RSA Authentication Manager 6.1 for UNIX
インストール 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 for UNIX Installation 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-6102

目次

はじめに

本書では、RSA Authentication Manager 6.1 for UNIX をインストールする手順について説明します。

対象となる読者

本書は、UNIX セキュリティ システム管理者を対象としています。RSA Authentication Manager ソフトウェアをインストールする管理者は、UNIX、Authentication Manager プラットフォーム、オペレーティング システムのバージョン、およびシステム周辺機器について理解している必要があります。

ディレクトリ名

このマニュアルでは、次の規則に基づいて特定のディレクトリ名を表記しています。

マニュアル内での表記	定義	実際のディレクトリ パス
ACEDATA	RSA Authentication Manager データ ディレクトリ	**¥RSA Authentication Manager¥data**
ACEDOC	RSA Authentication Manager ドキュメント ディレクトリ	**¥RSA Authentication Manager¥doc**
ACEPROG	RSA Authentication Manager プログラム ディレクトリ	**¥RSA Authentication Manager¥prog**

マニュアル

RSA Authentication Manager for UNIX、RSA Authentication Manager for Windows 2000、および RSA Authentication Manager for Windows 2003 は 1 枚の CD-ROM で提供されます。CD-ROM には、次のものも含まれています .

- Windows 2000 および Windows 2003 で稼動する RSA Authentication Manager Remote Administration のオンライン ヘルプ (英語版)
- UNIX、Windows 2000、および Windows 2003 用の英語版ドキュメント ファイル (PDF 形式)

RSA Authentication Manager 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『RSA Authentication Manager 6.1 Getting Started』を参照してください。

PDF ファイルで提供されるマニュアル

次のいずれかの場所にある PDF ファイルを印刷して使用できます。

- RSA Authentication Manager CD-ROM の ¥auth.mgrdoc
- ハードディスク ドライブの RSA Security¥RSA Authentication Manager¥doc ローカル ディレクトリ (インストール プロセスでマニュアルのインストールを選択した場合)

メモ：認証手順のテンプレートが Microsoft Word (.doc) ファイルで提供されます。このファイルは必要に応じて変更し、エンド ユーザに渡すことができます。Microsoft Word を使用できない環境では、PDF 形式の認証手順を配布してください。

RSA SecurID Authenticator SID800 を導入する場合、エンド 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。

セキュリティ上の理由から、プラットフォームに対応する最新版の Adobe Reader は、**www.adobe.com** で入手してください。

RSA Authentication Manager マニュアルの構成

インストール時に、英語版マニュアルの PDF ファイルを CD-ROM からハード ディスク ドライブにコピーできます。この場合、英語版マニュアルは、RSA Authentication Manager インストール ディレクトリの下にある ***ACEDOC*** サブディレクトリにコピーされます。マニュアルをインストールしなくても、RSA Authentication Manager CD-ROM のトップレベルにある **aceservdoc** ディレクトリから、いつでもマニュアルにアクセスできます (日本語版マニュアルは、日本語ドキュメント CD-ROM にあります)。

ヘルプ

RSA Authentication Manager 6.1 は詳細なヘルプ システムを備えており、UNIX システム上で動作している RSA Authentication Manager を管理するために、Windows システムでリモート アドミニストレーションを実行するときに使用できます。ヘルプには次のいずれかの方法でアクセスできます。

- 各ダイアログボックスの [Help] ボタンをクリックする方法
- RSA Authentication Manager Host Mode の [Help] メニューの [Help for Database Administration] を選択する方法

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ます。

電話をかけるときは、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。UNIX プラットフォームで「sdinfo」と入力して、この番号を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。
- 名前解決サービス (DNS など) の有無。

1 RSA Authentication Manager の要件

RSA Authentication Manager 6.1 ソフトウェアをインストールするシステムの要件を確認するには、この章を参照してください。システムは、この章に示されているソフトウェア、ハードウェア、および構成の要件を満たしている必要があります。

システムが要件を満たしていない場合は、RSA セキュリティ正規販売代理店にご連絡ください。

ライセンスの種類

RSA Authentication Manager では、インストール時と日常の操作や管理作業でベース ライセンスとアドバンスド ライセンスの制限が適用されます。どちらのライセンスもパーマネント ライセンスです。

ベース ライセンス

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。
- 1 台のプライマリ Authentication Manager と 1 台のレプリカ Authentication Manager 構成を 1 つ (1 レルム) 稼動できます。

アドバンスド ライセンス

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。

ライセンスとアクティブ ユーザの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

インストールの要件

このセクションでは、新規インストールおよびアップグレードの要件について説明します。示されている**最低限**の要件をシステムが満たす場合のみ、項目の横にチェックマークを記入してください。チェックマークを記入できない項目がある場合は、RSA Authentication Manager ソフトウェアのインストールを行わないでください。

サポートされるプラットフォームとハードウェア

RSA Authentication Manager を実行するには、以下のいずれかのバージョンの UNIX オペレーティング　システムが必要です。以下のプラットフォーム以外に RSA Authentication Manager 6.1 ソフトウェアをインストールした場合、RSA セキュリティはサポートを提供できません。

- ❑ PA-RISC 2.x プロセッサで動作する HP-UX 11i
- ❑ PowerPC および RISC/6000 プロセッサで動作する IBM AIX 5L v 5.2
- ❑ UltraSparc プロセッサで動作する Solaris 9
- ❑ Red Hat Enterprise Linux 3.0

プラットフォームに関する情報を表示するには、**uname -a** コマンドを使用します。

システム パッチ

次のシステム パッチをインストールする必要があります。

- ❑ HP-UX 11i：**BUNDLE 11i** (B.11.11.0306.1) および **GOLDBASE11i** (B.11.11.0412.5)
- ❑ IBM AIX 5L v 5.2：APAR IY 44173
- ❑ Red Hat Enterprise Linux 3.0:Legacy Software Development -- Red Hat Enterprise Linux 3.0 CD-ROM にある Red Hat Package Manager からアクセス可能

高可用性

RSA Authentication Manager 6.1 は、Solaris 9 上の Veritas Cluster Server で高可用性機能をサポートすることが確認されています。

ディスク容量

インストールを開始する前に、次に示す必要な容量を確保してください。システムの空きディスク容量が十分でない場合は、インストールの処理が終了します。**/ace** ディレクトリまたは **/ace_tmp** ディレクトリを別のファイル システムとしてマウントしても、必要なディスク容量を削減することはできません。

- ❑ RSA Authentication Manager ファイルをインストールするには、400 MB のディスク容量が必要です。
- ❑ プロセッサあたり 128 MB の物理メモリの他に、1,000 ユーザあたり 1 MB の物理メモリが必要です。
- ❑ RSA Authentication Managerデータベースの増大に備えて、1,000ユーザあたり 1 MB の空きディスク容量を確保しておく必要があります。
- ❑ ログ データベースの増大に備えて、1 GB を確保しておく必要があります。
- ❑ スワップ ファイルは、物理メモリの 2 倍以上の大きさが必要です。

ドライブ

- RSA Authentication Managerソフトウェア CD-ROMおよびライセンスCD-ROMをマウントできる CD-ROM ドライブが必要です。NFS 機能を使用してアクセスできるワークステーションに、ローカル CD-ROM ドライブを接続して使用することもできます。

  RSA Authentication Manager ソフトウェア配布メディアをマウントする CD-ROM ドライブは、CD-ROM を読み取るワークステーションと互換性があることが必要です。また、ドライブのデフォルトのアクセス権が変更されないようにしなければなりません。

ホスト名

- NIS や DNS などのネーム サーバを使用している場合、プライマリとレプリカのプライマリ ホスト名 (**ブート名**とも呼びます) は、次の条件を満たしている必要があります。
  - マシンのエイリアス リストでファースト ネームとして登録されている必要があります。また、マシンのエントリには、IP アドレスに続けて完全修飾名 (FQDN) が指定されている必要があります。
  - マルチホーム マシンの場合は、ホスト名がプライマリ ネットワーク インタフェース カードに対応している必要があります。

カーネル構成

- システムのカーネル構成値が、付録 B「カーネル パラメータの変更」に示されている最小値以上であることを確認します。カーネルの設定を変更する場合は、システムで動作しているすべてのアプリケーションを停止します。設定値が最小値を下回る場合は、カーネル構成を変更してください。パラメータ名では大文字と小文字が区別されるので、名前の指定や検索では、表に**示されているとおり**の名前を使用してください。

インストールに関する重要なガイドライン

- プライマリ マシンとレプリカ マシンは、RSA Authentication Manager 専用として使用することをお勧めします。
- Authentication Manager マシンはセキュリティが確保されている場所に設置し、信任された人だけがアクセスできるようにしてください。
- 各 Authentication Manager マシンの名前は、ネットワーク上の完全修飾コンピュータ名 (ドメイン名付きのマシン名) でなければなりません。
- 同じ物理プラットフォームで複数のRSA Authentication Managerを実行しないでください。
- RSA Authentication Manager ソフトウェアをネットワーク ドライブにインストールしないでください。
- パス名に空白文字を含むディレクトリにRSA Authentication Managerソフトウェアをインストールしないでください。空白文字が含まれていると、インストールが失敗します。
- インストールの前に、ファイルのバックアップ コピーを作成してください。オリジナルのライセンス ファイル、トークン シード レコード ファイル、RSA Authentication Manager 6.1 CD-ROM をはじめ、作成したすべてのコピーを安全な場所に保管してください。

複数のレルムのマージ

複数のレルムのデータベースを 1 つの 6.1 レルムにマージ (結合) するには

1. 1 つのレルムを RSA Authentication Manager 6.1 にアップグレードします。
2. ダンプ ユーティリティとロード ユーティリティ(**sddump** と **sdload**) を使用して他のレルムのデータベースをダンプし、6.1 データベースにマージします。

詳細については、付録 D「データベース ユーティリティ」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 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。時刻の設定に 1 分を超えるずれが生じると、認証が失敗します。

プライマリ RSA Authentication Manager 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 : タイム シンクロナイゼーションが正しく動作するためには、必要に応じて時刻をリセットできるように、プライマリとレプリカの RSA Authentication Manager プロセスが root 権限で動作している必要があります。

インストール前のチェックリスト

RSA Authentication Manager ソフトウェアをインストールする前に、日本語マニュアル CD-ROM の『Readme』(英語版は **authmgr_readme.pdf**) をお読みください。『Readme』には、RSA Authentication Manager 6.1 の構成およびインストールに関する重要な情報が記載されています。また、標準ドキュメントへの記載が間に合わなかったソフトウェアの問題についても説明しています。

RSA Authentication Manager ソフトウェアをインストールする場合は、次のチェックリストを使用して、インストールに必要なすべてのハードウェア、ソフトウェア、および情報が揃っていることをあらかじめ確認してください。

次の CD-ROM とフロッピー ディスクが必要です。

- ❑ RSA Authentication Manager CD-ROM。
- ❑ ライセンス CD-ROM。

重要 : インストールを開始する前にライセンス ファイルのコピーを作成しておき、オリジナルのファイル、トークン シード レコード ファイル、RSA Authentication Manager 6.1 CD-ROM をはじめ、作成したすべてのコピーを安全な場所に保管してください。また、ライセンスのバックアップ コピーは、RSA Authentication Manager ソフトウェアをインストールした**後**に作成する必要があります。ライセンス ファイルは、インストール中に変更されます。このため、***ACEDATA*** ディレクトリ内のライセンスが失われたり、破損した場合、オリジナルのライセンス ファイルを使用しても、データベースにアクセスすることはできません。データベースにアクセスするには、変更されたライセンス ファイルを使用するしか方法がありません。

- ❑ トークン レコード ファイル (トークンを新規購入した場合)。

メモ : RSA SecurID トークンを新規購入されたお客様へは、1 つ以上の ASCII ファイルまたは XML ファイルに保存されているトークン シード レコードを登録した DOS ファイルが提供されます。トークン レコード ファイルが RSA Authentication Manager パッケージで提供されることはありません。

次のものおよび情報が必要です。

- ❑ この章で説明しているハードウェア、ディスク容量、メモリ、およびプラットフォームの要件をすべて満たすマシン。
- ❑ マシンの Administrator (root) 権限。

  sdsetup ユーティリティを使用して実行するインストール作業および構成作業には、root 権限が必要です。
- ❑ レプリカをインストールする予定のレプリカの名前と IP アドレス。
- ❑ プライマリをインストールした後にレプリカを定義する必要があります。レプリカ (購入したライセンスの種類に応じて最大 10 個) は、レプリカ管理ユーティリティ (**sdsetup -repmgmt**) を使用して追加できます。実際に使用するコマンドについては、本書の該当する章にその手順が説明されています。レプリカ管理ユーティリティの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。
- ❑ レプリカ パッケージをレプリカに配布する方法。

  レプリカ パッケージをレプリカに配布するには、2 種類の方法があります。

  – プライマリ上で Push DB Assisted Recovery 機能を有効にします。レプリカをインストールして起動した後に、レプリカ パッケージがレプリカに送信されます。
  – Push DB 機能を無効にして、レプリカ パッケージを作成します。作成したレプリカ パッケージをレプリカに手動でコピーして、レプリカをインストールします。

    Push DB 機能を無効にする方法の詳細については、94 ページの「データベース プッシュの無効化」を参照してください。

インストール前の操作

特に指示のない限り、RSA Authentication Manager ソフトウェアを実行するすべてのマシンで各操作を実行します。説明がわかりにくい場合や、示されている操作を実行できない場合は、操作を中断して RSA セキュリティ正規販売代理店にご連絡ください。

RSA Authentication Manager をインストールする前に、次の操作を実行します。

1. ターゲット マシンの完全なシステム バックアップを作成します。現在の完全なシステム バックアップを作成しておけば、万一データ損失が発生しても、問題に対処できます。アップグレードを実行する場合は、バックアップを作成する前にすべての RSA Authentication Manager プロセスを停止してください。レポート作成ユーティリティを停止するには、次のコマンドを入力します。

   ```
   ACEUTILS/rptconnect stop
   ```

   RSA Authentication Manager サービスとデータベース ブローカを停止します。次のコマンドを入力します。

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```

2. Authentication Manager のシステム時刻を設定します。RSA Authentication Manager が正しく動作するためには、システム時刻が正確であることが重要です。
   - **新規インストールの場合**は、Authentication Manager のシステム時刻を、(世界協定時) ＋ (サーバが設置されている場所のタイム ゾーンのオフセット) で求められる時刻に設定します。日本時間は時報で確認してください。
   - **アップグレードを実行していて、ターゲット マシンが既存の Authentication Manager マシンでない場合**は、ターゲット マシンの時刻を既存の Authentication Manager の時刻に一致させます。時刻が既存の Authentication Manager の時刻と一致していないと、一部またはすべてのトークン保持者のアクセスが拒否される可能性があります。

3. RSA Authentication Manager サブディレクトリ、データベース、およびプログラム ファイルがすべてインストールされるパーマネント RSA Authentication Manager トップレベル ディレクトリを作成します。アップグレードを実行している場合は、既存のトップレベル ディレクトリを使用します。

   RSA Authentication Manager トップレベル ディレクトリは次の条件を満たしている必要があります。
   - すべての RSA Authentication Manager ファイルを格納し、データ ファイルの増大にも対応できるだけの十分なディスク容量を備えている。
   - NFS などを介してネットワークから利用できるパーティション上にない。

4. RSA Authentication Manager のサービス名とポート番号を **/etc/services** に追加します。これらのエントリがまだ指定されていない場合は、次の行を **/etc/services** に追加します。すべてのサービスをすぐに使用しない場合でも、エントリをここで追加しておくとよいでしょう。

```
securid         5500/udp
securidprop_00 5505/tcp
securidprop_01 5506/tcp
securidprop_02 5507/tcp
securidprop_03 5508/tcp
securidprop_04 5509/tcp
securidprop_05 5510/tcp
securidprop_06 5511/tcp
securidprop_07 5512/tcp
securidprop_08 5513/tcp
securidprop_09 5514/tcp
securidprop_10 5515/tcp
sdlog           5520/tcp
sdserv          5530/tcp
sdreport        5540/tcp
sdadmind        5550/tcp
sdlockmgr       5560/tcp
sdcommd         5570/tcp
sdoad           5580/tcp
tacacs          49/tcp      #TACACS+
```

上の値は v6.1 のデフォルト値です。このとおりに指定する必要はありません。ただし、次の条件を満たしている必要があります。

- レプリケーション サービスのサービス名は、認証サービス名に “prop” を付けた名前でなければなりません。たとえば、認証サービス名が **securid** の場合は **securidprop** になり、**auth** の場合は **authprop** になります。

  デフォルトでは、**sdsetup -repmgmt** ユーティリティを使用してシステムにレプリカを追加するときに、レプリカにレプリケーション サービス名とポート番号が割り当てられます。デフォルトのポート番号は 5506 から始まります。5505 はプライマリに割り当てられます。デフォルトのポート名には 2 桁の数字が追加されます。このため、プライマリが **securidprop_00** の場合、システムに追加された最初のレプリカは**securidprop_01**になります。同じ名前とポート番号を、プライマリとすべてのレプリカ上の **services** ファイルに追加する必要があります。

- UNIX サーバと、そのサーバを管理する Windows マシンは、**sdlog**、**sdserv**、および **sdadmind** に、同じサービス名とポート番号のエントリが登録されている必要があります。

デフォルトのサービス名とポート番号を使用しない場合は、『RSA Authentication Manager 6.1 管理者ガイド』の付録 F「RSA Authentication Manager の構成 (UNIX)」の説明に従ってこれらのパラメータを変更し、Authentication Manager の **/etc/services** ファイルに適切なエントリを作成する必要があります。

5. Authentication Manager のホスト名を **hosts** ファイルに追加します。**/etc/hosts** 内のプライマリとレプリカのエントリを確認します。エントリがない場合は追加します。レプリカを後で追加する場合は、現時点でそのホスト名が **hosts** ファイルに登録されていなくてもかまいません。**hosts** ファイル内のエントリの要件については、13 ページの「ホスト名」を参照してください。

DNS がある場合は、**hosts** ファイルに Authentication Manager の名前を登録する必要はありませんが、リバース ルックアップが有効でなければなりません。コマンド プロンプトに対して、「nslookup ***machine name***」と入力します。マシンの IP アドレスが返される場合は、**hosts** ファイルに Authentication Manager の名前を追加する必要はありません。

6. RSA Authentication Manager 管理者を指定します。RSA Authentication Manager 管理者で構成される UNIX グループを作成します。このような UNIX グループがない場合は、**/etc/group** ファイルを編集してグループを作成し、そのグループのすべてのメンバを RSA Authentication Manager 管理者として Authentication Manager データベースに登録します。RSA Authentication Manager ファイルのアクセス権を適切に設定するには、このような UNIX グループを作成する必要があります。

7. RSA Authentication Manager ファイル オーナを指定します。

   指定したファイル オーナは、インストール時に、唯一の RSA Authentication Manager 管理者としてデータベースに追加されます。Authentication Manager 管理者で構成される UNIX グループのメンバの 1 人を、すべての RSA Authentication Manager ファイルのオーナとして選択します。このアカウントのプライマリ UNIX グループ ID (GID) が、前のステップで作成した管理者で構成される UNIX グループの ID であることを確認します。

   ローリング アップグレードを実行している場合は、ファイル オーナは既に選択されています。ここで別のファイル　　オーナを選択する必要はありません。Authentication Manager の現在のファイル オーナを確認するには、Authentication Manager 上で **sdinfo** を実行します。別のファイル オーナを選択する場合は、管理者で構成される UNIX グループのメンバの 1 人を選択します。選択するメンバは、レルム管理者として RSA Authentication Manager データベースに既に登録されている必要があります。

8. Authentication Manager の **/etc/passwd** ファイルに RSA Authentication Manager ファイル オーナのエントリがあることを確認します。そのアカウントのエントリがない場合は追加します。

9. カーネル パラメータの値が、付録 B「カーネル パラメータの変更」に示されている要件を満たすように構成されていることを確認します。

次のステップ

次のいずれかの操作を実行します。

- この章に示した要件をシステムが満たしていない場合は、ただちに操作を**中止**してください。第 2 章「RSA Authentication Manager のインストール」には進まずに、RSA セキュリティ正規販売代理店にご連絡ください。
- インストール前の操作が正しく終了し、RSA Authentication Manager の新規インストールを実行する場合には、その操作手順について、第 2 章「RSA Authentication Manager のインストール」を参照してください。
- インストール前の操作が正しく終了し、RSA ACE/Server 5.1 または 5.2 からのアップグレードを実行する場合は、第 3 章「RSA Authentication Manager へのアップグレード」を参照してください。

2 RSA Authentication Manager のインストール

プライマリ Authentication Manager とレプリカ Authentication Manager に RSA Authentication Manager ソフトウェアをインストールし、インストール後の操作を実行するには、この章で説明する手順を実行してください。

プライマリ ソフトウェアのインストール

このセクションのインストール手順では、Authentication Manager ワークステーションで RSA Authentication Manager 6.1 CD-ROM (RSA Authentication Manager ソフトウェアとライセンス) をマウントできることを前提にしています。インストール先の Authentication Manager ワークステーションにローカル CD-ROM ドライブがない場合は、NFS機能を使用してCD-ROMドライブ マウント ポイントをAuthentication Manager ワークステーションにエクスポートすることで、ドライブをマウントし、CD-ROM からインストールできます。また、CD-ROM の適切なディレクトリをワークステーションのディレクトリにコピーして、そのディレクトリからインストールすることもできます。

