されることがあります。どちらの識別子が示されるかは、書式設定によって異なります (詳細については、159 ページを参照してください)。認証ログ レコードの場合は、認証によってユーザのレコードが変更されるため、ログインしているユーザは **Current User** ではなく、**Affected User** として示されます。

ログ レコードの 2 行目

Date と **Time** (日時)。記録されたイベントが発生した日時をローカル時刻で表します。

Description of the Event or Action (イベントまたはアクションの内容)。ログの詳細については、付録 C「トラブルシューティング」を参照してください。

(Site (サイト))。該当する場合は、右側のカラムにかっこで囲まれたサイト名が示されます。これは、現在のエージェント ホストが関連付けられているサイトです。サイト情報は認証ログ レコードには記録されません。

Authentication Manager **Name** または **Realm Name** (Authentication Manager 名またはレルム名)。名前が右側のカラムに示されます。

- ローカル認証イベントの場合は、Authentication Manager 名を示します。
- レルム間認証イベントの場合は、リモート レルムの名前を示します。

ログ レコードの 3 行目

Date と **Time** (日時)。記録されたイベントが発生した日時をローカル時刻で表します。

Affected User Name (影響を受けるユーザ)。この行が記録されるのは、[Report Format] ダイアログ ボックスの [Full User Names] チェックボックスをオンにした場合だけです。この機能が有効になっている場合は、影響を受けるユーザのファースト ネームとラスト ネーム (48 文字以内) が各イベント エントリの 3 行目に記録されます。

レポートの種類

各ログ レコードの内部には、重大度を示すコードが含まれます。レポートに含まれるレコードの種類に応じて、**Activity** (アクティビティ)、**Exception** (例外)、**Incident** (重大なイベント) の各レポートがあります。**Activity** レポートには、重大度が低いものから高いものまで、すべてのレコードが含まれます。**Exception** レポートと **Incident** レポートの内容は、それよりも限定されます。

レポートの種類には、この他に **Usage Summary** (使用状況の要約) があります。これには、システムで発生した特定の種類のアクティビティの回数が表示されます。**Usage Summary** には、ログ メッセージは含まれません。

すべてのレポートの制約事項

レポートの内容はレポートの種類によって制限されますが、その他にすべてのレポートに適用される制約事項があります。レポートにどのレコードが含まれるかは、現在のRSA Authentication Manager Host Mode セッションで設定した選択条件によって決まります (詳細については、159 ページの「レポートの内容の選択条件」を参照してください)。

Activity レポート

Activity レポートには、すべての種類のログ レコードが含まれます。前のセクション「すべてのレポートの制約事項」で説明した制約事項が適用される場合にだけ、ログ レコードが **Activity** レポートから除外されます。

Exception レポート

Exception とは、セキュリティ管理者にとって重要なイベントです。Exception が必ずしもセキュリティ違反を示すわけではありませんが、セキュリティ違反の可能性を示すことがあります。たとえば、ユーザが認証を要求したときや、管理者がデータを編集しようとしたときに発生するエラーは、攻撃者が PIN を推測しようとしたり、使い慣れていないツールでデータベースを編集しようとした結果とも考えられます。

Incident レポート

Incident とは、重大な結果をもたらす複数の関連するイベントです (たとえば、一連のイベントが攻撃回避アクションを起動した場合)。Incident が必ずしもセキュリティ違反を示すわけではありませんが、これらはセキュリティ管理者が注意する必要があるイベントです。次のいずれかのアクションの原因となる一連のイベントが **Incident** レポートに含まれます。

- New PIN Received (新しい PIN を受信しました)
- PIN Created by User (ユーザが PIN を作成しました)
- Next Tokencode On (ネクスト トークンコード モードがオンです)
- Token Disabled, Many Failures (何度も認証に失敗したため、トークンが無効になりました)
- Token Disabled, Suspect Stolen (盗まれた可能性があるため、トークンが無効になりました)

先に起こったイベントが実行中のレポートの対象外である場合は、レポートには「Preceding events not included (前のイベントは含まれません)」というメッセージが含まれます。

Usage Summary (使用状況の要約)

Usage Summary には、レポートの対象期間に特定のアクティビティが実行された回数が示されます。

Usage Summary には次の 2 つのセクションがあります。**General Activity** (全般的なアクティビティ) には、すべてのログイン、トークン、インフラストラクチャ障害、レポート レコード アクティビティが示されます。**Filtered Activity** (フィルタリングされたアクティビティ) には、Usage Summary を作成する前に [Log Entry Selection Criteria] ダイアログ ボックスで指定した要素 (グループ、ユーザ、サイト、レルム) のログインとトークン レコード アクティビティが示されます。

Usage Summary に含まれる情報は次のとおりです。

Denied accesses … アクセスの試みが失敗した回数。

Allowed accesses … アクセスの試みが成功した回数。

Average accesses per day … レポートの対象期間に記録された、成功したアクセスの試みの総数を期間の日数で除算した値。

New tokens assigned … トークン割り当て操作が実行された回数。

New PIN modes set … 管理者がトークンを New PIN モードに設定した回数。

System time changes … [Edit System Parameters] ダイアログ ボックスの [Set clock offset to 0] ボタンが使用された回数。

Report Records … 各種類のレポートが作成された回数。

レポートの作成

RSA Authentication Manager レポートを作成するには

1. [Report] メニューの [Report Format] を選択します。

   [Report Format] ダイアログ ボックスが表示されます。

   実行されるレポートには、このダイアログ ボックスに表示される値が使用されます。これらの書式設定は、RSA Authentication Manager Host Mode セッションが終了した後も保存されます。変更するには、次のセクション「レポートの書式設定」を参照してください。

   レポートを初めて使用する場合は、[Output to] の値を [Screen] に設定すると、レポートを画面で確認できます。
2. [OK] をクリックします。
3. [Report] メニューで、レポートの種類 ([Activity]、[Exception]、[Incident]、[Usage Summary]) を選択します。

   [Report Selection Criteria] ダイアログ ボックスが表示されます。表示される値は、この RSA Authentication Manager Host Mode セッションで設定した最新の値です。
4. 表示された値を使用してレポートを作成するには、[OK] をクリックします。

   設定した選択条件を使用せずに、すべてのユーザ、エージェント ホスト、サーバなどについてのレポートを指定するには、[Clear] をクリックします。すべての選択条件が「*」に設定されるため、レポートにはすべてのアイテムが含まれます。[OK] をクリックします。

   選択条件の詳細については、159 ページの「レポートの内容の選択条件」を参照してください。

   レポートの 1 ページ目に、現在有効な選択条件が表示されます。次ページ以降には、古いレコードから新しいレコードの順に、選択したログ レコードが表示されます。

   ログ モニタ レポートの場合は、[Hold] チェックボックスをオンにすると、スクロールを停止できます (詳細については、164 ページの「ログ モニタとレポート作成」を参照してください)。
5. レポートを閉じるには、[Exit] をクリックします。

レポートの書式設定

レポートを実行するときは、[Report Format] ダイアログ ボックスの値が適用されます。内容の選択条件とは異なり、書式設定変数の変更結果は保存され、次回の RSA Authentication Manager Host Mode セッションにも適用されます。最後のセッション以降に別の管理者が書式設定を変更すると、その変更結果が現在のデフォルト値になります。レポートを実行する前に、[Report Format] の変数が適切に設定されているかどうかを確認してください。

[Report Format] の変数を変更するには

1. [Report] メニューの [Report Format] を選択します。
   [Report Format] ダイアログ ボックスが表示されます。
2. 次の条件に従ってレポートの書式を設定します。
   ヘッダ印刷の設定 … この設定は、レポートをファイルに出力する場合にだけ使用されます。[Header] チェックボックスがオンの場合は、各ページの先頭に次の情報が表示されます。
   - 現在のページのページ番号とレポートの総ページ数
   - レポートのタイトル
   - 使用された時刻選択条件
   - レポートの作成日時

   ページ区切りの設定 … この設定は、レポートをファイルに出力する場合にだけ使用されます。[Page break] チェックボックスがオンの場合は、各ページの後にページ区切り文字が挿入されます。[Page break] チェックボックスがオフの場合は、レポートは基本的に 1 ページになります。この 1 ページのレポートにはヘッダが 1 つ含まれ、ページ区切り文字は含まれません。

   各ページの行数の指定 … この設定は、レポートをファイルに出力し、ページ区切りをオンに設定している場合にだけ使用されます。1 ページには、ページ区切りの前に最大 98 行まで設定できます。1 ページの行数には偶数を指定してください。奇数を指定すると、それより 1 行少ない偶数に切り捨てられます。

   ユーザ名の表示方法の指定 … [Full User names] チェックボックスがオンの場合は、影響を受ける各ユーザのファースト ネームとラスト ネーム (48 文字以内) が、記録される各イベントの 3 行目に表示されます。[Full User names] チェックボックスがオフの場合は、ユーザのフルネームは、記録されるイベントの 1 行目に表示され、3 行目は表示されません。

   影響を受けるトークン / ユーザの識別方法の指定 … トークンがレポートの [Affected User] カラムで識別される場合は、トークンのシリアル番号と割り当てられたユーザの名前のいずれか一方または両方が表示されます。[Affected token identifier] で、[Serial No./Name] (シリアル番号と名前の両方を表示)、[Serial No.] (シリアル番号のみを表示)、[Name] (名前のみを表示) のいずれかのボタンを選択します。

   レポートのタイトルのカスタマイズ … レポートのデフォルトのタイトルは、レポートの種類を示します。[Report Format] ダイアログ ボックスのタイトル フィールドに、別のタイトルを入力できます。各タイトルには 34 文字以内のテキストを指定します。タイトルではすべての半角文字を使用できます。

レポートの内容の選択条件

レポートに含まれるレコードを制限するには、[Report] メニューの [Selection Criteria] を選択します。

[Report Selection Criteria] ダイアログ ボックスが表示されます。

[Specify report by] で、レポートの範囲を指定します。

- レポートを特定のページ数に制限するには、[Pages] をクリックし、[Last:] ボックスにページ数を指定します。ページ サイズは、[Report Format] ダイアログ ボックスで指定した各ページの行数をもとに計算されます。詳細については、159 ページの「レポートの書式設定」を参照してください。

  メモ：ページ数は、レポートを画面に表示することを前提にして計算されます。レポートをファイルに出力する場合は、ページ数が異なる可能性があります。

- レポートを特定の日数に制限するには、[Days] をクリックし、[Last:] ボックスに日数を指定します。
- ログ データベースの最初から現在までのすべてのレコードを指定するには、[Entire] をクリックします。
- レポートを特定の日付範囲に制限するには、[Date] をクリックします。レポートのデフォルトの日付範囲は、現在から 30 日以前までです。別の範囲を入力するには、世界協定時ではなく、24 時間形式のローカル時刻で [From Date] ボックスと [To Date] ボックスに期間を入力します。この場合、***mm/dd/yyyy*** という形式を使用します (***mm*** は月、***dd*** は日、***yyyy*** は年を表します)。[From Date] フィールドに、対象とする最も古いレコードの日付と時刻を入力します。[To Date] フィールドに、対象とする最新のレコードの日付と時刻を入力します。データベースに格納されている最新のレコードを指定するには、このフィールドを空白にします。

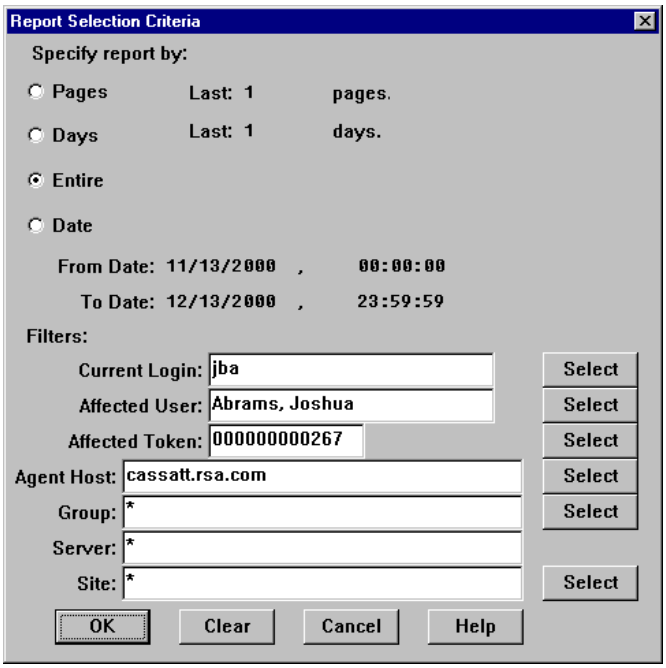
1 つまたは複数の選択フィールドに設定を入力します。選択フィールドにアスタリスク (*) だけが指定されている場合は、その変数に基づく制限は適用されません。

メモ：Activity レポート、Exception レポート、Incident レポート、Usage Summary レポートを作成するときに、**1 つ**のフィールドだけに条件を入力すると、レスポンスを向上できます。フィールドには完全一致の条件を入力することも、ワイルドカードを使用することもできます。たとえば、[Affected User] フィールドに「Joshua Abr*」と入力すると、データベース内のユーザのうち、ファースト ネームが **Joshua** であり、ラスト ネームが **Abr** で始まるすべてのユーザのレポートが作成されます。完全一致 (「Joshua Abrams」) を入力すると、Authentication Manager データベース内のユーザのうち、**Joshua Abrams** という名前のすべてのユーザのレポートが作成されます。

図に示す選択条件を使用すると、次の**すべて**の条件を満たすアクティビティだけを含むレポートが作成されます。

- “jba” というログイン名のユーザが実行したアクティビティ
- “Abrams, Joshua” という名前のユーザのレコードを変更したアクティビティ
- シリアル番号が 000000000267 のトークンのレコードを変更したアクティビティ

- “cassatt” という名前のエージェント ホストで実行されたアクティビティ



サーバ情報やサイト情報をもとにログ レコードを除外することはできません。各選択フィールドについては、この後詳しく説明します。

レポートを作成するときに、最新のイベントに制限するのではなく、特定の期間に制限することができます。その場合は、[Date] ボタンを選択します。時間は、世界協定時ではなく、24 時間形式のローカル時刻で入力します。***mm/dd/yyyy*** という形式を使用してください (***mm*** は月、***dd*** は日、***yyyy*** は年を表します)。[From Date] フィールドに、対象とする最も古いレコードの日付と時刻を入力します。ログ データベースの最初からすべてのレコードを指定するには、このフィールドを空白にします。[To Date] フィールドに、対象とする最新のレコードの日付と時刻を入力します。データベースに格納されている最新のレコードを指定するには、このフィールドを空白にします。

レポートに含めるログ レコードの選択には、さまざまな条件を使用できます。各ボックスの横に表示される [Select] ボタンを使用すると、簡単に操作できます。[Select] ボタンを使用せずに、フィールドに直接入力する場合は、設定を慎重に入力してください。入力された名前やシリアル番号が正しいかどうかは自動的には確認されません。たとえば、実際のグループ名が **Marketing** の場合に、[Group] フィールドに「Market」と入力すると、システムはレポートに含めるレコードを見つけることができません。しかし、レポートが実行されるまで、誤って入力したかどうかはわかりません。

選択条件	含まれるアクティビティ
[Current Login]	指定したユーザが実行したアクティビティ。ユーザの名前ではなく、ユーザのログインを入力してください。
[Affected User]	特定のユーザに影響した操作のレコード。ユーザのログインではなく、ユーザ名を入力してください。
[Affected Token]	特定のトークンに影響した操作のレコード。トークンのシリアル番号を指定してください。

選択条件	含まれるアクティビティ
[Agent Host]	指定したエージェント ホストに関連するアクティビティ。指定したエージェント ホストで実行されたログインの試みと、Authentication Manager の **sdserv** データベースに格納されているエージェント ホストの情報の変更が報告されます。
[Group]	指定したグループに影響した管理操作 (グループ メンバの追加や削除など)。グループをもとに選択したレポートには、グループ メンバのログイン アクティビティは含まれません。
[Server]	指定したプライマリ、レプリカ、またはレルムで実行されたアクティビティ。
[Site]	指定したサイトに影響するすべての管理操作 (サイト内でのグループやエージェント ホストの作成など)。サイトをもとに選択されたレポートには、ログイン アクティビティは含まれません。

すべての選択条件をデフォルト値にリセットするには、[Clear] をクリックします。

選択条件を選択した後、[OK] をクリックしてダイアログ ボックスを閉じます。

次にレポートを実行したときに作成されるレポートには、入力した選択条件をすべて満たすレコードだけが含まれます。管理者が選択値を変更するか、または現在の RSA Authentication Manager Host Mode セッションを終了するまで、選択されている値は有効です。

ファイルへのレポートの出力

ログ モニタ レポートも含めて、すべての種類の監査証跡レポートは ASCII テキスト ファイルとして保存できます。

レポートをファイルとして保存するには

1. [Report] メニューの [Report Format] を選択します。
   [Report Format] ダイアログ ボックスが表示されます。
2. [Output to] で [File] を選択します。
3. 特定のファイル名をステップ 6 で表示されるデフォルト ファイル名にするには、その名前を [Report filename] フィールドに入力します。
   名前を入力するときは、オペレーティング システムの文字制限の規則に従ってください。
4. 他の書式を設定します。
   詳細については、159 ページの「レポートの書式設定」を参照してください。
5. [OK] をクリックします。
6. [Report] メニューで、作成するレポートを選択します。

[Report Filename] ダイアログ ボックスが表示され、レポート ファイルの名前が要求されます。ステップ 3 で [Report Format] ダイアログ ボックスにファイル名を入力した場合は、その名前がボックスに表示されます。別のパスとファイル名を指定することもできます。既存のファイルを選択するか、選択できるパスを表示するには、[Browse] ボタンをクリックします。

7. パスとファイル名を指定した後、[OK] をクリックして [Report Filename] ダイアログ ボックスを閉じ、レポートを作成します。

レポートをファイルに保存すると、指定したファイル名でレポートが保存されたことを示すメッセージ ボックスが表示されます。

このレポート ファイルは安全な場所に保管してください。レポートには、サーバ名、エージェント ホスト名、ユーザ名など、システムに関する多くの情報が含まれています。この情報は不正に使用されないように保護する必要があります。

拡張データ レポート

拡張レコードのレポートを作成するには

1. [Report] メニューの [Extension Data] を選択します。

   [Report Selection Criteria] ダイアログ ボックスが表示されます。

2. レポートの書式を指定します。

   [Output to] … レポートをモニタに表示するには、[Screen] をクリックします。レポートを ASCII テキスト ファイルとして保存するには、[File] をクリックします。

   [Need] … これらの値は、レポートをファイルに出力する場合にだけ使用されます。レポートのタイトルをファイルに追加するには、[Header] チェックボックスをオンにします。各ページの後にページ区切り文字を追加するには、[Page Break] チェックボックスをオンにします (次の項目の [Lines per page] でページの長さを設定します)。[Page Break] チェックボックスがオフの場合は、レポートは基本的に 1 ページになります。この 1 ページのレポートにはヘッダが 1 つ含まれ、ページ区切り文字は含まれません。

   [Lines per page] … この設定は、レポートをファイルに出力し、[Page Break] チェックボックスがオンになっている場合にだけ使用されます。1 ページの行数を 9 ～ 60 行の範囲で設定します。

   [Report Title] … レポートのデフォルトのタイトルは、レポートの種類を示します。[Report Title] フィールドに別のタイトルを入力して、レポートのデフォルトのタイトルを変更できます。タイトルには 60 文字以内のテキストを指定します。すべての文字を使用できます。

3. レポートの内容を指定します。

   レポートに含める拡張データの種類を指定するには、[Extension Type] リストでカテゴリをクリックします。

4. 1 つまたは複数の選択フィールドに設定を入力します。

   - エージェント ホスト、グループ、サイト、ユーザ拡張データの場合は、拡張データに関連するエージェント ホスト、グループ、サイト、ユーザ名をそれぞれ指定します。トークン拡張データの場合は、トークンのシリアル番号を指定します。ログ拡張データの場合は、メッセージを指定します。
   - 特定のキー値を含む拡張レコードをレポートに出力するには、[Key] フィールドに値を入力します。

- 特定のデータ値を含む拡張レコードをレポートに出力するには、[Data] フィールドに値を入力します。

各ボックスの横に表示される [Select] ボタンを使用すると、簡単に操作できます。[Select] ボタンを使用せずにフィールドに設定を入力する場合は、慎重にデータを入力してください。入力された名前やシリアル番号が正しいかどうかは自動的には確認されません。

選択フィールドにアスタリスク (*) だけが指定されている場合、レポートに含まれるレコードには、その変数に基づく制限は適用されません。そのフィールドのすべての値が受け入れられます。

5. 表示された設定を使用してレポートを作成するには、[OK] をクリックします。

拡張データ レポートの内容

各レポートには、次の情報が含まれます。

- レポート作成の選択条件
- レポートの作成日時
- 拡張データの種類によっては、次の情報も含まれます。
  - **[Agent Host]**：エージェント ホスト名とネットワーク アドレス
  - **[Group]**：グループ名とサイト名
  - **[Log message]**：ログ メッセージと、メッセージが作成されたローカル時刻
  - **[Site]**：サイト名
  - **[Token]**：トークンのシリアル番号とユーザ名
  - **[User]**：ユーザのファースト ネーム、ラスト ネーム、デフォルト ログイン
- 選択条件を満たすすべてのレコード

ログ モニタとレポート作成

このセクションでは、RSA Authentication Manager システムのアクティビティを監視する方法について説明します。また、定期的にシステム アクティビティが格納されるログ ファイルについても説明します。

RSA Authentication Manager Host Mode からログ モニタ セッションを起動すると、アクセスの試みやデータベース アドミニストレーションなどのアクティビティのレコードが監査証跡に書き込まれると同時に、そのレコードを確認できます。

RSA Authentication Manager には、ログ イベントをシステム ログに送信する機能もあります。この機能を使用すると、システムの問題発生を通知するサードパーティ製のツールを利用して、システムを監視することもできます。

ログ メンテナンスを目的として、ログ ファイルにシステム アクティビティが定期的に格納されるように Authentication Manager を設定できます。このテキスト ファイルにアクセスすると、RSA Authentication Manager のアクティビティに関する履歴のレコードを表示できます。ログ ファイルは CSV (カンマ区切り形式) として書き込まれるので、内容をサードパーティ製のツールにインポートしてデータを表示したり、カスタム レポートを作成することもできます。

ログ モニタ オプション

モニタの種類を示すサブメニュー ([Activity]、[Exception]、[Incident]) を表示するには、[Report] メニューの [Log Monitor] を選択します。このサブメニューを使用して、すべてのアクティビティを監視するセッションを開始でき、例外や重大なイベントなどの注意が必要なアクティビティだけを監視するセッションを開始することもできます。156 ページの「レポートの種類」を参照してください。

メモ : ログ モニタを使用するには、プライマリ上のデータベースに接続されている必要があります。

ログ モニタの種類を選択すると、[Log Monitor Selection Criteria] ダイアログ ボックスが表示されます。特定のユーザや特定のエージェント ホストでのアクティビティだけを監視するには、選択条件を設定し、[OK] をクリックします。ライブ レポート ウィンドウが開き、アクティビティが発生するとただちに報告されます (詳細については、159 ページの「レポートの内容の選択条件」を参照してください)。

レポート ウィンドウが表示されると、継続的なリアルタイム監視が開始されます。レポート ウィンドウを閉じずにログ モニタを一時的に停止するには、[Hold] チェックボックスをオンにします。監視が停止されると、ナビゲーション ボタン ([Previous]、[Next]、[Go To]) が有効になります。これらのボタンを使用して、レポートの各ページに移動します。

ログ モニタは、各セッションで最大 100 ページを表示できます。

ログ モニタ セッションを終了するには、[Exit] をクリックします。モニタ ウィンドウが閉じ、RSA Authentication Manager Host Mode のメイン メニューに戻ります。

sdlogmon コマンドの使い方

UNIX サーバでは、RSA Authentication Manager Host Mode の外部からログ モニタを開始することもできます。プライマリのコマンド ライン プロンプトで、次のコマンドを入力します。

```
sdlogmon [-type] [-t] [-f filename]
```

引数	説明
-type	実行するモニタの種類を指定するには、この引数を使用します。すべてのアクティビティを監視するときは **-a** (この引数を省略した場合のデフォルト)、例外のみを監視するときは **-e**、重大なイベントのみを監視するときは **-i** を指定します。
-t	長いファイルの末尾に記録されている新しいアクティビティを表示するには、“tail” 引数を使用します。上にスクロールして、前のアクティビティを表示することができます。この引数を省略すると、ログ モニタはキャラクタ モードのライブ レポート ウィンドウ (165 ページを参照) で実行されます。 この引数は、画面出力の場合 (**-f** 引数が使用されていない場合) にだけ使用してください。
-f *filename*	画面ではなく、ファイルに出力するには、この引数を使用します。**-f** 引数のすぐ後にファイル名を指定します。**-f** 引数を使用する場合、**-t** 引数は指定できません。

ログ モニタ セッションを終了するには、CTRL+C を押します。この操作により、コマンド ラインに戻ります。

システム ログ内の Authentication Manager イベントの監視

RSA Authentication Manager のアクティビティを追跡する方法として、ホストマシンのイベント ログ (Windows) またはシステム ログ (UNIX) に送信されるイベントを監視する方法もあります。これらのログはシステムの一部です。

サードパーティ製のネットワーク管理用 SNMP (Simple Network Management Protocol) ツールは、一般に各種コンピュータのシステム ログを監視するように設定できます。また、重大な問題 (RSA Authentication Manager の機能停止など) が発生したときに担当者に電子メール メッセージを送信したり、ポケットベルを鳴らすように設定することもできます。

RSA Authentication Manager の動作には、一般的なイベントの種類として次の 2 つがあります。

- 監査ログ データベースに送信されるイベント。
- RSA Authentication Manager プロセスに関連するその他のイベント。後で説明するように一部の例外がありますが、基本的には**自動的**にホスト マシン (一般にプライマリ サーバまたはレプリカ サーバ) のシステム ログに記録されます。

RSA Authentication Manager Host Mode には、システム ログに送信される監査ログ データベースのメッセージを指定できるツールが用意されています。詳細については、281 ページの「イベント ログまたはシステム ログへの監査ログ メッセージの送信」を参照してください。

ログ データベースのメッセージをフィルタリングして重複を防ぐことによって、システム ログを基本的なログ記録の手段として利用できます。フィルタリング機能を使用すると、指定された種類のメッセージをログ データベースから除外できます。詳細については、154 ページの「ログ フィルタリング」を参照してください。

RSA Authentication Manager では、**すべて**のプロセスからのイベントに対して、フィルタリングやシステム ログへの記録を指定できます。RSA Authentication Manager の環境では複数のサーバが使用されるので、導入環境に含まれるプライマリとすべてのレプリカに対して、フィルタリングとシステム ログへの記録の設定を行う必要があります。

メモ: RSA Authentication Manager のすべてのプロセスの説明については、付録 B「サービスとプロセス」を参照してください。RSA Authentication Manager 関連の重要なシステム ログ メッセージの一覧と説明については、付録 C「トラブルシューティング」の「メッセージ」を参照してください。

システム ログには、ローカルとリモートの 2 種類があります。ローカルのシステム ログへの記録は、プロセスを実行しているホスト マシン上で、RSA Authentication Manager データベースに接続されているすべてのプロセスによって実行されます。ただし、Remote Administration プロセス、RADIUS プロセス (ローカルおよびリモート)、Job Executor (JSED) プロセスは例外です。これらの例外の場合は、リモートからシステム ログに記録されます。これについては以下で説明します。

Remote Administration 関連イベントのシステム ログへの記録

[RSA Authentication Manager 6.1 Administration - Remote Mode] コマンドを使用すると、Remote Administration を起動したコンピュータ上ではなく、リモート ホスト コンピュータ上でリモート セッションがシステム ログに記録されます。

ホスト コンピュータは、レルム内のプライマリまたはレプリカのいずれかです。システム ログへの記録は、Remote Administration プロセスが**最初**に接続された Authentication Manager の **sdadmind** プロセスによって処理されます。つまり、レルム内の別の Authentication Manager に切り替えた後も、システム ログへの記録は最初の Authentication Manager (最初に認証が行われた Authentication Manager) で続行されます。

RADIUS サーバ関連イベントのシステム ログへの記録

RADIUS サーバ アクティビティのログへの記録については、『RSA RADIUS Server 6.1 Administrator's Guide』を参照してください。

Job Executor 関連イベントのシステム ログへの記録

Job Executor (JSED) プロセスは、定期的にライセンスの有効性を確認するとともに、LDAP 同期を処理します。

ログの記録方式は、ローカル RADIUS サーバの場合と同じです。「Job Executor server started (Job Executorサーバが起動しました)」と「Job Executor server stopped (Job Executor サーバが停止しました)」の 2 つのイベントをデータベース監査ログに送信します。これらのイベントを監査ログから除外することはできますが、システム ログに送信するように指定することはできません。

ただし、JSED はサーバが起動または停止したときに、それぞれのメッセージを自動的にシステム ログに送信します。

ログ アーカイブ ファイルの使い方

ログ メンテナンスの自動化を有効にすると、RSA Authentication Manager 監査証跡を 1 つまたは複数のログ アーカイブ ファイルに定期的に格納できます (詳細については、153 ページの「ログ データベースの自動メンテナンスのスケジュール」を参照してください)。

ログ アーカイブ ファイルは、いつでも表示できます。たとえばセキュリティ上の理由や統計分析のために、Authentication Manager 内の特定の種類のトランザクション履歴を調査する必要がある場合に使用できます。

ログ アーカイブ ファイルのデフォルト名は、**logcsv** です。アーカイブ ファイルのログ データは、CSV (カンマ区切り形式) として保存されるので、Microsoft Excel などのサードパーティ製アプリケーションにインポートできます。

ログ アーカイブ データをアプリケーションにインポートした後、使用しているアプリケーションに応じて、データをフィルタリング、書式設定、整理して、さまざまなカスタム レポートとして出力できます。

このセクションでは、**logcsv** ファイルの形式について説明します。**logcsv** ファイルは、カンマで区切られた 17 のフィールドを含む複数のレコードで構成されています。各レコードの末尾にはライン フィードがあります。表計算ソフトにインポートすると、各レコードは 17 の列 (A - Q) で構成される 1 つの行として書式設定されます。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	2	1/24/2003	2:34:56	1/23/2003	21:34:56	4014	sdsetup							dpal	0	0	Added user
3	3	1/24/2003	2:34:56	1/23/2003	21:34:56	4019	sdsetup							dpal	0	0	Changed user admin level
4	4	1/24/2003	2:41:22	1/23/2003	21:41:22	6507		--------	---->				EUSLONER.NA.RSA		0	0	ALM thread started
5	5	1/24/2003	2:41:22	1/23/2003	21:41:22	1143	SYSTEM				No entries filtered.		EUSLONER.NA.RSA		1364	0	Log Filter Summary
6	6	1/24/2003	2:41:23	1/23/2003	21:41:23	1149		SYSTEM	----->			EUSLONE	EUSLONER.NA.RSA		0	0	Job Executor server started
7	7	1/24/2003	2:41:23	1/23/2003	21:41:23	2004		SYSTEM	accepted 1228				EUSLONER.NA.RSA		0	0	Accepted started

次の表は各列の内容を示しています。

列	説明
A	ログ エントリ ID (一意の識別子)。
B	GMT 日付。
C	GMT 時刻。
D	ローカル日付。
E	ローカル時刻。
F	メッセージ番号。
G	操作を実行した管理者の名前。このフィールドには、操作を実行したサービスまたはユーティリティの名前が格納されることもあります。
H	操作を実行したユーザのデフォルト ログイン。このフィールドには、操作を実行したサービスまたはユーティリティを示す文字列が格納されることもあります。
I	トークンのシリアル番号 (トークンのアクティビティが発生しない操作の場合、このフィールドは空欄のままか、またはプレースホルダが格納されます)。
J	管理操作にかかわったサイト名。認証アクティビティが実行されている間、このフィールドは空欄になります。
K	管理操作にかかわったグループ名。認証アクティビティが実行されている間、このフィールドは空欄になります。
L	操作にかかわったエージェント ホスト名 (エージェント ホストの IP アドレスが格納されることもあります)。認証アクティビティが実行されている間、このフィールドにデータが格納されます。
M	操作を実行した Authentication Manager、または操作が関連する Authentication Manager の名前。
N	操作の影響を受けたユーザの名前。
O	イベントを記録したアプリケーションのプロセス ID (一般には空欄です)。
P	メッセージのエラー レベル。
Q	メッセージ テキスト。

RSA Authentication Manager レポート作成ユーティリティ (Windows)

RSA Authentication Manager ソフトウェアに含まれるレポート作成ユーティリティを使用すると、**sdlog** データベースに対して監査証跡レポートを作成および実行し、**sdserv** データベースに対してトークン統計レポートを作成および実行できます。このユーティリティには、選択したユーザに対応するユーザ レコードから、その情報を取得して画面に表示する機能もあります。

レポート作成ユーティリティのインストール

レポート作成ユーティリティ ソフトウェアは、RSA Authentication Manager をインストールするときに ***ACEUTILS*** ディレクトリにコピーされます。レポート作成ユーティリティを単独でインストールする必要はありません。

レポート作成ユーティリティの起動と停止

レポート作成ユーティリティを起動するには

1. コマンド プロンプトで次のように入力して、レポート データベース サーバを起動します。

   ```
   ACEUTILS¥rptconnect start
   ```

2. 次のように入力して、レポート作成ユーティリティを実行します。

   ```
   ACEUTILS¥sdreport
   ```

メモ: レポート作成ユーティリティは、バッチ モードで実行することもできます。バッチ モードでは、[RSA Authentication Manager Reports] ダイアログ ボックスは表示されません。バッチ モードでデータベースに接続するには、「ACEUTILS¥rptconnect start batch」と入力します。

[RSA Authentication Manager Reports] ダイアログ ボックスが表示されます。

レポート作成ユーティリティを停止するには

1. [RSA Authentication Manager Reports] ダイアログ ボックスで、[File] メニューの [Exit] を選択します。
2. コマンド プロンプトで次のように入力して、レポート データベース サーバを停止します。

   ```
   ACEUTILS¥rptconnect stop
   ```

重要： この方法でレポート作成ユーティリティを停止しないと、ユーティリティはロックされ、***ACEUTILS*¥sdrpt.lk** というロック ファイルが作成されます。その場合は、ロック ファイルを削除して、もう一度操作を実行してください。

実行するレポートの選択

[RSA Authentication Manager Reports] ダイアログ ボックスでは、実行するレポートを 2 つのリスト ([Standard Reports] と [Custom Reports]) から選択できます。

- [Standard Reports] (標準レポート) はあらかじめ定義されているレポートであり、変更や削除はできません。標準レポートには、4 種類のヒストグラムと 4 種類のトークン リスト レポートがあります。
- [Custom Reports] (カスタム レポート) は、作成、変更、削除することができます。管理者がカスタム レポートを作成しない限り、[Custom Reports] リストには何も表示されません。

[Run List] の使い方

レポート作成ユーティリティでは、[Run List] 以外からレポートを実行することはできません。レポートを実行するには、最初にレポートを [Standard Reports] リストまたは [Custom Reports] リストから [Run List] に移動する必要があります。

- レポートを [Run List] に移動するには、[Standard Reports] リストまたは [Custom Reports] リストでレポートを反転表示し、[Add] をクリックします。CTRL キーを押しながら選択するレポートをクリックすると、複数のレポートを反転表示できます。
- [Run List] からレポートを削除するには、レポートを反転表示し、[Remove] をクリックします。[Run List] からレポートを削除すると、レポートは元のリストに戻ります。

[Run List] は、あるセッションで実行するレポートについてだけ使用することも、リストの内容を保存して、レポート作成ユーティリティを起動したときに常に同じファイルのセットを実行するようにしておくこともできます。リストを保存しないと、ユーティリティの起動時にリストは空白になります。リストを保存すると、最後に保存したときと同じファイルがリストに含まれます。

ユーティリティにはあらかじめ 8 つの標準レポートが用意されており、カスタム レポートは添付されていません。しかし、実際にユーティリティを使い始めると、多数のカスタム レポートを作成することが予想されます。作成したカスタム レポートには、使用頻度の高いものと、あまり使用しないものとがあります。[Run List] を保存しておくと、使用頻度の高いレポートを見つけやすい場所に保管できます。あまり使用しないレポートについても、[Standard Reports] リストまたは [Custom Reports] リストに残るので、紛失することがありません。

[Run List] を保存するには、[File] > [Save Run List] の順にクリックします。標準の [Run List] の内容を変更するには、新しいリストを作成し、古いリストの代わりに保存します。

レポートの [Run List] の保存

実行するレポートのリストを保存するには

[RSA Authentication Manager Reports] ダイアログ ボックスで、[File] メニューの [Save Run List] を選択します。

[Run List] に含まれるレポートのリストが保存されます。

[Run List] からレポートを実行するには

1. [From] フィールドと [To] フィールドにログ日付を入力し、実行するレポートの日付の範囲を定義します。

日付の範囲を指定しないと、ログ レコードの日付にかかわらず、関連するすべての情報が含まれるようになります。

2. 実行するレポートを選択します。
3. [Run Report(s)] をクリックします。

標準レポートの種類

ヒストグラム レポート

ヒストグラム レポートには、アクティビティの回数を 1 時間単位で示す数字が記録されます。この回数は、アクティビティのピーク値や、時間ごとの負荷を把握するのに役立ちます。出力ファイル (拡張子は .xls) を表計算ソフトにインポートして、グラフを作成することもできます。

- **[Histogram - Accepted]** … 認証が成功した回数を示します。指定された期間内の 1 時間ごとの回数です。
- **[Histogram - Attempts]** … アクセスの試みの回数 (成功した回数と失敗した回数) を示します。指定された期間内の 1 時間ごとの回数です。
- **[Histogram - Bad PASSCODE]** … PASSCODE が無効であるためにログインの試みが失敗した回数を示します。指定された期間内の 1 時間ごとの回数です。
- **[Histogram - Bad PIN]** … 正しいトークンコードと不正な PIN の組み合わせでログインの試みが失敗した回数を示します。指定された期間内の 1 時間ごとの回数です (この回数は、RSA SecurID スタンダード カードとキーホルダにだけ適用されます)。

トークン リスト レポート

次のトークン リストは、ユーザの認証に関する問題への対処に役立ちます。必要なリストを作成するには、175 ページの「トークン統計レポートの作成」の説明に従って Token Statistics Report Builder を使用してください。

- **[Token - Disabled]** … 無効な各トークンのシリアル番号、割り当てられたユーザの名前とログインを示します。
- **[Token - New PIN]** … New PIN モードの各トークンのシリアル番号、割り当てられたユーザの名前とログイン モードを示します。
- **[Token - Wait 1 Tokencode]** … ネクスト トークンコード モードのトークンのうち、すでに正しいトークンコードが 1 回入力されているトークンを示します。各トークンについて、シリアル番号、割り当てられたユーザの名前とログインを示します。
- **[Token - Wait 2 Tokencodes]** … ユーザにアクセスを許可する前に、2 つの正しいトークンコードが必要なトークンを示します。各トークンについて、シリアル番号、割り当てられたユーザの名前とログインを示します。

レポート出力ファイル

[RSA Authentication Manager Reports] ダイアログ ボックスからレポートを実行すると、その出力は 2 つのテキスト ファイルに格納されます。ファイルの 1 つは拡張子が **.txt** であり、そのままで判読できる形式です。もう 1 つのファイルは拡張子が **.xls** であり、表計算ソフトと互換性のある形式です。

標準レポートの場合、完全なファイル名はレポートの内容と形式によって決まります。たとえば、[Histogram - Attempts] の出力の完全なファイル名は、**attempts.txt** と **attempts.xls** です。各標準レポートには、あらかじめ固有の名前が定義されています。カスタム レポートの場合、ファイル名は指定する必要がありますが、拡張子はレポート作成ユーティリティが追加します。レポートの種類にかかわらず、ファイル名が他のレポートと重複しないように指定してください。

レポート出力ファイルは、***ACEUTILS*¥output** ディレクトリのサブディレクトリに格納されます。サブディレクトリが存在しない場合は自動的に作成され、***yyyymmdd*** という形式でレポートの実行日を示す名前が付けられます。同じ種類のレポートが 1 日に 2 回以上実行された場合、前の出力は最新の出力で上書きされます。

例: 2001 年 3 月 1 日に、[Run List] で [Histogram - Accepted] を反転表示し、[Run Report(s)] をクリックしたとします。**accepted.txt** と **accepted.xls** の 2 つのファイルが作成され、***ACEUTILS*¥output¥20010301** に格納されます。

カスタム レポートの作成と管理

レポート作成ユーティリティには、カスタム レポート定義のダイアログ ボックスが 3 つあります。これらのダイアログ ボックスを使用すると、新しいレポートを作成できるだけでなく、既存のレポートを編集または削除できます。

カスタム レポートを作成、編集、削除するには

1. [RSA Authentication Manager Reports] ダイアログ ボックスの [Create New Report] をクリックします。

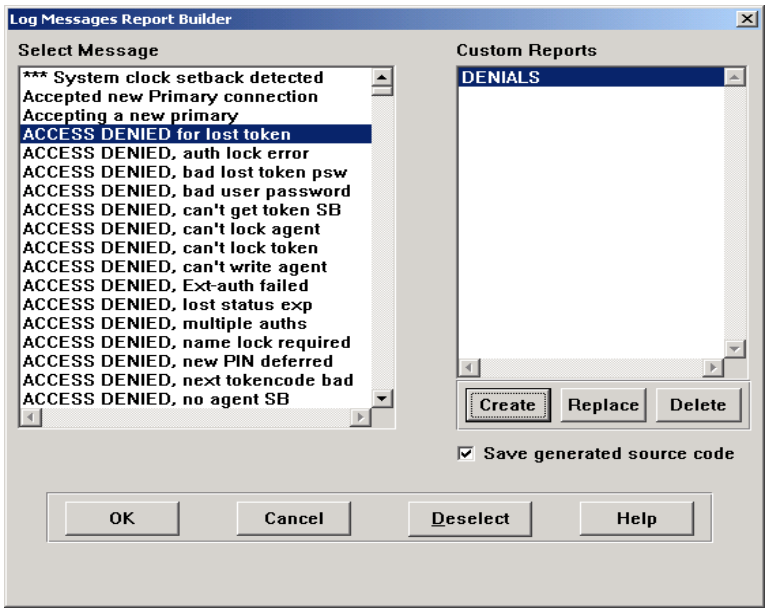
   [Select Report Type] ダイアログ ボックスが表示されます。

2. [Log Entry]、[Histogram]、[Token Statistics] のいずれかを選択します。

   選択した種類に応じて、次のいずれかのダイアログ ボックスが表示されます。

   - [Log Messages Report Builder]
   - [Log Messages Histogram Builder]
   - [Token Statistics Report Builder]

   これらのダイアログ ボックスに共通な機能として、[Custom Reports] リストがあります。このリストには、現在定義されているレポートのうち、選択した種類に含まれるすべてのカスタム レポートの名前が表示されます。例として、[Log Messages Report Builder] ダイアログ ボックスの右側を確認してください。



3. 新しいレポートの作成方法の 1 つに、既存のレポートを選択し、定義を変更する方法があります。レポートを選択すると、レポートを定義している設定が画面に表示されます (たとえば [Log Messages Report Builder] ダイアログ ボックスでは、レポートの内容として指定されたログ メッセージが [Select Message] リストで反転表示されます)。これらの設定を変更し、[Replace] をクリックすると、前の定義の代わりに新しいレポート定義を保存できます。

4. 既存のレポートを使用せずに新しいレポートを作成するには、[Create] をクリックします。新しいレポートが [Custom Reports] リストに追加されます。レポートの種類ごとの作成手順については、次の 3 つのセクションで詳しく説明します。

5. [Custom Reports] リストからレポートを削除するには、レポートを選択し、[Delete] をクリックします。

6. 作成したレポートの編集可能な 4GL コードを保存するには、[Save generated source code] チェックボックスをオンにします。

   このチェックボックスがオフの場合は、コンパイルされた 4GL コードだけが作成されます。このチェックボックスがオンの場合は、コンパイルされたコードに加え、判読と編集が可能な 4GL ソース コードが作成されます。

ログ エントリ レポートの作成

[Log Messages Report Builder] ダイアログ ボックスを使用すると、[Select Message] リストから対応するログ メッセージを選択することにより、1 つまたは複数の種類のイベントのすべてのログ レコードを含むレポートを作成できます。たとえば、トークンを無効にする RSA Authentication Manager のすべてのインスタンスを示すレポートを定義できます。また、ユーザ レコードやトークン レコードに対する変更を示す、すべてのログ レコードを含むレポートを作成することもできます。

ログ レポートには、Authentication Manager の監査証跡から取得できる詳細情報が含まれます。エントリには、イベントの発生日時、現在のユーザと影響を受けるユーザ (該当する場合)、イベントに関する 1 行の説明が示されます。

カスタム ログ エントリ レポートを定義するには

1. [RSA Authentication Manager Reports] ダイアログ ボックスの [Create Report] をクリックして、[Select Report Type] ダイアログ ボックスを表示します。
2. [Log Entry] > [OK] の順にクリックします。

   [Log Messages Report Builder] ダイアログ ボックスが表示されます。
3. [Select Message] リストで、1 つまたは複数のメッセージを選択します (メッセージの選択を取り消す場合は、そのメッセージにカーソルを置き、[Deselect] をクリックします)。

   このレポートを実行すると、指定した日付について、選択したメッセージの 1 つで示される各イベントの発生が報告されます。
4. [Create] をクリックします。

   [Create a New Report] ダイアログ ボックスが表示され、新しいレポートの説明とファイル名が要求されます。
5. レポート作成ユーティリティのユーザが新しいレポートを識別できるように、短くわかりやすい名前 (25 文字以内) を入力します。この名前は [Custom Reports] リストや [Run List] に表示されます。

   わかりやすい名前の他に、レポート出力ファイルと、レポート ソース コード ファイル (必要な場合) のファイル名を入力します (8 文字以内)。

   メモ： レポートの種類にかかわらず、他のレポートで使用されている説明やファイル名は指定しないでください。
6. [OK] をクリックします。

   [Log Messages Report Builder] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。
7. [Log Messages Report Builder] ダイアログ ボックスの [OK] をクリックします。

   [RSA Authentication Manager Reports] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

ログ アクティビティのヒストグラムの作成

ヒストグラムは、アクティビティの回数を時間単位で示したものです。このレポートには、ユーザ名やエージェント ホスト名など、イベントの詳細情報は示されません。

[Log Messages Histogram Builder] ダイアログ ボックスは、タイトル以外は [Log Messages Report Builder] ダイアログ ボックスとよく似ています。レポートの定義方法も同じです。レポートに含めるイベントは、対応するログ メッセージを選択することにより定義します。これらの 2 種類のレポートの違いは、出力の内容だけです。[Log Messages Report Builder] ダイアログ ボックスのレポートの場合は、完全で詳細なログ エントリが出力され、[Log Messages Histogram Builder] ダイアログ ボックスのレポートの場合は、統計情報が出力され、詳細情報は出力されません。

ログ アクティビティのヒストグラムを作成するには

1. [RSA Authentication Manager Reports] ダイアログ ボックスの [Create Report] をクリックして、[Select Report Type] ダイアログ ボックスを表示します。
2. [Histogram] を選択し、[OK] をクリックします。

[Log Messages Histogram Builder] ダイアログ ボックスが表示されます。

3. [Select Message] リストで、1 つまたは複数のメッセージを選択します (メッセージの選択を取り消す場合は、そのメッセージにカーソルを置き、[Deselect] をクリックします)。

   このレポートを実行すると、指定した日付について、選択したメッセージの 1 つで示される各イベントの発生回数が報告されます。

4. [Create] をクリックして新しいレポートを追加します。[Create a New Report] ダイアログ ボックスが表示されます。

5. レポート作成ユーティリティのユーザが新しいレポートを識別できるように、短くわかりやすい名前 (25 文字以内) を入力します。この名前は [Custom Reports] リストや [Run List] に表示されます。

   また、レポート出力ファイルと、レポート ソース コード ファイル (必要な場合) のファイル名を入力します (8 文字以内)。

   メモ：レポートの種類にかかわらず、他のレポートで使用されている説明やファイル名は指定しないでください。

6. [OK] をクリックします。

   [Log Messages Histogram Builder] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

7. [Log Messages Histogram Builder] ダイアログ ボックスの [OK] をクリックします。

   [RSA Authentication Manager Reports] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

トークン統計レポートの作成

トークン統計レポートは、レポート定義で指定した各カテゴリのトークンの数を示します。トークン数の他に、統計に含まれる各トークンのシリアル番号、ユーザのファースト ネームとラスト ネームも出力されます。[Token Statistics Report Builder] ダイアログ ボックスのデフォルト設定では、レルム内のすべてのトークンが含まれるようにレポートが定義されています。選択や指定によりこれらの設定を変更することで、レポートの内容をより詳細に定義したトークンのセットに制限できます。

トークン統計レポートを作成するには

1. [RSA Authentication Manager Reports] ダイアログ ボックスの [Create Report] をクリックして、[Select Report Type] ダイアログ ボックスを表示します。

2. [Token Statistics] を選択し、[OK] をクリックします。

   [Token Statistics Report Builder] ダイアログ ボックスが表示されます。

3. カスタム レポートに含めるトークンを指定するための条件を選択します。必要のない条件はクリアしてください。

   [Tokens which shut down before] … この日付より前にシャットダウンされる (有効期限が切れる) すべてのトークンがレポートに含まれます。

   [Logins which occurred after] … この日付より後に実行されたすべてのログインがレポートに含まれます。

   [Bad tokencode counts greater than] … 1 回のログインで入力された不正なトークンコードの数がこのフィールドの値を超えると、イベントがレポートに含まれます。

[Bad PIN counts greater than] … 1 回のログインで入力された不正な PIN の数がこのフィールドの値を超えると、イベントがレポートに含まれます。

[Token type] … このレポートに含める 1 つまたは複数のトークン タイプを選択します。

[Token Enabled]、**[New PIN Mode]**、**[Token Lost]**、**[Next Tokencode Status]** … このレポートに含める項目をクリックします。

4. [Create] をクリックします。

   新しいレポートの説明とファイル名を入力します。

5. レポート作成ユーティリティのユーザが新しいレポートを識別できるように、短くわかりやすい名前 (25 文字以内) を入力します。この名前は [Custom Reports] リストや [Run List] に表示されます。

   また、レポート出力ファイルと、レポート ソース コード ファイル (必要な場合) のファイル名を入力します (8 文字以内)。

   メモ：レポートの種類にかかわらず、他のレポートで使用されている説明やファイル名は指定しないでください。

6. [OK] をクリックします。

   [Token Statistics Report Builder] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

7. [Token Statistics Report Builder] ダイアログ ボックスの [OK] をクリックします。

   [RSA Authentication Manager Reports] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

ユーザ情報の表示

ユーザ情報を表示するには

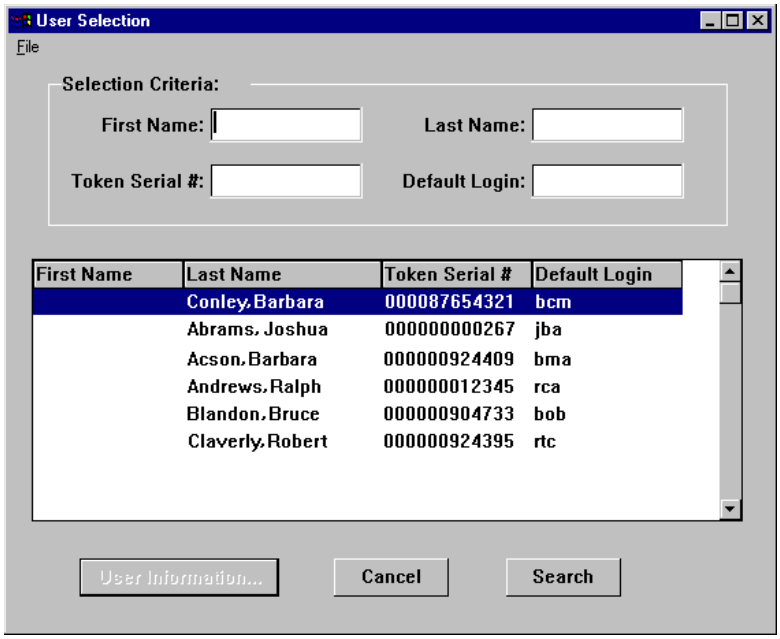
1. [RSA Authentication Manager Reports] ダイアログ ボックスで、[Users] メニューの [User Information] をクリックします。

   [User Selection] ダイアログ ボックスが表示され、ユーザ リストにエントリが表示されます。

2. リストからユーザを探すには、ダイアログ ボックスの上部の選択条件フィールドに情報を入力します。

3. [User Information] をクリックして、選択したユーザに関する情報を表示します。

[User Information] ダイアログ ボックスが表示され、選択したユーザに関する詳細情報が表示されます。



コマンド ラインからのレポートの実行

コマンド ラインからレポートを実行するには、**rptrun** ユーティリティを使用します。**rptrun** の最初の引数には、レポートの 4GL コードの完全なパスとファイル名を指定する必要があります。標準レポートの 4GL コードへのパスは ***ACEUTILS*¥std_rpt** で、カスタム レポートの 4GL コードへのパスは ***ACEUTILS*¥cust_rpt** です。カスタム レポートの 4GL コードのファイル名は、レポートの作成時に指定した名前の後に .p という拡張子を追加したものです。

開始日と終了日を指定するコマンド ライン引数

rptrun コマンドに開始日と終了日を指定すると、ログ レポートとヒストグラムは、監査証跡全体ではなく、指定された期間だけが対象になります。たとえば、次のコマンドを使用すると、2001 年 9 月に成功したログインの試みを示す標準レポートが作成されます。

```
rptrun ACEUTILS¥std_rpt¥accepted.p 09/01/2001 09/30/2001
```

トークンの有効期限と最終ログイン日を指定するコマンド ライン引数

rptrun ユーティリティを使用してトークン統計レポートを実行する場合は、4GL コードのパスとファイル名の後に 2 つの引数を入力する必要があります。最初の引数はトークンの有効期限で、2 番目の引数は最終ログイン日です。有効期限と最終ログイン日がレポートの選択条件ではない場合も、これらの日付を入力する必要があります (レポートに日付が不要な場合は無視されます)。有効期限の日付が選択条件の場合は、この日付またはそれより前に有効期限が切れるトークンが選択されます。最終ログイン日が選択条件の場合は、この日付またはそれより後に認証に使用されたトークンが選択されます。

コマンドの構文は次のとおりです。

```
rptrun full_path expiration_date last_login_date
```

たとえば、次のコマンドでは、日付は選択条件ではありません。

```
rptrun ACEUTILS¥std_rpt¥disabled.p 01/01/2001 01/01/2001
```

次のコマンドでは、トークンの有効期限は選択条件です。

```
rptrun ACEUTILS¥cust_rpt¥expire.p 01/31/1999 01/01/2003
```

RSA Authentication Manager レポート作成ユーティリティ (UNIX)

RSA Authentication Manager ソフトウェアに含まれるレポート作成ユーティリティを使用すると、**sdlog** データベースに対して監査証跡レポートを作成および実行し、**sdserv** データベースに対してトークン統計レポートを作成および実行できます。このユーティリティには、選択したユーザに対応するユーザ レコードから、その情報を取得して画面に表示する機能もあります。

UNIX インタフェースの基本操作

レポート作成ユーティリティは、UNIX システムのキャラクタ モード (TTY モード) で動作します。インタフェースの基本操作は次のとおりです。

- メニュー バーをアクティブにするには、F3 キーまたは PF3 キーを押します。
- メニュー バーがアクティブになったら、矢印キーを使用するか、またはメニュー タイトル内の下線付きの文字を入力することで、メニュー間を移動できます。
- メニューがアクティブになり、表示されたら、オプション名の下線付きの文字を入力するか、または矢印キーでオプションに移動し、RETURN キーを押してオプションを選択します。
- オプション ボックスでは、アクションは現在アクティブなボックス領域の内部でのみ、キーを押すことによって開始できます。フォーカス領域は長方形で反転表示されます。
- オプション ボックスのある領域から、順方向の別の領域に移動するには、TAB キーを押します。逆方向に移動するには、CTRL+U キーを押します。
- 領域内のアイテムから別のアイテムに移動するには、矢印キーを押します。
- リスト アイテムを反転表示するには、矢印キーを使用します。
- リスト アイテム、オプション ボタン、チェックボックスを選択するには、スペース バーまたは RETURN キーを押します。
- チェックボックスまたはオプション ボタンが反転表示されている場合は、RETURN キーを押してオンとオフを切り替えることができます。
- コマンド ボタンが反転表示されている場合は、RETURN キーを押すと、アクションが実行されます。他のボタンが反転表示されていない場合は、RETURN キーを押すと、デフォルト ボタンに関連付けられているアクションが実行されます (デフォルト ボタンは [OK] であることが多く、ダイアログ ボックスが閉じることがあります)。
- ボックスで RETURN キーを押す操作は、TAB キーを押す操作と同じです。この操作を行うと、カーソルがフィールドの外に移動します。
- [Cancel] を選択するか、F4 キーまたは PF4 キーを押すと、保存していないダイアログ ボックスでの変更内容は取り消され、ダイアログ ボックスが閉じます。
- ESC キーを使用してボックスを閉じることはできません。

- 日付フィールドで BACKSPACE キーを使用しても、カーソルが移動するだけです。日付フィールドを変更するには、フィールドの内容を上書きします。
- アクティブではないボタンもアクティブなボタンと同じように表示されますが、アクティブになっていない限り、カーソルをそのボタンに移動することはできません。

レポート作成ユーティリティのインストール

レポート作成ユーティリティ ソフトウェアは、RSA Authentication Manager をインストールするときに ***ACEUTILS*** ディレクトリにコピーされます。

これまでレポート作成ユーティリティを使用していて、アップグレードする場合は、次の手順に従ってレポート作成ユーティリティのデータベースおよび作成したカスタム レポートを復元してください。

- カスタム レポート出力ファイルを復元するには、**ace_tmp/utils/cust_rpt** ディレクトリのファイルを ***ACEUTILS*/cust_rpt** にコピーします。
- データベースを復元するには、**ace_tmp/utils** ディレクトリの **sdrpt.db** を ***ACEUTILS*** ディレクトリにコピーします。

レポート作成ユーティリティの起動と停止

レポート作成ユーティリティを起動するには

1. プライマリで RSA Authentication Manager データベース ブローカが実行されていることを確認します。データベース ブローカが実行されていない場合は、次のように入力して起動します。

   ```
   ACEPROG/sdconnect start
   ```

2. 次のように入力して、レポート データベース サーバを起動します。

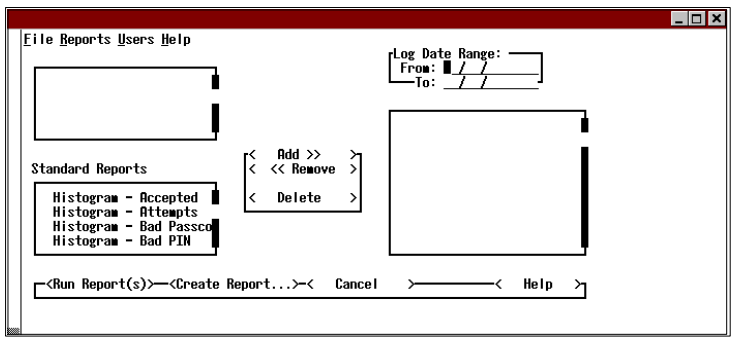
   ```
   ACEUTILS/rptconnect start
   ```

3. 次のように入力して、レポート作成ユーティリティを実行します。

   ```
   ACEUTILS/sdreport
   ```

メモ: レポート作成ユーティリティは、バッチ モードで実行することもできます。レポート作成ユーティリティをバッチ モードで実行する場合には、[RSA Authentication Manager Reports] ダイアログ ボックスは表示されません。バッチ モードでデータベースに接続するには、「ACEUTILS/rptconnect start batch」と入力してください。

[RSA Authentication Manager Reports] ダイアログ ボックスが表示されます。



レポート作成ユーティリティを停止するには

1. F3 キーを押して [RSA Authentication Manager Reports] ダイアログ ボックスのメニュー バーをアクティブにします。
2. 「F」と入力して [File] メニューを表示し、「x」と入力して [Exit] を選択します。
3. コマンド プロンプトで次のように入力して、レポート データベース サーバを停止します。

```
ACEUTILS/rptconnect stop
```

重要：この方法でレポート作成ユーティリティを停止しないと、ユーティリティはロックされ、***ACEUTILS*/sdrpt.lk** というロック ファイルが作成されます。その場合は、ロック ファイルを削除して、もう一度操作を実行してください。

実行するレポートの選択

[RSA Authentication Manager Reports] ダイアログ ボックスでは、レポートを 2 つのリスト ([Standard Reports] と [Custom Reports]) から選択できます。

- [Standard Reports] (標準レポート) はあらかじめ作成されているレポートであり、変更や削除はできません。標準レポートには、4 種類のヒストグラム レポートと 4 種類のトークン リスト レポートがあります。
- [Custom Reports] (カスタム レポート) は、作成、変更、削除することができます。管理者がカスタム レポートを作成しない限り、[Custom Reports] リストには何も表示されません。

[Run List] の使い方

レポート作成ユーティリティでは、[Run List] 以外からレポートを実行することはできません。レポートを実行するには、最初にレポートを [Standard Reports] リストまたは [Custom Reports] リストから [Run List] に移動する必要があります。

- レポートを [Run List] に移動するには、[Standard Reports] リストまたは [Custom Reports] リストでレポートを反転表示し、[Add] をクリックします。CTRL キーを押しながら選択するレポートをクリックすると、複数のレポートを反転表示できます。
- [Run List] からレポートを削除するには、レポートを反転表示し、[Remove] をクリックします。[Run List] からレポートを削除すると、レポートは元のリストに戻ります。

[Run List] は、あるセッションで実行するレポートについてだけ使用することも、リストの内容を保存して、レポート作成ユーティリティを起動したときに常に同じファイルのセットを実行するようにしておくこともできます。リストを保存しないと、ユーティリティの起動時にリストは空白になります。リストを保存すると、最後に保存したときと同じファイルがリストに含まれます。

ユーティリティにはあらかじめ 8 つの標準レポートが用意されており、カスタム レポートは添付されていません。しかし、実際にユーティリティを使い始めると、多数のカスタム レポートを作成することが予想されます。作成したカスタム レポートには、使用頻度の高いものと、あまり使用しないものとがあります。[Run List] を保存しておくと、使用頻度の高いレポートを見つけやすい場所に保管できます。あまり使用しないレポートについても、[Standard Reports] リストまたは [Custom Reports] リストに残るので、紛失することがありません。

[Run List] を保存するには、[File] > [Save Run List] の順にクリックします。標準の [Run List] の内容を変更するには、新しいリストを作成し、古いリストの代わりに保存します。

[Run List] からレポートを実行するには

1. [From] フィールドと [To] フィールドにログ日付を入力し、実行するレポートの日付の範囲を定義します。
   日付の範囲を指定しないと、ログ レコードの日付にかかわらず、関連するすべての情報が含まれるようになります。
2. 実行するレポートを反転表示します。
3. [Run Report(s)] を選択します。

標準レポートの種類

ヒストグラム レポート

ヒストグラム レポートには、アクティビティの回数を 1 時間単位で示す数字が記録されます。この回数は、アクティビティのピーク値や、時間ごとの負荷を把握するのに役立ちます。出力ファイル (拡張子は .xls) を表計算ソフトにインポートして、グラフを作成することもできます。

- **[Histogram - Accepted]** … 認証が成功した回数を示します。指定された期間内の 1 時間ごとの回数です。
- **[Histogram - Attempts]** … アクセスの試みの回数 (成功した回数と失敗した回数) を示します。指定された期間内の 1 時間ごとの回数です。
- **[Histogram - Bad PASSCODE]** … PASSCODE が無効であるためにログインの試みが失敗した回数を示します。指定された期間内の 1 時間ごとの回数です。
- **[Histogram - Bad PIN]** … 正しいトークンコードと不正な PIN の組み合わせでログインの試みが失敗した回数を示します。指定された期間内の 1 時間ごとの回数です (この回数は、RSA SecurID スタンダード カードとキーホルダにだけ適用されます)。

トークン リスト レポート

次のトークン リストは、ユーザの認証に関する問題への対処に役立ちます。必要なリストを作成するには、185 ページの「トークン統計レポートの作成」の説明に従って Token Statistics Report Builder を使用してください。

- **[Token - Disabled]** … 無効な各トークンのシリアル番号、割り当てられたユーザの名前とログインを示します。
- **[Token - New PIN]** … New PIN モードの各トークンのシリアル番号、割り当てられたユーザの名前とログイン モードを示します。
- **[Token - Wait 1 Tokencode]** … ネクスト トークンコード モードのトークンのうち、すでに正しいトークンコードが 1 回入力されているトークンを示します。各トークンについて、シリアル番号、割り当てられたユーザの名前とログインを示します。
- **[Token - Wait 2 Tokencodes]** … ユーザにアクセスを許可する前に、2 つの正しいトークンコードが必要なトークンを示します。各トークンについて、シリアル番号、割り当てられたユーザの名前とログインを示します。

レポート出力ファイル

[RSA Authentication Manager Reports] ダイアログ ボックスからレポートを実行すると、その出力は 2 つのテキスト ファイルに格納されます。ファイルの 1 つは拡張子が **.txt** であり、そのままで判読できる形式です。もう 1 つのファイルは拡張子が **.xls** であり、表計算ソフトと互換性のある形式です。

標準レポートの場合、完全なファイル名はレポートの内容と形式によって決まります。たとえば、[Histogram - Attempts] の出力の完全なファイル名は、**attempts.txt** と **attempts.xls** です。各標準レポートには、あらかじめ固有の名前が定義されています。カスタム レポートの場合、ファイル名は指定する必要がありますが、拡張子はレポート作成ユーティリティが追加します。レポートの種類にかかわらず、ファイル名が他のレポートと重複しないように指定してください。

レポート出力ファイルは、***ACEUTILS*/output** ディレクトリのサブディレクトリに格納されます。サブディレクトリが存在しない場合は自動的に作成され、***yyyymmdd*** という形式でレポートの実行日を示す名前が付けられます。同じ種類のレポートが 1 日に 2 回以上実行された場合、前の出力は最新の出力で上書きされます。

例：01.03.05 に、[Run List] で [Histogram - Accepted] を反転表示し、[Run Report(s)] をクリックしたとします。**accepted.txt** と **accepted.xls** の 2 つのファイルが作成され、***ACEUTILS*/output/20050301** に格納されます。

カスタム レポートの作成と管理

レポート作成ユーティリティには、カスタム レポート ダイアログ ボックスが 3 つあります。これらのダイアログ ボックスを使用すると、新しいレポートを作成できるだけでなく、既存のレポートを編集または削除できます。

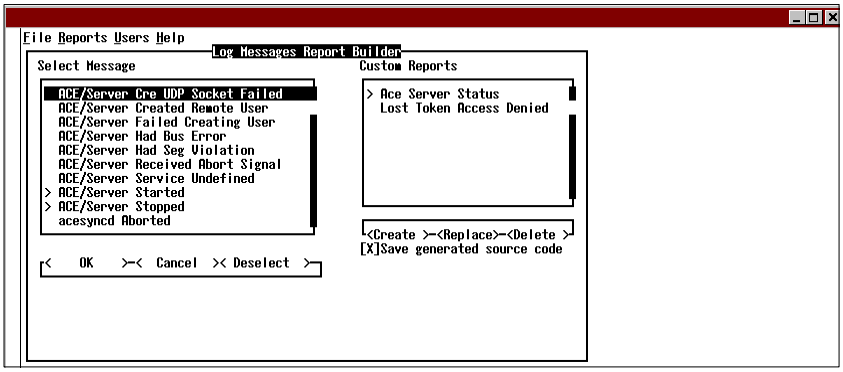
カスタム レポートを作成、編集、削除するには

1. F3 キーを押して [RSA Authentication Manager Reports] ダイアログ ボックスのメニュー バーをアクティブにし、「R」と入力して [Reports] メニューを表示します。
2. [Create New Report] を選択し、RETURN キーを押します。

   [Select Report Type] ダイアログ ボックスが表示されます。
3. [Log Entry]、[Histogram]、[Token Statistics] のいずれかを選択します。

   選択した種類に応じて、次のいずれかのダイアログ ボックスが表示されます。
   - [Log Messages Report Builder]
   - [Log Messages Histogram Builder]
   - [Token Statistics Report Builder]

これらのダイアログ ボックスに共通な機能として、[Custom Reports] リストがあります。このリストには、現在定義されているレポートのうち、選択した種類に含まれるすべてのカスタム レポートの名前が表示されます。例として、[Log Messages Report Builder] ダイアログ ボックスの右側を確認してください。



4. 新しいレポートの作成方法の 1 つに、既存のレポートを選択し、定義を変更する方法があります。レポートを選択すると、レポートを定義している設定が画面に表示されます (たとえば [Log Messages Report Builder] ダイアログ ボックスでは、レポートの内容として指定されたメッセージが [Select Message] リストで反転表示されます)。これらの設定を変更し、[Replace] を選択すると、前の定義の代わりに新しいレポート定義を保存できます。
5. 既存のレポートを使用せずに新しいレポートを作成するには、[Create] を選択します。新しいレポートが [Custom Reports] リストに追加されます。レポートの種類ごとの作成手順については、次の 3 つのセクションで詳しく説明します。
6. [Custom Reports] リストからレポートを削除するには、レポートを反転表示し、[Delete] を選択します。
7. 作成したレポートの編集可能な 4GL コードを保存するには、TAB キーを押して [Save generated source code] ボックスに移動し、RETURN キーを押してマークします。

   このボックスがマークされていない場合は、コンパイルされた 4GL コードだけが作成されます。このボックスがマークされている場合は、コンパイルされたコードに加え、判読と編集が可能な 4GL ソース コードが作成されます。

ログ エントリ レポートの作成

[Log Messages Report Builder] ダイアログ ボックスを使用すると、[Select Message] リストから対応するログ メッセージを選択することにより、1 つまたは複数の種類のイベントのすべてのログ レコードを含むレポートを作成できます。たとえば、トークンを無効にする RSA Authentication Manager のすべてのインスタンスを示すレポートを定義できます。また、ユーザ レコードやトークン レコードに対する変更を示す、すべてのログ レコードを含むレポートを作成することもできます。

ログ レポートには、Authentication Manager の監査証跡から取得できる詳細情報が含まれます。エントリには、イベントの発生日時、現在のユーザと影響を受けるユーザ (該当する場合)、イベントに関する 1 行の説明が示されます。

カスタム ログ エントリ レポートを定義するには

1. F3 キーを押して [RSA Authentication Manager Reports] ダイアログ ボックスのメニュー バーをアクティブにし、「R」と入力して [Reports] メニューを表示します。
2. [Create New Report] を選択し、RETURN キーを押します。

[Select Report Type] ダイアログ ボックスが表示されます。

3. [Log Entry] を選択し、[OK] を選択します。

   [Log Messages Report Builder] ダイアログ ボックスが表示されます。

4. [Select Message] リストで、レポートに含めるメッセージを反転表示し、RETURN キーを押して選択します。メッセージを追加するには、この手順を繰り返します。

   このレポートを実行すると、指定した日付について、選択したメッセージの 1 つで示される各イベントの発生回数が報告されます。

5. 必要なメッセージをすべて選択したら、[Select Message] リストの下の [OK] を反転表示し、RETURN キーを押します。

6. [Custom Reports] リストの下の [Create] を反転表示し、RETURN キーを押します。

   [Create a New Report] ダイアログ ボックスが表示され、新しいレポートの説明とファイル名が要求されます。

7. レポート作成ユーティリティのユーザが新しいレポートを識別できるように、短くわかりやすい名前 (25 文字以内) を入力します。この名前は [Custom Reports] リストや [Run List] に表示されます。

   わかりやすい名前の他に、レポート出力ファイルと、レポート ソース コード ファイル (必要な場合) のファイル名を入力します (8 文字以内)。

   メモ：レポートの種類にかかわらず、他のレポートで使用されている説明やファイル名は指定しないでください。

8. [OK] を選択し、RETURN キーを押します。

   [Log Messages Report Builder] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

9. [Log Messages Report Builder] ダイアログ ボックスの [OK] を選択し、RETURN キーを押します。

   [RSA Authentication Manager Reports] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

ログ アクティビティのヒストグラムの作成

ヒストグラムは、アクティビティの回数を時間単位で示したものです。このレポートには、ユーザ名やエージェント ホスト名など、イベントの詳細情報は示されません。

[Log Messages Histogram Builder] ダイアログ ボックスは、タイトル以外は [Log Messages Report Builder] ダイアログ ボックスと同じです。レポートの定義方法も同じです。レポートに含めるイベントは、対応するログ メッセージを選択することにより定義します。これらの 2 種類のレポートの違いは、出力の内容だけです。[Log Messages Report Builder] ダイアログ ボックスのレポートの場合は、完全で詳細なログ エントリが出力され、[Log Messages Histogram Builder] ダイアログ ボックスのレポートの場合は、統計情報が出力され、詳細情報は出力されません。

ログ アクティビティのヒストグラムを作成するには

1. F3 キーを押して [RSA Authentication Manager Reports] ダイアログ ボックスのメニュー バーをアクティブにし、「R」と入力して [Reports] メニューを表示します。

2. [Create New Report] を選択し、RETURN キーを押します。

   [Select Report Type] ダイアログ ボックスが表示されます。

3. [Histogram] を選択し、[OK] を選択します。

   [Log Messages Histogram Builder] ダイアログ ボックスが表示されます。

4. TAB キーを押して [Select Message] リストに移動します。

5. 矢印キーを押してメッセージを反転表示し、RETURN キーを押してメッセージを選択します。複数のメッセージを選択するには、選択する各メッセージについてこの手順を繰り返します。

   選択した各メッセージの発生回数がレポートに出力されます。

6. 必要なメッセージをすべて選択したら、[Select Message] リストの下の [OK] を反転表示し、RETURN キーを押します。

7. [Custom Reports] リストの下の [Create] を反転表示し、RETURN キーを押します。

   [Create a New Report] ダイアログ ボックスが表示され、新しいレポートの説明とファイル名が要求されます。

8. レポート作成ユーティリティのユーザが新しいレポートを識別できるように、短くわかりやすい名前 (25 文字以内) を入力します。この名前は [Custom Reports] リストや [Run List] に表示されます。

   わかりやすい名前の他に、レポート出力ファイルと、レポート ソース コード ファイル (必要な場合) のファイル名を入力します (8 文字以内)。

   メモ：レポートの種類にかかわらず、他のレポートで使用されている説明やファイル名は指定しないでください。

9. [OK] を選択し、RETURN キーを押します。

   [Log Messages Histogram Builder] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

10. [Log Messages Histogram Builder] ダイアログ ボックスの [OK] を選択し、RETURN キーを押します。

    [RSA Authentication Manager Reports] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

トークン統計レポートの作成

トークン統計レポートは、レポート定義で指定した各カテゴリのトークンの数を示します。トークン数の他に、統計に含まれる各トークンのシリアル番号、ユーザのファースト ネームとラスト ネームも出力されます。[Token Statistics Report Builder] ダイアログ ボックスのデフォルト設定では、レルム内のすべてのトークンが含まれるようにレポートが定義されています。選択や指定によりこれらの設定を変更することで、レポートの内容をより詳細に定義したトークンのセットに制限できます。

トークン統計レポートを作成するには

1. F3 キーを押して [RSA Authentication Manager Reports] ダイアログ ボックスのメニュー バーをアクティブにし、「R」と入力して [Reports] メニューを表示します。

2. [Create New Report] を選択し、RETURN キーを押します。

   [Select Report Type] ダイアログ ボックスが表示されます。

3. [Token Statistics] を選択し、[OK] を選択します。

   [Token Statistics Report Builder] ダイアログ ボックスが表示されます。

4. カスタム レポートに含める選択条件を指定します。

   [Tokens which shut down before] … この日付より前にシャットダウンされる(有効期限が切れる) すべてのトークンがレポートに含まれます。

   [Logins which occurred after] … この日付より後に実行されたすべてのログインがレポートに含まれます。

   [Bad tokencode counts greater than] … 1 回のログインで入力された不正なトークンコードの数がこのフィールドの値を超えると、イベントがレポートに含まれます。

   [Bad PIN counts greater than] … 1 回のログインで入力された不正な PIN の数がこのフィールドの値を超えると、イベントがレポートに含まれます。

   [Token type] … このレポートに含める 1 つまたは複数のトークン タイプをマークします。トークン タイプの詳細については、14 ページの「RSA SecurID トークンと二要素認証」を参照してください。

   [Token Enabled]、**[New PIN Mode]**、**[Token Lost]**、**[Next Tokencode Status]** … このレポートに含める項目をマークします。

5. すべてのレポート条件を指定したら、選択した項目の下に表示されている [OK] を選択し、RETURN キーを押します。

6. [Custom Reports] リストの下の [Create] を選択し、RETURN キーを押します。

   新しいレポートの説明とファイル名を入力するように要求されます。

7. レポート作成ユーティリティのユーザが新しいレポートを識別できるように、短くわかりやすい名前 (25 文字以内) を入力します。この名前は [Custom Reports] リストや [Run List] に表示されます。

   わかりやすい名前の他に、レポート出力ファイルと、レポート ソース コード ファイル (必要な場合) のファイル名を入力します (8 文字以内)。

   メモ：レポートの種類にかかわらず、他のレポートで使用されている説明やファイル名は指定しないでください。

8. [OK] を選択し、RETURN キーを押します。

   [Token Statistics Report Builder] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

9. [Token Statistics Report Builder] ダイアログ ボックスの [OK] を選択し、RETURN キーを押します。

   [RSA Authentication Manager Reports] ダイアログ ボックスの [Custom Reports] リストに新しいレポートが表示されます。

ユーザ情報の表示

ユーザ情報を表示するには

F3 キーを押して [RSA Authentication Manager Reports] ダイアログ ボックスのメニューバーをアクティブにし、「U」と入力して [Users] メニューを表示します。

1. [User Information] を選択し、RETURN キーを押します。

   [User Selection] ダイアログ ボックスが表示され、[User] リストにエントリが表示されます。

2. リストからユーザを探すには、ダイアログ ボックスの上部の選択条件フィールドに情報を入力します。

3. 選択したユーザのデータを表示するには、[User Information] を選択し、RETURN キーを押します。

   [User Information] ダイアログ ボックスが表示され、選択したユーザに関する詳細情報 (ファースト ネームとラスト ネーム、トークンのシリアル番号など) が表示されます。

コマンド ラインからのレポートの実行

コマンド ラインからレポートを実行するには、**rptrun** ユーティリティを使用します。**rptrun** の最初の引数には、レポートの 4GL コードの完全なパスとファイル名を指定する必要があります。標準レポートの 4GL コードへのパスは ***ACEUTILS*/std_rpt** で、カスタム レポートの 4GL コードへのパスは ***ACEUTILS*/cust_rpt** です。カスタム レポートの 4GL コードのファイル名は、レポートの作成時に指定した名前の後に .p という拡張子を追加したものです。

開始日と終了日を指定するコマンド ライン引数

rptrun コマンドに開始日と終了日を指定すると、ログ レポートとヒストグラムでは、監査証跡全体ではなく指定された期間だけが対象になります。たとえば、次のコマンドを使用すると、2005 年 1 月に成功したログインの試みを示す標準レポートが作成されます。

```
rptrun ACEUTILS/std_rpt/accepted.p 01/01/2005 01/31/2005
```

トークンの有効期限と最終ログイン日を指定するコマンド ライン引数

rptrun ユーティリティを使用してトークン統計レポートを実行する場合は、4GL コードのパスとファイル名の後に 2 つの引数を入力する必要があります。最初の引数はトークンの有効期限で、2 番目の引数は最終ログイン日です。有効期限と最終ログイン日がレポートの選択条件ではない場合も、これらの日付を入力する必要があります (レポートに日付が不要な場合は無視されます)。有効期限の日付が選択条件の場合は、この日付またはそれより前に有効期限が切れるトークンが選択されます。最終ログイン日が選択条件の場合は、この日付またはそれより後に認証に使用されたトークンが選択されます。

コマンドの構文は次のとおりです。

```
rptrun full_path expiration_date last_login_date
```

たとえば、次のコマンドでは、日付は選択条件ではありません。

```
rptrun ACEUTILS/std_rpt/disabled.p 01/01/1999 01/01/2003
```

次のコマンドでは、トークンの有効期限は選択条件です。

```
rptrun ACEUTILS/cust_rpt/expire.p 01/31/1999 01/01/2003
```

カスタム SQL クエリの作成と実行

RSA Authentication Manager では、データを Progress Software 社のリレーショナル データベース管理システム (RDBMS) で管理しています。**sdserv** (ユーザ データベース) と **sdlog** (監査ログ データベース) の 2 つのデータベースを使用できます。

カスタム クエリを使用すると、SQL (Structured Query Language) でデータベースにクエリを発行し、データを CSV、HTML、または XML ファイルに出力するように指定できます。サードパーティのソフトウェアを使用して、データをインポートし、各種の便利なレポートを作成することもできます。

SQL の使用経験がない場合も、RSA Authentication Manager に付属のサンプル クエリを実行できます。

SQL の使用経験がある場合は、独自のクエリを作成して、RSA Authentication Manager データベースに対して実行できます。組織の要望に合わせて、徐々にカスタム クエリのライブラリを構築していくことも可能です。

メモ: セキュリティ上の理由から、カスタム クエリを作成およびコンパイルし、必要に応じて共有できるのは、レルム管理者に限られています。詳細については、200 ページの「カスタム クエリのアドミニストレーション スコープ」を参照してください。

カスタム クエリ ツールの基本的な使い方

このセクションでは、RSA Authentication Manager に用意されているサンプル クエリをコンパイル、実行、および管理するための基本的な方法について説明します。

SQL の使用経験がある場合は、カスタム クエリを開発する方法について、190 ページの「カスタム クエリの作成と編集」と、191 ページの「カスタム クエリの SQL 構文と記述方法」を参照してください。

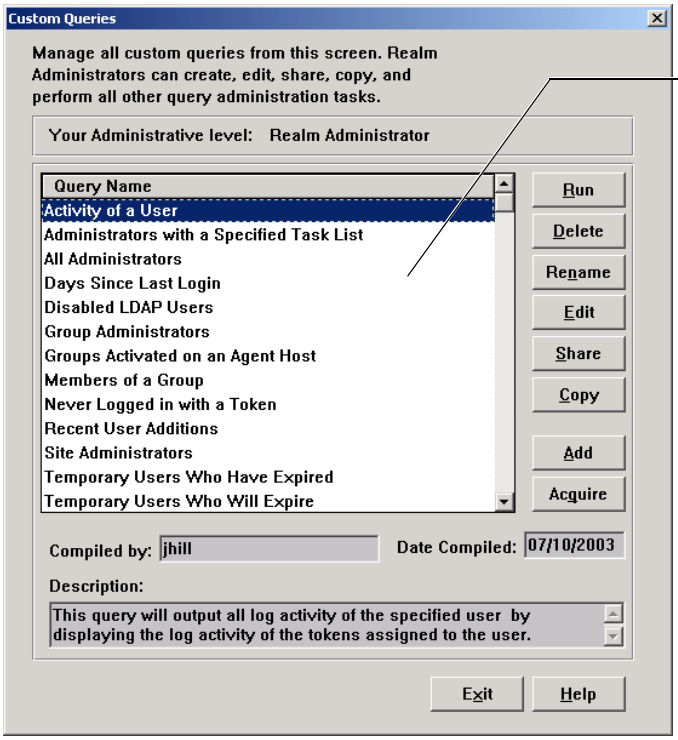
カスタム クエリ ツールは、RSA Authentication Manager Host Mode から利用できます。

操作手順:

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Host Mode] (または [RSA Authentication Manager Remote Mode] の順にクリックします。
2. [Report] > [Custom Queries] の順に選択します。

   [Custom Queries] ダイアログ ボックス (189 ページを参照) が表示されます。このダイアログ ボックスから、RSA Authentication Manager でのカスタム クエリのあらゆるアクティビティを管理できます。

メモ : カスタム クエリのいずれのダイアログ ボックスでも、[Help] をクリックすると、状況依存のヘルプや操作手順の情報を参照できます。



アドミニストレーション レベルとクエリ権限

セキュリティ上の理由から、クエリの作成、編集、共有など、カスタム クエリ ツールの全機能にアクセスできるのは、レルム管理者のみに制限されています。

サイト管理者またはグループ管理者が [Custom Queries] コマンドを実行すると、その管理者のアドミニストレーション レベルが検知され、別バージョンの [Custom Queries] ダイアログ ボックスが表示されます。このバージョンでは、[Acquire]、[Run]、[Rename]、および [Delete] の 4 つのオプションのみを利用できます。

また、サイト管理者およびグループ管理者は、共有クエリのリストから入手したクエリ以外は実行できません。

セキュリティ上の理由から、スコープ機能によってレルム管理者が共有クエリの実行に必要なアドミニストレーション レベル (レルム、サイト、またはグループ) を指定できるようになっています。詳細については、200 ページの「カスタム クエリのアドミニストレーション スコープ」を参照してください。

サンプル クエリの使い方

レルム管理者の場合、コンパイルされていないサンプル クエリが [Custom Queries] ダイアログ ボックスに表示されます。このサンプル クエリはコンパイル、コピー、編集、実行、および共有できます。

サンプル クエリを使用するには、最初にコンパイルする必要があります。リスト上でクエリを選択し、[Edit] をクリックします。次に、その後に表示される各ダイアログ ボックスの指示に従って操作します。コンパイルが終了すると、クエリが実行環境にバインドされ、レルム内でのみ使用できるようになります (詳細については、190 ページの「クエリの編集」を参照してください。複数のレルムがある場合は、205 ページの「複数のレルム間でのクエリの管理」を参照してください)。

メモ : サンプル クエリの一覧と説明については、ヘルプを参照してください。サンプル クエリを修正する場合は、最初にサンプル クエリをコピーし、コピーに対して修正を加えることをお勧めします。

カスタム クエリの作成と編集

SQL の使用経験があるレルム管理者は、目的に合わせてカスタム クエリを作成したり、既存のクエリを編集できます。

クエリの新規作成

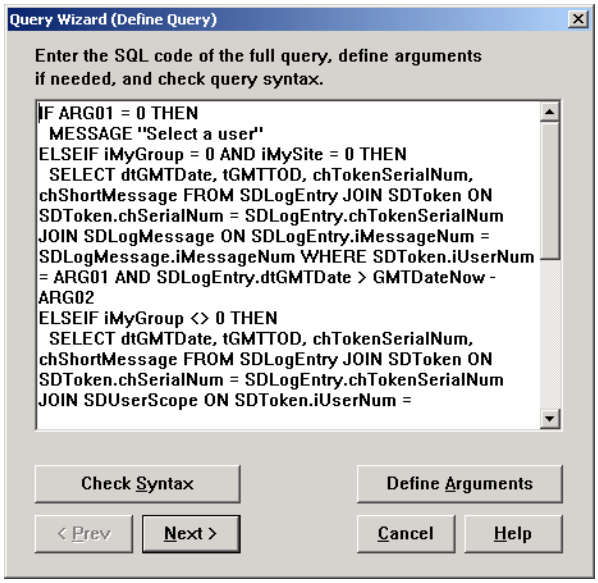
新しいクエリを作成するには、[Add] ボタンを使用します。Query Wizard の指示に従って操作を進めます。

操作手順 : [Report] > [Custom Queries] > [Add] の順にクリックします。[Query Wizard (Query Name)] ダイアログ ボックスが表示されます。各手順の詳細については、ヘルプを参照してください。

詳細については、191 ページの「カスタム クエリの SQL 構文と記述方法」および 200 ページの「カスタム クエリに関する高度なアプリケーション ノート」を参照してください。

クエリの編集

レルム管理者以外は、[Edit] (編集) オプションを使用できません (189 ページの「アドミニストレーション レベルとクエリ権限」を参照)。[Custom Queries] でクエリの名前を選択し、[Edit] をクリックします。Query Wizard の [Define Query] 画面が表示されます。



SQL コードとクエリの引数の編集が終了したら、構文を確認し、Query Wizard の残りの操作を完了します。

関連情報については、次のセクション「カスタム クエリの SQL 構文と記述方法」と、200 ページの「カスタム クエリに関する高度なアプリケーション ノート」を参照してください。

カスタム クエリの SQL 構文と記述方法

このセクションでは、カスタム クエリでの SQL の使い方について説明し、正しい構文の例として多くの SQL コードを示します。RSA Authentication Manager に用意されているサンプル クエリを参照し、内容を理解しておくことをお勧めします。

データベース スキーマ

RSA Authentication Manager データベースは、相互に関連するテーブルのセットである**スキーマ**として構成されています。カスタム クエリの機能を効果的に使用するには、スキーマ テーブルの名前と、含まれているデータについて把握しておく必要があります。

たとえば、**SDUser** テーブルには、データベースに定義されている各ユーザに関連する 30 以上のフィールドが含まれています。ファースト ネームとラスト ネーム (**chFirstName**、**chLastName**)、ログイン (**chDefaultLogin**) などのフィールドがあります。**SDUser** テーブルは、RSA Authentication Manager のデータベース スキーマに 100 以上存在するテーブルのうちの 1 つです。

メモ : すべてのスキーマ テーブルとその内容に関する総合的な情報については、ヘルプを参照してください。また、『Administration Toolkit Reference Guide』(**authmgr_admin_toolkit.pdf**) でもスキーマについて説明しています。

クエリの長さと構文に関する一般的な規則

カスタム クエリの場合、クエリが有効であるためには、次の条件を満たしている必要があります。

- 必ず **SELECT** ステートメントが含まれている必要があります。詳細については、次のセクション「SELECT ステートメントの構文」を参照してください。
- 1 つのクエリに指定できるステートメントの数は 32 までです。また、クエリの長さは 4,096 バイト以内である必要があります。
- 1 つのクエリに複数の **SELECT** ステートメントを指定する場合は、そのすべてが同じフィールド セットを同じ順番で返す必要があります。複数の SELECT ステートメントで選択されたフィールドが、同一であることもあります。逆に、名前と種類が同じで、文字フィールドの場合はサイズが同じであっても、選択されたフィールドが別のデータベース テーブルのフィールドであることもあります (たとえば、**SDUser** テーブルの **chDefaultLogin** と **SDUserScope** テーブルの **chDefaultLogin**)。また、クエリ内のすべての SELECT ステートメントで、フィールドが同じ位置にある必要があります。
- カスタム クエリでは、**大文字と小文字が区別されません**。このため、大文字と小文字をどのように組み合わせてもかまいません。
- **MESSAGE** ステートメントはオプションであり、条件句 (IF/THEN、ELSEIF、ELSE) でのみ使用できます。詳細については、198 ページの「ユーザ入力を検証する条件句の使い方」を参照してください。

SELECT ステートメントの構文

カスタム クエリでは、RSA Authentication Manager のユーザ データベース (**sdserv**) およびログ データベース (**sdlog**) に対する操作が**読み取り**のみに制限されます。データベースに対して書き込みまたは変更を実行するクエリは使用できません。このため、サンプル クエリではおもに **SELECT** ステートメントが使用されています。

カスタム クエリで使用する SELECT ステートメントの構文は次のとおりです。角かっこ ([ ]) で囲まれたエントリはオプション (省略可能) です。

```
SELECT {*|column-list} FROM {table-name|explicit-join}
[WHERE search-condition]
[GROUP BY column[,column]...]
[HAVING search-condition]
[ORDER BY sort-criteria]
```

SELECT ステートメントでは、検索する**列名** (データ フィールド) を指定し、データが格納されているデータベース テーブルを **FROM** 句に指定します。次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
```

この例では、**sdserv** データベースにある SDUser テーブルから、すべてのユーザのデフォルト ログイン、ラスト ネームとファースト ネームを取得します。

メモ : sdserv (ユーザ データベース) と **sdlog** (監査ログ データベース) にあるすべてのテーブル名は一意に設定されているので、クエリにデータベース名を指定する必要はありません。

テーブル内のすべてのフィールドを取得するには、SELECT ステートメントの列名にワイルドカードとしてアスタリスク (*) を使用します。次の例を参照してください。

```
SELECT * FROM SDUser
```

列名以外の構文要素でアスタリスクをワイルドカードとして使用することはできません。たとえば、次の構文は指定**できません**。このように指定すると、エラーが発生します。

```
SELECT SDUser.*
```

データを取得する式の使い方

SELECT ステートメントで列名を指定する方法として、**式**を使用する方法もあります。式を使用すると、関数によってデータを取得することができます。カスタム クエリでは、数値を取得する関数のみがサポートされています。次の関数を使用できます。

COUNT : この関数は、結果のレコード件数をカウントします。次の例を参照してください。

```
SELECT COUNT(DISTINCT chLastName) FROM SDUser
```

この例では、SDUser テーブル内のラスト ネームの数をカウントします。重複しているラスト ネームはカウントから除外されます。

MAX : この関数は、特定のフィールドの最大値を取得します。次の例を参照してください。

```
SELECT MAX(iUserNum) FROM SDUser
```

この例では、最大ユーザ番号、または最後にデータベースに追加されたユーザの番号を取得します。

MIN：この関数は、特定のフィールドの最小値を取得します。次の例を参照してください。

```
SELECT MIN(iUserNum) + 1 FROM SDUser
```

この例では、SDUser テーブルから、2 番目に小さいアクティブなユーザ番号を取得します。

メモ：オペランド (“+ 1” など) を使用して、関数に変更を加えることができます。この場合は、オペランドと関数の間にスペースを追加する必要があります。スペースが追加されていない場合は、構文エラーが発生します。

SELECT ステートメントでの結合の使い方

SELECT ステートメントを使用する場合、データを単一のテーブルから取得することも、複数のテーブルから取得することもできます。複数のテーブルからデータを取得するには、テーブルの結合を使用します。結合には、次の 3 種類があります。

INNER (内部結合) : 内部結合は、左のテーブルのレコードを右のテーブルの関連レコードと結合して返します (SELECT ステートメントに最初に指定されたテーブルを左のテーブルと呼びます)。内部結合では、選択条件に一致するフィールドのみが抽出されます。次の例を参照してください。

```
SELECT chDefaultLogin FROM SDUser JOIN SDToken ON
SDUser.iUserNum=SDToken.iUserNum
```

このステートメントは、トークン (パスワードを含む) が割り当てられているユーザのみのログイン名を抽出します。INNER を省略して JOIN 句だけを指定しても、内部結合と解釈されます。明示的に INNER JOIN 句を指定してもかまいません。

LEFT[OUTER] (左外部結合) : 左外部結合では、最初 (左) のテーブルの全レコードが結果に抽出された後、2 番目 (右) のテーブルで選択条件に一致するフィールドのみが結合されます。次の例を参照してください。

```
SELECT chLastName, chFirstName, chSerialNum FROM SDUser LEFT
JOIN SDToken ON (SDUser.iUserNum = SDToken.iUserNum)
```

このステートメントは、SDUser テーブル内の全ユーザの名前を出力します。ユーザにトークンが割り当てられている場合は、トークンのシリアル番号も出力されます。OUTER を省略して LEFT JOIN だけを指定しても、外部結合と解釈されます。明示的に LEFT OUTER JOIN 句を指定してもかまいません。

RIGHT[OUTER] (右外部結合) : 右外部結合では、2 番目 (右) のテーブルの全レコードが結果に抽出された後、最初 (左) のテーブルで選択条件に一致するフィールドのみが結合されます。たとえば、上記の LEFT JOIN とは逆に、ユーザに割り当てられているかどうかにかかわらず、データベース内の全トークンのシリアル番号を取得するには、次のクエリを使用します。

```
SELECT chLastName, chFirstName, chSerialNum FROM SDUser
RIGHT JOIN SDToken ON (SDUser.iUserNum = SDToken.iUserNum)
```

OUTER を省略して RIGHT JOIN を指定しても、外部結合と解釈されます。明示的に RIGHT OUTER JOIN 句を指定してもかまいません。また、RIGHT JOIN で結合できるテーブルは 2 つまでです。

SELECT ステートメントでより詳細に列名を定義するには、複数の結合を指定します。たとえば、データベース内の全グループ管理者を抽出するには、次のクエリを使用します。

```
SELECT chDefaultLogin, chLastName, chFirstName,
SDGroup.chName, SDSite.chName FROM SDAdministrativeRole
```

```
JOIN SDUser ON SDUser.iUserNum =
SDAdministrativeRole.iUserNum
JOIN SDGroup ON SDAdministrativeRole.iGroupNum =
SDGroup.iGroupNum
LEFT OUTER JOIN SDSite ON SDGroup.iSiteNum = SDSite.iSiteNum
ORDER BY chDefaultLogin
```

メモ：1 つの SELECT ステートメントに、内部結合と左外部結合、または内部結合と右外部結合を同時に指定できますが、右外部結合と左外部結合の両方を指定することは**できません**。

また、カスタム クエリでは、テーブル結合の対象となるフィールド名として、テーブル名、ピリオド、および列名をこの順番で指定する必要があります。次の例を参照してください。

正：

```
JOIN SDAdministrativeRole ON SDUSer.iUserNum =
SDAdministrativeRole.iUserNum
```

誤：

```
JOIN SDAdministrativeRole ON iUserNum
```

このセクションに示す SELECT ステートメントの例では、**明示的**な結合を使用しています (つまり、各種の JOIN 句が指定されています)。テーブルの結合は**暗黙**に指定することもできます。次の例を参照してください。

```
SELECT chDefaultLogin FROM SDUser, SDToken WHERE
SDUser.iUserNum=SDToken.iUserNum
```

メモ：暗黙の結合は、処理に時間がかかるので、適切な方法では**ありません**。どちらの方法も使用できる場合は、一般に効率のよい明示的な結合を使用してください。

次のセクションでは、テーブルの結合に使用する検索条件について詳しく説明します。テーブルの結合に関するその他の情報については、203 ページの「テーブルの結合の推奨される運用方法」を参照してください。

ON 検索条件の使い方

明示的なテーブルの結合では、**ON** 検索条件を使用する必要があります。この条件句を結合で使用するのは、次の 2 つの目的のためです。

テーブルの関連付け：ほとんどのリレーショナル データベースと同様に、RSA Authentication Manager データベースのテーブルの多くは、他のテーブルと関連があります。たとえば、SDUser テーブルと SDToken テーブルの両方に **iUserNum** フィールドがあります。このフィールドは、ユーザとユーザに割り当てられたトークンとの対応関係を示します。次の例では、この対応関係を SELECT ステートメントで使用しています。

```
SELECT chLastName, chFirstName, chDefaultLogin FROM SDUser
JOIN SDToken ON SDUser.iUserNum=SDToken.iUserNum
```

RSA Authentication Manager データベースのテーブル間には、他にもいろいろな対応関係があります。対応関係の種類には、1 対 1、0 対 1、1 対多、0 対多があります。テーブル間の関連の詳細については、ヘルプのデータベース スキーマに関する説明を参照してください。

テーブルのフィルタリング：ON 検索条件を使用して、検索条件に一致するレコードのみを選択することもできます。このようなフィルタ条件には、論理演算子 (AND、OR、NOT) でつながれた 1 つまたは複数の論理式が含まれます。次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName, chSerialNum
FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum AND SDUser.chLastName BEGINS "A" AND
SDUser.bTempUser = YES
```

このステートメントは、ラスト ネームが “A” で始まる全テンポラリ ユーザのログイン、ラスト ネームとファースト ネーム、およびトークンのシリアル番号を抽出します。

WHERE 検索条件の使い方

クエリの出力に対するフィルタ条件を設定するには、WHERE 句を使用します。ON 句とは異なり、結合を指定しない場合にも WHERE 句を使用できます。次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE SDUser.chLastName BEGINS "A" AND SDUser.bTempUser =
YES
```

この例では、ラスト ネームが “A” で始まるテンポラリ ユーザのログイン、ラスト ネームとファースト ネームを抽出します。SDUser テーブルのみを対象として検索します。

WHERE 句は、テーブルの結合で使用される ON 句の中に指定することもできます。次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName,
dateLastLogin, todLastLogin FROM SDUser JOIN SDToken ON
SDUser.iUserNum = SDToken.iUserNum WHERE
SDToken.DateLastLogin < GMTDateNow ORDER BY chDefaultLogin
```

この例では、ユーザのログイン、ラスト ネームとファースト ネーム、および最終ログインの日付と時刻を抽出します。

GROUP BY 句および HAVING 句の使い方

ある列または複数の列の値が同一のレコードを 1 つのレコードにマージするには、GROUP BY 句を使用します。次の例を参照してください。

```
SELECT chLastName, chFirstName FROM SDUser JOIN SDToken ON
SDUser.iUserNum = SDToken.iUserNum GROUP BY SDToken.iUserNum
HAVING COUNT(DISTINCT SDToken.iTokenNum) > 2
```

この例では、3 つ以上のトークンが割り当てられているユーザを検索します。複数のトークンが割り当てられたユーザの単純なリストが必要な場合は、GROUP BY 句を使用すると、トークンごとに 1 行ではなく、ユーザごとに 1 行ずつ出力できるので便利です。

この例のように、GROUP BY 句の適用結果に対して、さらに 1 つ以上の条件を指定するには、HAVING 句を使用します。

ORDER BY 句によるソート順の指定

1 つ以上の列の値を基準としてクエリの実行結果をソートするには、ORDER BY 句を使用します。次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
```

```
ORDER BY chLastName
```

この例では、ユーザのラスト ネームのアルファベット順にレコードがソートされます。

演算子を使用した論理式の作成

演算子を使用して論理式を作成すると、JOIN 句、ON 句、WHERE 句、および HAVING 句の適用結果に対してさらに条件を指定できます。演算子には、次の 3 種類があります。

比較演算子：これらの演算子は、数値、バイナリ、日付、およびその他の関数に対して使用できます。

< ～より大きい
> ～より小さい
= 等しい
<> 等しくない

次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName, dateEnd,
todEnd FROM SDUser WHERE SDUser.bTempUser = TRUE AND
dateEnd < GMTDateNow AND SDUser.iJobNum = 0 ORDER BY
chDefaultLogin
```

この例では、有効期限の切れた全テンポラリ ユーザのログイン、ラスト ネームとファースト ネーム、および有効期限の日付と時刻を抽出します。

ブール演算子：AND、OR、および NOT 演算子を使用すると、検索条件を結合、追加、および除外できます。

次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName, iType,
chSerialNum FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.iType = 2 AND dateDeath >
GMTDateNow AND NOT dateDeath < 12/31/2006 ORDER BY
chDefaultLogin
```

この例では、アクティブなキーホルダ トークンが割り当てられているユーザのうち、2006 年 12 月 31 日より前に有効期限が切れるユーザのログイン、ラスト ネームとファースト ネーム、およびトークンのタイプとシリアル番号を抽出します。

マッチング演算子：これらの演算子を使用すると、さまざまなマッチング条件を指定することによって、検索条件を絞り込むことができます。

BEGINS
BETWEEN
IN
LIKE
MATCHES

次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName, chSerialNum
FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.chSerialNum BEGINS
"000029949" AND SDToken.chSerialNum NOT BEGINS "000029950"
ORDER BY chSerialNum
```

この例では、シリアル番号が 000029949000 ～ 000029949999 の範囲にあるトークンが割り当てられているユーザのログイン、ラスト ネームとファースト ネーム、およびトークンのシリアル番号を抽出します(実際のシリアル番号の文字長は 12 文字です)。

BETWEEN 演算子を使用して同様のクエリを作成することもできます。ただし、BETWEEN で範囲を指定する場合、使用できるのは整数のみです。

```
SELECT chDefaultLogin, chLastName, chFirstName, iType,
chSerialNum FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.chSerialNum BETWEEN
"000029949000" AND "000029949999" ORDER BY chSerialNum
```

同様に、LIKE 演算子を使用してクエリを作成することもできます。

```
SELECT chDefaultLogin, chLastName, chFirstName, iType,
chSerialNum FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.chSerialNum LIKE "000029949%"
ORDER BY chSerialNum
```

この例では、パーセント記号 (%) が、0 文字以上の文字に対応するワイルドカードとして使用されていることに注意してください。同様に、アンダースコア (_) は、任意の 1 文字に対応するワイルドカードとして使用できます。

式での LENGTH 関数および DATE 関数の使い方

JOIN 句、WHERE 句、または HAVING 句内の式では、LENGTH 関数および DATE 関数を使用できます。

LENGTH：この関数を使用すると、たとえば特定の文字長のフィールドのみを選択することによって、検索条件を絞り込むことができます。次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < 6
```

この例では、ログインの文字長が 6 文字未満のユーザをすべて検索します。

DATE：この関数は、日付を指定することによって検索条件を絞り込みます。DATE 関数の構文は次のとおりです。

```
DATE(month,day,year)
DATE(mm/dd/yyyy)
```

次の例を参照してください。

```
SELECT chDefaultLogin, chLastName, chFirstName,
chSerialNum, dateDeath FROM SDUserScope JOIN SDToken ON
SDUserscope.iUserNum = SDToken.iUserNum WHERE
SDToken.dateLastLogin = DATE(01,01,1986)
```

この例では、トークンが割り当てられているユーザのうち、トークンを使用して認証を実行したことがないユーザのログイン、名前、およびトークンのシリアル番号と有効期限の日付を抽出します。1986 年 1 月 1 日は、新しいトークンに割り当てられる発行日 (つまり、**クロックゼロ**日付) です。

ユーザ入力を求める引数の使い方

クエリに日付、数値などの固定のデータを指定せずに**引数**を定義しておくと、クエリのユーザが実行時に値を指定できます。クエリ内で引数のプレースホルダ (**ARG01** など) を使用します。

クエリの引数を定義するには、[Query Wizard (Define Query)] ダイアログ ボックス (190 ページを参照) を表示します。

操作手順：[Report] > [Custom Queries] > [Add] (既存のクエリを編集する場合は [Edit]) の順にクリックします。各手順の詳細については、ヘルプを参照してください。

1 つのクエリに対して 12 までの引数を定義できます。引数には、**ARG01**、**ARG02**、... **ARG12** という名前があらかじめ定義されています。

前のセクションでは、LENGTH 関数の例で、式に固定の数値 (“< 6”) を使用しました。

引数を使用してクエリのユーザが数値を指定できるようにすると、より柔軟なクエリを作成できます。この場合、クエリは次のようになります。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < ARG01
```

この例では、クエリを実行するユーザが入力した文字数よりログインの文字数が少ないユーザをすべて検索します。ARG01 を定義するときに、ユーザがクエリを実行すると表示されるプロンプトを指定することもできます。次の例を参照してください。

```
Enter the minimum character count in users' logins (ユーザのログインの最小文字数を入力してください)
```

定義できる引数には、次の 2 種類があります。

特定の型の引数：指定できる引数は、NUMBER、STRING、LOGICAL (真または偽)、DATE のいずれかです。クエリを実行するユーザに対して、引数の値を入力するためのダイアログ ボックスが表示されます。

選択可能な引数：指定できる引数は次の表に示す項目のいずれかであり、整数値を返します。クエリを実行するユーザに対して、引数を選択するためのドロップダウン リストを含むダイアログ ボックスが表示されます。

選択可能な項目	戻り値 (整数値)
Users	SDUser の iUserNum
Tokens	SDToken の iTokenNum
Groups	SDGroup の iGroupNum
Sites	SDSite の iSiteNum
Profile	SDProfile の iProfileNum
Agent Hosts	SDClient の iClientNum
Task Lists	SDTaskList の iTaskNum

メモ：SELECT ステートメントで引数を列名として使用することはできません。

ユーザ入力を検証する条件句の使い方

実行を中断してユーザに入力を求めるクエリを作成する場合は、ユーザが入力した内容を検証するしくみが必要です。

入力内容を検証するには、条件句の IF、THEN、ELSEIF、および ELSE を使用します。条件ステートメントの一般的な構文は次のとおりです。

```
IF condition THEN
statement
[ELSEIF condition THEN
statement]
```

```
ELSE
statement
```

このように、条件ステートメントには IF 句、THEN 句、および ELSE 句が必須です。ELSEIF 句は構文に複数の条件を追加するときに使用できますが、必須ではありません。1 つの条件ステートメントには、最高で 32 の句を指定できます。

条件構文を使用してユーザの入力を検証するしくみを説明するため、前のセクションで使用した例をもう一度示します。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < ARG01
```

この単純なクエリは、クエリを実行するユーザが入力した文字数より、デフォルト ログインの文字数が少ないユーザを出力します。

クエリのユーザが入力する数が大きすぎたり、小さすぎたりするのを防ぐには、条件句を使用します。次の例を参照してください。

```
IF ARG01 < 1 OR ARG01 > 16 THEN
MESSAGE "Please enter a number between 1 and 16"
ELSE
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < ARG01
```

このクエリでは、ユーザが適切な引数を入力することが保証されるので、適切な結果を得ることができます。

条件は先頭から末尾に向かって評価されるので、入力を確認する句を条件の先頭に組み込む必要があります。その後に、実際の SELECT ステートメントを実行する条件を記述します。たとえば、サンプル クエリの「Administrators_with_a_Specified_Task_List」は、このルールに従って記述されています。

```
IF ARG01 = 0 THEN
MESSAGE "Select a Task List"
ELSEIF iMyGroup <> 0 OR iMySite <> 0 THEN
MESSAGE "You must be a Realm Administrator to run this query"
ELSE
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
JOIN SDAdministrativeRole ON SDUSer.iUserNum =
SDAdministrativeRole.iUserNum WHERE
SDAdministrativeRole.iListNum = ARG01 ORDER BY
SDUser.chDefaultLogin
```

このクエリはユーザがタスク リストを選択したことと、ユーザがレルム管理者であることを確認します。確認が終了した後にのみSELECTステートメントが実行されます。

条件句は、入力内容の検証以外の用途にも使用できます。たとえば、複数の SELECT ステートメントから、ユーザの入力に基づいて 1 つのステートメントのみを実行するような、複雑なクエリを作成することもできます。この目的で条件句が使用されているサンプル クエリが多数あります。たとえば、「Users_with_Tokens_(matching_wildcard) 」というサンプル クエリを参照してください。

条件句のその他の用途として、クエリにアドミニストレーション スコープを組み込むことができます。詳細については、200 ページの「カスタム クエリのアドミニストレーション スコープ」を参照してください。

式でのグローバル定数の使い方

カスタム クエリ ツールには、引数だけでなく、あらかじめ定義されたグローバル定数のセットが用意されています。グローバル定数は、式に指定して使用できます。次の表は、グローバル定数の一覧です。

名前	データ型	値
iMyLogin	number	現在の管理者の iUserNum。
iMyGroup	number	現在の管理者が属するグループの **iGroupNum** (グループ スコープがある場合)。それ以外の場合、レルム管理者およびサイト管理者に対応する 0 が返されます。
iMySite	number	現在の管理者が属するサイトの **iSiteNum** (サイト スコープがある場合)。それ以外の場合、レルム管理者およびサイト管理者に対応する 0 が返されます。
chMyLogin	string	現在の管理者のデフォルト ログイン。
chMyGroup	string	現在の管理者が属するグループのグループ名 (グループ スコープが割り当てられている場合)。それ以外の場合は、空文字列が返されます。
chMySite	string	現在の管理者が属するサイトのサイト名 (サイト スコープが割り当てられている場合)。それ以外の場合は、空文字列が返されます。
LocalTimeNow	number	ローカル時刻の午前 0 時を基準とした秒数。
LocalDateNow	date	mm/dd/yyyy の形式で表される現在のローカル日付。
GMTTimeNow	number	グリニッジ標準時 (世界協定時 (UTC) とも呼ばれます) の午前 0 時を基準とした秒数。
GMTDateNow	date	mm/dd/yyyy の形式で表される GMT 日付。

グローバル定数の使用例については、サンプル クエリを参照してください。アドミニストレーション スコープで使用する定数の詳細ついては、200 ページの「カスタム クエリのアドミニストレーション スコープ」を参照してください。

メモ : SELECT ステートメントでグローバル定数を列名として使用することはできません。

カスタム クエリに関する高度なアプリケーション ノート

このセクションでは、カスタム クエリを最適な方法で使用するためのヒント、テクニック、および推奨される運用方法を示します。

カスタム クエリのアドミニストレーション スコープ

セキュリティ上の理由から、カスタム クエリを作成する操作、および他の管理者とカスタム クエリを共有する操作は、レルム管理者 (アクセス レベルの最も高い管理者) だけが実行できます。これは主に、下位レベル (サイトおよびグループ) の管理者が機密性の高いデータにアクセスするのを防止するためです。

カスタム クエリでアドミニストレーション スコープを使用する場合、次の 2 つの方法があります。

スコープ条件をクエリの実際の SQL コードに組み込む：アドミニストレーション スコープをカスタム クエリの SQL コードに直接組み込むことができます。クエリを実行するユーザのアドミニストレーション レベルに応じて、異なるアクティビティを実行するクエリの構文を作成できます。RSA Authentication Manager 環境では、(**スコープ**の高い順から) レルム、サイト、およびグループの 3 つのレベルの管理者が定義されます。

スコープをクエリに組み込むには、次の説明に従って、グローバル定数 iMySite および iMyGroup を使用します。

- 現在のユーザがレルム管理者であることを確認するには、iMySiteおよびiMyGroupの両方が 0 であることを確認します。
- 現在のユーザがサイト管理者であることを確認するには、iMySite が 0 ではなく、iMyGroup が 0 であることを確認します。
- 現在のユーザがグループ管理者であることを確認するには、iMyGroup が 0 ではないことを確認します。
- iMySite および iMyGroup の両方が 0 ではない場合、現在のユーザはサイト内グループのグループ管理者です。この場合、**chMyGroup** フィールドおよび **chMySite** フィールドには、このグループ管理者のグループ名とサイト名が含まれます。

RSA Authentication Manager ユーザ データベースの **SDUserScope** テーブルには、すべてのユーザのスコープが記録されます。クエリでこのテーブルを使用して、サイト管理者およびグループ管理者のユーザ レコードを選択できます。サイト管理者の場合は、次の構文を使用します。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM
SDUserScope WHERE SDUserScope.iSiteNum = iMySite
```

同様に、グループ管理者の場合は、次の構文を使用します。

```
SELECT chDefaultLogin, chLastName, chFirstName FROM
SDUserScope WHERE SDUserScope.iGroupNum = iMyGroup
```

クエリのアドミニストレーション スコープの例については、サンプル クエリの「Administrators_with_a_Specified_Task_List」、「All_Administrators」、「Group_Administrators」、および「Site_Administrators」を参照してください。

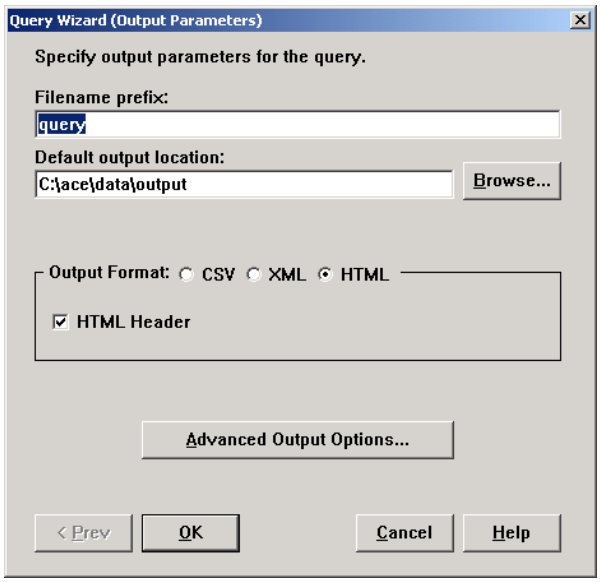
Query Wizard でクエリのアクセス レベルを指定する：Query Wizard を使用して、ネットワーク上の共通の保存場所で共有できるようにしたクエリにアクセス可能なサイト管理者およびグループ管理者を指定できます。

[Query Wizard (Query Access Level)] ダイアログ ボックスでは、サイト管理者およびグループ管理者に対して [None] または [All] を指定したり、クエリにアクセス可能な管理者が属するサイトまたはグループを選択することができます。この設定によって、ネットワーク上の共通の保存場所でクエリを共有できるようにしても、クエリを参照および実行できるのは、アクセスが許可された管理者のみとなります。

[Query Wizard (Query Access Level)] ダイアログ ボックスでスコープを設定する方法ついては、ヘルプを参照してください。クエリの共有の詳細については、ヘルプと 204 ページの「共有クエリの保存場所の設定」を参照してください。

サードパーティ製のレポート ツールで使用するための出力形式の調整

クエリの作成時または編集時、およびコンパイルしたクエリの実行時に、[Query Wizard (Output Parameters)] ダイアログ ボックスが表示されます。



[Query Wizard (Output Parameters)] ダイアログ ボックスでは、データのデフォルトの出力形式や、その他の詳細なオプションを指定できます。基本的な設定として、CSV、HTML、または XML の出力形式を指定できます。

クエリの実行時にデフォルトの設定をそのまま使用することも、設定を変更することもできます。

選択する形式は、データを表示するプログラムに応じて異なります。CSV (カンマ区切り形式) は、Microsoft Excel などの表計算ソフトにインポートする場合に適しています。

Web ブラウザでデータを表示する場合は、出力形式として HTML を選択します。Crystal Decisions 社の Crystal Reports など、レポート ツールでデータを表示する場合は、XML を選択します。

出力形式を選択すると、次の表に示すように、対象の形式に対応するオプションが表示されます。

出力形式	オプション	説明
CSV	[CSV Header]	クエリに定義された列名を出力ファイルに追加するかどうかを指定します。
	[Separator]	CSV 出力の値を区切る文字を指定します。デフォルトではカンマが使用されます。
	[Qualifier]	CSV 出力の各フィールドの先頭と末尾を示す文字を指定します。
HTML	[HTML Header]	クエリに定義された列名を HTML 出力ファイルに追加するかどうかを指定します。

出力形式	オプション	説明
XML	[XML Tag]	レポートの XML タイトルを指定します。Crystal Decisions 社の Crystal Reports など、XML 処理ソフトを使用する場合に役立ちます。
	[Column names as tags]	列名を XML タグとして追加するかどうかを指定します。選択しないと、列のタグはデータベースのフィールドになります。

[Query Wizard (Output Parameters)] ダイアログ ボックスの [Advanced Output Options] をクリックして、その他のオプションが含まれる別のダイアログ ボックスを表示します。このダイアログ ボックスでは、次のオプションを指定できます。

- 出力するレコード数の限度
- クエリの実行後すぐに起動されるデータ表示用のプログラム
- 指定された出力形式では正しく処理できない特殊文字の削除または置換の選択

テーブルの結合の推奨される運用方法

一般に、複数の JOIN ステートメントを使用するクエリを実行すると、特にデータベース内の大きなテーブルを処理する場合に、コンピュータの CPU に大きな負荷がかかります。

このようなクエリを直接プライマリまたはレプリカで実行すると、データベースの調整、レプリケーション、および認証の処理で、Authentication Manager の全体的なパフォーマンスが大きな影響を受けることがあります。

以下に、テーブルの結合を効果的に使用するためのガイドラインを示します。

- 明示的な結合を使用します。処理に時間がかかり、効率も悪いので、暗黙の結合は使用しないようにしてください。
- 2 つのテーブルを結合する場合は、レコードが少ない方のテーブルをレコードが多い方のテーブルに結合するように指定します。たとえば、サンプル クエリの「Activity_of_a_User」では、SDTokenテーブルをSDLogEntryテーブルに結合します。
- 左外部結合と右外部結合を同時に使用しないでください。
- 内部結合と左外部結合を一緒に使用して、複数のテーブルを結合することは可能です。複数の結合方法を同時に使用する場合は、内部結合をまとめて最初 (左) に指定し、すべての左外部結合を 2 番目 (右) に指定すると効率的です。

クエリの保存と整理

クエリはデフォルトで ***ACEDATA*** フォルダのサブディレクトリに保存されます。一般的な保存先は次のとおりです。

```
c:¥ace¥data¥queries
```

各クエリは、このパスのサブディレクトリに保存されます。新しいクエリの名前を指定すると、クエリの保存先となるサブディレクトリの名前も決まります。たとえば、“my_first_query” という名前のクエリは、次の場所に保存されます。

```
c:¥ace¥data¥queries¥my_first_query
```

この例では、クエリに関連する実際のファイルが“my_first_query”フォルダに保存されます。次の表は、クエリ関連のファイルの内容を示しています。

ファイル名	内容	説明
definition.txt	コンパイルする前のクエリです。引数、条件、ステートメント、説明、アクセス レベル、および構成情報が含まれます。	このファイルの名前は常に同じです。Query Wizard で [Finish] をクリックすると、クエリの名前が付いたフォルダに作成されます。他のレルムと共有したり、他のプラットフォームでコンパイルするために共有できるのは、コンパイルされていないクエリのみです (このためには、**definition.txt** ファイルを手動で共有します)。
query.r	コンパイルされたクエリです。	実行できるのは、コンパイルされたクエリのみです。
runtime.txt	前回クエリを実行したときに指定された指示です。出力形式、出力フォルダなどの情報が含まれます。	クエリが少なくとも 1 回は実行されないと、このファイルは作成されません。
acquery.r	共有ポイントから入手されたクエリです。	コンパイルされたクエリのうち、作成者 (レルム管理者) が共有できるようにしたクエリのみを入手できます。保存先として新しいサブディレクトリが **c:¥ace¥data¥queries** に作成されます。**definition.txt** は含まれません。クエリを実行すると、**runtime.txt** が作成されます。

共有クエリの保存場所の設定

レルム管理者がコンパイルされたクエリを組織で共有できるようにする場合、他の管理者がアクセスできるネットワーク上のディレクトリを設定する必要があります。

通常は、共有する保存場所を RSA Authentication Manager のインストール ディレクトリ以外の場所に作成してください。たとえば Windows の場合、RSA Authentication Manager のデフォルトのインストール ディレクトリは **C:¥ACE** です。このディレクトリ ツリーの中または下に共有ディレクトリを作成しないでください。

重要 : ある OS のプラットフォームで作成およびコンパイルされたクエリは、別の OS を実行しているコンピュータで共有および実行できません。たとえば、プライマリおよびレプリカでは Sun Solaris、リモート アドミニストレーション マシンでは Microsoft Windows を実行しているとします。この場合、Windows マシンのユーザが Solaris マシンでコンパイルされたクエリを入手して実行することはできません。

レプリカでのクエリの実行

RSA Authentication Manager 環境にレプリカをインストールする主な目的は、認証の実行です。

ただし、レプリカではユーザ データベースのコピーをローカルで管理していることに加えて、RSA Authentication Manager Host Mode もインストールされています (ローカルおよびリモートの両方)。

このため、カスタム クエリをレプリカ上で実行することもできます。プライマリが一時的にサービスを停止している場合や負荷が高い場合などは、レプリカでカスタム クエリを実行できると便利です。

レプリカで RSA Authentication Manager Host Mode コマンドを使用すると、クエリを実行するたびにデータベースのローカル コピーが検索されます。

レプリカでクエリを実行する場合は、次のことに注意してください

- データベースの調整はバックグラウンド プロセスとして実行されるので、レプリカ上のユーザ データベース (**sdserv**) は、プライマリのデータより多少古いことがあります (一般には数分の違いですが、認証の負荷が集中する期間は、違いが大きくなることがあります)。
- ログ データベース (**sdlog**) には、そのレプリカのアクティビティに関するデータしか記録されません。プライマリのログ データベースのみがレルム内の全 Authentication Manager のアクティビティを調整します。
- レプリカにはすべてのサンプル クエリが保存されますが、他の Authentication Manager で作成されたクエリは、自動的に利用できるようにはなりません。

複数のレルム間でのクエリの管理

クエリがコンパイルされた後、クエリは特定のレルムにリンクされます。サイトに複数のレルムがあり、クエリをレルム間で共有する場合は、カスタム クエリの機能に組み込まれた一般的な共有および入手の方法は使用できません。

このような場合は、2 番目のレルムのレルム管理者に **definition.txt** ファイルを提供します。ファイルを提供された管理者は、この定義ファイルに基づいて新しくクエリを作成します。**definition.txt** ファイルからクエリを作成する手順については、ヘルプを参照してください。

複数のレルムのレルム管理者が独自のクエリをレルム間で共有できるようにする場合は、いくつかの準備が必要です。

このような管理者は通常、リモート アドミニストレーションを使用して、必要に応じて各レルムにログインすることによって、レルムを管理しています。

あるレルムにログインし、カスタム クエリにアクセスしてサンプル クエリのいずれか (たとえば、サンプル クエリの「Recent_User_Additions」) をコンパイルする場合について考えてみましょう。

リモート アドミニストレーションのセッション中に別のレルムにログインし、カスタム クエリにアクセスすると、利用可能なクエリの中に「Recent_User_Additions」がないことに気付くでしょう。このクエリは、最初のレルムでのみ利用可能です。

コンパイルされていないクエリのコピーを複数作成しておくと、適切に処理できます。次の例を参照してください。

```
Recent User Additions ( レルム 1)
Recent User Additions ( レルム 2)
Recent User Additions ( レルム 3)
```

これで、リモート アドミニストレーションで各レルムにログインし、そのレルム用に確保したコピーをコンパイルできます。

カスタム クエリのトラブルシューティング

カスタム クエリでの作業中にエラー メッセージが表示され、対処方法がわからない場合は、293 ページの「メッセージ」を参照してください。

10 その他の管理タスク

この章では、システム パラメータの変更、システム拡張データの変更、承認手順のカスタマイズなど、必要に応じて行うその他の管理タスクについて説明します。

システム パラメータの変更

[System Parameters] ダイアログ ボックスには、RSA Authentication Manager のシステム レベルの設定が表示されます。管理者はこれらの設定についてよく理解しておくことが必要です。これらの設定を表示し、変更するには、[System] > [System Configuration] > [Edit System Parameters] の順にクリックします。[System Parameters] ダイアログ ボックスが表示されます。

[System Parameters] ダイアログ ボックスに表示されるオプションとフィールドは次のとおりです。

[Allow agent host auto-registration] … このチェックボックスをオンにすると、システムは新規エージェント ホストから情報を受け付け、そのエージェント ホストを Authentication Manager データベースに登録できます。管理者がエージェント ホスト レコードを作成する必要はありません。

このチェックボックスの設定によって、他の自動登録機能を使用できるかどうかが制御されるわけでは**ありません**。このチェックボックスがオフの場合も、エージェント ホストは Authentication Manager データベースで自分の IP アドレスを更新し、Authentication Manager から新しい設定情報を使用して自分の **sdconf.rec** ファイルを更新できます。

システムに自動登録機能を設定する方法については、54 ページの「自動登録されるエージェント ホスト」を参照してください。

[Store time of last login in token records] … (この チェックボックスは [Token, PIN and Password Parameters] ダイアログ ボックスにあります。) このチェックボックスがオンの場合は、ユーザが最後にログインした時刻が、ユーザに割り当てられたトークンのトークン レコードに記録されます。トークン レコードを表示すれば、ユーザが最後に認証に成功した日時を確認できます。この機能を無効にすると、認証速度を向上できます。ただし、ユーザの認証時にトークン レコードは更新されないので、ユーザが最後に認証に成功した日時を確認することはできません。

[Allow Push DB Assisted Recovery] … このチェックボックスがオンの場合は、パッケージで指定された1つまたは複数のレプリカにレプリカ パッケージが作成されるたびに、データベース ファイルが自動的に**プッシュ**されます。この機能は、新しくインストールされたレプリカに初期データベースを配布する目的で使用できます。また、データベースを復旧するのにも便利です。Windows 2000 または Windows 2003 の場合は 92 ページの「復元手順」、UNIX の場合は 140 ページの「復元手順」を参照してください。

[Allow remote administration] … このチェックボックスがオンの場合は、RSA Authentication Manager データベースのアドミニストレーションを、Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server (Service Pack 4)、Windows XP Professional、または Windows 2003 Server マシンから実行できます。

メモ：UNIX プラットフォームの場合、**sdadmin** プログラムで RSA Authentication Manager ソフトウェアのほとんどの機能にアクセスできますが、Remote Administration を使用すると、グラフィカル ユーザ インタフェースを介して RSA Authentication Manager データベースを管理できます。さらに、Remote Administration は RSA Authentication Manager ソフトウェアのすべての管理機能にアクセスできる唯一の方法です。

[Enable Windows password integration at system level] … このチェックボックスがオンの場合は、保護されているリソースに対してユーザが RSA SecurID PASSCODE を入力し、認証されると、ログイン パスワードが Windows 認証サービスに自動的に送信されます。これはシステム全体で有効な設定であり、RSA Authentication Agent 6.0 (または) 6.1 for Microsoft Windows ソフトウェアを実行しているすべてのエージェント ホストに適用されます。エージェント単位にこのパラメータを無効にする方法については、59 ページの「エージェントごとのオフライン認証とパスワードの統合の設定」を参照してください。

[Administrator Authentication Methods] … 管理者が Remote Administration や Quick Admin の認証時に使用できる認証方式を指定します。トークン タイプの詳細については、14 ページの「RSA SecurID トークンと二要素認証」を参照してください。

[PIN Options] (このオプションは、[Token, PIN and Password Parameters] ダイアログ ボックスにあります)

- **[User-created PINs allowed]** … このチェックボックスがオンの場合は、ユーザが作成した PIN とシステムが生成した PIN の両方を使用できます。
- **[User-created PINs required]** … ユーザが自分で PIN を作成しなければならないモードになります。
- **[Alphanumeric PINs allowed]** … このチェックボックスがオンの場合は、システムもユーザも PIN の作成で、数字だけでなく英字も使用できます。しかし、既存の PIN には影響ありません (RSA SecurID PINPAD およびソフトウェア トークンの PIN では、英字は使用できません)。
- **[Min PIN length: [4]]** … システムで使用できる PIN の最小文字数を指定します。4 文字以上に設定してください。6 文字を推奨しています。
- **[Max PIN length: [8]]** … システムで使用できる PIN の最大文字数を指定します。8 文字以下に設定してください。

  システムにとって最適な PIN 設定、および PIN パラメータの設定手順については、103 ページの「PIN に関するオプション」を参照してください。

[RSA Authentication Manager Date and Time] … Authentication Manager の日付フィールドと時刻フィールドには、現在の日付と時刻が表示されます。システム クロックとトークン クロックの同期が数分以上ずれると、サーバでオフセットを変更しなければならないことがあります。

> **メモ：**システム クロック オフセットを変更した場合は、すべてのユーザに通知してください。また、認証を受けるユーザに 60 秒待機するように指示し、ユーザのトークンと Authentication Manager との同期がとれるようにします。

- **[Set clock offset to 0]** … システム クロック オフセットを削除するには、このオプションを選択します。
- **[Set clock offset by token]** … このボタンをクリックすると、ブラウザが表示され、トークン シリアル番号のリストが表示されます。そのリストから、オフセットを設定するトークンを選択します。詳細については、オンライン ヘルプを参照してください。

オフセット値を入力すると、[Computed offset currently applied] フィールドにこの値が表示されます。

システム拡張データの変更

システム拡張レコードの情報を変更するには、[System] メニューの [Edit System Extension Data] オプションを使用します。システム拡張レコードには、カスタム アドミニストレーション プログラムからアクセスできるカスタマ定義情報が格納されています。

RSA Authentication Manager Administration Toolkit を使用してカスタム アドミニストレーション プログラムを作成する方法については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

システム拡張データを編集するには

1. [System] メニューの [Edit System Extension Data] を選択します。

   [Edit System Extension Data] ダイアログ ボックスが開き、システム名と、そのシステムに対して定義されているレコードが表示されます。各レコードはセカンダリ キー (48 バイト以内) とデータ (80 バイト以内) で構成されます。

2. これらのレコードは追加、変更、削除できます。同じキーを使用して複数のレコードを作成することはできますが、1 つの拡張データベース テーブルに重複するレコード (キーとデータ値が同一のレコード) を作成することはできません。

   - 既存のレコードを変更するには、レコードを選択し、[Key] フィールドと [Data] フィールドに表示される情報を変更し、[Save] をクリックします (これらのフィールドのいずれかに入力するまで、[Save] ボタンは使用できません)。

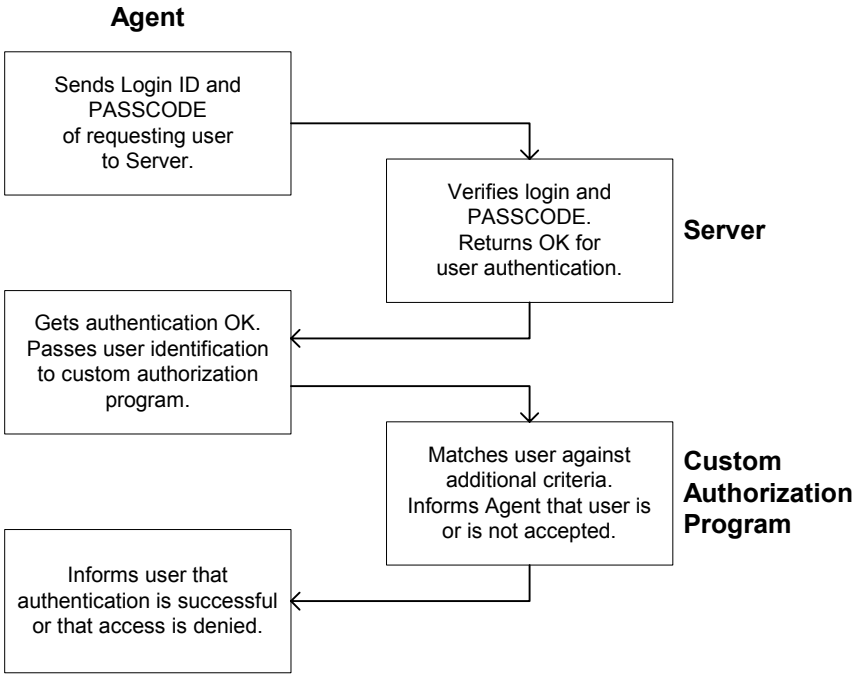
     レコードを変更せずにフィールドをクリアするには、[Clear] をクリックします。
   - 新規レコードを作成するには、必要に応じて [Clear] をクリックして、[Key] フィールドと [Data] フィールドをクリアします。次に、新規レコードの情報を入力し、[Save] をクリックします。
   - レコードを削除するには、レコードを選択し、[Delete] をクリックします。確認のために [OK] をクリックします。

3. [Exit]をクリックして[Edit System Extension Data]ダイアログ ボックスを閉じます。

承認手順のカスタマイズ

External Authorization を使用すると、汎用アプリケーション プログラム インタフェース (API) を使用して、組織内のユーザの承認条件をカスタマイズできます。このようにしてカスタマイズした承認機能は、RSA Authentication Manager 認証に代わるものではなく、それに追加される機能です。External Authorization が有効に設定されている場合、ユーザは追加条件を満たさなければ、システムへのアクセスが許可されません。

次の図は、RSA Authentication Agent が External Authorization を含むシステムで認証要求をどのように処理するかを示しています。



ユーザがシステムにアクセスしようとすると、エージェントと Authentication Manager は通常の方法で認証のやり取りを実行します。ユーザが認証を受けると、External Authorization プロセスが開始されます。定義した条件を使用して、プログラムは認証を受けたユーザにアクセスを許可するかどうかを決定します。

たとえば、認証を受けたユーザを、安全なサイトに現在チェックインしている社員のリストと照合することができます。

External Authorization リモート ログイン オプションが有効に設定されている場合は、リモート レルムから認証を要求したユーザに対して、同じカスタム条件を適用できます。

メモ：レルム間認証環境では、この環境に参加するすべてのレルムで、External Authorization を有効にするか、External Authorization を無効にするか、どちらかに統一する必要があります。External Authorization が有効なレルムと無効なレルムとが混在していると、レルム間認証は失敗します。レルム間認証については、第 4 章「レルム アドミニストレーション」を参照してください。

RSA セキュリティでは特定の External Authorization コードを**提供していません**。テンプレート ソース ファイルをもとに、独自の External Authorization ルーチンを作成し、次に RSA セキュリティが提供する 4 つのスタブ ルーチンの代わりに、カスタマイズしたルーチンを使用する必要があります。カスタマイズしたルーチンは次の条件を満たさなければなりません。

- External Authorization API に準拠しなければなりません。
- RSA Authentication Manager認証プロセスと密接に統合された承認の枠組みを定義しなければなりません。

External Authorization のインストールとカスタマイズの詳細については、『External Authorization API Guide』(***ACEDOC*** ディレクトリの **authmgr_authorization_api.pdf**) を参照してください。

External Authorization オプションの選択

[Authorization Information] ダイアログ ボックスのオプションのどちらか一方または両方を選択すると、システムですでに設定されている承認条件が有効になります。

External Authorization を有効にするには

1. [System] > [Edit Authorization Parameters] の順にクリックします。

   [Authorization Information] ダイアログ ボックスが表示されます。デフォルト設定では、External Authorization は無効に設定されています。

2. [Enable External Authorization] チェックボックスをオンにして、ユーザがローカル システムにログオンできるようにします。

   [Enable External Authorization] オプションだけを有効に設定した場合は、承認条件を満たすユーザはローカル システムにログオンできます。しかし、リモート システムからログオンすることはできません。

3. ローカル システムだけでなく、リモート システムからもログオンできるようにするには、[Enable Authorization of Remote Login Requests] を選択します。

   メモ：[Enable Authorization of Remote Login Requests] を選択するには、その前に [Enable External Authorization] を選択しなければなりません。

   [Enable Authorization of Remote Login Requests] を選択した場合、リモート レルムのユーザは、まず認証を受け、次にホーム レルムから受け取ったカスタム条件に対してローカルでチェックされます。その後、アクセスが許可されます。

4. 選択したオプションを有効にするには、その前に Authentication Manager をいったん停止し、再起動しなければなりません。[スタート] > [設定] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックし、表示されたダイアログボックスを使用して停止 / 再起動してください。

External Authorization の停止と再起動

External Authorization が失敗した場合、External Authorization を無効に設定するか、または Authentication Manager を再起動するまで、その後の認証要求は拒否されます。

External Authorization を停止するには

1. [System] メニューの [Edit Authorization Parameters] を選択します。

   [Authorization Information] ダイアログ ボックスが表示されます。

2. [Enable External Authorization] チェックボックスをオフにします。

3. [RSA Authentication Manager Control Panel] で Authentication Manager を再起動します。

External Authorization を再起動するには

1. External Authorization を有効に設定します。

   手順については、211 ページの「External Authorization オプションの選択」を参照してください。

2. [RSA Authentication Manager Control Panel] で Authentication Manager を再起動します。

これで External Authorization は有効になりました。

11 プログラム ファイルとデータ ファイル

この章では、システムを保護するために連携動作する RSA Authentication Manager プログラム、RSA Authentication Agent プログラム、RSA Authentication Manager データなどのコンポーネントについて説明します。

RSA Authentication Manager ソフトウェア

RSA Authentication Manager マシンにインストールされているプログラムは、次の機能を提供します。

- 構成ツール
- 保護されているネットワーク リソースに対する継続的な認証サービス
- RSA Authentication Manager システムとそのデータの管理用ツール
- 認証およびアドミニストレーション アクティビティのリアルタイム監視

このセクションでは、RSA Authentication Manager プログラムが実行する機能について説明します。

Configuration Management

Configuration Management アプリケーションは、RSA Authentication Manager システムを構成し、構成値を変更するために使用します。構成データの変更については、第 12 章「RSA Authentication Manager の構成 (Windows)」を参照してください。

ユーザの認証

RSA Authentication Manager 認証サービスは RSA Authentication Agent ソフトウェアと連携動作してユーザを認証します。認証サービスをプライマリ Authentication Manager で起動すると、レプリケーション サービスが起動されます。

エージェント ホストはユーザに対して RSA SecurID PASSCODE を要求し、ユーザの応答を認証サービスに送信します。認証サービスは、ユーザが Authentication Manager データベースに登録されているかどうか、PASSCODE がユーザのトークンにとって正しいかどうか確認します。この情報をもとに、認証サービスはアクセスを許可するのか、拒否するのかをエージェント ホストに指示します。

データベースの管理

権限が与えられた RSA Authentication Manager 管理者は、ユーザの追加、トークンの割り当て、アクティビティ レポートの実行、古いログ レコードの消去などの作業を実行できます。アドミニストレーション タスクはプライマリ マシンで実行でき、Remote Administration を実行するように設定されたマシンで実行することもできます。

プライマリ上でRSA Authentication Manager Host Mode を実行するときは、RSA SecurID 認証は必要ありません。この場合、Authentication Manager ソフトウェアがインストールされているディレクトリへのアクセス権がユーザに与えられているかどうかだけが確認されます。ただし、リモートから Authentication Manager データベースを管理しようとする場合は、まず、認証を受けなければなりません。認証を受けるには、管理者は管理対象の RSA Authentication Manager データベースに登録されている RSA SecurID トークンを使用する必要があります。

RSA Authentication Manager Host Mode の機能については、本書全体で詳しく説明していますので、ここでは特に説明しません。特定のアドミニストレーション タスクの操作手順については、目次または索引から該当箇所を検索してください。

プログラマは Administration Toolkit を使用して、カスタマイズしたアドミニストレーション プログラムを作成できます。詳細については、『Administration Toolkit Reference Guide』(***ACEDOC*** ディレクトリの **authmgr_admin_toolkit.pdf**) を参照してください。

アクティビティのリアルタイム監視

RSA Authentication Manager Host Mode からリアルタイム ログ モニタを開始できます。[Report] メニューの [Log Monitor] を選択します。プライマリやレプリカでログ モニタを直接実行することもできます。

操作手順 : [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Log Monitor] の順にクリックしてください。詳細については、[Help] をクリックして表示される情報を参照してください。

レルム ステータスの判断

RSA Authentication Manager のデータベースの各レルムにメッセージを送信するには、**_aceping** コマンドを使用します。**_aceping** コマンドは、レルム間通信が正常に動作しているかどうか、および暗号化 / 復号化が正しく実行されているかどうかを判断します。ping が実行された各レルムは、レルム ステータスを応答します。**_aceping** 出力は画面に表示されます。

_aceping は、プライマリのコマンド ライン プロンプトからのみ実行できます。

メモ : UNIX システムの場合のコマンドは **aceping** です。

コマンド ライン引数

_aceping を実行するには、次のように入力します。

```
ACEPROG¥_aceping number_of_times interval 0
```

斜体は各自で指定する値を表します。次の表は、各パラメータについて説明しています。

パラメータ	説明
number_of_times	**ping** 要求をブロードキャストする回数。最後の ping 要求が送信された後に、実行は停止します。0 の場合は、管理者が停止するまで、コマンドが繰り返されます。
interval	ping の間隔 (秒数)。
0	0 はポート番号を表します。**_aceping** コマンドは **sdconf.rec** に登録されている認証ポート番号を使用します。

たとえば、***ACEPROG*** ディレクトリが **ace¥prog** の場合は、次のように入力します。

```
ace¥prog¥_aceping 0 5 0
```

このコマンドはレルムに対して、管理者がコマンドを停止するまで、5 秒おきに ping を実行します。

_aceping の出力

_aceping では、ping 要求と ping 応答に関する情報が出力されます。

各要求パケットには次の情報が含まれます。

- 送信時刻
- 要求 ID
- ping したレルムに関する情報 (レルム名、Authentication Manager が優先サーバであるのかフェールオーバ サーバであるのか、プライマリ ネットワーク アドレス、ポート番号)

各応答パケットには次の情報が含まれます。

- 受信時刻
- 要求 ID
- 応答しているレルムの名前、サーバが優先サーバであるのかフェールオーバ サーバであるのか、応答の送信元のネットワーク アドレス、ポート番号、応答がセカンダリ ノードから受信された場合はプライマリ ネットワーク アドレス
- ラウンド トリップ時間
- **_aceping** ポート番号
- ステータス メッセージおよびエラー メッセージ

RSA Authentication Agent ソフトウェア

次のハードウェアおよびソフトウェア リソースは、RSA Authentication Agent ソフトウェアを実行することができ、RSA SecurID による保護の対象として設定できます。

- Windows NT、Windows 2000、Windows XP、および Windows 2003 ワークステーションとサーバ
- Sun Solaris、HP-UX、および IBM AIX UNIX ワークステーション
- Novell NMAS (Novell Modular Authentication Service) サーバ
- iPlanet/Sun ONE Web サーバ
- Apache Web サーバ
- RSA Authentication Manager Authentication API を呼び出すユーザ開発アプリケーション
- RSA Authentication Agent コードが組み込まれているコミュニケーション サーバ、VPN サーバ、ファイアウォール、ルータ、およびその他のデバイスとアプリケーション

RSA Authentication Agent の詳細については、米 RSA Security の Web サイトを参照してください。URL は **www.rsasecurity.com/node.asp?id=1174** です。

RSA Authentication Agent ソフトウェアは、認証ダイアログ プログラムや構成情報を表示するプログラムも含めて、複数のプログラムで構成されます。このセクションでは、これらのプログラムが実行する機能について簡単に説明します。エージェント ソフトウェアの詳細については、パッケージに付属しているマニュアルを参照してください。

ユーザ認証ダイアログ

RSA Authentication Agent 6.1 ソフトウェアは RSA Authentication Manager と連携動作して、ユーザの識別と認証を行います。標準の Windows ログオン画面ではなく、ユーザにログオン名と RSA SecurID PASSCODE の入力を要求する画面が表示されます。

メモ：旧バージョンのエージェントの場合は、ユーザがエージェント ホスト マシンにログインするときに、ログイン名 (および必要な場合はパスワード) を入力します。エージェント ホストは、このログインが RSA SecurID 認証の対象として指定されているかどうかを確認します。指定されている場合は、PASSCODE の入力を求めるプロンプトが表示されます。

ユーザがエージェント ホスト マシンを使用することを承認されているかどうか確認するために、ユーザの応答がサーバに送信されます。PASSCODE が正しく、ユーザがエージェント ホストでアクティブ化されている場合は、サーバはこの情報をエージェント ホストに送信します。エージェント ホストはユーザに次のメッセージを表示します。

```
PASSCODE accepted （PASSCODE が受け付けられました ）
```

PASSCODE が不正な場合や、何らかの理由でユーザにアクセスが許可されない場合は (たとえば、トークンが無効に設定されている場合や、エージェント ホストが制限されているのに、ユーザがアクティブ化されていない場合)、エージェント ホストは次のメッセージを表示します。

```
Access denied （ アクセスは拒否されました ）
```

アクセスが拒否された場合の対処法については、付録 C「トラブルシューティング」を参照してください。

構成情報の表示

RSA Authentication Manager マシンでは、Configuration Management アプリケーションで **sdconf.rec** ファイルの内容を表示します。RSA Authentication Agent for Microsoft Windows では、認証テスト機能を使用してこの情報を表示します。RSA Authentication Agent for UNIX では、**sdinfo** を実行します。他のエージェントでは、適切なユーティリティを実行してください。