プライマリ ソフトウェアをインストールするには

1. 目的のプライマリに **root** でログオンします。
2. アップグレードを実行している場合は、ステップ 3 に進みます。新規インストールの一部としてプライマリをインストールする場合は、次のファイルをライセンス CD-ROM からワークステーションのインストール ディレクトリにコピーします。

   license.rec

   server.cer

   server.key

   sdti.cer

   ファイル名は、**すべて小文字**で指定する必要があります。

   ステップ 3 をスキップしてステップ 4 に進みます。
3. 次のいずれかの手順を実行します。
   - プライマリを同じシステムでアップグレードする場合は、ステップ 2 に示したファイルをカレント ディレクトリに**コピーしないでください**。この処理はアップグレードの中で自動的に行われます。
   - プライマリを新しいシステムでアップグレードする場合は、ステップ 2 に示したファイルを、既存の ***ACEDATA*** ディレクトリからカレント ディレクトリにコピーする必要があります。
4. サーバのトップレベル ディレクトリ以外の場所に、CD-ROM ドライブのマウント ポイント ディレクトリを作成します。

   ```
   mkdir /cdrom
   ```

メモ：カレント ディレクトリが書き込み可能であることを確認します。CD-ROM 上のディレクトリに移動して、RSA Authentication Manager 6.1 ソフトウェアをインストールしないでください。

5. CD-ROM ドライブをマウントします。各オペレーティング システムの **mount** コマンドは、以下の表で確認してください。

OS	コマンド
Solaris と Linux	ボリューム マネージャが CD-ROM を自動的にマウントするので不要です。
HP-UX	実行パスの **/usr/sbin** を使用して、**root** で次のように入力します。 `mount -F cdfs /dev/dsk/c3t2d0 /cdrom`
AIX	`mount -o ro -v cdrfs /dev/cd0 /cdrom`

メモ：CD-ROM のデバイス名は、ホストに応じて異なります。HP-UX システムでは、デバイス名はシステムで使用している CD ドライバに応じて異なります。「unknown command (不明コマンド)」というエラー メッセージが返された場合は、オペレーティング システムのドキュメントを参照してください。

6. **/cdrom/*platform*** ディレクトリを指定します。***platform*** には、使用しているオペレーティング システムの略称を指定します。

OS	プラットフォームの略称	ディレクトリ
Solaris	sol	**/cdrom/*cd_name*/sol**
HP-UX	hp	**/cdrom/hp**
AIX	aix	**/cdrom/aix**
Linux	linux	**/cdrom/linux**

Solaris では、CD-ROM の名前をディレクトリ パスに指定する必要があります。

7. 次のコマンドを入力して、プライマリ Authentication Manager のインストールを開始します。

```
/cdrom/platform/sdsetup -primary[-f fileowner]
[-o yes] [-p path][-r {yes|no}]
```

自動移行アップグレードを実行している場合は、既存の RSA Authentication Manager が格納されているトップレベル ディレクトリからこのコマンドを実行します。

角かっこ内の引数は省略してもかまいません。省略した場合は、インストール時に入力が求められます。斜体の部分には実際の値を指定します。

コマンド ラインにパラメータをすべて指定した場合は、オーダ元の国を選択し、ライセンス契約に同意すると、インストール プログラムが最後まで自動的に実行されます。

引数の指定を一部省略し、インストール プログラムでその値が必要とされる場合は、国を選択し、ライセンス契約に同意した後、値の入力が求められます。各プロンプトに応答しないと、インストールを続行できません。

引数をまったく指定せずに sdsetup primary コマンドを実行した場合は、インストール プログラムの最初の部分が対話形式で実行されます。国の選択とライセンス契約の同意が求められ、設定する必要がある構成値の入力が求められます。表示されるすべての質問に答えると、インストール プログラムが自動的に実行され、終了します。

コマンド ライン引数

-f *fileowner*	Authentication Manager を準備するときに選択したファイル オーナの名前を指定します。
-o yes | no	**ace/prog** サブディレクトリから既存のファイルを削除せずに、再インストールします。**-o yes** を指定すると、インストール プログラムによって **ace** の内容が **ace_tmp** に移動されます。**-o no** を指定すると、インストールは終了します。
-p *path*	Authentication Manager を準備するときに選択または作成した RSA Authentication Manager のトップレベル ディレクトリのパス名を指定します。

コマンド ライン引数の例

RSA Authentication Manager のインストールに備えて適切に準備されている HP システムで次のサンプル コマンドを実行すると、コマンドの後に示した結果が得られます。

```
/cdrom/aceserv/hp/sdsetup -primary -f smith -o yes -p /top -r yes
```

- このサンプル コマンドには、ユーザが入力しなければならない構成パラメータ値がすべて指定されています。ただし、インストール プログラムが必要とする構成情報はこの他にもあるため、次の操作を実行する必要があります。
  - オーダ元の国を選択します。
  - ライセンス契約に同意します。
- RSA Authentication Manager ファイルのオーナは **smith** というユーザです。このため、smith というプライマリ UNIX グループのすべてのメンバに、RSA Authentication Manager プログラムを実行できる権限が与えられます。
- Authentication Manager ファイルはすべて、**/top** のサブディレクトリに格納されます。
- **/top/ace** 内で検出されたファイルは **/top/ace_tmp** に移動されます。このとき、ファイルの移動は通知されません。また、**/top/ace_tmp** 内の既存のファイルは削除されます。削除も通知されません。
- アップグレードで、**/top/ace/data** にデータベース ダンプ ファイルが格納されている場合は、これらのファイルを 6.1 データベースに移行するかどうか確認が求められます。「y」(Yes) または「n」(No) を入力し、ENTER キーを押します。

インストール プロンプト

コマンド ラインに必要な情報が指定されていない場合、インストール プログラムは、プロンプトを表示して入力を求めます。プロンプトは、スタートアップ画面がいくつか表示された後に表示されます。ここでは、表示される順にプロンプトを説明します。

オーダ元の国

RSA Authentication Manager ソフトウェアのオーダ元の国を選択できます。「y」(Yes) または「n」(No) を入力すると、適切なライセンスが表示されます (日本のお客様は「n」を入力してください)。

ライセンス契約

オーダ元の国を選択すると、RSA Authentication Manager ソフトウェアの使用条件が表示されます。「A」と入力して、ライセンス契約に同意します。この条件に同意しないと、インストール プログラムは終了します。

ファイル オーナ

ファイル オーナの入力が求められた場合は、18 ページのステップ 7 で指定したログオン名またはユーザ名を入力します。メッセージに従って、入力した名前を確認します。

パス

Authentication Manager を準備するときに選択または作成した RSA Authentication Manager のトップレベル ディレクトリのパス名を指定します。指定するパスに、すべての Authentication Manager サブディレクトリ、データベース、およびプログラム ファイルが格納されます。

上書き

マシンで既存の RSA Authentication Manager ソフトウェアが検出されると、このプロンプトが表示されます。上書きするには「y」、再指定するには「r」、終了するには「q」を、それぞれ入力します。

ace/data サブディレクトリに RSA Authentication Manager データベースのダンプ ファイルがある場合は、既存のダンプ ファイルを使用してデータベースの移行を実行するのか、現在のデータベースからダンプ ファイルを作成し、そのファイルを使用してデータベースを 6.1 に移行するのか、確認が求められます。「yes」と入力すると、既存のダンプ ファイルを使用してデータベースが作成されます。「no」と入力すると、既存のデータベースからダンプ ファイルが作成され、そのファイルを使用して新しいデータベースが作成されます。既存の RSA Authentication Manager ファイルは **ace_tmp** に移動され、**ace_tmp** の現在の内容に上書きされます。

重要 : ace_tmp に移動されたファイルは、削除したり、別の場所に移動したりできます。**ace_tmp** 内のファイルを移動したり、バックアップを作成したりしないで Authentication Manager ソフトウェアを再インストールまたはアップグレードすると、**ace_tmp** の内容はこのインストールによって上書きされ、永久に失われてしまいます。

アップグレードに関する警告

このプロンプトは、プライマリのアップグレードを実行している場合に表示されます。これは、既存のファイルのバックアップを作成するように、注意を促すためのものです。「o」と入力して、インストールを続行します。

レプリカ

新規インストールの場合は、レプリカを追加し、レプリカ パッケージを作成するかどうか、確認を求められます。アップグレードを実行している場合は、データベース内の既存のレプリカについて、レプリカ パッケージを作成するかどうか、確認を求められます。詳細については、27 ページの「レプリカをサポートするためのシステムの準備」および 28 ページの「データベースへのレプリカの追加」を参照してください。

以前のバージョンからアップグレードしている場合は、データベースにレプリカを追加することもできます。購入したライセンスに応じて、RSA Authentication Manager に設定できるレプリカの個数が異なります。ライセンスの詳細については、11 ページの「ライセンスの種類」参照してください。

プライマリのインストールの終了

インストールが正しく終了すると、メッセージが表示され、Authentication Manager の構成情報とライセンス情報が表示されます。データベース内のユーザやレプリカの数がライセンスの制限を超える場合は、アップグレード違反に関する情報が表示されます。ライセンスの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の第 1 章「概要」を参照してください。

解決できないサービス名についてのメッセージも表示された場合は、**/etc/services** に入力したサービス名が間違っているか (17 ページを参照)、またはデフォルト以外のサービス名を選択した可能性があります。デフォルト以外のサービス名を選択した場合は、Authentication Manager の構成ファイルの変更について、『RSA Authentication Manager 6.1 管理者ガイド』の「RSA Authentication Manager の構成 (UNIX)」の章を参照してください。

インストール後のセットアップ

このセクションでは、インストール後のプライマリについて説明します。また、レプリカに RSA Authentication Manager ソフトウェアをインストールする前に、プライマリ上で実行しなければならない操作についても説明します。

RSA Authentication Manager for UNIX データベースのアドミニストレーションの多くは、Windows マシン上でリモートに実行されます。ただし、UNIX サーバの構成と、一部のセットアップ操作は、UNIX サーバ上で直接実行する必要があります。このセクションでは、このようなセットアップ操作について説明します。

UNIX サーバ上で再構成とアドミニストレーションを行うときのインタフェースは、コマンド ラインと、TTY モード (キャラクタベース) のサーバ アドミニストレーション プログラムに限られます。キャラクタ モードで **sdadmin** を使用したことがない場合は、25 ページの「トークン レコードの抽出およびインポート」を参照してください。

セキュリティの要件

次の一覧は、セキュリティの要件と問題を示しています。RSA Authentication Manager マシンがこれらの要件を満たすことを確認してください。

- ❑ RSA Authentication Manager コンピュータは、安全な状態でなければなりません。信任された人だけがプライマリとレプリカに物理的にアクセスできる状態を確保します。また、Authentication Manager は RSA SecurID で保護されている必要があります。
- ❑ UNIX 管理者だけがプライマリとレプリカにアカウントを持っている必要があります。
- ❑ **rsh** コマンドと **rcp** コマンドを無効にしてください。これらのコマンドが有効な場合、RSA SecurID による保護を提供できません。
- ❑ **rexec** や、UNIX セキュリティを無視するその他のルーチンを使用しないでください。必要に応じて、**rexec** デーモンとその他のデーモンを無効にしてください。また、**hosts.equiv** ファイルと **.rhosts** ファイルも使用しないようにしてください。AIX プラットフォームの場合、**hosts.equiv** ファイルや **.rhosts** ファイルがあると PASSCODE プロンプトが表示されないので、この要件は AIX プラットフォームの場合に特に重要です。
- ❑ RSA SecurID 認証が **/etc/passwd** ファイルを通じて起動される場合は、ユーザ シェルを起動しない、つまり **sdshell** と PASSCODE 処理を起動しないようなすべてのサインオンの状況を回避します。
- ❑ **chsh** コマンドと **passwd** コマンドは、管理者だけが使用するようにしなければなりません。ユーザが **/etc/passwd** ファイルを変更し、自分のログオン シェルを **sdshell** 以外に変更すると、RSA SecurID PASSCODE を入力しなくても、システムにアクセスできてしまいます。**chsh** がサポートされる場合、**/etc/shells** ファイルには sdshell **だけ**が含まれているようにしなければなりません。このようにすると、**chsh** および **passwd** 同等コマンド (**passwd -s**) は無効になります。HP-UX システムの場合は、**chsh** を手動で無効にする必要があります。

Telnet

telnet を使用する場合は、暗号化された telnet を使用するか、コマンド ライン モードで telnet を使用します。どちらも使用できない場合は、構成レコードに対して次のいずれかの変更を行います。

- PASSCODE が一度に 1 文字ずつクリア テキストで送信されてしまうので、[Bad PASSCODEs before Next Tokencode] と [Bad PASSCODEs before Disabling Token] の設定を小さい値に変更します。
- [Response Delay] の値を大きくして、Authentication Manager が PASSCODE の最終文字を検出できるようにします。

構成レコードの変更については、『RSA Authentication Manager 6.1 管理者ガイド』の「RSA Authentication Manager の構成 (UNIX)」の章を参照してください。

syslog へのレプリケーション メッセージの記録

RSA Authentication Manager レプリケーション ステータス メッセージを syslog に記録する場合は、各 Authentication Manager の **syslog.conf** ファイルを編集して、***.info** サフィックスを含むメッセージを指定します。データベースの変更がレプリケートされるときに、このステータス メッセージが記録されます。

テキスト エディタを使用して **/etc/syslog.conf** ファイルを開き、システム ログ ファイルを指定する行に ***.info** を追加してください。

注意 : レプリケーション ステータス メッセージを記録すると、syslog が短時間で大きくなる可能性があります。レプリケーションの処理が行われていることを確認する必要がある場合のみ、このメッセージを syslog に記録することをお勧めします。このステータス メッセージを記録する必要がある場合は、syslog を頻繁に整理してください。

認証のテスト

プライマリとレプリカが正しくインストールされ、これらをエージェント ホストとして保護できるかどうかを確認するには、このセクションの手順を実行します。

トークン レコードの抽出およびインポート

トークン レコード (**.asc** ファイルまたは **.xml** ファイル) が格納されている CD-ROM を受け取った場合は、データベースにトークンをインポートし、トークンをユーザに割り当てるために、通常の方法でフロッピー ディスクまたは CD-ROM からトークン レコードを取り出し、プライマリに転送する必要があります。

メモ : アップグレードを実行している場合、既存のトークン レコードは 6.1 データベースに自動的に移行されます。

重要 : トークン レコードを取り出してインポートした後、システム上のすべてのトークン レコード ファイルを削除し、フロッピー ディスクを安全な場所に保管してください。トークン レコードには重要で機密性の高い情報が含まれているので、信任された人だけが扱うようにしてください。

トークン レコードをデータベースにインポートするには、キャラクタベースの RSA Authentication Manager Host Mode の **sdadmin** を使用するか、Windows ベースのマシンで Remote Administration ソフトウェアを使用します。**sdadmin** を使用してトークンをインポートする手順は次に示すとおりです。**sdadmin** の詳細については、付録 D「データベース ユーティリティ」の「sdadmin の使用」を参照してください。

トークンをインポートするには

1. プライマリに RSA Authentication Manager ファイル オーナとしてログオンします。
2. データベース ブローカを起動します。

   ```
   ACEPROG/sdconnect start
   ```

3. RSA Authentication Manager アドミニストレーション プログラムを実行します。

   ```
   ACEPROG/sdadmin
   ```

   Authentication Manager アドミニストレーション プログラムの使い方については、88 ページの「インタフェースの規則」を参照してください。

4. [Token] メニューの [Import Tokens] を選択します。
5. 最初に提供された RSA Authentication Manager ソフトウェア パッケージに同梱されていたフロッピー ディスクまたは CD-ROM から取り出したトークン レコード ファイルのパスとファイル名を入力します。

ユーザのための RSA SecurID 認証の実装

以下の手順は、ユーザを RSA Authentication Manager データベースに追加し、トークンをユーザに割り当て、エージェント ホスト上でユーザをアクティブ化する方法を示しています。この手順を終了すると、テスト ユーザを使用して、エージェント ホストから RSA Authentication Manager へのローカル認証をテストできます。ローカル認証の場合、RSA Authentication Manager はエージェント ホストとしての役割も果たします (RSA Authentication Manager と RSA Authentication Agent の両方が同じマシンにあるため)。このため、テスト ユーザが Authentication Manager にログオンすると、RSA SecurID 認証を求めるプロンプトが表示されます。

重要：RSA Authentication Manager 管理者をテスト ユーザとして使用しないでください。テスト認証が失敗した場合、システムがロックされてしまいます。

RSA SecurID 認証を実装するには

1. RSA Authentication Manager アドミニストレーション プログラムで、テスト ユーザ用のローカル ユーザ レコードを作成します。[Users] > [Add User] の順に選択します。適切な情報を入力します。[OK] をクリックして [Add User] ダイアログ ボックスを閉じます。
2. トークンをテスト ユーザに割り当てます。[Assign Token] をクリックします。

   シリアル番号でトークン レコードを選択します。トークンの背面に記載されているシリアル番号と一致するトークンを検索します。
3. [Agent Host] > [List Agent Hosts] の順にクリックし、プライマリとレプリカがエージェント ホストとして登録されていることを確認します。
4. プライマリまたはレプリカがエージェント　ホストとして登録されていない場合は、[Agent Host] > [Add Agent Host] の順にクリックし、マシンのホスト名を入力します。次に、[Agent type: UNIX Agent Host] を選択し、[User Activations] を選択して、RSA SecurID の認証を受けた後でテスト ユーザがマシンにアクセスできるように定義します。
5. [File] メニューの [Exit] を選択して、**sdadmin** を終了します。

テスト認証の実行

テスト認証を実行することによって、RSA Authentication Manager のインストールと構成が正しく行われたことを確認できます。

RSA SecurID 認証をテストするには

1. **aceserver** がまだ実行されていない場合は、次のコマンドを入力して Authentication Manager 上で起動します。

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```
2. テスト認証ユーティリティを実行します。次のコマンドを入力します。

ACEPROG/sdtestauth

ユーザ ID と RSA SecurID PASSCODE の入力が求められます。

3. 「Enter PASSCODE (PASSCODE を入力してください)」プロンプトに対して、前のステップ 2 で割り当てた RSA SecurID トークンに表示されているコードを入力します。ENTER キーを押します。画面の指示に従って、個人識別番号 (PIN) を取得します。

4. PIN を受け取るか、選択すると、再び PASSCODE の入力が求められます。新しいトークンコードが表示されるのを待ち、PIN と現在の RSA SecurID トークンコードの組み合わせを入力します。特に、**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場合**は、PIN に続いて、カードに表示されているコードを入力します。**RSA SecurID PINPAD を使用している場合**は、カード自体に PIN を入力し、カード下部のダイアモンドを押してください。「Enter PASSCODE (PASSCODE を入力してください)」プロンプトに対して、PINPAD に表示されるコードを入力します。

   インストールとセットアップのすべての手順を指示されたとおりに実行し、正しい PASSCODE を入力したにもかかわらず、常にアクセスを拒否される場合は、『RSA Authentication Manager 6.1 管理者ガイド』の付録「トラブルシューティング」を参照してください。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。

レプリカをサポートするためのシステムの準備

1. レプリカ ワークステーションが、第 1 章「RSA Authentication Manager の要件」に示されているすべてのシステム要件を満たしているかどうかをまだ確認していない場合は、その確認を行います。

2. 14 ページの「インストール前のチェックリスト」の説明に従ってワークステーションを準備します。

3. レプリケーション サービスの通信サービス名とポート番号が各 Authentication Manager の **/etc/services** ファイルに登録されていることを確認します。デフォルトのサービス名とポート番号の一覧については、17 ページを参照してください。

4. 必要に応じて、プライマリ / レプリカ通信プログラム **acesyncd** は、24 時間ごとにレプリカのシステム クロックをプライマリのシステム クロックに一致させます。新規インストールで、プライマリとレプリカのシステム クロックの同期がとれていない場合は、システム クロックのずれによって、スケジュールされている作業やその他の時間ベースのアプリケーションに混乱をきたす可能性があります。このような場合は、レプリカのクロックを手動で変更し、必要なすべての調整を行うことで混乱を回避できます。既存の Authentication Manager をアップグレードする場合は、レプリカのクロックを手動で変更する必要はありません。

   メモ：レプリカのクロックを変更するには、root 権限が必要です。また、NTP を使用する場合は、プライマリと各レプリカ上で有効にする必要があります。詳細については、14 ページの「正確なシステム時刻の維持」を参照してください。

5. アップグレードを実行している場合は、構成の終了後、プライマリに登録されているすべてのエージェント ホストを更新します。UNIX エージェント ホスト、およびその他の特定の RSA Authentication Agent の場合は、各エージェント ホストのデータ ディレクトリに、変更された **sdconf.rec** ファイルをインストールします。

旧バージョンのエージェント ホストによっては、別のアクティング マスタ / スレーブのペアを使用するように構成されている **sdconf.rec** ファイルが必要な場合があります。

6. サードパーティ デバイスなど、その他の種類のエージェントの場合は、構成ファイルの変更が必要な可能性があります。各エージェント タイプの構成の更新については、各エージェントのマニュアルを参照してください。
7. 次のセクションの指示に従って、レプリカをデータベースに追加します。
   アップグレードでデータベースの自動移行を実行している場合は、30 ページの「レプリカ ソフトウェアのインストール」に進みます。