RSA Authentication Manager ソフトウェアとエージェント ソフトウェアの両方が 1 台の Windows 2000 または Windows 2003 マシンにインストールされている場合は、**sdconf.rec** ファイルが 2 つあり、それぞれ ***ACEDATA*** ディレクトリと ***%SYSTEMROOT%*¥system32** ディレクトリに格納されています。

構成レコードの内容については、第 12 章「RSA Authentication Manager の構成 (Windows)」を参照してください。

エージェント ホストの自動登録と更新

sdadmreg ユーティリティを使用すると、新規エージェント ホストをサーバ データベースに自動的に登録できます。また、既存のエージェント ホストのアドレスが DHCP によって変更された場合は、サーバ データベースに登録されている IP アドレスが自動的に更新され、Authentication Manager の構成が変化したことをエージェント ホストが検出した場合は、エージェント ホストの **sdconf.rec** ファイルが自動的に更新されるようにすることもできます。詳細については、64 ページの「エージェント ホストの自動登録 / 更新」を参照してください。

通信の暗号化と復号化

エージェント ホストと RSA Authentication Manager の間の通信や、レルム間認証を行うときのレルム Authentication Manager 間の通信は、不正な攻撃者から防御するために暗号化されます。エージェント ホストが認証要求メッセージを Authentication Manager に送信する場合は、**ノード シークレット**を使用してデータを暗号化します。ノード シークレットとは、エージェント ホストと Authentication Manager だけが知っている擬似乱数データの文字列です。レルム シークレットの詳細については、222 ページの「ノード シークレット ファイル」を参照してください。

レルム Authentication Manager が別のレルム Authentication Manager に認証要求メッセージを送信する場合は、**レルム シークレット**を使用して要求を暗号化します。レルム シークレットは 2 台の Authentication Manager しか知らない情報です。レルム シークレットの詳細については、83 ページの「レルムの作成と変更」を参照してください。

Authentication Manager は要求を受信すると、その要求を復号することができます。これは、その Authentication Manager がノード シークレットまたはレルム シークレット (およびその他の特定の情報) を知っているからです。どちらの方向の通信でも同じ処理が実行されます。どちらの側も (両方が Authentication Manager であるか、一方が Authentication Manager で他方がエージェント ホストであるかに関係なく)、暗号化と復号化に同じシークレットを使用します。

エージェント ホストを削除後に再作成したり、ノード シークレット ファイルが誤って削除された場合は、Authentication Manager に記録されているノード シークレットとエージェント ホストのノード シークレットが一致しなくなる可能性があります。このような不一致が発生すると、デバイス間でやり取りされるメッセージが復号されなくなり、このエージェント ホストにログインしようとしたすべてのユーザのアクセスが拒否され、「Node Verification Failed (ノードの検証に失敗しました)」というメッセージが監査証跡に記録されます。この場合は、363 ページの「Node verification failed (137) (ノードの検証に失敗しました)」を参照してください。

同様に、ローカル レルム レコードが削除された後、再インストールされた場合は、リモート レルムのレルム シークレットが消失する可能性があります。この場合、ローカルAuthentication Managerは他のレルムからログインしようとするすべてのユーザのアクセスを拒否し、「Could not decrypt XR message (XR メッセージを復号できませんでした)」というメッセージを監査証跡に記録します。この場合は、330 ページの「Could Not Decrypt XR Message (8220) (XR メッセージを復号できませんでした)」を参照してください。

RSA Authentication Manager データ

RSA Authentication Manager データは、Authentication Manager マシンの Authentication Manager データベースとログ データベース、**sdconf.rec** ファイルと **license.rec** ファイルに格納されます。このセクションでは、これらのデータベースとファイルについて説明します。

Authentication Manager データベース

Authentication Manager データベースにはシステム パラメータ、トークン レコードとユーザ レコード、エージェント ホスト情報、レルム情報、サイト情報、グループ情報が格納されます。Authentication Manager データベースには次のファイルが含まれます。

sdserv.b1
sdserv.d1
sdserv.db
sdserv.lg
sdserv.st
sdserv.vrs

データベースが使用中の場合は、**sdserv.lk** という追加ファイルも作成されます。

次の**システム パラメータ**は Authentication Manager データベースに格納されます。

- エージェント ホストの自動登録が許可されているかどうか
- 交換されたトークンがデータベースから自動的に削除されるかどうか
- すべてのユーザ パスワードの有効期限が切れるまでの日数
- データベースをリモートから管理できるかどうか
- 許可されている管理者認証方法
- PIN が固定長であるのか、可変長であるのか
- PIN が英数字であるのか、数字のみであるのか

データベースには、各エージェント ホストに関して次の情報を含む**エージェント ホスト** レコードが格納されます。

- エージェント ホスト名と IP アドレス
- エージェント ホストがすべてのユーザに対してオープンであるのかどうか

- エージェント ホストがすべてのユーザに対してオープンでない場合、エージェント ホストの承認されたユーザとグループのリスト

トークン レコードは Authentication Manager データベースに格納されます。各 RSA SecurID トークン レコードには、次のようにトークン自体に関して変更できない情報が格納されます。

- トークンの種類 (RSA SecurID スタンダード カード、PINPAD、キーホルダ、ソフトウェア トークン (以前の名称は SoftID))
- シリアル番号
- トークンに表示されるコードの長さ
- コードが変化する間隔
- トークンが New PIN モードであるかどうか

トークン レコードの内容については、115 ページの「トークン レコードの内容」を参照してください。

レルム レコードには、レルム間認証ネットワーク内の他のレルムに関して、次の情報が格納されます。

- プライマリのネットワーク名と IP アドレス
- レプリカのネットワーク名と IP アドレス
- レルムの信頼関係が確立されているかどうか

ユーザ レコードも Authentication Manager データベースに格納され、次の情報が格納されます。これらの情報は、RSA Authentication Manager Host Mode を使用して設定できます。

- 割り当てられているユーザの名前
- ユーザのログイン
- ユーザがログインできる期間
- リモート ユーザのホーム レルム情報

ユーザ レコードの内容については、113 ページの「ユーザ レコードの内容」を参照してください。

ログ データベース

RSA Authentication Manager は認証試行と、RSA Authentication Manager Host Mode を通じて実行された各処理のレコードを記録します。この監査証跡はログ データベースに格納されます。このデータベースは次のファイルで構成されます。

sdlog.b1
sdlog.d1
sdlog.db
sdlog.lg
sdlog.st
sdlog.vrs

データベースが使用中の場合は、**sdlog.lk** という追加ファイルが作成されます。

RSA Authentication Manager Host Mode を使用すれば、次の目的でログ データに対してさまざまなレポートを実行できます。

- セキュリティに関する問題点の確認
- セキュリティが侵害されたかどうかの確認
- 問題があるためにログインできないユーザの支援

レポートの作成方法については、第 9 章「レポート」を参照してください。

重要 : ログ データベースのサイズを制限するのは、Authentication Manager マシンで使用できるディスク容量だけです。**データベース ファイルが際限なく大きくならないように注意してください。また 90% 以上満杯にならないように注意することも必要です。**定期的にバックアップを作成し、古いログ レコードは削除してください。詳細については、第 8 章「ログ データベースのメンテナンス」を参照してください。

sdconf.rec ファイル

RSA Authentication Manager 構成ファイル **sdconf.rec** は、インストール プロセスによって作成されます。ファイルの情報は、Configuration Management アプリケーションを使用して Authentication Manager 上で表示または変更できます。**sdconf.rec** ファイルは各 Authentication Manager の ***ACEDATA*** ディレクトリに格納されます。

操作手順 : [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Configuration Management] の順にクリックします。構成値の詳細については、[Help] をクリックするか、第 12 章「RSA Authentication Manager の構成 (Windows)」または第 14 章「RSA Authentication Manager の構成 (UNIX)」を参照してください。

エージェント ホストの構成ファイル

エージェント ホストをインストールする場合は、構成ファイル (**sdconf.rec**) を生成し、エージェント ホストにコピーしなければなりません。ただし、RSA Authentication Agent コードが組み込まれ、独自の構成レコードを用意しているサードパーティ デバイスの場合は、その必要はありません。Authentication Manager の ***ACEDATA*** ディレクトリにある構成ファイルは、エージェント ホストに対して生成するすべての構成ファイルのテンプレートとして使用できます。

操作手順 : RSA Authentication Manager Host Mode を起動した後、[Agent Host] > [Edit Agent Host] > [Assign Acting Servers] > [Generate Configuration File] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

旧バージョンのエージェント ホストの構成ファイルには、旧バージョンのエージェント ホストからの認証要求を処理するアクティング マスタ Authentication Manager とアクティング スレーブ Authentication Manager の情報が含まれていなければなりません。旧バージョンのエージェント ホストに対してアクティング マスタ Authentication Manager とアクティング スレーブ Authentication Manager を指定する必要があります。詳細については、24 ページの「ファイアウォールを介した Authentication Manager とエージェント ホストの通信」を参照してください。

操作手順 : [Agent Host] > [Edit Agent Host] > [Assign Acting Servers] の順にクリックします。詳細については、[Help] をクリックして表示される情報を参照してください。

ACEPROG ディレクトリの **sdcfgedit_ui.exe** ユーティリティを使用して、構成ファイルでアクティング マスタとアクティング スレーブを指定する方法もあります。詳細については、74 ページの「旧バージョンのエージェント ホスト」を参照してください。

プライマリ、レプリカ、およびすべてのエージェント ホストの構成には、互換性がなければなりません。互換性が維持されていないと、これらのマシン間で通信できません。詳細については、316 ページの「Cannot initialize Agent Host-server communications (エージェント ホストとサーバの間の通信を初期化できませんでした)」のエラー メッセージの説明を参照してください。

license.rec ファイル

RSA Authentication Manager の購入時に納入されるパッケージには、お客様のサイトに固有のライセンス ファイル (**license.rec**) を記録したフロッピーが同梱されています。**license.rec** ファイル内の設定は、お客様と RSA セキュリティとのライセンス契約に従って行われます。

RSA Authentication Manager 6.1 では、Version 4 のライセンス レコードを使用しており、ライセンスの制限に従っているかどうか確認されます。5.1 より前のリリースの RSA ACE/Server では、Version 3 の **license.rec** ファイルを使用していました。以前のバージョンの RSA ACE/Server からアップグレードすると、セットアップ プログラムによって、元の **license.rec** が Version 4 形式に変換されます。

RSA Authentication Manager 6.1 で license.rec ファイルのデータを表示するには

次のいずれかの操作を実行します。

- Windows の場合

  プライマリまたはレプリカ、あるいは Remote Administration 用に構成したマシンで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Configuration Management] の順にクリックします。

- UNIX の場合は、次のコマンドを入力します。

  ```
  Run ACEPROG/sdinfo
  ```

Configuration Management の設定では、ライセンスに関して次の情報が定義されます。

メモ : RSA Authentication Manager 6.1 for UNIX Configuration Management の設定で定義される正確なライセンス情報については、244 ページの「RSA Authentication Manager の構成の概要」を参照してください。

License …発行されたライセンスが**ベース** ライセンスであるのか、**アドバンスド** ライセンスであるのか。

Status …ライセンスが**パーマネント**であるのか、**評価用**であるのか。

Expiration Date …通常は **None**。ただし、ライセンスのステータスが違反または評価用の場合は、実際の日付が設定されていることもあります。

Licensed Active Users …レルム内で同時にアクティブ化できる RSA SecurID ユーザの数。

アクティブ ユーザについては、274 ページの「ライセンスのアップグレードまたは変換」を参照してください。

Licensed Replicas …登録できるレプリカ サーバの数。ベース ライセンスの場合は **1** 台、アドバンスド ライセンスの場合は **10** 台です。

Licensed Realms … 登録できるレルムの数。ベース ライセンスの場合は **1**、アドバンスド ライセンスの場合は **6** です。

Windows の [Configuration Management] ダイアログ ボックスの場合は、[License Information] の下に [More] ボタンもあります。[More] をクリックすると、別のダイアログ ボックスに以下の追加エントリが表示されます。

License Created …ライセンスが作成された日付 (*mm/dd/yy*)。

License ID …固有のカスタマ識別子。RSA セキュリティ正規販売代理店に連絡する場合は、この番号が必要です。

Licensee …お客様の会社名と住所。

RSA Authentication Manager ライセンスの概要については、付録 A「ライセンス」を参照してください。

ノード シークレット ファイル

エージェント ホストと Authentication Manager の間でやり取りされるパケットは、ノード シークレットを使用して暗号化されます。ノード シークレットはエージェント ホストと Authentication Manager だけが知っている擬似乱数の文字列とその他のデータとの組み合わせです。ノード シークレット ファイルの作成と送信は、自動配布か手動配布のいずれかの方法で行います。

メモ：ノード シークレットがない場合や、一致しない場合は、エージェント ホストと RSA Authentication Manager の間の通信は不可能です。このような不一致が生じた場合は、システムによって「Node Verification Failed (ノードの検証に失敗しました)」というエラーがログに記録されます。このエラーへの対処法については、363 ページの「Node verification failed (137) (ノードの検証に失敗しました)」を参照してください。

自動配布の場合の推奨される運用方法

自動配布 (デフォルト設定) を使用する場合、エージェント ホストで最初に認証が成功したときに、それに対する応答として Authentication Manager は自動的にノード シークレットを作成してエージェント ホストに送信します。ノード シークレットを含む送信は、ユーザの PASSCODE から生成されたキーとその他の情報を組み合わせて暗号化されます。

- 4.4.0 以降のバージョンの Windows エージェントの場合、ノード シークレット ファイルはシステム レジストリに格納されます。
- 旧バージョンのエージェント (4.4.0 より前) の場合、ノード シークレット ファイルは ***%SYSTEMROOT%¥system32*** ディレクトリに格納されます。
- すべての UNIX エージェントでは、ノード シークレット ファイルは ***ACEDATA*** ディレクトリに格納されます。

ノード シークレット ファイルのデフォルト名は **securid** です。

自動配布の場合、各エージェント ホストで最初の認証が行われる状況を注意深く制御しないと、ノード シークレットの不正取得が可能になります。

- ノード シークレットの配布が完了するまでは、エージェント ホストを [Open to All Locally Known Users] に設定**しない**でください。そのエージェント ホストでは、管理者だけが認証されるようにしておきます。このパラメータは [Add Agent Host] ダイアログ ボックスで設定できます。手順については、第 3 章「エージェントとエージェント ホスト上でのアクティブ化」を参照してください。
- システムでリモート ユーザに対して **telnet** または **rlogin** を使用している場合は、ノード シークレットの盗難を防止するために、新しいクライアントでの最初の認証を絶対にリモートから行わないようにしてください。**telnet** や **rlogin** などのアプリケーションを通じて、認証を受ける最初のユーザがリモートから接続した場合、そのユーザの PASSCODE は暗号化されずに送信されるので、攻撃者は簡単にその情報を傍受して、ノード シークレットを生成できます。
- 最初の認証時に可能な最長の PASSCODE、つまり 12 文字以上を使用するようにすれば、解読時間が大幅に長くなり、攻撃を受ける可能性を大幅に軽減できます。

管理者は最初の認証を自分自身でローカルで行い、十分な長さの PIN を設定したトークンを使用することで、攻撃に対して最大限の保護を講じることができます。

手動配布の場合の推奨される運用方法

ノード シークレットを手動で送信する場合は、ノード シークレットを作成するよう Authentication Manager に指示する必要があります。次に、ノード シークレットをエージェント ホストに配布し (たとえば、フロッピー ディスクで)、ノード シークレット ロード ユーティリティを使用してノード シークレットをエージェント ホストにロードします。このノード シークレットはパスワードで保護されています。

エージェント ホストでノード シークレット ロード ユーティリティを実行すると、ユーティリティはノード シークレット ファイルを復号し、名前を認証サービスと同じ名前 (通常は **securid**) に変更します。次に、名前変更後のファイルを Windows マシンの場合は ***%SYSTEMROOT%¥system32*** ディレクトリに、UNIX マシンの場合は ***ACEDATA*** ディレクトリに格納します。

- 4.4.0 以降のエージェントは、名前変更後のノード シークレット ファイルを ***%SYSTEMROOT%¥system32*** ディレクトリからシステム レジストリにコピーし、***%SYSTEMROOT%¥system32*** ディレクトリのノード シークレット ファイルを削除します。
- 旧バージョンのエージェント (4.4.0 より前) は、名前変更後のノード シークレット ファイルを ***%SYSTEMROOT%¥system32*** ディレクトリにそのまま置いておきます。
- すべての UNIX エージェントは、名前変更後のノード シークレット ファイルを ***ACEDATA*** ディレクトリにそのまま置いておきます。

手動配布の場合、ノード シークレットを作成した後、エージェント ホストに配布するのは管理者の役割です。セキュリティ上の理由から、次のガイドラインに従ってください。

- 可能な最長の**英数字**のパスワード (12 文字以上)。
- 可能であれば、ノード シークレットを**フロッピー ディスク**で RSA Authentication Agent 管理者に配布し、パスワードを口頭で伝えます。パスワードを書き留めることはしないでください。ノード シークレットを電子メールで配布する場合は、パスワードを別のメールで送信します。
- ノード シークレットの配布に関係するユーザ全員が**信任された**人物であることを確認してください。

ノード シークレットの作成と送信の詳細については、ヘルプの「Creating a Node Secret」を参照してください。

データベースの調整

プライマリとレプリカのいずれか一方または両方の動作が中断された後、2 つの Authentication Manager の間の通信が再確立されると、データベースが調整されます。調整が完了すると、プライマリとレプリカの **sdserv** データベースには同じ情報が格納されます。

メモ : SDI_ASD_SYSLOG 環境変数を設定しない限り、調整プロセスは **syslog** またはイベント ログにレコードの更新やカウントを行いません。データが変更された場合、デフォルトでは、調整プロセスが調整完了を示すメッセージを表示します。詳細なシステム イベント ログ メッセージを有効にするには、データベース ブローカ サーバを起動する前に、**SDI_ASD_SYSLOG** 環境変数を設定します。**SDI_ASD_SYSLOG** 環境変数を設定するには、コントロール パネルの [システム] をクリックし、[詳細] タブの [環境変数] ボタンをクリックします。Windows では、**SDI_ASD_SYSLOG** 環境変数を**システム変数**として設定し、変更が反映されるようにシステムを再起動します。

データベースを調整する場合、同期サービス (**syncsrvc**) は次の規則に従います。

ログ レコードの変更。レプリカで記録されているすべてのログ レコードは、データベースの調整でプライマリのデータベースに追加されます。プライマリがレプリカのデータベースにログ レコードを送信することはありません。

エージェント ホスト レコードの変更。調整の後、エージェント ホスト レコードには最新のノード シークレット ステータス情報が格納されます。この処理は、送信元がプライマリとレプリカのどちらであるかに関係なく行われます。エージェント ホスト レコードの他のすべての情報は、プライマリ データベースから取り込まれます。

トークン レコードの変更。調整時に、**syncsrvc** は各トークン レコードのプライマリのコピーをレプリカのコピーと比較します。2 つのコピーが異なる場合は、どの項目が異なるかに応じて処理が異なります。

- **トークンの割り当て**が異なる場合は、プライマリのコピーが使用されます。トークン レコード全体がレプリカのデータベースに送信されます。他のフィールドは比較されません。
- **前回のログイン試行**が異なる場合は、最新のログインが記録されたトークン レコード内の **Bad PIN count**、**Bad PASSCODE count**、**Next Tokencode mode**、および **Time Synchronization value** が調整後の値として使用されます。

  この規則には、1 つの例外があります。プライマリとレプリカの両方で前回のログインが失敗した場合は、各フィールドが比較され、**Bad PIN count** と **Bad PASSCODE count** については大きい方が格納され、**Time Synchronization value** はプライマリのコピーの値が使用されます。**Next Tokencode mode** は、どちらか一方のコピーでオンになっているときはオンになります。
- トークンの **enabled (有効) ステータス**が異なる場合には、最新の変更が調整後のステータスになります。
- トークンの **New PIN ステータス**が異なる場合は、最新の変更が調整後のステータスになります。
- **PIN** 情報が異なる場合には、最新の PIN が使用されます。

メモ : syncserv は、同様の規則を使用してユーザ レコードとワンタイム パスワード レコードも調整します。

エラー。調整の途中でエラーが発生した場合 (たとえば、送信タイムアウトやロック エラー)、現在のトランザクションはデータベースに書き込まれません。

調整中に要約メッセージとステータス メッセージがイベント ログに送信されます。次の例を参照してください。

```
...Primary Sent 1 System Changes to the Replica
...Primary Sent 100 User Changes to the Replica
...Primary Sent 200 User Changes to the Replica
...Primary Sent 342 User Changes to the Replica
...Primary Sent 100 Token Changes to the Replica
...Primary Sent 200 User Changes to the Replica
...Primary Sent 300 User Changes to the Replica
...Primary Sent 403 User Changes to the Replica
...Primary Sent 11 Agent Host Changes to the Replica
...Primary Sent 10 Group Changes to the Replica
```

調整トランザクションのイベント ログのサンプルについては、284 ページの「イベント ログとシステム ログの例」を参照してください。

RSA Authentication Manager インストール情報およびパッチ情報の表示

プライマリ、レプリカ、またはリモート アドミニストレーション マシンの [RSA Authentication Manager Control Panel] から、次の情報を表示できます。

- 現在のインストール内容の詳細
- インストールされているパッチの詳細

インストール情報およびパッチ情報を表示するには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。
2. Control Panel のツリーから、[View Installation & Patch Information] を選択します。

12 RSA Authentication Manager の構成 (Windows)

この章では、RSA Authentication Manager の構成管理について説明します。

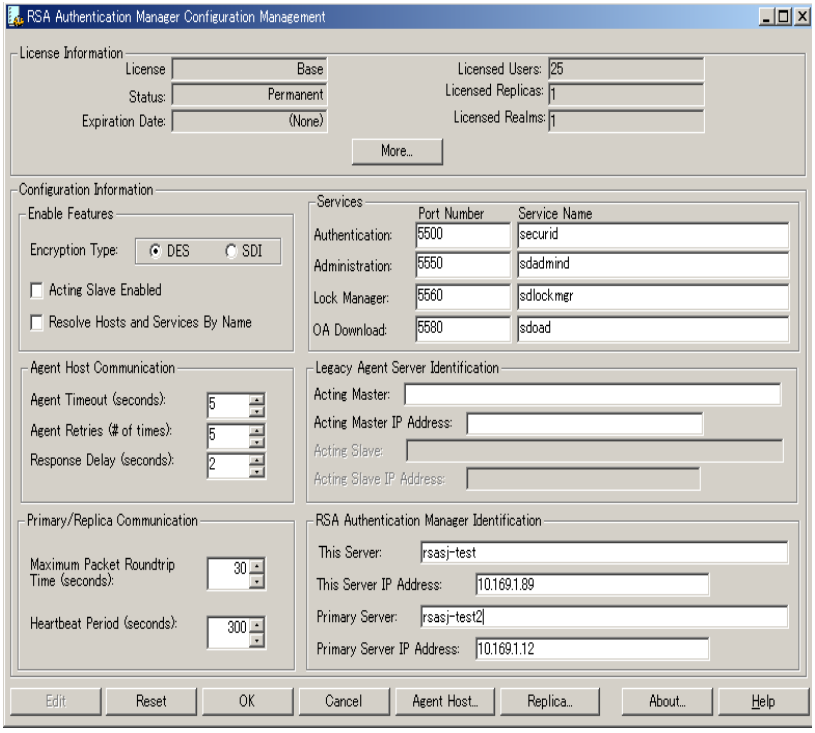
RSA Authentication Manager の構成情報は、Authentication Manager の ***ACEDATA*** ディレクトリの **sdconf.rec** ファイルに格納されています。構成レコードには、RSA Authentication Manager サービス、エージェント ホストと Authentication Manager の通信、Authentication Manager の識別、システムで有効に設定されている機能についての情報が含まれています。

エージェント ホストをインストールするときに、RSA Authentication Manager Host Mode を使用して構成ファイルを生成し、エージェント ホストにコピーする必要があります (RSA Authentication Agent コードが組み込まれ、独自の構成レコードを保有するサードパーティ デバイスの場合は必要ありません)。プライマリ Authentication Manager の ***ACEDATA*** ディレクトリに格納されている **sdconf.rec** ファイルは、エージェント ホストに配布する構成ファイルのテンプレートとして使用できます。

注意：sdconf.rec ファイルをコピーする場合、***ACEDATA*** ディレクトリからエージェント ホストに直接コピーしないでください。新しい構成レコードを作成することにより、入力した必須情報 (たとえば、旧バージョンのエージェント ホストをサポートするために必要なアクティング マスタ / アクティング スレーブの情報や、ファイアウォールを介した認証をサポートするために必要な IP アドレスのエイリアスの情報など) が新しいエージェント ホストの **sdconf.rec** ファイルに確実に含まれるようにしてください。

RSA Authentication Manager システムの現在の構成設定を表示または変更するには、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Configuration Management] の順にクリックします。

[Configuration Management] ダイアログ ボックスが表示されます。この章では、このダイアログ ボックスの各パネルについて説明します。



構成ファイル (**sdconf.rec**) をレプリカにコピーするときは、レプリカで Configuration Management アプリケーションを実行してから、[This Server] (右下の [RSA Authentication Manager Identification] パネル) の値をプライマリの名前からレプリカの名前に変更しなければなりません。詳細については、236 ページの「更新した構成ファイルの配布」を参照してください。

メモ : sdconf.rec ファイルは Configuration Management アプリケーションによって作成されます。エージェントでは **DES** 暗号方式または **SDI** 暗号方式を使用できます。各エージェント ホストには、使用する暗号方式の種類が正しく指定された **sdconf.rec** ファイルが必要です。**DES** 暗号方式を使用するエージェントと **SDI** 暗号方式を使用するエージェントの両方がある場合は、各エージェント ホストに配布する **sdconf.rec** ファイルに暗号方式が正しく設定されていることを確認してください。

[License Information] (ライセンス情報)

[Configuration Management] ダイアログ ボックスの一番上のパネルには、現在のライセンスに関するデータが表示されます。この情報の内容は、インストール時に指定した **license.rec** ファイルによって決まります。ライセンスは RSA セキュリティ社が作成するものなので、このダイアログ ボックスで情報を変更することはできません。

追加情報

- ライセンスの変更の詳細については、ヘルプの「Upgrading the RSA Authentication Manager License」を参照してください。
- [License Information] パネルに表示されるデータ フィールドについては、221 ページの「license.rec ファイル」を参照してください。

ライセンスのオプションとライセンス チェック機能、および一時使用の評価用ライセンスの切り替え方法の詳細については、付録 A「ライセンス」を参照してください。

RSA Authentication Manager でのライセンス レコードの更新

RSA Authentication Manager 6.1 では、インストール時だけでなく、通常の操作中にも定期的にライセンスの制限が確認されます。たとえば、ライセンスで許容されている以上にアクティブ ユーザがデータベースに登録されている場合は、警告メッセージが表示され、それ以降、ユーザをアクティブ化できなくなります。

ユーザまたはサイトが現在のライセンスの制限を超えて増加することが予想される場合は、RSA セキュリティ正規販売代理店から新しいライセンスを入手してください。

新しいライセンスを入手したら、このセクションの説明に従って RSA Authentication Manager のライセンス レコードを更新してください。UNIX システム上で RSA Authentication Manager を使用している場合は、243 ページの「RSA Authentication Manager for UNIX でのライセンス レコードの更新」を参照してください。

重要：複数のレルムを使用する場合は、RSA セキュリティ社からアドバンスド ライセンスを購入する必要があります。アドバンスド ライセンスでは、6 枚のフロッピー ディスクで 6 つの **license.rec** ファイルが提供されます。各フロッピー ディスクにラベルを付け、レルムごとに異なるフロッピー ディスクを割り当てて使用してください。レルムごとに割り当てた **license.rec** を使用して、各レルムについて次のアップグレード手順を繰り返します。

ライセンスをアップグレードするには

1. レルムのプライマリに Windows Administrator としてログオンします。
2. RSA Authentication Manager プロセスが実行されていないことを確認します。Authentication Manager またはデータベース ブローカが動作している場合は、Authentication Manager マシンで [RSA Authentication Manager Contorl Panel] を開き、ツリーの [Start & Stop RSA Auth Mgr Services] アイコンをダブルクリックします。

   [Start & Stop RSA Authentication Manager Services] ダイアログ ボックスが表示されます。

3. Authentication Manager とデータベース ブローカの両方を停止するには、[Stop Services] の [Stop All] をクリックします。もう一度 [OK] をクリックして、ダイアログ ボックスを閉じます。
4. [スタート] > [設定] > [コントロール パネル] > [アプリケーションの追加と削除] の順にクリックします。

   Windows 標準の [アプリケーションの追加と削除] ダイアログ ボックスが表示されます。
5. スクロールして [RSA Authentication Manager] を選択し、[変更 / 削除] をクリックします。

   [RSA Authentication Manager Maintenance] ダイアログ ボックスが表示されます。
6. [Modify] を選択し、[Next] をクリックします。
7. [Upgrade License] を選択し、[Next] をクリックします。
8. 必要に応じて、現在のレルムの新しい **license.rec** ファイルがある場所を指定します (デフォルトのパスは A: です)。[Next] をクリックします。

   有効な **license.rec** ファイルの場所を指定すると、次のメッセージが表示されます。

   ```
   License has been successfully upgraded. ( ライセンスが正しくアップグレードされました )
   ```
9. メッセージのダイアログ ボックスで [OK] をクリックします。次のダイアログ ボックスで [Finish] をクリックして操作を終了し、RSA Authentication Manager Maintenance プログラムを閉じます。
10. [閉じる] をクリックして、Windows の [アプリケーションの追加と削除] ダイアログ ボックスを閉じます。

メモ : 次回 RSA Authentication Manager を起動すると、レルム内のレプリカで新しいライセンスが自動的に有効になります。

[Configuration Information] (構成情報)

画面の中央 (ライセンス情報の下) には、構成情報が表示されます。これらのパラメータは、プライマリまたはレプリカ上でのみ編集できます。リモート アドミニストレーション マシンでは、この情報を表示できますが、編集することはできません。この情報を RSA Authentication Agent for Microsoft Windows で表示するには、テスト認証のテスト機能を使用します。UNIX エージェント ホストでこの情報を表示するには、**sdinfo** コマンドを実行します。

メモ : sdconf.rec ファイルを変更した場合は、RSA Authentication Manager を再起動して変更を反映する必要があります。自動登録を使用しているエージェント ホストがある場合は、データベース ブローカを停止して、エージェント ホストの **sdconf.rec** ファイルを更新する必要があります。

[Enable Features] (有効にする機能)

パラメータ	説明
Encryption Type	エージェント ホストと Authentication Manager 間の通信に使用する暗号方式で、DES と SDI のいずれかを指定します。システムが以前に SDI 暗号方式で構成されている場合は、[SDI] をクリックしてください。それ以外の場合は、[DES] をクリックしてください。
Acting Slave Enabled	このチェックボックスがオンの場合は、旧バージョンのエージェント ホストをサポートするためのアクティング マスタとアクティング スレーブを指定できます。詳細については、233 ページの「ホスト名とサービス名の解決」を参照してください。
Resolve Hosts and Services By Name	RSA Authentication Manager とエージェントでホスト名とサービス名を解決する方法を指定します。[Resolve Hosts and Services By Name] チェックボックスがオフの場合には、名前は IP アドレスを使用して解決されます。[Resolve Hosts and Services By Name] チェックボックスがオンの場合には、名前はホスト名を使用して解決されます。

[Encryption Type] の設定は、RSA Authentication Agent **だけ**が使用します。一部のエージェントが SDI 暗号方式を使用する場合は、[Encryption Type] の設定を DES から SDI に変更し、構成レコードを保存してください。次に、Authentication Manager との通信に SDI を使用するエージェント ホストにだけ、新しい **sdconf.rec** ファイルをコピーします。その後、Configuration Management アプリケーションで [Encryption Type] を [DES] に戻し、デフォルト設定を保存してください。

[Agent Host Communication] (エージェント ホストの通信)

パラメータ	説明
Agent Timeout	エージェント ホストと Authentication Manager 間の通信の確立を試みる間隔 (秒単位)。指定できる値は 1 ～ 20 です。デフォルト値は 5 です。
Agent Retries	「Cannot initialize agent host-Server communication. (エージェント ホストとサーバ間の通信を初期化できません)」というエラー メッセージが返されるまでに、エージェント ホストが Authentication Manager との通信の確立を試みる回数。指定できる値は 1 ～ 6 です。デフォルト値は 5 です。
Response Delay	応答がエージェント ホストに返されるまでに認証要求が保留される時間 (秒単位)。この遅延の値は、暗号化されていない telnet 接続でログインが実行される場合に、そのネットワーク上で特定の種類の攻撃をトラップするために使用されます。この設定を有効にするには、[Agent Timeout] の値に [Agent Retries] の値を乗算した値よりも小さい値を指定します。指定できる値は 0 ～ 15 です。デフォルト値は 2 です。

[Agent Timeout]、[Agent Retries]、[Response Delay] のいずれかを変更した場合は、更新された **sdconf.rec** ファイルのコピーをすべてのエージェント ホストに配布してください。

[Primary/Replica Communication] (プライマリとレプリカ間の通信)

これらの値のいずれかを変更した場合は、更新された **sdconf.rec** ファイルのコピーをすべてのレプリカに配布し、[RSA Authentication Manager Control Panel] を使用して適用します。詳細については、236 ページの「更新した構成ファイルの配布」を参照してください。

パラメータ	説明
Maximum Packet Roundtrip Time	パケット受信確認のタイムアウト時間。ある Authentication Manager で、別の Authentication Manager がデータ パケットを受信したことを確認するまでに待機する時間 (秒単位) です。タイムアウト時間に達すると、送信元の Authentication Manager は接続を再確立しようとします。タイムアウト時間は、1 ～ 300 秒の値に設定できます。デフォルト値は 30 です。
Heartbeat Period	この値は、レプリケーション サービスの接続を監視するために使用されます。[Heartbeat Period] に指定された期間にレプリケーション アクティビティがない場合、Authentication Manager では接続が無効であると見なします。接続が無効になっていることをプライマリが検出すると、接続を再確立しようとします。接続が無効になっていることをレプリカが検出すると、レプリケーション サービス ポートでの受信を続行しようとします。指定できる値は 30 ～ 1800 秒です。この値の下限は、常に [Maximum Packet Roundtrip Time] の値の 2 倍です。つまり、この値は、**最低でも**常に [Maximum Packet Roundtrip Time] の値の 2 倍に設定する必要があります。

[Services] (サービスの構成)

パラメータ	説明
Authentication	**services** ファイルに指定されている認証サービスのポート番号と名前。認証サービス プロセスのデフォルト名は *securid* で、デフォルト ポート番号は 5500 です。
Administration	**services** ファイルに指定されているアドミニストレーション サービスのポート番号と名前。アドミニストレーション サービス プロセスのデフォルト名は *sdadmind* で、デフォルト ポート番号は 5550 です。アドミニストレーション サービスは、リモート アドミニストレーションで使用されます。
Lock Manager	**services** ファイルに指定されているロック マネージャのポート番号と名前。ロック マネージャ プロセスのデフォルト名は *sdlockmgr* で、デフォルト ポート番号は 5560 です。

パラメータ	説明
OA Download	**services** ファイルに指定されているオフライン認証ダウンロード サービスのポート番号と名前。OA (オフライン認証) ダウンロード プロセスのデフォルト名は *sdoad* で、デフォルト ポート番号は 5580 です。

ホスト名とサービス名の解決

[Resolve Hosts and Services By Name] チェックボックスの指定によって、RSA Authentication Manager がサーバを識別する方法が決まります。**sdconf.rec** ファイル (Authentication Manager 自体を識別する場合やプライマリと通信する場合) または RSA Authentication Manager データベース (レプリカと通信する場合) の情報を確認し、DNS サーバまたは hosts ファイルおよび services ファイルのエントリと比較します。

- チェックボックスがオンの場合、Authentication Manager は RSA Authentication Manager で実行中のプロセスと RSA Authentication Agent の認証要求をホスト名によって解決します。**/etc/hosts** ファイル、**/etc/services** ファイル、またはネーム サーバを使用して名前を解決します。ホスト名で解決する場合は、名前付けの方式がシステム内で統一されている必要があります。たとえば、ネットワーク上または **hosts** ファイルおよび **services** ファイルで完全修飾名を使用している場合は、**sdconf.rec** ファイルおよび RSA Authentication Manager データベースでも完全修飾名を使用する必要があります。ネットワーク上または **hosts** ファイルおよび **services** ファイルで短い名前を使用している場合は、**sdconf.rec** ファイルおよび RSA Authentication Manager データベースでも短い名前を使用する必要があります。
- チェックボックスがオフの場合、Authentication Manager は RSA Authentication Manager で実行中のプロセスと RSA Authentication Agent の認証要求を IP アドレスによって解決します。RSA Authentication Manager のプロセスの解決には、Authentication Manager では **sdconf.rec** ファイルの IP アドレスを使用します。**sdconf.rec** ファイルの IP アドレスがローカル マシンの IP アドレスに一致しない場合、Authentication Manager では **/etc/hosts** ファイルを確認します。また、必要な場合はネーム サーバの IP アドレスも確認します。RSA Authentication Agent の認証要求では、Authentication Manager は UDP パケットの IP アドレスを使用して、RSA Authentication Manager データベースの RSA Authentication Agent を探します。IP アドレスによる解決は、もっとも柔軟な方法です。たとえば、**hosts** ファイルで短い名前を使用し、DNS ネーム サーバで完全修飾名を使用していても、RSA Authentication Manager は IP アドレスを確認することによって識別を解決できます。

hosts ファイルと DNS サーバの両方を使用する場合、各 Authentication Manager のエントリが両方で同一であり、完全修飾名 (たとえば単に **okeefe** ではなく **okeefe.painter.com**) である必要があります。コンピュータ上の名前自体が完全修飾名である必要はありませんが、完全修飾名でない場合も同一であることが必要です (つまり、単に **okeefe** でもかまいませんが、**okeefe_pc** とすることはできません)。

Authentication Manager 名を変更した場合は、更新された **sdconf.rec** ファイルのコピーをレプリカとすべてのエージェント ホストに配布してください。

[Legacy Agent Server Identification] (旧バージョンのエージェントをサポートするサーバの指定)

パラメータ	説明
Acting Master	アクティング マスタの名前。
Acting Master IP Address	アクティング マスタの IP アドレス。
Acting Slave	アクティング スレーブの名前。
Acting Slave IP Address	アクティング スレーブの IP アドレス。

レプリカにアクティング マスタまたはアクティング スレーブの役割を割り当てる場合は、旧バージョンのエージェント ソフトウェアが動作するすべてのマシンに新しい **sdconf.rec** ファイルのコピーを配布します。[Add Agent Host] メニューを使用して旧バージョンのエージェント ホストを追加し、これらをサポートするために別のレプリカをアクティング マスタおよびアクティング スレーブとして定義する場合は、**sdconf.rec** ファイルを各エージェント ホストにコピーします。Windows エージェント ホストの場合は ***%SYSTEMROOT%¥system32*** ディレクトリにコピーし、UNIX エージェント ホストの場合は ***ACEDATA*** ディレクトリにコピーしてください。詳細については、第 3 章「エージェントとエージェント ホスト上でのアクティブ化」を参照してください。

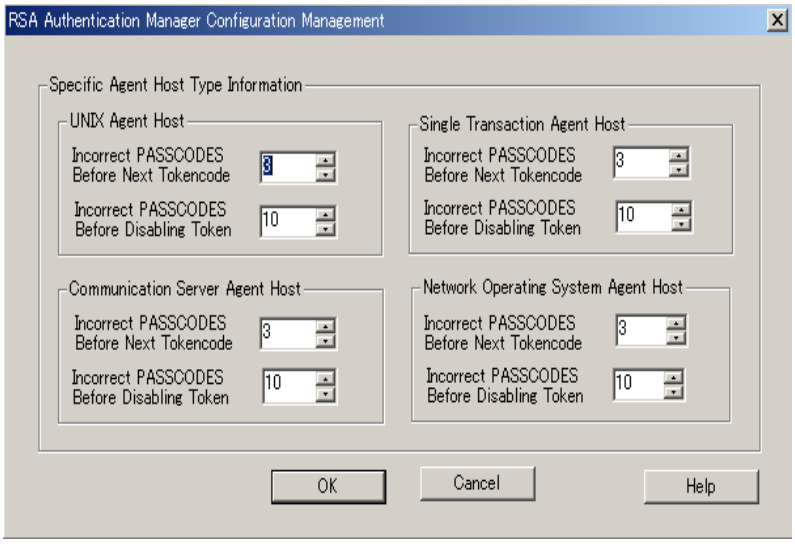
メモ：[Acting Slave Enabled] チェックボックス (231 ページを参照) がオフの場合、指定できるのはアクティング マスタだけです。この場合、図に示したように、アクティング スレーブのボックスは使用できません。

[RSA Authentication Manager Identification] (プライマリとレプリカの指定)

パラメータ	説明
This Server	Configuration Management アプリケーションを実行している Authentication Manager の名前。
This Server IP Address	Configuration Management アプリケーションを実行している Authentication Manager の IP アドレス。
Primary Server	プライマリ Authentication Manager の名前。
Primary Server IP Address	プライマリ Authentication Manager の IP アドレス。

エージェント ホストの PASSCODE の設定

トークンをネクスト トークンコード モードにするか、または無効にするまでに、エージェント ホストが許容する不正な PASSCODE による認証の試みの回数を設定するには、[Configuration Management] ダイアログ ボックスの [Agent Host] をクリックします。[Configuration Management] ウィンドウに [Specific Agent Host Type Information] が表示されます。



ウィンドウには、4 種類のエージェントホストが表示されます。種類ごとに異なるパラメータを設定できます。この手順については、61 ページの「不正な PASSCODE を処理するエージェントの設定」を参照してください。

メモ: RSA Authentication Agent for Microsoft Windows は [Network Operating System Agent Host] です。

このダイアログ ボックス設定のいずれかを変更した場合は、更新された **sdconf.rec** ファイルのコピーをすべてのレプリカに配布し、[RSA Authentication Manager Control Panel] を使用して適用します。次のセクション「更新した構成ファイルの配布」を参照してください。

パラメータ	説明
Incorrect PASSCODES Before Next Tokencode	トークンがネクスト トークンコード モードになるまでに許容される認証の失敗の回数。指定できる値は 1 ～ 20 です。デフォルト値は 3 ですが、暗号化されていない telnet を使用する場合は、それより小さい値に設定することをお勧めします。
Incorrect PASSCODES Before Disabling Token	トークンが無効になるまでに許容される認証の失敗の回数。指定できる値は 2 ～ 25 です。デフォルト値は 10 ですが、暗号化されていない telnet を使用する場合は、それより小さい値に設定することをお勧めします。この値が [Incorrect PASSCODES Before Next Tokencode] の値に 1 以上を加えた値でないと、トークンがネクスト トークンコード モードになることはありません。

更新した構成ファイルの配布

プライマリで Configuration Management アプリケーションを使用して Authentication Manager の構成ファイルを変更した場合は、影響を受けるレプリカとエージェント ホストに更新された **sdconf.rec** を配布する必要があります。

操作手順については、ヘルプの「Distributing the Configuration Update」を参照してください。

メモ : sdconf.rec ファイルは Configuration Management アプリケーションによって作成されます。エージェントは **DES** 暗号方式または **SDI** 暗号方式を使用できます。各エージェント ホストには、使用する暗号方式が正しく設定された **sdconf.rec** ファイルが必要です。**DES** 暗号方式を使用するエージェントと **SDI** 暗号方式を使用するエージェントの両方がある場合は、各エージェント ホストに配布する **sdconf.rec** ファイルに暗号方式が正しく設定されていることを確認してください。

プライマリで Configuration Management アプリケーションを使用して Authentication Manager の構成ファイルを変更した場合は、次の手順に従ってください。

1. 変更の影響を受ける各レプリカの***ACEDATA***ディレクトリに新しい**sdconf.rec**ファイルをコピーします。レプリカで DOS コマンド プロンプトを使用して ***ACEPROG*** ディレクトリに移動し、次のように入力します。

   ```
   sdconfig -update
   ```

   このコマンドを実行すると、レプリカの構成ファイルで [This Server] の名前と IP アドレスが更新されます。

2. プライマリとレプリカをいったん停止してから再起動して、新しい構成を有効にします。

3. 次のいずれかの操作を実行します。
   - 影響を受ける RSA Authentication Agent の ***ACEDATA*** ディレクトリに新しい **sdconf.rec** ファイルをコピーします。または、新しい **sdconf.rec** ファイルを使用できるようにして、適切なエージェントのマニュアルの説明に従って構成を更新するように管理者に指示してください。
   - 旧バージョンのエージェント ホストがある場合は、[Generate Configuration Files] を使用して各アクティング マスタとアクティング スレーブのペアの構成ファイルを新しく生成します。

次の 4 つ以外の構成値を変更した場合は、エージェント ホスト ワークステーションに新しい **sdconf.rec** をインストールする必要があります。

- [Maximum Packet Roundtrip Time]
- [Heartbeat Period]
- [Incorrect PASSCODES Before Next Tokencode]
- [Incorrect PASSCODES Before Disabling Token]

これらの構成値だけを変更した場合は、エージェント ホスト ワークステーションに新しい **sdconf.rec** をインストールする必要はありません。

メモ : RSA Authentication Manager と RSA Authentication Agent の両方を実行する Windows マシンには、***ACEDATA*** ディレクトリと ***%SYSTEMROOT%*¥system32** ディレクトリの両方に **sdconf.rec** ファイルが必要です。

米 RSA Security 社が開発した RSA Authentication Agent 以外のエージェントでは、**sdconf.rec** ファイルを格納し、読み取ることができない可能性があります。一般に、RSA Authentication Agent コードが組み込まれているサードパーティ デバイスは、そのデバイス タイプに固有の構成ファイルを使用します。このようなエージェントに新しい構成情報を配布するには、デバイス メーカーのマニュアルの指示に従ってデバイスを再構成してください。

複数のネットワーク インタフェース間の認証

複数のネットワーク インタフェース間で認証を実行できるように RSA Authentication Manager を設定するには、エイリアス IP アドレスのリストを作成し、各エイリアス IP アドレスに対して新しい構成ファイルを生成する必要があります。IP アドレスはネットワーク内で一意になるように指定してください。

UNIX での複数のネットワーク インタフェース間の認証については、第 15 章「レプリカ管理ユーティリティ (UNIX)」を参照してください。

エイリアス IP アドレスのリストを作成するには

1. [RSA Authentication Manager Contorl Panel] でプライマリのすべてのプロセスをシャットダウンします。
2. プライマリで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックします。
3. 変更する Authentication Manager を選択します。この Authentication Manager が**マルチホーム** Authentication Manager となります。
4. [Details] をクリックします。

   [RSA Authentication Manager Replica Information] ダイアログ ボックスが表示されます。
5. [Alias Information] パネルの [IP Address] ボックスにエイリアス IP アドレスを入力し、[Add] をクリックします。
6. マルチホーム Authentication Manager に割り当てるすべてのエイリアス IP アドレスについて、ステップ 5 を繰り返します。

   メモ：エイリアス IP アドレスは 3 つまで指定できます。
7. エイリアス IP アドレスの追加が終了したら、[OK] をクリックします。
8. プライマリを再起動します。

各エイリアス IP アドレスの構成ファイルを生成するには

1. RSA Authentication Management Host Mode で、[Agent Host] > [Add Agent Host] の順にクリックします。
2. エイリアス IP アドレスを割り当てる RSA Authentication Agent を追加します。詳細については、ヘルプの「Add Agent Host」を参照してください。
3. RSA Authentication Agent をエージェント ホストとして追加したら、[Assign Acting Servers] をクリックします。

4. マルチホーム Authentication Manager をアクティング マスタまたはアクティング スレーブとして使用するには、[IP Address] ドロップダウン メニューで適切なエイリアス IP アドレスを選択します。
5. [Generate Configuration File] をクリックします。
6. メッセージが表示されたら、[Yes] をクリックします。
7. 新しい **sdconf.rec** ファイルを適切な場所に保存します。
8. 対象の RSA Authentication Agent の **%***SYSTEMROOT***%¥system32** ディレクトリ (Windowsの場合)または***ACEDATA***ディレクトリ(UNIXの場合)に新しい**sdconf.rec** をコピーします。
9. 追加した各エイリアス IP アドレスについて、ステップ 1 ～ 8 を繰り返します。

13 レプリカ管理ユーティリティ (Windows)

RSA Authentication Manager レプリカ管理ユーティリティを使用すると、レルム内のレプリカを構成できます。プライマリから次の操作を行うことができます。

- レルムにレプリカを追加したり、レルムからレプリカを削除できます。
- レプリカに関する情報を表示および編集できます。
- レプリカ用にレプリカ パッケージを作成できます。

レプリカでは、プライマリとレプリカに関する情報を表示することだけが可能です。

レプリカ管理ユーティリティの操作手順については、レプリカ管理ユーティリティのヘルプを参照してください。

メモ：レプリカ管理ユーティリティで行う一部の操作では、**sdconf.rec** ファイルが変更されます。構成管理ユーティリティで変更操作を行うと、レプリカ管理ユーティリティで行った変更を上書きする可能性があるため、構成管理ユーティリティが実行されていないことを前もって確認してください。

レプリカ管理ユーティリティを起動するには

1. [RSA Authentication Manager Control Panel] を使用して、RSA Authentication Manager (プライマリまたはレプリカ) 上のすべてのサービスを停止します。

   すべての管理セッションが切断されます。

2. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックします。

   レプリカに接続している場合やデータベース ブローカを停止していない場合、使用できるボタンは [Details] ボタンだけで、Authentication Manager のリストの上に [READ ONLY Access to database] が表示されます。

レプリカ Authentication Manager 情報の表示

次の表は、[RSA Authentication Manager Replica Information] ダイアログ ボックスに表示される情報の一覧です。[RSA Authentication Manager Replica Information] ダイアログ ボックスを表示するには、レプリカ管理ユーティリティのメイン画面にある [Details] をクリックします。

情報	説明
＜マシン名＞ is a Replica または ＜マシン名＞ is a Primary	選択されている Authentication Manager がプライマリであるのか、レプリカであるのか。
Authentication Manager 情報	
Hostname	Authentication Manager のホスト名。
IP Address	Authentication Manager の IP アドレス。
Service Name	プライマリとレプリカが通信するときに使用するサービスの名前。デフォルトの名前は **securidprop_##** であり、## は 00 ～ 10 の範囲の 2 桁の数字です。新規プライマリの場合、デフォルトの名前は **securidprop_00** です。
Service Port Number	プライマリとレプリカが通信するときに使用するポート番号。新規プライマリの場合、デフォルトのポート番号は 5505 です。
Begin Replication Service	プライマリが起動してからレプリケーション サービスが起動するまでの秒数。
Replicate Database Changes Every	データベースの変更がレプリケートされる間隔 (秒単位)。
エイリアス情報	
Alias List	この Authentication Manager に割り当てたエイリアス IP アドレスのリスト。エイリアスを削除する場合は、リストから目的のエイリアスを選択し、[Remove] をクリックします。
IP Address	Authentication Manager に割り当てるエイリアス IP アドレスを入力し、[Add] をクリックします。このボックスと [Add] ボタンを使用できない場合は、Authentication Manager に割り当てられているエイリアスの個数がすでに最大値に達しています。

情報	説明
レプリカ ステータス情報	
Replica Number	レプリカの個数。0 ～ 10 の範囲の値です。
Replica Sequence Number	レプリカ シーケンス番号は、プライマリとレプリカが正しいデータベースを使用していることを確認するためのものです。この番号は、さまざまなタイミング (レプリカを追加する場合やレプリカ パッケージを作成する場合など) で大きくなります。 レプリカが起動し、プライマリへの接続を試みると、両方の Authentication Manager がレプリカ シーケンス番号の値を確認し、プライマリとレプリカの間の初期通信が行われたことを確認します。 レプリカ シーケンス番号が一致していれば、正しいレプリカ パッケージがレプリカにインストールされています。2 つの番号が一致しない場合は、レプリカを停止し、プライマリ上で新しいレプリカ パッケージを作成して、レプリカに送信する必要があります。
Able to Authenticate	[Yes] の場合、レプリカはユーザを認証し、プライマリに対してデータベースの変更をレプリケートできます。[No] の場合、レプリカはユーザを認証し、プライマリに対してデータベースの変更をレプリケートできません。
Initial Primary/Replica Communication has Occurred	[Yes] の場合、プライマリとレプリカの間の初期通信パスは正常に行われました。プライマリとレプリカ間の初期通信が正常に行われたということは、各 Authentication Manager 上のレプリカ シーケンス番号が一致することを表します。[No] の場合、プライマリとレプリカの間の初期通信はまだ行われていません。
Replica Marked for Unconditional Push	[Yes] の場合、データベースのバックアップ コピーをプライマリに復元することでプライマリを復元しました。新しいデータベースは、Push DB Assisted Recovery 機能を使用して既存のすべてのレプリカに配布する必要があります。プライマリがデータベースをプッシュできるように、プライマリのシステム パラメータで [Push DB Assisted Recovery] をオンにしてください。完全なレプリカ パッケージまたは部分的なレプリカ パッケージをレプリカに適用する必要はありません。それ以外の場合、この値は [No] です。

操作手順については、レプリカ管理ユーティリティのヘルプを参照してください。

14 RSA Authentication Manager の構成 (UNIX)

この章では、RSA Authentication Manager の構成を変更する方法について説明します。

RSA Authentication Manager for UNIX でのライセンス レコードの更新

RSA Authentication Manager ライセンスの制限をアップグレードするには、RSA セキュリティ正規販売代理店から新しいライセンス レコードを購入する必要があります。アップグレードの理由としては、アクティブなユーザ数の増加、レプリカ Authentication Manager の追加、レルム数の増加などがあります。

新しいライセンス レコード (**license.rec**) ファイルを入手したら、このセクションの説明に従ってインストールしてください。

RSA Authentication Manager のラインセンスに関する一般情報については、付録 A「ライセンス」を参照してください。トラブルシューティングの情報については、293 ページの「メッセージ」を参照してください。

ライセンス レコードを更新するには

1. プライマリ Authentication Manager に **root** でログオンします。
2. トップ レベルの RSA Authentication Manager ディレクトリ以外のディレクトリに移動します。
3. 新しい **license.rec** ファイルが格納された 3.5 インチ フロッピー ディスクを、Authentication Manager または他のワークステーションのフロッピー ディスク ドライブに挿入します。このドライブから、通常のコピー手順で **license.rec** ファイルをカレント ディレクトリにコピーします。

   重要：マルチサーバ ライセンスを購入した場合、パッケージには Authentication Manager 1 ～ 6 に対応するラベルが付いた 6 枚のライセンス フロッピー ディスクがあります。各プライマリにフロッピー ディスクを 1 枚ずつ割り当て、ラベルに Authentication Manager の名前を記入してください。インストールするときは、**常に**その Authentication Manager に対応するフロッピー ディスクを使用してください。

4. 既存の **license.rec** のバックアップ (**license.old**) を自動的に作成し、新しいライセンス レコードをインストールするには、次のように入力してください。

   ```
   ACEPROG/sdsetup  -license
   ```

   ***ACEPROG*/sdsetup** を実行する前に、既存の **license.rec** のバックアップを手動で作成する必要はありません。ただし、バックアップ ファイルを手動で作成する場合は、**license.old** という名前を使用しないでください。

   メモ：現在の作業ディレクトリにコピーされた **1version** ファイルは、内部的に使用されます。このファイルに関する操作は必要ありません。

5. **aceserver** プロセスをいったん停止してから再起動して、新しいライセンスを有効にします。

   RSA Authentication Manager が再起動すると、プライマリはレルム内のレプリカとの通信を再確立しようとします。通信が再確立されると、プライマリはレプリカに対して新しいライセンス レコードを自動的に有効にします。

RSA Authentication Manager の構成の概要

インストール プログラムが構成ファイルに値を格納し、プログラムが終了すると、ライセンス情報とともにその値が表示されます。

構成ファイル (***ACEDATA*/sdconf.rec**) の値は、次のいずれかです。

- インストール時に管理者が指定した値 (RSA Authentication Manager ファイル オーナの名前など)
- システム セキュリティとユーザの利便性のバランスを考慮して Authentication Manager が選択および設定したデフォルト値
- ***ACEDATA*** ディレクトリにある既存の Authentication Manager の構成ファイルの情報にもとづいて設定された値

システムの現在の構成設定を表示するには、***ACEPROG*/sdinfo** を実行します。次の表は、表示される情報の内容を示しています。

パラメータ	説明
License Creation	ライセンスの作成日。
License ID	ライセンスの作成時に生成されたライセンス ID 番号。
RSA Authentication Manager version	現在のソフトウェアの完全なバージョン番号。***ACEDATA*/version.txt** に格納されている番号と同じです。
Evaluation	このフィールドは、トライアル ライセンスを使用している場合にのみ表示されます。トライアル ライセンスには一定の有効期限があり、期限が切れると RSA Authentication Manager は動作しなくなります。パーマネント ライセンスへの切り替えの詳細については、274 ページの「ライセンスのアップグレードまたは変換」を参照してください。
Violation	このフィールドは、**アップグレード違反**モード (インストール時に確認) のライセンスを使用している場合にのみ表示されます。詳細については、274 ページの「ライセンスのアップグレードまたは変換」を参照してください。
Expiration	このフィールドは、トライアル ライセンスを使用している場合にのみ表示されます。RSA Authentication Manager の評価 (トライアル) 版を使用しているか、またはアップグレード違反モードのライセンスを使用している場合が該当します。
Config File Version	現在の構成ファイルの完全なバージョン番号。

パラメータ	説明
File ownership	RSA Authentication Manager プログラムとデータ ファイルのオーナである管理者のログイン。
Agent retry *value*	「Cannot initialize Agent Host-server communication. (エージェント ホストとサーバ間の通信を初期化できません)」というメッセージが返されるまでに、エージェント ホストが Authentication Manager との通信の確立を試みる回数。
Agent retry *interval* (Agent Timeout)	エージェント ホストと Authentication Manager 間の通信の確立を試みる間隔 (秒単位)。
DES/RC5 Encryption	エージェント ホストと Authentication Manager 間の通信に使用する暗号方式。DES (Data Encryption Standard) または RC5 (米 RSA Security 社が商標を持つ暗号方式) です。
TACACS Plus	有効になっている場合は、**aceserver** を実行したときに TACACS+ サーバが自動的に起動されます。
Primary RSA Authentication Manager と Primary RSA Authentication Manager Address	プライマリ Authentication Manager の名前と IP アドレス。
This Server と This Server Address	**sdinfo** を実行している Authentication Manager の名前と IP アドレス。
Acting Master Server	アクティング マスタの名前と IP アドレス。
Acting Slave Server	アクティング スレーブの名前と IP アドレス。
Replica Timeout	プライマリからレプリカへ、およびレプリカからプライマリへのパケット受信確認のタイムアウト時間。ある Authentication Manager で、別のサーバがデータ パケットを受信したことを確認するまでに待機する時間を秒単位で示します (1 ～ 300)。タイムアウト時間に達すると、送信元の Authentication Manager はプライマリとレプリカ間の接続を再確立しようとします。
Replica Heartbeat	レプリケーション サービスの接続を確認するために使用する値。[Replica Heartbeat] に指定された期間にレプリケーション アクティビティがない場合、Authentication Manager では接続が無効であると見なします。接続が無効になっていることをプライマリが検出すると、接続を再確立しようとします。接続が無効になっていることをレプリカが検出すると、レプリケーション サービス ポートでの受信を続行しようとします。この間隔は、30 ～ 1800 秒の範囲で設定できます。この値の下限は、常に [Replica Timeout] の値の 2 倍です。つまり、[Replica Heartbeat] の値は、**最低でも**常に [Replica Timeout] の値の 2 倍に設定する必要があります。

パラメータ	説明
Authentication service と port number	エージェント ホストと Authentication Manager 間の通信のサービス名とポート番号。システム上のすべての **/etc/services** ファイルの内容と一致している必要があります (デフォルト サービス名は **securid** で、デフォルト ポート番号は **5500** です)。
Addresses	IP アドレスの解決方法。[By IP address in ACE/Server database] は、Authentication Manager プログラムとエージェント ホストが、**/etc/hosts** ファイル、**/etc/services** ファイル、またはネーム サーバを参照せずにサーバ名とサービス名を解決することを表します。その代わりに、Authentication Manager の **sdconf.rec** ファイルを参照します。 [By name in host file or name service] は、**/etc/hosts** ファイル、**/etc/services** ファイル、またはネーム サーバを使用して名前を解決することを表します。この方法は便利ですが、安全性は **/etc/hosts** ファイル、**/etc/services** ファイル、またはネーム サーバの安全性に依存します。これらの安全性を確保する必要があります。
Administration service と port number	アドミニストレーション サービスのサービス名とポート番号。システム上のすべての **/etc/services** ファイルの内容と、リモート アドミニストレーション マシンのサービス エントリに一致している必要があります (デフォルト名は **sdadmind** で、デフォルト ポート番号は **5550** です)。
Lock Manager service と port number	ロック マネージャのサービス名とポート番号 (デフォルト名は **sdlockmgr** で、デフォルト ポート番号は **5560** です)。
Bad PASSCODES before setting Next Tokencode	エージェントの種類ごとの、不正な認証の試みの許容回数。この回数を超えると、トークンはネクスト トークンコード モードになります。
Bad PASSCODES before Disabling Token	エージェントの種類ごとの、不正な認証の試みの許容回数。この回数を超えると、トークンは無効になります。
Response delay	応答がエージェント ホストに返されるまでに認証要求が保留される時間 (秒単位)。この設定は、暗号化されていない telnet 接続でログオンが実行される場合に、そのネットワーク上で特定の種類の攻撃をトラップします。
Alias IP Address List	レルム内のすべての Authentication Manager の実際の IP アドレスとそのエイリアス。IP アドレスのエイリアスは、レプリカ管理ユーティリティを使用して指定します。各 Authentication Manager では、IP アドレスのエイリアスを 3 つまで使用できます。
License	ベース ライセンスまたはアドバンスド ライセンスのライセンス レベル。

パラメータ	説明
Number Licensed Active Users	ライセンスで許可されている RSA Authentication Manager データベースのユーザ数 (各ユーザにはトークンを 3 つまで割り当てることができるため、ライセンスで許可されるトークンの数はこれより多くなることがあります)。
Number Licensed Replicas	ベース ライセンスを所有している場合は **1** です。アドバンスド ライセンスを所有している場合は **10** です。
Number Licensed Realms	ベース ライセンスを所有している場合は **1** です。アドバンスド ライセンスを所有している場合は **6** です。

構成の変更

このセクションでは、それぞれの状況に最適なインストールの構成値を選択するのに役立つ情報を示します。構成ファイル (**sdconf.rec**) をレプリカにコピーするときには、レプリカで **sdconfig -update** を実行する必要があります。

メモ：sdconf.rec ファイルを変更した場合は、RSA Authentication Manager を再起動して変更を反映する必要があります。自動登録を使用しているエージェント ホストがある場合は、データベース ブローカを停止して、エージェント ホストの **sdconf.rec** ファイルを更新する必要があります。

RSA Authentication Manager の構成を変更するには

1. プライマリに **root** でログオンします。
2. ***ACEPROG*/sdsetup -config** を実行します。
3. 構成に関する一連の質問が表示されます。これらの質問に答えることによって、プライマリの ***ACEDATA*** ディレクトリにある **sdconf.rec** ファイルに現在格納されている値を変更できます。表示されるプロンプトは、システムとともに購入したオプションによって異なります。表示される各プロンプトに対する応答の方法については、次の説明を参考にしてください。

   How many seconds should an agent wait before retrying? (エージェントが再試行を開始するまでの待ち時間を何秒に設定しますか)

   エージェント ホストとAuthentication Manager間で通信の確立を試行する間隔を秒単位で指定します。この値は、[Agent Timeout] 値として **sdconf.rec** に格納されます。指定できる値の範囲は 1 ～ 20 で、デフォルト値は 5 です。

   How many times should an agent retry before reporting failure? (失敗を報告するまでにエージェントが再試行する回数を何回に設定しますか)

   「Cannot initialize Agent Host-server communication. (エージェント ホストとサーバ間の通信を初期化できません)」というメッセージが返されるまでに、エージェント ホストが Authentication Manager との通信の確立を試行する回数を指定します。指定できる値の範囲は 1 ～ 6 で、デフォルト値は 5 です。

Do you want to use DES/RC5 encryption? (DES/RC5 暗号方式を使用しますか)

Authentication Manager とエージェント ホスト間の通信を DES/RC5 暗号方式と SDI 暗号方式のどちらで保護するかを指定します。デフォルトの暗号方式は DES/RC5 です。すべてのエージェント ホスト ワークステーションで SDI 暗号方式を使用するように設定されている場合は、SDI を指定します。

一部のエージェント ホストだけが SDI 暗号方式を使用するように登録されている場合は、そのエージェント ホスト レコードの暗号方式を変更するか、または **sdconf.rec** を 2 種類作成する必要があります。一方の値はデフォルト値の DES/RC5 で、もう一方の値は SDI に設定します。詳細については、251 ページの「更新した構成ファイルの配布」を参照してください。

How many wrong PASSCODEs before a token is set to Next Tokencode? (トークンがネクスト トークンコード モードに設定されるまでに入力できる不正な PASSCODE の回数を何回に設定しますか)

トークンがネクスト トークンコード モードに設定されるまでに、不正な RSA SecurID PASSCODE によるログインの失敗を何回まで許容するかを設定します。このモードを有効にすると、不正な PASSCODE が指定した回数だけ入力された場合に、Authentication Manager は次に表示されるコードの入力を要求します。ユーザがトークンに表示される次のコードを入力しないと、アクセスは拒否されます。4 種類のエージェント ホスト (UNIX エージェント、コミュニケーション サーバ、シングル トランザクション エージェント、NOS エージェント) に対して回数を設定できます。指定できる値の範囲は 1 ～ 20 です。デフォルト値は 3 ですが、暗号化された telnet やライン モードの telnet を使用していない場合は、それより小さい値に設定することをお勧めします。

How many wrong PASSCODEs before a token is set disabled? (トークンが無効になるまでに入力できる不正な PASSCODE の回数を何回に設定しますか)

トークンが無効になるまでに、不正な RSA SecurID PASSCODE によるログインの失敗を何回まで許容するかを設定します。4 種類のエージェント ホスト (UNIX エージェント、コミュニケーション サーバ、シングル トランザクション エージェント、NOS エージェント) に対して回数を設定できます。指定できる値の範囲は 2 ～ 25 で、デフォルト値は 10 です。この値は常に、前に説明したネクスト トークンコード モードになるまでの不正な PASSCODE の回数の値に、1 以上を加えた値である必要があります。暗号化されていない telnet を使用する場合は、これらの値を小さく設定することをお勧めします。

Which administrator should own the RSA Authentication Manager files? (RSA Authentication Manager ファイルを所有する管理者を指定してください)

RSA Authentication Manager 管理者で構成される UNIX グループのメンバから、すべての Authentication Manager ファイルのオーナとなるメンバを指定します。

Which port number should be used for authentication? (認証に使用するポート番号を指定してください)

/etc/services に指定した認証サービスのポート番号を入力します。デフォルト値は 5500 です。

What is the service name you will use? (使用するサービス名を指定してください)

認証サービスの名前 (デフォルト値は **securid**) を入力します。これは、**/etc/services** ファイルまたはインフォメーション サーバに指定した名前です。

Do you want to resolve hosts and services by name? (ホストとサービスを名前で解決しますか)

「y」と入力すると、Authentication Manager は RSA Authentication Manager で実行中のプロセスと RSA Authentication Agent の認証要求をホスト名によって解決します。**/etc/hosts** ファイル、**/etc/services** ファイル、またはネーム サーバを使用して名前を解決します。ホスト名で解決する場合は、名前付けの方式がシステム内で統一されている必要があります。たとえば、ネットワーク上または **hosts** ファイルおよび **services** ファイルで完全修飾名を使用している場合は、**sdconf.rec** ファイルおよびRSA Authentication Managerデータベースでも完全修飾名を使用する必要があります。ネットワーク上または **hosts** ファイルおよび **services** ファイルで短い名前を使用している場合は、**sdconf.rec** ファイルおよびRSA Authentication Managerデータベースでも短い名前を使用する必要があります。

「n」と入力すると、Authentication Manager は RSA Authentication Manager で実行中のプロセスと RSA Authentication Agent の認証要求を IP アドレスによって解決します。RSA Authentication Manager のプロセスの解決には、Authentication Manager では **sdconf.rec** ファイルの IP アドレスを使用します。**sdconf.rec** ファイルの IP アドレスがローカル マシンの IP アドレスに一致しない場合、Authentication Manager では **/etc/hosts** ファイルを確認します。また、必要な場合はネーム サーバの IP アドレスも確認します。RSA Authentication Agent の認証要求では、Authentication Manager は UDP パケットの IP アドレスを使用して、RSA Authentication Manager データベースの RSA Authentication Agent を探します。IP アドレスによる解決は、もっとも柔軟な方法です。たとえば、**hosts** ファイルで短い名前を使用し、DNS ネーム サーバで完全修飾名を使用していても、RSA Authentication Manager は IP アドレスを確認することによって識別を解決できます。

What is the name or address of the Primary RSA Authentication Manager? (プライマリ RSA Authentication Manager の名前またはアドレスを指定してください)

プライマリの名前または IP アドレスを入力します。入力する値は **hosts** ファイルの値である必要があります。また、マシンはネットワークに接続されている必要があります。

Which port number should administration use? (アドミニストレーションで使用するポート番号を指定してください)

/etc/services に指定したポート番号を入力します。

What is the service name you will use? (使用するサービス名を指定してください)

リモート アドミニストレーション サービスの名前 (デフォルト値は **sdadmind**) を入力します。これは、**/etc/services** ファイルまたはインフォメーション サーバに指定した名前です。この名前は、リモート アドミニストレーション マシン上のサービス エントリに一致している必要があります。

Which port number should the lock manager use? (ロック マネージャで使用するポート番号を指定してください)

/etc/services に指定したポート番号を入力します。

What is the service name you will use? (使用するサービス名を指定してください)

ロック マネージャ サービスの名前 (デフォルト値は **sdlockmgr**) を入力します。これは、**/etc/services** ファイルまたはインフォメーション サーバに指定した名前です。

Do you want to use TACACS Plus? (TACACS Plus を使用しますか)

「y」と入力すると、**aceserver** を起動したときに TACACS+ デーモンも自動的に起動します。

Do you want to specify an acting master server? (アクティング マスタ サーバを指定しますか)

システムに v5.0 より前の RSA Authentication Agent ソフトウェアを使用しているエージェント ホストがある場合は、「y」と入力します。

古いソフトウェアを実行する旧バージョンのエージェントは、Authentication Manager を識別するために **sdconf.rec** ファイルを使用します。ただし、このファイルでは、マスタとスレーブという 2 つの Authentication Manager しか識別できません。旧バージョンのエージェントから RSA Authentication Manager 6.1 が認証要求を受け付けるには、いずれかのレプリカがマスタとして動作 (アクティング) する必要があります。このため、レプリカを**アクティング** マスタとして指定する必要があります。アクティング マスタが機能していない場合は、アクティング スレーブが旧バージョンのエージェントからの要求に応答します。

システムに旧バージョンのエージェント ソフトウェアを使用するエージェント ホストがない場合は、「n」と入力します。

What is the name or address of the acting master server? (アクティング マスタ サーバの名前またはアドレスを指定してください)

アクティング マスタを指定する場合は、アクティング マスタとして使用するレプリカの名前または IP アドレスを入力します。入力する値は **hosts** ファイルの値である必要があります。また、マシンはネットワークに接続されている必要があります。

Do you want to specify an acting slave server? (アクティング スレーブ サーバを指定しますか)

システムに旧バージョンのエージェント ソフトウェアを使用するエージェント ホストがある場合は、「y」と入力します (詳細については、「Do you want to specify an acting master server? (アクティング マスタ サーバを指定しますか)」を参照してください)。

アクティング スレーブは、アクティング マスタが機能しなくなると、旧バージョンのエージェントの要求に応答します。

システムに旧バージョンのエージェント ソフトウェアを使用するエージェント ホストがない場合は、「n」と入力します。

What is the name or address of the acting slave server? (アクティング スレーブ サーバの名前またはアドレスを指定してください)

アクティング スレーブを指定する場合は、アクティング スレーブとして使用するレプリカの名前または IP アドレスを入力します。入力する値は **hosts** ファイルの値である必要があります。また、マシンはネットワークに接続されている必要があります。

The Primary expects an acknowledgment for each packet it sends to a Replica. How many seconds should the Replica wait for this acknowledgment? (プライマリはレプリカに送信した各パケットの受信確認を待ちます。受信確認のためのレプリカの待ち時間を何秒に設定しますか)

接続が無効であると見なされる前に、プライマリがレプリカからパケットの受信確認を受け取るまでの待ち時間を秒単位で入力します。受信確認のタイムアウト時間に達すると、Authentication Manager は接続を再確立しようとします。この値には、[Replica Timeout] というラベルが付いています。タイムアウト時間は、1 ～ 300 秒の値に設定できます。

Heartbeat in seconds (Heartbeat 値を秒単位で指定してください)

この値は、レプリケーション サービスの接続を確認するために使用されます。[Replica Heartbeat] に指定された期間にレプリケーション アクティビティがない場合、Authentication Manager では接続が無効であると見なします。接続が無効になっていることをプライマリが検出すると、接続を再確立しようとします。接続が無効になっていることをレプリカが検出すると、レプリケーション サービス ポートでの受信を続行しようとします。この間隔は、30 ～ 1800 秒の範囲で設定できます。この値の下限は、常に [Replica Timeout] の値の 2 倍です。つまり、[Replica Heartbeat] の値は、**最低でも**常に [Replica Timeout] の値の 2 倍に設定する必要があります。プロンプトには適切な範囲が表示されます。