データベースへのレプリカの追加

レプリカに RSA Authentication Manager ソフトウェアをインストールする前に、プライマリのデータベースに各レプリカを追加し、レプリカ パッケージを作成する必要があります。レプリカ パッケージには、レプリカのインストールに必要なライセンス ファイルとデータベース ファイルが含まれています。

データベースにレプリカを追加するには

1. プライマリに **root** でログオンします。
2. レポート作成ユーティリティを停止します。次のコマンドを入力します。
   ```
   ACEUTILS/rptconnect stop
   ```
3. RSA Authentication Manager サービスとデータベース ブローカを停止します。次のコマンドを入力します。
   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```
4. 次のコマンドを入力します。
   ```
   ACEPROG/sdsetup -repmgmt add (または sdrepmgmt add)
   ```
5. レプリカに関する次の情報を、指示に従って入力します。
   - レプリカ マシンのホスト名。完全修飾名 (FQDN) を指定する必要があります。IP アドレスは自動的に解決されます。
   - レプリカが使用するエイリアス IP アドレス。このアドレスを使用して、ファイアウォールを通じての認証が必要なエージェント ホストを構成できます。
   - プライマリとレプリカ間の通信に使用するレプリケーション サービスのサービス名とポート番号。
   - デフォルトでは、サービス名は **securidprop** に番号が追加された形式です。たとえば、追加された最初のレプリカは **securidprop_01** というサービス名を使用します。レプリカを追加するたびに、サービス名に 1 が加算されます。
   - デフォルトでは、レプリカがプライマリとの通信に使用するポート番号は 5506 から始まり、レプリカを追加するたびに番号に 1 が加算されます。
   - プライマリが起動してから、最初のレプリケーションが試行されるまでの秒数 (スタートアップ遅延間隔)。
   - プライマリがレプリケーションを実行する頻度 (レプリケーション間隔)。

6. 追加するレプリカごとにステップ 5 を繰り返します。
7. データベース内のすべてのレプリカのリストを表示するには、次のコマンドを入力します。

   ```
   ACEPROG/sdsetup -repmgmt list
   ```

   sdsetup -repmgmt ユーティリティの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。
8. 次の「レプリカ パッケージの作成」の指示に従います。

レプリカ パッケージの作成

レプリカ パッケージは、レプリカ ソフトウェアをインストールするために必要なデータベース ファイルとライセンス ファイルで構成されます。以下の手順を実行するには、「データベースへのレプリカの追加」の説明に従って、レプリカがあらかじめ追加されていることが必要です。

レプリカ パッケージを作成するには

1. プライマリに **root** でログオンします。
2. レポート作成ユーティリティを停止します。次のコマンドを入力します。

   ```
   ACEUTILS/rptconnect stop
   ```
3. RSA Authentication Manager のデータベース ブローカとプロセスを停止します。次のコマンドを入力します。

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```
4. 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
   ```

   データベース内の現在のレプリカの数と、ライセンスで許可される数についての情報が表示されます。

   レプリカ パッケージを作成する前に、新規レプリカを追加するかどうか、確認を求められます。
5. 新規レプリカを追加する場合は、「y」と入力します。新規レプリカを追加しない場合は、「n」と入力し、ENTER キーを押します。

   ACEDATA ディレクトリに **replica_package** ディレクトリが作成され、その中にさらに 2 つのディレクトリが作成されます。データベース ファイル (**sdserv.db**、**sdserv.bi**、**sdserv.lg**、および **sdserv.vrs**) が格納される **database** ディレクトリと、ライセンス ファイル (**license.rec**、**sdconf.rec**、**sdrepnodes.txt**、**server.cer**、**server.key**、および **sdti.cer**) が格納される **license** ディレクトリです。ローリング アップグレードを実行している場合は、**license** ディレクトリに **uidxlate.map** というファイルも格納されます。
6. **license** ディレクトリのみを各レプリカにコピーします。レプリカをインストールし、起動すると、プライマリはデータベース ファイルをプッシュします。

   プライマリで Push DB 機能が無効な場合は、**replica_package** ディレクトリの内容を各レプリカ マシンにコピーします。

どちらの場合も、ディレクトリは RSA Authentication Manager トップレベル ディレクトリ以外でなければなりません。

レプリカ パッケージを作成する場合は、できるだけ早くレプリカに配布してください。レプリカ パッケージを作成すると、プライマリは、最初のレプリケーション パスでレプリカに送信するデータベースへの変更の保存を開始します。レプリカ パッケージの作成とインストールが遅くなればなるほど、プライマリは多くの変更をレプリカに送信しなければなりません。

7. プライマリを起動します。

```
ACEPROG/sdconnect start
ACEPROG/aceserver start
```

8. 次のセクションの指示に従って、レプリカ ソフトウェアをインストールします。

レプリカ ソフトウェアのインストール

このセクションのインストール手順では、Authentication Manager ワークステーションで RSA Authentication Manager 6.1 CD-ROM をマウントできることを前提にしています。インストール先の Authentication Manager ワークステーションにローカル CD-ROM ドライブがない場合は、NFS 機能を使用して CD-ROM ドライブ マウント ポイントを Authentication Manager ワークステーションにエクスポートすることで、ドライブをマウントし、CD-ROM からインストールできます。また、適切なディレクトリ構造を CD-ROM からワークステーションのディレクトリにコピーすることで、ワークステーション ディレクトリからインストールすることもできます。

レプリカ ソフトウェアをインストールするには

1. レプリカに **root** でログオンします。
2. CD-ROM ドライブのマウントポイント ディレクトリを作成します。

```
mkdir /cdrom
```

3. CD-ROM ドライブをマウントします。各プラットフォームの **mount** コマンドは、以下の表で確認してください。

OS	コマンド
Solaris と Linux	ボリューム マネージャが CD-ROM を自動的にマウントするので不要です。
HP-UX	実行パスの **/usr/sbin** を使用して、**root** で次のように入力します。 `mount -F cdfs /dev/dsk/c3t2d0 /cdrom`
AIX	`mount -o ro -v cdrfs /dev/cd0 /cdrom`

メモ：CD-ROM のデバイス名は、ホストに応じて異なります。HP-UX システムでは、デバイス名はシステムで使用している CD ドライバに応じて異なります。「unknown command (不明コマンド)」というエラー メッセージが返された場合は、オペレーティング システムのドキュメントを参照してください。

4. インストール元の **/cdrom/aceserv/*platform*** ディレクトリを指定します。***platform*** には、使用しているオペレーティング システムの略称を指定します。

OS	プラットフォームの略称	ディレクトリ
Solaris	sol	**/cdrom/*cd_name*/sol**
HP-UX	hp	**/cdrom/hp**
AIX	aix	**/cdrom/aix**
Linux	linux	**/cdrom/linux**

Solaris では、CD-ROM の名前をディレクトリ パスに指定する必要があります。

5. 次のコマンドを入力して、レプリカのインストールを開始します。

```
/cdrom/aceserv/platform/sdsetup -replica [-o yes]
[-p path] [-R path]
```

角かっこ内の引数は省略してもかまいません。省略した場合は、インストール時に入力が求められます。斜体の部分には実際の値を指定します。

コマンド ラインにパラメータをすべて指定した場合は、オーダ元の国を選択し、ライセンス契約に同意すると、インストール プログラムが最後まで自動的に実行されます。

引数の指定を一部省略し、インストール プログラムでその値が必要とされる場合は、プログラムの開始後 5 ～ 10 分以内に値の入力が求められます。プロンプトに応答しないと、インストールを続行できません。

引数をまったく指定せずに sdsetup -replica コマンドを実行した場合は、インストール プログラムの最初の部分が対話形式で実行され、設定する必要がある構成値の入力が求められます。表示されるすべての質問に答えると、インストール プログラムが自動的に実行され、終了します。

コマンド ライン引数

-o yes | no	アップグレードを実行している場合、この引数を指定すると、最初に **ace/prog** サブディレクトリから既存のファイルを削除せずに、再インストールを実行できます。**-o yes** を指定すると、インストール プログラムによって **ace** の内容が **ace_tmp** に移動されます。**-o no** を指定すると、インストールは終了します。
-p *path*	Authentication Manager を準備するときに選択または作成した RSA Authentication Manager のトップレベル ディレクトリのパス名を指定します。レプリカとプライマリで同じパス名を使用します。
-R *path*	プライマリからレプリカにコピーしたレプリカ パッケージ ファイルが格納されているディレクトリのパス名を指定します。

インストール プロンプト

コマンド ラインに必要な情報が指定されていない場合、インストール プログラムは、プロンプトを表示して入力を求めます。プロンプトは、スタートアップ画面がいくつか表示された後に表示されます。ここでは、表示される順にプロンプトを説明します。

RSA Authentication Manager トップレベル ディレクトリ

Authentication Managerを準備するときに選択または作成したディレクトリのパス名を指定します。指定するパスに、すべての RSA Authentication Manager サブディレクトリ、データベース、およびプログラム ファイルが格納されます。レプリカとプライマリで同じパス名を使用します。

レプリカ パッケージ

レプリカ パッケージ ファイルが格納されているディレクトリのパス名を指定します。[System Parameters] ダイアログ ボックスの [Push DB Assisted Recovery] チェックボックスがオンの場合は、指定のパスにライセンス ファイルのみが格納されている必要があります。[System Parameters] ダイアログ ボックスの [Push DB Assisted Recovery] チェックボックスが**オフ**の場合は、指定のパスにライセンス ファイルとデータベース ファイルが格納されている必要があります。

重要：ace_tmp に移動されたファイルは、削除したり、別の場所に移動したりできます。**ace_tmp** 内のファイルを移動したり、バックアップを作成したりしないで RSA Authentication Manager ソフトウェアを再インストールまたはアップグレードすると、**ace_tmp** の内容はこのインストールによって上書きされ、永久に失われてしまいます。

レプリカのインストールの終了

インストールが正しく終了すると、メッセージが表示され、Authentication Manager の構成情報とライセンス情報が表示されます。データベース内のユーザやレプリカの個数がライセンスの制限を超える場合は、アップグレード違反に関する情報が表示されます。ライセンスの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の「概要」の章を参照してください。

サービス名とポート番号に関するトラブルシューティング

解決できないサービス名についてのメッセージも表示された場合は、**/etc/services** に入力したサービス名が間違っているか (17 ページを参照)、またはデフォルト以外のサービス名を選択した可能性があります。Authentication Manager の構成ファイルの変更については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

スタートアップ プロセスの監視

レプリカを起動する前に、次のコマンドを実行して、プライマリでログ モニタを開始できます。

```
ACEPROG/sdlogmon -t
```

このコマンドを実行すると、ログ モニタが表示され、プライマリとレプリカ間で通信が確立されていることを確認できます。PushDB (最新のデータベースをレプリカに送信するプロセス) が有効な場合は、このプロセスが起動することを示すメッセージが表示されます。プライマリによって、レプリカのデータベース ブローカと認証プロセスがシャットダウンされ、データベースがプッシュされます。続いて、レプリカのデータベース ブローカと認証プロセスが再起動されます。PushDB の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の「概要」の章を参照してください。

レプリカの起動

レプリカを起動するには

1. Authentication Manager に RSA Authentication Manager ファイル オーナとしてログオンします。
2. データベース ブローカを起動します。

   ```
   ACEPROG/sdconnect start
   ```

   データベース ブローカが起動されていることを示す一連のメッセージが表示されます。スタートアップが終了すると、次のメッセージが表示されます。

   ```
   Database broker start operation completed (データベース ブローカのスタートアップ処理が終了しました )
   ```

   Push DB 機能が有効な場合は、ステップ 3 をスキップします。プライマリはレプリカ上のブローカを直ちに停止し、レプリカにデータベースをプッシュします。プッシュが終了すると、レプリカ上のブローカと認証サービスをプライマリが再起動するので、**aceserver start** コマンドを実行する必要はありません。
3. 認証サービスを起動します。

   ```
   ACEPROG/aceserver start
   ```

   RSA Authentication Manager が起動していることを示す一連のメッセージが表示されます。スタートアップが終了すると、次のメッセージが表示されます。

   ```
   RSA ACE/Server start operation completed (RSA ACE/Server のスタートアップ処理が終了しました )
   ```

   これで、レプリカはユーザを認証できる状態になりました。

次のステップ

重要：ライセンスのバックアップ コピーは、RSA Authentication Manager ソフトウェアをインストールした後に作成する必要があります。ライセンス ファイルは、インストール中に変更されます。このため、***ACEDATA*** ディレクトリ内のライセンスが失われたり、破損した場合、オリジナルのライセンス フロッピー ディスクを使用しても、データベースにアクセスすることはできません。データベースにアクセスするには、変更されたライセンス ファイルを使用するしか方法がありません。

TACACS+ デバイスをインストールし、RSA Authentication Manager で TACACS+ プロトコルのサポートを有効化する方法については、第 5 章「RSA Authentication Manager の TACACS+ サポート」を参照してください。

3 RSA Authentication Manager へのアップグレード

RSA ACE/Server 5.1以上(およびパッチ バージョン)、またはRSA Authentication Manager 6.0 以上 (およびパッチ バージョン) を使用している場合、RSA Authentication Manager 6.1 にアップグレードできます。

次の条件が満たされる場合には、自動移行 (プライマリだけの場合) またはローリング アップグレード (1 つ以上のレプリカがある場合) を実行できます。

- 旧バージョンと同じディレクトリ内の既存のソフトウェアの上に RSA Authentication Manager 6.1 をインストールする。
- RSA Authentication Manager 6.1 でサポートされるバージョンのオペレーティング システムで実行している。

RSA Authentication Manager インストール プログラムが **ace/data** サブディレクトリから v5.1 以降のデータベースを検出し、**ace/prog** サブディレクトリから適切な移行ツールを検出すると、データは自動的に 6.1 データベースに移行されます。

重要: **ace/data** ディレクトリにデータベースのダンプ ファイル (拡張子が .dmp のファイル) がある場合は、そのファイルを使用するか、または、既存のデータベースをダンプおよびロードするか、確認を求められます。

アップグレード前のチェックリスト

RSA Authentication Manager 6.1 ソフトウェアをアップグレードする前に、日本語マニュアル CD-ROM の『Readme』(英語版は **authmgr_readme.pdf**) をお読みください。『Readme』には、構成およびインストールに関する重要な情報が記載されています。また、標準マニュアルへの記載が間に合わなかったソフトウェアの問題についても説明しています。

重要：現在、RSA RADIUS サーバを使用していて、RSA RADIUS サーバ 6.1 へ移行する場合は、プライマリとレプリカをアップグレードする**前**に、付録 A「RSA RADIUS サーバの移行」を参照してください。

アップグレードに必要なもの

- ❑ 第 1 章「RSA Authentication Manager の要件」に説明されているハードウェア、ディスク容量、メモリ、およびプラットフォームの要件をすべて満たすマシン。
- ❑ Authentication Manager にインストールする RSA Authentication Manager ソフトウェア。ソフトウェアはサポートされているバージョンでなければなりません。
- ❑ 既存のプライマリ Authentication Manager の **sdserv** および **sdlog** データベース ファイルと、既存のレプリカ Authentication Manager の **sdserv** データベース ファイルのバックアップ コピーを作成できるだけの十分なディスク容量 (別システムの方が適切です)。

  メモ：データベース ファイルのバックアップを作成する前に、すべての RSA Authentication Manager プロセスを停止してください。

- プライマリおよびレプリカでの root 権限と Administrator 権限。
- RSA Authentication Manager 6.1 CD-ROM。
- 既存のプライマリのライセンス ファイルまたは新しいライセンス ファイル。新しいライセンス ファイルを受け取った場合は、アップグレードを実行した後で適用することをお勧めします。

重要： RSA ACE/Server 5.0 アドバンスド ライセンスから RSA Authentication Manager 6.1 アドバンスド ライセンスへアップグレードする場合は、RSA セキュリティ社から新しいライセンス ファイルを取得し、アップグレードを実行した後で適用する必要があります。新しいライセンスを適用しないと、RSA Authentication Manager は**アップグレード違反**モードになるので注意してください。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。ライセンスのアップグレード方法をはじめ、アップグレードの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

必要な情報

- 追加するレプリカの名前と IP アドレス。
- ライセンスで認められる数のレプリカ。
- RSA Authentication Manager ベース ライセンスを所有している場合は、1 台のレプリカをインストールできます。RSA Authentication Manager アドバンスド ライセンスを所有している場合は、最大 10 台のレプリカをインストールできます。

プライマリのアップグレードの準備

重要： プライマリとレプリカが RSA Authentication Agent ソフトウェアで保護されている場合は、アップグレードを行う前に、プライマリとレプリカでローカル アクセス保護をオフにしてください。オフにしておかないと、場合によってはマシンがロックされてしまいます。ローカル アクセス保護を有効にする方法については、RSA Authentication Agent のマニュアルを参照してください。

RSA Authentication Manager ソフトウェアをアップグレードする前に、プライマリに Administrator でログオンし、次の操作を実行してください。

操作 1：プライマリの RSA Authentication Manager サービスの停止

アップグレードする Authentication Manager で RSA Authentication Manager サービスが動作している間は、RSA Authentication Manager ソフトウェアをアップグレードできません。また、システムで設定されている可能性のある RSA Authentication Manager の自動起動機能を無効にする必要があります。

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。プライマリで **aceserver** を停止すると、代わりにレプリカがユーザの認証とログへの記録を行いますが、データベースを管理することはできません。

RSA Authentication Manager の停止

すべての管理者が **sdadmin**、**sdlogmon**、および **sdreport** を終了していることを確認してください。レポート作成ユーティリティを停止するには、次のコマンドを入力します。

```
ACEUTILS/rptconnect stop
```

サービスとデータベース ブローカを停止するには、次のコマンドを入力します。

```
ACEPROG/aceserver stop
ACEPROG/sdconnect stop
```

操作 2：プライマリのデータベース ファイルとライセンス ファイルのバックアップ

すべての RSA Authentication Manager プロセスを停止した後、Authentication Manager 上のデータベース ファイル、ライセンス ファイル、構成ファイル、および RADIUS アカウント ファイルのバックアップ コピーを作成します。

データベース ファイルとライセンス ファイルは、***ACEDATA*** ディレクトリ (**ace/data** など) に保存されています。データベース ファイルとライセンス ファイルのバックアップを作成するには、***ACEDATA*** ディレクトリをコピーしてください。

デフォルトでは、RADIUS アカウント ファイルは ***ACEDATA*¥radacct** ディレクトリに保存されています。別のディレクトリを指定すると、フル パスが RADIUS 構成ユーティリティ (***ACEPROG*/rtconfig**) の [Accounting] メニューに表示されます。RADIUS アカウント ファイルのバックアップを作成するには、***ACEDATA*¥radacct** ディレクトリ、またはユーザ指定のディレクトリ内の**すべて**のディレクトリのコピーを作成します。

これでプライマリをアップグレードできる状態になりました。次の「プライマリのアップグレード」を参照してください。

プライマリのアップグレード

プライマリをアップグレードする手順は、第 2 章「RSA Authentication Manager のインストール」の次のセクションに説明されています。

- 「プライマリ ソフトウェアのインストール」
- 「インストール後のセットアップ」
- 「認証のテスト」

各セクションの手順を実行した後、プライマリを起動します。次のコマンドを入力します。