How many seconds should the Authentication Manager queue agent responses? (Authentication Manager がエージェントの応答をキューイングする時間を何秒に設定しますか)

応答がエージェント ホストに返されるまでに、認証要求が保留される時間を秒単位で入力します。このオプションは、暗号化されていない telnet 接続でログインが実行される場合に、そのネットワーク上で特定の種類の攻撃をトラップするために使用されます。値を 2 秒に設定すると、パフォーマンスは低下しません。入力できる最大値は 15 秒ですが、[Agent Retries] 値に [Agent Timeout] 値を乗算した値を超える値は入力しないでください。たとえば、[Agent Retries] 値の設定が 2 で、[Agent Timeout] 値の設定が 2 の場合、遅延の値として 4 より大きい値は使用しないでください。

sdconf.rec に格納されているサービス名やサービス ポート番号が **/etc/services** ファイルにない場合は、警告メッセージが表示されます。メッセージには、解決できないサービス名とポート番号が示されます。これらの情報は慎重に確認してください。これらが正しくない場合は、「r」(reconfigure : 再構成) と入力して **sdconf.rec** の値を変更します。表示された内容が正しい場合は、「s」と入力してシェルに移動し、**/etc/services** を編集してこれらの行を追加または変更してください。

更新した構成ファイルの配布

メモ : sdconf.rec ファイルは Configuration Management アプリケーションによって作成されます。エージェントは **DES** 暗号方式または **SDI** 暗号方式を使用できます。各エージェント ホストには、使用する暗号方式が正しく設定された **sdconf.rec** ファイルが必要です。一部のエージェント ホストだけが SDI 暗号方式を使用するように登録されている場合は、そのエージェント ホスト レコードの暗号方式を変更するか、または **sdconf.rec** を 2 種類作成する必要があります。一方の値はデフォルト値の DES/RC5 で、もう一方の値は SDI に設定します。各エージェント ホストに配布する **sdconf.rec** ファイルの暗号方式が正しく設定されていることを確認してください。

プライマリで ***ACEPROG*/sdsetup -config** を実行して Authentication Manager の構成ファイルを変更した場合は、**aceserver** をいったん停止してから再起動して、新しい構成値を有効にしてください。

変更した構成値が、[Replica Timeout]、[Replica Heartbeat]、[Bad PASSCODES before setting Next Tokencode]、[Bad PASSCODES before Disabling Token] だけの場合は、新しい **sdconf.rec** をエージェント ホスト ワークステーションにインストールする必要はありません。それ以外の構成値を変更した場合は、新しい **sdconf.rec** をインストールする必要があります。次の手順に従ってインストールしてください。

レプリカとエージェント ホスト ワークステーションに新しい sdconf.rec ファイルをインストールするには

1. 新しい構成ファイルの ***ACEDATA*/sdconf.rec** をプライマリからターゲット UNIX ワークステーションにコピーします。
2. ターゲット ワークステーションに **root** でログインします。
3. **sdconf.rec** をコピーしたディレクトリに移動します。
4. 次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -config
   ```

   これにより、新しい構成ファイルがターゲット ワークステーションの ***ACEDATA*** ディレクトリにインストールされます。ファイルを単に ***ACEDATA*** ディレクトリにコピーするだけのコマンドは使用しないでください。その代わりに、***ACEPROG*/sdsetup -config** コマンドを使用します。
5. エージェント ホスト ワークステーションでは、新しい構成ファイルは、インストールと同時に有効になります。レプリカでは、インストール後にそのマシンで **aceserver** をいったん停止してから再起動しないと、新しい構成は有効になりません。

UNIX ワークステーション以外で、米 RSA Security 社が開発した RSA Authentication Agent ではないエージェント ホストを使用する場合、**sdconf.rec** ファイルを格納し、読み取ることができない可能性があります。一般に、RSA Authentication Agent コードが組み込まれているサードパーティ デバイスは、そのデバイス タイプに固有の構成ファイルを使用します。このようなエージェント ホストに新しい構成情報を配布するには、デバイス メーカーのマニュアルの指示に従ってデバイスを再構成する必要があります。

RSA Authentication Agent for Microsoft Windows など、RSA Security 社が開発した UNIX 以外のプラットフォーム用の RSA Authentication Agent は、**sdconf.rec** を格納し、読み取ることにより、構成情報を使用できます。すべてのエージェント ホスト管理者が新しい **sdconf.rec** を使用できるようにした上で、適切な RSA Authentication Agent のマニュアルの説明に従ってエージェント ホストの構成を更新するように指示してください。

エージェント ホストの名前または IP アドレスの変更

エージェント ホストの自動登録および更新プログラム (**sdadmreg**) を使用していない場合、エージェント ホストの IP アドレスを変更するには、このセクションの手順に従って RSA Authentication Manager データベースを更新してください。**sdadmreg** のインストールと使用方法については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

エージェント ホストの名前または IP アドレスを変更するには

1. Authentication Manager の **/etc/hosts** ファイルまたはシステムのインフォメーション サービスを、エージェント ホストの新しい名前または IP アドレスに更新します。
2. アドミニストレーション マシンで、RSA Authentication Manager Host Mode を実行します。
3. [Agent Host] メニューの [Edit Agent Host] をクリックします。
4. エージェント ホスト マシンの名前を変更した場合は、[Name] フィールドを編集し、TAB キーを押します。

   名前は変更せずに IP アドレスを変更した場合は、TAB キーを押して [Name] フィールドの外にカーソルを移動します。

   どちらの場合も、TAB キーを押すと、ステップ 1 に示した **/etc/hosts** またはインフォメーション サービスのエントリにもとづき、[Network address] フィールドが自動的に更新されます。

エージェント ホストの複数の IP アドレス

エージェント ホストを RSA Authentication Manager データベースに追加するときに、[Add Agent Host] ダイアログ ボックスの [Name] フィールドにマシンのプライマリ名を入力します。TAB キーを押して [Name] フィールドを終了すると、ローカル **hosts** ファイルまたはネーム サーバの情報にもとづき、エージェント ホストの IP アドレスが [Network address] フィールドに自動的に表示されます。このネットワーク アドレスは、エージェント ホストで **sdinfo** (または **clntchk**) を実行したときに表示されるアドレスと同じです。

エージェント ホストに複数のノード名と IP アドレスがある場合は、セカンダリ ノードとして Authentication Manager データベースに複数の名前を登録できます。

複数のノード名と IP アドレスがあるエージェント ホストを登録するには

1. アドミニストレーション マシンで、RSA Authentication Manager Host Mode を実行します。
2. [Agent Host] メニューの [Edit Agent Host] をクリックし、更新対象のレコードがあるエージェント ホストを選択します。
3. [Secondary Nodes] ボタンをクリックします。

   [Select Secondary Node] ダイアログ ボックスが表示され、既存のセカンダリ ノードが表示されます。

4. セカンダリ ノードのリストに新しい名前を追加するには、ボックスに名前を入力します。TAB キーを押してフィールドを終了するか、[OK] をクリックしてダイアログ ボックスを閉じます。

5. 入力した名前がローカル **hosts** ファイルまたはネーム サーバにある場合は、[Add Secondary Node] ダイアログ ボックスが開き、エージェント ホストのプライマリ名、新しいセカンダリ名とセカンダリ ネットワーク アドレスが表示されます。[OK] をクリックしてこのノード情報をリストに追加します。

15 レプリカ管理ユーティリティ (UNIX)

RSA Authentication Manager レプリカ管理ユーティリティ (**sdsetup -repmgmt** または **sdrepmgmt**) を使用すると、レルム内のレプリカを構成できます。プライマリから次の操作を行うことができます。

- レルムにレプリカを追加したり、レルムからレプリカを削除できます。
- レプリカまたはプライマリの名前または IP アドレスを変更できます。
- レプリカに関する情報を表示および編集できます。
- プライマリ データベースをレプリカにプッシュできます。

レプリカでは、プライマリとレプリカに関する情報の表示のみを行うことができます。

レプリカ管理ユーティリティの起動

レプリカ管理ユーティリティを実行すると、Authentication Manager に関する情報をいつでも表示できます。ただし、Authentication Manager 情報を変更する場合は、データベース ブローカをシャットダウンする必要があります。ブローカをシャットダウンすると、データベースに接続しているすべての管理セッションが切断されます。コマンド ラインで次のコマンドを入力します。

```
ACEUTILS/rptconnect stop
```

レポート作成ユーティリティが停止します。続いて次のコマンドを入力してください。

```
ACEPROG/aceserver stop
ACEPROG/sdconnect stop
```

対話モードとコマンド ライン モード

ユーティリティを実行するには、対話モードとコマンド ライン モードの 2 種類の方法があります。対話モードでは、画面の指示に従って情報を 1 つずつ入力します。コマンド ライン モードでは、263 ページの「構文」に示されているオプションと引数を使用して、必要なすべての情報を 1 つのコマンドで入力できます。対話モードを使用できるのは、レプリカを追加、変更、削除、または交換する場合だけです。コマンド ライン モードは、すべてのレプリカ管理作業で使用できます。

ユーティリティを対話モードで実行するには、次のセクションで説明するコマンドだけを入力します。コマンド ライン モードで実行するには、必要なすべてのオプションと引数を指定する必要があります。必要なすべてのオプションと引数が指定されていない場合、コマンドは実行されず、失敗のメッセージが表示されます。

レプリカの追加

レプリカ管理ユーティリティの対話モードでは、レプリカに関する情報の入力が求められます。対話モードでレプリカを追加するには、コマンド プロンプトで次のコマンドを入力します。

```
sdsetup -repmgmt add
```

画面の指示に従って操作を完了します。

Name of the Replica (レプリカの名前)

レプリカ名を入力すると、RSA Authentication Manager はデータベース内でレプリカ名の解決を試みます。名前が解決されなくても、その名前を使用できます。別の名前を入力することもできます。

IP Address (IP アドレス)

レプリカ名が解決されると、有効な IP アドレスが表示されます。表示されたアドレスを使用することも、別のアドレスを指定することもできます。指定したアドレスが無効の場合は、再び入力が要求されます。

Alias IP Addresses (エイリアス IP アドレス)

最大 3 つのエイリアス IP アドレスを指定できます。レプリカがファイアウォールを経由してプライマリと通信している場合は、少なくとも、プライマリ Authentication Manager が認識していて有効なメインの IP アドレスまたは 1 つのエイリアスを指定する必要があります。

Service Name (サービス名)

デフォルトのサービス名を使用するか、別のサービス名を指定します。使用するサービス名は、**services** ファイルにエントリとして追加されている必要があります。デフォルトの名前は **securidprop_##** です。## は 00 ～ 10 の範囲の 2 桁の数字です。

Service Port (サービス ポート)

デフォルトのポート番号を使用するか、別のポート番号を指定します。使用するポート番号は、**services** ファイルにエントリとして追加されている必要があります。プライマリのデフォルト値は 5505 です。レプリカを追加するたびに、番号は 1 つずつ増加します。たとえば、最初に追加するレプリカの番号は 5506 になります。

Delay (遅延)

プライマリが起動してからレプリケーション サービスが起動するまでの秒数。最初に追加するレプリカのデフォルト値は 10 です。2 番目以降の各レプリカでは、値が 10 ずつ増加します。

Interval (間隔)

データベースの変更がレプリケートされる間隔(秒単位)。デフォルト値は100秒です。

レプリカの変更

レプリカ情報を変更するには、コマンド プロンプトで次のコマンドを入力します。

```
sdsetup -repmgmt modify
```

最初のプロンプトで、変更するレプリカの名前を指定します。残りのプロンプトは、レプリカを追加するときに表示されるプロンプトと同じです。詳細については、前のセクション「レプリカの追加」を参照してください。

レプリカの交換

レプリカを交換するには、次のコマンドを入力します。

```
sdsetup -repmgmt replace
```

交換するレプリカの名前または IP アドレスの入力が求められます。次に、新しいレプリカの名前の入力が求められます。レプリカの交換の詳細については、142 ページの「レプリカのハードウェアの交換」を参照してください。

メモ：レプリカを交換する場合は、レプリカをあらかじめシャットダウンしておいてください。レプリカを最初にシャットダウンせずに交換すると、レプリカはデータベースからは削除されますが、無効になっていません。この状態では、レプリカはプライマリと通信できません。

レプリカの削除

レプリカを削除するには、次のコマンドを入力します。

```
sdsetup -repmgmt delete Replica name
```

レプリカを削除すると、データベースからレプリカのエントリが削除されます。

重要：レプリカを再び使用する予定がない場合でも、レプリカをシャットダウンしてユーザの認証を停止し、レプリカ マシンから RSA Authentication Manager ソフトウェアをアンインストールする必要があります。

Authentication Manager 情報の表示

すべてのレプリカに関する情報を表示するには、次のコマンドを入力します。

```
sdsetup -repmgmt list
```

1 つのレプリカに関する情報を表示するには、次のコマンドを入力します。

```
sdsetup -repmgmt list Replica name
```

次の表は、**list** オプションで表示される情報を示しています。

情報	説明
Replica #	選択した Authentication Manager のレプリカ番号と、Authentication Manager のホスト名。
IP Address	Authentication Manager の IP アドレス。
Replica Service Name	プライマリとレプリカが通信するときに使用するサービスの名前。デフォルトの名前は **securidprop_##** です。## は 00 ～ 10 の範囲の 2 桁の数字です。
Service Port Number	プライマリとレプリカが通信するときに使用するポート番号。
Startup Delay Interval	プライマリが起動してからレプリケーション サービスが起動するまでの秒数。プライマリでは、このフィールドは使用されません。
Replication Interval	データベースの変更がレプリケートされる間隔 (秒単位)。
Enabled	レプリカがユーザを認証し、プライマリに対してデータベースの変更をレプリケートできるかどうかを指定します。 表示される値は次のとおりです。 **0**: レプリカは、ユーザの認証や変更のレプリケートを実行できません。 **1**: レプリカはユーザを認証し、プライマリに対してデータベースの変更をレプリケートできます。
Primary	Authentication Manager がプライマリであるのか、レプリカであるのかを指定します。 表示される値は次のとおりです。 **0**: レプリカ **1**: プライマリ
Connected	プライマリとレプリカの間の初期通信パスが正常に行われたかどうかを示します。 表示される値は次のとおりです。 **0**: プライマリとレプリカの間の初期通信は行われませんでした。 **1**: プライマリとレプリカの間の初期通信は正常に行われました。

情報	説明
Replica Marked for Unconditional Push	**1** の場合、データベースのバックアップ コピーをプライマリに復元することでプライマリを復元しました。新しいデータベースは、Push DB Assisted Recovery 機能を使用して既存のすべてのレプリカに配布する必要があります。プライマリがデータベースをプッシュできるように、プライマリのシステム パラメータで [Push DB Assisted Recovery] をオンにしてください。完全なレプリカ パッケージまたは部分的なレプリカ パッケージをレプリカに適用する必要はありません。それ以外の場合、この値は **0** です。
Replica Sequence Number	レプリカ シーケンス番号は、プライマリとレプリカが正しいデータベースを使用していることを確認するためのものです。この番号は、さまざまなタイミング (レプリカを追加する場合やレプリカ パッケージを作成する場合など) で大きくなります。 レプリカが起動し、プライマリとの接続を試みると、両方の Authentication Manager は Connected フラグの値と、Replica Sequence Number (レプリカ シーケンス番号) の値を調べます。 レプリカ シーケンス番号が一致していれば、正しいレプリカ パッケージがレプリカにインストールされています。2 つの番号が一致しない場合は、レプリカを停止し、プライマリ上で新しいレプリカ パッケージを作成して、レプリカに送信する必要があります。

プライマリの名前または IP アドレスの変更

プライマリの名前または IP アドレスを変更するには

1. プライマリで ***ACEPROG*** ディレクトリに移動します。
2. プライマリの名前を変更するには、次のコマンドを入力します。

   ```
   sdsetup -repmgmt modify old name name new name
   ```

   プライマリの IP アドレスを変更するには、次のコマンドを入力します。

   ```
   sdsetup -repmgmt modify old address address new address
   ```

   プライマリの名前と IP アドレスの両方を変更するには、次のコマンドを入力します。

   ```
   sdsetup -repmgmt modify old name name new name address new
   address
   ```

3. プライマリ システムで名前または IP アドレスを変更し、マシンを再起動します。
4. プロンプトで次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -repmgmt list
   ```

   レプリカ管理ユーティリティを実行すると、システム名 (または IP アドレス) とデータベース内のプライマリ名が一致するかどうか確認されます。

次のメッセージが表示された場合は、「y」と入力して変更を確認します。

```
The name and/or IP address of this Primary Server has changed
(このプライマリ サーバの名前または IP アドレスが変更されました)

from: (変更前)
old_namenn.nn.nn.nn
to: (変更後)
new_namenn.nn.nn.nn
Type 'No' to cancel: (キャンセルするには「no」と入力します)
```

次のいずれかのメッセージが表示された場合は、システム情報を変更していないか、またはステップ 2 で指定した情報と異なる情報に変更したと考えられます。

```
You are about to complete the change of this Primary Server's
name and/or IP address, however, the name previously specified
does not match the name of this system.
Do you want to accept this name? [new_name]
Enter 'YES' to continue or ¥NO' to cancel
(このプライマリ サーバの名前または IP アドレスの変更を完了しようとしていますが、指定した名前はこのシステムの名前と一致しません。この名前を登録しますか。登録する場合は「YES」、キャンセルする場合は「NO」と入力してください)

You have initiated the procedure to change the name and/or IP
address of this primary RSA ACE/Server. The name and/or IP
address of this system has not yet changed. Follow the
instructions for changing the name and reboot the system.
(このプライマリ RSA ACE/Server の名前または IP アドレスの変更を開始しました。このシステムの名前または IP アドレスはまだ変更されていません。指示に従って名前を変更した後、システムを再起動してください)
```

5. プライマリで Push DB が有効に設定されている場合は、***ACEDATA*/replica_package/license** ディレクトリだけをすべてのレプリカにコピーします。プライマリで Push DB が無効に設定されている場合は、***ACEDATA*/replica_package** ディレクトリをすべてのレプリカにコピーします。

   Push DB の詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

6. レプリカ パッケージを適用します。レプリカで次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -apply_package pathname
   ```

   pathname はレプリカ パッケージ ファイルの場所です。

プライマリの名前を変更した場合は、次の操作を実行する必要があります。

メモ: これらの操作を実行する場合は、必要に応じて関連ヘルプを表示できるように、Remote Administration を使用してください。Remote Administration を有効にするには、プライマリでまず、以下の最初の項目を実行する必要があります。その後、リモート アドミニストレーション マシンで他の操作を任意の順序で実行できます。Remote Administrationの詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』または第 2 章「RSA Authentication Manager Administration アプリケーションの使用」を参照してください。

- すべてのリモート アドミニストレーション マシンで、**sdconf.rec** および **server.cer** ファイルをプライマリの ***ACEDATA*** ディレクトリからリモート アドミニストレーション マシンにコピーし、プライマリをリモート アドミニストレーション マシンから削除し、新しい **sdconf.rec** ファイルを使用してプライマリを追加します。詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。
- Authentication Manager をレルム間認証用のリモート レルム Authentication Manager またはローカル レルム Authentication Manager として指定する場合は、新しい名前または IP アドレスを反映するように、ローカル レルム データベースおよびリモート レルム データベースのレルム レコードを編集します。詳細については、ヘルプの「Edit Realm」を参照してください。
- Authentication Manager を RADIUS サーバとして定義する場合は、新しい名前または IP アドレスを使用するように、すべての RADIUS クライアントを構成します。構成手順については、NAS デバイスのマニュアルを参照してください。さらに、新しい名前または IP アドレスを反映するように、RSA RADIUS サーバのエージェント ホスト レコードを変更する必要があります。変更方法については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』の「サーバをエージェント ホストとしてプライマリ データベースへ追加」を参照してください。
- Authentication Manager を旧バージョンのエージェント ホストのアクティング Authentication Manager として定義する場合は、この Authentication Manager をアクティング マスタまたはアクティング スレーブとして使用する旧バージョンのすべてのエージェント ホストに対して、新しい **sdconf.rec** ファイルを作成し、その **sdconf.rec** ファイルをエージェント ホストに配布します。詳細については、ヘルプの「Assign Acting Servers」を参照してください。
- Authentication Manager を v5 のエージェント ホストの **sdopts.rec** ファイルに指定する場合は、Authentication Manager の新しい名前または IP アドレスを反映するように、エージェント ホストで **sdopts.rec** ファイルを編集します。

複数のネットワーク インタフェース間の認証

メモ: Windows システムでのすべてのネットワーク インタフェース間の認証については、237ページの「複数のネットワーク インタフェース間の認証」を参照してください。

複数のネットワーク インタフェース間で認証を行うように RSA Authentication Manager を設定するには、エイリアス IP アドレス リストを作成し、各エイリアス IP アドレスに対して新しい構成ファイルを作成する必要があります。

エイリアス IP アドレスのリストを作成するには

1. プライマリのすべてのプロセスをシャットダウンします。詳細については、263 ページの「コマンド ラインでの操作」を参照してください。
2. プライマリで ***ACEPROG*** ディレクトリに移動します。
3. プロンプトで次のコマンドを入力します。

```
sdsetup -repmgmt modify
```

4. プロンプトで、変更する Authentication Manager の名前を入力します。この Authentication Manager が**マルチホーム** Authentication Manager となります。

5. [Replica Service Name]、[Startup Delay Interval]、および [Replication Interval] に対してはデフォルトを使用します。
6. 「Alias1」というプロンプトが表示されたら、Authentication Manager のエイリアス IP アドレスを入力します。
7. 「Alias2」および「Alias3」というプロンプトに対しても、ステップ6を繰り返します。

メモ：エイリアス IP アドレスは 3 つまで指定できます。

8. プライマリを再起動します。

次の手順は TTY モードで実行できますが、Remote Administration を使用することを推奨します。Remote Administration の詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』または第 2 章「RSA Authentication Manager Administration アプリケーションの使用」を参照してください。

各エイリアス IP アドレスの構成ファイルを生成するには

1. Remote Administration インタフェースで、[Agent Host] > [Add Agent Host] の順にクリックします。
2. エイリアス IP アドレスを割り当てる RSA Authentication Agent を追加します。詳細については、ヘルプの「Add Agent Host」を参照してください。
3. RSA Authentication Agent をエージェント ホストとして追加したら、[Assign Acting Servers] をクリックします。
4. マルチホーム Authentication Manager をアクティング マスタまたはアクティング スレーブとして使用するには、[IP Address] ドロップダウン メニューで適切なエイリアス IP アドレスを選択します。
5. [Generate Config File] をクリックします。
6. プロンプトが表示されたら、[Yes] をクリックします。
7. 新しい **sdconf.rec** ファイルを適切な場所に保存します。
8. 新しい **sdconf.rec** を、作成した RSA Authentication Agent の **%*SYSTEMROOT*%¥system32** ディレクトリ (Windows) または ***ACEDATA*** ディレクトリ (UNIX) にコピーします。
9. 追加した各エイリアス IP アドレスについて、ステップ 1 ～ 8 を繰り返します。

コマンド ラインでの操作

レプリカ管理ユーティリティを実行すると、Authentication Manager に関する情報をいつでも表示できます。ただし、Authentication Manager 情報を変更する場合は、データベース ブローカをシャットダウンする必要があります。ブローカをシャットダウンすると、データベースに接続しているすべての管理セッションが切断されます。

構文

sdsetup -repmgmt ユーティリティの構文は次のとおりです。

```
sdsetup -repmgmt [add|modify [Replica name|IP address]]
[name|address|servicename|port|delay|interval|alias IP
address, IP address, IP address]

sdsetup -repmgmt [list|delete] Replica_name
```

次の表は、**sdsetup -repmgmt** ユーティリティのオプションを示しています。

オプション	引数	説明
add	name *Replica name* または address *Replica IP address*	データベースにレプリカ Authentication Manager を追加します。
list	*Replica name* または *Replica IP address* または なし	引数を省略すると、すべてのレプリカ Authentication Manager に関する詳細情報が出力されます。引数を指定すると、指定したレプリカ Authentication Manager に関する情報が出力されます。
delete	*Replica name* または *Replica IP address*	指定されたレプリカ Authentication Manager を削除します。

オプション	引数	説明
modify		特定のレプリカの構成情報を変更します。レプリカは、完全修飾名または IP アドレスによって指定します。次の情報を変更できます。
	Replica name または ***Replica IP address***	レプリカ Authentication Manager (またはプライマリ Authentication Manager) の名前。
	address ***IP address of the Replica (*** または ***Primary)***	レプリカ Authentication Manager (またはプライマリ Authentication Manager) の IP アドレス。
	name ***name of the Replica (*** または ***Primary)***	プライマリ / レプリカ通信で使用されているサービス名。
	servicename ***name of the service***	プライマリでサービス名を変更する場合は、**sdsetup -port_config** コマンドを使用してレプリカでサービス名を変更する必要があります。
	port ***port number***	プライマリ / レプリカ通信で使用されているポート番号。プライマリでサービス ポート番号を変更する場合は、**sdsetup -port_config** コマンドを使用してレプリカでサービス ポート番号を変更する必要があります。
	delay ***number of seconds***	プライマリが起動してからレプリケーション サービスが起動するまでの秒数。
	interval ***number of seconds***	プライマリとレプリカが調整を行うまでの待ち時間。
	alias ***ip1***, ***ip2***, ***ip3***	Authentication Manager のエイリアス IP アドレス。エイリアス IP アドレスを使用すると、エージェント ホストは、ファイアウォールを経由して認証要求を送信できます。最大 3 つのエイリアスを指定できます。

レプリカの追加 (コマンド ライン)

レプリカを追加するには、次のコマンドを入力します。

```
sdsetup -repmgmt add name Replica name
```

RSA Authentication Manager データベースにレプリカが追加されます。**list** オプションを使用した場合は、レプリカの名前と情報が表示されます。

必要に応じて、データベースに Authentication Manager を追加するときに、エイリアス IP アドレスをレプリカに割り当てることができます。次のコマンドを入力します。

```
sdsetup -repmgmt add name Replica name alias IP address, IP
address, IP address
```

1 つの Authentication Manager に対して最大 3 つのエイリアス アドレスを追加できます。レプリカを追加した後でも、**modify** オプションを使ってエイリアスを割り当てることができます。その場合も、割り当てることができるエイリアスの数は最大 3 つです。

レプリカの追加が終了した後、レプリカ パッケージを作成する必要があります。詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

エイリアス IP アドレスの割り当て

1 つの Authentication Manager に対して最大 3 つのエイリアス IP アドレスを割り当てることができます。Authentication Manager にエイリアス IP アドレスを割り当てるには、次のコマンドを入力します。

```
sdsetup -repmgmt modify Replica_name alias IP address, IP
address, IP address.
```

IP アドレスの 1 つを変更する必要がある場合は、リスト内で変更しない各エイリアスを再入力し、削除する IP アドレスの代わりに新しい IP アドレスを入力します。

たとえば、エイリアスのリストに次の IP アドレスが登録されているとします。

```
1.2.3.4
1.2.3.5
1.2.3.6
```

エイリアス **1.2.3.6** を **1.2.3.7** に変更する場合は、次のコマンドを入力します。

```
sdsetup -repmgmt 1.2.3.4, 1.2.3.5, 1.2.3.7
```

1.2.3.5 を削除し、他のエイリアスはそのまま登録しておく場合は、次のコマンドを入力します。

```
sdsetup -repmgmt 1.2.3.4, 1.2.3.7
```

すべてのエイリアスを削除する場合は、次のコマンドを入力します。

```
sdsetup -repmgmt ,,
```

メモ : add オプションを使用してレプリカを追加するときに、エイリアス IP アドレスを割り当てることもできます。

レプリカ情報の変更 (コマンド ライン)

レプリカ情報 (たとえば、サービス名やサービス ポート番号) を変更した場合、次回のレプリケーション パスが実行されるまで、どのレプリカでも変更結果を表示できません。レプリカに関する最新の情報を表示するには、レプリカ管理ユーティリティをプライマリで実行します。すべてのレプリカに関する情報を表示するには、次のコマンドを入力します。

```
sdsetup -repmgmt list
```

1 つのレプリカに関する情報を表示するには、次のコマンドを入力します。

```
sdsetup -repmgmt list Replica name
```

次の例では、スタートアップ遅延時間をデフォルト値の 10 から 15 に変更する方法を示しています。**modify** オプションの引数の詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

スタートアップ遅延時間を変更するには

1. ***ACEPROG*** ディレクトリに移動します。
2. コマンド ラインで次のコマンドを入力します。

   ```
   sdsetup -repmgmt modify Server_name delay 15
   ```

サービス名またはサービス ポート番号を変更するには

1. ***ACEPROG*** ディレクトリに移動します。
2. コマンド ラインで次のコマンドを入力します。

   ```
   sdsetup -port_config portnum "new_portname" "new_portnum"
   ```

   portnum は変更前のポート番号、*portname* は新しいポート名、*new_portnum* は新しいポート番号です。元の名前またはポート番号を変更しない場合は、新しい名前または番号の代わりに 2 つの引用符を指定します。たとえば、ポート 5508 の情報を securidprop_03 から securidprop_20 に変更するには、次のコマンドを入力します。

   ```
   sdsetup -port_config 5508 "" "securidprop_20"
   ```

レプリカの名前または IP アドレスを変更するには

1. OS でレプリカ システムの名前または IP アドレスを変更し、マシンを再起動します。
2. プライマリで ***ACEPROG*** ディレクトリに移動します。
3. **ping** または **telnet** コマンドを使用して、変更中のレプリカにプライマリからアクセスできるかどうか確認します。
4. レプリカの名前と IP アドレスのいずれか一方または両方を、次のように RSA Authentication Manager で変更します。

   レプリカの名前を変更するには、次のコマンドを入力します。

   ```
   sdsetup -repmgmt modify oldname name newname
   ```

   レプリカの IP アドレスを変更するには、次のコマンドを入力します。

   ```
   sdsetup -repmgmt modify oldaddress address newaddress
   ```

   メモ : レプリカの名前を変更すると、RSA Authentication Manager は IP アドレスを自動的に解決します。同様に、レプリカの IP アドレスを変更すると、RSA Authentication Manager は名前を自動的に解決します。

5. プロンプトで次のコマンドを入力します。

```
sdsetup -repmgmt list Replica_name
```

Replica_name は新しいレプリカ名です。

レプリカ管理ユーティリティを実行すると、システム名 (または IP アドレス) とデータベース内のレプリカ名が一致するかどうか確認されます。

情報が一致しない場合は、システム情報を変更していないか、またはステップ 4 で指定した情報と異なる情報に変更したと考えられます。

6. プライマリで Push DB 機能が有効な場合は、***ACEDATA*/replica_package/license** ディレクトリだけをレプリカにコピーします。プライマリでが Push DB 機能が無効な場合は、***ACEDATA*/replica_package**ディレクトリをレプリカにコピーします。

   Push DB の詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』を参照してください。

7. レプリカ パッケージを適用します。レプリカで次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -apply_package pathname
   ```

   pathname はレプリカ パッケージ ファイルの場所です。

レプリカの名前を変更した場合は、次の操作を実行する必要があります。

メモ : これらの操作を実行する場合は、必要に応じて関連ヘルプを表示できるように、Remote Administration を使用してください。Remote Administration の詳細については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』または第 2 章「RSA Authentication Manager Administration アプリケーションの使用」を参照してください。

- Authentication Manager をレルム間認証用のリモート レルム Authentication Managerまたはローカル レルムAuthentication Managerとして指定する場合は、新しい名前またはIP アドレスを反映するように、ローカル レルム データベースおよびリモート レルム データベースのレルム レコードを編集します。詳細については、ヘルプの「Edit Realm」を参照してください。
- Authentication Manager を RADIUS サーバとして定義する場合は、新しい名前または IP アドレスを使用するように、すべての RADIUS クライアントを構成します。構成手順については、NAS デバイスのマニュアルを参照してください。さらに、新しい名前または IP アドレスを反映するように、RSA RADIUS サーバのエージェント ホスト レコードを変更する必要があります。変更方法については、『RSA Authentication Manager 6.1 for UNIX インストール ガイド』の「サーバをエージェント ホストとしてプライマリ データベースへ追加」を参照してください。
- Authentication Manager を旧バージョンのエージェント ホストのアクティング Authentication Manager として定義する場合は、この Authentication Manager をアクティング マスタまたはアクティング スレーブとして使用する旧バージョンのすべてのエージェント ホストに対して、新しい **sdconf.rec** ファイルを作成し、その **sdconf.rec** ファイルをエージェント ホストに配布します。詳細については、ヘルプの「Assign Acting Servers」を参照してください。
- Authentication Manager を v5.0 以降のエージェント ホストの **sdopts.rec** ファイルに指定する場合は、Authentication Manager の新しい名前または IP アドレスを反映するように、エージェント ホストで **sdopts.rec** ファイルを編集します。

A ライセンス

この付録では、アクティブ ユーザの概念、ライセンスの種類、ライセンスの管理、レルム間環境のライセンス、ライセンスの更新手順など、RSA Authentication Manager のライセンスについて説明します。

アクティブ ユーザ

RSA Authentication Manager では、ライセンス管理でアクティブ ユーザという概念を使用しています。アクティブ ユーザとは、次の条件を満たすユーザのことです。

- RSA Authentication Manager データベースにユーザ レコードが登録されています。
- 1 ～ 3 個のトークン (または 1 つのユーザ パスワードと 1 ～ 2 個のトークンの組み合わせ) が割り当てられています。

たとえば、2 つのトークンと 1 つのユーザ パスワードが割り当てられているユーザは、**1** 人のアクティブ ユーザとしてカウントされます。RSA Authentication Manager データベースに登録されていても、トークンやユーザ パスワードが割り当てられていないユーザはアクティブ ユーザでは**ありません**。

メモ : 有効期限の切れたトークンが割り当てられているユーザは、アクティブ ユーザとしてカウントされます。有効期限の切れたトークンの割り当ての解除については、ヘルプの「Unassigning a Token」を参照してください。

ライセンスの種類

RSA Authentication Manager では、ベース ライセンスとアドバンスド ライセンスの 2 種類のパーマネント ライセンスが提供されます。

メモ : RSA Authentication Manager では、一時的なトライアル ライセンスとして評価用ライセンスも使用できます。

RSA Authentication Manager ベース ライセンスでは、次の環境で RSA Authentication Manager ソフトウェアを使用できます。

- 購入した「アクティブ ユーザ数の範囲」で指定される数まで、アクティブ ユーザを登録できます。
- 1 台のプライマリと 1 台のレプリカ構成を 1 つ (1 レルム) 稼動できます。

RSA Authentication Manager アドバンスド ライセンスでは、次の環境で RSA Authentication Manager ソフトウェアを使用できます。

- インストール全体で、購入した「アクティブ ユーザ数の範囲」で指定される数まで、アクティブ ユーザを登録できます。

  メモ：アクティブ ユーザ数はインストールあたりの値であり、レルムあたりの値では**ありません**。たとえば、ユーザ数の範囲が 1000 で、レルムが 2 つある場合、両方のレルム全体で最大 1000 ユーザを登録できます。各レルムで 1000 ユーザを登録することはできません。詳細については、274 ページの「レルム間環境」を参照してください。

- 1 台のプライマリに対して最大 10 台のレプリカ構成を 6 つ (6 レルム) 稼動できます。7 つ以上のレルムにソフトウェアをインストールする場合は、複数のアドバンスド ライセンスを購入する必要があります。たとえば、10 のレルムが必要な場合は、アドバンスド ライセンスを 2 つ購入してください。
- 正常に動作することが確認されている高可用性ハードウェア システムにインストールできます。現在認定されている高可用性プラットフォームは、Solaris 9 上の Veritas Cluster Server だけです。

ライセンスの制限の管理

RSA Authentication Manager 6.1 ソフトウェアでは、インストール時と日常の操作や管理作業でライセンスの制限が管理されます。

インストール時のライセンスの管理

RSA Authentication Manager を旧バージョンからアップグレードする場合も、新規インストールする場合も、ライセンス ファイル (**license.rec**) の場所を指定する必要があります。オリジナル フロッピー ディスクまたはハード ディスク ドライブにコピーした v3 (5.1 以前の形式) のライセンス ファイル、または v4 (5.1、5.2、および 6.0) のライセンス ファイルを指定できます。

RSA Authentication Manager の旧バージョンからアップグレードする場合は、セットアップ プログラムで、現在のインストールの内容が現在のライセンス条項のもとで有効であるかどうか確認されます。ライセンスで認められている数より多くのアクティブ ユーザまたはレプリカがデータベースに登録されている場合、RSA Authentication Manager は**アップグレード違反**モードになります。アップグレード違反モードになると、ライセンスは 90 日間有効のテンポラリ ライセンスになります。ライセンスの有効期限が切れると、**違反**モードになり、ユーザを新しくアクティブ化したり、新しいレプリカを追加したりできなくなります。

次のいずれかの操作を行って、90 日以内に RSA Authentication Manager 6.1 がライセンス条項に準拠するように (準拠モードになるように) しなければなりません。

- アップグレード違反の状況に応じて、レプリカを削除するか、アクティブ ユーザの数を削減します。
- RSA セキュリティからライセンス条項に準拠する新しいライセンスを購入します。

新しいライセンスの購入については、RSA セキュリティ正規販売代理店にお問い合わせいただくか、**www.rsasecurity.com/contact/** にアクセスしてください。

RSA Authentication Manager の各ライセンス モードについては、273 ページの表を参照してください。

日常操作および管理作業でのライセンスの管理

RSA Authentication Manager 6.1 の日常の管理作業を行っているときに、有効なライセンスが**違反**モードになることがあります。RSA Authentication Manager は定期的にライセンスの状況を確認します。たとえば、ライセンスで認められている数より多くのユーザをアクティブ化すると、RSA Authentication Manager でこのことが検出され、警告メッセージが表示されます。

`There are too many active users in the database` (データベースに定義されているアクティブ ユーザの数が多すぎます)

ライセンスが違反モードになると、追加ユーザをアクティブ化したり、新しいレプリカを追加することができません。

次のいずれかの操作を行って、ただちに RSA Authentication Manager 6.1 がライセンス条項に準拠するように (準拠モードになるように) しなければなりません。

- アップグレード違反の状況に応じて、レプリカを削除するか、アクティブ ユーザの数を削減します。
- RSA セキュリティからライセンス条項に準拠する新しいライセンスを購入します。

新しいライセンスの購入については、RSA セキュリティ正規販売代理店にお問い合わせいただくか、**www.rsasecurity.com/contact/** にアクセスしてください。

RSA Authentication Manager の各ライセンス モードについては、次の表を参照してください。

モード	このモードになった理由	このモードで可能な操作
ライセンス準拠	RSA Authentication Manager データベースに登録されているアクティブ ユーザおよびレプリカの数がライセンスの制限の範囲内です。	追加ユーザをアクティブ化できます。アドバンスド ライセンスを保有している場合は、新しいレプリカを追加できます。
アップグレード違反	RSA Authentication Manager の旧バージョンからアップグレードしましたが、RSA Authentication Manager データベースに登録されているアクティブ ユーザまたはレプリカの数がライセンスの制限を超えています。	アップグレード違反モードになると、ライセンスは 90 日間有効なテンポラリ ライセンスに切り替わります。90 日間は、追加ユーザをアクティブ化したり、新しいレプリカを追加できます。
違反	• 90 日間の**アップグレード違反**期間が経過しました。 • 通常の RSA Authentication Manager 6.1 の管理作業で、ライセンスで認められている数より多くのユーザをアクティブ化したか、多くのレプリカを追加しました。	追加ユーザをアクティブ化したり、新しいレプリカを追加することはできません。

レルム間環境

レルム間環境をサポートするには、全レルムにおけるアクティブ ユーザの総数をサポートできるだけの、1 つまたは複数のアドバンスド ライセンスを購入する必要があります。

次の表は、レルム間状況のいくつかの例と、それをサポートするために必要なライセンスを示しています。

状況	必要なライセンス
2 つの部門間にレルム間認証の関係を設定する必要がある場合。1 つの部門はアドバンスド ライセンスを所有しており、もう 1 つの部門はベース ライセンスを所有しています。	次のいずれかの操作を行います。 • ベース ライセンスを所有する部門がライセンスをアドバンスド ライセンスにアップグレードします。 • もう一方の部門が所有するアドバンスド ライセンスで追加のユーザとレルムをサポートできる場合は、ベース ライセンスを所有する部門はそのアドバンスド ライセンスにアップグレードできます (1 つのアドバンスド ライセンスで 6 レルムまで稼動できます)。
2 つの部門がベース ライセンスを所有しているときに、部門間にレルム間認証の関係を設定する必要がある場合。	次のいずれかの操作を行います。 • 両方の部門がそれぞれ、アドバンスド ライセンスにアップグレードします。 • 両方の部門が、両方のレルム全体のユーザの総数をサポートする 1 つのアドバンスド ライセンスにアップグレードします。
別の会社との間にレルム間認証の関係を設立する必要がある場合。	各会社がそれぞれアドバンスド ライセンスを所有する必要があります。

ライセンスのアップグレードまたは変換

ライセンスの制限を超えた場合や、評価用ライセンスの有効期限が切れた場合は、RSA セキュリティから新しい **license.rec** を入手する必要があります。RSA セキュリティ正規販売代理店にお問い合わせいただくか、**www.rsasecurity.com/contact/** にアクセスしてください。

RSA Authentication Manager での **license.rec** の更新については、229 ページの「[License Information] (ライセンス情報)」、または 243 ページの「RSA Authentication Manager for UNIX でのライセンス レコードの更新」を参照してください。

B サービスとプロセス

メモ：RSA RADIUS サーバのサービスとプロセスについては、『RSA RADIUS Server 6.1 Administrator's Guide』を参照してください。

サービスとネットワーク ポート (Windows および UNIX)

次の表は、RSA Authentication Manager が使用するデフォルトのネットワーク ポートに関する情報を示しています。

サービス名	ポート番号	プロトコル	方向	使用目的
securid	5500	UDP	• RSA Authentication Agent から RSA Authentication Manager へ • レルム間環境で RSA Authentication Manager から RSA Authentication Manager へ	• RSA Authentication Agent API を使用して構築されるアプリケーションも含めて、RSA SecurID 認証を行う RSA Authentication Agent 通信 (たとえば Remote RADIUS サーバなど)。 • レルム間認証。
securidprop_00 から最大 **securidprop_10** まで、ただし、**securidprop_00 = 5505**、**securidprop_01 =5506** など	5505 ～ 5515	TCP	プライマリからレプリカへ	プライマリとすべてのレプリカ間でのデータベース レプリケーション。ただし、 securidprop_00 = 5505 (プライマリ)、 securidprop_01 = 5506 (1 番目のレプリカ)、 securidprop_02 = 5507 (2 番目のレプリカ) など。
sdlockmgr	5560	TCP	プライマリまたはレプリカからレルム内の他の Authentication Manager へ	レルム内の他のすべての Authentication Manager とのロック マネージャ通信。 プライマリとレプリカが必要とするサービスです。RSA SecurID 認証が発生したときに、認証情報を高速に転送するために使用されます。

サービス名	ポート番号	プロトコル	方向	使用目的
sdreport	5540	TCP	ローカル	ローカル レポート データベース通信。 ファイアウォールの中では、このポートを開く必要はありません。
sdadmind	5550	TCP	Remote Administration またはエージェント ホストの自動登録機能から RSA Authentication Manager へ	Remote Administration 認証とエージェント ホストの自動登録機能。
sdcommd	5570	TCP	Web サーバからプライマリ サーバへ	Web サーバで稼動する **ACECOMPROXY** と RSA Authentication Manager データベースの間の通信。 たとえば、Quick Admin、RSA SecurID Web Express など。
sdlog と **sdserv**	5520 と 5530	TCP	Remote Administration からレルム内の任意のプライマリまたはレプリカへ	**sdlog** データベースと **sdserv** データベースへの接続に使用される Remote Administration ポート。 初期接続が確立された後、Progress Software データベース ブローカは、データベース ブローカによる継続的な処理のために、動的に割り当てられたポート (**-minport**、**-maxport** など) に接続を渡します。
sdlog と **sdserv**	-minport ～ -maxport	TCP	Remote Administration からレルム内の任意のプライマリまたはレプリカへ	Remote Administration データベース接続。セッションごとに 2 ポートを使用します。 Windows マシンの場合は **/ace/rdbms32/startup.pf** で構成し、UNIX マシンの場合は **/ace/prog/sdserv.pf** および **/ace/prog/sdlog.pf** で構成します。 Windows マシンでは、**-minport** は 3000 より大きくなければなりません。 **-maxport** は、すべてのシステムで、システムがサポートする最大ポート範囲よりも小さくなければなりません。

サービス名	ポート番号	プロトコル	方向	使用目的
sdoad	5580	TCP	RSA Authentication Agent 6.1 からプライマリへ プライマリから RSA Authentication Agent 6.1 へ	オフライン認証イベント (OA データ ダウンロード要求、パスワードの統合と更新、ログのアップロードなど)。
tacacs	49	TCP	TACACS+ クライアントからすべての RSA Authentication Manager へ	(UNIX のみ) TACACS+ 通信。
aceserv_be.exe (Windows) **_aceserver_be** (UNIX)	MinimumBE port MaximumBE port	UDP	ローカル専用またはレルム間	RSA Authentication Manager **acesrvc_be.exe** (Windows) および **_aceserver_be** (UNIX) が通信するポートの範囲を定義します。 11 以上のポート範囲を定義し、その範囲をファイアウォール内で構成する必要があります。使用可能な任意のポートを使用します。次の例を参照してください。 MINIMUM_BE_PORT=10000 MAXIMUM_BE_PORT=10010 Windows では、[RSA Authentication Manager Control Panel] を使用して設定します。 UNIX マシンの場合は、環境変数 **MINIMUM_BE_PORT** および **MAXIMUM_BE_PORT** を通じて設定します。

RSA Authentication Manager プロセス (Windows および UNIX)

RSA Authentication Manager プロセスは、Windows マシンの場合はタスク マネージャで、UNIX マシンの場合は **ps** コマンドを実行することにより確認できます。

プロセス	説明
_mprshut	**sdserv** データベースと **sdlog** データベースに関するタスクを実行します。システムでは、このプロセスの複数のインスタンスが実行します。
jsed	RSA Authentication Manager におけるシステム管理タスクのスケジューリングを有効にします。一般に、ジョブ スケジューラと呼ばれています。
logmaintthd	ログ管理タスクを実行します。
_mprosrv	データベース ブローカとデータベース サーバ プロセスを制御します。 ブローカは、データベースとその共有メモリを制御します。Remote Administration 接続の場合のように、ネットワークがデータベースとの接続を要求すると、ブローカがデータベース サーバ プロセスを起動します。 **sdlog** データベースと **sdserv** データベースには、それぞれ 1 つのデータベース ブローカ プロセスがあります。 一度に実行できるサーバ プロセスの数に制限はなく、その数はネットワーク要求の数によります。
sdadmind	Remote Administration 認証とエージェント ホストの自動登録機能を RSA Authentication Manager に接続します。
_aceserver_fe (UNIX) **acesrvc (Windows)**	**フロントエンド**と呼ばれる RSA Authentication Manager 認証エンジン プロセス。 認証の場合は、1 つのフロントエンド プロセスを複数のバックエンド プロセスに関連付けることができます。認証試行はまず、フロントエンド プロセスに渡されます。バックエンド プロセスが使用可能になると、フロントエンド プロセスは認証試行をバックエンド プロセスに配布します。 認証プロセスは、プライマリまたはレプリカで [RSA Authentication Manager Control Panel] を使用して設定できます。
_aceserver_be (UNIX) **aceservc_be (Windows)**	**バックエンド**と呼ばれる RSA Authentication Manager 認証エンジン プロセス。 一度に複数のバックエンド プロセス (フロントエンド プロセスから認証要求を受け取るプロセス) を実行できます。 認証プロセスは、プライマリまたはレプリカで [RSA Authentication Manager Control Panel] を使用して設定できます。

プロセス	説明
sdcommd	Quick Admin デーモンです。Quick Admin と Web Express に、RSA Authentication Manager データベースへのアクセス機能を提供します。
acesyncd (UNIX) **syncservc (Windows)**	レプリケーション プロセスです。プライマリでは、アクティブなレプリカごとに 1 つの **acesyncd** プロセスが実行されます。各レプリカでは、1 つの **acesyncd** プロセスだけが実行されます。
brksrv (Windows のみ **)**	RSA Authentication Manager ブローカを起動および停止します。
sdoad	RSA Authentication Agent からオフライン認証イベントを受信し、処理します (OA データ ダウンロード要求、パスワードの統合と更新、ログのアップロードなど)。

サービス コントロール マネージャ サービス (Windows のみ)

次の表は、RSA Authentication Manager のさまざまな要素の開始と終了を制御する RSA Authentication Manager サービスに関する情報を示しています。これらのサービスを管理するには、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順に選択します。

サービス名	説明
RSA Authentication Manager Administration Daemon	Remote Administration の要求を処理します。
RSA Authentication Manager Authentication Engine	認証サービスを提供します。
RSA Authentication Manager Broker	データベースへのアクセス機能を提供します。
RSA Authentication Manager Job Executor Daemon	ジョブ スケジューリングを実行します。
RSA Authentication Manager Log Maintenance Daemon	ログのメンテナンスを実行します。
RSA Authentication Manager QuickAdmin Daemon	Quick Admin と Web Express に対して RSA Authentication Manager データベースへのアクセス機能を提供します。

サービス名	説明
RSA Authentication Manager Replication Engine 0 から **RSA Authentication Manager Replication Engine 10**	プライマリとレプリカの間のレプリケーションを提供します。ここで、 RSA Authentication Manager Replication Engine 0 = プライマリ、 RSA Authentication Manager Replication Engine 1= 1 番目のレプリカ、 RSA Authentication Manager Replication Engine 2= 2 番目のレプリカ。以下も同様です。 プライマリでは、レプリカごとに 1 つのサービスのインスタンスが実行されます。レプリカでは、サービスの 1 つのインスタンスだけが実行されます。
RSA RADIUS Server	RSA RADIUS サービスを提供します。 **メモ：**このサービスは、RSA RADIUS がローカルにインストールされている場合にだけ表示されます。

C トラブルシューティング

この付録では、一般的に発生する RSA Authentication Manager の問題を把握し、対処するのに役立つ情報をまとめます。この付録は次のセクションに分かれています。

- イベント ログまたはシステム ログへの監査ログ メッセージの送信
- イベント ログとシステム ログの例
- SNMP によるメッセージのフィルタリング
- エラー状況
- 問題の解決方法
- メッセージ (アルファベット順)
- メッセージの ID 番号

メモ : この後のセクションでは、Authentication Manager とエージェント ホストのデータ ディレクトリを ***ACEDATA*** ディレクトリ、プログラム ファイル ディレクトリを ***ACEPROG*** ディレクトリとして表記しています。これらの名前が斜体 (***ACEDATA***、***ACEPROG***) で示されている場合は、実際のディレクトリ名を指定することを表しています。

イベント ログまたはシステム ログへの監査ログ メッセージの送信

[Log to System Log] オプションを使用すると、Authentication Manager に関連する監査ログ メッセージをイベント ログ (Windows) またはシステム ログ (UNIX) に送信できます。ログに送信できるのは、Authentication Manager に関連するメッセージだけです。必要な情報だけを取得できるように、ログに送信するメッセージの種類を選択する条件を指定できます。Windows では、RSA Authentication Manager からのメッセージは、イベント ログのアプリケーション ログの部分に記録されます。

メモ : RSA Authentication Manager Host Mode のメッセージをイベント ログに送信することはできません。

[Log to System Log] 機能は複数の方法で使用できます。

- あらかじめ選択条件を設定しておき、監視の目的でメッセージを収集するために、ピーク時に [Log to System Log] を有効にする方法。
- 特定の条件を指定して [Log to System Log] を有効にしておき、Authentication Manager が実行されているときに、必要に応じて条件を変更して、特定のトラブルを解決するための情報を収集する方法。
- 監査ログから収集したすべてのメッセージを特定のファイルに送信するか、または監査ログ メッセージを種類別に異なるファイルに送信するように、イベント ログを構成する方法。
- イベント ログで特定の監査ログ メッセージを確認することにより、市販のネットワーク管理ツールを使用して Authentication Manager のアクティビティを監視する方法。

[Log to System Log] 機能は、RSA Authentication Manager Host Mode のメイン メニューでオンとオフを切り替えることができます。メッセージ選択条件は、RSA Authentication Manager が実行されているときも、停止しているときも変更できます。Authentication Manager が実行されている場合は、いったん終了してから再起動しなければ、新しい選択条件は有効になりません。Authentication Manager が実行されていない場合は、次回起動したときに、変更した条件が有効になります。

メモ：メッセージがイベント ログまたはシステム ログに送信されるのは、Authentication Manager が実行されている場合だけです。

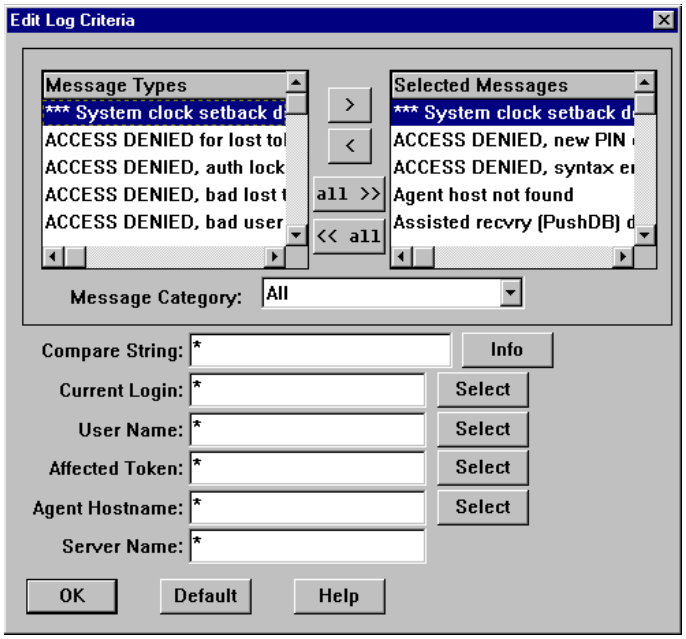
イベント ログに送信するメッセージを選択するときは、条件としてメッセージのタイプ、現在のログイン、影響を受けるユーザ名、影響を受けるトークン、エージェント ホスト、または Authentication Manager を指定できます。また、メッセージと文字列を対応付けることもできます。選択条件が複雑な場合は、システムが条件をもとにメッセージを評価し、メッセージをイベント ログまたはシステム ログに書き込むときに、Authentication Manager のパフォーマンスが少し低下する可能性があります。

この機能を使用するには、[Log] > [Log to System Log] の順にクリックします。

監査ログ メッセージをイベント ログまたはシステム ログに送信するための選択条件を設定するには

1. [Log] > [Edit System Log Parameters] の順にクリックします。

   [Edit Log Criteria] ダイアログ ボックスに、選択できるメッセージ タイプの一覧、イベント ログまたはシステム ログに送信するメッセージとしてすでに選択されているメッセージの一覧、および追加選択条件が表示されます。



   メモ：RSA Authentication Manager のインストール時に、[Exception/Incident] カテゴリのメッセージはイベント ログに送信するように設定されます。

2. [Message Types] の一覧で選択できるメッセージ タイプを変更するには、ドロップダウン リストで [Message Category] を選択します。

次の表は [Message Category] オプションについて説明しています。

メッセージ カテゴリ	含まれるアクティビティ
[Exception/Incident]	不正な認証のアクティビティと試行
[Server]	認証のアクティビティと操作
[Syncsrvc]	調整アクティビティ
[Realm]	レルム間アクティビティ
[RADIUS]	RADIUS サーバのアクティビティ
[Offline Authentication]	エマージェンシー PASSCODE の表示やダウンロードの失敗などの、オフライン認証イベント

3. 選択したメッセージの一覧にメッセージ タイプを追加するには、[Message Types] の一覧でメッセージ タイプを反転表示し、[>] をクリックします。現在のカテゴリのすべてのメッセージ タイプを選択する場合は、[all >>] をクリックします。

   [Selected Messages] の一覧からメッセージ タイプを削除するには、削除するメッセージ タイプを反転表示し、[<] をクリックします。現在のカテゴリのすべてのメッセージを削除する場合は、[<< all] をクリックします。

4. 選択したメッセージ タイプに追加条件を適用するには、選択フィールドを使用します。

   識別子の一覧から選択するには、[Select] ボタンをクリックします。[Select] ボタンを使用せずに、フィールドに直接入力する場合は、設定を慎重に入力してください。入力した識別子が正しいかどうかは自動的に確認されません。たとえば、正しいユーザ名が **John Smythe** である場合に、ユーザ名として「Jon Smith」と入力しても、入力したユーザ名が存在しないことは通知されません。

メッセージの選択条件	イベント ログに送信されるメッセージ
[Current Login]	指定のユーザが実行した操作に関するメッセージ。ユーザのログインではなく、ユーザ名を入力してください。
[User Name]	特定のユーザに影響する操作に関するメッセージ。ユーザのログインではなく、ユーザ名を入力してください。
[Affected Token]	特定のトークンに影響する操作に関するメッセージ。トークンのシリアル番号を指定してください。
[Agent Hostname]	指定のエージェント ホストに関連するアクティビティを示すメッセージ。
[Server Name]	特定の Authentication Manager (プライマリ、レプリカ、またはリモート レルム) でのアクティビティを示すメッセージ。

選択フィールドを空白にすると、そのフィールドは、イベント ログまたはシステム ログに送信するメッセージの選択条件として使用されません。

5. 複数のログイン、ユーザ、トークン、エージェント ホスト、Authentication Manager のアクティビティによって生成されたログ メッセージを選択するには、名前またはトークン シリアル番号を文字列として [Compare String] フィールドに入力します。名前やシリアル番号を入力するときは、Authentication Manager データベースに登録されているとおりに**正確**に入力してください。

   このフィールドの使い方を表示するには、[Info] をクリックします。パイプ文字 (|) で区切って、複数の文字列を入力できます。区切り文字の左右にスペースを指定することはできません。最後の文字列の後にも区切り文字を指定してください。

6. すべての選択条件をデフォルト値にリセットするには、[Default] をクリックします。デフォルトにリセットすると、すべての Exception/Incident メッセージがイベント ログまたはシステム ログに送信されます。

7. 選択条件の設定が終了したら、[OK] をクリックします。[Edit Log Criteria] ダイアログ ボックスで条件を変更した場合 (ステップ 1) は、[Log to System Log] が自動的にオンまたはオフに切り替わります。

イベント ログへの監査ログ メッセージの送信を開始または停止するには

- [Log] メニューの [Log to System Log] をクリックし、この機能をオンまたはオフに設定します。[Log to System Log] がオンになっているときは、メニュー項目の前にチェック マークが表示されます。
- [Log to System Log] をオンにするには、システム ログに送信するメッセージ タイプを少なくとも 1 つ選択する必要があります。メッセージ タイプが選択されていない場合は、[Edit System Log Parameters] を使用してメッセージ タイプを少なくとも 1 つ選択します。

メモ: RSA Authentication Manager プロセスで 1 日に 10,000 を超えるレコードがイベント ログまたはシステム ログに書き込まれると、「Too Many Syslog Messages Per Day (1 日に書き込まれた Syslog メッセージの数が多すぎます)」というメッセージがログに記録され、ログ カウントは 0 にリセットされます。

イベント ログとシステム ログの例

このセクションでは、プライマリ Authentication Manager とレプリカ Authentication Manager のイベント ログ (UNIX ではシステム ログ) のサンプルを示します。このサンプルは典型的なトランザクションを示しています。サンプル ログの後に、レプリカ Authentication Manager の操作とデータベースの調整のためにイベント ログに記録される一般的なエラー メッセージについて説明しています。**syncsrvc** (UNIX の場合は **acesyncd**) イベントのログの詳しい説明が必要な場合は、RSA セキュリティ正規販売代理店にご連絡ください。その場合、イベント ログのエントリの内容をカスタマ サービス担当者にご連絡ください。

プライマリ Authentication Manager でのイベント ログ / システム ログの例

Acesyncd Primary Started 0 0. [acesyncd.c.529.1]

Primary Unable To Connect To Replica 145.1.5.40 Port 7512 MsgLib Connect()....

Primary Will Retry Every 30 Seconds 0 0. [mloop.c.87.3]

Primary Has Connected To Replica 0 0. [mloop.c.66.4]

Primary Requesting LogEntry Changes From Replica 0 0. [mscomm.c.1264.5]

Primary Received 2 Modified LogEntry Records From Replica 0 0. [mscomm.c.1....
Primary Requesting Token Changes From Replica 0 0. [mscomm.c.1264.7]
Primary Received 0 Modified Token Records From Replica 0 0. [mscomm.c.135....
Primary Requesting Agent Host Changes From Replica 0 0. [mscomm.c.1264.9]
Primary Received 0 Modified Agent Host Records From Replica 0 0. [mscomm.c.135....
Primary Requesting System Changes From Replica 0 0. [mscomm.c.1264.11]
Primary Received 1 Modified System Records From Replica 0 0. [mscomm.c.13....
Primary Requesting LogEntry Changes From Replica 0 0. [mscomm.c.1264.13]
Primary Received 0 Modified LogEntry Records From Replica 0 0. [mscomm.c.1....
Primary Successfully Received Replica Records 0 0. [mloop.c.195.15]
Primary Sent 1 System Changes To The Replica 0 0. [perelt.c.409.16]
Primary Sent 100 User Changes To The Replica 0 0. [perelt.c.914.17]
Primary Sent 200 User Changes To The Replica 0 0. [perelt.c.914.18]
Primary Sent 300 User Changes To The Replica 0 0. [perelt.c.914.19]
Primary Sent 400 User Changes To The Replica 0 0. [perelt.c.914.20]
Primary Sent 500 User Changes To The Replica 0 0. [perelt.c.914.21]
Primary Sent 566 User Changes To The Replica 0 0. [perelt.c.970.24]
Primary Sent 100 Token Changes To The Replica 0 0. [perelt.c.1475.25]
Primary Sent 200 Token Changes To The Replica 0 0. [perelt.c.1475.26]
Primary Sent 300 Token Changes To The Replica 0 0. [perelt.c.1475.27]
Primary Sent 400 Token Changes To The Replica 0 0. [perelt.c.1475.28]
Primary Sent 500 Token Changes To The Replica 0 0. [perelt.c.1475.29]
Primary Sent 600 Token Changes To The Replica 0 0. [perelt.c.1475.30]
Primary Sent 700 Token Changes To The Replica 0 0. [perelt.c.1475.31]
Primary Sent 754 Token Changes To The Replica 0 0. [perelt.c.1531.35]
Primary Sent 21 Agent Host Changes To The Replica 0 0. [perelt.c.3214.36]
Primary Sent 24 Group Changes To The Replica 0 0. [perelt.c.4336.37]
Primary Sent 9 Administrator Changes To The Replica 0 0. [perelt.c.4897.38]
Primary Sent 100 EnabledGroup Changes To The Replica 0 0....
Primary Sent 131 EnabledGroup Changes To The Replica 0 0....
Primary Sent 100 GroupMember Changes To The Replica 0 0....
Primary Sent 200 GroupMember Changes To The Replica 0 0....
Primary Sent 300 GroupMember Changes To The Replica 0 0....
Primary Sent 400 GroupMember Changes To The Replica 0 0....
Primary Sent 479 GroupMember Changes To The Replica 0 0....
Primary Successfully Reconciled Databases 0 0. [mscomm.c.1019.49]

レプリカ Authentication Manager でのイベント ログの例

Replica Successfully Bound To Port 7512 0 0. [acesyncd.c.463.1]
Acesyncd Replica Started 0 0. [acesyncd.c.534.2]
Primary Has Connected To Replica 0 0. [sloop.c.79.3]
Replica Correcting Clock By -137 Seconds 0 0. [mscomm.c.736.4]
Primary Requesting Modified Log Entries From Replica 0 0. [mscomm.c.1812.5]

Replica Sent 2 Modified Log Entries To Primary 0 0. [mscomm.c.1834.6]
Primary Requesting Modified Token Records From Replica 0 0. [mscomm.c.161....
Replica Sent 0 Modified Token Records To Primary 0 0. [mscomm.c.1639.8]
Primary Requesting Modified Agent Host Records From Replica 0 0. [mscomm.c.167....
Replica Sent 0 Modified Agent Host Records To Primary 0 0. [mscomm.c.1694.10]
Primary Requesting Modified System Records From Replica 0 0. [mscomm.c.17....
Replica Sent 1 Modified System Record To Primary 0 0. [mscomm.c.1790.12]
Replica Sent 2 Modified Log Entries To Primary 0 0. [mscomm.c.1834.13]
Replica Successfully Reconciled Databases 0 0. [mscomm.c.1038.14]

SNMP によるメッセージのフィルタリング

SNMP トラッピングを使用する管理者の負荷を軽減するために、一部のメッセージには識別番号が含まれています。この番号を使用すると、トラップするメッセージの指定が簡単になります。トラップできるのは、RSA Authentication Manager がイベント ログに送信するメッセージだけです。この付録では、メッセージのすぐ後にかっこで囲んでメッセージ番号を示しています。401 ページの「メッセージの ID 番号」には、「Cannot Check Dependency for *NAME* (*NAME* の依存関係をチェックできませんでした)」というメッセージなどのように、共通形式のメッセージの番号の一覧を示しています。

エラー状況

このセクションでは、次の場合に発生する可能性があるエラー状況について説明します。

- リモート管理者も含めて、ユーザが認証を受ける場合
- 管理者が RSA Authentication Manager Host Mode を使用する場合

重要：RSA Authentication Manager のシステム時刻が正確でないと、これまで RSA Authentication Manager の認証を受けたことがないユーザや、新しいトークンを使用するユーザは、アクセスを拒否される可能性があります。新規ユーザに対応するために、システム時刻を変更することは絶対に**避けてください**。システム時刻を変更すると、既存のユーザのアクセスが拒否されてしまいます。このような場合は、RSA セキュリティ正規販売代理店にご連絡ください。

認証に関連するエラー状況

ユーザがアクセスを拒否された場合

Authentication ManagerでPASSCODEが正しい値として認識されないと、「Access Denied (アクセスが拒否されました)」というメッセージが表示されます。セキュリティ上の理由から、ログインに失敗した人に対してエラーの理由が表示されることはありません。承認されているユーザがアクセスを拒否された場合、問題を解決するには、管理者の支援が必要です。

ユーザのログイン試行レポートを作成するには

1. RSA Authentication Manager Host Mode を実行します。

2. [Report] > [Activity] の順にクリックして、[Report Selection Criteria] ダイアログ ボックスを開きます。
3. [Date] をクリックします。
4. [From Date] フィールドと [To Date] フィールドを使用して、ユーザのアクセスが拒否された期間を定義します。
5. [OK] をクリックしてダイアログ ボックスを閉じ、Activity レポートを作成します。

   ユーザのログイン試行の失敗に対応するログ レコードがレポートに表示されない場合は、290 ページの「ログイン試行のログ レコードが記録されていない場合」を参照してください。

   失敗したログイン試行を示すログ レコードがレポートに記録されている場合は、そのレポートで認証試行に対して記録されているメッセージのテキストを検索してください。このテキストの後に、問題の詳細な説明と解決方法が示されています。

ユーザがログインに失敗したことを示すメッセージが表示され、アクセスが許可されない場合でも、次の 2 つの状況では、監査証跡に肯定的なログ メッセージ (たとえば、PASSCODE が受け付けられたことを示すメッセージや、New PIN 操作が正常終了したことを示すメッセージなど) が記録されます。

- Authentication Manager やネットワークの負荷が非常に高い場合、Authentication Manager は PASSCODE または新しい PIN を受け付け、メッセージをエージェント ホストに通知しようと試みますが、エージェント ホストはそのメッセージを受信する前にタイムアウトになります。したがって、エージェント ホストはユーザに対して「Access Denied (アクセスが拒否されました)」(または「PIN rejected (PIN が拒否されました)」) というメッセージを表示します。

  メモ：ユーザが複数のトークンを持っている場合、Authentication Manager は一致するものが見つかるまで各トークンを順に確認するため、エージェントのタイムアウトによってアクセスが拒否される可能性が高くなります。

  この状況が発生した場合は、認証が成功するまで、次のトークンコードが表示されるのを待ち、そのトークンコードを再入力するようにユーザに指示するか、または**エージェントのタイムアウト**値を大きくして、新しい **sdconf.rec** ファイルを作成し、各エージェント ホストに配布します。Windows で**エージェントのタイムアウト**値を大きくするには、Configuration Management アプリケーションを使用します。UNIX の場合は、**sdsetup -config** コマンドを使用します。
- エージェント ホストの **sdconf.rec** ファイル (または他の構成方法) に定義されている暗号方式と、エージェント ホスト レコードに指定されている暗号方式が一致しない場合。

  エージェント ホスト レコードに暗号方式が正しく設定されていない場合は、[Agent Host] メニューの [Edit Agent Host] をクリックして設定を変更します。**sdconf.rec** ファイルの暗号方式の設定に誤りがある場合は、新しい **sdconf.rec** ファイルを作成し、エージェント ホストに配布します。

sdconf.rec ファイルの配布の詳細については、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。

管理者を含むすべてのユーザのアクセスが拒否されてしまう場合

すべての RSA SecurID トークン保有者のアクセスが拒否された場合は、おそらく Authentication Manager のクロックが数分以上ずれていると考えられます。Windows の場合は Administrator として、UNIX の場合は root としてログオンし、次の「すべてのユーザのアクセスが拒否されてしまう場合」の指示に従ってください。

Administrator アカウントも RSA SecurID によって保護されていて、管理者もアクセスが拒否される場合には、RSA セキュリティ正規販売代理店にご連絡ください。

すべてのユーザのアクセスが拒否されてしまう場合

どのトークン保有者も認証を受けることができない場合は、Windows では Administrator、UNIX では root としてログオンし、システム クロックが正しく設定されているかどうかを確認してください。クロックを正しい時刻に設定し、認証を再実行します。Administrator アカウントも RSA SecurID によって保護されていて、管理者もアクセスが拒否される場合には、RSA セキュリティ正規販売代理店にご連絡ください。

何らかの理由でシステム時刻を正しく設定できない場合は、RSA Authentication Manager データベースにオフセットを入力する必要があります。その後、Authentication Manager はこのオフセットによって調整されたシステム時刻を基準にして認証コードを生成するようになります。

Authentication Manager のクロックとトークンのクロックの差をもとに、システム クロックのオフセットを設定するには

1. RSA Authentication Manager Host Mode を起動します。
2. [System] > [System Configuration] > [Edit System Parameters] > [Set clock offset by token] の順にクリックします。
3. トークン シリアル番号の一覧が表示されます。オフセットの設定に使用するトークンを選択し、[OK] をクリックします。

   [Set Clock Offset by Token] ダイアログ ボックスが表示され、選択したトークンに表示されるコードを入力するように指示されます。
4. そのトークンに現在表示されているコードを入力し、[OK] をクリックします。

   [Set Clock Offset by Token] ダイアログ ボックスに別のプロンプトと入力フィールドが表示されます。この 2 番目のプロンプトでは、コードが変化するまで待つように指示されます。
5. トークンに表示される次のコードを入力し、[OK] をクリックします。もう一度 [OK] をクリックして、メッセージ ボックスを閉じます。
6. [System Parameters] ダイアログ ボックスの [OK] をクリックします。

   [Computed offset currently applied] フィールドに値が表示されます。
7. [OK] をクリックして、[System Parameters] ダイアログ ボックスを閉じます。
8. システム レコードの変更内容を保存するかどうか質問されます。[Yes] をクリックして、クロック オフセットを保存します。[No] をクリックすると、オフセットや他のシステム パラメータは変更されません。

システム クロックのオフセットを削除するには

1. [System] >[System Configuration] > [Edit System Parameters] の順にクリックします。
2. [Set Server Clock Offset to 0] ボタンをクリックします。
3. [OK] をクリックして、[System Parameters] ダイアログ ボックスを閉じます。

   システム レコードの変更内容を保存するかどうか質問されます。
4. クロック オフセットとして 0 を保存する場合は、[Yes] をクリックします。[No] をクリックすると、オフセットや他のシステム パラメータは変更されません。

認証試行中にエージェント ホストがハングした場合

いくつかの条件によって、認証試行中に Authentication Manager がエージェント ホストに応答できないことがあります。この問題が発生すると、エラー メッセージ「Cannot initialize Agent Host-server communications (エージェント ホストとサーバの間の通信を初期化できませんでした)」(316 ページ) が表示されることがあります。また、システムが動作していないように見え、メッセージが表示されないこともあります。

問題の原因を確認し、エージェント ホストと Authentication Manager の間の通信を可能にするには

1. Authentication Manager から各エージェント ホストに対して (**system32** ディレクトリで) **ping** コマンドを実行して、Authentication Manager と各エージェント ホストの間にネットワーク接続が確立されていることを確認します。
2. RSA Authentication Manager サービスが実行されていることを確認します。

   Windows の場合は、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックし、左側のツリーから [Start & Stop RSA Authentication Manager Services] を選択します。

   UNIX の場合は、**root** として次のように入力します。

   ```
   ps -ax | grep aceserver (BSD の場合 )
   ps -ef | grep aceserver (System V の場合 )
   ```

   このコマンドを実行しても **aceserver** プロセスが表示されない場合は、プロセスを起動する必要があります。データベース ブローカが実行されていない場合は、次のコマンドを使用して起動します。