```
ACEPROG/sdconnect start
ACEPROG/aceserver start
```

レプリカのアップグレードの準備

レプリカをアップグレードする前に、次の操作を実行してください。

操作 1：プライマリのレプリカ パッケージのコピー

プライマリのアップグレード プロセスによって、レプリカのレプリカ パッケージが ***ACEDATA*¥replica_package** ディレクトリ (または REP_ACE 環境変数で指定されるディレクトリ) に作成されます。

次のいずれかの操作を実行します。

- プライマリで Push DB Assisted Recovery 機能が有効になっている場合は、***ACEDATA*¥replica_package¥license** ディレクトリを、レプリカ マシンの RSA Authentication Managerディレクトリ以外のテンポラリ ディレクトリにコピーします。レプリカをアップグレードし、起動すると、プライマリがデータベース ファイルをレプリカにプッシュします。
- プライマリで Push DB Assisted Recovery 機能が無効な場合は、***ACEDATA*¥replica_package** ディレクトリの内容を、レプリカ マシンの RSA Authentication Managerディレクトリ以外のテンポラリ ディレクトリにコピーします。

レプリカのアップグレード時に、ライセンス ファイルの場所を指定する必要があります。

操作 2：レプリカのすべての RSA Authentication Manager サービスの停止

アップグレードする Authentication Manager で RSA Authentication Manager サービスが動作している間は、RSA Authentication Manager ソフトウェアをアップグレードできません。37 ページの「RSA Authentication Manager の停止」を参照してください。

これでレプリカをアップグレードできる状態になりました。操作手順については、次の「レプリカのアップグレード」を参照してください。

レプリカのアップグレード

レプリカをアップグレードする手順は、第 2 章「RSA Authentication Manager のインストール」の次のセクションに説明されています。

- 「レプリカ ソフトウェアのインストール」
- 「レプリカのインストールの終了」

この 2 つのセクションの手順を実行した後、再びこのセクションに戻ってください。

次のステップ

TACACS+ デバイスをインストールし、RSA Authentication Manager で TACACS+ プロトコルのサポートを有効化する方法については、第 5 章「RSA Authentication Manager の TACACS+ サポート」を参照してください。

4 Remote Administration ソフトウェアのインストール

Remote Administration ソフトウェアでは、グラフィカル ユーザ インタフェースを通じて RSA Authentication Manager データベースを管理できます。また、Remote Administration ソフトウェアは、RSA Authentication Manager Host Mode が備えているすべての管理機能にアクセスできる唯一の方法です。UNIX プラットフォーム上の RSA Authentication Manager データベースは、次のオペレーティング システムが動作しているマシンからリモート管理できます。

- Windows 2003 Server
- Windows 2000 Professional、Windows 2000 Server、および Windows 2000 Advanced Server
- Windows XP Professional

ブラウザベースの RSA Authentication Manager Quick Admin ソフトウェアを使用して、一般的ないくつかの操作を実行することもできますが、データベース管理のすべての作業を実行することはできません。詳細については、第 6 章「Quick Admin ソフトウェアのインストール」を参照してください。

メモ：Remote Administration アプリケーションを使用して変更できるのは、プライマリ サーバのデータベースだけです。レプリカ サーバのデータベースに接続する場合、接続は読み取り専用です。レポートの実行、ログ モニタの実行、データベース情報の表示はできますが、レプリカ データベースの管理情報を変更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認証方式の設定

RSA Authentication Manager は、デフォルトでリモート アドミニストレーションを実行できるように構成されています。ただし、リモート管理者が Remote Administration を通じてログオンするときに使用するトークンの種類 (つまり認証**方式**) を選択する必要があります。管理者の認証方式には、RSA SecurID カードとキーホルダ、紛失したトークン用のパスワード、ソフトウェア トークン、およびユーザ パスワードの 4 種類があります。

管理者の認証方式を設定するには

1. プライマリ サーバで ***ACEPROG*** ディレクトリに移動し、**sdadmin** を実行します。
2. [System] メニューの [System Configuration] を選択し、続いて [Edit System Parameters] を選択します。
3. [Administrator Authentication Methods] の項目で、リモート管理者を認証するための方式を選択します。

インストールおよびアップグレードのチェックリスト

RSA Authentication Manager Remote Administration ソフトウェアの導入に先立ち、次のチェックリストを使用して、必要なすべてのハードウェア、ソフトウェア、およびアップグレードに必要な情報が揃っていることをあらかじめ確認してください。

- ❑ Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server (Service Pack 4)、Windows XP Professional、または Windows 2003 Server が動作している Intel Pentium プロセッサ搭載のマシン。必要なハードウェア、ディスク容量、およびメモリの詳細については、第 1 章「RSA Authentication Manager の要件」を参照してください。

  メモ：マシンは、セキュリティが確保される場所に設置し、信任された人だけがアクセスできるようにしてください。RSA SecurID 認証で保護されるのは、RSA Authentication Manager Host Mode だけです。マシン自体を RSA SecurID で保護するには、RSA Authentication Agent for Windows ソフトウェアをインストールする必要があります。

- ❑ プライマリにインストールする RSA Authentication Manager ソフトウェア。ソフトウェアはサポートされるバージョンでなければなりません。

  RSA Authentication Manager ソフトウェアのバージョンと、インストールする Remote Administration ソフトウェアのバージョン番号は、パッチ レベルまで一致していなければなりません。以前のバージョンの RSA Authentication Manager で提供されたRemote Administrationソフトウェアがインストールされている場合、Remote Administration ソフトウェアをアップグレードしない限り、RSA Authentication Manager 6.1 データベースをリモート管理することはできません。Remote Administration ソフトウェアをアップグレードすると、アップグレードされた Remote Administration ソフトウェアが動作しているマシンから、6.1 以前のデータベースを管理できなくなります。

- ❑ プライマリおよびリモート マシンでのローカル Administrator 権限。

- ❑ プライマリ上の **sdconf.rec** ファイルと **server.cer** ファイルへのアクセス権。

  ACEDATA ディレクトリにある **sdconf.rec** ファイルと **server.cer** ファイルをフロッピー ディスクにコピーします。または、リモート アドミニストレーション マシンからこれらのファイルにアクセスできるようにします。

Remote Administration の新規インストール

各コンポーネントはそれぞれ専用のマシンで実行することをお勧めします。しかし、複数のコンポーネントを同じマシンで実行する場合は、次のガイドラインに従ってください。

Remote RADIUS、Remote Administration、およびエージェント ホスト自動登録プログラムを同じマシンにインストールする場合は、次の順序でコンポーネントをインストールする必要があります。

- エージェント ホスト自動登録プログラム
- Remote Administration
- Remote RADIUS

Remote RADIUS、Remote Administration、およびエージェント ホスト自動登録プログラムを同じマシンからアンインストールする場合は、次の順序でコンポーネントをアンインストールする必要があります。

- Remote RADIUS
- Remote Administration
- エージェント ホスト自動登録プログラム

Remote Administration ソフトウェアをインストールするには

1. リモート マシンにローカルの Administrator としてログオンし、RSA Authentication Manager 6.1 CD-ROM を CD-ROM ドライブに挿入します。
2. RSA Authentication Manager CD-ROM の **aceserv¥windows¥** ディレクトリにある **setup.exe** をダブルクリックします。
3. [Select Language] ダイアログボックスが表示されるまで、画面の指示に従います。[Select Language] ダイアログボックスで [English] を選択します。
4. [Slelct Installation Type] ダイアログ ボックスが表示されるまで、画面の指示に従います。[Remote Administration Client] チェックボックスをオンにして、[Next] をクリックします。
5. [RSA Authentication Manager License Files] ダイアログ ボックスが表示されるまで、画面の指示に従います。**sdconf.rec** ファイルと **server.cer** ファイルが格納されているディスクまたはディレクトリを参照し、[Next] をクリックします。
6. 画面の指示に従ってインストールを完了します。
7. DNS を使用していない場合は、サーバの名前と IP アドレスを、リモート アドミニストレーション マシンの **hosts** ファイルに追加します。

   Windows 2000 または Windows 2003 マシンの場合、**hosts** ファイルは ***%SystemRoot%*¥System32¥drivers¥etc¥** にあります。

Remote Administration のアップグレード

重要：Remote RADIUS もインストールされているマシンで Remote Administration をアップグレードする場合は、最初に Remote RADIUS をアンインストールし、Remote Administration のアップグレードを実行した後、Remote RADIUS を再インストールする必要があります。

Remote Administration ソフトウェアをアップグレードするには

1. リモート マシンにローカルの Administrator としてログオンし、RSA Authentication Manager 6.1 CD-ROM を CD-ROM ドライブに挿入します。
2. RSA Authentication Manager CD-ROM の **aceserv¥windows¥** ディレクトリにある **setup.exe** をダブルクリックします。
3. [Installation Options] ダイアログ ボックスが表示されるまで、画面の指示に従います。[Upgrade Remote Administration] チェックボックスをオンにして、[Next] をクリックします。

4. 画面の指示に従ってインストールを完了します。

リモート管理する RSA Authentication Manager の追加

Remote Administration ソフトウェアが動作しているマシンから追加データベースを管理する必要がある場合は、このセクションの手順を実行してください。40 ページの説明に従って、Remote Administration ソフトウェアがあらかじめインストールされている必要があります。

手順の中で、プライマリにある **server.cer** ファイルと **sdconf.rec** ファイルの場所が要求されます。

リモート管理するサーバを追加するには

1. [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。

   [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。

2. [RSA Authentication Manager for Windows]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。

3. [Modify] を選択し、[Next] をクリックします。

4. [Add/Remove Remote Administration] を選択し、[Next] をクリックします。

5. [Add] をクリックします。

6. 表示される指示に従って RSA Authentication Manager Maintenance の操作を完了し、[Finish] をクリックします。

7. DNS を使用していない場合は、サーバの名前と IP アドレスを、リモート アドミニストレーション マシンおよびプライマリの **hosts** ファイルに追加し、管理するサーバからリモート アドミニストレーション マシンを解決できることを確認します。**hosts** ファイル内のエントリの要件については、13 ページの「ホスト名」を参照してください。

   Windows 2000 または Windows 2003 マシンの場合、**hosts** ファイルは ***%SystemRoot%*¥System32¥drivers¥etc¥** にあります。

   DNS がある場合は **hosts** ファイルにサーバ名を登録する必要はありませんが、リバース ルックアップが有効でなければなりません。コマンド プロンプトに対して、「nslookup ***machine name***」と入力します。マシンの IP アドレスが返される場合は、**hosts** ファイルにサーバ名を追加する必要はありません。

メモ：リモート アドミニストレーション サーバを削除するには、同じ手順を使用します。ステップ 5 で、削除するリモート アドミニストレーション サーバを反転表示し、[Remove] をクリックします。

リモート アドミニストレーション ポートの設定

リモート アドミニストレーションでは TCP を使用し、RSA Authentication Manager で動作しているリモート アドミニストレーション セッションごとに、2 つのポートをオープンします。リモート アドミニストレーション接続で使用するポート番号の範囲を指定することで、同時にオープンできるポート数を制限できます (この結果、同時に実行できるリモート アドミニストレーション セッションの数が制限されます)。範囲は、RSA Authentication Manager ごとに指定する必要があります。

ポート番号の範囲を指定するには

1. レポート作成ユーティリティを停止します。次のコマンドを入力します。

   ```
   ACEUTILS/rptconnect stop
   ```

2. RSA Authentication Manager サービスとデータベース ブローカを停止します。次のコマンドを入力します。

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```

3. **ace/rdbms** ディレクトリ (UNIX) で、**startup.pf** ファイルのバックアップ コピーを作成します。**startup.old** という名前を指定してください。

4. テキスト エディタで **startup.pf** ファイルを開き、ファイルの末尾に次の 2 行を追加します。

   ```
   -minport [ 最小ポート番号 ]
   -maxport [ 最大ポート番号 ]
   ```

   指定したポートが最小ポート番号として使用されることはありません。TCP が使用する先頭のポートは、常に指定した最小ポート番号に 1 を加えた番号です。このため、指定するポートの範囲には、必要なポート数より常に 1 つ多いポートを含んでおく必要があります。たとえば、リモート接続数が 10 の場合、必要なポート数は 20 なので、21 のポート範囲を指定する必要があります。

   たとえば、ポート 3001 ～ 3020 を使用するには、ファイルに次の行を追加します。

   ```
   -minport 3000
   -maxport 3020
   ```

   他のサービスが使用しているポート番号を範囲に含まないでください。

   Progress Software Development Toolkit を使用している場合は、RSA Authentication Manager 6.1 に付属している **startup.pf** とは異なるファイルが使用されている可能性があります。この場合は、ここで説明する手順に従って、両方の **startup.pf** ファイルを編集してください。

5. RSA Authentication Manager を再起動します。次のコマンドを入力します。

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

5 RSA Authentication Manager の TACACS+ サポート

この章の内容は、コミュニケーション サーバやルータに詳しいネットワーク管理者が対象です。

RSA Authentication Manager は、TACACS+ 2.1 を実行しているルータとコミュニケーション サーバに対して、RSA SecurID アクセス制御機能を提供できます。TACACS+ 2.1 は、TACACS (Terminal Access Controller Access Control System) Plus とも呼ばれます。

TACACS+ は、より詳細なアカウンティング情報を提供し、認証プロセスとオーソライゼーション プロセスを強力に管理します。TACACS+ は、RSA Authentication Manager のネクスト トークンコード モードと New PIN モードもサポートします。

TACACS のサポートは、クライアント コードとサーバ コードから成る、Cisco Systems 社のセキュリティ ソフトウェアを通じて提供されます。クライアント コードは、Cisco Systems 社や他社のルータおよびコミュニケーション サーバとともに、標準ソフトウェアの一部として配布されます。サーバ コードは、RSA Authentication Manager に組み込まれています。

この章では、次のことについて説明します。

- RSA Authentication Manager を構成して TACACS+ クライアント デバイスをサポートする方法、および TACACS+ クライアント デバイスを構成する方法。
- TACACS+ で Enable モードを保護する方法。

TACACS+ デバイスの構成は、以下のスタートアップ ファイルと、スタートアップ ファイルで定義される構成ファイルを通じて管理されます。

```
ACEDATA/sdtacplus.arg
```

スタートアップ ファイルは、Cisco Systems 社の TACACS+ ソフトウェアに必要なコマンド ライン引数を提供します。スタートアップ ファイルは、**sdtacplus.cfg** という名前のプロトコル固有の構成ファイルも定義します。この構成ファイルには、次の情報が格納されています。

- RSA SecurID の認証を受けるユーザに関する情報
- 各種 TACACS+ 構成パラメータの設定

TACACS+ サポートを有効にして RSA Authentication Manager システムを起動すると、スタートアップ ファイルに指定されている構成ファイルが検索されます。

TACACS+ デバイスでの認証

TACACS+ ユーザの認証

1. 保護されているポートを通じてユーザがログオン セッションを起動すると、ユーザ名の入力が求められます。
2. ユーザ名の入力後、このユーザが構成ファイルの中で RSA SecurID ユーザとして登録されている場合は、次のプロンプトが表示されます。

   ```
   Enter PASSCODE: (PASSCODE を入力してください)
   ```

ユーザの応答は、Authentication Manager で実行中の **_sdtacplusd** へ送られます。暗号化の詳細については、49 ページの「TACACS+ 構成ファイルのサンプル」を参照してください。

3. **_sdtacplusd** は、要求を受け取ると RSA Authentication Agent コードを起動します。このコードが **aceserver** と通信します。ネットワーク障害や、**aceserver** が実行されていないために認証サービスを使用できない場合は、2 番目の認証方式が起動されます。2 番目の認証方式がない場合は、TACACS+ クライアントから次のメッセージが表示されます。

   ```
   No response from authentication TACACS server. (認証 TACACS サーバから応答がありません)
   ```

   aceserver は、クライアントから認証要求を受け取ると、PASSCODE のチェックを実行してユーザの身元を認証します。Authentication Manager は認証結果をクライアント デバイスに送り、そこで「PASSCODE Accepted (PASSCODE が受け付けられました)」または「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。または、必要に応じて、New PIN 操作やネクスト トークンコード手順が実行されます。

   再試行の失敗が指定された回数に達すると、クライアントは「Authentication failed (認証できませんでした)」というメッセージを表示します。接続は切断され、ログオン セッションを再起動しなければなりません。

TACACS+ サポートの有効化と構成

TACACS+ サポートを有効化し、構成するには

1. RSA Authentication Manager Host Mode を実行し、[Add Agent Host] を選択して、TACACS+ デバイスをエージェント ホストとして RSA Authentication Manager データベースに登録します。エージェント タイプとして [Communication Server] を選択します。TACACS+ デバイス上でユーザまたはユーザ グループをアクティブ化します。詳細については、ヘルプの「Add Agent Host」を参照してください。
2. RSA Authentication Manager Host Mode を終了します。
3. **/etc/services** に次の行が指定されていることを確認します。

   ```
   tacacs 49/tcp
   ```

4. TACACS+ をサポートするようにシステムがまだ構成されていない場合は、**sdsetup -config** を実行して、サポートを有効にします。**sdsetup -config** の実行の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の付録「RSA Authentication Manager の構成 (UNIX)」を参照してください。
5. RSA Authentication Manager 6.1 をインストールする前に、カスタマイズされた **sdtacplus** 引数ファイルおよび構成ファイルを使用していた場合は、これらのファイルを **ace_tmp** から **ace/data** サブディレクトリにコピーして、インストール プログラムによって作成されたデフォルト ファイルに上書きします。

   新規インストールの場合は、**ace/data** サブディレクトリに格納されているデフォルトの **sdtacplus.arg** を変更し、TACACS+ ソフトウェアのコマンド ライン引数を指定します。このファイルの中の引数はすべて、大文字と小文字が区別されます。
6. デフォルトの構成ファイルを次のように変更します。
   - RSA SecurID 認証を受けるユーザを指定します。

- TACACS+ 構成オプションを設定します。
- クライアント / サーバ通信を保護する暗号鍵を指定します。

サンプルの **sdtacplus** 構成ファイルを参照して、構成ファイル内で RSA SecurID ユーザを指定する方法と、TACACS+ 構成オプションを設定する方法を確認してください。

7. クライアント / サーバ通信を暗号化するには、構成ファイルに次のような行を指定する必要があります。

```
key = old+gnu$8a1u
```

old+gnu$8a1u は、ユーザが定義した鍵の例です。鍵に空白が含まれる場合は、鍵全体を二重引用符で囲んでください。

メモ : ユーザが定義した鍵は、各 TACACS+ クライアント デバイス上の構成ファイルに入力する必要があります。さらに、クライアント / サーバ通信の暗号化の種類を DES に設定する必要があります。

8. 変更した **sdtacplus.arg** ファイルと **sdtacplus.cfg** ファイルを、レプリカの ***ACEDATA*** ディレクトリにコピーします。

9. **aceserver** プロセスを停止せずに TACACS+ 構成ファイルを再び読み取るには、次のコマンドを実行します。

```
kill -USR1 (pid)
```

(pid) は、**_sdtacplusd** のプロセス id です。この機能は、TACACS+ の 'cfg' テーブルを変更するときに特に効果的です。

TACACS+ 引数ファイルのサンプル

```
#################################################################
#                    ACE/Server TACACS+ command line argument file
#
#################################################################
# This file or one patterned after it should be kept as sdtacplus.arg
# Customize your TACACS+ application by choosing the desired options
# Specify the name of the optional TACACS+ configuration file.See your Cisco
# manual for complete details.
-Csdtacplus.cfg
# To make sure that this TACACS+ configuration file has no errors, uncomment
# the following line.When you run _sdtacplusd, this file will be read and
# processed, but the server will terminate itself afterwards.
# -P
# Disallow TACACS+ forking, thus only runs single threaded
# -g
# Allows the user to specify an alternate prompt string to Enter PASSCODE:
# for password logins.If nothing is specified, displays Enter PASSCODE:
# under current schema
# -mEnter Password:
# Display the version number and exit
# -v
# ======================================================
# Normally, only messages at error level or above are written to syslog.
# To write TACACS+ info messages to the syslog, this option takes a
parameter
# based on a sum of the following options:
#number information about
# 1     general
# 2     parsing
# 4     forking
# 8     authorization
# 16    authentication
# 32    passwords
# 64    accounting
# 128   configuration
# 256   packet
# 512   hex
# 1024  md5 hash
# 2048  xor
# 4096  clean
# 8192  subst
#
# For more information on the various debug flags, see your Cisco manual.
# -d16383
# Write TACACS+ info/debug messages to the console (only when -d set).
# -t
# ======================================================
#################################################################
```

TACACS+ 構成ファイルのサンプル

TACACS+ 構成ファイルのデフォルトの場所と名前は ***ACEDATA*/sdtacplus.cfg** です。このファイルは、TACACS+ スタートアップ ファイル (***ACEDATA*/sdtacplus.arg)** 内の行で指定されます。

構成値は次の形式で入力します (スペース、および大文字と小文字の区別に特に注意してください)。

```
#################################################################
#                     ACE/Server TACACS+ configuration file
#
#################################################################
# This file or one patterned after it should be kept as sdtacplus.cfg
# Customize your TACACS+ application by uncommenting the desired lines in
# this file
# Refer to Cisco manual for additional configuration of TACACS+
# The following are examples of different TACACS+ configurations
#
# Encryption key is used to secure communication between sdtacplus daemon
# and NAS and is recommended to be used
# If the following encryption key is used, issue command
# ”tacacs-server key your_encryption_key” on the NAS
# key = ”your_encryption_key”
#To write all accounting data sent from the access server into file
# /var/tmp/accounting.log on the TACACS+ server  uncomment the
# following line
# accounting file = /var/tmp/accounting.log
# default authorization = permit
# Add users:testuser1 - testuser3 to the ACE/Server Database
# to enable SecurID authentication.Also add both the name of your
# router/comm server and the UNIX client to the client table;
# user = testuser1
# {
# member of group secure
#member = secure
#individual user declaration can be used to override the group settings
#for instance the following login selection will override group
#”secure” login
# and will use regular password ”whatever” instead of SecurID PASSCODE
#login = cleartext whatever
# following restricted telnet command will allow access only to the range
# of ip addresses from 111.1.1.1 to 111.1.1.9;
# Note:This will deny telnet access to other ip addresses
# Issue command ”aaa authorization commands 1 tacacs+ if-authenticated”
# or ”aaa authorization commands 15 tacacs+ if-authenticated” on the NAS
#        cmd = telnet
#       {
#       permit ”111¥.1¥.1¥.[1-9] ”
#       }
# }
# user = testuser2
# {
#Use DES encrypted password ”securid” to login to NAS
#login = des xAWcPaFGcWp8g
```

```
# When using PPP to connect to NAS issue following commands first:
# For selected line (ex. line 1) on NAS:
#”autoselect ppp”
# ”transport input all”
# ”rxspeed 19200”
# ”txspeed 19200”
# ”modem InOut”
# For selected asynchronous line (ex. interface async 1) on NAS:
# ”encapsulation ppp”
# ”async default ip address 111.1.1.116”
# ”async mode interactive”
# ”ppp authentication chap” or ”ppp authentication pap”
# If CHAP authentication is used with PPP uncomment the following line;
# chap = cleartext chap_passwd
# When using PPP to connect to NAS issue following commands first:
# For selected line (ex. line 1) on NAS:
# ”autoselect ppp”
# ”transport input all”
# ”rxspeed 19200”
# ”txspeed 19200”
# ”modem InOut”
#        service = ppp protocol = ip {
# Assign local host the following ip address for PPP negotiations
#addr=111.1.1.116
#}
# }
# user = testuser3
# {
#member = secure
# }
# group = secure
# {
#login = securid
#        cmd = telnet
#{
#
# Deny telnet access to 222.2.(any extension).1
#deny ”222¥.2¥.[0-9]+¥.1 ”
# Allow telnet to the rest of ip addresses
#permit .*
# }
# }
```

Cisco Systems 社の TACACS+ クライアント デバイスの構成

メモ：構成中に TACACS+ コマンドについてのヘルプ情報が必要な場合は、次のように入力してください。

```
tacacs ?
```

Cisco Systems 社の TACACS+ デバイスを構成するには

1. クライアント デバイスにログオンし、「enable」(および必要に応じてパスワード) と入力して、権限モードを開始します。

   クライアントが RSA SecurID の保護を受けている状態で権限モードを開始するには、ユーザがサイト管理者として RSA Authentication Manager データベースに登録されている必要があり、そのユーザのタスク リストにクライアントを編集する権限が割り当てられている必要があります。

2. 現在の構成を確認するには、次のコマンドを入力します。

   ```
   show config
   ```

3. 次のコマンドを入力して、ターミナルから Configuration モードを開始します。

   ```
   config t
   ```

4. 次のコマンドを入力して、TACACS+ サーバの IP アドレスとホスト名を関連付けます。

   ```
   ip host hostname ip-address
   ```

   hostname には、*ip-address* というアドレスを持つホスト マシンの名前を指定します。このステップは省略してもかまいません。ただし、このステップを省略すると、この後のすべてのステップで、ホストを指定するときに、その IP アドレスで参照しなければなりません。これ以降のステップでは、ホスト名と IP アドレスの関連付けが行われているものとします。以下に例を示します。

   ```
   ip host cassatt 192.168.10.23
   ```

   レプリカ Authentication Manager についても、同じ関連付けを行います。

5. 次のコマンドを入力して、このホストが TACACS+ サーバ ホスト名として使用されることを指定します。

   ```
   tacacs-server host hostname
   ```

   クライアント デバイスから TACACS+ および RSA Authentication Manager 認証を削除するには、次のコマンドを入力します。

   ```
   no tacacs-server host hostname
   ```

   サーバを実行しているホストを変更するには、上に示したコマンドで最初にホスト名を削除し、次のコマンドで新しいホスト名を定義します。

   ```
   tacacs-server host newhostname
   ```

6. レプリカの場合は、別の ***tacacs-server host*** コマンドでレプリカ Authentication Manager ホスト名を指定します。

   Authentication Manager ホスト名を指定する順序によって、クライアント デバイスが有効な RSA Authentication Manager を検索する順序が決まります。

7. TACACS で保護されているライン上で実行できるログオンの試行回数を設定します。RSA Authentication Manager のデフォルト設定では、試行が 3 回失敗すると、接続は切断されます。クライアント デバイスにも独自の再試行制限があります。**2 つの制限値のうち、小さい方の値が優先されます。**

   切断までに 3 回の試行を認めるという設定は、ユーザの利便性とセキュリティのバランスをとる上で適切な設定です。さらにセキュリティを向上するには、この回数を減らします。ただし、回数を減らすと、PASSCODE を間違って入力したユーザは、ログオン セッションを再起動しなければならなくなるため、ログオン時の操作が煩雑になります。

   回線のノイズやネットワーク トラフィックの増大によって、有効なログオンが正しく認識されない可能性がある場合は、許容再試行回数を増やします。ただし、この値より、***ACEDATA*/sdconf.rec** に格納されている RSA Authentication Manager Agent Retry 回数の方が優先されることに注意してください。

   新しい許容試行回数を設定するには、次のコマンドを入力します。

   ```
   tacacs-server attempts count
   ```

   count には、試行回数を指定します。デフォルト値 (3) に戻すには、次のコマンドを入力します。

   ```
   no tacacs-server attempts
   ```

8. 再試行制御値を設定します。これは、クライアント デバイスが稼動中の Authentication Manager を検出するために、RSA Authentication Manager ホスト リスト全体を検索する回数です。

   デフォルト値は 2 回であり、これはユーザの利便性とセキュリティのバランスをとる上で適切な設定です。さらにセキュリティを向上するには、この回数を減らします。ただし、回数を減らすと、最初の試行で Authentication Manager が見つからないときにセッションを再起動しなければならなくなるため、ログオン時の操作が煩雑になります。

   回線のノイズやネットワークの混雑によって、Authentication Manager の存在が正しく認識されない可能性がある場合は、許容再試行回数を増やします。

   新しい再試行回数を設定するには、次のコマンドを入力します。

   ```
   tacacs-server retransmit retries
   ```

   retries には、再試行回数を指定します。デフォルト値 (2) に戻すには、次のコマンドを入力します。

   ```
   no tacacs-server retransmit
   ```

9. クライアントが RSA Authentication Manager からの応答を待つ秒数を指定します。Cisco Systems 社のデバイスのデフォルト値は 5 秒です。ただし、回線の混雑やノイズによって発生するタイムアウトを防ぎ、ネクスト トークンコード プロシージャの際のパフォーマンスを向上するには、値を 10 秒以上に設定することをお勧めします。ユーザが PASSCODE を入力してから「Access Denied (アクセスが拒否されました)」メッセージが表示され、ユーザ名を求めるプロンプトが再表示されるまでに長い時間がかかる場合は、値を 10 秒以上に設定します。

   秒数を増やすには、次のコマンドを入力します。

   ```
   tacacs-server timeout seconds
   ```

   seconds には、応答を待つ秒数を指定します。

10. デバイスで TACACS+ を有効にするには、次の行を追加します。

    ```
    aaa new-model
    ```

保護する各ラインで使用される認証方法 (RSA SecurID 認証など) をリスト形式で指定します。構文は次のとおりです。

```
aaa authentication login default [ または list_name] method 1 ...
method 4
```

4 つの方法を指定できます。指定できる値は次のとおりです。

```
tacacs+   TACACS+ を使用します。
line      ライン パスワードを使用します。
enable    enable パスワードを使用します。
none      認証を使用しません。
```

none は使用しないようにしてください。

各方法は指定されている順に実行されます。認証情報が不正だったためではなく、デバイスまたはネットワークの障害が原因で、最初の方法が失敗した場合のみ、次の方法が試みられます。最初に TACACS+ を指定し、次にライン パスワードを指定するのが最も安全な順序です。次の順序で指定することをお勧めします。

```
aaa authentication login securid tacacs+
aaa authentication login securid2 tacacs+ line
```

list_name **securid** は、TACACS+ を唯一の認証方式として指定しています。**securid** が指定されている場合、ユーザがログオンすると、RSA SecurID PASSCODE の入力が求められます。失敗すると、アクセスは拒否されます。

list_name **securid2** は、TACACS+ を最初の認証方式として指定しています。TACACS+ サーバへのネットワーク接続が動作していなかったり、TACACS+ サーバが稼動していないなどの理由で認証に失敗すると、list_name **securid2** の 2 番目の認証方法が使用されます。**securid2** が指定されている場合、ユーザがログオンすると、RSA SecurID PASSCODE の入力が求められます。この方法が失敗すると、パスワードの入力が求められます。list_name **securid2** で保護されるラインに対して指定されているパスワードを入力します。**securid2** の使い方については、次のステップを参照してください。

メモ：TACACS+ 認証で間違った PASSCODE を入力することは、**失敗**ではなく、**エラー**と呼びます。ユーザが入力した RSA SecurID 認証情報にエラーがある場合、次の代替認証方式が起動されることはありません。

11. 保護するクライアント デバイス ライン上で RSA SecurID 認証を有効にします。コンソール ポートに接続されているターミナルに対して、次のコマンドを入力します。

```
line con 0 password <password>
login authentication securid2
```

list_name **securid2** は、コンソール ポートを構成する場合のみ使用します。**securid2** が指定されている場合、RSA SecurID による認証に失敗すると、アクセスを許可するかどうかはパスワードによって判断されます。**aceserver** が実行されていない場合や、Authentication Manager への接続が切断されている場合でも、管理者は、コンソール ポートに対して定義されているパスワードを使用して、コンソール ポート経由でクライアント デバイスにログオンできます。

補助ポートに接続しているターミナルに対して、次のコマンドを入力します。

```
line aux 0
login authentication securid
```

番号 0 ～ ***max*** の仮想ラインに接続しているターミナルに対して、次のコマンドを入力します。

```
line vty 0 max
login authentication securid
```

max の値は、クライアント デバイスの構成によって異なります。

12. 特定の仮想ラインを保護しないようにするには、各ラインを個別に構成します。たとえば、次のように構成します。

```
line vty 0 2
login authentication securid

line vty 3
password xyzzy
login authentication line

line vty 4 max
login authentication securid
```

この場合、仮想ライン 3 には、パスワード xyzzy を使用してアクセスします。ライン 3 へのアクセスは、RSA Authentication Manager の制御を受けません。デバイス内の他のすべての仮想ラインは、RSA SecurID 認証を要求します。

デバイスと RSA Authentication Manager との間の接続が失われた場合に備えて、このような構成を実装します。これは、プライマリが 1 台だけでレプリカがない場合に特に重要です。1 台しかない Authentication Manager のハードウェアが故障し、修理に時間がかかるような場合、すべてのラインに RSA SecurID 認証が設定されていると、保護されているデバイスに誰もアクセスできません。

ラインに RSA Authentication Manager 認証の保護を設定しない場合は、別の方法でそのラインを保護するようにしてください。少なくとも、そのラインに接続しているターミナルが物理的に安全な場所に設置されていることが必要です。

13. ルータではなく、仮想ライン、コンソール ライン、および補助ラインを備えているコミュニケーション サーバを使用している場合は、次のコマンドを使用して、番号 0 ～ ***max*** のラインに対して RSA SecurID 認証を設定します。***max*** の値は、コミュニケーション サーバの構成に応じて異なります。次のコマンドを入力します。

```
line 0 max
login authentication securid
```

各ラインを個別に構成することもできます。

```
line 0
login authentication securid

line 1
login authentication securid2

line 2 max
login authentication securid
```

上の構成の場合、ライン 1 には 1 番目の方法として TACACS+ RSA SecurID 認証が設定され、2 番目の方法として list_name **securid2** に定義されているライン パスワードが設定されます。Authentication Manager が正常に動作しなかったり、ネットワーク接続が切断されたために RSA SecurID 認証が失敗する場合に備えて、管理者にパスワードを求めるプロンプトが表示されるようにしておくと便利です。

list_name **securid2** は、管理者が使用するラインを構成する場合にだけ使用します。**securid2** が指定されている場合、RSA SecurID による認証に失敗すると、アクセスを許可するかどうかはパスワードによって判断されます。Authentication Manager が動作していない場合や、Authentication Manager への接続が切断されている場合でも、管理者は、ラインに対して定義されているパスワードを使用して、このライン経由でクライアント デバイスにログオンできます。

14. TACACS+ では、クライアントと Authentication Manager の間でやり取りされるメッセージがクリア テキストで送信されないように、暗号化できます。通信を暗号化するには、次に示すような行をクライアントの構成ファイルに追加します。

    ```
    tacacs-server key 1234abcd
    ```

    1234abcd は暗号鍵の例です。Authentication Manager の構成ファイルと他の TACACS+ クライアントの構成ファイルに、同じ鍵を入力します。

    この時点で、新しい構成パラメータはすべて設定され、その値は有効になっていますが、まだ保存されていません。値の保存はステップ 16 で行います。CTRL+Z キーを押して Configuration モードを終了します。

15. 構成を保存する前に、選択したオプションをテストし、予想したとおりの動作をするかどうか確認します。たとえば、一連のログオンを実行して、ログオンの利便性の点でも、セキュリティの点でも、タイムアウトと再試行の値が自分の環境にとって最適であるかどうか確認します。

16. 次のコマンドを入力して設定を保存します。

    ```
    write memory
    ```

    重要： この操作を行わないと、クライアント デバイスの電源を切ったり、プラグを抜いたりしたときに、設定値が失われてしまいます。

    構成値をリモート ファイルに保存するには、Cisco Systems 社のマニュアルの **write network** コマンドの説明を参照してください。

    これで、TACACS+ クライアント デバイスの構成は完了です。Cisco Systems 社のアカウンティング機能またはオーソライゼーション機能を使用するには、Cisco Systems 社の構成マニュアルを参照してください。

Enable モードの保護

Enable モードを RSA SecurID で保護するには、このセクションの手順に従ってください。構成が終了した後、RSA Authentication Manager データベースにサイト管理者として登録され、タスク リストに TACACS+ クライアントのエージェント ホスト レコードを編集する権限が割り当てられているユーザは、RSA SecurID 認証を受けた後に Enable モードを開始できます。管理者でないユーザが Enable モードを開始しようとしても、「Enter PASSCODE (PASSCODE を入力してください)」プロンプトが表示されるだけで、アクセスできません。Enable モードを保護するには 2 つの方法があります。

- すべてのユーザを認証し、指定されている RSA Authentication Manager 管理者にのみ Enable モードの開始を許可する方法
- すべてのユーザに Enable モードの開始を許可するが、ユーザがレベル 15 コマンドを実行しようとするときに、RSA SecurID 認証を求める方法

なるべく、最初の保護方法を使用するようにしてください。

すべてのユーザの認証

Configuration モードで次のコマンドを入力します。

```
enable password password
aaa authentication enable default tacacs+ enable
```

Enable モードを開始できるのは、クライアントのエージェント ホスト レコードを編集できる権限がタスク リストに割り当てられているサイト管理者だけです。承認されていないユーザは、「Enter PASSCODE (PASSCODE を入力してください)」プロンプトが表示されても、Enable モードを開始できません。

RSA Authentication Manager が動作していなかったり、Authentication Manager への接続が切断されているなどの理由で、TACACS+ 認証が失敗した場合は、Enable パスワードを求めるプロンプトが表示されます。

レベル 15 コマンドを実行するユーザの認証

次のコマンドを入力します。

```
enable password password
aaa authorization commands 1 tacacs+
```

この場合、ユーザが「enable」と入力すると、Enable パスワードの入力が求められ、RSA SecurID 認証は行われません。ただし、ユーザがレベル 15 コマンドを実行しようとすると、TACACS+ 認証プロトコルによってのみチェックされます。

ユーザにすべてのコマンドの権限を与えるには、TACACS+ 構成ファイルに次の行を入力します。

```
user username {
default service = permit
}
```

他のユーザ レベル コマンドを中かっこで囲んで指定することもできますが、これらのコマンドは **default service = permit** の後の行に指定する必要があります。

6 Quick Admin ソフトウェアのインストール

この章では、RSA Authentication Manager Quick Admin ソフトウェアをインストールする方法について説明します。このソフトウェアを使用すると、システム管理者やヘルプ デスク管理者は Web ブラウザを使用して、RSA Authentication Manager プライマリ データベースに登録されているユーザ、トークン、および拡張レコード データを表示し、変更できます。

Quick Admin の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』および Quick Admin のオンライン ヘルプを参照してください。

Quick Admin アーキテクチャ

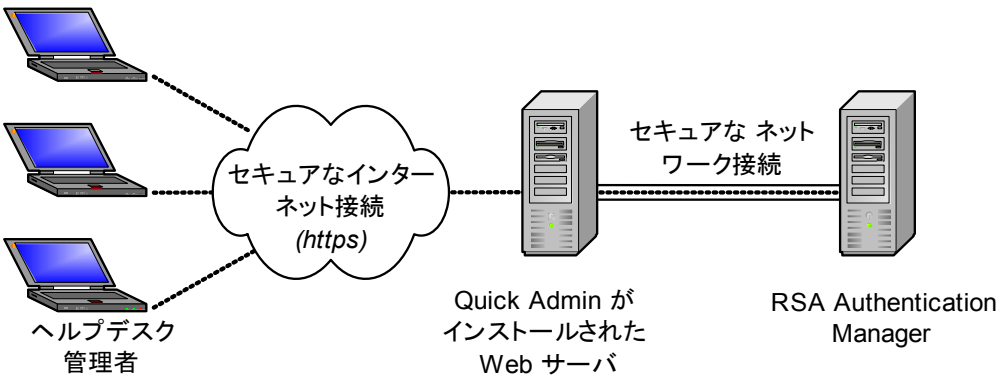
Quick Admin は以下で構成されています。

- Web サーバを通じてアクセス可能な Java サーブレット。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 デーモン。このデーモンは、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。

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。



システム要件

Quick Admin ユーザは、システムに Internet Explorer 5.5 (Service Pack 1) 以上、あるいは Netscape Communicator 6.22 または 7.1 をインストールし、画面の解像度を 800 × 600 ピクセル以上に設定する必要があります。さらに、ブラウザでページ キャッシュをオフにしてください。

Windows 2000 および Windows 2003

次の表は、Windows 2000 マシンまたは Windows 2003 マシンに Quick Admin をインストールするための要件の一覧です。

	Windows 2000	Windows 2003
Web サーバ (JavaScript が有効になっている必要があります)	Internet Information Server (IIS) 5.0	Internet Information Server (IIS) 6.0
Service Pack	Service Pack 4	なし

次の点に注意してください。

- ユーザ名とパスワードがクリア テキストで送信されないように、セキュリティに優れた通信方式 (**HTTPS**) を使用してください。
- Web サーバ ホストのセキュリティは、Microsoft 社が提供する最新のガイドラインに従って確保してください。IIS のセキュリティの詳細については、**www.microsoft.com/technet/** にある Microsoft TechNet を参照してください。

Solaris

Quick Admin は、Java System 6.1 Web サーバ (JavaScript 対応) を装備し、Solaris 9 を稼動している UltraSparc システムにのみインストールしてください。

次の点にも注意してください。

- ユーザ名とパスワードがクリア テキストで送信されないように、セキュリティに優れた通信方式 (**HTTPS**) を使用してください。
- Web サーバ ホストのセキュリティは、最新の Sun Microsystems 社のガイドラインに従って確保してください。詳細については、**http://docs.sun.com/db/prod/s1websrv** を参照してください。

インストール前のチェックリストと操作

チェックリスト

RSA Authentication Manager Quick Admin ソフトウェアをインストールする前に、次のファイルと情報が揃っていることを確認してください。

- ❑ RSA Authentication Managerプライマリの**RSA Authentication Manager¥data**ディレクトリにある **server.cer** ファイルのコピー。
- ❑ プライマリの **RSA Authentication Manager¥data** ディレクトリにある **sdti.cer** ファイルのコピー。
- ❑ プライマリの完全修飾 DNS 名。
- ❑ プライマリの IP アドレス。
- ❑ Quick Adminデーモン(**sdcommd**)が動作しているポート番号。デフォルト ポートは **5570** です。

  ポートの割り当てを変更するには、**RSA Authentication Manager¥prog** ディレクトリ内の **sdcommdconfig.txt** ファイル(Solarisの場合は**sdcommd.conf**)を編集します。

操作

RSA Authentication Manager プライマリ ホストで次の操作を実行します。操作の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

- ❑ **RSA Authentication Manager¥prog** ディレクトリ内の **hosts.conf** ファイルに次のエントリを追加します。Quick Admin Web サーバの完全修飾 (DNS) 名と IP アドレス、およびホスト名と IP アドレス。以下の例を参照してください。