   ```
   ACEPROG/sdconnect start
   ```

   次に、**aceserver** プロセスを起動します。

   ```
   ACEPROG/aceserver start
   ```

3. Authentication Manager プロセスが実行されているにもかかわらず、このエラーが発生し、問題が UNIX 版のエージェント ホストにある場合は、エージェント ホストで **sdshell** ファイルに対するアクセス権を確認してください。**ls -al** コマンドを使用して、エージェント ホストの ***ACEPROG*** ディレクトリの一覧を表示します。アクセス権は **--s--x--x** に設定されているはずです。異なる場合は、**root** で次のように入力して変更してください。

   ```
   chmod 4111 sdshell
   ```

   メモ : RSA Authentication Manager サービスや **sdshell** へのアクセス権に問題がない場合は、エージェント ホストで設定されているサーバに関する情報を確認してください。この問題が発生する可能性がもっとも高いのは、サーバが 2 つの IP アドレスを持つゲートウェイである場合です。

4. RSA Authentication Manager サービスや **sdshell** へのアクセス権に問題がない場合は、Authentication Manager の場所に関する正しい情報がエージェント ホストに格納されているかどうかを確認します。Configuration Management アプリケーションを使用して、IP アドレスを表示します。エージェント ホストに適したユーティリティを使用して、エージェント ホストの **sdconf.rec** ファイルの内容を確認します (たとえば、Windows のエージェント ホストでは Authentication Test 機能を使用し、UNIX のエージェント ホストでは **sdinfo** コマンドを使用します)。

   旧バージョンのエージェント ホストの場合は、情報が表示されたら、Authentication Manager 名とアドレスを書き留めます。RSA Authentication Manager のプライマリまたはリモート アドミニストレーション マシンに Administrator としてログインし、RSA Authentication Manager Host Mode を実行します。[Agent Host] > [Edit Agent Host] > [Assign Acting Servers] の順にクリックします。エージェント ホスト レコードでアクティング Authentication Manager のエイリアス IP アドレスを使用している場合を除き、[Current Server Assignments] をエージェント ホストの構成ファイルに定義されているマスタおよびスレーブと一致させる必要があります。詳細については、[Help] をクリックして表示される情報を参照してください。

   エージェント ホストで正しくない情報が表示される場合は、エージェント ホスト用に新しい構成ファイルを作成し、エージェント ホストにコピーしてください。

アドミニストレーションに関連するエラー状況

項目の削除または一覧表示によって表示されるエラー メッセージ

一覧表示オプション (たとえば [List Agent Hosts] や [List Groups]) または削除オプション (たとえば [Delete Users] や [Delete Tokens]) を使用しようとしたときにエラー メッセージが表示された場合は、その操作を再実行してください。認証のためにレコードが使用されていたか、別の管理者によってレコードが使用されていたために、1 つ以上のレコードがロックされていた可能性があります。問題を解決できない場合は、Authentication Manager のディスク容量が不足していないかどうかを確認してください。

変換またはインポートによって名前が変更された場合

RSA Authentication Manager の以前のバージョンからレコードをインポートまたは変換すると、一部の名前が変更される可能性があります。インポートや変換では、次の規則に従って、無効文字が Authentication Manager で使用できる文字に変換されます。

- TAB はスペースに変更されます。
- 印刷不可文字はスペースに変更されます。
- 先頭と末尾のスペースは削除されます。
- パーセント記号 (%) はスペースに変更されます。

これらの変更によって、ユーザ名、シェル、エージェント ホスト名、グループ名などのフィールドも影響を受ける可能性があります。

ログイン試行のログ レコードが記録されていない場合

ターミナル サーバを使用しているときに、ログインの失敗がログに記録されない場合は、ターミナル サーバで RSA Authentication Manager の定義が設定されていない可能性があります。ターミナル サーバを正しく構成する方法については、ターミナル サーバのマニュアルを参照してください。

ログイン操作でサーバのタイムアウトが発生する場合

一部のプラットフォームでは、New PIN 操作またはネクスト トークンコード操作で Authentication Managerがタイムアウトになることがあります。このような場合は、トークンのカウントダウン インディケータの表示が小さくなるのを待ち、その後で操作を再実行するようにユーザに指示してください。

ログ メッセージで文字化けが発生する場合

RSA Authentication Manager ソフトウェアの日本語版がインストールされているレルムと英語版がインストールされているレルムの間でレルム間認証を実行しようとすると、文字化けが発生することがあります。認証メッセージに日本語が含まれている場合、英語版のログ データベースではその文字が正しく表示されません。

問題の解決方法

ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合

このセクションで説明するメッセージがイベント ログまたはシステム ログに記録されている場合は、次の手順を実行してください。

1. データベース ブローカを経由してデータベースへの接続が確立されていることを確認します。Windows の場合は、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックし、左側のツリーから [Start & Stop RSA Authentication Manager Services] を選択します。UNIX の場合は、**sdconnect start** を実行します。
2. ネットワーク接続を確認します。ネットワークがダウンしている場合は、これらのメッセージが 1 つ以上記録され、そのすぐ後に「Primary Breaking Connection (プライマリは接続を切断します)」または「Replica Breaking Connection (レプリカは接続を切断します)」メッセージが記録されます。
3. 上記の 2 つの手順を実行しても問題を解決できない場合は、データベースが壊れている可能性があり、致命的なエラーを示す「Daemon Stopping... (デーモンが停止します)」というメッセージが記録されます。詳細については、RSA セキュリティ正規販売代理店にお問い合わせください。

LDAP 同期に関連するエラー メッセージ

サポートされる 3 つの LDAP ディレクトリ サーバのいずれかに接続する同期ジョブに、大量 (1,000 以上) のユーザ レコードを返すクエリが含まれている場合、次のいずれかのメッセージが表示されます。

```
Timelimit exceeded ( タイムリミットを超えました )
Sizelimit exceeded ( サイズリミットを超えました )
```

これらの問題は通常、LDAP サーバの設定によって発生します。LDAP ディレクトリ サーバで、同期ジョブから発生する大量のクエリに対応するには、接続タイムアウト、最大接続アイドル タイム、最大ページ サイズ、最大クエリ期間、および最大テーブル サイズのデフォルト値を大きくします。これらの設定の実際の名前、および値の変更方法は、使用している LDAP サーバに応じて異なります。詳細については、LDAP サーバのマニュアルを参照してください。

メモ：LDAP サーバに関する情報は、**http://www.openldap.org** で入手できます。

RSA Authentication Manager では、プライマリ マシンで以下の 2 つの環境変数の設定も大きい値に変更することができます。

```
RSA_LDAP_SEARCH_TIMEOUT
RSA_LDAP_BIND_TIMEOUT
```

RSA Authentication Manager では、これらの環境変数のデフォルト値は 1200 秒 (20 分) と 300 秒 (5 分) です。これらの値は最適化されており、大量のクエリに対しても問題なく機能するはずです。しかし、より大きなタイムアウト値 (秒単位) を設定した環境変数を追加することで、これらの設定を拡大することができます。環境変数の追加の詳細については、Windows のヘルプを参照してください。

各同期ジョブに関連付けられている LDAP クエリ フィルタを編集することで、データベースの検索を制限することもできます。

External Authorization のタイムアウトに関連するメッセージ

External Authorization の **iSDExtAuthorCheck()** または **iSDExtAuthorGetHomeData()** ルーチンの処理に時間がかかりすぎる場合は、Authentication Manager で認証要求がタイムアウトになり、そのことを示すメッセージがユーザに表示されます。

External Authorization のタイムアウト メッセージに対処するには

1. RSA Authentication Manager Host Mode を起動します。
2. [System] > [Edit Authorization Parameters] の順にクリックします。
3. External Authorization のオプションをオフにします。

   このようにすると、管理者が問題に対処している間に、Authentication Manager でデフォルトの認証ルーチンを使用してアクセス要求を処理できるようになります。
4. **iSDExtAuthorCheck()** ルーチンと **iSDExtAuthorGetHomeData()** ルーチンの処理に時間がかかりすぎる原因を調べます。原因がわかったら、ルーチンを変更して処理時間を短縮します。
5. RSA Authentication Manager Host Mode で、[System] > [Edit Authorization Parameters] の順にクリックします。
6. External Authorization のオプションを再びオンにします。
7. Authentication Manager を再起動して、External Authorization のオプションを有効にします。

External Authorization ルーチンの詳細については、『External Authorization API Guide』(***ACEDOC*** ディレクトリの **authmgr_authorization_api.pdf**) を参照してください。

プライマリとレプリカ間の通信の開始に関連する問題の解決

プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) を開始するときに問題が発生した場合は、次の手順を実行して問題を解決してください。

syncsrvc (acesyncd) に関連する問題に対処するには

1. データベース ブローカを経由してデータベースへの接続が確立されていることを確認します。[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックし、左側のツリーの [Start & Stop RSA Authentication Manager Services] をクリックします。
2. プライマリとレプリカが同じ種類のコンピュータで、同じバージョンのオペレーティング システムを実行していることを確認します。

メッセージ

このセクションでは、画面、RSA Authentication Manager 監査ログ、イベント ログ (Windows)、システム ログ (UNIX) に表示 (記録) されるメッセージの一覧を示します。かっこで囲まれたエラー番号は、SNMP を使用してメッセージをフィルタリングするときに使用できます。詳細については、286 ページの「SNMP によるメッセージのフィルタリング」を参照してください。

ACCESS DENIED,OA previous tokcode (8961) (アクセスは拒否されました、OA の以前のトークンコード)

ユーザがオフライン認証で古いトークンコードを再利用しようとしました。これは通常、ユーザのエラーです。

Agent Request for Passwd Denied (8973) (エージェントからのパスワード要求が拒否されました)

Authentication Manager は、エージェントから送られたユーザの Windows パスワードの要求を拒否しました。Windows パスワードの統合がシステム レベルで無効になっているか、この特定のエージェント ホストで無効になっているか、または Authentication Manager がユーザの Windows パスワードをデータベースに登録していないことが原因であると考えられます。

A process timeout occurred while performing database broker management (15042) (データベース ブローカ管理の実行中にプロセス タイムアウトが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

A Progress Utility error occurred while performing database broker management. (15043) (データベース ブローカ管理の実行中に Progress ユーティリティでエラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

A SELECT statement can select valid column names only. Arguments, numbers, or predefined variables are not allowed (SELECT ステートメントでは、有効な列名だけを選択できます。引数、数字、定義済み変数を選択することはできません)

これは、列名として正しくないテーブル フィールド名を使用したために発生する構文エラーです。詳細については、ヘルプの「RSA Authentication Manager Database Schema」を参照してください。

AALM failed to connect to log database (%1) (15994) (AALM がログ データベースに接続できませんでした)

RSA Authentication Manager を停止し、すべての RSA Authentication Manager プロセスが停止していることを確認します。また、データベースのダンプ操作やロード操作を行っている管理者がいないことも確認します。RSA Authentication Manager を再起動します。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

AALM failed to daemonize (15993) (AALM でデーモンを起動できませんでした)

RSA Authentication Manager の起動時に Automated Log Maintenance デーモンを起動できなかった場合、このメッセージがログに記録されます。通常、このメッセージは次のいずれかのメッセージの後に記録されます。

```
Log Maintenance Had Seg Violation （ログ メンテナンスでセグメンテーション違反が発生しました）
Log Maintenance Had a Bus Error （ログ メンテナンスでバス エラーが発生しました）
Log Maintenance Aborted （ログ メンテナンスがアボートしました）
Log Maintenance Stopped （ログ メンテナンスが停止しました）
```

[Automated Log Maintenance] が有効になっているかどうかを確認してください。RSA Authentication Manager Host Mode で、[Log] > [Automate Log Maintenance] の順にクリックし、[Enable Automatic Audit Log Maintenance] チェックボックスがオンになっていることを確認した後、Authentication Manager をいったん停止して再起動します。

AALM failed to get maintenance schedule (15998) (AALM でメンテナンス スケジュールを取得できませんでした)

Automated Log Maintenance デーモンがログ データベースに接続できない場合、このメッセージがログに記録されます。データベース ブローカを再起動してください。

AALM failed to initialize database context (%1) (15992) (AALM でデータベース コンテキストを初期化できませんでした)

RSA Authentication Manager を停止し、すべての RSA Authentication Manager プロセスが停止していることを確認します。また、データベースのダンプ操作やロード操作を行っている管理者がいないことも確認します。RSA Authentication Manager を再起動します。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

AALM failed to UPDATE maintenance schedule (15999) (AALM でメンテナンス スケジュールを更新できませんでした)

ログ メンテナンス デーモンがデータベースに書き込むことができませんでした。プライマリを再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

AALM unable to set logmaintsvr credentials (15997) (AALM で logmaintsvr クレデンシャルを設定できませんでした)

RSA セキュリティ正規販売代理店にご連絡ください。

ACCESS DENIED, auth lock error (1140) (アクセス拒否、認証ロック エラー)

認証要求を処理する前に、Authentication Manager でユーザ名またはユーザのトークンをロックできませんでした。名前またはトークンがすでにロックされている可能性があります。過去に使用されたトークンコードを使用した場合にも、このメッセージが表示されます。

ACCESS DENIED, Bad Lost Token PSW (1083) (アクセス拒否、紛失したトークンのパスワードが不正です)

ユーザが認証を受けるときに、割り当てられているテンポラリ パスワードとは異なるパスワードを入力しました。ユーザがパスワードを忘れてしまった場合は、新しいパスワードを作成して、ユーザに通知してください。

ACCESS DENIED, Bad User Password (1091) (アクセス拒否、ユーザ パスワードが不正です)

ログ レコードに正しいログインが記録されている場合は、ユーザに割り当てられているユーザ パスワードと異なるパスワードが認証時に入力されたと考えられます。[Edit User] ダイアログ ボックスの [Set/Change User Password] ボタンを使用して、ユーザのパスワードを変更し、ユーザ パスワードを Change Required モードに設定してください。

このメッセージが表示される可能性のあるその他の状況については、297 ページの「ACCESS DENIED, PASSCODE Incorrect (1008) (アクセス拒否、PASSCODE が不正です)」を参照してください。

ACCESS DENIED, Can't Get Token SB (1041) (アクセス拒否、トークン SB を取得できませんでした)

詳細については、RSA セキュリティ正規販売代理店にお問い合わせください。

ACCESS DENIED, Can't Lock Token (1038) (アクセス拒否、トークンをロックできませんでした)

認証サービスがトークンをロックできなかったために、トークンを使用してログオンできませんでした。

ACCESS DENIED, Can't Write [Lock] Agent (1039) (アクセス拒否、エージェント ホスト レコードを書き込む (ロックする) ことができませんでした)

ノード シークレット ステータスを更新するために、認証サービスがエージェント ホスト レコードをロックできないか、またはエージェント ホスト レコードに書き込むことができなかったため、ユーザはログオンできませんでした。

ACCESS DENIED, Ext-auth failed *login user Agent Host server token* (1110) (アクセス拒否、Ext-auth の処理が失敗しました)

このメッセージは、RSA Authentication Manager で External Authorization をアクティブ化したときに表示されます。External Authorization のルーチンでユーザのアクセス試行が拒否されました。まず、どの External Authorization ルーチンからエラーが返されたかをイベント ログ内のメッセージで確認します。このメッセージだけではエラーについての説明が不十分な場合は、メッセージを作成したプログラマに問い合わせてください。

ACCESS DENIED, Lost Password Exp (アクセス拒否、紛失したトークンのパスワードの有効期限が切れています)

紛失した (Lost) トークンに割り当てられている固定パスワードを使用してログオンが試行されました。しかし、固定パスワードの有効期限が切れています。紛失したこのトークンに対して、新しいパスワードを作成してください。

ACCESS DENIED, Lost Token (アクセス拒否、紛失したトークンでログオンが試行されました)

Lost (紛失) ステータスのトークンのトークンコードを使用してログオンが試行されました。紛失したトークンが後で見つかった場合は、現在トークンを使用している人が本来の正しいユーザであるかどうかを確認してください。正しいユーザであることを確認できた場合は、ステータスを Not Lost に変更してください。

ACCESS DENIED, multiple auths (1141) (アクセス拒否、複数の認証)

このメッセージは、ネットワークへの攻撃が試みられたことを警告するために、RSA Authentication Manager 監査証跡に書き込まれます。認証サービスがこのような攻撃を検出し、アクセスを防止しました。

このメッセージが表示された場合は、**トークンをただちに New PIN モードに設定し、以前の PIN を消去してください**。詳細については、127 ページの「New PIN モードの設定」を参照してください。

ACCESS DENIED, name lock required (1142) (アクセス拒否、名前ロックが要求されました)

Authentication Manager に認証要求を送信する前に、エージェント ホストでユーザ名の名前ロック要求を発行する必要があります。Authentication Manager が認証要求を受信した時点で、このロックは存在しませんでした。名前がすでにロックされているか、または名前のロックが削除されている可能性があります。

一部のサードパーティ エージェントでは、名前ロックは必要ありません。名前ロックが存在しないために、Authentication Manager がロックを待機してアクセスを拒否することを防ぐには、エージェント ホストの [Edit Agent Host] ダイアログ ボックスを開き、必要に応じて [Requires Name Lock] チェックボックスをオフにします。

ACCESS DENIED, New PIN Deferred (147) (アクセス拒否、New PIN モードが続行しています)

New PIN プロンプトで、ユーザが新しい PIN を指定したり受け取ったりすることなく、操作を取り消しました。ユーザのトークンはまだ New PIN モードです。

ACCESS DENIED, Next Tokencode Bad (1000) (アクセス拒否、ネクスト トークンコードが不正です)

ユーザがネクスト トークンコード プロンプトに応答しようとしましたが、トークンに対して不正なコードを入力しました。したがって、ユーザのアクセスは拒否されました。ネクスト トークンコードの詳細については、125 ページの「PIN が盗まれたり、他人に知られた場合」を参照してください。

ACCESS DENIED, No Agent SB (1042) (アクセス拒否、エージェント ホストの SB がありません)

詳細については、RSA セキュリティ正規販売代理店にお問い合わせください。

ACCESS DENIED, No Token Assigned (アクセス拒否、トークンが割り当てられていません)

ユーザがログインしようとしましたが、トークンが割り当てられていないため、システムへのアクセスが許可されませんでした。このユーザにトークンを割り当てる前に、セキュリティが脅かされる危険性がないかについて、他のシステム管理者に確認してください。

ACCESS DENIED, Node Verification Failed (アクセス拒否、ノードの検証に失敗しました)

このメッセージは、次の場合にログに記録される可能性があります。

- エージェント ホストの **sdconf.rec** ファイル (または他の構成方法) に定義されている暗号方式と、エージェント ホスト レコードに指定されている暗号方式が一致しない場合。

  エージェント ホスト レコードに暗号方式が正しく設定されていない場合は、[Agent Host] メニューの [Edit Agent Host] をクリックして設定を変更します。**sdconf.rec** ファイルの設定が正しくない場合は、**sdconf.rec** ファイルの配布方法の詳細について、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。
- エージェント ホストがAuthentication Managerデータベースからいったん削除された後に再登録されたか、または、以前は別の Authentication Manager に関連付けられていました。この問題を解決するには、363 ページの「Node verification failed (137) (ノードの検証に失敗しました)」に示した手順を実行してください。
- ノード シークレット ファイルがエージェント ホストから削除されています。この問題を解決するには、363 ページの「Node verification failed (137) (ノードの検証に失敗しました)」のステップ 2 とステップ 3 を実行してください。

問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

ACCESS DENIED, Outside User Time (1003) (アクセス拒否、ユーザのアクセス可能時間外です)

ユーザのレコードに定義されている開始日時と終了日時の範囲外に、ユーザがログオンしようとしました。

ACCESS DENIED, PASSCODE Incorrect (1008) (アクセス拒否、PASSCODE が不正です)

ログ レコードに正しいログインが記録されている場合。このイベントを示すレコードが記録されていても、ユーザが正しくログインしたことが記録されている場合は、多くの理由が考えられます。もっとも一般的な理由として、ユーザが PASSCODE を正しく入力しなかったことが考えられます。ユーザが 1 回または 2 回だけ認証を受けようとした後、管理者に問題を連絡した場合は、操作を再実行するように指示してください。

操作を再実行してもアクセスが拒否される場合は、トークンのクロックとシステムのクロックの同期がとれていない可能性があります。システム時刻が正しいにもかかわらず、ユーザのアクセスが拒否された場合は、トークンの同期をとり直します。手順については、128 ページの「トークンの同期のとり直し」を参照してください。

トークンの同期をとり直しても問題を解決できない場合は、ユーザが間違った PIN を入力した可能性があります。その場合は、トークンを New PIN モードに設定し、ユーザに対して、新しい PIN を受け取るか作成するかして、その PIN を使用してログオンするように指示してください。

ログ レコードに不正なログオンが記録されている場合。アクセスが拒否されているユーザのログ レコードが記録されておらず、誤って別のユーザのレコードが記録されている場合は、問題はいずれかの識別子にあります。エージェント ホストでユーザがアクティブ化されたとき、またはグループに追加されときに、不正なログオンが指定されたと考えられます。直接アクティブ化されたユーザの一覧またはグループ メンバの一覧 (このエージェント ホストでユーザに適用されるいずれか一方の一覧) を作成し、ユーザのトークンのシリアル番号に対して正しいログオンが登録されていることを確認してください。正しくない場合は、アクティブ化を再実行し、ユーザのログオンを正しく指定してください。

このメッセージは、エージェント ホストですでに使用されているログオンを使用してユーザがアクティブ化された場合にも表示されます。2 人のユーザが同じエージェント ホストで同じログオンを使用すると、いずれか一方のトークン保有者がエージェント ホストにログオンできなくなります。これは、認証サービスがもう 1 人のトークン保有者の PASSCODE を待機しているからです。いずれか一方のユーザのログオンを変更してください。

ACCESS DENIED, PIN Rejected (1007) (アクセス拒否、PIN が拒否されました)

ユーザが入力した PIN が、システムで設定されている PIN の長さまたは使用できる文字の規則に従っていないため、New PIN 操作を完了できませんでした。トークンはまだ New PIN モードです。ユーザは操作を再実行する必要があります。今度はシステムの要件を満たす PIN を選択するように指示してください。

ACCESS DENIED, Previous Tokencode (1003) (アクセス拒否、以前に使用したトークンコードを使用してログイン試行しました)

入力された PASSCODE は、そのコードを使ってアクセスに成功したかどうかにかかわらず、トークンに以前に表示されたトークンコードをベースにしています。以前に使用したトークンコードまたは PASSCODE の再利用が禁止されているのは、承認されていない人が (たとえば、電子的な盗聴によって) PASSCODE を不正に取得して再利用することを防ぐためです。

Access Denied (RSA Authentication Manager Quick Admin) (アクセス拒否 (RSA Authentication Manager Quick Admin))

Quick Admin にログオンできない場合は、次のことを確認してください。

- ログオン ページで入力したユーザ ID が RSA Authentication Manager データベースに登録されていて、このユーザがエージェント ホスト (Quick Admin Web サーバ ホスト) でアクティブ化されていることを確認します。
- 入力したユーザ ID にトークンまたはユーザ パスワードが割り当てられていることを確認します。
- 入力したユーザ ID に十分な RSA Authentication Manager 管理権限が割り当てられていることを確認します。
- プライマリ Authentication Manager の **sdti.cer** および **server.cer** ファイルの有効なコピーが、Web サーバ ホストの ***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥WEB-INF¥certs¥*servername*** サブディレクトリに格納されているかどうかを確認します。
- 問題をさらに詳しく診断するには、RSA Authentication Manager の Activity ログを調べてください。

ACCESS DENIED, Syntax Error (146) (アクセス拒否、構文エラー)

ユーザが「Enter PASSCODE (PASSCODE を入力してください)」プロンプトで不正な文字列を入力しました。たとえば、PASSCODE を入力せずに RETURN を押したと考えられます。

ACCESS DENIED, Token Disabled (1004) (アクセス拒否、トークンは無効です)

ユーザがログオンしようとしましたが、ユーザのトークンが (システムまたは管理者によって) 無効に設定されているため、システムへのアクセスが許可されませんでした。122 ページの「トークンの無効化」、および 122 ページの「トークンが盗まれたり、紛失した場合」を参照してください。トークンを再び有効に設定する前に、セキュリティが脅かされる危険性がないかについて、他のシステム管理者に確認してください。

トークンを有効にするには

RSA Authentication Manager Host Mode で、[Token] > [Edit Token] の順にクリックします。無効になっているトークンを選択して [Edit Token] ダイアログボックスを開き、[Enabled] チェックボックスをオンにします。必要に応じて [Help] をクリックして、表示される情報を参照してください。

ACCESS DENIED, Token Expired (1072) (アクセス拒否、トークンの有効期限が切れています)

ユーザがログオンしようとしましたが、ユーザのトークンの有効期限が切れているため、システムへのアクセスは許可されませんでした。有効期限が切れたトークンは、交換する必要があります。

ACCESS DENIED, Token ToD Bad (1001) (アクセス拒否、トークンの ToD が不正です)

有効期限が切れたトークンを使用してログオンしようとしたか、またはユーザ レコードに指定されているテンポラリ ユーザの期間外にログオンしようとしました。[Add User] または [Edit User] オプションを使用して、これらの日付を適切に設定してください。

ACCESS DENIED, Tokencode Repeated (アクセス拒否、トークンコードが繰り返し使用されました)

システムへのアクセスで過去に使用された PASSCODE が入力されました。以前に使用した PASSCODE の再利用が禁止されているのは、承認されていない人が (たとえば、電子的な盗聴によって) PASSCODE を不正に取得して再利用することを防ぐためです。

ACCESS DENIED, Write Token Failed (1006) (アクセス拒否、トークン レコードの書き込みに失敗しました)

認証サービスがトークン レコードに書き込むことができなかったため、トークンを使用してログオンできませんでした。

ACE/Server attempted start from *hostname*: Unknown host (ACE/Server を *hostname* から起動しようとしましたが、これは不明ホストです)

このマシンは、**sdconf.rec** ファイルに定義されている Authentication Manager に対応しません。Windows の場合は、Configuration Management アプリケーションを使用して、プライマリのホスト名と IP アドレスを確認してください。UNIX の場合は、**sdsetup -config** コマンドを使用します。

ACE/Server Error: calloc failed errno = ... (ACE/Server エラー：calloc の失敗 errno = ...)

RSA Authentication Manager サービスがメモリを割り当てることができませんでした。マシンで割り当てられているメモリ リソースを確認してください。

ACE/Server Can't Bind UDP Socket (1053) (ACE/Server で UDP ソケットをバインドできませんでした)

***%SYSTEMROOT%*¥system32¥drivers¥etc¥services** (UNIX の場合は **etc/services**) ファイルで認証サービスに対して定義されているポートで他のプロセスが実行されていたため、認証サービスの起動時にソケットをバインドできませんでした。問題を解決する方法については、302 ページの「ACM ERROR: Unable to bind the socket for ACE/Server (ACM エラー：ACE/Server に対してソケットをバインドできませんでした)」を参照してください。

ACE/Server Can't Set UDP Sock Opt (1054) (ACE/Server で UDP ソケットオプションを設定できませんでした)

Authentication Manager で UDP ソケット オプションを設定できませんでした。システム管理者にご相談ください。

ACE/Server Create UDP Socket Fail (1051) (ACE/Server で UDP ソケットを作成できませんでした)

たとえば、ソケットの数が不足しているために認証サービスを起動できないなど、システム上の問題があります。システム管理者にご相談ください。

ACE/Server error %d from errSDLicenseRead errno . . . . (errSDLicenseRead からの ACE/Server エラー)

RSA Authentication Manager サービスがライセンス レコードを読み取ることができませんでした。**license.rec** ファイルが ***ACEDATA*** ディレクトリに登録されていることを確認し、ファイルのアクセス権が適切であるかどうかを確認してください。

ACE/Server error closing system handle . . . . (システム ハンドル ... を閉じるときに ACE/Server エラーが発生しました)

Progress のエラーです。Windows の場合はイベント ログ、UNIX の場合はシステム ログで、RSA Authentication Manager サービスおよび Progress Software データベース ソフトウェアによるその他のエラーを検索してください。

ACE/Server Error: strdup failed errno = ... (ACE/Server エラー：strdup の失敗)

RSA Authentication Manager サービスがメモリを割り当てることができなかった可能性があります。マシンで割り当てられているメモリ リソースを確認してください。

ACE/Server error updating the system record . . . . (15021) (ACE/Server エラー：システム レコードの更新でエラーが発生しました)

Progress のエラーです。Windows の場合はイベント ログ、UNIX の場合はシステム ログで、RSA Authentication Manager サービスおよび Progress Software データベース ソフトウェアによるその他のエラーを検索してください。

ACE/Server exiting: setsockopt() call failed (ACE/Server の終了：setsockopt() 呼び出しの失敗)

ネットワークの接続と設定を確認してください。

ACE/Server failed to fetch system handle . . . . (ACE/Server はシステム ハンドルをフェッチできませんでした)

Progress のエラーです。Windows の場合はイベント ログ、UNIX の場合はシステム ログで、RSA Authentication Manager サービスおよび Progress Software データベース ソフトウェアによるその他のエラーを検索してください。

ACE/Server failed to get exclusive lock on system record . . . . (ACE/Server はシステム レコードを排他的にロックできませんでした)

別のアプリケーションがシステム レコードを排他的にロックしています。すべてのアドミニストレーション セッションを閉じ、RSA Authentication Manager サービスを再起動してください。

ACE/Server failed to open system record . . . . (ACE/Server はシステム レコードを開くことができませんでした)

Progress のエラーです。Windows の場合はイベント ログ、UNIX の場合はシステム ログで、RSA Authentication Manager サービスおよび Progress Software データベース ソフトウェアによるその他のエラーを検索してください。

ACE/Server Primary will handle authentication requests (今後はプライマリの RSA ACE/Server が認証要求を取り扱います)

プライマリとレプリカとの間の接続が復元され、プライマリがエージェント ホストからの認証要求に応答しています。

ACE/Server recvfrom failed (ACE/Server recvfrom の失敗)

ネットワークの接続と設定を確認してください。

ACE/Server Replica started (RSA ACE/Server がレプリカで起動されました)

RSA Authentication Manager サービスがレプリカで起動されました。

ACE/Server service exited abnormally . . . . (RSA ACE/Server サービスが異常終了しました)

Window の場合はイベント ログ、UNIX の場合はシステム ログで、RSA Authentication Manager サービスおよびデータベースから、認証サービスの失敗に関する追加情報を示す他のメッセージが記録されていないかどうかを確認してください。

ACE/Server service exited normally (ACE/Server サービスが正常に終了しました)

RSA Authentication Manager サービスが停止されました。

ACE/Server service started (ACE/Server サービスが開始されました)

RSA Authentication Manager サービスが開始されました。

ACE/Server service stopped (ACE/Server サービスが停止されました)

RSA Authentication Manager サービスが停止されました。

ACE/Server unable to set ACE/Server credentials (ACE/Server は ACE/Server クレデンシャルを設定できませんでした)

license.rec ファイルが存在することを確認し、ファイルのアクセス権が適切であるかどうかを確認してください。

Acesyncd aborted (2001) (acesyncd がアボートしました)

問題の正確な内容を示す他のメッセージが登録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Acesyncd had a bus error (2002) (acesyncd でバス エラーが発生しました)

問題の内容を詳細に記述したメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Acesyncd had seg violation (2003) (acesyncd でセグメンテーション違反が発生しました)

問題の内容を詳細に記述したメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Acesyncd Primary Started (プライマリで acesyncd が起動されました)

このステータス メッセージは、プライマリでレプリケーション プロセスが起動されたことを示します。

Acesyncd Replica Started (レプリカで acesyncd が起動されました)

このステータス メッセージは、レプリカでレプリケーション プロセスが起動されたことを示します。

ACM ERROR: Unable to bind the socket for ACE/Server (ACM エラー : ACE/Server に対してソケットをバインドできませんでした)

このメッセージは、サービスが停止されてから再起動されるまでの間に、オペレーティング システムがソケットを閉じるのが間に合わなかったか、または ***%SYSTEMROOT%*¥system32¥drivers¥etc¥services** (***%SYSTEMROOT%*** はルート ディレクトリであり、たとえば **winnt**) ファイルで RSA Authentication Manager サービス用として定義されているポートで他のプロセスが起動されたことを示します。

RSA ACE/Server サービスが使用するポート番号を変更するには

1. プライマリとレプリカで RSA Authentication Manager サービスを停止します。
2. **services** ファイルを編集してポート番号を変更します。Windows の場合、ファイルは ***%SYSTEMROOT%¥system32¥drivers¥etc¥services*** ディレクトリにあります。UNIX の場合は、ファイルは **/etc** ディレクトリにあります。
3. RSA Authentication Manager 構成ファイル (**sdconf.rec**) を変更します。Windows でポート番号を変更するには、Configuration Management アプリケーションを使用します。UNIX の場合は、**sdsetup -config** コマンドを使用します。
4. 新しい構成ファイルを作成して、レプリカおよびエージェント ホストに配布します。ファイル (プライマリの ***ACEDATA*** ディレクトリにある **sdconf.rec**) をレプリカの ***ACEDATA*** ディレクトリにコピーし、Configuration Management アプリケーションを実行して、**sdconf.rec** ファイルを更新します。

   sdconf.rec ファイルの配布の詳細については、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。

   メモ : sdconf.rec ファイルは Configuration Management アプリケーションによって作成されます。エージェント ホストでは **DES** または **SDI** 暗号方式を使用できますが、各エージェント ホストには、使用する暗号方式に対応する **sdconf.rec** ファイルが必要です。**DES** 暗号方式を使用するエージェント ホストと **SDI** 暗号方式を使用するエージェント ホストの両方がある場合は、各エージェント ホストに配布する **sdconf.rec** ファイルに暗号方式が正しく設定されていることを確認してください。
5. **ftp** を使用してファイルをコピーする場合は、バイナリ モードを選択してください。
6. プライマリとレプリカで RSA Authentication Manager サービスを再起動します。

Admin Server (sdadmind) and remote administrative client (Host: %1) are not the same version (16197) (アドミニストレーション サーバ (sdadmind) とリモート アドミニストレーション クライアント (ホスト : %1) のバージョンが異なります)

管理者がデータベースに接続するために使用した Remote Administration ソフトウェアのバージョンが正しくありません。Remote Administration ソフトウェアのバージョンが古いと考えられます。Remote Administration ソフトウェアを RSA Authentication Manager と同じバージョンにアップグレードしてください。

Agent Host has no Acting Servers (1138) (エージェント ホストにアクティング サーバがありません)

v5.0 より前のバージョンの RSA Authentication Manager ソフトウェアを実行しているエージェント ホストのデータベースで、アクティング マスタとアクティング スレーブが割り当てられていません。詳細については、24 ページの「ファイアウォールを介した Authentication Manager とエージェント ホストの通信」および 233 ページの「ホスト名とサービス名の解決」を参照してください。

Agent Host not found (130) (エージェント ホストが見つかりません)

ユーザが認証を受けるには、Authentication Manager 自体も含めて、ネットワーク上の各マシンが Authentication Manager データベースにエージェント ホストとして登録されている必要があります。このログ メッセージは、ユーザがログオンしようとしているマシンの名前がエージェント ホストの一覧に登録されていないことを示します。

このメッセージにエージェント ホストのホスト名ではなく、IP アドレスが示されている場合は、Authentication Manager が IP アドレスを解決できない問題があることを表します。このアドレスが **hosts** ファイルまたはネーム サーバ データベースに定義されていることと、エージェント ホストが Authentication Manager データベースに定義されていることを確認してください。エージェント ホストがデータベースに登録されていない場合は、[Agent Host] メニューの [Add Agent Host] を使用して登録します。エージェント ホストを作成した後、そのエージェント ホストでユーザを直接アクティブ化するか、またはグループを通じてアクティブ化してください。これらの操作の詳細については、第 3 章「エージェントとエージェント ホスト上でのアクティブ化」を参照してください。

このメッセージが表示されても、エージェント ホストが実際に作成され、エージェント ホストの一覧 ([Agent Host] メニューのオプションを使用) に表示される場合は、Authentication Manager をいったん停止してから再起動してください。Windows では、[RSA Authentication Manager Control Panel] を使用します。UNIX では、**aceserver start** コマンドと **aceserver stop** コマンドを使用します。この操作を実行すると、エージェント ホストのデータベースが起動時に再度読み取られるため、問題を解決できるはずです。

Agent Host not found in Server database, but cannot delete Agent Host delta (15249) (サーバ データベースでエージェント ホスト レコードが見つかりませんでしたが、エージェント ホストのデルタを削除できませんでした)

レプリケーション パスで、レプリケーション サービスはデータベース レコードを変更しようとしましたが、そのレコードにアクセスできませんでした。管理者がレプリケーション パスの途中でレコードを編集した場合は、この問題が発生することがあります。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、レプリカに適用してください。

Agent Host record is locked and cannot be updated. Will attempt to update at next replication pass. %1 (15118) (エージェント ホスト レコードがロックされているため、更新できません。次のレプリケーション パスで更新します)

このメッセージが繰り返し記録される場合は、レプリカを再起動してください。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Aggregate functions other than COUNT, MIN or MAX are not supported (COUNT、MN、MAX 以外の集計関数はサポートされません)

サポートされない集計関数 (たとえば AVG) をクエリで使用すると、このメッセージが表示されます。カスタム クエリでサポートされる集計関数は、COUNT、MIN、および MAX だけです。

ALL is not supported in the list of output fields (出力フィールドのリストで、ALL は使用できません)

列名に複数のフィールドが含まれている場合は、SELECT ステートメントで ALL オプションを使用できません。デフォルト設定では、列名に指定されているフィールドからすべてのデータが選択されるため、ALL は不要です。

All SELECT statements must return same set of fields in the same order (すべての SELECT ステートメントが同じフィールド セットを同じ順序で返さなければなりません)

複数の SELECT ステートメントを含む複雑なクエリでは、すべての SELECT ステートメントに同じ順序で同じ列名を指定する必要があります。

An error occurred while creating a process for database broker management (15041) (データベース ブローカ管理用のプロセスの生成中にエラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

An error occurred while reading the registry for database broker management (15040) (データベース ブローカ管理用のレジストリの読み取りでエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

An Error Occurred While Reconciling Databases (15192) (データベースの調整でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

An Error Occurred While Walking Databases (データベースの検索でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

An unexpected word was encountered in the query (期待していない単語がクエリから検出されました)

このエラーは通常、認識される単語が SQL コードの予期しない場所で検出されたときに発生します。たとえば、IF-THEN-ELSE 条件ステートメントで、THEN が必要な場所から、構文チェッカが SELECT を検出すると、このエラーが発生します。

An unknown error was encountered (不明エラーが検出されました)

カスタム クエリのファイル階層構造に壊れたファイルや消失したファイルがあると、このエラーが発生することがあります。このエラーが発生した場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Application Log is Full (アプリケーション ログが満杯です)

ユーザ、管理者、または RSA Authentication Manager プロセスによるアクションのたびに、RSA Authentication Manager アプリケーションは Windows のイベント ログの機能であるアプリケーション ログにエントリを書き込みます。ログのサイズは固定されているため、エントリでいっぱいになると、RSA Authentication Manager の起動時にこのメッセージが画面に表示されます。

アプリケーション ログのエントリは一般に、デバッグ以外に使用することはありません。このメッセージが表示されないようにするには、次の方法をお勧めします。

- 可能な場合は、ログのサイズをデフォルトの 512 KB よりも大きくします。
- 新しいエントリが追加されたときに、もっとも古いエントリに上書きするようにログを設定します。これによってログが満杯になるのを防止でき、しかもデバッグで必要な場合は、最新のエントリを利用できます。

Windows のイベント ログのオプションを設定するには

1. [スタート] > [プログラム] > [管理ツール] > [イベント ビューア] の順にクリックして、イベント ログを表示します。
2. 左ペインで [アプリケーション] を選択して右クリックし、[プロパティ] を選択します。
3. ログのサイズを大きくするのに必要な空きディスク容量がある場合は、[最大ログ サイズ] ボックスに新しい値 (KB 単位) を入力するか、またはこのボックスの上向き矢印ボタンをクリックし、64 KB 刻みでサイズを大きくします。新しいログ サイズは、少なくとも 1 MB (1024 KB) に設定してください。
4. [必要に応じてイベントを上書きする] をクリックします。
5. [OK] をクリックして、イベント ビューアを終了します。

Archive Error: %1 failed; errno %2 (15996) (アーカイブ エラー)

ログ メンテナンス デーモンがデータベースにアクセスして、データをアーカイブすることができませんでした。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Assisted recvry (PushDB) disabled (2288) (データベース プッシュ機能 (Push DB) が無効です)

レプリカが新しいデータベースを必要としていることがマークされているのに、システム パラメータの設定では Push DB Assisted Recovery (データベース プッシュ) 機能が許可されていません。Push DB が無効になっている場合、プライマリはレプリカにレプリカ パッケージを送信できません。Push DB 機能を有効にするには、[System] > [System Configuration] > [Edit System Parameters] の順にクリックし、[Allow Push DB Assisted Recovery] チェックボックスをオンにします。

Push DB Assisted Recovery (データベース プッシュ) 機能を使用してデータベース レプリカ パッケージをレプリカに送信する場合は、この機能が有効になるようにプライマリでシステム パラメータを設定した後、プライマリで新しいレプリカ パッケージを作成し、レプリカを再起動します。レプリカを再起動すると、プライマリはレプリカ パッケージをレプリカに送信します。

Push DB Assisted Recovery 機能を使用する必要がない場合は、レプリカ パッケージを作成し、レプリカ パッケージ内のファイルをレプリカの ***ACEDATA*** ディレクトリにコピーしてから、レプリカを再起動してください。

Attempt To Start Demon On Unauthorized Host (承認されていないホストでデーモンを起動しようとしました)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

AUTH IGNORED, TRIAL EXPIRED (1009) (認証は無視されました、トライアルの有効期限が切れています)

トライアル用の RSA Authentication Manager ソフトウェアの有効期限が切れています。ユーザは今後も認証を受けることができますが、認証サービスを停止した場合、再起動することはできず、管理アプリケーションを実行することもできません。トライアル ソフトウェアを削除するか、または製品版のソフトウェアに移行する必要があります。RSA Authentication Manager ソフトウェアを購入する方法については、RSA セキュリティ正規販売代理店にお問い合わせください。

AUTHENTICATION Failed to get socket desc from server context. (15076) (認証サービスでサーバ コンテキストからソケット記述を取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

Breaking connection with message %1 (15151) (メッセージ %1 で接続が切断されました)

レプリカがプライマリとの通信を切断しようとしたときに、エラーが発生しました。プライマリがレプリカにデータベースをプッシュしているときに、このメッセージが表示された場合は、レプリカをいったん停止した後、再起動してください。

Broker for sdlog started (sdlog のブローカが起動されました)

sdlog のブローカが起動されました。

Broker for sdserv started (sdserv のブローカが起動されました)

sdserv のブローカが起動されました。

Broker service started (ブローカ サービスが開始されました)

データベース ブローカを担当するサービスが開始されました。

Broker service stopped (ブローカ サービスが停止されました)

データベース ブローカを担当するサービスが停止されました。その他のイベント ログ メッセージを確認してください。

Brokers restarted (2292) (ブローカが再起動されました)

Push DB が正常に実行されている場合は、「Start rep pack reinstall (レプリカ パッケージの再インストールを開始します)」というメッセージの後に、このメッセージが記録されます。

Bus Error (%1) (16202) (バス エラー)

RSA Authentication Manager プロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**、および **sdadmind**、**acesrvc**、**acesrvc_be**、**logmainthd**) が異常終了すると、このメッセージが表示されます。メッセージに示されているエラーを確認してください。RSA Authentication Manager ソフトウェアに関連しない問題の場合は、適切な処置をとり、問題が解決されたら RSA Authentication Manager を再起動してください。RSA Authentication Manager ソフトウェアに関連する問題の場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Can't Share Lock System On Replica (15205) (レプリカでロック システムを共有できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot acquire query and save it with the specified name. Query with same name already exists locally or provided name includes invalid symbols (クエリを入手して、指定された名前で保存することができませんでした。同じ名前のクエリがすでにローカルに存在するか、指定された名前に不正な記号が含まれています)

共有クエリを入手するときに、別の共有クエリですでに使用されている名前を割り当てたか、または使用した名前に不正な文字が含まれていました。

Cannot Check Delete Dependency for *NAME* (*NAME* の削除の依存関係をチェックできませんでした) (個別のメッセージについては、401 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Check Dependency for *NAME* (*NAME* の依存関係をチェックできませんでした) (個別のメッセージについては、402 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Close System Table %1 (15263) (システム テーブルを閉じることができませんでした)

このメッセージが繰り返し表示される場合は、プライマリをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Close System Table (15263) (システム テーブルを閉じることができませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot close trace file. It is not open (トレース ファイルを閉じることができませんでした。トレース ファイルは開かれていません)

トレース ファイルを使用すると、プライマリとレプリカの間の通信の問題を解決するのに役立ちます。パケット トレースを有効にし、結果を表示する方法については、RSA セキュリティ正規販売代理店にお問い合わせください。

Cannot compare Agent last modified dates for merge (15117) (マージ操作でエージェントの最終変更日を比較できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Compare System L Dates for Merge (15203) (マージ操作でシステムの L 日付を比較できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Compare Token E Dates for Merge (マージ操作でトークンの E 日付を比較できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Compare Token L Dates for Merge (マージ操作でトークンの L 日付を比較できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Compare Token LE Dates for Merge (マージ操作でトークンの LE 日付を比較できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Compare Token P Dates for Merge (マージ操作でトークンの P 日付を比較できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Copy Delta To *NAME* To Delete On Replica (*NAME* にデルタをコピーしてレプリカで削除することができませんでした) (個別のメッセージについては、404 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot copy file (*OS error code*) (ファイルをコピーできませんでした)

コピーしようとしたファイルが壊れているか、または消失しています。

Cannot Copy *NAME* Delta (*NAME* のデルタをコピーできませんでした) (個別のメッセージについては、405 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot copy query using specified name. Query with same name already exists locally or provided name includes invalid symbols (指定された名前を使用してクエリをコピーできませんでした。同じ名前のクエリがすでにローカルに存在するか、または指定された名前に不正な記号が含まれています)

クエリをコピーするときに、別のクエリですでに使用されている名前を割り当てたか、または使用した名前に不正な文字が含まれていました。

Cannot create destination folder (*OS error code*) (コピー先フォルダを作成できませんでした)

コピー操作の実行時に、クエリ フォルダの作成で問題が発生しました。親フォルダ (クエリ) の名前が変更されたか、他の重大な OS エラーが発生した可能性があります。

Cannot Create (Update) *NAME* On Replica (レプリカで *NAME* を作成 (更新) できませんでした) (個別のメッセージについては、406 ページを参照してください)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Decode Primary Agent Host SB for Merge (マージ操作でプライマリ エージェント ホストの SB をデコードできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Decode Primary Token SB (プライマリ トークンの SB をデコードできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Decode Replica Agent Host SB for Merge (マージ操作でレプリカ エージェント ホストの SB をデコードできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot decode Replica token SB (レプリカ トークンの SB をデコードできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Decrypt Primary System SB for Merge (15201) (マージ操作でプライマリ システムの SB を復号できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Decrypt Replica System SB for Merge (15202) (マージ操作でレプリカ システムの SB を復号できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot decrypt system record (15026) (システム レコードを復号できませんでした)

データベース内の機密データの復号で問題が発生しました。***ACEDATA*** ディレクトリに正しいライセンス レコードが登録されているかどうかを確認してください。

Cannot Delete Log Entry (15230) (ログ エントリを削除できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Delete *NAME* Delta (*NAME* のデルタを削除できませんでした) (個別のメッセージについては、408 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Delete *NAME* On Replica (レプリカで *NAME* を削除できませんでした) (個別のメッセージについては、409 ページを参照してください)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot delete query (*OS error code*) (クエリを削除できませんでした)

指定されたクエリを削除するときに問題が発生しました。クエリの名前が変更されたか、OS の標準的な手段で削除されたか、他の重大な OS エラーが発生した可能性があります。

Cannot determine number of attempted authentications associated with this token. Delete the token, and then reimport it to the database. (15214) (このトークンを使用して行われた認証の試行回数を判断できませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot determine the correct ETC Date associated with this token. Delete the token, and then reimport it to the database (21000) (このトークンに割り当てられている正しい ETC 日付を判断できませんでした。トークンを削除した後、データベースに再インポートしてください)

クロックのドリフトまたは何らかの内部的な問題があるために、Authentication Managerがトークンの正しいエマージェンシー トークンコード日付を判断できませんでした。メッセージに示されているように、トークン レコードをいったん削除し、Authentication Manager データベースに再インポートしてください。問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot determine the correct PIN number associated with this token. Delete the token, and then reimport it to the database (15215) (このトークンに割り当てられている正しい PIN 番号を判断できませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot determine the last successful authentication associated with this user (15217) (このユーザが最後に成功した認証を判断できませんでした)

レプリケーション パスでユーザ レコードを更新できませんでした。

Cannot determine the last successful EAP date associated with this user (21003) (このユーザが最後に成功した EAP 日付を判断できませんでした)

エマージェンシー PASSCODE のマージ日付が競合するために、レプリケーション パスでユーザ レコードを更新できませんでした。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。レプリカ パッケージを適用しても問題を解決できない場合は、RSA セキュリティ正規販売代理店へご連絡ください。

Cannot determine when the last login occurred with this token. Delete the token, and then reimport it to the database (15213) (このトークンを使用して最後にログインが行われた日時を判断できませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot determine when token was enabled. Delete the token, and then reimport it into the database (15212) (トークンが有効化された日時を判断できませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot determine when token was marked lost. Delete the token, and then reimport it into the database (トークンが紛失したトークンとしてマークされた日時を判断できませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Exclusive Lock Agent Host for Merge (マージ操作でエージェント ホストを排他的にロックできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Exclusive Lock *NAME* Delta (*NAME* のデルタを排他的にロックできませんでした) (個別のメッセージについては、411 ページを参照してください)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Exclusive Lock System (15264) (システムを排他的にロックできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Exclusive Lock System for Merge (15199) (マージ操作でシステムを排他的にロックできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Exclusive Lock Token for Merge (マージ操作でトークンを排他的にロックできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot execute query. Output directory does not exist (クエリを実行できませんでした。出力ディレクトリが存在しません)

クエリの標準出力ディレクトリ (デフォルト名は **output**) が ***ACEDIR*** に存在しないため、クエリを実行できませんでした。

Cannot execute query. Query file is missing or corrupt (クエリを実行できませんでした。クエリ ファイルが存在しないか、または壊れています)

新しいクエリを作成 (またはサンプル クエリを編集) すると、ユーザのレルム用にクエリがコンパイルされます。コンパイルされたクエリの名前は **query.r** で、クエリ フォルダに保存されます。このエラーが発生した場合は、**query.r** ファイルに何らかの問題があります。ファイルが削除されたか、名前が変更されたか、壊れている可能性があります。

Cannot Fetch *NAME* Delta (*NAME* のデルタをフェッチできませんでした) (個別のメッセージについては、412 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Fetch System Record (15262) (システム レコードをフェッチできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Find *NAME* To Delete On Replica (レプリカで *NAME* を検索して削除することができませんでした) (個別のメッセージについては、413 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Find Pending Delete for *NAME* (*NAME* の削除保留を見つけることができませんでした) (個別のメッセージについては、415 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot find the user record for token serial number 000000*nnnnnn* (トークン シリアル番号 000000*nnnnnn* に対応するユーザ レコードが見つかりませんでした)

このメッセージは次の場合に表示されます。

- トークン レコードが壊れている場合。
- ユーザが削除されたにもかかわらず、トークン　レコードが更新されていない場合。

  ユーザが削除されていないかどうかを確認してください。削除されていない場合は、元のトークンの割り当てを解除します。その後、別のトークンをユーザに割り当ててください。

Cannot fully read query data. Using default values for undefined and improperly configured parameters (クエリ データを完全に読み取ることができませんでした。未定義のパラメータや設定が誤っているパラメータに対してはデフォルト値を使用します)

新しいクエリを作成 (またはサンプル クエリを編集) すると、ユーザのレルム用にクエリがコンパイルされ、必要なファイルがクエリ フォルダに保存されます。コンパイルされたクエリ (**query.r**) の他に、出力フォーマットなどの項目を定義する **runtime.txt** ファイルが作成されます。このエラーが発生した場合は、**runtime.txt** ファイルに何らかの問題があります。ファイルが削除されたか、名前が変更されたか、壊れている可能性があります。

Cannot get system time (%1) (15063) (システム時刻を取得できませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot get the local database directory (ローカル データベース ディレクトリを取得できませんでした)

新しいクエリを作成または実行しようとしたときに、カスタム クエリ機能が RSA Authentication Manager データベース ディレクトリの場所を判断できませんでした。***ACEDATA*** ディレクトリは通常、**c:¥ace¥data** にあります。ディレクトリが削除されたか、名前が変更されたか、壊れている場合は、このエラーが発生します。

Cannot initialize Agent Host-server communications (エージェント ホストとサーバの間の通信を初期化できませんでした)

これは、289 ページの「認証試行中にエージェント ホストがハングした場合」に説明されている問題と同じです。そこに示されている対処法を参照してください。

Cannot Locate *NAME* To Delete On Replica (レプリカで *NAME* を検索して削除することができませんでした) (個別のメッセージについては、416 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Mark Agent Host Delta for Merge (マージ操作でエージェント ホストのデルタをマークできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Mark System Delta for Merge (15200) (マージ操作でシステムのデルタをマークできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Mark Token Delta for Merge (マージ操作でトークンのデルタをマークできませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Match Delta State for *NAME* (*NAME* のデルタの状態を照合できませんでした) (個別のメッセージについては、418 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot merge Agent Host record from the Primary because the security block could not be decrypted. Delete the Agent Host and then re-add it to the Primary database (15115) (セキュリティ ブロックを復号できなかったため、プライマリからエージェント ホスト レコードをマージできませんでした。エージェント ホストを削除した後、プライマリのデータベースに再登録してください)

レプリケーション パスでエージェント ホスト レコードを更新できませんでした。エージェント ホストをデータベースから削除し、もう一度登録してください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot merge Agent Host record to the Primary because the security block could not be decrypted. Delete the Agent Host and then re-add it to the Replica database (21001) (セキュリティ ブロックを復号できなかったため、エージェント ホスト レコードをプライマリにマージできませんでした。エージェント ホストを削除した後、レプリカのデータベースに再登録してください)

レプリケーション パスでエージェント ホスト レコードを更新できませんでした。エージェント ホストをデータベースから削除し、もう一度登録してください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot merge token record from the Primary because the security block could not be decrypted. Delete the token, and then reimport it to the database (15210) (セキュリティ ブロックを復号できなかったため、プライマリからトークン レコードをマージできませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot merge token record from the Replica because the security block could not be decrypted. Delete the token, and then reimport it to the database (15211) (セキュリティ ブロックを復号できなかったため、レプリカからトークン レコードをマージできませんでした。トークンを削除した後、データベースに再インポートしてください)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot merge token record to the Primary because the security block could not be decrypted (セキュリティ ブロックを復号できなかったため、トークン レコードをプライマリにマージできませんでした)

レプリケーション パスでトークン レコードを更新できませんでした。トークンをデータベースから削除し、再インポートしてください。それでもこのメッセージが表示される場合は、データベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Cannot merge User record from the Primary because the security block could not be decrypted. Delete the User (record) and then re-add it to the Primary database (21002) (セキュリティ ブロックを復号できなかったため、プライマリからユーザ レコードをマージできませんでした。ユーザ (レコード) を削除した後、プライマリのデータベースに再登録してください)

Authentication Manager がレプリケーション パスでユーザ レコードのセキュリティ ブロックに関する内部的な問題を検出したため、処理を続行できませんでした。ユーザ レコードを削除して、再作成してください。それでも問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot merge User record to Primary because its security block could not be decrypted. Delete the User and then re-add it to the database (21001) (セキュリティ ブロックを復号できなかったため、ユーザ レコードをプライマリにマージできませんでした。ユーザを削除した後、データベースに再登録してください)

Authentication Manager がレプリケーション パスでユーザ レコードのセキュリティ ブロックに関する内部的な問題を検出したため、処理を続行できませんでした。ユーザ レコードを削除して、再作成してください。それでも問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Open *NAME* Delta Cursor (*NAME* のデルタ カーソルを開くことができませんでした) (個別のメッセージについては、419 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Open System Table (システム テーブルを開くことができませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Open System Table %1 (15261) (システム テーブルを開くことができませんでした)

このメッセージが繰り返し表示される場合は、プライマリを再起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Read *NAME* Commit Response (*NAME* のコミット応答を読み取ることができませんでした) (個別のメッセージについては、420 ページを参照してください)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot read system record (15027) (システム レコードを読み取ることができませんでした)

Progress のエラーです。Windows の場合はイベント ログ、UNIX の場合はシステム ログで、RSA Authentication Manager サービスおよび Progress データベース ソフトウェアによるその他のエラーを検索してください。

Cannot rename query using specified name. Query with same name already exists locally or provided name includes invalid symbols (指定された名前を使用してクエリの名前を変更できませんでした。同じ名前のクエリがすでにローカルに存在するか、または指定された名前に不正な記号が含まれています)

既存の名前または不正な文字を含む名前を使用しようとしました。以下の文字は使用できません。

{} ~ " ; ' [ ] , / @ < > ^ |

Cannot resolve service %1 by name (15023) (サービスを名前で解決できませんでした)

メッセージに指定されているサービス名に問題があります。サービスの名前とポート番号が構成管理ユーティリティで正しく設定されているかどうかを確認してください。UNIX では、**sdsetup -repmgmt list** を実行します。

Cannot Save *NAME* On Replica (レプリカで *NAME* を保存できませんでした) (個別のメッセージについては、422 ページを参照してください)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send Agent Host delta to Primary. Agent Host record may be locked by another administrator. Will attempt to send delta at next replication pass. %1 (15114) (エージェント ホストのデルタをプライマリに送信できませんでした。エージェント ホスト レコードが他の管理者によってロックされている可能性があります。次のレプリケーション パスでデルタを送信します)

このメッセージが繰り返し記録される場合は、レプリカを再起動してください。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send Agent Host delta to Primary. Will attempt to send at next replication pass. %1 (15251) (エージェント ホストのデルタをプライマリに送信できませんでした。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Cannot Send Agent Host To Primary (エージェント ホスト レコードをプライマリに送信できませんでした)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot send log entry record to Primary. Will attempt to send at next replication pass. %1 (15229) (ログ エントリ レコードをプライマリに送信できませんでした。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Send Log Entry To Primary (ログ エントリをプライマリに送信できませんでした)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Send *NAME* Commit Request to Replica (*NAME* のコミット要求をレプリカに送信できませんでした) (個別のメッセージについては、423 ページを参照してください)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Send *NAME* To Replica (*NAME* をレプリカに送信できませんでした) (個別のメッセージについては、425 ページを参照してください)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot send one-time password delta. One-time password record may be locked by another administrator. Will attempt to send at next replication pass. %1 (15244) (ワンタイム パスワードのデルタを送信できませんでした。ワンタイム パスワード レコードが他の管理者によってロックされている可能性があります。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、プライマリをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send one-time password record to Primary. Will attempt to send at next replication pass. %1 (15245) (ワンタイム パスワード レコードをプライマリに送信できませんでした。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Cannot Send System To Primary (システム レコードをプライマリに送信できませんでした)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot send token delta to Primary. Token record may be locked by another administrator. Will attempt to send delta at next replication pass. %1 (15209) (トークン デルタをプライマリに送信できませんでした。トークン レコードが他の管理者によってロックされている可能性があります。次のレプリケーション パスでデルタを送信します)

このメッセージが繰り返し記録される場合は、レプリカを再起動してください。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send token delta. Token record may be locked by another administrator. Will attempt to send at next replication pass. %1 (15207) (トークン デルタを送信できませんでした。トークン レコードが他の管理者によってロックされている可能性があります。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、プライマリをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send token record to Primary. Will attempt to send at next replication pass. %1 (15239) (トークン レコードをプライマリに送信できませんでした。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Cannot Send Token To Primary (トークン レコードをプライマリに送信できませんでした)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot send user delta to Primary. User record may be locked by another administrator. Will attempt to send delta at next replication pass. %1 (15208) (ユーザ デルタをプライマリに送信できませんでした。ユーザ レコードが他の管理者によってロックされている可能性があります。次のレプリケーション パスでデルタを送信します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send user delta. Token record may be locked by another administrator. Will attempt to send at next replication pass. %1 (15206) (ユーザ デルタを送信できませんでした。トークン レコードが他の管理者によってロックされている可能性があります。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、プライマリをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot send user record to Primary. Will attempt to send at next replication pass. %1 (15234) ユーザ レコードをプライマリに送信できませんでした。次のレプリケーション パスで送信します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot share query and save it with the specified name. Query with same name or a folder with same name includes invalid symbols (クエリを共有して、指定された名前で保存することができませんでした。同じ名前のクエリまたは同じ名前のフォルダに不正な記号が含まれています)

既存の名前または不正な文字を含む名前を使用しようとしました。以下の文字は使用できません。

{} ~ " ; ' [ ] , / @ < > ^ |

Cannot start default application for the output file (出力ファイルのデフォルト アプリケーションを起動できませんでした)

クエリを実行する場合、出力ファイルの形式を指定することができ、クエリの出力が生成された後、デフォルト アプリケーションを自動的に起動するかどうかも指定できます。デフォルト アプリケーションを起動するときに、RSA Authentication Manager で問題が検出されました。パスが正しくないか、アプリケーションが壊れているか、存在しないか、他の重大な問題が発生した可能性があります。

Cannot Update Agent Host for Merge (マージ操作でエージェント ホストを更新できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot update locked system record (ロックされているシステム レコードを更新できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot update locked system record %1 (15274) (ロックされているシステム レコードを更新できませんでした)

RSA Authentication Manager をいったん停止し、起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Update *NAME* On Replica (レプリカで *NAME* を更新できませんでした) (個別のメッセージについては、426 ページを参照してください)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Update System for Merge (15204) (マージ操作でシステムを更新できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot update token (%1) (15064) (トークンを更新できませんでした)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot Update Token for Merge (マージ操作でトークンを更新できませんでした)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Cannot Update (Create) *NAME* On Replica (レプリカで *NAME* を更新 (作成) できませんでした) (個別のメッセージについては、428 ページを参照してください)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Cannot upgrade license...There are too many active users and Replicas in the database (ライセンスをアップグレードできませんでした。データベースに定義されているアクティブ ユーザとレプリカの数が多すぎます)

現在のインストールの内容は、指定された **license.rec** ファイルの制限を超えているため、ユーティリティはこのファイルを適用できませんでした。ライセンスで制限されている数より多くのアクティブ ユーザおよびレプリカが定義されています。

ライセンスのアップグレード プロセスで、正しい **license.rec** ファイルを指定しているかどうかを確認してください。問題を解決できない場合は、現在より多くの数のアクティブ ユーザを定義できる新しいアドバンスド ライセンスを入手してください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Cannot upgrade license...There are too many active users in the database (ライセンスをアップグレードできませんでした。データベースに定義されているアクティブ ユーザの数が多すぎます)

現在のインストールの内容は、指定された **license.rec** ファイルの制限を超えているため、ユーティリティはこのファイルを適用できませんでした。ライセンスで制限されている数より多くのアクティブ ユーザがすでに定義されています。

ライセンスのアップグレード プロセスで、正しい **license.rec** ファイルを指定しているかどうかを確認してください。問題を解決できない場合は、現在より多くの数のアクティブ ユーザを定義できるライセンスを入手してください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Cannot upgrade license...There are too many Replicas in the database (ライセンスをアップグレードできませんでした。データベースに定義されているレプリカの数が多すぎます)

現在のインストールの内容は、指定された **license.rec** ファイルの制限を超えているため、ユーティリティはこのファイルを適用できませんでした。この場合、RSA Authentication Managerデータベースに登録できる数より多くのレプリカがすでに登録されています。

ライセンスのアップグレード プロセスで、正しい **license.rec** ファイルを指定しているかどうかを確認してください。問題を解決できない場合は、アドバンスド ライセンスを入手してください。アドバンスド ライセンスでは、各レルムで最大 10 台のレプリカを定義できます。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Cannot upgrade license...You are attempting to upgrade your Permanent license with an Evaluation license (ライセンスをアップグレードできませんでした。パーマネント ライセンスを評価用ライセンスにアップグレードしようとしています)

指定された **license.rec** ファイルは評価用ライセンスであるため、ユーティリティはこのファイルを適用できませんでした。評価用ライセンスは一定期間だけ有効であり、その期間は通常、ライセンスをインストールしたときからではなく、ライセンスが発行されてから90日間です。ライセンスのアップグレード プロセスで、正しい**license.rec** ファイルを指定しているかどうかを確認してください。問題を解決できない場合は、適切なライセンスを入手してください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Cannot upgrade license...You cannot apply a license that is in violation (ライセンスをアップグレードできませんでした。違反モードのライセンスを適用することはできません)

指定された **license.rec** ファイルは**アップグレード違反**モードであるため、ユーティリティはこのファイルを適用できませんでした。アップグレード違反モードになると、ライセンスは 90 日間有効のテンポラリ ライセンスになります。

ライセンスのアップグレード プロセスで、正しい **license.rec** ファイルを指定しているかどうかを確認してください。問題を解決できない場合は、適切なライセンスを入手してください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Cannot use a wildcard while joining tables (テーブルの結合でワイルドカードを使用できませんでした)

ワイルドカード文字 (*) は、1 つのテーブルから選択する場合にだけ使用できます。複数のテーブルから選択するときに (テーブル結合)、ワイルドカードを使用することはできません。

Cannot Write Push Response %1 (15272) (プッシュ応答を書き込むことができませんでした)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。再起動した後もメッセージが記録される場合は、新しいレプリカ パッケージを作成し、手動で適用します。

Can't get server context, FIND REALM FAILED (15082) (サーバ コンテキストを取得できませんでした。レルムの検索が失敗しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Can't get server context, OPEN REALM FAILED (15081) (サーバ コンテキストを取得できませんでした。レルムを開く操作が失敗しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Certificate verification failed and RSA ACE/Server will not start. The server.cer file either is corrupt or does not match the embedded root certificate (15030) (証明書の検証が失敗し、RSA ACE/Server を起動できませんでした。server.cer ファイルが壊れているか、埋め込まれているルート証明書と一致しません)

server.cer ファイルが不正です。**server.cer** ファイルをレプリカからコピーするか、または RSA Authentication Manager に付属しているオリジナルのライセンス フロッピー ディスクからコピーしてください。

Certificate verification failed and RSA ACE/Server will not start. The server.cer file was not found (15029) (証明書の検証が失敗し、RSA ACE/Server を起動できませんでした。server.cer ファイルが見つかりませんでした)

Authentication Manager の起動時に、***ACEDATA*** ディレクトリに **server.cer** ファイルが必要です。***ACEDATA*** ディレクトリに **server.cer** ファイルが格納されているかどうかを確認してください。ファイルが見つからない場合は、レプリカからコピーするか、または RSA Authentication Manager に付属しているオリジナルのライセンス フロッピー ディスクからコピーしてください。

Close realm cursor failed (%1) (15070) (レルム カーソルを閉じることができませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Close token cursor failed (%1) (15069) (トークン カーソルを閉じることができませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

COLLISION, agt rec, Accepting Rem (162) (競合、エージェント レコード、リモートの情報を使用します)

レプリケーション パスまたは認証で競合が発生しました。他の Authentication Manager のデータベースでエージェント ホスト レコードが変更された結果、このメッセージが記録された Authentication Manager のデータベースのエージェント ホスト レコードとの間で競合が発生しました。この Authentication Manager のデータベースを更新することで、競合は解決されました。

COLLISION, agt rec, Local IP (競合、エージェント レコード、ローカル IP アドレスを使用します)

レプリケーション パスまたは認証で競合が発生しました。他の Authentication Manager のデータベースでエージェント ホスト レコードの IP アドレスが変更された結果、このメッセージが記録された Authentication Manager のデータベースのエージェント ホスト レコードの IP アドレスとの間で競合が発生しました。他の Authentication Manager のデータベースを更新することで、競合は解決されました。

COLLISION, agt rec, Local Secret (173) (競合、エージェント レコード、ローカル シークレットを使用します)

レプリケーション パスまたは認証で競合が発生しました。他の Authentication Manager のデータベースでエージェント ホスト レコードのノード シークレットが変更された結果、このメッセージが記録された Authentication Manager のデータベースのエージェント ホスト レコードのノード シークレットとの間で競合が発生しました。他の Authentication Manager のデータベースを更新することで、競合は解決されました。

COLLISION, agt rec, Remote IP (競合、エージェント レコード、リモート IP を使用します)

レプリケーション パスまたは認証で競合が発生しました。他の Authentication Manager のデータベースでエージェント ホスト レコードの IP アドレスが変更された結果、このメッセージが記録された Authentication Manager のデータベースのエージェント ホスト レコードの IP アドレスとの間で競合が発生しました。この Authentication Manager のデータベースを更新することで、競合は解決されました。

COLLISION, agt rec, Remote Secret (172) (競合、エージェント レコード、リモート シークレットを使用します)

レプリケーション パスまたは認証で競合が発生しました。他の Authentication Manager のデータベースでエージェント ホスト レコードのノード シークレットが変更された結果、このメッセージが記録された Authentication Manager のデータベースのエージェント ホスト レコードのノード シークレットとの間で競合が発生しました。この Authentication Manager のデータベースを更新することで、競合は解決されました。

COLLISION, multiple node secrets (177) (競合、複数のノード シークレット)

RSA Authentication Manager は、同じ IP アドレスを使用するエージェント ホストから複数のノード シークレットを受信しました。この状況はネットワークへの不正な侵入によって発生した可能性があるため、Authentication Manager はエージェント ホスト レコードにノード シークレットを入力しません。Authentication Manager とエージェント ホストとの間の通信を可能にするには、ノード シークレットをいったん解除した後、新しいノード シークレットを設定する必要があります。

1. エージェント ホストでノード シークレット ファイルを消去します。

   エージェント ホストでノード シークレットを消去する方法については、RSA Authentication Manager ソフトウェアのマニュアルを参照してください。

2. 自動配布 (Automatic Delivery) 機能を使用している場合は、Authentication Manager でノード シークレット ファイルを消去します。手動配布 (Manual Delivery) 機能を使用している場合は、このステップは不要です。

   RSA Authentication Manager 上でノード シークレットを消去するには、エージェント ホストの [Edit Agent Host] ダイアログ ボックスを開き、[Node Secret Created] チェックボックスをオフにします。

3. ノード シークレットがエージェント ホストと Authentication Manager の両方で消去された場合は、次の操作を実行してください。
   - 自動配布 (Automatic Delivery) 機能を使用して新しいノード シークレットを作成する場合は、制御された初期認証を設定して、新しいノード シークレットを設定します。詳細については、19 ページの「データの暗号化」を参照してください。
   - 手動配布 (Manual Delivery) 機能を使用して新しいノード シークレットを作成する場合は、ヘルプの「Creating a Node Secret」を参照してください。

   ノード シークレットの配布方法の詳細については、222 ページの「ノード シークレット ファイル」を参照してください。

COLLISION, tok rec, Enabled on Remote (競合、トークン レコード、リモートで有効になりました)

トークンが他の Authentication Manager で有効になりました。このメッセージが記録された Authentication Manager のトークン レコードは、他の Authentication Manager の有効化情報で更新されました。

COLLISION, tok rec, Failed Logins (164) (競合、トークン レコード、ログインに失敗しました)

このメッセージが記録された Authentication Manager と他の Authentication Manager の両方で、このトークンを使用した認証が失敗しました。両方の Authentication Manager で失敗した認証回数が加算され、トークン レコードはその合計回数で更新されました。

COLLISION, tok rec, Last Login on Remote (競合、トークン レコード、リモートでログイン)

このトークンを使用して最後に行われた認証は他のAuthentication Managerで成功しました。この Authentication Manager のトークン レコードはこの情報で更新されました。

COLLISION, tok rec, Pin set Last on Remote (競合、トークン レコード、リモートで PIN 設定)

このトークンの最新の PIN 設定が他の Authentication Manager で行われました。このメッセージが記録された Authentication Manager のトークン レコードは、この PIN 設定で更新されました。

COLLISION, tok rec, Rep Used (168) (競合、トークン レコード、交換用トークンを使用します)

他の Authentication Manager で交換用トークンが発行されました。このメッセージが記録された Authentication Manager で発行されたオリジナル トークンの割り当ては解除されました。

Connection closed even though passcode accepted (PASSCODE は受け付けられましたが、接続が切断されました)

このメッセージは、ユーザの UNIX シェルが無効な場合に表示されます。ユーザをグループに追加するときや、エージェント ホスト上でアクティブ化するときに指定したシェルを確認します。シェルが有効であることと、スペルが間違っていないことを確認してください。

エージェント ホストのシェルが正しくない場合は、ユーザ レコードに指定されているシェルも確認してください。

Could Not Decrypt XR Message (8220) (XR メッセージを復号できませんでした)

ローカル レルムとリモート レルムのレルム シークレットが一致しません。レルム シークレットを再設定するには、[Edit Realm] ダイアログ ボックスの [Establish Realm Secret] をクリックします。

Created User Password (4539) (ユーザ パスワードが作成されました)

新しいユーザ パスワードがユーザによって作成されました。

CSV separator cannot be empty (CSV ファイルの区切り文字は必ず指定する必要があります)

[Query Wizard (Output Parameters)] ダイアログ ボックスで、[Separator] フィールドには文字を指定する必要があります。デフォルト設定はカンマですが、他の文字も指定できます。