  ```
  test.rsasecurity.com, 10.1.2.3
  test, 10.1.2.3
  ```

  メモ：変更を反映するには、RSA Authentication Manager を再起動する必要があります。

- ❑ 各 Quick Admin ユーザの管理者権限を **Administrator** に設定し、必要なタスク リストを割り当てます。
- ❑ RSA Authentication Manager のシステム パラメータで、リモート アドミニストレーションを有効に設定します。
- ❑ [スタート] > [設定] > [コントロール パネル] > [管理ツール] > [サービス]の順にクリックして、プライマリで RSA Authentication Manager Quick Admin デーモンが実行されていることを確認します。

Windows での Quick Admin のインストールと構成

Windows 2000 または Windows 2003 システムで Quick Admin を実行するには、ここで説明する手順に従って Quick Admin ソフトウェアをインストールし、Microsoft Internet Information Services (IIS) を構成する必要があります。

操作を開始する前に、Web サーバ ホスト システムにサポートされるバージョンの Microsoft IIS がインストールされていることを確認します。また、Tomcat を使用する他の製品が Web サーバ ホスト システムに現在インストールされていないことも確認します。

メモ: Web サーバ ホストにインストールされている Quick Admin のバージョンが古い場合は、新しいバージョンをインストールする前に、古いバージョンをアンインストールする必要があります。詳細については、65 ページの「旧バージョンから Quick Admin 6.1 へのアップグレード」を参照してください。RSA Quick Admin 6.1 と RSA SecurID WebExpress 1.3 を同じ Web サーバ ホストにインストールする場合は、65 ページの「同じシステムへの Quick Admin と Web Express のインストール」を参照してください。この場合は、両方の製品が同じ Tomcat サーブレット エンジンを共有します。

Quick Admin ソフトウェアを Windows 2000 または Windows 2003 にインストールするには

1. Web サーバ ホストの World Wide Web Publishing サービスを停止します。

   操作手順については、Internet Information Server (IIS) のマニュアルを参照してください。

2. RSA Authentication Manager 6.1 CD-ROM を Web サーバ ホストの CD-ROM ドライブに挿入し、CD-ROM の **QuickAdmin¥Windows** ディレクトリを参照します。

3. [quickadmin.exe] アイコンをダブルクリックします。

   Quick Admin Setup Wizard が表示されます。

4. 画面の指示に従って Setup Wizard を完了し、[Finish] をクリックします。

   セットアップで、“RSA Web Service” という名前の Windows サービスがインストールされることに注意してください。.

5. Microsoft IIS のバージョン (5 または 6) に応じて、ここで説明する適切な IIS 構成手順を実行します。

Tomcat サーブレット エンジンを使用して Microsoft IIS 5 を構成するには

1. Windows のコントロール パネルで、[管理ツール] > [インターネット インフォメーション サービス (IIS) マネージャ] の順にクリックします。

2. [IIS] ウィンドウの左側のナビゲーション パネルでローカル コンピュータ エントリを展開して、既定の Web サイトを表示します。

3. 既定の Web サイトとして、Quick Admin アプリケーションの仮想ディレクトリを指定します。

   - [IIS マネージャ] ウィンドウの左側のナビゲーション パネルで、既定の Web サイトを右クリックします。表示されるメニューで [新規作成] > [仮想ディレクトリ] の順に選択します。仮想ディレクトリの作成ウィザードが表示されます。

- [次へ] をクリックします。
- [エイリアス] テキスト ボックスに「tomcat」と入力し、[次へ] をクリックします。
- ***Quick Admin installation directory*¥Tomcat¥conf** ディレクトリを参照し、[次へ] をクリックします。
- [読み取り]、[ASP 等のスクリプトを実行する]、および [ISAPI アプリケーションや CGI 等を実行する] オプションを選択し、[次へ] をクリックします。
- [完了] をクリックします。

4. Quick Admin ISAPI Redirector を既定の Web サイトに追加します。
   - 既定の Web サイトを右クリックし、表示されるメニューで [プロパティ] を選択します。
   - [ISAPI フィルタ] タブを選択し、[追加] をクリックします。
   - フィルタ名として「tomcat」と入力します。
   - ***Quick Admin installation directory*¥Tomcat¥conf** ディレクトリを参照し、[isapi_redirector.dll] を選択し、[開く] をクリックします。
   - [OK] をクリックして [プロパティ] ダイアログ ボックスを閉じます。
5. Web サーバ ホストで必要なサービスを起動します。
   - Windows のコントロール パネルで、[管理ツール] > [サービス] の順にクリックします。
   - [サービス] ウィンドウで、以下の 3 つのサービスが起動していることを確認します。
     - IIS Admin Service
     - World Wide Web Publishing Service
     - RSA Web Service
   - 3 つのサービスのいずれかが停止している場合は起動してください。

Tomcat サーブレット エンジンを使用して Microsoft IIS 6 を構成するには

1. Windows のコントロール パネルで、[管理ツール] > [インターネット インフォメーション サービス (IIS) マネージャ] の順にクリックします。
2. [IIS] ウィンドウの左側のナビゲーション パネルでローカル コンピュータ エントリを展開して、既定の Web サイトを表示します。
3. 既定の Web サイトとして、Quick Admin アプリケーションの仮想ディレクトリを指定します。
   - [IIS マネージャ] ウィンドウの左側のナビゲーション パネルで、既定の Web サイトを右クリックします。表示されるメニューで [新規作成] > [仮想ディレクトリ] の順に選択します。
   - 仮想ディレクトリの作成ウィザードで [次へ] をクリックします。
   - [エイリアス] テキスト ボックスに「tomcat」と入力し、[次へ] をクリックします。
   - ***Quick Admin installation directory*¥Tomcat¥conf** ディレクトリを参照し、[次へ] をクリックします。

- [読み取り]、[ASP 等のスクリプトを実行する]、および [ISAPI アプリケーションや CGI 等を実行する] 権限を選択し、[次へ] をクリックします。
- [完了] をクリックします。

4. Quick Admin ISAPI Redirector を既定の Web サイトに追加します。
   - 既定の Web サイトを右クリックし、表示されるメニューで [プロパティ] を選択します。
   - [ISAPI フィルタ] タブを選択し、[追加] をクリックします。
   - フィルタ名として「tomcat」と入力します。
   - ***Quick Admin installation directory*¥Tomcat¥conf** ディレクトリを参照し、[isapi_redirector.dll] を選択し、[開く] をクリックします。
   - [ホーム ディレクトリ] タブを選択し、[設定] をクリックします。
   - [アプリケーションの構成] ダイアログ ボックスの [追加] をクリックします。
   - ***Quick Admin installation directory*¥Tomcat¥conf** ディレクトリを参照し、[isapi_redirector.dll] を選択し、[開く] をクリックします。
   - [拡張子] テキストボックスに次のように入力します。

     ```
     jsp
     ```

     [OK] をクリックします。
   - [OK] をクリックして [設定] ダイアログ ボックスを閉じます。
   - [OK] をもう一度クリックして [プロパティ] ダイアログ ボックスを閉じます。
5. Web サーバ拡張として Tomcat を追加します。
   - [IIS マネージャ] ウィンドウの左側のナビゲーション パネルで、[Web サービス拡張] を右クリックし、表示されるメニューで [新しい Web サービス拡張を追加] を選択します。
   - [拡張名] テキスト ボックスに「tomcat」と入力し、[追加] をクリックします。
   - ***Quick Admin installation directory*¥Tomcat¥conf** ディレクトリを参照し、[isapi_redirector.dll] を選択し、[開く] をクリックします。
   - [ファイルの追加] ダイアログ ボックスの [OK] をクリックします。
   - [拡張の状態を許可済みに設定する] オプションを選択します。
   - [OK] をクリックします。
6. Web サーバ ホストで必要なサービスを起動します。
   - Windows のコントロール パネルで、[管理ツール] > [サービス] の順にクリックします。
   - [サービス] ウィンドウで、以下の 3 つのサービスを確認します。
     - IIS Admin Service
     - World Wide Web Publishing Service
     - RSA Web Service
   - 3 つのサービスのいずれかが動作していない場合は起動してください。

Microsoft IIS の構成が完了すると、RSA Authentication Manager Quick Admin アプリケーションを使用できるようになります。

Quick Admin にログオンするには、Web ブラウザで **https://*servername*/quickadmin/** を指定します。*servername* は、Web サーバ ホストの名前です。

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。

Solaris での Quick Admin のインストールと構成

Solaris 9 システムで Quick Admin を実行するには、ここで説明する手順に従って Quick Admin ソフトウェアをインストールし、Sun Java Systems Web サーバを構成する必要があります。

操作を開始する前に、Web サーバ ホスト システムにサポートされる Sun Java Systems Web サーバがインストールされていることを確認します。また、Tomcat サーブレット エンジンを使用する他の製品が Web サーバ ホスト システムに現在インストールされていないことも確認します。

メモ：Web サーバ ホストにインストールされている Quick Admin のバージョンが古い場合は、新しいバージョンをインストールする前に、古いバージョンをアンインストールする必要があります。詳細については、65 ページの「旧バージョンから Quick Admin 6.1 へのアップグレード」を参照してください。RSA Quick Admin 6.1 と RSA SecurID WebExpress 1.3 を同じ Web サーバ ホストにインストールする場合は、65 ページの「同じシステムへの Quick Admin と Web Express のインストール」を参照してください。この場合は、両方の製品が同じ Tomcat サーブレット エンジンを共有します。

Solaris で Quick Admin をインストールするには

1. Web サーバ上のすべての Web サービスを停止します。
2. RSA Authentication Manager CD-ROM を Web サーバ ホストの CD-ROM ドライブに挿入します。
3. CD-ROM 上の次のディレクトリに移動します。

   ```
   /cdrom/cd_name/QuickAdmin/UNIX
   ```

   cd_name には、RSA Authentication Manager CD-ROM の名前を指定します。
4. 次のコマンドを入力します。

   ```
   ./quickadmin.sh
   ```

   Quick Admin セットアップ スクリプトが起動します。
5. 画面の指示に従います。
6. インストール スクリプトが終了したら、以下の手順に従って、Tomcat を使用して Web サーバを構成する必要があります。

Quick Admin 用に Java System (SunOne) 6.1 Web サーバを構成するには

1. ***web server installation directory*/https-*hostname*/config** ディレクトリに移動します。
2. テキスト エディタを使用して、**magnus.conf** ファイルを開き、ファイルの末尾に次のデータ行を入力します。

```
Init fn="load-modules" funcs="jk_init,jk_service" shlib="Quick
Admin Install Dir/Tomcat/conf/nsapi_redirector.so"

Init fn="jk_init" worker_file="Quick Admin Install Dir/
Tomcat/conf/workers.properties" log_level="error"
log_file="Quick Admin Install Dir/Tomcat/logs/nsapi.log"
```

3. 変更を保存し、**magnus.conf** ファイルを閉じます。
4. **obj.conf** ファイルを開き、**<Object name="default">** タグの直後に次のデータ行を入力します。

```
NameTrans fn="assign-name" from="/quickadmin" name="rsaweb"

NameTrans fn="assign-name" from="/quickadmin/*" name="rsaweb"

NameTrans fn="assign-name" from="/jsp-examples" name="rsaweb"

NameTrans fn="assign-name" from="/jsp-examples/*" name="rsaweb"

NameTrans fn="assign-name" from="/servlets-examples"
name="rsaweb"

NameTrans fn="assign-name" from="/servlets-examples/*"
name="rsaweb"
```

5. **obj.conf** ファイルの末尾に、次の行を追加します。

```
<Object name="rsaweb">

ObjectType fn=force-type type=text/plain

Service fn="jk_service" worker="RSAWorker"

</Object>
```

6. 変更を保存し、**obj.conf** ファイルを閉じます。
7. ***Quick Admin installation directory*/Tomcat/bin** ディレクトリに移動し、次のコマンドを使用して Tomcat を起動します。

```
./startup.sh
```

8. Java Systems (SunOne) Web サーバを起動します。

これで、Solaris Web サーバ ホストに RSA Authentication Manager Quick Admin がインストールされ、構成されました。

Quick Admin にログオンするには、**https://*servername*/quickadmin/** を参照します。*servername* は、Web サーバ ホストの名前です。

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。また、Tomcat をいったん停止して再起動する必要がある場合は、Java Systems (SunOne) Web サーバもいったん停止して再起動してください。

旧バージョンから Quick Admin 6.1 へのアップグレード

Quick Admin 5.2 または 6.0 から Quick Admin 6.1 にアップグレードするには、プラットフォームに応じて、次のいずれかの手順を使用します。

Windows マシンの場合

Windows マシンで Quick Admin をアップグレードするには

メモ：アップグレードの実行時に、Quick Admin ディレクトリを使用している管理者がいないことを確認します。

1. Quick Admin 5.2 または 6.0 を Web サーバ ホストから完全にアンインストールします。
   アンインストールする前に、Quick Admin に関連するすべてのサービスを停止してください。詳細については、『RSA ACE/Server 5.2 for Windows インストール ガイド』または『RSA Authentication Manager 6.0 for Windows インストール ガイド』を参照してください。
2. 60 ページの「Windows での Quick Admin のインストールと構成」の説明に従って、Quick Admin 6.1 をインストールします。

Solaris マシンの場合

Solaris マシンで Quick Admin をアップグレードするには

メモ：アップグレードの実行時に、Quick Admin ディレクトリを使用している管理者がいないことを確認します。

1. Quick Admin 5.2 または 6.0 を Web サーバ ホストからアンインストールします。
   アンインストールする前に、Quick Admin に関連するすべてのサービスを停止してください。詳細については、『RSA ACE/Server 5.2 for UNIX インストール ガイド』または『RSA Authentication Manager 6.0 for UNIX インストール ガイド』を参照してください。
2. 63 ページの「Solaris での Quick Admin のインストールと構成」の説明に従って、Quick Admin 6.1 をインストールします。

同じシステムへの Quick Admin と Web Express のインストール

Quick Admin 6.1 と Web Express 1.3 はいずれも、Apache Software Foundation Tomcat 5.5.7 サーブレット エンジンを使用し、同じ Web サーバ ホストで実行できます。同じホストで実行する場合、これらのアプリケーションは同じバージョンの Tomcat を共有します。

Web Express 1.3 のインストールと構成については、使用しているプラットフォームの『RSA Web Express 1.3 Installation and Configuration Guide』を参照してください。

重要 : 以前のバージョンの Quick Admin および Web Express は、Macromedia 社の JRun サーブレット エンジンを使用しており、新しい Tomcat ベースのバージョンとは互換性がありません。新しいバージョンをインストールする前に、古いバージョンの Quick Admin および Web Express を Web サーバ ホストからアンインストールしてください。古いバージョンの Quick Admin のアンインストールについての詳細は、使用しているプラットフォームの『RSA ACE/Server 5.2 for UNIX インストール ガイド』または『RSA Authentication Manager 6.0 for UNIX インストール ガイド』を参照してください。古いバージョンの Web Express のアンインストールについての詳細は、使用しているプラットフォームの『RSA Web Express 1.3 Installation and Configuration Guide』を参照してください。

Quick Admin 6.1 をインストールするには、プラットフォームに応じて、次のいずれかの手順を使用します。

Windows マシンの場合

Windows に Web Express 1.3 がインストールされている状態で Quick Admin 6.1 をインストールするには

1. Windows のコントロール パネルで、[管理ツール] > [サービス] の順にクリックし、Web サーバ ホストで以下のサービスを停止します。
   - World Wide Web Publishing Service
   - RSA Web Service
2. RSA Authentication Manager 6.1 CD-ROM を Web サーバ ホストの CD-ROM ドライブに挿入し、CD-ROM の **QuickAdmin¥Windows** ディレクトリを参照します。
3. [quickadmin.exe] アイコンをダブルクリックします。
   Quick Admin Setup Wizard が表示されます。
4. 画面の指示に従って Setup Wizard を完了し、[Finish] をクリックします。
5. Windows のコントロール パネルで、[管理ツール] > [サービス] の順にクリックし、Web サーバ ホストで以下のサービスを再起動します。
   - World Wide Web Publishing Service
   - RSA Web Service

Solaris マシンの場合

Solaris に Web Express 1.3 がインストールされている状態で Quick Admin 6.1 をインストールするには

1. Web サーバ上のすべての Web サービスを停止します。
2. RSA Authentication Manager CD-ROM を Web サーバ ホストの CD-ROM ドライブに挿入します。
3. CD-ROM 上の次のディレクトリに移動します。
   ```
   /cdrom/cd_name/QuickAdmin/UNIX
   ```
   cd_name には、RSA Authentication Manager CD-ROM の名前を指定します。
4. 次のコマンドを入力します。

```
./quickadmin.sh
```

Quick Admin セットアップ スクリプトが起動します。

5. 画面の指示に従います。
6. Web サーバですべての Web サービスを再起動します。

Quick Admin の設定の変更

Quick Admin 環境を変更する必要がある場合は、**quickadminconfig.properties** ファイルを編集しなければなりません。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。

次の表は、変更できるパラメータの一覧です。これらの値の多くはインストール時に設定されます。変更する場合は、十分注意してください。また、properties ファイルの **##DO NOT MODIFY##** セクション内のパラメータは変更しないでください。

表に示したディレクトリ パスは、***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin** ディレクトリを基準にした相対パスです。

メモ：quickadminconfig.properties ファイルを変更した場合は、RSA Web Services (Tomcat) をいったん停止して再起動することで、変更を反映する必要があります。

Quick Admin の設定

パラメータ	値
ACE_SERVER	RSA Authentication Manager プライマリの完全修飾名。
ACE_IP	RSA Authentication Manager プライマリの IP アドレス。
CERT_PATH	RSA Authentication Manager プライマリから、**sdti.cer** および **server.cer** ファイルのコピーを格納しているディレクトリへのパス。 デフォルト パスは **certs/** です。 複数のプライマリから証明書を追加する手順については、73 ページの「複数のプライマリ サーバの管理」を参照してください。
ACE_PORT	RSA Authentication Manager Quick Admin デーモンがリスニングしているプライマリ TCP ポート。 デフォルト ポートは **5570** です。
REPORT_PATH	Quick Admin がレポート ファイルを書き込むディレクトリへのパス。 デフォルト パスは **reports/** です。 **重要：**レポートを実行するたびに新しいテキスト ファイルが作成されるので、定期的に **reports** ディレクトリの内容を削除して、ディスク容量を確保するようにしてください。

パラメータ	値
PROP_PATH	**quickadminconfig.properties** ファイルを格納しているディレクトリへのパス。 デフォルト パスは **properties/** です。
MAX_SEARCH	ユーザが RSA Authentication Manager データベースを検索するときに返されるオブジェクト (ユーザ レコードやトークン レコードなど) の最大数。 この値は、ユーザが検索を実行する場合の Quick Admin アプリケーションのパフォーマンスに大きく影響します。あまり大きな値を設定すると、アプリケーションのパフォーマンスが低下します。 このパラメータのデフォルト値は **150** です。
MAX_REPORT	ユーザがレポートを作成するときに返されるオブジェクト (ユーザ レコードやトークン レコードなど) の最大数。 この値は、ユーザがレポートを作成する場合の Quick Admin アプリケーションのパフォーマンスに大きく影響します。あまり大きな値を設定すると、アプリケーションのパフォーマンスが低下します。 このパラメータのデフォルト値は **300** です。
HTML_SRC	ユーザに対して表示されるフォームを作成するときに Quick Admin アプリケーションが使用する HTML テンプレートを格納しているディレクトリへのパス。 デフォルト パスは **quickadmin/** です。 **メモ : quickadmin/** は、***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin** ディレクトリを基準にした相対パスでは**ありません**。

パスワード トークンの有効期限の設定

メモ：各パスワード パラメータに設定する値によって、他のパスワード パラメータに設定した値の意味が変わります。詳細については、71 ページの「パスワード トークンの有効期限の設定が相互に及ぼす影響」を参照してください。

パラメータ	値
USER_PWD_LIFETIME_DAYS USER_PWD_LIFETIME_HOURS	ユーザ パスワードの有効期限が切れるまでの日数と時間を指定します。日数、時間、または日数と時間の両方を設定できます。 たとえば、USER_PWD_LIFETIME_DAYS=5 および USER_PWD_LIFETIME_HOURS=3 を指定すると、ユーザ パスワードの有効期限は 123 時間で切れます。 指定できる値は、0 ～ 8760 日、0 ～ 23 時間の範囲です。 時間と日数を組み合わせて指定する場合、8760 日、つまり 24 年を超える値は指定できません。 これらのパラメータのデフォルト値は次のとおりです。 USER_PWD_LIFETIME_DAYS=30 USER_PWD_LIFETIME_HOURS=0
LOST_TOKEN_CONTROL_FLAG	紛失したトークンのユーザ パスワードに設定されている日数と時間を、Quick Admin インタフェースで変更できるかどうかを指定します。**fixed** に設定されている場合、日数と時間をインタフェースで変更できません。未定義であったり、コメント アウトされている場合は、日数と時間をインタフェースで変更できます。 デフォルト設定は未定義です。
LOST_TOKEN_PWD_LIFETIME_DAYS LOST_TOKEN_PWD_LIFETIME_HOURS	紛失したトークンの代わりに提供されたユーザ パスワードの有効期限が切れるまでの日数と時間を指定します。日数、時間、または日数と時間の両方を設定できます。この設定は固定パスワードとワンタイム パスワードの両方に適用されます。 たとえば、LOST_TOKEN_PWD_LIFETIME_DAYS=5 および LOST_TOKEN_PWD_LIFETIME_HOURS=3 を指定すると、ユーザ パスワードの有効期限は 123 時間で切れます。 指定できる値は、0 ～ 8760 日、0 ～ 23 時間の範囲です。 時間と日数を組み合わせて指定する場合、8760 日、つまり 24 年を超える値は指定できません。 これらのパラメータのデフォルト値は次のとおりです。 LOST_TOKEN_PWD_LIFETIME_DAYS=7 LOST_TOKEN_PWD_LIFETIME_HOURS=0 紛失したトークンの代わりに使用するテンポラリ パスワードの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

パラメータ	値
FIXED_PWD_LIFETIME_DAYS FIXED_PWD_LIFETIME_HOURS	紛失したトークンの代わりに提供された固定パスワードの有効期限が切れるまでの日数と時間を指定します。固定パスワードは、有効期限が切れるまで繰り返し使用できます。このパラメータを設定すると、固定パスワードに適用される LOST_TOKEN_PWD_LIFETIME_DAYS パラメータと LOST_TOKEN_PWD_LIFETIME_HOURS パラメータを無効にすることができます。 日数、時間、または日数と時間の両方を設定できます。 たとえば、FIXED_PWD_LIFETIME_DAYS=5 および FIXED_PWD_LIFETIME_HOURS=3 を指定すると、ユーザ パスワードの有効期限は 123 時間で切れます。 指定できる値は、0 ～ 8760 日、0 ～ 23 時間の範囲です。 時間と日数を組み合わせて指定する場合、8760 日、つまり 24 年を超える値は指定できません。 これらのパラメータのデフォルト値は次のとおりです。 FIXED_PWD_LIFETIME_DAYS=7 FIXED_PWD_LIFETIME_HOURS=0
OTP_PWD_LIFETIME_DAYS OTP_PWD_LIFETIME_HOURS	紛失したトークンの代わりに提供されたワンタイム パスワード (OTP) セットの有効期限が切れるまでの日数と時間を指定します。ワンタイム パスワードはそれぞれ 1 回だけ使用でき、指定した日付に有効期限が切れます。日数、時間、または日数と時間の両方を設定できます。このパラメータを設定すると、OTP に適用される LOST_TOKEN_PWD_LIFETIME_DAYS パラメータと LOST_TOKEN_PWD_LIFETIME_HOURS パラメータを無効にすることができます。 たとえば、OTP_PWD_LIFETIME_DAYS=5 および OTP_PWD_LIFETIME_HOURS=3 を指定すると、ユーザ パスワードの有効期限は 123 時間で切れます。 指定できる値は、0 ～ 8760 日、0 ～ 23 時間の範囲です。 時間と日数を組み合わせて指定する場合、8760 日、つまり 24 年を超える値は指定できません。 これらのパラメータのデフォルト値は次のとおりです。 OTP_PWD_LIFETIME_DAYS=7 OTP_PWD_LIFETIME_HOURS=0

パスワード トークンの有効期限の設定が相互に及ぼす影響

各パスワード パラメータに設定する値によって、他のパスワード パラメータに設定した値の意味が変わります。次の表は、各パスワード パラメータの設定が相互に及ぼす影響を示しています。

定義されているパラメータ	LOST_TOKEN_CONTROL_FLAG が FIXED に設定されている場合	LOST_TOKEN_CONTROL_FLAG が未定義の場合
なし	デフォルト値が適用される	デフォルト値が適用される
LOST	LOST で定義されている値が FIXED と OTP に適用される	LOST で定義されている値が FIXED と OTP に適用される
LOST FIXED	LOST で定義されている値が OTP に適用される	FIXED で定義されている値が OTP に適用される
LOST OTP	LOST で定義されている値が FIXED に適用される	LOST で定義されている値が FIXED と OTP に適用される
LOST FIXED OTP	FIXED と OTP で定義されている値が LOST で定義されている値を無効にする	FIXED で定義されている値が OTP に適用される
FIXED	デフォルト値が OTP に適用される	FIXED で定義されている値が OTP に適用される
OTP	デフォルト値が FIXED に適用される	LOST のデフォルト値が FIXED と OTP に適用される

Quick Admin のタイムアウトの設定

パラメータ	値
ACE_REPLY_TIMEOUT	Quick Admin が RSA Authentication Manager からの応答を待つ時間を指定します。この時間が過ぎるとエラー メッセージが返されます。 最大値：2147483647 値の単位はミリ秒 (100 = 1 秒) です。 デフォルト設定は 60000 です。
ACE_REPLY_RETRY	Quick Admin が RSA Authentication Manager からの応答をチェックする間隔を指定します。 最大値：2147483647 値の単位はミリ秒 (100 = 1 秒) です。 デフォルト設定は 500 です。

デバッグのオン / オフの設定

パラメータ	値
Verbose	Quick Admin、および RSA Authentication Manager との通信に関するデバッグ情報をログ ファイル (Solaris の場合は **catalina.out**、Windows の場合は **stdout_*date*.log**) に書き込むかどうかを指定します。Verbose フラグは、他のすべての *_Verbose フラグを無効にします。Verbose フラグで *_Verbose フラグが無効になるのを回避するには、行の先頭に # 記号を挿入します。以下の例を参照してください。 `#Verbose=no` ログ ファイルは通常、***Quick Admin installation directory*¥Tomcat¥logs** ディレクトリにあります。 ログ ファイルのサイズはすぐに大きくなるので注意してください。デバッグをオンにする場合は、ログ ファイルのサイズを必ず監視してください。 このパラメータのデフォルト値は **no** です。
Init_Verbose	Quick Admin スタートアップ ルーチンからのデバッグ情報をログ ファイル (Solaris の場合は **catalina.out**、Windows の場合は **stdout_*date*.log**) に書き込むかどうかを指定します。 Verbose フラグが他のすべての *_Verbose フラグを無効にすることに注意してください。 このパラメータのデフォルト値は **no** です。
Login_Verbose SearchPage_Verbose EditToken_Verbose EditUser_Verbose Report_Verbose EditExtension_Verbose	これらのパラメータは、対応する Quick Admin フォームに関連する処理からのデバッグ情報をログ ファイル (Solaris の場合は **catalina.out**、Windows の場合は **stdout_*date*.log**) に書き込むかどうかを指定します。 Verbose フラグが他のすべての *_Verbose フラグを無効にすることに注意してください。 たとえば、**EditUser_Verbose** パラメータに対して「yes」と入力すると、[Edit User] フォームでユーザが実行する操作に関する情報がファイルに書き込まれます。 これらのパラメータのデフォルト値は **no** です。

RSA Authentication Manager 通信設定の変更

RSA Authentication Manager プライマリと Quick Admin サーバとの間の通信は、プライマリの構成ファイルの設定で制御されます。

- RSA Authentication Manager プライマリが Windows 上で動作している場合は、設定は **RSA Authentication Manager¥prog¥sdcommdconfig.txt** ファイルにあります。
- RSA Authentication Manager プライマリが UNIX 上で動作している場合は、設定は **RSA Authentication Manager/prog/sdcommd.conf** ファイルにあります。

次の表は、構成ファイルの設定値の一覧です。

パラメータ	値
Windows port (UNIX の場合は TCP Port)	プライマリで RSA Authentication Manager Quick Admin デーモンが動作している TCP ポート。 デフォルト値は **5570** です。
Verbose	詳細なログ メッセージを Windows イベント ビューアまたは UNIX **syslog** に書き込むかどうかを指定します。 デフォルト値は **no** です。
Inactivity TimeOut	Quick Admin セッションのタイムアウトを制御します。ユーザが Quick Admin セッションを指定した時間だけオープンしたままにすると、セッションは自動的に閉じます。 インアクティビティ パラメータは、分単位で指定する必要があります。 デフォルト値は **15** です。 **重要：Inactivity TimeOut** の値は、Tomcat セッションのタイムアウト値より**大きな値に設定する必要があります**。セッション タイムアウト値は、***Quick Admin installation directory*¥Tomcat¥conf¥web.xml** ファイルまたは ***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥WEB-INF¥web.xml** ファイルに設定します。セッション タイムアウト値を両方のファイルに指定し、2 つの値が異なる場合には、2 番目のファイルに指定した設定が優先されます。セッション タイムアウト値を設定しておくと、RSA Authentication Manager Quick Admin デーモンがプライマリ サーバでタイムアウトになる前に、セッションがタイムアウトします。セッション タイムアウトを設定しないと、Quick Admin ユーザはセッションを正常に終了できないことがあります。

複数のプライマリ サーバの管理

Quick Adminでは、1つのQuick Adminサーバを通じて複数のRSA Authentication Managerプライマリを管理できます。

複数のプライマリ サーバに対して Quick Admin を使用するには

1. ***Quick Admin installation directory*¥Tomcat¥webapps¥quickadmin¥WEB-INF¥certs** ディレクトリの下に、サーバごとに新しいサブディレクトリを作成します。管理するプライマリごとにサブディレクトリを作成する必要があります。

   サブディレクトリの名前は、プライマリのホスト名と同じでなければなりません。たとえば、**cassatt** と **vermeer** というサーバに対して Quick Admin を使用するには、**cassatt** と **vermeer** という名前のサブディレクトリを作成します。

2. 各サーバの **RSA Authentication Manager¥data** ディレクトリから **sdti.cer** 証明書ファイルと **server.cer** 証明書ファイルのコピーを取得し、**certs** の下の該当するサブディレクトリに保存します。たとえば、サーバ **cassatt** の証明書ファイルは、**cassatt** サブディレクトリにコピーします。

3. Quick Admin にログオンしたら、ログオン ページの [Realm] ボックスにサーバ名を入力します。

   Quick Admin は、指定のプライマリに接続します。プライマリを指定しなかった場合は、Quick Admin のインストール時に指定したプライマリに接続します。

Quick Admin のアンインストール

Quick Admin をアンインストールするには、プラットフォームに応じて、次のいずれかのセクションを参照してください。

Windows マシンの場合

Quick Admin ソフトウェアを Windows マシンから削除するには

1. Windows のコントロール パネルで [プログラムの追加と削除] をダブルクリックします。
2. [RSA Quick Admin 6.1] を選択し、[削除] をクリックします。

   Quick Admin Setup Wizard が表示されます。
3. [Complete Uninstall] を選択し、[Next] をクリックします。

   重要： Web Express 1.3 がインストールされていて、ここでアンインストールしない場合は、[Complete Uninstall] の代わりに [Undeploy RSA Quick Admin 6.1] を選択します。
4. 画面の指示に従って Setup Wizard を完了し、[Finish] をクリックします。
5. システムを再起動します。

Quick Admin エントリを IIS から削除するには

重要： この Web サーバに Web Express 1.3 をインストールしたままにしておく場合は、この手順は実行しないでください。

1. Windows のコントロール パネルで、[管理ツール] > [インターネット インフォメーション サービス (IIS) マネージャ] の順にクリックします。
2. [IIS] ウィンドウの左側のナビゲーション パネルでローカル コンピュータ エントリを展開して、既定の Web サイトを表示し、既定の Web サイトをクリックして展開します。
3. 既定の Web サイトの下の [tomcat] を右クリックし、表示されるメニューで [削除] を選択します。
4. [IIS] ウィンドウの左側のナビゲーション パネルで、既定の Web サイトを右クリックし、表示されるメニューで [プロパティ] を選択します。
5. [ISAPI フィルタ] タブを選択します。
6. リストから [tomcat] フィルタを選択し、[削除] をクリックします。
7. [OK] をクリックします。

8. インターネット インフォメーション サービス (IIS) マネージャを終了します。

Solaris マシンの場合

Quick Admin ソフトウェアを Solaris マシンから削除するには

1. Tomcat サーブレット エンジンを停止します。
   - ***Quick Admin installation directory*/Tomcat/bin** ディレクトリに移動します。
   - 次のコマンドを入力します。

     ```
     ./shutdown.sh
     ```
2. Quick Admin を削除します。
   - Quick Admin インストール ディレクトリの親ディレクトリに移動します。
   - 次のコマンドを入力します。

     ```
     rm -rf Quick Admin installation directory
     ```

A RSA RADIUS サーバの移行

この付録では、次の方法について説明します。

- RSA Authentication Manager 6.1 へのアップグレードの一部として、以前のバージョンの RSA RADIUS サーバから RSA RADIUS サーバ 6.1 に移行する方法
- 既存の RSA RADIUS ユーザ拡張データを RSA RADIUS サーバ 6.1 で必要とされる形式に変換する方法

RSA RADIUS サーバ 6.1 への移行

ここでは、RSA Authentication Manager 6.1 へのアップグレードの一部として、6.1 より前のバージョンの RSA RADIUS サーバを RSA RADIUS サーバ 6.1 に移行するのに必要な操作について説明します。

RSA RADIUS 6.1 に移行するには

1. RSA RADIUS ユーザにユーザ拡張データを割り当てている場合は、テスト変換を実行します。操作手順については、78 ページの「テスト変換の実行」を参照してください。
2. RSA RADIUS サーバに対してプロンプトを設定している場合は、適切な ***ACEDATA*¥radius.cfg** ファイルのバックアップを作成します。
3. プライマリ Authentication Manager をアップグレードします。操作手順については、36 ページの「プライマリのアップグレードの準備」、および 37 ページの「プライマリのアップグレード」を参照してください。
4. **radius.cfg** ファイルをプライマリの ***ACEDATA*** ディレクトリにコピーします。
5. RSA RADIUS ユーザにユーザ拡張データを割り当てている場合は、完全な変換を実行します。操作手順については、79 ページの「完全な変換の実行」を参照してください。
6. レプリカ Authentication Manager をアップグレードします。操作手順については、37 ページの「レプリカのアップグレードの準備」、および 38 ページの「レプリカのアップグレード」を参照してください。
7. RSA RADIUS サーバ 6.1 をインストールします。操作手順については、『RSA RADIUS Server 6.1 Administrator's Guide』を参照してください。

RSA RADIUS ユーザ拡張データの変換

拡張レコードを使用すると、Authentication Manager プログラムの実行には必要ないものの、組織にとって役立つ追加データベース情報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 RADIUS サーバ 6.1 で必要とされるユーザ拡張データの形式は、以前のバージョンの RSA RADIUS サーバで必要とされる形式と異なります。以前のバージョンでは、ユーザ拡張データのキーの部分はどのような文字列でもかまいませんでした。6.1 では、キーは次の形式でなければなりません。

ATTR<*valid attribute number*>_<*unique identifier*>

新しい形式の詳細については、オンライン ヘルプを参照してください。

RADIUS 固有のユーザ拡張データを RSA RADIUS 6.1 に移行する場合は、**rsaextconv** プログラムを使用してデータを変換する必要があります。**rsaextconv** プログラムは、次の処理を行うコマンドライン ユーティリティです。

- 現在のキーをもとに、新しい拡張キーを作成します。
- プロファイル リンクを新しい拡張キーに設定します。
- 古い拡張キーを削除します。

テスト変換の実行

テスト変換では、実際の変換は行わずに、データベース内のユーザ拡張情報がどのように変更されるかだけを示します。テスト変換を行うことで、既存の問題を手動で解決できます。

重要：RSA Authentication Manager 6.1 にアップグレードする**前**に、既存のユーザ拡張データのテスト変換を行ってください。RSA Authentication Manager 6.1 にアップグレードした後、RADIUS サーバのプロファイルでアトリビュートと値の組み合わせを編集することはできません。

さらに、テスト変換を実行すると、RSA Authentication Manager 6.1 にアップグレードした後、RADIUS ユーザのためにどの程度のダウンタイムを見込めばよいかもあらかじめ計画することができます。

Remote Administration を通じてテスト変換を実行するには

1. 適切なサーバに対してRemote Administrationセッションを開き、RSA Authentication Manager 6.1 CD-ROM を CD-ROM ドライブに挿入します。
2. [File] > [Run Custom 4GL] の順にクリックします。
3. **<*CD drive*>:¥aceserv¥windows¥rsaextconv.p** を参照し、[OK] をクリックします。

テスト変換の結果は、***ACEPROG*¥progui¥rsaextconv.log** に記録されます。満足できる結果が得られたら、RSA Authentication Manager 6.1 にアップグレードし、その後、完全な変換を実行します。

完全な変換の実行

RSA Authentication Manager 6.1 に変換した後、RSA RADIUS サーバ 6.1 をインストールする前に、**rsaextconv** プログラムを実行して完全な変換を行います。

メモ：RSA Authentication Manager 6.1 にアップグレードする前に、テスト変換を実行していない場合は、次のコマンドを使用してテスト変換を実行できます。

```
ACEPROG/rsaextconv -f -d
```

テスト変換の結果は、***ACEPROG*¥rsaextconv.log** に記録されます。RSA Authentication Manager 6.1 にアップグレードした後、RADIUS サーバのプロファイルでアトリビュートと値の組み合わせを編集することはできません。

RSA Authentication Manager 6.1 で完全な変換を実行するには

次のコマンドを使用して、完全な変換を行います。

```
ACEPROG/rsaextconv -f -e
```

テスト変換の結果は、***ACEPROG*¥rsaextconv.log** に記録されます。

トラブルシューティング

次の表は、**rsaextconv** プログラムを実行するときに表示される可能性のある 4 種類のエラー メッセージと、各エラーへの対処法を示しています。

エラー メッセージ トピック	対処法
データベース関連	• 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、左側のメニューから [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。 • ネットワーク接続を確認します。 これらの方法で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ます。RSA セキュリティ正規販売代理店にご連絡ください。
パラメータ関連	79 ページの「完全な変換の実行」の説明を参照して、プロシージャをもう一度実行します。
サーバ ID 関連	次のサーバ情報が一致しているかどうか確認します。 • ネットワーク ID • レプリカ テーブル • 構成レコード
ログ ファイル関連	• ディスクが満杯でないかどうか確認します。 • 適切な権限があるかどうか確認します。

B カーネル パラメータの変更

RSA Authentication Manager は、UNIX オペレーティング システムの共有メモリ リソースを必要とします。この付録にはシステム パラメータの最小値の条件が記載されていますが、システムがその条件を満たさない場合は、UNIX カーネル構成値を変更しなければなりません。

この付録またはオペレーティング システムのマニュアルの説明を参照して、RSA Authentication Managerをインストールして操作するために最低限必要な値まで、UNIX リソースの設定値を大きくしてください。RSA Authentication Manager データベースへのアドミニストレーション接続を追加するには、値をさらに大きくしなければならない可能性があります。データベースへの接続を追加すると、より多くの Remote Administration セッションや RSA Quick Admin セッションを実行できます。

この付録に示されている最小値は、Authentication Manager が RSA Authentication Manager ソフトウェア専用であることを前提にしています。

システムをインストールし、実行している間、システム リソース エラーが報告されることは一般にありません。ただし、エラーが報告される場合は、ここで説明する手順を再び実行してください。値が小さすぎるというエラー メッセージが表示された場合は、設定値を 50% ほど大きくします。必要に応じて、この手順を繰り返します。パラメータ名では大文字と小文字が区別されるので、名前の指定や検索では、表に示されているとおりの名前を使用してください。

このセクションのすべての手順は、**root** ユーザでコンソールにログオンしている状態で実行します。

メモ：Red Hat Enterprise LINUX 3.0 では、カーネルを変更する必要はありません。

HP-UX のカーネル パラメータの変更

HP-UX のカーネル パラメータを変更するには

1. 現在のカーネル構成のバックアップを作成します。
2. 次のコマンドを使用して、システムをシングル ユーザ モードにします。

   ```
   shutdown
   ```

   カーネルの再構成が終了するまで、ユーザがシステムを利用しないようにしてください。
3. HP-UX システム アドミニストレーション ユーティリティを実行します。以下のメニュー項目を選択します。

   ```
   sam
   Kernel Configuration ->
   Configurable Parameters ->
   ```

4. [Configurable Parameters] リストで、各カーネル パラメータの値を確認して、必要に応じて変更します。各パラメータの値が必要最低限の値になるように変更します。データベースへのアドミニストレーション接続を増やす場合は、それに適した値に設定します。

メモ：semmni パラメータの値は、16 に設定することをお勧めします。RSA Authentication Manager は 3 セットのセマフォを必要とするため、オペレーティング システムの構成によっては、このパラメータの値をもっと大きな値に設定しなければならない場合があります。

パラメータ	最小値
nproc	640
shmmni	64
shmseg	16
shmmax	16777216
semmni	16
semmns	500
semmnu	500
max_threads_proc	300

変更するパラメータを強調表示するか、[Actions] メニューの [Modify Configurable Parameter] を選択します。ダイアログ ボックスが表示され、変更後のパラメータの値を入力するよう求められます。

```
highlight parameter
Actions -> Modify Configurable Parameter
```

5. [Actions] メニューの [Create a New Kernel] を選択して、新しいカーネルをコンパイルします。カーネルをビルドしてコンピュータを再起動するよう指示されます。「Yes」と応答します。変更前のカーネルは **/SYSBCKUP** として自動的にバックアップされます。

```
Actions -> Create a New Kernel
Should the system be rebooted?Yes
```

IBM AIX のカーネル パラメータの変更

IBM AIX のカーネル パラメータを変更するには

1. テキスト エディタを使用して **/etc/security/limits** を編集することで、**fsize** の値を **4194303** に設定します。次の例では、“vi” エディタを使用しています。

   ```
   vi    /etc/security/limits
   ```

2. システムからいったんログオフし、再びログオンして、変更を反映します。システムを起動する必要はありません。

   RSA Authentication Manager ファイル オーナの場合のみ、**fsize** を編集しなければならない場合があります。

Solaris のカーネル パラメータの変更

システムをシングル ユーザ モードに設定する必要はありませんが、カーネルを再構成している間、他のユーザがシステムを使用しないようにしてください。

Solaris のカーネル パラメータを変更するには

1. 現在のバージョンの構成ファイルをコピーして、現在のカーネル構成パラメータを保存します。

   ```
   cp    /etc/system    /etc/system.old
   ```

   現在のカーネル構成に戻す必要がある場合は、保存したこのファイルを復元し、ステップ 5 に示す手順でシステムを再起動します。

2. Solaris カーネルは動的に構成されます。構成ファイルを編集すると、カーネル構成が変更されます。任意のテキスト エディタを使用してカーネル構成ファイルを変更します。次の例では、“vi” エディタを使用しています。

   ```
   vi    /etc/system
   ```

3. 次の表に示されているすべてのパラメータが最小値以上の値であることを確認します。

   メモ：semmni パラメータの値は、16 に設定することをお勧めします。RSA Authentication Manager は 3 セットのセマフォを必要とするため、オペレーティング システムの構成によっては、このパラメータの値をもっと大きな値に設定しなければならない場合があります。

パラメータ	最小値
shmsys:shminfo_shmmni	64
shmsys:shminfo_shmseg	16
shmsys:shminfo_shmmax	16777216
semsys:seminfo_semmni	16
semsys:seminfo_semmsl	200
semsys:seminfo_semmns	500
semsys:seminfo_semmnu	500

たとえば、**shmsys:shminfo_shmmni** パラメータの場合は、次のような行を定義してください。

```
set shmsys:shminfo_shmmni=64
```

4. システム上に他のユーザがいないことを確認します。
5. コンピュータをシャットダウンし、[OK] プロンプトで再起動します。次のコマンドを入力します。