Database Inconsistency. Replica Rejecting *NAME* Delta (データベースに不一致があります。レプリカは *NAME* のデルタを拒否しました) (個別のメッセージについては、429 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Date range for fixed PSW modified (3556) (固定パスワードの日付の範囲が変更されました)

これはステータス メッセージで、紛失したトークンに割り当てられた固定パスワードの有効日数の範囲が変更されたことを示します。

date time Ext-auth Check error *-nnnnn login user Agent Host server token* (8401) (Ext-auth チェック エラー)

このメッセージは、RSA Authentication Manager で External Authorization をアクティブ化したときに表示されます。**iSDExtAuthorCheck()** ルーチン用にこのメッセージを作成したプログラマから、このメッセージに割り当てられている戻り値を説明した一覧が提供されています。その一覧を参照してください。**iSDExtAuthorCheck()** ルーチンは、ユーザがエージェント ホストにログインすることを承認します。

date time Ext-auth Home-data error *-nnnnn login user Agent Host server token* (8403) (Ext-auth ホームデータ エラー)

このメッセージは、RSA Authentication Manager で External Authorization をアクティブ化したときに表示されます。**iSDExtAuthorGetHomeData()** ルーチン用にこのメッセージを作成したプログラマから、このメッセージに割り当てられている戻り値を説明した一覧が提供されています。その一覧を参照してください。**iSDExtAuthorGetHomeData ()** ルーチンは、レルム間認証の一部として返されるローカル情報を取得します。

Definition.txt file is corrupted and cannot be loaded (definition.txt ファイルが壊れているため、ロードできませんでした)

definition.txt ファイルには、SQL コードや、クエリに関するその他の情報が格納されています。そのファイルが壊れています。

Delete Error: %1 failed; errno %2 (15995) (削除エラー)

ログ メンテナンス デーモンがデータベースにアクセスして、レコードを削除することができませんでした。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Delta Record Exists Without Agent Host. Deleting (エージェント ホストがないのにデルタ レコードが存在します。削除します)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Delta Record Exists Without Token. Deleting (トークンがないのにデルタ レコードが存在します。削除します)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Destination folder has invalid permissions (OS error code) (コピー先フォルダのアクセス権が正しくありません)

クエリをコピーするときや、特定のディレクトリへの出力を指定するときに、適切なアクセス権のないコピー先 (出力先) を指定しました。

DISTINCT is not supported in the list of output fields (出力フィールドのリストで、DISTINCT はサポートされません)

SELECT ステートメントの列名で、DISTINCT 句を使用しています。DISTINCT はクエリの出力先を修飾する場合にだけ使用できます (たとえば、WHERE 句の後やテーブル結合の内部)。

Domain Secret Update Failed (8957) (ドメイン シークレットを更新できませんでした)

指定されたエージェントのドメイン シークレットを Authentication Manager データベースで更新できませんでした。エージェント レコードが壊れているか、セキュリティ ブロックの復号で問題が発生したと考えられます。問題を解決するには、まず、エージェント ホストを再起動してください。再起動しても問題を解決できない場合は、エージェント ホストをいったん削除して、再登録することで、ノード シークレットを消去します。問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Entered Log Monitoring (7008) (ログ モニタを開始しました)

管理者がログ モニタ セッションを開始しました。ログ モニタの詳細については、164 ページの「ログ モニタとレポート作成」を参照してください。

err in get a token record (%1) (15073) (トークン レコードの取得でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

err in get a admin record (%1. (15074) (アドミニストレーション レコードの取得でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error %1 setting Response Delay (15100) (応答遅延の設定でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error accepting connection (2006) (接続の受け付けでエラーが発生しました)

このメッセージは、RSA Authentication Manager の起動時または停止時に表示される可能性があります。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error closing system to get SB Keys (15129) (SB キー取得のためにシステムを終了しているときにエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Error comparing agent host L dates (2283) (エージェント ホストの L 日付の比較でエラーが発生しました)

このメッセージは、レプリケーション パスでデータベース レコードをマージしているときに表示される可能性があります。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error comparing lost dates (2334) (紛失日付の比較でエラーが発生しました)

RSA Authentication Manager は、トークンが紛失トークンとしてマークされた日付を判断できません。このメッセージが 1 回だけ記録されている場合は、トークンをいったん削除した後、データベースに再インポートしてください。このメッセージが何度もログに記録されている場合は、この Authentication Manager のデータベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Error comparing token ETC dates (2331) (トークンの ETC 日付の比較でエラーが発生しました)

このトークンのエマージェンシー トークンコード(ETC)の有効期限を判断できませんでした。このメッセージが 1 回だけ記録されている場合は、トークンをいったんエクスポートした後、データベースに再インポートしてください。このメッセージが何度もログに記録されている場合は、Authentication Manager のデータベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Error comparing user EAP dates (2330) (ユーザの EAP 日付の比較でエラーが発生しました)

ユーザ レコードのオフライン エマージェンシーPASSCODE の日付のマージで競合が発生しました。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。レプリカ パッケージを適用しても問題を解決できない場合は、RSA セキュリティ正規販売代理店へご連絡ください。

Error Committing Data on Replica (2007) (レプリカでデータをコミットするときにエラーが発生しました)

おそらく、このデータベースに対してサポートされていないアクセスが実行されたことが原因でレプリカ Authentication Manager データベースが壊れると、このエラーが発生します。カスタム アドミニストレーション プログラムはプライマリのデータベースのみで使用してください。レプリカ Authentication Manager のデータベースへの直接アクセスはサポートされないため、データベースが壊れる可能性があります。

Error comparing system dates (2009) (システム日付の比較でエラーが発生しました)

このメッセージは、レプリケーション パスでデータベース レコードをマージしているときに表示される可能性があります。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error Comparing Tkn Enable Dates (2011) (トークンの有効化の日付の比較でエラーが発生しました)

トークンの有効化の日付が不明です。このメッセージが 1 回だけ記録されている場合は、トークンをいったんエクスポートした後、データベースに再インポートしてください。このメッセージが何度もログに記録されている場合は、この Authentication Manager のデータベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Error Comparing Token Last Dates (2010) (トークンの最終日付の比較でエラーが発生しました)

このトークンを使用して行われた認証の試行回数が不明です。このメッセージが 1 回だけ記録されている場合は、トークンをいったんエクスポートした後、データベースに再インポートしてください。このメッセージが何度もログに記録されている場合は、この Authentication Manager のデータベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Error Comparing Token Last Logins (2012) (トークンの最終ログインの比較でエラーが発生しました)

このトークンを使用して行われた最後のログインが不明です。このメッセージが 1 回だけ記録されている場合は、トークンをいったんエクスポートした後、データベースに再インポートしてください。このメッセージが何度もログに記録されている場合は、この Authentication Manager のデータベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Error Comparing Token PIN Dates (2013) (トークンの PIN 日付の比較でエラーが発生しました)

このトークンの PIN が不明です。このメッセージが 1 回だけ記録されている場合は、トークンをいったんエクスポートした後、メッセージが記録されている Authentication Manager のデータベースに再インポートしてください。このメッセージが何度もログに記録されている場合は、この Authentication Manager のデータベースが壊れている可能性があります。RSA セキュリティ正規販売代理店にご連絡ください。

Error comparing user R A dates (2282) (R A 日付の比較でエラーが発生しました)

リモート ユーザ レコードのリモート アクセス日付のマージで競合が発生しました。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。レプリカ パッケージを適用しても問題を解決できない場合は、RSA セキュリティ正規販売代理店へご連絡ください。

Error: connection timed out (2015) (エラー：接続タイムアウト)

このメッセージは、RSA Authentication Manager の起動時または停止時に表示される可能性があります。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error copying integer field from buffer (バッファから整数フィールドをコピーしているときにエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Error creating agent delta (2016) (エージェント デルタの作成でエラーが発生しました)

レプリカでデータベースのバックアップを作成し、レプリカ パッケージを作成し、手動でレプリカに適用するか、または Push DB を使用して適用してください。この操作を行っても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error Creating Record (15137) (レコードの作成でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error creating record on replica (2017) (レプリカでレコードの作成中にエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error creating system delta (2018) (システム デルタの作成でエラーが発生しました)

レプリカでデータベースのバックアップを作成し、レプリカ パッケージを作成し、手動でレプリカに適用するか、または Push DB を使用して適用してください。この操作を行っても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting Primary agent SB (2019) (プライマリでエージェント SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。プライマリでエージェント ホスト レコードのセキュリティ ブロックを復号できないため、更新されたエージェント ホスト レコードをレプリカに送信できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting primary sys SB (2020) (プライマリでシステム SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。データベース内の特定のフィールドを暗号化するために使用されるセキュリティ ブロックを Authentication Manager で復号できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting Primary token SB (2021) (プライマリでトークン SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。プライマリでトークン レコードのセキュリティ ブロックを復号できないため、エージェント ホスト レコードの変更をレプリカに反映できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting replica agent SB (2022) (レプリカでエージェント SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。レプリカでエージェント ホスト レコードのセキュリティ ブロックを復号できないため、エージェント ホスト レコードの変更をレプリカに反映できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting replica sys SB (2023) (レプリカでシステム SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。データベース内の特定のフィールドを暗号化するために使用されるセキュリティ ブロックを Authentication Manager で復号できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error Decrypting Replica Token SB (2024) (レプリカでトークン SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。レプリカでトークン レコードのセキュリティ ブロックを復号できないため、エージェント ホスト レコードの変更をレプリカに送信できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting system sec-blk (2025) (システム セキュリティ ブロックの復号でエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。データベース内の特定のフィールドを暗号化するために使用されるセキュリティ ブロックを Authentication Manager で復号できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting system security block (15130) (システム セキュリティ ブロックの復号でエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Error decrypting primary user SB (2333) (プライマリでユーザ SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。プライマリでユーザ レコードのセキュリティ ブロックを復号できないため、エージェント ホスト レコードの変更をレプリカに反映できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error decrypting replica user SB (2332) (レプリカでユーザ SB の復号中にエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。レプリカでトークン レコードのセキュリティ ブロックを復号できないため、エージェント ホスト レコードの変更をレプリカに送信できませんでした。RSA セキュリティ正規販売代理店にご連絡ください。

Error deleting delta *NAME* (*NAME* のデルタの削除でエラーが発生しました) (個別のメッセージについては、430 ページを参照してください)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error deleting delta task item (2270) (タスク アイテムのデルタの削除でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error deleting delta tasklist (2258) (タスクリストのデルタの削除でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error Deleting *NAME* (*NAME* の削除でエラーが発生しました) (個別のメッセージについては、431 ページを参照してください)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Deleting Record %1 (15139) (レコードの削除でエラーが発生しました)

レプリカがレコードの削除要求に応答しようとしたときに、エラーが発生しました。ログに記録されている他のメッセージを確認してください。新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Error exporting token by user (7521) (ユーザによるトークンのエクスポートでエラーが発生しました)

データベースに競合するデータが登録されている可能性があります。RSA Authentication Manager Host Mode (UNIX では **sdadmin**) をいったん停止した後、再起動し、トークンをもう一度エクスポートしてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error exporting token by user (7521) (ユーザによるトークンのエクスポートでエラーが発生しました)

データベースに競合するデータが登録されている可能性があります。RSA Authentication Manager Host Mode (UNIX では **sdadmin**) をいったん停止した後、再起動し、トークンをもう一度エクスポートしてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error fetching system to get SB Keys (15128) (SB キー取得のためにシステムをフェッチしているときにエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Error handling heartbeat (2072) (ハートビートの処理でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error loading security block keys (2073) (セキュリティ ブロック キーのロードでエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。データベース暗号鍵のロードでエラーが発生すると、このメッセージが表示されます。RSA セキュリティ正規販売代理店にご連絡ください。

Error Modifying Record (15138) (レコードの変更でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error modifying record on replica (2074) (レプリカでレコードを変更するときにエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error non HB received in vASDProcessHBs! (エラー : vASDProcessHBs で HB 以外を受信しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error occurred while parsing line *line number* of the runtime parameters file. Do you want to ignore error and continue parsing? (実行時パラメータ ファイルの行 *line number* の解析でエラーが発生しました。エラーを無視して解析を続行しますか)

runtime.txt ファイルで問題が検出されました。通常、ファイルが壊れていることが問題の原因です。操作を続行することができます。クエリの実行でさらに問題が発生した場合は、クエリを編集して再コンパイルしてください。

Error on start of sdlog broker (15036) (sdlog のブローカの起動でエラーが発生しました)

sdlog データベースのブローカの起動でエラーが発生しました。イベント ログの他のメッセージを確認してください。

sdlog データベースへの接続が切断されています。RSA Authentication Manager サービスがログ メッセージを書き込むことができないため、サービスが終了しました。

Error on start of sdserv broker (15035) (sdserv のブローカの起動でエラーが発生しました)

sdserv データベースのブローカの起動でエラーが発生しました。イベント ログの他のメッセージを確認してください。

sdserv データベースへの接続が切断されています。RSA Authentication Manager サービスがログ メッセージを書き込むことができないため、サービスが終了しました。

Error opening license.rec file (2308) (license.rec ファイルを開くときにエラーが発生しました)

Authentication Manager の起動時に、***ACEDATA*** ディレクトリに **license.rec** ファイルが必要です。**license.rec** ファイルが存在しないか、壊れています。RSA セキュリティ正規販売代理店にご連絡ください。

Error opening rep pack file (2296) (レプリカ パッケージ ファイルを開くときにエラーが発生しました)

レプリカ パッケージがプライマリの期待される場所に存在しないか、レプリカがプライマリから受信したレプリカ パッケージ ファイルに書き込むことができませんでした。プライマリがレプリカ パッケージを見つけることができない場合は、Windows では **ACEREP**、UNIX では **REP_ACE** として指定されているディレクトリにレプリカ パッケージを作成してください。レプリカがプライマリから受信したパケットに書き込むことができない場合は、システム パラメータでデータベース プッシュ (Push DB Assisted Recovery) 機能を無効にし、レプリカの ***ACEDATA*** ディレクトリにレプリカ パッケージを手動でコピーしてください。

Error opening system to get SB Keys (15127) (SB キー取得のためにシステムを開始しているときにエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。詳細については、RSA セキュリティ正規販売代理店にお問い合わせください。

Error operating with folder browser (フォルダ ブラウザの操作でエラーが発生しました)

Query Wizard の [Add]、[Acquire]、および [Share] ダイアログ ボックスでは、共通のフォルダ ブラウザ (参照) が使用されます。Query Wizard がフォルダ ブラウザ (参照) の操作を続行できませんでした。この操作の実行中に、管理者または他の人がオペレーティング システム内のファイルまたはフォルダの名前を変更すると、このエラーが発生することがあります。また、ハードウェアや OS に重大な問題が発生している可能性もあります。

Error past end of buff in errCopyBuffStrToStr (errCopyBuffStrToStr でバッファの最後を越えるエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Error past end of string in errCopyStrToBuffStr (errCopyStrToBuffStr で文字列の最後を越えるエラーが発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Error processing modified Agent Host records on Replica (15260) (変更されたエージェント ホスト レコードをレプリカで処理中にエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Processing Modified Log Entries On Replica (15269) (変更されたログ エントリをレプリカで処理中にエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Processing Modified OneTimePassword Records On Replica %1 (15258) (変更されたワンタイム パスワード レコードをレプリカで処理中にエラーが発生しました)

このメッセージは、レプリケーションでエラーが発生したことを示します。このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Error Processing Modified System Records On Replica (15266) (変更されたシステム レコードをレプリカで処理中にエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Processing Modified Token Records On Replica (15256) (変更されたトークン レコードをレプリカで処理中にエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Processing Modified User Records On Replica %1 (15255) (変更されたユーザ レコードをレプリカで処理中にエラーが発生しました)

このメッセージは、レプリケーションでエラーが発生したことを示します。このメッセージが繰り返し記録される場合は、レプリカを再起動してください。再起動した後もメッセージが表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Error Processing New Log Entries On Replica (15271) (新しいログ エントリをレプリカで処理中にエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error propagating license rec (2307) (license rec の送信でエラーが発生しました)

プライマリが **license rec** ファイルをレプリカに送信できませんでした。レプリカを再起動してください。このメッセージが引き続き表示される場合は、プライマリを再起動してください。プライマリを再起動しても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error Reading Heartbeat Response (ハートビート応答の読み取りでエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Reading Heartbeat Response (15198) (ハートビート応答の読み取りでエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Reading Packet (15132) (パケットの読み取りでエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error reading rep pack file (2297) (レプリカ パッケージ ファイルの読み取りでエラーが発生しました)

プライマリはレプリカ パッケージを見つけましたが、読み取ることができませんでした。レプリカ パッケージが壊れているか、レプリカ パッケージが適切な場所に存在しないため、プライマリがレプリカ パッケージを開くことができませんでした。レプリカは自動的にシャットダウンされます。プライマリで新しいレプリカ パッケージを作成し、レプリカを再起動してください。

Error Receiving Heartbeat (15136) (ハートビートの受信でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error: replica clock can't be set (2086) (エラー：レプリカのクロックを設定できませんでした)

レプリカのクロックとプライマリのクロックの同期がとれている (シンクロナイズしている) ことを確認してください。レプリカの時刻は、プライマリの時刻の 30 秒以内に設定する必要があります。UNIX では、RSA Authentication Manager が root 以外のユーザによって起動されると、このエラーが発生します。その場合は、root としてログオンし、Authentication Manager を再起動してください。

Error Responding To Agent Host Request (エージェント ホスト要求への応答でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error responding to Agent request %1 (15147) (エージェントの要求への応答でエラーが発生しました)

レプリカがエージェント ホスト レコードの変更要求に応答しようとしたときに、エラーが発生しました。ログに記録されている他のメッセージを確認してください。新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Error Responding to Commit Request Record (15140) (コミット要求レコードへの応答でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Responding To Log Entry Request (15142) (ログ エントリ要求への応答でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Responding To OneTimePassword Request %1 (15146) (ワンタイム パスワード要求への応答でエラーが発生しました)

レプリカがワンタイム パスワード レコードの変更要求に応答しようとしたときに、エラーが発生しました。ログに記録されている他のメッセージを確認してください。新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Error Responding To Push Query %1 (15141) (プッシュ クエリへの応答でエラーが発生しました)

プライマリがデータベースをレプリカにプッシュできませんでした。レプリカを再起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

Error responding to push request (2075) (プッシュ要求への応答でエラーが発生しました)

プライマリがデータベースをレプリカにプッシュできませんでした。レプリカを再起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

Error Responding To Reconcile Done Msg (15148) (調整終了メッセージへの応答でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Responding To System Request (15145) (システム レコード要求への応答でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Responding To Token Request (15144) (トークン レコード要求への応答でエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Responding To User Request %1 (15143) (ユーザ レコード要求への応答でエラーが発生しました)

レプリカがユーザ レコードの変更要求に応答しようとしたときに、エラーが発生しました。ログに記録されている他のメッセージを確認してください。新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。

Error saving query (クエリの保存でエラーが発生しました)

クエリを保存するときに問題が発生しました。ファイル システムに問題がある可能性があります。このエラーが発生した場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error selecting packet (2079) (パケットの選択でエラーが発生しました)

レプリカが誤ったサービス ポート番号でプライマリからのパケットを受信している可能性があります。レプリカ管理ユーティリティを使用して、ポート番号と名前を確認してください。

Error searching database (2078) (データベースの検索でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error sending heartbeat (2080) (ハートビートの送信でエラーが発生しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error sending replica agent hosts (2081) (レプリカでエージェント ホストの送信中にエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error sending replica log entries (2082) (レプリカでログ エントリの送信中にエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error sending replica OTPs (2191) (レプリカで OTP の送信中にエラーが発生しました)

レプリケーション パスで、1 つ以上の使用済みワンタイム ユーザ パスワード (OTP) をレプリカからプライマリに送信できませんでした。このメッセージが引き続き表示される場合は、レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。新しいレプリカ パッケージを適用しても問題を解決できない場合は、RSA セキュリティ正規販売代理店へご連絡ください。

Error sending replica system (2083) (レプリカでシステム レコードの送信中にエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error sending replica tokens (2084) (レプリカでトークン レコードの送信中にエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error sending replica users (2278) (レプリカでユーザ レコードの送信中にエラーが発生しました)

ユーザ レコードの要求に応答しているときにエラーが発生しました。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error Setting Replica Clock (2085) (レプリカのクロックの設定でエラーが発生しました)

レプリケーション パスで復号 (セキュリティ ブロックからの読み取りまたはセキュリティ ブロックへの書き込み) に失敗すると、このエラー メッセージが表示されます。**syncsrvc** でレプリカのクロックを設定しようとしたときに、通信エラーが発生しました。

Error Status *error number* (エラー ステータス *error number*)

Quick Admin にログオンしようとしたときに、Tomcat で問題が発生したか、または Tomcat サーバが RSA Authentication Manager Quick Admin デーモンと通信できない場合、これらのエラー メッセージが表示されます。これらのエラーを解決するには、次のことを確認してください。

- Web サーバが実行されているかどうかを確認します。
- Tomcat サーバが Web サーバで実行されているかどうかを確認します。

  Default サーバをテストするには、**http://*QuickAdmin host*/servlets-examples** にアクセスして、サンプル サーブレットを実行します。
- プライマリ RSA Authentication Manager で RSA Authentication Manager の Quick Admin Daemon サービスが実行されていることを確認します。

- RSA Authentication Manager とデータベース ブローカが起動されていることを確認します。

また、Tomcat イベント ログ ファイルも確認してください (Web サーバ ホストの ***Quick Admin installation directory*¥Tomcat¥logs** サブディレクトリにあります)。Windows ホストの場合、ログ ファイル名は **stdout_*date*.log** です。Solaris の場合、ログ ファイル名は **catalina.out** です。

エラー メッセージを表示するだけで、再作成しない場合は、**quickadmin¥WEB-INF¥properties¥errormsg.properties** ファイルを開いてください。

Error swapping comm params (2088) (通信パラメータのスワップでエラーが発生しました)

新しいレプリカ パッケージを作成し、手動で適用してください。

Error swapping comm params 2 (2087) (通信パラメータ 2 のスワップでエラーが発生しました)

新しいレプリカ パッケージを作成し、手動で適用してください。

Error Swapping Communication Parameters (15135) (通信パラメータのスワップでエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error Swapping Encryption Keys (15133) (暗号鍵のスワップでエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Error swapping encryption keys (2089) (暗号鍵のスワップでエラーが発生しました)

暗号鍵に問題があるため、プライマリとレプリカが通信できません。ファイル **server.cer**、**server.key**、**sdti.cer** がプライマリの ***ACEDATA*** ディレクトリにあるかどうかを確認してください。これらのファイルが存在する場合は、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error Swapping Protocol Versions (15134) (プロトコル バージョンのスワップでエラーが発生しました)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Error synching comm params (2090) (通信パラメータのシンクロナイズでエラーが発生しました)

新しいレプリカ パッケージを作成し、手動で適用してください。

Error Transferring *NAME* (*NAME* の転送でエラーが発生しました)

レプリケーション パスでエラーが発生しました。*NAME* は、エラーが発生したときに転送されていたデータベース フィールドを示します。個別のメッセージについては、433 ページを参照してください。

Error: unexpected packet received (2077) (エラー：予測していないパケットを受信しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error updating agent host record (2116) (エージェント ホスト レコードの更新でエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error updating system record (2117) (システム レコードの更新でエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error updating token (2119) (トークン レコードの更新でエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error updating token delta (2118) (トークンのデルタの更新でエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error updating user (2279) (ユーザ レコードの更新でエラーが発生しました)

レプリケーション パスで、プライマリがユーザ レコードの変更情報をレプリカに送信しましたが、レプリカでデータベースを更新できませんでした。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error updating user delta (2281) (ユーザのデルタの更新でエラーが発生しました)

このメッセージはレプリケーションに問題があることを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Error waiting for response (2120) (応答を待機しているときにエラーが発生しました)

レプリケーション管理ユーティリティで設定されているレプリカの情報 (ホスト名、IP アドレス) が、DNS サーバまたはシステムの **hosts** ファイルに登録されている情報と同じであるかどうかを確認してください。IT 部門に連絡して、ネットワークの問題に対処しなければならない可能性があります。

Error While Traversing Database (データベースのトラバースでエラーが発生しました)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291ページの「ネットワーク接続が切断されたか、またはAuthentication Manager がダウンしている可能性がある場合」を参照してください。

Evading Trial and Error Attack (135) (Trial and Error Attack (試行錯誤攻撃) を回避しています)

RSA Authentication Manager 認証プロセスで一連のログイン試行の失敗が検出されたため、攻撃を回避するために認証ダイアログの速度が低下されました。

Expired lost status cleared (1703) (有効期限の切れた紛失ステータスが消去されました)

有効期限の切れた紛失ステータスのトークンを使用してユーザが認証を受けようとしたため、RSA Authentication Manager は、トークンの有効期限の切れた紛失ステータスを消去し、そのトークンに割り当てられていた固定パスワードを削除しました。

Expressions other than those containing COUNT, MAX or MIN functions are not supported in the list of output fields (COUNT、MAX、MIN 以外の関数を含む式は、出力フィールドの一覧でサポートされません)

SELECT ステートメントの列名で使用できる関数は、COUNT、MAX、および MIN だけです。その他の式 (たとえば BEGINS、MATCHES、HAVING など) は、SELECT ステートメントで出力を修飾する部分 (たとえば WHERE 句の後やテーブル結合の内部) でのみ使用できます。

External Authorization Initialization error, *errstring* (External Authorization 初期化エラー、*errstring*)

このメッセージは、RSA Authentication Manager で External Authorization をアクティブ化したときに表示されます。**iSDExtAuthorInit()** ルーチン用にこのメッセージを作成したプログラマから、このメッセージに割り当てられている戻り値を説明した一覧が提供されています。詳細については、このリストを参照してください。**iSDExtAuthorInit()** ルーチンは、External Authorization 初期化タスクを実行します。

External Authorization Shutdown error, *errstring* (External Authorization シャットダウン エラー、*errstring*)

このメッセージは、RSA Authentication Manager で External Authorization をアクティブ化したときに表示されます。**iSDExtAuthorShutdown()** ルーチン用にこのメッセージを作成したプログラマから、このメッセージに割り当てられている戻り値を説明した一覧が提供されています。詳細については、このリストを参照してください。**iSDExtAuthorShutdown()** ルーチンは External Authorization をシャットダウンします。

Failed inserting realm record (%1) (15079) (レルム レコードを追加できませんでした)

RSA Authentication Manager がレルム レコードをデータベーベースに追加できませんでした。ローカル レルムでリモート レルム レコードを削除し、リモート レルムでローカル レルム レコードを削除した後、レルム間の関係を再確立してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed signal setup, Daemon Stopping (%1) (16203) (シグナルの設定に失敗しました。デーモンは停止します)

RSA Authentication Manager プロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**、および **sdadmind**、**acesrvc**、**acesrvc_be**、**logmainthd**) が異常終了すると、このメッセージが表示されます。メッセージに示されているエラーを確認してください。RSA Authentication Manager ソフトウェアに関連しない問題の場合は、適切な処置をとり、問題が解決されたら RSA Authentication Manager を再起動してください。RSA Authentication Manager ソフトウェアに関連する問題の場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to allocate memory (%1) (15009) (メモリを割り当てることができませんでした)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to clear the PIN for token serial number 000000*nnnnnn*. The token replacement process will stop (トークン シリアル番号 000000*nnnnnn* の PIN を消去できませんでした。トークン交換プロセスは停止します)

トークン レコードが壊れている可能性があります。トークン レコードをデータベースから削除した後、別のトークンを割り当ててください。

Failed to close system table cursor (%1) (15020) (システム テーブル カーソルを閉じることができませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to connect to the [RSA ACE/Server *IP Address*] with port = 5570. Wrong ACE/Server port number or ACE Web Admin service is down. Error code: 109 (ポート 5570 で [RSA ACE/Server *IP Address*] に接続できませんでした。RSA ACE/Server ポート番号が正しくないか、または RSA ACE Web Admin サービスがダウンしています。エラー コード : 109)

RSA Authentication Manager 上の ***ACEPROG¥*hosts.conf** ファイルに不正なシステム名または IP アドレスが定義されています。**hosts.conf** ファイルに Quick Admin の Web サーバ システム名のスペルが正しく指定され、ホスト名 (たとえば **cassatt**) と完全修飾 DNS 名 (たとえば **cassatt.rsasecurity.com**) の両方が入力されていることを確認し、必要に応じて編集してください。また、IP アドレスが正しいかどうかも確認します。

Failed to connect to the card reader (カード リーダに接続できませんでした)

カード リーダがコンピュータに正しく接続されていないか、またはカード リーダが正常に動作していません。カード リーダがコンピュータに正しく接続されているかどうかを確認してください。必要に応じて、カード リーダを交換してください。

Failed to create socket (%1) (15008) (ソケットを作成できませんでした)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to daemonize process (%1) (15016) (プロセスのデーモンを起動できませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to fetch system record (%1) (15019) (システム レコードをフェッチできませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed To fully Send Database to Replica %1 (15191) (データベースをレプリカに完全に送信できませんでした)

プライマリがデータベースをレプリカにプッシュできませんでした。レプリカを再起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

Failed to get the PIN for token serial number 000000*nnnnnn* (トークン シリアル番号 000000*nnnnnn* の PIN を取得できませんでした)

このシリアル番号のトークン レコードが壊れています。別のトークンを割り当ててください。

Failed to load the seed in file filename. This file is bound to a different device. Please contact your RSA SecurID administrator. (filename で示されるファイルにシードをロードできませんでした。このファイルは別のデバイスにバインドされています。RSA SecurID 管理者に連絡してください)

管理者がソフトウェア トークンを発行した場合、ユーザはトークン ファイルを PC または他のデバイスにインストールできます。ユーザがソフトウェア トークンをインストールしたデバイスが、トークンに関連付けられているデバイスと異なる場合には、このメッセージがユーザに表示されます。

トークン レコードの拡張フィールド **DeviceSerialNumber** に定義されているシリアル番号と、ユーザがトークン ファイルをインストールしているデバイスのシリアル番号とが一致しているかどうかを確認してください。ユーザに対して、トークン ファイルを正しいデバイスにインストールするように指示してください。ユーザがトークンを別のデバイスにインストールしなければならない場合は、トークンを再発行し、トークン レコードの拡張フィールドに新しいデバイスのシリアル番号を定義してください。ソフトウェア トークンの再発行の詳細については、ヘルプの「Reissue Software Token」を参照してください。

Failed to Lock *recordtype* Record (*recordtype* レコードをロックできませんでした)

承認されたユーザがアクセスを拒否され、このメッセージがその拒否イベントに対するログ メッセージとして記録されている場合は、ユーザの認証に必要なレコードが他の操作で使用されていたと考えられます。レコード タイプ (***recordtype***) は、エージェント ホスト レコード、システム レコード、トークン レコードのいずれかです。認証できない状況は一時的なもので、レコードを使用している他の操作が完了すると、認証は可能になります。

また、**syncsrvc** でレコードを排他的にロックしようとしたものの、ロックできなかった場合も、このメッセージがログに記録されることがあります。

このエラーは、カスタム アドミニストレーション プログラムがレプリカ データベースにアクセスしている場合にも発生します。カスタム アドミニストレーション プログラムはプライマリのデータベースのみで使用してください。レプリカ データベースへの直接アクセスはサポートされないため、データベースが壊れる可能性があります。個別のメッセージについては、434 ページを参照してください。

Failed to open system table cursor (%1) (15018) (システム テーブル カーソルを開くことができませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to read license (15010) (ライセンスを読み取ることができませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Failed to read system record (1158) (システム レコードを読み取ることができませんでした)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to retrieve the config record (15077) (構成レコードを取得できませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Failed to set socket options (%1). (15017) (ソケット オプションを設定できませんでした)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to start offline authentication Download Manager (20006) (オフライン認証 Download Manager を起動できませんでした)

sdoad サービスのコンポーネントを起動できませんでした。このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to start offline authentication Ticket Manager (20005) (オフライン認証 Ticket Manager を起動できませんでした)

sdoad サービスのコンポーネントを起動できませんでした。このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Failed to Stop Brokers %1 (15178) (ブローカを停止できませんでした)

レプリカをいったん停止し、起動してください。

Failed to Stop Replica %1 (15175) (レプリカを停止できませんでした)

レプリカをいったん停止し、起動してください。

Failed updating realm record (%1). (15080) (レルム レコードを更新できませんでした)

RSA Authentication Manager がデータベースのレルム レコードを更新できませんでした。ローカル レルムでリモート レルム レコードを削除し、リモート レルムでローカル レルム レコードを削除した後、レルム間の関係を再確立してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Fatal error execing acesyncd (%1) (15012) (acesyncd の実行で致命的なエラーが発生しました)

レプリケーション プロセス (**acesyncd**) を起動できませんでした。オペレーティング システムまたはネットワーク リソースで個別のメッセージを確認してください。

Fatal Error: %1 (15109) (致命的なエラー)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Fewer BEs (%1) (16221) (BE プロセスのいずれかが動作していません)

認証サービスに問題があります。RSA Authentication Manager では、通常の操作の一部として、システムの各プロセッサに対して 2 つのバックエンド (BE) 認証プロセス (**acesrvc_be**) が生成されます。何らかの理由で、プロセスの 1 つが動作していません。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

General error in broker server. %1 (15037) (ブローカ サーバで一般エラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

General error in RSA ACE/Server acesrvc service %1 (15046) (RSA ACE/Server acesrvc サービスで一般エラーが発生しました)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

General error in RSA ACE/Server syncsrvc service %1 (15827) (RSA ACE/Server syncsrvc サービスで一般エラーが発生しました)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Get Agent host failed (%1) (15052) (エージェント ホスト レコードを取得できませんでした)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Get enabled user failed (%1) (15067) (有効化されているユーザを取得できませんでした)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Get node by name failed (%1) (15053) (名前によってノードを取得できませんでした)

エージェント ホストを検索しているときに、エラーが発生しました。メッセージが引き続き表示される場合は、データベースに登録されているレプリカの情報 (ホスト名、IP アドレス) が、DNS サーバまたはシステムの **hosts** ファイルに登録されている情報と同じであるかどうか確認してください。

Get node by net addr failed (%1) (15051) (ネットワーク アドレスによってノードを取得できませんでした)

レプリケーション管理ユーティリティで設定されているレプリカの情報 (ホスト名、IP アドレス) が、DNS サーバまたはシステムの **hosts** ファイルに登録されている情報と同じであるかどうかを確認してください。IT 部門に連絡して、ネットワークの問題に対処しなければならない可能性があります。

Good Tokencode/Bad PIN Detected (1010) (正しいトークンコード / 不正な PIN が検出されました)

RSA Authentication Manager に送信された PASSCODE で、トークンコードは正しいのですが、PIN が不正でした。このメッセージは、不正なユーザが承認されているユーザのトークンを入手して、正しい PIN を推測している可能性があることを示します。トークンコードと PIN を別々に入力する必要のあるトークン (RSA SecurID スタンダード カードとキーホルダ) は、認証要求で正しいトークンコードと不正な PIN の組み合わせが3回連続して入力されると、無効になります(3回という回数は変更できません)。

Group and Site administrators do not have permission to delete queries that are not acquired (グループ管理者とサイト管理者には、入手していないクエリを削除する権限がありません)

グループ管理者またはサイト管理者がカスタム クエリ フォルダからクエリを削除しようとしています。しかし、そのクエリを個人的に入手したわけではないので、クエリを削除する権限がありません。

Group and Site administrators do not have permission to rename queries that are not acquired (グループ管理者とサイト管理者には、入手していないクエリの名前を変更する権限がありません)

グループ管理者またはサイト管理者がカスタム クエリ フォルダ内のクエリの名前を変更しようとしています。しかし、そのクエリを個人的に入手したわけではないので、クエリの名前を変更する権限がありません。

grp-mem db close error (%1) (15071) (グループ メンバのデータベースを閉じるときにエラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

grp-mem db fetch error (%1) (15072) (グループ メンバのデータベースをフェッチするときにエラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

grp-mem db open error (%1) (15068) (グループ メンバのデータベースを開くときにエラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

If you go back, you will lose changes to this screen. Do you want to continue? (元に戻ると、この画面で行った変更は失われます。操作を続行しますか) (このメッセージは再表示されません)

Query Wizard のダイアログ ボックスのいずれかで [Back] をクリックするたびに、現在のダイアログ ボックスで行った変更 (たとえば引数の定義) は失われます。

Incorrect order of the sections in the definition file (定義ファイル内のセクションの順序が正しくありません)

definition.txt が壊れている場合や、このファイルを手動で変更した場合 (この操作は推奨できません) は、このメッセージが表示されます。

Insert Realm Bad Tokencode (8229) (レルムの追加でトークンコードが不正でした)

レルム シークレットの設定時に、管理者が不正なトークンコードを入力しました。ネットワーク関連の遅延が発生したことが原因で、トークンコードが変化するまでにレルム シークレット メッセージがリモート管理者のレルムに到達しなかった場合には、このメッセージがログに記録される可能性があります。また、トークン クロックとシステム クロックの同期がとれていない場合や (128 ページの「トークンの同期のとり直し」を参照)、レルム シークレットを開始した管理者が間違ったトークンコードを入力した場合も、このメッセージが記録されます。

Insert Realm Failed (8230) (レルムの追加に失敗しました)

RSA Authentication Manager がターゲット レルムとの間でレルム シークレットを設定できませんでした。このため、ローカル レルムがリモート レルム データベースに追加されていない可能性があります。このエラーが発生する可能性があるのは、2 つのレルム間のネットワーク接続が切断された場合、トークン クロックとシステム クロックの同期がとれていない場合、レルム シークレットを開始した管理者が不正なトークンコードを入力した場合のいずれかです。エラーの詳細については、リモート レルムのログ メッセージ データベースを確認してください。レルム シークレットを設定する管理者は、リモート管理者から新しいトークンコードを取得して、操作を再実行する必要があります。

Insert Realm Not Allowed (8225) (レルムの追加は許可されていません)

レプリカがリモート レルムで実行中に、管理者がレルム シークレット トランザクションを設定しようとしました。レルム シークレットは、プライマリ サーバ (旧バージョンのレルムではマスタ サーバ) を優先サーバとして使用して最初に設定する必要があります。レルム シークレットが設定された後、優先サーバとフェールオーバ サーバを変更または更新することができます。

Insert Realm Not Authorized (8228) (レルムの追加は承認されていません)

レルム シークレットの設定時に、管理者が承認されていないユーザに割り当てられているトークンコードを入力しました。レルム シークレット トランザクションを暗号化するには、レルム管理者のトークンコードを使用する必要があります。

Insert Realm Succeeded (8201) (レルムの追加に成功しました)

RSA Authentication Manager はデータベースに新しいレルムを追加しました。

Insert Realm Token Not Found (8227) (レルムの追加でトークンが見つかりませんでした)

レルム シークレットの設定時に、管理者が不正なトークン シリアル番号を入力しました。レルム シークレットを設定する管理者は、リモート管理者に連絡して、正しいシリアル番号とトークンコードを取得する必要があります。

Insert Realm Tokencode Repeated (8226) (レルムの追加でトークンコードが繰り返し使用されました)

レルム シークレットの設定時に、管理者がすでに使用されているトークンコードを入力しました。他の目的 (たとえばログオン、レルムの設定、トークンの同期のとり直し) で使用されたトークンコードをレルム シークレットの設定に使用することはできません。どのような状況でも、PASSCODE やトークンコードの再利用は禁止されています。

Internal error generating argument file (引数ファイルの生成で内部エラーが発生しました)

クエリ コンパイラで内部エラーが検出されました。このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Internal Error. Report to RSA Security Inc. (内部エラー、RSA セキュリティ正規販売代理店にご連絡ください)

クエリの作成またはコンパイル処理で内部エラーが検出されました。このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Invalid condition (条件指定に誤りがあります)

SQL 条件コード (IF、THEN、ELSEIF、ELSE) に構文エラーがあります。反転表示されている文字列に誤りがあります。SQL 条件コードを確認し、エラーを修正してください。

Invalid default. For DATE enter date in MM/DD/YYYY format (デフォルトに誤りがあります。DATE に対しては、MM/DD/YYYY の形式で日付を入力してください)

[Query Wizard (Argument Details)] ダイアログ ボックスの DATE 引数に構文エラーがあります。日付は MM/DD/YYYY の形式で入力してください。

Invalid default. For LOGICAL enter TRUE or FALSE (デフォルトに誤りがあります。LOGICAL に対しては、TRUE または FALSE を入力してください)

[Query Wizard (Argument Details)] ダイアログ ボックスの LOGICAL 引数に構文エラーがあります。この引数には TRUE または FALSE を入力する必要があります。

Invalid default. For NUMBER enter digits only; maximum is 9 digits (デフォルトに誤りがあります。NUMBER に対しては、9 桁以内の数字のみを入力してください)

[Query Wizard (Argument Details)] ダイアログ ボックスの NUMBER 引数に構文エラーがあります。1 ～ 9 桁の数字を入力してください。

Invalid default. For STRING enter valid characters only. See help for details (デフォルトに誤りがあります。STRING に対しては、有効な文字だけを入力してください。詳細についてはヘルプを参照してください)

[Query Wizard (Argument Details)] ダイアログ ボックスの STRING 引数に構文エラーがあります。以下の文字を除き、有効な ASCII 文字を入力できます。

{} ~ " ; ' [ ] , / @ < > ^ |

Invalid message statement (メッセージ ステートメントに誤りがあります)

SQL コードの MESSAGE ステートメントに構文エラーがあります。反転表示されている文字列に誤りがあります。MESSAGE ステートメントを確認し、エラーを修正してください。

Invalid query name or query with such name already exists (クエリ名が不正であるか、またはすでに存在する名前です)

Query Wizard でクエリに名前を付けるときに、すでに使用されているクエリ名を入力したか、または以下の不正な文字を 1 文字以上入力しました。

¥ / : * ? " < > |

Invalid range of the Back End ports. (15014) (バックエンド ポートの範囲が誤っています)

Authentication Manager を再起動します。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Invalid SELECT statement (SELECT ステートメントに誤りがあります)

SELECT ステートメントに構文エラーがあります。反転表示されている文字列に誤りがあります。SELECT ステートメントを確認し、エラーを修正してください。このメッセージは、テーブル名のスペルが誤っている場合や、不正な名前を入力したときに表示されます。

Invalid SELECT statement has been specified in the query definition (誤った SELECT ステートメントがクエリ定義に指定されています)

このエラーが発生するのは、クエリの **definition.txt** ファイルを手動で編集した場合だけです。このような操作は推奨できません。

Invalid symbols in the command line (コマンド ラインに誤ったシンボルが指定されています)

Query Wizard で、Launch External Application コマンド ライン フィールドに誤ったシンボルを入力しました。フィールドの入力に誤りがないか確認し、必要に応じて修正してください。

Invalid symbols in the field. See the Help for details (フィールドに誤ったシンボルを入力しました。詳細については、ヘルプを参照してください)

Query Wizard で、テキスト フィールドのいずれか (メッセージに示されているフィールド) に以下の不正な文字を 1 文字以上入力しました。

{} ~ " ; ' [ ] , / @ < > ^ |

Iteration count out of range (1157)(繰り返し回数が正しい範囲でありません)

RADIUS クライアントが RSA EAP Protected OTP クレデンシャルを作成するために使用した繰り返し回数が正しい範囲でありません。クレデンシャルの設定は、RSA Authentication Manager または RADIUS クライアントで編集できます。RSA Authentication Manager での RSA EAP Protected OTP の設定については、ヘルプを参照してください。RADIUS クライアントでクレデンシャルの設定を変更する方法については、クライアント ソフトウェアのマニュアルを参照してください。

License active user limit being approached (アクティブ ユーザの数がライセンスの制限に近づいています)

ライセンスの制限を超えると、**違反**モードになります。

次の場合には、違反モードになります。

- RSA Authentication Manager を新規インストールし、ライセンスの制限を超えた場合。
- これまでライセンスがアップグレード違反モードであり、ここで違反モードになった場合。

ライセンスが違反モードになると、新たに追加ユーザをアクティブ化することができません。

ライセンスの制限を超えた後、システムを準拠モードに戻すには、RSA セキュリティ正規販売代理店から適切な新しいライセンスを入手する必要があります。または、アクティブ ユーザの数がライセンスの制限内になるように、十分な数のユーザを非アクティブ化して、システムを準拠モードに戻してください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

License Copy Failed %1 (15158) (ライセンスをコピーできませんでした)

このメッセージが引き続き表示される場合は、プライマリとレプリカを再起動してください。この操作を行っても問題を解決できない場合は、レプリカを再インストールしてください。

License copy failed (2310) (ライセンスをコピーできませんでした)

プライマリが **license rec** ファイルをレプリカに送信できませんでした。レプリカを再起動してください。このメッセージが引き続き表示される場合は、プライマリを再起動してください。プライマリを再起動しても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

License Packet Send Failed %1 (15157) (ライセンス パケットを送信できませんでした)

このメッセージが引き続き表示される場合は、プライマリとレプリカを再起動してください。この操作を行っても問題を解決できない場合は、レプリカを再インストールしてください。

License packet send failed (2309) (ライセンス パケットを送信できませんでした)

プライマリが **license rec** ファイルをレプリカに送信できませんでした。レプリカを再起動してください。このメッセージが引き続き表示される場合は、プライマリを再起動してください。プライマリを再起動しても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Lock manager network error reading operation from: %1 Error: %2 Connection closed (15095) (読み取り操作でロック マネージャ ネットワーク エラーが発生しました。接続は切断されました)

このメッセージは、RSA Authentication Manager の起動時とシャットダウン時に表示されます。また、プライマリがデータベースをレプリカにプッシュするときも表示されます。他の場合にこのメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Lock manager network error sending operation to: *SERVER NAME* (15096) (*SERVER NAME* への送信操作でロック マネージャ ネットワーク エラーが発生しました)

レプリカのロック マネージャが別のレプリカへの接続を確立しようとしたときに、データベースへの特定の変更が第 2 のレプリカにまだレプリケートされていないために、第 2 のレプリカが接続への肯定応答を拒否した場合は、このメッセージが第 1 のレプリカのログに記録されます。

たとえば、A と B の 2 つのレプリカがあるとします。レプリカ A に対して新しいレプリカ パッケージを作成した直後に、プライマリがレプリカ A に新しいデータベースをプッシュしました。Push DB プロセスの一部として、レプリカ A はロック マネージャを再起動し、ロック マネージャはデータベースに登録されているすべてのレプリカとの間で接続を確立しようとします。プライマリがレプリカ B への次のレプリケーションを実行する前に、レプリカ A のロック マネージャがレプリカ B に接続しようとすると、レプリカ B はレプリカ A でデータベースに対して加えられた変更を認識していないので、接続を切断します。プライマリがレプリカ B に変更をレプリケートするまで、このメッセージが記録されます。

Lock manager server rejected client connection from: %1 (15097) (ロック マネージャ サーバがクライアント接続を拒否しました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Lost Token Authenticated (1080) (紛失したトークンによる認証)

ユーザが「Enter PASSCODE (PASSCODE を入力してください)」プロンプトで正しい PIN とテンポラリ パスワードを入力すると、このメッセージが記録されます。

Lost token status cleared (1702) (トークンの Lost ステータスが消去されました)

以前に紛失したトークン (Lost) としてマークされていたトークンと、そのトークンに割り当てられていた固定パスワードを使用して、ユーザが正しく認証を受けることができた場合、このメッセージが表示されます。RSA Authentication Manager はそのトークンを Not Lost ステータスとしてマークし、固定パスワードを削除します。

Missing ELSE condition (ELSE 条件が指定されていません)

クエリに条件ステートメントの IF 句が指定されていますが、ELSE 句を含むステートメントが指定されていません。

NAME Already Exists On Replica (*NAME* はレプリカにすでに存在します) (個別のメッセージについては、435 ページを参照してください)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Next Tokencode Accepted (1057) (ネクスト トークンコードが受け付けられました)

ログインが成功した後、ユーザがトークンを所有していることを確認するために、次に表示されるコードが要求されました。プロンプトの指示に従って、次に表示されるコードを正しく入力すると、このメッセージが記録されます。ネクスト トークンコード モードの詳細についてと、攻撃回避でのこのモードの使用については、125 ページの「PIN が盗まれたり、他人に知られた場合」を参照してください。

Next Tokencode On (144) (ネクスト トークンコード モードがオンです)

ログインの試行が連続して失敗すると、トークンはネクスト トークンコード モードに設定されます。このモードでは、2 つの連続する PASSCODE を正しく入力しないと、ユーザのアクセスが許可されません。前の「Next Tokencode Accepted (ネクスト トークンコードが受け付けられました)」の説明を参照してください。

Next Tokencode Requested (1002) (ネクスト トークンコードが要求されました)

ログインが成功した後、ユーザがトークンを所有していることを確認するために、次に表示されるコードが要求されました。「Next Tokencode Accepted (ネクスト トークンコードが受け付けられました)」の説明を参照してください。

次の 2 つの状況では、ユーザがアクセスを許可されなかった場合でも、「Next Tokencode Requested (ネクスト トークンコードが要求されました)」というメッセージがログに記録されます。

- Authentication Manager やネットワークの負荷が非常に高い場合、Authentication Manager は PASSCODE または新しい PIN を受け付け、メッセージをエージェント ホストに通知しようと試みますが、エージェント ホストはそのメッセージを受信する前にタイムアウトになります。したがって、エージェント ホストはユーザに対して「Access Denied (アクセスが拒否されました)」(または「PIN rejected (PIN が拒否されました)」) というメッセージを表示します。

  この状況が発生した場合は、認証が成功するまで、次のトークンコードが表示されるのを待ち、そのトークンコードを再入力するようにユーザに指示するか、または**エージェントのタイムアウト**値を大きくして、新しい **sdconf.rec** ファイルを作成し、各エージェント ホストに配布します。Windows で**エージェントのタイムアウト**値を大きくするには、Configuration Management アプリケーションを使用します。UNIX の場合は、**sdsetup -config** コマンドを使用します。

  sdconf.rec ファイルの配布の詳細については、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。

  メモ：ユーザが複数のトークンを持っている場合、Authentication Manager は一致するものが見つかるまで各トークンを順に確認するため、エージェントのタイムアウトによってアクセスが拒否される可能性が高くなります。

- エージェント ホストの **sdconf.rec** ファイル (または他の構成方法) に定義されている暗号方式と、エージェント ホスト レコードに指定されている暗号方式が一致しない場合。

  エージェント ホスト レコードに暗号方式が正しく設定されていない場合は、[Agent Host] メニューの [Edit Agent Host] をクリックして設定を変更します。**sdconf.rec** ファイルの暗号方式の設定に誤りがある場合は、第 12 章「RSA Authentication Manager の構成 (Windows)」を参照して、新しい構成ファイルをエージェント ホストにコピーしてください。

No Agent Host Access Times Enabled (エージェント ホストのアクセス可能時間外です)

ユーザはエージェント ホスト上で直接アクティブ化されていますが、アクセスを許可されている時間外にアクセスしようとしたため、認証を受けることができませんでした。

No Agent Host/Group Times Enabled (1084) (エージェント ホストまたはグループのアクセス可能時間外です)

ユーザはエージェント ホスト上で直接アクティブ化され、同時にグループを通じてもアクティブ化されていますが、どちらのアクティブ化でもアクセス時間の制限を受けていて、その時間外であるため、認証を受けることができませんでした。

No authentication service. No RSA ACE/Server Back Ends registered (16210) (認証サービスが動作していません。RSA ACE/Server バックエンドは登録されていません)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

No CONDITION section has been specified in the query definition (CONDITION セクションがクエリ定義に指定されていません)

definition.txt ファイルに必要なセクションがありません。クエリの **definition.txt** ファイルを手動で編集すると、このエラーが発生することがあります。このような操作は推奨できません。また、ファイルが壊れている可能性もあります。この問題に対処するには、クエリを編集して、再コンパイルしてください。

No Group Access Times Enabled (1086) (グループのアクセス可能時間外です)

ユーザはグループを通じてエージェント ホスト上でアクティブ化されていますが、アクセスを許可されている時間外にアクセスしようとしたため、認証を受けることができませんでした。

No group has been selected (グループが選択されていません)

[Query Wizard (Query Access Level)] ダイアログ ボックスで、アクセス レベルをグループ レベルに設定しましたが、グループを指定しませんでした。

No name has been specified for the query in the 'Copy as' line ([Copy as] 行にクエリの名前が指定されていません)

既存のクエリのコピーを作成しようとしていますが、コピーの名前を指定していません。

No name has been specified for the query in the 'Save as' line ([Save as] 行にクエリの名前が指定されていません)

[Acquire Shared Queries] ダイアログ ボックスで、クエリを入手していますが、クエリを保存するときの名前を入力していません。

No One-Time Passwords (1088) (ワンタイム パスワードがありません)

ユーザはワンタイム パスワードを使用して認証を受けようとしましたが、使用できるパスワードが残っていません。このメッセージは、手持ちのワンタイム パスワードが 1 セットだけであり、そのセットの有効期限が切れた場合に、「One-Time Password Set Expired (ワンタイム パスワード セットの有効期限が切れました)」メッセージとともに記録されます。

No query has been selected for acquisition (入手するクエリが選択されていません)

[Acquire Shared Queries] ダイアログ ボックスで、[OK] をクリックする前に、入手するクエリを選択する必要があります。

No Realm Secret Established (8219) (レルム シークレットが設定されていません)

認証を要求しているレルムとローカル Authentication Manager との間で、レルム シークレットが設定されていません。レルム シークレットを設定するには、[Edit Realm] ダイアログ ボックスの [Establish Realm Secret] をクリックします。

No Response From Remote Realm (リモート レルムから応答がありません)

認証要求を受信したレルムが応答しなかったために、ローカル エージェント ホストでタイムアウトが発生しました。リモート レルム Authentication Manager が動作していないか、またはネットワーク接続が切断されている可能性があります。この問題が何度も発生する場合は、**エージェントのタイムアウト**値を大きくすることを検討してください。手順については、367 ページの「PASSCODE Accepted (1011) (PASSCODE が受け付けられました)」を参照してください。

No SELECT section has been specified in the query definition (SELECT セクションがクエリ定義に指定されていません)

definition.txt ファイルに必要なセクションがありません。クエリの **definition.txt** ファイルを手動で編集すると、このエラーが発生することがあります。このような操作は推奨できません。また、ファイルが壊れている可能性もあります。この問題に対処するには、クエリを編集して、再コンパイルしてください。

No site has been selected (サイトが選択されていません)

[Query Wizard (Query Access Level)] ダイアログ ボックスで、アクセス レベルをサイト レベルに設定しましたが、実際のサイトを指定しませんでした。

Node Secret Sent to Agent Host (1045) (ノード シークレットがエージェント ホストに送信されました)

自動配布 (Automatic Delivery) 機能を使用している場合、Authentication Manager がエージェント ホストから認証成功の通知を初めて受信すると、このメッセージがログに記録されます。ノード シークレットの配布方法の詳細については、222 ページの「ノード シークレット ファイル」を参照してください。

ノード シークレットが一致しない場合や、設定されていない場合は、エージェント ホストと Authentication Manager との間の通信を確立できません。ノード シークレットに問題がある場合には、「Node Verification Failed (ノードの検証に失敗しました)」エラーがログに記録されます。詳細については、295 ページの「ACCESS DENIED, Bad Lost Token PSW (1083) (アクセス拒否、紛失したトークンのパスワードが不正です)」を参照してください。

Node verification failed (137) (ノードの検証に失敗しました)

通信パケットを復号できない場合、このメッセージがログに記録されます。エージェント ホストと Authentication Manager の間で送信されるパケットは、エージェント ホストの IP アドレスとノード シークレットを含む鍵で暗号化されます。ノード シークレットは、エージェント ホストと Authentication Manager だけが知っているランダムな文字列です。

エージェント ホストをいったん削除して再作成したり、ノード シークレット ファイルを削除すると、Authentication Manager に記録されているノード シークレットとエージェント ホストに記録されているノード シークレットの間に不一致が生じるため、この問題が発生します。この場合、このエージェント ホストからの認証要求は成功しません。

問題に対処するには

1. エージェント ホストでノード シークレット ファイルを消去します。

- RSA ACE/Agent for Windows 5.2 以降のソフトウェアを実行しているエージェント ホストの場合は、RSA Authentication Manager アプリケーションを起動し、[高度な設定] を選択し、ノード シークレットで [消去] をクリックします。
- 旧バージョン (4.4x 以前) の RSA ACE/Agent for Windows ソフトウェアを実行しているエージェント ホストの場合は、***%SYSTEMROOT%¥system32*** ディレクトリ内のノード シークレット ファイルを削除します。デフォルトのファイル名は **securid** です。
- RSA ACE/Agent for Windows 4.4x ソフトウェアを実行しているエージェント ホストの場合は、システム レジストリ内のノード シークレット ファイルを削除します。デフォルトのファイル名は **securid** です。
- RSA Authentication Manager for UNIX ソフトウェアを実行しているエージェント ホストの場合は、***ACEDATA*** ディレクトリ内のノード シークレット ファイルを削除します。デフォルトのファイル名は **securid** です。

2. 自動配布 (Automatic Delivery) 機能を使用している場合は、Authentication Manager でノード シークレット ファイルを消去します。手動配布 (Manual Delivery) 機能を使用している場合は、このステップは不要です。

   RSA Authentication Manager 上でノード シークレットを消去するには、エージェント ホストの [Edit Agent Host] ダイアログ ボックスを開き、[Node Secret Created] チェックボックスをオフにします。

3. ノード シークレットがエージェント ホストと Authentication Manager の両方で消去された場合は、次の操作を実行してください。
   - デフォルトの自動配布 (Automatic Delivery) 機能を使用している場合は、エージェント ホストで認証に次回成功したときに、ノード シークレット ファイルがエージェント ホストに再送されます。この処理が実行されると、[Node Secret Created] チェックボックスがオンになります。
   - 手動配布 (Manual Delivery) 機能を使用して新しいノード シークレットを作成する場合は、ヘルプを参照してください。

   ノード シークレットの配布方法の詳細については、222 ページの「ノード シークレット ファイル」を参照してください。

「Node verification failed (ノードの検証に失敗しました)」というメッセージは、次の場合にもログに記録されます。

- エージェント ホストの**sdconf.rec**ファイルに定義されている暗号方式とAuthentication Manager のエージェント ホスト レコードの暗号方式が一致しない場合。

  エージェント ホスト レコードに暗号方式が正しく設定されていない場合は、[Agent Host] メニューの [Edit Agent Host] をクリックして設定を変更します。**sdconf.rec** ファイルの設定が正しくない場合は、**sdconf.rec** ファイルの配布方法の詳細について、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。
- ノード シークレットが作成される前に、リモート ユーザがレルム間認証エージェント ホストで認証を受けようとした場合。認証を要求しているユーザがエージェント ホスト上でアクティブ化されていない場合は、「Node Verification Failed (ノードの検証に失敗しました)」メッセージとともに「User Not on Agent Host (ユーザがエージェント ホスト上でアクティブ化されていません)」メッセージがログに記録されます。
- Authentication Manager でノード シークレット ファイルを作成したが、そのファイルをエージェント ホストに手動で配布しなかった場合。操作手順については、ヘルプを参照してください。

Not Acting Server for this Agent (1139) (このエージェントのアクティング サーバがありません)

要求を受信した Authentication Manager には、エージェント ホストのアクティング マスタまたはアクティング スレーブが割り当てられていません。詳細については、303 ページの「Agent Host has no Acting Servers (1138) (エージェント ホストにアクティング サーバがありません)」を参照してください。

No User Password in DB (8976) (データベースにユーザ パスワードがありません)

エージェントからユーザの Windows ログイン パスワードが要求されましたが、ユーザのパスワードがデータベースに登録されていないため、要求は拒否されました。その結果、承認されたユーザがログインできない場合は、ユーザを New PIN モードに設定し、もう一度認証を受けるようにユーザに連絡してください。問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Number of records cannot be a negative number (レコードの数として負の数値を指定することはできません)

Query Wizard の [Advanced Parameters] ダイアログ ボックスの [record limit] フィールドに負の数値 (たとえば "-100") を入力しようとしました。正の数値 (たとえば "100" や "+100") を入力してください。

OA PIN+Tokencode Length Invalid (8967) (オフライン認証で、PIN + トークンコードの長さが不正です)

ユーザが入力した PIN + トークンコードの長さが、[Edit Offline Authentication] ダイアログ ボックスで設定されている長さより短いため、ユーザは認証を受けることができませんでした。ユーザを New PIN モードに設定した後、もう一度ログオンして、セキュリティ ポリシーを満たす新しい PIN を作成するようにユーザに連絡してください。たとえば、PIN + トークンコードの長さが 12 文字に設定されていて、6 桁のトークンコードが表示されるトークンを使用している場合は、ユーザの PIN は 6 文字でなければなりません。

Offline authentication service failed to initialize context (20002) (オフライン認証サービスがコンテキストを初期化できませんでした)

sdoad サービスのコンポーネントを起動できませんでした。このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Offline authentication service configuration error (20003) (オフライン認証サービスの構成エラー)

sdoad サービスのコンポーネントを起動できませんでした。このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Offline authentication service DB initialization error (20004) (オフライン認証サービスの DB 初期化エラー)

sdoad サービスのコンポーネントを起動できませんでした。このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Offline-Auth Download Failed (8953) (オフライン認証ダウンロードに失敗しました)

指定されたユーザのオフライン認証ダウンロードに失敗しました。[Edit Offline Authentication] ダイアログ ボックスの [Enable verbose offline authentication logging] を選択し、ログ モニタを起動した後、オフライン日数をもう一度ダウンロードするようにユーザに連絡してください。操作を正しく実行できない場合は、ログ モニタに問題の説明が記録されるはずです。問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Offl-Auth PASSCODE REUSE detected (8960) (オフライン認証で PASSCODE の再利用が検出されました)

ユーザが認証を受けるために、同じ PASSCODE を 2 回以上使用しました。これは通常、ユーザのエラーです。トークンに表示されるトークンコードが変わるまで待ち、変わったら新しいトークンコードを入力してもう一度認証を受けるように、ユーザに連絡してください。

Offline-Auth Policy Failed (8959) (オフライン認証でポリシー データの取得に失敗しました)

エージェントが Authentication Manager からオフライン認証のポリシー データを要求したときに、問題が検出されました。エージェント ホスト レコードを Authentication Manager データベースからいったん削除して、再作成した後、もう一度ポリシー データを要求してください。問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Offline-Auth Request Denied (8963) (オフライン認証要求が拒否されました)

システム レベルまたはエージェント レベルでオフライン認証が無効に設定されている場合、使用したトークンの種類が無効に設定されている場合、またはユーザがすでに十分なオフライン認証データを取得している場合は、このメッセージが表示されることがあります。

Old Primary. Shutting down (2322) (古いプライマリ、シャットダウンします)

新しいプライマリを指名した後、古いプライマリが新しいプライマリと通信しようとすると、このメッセージが表示されます。このメッセージが表示され、新しいプライマリを指名していない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

One-time password not found in Server database, but cannot delete one-time password delta. (サーバ データベースでワンタイム パスワードが見つかりませんでしたが、ワンタイム パスワードのデルタを削除できませんでした)

レプリケーション パスで、レプリケーション サービスはデータベース レコードを変更しようとしましたが、そのレコードにアクセスできませんでした。管理者がレプリケーション パスの途中でレコードを編集した場合は、この問題が発生することがあります。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、レプリカに適用してください。

One-Time Password Set Expired (1087) (ワンタイム パスワード セットの有効期限が切れました)

ワンタイム パスワード セットの有効期限が切れ、RSA Authentication Manager によって削除されました。削除されたパスワードの他に、認証に使用できるワンタイム パスワード セットがユーザに割り当てられている可能性があります。

One-time Password used to authenticate twice (%1) (15087) (ワンタイム パスワードが認証のために 2 回使用されました)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

PASSCODE Accepted (1011) (PASSCODE が受け付けられました)

ユーザが「Enter PASSCODE (PASSCODE を入力してください)」プロンプトで有効な PASSCODE を入力すると、このメッセージがログに記録されます。

次の 2 つの状況では、ユーザがアクセスを許可されなかった場合でも、「PASSCODE Accepted (PASSCODE が受け付けられました)」メッセージがログに記録されます。

- Authentication Manager やネットワークの負荷が非常に高い場合、Authentication Manager は PASSCODE または新しい PIN を受け付け、メッセージをエージェント ホストに通知しようと試みますが、エージェント ホストはそのメッセージを受信する前にタイムアウトになります。したがって、エージェント ホストはユーザに対して「Access Denied (アクセスが拒否されました)」(または「PIN rejected (PIN が拒否されました)」) というメッセージを表示します。

  この状況が発生した場合は、認証が成功するまで、次のトークンコードが表示されるのを待ち、そのトークンコードを再入力するようにユーザに指示するか、または**エージェントのタイムアウト**値を大きくして、新しい **sdconf.rec** ファイルを作成し、各エージェント ホストに配布します。Windows で**エージェントのタイムアウト**値を大きくするには、Configuration Management アプリケーションを使用します。UNIX の場合は、**sdsetup -config** コマンドを使用します。

  sdconf.rec ファイルの配布の詳細については、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。

  メモ : ユーザが複数のトークンを持っている場合、Authentication Manager は一致するものが見つかるまで各トークンを順に確認するため、エージェントのタイムアウトによってアクセスが拒否される可能性が高くなります。

- エージェント ホストの **sdconf.rec** ファイル (または他の構成方法) に定義されている暗号方式と、エージェント ホスト レコードに指定されている暗号方式が一致しない場合。

  エージェント ホスト レコードに暗号方式が正しく設定されていない場合は、[Agent Host] メニューの [Edit Agent Host] を使用して設定を変更します。**sdconf.rec** ファイルの暗号方式の設定に誤りがある場合は、第 12 章「RSA Authentication Manager の構成 (Windows)」または第 14 章「RSA Authentication Manager の構成 (UNIX)」を参照して、新しい構成ファイルをエージェント ホストにコピーしてください。

PASSCODE REUSE ATTACK Detected (149) (PASSCODE の再利用による攻撃が検出されました)

入力された PASSCODE は、トークンに過去に表示され、アクセスが許可されたトークンコードをベースにしたものです。以前に使用したトークンコードまたは PASSCODE の再利用が禁止されているのは、承認されていない人が (たとえば、電子的な盗聴によって) PASSCODE を不正に取得して再利用することを防ぐためです。

Password Authentication (1092) (パスワードによる認証)

ユーザが「Enter PASSCODE (PASSCODE を入力してください)」プロンプトで有効なユーザ パスワードを入力すると、このメッセージがログに記録されます。監査ログでは、ユーザ パスワードのシリアル番号は常に UPW から始まります。

Pepper length out of range (1156) (RSA EAP Protected OTP クレデンシャルの長さが正しい範囲でありません)

RADIUS クライアントから送信された RSA EAP Protected OTP クレデンシャルの長さが正しい範囲でありません。クレデンシャルの設定は、RSA Authentication Manager または RADIUS クライアントで編集できます。RSA Authentication Manager での RSA EAP Protected OTP の設定については、ヘルプを参照してください。RADIUS クライアントでクレデンシャルの設定を変更する方法については、クライアント ソフトウェアのマニュアルを参照してください。

Press spacebar to continue (操作を続行するには、スペースバーを押してください)

管理アプリケーションを実行しているときにこのメッセージが表示された場合は、ソフトウェアに問題があると考えられます。メッセージが表示されたときに実行していた操作を書き留め、RSA セキュリティ正規販売代理店にご連絡ください。

Prev Tokencode/Bad PIN Detected (1144) (過去に表示されたトークンコード / 不正な PIN が検出されました)

RSA Authentication Manager に送信された PASSCODE に、過去にトークンに表示されたことのあるトークンコードと不正な PIN が含まれています。このメッセージは、電子的な盗聴など、何らかの方法で有効なトークンコードを入手した人が正しい PIN を推測しようとしている可能性があることを示します。

Primary and Replica Sent XR Response (8223) (プライマリとレプリカから相互に応答が送信されました)

レルムのプライマリとレプリカの両方から、認証要求に対する応答が送信されました。この状況は、プライマリとレプリカの間のネットワーク接続が切断されていることを示します。

Primary Breaking Connection %1 (15219) (プライマリが接続を切断します)

このメッセージは、認証プロセスがプライマリで停止されたときに表示され、その後、「ACE/Server Replica will handle authentication requests (RSA ACE/Server レプリカが認証要求を処理します)」メッセージが表示されます。

Primary cannot connect to replica (2121) (プライマリがレプリカに接続できませんでした)

レプリケーション管理ユーティリティで設定されているレプリカの情報 (ホスト名、IP アドレス) が、DNS サーバまたはシステムの **hosts** ファイルに登録されている情報と同じであるかどうかを確認してください。IT 部門に連絡して、ネットワークの問題に対処しなければならない可能性があります。

Primary Has Connected To Replica. (プライマリがレプリカに接続されました)

このステータス メッセージは、プライマリとレプリカの間の通信が確立されたことを示します。

Primary Received ... Changes From Replica (プライマリはレプリカから ... の変更を受信しました)

このステータス メッセージは、レプリケーション パスで表示されます。

Primary Received ... Modified ... Records From Replica (プライマリはレプリカから ... のレコードを受信し、... のレコードを変更しました)

このステータス メッセージは、レプリケーション パスで表示されます。

Primary Requesting ... Changes From Replica (プライマリはレプリカから ... の変更を要求しています)

このステータス メッセージは、レプリケーション パスで表示されます。

Primary Shut Down Connection %1 (15197) (プライマリが接続をシャットダウンしています)

プライマリとレプリカの間の接続が停止しました。

Primary Successfully Received Replica Records (プライマリでレプリカレコードを正しく受信しました)

レプリカ データベースに対する変更がレプリケーション パスでプライマリによって受信されました。

Primary Unable To Connect To Replica (プライマリからレプリカに接続できませんでした)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Primary unable to connect to Replica %1 (15119) (プライマリはレプリカに接続できませんでした)

このメッセージは、データベースのプッシュでプライマリがレプリカに接続しようとしたとき、またはレプリカが起動またはシャットダウンされるときに表示されることがあります。

Primary Will Retry Every ... Seconds (プライマリは ... 秒ごとに再試行します)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Progress brokers are busy. If the brokers aren't running, delete .lk files in the data directory (15039) (Progress ブローカはビジー状態です。ブローカが動作していない場合は、データ ディレクトリの .lk ファイルを削除してください)

.lk ファイルを削除しても問題を解決できない場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

PushDB failed after receipt (2289) (レプリカ パッケージの受信後に Push DB でエラーが発生しました)

このメッセージは、レプリカがプライマリからレプリカ パッケージを受信した後、インストールできなかったときに、「Start rep pack reinstall (レプリカ パッケージの再インストールを開始します)」メッセージの後に、ログに記録されます。レプリカのデフォルトのレプリカ パッケージ ディレクトリから ***ACEDATA*** ディレクトリにレプリカ パッケージをコピーした後、レプリカを再起動してください。

PushDB failed on replica (2286) (Push DB がレプリカで失敗しました)

このメッセージは、プライマリがデータベースをレプリカに送信しようとして、送信に失敗したときにログに記録されます。このメッセージの前に診断メッセージが記録されます。たとえば、このメッセージの直前に「Error opening rep pack file (レプリカ パッケージ ファイルを開くときにエラーが発生しました)」や「Error reading rep pack file (レプリカ パッケージ ファイルの読み取りでエラーが発生しました)」メッセージがログに記録されることがあります。プライマリがレプリカにレプリカ パッケージを送信するときに、パケットに問題があった場合は、「Rep Pack send failed (レプリカ パッケージを送信できませんでした)」メッセージがレプリカに記録されます。

PushDB-Assisted Recovery (PushDB) Disabled. Replica Package must be applied manually. %1 (15163) (PushDB-Assisted Recovery (Push DB) 機能は無効になっています。レプリカ パッケージは手動で適用する必要があります)

レプリカ パッケージを手動で適用するか、またはシステム パラメータで PushDB-Assisted Recovery 機能を有効にしてください。

PushDB-Error Reading Replica Package File %1 (15169) (レプリカ パッケージ ファイルの読み取りで Push DB エラーが発生しました)

プライマリがデータベースをレプリカにプッシュできませんでした。レプリカをいったん停止し、起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

PushDB-Failed After Replica Received Replica Package %1 (15165) (レプリカがレプリカ パッケージを受信した後、Push DB が失敗しました)

レプリカがプライマリからプッシュされたレプリカ パッケージを適用できませんでした。レプリカをいったん停止し、起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

PushDB-failed on Replica %1 (15161) (レプリカで Push DB が失敗しました)

プライマリがデータベースをレプリカにプッシュできませんでした。レプリカを再起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

PushDB-Replica Server Restart Failed %1 (15171) (Push DB でレプリカ サーバを再起動できませんでした)

プライマリからプッシュされたデータベースを受信した後、レプリカを再起動できませんでした。レプリカをいったん停止し、起動してください。

PushDB-SDSERV Copy Failed on Replica Package Install %1 (15166) (Push DB でレプリカ パッケージのインストール時に SDSERV をコピーできませんでした)

レプリカがプライマリからプッシュされたレプリカ パッケージを適用できませんでした。レプリカをいったん停止し、起動してください。それでもメッセージが表示される場合は、レプリカ パッケージを手動で適用してください。

Realm Responded Late (8221) (レルムの応答が遅すぎます)

ローカル エージェント ホストでタイムアウトが発生した後、レルムが応答しました。リモート レルム Authentication Manager が動作していないか、またはネットワーク接続が切断されている可能性があります。この問題が何度も発生する場合は、**エージェントのタイムアウト**値を大きくすることを検討してください。手順については、367 ページの「PASSCODE Accepted (1011) (PASSCODE が受け付けられました)」を参照してください。

Received Abort Signal (%1) (16201) (アボート シグナルを受信しました)

RSA Authentication Manager プロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**、および **sdadmind**、**acesrvc**、**acesrvc_be**、**logmainthd**) が異常終了すると、このメッセージが表示されます。メッセージに示されているエラーを確認してください。RSA Authentication Manager ソフトウェアに関連しない問題の場合は、適切な処置をとり、問題が解決されたら RSA Authentication Manager を再起動してください。RSA Authentication Manager ソフトウェアに関連する問題の場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Remote error inserting realm (レルムの追加でリモート エラーが発生しました)

ローカル レルムのレルム レコードがリモート データベースにすでに格納されているときに、リモート レルムをデータベースに追加しようとしたり、リモート レルムとの間でレルム シークレットを設定しようとすると、このメッセージが表示されます。このメッセージが表示された場合は、ローカル レルム レコードをリモート データベースから削除する必要があります。

Removed User Password (4541) (ユーザ パスワードが削除されました)

管理者はこのユーザ レコードからこのユーザ パスワードを削除しました。パスワードが削除されたユーザは、そのパスワードを使用して認証を受けることができなくなります。また、新しいパスワードを作成したり、システムで作成されたパスワードを取得することもできません。

Rep authenticating prematurely (2304) (レプリカの認証が途中で終了しました)

プライマリとレプリカが動作していることと、接続が正しく機能していることを確認してください。動作していない場合は、起動してください。それでも問題を解決できない場合は、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。

Rep name in DB doesn't match host (2303) (データベース内のレプリカの名前がホストの情報と一致しません)

データベースに定義されている名前および IP アドレスと、ネットワーク上の名前および IP アドレスとが一致しないため、プライマリがレプリカと通信できませんでした。レプリケーション管理ユーティリティで設定されているレプリカの名前および IP アドレスが、DNS サーバまたはローカルの **hosts** ファイルに指定されている名前および IP アドレスとが一致するかどうか確認してください。

Rep name in DB doesn't match host (2303) (データベース内のレプリカの名前がホストの情報と一致しません)

データベースに定義されている名前および IP アドレスと、ネットワーク上の名前および IP アドレスとが一致しないため、プライマリがレプリカと通信できませんでした。レプリケーション管理ユーティリティで設定されているレプリカの名前および IP アドレスが、DNS サーバまたはローカルの **hosts** ファイルに指定されている名前および IP アドレスとが一致するかどうか確認してください。

Rep needs initial primary connect (2305) (レプリカは初期プライマリ接続を必要としています)

プライマリはレプリカと通信していません。以下の一覧の各操作を実行し、そのつど、問題が解決されたかどうか確認してください。各操作を実行した後もこのメッセージが記録される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

- プライマリとレプリカが動作していることと、接続が正しく機能していることを確認してください。動作していない場合は、いったん起動した後、停止してください。
- レプリカ用の新しいレプリカ パッケージを作成し、Push DB を使用するか、手動で適用してください。
- 各 Authentication Manager の構成情報を調べて、名前と IP アドレスが正しく設定されているかどうか確認してください。

Rep pack not for this replica (2306) (レプリカ パッケージはこのレプリカ用でありません)

レプリカ用の新しいレプリカ パッケージを作成し、適用してください。メッセージが引き続き記録される場合は、レプリケーション管理ユーティリティで設定されているレプリカの情報 (ホスト名、IP アドレス) が、DNS サーバまたはシステムの **hosts** ファイルに登録されている情報と同じであるかどうか確認してください。

Rep pack packet send failed (2298) (レプリカ パッケージのパケットの送信が失敗しました)

このメッセージは、プライマリからレプリカに送信されたパケットに問題があったことを示します。レプリカはシャットダウンし、Push DB プロセスは停止します。このメッセージが繰り返し記録される場合は、レプリカを再起動してください。再起動した後もメッセージが記録される場合は、新しいレプリカ パッケージを作成し、手動で適用します。

Rep pack processed by replica (2287) (レプリカ パッケージがレプリカで処理されました)

レプリカ パッケージがレプリカにインストールされ、更新された新しいデータベースが作成されました。レプリカ パッケージを処理した後、レプリカは再起動され、プライマリに接続されます。Push DB が正常に実行されている場合は、「Start rep pack reinstall (レプリカ パッケージの再インストールを開始します)」というメッセージの後に、このメッセージが記録されます。

Repeated Failures to Lock System Record (15273) (システム レコードをロックできないエラーが繰り返し発生しました)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Replica Breaking Connection %1 (15220) (レプリカが接続を切断します)

このメッセージは、認証プロセスがレプリカで停止されたときに表示され、その後、「ACE/Server Primary will handle authentication requests (RSA ACE/Server プライマリが認証要求を処理します)」メッセージが表示されます。

Replica Correcting Clock By ...Seconds (レプリカは ... 秒だけクロックを修正しました)

このメッセージは、レプリカがプライマリの時刻と一致するようにクロックを設定していることを示します。

Replica Is Not Currently Configured (レプリカは現在構成されていません)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Replica Received Unexpected Packet (15149) (レプリカで予測していないパケットを受信しました)

このメッセージが表示され、「Primary Successfully Reconciled Databases (プライマリでデータベースの調整に成功しました)」または「Replica Successfully Reconciled Databases (レプリカでデータベースの調整に成功しました)」というメッセージが表示されなかった場合は、データベースが壊れているか、またはデータベース間に大きな不一致が発生していると考えられます。このメッセージが表示される場合は、エラーの原因を示す他のメッセージも一緒に表示される可能性があります。

291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。このメッセージが表示され、調整が成功したことを示すメッセージが表示されない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Replica Rejecting *NAME* Delta (レプリカは *NAME* のデルタを拒否しています)

プライマリからレプリカのデータベースに変更情報 (たとえば、エージェント ホストの作成やユーザ レコードの削除) を送信できませんでした。プライマリとレプリカの両方で [RSA Authentication Manager Control Panel] を使用して、サービスとデータベース ブローカを停止します。レプリカ パッケージを作成し、レプリカにコピーまたはプッシュしてください。その後、両方のマシンで RSA Authentication Manager サービスを再起動します。個別のメッセージについては、436 ページを参照してください。

Replica reqs re-connect (2284) (レプリカは再接続を要求しています)

このステータス メッセージは、レプリカでデータベースのインストールが成功した後、レプリカがプライマリに接続する必要があることを示しています。Push DB が正常に実行されている場合は、「Shutting down Replica (レプリカをシャットダウンします)」というメッセージの後に、このメッセージが記録されます。

Replica requires PushDB (2285) (レプリカは Push DB を要求しています)

このメッセージは、レプリカ管理ユーティリティを使用して、新しいレプリカパッケージを作成したときに表示されます。Push DB Assisted Recovery (データベース プッシュ) 機能を有効にするようにシステム パラメータを設定しているときに、新しいレプリカ パッケージを作成すると、プライマリはデータベースをレプリカにプッシュします。Push DB Assisted Recovery 機能が有効に設定されていない場合は、このメッセージの後に「Assisted recvry (PushDB) disabled (データベース プッシュ (Push DB) 機能が無効です)」というメッセージが表示されます。

Replica restart failed (2293) (レプリカの再起動が失敗しました)

このメッセージは、レプリカ パッケージをインストールした後、レプリカを再起動できなかった場合に、「Start rep pack reinstall (レプリカ パッケージの再インストールを開始します)」というメッセージの後にログに記録されます。レプリカを手動で再起動してください。Windows では、[RSA Authentication Manager Control Panel] を使用します。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

Replica Shut Down Connection %1 (15196) (レプリカが接続をシャットダウンしています)

レプリカとプライマリの間の接続が停止しました。

Replica Unable To Bind To Port ... (レプリカをポートにバインドできませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Replica Unable To Correct Clock %1 (15222) (レプリカがクロックを修正できませんでした)

レプリカがシステム クロックの時刻を修正できませんでした。クロックを手動で再設定してください。

Request Recvd From Unknown Realm (8216) (不明レルムから要求を受信しました)

ローカルAuthentication Managerのデータベースに定義されていないレルムから認証要求を受信しました。レルム レコードが壊れているか、データベースから誤って削除された可能性があります。[Add Realm] ダイアログ ボックスを使用してレルムを追加し、新しいレルム シークレットを設定してください。

Response Delay cannot be increased. Adjust client timing parameters. Max. Avg. Latency: %1 secs (to %2) (15099) (応答遅延時間を延長できませんでした。クライアントのタイミング パラメータを調整してください。最大平均遅延時間：... 秒)

レプリケーション管理ユーティリティで設定されているレプリカの情報 (ホスト名、IP アドレス) が、DNS サーバまたはシステムの **hosts** ファイルに登録されている情報と同じであるかどうかを確認してください。IT 部門に連絡して、ネットワークの問題に対処しなければならない可能性があります。

Restarting replica (2294) (レプリカを再起動しています)

レプリカ パッケージをインストールした後、レプリカを再起動しています。Push DB が正常に実行されている場合は、「Start rep pack reinstall (レプリカ パッケージの再インストールを開始します)」というメッセージの後に、このメッセージが記録されます。

RSA ACE/Server Back End cannot get Front End sockadd. (16211) (RSA ACE/Server バックエンドがフロントエンドの sockaddr を取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End cannot get IP address (16215) (RSA ACE/Server バックエンドが IP アドレスを取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End cannot get its own port data (16214) (RSA ACE/Server バックエンドが独自のポート データを取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End cannot get the FE process handle (16217) (RSA ACE/Server バックエンドがフロントエンドのプロセス ハンドルを取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End cannot get the FE socket data (16213) (RSA ACE/Server バックエンドがフロントエンドのソケット データを取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End cannot set the FE socket data (16216) (RSA ACE/Server バックエンドがフロントエンドのソケット データを設定できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End noticed Front End is down (16212) (RSA ACE/Server バックエンドは、フロントエンドがダウンしていることを検出しました)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Back End unable to connect to the Offline Authentication Data Daemon (22000) (RSA ACE/Server バックエンドは、オフライン認証データ デーモンに接続できませんでした)

sdload サービスのコンポーネントを起動できませんでした。このメッセージが表示された場合は、Authentication Manager を再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

RSA ACE/Server cannot decrypt system security block . . . . (15022) (RSA ACE/Server はシステム セキュリティ ブロックを復号できませんでした)

データベース内の機密データの復号で問題が発生しました。***ACEDATA*** ディレクトリに正しいライセンス レコードが登録されているかどうかを確認してください。

RSA ACE/Server cannot retrieve Back End information (16209) (RSA ACE/Server バックエンド情報を取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Fatal - current system date precedes license creation date (16253) (RSA ACE/Server の致命的なエラー、現在のシステム日付がライセンスの作成日より前の日付です)

システム クロックの日付が、ライセンスの作成日より前の日時に設定されています。システムのクロックを再設定してください。

RSA ACE/Server Fatal - License Expired (16252) (RSA ACE/Server の致命的なエラー、ライセンスの有効期限が切れています)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

RSA ACE/Server Fatal Error forking %1 (15054) (フォーク処理で RSA ACE/Server の致命的なエラーが発生しました)

このメッセージが表示された場合は、Authentication Manager を起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

RSA ACE/Server Fatal Error Starting sdradiusd %1 (16185) (sdradiusd の起動で RSA ACE/Server の致命的なエラーが発生しました)

プライマリがデータベースをレプリカにプッシュした後、レプリカは再起動します。この場合、RADIUS サーバがレプリカを再起動できませんでした。レプリカをいったん停止し、再起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

RSA ACE/Server Front End cannot get a work queue entry (16219) (RSA ACE/Server フロントエンドがワーク キュー エントリを取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Front End cannot get back end info (16220) (RSA ACE/Server フロントエンドがバックエンドの情報を取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server Front End cannot get socket data (16218) (RSA ACE/Server フロントエンドがソケット データを取得できませんでした)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server No Back Ends registered with the Front End (16208) (RSA ACE/Server バックエンドがフロントエンドに登録されていません)

認証サービスに問題があります。認証要求を受け付けるフロントエンド サービスと、要求を処理するバックエンド サービスで、通信に関連する何らかのエラーが発生しました。Authentication Manager を再起動します。Windows では、[RSA Authentication Manager Control Panel] を使用して Authentication Manager をいったん停止した後、起動してください。UNIX では、**aceserver stop** コマンドと **aceserver start** コマンドを使用します。

RSA ACE/Server out of memory (15078) (RSA ACE/Server のメモリがなくなりました)

システム メモリがいっぱいになったか、または不足しています。メモリを使用しているプロセスを確認してください。ご使用のプラットフォームの『インストール ガイド』を参照して、システムがメモリの最低要件を満たしているかどうかを確認してください。

sdserv copy failed on reinstall (2291) (再インストールで sdserv がコピーに失敗しました)

レプリカにレプリカ パッケージをインストールするときに、Authentication Manager データベース ファイルを ***ACEDATA*** ディレクトリにコピーできませんでした。このメッセージの直後に、「Replica restart failed (レプリカの再起動が失敗しました)」メッセージが記録されます。

Segmentation violation (%1) (16200) (セグメンテーション違反)

RSA Authentication Manager プロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**、および **sdadmind**、**acesrvc**、**acesrvc_be**、**logmainthd**) が異常終了すると、このメッセージが表示されます。メッセージに示されているエラーを確認してください。RSA Authentication Manager ソフトウェアに関連しない問題の場合は、適切な処置をとり、問題が解決されたら RSA Authentication Manager を再起動してください。RSA Authentication Manager ソフトウェアに関連する問題の場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Select Error On Connection (15195) (接続時に選択エラーが発生しました)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Select Error On Well Known Port (15150) (認識されるポートで選択エラーが発生しました)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Set User Password (4540) (ユーザ パスワードを設定しました)

管理者がユーザのユーザ パスワードを定義しました。パスワードは Change Required モードに設定されました。

Shutting down replica (2299) (レプリカをシャットダウンします)

Push DB の処理が成功しても、レプリカのデータベースまたはレプリカ パッケージに問題がある場合は、レプリカがシャットダウンされます。Push DB の処理が成功すると、このメッセージの前に「Rep pack processed by Replica (レプリカでレプリカ パッケージが処理されました)」というメッセージが記録されます。問題が発生すると、このメッセージの前に「Push DB failed on Replica (レプリカで Push DB が失敗しました)」というメッセージや、Push DB 処理に関連するその他のエラー メッセージが記録されることがあります。追加メッセージは、問題の正確な内容を示します。

SIGPIPE, write with no one to read, resending (%1) (16204) (SIGPIPE、読み取り対象がない書き込み、再送します)

RSA Authentication Manager プロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**、および **sdadmind**、**acesrvc**、**acesrvc_be**、**logmainthd**) が異常終了すると、このメッセージが表示されます。メッセージに示されているエラーを確認してください。RSA Authentication Manager ソフトウェアに関連しない問題の場合は、適切な処置をとり、問題が解決されたら RSA Authentication Manager を再起動してください。RSA Authentication Manager ソフトウェアに関連する問題の場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Simultaneous Login Detected (148) (同時ログインが検出されました)

このメッセージは、ネットワークへの攻撃が試みられたことを警告するために、RSA Authentication Manager 監査証跡に書き込まれます。認証サービスがこのような攻撃を検出し、アクセスを防止しました。

このメッセージが表示された場合は、**トークンをただちに New PIN モードに設定し、以前の PIN を消去してください**。詳細については、127 ページの「New PIN モードの設定」を参照してください。

Sizelimit exceeded (サイズリミットを超えました)

サポートされる 3 つの LDAP ディレクトリ サーバのいずれかに接続する同期ジョブに、大量 (1,000 以上) のユーザ レコードを返すクエリが含まれている場合は、このメッセージが表示されます。詳細については、331 ページの「date time Ext-auth Check error -nnnnn login user Agent Host server token (8401) (Ext-auth チェック エラー)」を参照してください。

Socket initialization failed %1 (15025) (ソケットの初期化が失敗しました)

Authentication Manager を再起動します。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Space symbol cannot be used as a text qualifier (スペース記号をテキスト修飾子として使用することはできません)

[Query Wizard (Output Parameters)] ダイアログ ボックスで、CSV 形式の [Qualifier] フィールドにスペース文字を入力しようとしました。デフォルトは二重引用符 (") 記号ですが、他の記号を使用して CSV の修飾子を指定することもできます (CSV ファイルを開くターゲット アプリケーションで他の修飾子がサポートされるかどうかを確認してください)。

ST Agent Host - No New PIN (1031) (ST エージェント ホスト - New PIN 操作ができませんでした)

New PIN 操作を対話方式で処理できないエージェント ホスト (シングル トランザクション エージェント ホスト) を経由してログオンしようとすると、アクセスは拒否され、このメッセージがログに記録されます。

RSA Authentication Manager Host Mode を実行し、[Token] > [Edit Token] の順にクリックして、トークンが New PIN モードであるかどうかを確認してください。

トークンが New PIN モードに設定された場合、ログオンするには、ユーザは新しい PIN を作成するか、システムから受け取る必要があります。リモートからではなく、直接ログオンしているユーザは、新しい PIN をただちに取得して、処理を続行できます。

ただし、ユーザが直接ログオンすることが不可能な場合や、不便な場合は、管理者が [Set PIN to Next Tokencode] (PIN を次のトークンコードに設定) 操作を実行する必要があります。この操作によって、ユーザは数値 PIN を取得します。この PIN は、他のすべての PIN と同様に、そのユーザだけが知っている情報です。127 ページの「New PIN モードの設定」を参照してください。

ST Agent Host - No Next Tokencode (1032) (ST エージェント ホスト - ネクスト トークンコード操作ができませんでした)

ネクスト トークンコード操作を対話方式で処理できないエージェント ホスト (シングル トランザクション エージェント ホスト) を経由してログオンしようとすると、アクセスは拒否され、このメッセージがログに記録されます。

この問題を解決するには、次のいずれかの操作を実行してください。

- ユーザが別の種類のエージェント ホストを経由してログオンできる場合は、次に表示されるトークンコードを要求するプロンプトが表示され、ネクスト トークンコード操作を終了できます。
- ユーザが直接ログオンすることが不可能な場合や、不便な場合は、管理者が [Resynchronize Token] (トークンの同期のとり直し) 操作を実行する必要があります。128 ページの「トークンの同期のとり直し」を参照してください。

Start rep pack reinstall (2290) (レプリカ パッケージの再インストールを開始します)

レプリカはレプリカ パッケージを受信し、インストールしようとしています。Push DB の処理が正常に実行されている場合は、「Shutting down Replica (レプリカをシャットダウンします)」というメッセージの後に、このメッセージが記録されます。

Starting PushDB (2295) (Push DB を開始します)

プライマリがレプリカ パッケージをレプリカに送信しようとしています。Push DB の処理が正常に実行されている場合は、「Replica Receives Push DB (レプリカが Push DB を受信しました)」というメッセージの後に、このメッセージが記録されます。

System clock setback detected (150) (システム クロックの巻き戻しが検出されました)

Authentication Manager でシステム クロックが遅れていることが検出されました。これはリプレイ アタックの可能性があること、つまりシステムのセキュリティが脅かされている可能性があることを示します。リプレイ アタックを行う攻撃者は、システム クロックを戻して、不正に取得した過去の PASSCODE を再利用してシステムにアクセスしようとします。

The database has rejected acesyncd's credentials (データベースが acesyncd のクレデンシャルを拒否しました)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

The default output location cannot be empty (デフォルトの出力先は必ず指定する必要があります)

[Query Wizard (Output Parameters)] ダイアログ ボックスで、[Default output location] フィールドが空白になっています。このフィールドには有効なパス名を指定してください。

The entry securid/securidprop ..... is invalid (エントリ securid/securidprop ..... が不正です)

このメッセージが表示された場合は、***%SYSTEMROOT%¥system32¥drivers¥etc¥services*** または DNS ネーム サーバに、認証サービスとレプリケーション サービスの名前を正しく定義した行が格納されていることを確認してください。

認証サービスのデフォルト名は **securid**、デフォルト ポート番号は 5500 です。レプリケーション通信サービスの名前は、認証サービスの名前に prop を追加したもので、プライマリのデフォルト名は **securidprop_00**、デフォルト ポート番号は 5505 です。各レプリカにはそれぞれのサービス名とポート番号が割り当てられます

デフォルトでは、レプリカのサービス名は **securidprop_01** や **securidprop_02** などに、ポート番号は 5506 や 5507 などになります。

認証サービスの正しい名前とポート番号を確認するには

[スタート] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックし、[Details] をクリックします。

[Replica Information] の Service 関連の情報が表示されます。

プライマリとレプリカの通信サービスの正しいサービス名とポート番号を確認するには

[スタート] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] > [Details] の順にクリックします。

[Service Name] フィールドと [Service Port Number] フィールドに情報が表示されます。

The file name prefix cannot be empty (ファイル名プリフィックスは必ず指定する必要があります)

[Query Wizard (Output Parameters)] ダイアログ ボックスで、[Filename prefix] フィールドが空白になっています。デフォルトは "query" です。このフィールドには、有効な文字列を指定してください。以下の文字以外は指定できます。

{} ~ " ; ' [ ] , / @ < > ^ |

The group specified in the query definition does not exist. The access level will be reset to default (クエリ定義に指定されたグループが存在しません。アクセス レベルはデフォルトにリセットされます)

実行中のクエリのクエリ アクセス レベルが特定のグループに設定されています。しかし、そのグループが存在しません。クエリが最後にコンパイルされた後、おそらく Authentication Manager データベースから削除されたと考えられます。

The name of this Server in the sdconf.rec file does not match the name of any Server in the database (16260) (sdconf.rec ファイルに定義されているこのサーバの名前がデータベースに定義されているどのサーバの名前とも一致しません)

sdconf.rec ファイルに定義されているこの Authentication Manager の名前を表示するには、構成管理ユーティリティを実行します。データベースに定義されているこの Authentication Manager の名前を表示するには、レプリケーション管理ユーティリティを実行します。問題を解決するには、構成ファイルまたはデータベースに定義されている Authentication Manager の名前を変更してください。

The query DESCRIPTION data is too long and will be truncated (クエリの DESCRIPTION データが長すぎるため、途中で切り捨てられます)

このエラーが発生するのは、クエリの **definition.txt** ファイルを手動で編集した場合だけです。このような操作は推奨できません。

The RSA ACE/Server on this system has established a connection with an old Primary, %1. The connection was refused (16181) (このシステムの RSA ACE/Server が古いプライマリとの接続を確立しました。接続は拒否されました)

新たに指名されたプライマリが古いプライマリに接続されました。古いプライマリはシャットダウンされます。新しいレプリカ パッケージを作成し、古いプライマリに手動で適用してください。

The RSA ACE/Server on this system has established a connection with an old Primary, %1. The connection was refused. Pushing database to that RSA ACE/Server (16180) (このシステムの RSA ACE/Server が古いプライマリとの接続を確立しました。接続は拒否されました。データベースをその RSA ACE/Server にプッシュします)

新たに指名されたプライマリが古いプライマリに接続されました。このメッセージへの対処は不要です。新しいプライマリが古いプライマリにデータベースをプッシュします。

The SELECT statement is too long (SELECT ステートメントが長すぎます)

このエラーが発生するのは、クエリの **definition.txt** ファイルを手動で編集した場合だけです。このような操作は推奨できません。

The site specified in the query definition does not exist. The access level will be reset to default (クエリ定義に指定されたサイトが存在しません。アクセス レベルはデフォルトにリセットされます)

実行中のクエリのクエリ アクセス レベルが特定のサイトに設定されています。しかし、そのサイトが存在しません。クエリが最後にコンパイルされた後、おそらく Authentication Manager データベースから削除されたと考えられます。

The system call gethostname() failed, error = %1 (15024) (システム呼び出し gethostname() が失敗しました)

このメッセージに示されたエラーを確認し、この問題に関連する他のメッセージが記録されていないか、ログを調べてください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

There are multiple asterisks in the query. Only one is allowed (クエリに複数のアスタリスクが指定されています。指定できるのは 1 つだけです)

クエリの列名にはワイルドカード文字としてアスタリスクを指定できますが、ワイルドカード文字は 1 文字しか指定できません。

There are too many active users and Replicas in the database/ Number of active users and Replicas in the database exceeds license limit (データベースに登録されているアクティブ ユーザとレプリカの数が多すぎます / データベース内のアクティブ ユーザおよびレプリカの数がライセンスの制限を超えています)

システムは**違反**モードまたは**アップグレード違反**モードです。

次の場合には、違反モードになります。

- RSA Authentication Manager を新規インストールし、ライセンスの制限を超えた場合。
- これまでライセンスがアップグレード違反モードであり、ここで違反モードになった場合。

ライセンスが違反モードになると、追加ユーザをアクティブ化したり、新しいレプリカを追加することができません。

RSA Authentication Manager をアップグレードしたときに、ライセンスの制限を超えた場合は、アップグレード違反モードになります。アップグレード違反モードになると、ライセンスは 90 日間有効のテンポラリ ライセンスになります。ライセンスの有効期限が切れると、**違反**モードになり、追加ユーザをアクティブ化したり、新しいレプリカを追加したりできなくなります。

システムを準拠モードに戻すには、RSA セキュリティ正規販売代理店から適切な新しいライセンスを入手する必要があります。または、アクティブ ユーザの数がライセンスの制限内になるように十分な数のユーザを非アクティブ化するか、1 つ以上のレプリカをデータベースから削除して、システムを準拠モードにすることもできます。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

There are too many active users in the database/ Number of active users in the database exceeds license limit/ Number of active users in the database reached license limit (データベースに登録されているアクティブ ユーザの数が多すぎます / データベース内のアクティブ ユーザの数がライセンスの制限を超えています / データベース内のアクティブ ユーザの数がライセンスの制限に達しました)

システムは**違反**モードまたは**アップグレード違反**モードです。

次の場合には、違反モードになります。

- RSA Authentication Manager を新規インストールし、ライセンスの制限を超えた場合。
- これまでライセンスがアップグレード違反モードであり、ここで違反モードになった場合。

ライセンスが違反モードになると、新たに追加ユーザをアクティブ化することができません。

RSA Authentication Manager をアップグレードしたときに、ライセンスの制限を超えた場合は、アップグレード違反モードになります。アップグレード違反モードになると、ライセンスは 90 日間有効のテンポラリ ライセンスになります。ライセンスの有効期限が切れると、**違反**モードになり、追加ユーザをアクティブ化することができなくなります。

システムを準拠モードに戻すには、RSA セキュリティ正規販売代理店から適切な新しいライセンスを入手する必要があります。または、アクティブ ユーザの数がライセンスの制限内になるように、十分な数のユーザを非アクティブ化して、システムを準拠モードに戻してください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

There are too many Replicas in the database/ Number of Replicas in the database exceeds license limit (データベースに登録されているレプリカの数が多すぎます / データベース内のレプリカの数がライセンスの制限を超えています)

システムは**違反**モードまたは**アップグレード違反**モードです。

次の場合には、違反モードになります。

- RSA Authentication Manager を新規インストールし、ライセンスの制限を超えた場合。
- これまでライセンスがアップグレード違反モードであり、ここで違反モードになった場合。

ライセンスが違反モードになると、新しいレプリカを追加することができません。

RSA Authentication Manager をアップグレードしたときに、ライセンスの制限を超えた場合は、アップグレード違反モードになります。アップグレード違反モードになると、ライセンスは 90 日間有効のテンポラリ ライセンスになります。ライセンスの有効期限が切れると、**違反**モードになり、新しいレプリカを追加することができなくなります。

システムを準拠モードに戻すには、RSA セキュリティ正規販売代理店から適切な新しいライセンスを入手する必要があります。または、1 つ以上のレプリカをデータベースから削除して、システムを準拠モードにすることもできます。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

This is an old Primary. Receiving DB Push. %1 (16183) (これは古いプライマリです。Push DB を受信中です)

古いプライマリが新しいプライマリからデータベースを受信しています。このメッセージへの対処は不要です。

This is an old Primary. Shutting down. Replica Package should be applied. %1 (16182) (これは古いプライマリです。シャットダウンします。レプリカ パッケージを適用する必要があります)

新しいプライマリが古いプライマリに接続しましたが、システム パラメータで Push DB 機能が有効に設定されていない場合は、古いプライマリがこのメッセージをログに記録します。新しいレプリカ パッケージを作成し、古いプライマリに手動で適用してください。

This query is from an older version of the ACE/Server. It must recompiled by a Realm Administrator (このクエリは RSA ACE/Server の旧バージョンから出されたものです。レルム管理者が再コンパイルする必要があります)

RSA Authentication Manager のバージョンが異なる場合は、クエリの下位互換性を保証することはできません。したがって、RSA Authentication Manager を新しいメジャー バージョンにアップグレードした場合は、他のメジャー バージョンで作成したクエリを再コンパイルする必要があります。

This query is not valid in this realm (このクエリはこのレルムでは無効です)

このクエリは他のレルムでコンパイルされているため、現在のレルムでは実行できません。

This tool must be run on the same machine as the ACE/Server (このツールは ACE/Server と同じマシンで実行しなければなりません)

Authentication Manager でこのメッセージが表示された場合

1. コントロール パネルを開き、[ネットワーク] をダブルクリックすると、コンピュータ名が表示されます。

   表示されるコンピュータ名は、**hosts** ファイルと DNS サーバのデータベースのいずれか一方または両方に登録されている Authentication Manager マシンにエイリアスとして登録されているはずです。

2. 名前が表示されない場合は、***%SYSTEMROOT%*¥system32¥drivers¥etc¥hosts** ファイルと DNS サーバ データベースのいずれか一方または両方を編集してください。

また、プライマリで Configuration Management アプリケーションを起動して、Authentication Manager 名が **sdconf.rec** ファイルに正しく定義されているかどうかも確認してください。名前が一致しない場合は、[Edit] オプションを使用して **sdconf.rec** ファイルを変更します。その後、新しい **sdconf.rec** ファイルをレプリカとすべてのエージェント ホストに配布してください。

sdconf.rec ファイルの配布の詳細については、236 ページ (Windows) または 251 ページ (UNIX) の「更新した構成ファイルの配布」を参照してください。

メモ : sdconf.rec ファイルは Configuration Management アプリケーションによって作成されます。エージェント ホストでは **DES** または **SDI** 暗号方式を使用できますが、各エージェント ホストには、使用する暗号方式に対応する **sdconf.rec** ファイルが必要です。**DES** 暗号方式を使用するエージェント ホストと **SDI** 暗号方式を使用するエージェント ホストの両方がある場合は、各エージェント ホストに配布する **sdconf.rec** ファイルに暗号方式が正しく設定されていることを確認してください。

Timed out trying to insert realm (レルムを追加しようとしましたが、タイムアウトが発生しました)

RSA Authentication Manager がリモート プライマリとの間でレルム シークレットを設定できませんでした。レルム シークレットを設定するには、ローカル レルムのプライマリとリモート レルムのプライマリのポート番号を同じ番号にする必要があり、リモート レルムのプライマリが動作していなければなりません。リモート レルムの管理者に連絡して、正しいポート番号を確認してください。最初に ***%SYSTEMROOT%¥system32¥drivers¥etc¥services*** ファイルを編集してポート番号を更新します。その後、Configuration Management アプリケーションを使用して、プライマリのポート番号を変更します。

Timelimit exceeded (タイムリミットを超えました)

サポートされる 3 つの LDAP ディレクトリ サーバのいずれかに接続する同期ジョブに、大量 (1,000 以上) のユーザ レコードを返すクエリが含まれている場合は、このメッセージが表示されます。詳細については、331 ページの「date time Ext-auth Check error -nnnnn login user Agent Host server token (8401) (Ext-auth チェック エラー)」を参照してください。

Token Disabled, Many Failures (145) (何度も認証に失敗したため、トークンが無効になりました)

正しいトークンコードと不正な PIN を使用して、3 回連続してログインを試行したことをシステムで検出されたか、不正な PASSCODE (PIN とトークンコードのいずれかが不正) をあらかじめ決められた回数より多く連続して使用したことがシステムで検出された場合、トークンは自動的に無効になります。この回数には 1 ～ 10 の値を設定できます。

メモ : ユーザが複数のトークンを使用している場合、そのユーザに割り当てられているすべてのトークンに対して不正なログインの回数が累積されます。

この攻撃回避機能の詳細については、122 ページの「トークンが盗まれたり、紛失した場合」を参照してください。

Token Disabled, Suspect Stolen (143) (盗まれた可能性があるため、トークンが無効になりました)

正しいトークンコードと不正な PIN を使用して、3 回連続してログインが試みられたことがシステムで検出されると、トークンは自動的に無効になります。この状況が発生するのは、RSA SecurID スタンダード カードおよびキーホルダの場合だけです。これらのトークンでは、ユーザは PASSCODE を入力する代わりに、トークンコードと PIN を個別に入力します。

メモ : ユーザが複数のトークンを使用している場合、そのユーザに割り当てられているすべてのトークンに対して不正なログインの回数が累積されます。

この攻撃回避機能の詳細については、122 ページの「トークンが盗まれたり、紛失した場合」を参照してください。

Token not found in Server database, but cannot delete token delta. (サーバ データベースでトークン レコードが見つかりませんでしたが、トークンのデルタを削除できませんでした)

レプリケーション パスで、レプリケーション サービスはデータベース レコードを変更しようとしましたが、そのレコードにアクセスできませんでした。管理者がレプリケーション パスの途中でレコードを編集した場合は、この問題が発生することがあります。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、レプリカに適用してください。

Token not found in Server database, but cannot delete token delta. %1 (15237) (サーバ データベースでトークンが見つかりませんでしたが、トークンのデルタを削除できませんでした)

このメッセージは、レプリケーションでエラーが発生したことを示します。レプリカ用に新しいレプリカ パッケージを作成し、手動で適用するか、または Push DB を使用して適用してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Token record is locked and cannot be updated. Will attempt to update at next replication pass.%1 (15218) (トークン レコードがロックされているため、更新できませんでした。次のレプリケーション パスで更新します)

このメッセージが繰り返し表示される場合は、プライマリをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Too many statements to process. The limit is 32 statements to a query (処理するステートメントの数が多すぎます。クエリに指定できるステートメントは 32 以内です)

クエリに 32 より多くの SQL ステートメントが指定されています。RSA Authentication Manager のカスタム クエリに指定できるステートメントは 32 以内です。

Trace file closed (トレース ファイルが閉じられました)

トレース ファイルを使用すると、プライマリとレプリカの間の通信の問題を解決するのに役立ちます。パケット トレースを有効にし、結果を表示する方法については、RSA セキュリティ正規販売代理店にお問い合わせください。

Trace File Opened (トレース ファイルが開かれました)

トレース ファイルを使用すると、プライマリとレプリカの間の通信の問題を解決するのに役立ちます。パケット トレースを有効にし、結果を表示する方法については、RSA セキュリティ正規販売代理店にお問い合わせください。

Trigger: %1 (15275) (トリガ)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Two different node secrets created for a single agent. Delete agent's secret and re-authenticate %1 (16226) (1 つのエージェントに対して 2 つの異なるノード シークレットが作成されました。エージェントのシークレットを削除し、再度認証を受けてください)

エージェント ホストのノード シークレットが、データベースに定義されているエージェント ホストのノード シークレットと一致しません。エージェント ホストからノード シークレットを削除し、データベースのエージェント ホスト レコードからノード シークレットを消去してください。

Unable to access common query storage. Check folder name (共通のクエリ保存領域にアクセスできませんでした。フォルダ名を確認してください)

[Share Queries] ダイアログ ボックスの [Folder containing shared queries] フィールドに入力したフォルダ名が正しくないか、またはそのフォルダにアクセスするのに必要なアクセス権がありません。

Unable to access query data (クエリ データにアクセスできませんでした)

[Query Wizard (Query Name)] ダイアログ ボックスで指定したフォルダ名が正しくないか、またはそのフォルダにアクセスするのに必要なアクセス権がありません。

Unable to access query repository (クエリ リポジトリにアクセスできませんでした)

ace/data/queries ディレクトリへのアクセスに問題があったため、Query Wizard でクエリ サブディレクトリを作成できませんでした。このディレクトリへの適切なアクセス権がないか、またはディレクトリが壊れているか消失している可能性があります。

Unable to assign a replacement for the current token (現在のトークンの代わりに交換用トークンを割り当てることができませんでした)

トークンのユーザ レコードを取得できない場合や、ユーザ レコードが見つからない場合は、このメッセージが表示されます。トークンのユーザ レコードがデータベースから削除されていないかどうかを確認してください。レコードが削除されている場合は、別のトークンを割り当てます。

このメッセージは、次の場合にも表示されることがあります。

- トークン レコードが壊れている場合。
- 交換前のトークンの PIN を取得できない場合。
- 交換用トークンの PIN の取得、コピー、消去ができない場合。

別の交換用トークンを割り当ててください。

Unable to assign a replacement token for token serial number 000000*nnnnnn* (トークン シリアル番号 000000*nnnnnn* の代わりに交換用トークンを割り当てることができませんでした)

トークンのユーザ レコードを取得できない場合や、ユーザ レコードが見つからない場合は、このメッセージが表示されます。トークンのユーザ レコードがデータベースから削除されていないかどうかを確認してください。レコードが削除されている場合は、別のトークンを割り当てます。

このメッセージは、次の場合にも表示されることがあります。

- トークン レコードが壊れている場合。

- 交換前のトークンの PIN を取得できない場合。
- 交換用トークンの PIN の取得、コピー、消去ができない場合。

別の交換用トークンを割り当ててください。

Unable to chdir to running directory (chdir を使用して実行中のディレクトリに切り替えることはできません)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to connect to sdlog (sdlog に接続できませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to connect to sdserv (sdserv に接続できませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to create running directory (実行中のディレクトリを作成することはできません)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to delete used one-time password (%1) (15086) (使用済みのワンタイム パスワードを削除できませんでした)

このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unable to determine IP address of Replica (レプリカの IP アドレスを判断できませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable To Determine Local IP Address (ローカル IP アドレスを判断できませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to find selected group in the database (選択されたグループをデータベースから見つけることができませんでした)

このエラーは、[Query Wizard (Query Access Level)] ダイアログ ボックスでグループを選択した直後、ダイアログ ボックスを閉じる前に、他の管理者がそのグループを削除した場合にだけ発生します。

Unable to find selected site in the database (選択されたサイトをデータベースから見つけることができませんでした)

このエラーは、[Query Wizard (Query Access Level)] ダイアログ ボックスでサイトを選択した直後、ダイアログ ボックスを閉じる前に、他の管理者がそのサイトを削除した場合にだけ発生します。

Unable to find site related to the selected group (選択されたグループに関連するサイトを見つけることができませんでした)

このエラーは、[Query Wizard (Query Access Level)] ダイアログ ボックスでサイトを選択した直後、サイトからグループの選択を開始する前に、他の管理者がそのサイトを削除した場合にだけ発生します。

Unable to initialize connection to Lock Manager. Check configuration settings (16222) (ロック マネージャへの接続を初期化できませんでした。構成ファイルの設定を確認してください)

ロック マネージャのポート番号またはサービス名が正しくない可能性があります。Configuration Managementアプリケーションを実行し、ロック マネージャが正しいポート番号およびサービス名を使用しているかどうかを確認してください。

Unable to load security block encryption keys (セキュリティ ブロック暗号鍵をロードできませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to locate ACE/Server host (RSA ACE/Server ホストを見つけることができませんでした)

RSA Authentication Manager のホスト名は、ローカルの **hosts** ファイルまたはネームサーバに登録しておく必要があります。このメッセージは、プライマリ、レプリカ、エージェント ホストのいずれかの名前が見つからない場合に表示されます。

Unable to locate current query configuration (現在のクエリ構成を見つけることができませんでした)

Query Wizard にクエリ データをロードするときに問題が発生しました。**definition.txt** ファイルが壊れているか、または他の重大な問題が発生している可能性があります。このメッセージが表示された場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unable to locate definition.txt file in the specified location (指定の場所から definition.txt ファイルが見つかりませんでした)

definition.txt ファイルをインポートするときに、定義ファイルが保存されていない場所を指定しました。

Unable to locate *service name* in the services file.... (services ファイルから *service name* を見つけることができませんでした)

このメッセージが表示された場合は、***%SYSTEMROOT%*¥system32¥drivers¥etc¥services** (***%SYSTEMROOT%*** は Windows NT のルート ディレクトリであり、たとえば **winnt**) または DNS ネーム サーバに、RSA Authentication Manager サービスの名前とポート番号を正しく定義した行が登録されていることを確認してください (この情報を確認する方法については、382 ページの「The entry securid/securidprop ..... is invalid (エントリ securid/securidprop ..... が不正です)」を参照してください)。

認証サービスのデフォルト名は **securid**、デフォルト ポート番号は 5500 です。レプリケーション通信サービスの名前は、認証サービスの名前に **prop** を追加したもので、プライマリのデフォルト名は **securidprop_00**、デフォルト ポート番号は 5505 です。各レプリカにはそれぞれのサービス名とポート番号が割り当てられますデフォルトでは、レプリカのサービス名は **securidprop_01** や **securidprop_02** などに、ポート番号は 5506 や 5507 などになります。その他の RSA Authentication Manager サービスとそのデフォルトは、External Authorization (**sdxauthd**、5540)、Remote Administration (**sdadmind**、5550)、RADIUS (**radius**、1645) です。

これらのデフォルト サービス名とポート番号は変更できますが、**services** ファイルや DNS ネーム サーバに登録されている情報と一致させる必要があります。詳細については、ご使用のプラットフォームの『インストール ガイド』を参照してください。

Unable to log in to database (データベースにログインできませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable To Resolve Port Number Of Service... (サービスのポート番号を解決できませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unable to Retrieve the system record. (15061) (システム レコードを取得できませんでした)

Authentication Manager を再起動します。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unable To Send Heartbeat %1 (15193) (ハートビートを送信できませんでした)

レプリカをいったん停止し、起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unable to Send License to Replica %1 (15156) (ライセンスをレプリカに送信できませんでした)

このメッセージが引き続き表示される場合は、プライマリとレプリカを再起動してください。この操作を行っても問題を解決できない場合は、レプリカを再インストールしてください。

Unable To Swap Encryption Keys %1 (15154) (暗号鍵をスワップできませんでした)

プライマリとレプリカは暗号鍵を交換できませんでした。レプリカを再起動してください。このメッセージが引き続き表示される場合は、プライマリを再起動してください。プライマリを再起動しても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unable To Swap Encryption Keys %1 (15154) (暗号鍵をスワップできませんでした)

プライマリとレプリカは暗号鍵を交換できませんでした。レプリカを再起動してください。このメッセージが引き続き表示される場合は、プライマリを再起動してください。プライマリを再起動しても問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unable To Sync Replica Clock %1 (15153) (レプリカがクロックを修正できませんでした)

システムがレプリカの時刻を自動的にリセットできませんでした。レプリカのクロックとプライマリのクロックの同期がとれている (シンクロナイズしている) ことを確認してください。レプリカの時刻は、プライマリの時刻の 30 秒以内に設定する必要があります。UNIX では、RSA Authentication Manager が root 以外のユーザによって起動されると、このエラーが発生します。その場合は、root としてログオンし、Authentication Manager を再起動してください。

Unable To Transfer Agent Hosts From Replica (レプリカからエージェント ホスト レコードを転送できませんでした)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Unable to transfer Agents from Replica %1 (15125) (レプリカからエージェント レコードを転送できませんでした)

レプリカのデータベースのバックアップを作成し、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。

Unable To Transfer Log Entries From Replica (レプリカからログ エントリを転送できませんでした)

このメッセージは、ネットワーク接続が切断されたか、プライマリが動作していないことを示します。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Unable to transfer log entries from Replica %1 (15121) (レプリカからログ エントリを転送できませんでした)

レプリカのデータベースのバックアップを作成し、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。

Unable to transfer one-time-passwords from Replica %1 (15124) (レプリカからワンタイム パスワードを転送できませんでした)

レプリカのデータベースのバックアップを作成し、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。

Unable To Transfer System From Replica (レプリカからシステム レコードを転送できませんでした)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Unable To Transfer Tokens From Replica (レプリカからトークン レコードを転送できませんでした)

ネットワーク接続が切断されたか、プライマリが動作していません。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Unable to transfer tokens from Replica %1 (15123) (レプリカからトークン レコードを転送できませんでした)

レプリカのデータベースのバックアップを作成し、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。

Unable to transfer user from Replica %1 (15122) (レプリカからユーザ レコードを転送できませんでした)

レプリカのデータベースのバックアップを作成し、レプリカ用の新しいレプリカ パッケージを作成し、手動で適用してください。

Unable to update system start time (15055) (システムの起動時刻を更新できませんでした)

Authentication Manager を再起動します。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unassigning Primary Server token because a replacement token was issued on a Replica Server (16235) (交換用トークンがレプリカ サーバで発行されているため、プライマリ サーバでトークンの割り当てを解除しました)

レプリカを経由してユーザが認証を受けたときに、ユーザの交換用トークンが有効になっていました。その結果、プライマリのデータベースは、レプリカを経由してトークンが有効化されたことを反映するように更新されます。

Unexpected error from errSDDemonize() (errSDDemonize() から予測していないエラーが返されました)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Unexpected packet received %1 (15194) (予測していないパケットを受信しました)

プライマリをいったん停止し、起動してください。メッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unexpected Packet. *NAME* Commit Response Expected (*NAME* のコミット応答を待機していましたが、予測しないパケットを受信しました) (個別のメッセージについては、439 ページを参照してください)

このメッセージが表示された場合は、データベースが壊れているか、データベース間に大きな不一致があるか、または壊れているファイルや消失したファイルがある可能性があります。291 ページの「ネットワーク接続が切断されたか、または Authentication Manager がダウンしている可能性がある場合」を参照してください。

Unknown Lost Token Auth Method (1089) (紛失したトークンの認証方式が不明です)

このメッセージが監査ログに記録されている場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Unknown word encountered (不明の単語が検出されました)

SQL で入力ミスすると、このメッセージが表示されることがあります。たとえば、「MESSAGE」と入力すべきなのに「MESSAG」と入力すると、このメッセージが表示されます。

Upgrade license check...You are attempting to upgrade an Advanced license with a Base license (ライセンスのアップグレード チェック ... アドバンスド ライセンスをベース ライセンスにアップグレードしようとしています)

ベース ライセンスを適用しようとしていますが、ベース ライセンスは現在使用中のアドバンスド ライセンスより制限が厳しくなります。RSA セキュリティが発行した最新バージョンのライセンスを使用しているかどうかを確認した後、ライセンスに問題がなければ、アップグレードをもう一度行ってください。RSA セキュリティ正規販売代理店から指示がない限り、ライセンスのダウングレードは行わないでください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Upgrade license check...Your current license has a higher active user limit than its replacement (ライセンスのアップグレード チェック ... アップグレード後のライセンスより現在使用中のライセンスの方が多くのアクティブ ユーザを登録できます)

現在使用中のライセンスよりアクティブ ユーザ数の制限の厳しいライセンスを適用しようとしています。RSA セキュリティが発行した最新バージョンのライセンスを使用しているかどうかを確認した後、ライセンスに問題がなければ、アップグレードをもう一度行ってください。RSA セキュリティ正規販売代理店から指示がない限り、ライセンスのダウングレードは行わないでください。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Upgrade Replica To Match Primary (プライマリと一致するようにレプリカをアップグレードします)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

User not found in Server database, but cannot delete user delta (15232) (サーバ データベースでユーザ レコードが見つかりませんでしたが、ユーザのデルタを削除できませんでした)

レプリケーション パスで、レプリケーション サービスはデータベース レコードを変更しようとしましたが、そのレコードにアクセスできませんでした。管理者がレプリケーション パスの途中でレコードを編集した場合は、この問題が発生することがあります。このメッセージが引き続き表示される場合は、新しいレプリカ パッケージを作成し、レプリカに適用してください。

User Not on Agent Host (131) (ユーザがエージェント ホスト上でアクティブ化されていません)

ユーザがアクティブ化されていないエージェント ホストにログオンしようとすると、アクセスは拒否され、このメッセージがログに記録されます。セキュリティ ポリシーに適合する場合は、第 3 章「エージェントとエージェント ホスト上でのアクティブ化」の説明に従って、ユーザを直接アクティブ化するか、またはグループを通じてアクティブ化してください。

このメッセージは、認証を要求しているユーザがエージェント ホスト上でアクティブ化されているものの、トークンが割り当てられていない場合にも表示されます。ログ レコードからユーザを特定できない場合は、認証を要求しているユーザのユーザ レコードが登録されていない可能性があります。

エージェント ホストがレルム間認証用に設定され、そのエージェント ホストでアクティブ化されていない別のレルムのユーザが、ノード シークレットの設定前にログオンを試みた場合、このメッセージと「Node Verification Failed (ノードの検証に失敗しました)」メッセージがログに記録されます。

User Password Update Failed (8955) (ユーザ パスワードを更新できませんでした)

Authentication Managerデータベースに登録されているユーザのWindowsパスワードを更新できませんでした。[System Parameters] ダイアログ ボックスで、他の管理者がWindowsパスワードの統合を無効に設定していないかどうか確認してください。また、Authentication Manager データベースに登録されているエージェント ホスト レコードに問題がある場合もあります。エージェント ホスト レコードをいったん削除して再登録することで、ノード シークレットを消去してください。ノード シークレットを消去すると、ユーザが次回認証を受けるときに、エージェントは Windows パスワードの入力を要求し、そのパスワードを Authentication Manager に再送します。問題を解決できない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

User record has been updated, but is currently locked. The updated record cannot be sent to Primary. Will attempt to update at next replication pass.%1 (15216) (ユーザ レコードは更新されましたが、現在ロックされています。更新されたレコードをプライマリに送信できません。次のレプリケーション パスで更新します)

このメッセージが繰り返し表示される場合は、レプリカをいったん停止した後、起動してください。それでもメッセージが表示される場合は、レプリカを再起動します。再起動した後もメッセージが引き続き表示される場合は、RSA セキュリティ正規販売代理店にご連絡ください。

Warning: Unable to open syslog (警告 : syslog を開くことができませんでした)

このメッセージが表示された場合は、プライマリとレプリカの間の通信を取り扱うプロセス (Windows の場合は **syncsrvc**、UNIX の場合は **acesyncd**) の開始で問題が発生したと考えられます。問題への対処法については、292 ページの「プライマリとレプリカ間の通信の開始に関連する問題の解決」を参照してください。

Work queue cannot allocate memory (16223) (ワーク キューがメモリを割り当てることができませんでした)

システム メモリがいっぱいになったか、または不足しています。ご使用のプラットフォームの『インストール ガイド』を参照して、システムがメモリの最低要件を満たしているかどうかを確認してください。

Write failed, file system is full (書き込み失敗、ファイル システムが満杯です)

空きディスク容量が十分でない場合は、Authentication Manager は正常に動作できません。**ディスクの空き容量が 10% 以下にならないようにしてください**。空き容量が 10% 以下になると、RSA Authentication Manager プログラムも含めて、**すべてのアプリケーションで問題が発生**する可能性があります。

XR ACCESS DENIED, Bad Passcode (8212) (アクセス拒否、PASSCODE が不正です)

ユーザが不正な PASSCODE を入力しました。ネットワーク関連の遅延が発生したことが原因で、トークンコードが変化するまでに認証要求がユーザのホーム レルムに到達しなかった場合、このメッセージがログに記録される可能性があります。このメッセージが表示されるその他の原因については、297 ページの「ACCESS DENIED, PASSCODE Incorrect (1008) (アクセス拒否、PASSCODE が不正です)」を参照してください。

XR ACCESS DENIED, Ext-auth failed *login user Agent Host server token* (8235) (アクセス拒否、Ext-auth の処理が失敗しました)

このメッセージは、RSA Authentication Manager で External Authorization をアクティブ化したときに表示されます。このメッセージは次の場合に表示されます。

- ホーム Authentication Manager で [Enable Authorization of Remote Requests] オプションがオンになっていないために、ユーザがリモート レルムからホーム Authentication Manager にアクセスできなかった場合。ユーザがリモート レルムからホーム Authentication Manager にアクセスすることを許可する場合は、このオプションをオンにします。
- **iSDExtAuthorGetHomeData()** 要求が失敗したために、ユーザがリモート レルムからホームAuthentication Managerにアクセスできなかった場合(**iSDExtAuthorGetHomeData()** ルーチンは、レルム間認証の一部として返されるローカル情報を取得します)。要求が失敗した理由を示すメッセージをイベント ログで確認してください。
- **iSDExtAuthorGetHomeData()** 要求が失敗した場合。要求が失敗した理由を示すメッセージをイベント ログで確認してください。

XR ACCESS DENIED, Next Code Bad (8207) (アクセス拒否、ネクスト トークンコードが不正です)

ユーザがネクスト トークンコード プロンプトに応答しようとしましたが、トークンに対して不正なコードを入力しました。したがって、認証要求は拒否されました。

ユーザが不正なトークンコードを入力したか、またはネットワークで遅延が発生したことが原因で、ユーザのネクスト トークンコードが変化する前に、認証要求がユーザのホーム レルムに到達しなかった場合は、このメッセージがログに記録されます。このメッセージが表示されるその他の原因については、125 ページの「PIN が盗まれたり、他人に知られた場合」を参照してください。

XR Agent Host Not Found (8217) (エージェント ホストが見つかりませんでした)

ローカル Authentication Manager でリモート レルムからの認証要求を受信しましたが、要求を出したリモート エージェント ホストに対応するエージェント ホスト レコードが見つかりませんでした。リモート レルムで RSA ACE/Server v3.1 より以前のバージョンが実行されている場合は、ユーザがリモート エージェント ホストにアクセスできるように、そのリモート エージェント ホストを RSA ACE/Server v3.1 またはそれ以降のデータベースに登録する必要があります。詳細については、81 ページの「一部のレルムが RSA ACE/Server 5.0.1 以降にアップグレードされていない場合」を参照してください。

XR Good Tokencode/Bad PIN Detected (8238) (正しいトークンコード / 不正な PIN が検出されました)

リモート レルムから RSA Authentication Manager に送信された PASSCODE で、トークンコードは正しいのですが、PIN が不正でした。このメッセージは、不正なユーザが正しく登録されているユーザのトークンを入手して、正しい PIN を推測しようとしている可能性があることを示します。

XR New PIN Created by User (8210) (New PIN がユーザによって作成されました)

ユーザがリモート レルムで認証を受けようとしたときに、新しい PIN を作成しました。

XR New PIN Rejected (8211) (New PIN が拒否されました)

リモート レルムで認証を受けようとしたユーザが New PIN 操作を正常に終了できませんでした。新しい PIN が、システムで設定されている長さまたは使用できる文字に関する規則に従っていないか、ユーザが New PIN プロセスをキャンセルしました。トークンはまだ New PIN モードです。

XR New PIN Required (8208) (New PIN が要求されました)

ユーザがリモート レルムで認証を受けようとしたときに、新しい PIN を作成するように要求されました。

XR New System Generated PIN (8209) (New PIN がシステムで生成されました)

ユーザがリモート レルムで認証を受けようとしたときに、システムで生成された PIN を受け取りました。

XR Next Tokencode On (8214) (ネクスト トークンコード モードがオンです)

リモート レルムにログインしようとしているユーザが連続してログインに失敗し、その失敗の回数があらかじめ定義されている回数に達すると、最後にこのメッセージが記録されます。ユーザは正しい PIN と不正なトークンコードを入力しました。トークンはネクスト トークンコード モードに設定されたため、2 つの連続する正しい PASSCODE を入力しないと、このユーザのアクセスは許可されません。ネクスト トークンコード モードの詳細については、125 ページの「PIN が盗まれたり、他人に知られた場合」を参照してください。

XR Next Tokencode Required (8206) (ネクスト トークンコードが要求されました)

リモート レルムで認証を受けようとしているユーザに対して、トークンを所有していることを確認するために、第 2 のコードが要求されました。ネクスト トークンコード モードの詳細については、125 ページの「PIN が盗まれたり、他人に知られた場合」を参照してください。

XR PASSCODE Accepted (8202) (PASSCODE が受け付けられました)

ユーザはリモート レルムでの認証で正しい PASSCODE を入力しました。

アクセスが許可されない場合でも、このメッセージがログに記録されることがあります。リモート Authentication Manager、ネットワーク、ユーザのホーム レルムの Authentication Managerのいずれかの負荷が高い場合は、認証応答を受信する前に、エージェント ホストでタイムアウトが発生する可能性があります。したがって、エージェント ホストはユーザに対して「Access Denied (アクセスが拒否されました)」メッセージを表示します。

このような場合は、**エージェントのタイムアウト**値を最大値まで大きくする必要があります。手順については、367 ページの「PASSCODE Accepted (1011) (PASSCODE が受け付けられました)」を参照してください。

XR Request Timed Out (8224) (要求がタイムアウトになりました)

他のレルムからの認証要求が解決される前に、エージェントでタイムアウトが発生しました。

XR Token Disabled, Many Failures (8213) (何度も認証に失敗しため、トークンが無効になりました)

リモート レルムで認証を受けようとしたときに、正しいトークンコードと不正な PIN を使用して、3 回連続してログインが試みられたことがシステムで検出されるか、あらかじめ指定されている回数だけ連続して不正な PASSCODE (PIN またはトークンコードのいずれかが不正) が使用されたことがシステムで検出されたため、ユーザのトークンが自動的に無効になりました。この攻撃回避機能の詳細については、122 ページの「トークンが盗まれたり、紛失した場合」を参照してください。

ユーザが複数のトークンを使用している場合、そのユーザに割り当てられているすべてのトークンに対して不正なログインの回数が累積されます。

XR User Not On Agent Host (8218) (ユーザがエージェント ホスト上でアクティブ化されていません)

RSA ACE/Server 3.0 または 3.0.1 を実行しているレルムのユーザがエージェント ホストで認証を受けようとしたときに、そのユーザが自分のホーム レルムの対応するエージェント ホスト レコード上でアクティブ化されていない場合、アクセスは拒否され、このメッセージがログに記録されます。ローカル レルムのセキュリティ管理者は、必要に応じてエージェント ホスト レコードでユーザをアクティブ化する必要があります。

ユーザがエージェント ホスト上でアクティブ化されておらず、ノード シークレットが設定されていない場合は、このメッセージと「Node Verification Failed (ノードの検証に失敗しました)」メッセージがログに記録されます。

You are not authorized to run this query (このクエリを実行する権限が与えられていません)

適切なスコープ レベルが割り当てられていないクエリを実行しようとしています。クエリをコンパイルおよび共有した管理者は、このクエリの使用を特定のレベル以上の権限を持つ管理者に制限していますが、その権限レベルが割り当てられていません。たとえば、サイト管理者やレルム管理者に制限されているクエリを、グループ管理者が実行しようとしている可能性があります。

You have not specified an application to launch (起動するアプリケーションが指定されていません)

Query Wizard の [Advanced (Parameters)] ダイアログ ボックスで、[Launch specified application] をオンにしましたが、フィールドにアプリケーションが指定されていません。起動するアプリケーションへの正しいパス名を指定してください。

Your RSA ACE/Server has an evaluation license...Your license will expire on *month day year*. (RSA ACE/Server のライセンスは評価用ライセンスです。ライセンスは *month day year* に有効期限が切れます)

評価用ライセンスは一定期間だけ有効であり、その期間は通常、ライセンスをインストールしたときからではなく、ライセンスが発行されてから 90 日間です。ライセンスの有効期限が切れると、Authentication Manager を再起動できなくなります。システムを準拠モードに戻すには、RSA セキュリティ正規販売代理店から適切なパーマネント ライセンスを入手する必要があります。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

Your RSA ACE/Server has an evaluation license...Your license expired on *month day year*. (RSA ACE/Server のライセンスは評価用ライセンスです。ライセンスは *month day year* に有効期限が切れます)

評価用ライセンスは一定期間だけ有効であり、その期間は通常、ライセンスをインストールしたときからではなく、ライセンスが発行されてから 90 日間です。ライセンスの有効期限が切れると、Authentication Manager を再起動できなくなります。システムを準拠モードに戻すには、RSA セキュリティ正規販売代理店から適切なパーマネント ライセンスを入手する必要があります。

ライセンスの詳細については、付録 A「ライセンス」を参照してください。

メッセージの ID 番号

以下の表は、イベント ログ、システム ログ、データベース ログに記録されるメッセージのうち、共通形式のメッセージの ID 番号と文字列の一覧です。ID 番号を使用すると、イベント ログ (Windows) またはシステム ログ (UNIX) に送信されるメッセージを選択するために、SNMP フィルタリングを実行できます。詳細については、286 ページの「SNMP によるメッセージのフィルタリング」を参照してください。

Cannot Check Delete Dependency for *NAME* (*NAME* の削除の依存関係をチェックできませんでした)

番号	メッセージ
16150	Cannot Check Delete Dependency for AdministrativeRole
15439	Cannot Check Delete Dependency for Administrator
15436	Cannot Check Delete Dependency for Agent Host
15443	Cannot Check Delete Dependency for Agent Host Extension
15434	Cannot Check Delete Dependency for AgentType

番号	メッセージ
15440	Cannot Check Delete Dependency for EnabledGroup
15441	Cannot Check Delete Dependency for EnabledUser
15438	Cannot Check Delete Dependency for Group
15444	Cannot Check Delete Dependency for GroupExtension
15442	Cannot Check Delete Dependency for GroupMember
15449	Cannot Check Delete Dependency for LogMessage
16024	Cannot Check Delete Dependency for Profile
15985	Cannot Check Delete Dependency for Realm
15989	Cannot Check Delete Dependency for RealmEnabledGroup
15987	Cannot Check Delete Dependency for RealmEnabledUser
15991	Cannot Check Delete Dependency for RealmExtension
15437	Cannot Check Delete Dependency for SecondaryNode
15435	Cannot Check Delete Dependency for Site
15448	Cannot Check Delete Dependency for SiteExtension
15431	Cannot Check Delete Dependency for System
15447	Cannot Check Delete Dependency for SystemExtension
16126	Cannot Check Delete Dependency for TaskList
16175	Cannot Check Delete Dependency for TaskListItem
15433	Cannot Check Delete Dependency for Token
15445	Cannot Check Delete Dependency for TokenExtension
15432	Cannot Check Delete Dependency for User
15446	Cannot Check Delete Dependency for UserExtension

Cannot Check Dependency for *NAME* (*NAME* の依存関係をチェックできませんでした)

番号	メッセージ
16151	Cannot Check Dependency for AdministrativeRole
15420	Cannot Check Dependency for Administrator
15417	Cannot Check Dependency for Agent Host

番号	メッセージ
15424	Cannot Check Dependency for Agent Host Extension
15415	Cannot Check Dependency for AgentType
16095	Cannot Check Dependency for AttributeValue
15421	Cannot Check Dependency for EnabledGroup
15422	Cannot Check Dependency for EnabledUser
15419	Cannot Check Dependency for Group
15425	Cannot Check Dependency for GroupExtension
15423	Cannot Check Dependency for GroupMember
15430	Cannot Check Dependency for LogMessage
15822	Cannot Check Dependency for OneTimePassword
16023	Cannot Check Dependency for Profile
15411	Cannot Check Dependency for RealmEnabledGroup
15410	Cannot Check Dependency for RealmEnabledUser
15412	Cannot Check Dependency for RealmExtension
15418	Cannot Check Dependency for SecondaryNode
15416	Cannot Check Dependency for Site
15429	Cannot Check Dependency for SiteExtension
15409	Cannot Check Dependency for System
15428	Cannot Check Dependency for SystemExtension
16176	Cannot Check Dependency for TaskListItem
15414	Cannot Check Dependency for Token
15426	Cannot Check Dependency for TokenExtension
15413	Cannot Check Dependency for User
15427	Cannot Check Dependency for UserExtension
16071	Cannot Check Dependency for Value

Cannot Copy Delta To *NAME* To Delete On Replica (*NAME* にデルタをコピーしてレプリカで削除することができませんでした)

番号	メッセージ
16145	Cannot Copy Delta To AdministrativeRole To Delete On Replica
15744	Cannot Copy Delta To Administrator To Delete On Replica
15748	Cannot Copy Delta To Agent Host Extension To Delete On Replica
15741	Cannot Copy Delta To Agent To Delete On Replica
15739	Cannot Copy Delta To AgentType To Delete On Replica
16044	Cannot Copy Delta To Attribute To Delete On Replica
16091	Cannot Copy Delta To AttributeValue To Delete On Replica
15745	Cannot Copy Delta To EnabledGroup To Delete On Replica
15746	Cannot Copy Delta To EnabledUser To Delete On Replica
15743	Cannot Copy Delta To Group To Delete On Replica
15749	Cannot Copy Delta To GroupExtension To Delete On Replica
15747	Cannot Copy Delta To GroupMember To Delete On Replica
15754	Cannot Copy Delta To LogMessage To Delete On Replica
15757	Cannot Copy Delta To LogMessage To Delete On Replica
15756	Cannot Copy Delta To LogReportFormat To Delete On Replica
15755	Cannot Copy Delta To OneTimePassword To Delete On Replica
16019	Cannot Copy Delta To Profile To Delete On Replica
15846	Cannot Copy Delta To Realm To Delete On Replica
15957	Cannot Copy Delta To RealmEnabledGroup To Delete On Replica
15935	Cannot Copy Delta To RealmEnabledUser To Delete On Replica
15979	Cannot Copy Delta To RealmExtension To Delete On Replica
15868	Cannot Copy Delta To Replica To Delete On Replica
15890	Cannot Copy Delta To SchedJob To Delete On Replica
15742	Cannot Copy Delta To SecondaryNode To Delete On Replica
15740	Cannot Copy Delta To Site To Delete On Replica
15753	Cannot Copy Delta To SiteExtension To Delete On Replica
15913	Cannot Copy Delta To SysLogCriteria To Delete On Replica
15736	Cannot Copy Delta To System To Delete On Replica

番号	メッセージ
15752	Cannot Copy Delta To SystemExtension To Delete On Replica
16121	Cannot Copy Delta To TaskList To Delete On Replica
16170	Cannot Copy Delta To TaskListItem To Delete On Replica
15738	Cannot Copy Delta To Token To Delete On Replica
15750	Cannot Copy Delta To TokenExtension To Delete On Replica
15737	Cannot Copy Delta To User To Delete On Replica
15751	Cannot Copy Delta To UserExtension To Delete On Replica
16067	Cannot Copy Delta To Value To Delete On Replica

Cannot Copy *NAME* Delta (*NAME* のデルタをコピーできませんでした)

番号	メッセージ
16127	Cannot Copy AdministrativeRole Delta
15284	Cannot Copy Administrator Delta
15281	Cannot copy Agent delta
15288	Cannot copy Agent host extension delta
15279	Cannot copy AgentType delta
16026	Cannot Copy Attribute Delta
16073	Cannot Copy AttributeValue Delta
15285	Cannot Copy EnabledGroup Delta
15286	Cannot Copy EnabledUser Delta
15283	Cannot Copy Group Delta
15289	Cannot Copy GroupExtension Delta
15287	Cannot Copy GroupMember Delta
15294	Cannot Copy LogMessage Delta
15297	Cannot Copy LogMessage Delta
15295	Cannot Copy LogReportFormat Delta
15296	Cannot Copy OneTimePassword Delta
16001	Cannot Copy Profile Delta
15828	Cannot Copy Realm Delta

番号	メッセージ
15939	Cannot Copy RealmEnabledGroup Delta
15917	Cannot Copy RealmEnabledUser Delta
15961	Cannot Copy RealmExtension Delta
15282	Cannot copy SecondaryNode delta
15280	Cannot Copy Site Delta
15293	Cannot Copy SiteExtension Delta
15895	Cannot Copy SysLogCriteria Delta
15276	Cannot Copy System Delta
15850	Cannot Copy System Delta
15872	Cannot Copy System Delta
15292	Cannot Copy SystemExtension Delta
16103	Cannot Copy TaskList Delta
16152	Cannot Copy TaskListItem Delta
15278	Cannot Copy Token Delta
15290	Cannot Copy TokenExtension Delta
15277	Cannot Copy User Delta
15291	Cannot Copy UserExtension Delta
16049	Cannot Copy Value Delta

Cannot Create (Update) *NAME* On Replica (レプリカで *NAME* を作成 (更新) できませんでした)

番号	メッセージ
16143	Cannot Create (Update) AdministrativeRole On Replica
15700	Cannot Create (Update) Administrator On Replica
15704	Cannot Create (Update) Agent Host Extension On Replica
15697	Cannot Create (Update) Agent On Replica
15695	Cannot Create (Update) AgentType On Replica
16042	Cannot Create (Update) Attribute On Replica
16089	Cannot Create (Update) AttributeValue On Replica

番号	メッセージ
15701	Cannot Create (Update) EnabledGroup On Replica
15702	Cannot Create (Update) EnabledUser On Replica
15699	Cannot Create (Update) Group On Replica
15705	Cannot Create (Update) GroupExtension On Replica
15703	Cannot Create (Update) GroupMember On Replica
15710	Cannot Create (Update) LogMessage On Replica
15713	Cannot Create (Update) LogMessage On Replica
15712	Cannot Create (Update) LogReportFormat On Replica
15711	Cannot Create (Update) OneTimePassword On Replica
16017	Cannot Create (Update) Profile On Replica
15844	Cannot Create (Update) Realm On Replica
15955	Cannot Create (Update) RealmEnabledGroup On Replica
15933	Cannot Create (Update) RealmEnabledUser On Replica
15977	Cannot Create (Update) RealmExtension On Replica
15866	Cannot Create (Update) Replica On Replica
15888	Cannot Create (Update) SchedJob On Replica
15698	Cannot Create (Update) SecondaryNode On Replica
15696	Cannot Create (Update) Site On Replica
15709	Cannot Create (Update) SiteExtension On Replica
15911	Cannot Create (Update) SysLogCriteria On Replica
15692	Cannot Create (Update) System On Replica
15708	Cannot Create (Update) SystemExtension On Replica
16119	Cannot Create (Update) TaskList On Replica
16168	Cannot Create (Update) TaskListItem On Replica
15694	Cannot Create (Update) Token On Replica
15706	Cannot Create (Update) TokenExtension On Replica
15693	Cannot Create (Update) User On Replica
15707	Cannot Create (Update) UserExtension On Replica

番号	メッセージ
16065	Cannot Create (Update) Value On Replica

Cannot Delete *NAME* Delta (*NAME* のデルタを削除できませんできませんでした)

番号	メッセージ
16133	Cannot Delete AdministrativeRole Delta
15480	Cannot Delete Administrator Delta
15477	Cannot Delete Agent Host Delta
15475	Cannot Delete AgentType Delta
16079	Cannot Delete AttributeValue Delta
15481	Cannot Delete EnabledGroup Delta
15482	Cannot Delete EnabledUser Delta
15479	Cannot Delete Group Delta
15485	Cannot Delete GroupExtension Delta
15483	Cannot Delete GroupMember Delta
15490	Cannot Delete LogMessage Delta
15493	Cannot Delete LogMessage Delta
15492	Cannot Delete LogReportFormat Delta
15491	Cannot Delete OneTimePassword Delta
15246	Cannot delete one-time password delta. One-time password record may be locked by another administrator. Primary Authentication Manager attempts to delete at next replication pass.
16007	Cannot Delete Profile Delta
15834	Cannot Delete Realm Delta
15945	Cannot Delete RealmEnabledGroup Delta
15923	Cannot Delete RealmEnabledUser Delta
15967	Cannot Delete RealmExtension Delta
15856	Cannot Delete Replica Delta
15878	Cannot Delete SchedJob Delta
15478	Cannot Delete SecondaryNode Delta

番号	メッセージ
15476	Cannot Delete Site Delta
15489	Cannot Delete SiteExtension Delta
15901	Cannot Delete SysLogCriteria Delta
15472	Cannot Delete System Delta
15488	Cannot Delete SystemExtension Delta
16109	Cannot Delete TaskList Delta
16158	Cannot Delete TaskListItem Delta
15420	Cannot delete token delta. Token record may be locked by another administrator. Primary Authentication Manager attempts to delete at next replication pass.
15474	Cannot delete token delta. Token record may be locked by another administrator. Attempts to delete at next replication pass.
15486	Cannot Delete TokenExtension Delta
15235	Cannot delete user delta. User record may be locked by another administrator. Primary Authentication Manager attempts to delete at next replication pass.
15473	Cannot delete user delta. User record may be locked by another administrator. Attempts to delete at next replication pass.
15487	Cannot Delete UserExtension Delta
16055	Cannot Delete Value Delta

Cannot Delete *NAME* On Replica. (レプリカで *NAME* を削除できませんでした)

番号	メッセージ
16148	Cannot Delete AdministrativeRole On Replica
15810	Cannot Delete Administrator On Replica
15484	Cannot Delete Agent Host Extension Delta
15814	Cannot Delete Agent Host Extension On Replica
15807	Cannot Delete Agent On Replica
15805	Cannot Delete AgentType On Replica
16032	Cannot Delete Attribute Delta
16047	Cannot Delete Attribute On Replica

番号	メッセージ
16094	Cannot Delete AttributeValue On Replica
15811	Cannot Delete EnabledGroup On Replica
15812	Cannot Delete EnabledUser On Replica
15809	Cannot Delete Group On Replica
15815	Cannot Delete GroupExtension On Replica
15813	Cannot Delete GroupMember On Replica
15820	Cannot Delete LogMessage On Replica
15824	Cannot Delete LogMessage On Replica
15823	Cannot Delete LogReportFormat On Replica
15821	Cannot Delete OneTimePassword On Replica
16022	Cannot Delete Profile On Replica
15849	Cannot Delete Realm On Replica
15960	Cannot Delete RealmEnabledGroup On Replica
15938	Cannot Delete RealmEnabledUser On Replica
15982	Cannot Delete RealmExtension On Replica
15871	Cannot Delete Replica On Replica
15893	Cannot Delete SchedJob On Replica
15808	Cannot Delete SecondaryNode On Replica
15806	Cannot Delete Site On Replica
15819	Cannot Delete SiteExtension On Replica
15916	Cannot Delete SysLogCriteria On Replica
15802	Cannot Delete System On Replica
15818	Cannot Delete SystemExtension On Replica
16124	Cannot Delete TaskList On Replica
16173	Cannot Delete TaskListItem On Replica
15804	Cannot Delete Token On Replica
15816	Cannot Delete TokenExtension On Replica
15803	Cannot Delete User On Replica

番号	メッセージ
15817	Cannot Delete UserExtension On Replica
16070	Cannot Delete Value On Replica

Cannot Exclusive Lock *NAME* Delta (*NAME* のデルタを排他的にロックすることができませんでした)

番号	メッセージ
16130	Cannot Exclusive Lock AdministrativeRole Delta
15350	Cannot Exclusive Lock Administrator Delta
15347	Cannot Exclusive Lock Agent Delta
15345	Cannot exclusive lock AgentType delta
16029	Cannot Exclusive Lock Attribute Delta
16076	Cannot Exclusive Lock AttributeValue Delta
15351	Cannot Exclusive Lock EnabledGroup Delta
15352	Cannot Exclusive Lock EnabledUser Delta
15349	Cannot Exclusive Lock Group Delta
15355	Cannot Exclusive Lock GroupExtension Delta
15353	Cannot Exclusive Lock GroupMember Delta
15360	Cannot Exclusive Lock LogMessage Delta
15362	Cannot Exclusive Lock LogReportFormat Delta
15363	Cannot Exclusive Lock LogReportFormat Delta
15361	Cannot Exclusive Lock OneTimePassword Delta
16004	Cannot Exclusive Lock Profile Delta
15831	Cannot Exclusive Lock Realm Delta
15942	Cannot Exclusive Lock RealmEnabledGroup Delta
15920	Cannot Exclusive Lock RealmEnabledUser Delta
15964	Cannot Exclusive Lock RealmExtension Delta
15853	Cannot Exclusive Lock Replica Delta
15875	Cannot Exclusive Lock SchedJob Delta
15348	Cannot Exclusive Lock SecondaryNode Delta

番号	メッセージ
15346	Cannot Exclusive Lock Site Delta
15359	Cannot Exclusive Lock SiteExtension Delta
15898	Cannot Exclusive Lock SysLogCriteria Delta
15342	Cannot Exclusive Lock System Delta
15358	Cannot Exclusive Lock SystemExtension Delta
16106	Cannot Exclusive Lock TaskList Delta
16155	Cannot Exclusive Lock TaskListItem Delta
15344	Cannot Exclusive Lock Token Delta
15356	Cannot Exclusive Lock TokenExtension Delta
15343	Cannot Exclusive Lock User Delta
15357	Cannot Exclusive Lock UserExtension Delta
16052	Cannot Exclusive Lock Value Delta
15354	Cannot Exclusively Lock Agent Host Extension Delta

Cannot Fetch *NAME* Delta (*NAME* のデルタをフェッチできませんできませんでした)

番号	メッセージ
16129	Cannot Fetch AdministrativeRole Delta
15328	Cannot Fetch Administrator Delta
15325	Cannot fetch Agent delta
15332	Cannot fetch Agent host extension delta
15323	Cannot fetch AgentType delta
16028	Cannot Fetch Attribute Delta
16075	Cannot Fetch AttributeValue Delta
15329	Cannot Fetch EnabledGroup Delta
15330	Cannot Fetch EnabledUser Delta
15327	Cannot Fetch Group Delta
15333	Cannot Fetch GroupExtension Delta
15331	Cannot Fetch GroupMember Delta
15338	Cannot Fetch LogMessage Delta

番号	メッセージ
15341	Cannot Fetch LogMessage Delta
15340	Cannot Fetch LogReportFormat Delta
15339	Cannot Fetch OneTimePassword Delta
16003	Cannot Fetch Profile Delta
15830	Cannot Fetch Realm Delta
15941	Cannot Fetch RealmEnabledGroup Delta
15919	Cannot Fetch RealmEnabledUser Delta
15963	Cannot Fetch RealmExtension Delta
15852	Cannot Fetch Replica Delta
15874	Cannot Fetch SchedJob Delta
15326	Cannot Fetch SecondaryNode Delta
15324	Cannot Fetch Site Delta
15337	Cannot Fetch SiteExtension Delta
15897	Cannot Fetch SysLogCriteria Delta
15320	Cannot Fetch System Delta
15336	Cannot Fetch SystemExtension Delta
16105	Cannot Fetch TaskList Delta
16154	Cannot Fetch TaskListItem Delta
15322	Cannot Fetch Token Delta
15334	Cannot Fetch TokenExtension Delta
15321	Cannot Fetch User Delta
15335	Cannot Fetch UserExtension Delta
16051	Cannot Fetch Value Delta
15262	Cannot Fetch System Record

Cannot Find *NAME* To Delete On Replica. (レプリカで *NAME* を検索して削除することができませんでした)

番号	メッセージ
16146	Cannot Find AdministrativeRole To Delete On Replica
15766	Cannot Find Administrator To Delete On Replica
15770	Cannot Find Agent Host Extension To Delete On Replica

番号	メッセージ
15763	Cannot Find Agent To Delete On Replica
15761	Cannot Find AgentType To Delete On Replica
16045	Cannot Find Attribute To Delete On Replica
16092	Cannot Find AttributeValue To Delete On Replica
15767	Cannot Find EnabledGroup To Delete On Replica
15768	Cannot Find EnabledUser To Delete On Replica
15765	Cannot Find Group To Delete On Replica
15771	Cannot Find GroupExtension To Delete On Replica
15769	Cannot Find GroupMember To Delete On Replica
15776	Cannot Find LogMessage To Delete On Replica
15779	Cannot Find LogMessage To Delete On Replica
15778	Cannot Find LogReportFormat To Delete On Replica
15777	Cannot Find OneTimePassword To Delete On Replica
16020	Cannot Find Profile To Delete On Replica
15847	Cannot Find Realm To Delete On Replica
15958	Cannot Find RealmEnabledGroup To Delete On Replica
15936	Cannot Find RealmEnabledUser To Delete On Replica
15980	Cannot Find RealmExtension To Delete On Replica
15869	Cannot Find Replica To Delete On Replica
15891	Cannot Find SchedJob To Delete On Replica
15764	Cannot Find SecondaryNode To Delete On Replica
15762	Cannot Find Site To Delete On Replica
15775	Cannot Find SiteExtension To Delete On Replica
15914	Cannot Find SysLogCriteria To Delete On Replica
15758	Cannot Find System To Delete On Replica
15774	Cannot Find SystemExtension To Delete On Replica
16122	Cannot Find TaskList To Delete On Replica
16171	Cannot Find TaskListItem To Delete On Replica

番号	メッセージ
15760	Cannot Find Token To Delete On Replica
15772	Cannot Find TokenExtension To Delete On Replica
15759	Cannot Find User To Delete On Replica
15773	Cannot Find UserExtension To Delete On Replica
16068	Cannot Find Value To Delete On Replica

Cannot Find Pending Delete for *NAME* (*NAME* の削除保留を見つけることができませんでした)

番号	メッセージ
16149	Cannot Find Pending Delete for AdministrativeRole
15396	Cannot Find Pending Delete for Administrator
15391	Cannot Find Pending Delete for Agent Host
15400	Cannot Find Pending Delete for Agent Host Extension
15389	Cannot Find Pending Delete for AgentType
16048	Cannot Find Pending Delete for Attribute
16096	Cannot Find Pending Delete for AttributeValue
15397	Cannot Find Pending Delete for EnabledGroup
15398	Cannot Find Pending Delete for EnabledUser
15395	Cannot Find Pending Delete for Group
15401	Cannot Find Pending Delete for GroupExtension
15399	Cannot Find Pending Delete for GroupMember
15406	Cannot Find Pending Delete for LogMessage
15408	Cannot Find Pending Delete for LogMessage
15392	Cannot Find Pending Delete for LogReportFormat
15407	Cannot Find Pending Delete for OneTimePassword
16025	Cannot Find Pending Delete for Profile
15984	Cannot Find Pending Delete for Realm
15988	Cannot Find Pending Delete for RealmEnabledGroup
15986	Cannot Find Pending Delete for RealmEnabledUser

番号	メッセージ
15990	Cannot Find Pending Delete for RealmExtension
15983	Cannot Find Pending Delete for Replica
15894	Cannot Find Pending Delete for SchedJob
15394	Cannot Find Pending Delete for SecondaryNode
15390	Cannot Find Pending Delete for Site
15405	Cannot Find Pending Delete for SiteExtension
15393	Cannot Find Pending Delete for SysLogCriteria
15386	Cannot Find Pending Delete for System
15404	Cannot Find Pending Delete for SystemExtension
16125	Cannot Find Pending Delete for TaskList
16174	Cannot Find Pending Delete for TaskListItem
15388	Cannot Find Pending Delete for Token
15402	Cannot Find Pending Delete for TokenExtension
15387	Cannot Find Pending Delete for User
15403	Cannot Find Pending Delete for UserExtension
16072	Cannot Find Pending Delete for Value

Cannot Locate *NAME* To Delete On Replica. (レプリカで *NAME* を検索して削除することができませんでした)

番号	メッセージ
16147	Cannot Locate AdministrativeRole Record To Delete On Replica
15788	Cannot Locate Administrator Record To Delete On Replica
15792	Cannot Locate Agent Host Extension Record To Delete On Replica
15785	Cannot Locate Agent Record To Delete On Replica
15783	Cannot Locate AgentType Record To Delete On Replica
16046	Cannot Locate Attribute Record To Delete On Replica
16093	Cannot Locate AttributeValue Record To Delete On Replica
15789	Cannot Locate EnabledGroup Record To Delete On Replica
15790	Cannot Locate EnabledUser Record To Delete On Replica

番号	メッセージ
15787	Cannot Locate Group Record To Delete On Replica
15793	Cannot Locate GroupExtension Record To Delete On Replica
15791	Cannot Locate GroupMember Record To Delete On Replica
15798	Cannot Locate LogMessage Record To Delete On Replica
15800	Cannot Locate LogReportFormat Record To Delete On Replica
15799	Cannot Locate OneTimePassword Record To Delete On Replica
15801	Cannot Locate OneTimePassword Record To Delete On Replica
16021	Cannot Locate Profile Record To Delete On Replica
15848	Cannot Locate Realm Record To Delete On Replica
15959	Cannot Locate RealmEnabledGroup Record To Delete On Replica
15937	Cannot Locate RealmEnabledUser Record To Delete On Replica
15981	Cannot Locate RealmExtension Record To Delete On Replica
15870	Cannot Locate Replica Record To Delete On Replica
15892	Cannot Locate SchedJob Record To Delete On Replica
15786	Cannot Locate SecondaryNode Record To Delete On Replica
15784	Cannot Locate Site Record To Delete On Replica
15797	Cannot Locate SiteExtension Record To Delete On Replica
15915	Cannot Locate SysLogCriteria Record To Delete On Replica
15780	Cannot Locate System Record To Delete On Replica
15796	Cannot Locate SystemExtension Record To Delete On Replica
16123	Cannot Locate TaskList Record To Delete On Replica
16172	Cannot Locate TaskListItem Record To Delete On Replica
15782	Cannot Locate Token Record To Delete On Replica
15794	Cannot Locate TokenExtension Record To Delete On Replica
15781	Cannot Locate User Record To Delete On Replica
15795	Cannot Locate UserExtension Record To Delete On Replica
16069	Cannot Locate Value Record To Delete On Replica

Cannot Match Delta State for *NAME* (*NAME* のデルタの状態を照合できませんでした)

番号	メッセージ
16131	Cannot Match Delta State for AdministrativeRole
15372	Cannot Match Delta State for Administrator
15369	Cannot Match Delta State for Agent
15376	Cannot Match Delta State for Agent Host Extension
15367	Cannot Match Delta State for AgentType
16030	Cannot Match Delta State for Attribute
16077	Cannot Match Delta State for AttributeValue
15373	Cannot Match Delta State for EnabledGroup
15374	Cannot Match Delta State for EnabledUser
15371	Cannot Match Delta State for Group
15377	Cannot Match Delta State for GroupExtension
15375	Cannot Match Delta State for GroupMember
15382	Cannot Match Delta State for LogMessage
15385	Cannot Match Delta State for LogMessage
15384	Cannot Match Delta State for LogReportFormat
15383	Cannot Match Delta State for OneTimePassword
16005	Cannot Match Delta State for Profile
15832	Cannot Match Delta State for Realm
15943	Cannot Match Delta State for RealmEnabledGroup
15921	Cannot Match Delta State for RealmEnabledUser
15965	Cannot Match Delta State for RealmExtension
15854	Cannot Match Delta State for Replica
15876	Cannot Match Delta State for Replica
15370	Cannot Match Delta State for SecondaryNode
15368	Cannot Match Delta State for Site
15381	Cannot Match Delta State for SiteExtension

番号	メッセージ
15899	Cannot Match Delta State for SysLogCriteria
15364	Cannot Match Delta State for System
15380	Cannot Match Delta State for SystemExtension
16107	Cannot Match Delta State for TaskList
16156	Cannot Match Delta State for TaskListItem
15366	Cannot Match Delta State for Token
15378	Cannot Match Delta State for TokenExtension
15365	Cannot Match Delta State for User
15379	Cannot Match Delta State for UserExtension
16053	Cannot Match Delta State for Value

Cannot Open *NAME* Delta Cursor (*NAME* のデルタ カーソルを開くことができませんでした)

番号	メッセージ
16128	Cannot Open AdministrativeRole Delta Cursor
15306	Cannot Open Administrator Delta Cursor
15303	Cannot open Agent host delta cursor
15310	Cannot open Agent host extension delta cursor
15301	Cannot open AgentType delta cursor
16027	Cannot Open Attribute Delta Cursor
16074	Cannot Open AttributeValue Delta Cursor
15307	Cannot Open EnabledGroup Delta Cursor
15308	Cannot Open EnabledUser Delta Cursor
15305	Cannot Open Group Delta Cursor
15311	Cannot Open GroupExtension Delta Cursor
15309	Cannot Open GroupMember Delta Cursor
15316	Cannot Open LogMessage Delta Cursor
15318	Cannot Open LogReportFormat Delta Cursor
15319	Cannot Open LogReportFormat Delta Cursor

番号	メッセージ
15317	Cannot Open OneTimePassword Delta Cursor
16002	Cannot Open Profile Delta Cursor
15829	Cannot Open Realm Delta Cursor
15940	Cannot Open RealmEnabledGroup Delta Cursor
15918	Cannot Open RealmEnabledUser Delta Cursor
15962	Cannot Open RealmExtension Delta Cursor
15851	Cannot Open Replica Delta Cursor
15873	Cannot Open SchedJob Delta Cursor
15304	Cannot Open SecondaryNode Delta Cursor
15302	Cannot Open Site Delta Cursor
15315	Cannot Open SiteExtension Delta Cursor
15896	Cannot Open SysLogCriteria Delta Cursor
15298	Cannot Open System Delta Cursor
15314	Cannot Open SystemExtension Delta Cursor
16104	Cannot Open TaskList Delta Cursor
16153	Cannot Open TaskListItem Delta Cursor
15300	Cannot Open Token Delta Cursor
15312	Cannot Open TokenExtension Delta Cursor
15299	Cannot Open User Delta Cursor
15313	Cannot Open UserExtension Delta Cursor
16050	Cannot Open Value Delta Cursor

Cannot Read *NAME* Commit Response (*NAME* のコミット応答を読み取ることができませんでした)

番号	メッセージ
16135	Cannot Read AdministrativeRole Commit Response
15524	Cannot Read Administrator Commit Response
15521	Cannot Read Agent Commit Response
15528	Cannot Read Agent Host Extension Commit Response

番号	メッセージ
15519	Cannot Read AgentType Commit Response
16034	Cannot Read Attribute Commit Response
16081	Cannot Read AttributeValue Commit Response
15525	Cannot Read EnabledGroup Commit Response
15526	Cannot Read EnabledUser Commit Response
15523	Cannot Read Group Commit Response
15529	Cannot Read GroupExtension Commit Response
15527	Cannot Read GroupMember Commit Response
15057	Cannot read log filtering configuration.
15534	Cannot Read LogMessage Commit Response
15537	Cannot Read LogMessage Commit Response
15536	Cannot Read LogReportFormat Commit Response
15535	Cannot Read OneTimePassword Commit Response
16009	Cannot Read Profile Commit Response
15836	Cannot Read Realm Commit Response
15947	Cannot Read RealmEnabledGroup Commit Response
15925	Cannot Read RealmEnabledUser Commit Response
15969	Cannot Read RealmExtension Commit Response
15858	Cannot Read Replica Commit Response
15880	Cannot Read SchedJob Commit Response
15522	Cannot Read SecondaryNode Commit Response
15520	Cannot Read Site Commit Response
15533	Cannot Read SiteExtension Commit Response
15056	Cannot read syslog criteria.
15903	Cannot Read SysLogCriteria Commit Response
15516	Cannot Read System Commit Response
15532	Cannot Read SystemExtension Commit Response
16111	Cannot Read TaskList Commit Response

番号	メッセージ
16160	Cannot Read TaskListItem Commit Response
15518	Cannot Read Token Commit Response
15530	Cannot Read TokenExtension Commit Response
15517	Cannot Read User Commit Response
15531	Cannot Read UserExtension Commit Response
16057	Cannot Read Value Commit Response

Cannot Save *NAME* On Replica. (レプリカで *NAME* を保存できませんでした)

番号	メッセージ
16141	Cannot Save AdministrativeRole On Replica
15656	Cannot Save Administrator On Replica
15660	Cannot Save Agent Host Extension On Replica
15653	Cannot Save Agent On Replica
15651	Cannot Save AgentType On Replica
16040	Cannot Save Attribute On Replica
16087	Cannot Save AttributeValue On Replica
15657	Cannot Save EnabledGroup On Replica
15658	Cannot Save EnabledUser On Replica
15655	Cannot Save Group On Replica
15661	Cannot Save GroupExtension On Replica
15659	Cannot Save GroupMember On Replica
15666	Cannot Save LogMessage On Replica
15669	Cannot Save LogMessage On Replica
15668	Cannot Save LogReportFormat On Replica
15667	Cannot Save OneTimePassword On Replica
16015	Cannot Save Profile On Replica
15842	Cannot Save Realm On Replica
15953	Cannot Save RealmEnabledGroup On Replica

番号	メッセージ
15931	Cannot Save RealmEnabledUser On Replica
15975	Cannot Save RealmExtension On Replica
15864	Cannot Save Replica On Replica
15886	Cannot Save SchedJob On Replica
15654	Cannot Save SecondaryNode On Replica
15652	Cannot Save Site On Replica
15665	Cannot Save SiteExtension On Replica
15909	Cannot Save SysLogCriteria On Replica
15647	Cannot Save System On Replica
15664	Cannot Save SystemExtension On Replica
16117	Cannot Save TaskList On Replica
16166	Cannot Save TaskListItem On Replica
15650	Cannot Save Token On Replica
15662	Cannot Save TokenExtension On Replica
15649	Cannot Save User On Replica
15663	Cannot Save UserExtension On Replica
16063	Cannot Save Value On Replica

Cannot Send *NAME* Commit Request to Replica (*NAME* のコミット要求をレプリカに送信できませんでした)

番号	メッセージ
16134	Cannot Send AdministrativeRole Commit Request to Replica
15502	Cannot Send Administrator Commit Request to Replica
15499	Cannot Send Agent Commit Request to Replica
15506	Cannot Send Agent Host Extension Commit Request to Replica
15497	Cannot Send AgentType Commit Request to Replica
16033	Cannot Send Attribute Commit Request to Replica
16080	Cannot Send AttributeValue Commit Request to Replica
15503	Cannot Send EnabledGroup Commit Request to Replica

番号	メッセージ
15504	Cannot Send EnabledUser Commit Request to Replica
15501	Cannot Send Group Commit Request to Replica
15507	Cannot Send GroupExtension Commit Request to Replica
15505	Cannot Send GroupMember Commit Request to Replica
15512	Cannot Send LogMessage Commit Request to Replica
15515	Cannot Send LogMessage Commit Request to Replica
15514	Cannot Send LogReportFormat Commit Request to Replica
15513	Cannot Send OneTimePassword Commit Request to Replica
16008	Cannot Send Profile Commit Request to Replica
15835	Cannot Send Realm Commit Request to Replica
15946	Cannot Send RealmEnabledGroup Commit Request to Replica
15924	Cannot Send RealmEnabledUser Commit Request to Replica
15968	Cannot Send RealmExtension Commit Request to Replica
15857	Cannot Send Replica Commit Request to Replica
15879	Cannot Send SchedJob Commit Request to Replica
15500	Cannot Send SecondaryNode Commit Request to Replica
15498	Cannot Send Site Commit Request to Replica
15511	Cannot Send SiteExtension Commit Request to Replica
15902	Cannot Send SysLogCriteria Commit Request to Replica
15494	Cannot Send System Commit Request to Replica
15510	Cannot Send SystemExtension Commit Request to Replica
16110	Cannot Send TaskList Commit Request to Replica
16159	Cannot Send TaskListItem Commit Request to Replica
15496	Cannot Send Token Commit Request to Replica
15508	Cannot Send TokenExtension Commit Request to Replica
15495	Cannot Send User Commit Request to Replica
15509	Cannot Send UserExtension Commit Request to Replica

Cannot Send *NAME* To Replica (*NAME* をレプリカに送信できませんでした)

番号	メッセージ
16132	Cannot Send AdministrativeRole to Replica
15458	Cannot Send Administrator to Replica
15113	Cannot send agent host delta. Token record may be locked by another administrator. Will attempt to send at next replication pass.
15462	Cannot Send Agent Host Extension to Replica
15455	Cannot Send Agent to Replica
15453	Cannot Send AgentType to Replica
16031	Cannot Send Attribute to Replica
16078	Cannot Send AttributeValue to Replica
15459	Cannot Send EnabledGroup to Replica
15460	Cannot Send EnabledUser to Replica
15457	Cannot Send Group to Replica
15463	Cannot Send GroupExtension to Replica
15461	Cannot Send GroupMember to Replica
15468	Cannot Send LogMessage to Replica
15471	Cannot Send LogMessage to Replica
15470	Cannot Send LogReportFormat to Replica
15469	Cannot Send OneTimePassword to Replica
16006	Cannot Send Profile to Replica
15833	Cannot Send Realm to Replica
15944	Cannot Send RealmEnabledGroup to Replica
15922	Cannot Send RealmEnabledUser to Replica
15966	Cannot Send RealmExtension to Replica
15855	Cannot Send Replica to Replica
15877	Cannot Send SchedJob to Replica
15456	Cannot Send SecondaryNode to Replica
15454	Cannot Send Site to Replica

番号	メッセージ
15467	Cannot Send SiteExtension to Replica
15900	Cannot Send SysLogCriteria to Replica
15265	Cannot Send System To Primary
15450	Cannot Send System to Replica
15466	Cannot Send SystemExtension to Replica
16108	Cannot Send TaskList to Replica
16157	Cannot Send TaskListItem to Replica
15452	Cannot Send Token to Replica
15464	Cannot Send TokenExtension to Replica
15451	Cannot Send User to Replica
15465	Cannot Send UserExtension to Replica
16054	Cannot Send Value to Replica

Cannot Update *NAME* On Replica. (レプリカで *NAME* を更新できませんでした)

番号	メッセージ
16144	Cannot Update AdministrativeRole On Replica
15722	Cannot Update Administrator On Replica
15726	Cannot Update Agent Host Extension On Replica
15719	Cannot Update Agent On Replica
15717	Cannot Update AgentType On Replica
16043	Cannot Update Attribute On Replica
16090	Cannot Update AttributeValue On Replica
15723	Cannot Update EnabledGroup On Replica
15724	Cannot Update EnabledUser On Replica
15721	Cannot Update Group On Replica
15727	Cannot Update GroupExtension On Replica

番号	メッセージ
15725	Cannot Update GroupMember On Replica
15732	Cannot Update LogMessage On Replica
15735	Cannot Update LogMessage On Replica
15734	Cannot Update LogReportFormat On Replica
15733	Cannot Update OneTimePassword On Replica
16018	Cannot Update Profile On Replica
15845	Cannot Update Realm On Replica
15956	Cannot Update RealmEnabledGroup On Replica
15934	Cannot Update RealmEnabledUser On Replica
15978	Cannot Update RealmExtension On Replica
15867	Cannot Update Replica On Replica
15889	Cannot Update SchedJob On Replica
15720	Cannot Update SecondaryNode On Replica
15718	Cannot Update Site On Replica
15731	Cannot Update SiteExtension On Replica
15912	Cannot Update SysLogCriteria On Replica
15714	Cannot Update System On Replica
15730	Cannot Update SystemExtension On Replica
16120	Cannot Update TaskList On Replica
16169	Cannot Update TaskListItem On Replica
15716	Cannot Update Token On Replica
15728	Cannot Update TokenExtension On Replica
15715	Cannot Update User On Replica
15729	Cannot Update UserExtension On Replica
16066	Cannot Update Value On Replica

Cannot Update (Create) *NAME* On Replica (レプリカで *NAME* を更新 (作成) できませんでした)

番号	メッセージ
16140	Cannot Update (Create) AdministrativeRole On Replica
15634	Cannot Update (Create) Administrator On Replica
15638	Cannot Update (Create) Agent Host Extension On Replica
15631	Cannot Update (Create) Agent On Replica
15629	Cannot Update (Create) AgentType On Replica
16039	Cannot Update (Create) Attribute On Replica
16086	Cannot Update (Create) AttributeValue On Replica
15635	Cannot Update (Create) EnabledGroup On Replica
15636	Cannot Update (Create) EnabledUser On Replica
15633	Cannot Update (Create) Group On Replica
15639	Cannot Update (Create) GroupExtension On Replica
15637	Cannot Update (Create) GroupMember On Replica
15644	Cannot Update (Create) LogMessage On Replica
15648	Cannot Update (Create) LogMessage On Replica
15646	Cannot Update (Create) LogReportFormat On Replica
15645	Cannot Update (Create) OneTimePassword On Replica
16014	Cannot Update (Create) Profile On Replica
15841	Cannot Update (Create) Realm On Replica
15952	Cannot Update (Create) RealmEnabledGroup On Replica
15930	Cannot Update (Create) RealmEnabledUser On Replica
15974	Cannot Update (Create) RealmExtension On Replica
15863	Cannot Update (Create) Replica On Replica
15885	Cannot Update (Create) SchedJob On Replica
15632	Cannot Update (Create) SecondaryNode On Replica
15630	Cannot Update (Create) Site On Replica
15643	Cannot Update (Create) SiteExtension On Replica

番号	メッセージ
15908	Cannot Update (Create) SysLogCriteria On Replica
15626	Cannot Update (Create) System On Replica
15642	Cannot Update (Create) SystemExtension On Replica
16116	Cannot Update (Create) TaskList On Replica
16165	Cannot Update (Create) TaskListItem On Replica
15628	Cannot Update (Create) Token On Replica
15640	Cannot Update (Create) TokenExtension On Replica
15627	Cannot Update (Create) User On Replica
15641	Cannot Update (Create) UserExtension On Replica
16062	Cannot Update (Create) Value On Replica

Database Inconsistency. Replica Rejecting *NAME* Delta (データベースに不一致があります。レプリカは *NAME* のデルタを拒否しました)

番号	メッセージ
16137	Database Inconsistency: Replica Rejecting AdministrativeRole Delta
16036	Database Inconsistency: Replica Rejecting Attribute Delta
16083	Database Inconsistency: Replica Rejecting AttributeValue Delta
16011	Database Inconsistency: Replica Rejecting Profile Delta
15838	Database Inconsistency: Replica Rejecting Realm Delta
15949	Database Inconsistency: Replica Rejecting RealmEnabledGroup Delta
15927	Database Inconsistency: Replica Rejecting RealmEnabledUser Delta
15971	Database Inconsistency: Replica Rejecting RealmExtension Delta
15860	Database Inconsistency: Replica Rejecting Replica Delta
15905	Database Inconsistency: Replica Rejecting SysLogCriteria Delta
16113	Database Inconsistency: Replica Rejecting TaskList Delta
16162	Database Inconsistency: Replica Rejecting TaskListItem Delta
16059	Database Inconsistency: Replica Rejecting Value Delta
15882	Database Inconsistency: SchedJob Rejecting SchedJob Delta
15568	Database Inconsistency: Replica Rejecting Administrator Delta

番号	メッセージ
15565	Database Inconsistency: Replica Rejecting Agent Delta
15572	Database Inconsistency: Replica Rejecting Agent Host Extension Delta
15563	Database Inconsistency: Replica Rejecting AgentType Delta
15569	Database Inconsistency: Replica Rejecting EnabledGroup Delta
15570	Database Inconsistency: Replica Rejecting EnabledUser Delta
15567	Database Inconsistency: Replica Rejecting Group Delta
15573	Database Inconsistency: Replica Rejecting GroupExtension Delta
15571	Database Inconsistency: Replica Rejecting GroupMember Delta
15578	Database Inconsistency: Replica Rejecting LogMessage Delta
15581	Database Inconsistency: Replica Rejecting LogMessage Delta
15580	Database Inconsistency: Replica Rejecting LogReportFormat Delta
15579	Database Inconsistency: Replica Rejecting OneTimePassword Delta
15566	Database Inconsistency: Replica Rejecting SecondaryNode Delta
15564	Database Inconsistency: Replica Rejecting Site Delta
15577	Database Inconsistency: Replica Rejecting SiteExtension Delta
15560	Database Inconsistency: Replica Rejecting System Delta
15576	Database Inconsistency: Replica Rejecting SystemExtension Delta
15562	Database Inconsistency: Replica Rejecting Token Delta
15574	Database Inconsistency: Replica Rejecting TokenExtension Delta
15561	Database Inconsistency: Replica Rejecting User Delta
15575	Database Inconsistency: Replica Rejecting UserExtension Delta

Error deleting delta *NAME* (*NAME* のデルタの削除でエラーが発生しました)

番号	メッセージ
2264	Error deleting delta admin role
2252	Error deleting delta ALM
2240	Error deleting delta ATTR
2242	Error deleting delta AV
2220	Error deleting delta CRX

番号	メッセージ
2239	Error deleting delta PROF
2219	Error deleting delta realm
2222	Error deleting delta REG
2221	Error deleting delta REU
2241	Error deleting delta VAL

Error deleting *NAME* (*NAME* の削除でエラーが発生しました)

番号	メッセージ
2238	Error deleting AV
2026	Error deleting admin
2263	Error deleting admin role
2029	Error deleting agent host
2027	Error deleting agent host extnsn
2028	Error deleting agent host type
2251	Error deleting ALM
2236	Error deleting attribute
2208	Error deleting CRX
2030	Error deleting delta admin
2036	Error deleting delta agent host
2031	Error deleting delta CCX
2032	Error deleting delta CGX
2049	Error deleting delta csite-x
2033	Error deleting delta CTX
2034	Error deleting delta CType
2035	Error deleting delta CUX
2037	Error deleting delta EG
2038	Error deleting delta EU
2039	Error deleting delta GM
2040	Error deleting delta group

番号	メッセージ
2042	Error deleting delta logmsg
2041	Error deleting delta LRF
2043	Error deleting delta node
2044	Error deleting delta site
2198	Error deleting delta syslog CR
2046	Error deleting delta system
2045	Error deleting delta sys-x
2047	Error deleting delta token
2048	Error deleting delta user
2050	Error deleting enabled group
2051	Error deleting enabled user
2054	Error deleting group
2052	Error deleting group extnsn
2053	Error deleting group member
2055	Error deleting log entry
2056	Error deleting log message
2057	Error deleting log rpt format8
2058	Error deleting node
2192	Error deleting one time pswrd
2235	Error deleting profile
2203	Error deleting realm
2059	Error deleting record on replica
2218	Error deleting REG
2275	Error deleting replica
2213	Error deleting REU
2061	Error deleting site
2060	Error deleting site extnsn
2197	Error deleting syslog CR

番号	メッセージ
2062	Error deleting system extnsn
2063	Error deleting system record
2269	Error deleting task item
2257	Error deleting tasklist
2065	Error deleting token
2064	Error deleting token extnsn
2067	Error deleting user
2066	Error deleting user extnsn
2237	Error deleting value

Error Transferring *NAME* (*NAME* の転送でエラーが発生しました)

番号	メッセージ
2199	Error transferring realm
2109	Error transfer replica tokens
2091	Error transferring admin
2259	Error transferring admin role
2094	Error transferring agent host
2092	Error transferring agent host ext
2093	Error transferring agent type
2247	Error transferring ALM
2244	Error transferring ATTR
2246	Error transferring AV
2204	Error transferring CRX
2095	Error transferring enabled group
2096	Error transferring enabled user
2099	Error transferring group
2097	Error transferring group extnsn
2098	Error transferring group member
2327	Error transferring job record
2100	Error transferring log message

番号	メッセージ
2101	Error transferring log rpt format
2102	Error transferring node
2243	Error transferring PROF
2214	Error transferring REG
2276	Error transferring replica
2105	Error transferring replica agents
2107	Error transferring replica logs
2106	Error transferring replica logs 2
2190	Error transferring replica OTPs
2108	Error transferring replica system
2277	Error transferring replica users
2209	Error transferring REU
2104	Error transferring site
2103	Error transferring site extnsn
2193	Error transferring syslog CR
2110	Error transferring system extnsn
2111	Error transferring system record
2265	Error transferring task item
2253	Error transferring tasklist
2113	Error transferring token
2112	Error transferring token extnsn
2115	Error transferring user
2114	Error transferring user extnsn
2245	Error transferring VAL

Failed to Lock *recordtype* Record (*recordtype* レコードをロックできませんでした)

番号	メッセージ
2068	Failed to lock agent host record
2069	Failed to lock system record
2070	Failed to lock token record

NAME Already Exists On Replica (*NAME* はレプリカにすでに存在します)

番号	メッセージ
16139	AdministrativeRole Already Exists On Replica
15612	Administrator Already Exists On Replica
15609	Agent Already Exists On Replica
15616	Agent Host Extension Already Exists On Replica
15607	AgentType Already Exists On Replica
16038	Attribute Already Exists On Replica
16085	AttributeValue Already Exists On Replica
15613	EnabledGroup Already Exists On Replica
15614	EnabledUser Already Exists On Replica
15611	Group Already Exists On Replica
15617	GroupExtension Already Exists On Replica
15615	GroupMember Already Exists On Replica
15622	LogMessage Already Exists On Replica
15624	LogReportFormat Already Exists On Replica
15625	LogReportFormat Already Exists On Replica
15623	OneTimePassword Already Exists On Replica
16013	Profile Already Exists On Replica
15840	Realm Already Exists On Replica
15951	RealmEnabledGroup Already Exists On Replica
15929	RealmEnabledUser Already Exists On Replica
15973	RealmExtension Already Exists On Replica
15862	Replica Already Exists On Replica
15884	SchedJob Already Exists On Replica
15610	SecondaryNode Already Exists On Replica
15608	Site Already Exists On Replica
15621	SiteExtension Already Exists On Replica
15907	SysLogCriteria Already Exists On Replica

番号	メッセージ
15604	System Already Exists On Replica
15620	SystemExtension Already Exists On Replica
16115	TaskList Already Exists On Replica
16164	TaskListItem Already Exists On Replica
15606	Token Already Exists On Replica
15618	TokenExtension Already Exists On Replica
15605	User Already Exists On Replica
15619	UserExtension Already Exists On Replica
16061	Value Already Exists On Replica

Replica Rejecting *NAME* Delta (レプリカは *NAME* のデルタを拒否しています)

番号	メッセージ
2126	Replica rejecting admin create
2127	Replica rejecting admin delete
2128	Replica rejecting admin modify
2248	Replica rejecting ALM create
2249	Replica rejecting ALM delete
2250	Replica rejecting ALM modify
2232	Replica rejecting AV create
2233	Replica rejecting AV delete
2234	Replica rejecting AV modify
2129	Replica rejecting CCX create
2130	Replica rejecting CCX delete
2131	Replica rejecting CCX modify
2132	Replica rejecting CGX create
2133	Replica rejecting CGX delete
2134	Replica rejecting CGX modify
2205	Replica rejecting CRX create

番号	メッセージ
2206	Replica rejecting CRX delete
2207	Replica rejecting CRX modify
2135	Replica rejecting CSiteX create
2136	Replica rejecting CSiteX delete
2137	Replica rejecting CSiteX modify
2138	Replica rejecting CSysX create
2139	Replica rejecting CSysX delete
2140	Replica rejecting CSysX modify
2141	Replica rejecting CTX create
2142	Replica rejecting CTX delete
2143	Replica rejecting CTX modify
2144	Replica rejecting CType create
2145	Replica rejecting CType delete
2146	Replica rejecting CType modify
2147	Replica rejecting CUX create
2148	Replica rejecting CUX delete
2149	Replica rejecting CUX modify
2153	Replica rejecting E group create
2154	Replica rejecting E group delete
2155	Replica rejecting E group modify
2156	Replica rejecting E user create
2157	Replica rejecting E user delete
2158	Replica rejecting E user modify
2159	Replica rejecting group create
2160	Replica rejecting group delete
2161	Replica rejecting group modify
2162	Replica rejecting grp mem create
2163	Replica rejecting grp mem delete

番号	メッセージ
2164	Replica rejecting grp mem modify
2168	Replica rejecting log msg create
2169	Replica rejecting log msg delete
2170	Replica rejecting log msg modify
2165	Replica rejecting LRF create
2166	Replica rejecting LRF delete
2167	Replica rejecting LRF modify
2171	Replica rejecting node create
2172	Replica rejecting node delete
2173	Replica rejecting node modify
2187	Replica rejecting OTP create
2188	Replica rejecting OTP delete
2189	Replica rejecting OTP modify
2223	Replica rejecting profile create
2224	Replica rejecting profile delete
2225	Replica rejecting profile modify
2200	Replica rejecting realm create
2201	Replica rejecting realm delete
2202	Replica rejecting realm modify
2215	Replica rejecting REG create
2216	Replica rejecting REG delete
2217	Replica rejecting REG modify
2271	Replica rejecting replica create
2272	Replica rejecting replica delete
2273	Replica rejecting replica modify
2210	Replica rejecting REU create
2211	Replica rejecting REU delete
2212	Replica rejecting REU modify

番号	メッセージ
2323	Replica rejecting schedjob create
2324	Replica rejecting schedjob delete
2325	Replica rejecting schedjob modify
2174	Replica rejecting site create
2175	Replica rejecting site delete
2176	Replica rejecting site modify
2177	Replica rejecting system create
2178	Replica rejecting system delete
2179	Replica rejecting system modify
2254	Replica rejecting tasklist create
2255	Replica rejecting tasklist delete
2256	Replica rejecting tasklist modify
2180	Replica rejecting token create
2181	Replica rejecting token delete
2182	Replica rejecting token modify
2183	Replica rejecting user create
2184	Replica rejecting user delete
2185	Replica rejecting user modify
2229	Replica rejecting value create
2230	Replica rejecting value delete
2231	Replica rejecting value modify

Unexpected Packet. *NAME* Commit Response Expected (*NAME* のコミット応答を待機していましたが、予測しないパケットを受信しました)

番号	メッセージ
16138	Unexpected Packet. AdministrativeRole Commit Response Expected
15590	Unexpected Packet. Administrator Commit Response Expected
15587	Unexpected Packet. Agent Commit Response Expected
15594	Unexpected Packet. Agent Host Extension Commit Response Expected

番号	メッセージ
15585	Unexpected Packet. AgentType Commit Response Expected
16037	Unexpected Packet. Attribute Commit Response Expected
16084	Unexpected Packet. AttributeValue Commit Response Expected
15591	Unexpected Packet. EnabledGroup Commit Response Expected
15592	Unexpected Packet. EnabledUser Commit Response Expected
15589	Unexpected Packet. Group Commit Response Expected
15595	Unexpected Packet. GroupExtension Commit Response Expected
15593	Unexpected Packet. GroupMember Commit Response Expected
15600	Unexpected Packet. LogMessage Commit Response Expected
15603	Unexpected Packet. LogMessage Commit Response Expected
15602	Unexpected Packet. LogReportFormat Commit Response Expected
15601	Unexpected Packet. OneTimePassword Commit Response Expected
16012	Unexpected Packet. Profile Commit Response Expected
15839	Unexpected Packet. Realm Commit Response Expected
15950	Unexpected Packet. RealmEnabledGroup Commit Response Expected
15928	Unexpected Packet. RealmEnabledUser Commit Response Expected
15972	Unexpected Packet. RealmExtension Commit Response Expected
15861	Unexpected Packet. Replica Commit Response Expected
15883	Unexpected Packet. SchedJob Commit Response Expected
15588	Unexpected Packet. SecondaryNode Commit Response Expected
15586	Unexpected Packet. Site Commit Response Expected
15599	Unexpected Packet. SiteExtension Commit Response Expected
15906	Unexpected Packet. SysLogCriteria Commit Response Expected
15582	Unexpected Packet. System Commit Response Expected
15598	Unexpected Packet. SystemExtension Commit Response Expected
16114	Unexpected Packet. TaskList Commit Response Expected
16163	Unexpected Packet. TaskListItem Commit Response Expected
15584	Unexpected Packet. Token Commit Response Expected

番号	メッセージ
15596	Unexpected Packet. TokenExtension Commit Response Expected
15583	Unexpected Packet. User Commit Response Expected
15597	Unexpected Packet. UserExtension Commit Response Expected
16060	Unexpected Packet. Value Commit Response Expected

用語集

Change Required モード

ユーザがユーザ パスワードを使用して初めて認証を受けようとすると、パスワードは Change Required モードに設定されます。これは New PIN モードに類似しています。ユーザは認証を受ける前に、新しいパスワードを作成しなければなりません。

New PIN モード

トークンの既存の PIN が他人に不正に知られた可能性がある場合や、承認されているユーザが PIN を忘れてしまった場合、管理者はトークンを New PIN モードに設定します。管理者が PIN をクリアした場合は、元の PIN は認証のために使用できなくなり、そのトークンを使用して次回認証を受けると、New PIN 手順が開始されます。管理者が PIN をクリアしなかった場合には、元の PIN を最後に 1 回だけ使用することができ、その後、New PIN ダイアログが開始されます。

PIN

ユーザだけが知っている秘密の個人識別番号。PIN は RSA SecurID 二要素認証システムの要素の 1 つです。

アクティブ化

ユーザが特定のエージェント ホストで (直接またはグループ メンバーシップによって) アクティブ化された場合、そのユーザのトークンが割り当て済みで、有効に設定されていれば、そのエージェント ホストで認証を受けることができます。この用語はオープン エージェント ホストには適用されません。

オープン エージェント ホスト

ユーザをエージェント ホスト上で直接アクティブ化したり、エージェント ホスト上でアクティブ化されたグループのメンバとして登録する必要がない場合、エージェント ホストは**オープン**です。RSA Authentication Manager データベースに登録されているユーザであれば、どのユーザでもオープン エージェント ホストで認証を受けることができます。

オフライン認証

コンピュータがドメインから切断されている場合や、RSA Authentication Manager への接続が一時的に使用できない場合でも、ユーザが正しい RSA SecurID PASSCODE を入力しなければ、コンピュータにアクセスできないように設定するオプション。

交換されたトークン

交換されたトークンとは、割り当てられたトークンのうち、交換用トークンによって交換されたトークンのことです。交換用トークンを使用して正しく認証を受けることができた場合は、交換されたトークンは自動的に割り当てが解除され、無効になります。

交換用トークン

交換用トークンとは、すでに割り当てられているトークン (たとえば、間もなく有効期限が切れるトークン) を交換するために提供されるトークンであり、まだ割り当てられていないトークンです。

削除

削除されたレコードは、RSA Authentication Manager データベースから永久に削除されます。

失効

失効したソフトウェア トークンとは、以前に発行されたソフトウェア トークンで、ユーザまたは選択されたユーザ カテゴリから割り当てが解除され、RSA Authentication Manager データベースで自動的に無効にされたトークンです。

制限されたエージェント ホスト
制限されたエージェント ホストとは、ローカルで認識されるすべてのユーザに対して必ずしもオープンではないエージェント ホストです。制限されたエージェント ホストで認証を受けるには、ユーザをそのエージェント ホスト上でアクティブ化しなければなりません。

ソフトウェア トークン
ソフトウェア トークンとは、ネットワーク リソースを保護するためのソフトウェア ベースのワンタイム パスワード認証方式であり、通常はリモート アクセスのために使用されます。

追加
トークン レコードは最初のインストール手順でデータベースに追加されるか、後で [Token] メニューの [Import Token] オプションを使用して追加されます。レコードが追加された後、ユーザがトークンを認証に使用するには、その前にトークンをユーザに割り当てなければなりません。

テンポラリ パスワード
紛失したパスワードの代わりに一時的に割り当てることができるパスワードです。

導入
(RSA SecurID ソフトウェア トークンの説明で使用される用語) ソフトウェア トークンが 1 人のユーザまたは選択されたユーザ カテゴリに発行されたことを示します。ソフトウェア トークンが導入されると、トークン レコード ファイルが作成されます。

トークン
RSA SecurID スタンダード カード、キーホルダ、PINPAD など、トークンコードを表示する持ち運び可能なデバイス。ユーザ パスワード、RSA SecurID スマート カード、およびソフトウェア トークンも、それぞれの特徴を備えた一種のトークンです。トークンは、RSA SecurID 二要素認証システムの要素の 1 つです。もう 1 つの要素はユーザの PIN です。

トークンコード
RSA SecurID トークンに表示されるコードです。トークンコードと PIN の組み合わせによって RSA SecurID 認証システムが構成されます。

トークン レコード
RSA Authentication Manager データベースには、システムの各トークンに対応するレコードが格納されており、トークンに関する情報が保存されています。

ネクスト トークンコード モード
トークンと Authentication Manager のシステム クロックの同期が大きくずれた場合や、認証の試みが連続して失敗した場合は、RSA Authentication Manager はそのトークンをネクスト トークンコード モードに設定します。2 つの連続するトークンコードを要求することで、ユーザが実際にトークンを所有しているかどうか確認されます。

発行
(RSA SecurID ソフトウェア トークンの説明で使用される用語) ソフトウェア トークンが有効に設定され、1 人のユーザまたは選択されたユーザ カテゴリに割り当てられたことを示します。

非アクティブ化
非アクティブ化されたグループまたはユーザは、その後特定の (制限された) エージェント ホストで認証を受けることができなくなります。この用語はオープン エージェント ホストには適用されません。

無効

無効に設定されたトークンはユーザに割り当てることができますが、認証のために使用することはできません。トークンは管理者の操作によって無効に設定されます。[Edit Token] ダイアログ ボックスで [Enabled] チェックボックスをオフにすると、トークンは無効になります。また、推測された (不正な) PIN やトークンコードが何度も試され、認証の失敗が一定の回数になると、トークンは自動的に無効になります。

有効

管理者またはシステムが無効に設定した場合を除き、割り当てられたトークンは有効です。割り当てられていないトークンには、有効 / 無効状態はありません。エージェント ホストで認証を受けるためにトークンを使用するには、トークンを割り当て、有効に設定しなければなりません。また、エージェント ホストがオープン エージェント ホストの場合を除き、トークンを割り当てるユーザをエージェント ホスト上でアクティブ化しなければなりません。

有効期限

トークンにあらかじめプログラミングされている有効期限が切れると、コードが表示されなくなります。トークンのシャットダウン期日は変更不可であり、トークン レコードに格納されています。シャットダウン期日は[Token] > [Edit Token]の順にクリックして表示できます。

ユーザ パスワード

ユーザ パスワードとは、ユーザが認証を受けるときに、PASSCODE プロンプトに対してパスワードを入力できるようにするための管理用トークンです。

割り当て

トークン レコードを割り当てると、そのレコードはシステムの特定のユーザのレコードにリンクされます。エージェント ホストで認証を受けるためにトークンを使用するには、トークンを割り当て、有効に設定しなければなりません。また、エージェント ホストがオープン エージェント ホストの場合を除き、トークンを割り当てるユーザをエージェント ホスト上でアクティブ化しなければなりません。

割り当ての解除

割り当てが解除されたトークンには、ユーザが関連付けられていません。トークンの割り当てを解除すると、トークン レコードとユーザ レコードの間のリンクはなくなります。管理者がトークンの割り当てを解除すると、PIN がクリアされ、[Last Login Date] フィールドには、トークンが認証のために最後に使用された日付が表示されます。[Last Login Date] は、認証のためにこれまで使用されたことのないトークンにとっては意味がなく、その場合は 1/1/1986 に設定されます。

索引

数字

4GL
- プロシージャの実行 、100、148
- レポートのコードの保存 、173、183

A

「Access Denied」メッセージ
- New PIN 手順 、127

ACEDATA 、29
_aceping コマンド
- 出力 、215
- 使用 、214
- 引数 、215

ACEPROG 、29
acquery.r ファイル 、204
Activity レポート 、157
- リアルタイム監視 、165

[Administrator Authentication] ダイアログ ボックス 、41
[Audit Trail Statistics] ダイアログ ボックス 、151
Authentication Manager、「RSA Authentication Manager」を参照 、13
Authorization、「External Authorization」を参照
[Authorization Information] ダイアログ ボックス 、211

C

[Configuration Management]
- ライセンス情報の表示内容 、229

[Configuration Management] ダイアログ ボックス 、228
- 暗号の種類 、231
- エージェント ホストの PASSCODE の設定 、235
- エージェント ホストの構成 、231
- 構成情報 、230
- サービスの情報 、232
- ホストの構成 、234
- ホスト名とサービス名の解決 、233

[Create a New Report] ダイアログ ボックス 、184、185
CSV 、202

D

[Database Compression] ダイアログ ボックス 、86
definition.txt ファイル 、204
DES 暗号方式 、228
DHCP のサポート 、66

E

[Edit Log Extension Data] ダイアログ ボックス 、99、147
「Encryption Error: -1」エラー メッセージ 、39
Exception レポート 、157
- リアルタイム監視 、165

[Extension Data Report] ダイアログ ボックス 、163
External Authorization
- オプション 、211
- タイムアウト メッセージ 、292
- 定義と使い方 、209
- 停止と再起動 、211

H

HTML 、202

I

Incident レポート 、157
- リアルタイム監視 、165

IP アドレス
- 複数のエージェント ホスト 、253
- 変更、エージェント ホスト 、253
- 変更時の注意 、233

J

JSED (Job Executor)
- システム ログへの記録 、167

L

Latin-1 言語サポート 、35
LDAP
- 同期の問題の解決 、291

LDAP (Lightweight Directory Access Protocol)
- admenv 比較ユーティリティ 、108
- sdaceldap ユーティリティ 、108
- マップ ファイル 、108
- ユーザの管理 、112

LDAP 同期 、57
LDAP マップ ファイル 、108
license.rec ファイル 、229、272
[Log Messages Histogram Builder] ダイアログ ボックス 、185
[Log Messages Report Builder] ダイアログ ボックス 、183、184
[Log] メニュー 、282

M

MS-IME システム ヘルプ、日本語入力 、36

N

New PIN モード 、127
NTP サービス 、16

P

PASSCODE
不正を処理するエージェント ホストの構成 、235
PASSCODE、不正
処理するエージェント ホストの構成 、61
PIN (個人識別番号)
英数字 PIN と数字 PIN 、103
オプション 、103
固定長 PIN と可変長 PIN 、104
盗難 、125
ユーザ作成 PIN とシステム生成 PIN 、104

Q

Query Wizard 、190
query.r ファイル 、204
Quick Admin 、44
アーキテクチャ 、44
アドミニストレーション権限 、45
管理者の認証 、48
管理者の認証方式 、48
検索 、49
検索のガイドライン 、49
スコープの無効化 、45
タスクの追加 、46
トラブルシューティング 、51
レポート 、49
レポートのガイドライン 、49

R

RADIUS サーバ
システム ログへの記録 、167
Remote Administration 、40
「Encryption Error: -1」エラー メッセージ 、39
サーバの構成 、39
システム ログへの記録 、166
定義と使い方 、38
認証方式 、40
[Report Format] ダイアログ ボックス 、159
[Report Selection Criteria] ダイアログ ボックス 、160
RSA ACE/Server
[Configuration Management] 、229
データベースの内容 、218
RSA Authentication Manager Quick Admin、「Quick Admin」を参照 、44
RSA Authentication Agent 6.1 、57
RSA Authentication Agent ソフトウェア
sdconf.rec の表示 、217
エージェント ホストの自動登録に関係するプログラム 、217
実行できるリソース 、216
通信の暗号化と復号化に関係するプログラム 、217
認証ダイアログに含まれているプログラム 、216
含まれているプログラム 、216
RSA Authentication Manager
Configuration Management 、213
[Contorl Panel] 、229
logcsv ファイル 、167
RSA Authentication Manager Host Mode の概要 、34
sdconf.rec ファイルの構成 、220
UNIX におけるレプリカの管理 、255
Windows システムのライセンス情報 、229
アーキテクチャ 、20
暗号の種類 、231
イベント、種類 、166
インストール後の実装手順 、35
インストールの要件 、36
エージェント ホストとレプリカの構成 、231
エージェント ホストの PASSCODE の設定 、235
カスタム クエリ 、187
更新した構成ファイルの配布 、236
構成ファイル 、217、244
構成ファイル、更新済みファイルの配布 、251
構成ファイル、変更 、247
構成ファイルの内容 、244
構成ファイルの配布 、251
構成ファイルの変更 、247
構成レコードのライセンス情報 (UNIX) 、244
このリリースの新機能 、27
サーバ名または IP アドレスの変更 、233
サービスとプロセス 、275
サービスの構成 、232
サンプル クエリ 、189
システム ログのイベントの監視 、166
使用するポート 、275
セキュリティ機能 、17
設定 、230
ディスク領域の要件 、85、133
データベース、SQL クエリ 、187
データベース スキーマ 、191
データベースの内容 、20
データベースのフィールドへの日本語の入力 、36
データベースの復元 、92
データベースのメンテナンス、「データベースのメンテナンス」を参照
日常操作でのライセンスの管理 、273
認証サービス 、213
バックアップ 、134
評価用ライセンスからパーマネント ライセンスへの変換 、401
複数のレルム用のライセンス フロッピー ディスク 、229

プライマリ サーバとレプリカ サーバのデータベースの調整 、223
プライマリ / レプリカ モデル 、21
プログラム ファイルとデータ ファイル、213、214
ホストの構成 、234
ホストの名前と IP アドレスの解決 、233
ホストの名前と IP アドレスの指定 、253
ホスト名とサービス名の解決 、233
ライセンス 、28
ライセンス情報 、221
ライセンスのアップグレード 、274
ライセンスのバージョン 、272
ライセンス レコードの更新 、243
ライセンス レコードの更新 (Windows) 、229
レプリカ管理 、239
レプリケーション サービス 、213
レポート、「レポート」を参照
レルム ステータスの判断 、214
ログ モニタ 、214
RSA Authentication Manager Host Mode 、214
概要 、34
終了 、35
メイン メニュー 、35
[RSA Authentication Manager Reports] ダイアログ ボックス 、169、179
[RSA Authentication Manager Services] ダイアログ ボックス 、229
RSA Authentication Manager、バックアップ 、86
RSA Authentication Manager のデータ 、218
license.rec ファイル 、221
sdconf.rec ファイル 、220
ノード シークレット ファイル 、222
RSA Authentication Manager のデータベース スキーマ 、191
RSA SecurID
トークン 、14
RSA SecurID トークン、「トークン」を参照 、14
[Run External Procedure] ダイアログ ボックス 、100、148
runtime.txt ファイル 、204

S

sdaceldap ユーティリティ 、108
構文 、109
sdadmin
インタフェースの基本操作 、178
sdcfgedit_ui.exe 、77
sdconf.rec ファイル 、55、220、227、244
内容の表示 、217
SDI 暗号方式 、228
sdlockmgr 、18
sdlogmon コマンド 、165
sdrepmgmt、レプリケーション間隔の設定 、21
[Select Report Type] ダイアログ ボックス 、172、182
[Set PIN to Next Tokencode] ダイアログ ボックス 、103
SNMP
ログ メッセージのフィルタリング 、286
SNMP (Simple Network Management Protocol) 、166
SNMP によるメッセージのフィルタリング 、286
SQL クエリ 、187
SQL クエリ、「カスタム クエリ」を参照
SSL 接続 、111
syncsrvc (acesyncd)
問題の解決 、292
[System Parameters] ダイアログ ボックス 、207

T

[Token Statistics Report Builder] ダイアログ ボックス 、175、185、186

U

Usage Summary 、157
[User Information] ダイアログ ボックス 、177、187
UTC、「世界協定時」を参照 、16

W

Web Express
Quick Admin と組み合わせたインストール 、51
Windows パスワードの統合 、57

X

XML 、202

あ

アーキテクチャ
Quick Admin 、44
アーキテクチャ、プライマリ / レプリカ 、21
アカウンタビリティ
セキュリティ システムの一部としての監査証跡 、17
アクセス時間
オープン エージェント ホストでの制限、119
ユーザとグループの編集 、120
アドバンスド ライセンス 、28
アドミニストレーション権限
Quick Admin 、45
アドミニストレーション スコープ 、30
アドミニストレーション レベルとクエリ権限 、189

タスク リスト 、30
定義 、31
[アプリケーションの追加と削除] 、230
暗号 、217
種類 、228、231
保護されるもの 、19

い

イベント ログ 、166
イベント ログ メッセージ
監査ログ メッセージの送信 、281
インストール
ライセンスの管理 、272
インポートとエクスポート、データベース レコード、91

え

エージェント ホスト 、53
PASSCODE の設定 、235
エージェント ホスト レコード 、54
オープン 、63
拡張データの変更 、55
グループのアクティブ化 、120
構成 、231
サーバとの通信 、217
作成 、54
自動登録 、54、64、217
自動負荷分散処理 、24、67
追加 、54
名前または IP アドレスの変更 、253
複数の IP アドレス 、253
変更 、54
ユーザとグループの非アクティブ化 、119
ユーザのアクティブ化 、119
リモート ユーザのアクティブ化 、79
リモート レルムでの重複レコードの作成 、79
レコード 、54
レルム間認証 、79
エージェント ホスト / サーバ
アーキテクチャ 、23
エマージェンシー PASSCODE 、61
エマージェンシー アクセス、テンポラリ パスワード、19
エマージェンシー コード 、61
必要になる状況 、60
エマージェンシー トークンコード 、61
エラー メッセージ 、293

お

オープン エージェント ホスト 、63
オフライン認証
エージェントごとの設定 、59
システム レベルでの設定 、57
設定 、57

か

外部 4GL プロシージャ
実行 、100、148
拡張データ
トークン 、117
変更 、55
拡張データ、変更 、147
グループ 、118
サイト 、131
システム 、209
ユーザ定義 、98
ログ 、99
拡張データ、ユーザ定義データの変更 、146
拡張データ レポート
作成 、163
内容 、164
カスタム クエリ 、187
CSV、HTML、または XML の出力形式 、202
DATE 関数 、197
GROUP BY 句 、195
HAVING 句 、195
LENGTH 関数 、197
Query Wizard 、190
SELECT ステートメントの構文 、192
SQL 構文と記述方法 、191
WHERE 検索条件 、195
アドミニストレーション スコープ 、200
基本的な使い方 、188
共有クエリの保存場所 、204
クエリの ON 検索条件 、194
クエリの ORDER BY 句 、195
クエリのアクセス レベル 、201
クエリの新規作成 、190
クエリの編集 、190
クエリの保存方法 、203
グローバル定数 、200
サンプル クエリ、使用 、189
条件句 、198
テーブルの結合 、193
テーブルの結合、推奨される運用方法 、203
トラブルシューティング 、205
引数 、197
複数のレルム間で管理 、205
メイン ダイアログ ボックス 、189
レプリカで実行 、204
論理演算子 、196
カスタム クエリの SQL 構文 、191
カスタム クエリのアドミニストレーション スコープ 、200
カスタム レポート
作成 、172、174、182、184
ログ エントリ レポート 、173、183
カタカナ
漢字への変換 、37
入力可能なデータ フィールドへの入力 、37

監査証跡レポート
作成 、158
種類 、156
書式設定 、159
制約事項 、157
ログ レコードの内容 、155
漢字
ひらがなとカタカナからの変換 、37
管理者の認証方式
Quick Admin 、48

き

旧バージョンのエージェント
アクティング マスタ / スレーブ サーバの割り当て 、234
アクティング マスタ / スレーブの割り当て 、250
サーバの識別 、234
共有クエリ 、204

く

クエリ、「カスタム クエリ」を参照
クエリの DATE 関数 、197
クエリの GROUP BY 句 、195
クエリの HAVING 句 、195
クエリの IF-THEN-ELSEIF-ELSE 条件句 、198
クエリの JOIN 句 、193
クエリの LENGTH 関数 、197
クエリのアクセス レベル 、201
クエリのグローバル定数 、200
クエリの条件句 、198
クエリのテーブルの結合
推奨される運用方法 、203
クエリの引数 、197
クライアント、「エージェント ホスト」を参照 、53
グループ
アクセス時間の設定 、120
エージェント ホスト上でのアクティブ化 、120
エージェント ホスト上での非アクティブ化 、120
作成 、117
使用する利点 、117
使用の制限 、117
使用例 、118
編集 、117
メンバーシップ リスト 、118
グループ拡張データ
変更 、118
グループの非アクティブ化 、120
グループ メンバーシップ リスト 、118

け

言語サポート
Latin-1 、35
アジア言語 、35
システムの設定 、35

こ

攻撃回避
RSA Authentication Manager の機能 、18
機能の要約 、126
トークンの New PIN モードへの設定 、127
トークンの使用 、123
盗まれた PIN 、125
攻撃者、システムの防御 、17
攻撃者からのボウギョ 、17
構成情報
RSA Authentication Manager 、230
sdconf.rec ファイル 、220
暗号の種類 、231
構成ファイル
更新済みファイルの配布 、251
内容 、244
変更 、247
構成ファイルの更新、配布 、236

さ

サーバ名、変更時の注意 、233
サービス 、275
Windows および UNIX 、275
Windows のみ 、279
サービス コントロール マネージャ 、279
ネットワーク ポート 、275
サイト、作成と変更 、130
サイト拡張データ、変更 、131

し

式 、192
時刻
シンクロナイゼーションとトークン コードの生成 、16
正確な設定を維持する重要性 、16
システム拡張データ
変更 、209
編集 、209
システム クロック
不正確なクロックによって発生する認証の問題 、288
システム ログ、サーバ イベントの監視 、166
実装手順
RSA Authentication Manager 、35
自動登録 、64
DHCP 、66
エージェント ホストに対して有効にする 、54
種類 、61
承認手順、セキュリティ機能の補足のためのカスタマイズ 、209

書式設定、レポート 、159

す

スレーブ Authentication Manager
　データベース ファイルの圧縮 、134

せ

制限されたエージェント ホスト
　リモート ユーザのアクティブ化 、79
世界協定時 (Coordinated Universal Time) 、16
セキュリティ
　攻撃回避機能 、18、126
　攻撃者からの防御 、17
　データの暗号化 、19
　ユーザのアカウンタビリティ 、17
　ユーザの責任 、121

そ

ソフトウェア トークン 、15

た

ダイアログ ボックス
　[Administrator Authentication] 、41
　[Authorization Information] 、211
　[Configuration Management] 、228
　[Create a New Report] 、184、185
　[Edit Log Extension Data] 、99、147
　[Log Messages Histogram Builder] 、185
　[Log Messages Report Builder] 、173、183、184
　[Report Format] 、159
　[Report Selection Criteria] 、160、163
　[Run External Procedure] 、100、148
　Security Dynamics、[RSA Authentication Manager Reports] 、169、179
　[Select Report Type] 、172、182
　[Select Server to Administer] 、41
　[Token Statistics Report Builder] 、175、185
　[User Information] 、177、187
　システム パラメータ 、207
タスク リスト、アドミニストレーション権限 、30

て

ディスク領域
　再利用 、85、133
　要件 、85、133
データの暗号化、保護されるもの 、19
データベース
　圧縮 、85、133
　バックアップと復元 、86、87、88、89、134、135、136、137
　復元 、89、92、137
　メンテナンス、「データベースのメンテナンス」を参照 、133
　レプリケーション 、21
データベースのメンテナンス 、85、133
　4GL プロシージャの実行 、100、148
　ディスク領域 、85、133
　ディスク領域の再利用 、85、133
　データベースのバックアップと復元 、137
　バックアップ、RSA Authentication Manager のデータ 、86、134、135、136
　　RSA Authentication Manager が実行されていない場合 、87
　　RSA Authentication Manager が実行されている場合 、88
　　データの復元 、90
　　データベースの復元 、89
　ユーザ定義データ 、98、146
　　変更 、99
　ユーザ定義データの変更 、147
　ログ データベース 、151、152、153
データベース ブローカ、停止 、229
データベース レコード、インポートとエクスポート 、91
テーブルの結合 、193
テンポラリ パスワード 、124
　エマージェンシー アクセス 、19

と

同期 、128
　トークンの同期のとり直し 、128
統合されたログの記録 、32
トークン 、14
　128 ビット アルゴリズム 、14
　64 ビット アルゴリズム 、14
　AES 、14
　PIN に関するオプション 、103
　PIN を必要としないトークン 、105
　SID 、14
　エクスポート 、113
　拡張データの変更 、117
　コードの生成とタイム シンクロナイゼーション 、16
　ソフトウェア 、15、114
　ソフトウェア トークンの再発行 、115
　ソフトウェア トークンの失効 、115
　ソフトウェア トークンの発行 、115
　タイム シンクロナイゼーション 、128
　同期のとり直し 、128
　盗難 、122
　トークン リスト レポート 、171、181
　複数
　　不正ログイン カウント 、123
　紛失 、122
　　テンポラリ パスワードの代替使用 、124
　無効化、自動 、122
　無効化、手動 、122

ユーザ パスワード、15
割り当て、114
割り当ての解除、121
割り当ての制限、15
トークンコード、14
トークン統計レポート、175、185
トークンのエクスポート、113
トークンの同期のとり直し、128
トークンの無効化
自動、122
手動、122
トークンの割り当て、114
トークンの割り当ての解除、121
トークン リスト レポート、171、181
トークン レコード
共有、113
内容、115
表示されない内容、116
トラブルシューティング
Quick Admin、51
エラー状況、286
ログイン試行の失敗、295

に

日本語
1 バイト フィールドへの入力、38
RSA Authentication Manager データベースのフィールドへの入力、36、37
ひらがなとカタカナから漢字への変換、37
認証、14
Quick Admin 管理者、48
エージェントとサーバ間のダイアログ、216
サービス、213
テンポラリ パスワードによるエマージェンシー アクセス、124
二要素、14
問題、最小限に抑える、121
リモート、38
New PIN モード、42
チャレンジ、40、41
ネクスト トークンコード モード、41
レルム間、79

ね

ネットワーク タイム プロトコル、16
ネットワーク ポート、275

の

ノード シークレット、19、217
エージェント ホストとサーバの通信、222
エラー メッセージ、297、328、363
自動配布、222
手動配布、223
送信、222
ログ メッセージ、363

は

ハードウェア障害の発生後にデータベースを復元、92
ハードウェア トークン、配布、120
パスワード、テンポラリ、124
バックアップ、RSA Authentication Manager、86、134、135、136
RSA Authentication Manager が実行されていない場合、87、90
RSA Authentication Manager が実行されている場合、88

ひ

ヒストグラム レポート、170、180
作成、173、174、183、184
評価用ライセンス、28
パーマネント ライセンスへの変換、401
標準レポート、170、180
[Run List]、170、180
トークン リスト、171、181
ひらがな
漢字への変換、37
入力可能なデータ フィールドへの入力、37

ふ

ブール演算子、196
複数のトークン、不正ログイン カウント、123
複数のネットワーク インタフェース
認証 (UNIX)、261
認証 (Windows)、237
複数のネットワーク インタフェース カード
システムの構成 (UNIX)、261
システムの構成 (Windows)、237
認証 (UNIX)、261
認証 (Windows)、237
プライマリ Authentication Manager、21
データの復元、139
データベース ファイルの圧縮、85、134
プライマリ サーバ
データの復元、91
名前または IP アドレスの変更 (UNIX)、259
プライマリ サーバとレプリカ サーバの識別、234
プライマリ サーバとレプリカ サーバの調整、223
プロセス、275、278
Windows および UNIX、278

へ

ベース ライセンス、28

ほ

ポート番号 、275
ホーム レルム 、25
ホストの名前と IP アドレス 、233
　指定 、253
ホスト名とサービス名の解決 、233

ま

マップ ファイル、LDAP 、108

め

メイン メニュー
　RSA Authentication Manager Host Mode 、35
メッセージ 、293
メッセージの ID 番号 、401
メニュー
　[Log] 、282
　RSA Authentication Manager Host Mode 、35
　レルム 、84

も

問題の解決
　External Authorization のタイムアウト 、292
　LDAP 同期 、291
　サーバのダウン 、291
　ネットワーク接続の切断 、291

ゆ

ユーザ
　アカウンタビリティの監査 、17
　アクティブ 、271
　エージェントでの非アクティブ化 、119
　エージェント ホスト上でのアクティブ化 、119
　責任 、121
　ユーザ レコード 、113
ユーザ、リモート
　レコードの自動作成 、79
　レコードの手動作成 、79
ユーザ定義の拡張データ 、98、146
　変更 、99、147
ユーザとグループのアクティブ化
　エージェント ホスト 、120
ユーザの責任 、121
ユーザ パスワード
　テンポラリ 、124
ユーザ パスワード トークン 、15
ユーザ レコード
　作成 、105
　内容 、113
　変更 、105

ら

ライセンス 、28、271
　アクティブ ユーザ 、271
　アドバンスド ライセンス 、272
　種類 、28
　制限の管理 、272
　ベース ライセンス 、271
　ライセンスのアップグレード 、274
　ライセンの種類 、271
　レルム間環境 、274
ライセンス情報 、229
　license.rec ファイルの内容 、221
　ライセンス レコードの更新 、243
ライセンス データ
　UNIX 構成レコード 、244
ライセンスのアップグレード 、274
ライセンスのバージョン 、272
ライセンス フロッピー ディスク 、229
ライセンス レコード、更新 、243
ライブラリ パス、LDAP 比較ユーティリティの設定 、108

り

リプレイ アタック 、18
リモート エイリアス、レルム間認証 、80
リモート管理者
　認証プロセス 、40、41
リモート ユーザ
　レコードの自動作成 、79
　レコードの手動作成 、79
リモート レルム 、25

れ

レプリカ
　削除 、257
レプリカ Authentication Manager 、21
　データの復元 、138
レプリカ管理ユーティリティ (UNIX) 、255
　エイリアス IP アドレスの割り当て 、265
　サーバ情報の表示 、258
　サービス名またはサービス ポート番号の変更 、266
　スタートアップ遅延時間の変更 、266
　名前または IP アドレスの変更 、266
　レプリカ情報の変更 、266
　レプリカの削除 、257
　レプリカの追加 、265
レプリカ管理ユーティリティ (Windows) 、239
レプリカ管理ユーティリティの起動 、255
レプリカ サーバ
　UNIX における管理 、255
　イベント ログの例 、285
　クエリの実行 、204
　クロックの設定エラー 、345
　情報の表示 、240
　データの復元 、90

レプリカの削除 、257
レプリカ パッケージ 、22
レプリケーション間隔 、21
レポート 、155
　拡張データ 、163
　カスタム 、170
　監査証跡、「監査証跡レポート」を参照
　コマンド ラインから実行 、177、187
　作成 、158
　種類 、155
　書式設定 、159
　内容の指定 、159
　標準、「標準レポート」を参照
　ファイルに出力 、162
　ユーザ情報の表示 、176、186
　ログ モニタ、「ログ モニタ レポート」を参照
レポート作成ユーティリティ 、169、178
　UNIX インタフェースの基本操作 、178
　インストール 、169、179
　カスタム 、170
　起動 、169、179
　実行するレポートの選択 、170、180
　実行するレポートのリストの保存 、170
　出力ファイル 、171、182
　停止 、169、180
　標準 、170
　標準レポート、「標準レポート」を参照
レルム 、25、83
　ステータスの判断 、214
　追加 、84
　ホーム 、25
　メニュー 、84
　ライセンス フロッピー ディスク 、229
　リモート 、25
レルム間アドミニストレーション、「エンタープライズ認証」を参照
レルム間認証 、79
　計画 、81
　デフォルト ログイン 、80
　リモート エイリアス 、80
　リモート ユーザ、レコードの自動作成 、79
　リモート ユーザ、レコードの手動作成 、79
レルム間モデル 、25
レルム シークレット 、19
　再設定 、330
　設定されていない 、362

ろ

ログ アーカイブ ファイル、使い方 、167
ログイン試行の失敗 、295
ログイン パスワードの統合 、57
　エージェントごとの設定 、59
　システム レベルでの設定 、59
ログ拡張データ 、98、146
　編集 、99、147
ログ データベース
　一定割合によるログ レコードの削除 、152
　自動メンテナンスのスケジューリング 、153
　データベース統計情報の表示 、151
　日付と時刻によるログ レコードの削除 、152
　ログ アーカイブ ファイルの形式 、167
　ログ レコードの削除 、152
ログの記録、統合 、32
ログ フィルタリング 、154
ログ メッセージ
　イベント ログ 、281
ログ モニタとレポート作成 、164
ログ モニタ レポート 、164、165
　ライブ レポート ウィンドウ 、165
ログ レコード
　削除 、152
　内容 、155
ロック マネージャ 、18
論理演算子 、196