```
reboot
```

C

UNIX から Windows への RSA Authentication Manager の転送

Windows から UNIX へ RSA Authentication Manager を転送するには

1. UNIX マシンに RSA Authentication Manager 6.1 を新規インストールします。手順については、第 1 章「RSA Authentication Manager の要件」を参照してください。

   インストールの終了後、UNIX マシンのデータベースには、RSA Authentication Manager 6.1 ソフトウェアをインストールした管理者のユーザ レコードが 1 つだけ登録された状態になります。

2. 既存の Windows プライマリ Authentication Manager で RSA Authentication Manager サービスを停止します。
   - [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。
   - [RSA Authentication Manager Control Panel] ダイアログ ボックスで、[Start & Stop RSA Authentication Manager Services] パネルの [Stop All] をクリックします。
   - 「RSA Authentication Manager stopped (RSA Authentication Managerが停止しました)」というメッセージが表示されたら、[OK] をクリックします。
   - 「RSA ACE/Server Database Broker service stopped (RSA ACE/Server データベース ブローカ サービスが停止しました)」というメッセージが表示されたら、[OK] をクリックします。

     [Start & Stop RSA Authentication Manager Services] パネルの [Stop All] をクリックします。
   - [Exit] をクリックして、Control Panel を閉じます。

3. Authentication Manager データベースのダンプ ファイルを作成します。
   - [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 (または ***ACEPROG*** ディレクトリにある **sddump.exe** をダブルクリックします)。

     [RSA Authentication Manager Database Dump] ダイアログ ボックスが表示されます。
   - [Dump Server Database] チェックボックスをオンにして、Authentication Manager ダンプ ファイルを作成することを指定します。
   - [OK] をクリックします。

   sdserv.dmp というファイルが ***ACEDATA*** ディレクトリに作成されます。

4. ダンプが終了したら、[Close] をクリックします。

5. UNIX システムに **/dump** ディレクトリを作成します。

6. RSA Authentication Manager が動作している Windows システムから **/dump** ディレクトリに、**sdserv.dmp** ファイルと **license.rec** ファイルをコピーします。**ftp** を使用してファイルを転送する場合は、バイナリ モードでコピーします。

メモ：これらのファイルを、プライマリの ***ACEDATA*** ディレクトリにコピーしないでください。

UNIX システムにダンプ ファイルが作成されます。これでダンプ ファイルをロードできる状態になりました。

ダンプ ファイルをロードするには

重要:データベースに接続しているアドミニストレーション セッションがないことを確認し、リモート管理者に対して、間もなくシャットダウンすることを通知してください。

1. プライマリでRSA Authentication Managerプロセスが動作していないことを確認します。次のコマンドを入力します。

   ```
   ./aceserver stop
   ./sdconnect stop
   ```

2. UNIXサーバでAuthentication Managerデータベース 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 -m -k /dump/license.rec
   ```

3. [Path of server dump file] フィールドに、ダンプ ファイルと **license.rec** ファイルのパスを入力するか、そのディレクトリを参照します。

4. [Server Database Load Options]パネルで、[Server dump file has a different license record than the current database] チェックボックスと [Merge records from server dump file with records in current database] チェックボックスをオンにします。

   重要：マージ モードでデータベースのロードを実行する場合は、あらかじめ現在のデータベースのバックアップを作成してください。マージ オプションの詳細については、93 ページページの「マージ ロジック」を参照してください。

5. [OK] をクリックします。

   sdload.exe プログラムによって、ダンプ ファイルが RSA Authentication Manager 6.1 データベースにロードされます。

6. [Close] をクリックします。

メモ：RSA Authentication Manager 6.1 UNIX マシンが RSA Authentication Manager 6.1 Windows マシンにレプリカとして自動的に追加されます。これを削除するには、[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。

D データベース ユーティリティ

この付録では、プライマリ Authentication Manager でインストール作業とアドミニストレーション作業を実行するときに使用するユーティリティについて説明します。ユーティリティの種類は次のとおりです。

- データベース アドミニストレーション アプリケーションの **sdadmin**。
- データベース ユーティリティ (**sddump**、**sdload**、**sdnewdb**、**dumpreader**)。既存のデータベースのダンプ、ダンプしたデータベースのロード、空のデータベースの新規作成、表示可能な各種形式へのダンプ ファイルの変換をそれぞれ実行します。

これ以外にも次に示すユーティリティがありますが、その説明はこの付録ではなく、関係する箇所で行います。

sdsetup -config。プライマリで構成レコードを編集できます。詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の付録「RSA Authentication Manager の構成 (UNIX)」を参照してください。

sdsetup -repmgmt。次の操作を実行できます。

- レプリカの追加または削除。
- レルム内の Authentication Manager に関する情報の表示。
- 新しいデータベースを必要とするレプリカのマーキング。
- レプリカ パッケージの作成。
- プライマリを交換するためのレプリカの指名。『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

loadsamusers。Windows システムの既存の SAM (Security Account Manager) データベースから RSA Authentication Manager データベースへユーザ情報を移動できます。このユーティリティの詳細については、付録 F「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。

sdaceldap。LDAP ディレクトリの情報を使用して、RSA Authentication Manager ユーザ レコードを作成および更新できます。このユーティリティの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

sdadmin の使用

sdadmin プログラムは、承認された 1 人または複数の管理者によって、UNIX プライマリで実行できます。**sdadmin** を実行するのに PASSCODE は必要ありません。代わりに、ユーザ レコードに RSA Authentication Manager の Administrator 権限が指定されているかどうかが確認されます。管理者でない人が **sdadmin** を実行しようとしても、プログラムは起動せず、ユーザ名を含むメッセージがログに記録されます。

sdadmin を初めて実行する場合は、インストール時に指定した RSA Authentication Manager ファイル オーナとしてログオンする必要があります。指定したアカウントがわからない場合は、**sdinfo** を実行し、[File Ownership] の行を調べます。

RSA Authentication Manager データベースに既に管理者が登録されている場合は、その中の 1 つの管理者のアカウントから **sdadmin** を実行できます。ただし、アカウントの UNIX グループ ID (GID) と、RSA Authentication Manager ファイル オーナの GID が同じでなければなりません。

メモ：sdadmin プログラムでは 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。

操作を始める前に、次の「インタフェースの規則」を参照して、プログラムの実行方法と、インタフェースの規則について理解しておいてください。

インタフェースの規則

- 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、ENTER 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。この領域のフォーカスは、四角形で強調表示されます。
- オプション ボックスの中で、ある領域から別の領域へ順方向に移動するには、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。
- 領域内で項目間を移動するには、矢印キーを使用します。
- リスト項目、オプション ボタン、またはチェックボックスにフォーカスがある場合、スペースバーを押して選択できます。リスト内では、矢印キーで項目を強調表示することもできます (ただし、先頭の項目は例外です。この項目は最初にリストを表示したときに強調表示されており、選択するにはスペースバーを使用する必要があります)。
- コマンド ボタンが反転表示されている場合は、ENTER キーを押すとアクションが実行されます。フォーカスがデフォルトのアクション ボタンに設定されたままになっている場合、ENTER キーを押すと、そのアクションが実行されます (多くの場合、[OK] ボタンはデフォルトのアクション ボタンに設定されており、ダイアログ ボックスが閉じる場合もあります)。
- 入力フィールドで ENTER キーを押す操作は、TAB キーを押す操作と同じです。
- チェックボックスまたはオプション ボタンにフォーカスがある場合は、ENTER キーを押してオンとオフを切り替えることができます。
- [Cancel] ボタンをクリックするか、F4 キーまたは PF4 キーを押すと、ダイアログ ボックスに加えた変更の中で、これまでに保存していないすべての変更が取り消されます。これらのアクションを実行すると、ボックスも閉じます。
- 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何も変化しません。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。
- ボタンを利用できない場合は、ボタンが表示されていても選択できません (カーソルがボタンに移動しません)。

- **sdadmin** を終了するには、[File] メニューの [Exit] を選択します。システムによっては CTRL+C キーを押して **sdadmin** を終了できますが、[File] メニューの [Exit] オプションでプログラムを正しく終了するようにしてください。

sdadmin の実行

sdadmin を実行するには

1. 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
   ```

   次のメッセージが表示される場合は、システムのカーネル構成値の一部を大きくしなければならない可能性があります。

   ```
   Warning: only 25 wait semaphores are available (警告 : 使用できる待ちセマフォは 25 個だけです )
   Maximum number of shared-memory segments per process exceeded.
   ( プロセスあたりの共有メモリ セグメントの最大数を超えています )
   ```

   UNIX 構成値を変更する手順については、付録 B「カーネル パラメータの変更」を参照してください。

2. RSA Authentication Manager アドミニストレーション プログラムを実行します。

   ```
   ACEPROG/sdadmin
   ```

重要 : sdadmin をバックグランド プロセスとして実行しないでください。また、**sdadmin** を実行している間は、絶対に席を離れないでください。他の人が管理者になりすましてシステムにアクセスし、RSA Authentication Manager データを変更する危険性があります。Authentication Manager を離れるときは、**sdadmin** を終了し、ログオフするようにしてください。

sddump によるデータベースのダンプ

sddump プログラムを実行すると、Authentication Manager データベースとログ データベースのダンプ ファイルが作成されます。

次の表は、**sddump** プログラムのオプションを示しています。

オプション	引数	説明
-s	なし	Authentication Manager データベースをダンプします。
-l	なし	ログ データベースをダンプします。
-d	*database name*	ダンプする Authentication Manager (またはログ) データベースの名前を指定します。
-f	*dump file name*	ダンプ ファイルの場所と名前がデフォルト (Authentication Manager データベース ダンプ ファイルの場合は **/ace/data/sdserv.dmp**、ログ データベース ダンプ ファイルの場合は **/ace/data/sdlog.dmp**) と異なる場合、ダンプ ファイルの名前を指定します。

オプション	引数	説明
-t	*table list*	ダンプする 1 つまたは複数のデータベース テーブルを指定します。テーブルの名前はカンマで区切ります。table list 引数には、実際のテーブル名に対応する識別子を指定します。この識別子については、次の「必須テーブル」を参照してください。
-p	なし	**-t** オプションで指定されるテーブル リスト内の各テーブルについて、必須テーブルをダンプします。
-r	なし	ダンプ ファイルにデルタ レコードを含めます。
-m	なし	データベースがアクティブな状態でダンプを実行します。
-g	なし	指定のグループ、そのメンバ、およびそのトークンをダンプします。
-u	*login*	指定のデフォルト ログインに基づき、ユーザ レコード (およびユーザが所有するトークン) をダンプします。
-k	*login*	**-u** と同じです。
-a	*serial number*	シリアル番号で指定される 1 つのトークンをダンプします。
-v	なし	詳細な出力情報を表示します。

-p オプションは、選択ダンプ モード **(-t)** を使用する場合のみ有効です。
オプション **-t**、**-g**、**-u**、および **-a** を同時に指定することはできません。

必須テーブル

データベースの部分的なダンプを実行する場合、テーブルによっては、ダンプ ファイル内の別のテーブルが必要になることがあります。必要なすべてのテーブルが指定されていないと、ダンプ ファイルをロードできません。指定したテーブルと共に、必要なすべてのテーブルをダンプするには、**-p** オプションを使用します。

次の表は、**-t** パラメータの引数として使用されるテーブル名の省略形の識別子、『Administration Toolkit Reference Guide』に記載されている対応テーブル名、およびデータベース内の各テーブルの必須テーブルを示しています。

識別子	データベース テーブル名	必須テーブル
administrator	SDAdministrator	SDUser
admrole	SDAdministrativeRole	SDAdministrator、SDTaskList、SDRealm、SDSite、SDGroup
attribute	SDAttribute	なし
attrvalue	SDAttributeValue	SDProfile、SDAttribute

識別子	データベース テーブル名	必須テーブル
aalm	SDAALM	なし
client	SDClient	SDSystem
clientext	CustClientExt	SDClient
enabledgroup	SDEnabledGroup	SDClient、SDGroup
enableduser	SDEnabledUser	SDClient、SDUser
groupext	CustGroupExtension	SDGroup
groupmem	SDGroupMember	SDGroup、SDUser
logext	CustLogExtension	SDLog
msg	SDLogMessage	なし
node	SDSecondaryNode	SDClient
onetimepassword	SDOneTimePassword	SDSystem、SDUser、SDToken
profile	SDProfile	なし
realmext	CustRealmExtension	SDRealm
realmenableduser	SDRealmEnabledUser	SDRealm、SDUser
realmenabledgroup	SDRealmEnabledGroup	SDRealm、SDGroup
site	SDSite	なし
siteext	CustSiteExtension	SDSite
sys	SDSystem	なし
sysext	CustSystemExtension	SDSystem
syslogcr	SDSysLogCriteria	なし
tasklist	SDTaskList	なし
tasklistitem	SDTaskListItem	SDTasklist
token	SDToken	SDSystem
tokenext	CustTokenExtension	SDToken
user	SDUser	なし
userext	CustUserExtension	SDUser
value	SDValue	SDAttribute

sdnewdb によるデータベースの新規作成

sdnewdbプログラムは新しい空のAuthentication Managerデータベースまたはログ データベースを作成し、既存の Authentication Manager データベースまたはログ データベースに上書きします。**sdnewdb** プログラムを使用する前に、データベース ファイルのバックアップを作成するか、ダンプ ファイルを作成してください。

メモ：新しいデータベースを作成すると新しい暗号鍵が作成され、データベース内の特定のフィールドを暗号化するのにその鍵が使用されます。既存のレプリカは、データベース プッシュ時に新しい鍵にアクセスできないため、新しいデータベースを復号できません。このため、レプリカ パッケージを手動でレプリカにコピーし、レプリカ パッケージを適用する必要があります。

sdnewdb プログラムの構文は次のとおりです。

```
sdnewdb [server|log|all]
```

パラメータの内容は次のとおりです。

server	新しい Authentication Manager データベースを作成することを指定します。
log	新しいログ データベースを作成することを指定します。
all	新しい Authentication Manager データベースとログ データベースを作成することを指定します。

sdload によるダンプ ファイルのロード

sdload プログラムは、データベース ダンプ ファイルを新しいデータベースにロードします。

次の表は、**sdload** プログラムの引数の一覧です。

オプション	引数	説明
-s	なし	Authentication Manager のダンプ ファイルをロードします。
-l	なし	ログ データベースのダンプ ファイルをロードします。
-d	*database name*	データベースのファイル名を指定します。この引数を省略した場合は、デフォルト値の ***ACEDATA*/sdserv** または **sdlog** が使用されます。
-f	*load file name*	ロードするダンプ ファイルの名前を指定します。
-a	なし	圧縮モード。ロードによって、データベース ファイルは圧縮されます。デルタ レコードはすべて保持されます。ダンプ前に使用していたデータベースより容量の小さなデータベースが作成されます。

オプション	引数	説明
-m	なし	**-d** 引数で指定されるデータベースにダンプ ファイルをマージします。詳細については、次の「マージ ロジック」を参照してください。
-c	なし	**-m** と一緒に指定すると、データベースとダンプ ファイルが競合しない場合のみ、ダンプ ファイルがマージされます。
-u	なし	v5.1 のダンプ ファイルをアップグレード モードでロードし、現在のシステムをプライマリとして追加します。
-t	*table list*	ダンプする 1 つまたは複数のテーブルを指定します。テーブルの名前はカンマで区切ります。
-r	なし	現在のシステムをプライマリとして指定します。壊れたデータベースまたは Authentication Manager を復旧する場合のみ、このオプションを使用してください。
-k	*license file*	ダンプ ファイルとともにロードされるライセンスを指定します。この引数は、ダンプ ファイルを (**-d** 引数で指定される) 新しいデータベースにロードする場合か、ダンプ ファイルをプライマリのデータベースにマージする場合に指定してください。

オプション **-t** は、マージ モード (**-m**) を使用する場合のみ有効です。
オプション **-a**、**-m**、**-u**、および **-r** を同時に指定することはできません。

マージ ロジック

-m オプションを使用してダンプ ファイルをデータベースにマージする場合、データベース内の情報は保持されます。ダンプ ファイルの情報が既存のデータベース内の情報と競合する場合は (ユーザ名やグループ名の重複など)、データベース内の情報が優先され、競合する情報は拒否されます。すべての競合は標準出力に出力されますが、出力先をファイルに設定して、後で確認することもできます。**-c** オプションを指定すると、競合がない場合のみ、情報がマージされます。このオプションは、データベースへの変更をコミットする前に、ダンプ ファイルとデータベースが競合しているかどうかを確認するときに使用します。

重要：マージ モードでデータベースのロードを実行する場合は、あらかじめ現在のデータベースのバックアップを作成してください。

データベース プッシュの無効化

データベース プッシュ (Push DB とも呼ばれます) とは、レプリカ パッケージのデータベース ファイルをレプリカに送信することで、レプリカのデータベースを自動的に更新する機能です。プライマリで [System Parameters] ダイアログ ボックスの [Allow Push DB Assisted Recovery] チェックボックスがオンの場合、レプリカ パッケージを作成すると、プライマリは ***ACEDATA¥replica_package*** ディレクトリ内のデータベースを指定のレプリカに送信します。

データベースをレプリカにプッシュする状況として、2 つの場合が考えられます。1 つはデータベースやハードウェアの復旧時に行われるプッシュであり、もう 1 つはレプリカの新規インストール時に行われるプッシュです。新規インストールの場合、Push DB 機能によって、レプリカ パッケージからレプリカへデータベース ファイルをコピーする時間も手間も省くことができます。

デフォルトでは、Push DB 機能は有効です。データベース ファイルをレプリカにプッシュしない場合は、次の手順を実行して Push DB を無効にしてください。

Push DB を無効にするには

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、プライマリに接続します。
2. [System] > [System Configuration]> [Edit System Parameters] の順にクリックします。
3. [Allow Push DB Assisted Recovery] チェックボックスをオフにします。
4. [OK] をクリックします。

Push DB を無効にした場合は、作成するレプリカ パッケージをレプリカに手動でコピーする必要があります。レプリカがインストールされている場合は、レプリカ パッケージを適用することも必要です。**sdsetup -apply_package** の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の「レプリカ管理ユーティリティ (UNIX)」の章を参照してください。

レプリカがインストールされていない場合は、インストール プロセスがレプリカ パッケージを使用します。レプリカのインストール時に、自分でレプリカ パッケージを適用する必要はありません。

メモ：レプリカでレプリカ管理ユーティリティを実行し、レプリカに関する情報を表示する場合、データベース プッシュが完了するまでは、デフォルト値が表示されます。

ダンプリーダ ユーティリティの使用

ダンプリーダ ユーティリティを使用すると、ダンプ ファイル内の RSA Authentication Manager データを表示できます。たとえば次のような場合に、このユーティリティは便利です。

- 複数のダンプ ファイルがあり、現在の RSA Authentication Manager データベースにインポートする前に、その内容を確認する場合。
- サードパーティのツールを使用して、ダンプ ファイルに含まれているデータからレポートを作成する場合。ダンプリーダ ユーティリティは、CSV、HTML、XML、および TXT 形式のファイルへの出力をサポートしています。

UNIX シェルからのダンプリーダ ユーティリティの実行

ダンプリーダ ユーティリティは、UNIX シェル プロンプトからのみ実行できます。

メモ: Windows プラットフォーム向けのダンプリーダ ユーティリティも用意されています。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。

dumpreader コマンドの構文とオプションを画面に表示するには、次のコマンドを入力します。

```
dumpreader
```

dumpreader コマンドの構文は次のとおりです。

```
dumpreader dumpfile format [parameter] [-c]
```

次の表は **dumpreader** のオプションと引数を示しています。

オプション	引数	説明
なし	*dumpfile*	このオプションは必須です。ダンプ ファイルの名前 (通常は **sdserv.dmp** または **sdlog.dmp**) を指定します。
なし	*format*	このオプションは必須です。ダンプ ファイルのデータが書き込まれるファイル形式を指定します。 • **CSV --** カンマ区切り形式。Microsoft Excel をはじめ、サードパーティのレポート形式にインポートできます。 • **HTML --** Hypertext Markup Language。Web ブラウザで表示できます。 • **XML --** Extended Markup Language。サードパーティのレポート アプリケーションにインポートできます。 **メモ :** CSV、HTML、および XML の場合、データベース内のテーブルごとに 1 つのファイルが作成されます。 • **XML2 --** XML に似ていますが、使用する DTD (Document Type Definition) が異なっており、すべての出力が 1 つのファイルにまとめられます。 • **TXT --** 構造化テキスト形式。テキスト エディタで表示できます。すべての出力が 1 つのファイルにまとめられます。

オプション	引数	説明
なし	*parameter*	省略可能です。CSV、HTML、および XML の場合は、データベースのテーブルにそれぞれ対応する、複数のファイルが書き込まれるディレクトリの名前を指定します。このパラメータを指定しないと、出力ファイルはカレント ディレクトリに書き込まれます。 XML2 と TXT の場合は、出力が書き込まれるファイルの名前を指定します。パラメータが指定されていない場合、出力は **stderr** (通常は端末) に対して行われます。パラメータが空で、二重引用符 (") で囲まれている場合は、**stdout** に対して出力されます。これも通常は端末です。
-c	なし	アドミニストレーション プログラムから **Export Tokens by User** コマンドと **Export Tokens** コマンドを実行して作成するダンプ ファイルの**統合**オプション。これらのダンプ ファイルは、この付録で説明しているダンプ ユーティリティで作成されるダンプ ファイルと内部構造が異なります。複数のテーブルの各部分の情報が混在しています。ダンプリーダは、別のテーブルの部分が検出されるたびに、新しい出力ファイルを作成します。**-c** オプションを使用すると、同じテーブルのすべての部分を統合し、統合されたテーブルを 1 つのファイルに送ることで、出力するファイル数を減らすことができます。 **-c** オプションで作成されるテーブルは、ダンプ ファイル内の順序ではなく、アルファベット順になります。

ダンプリーダの出力形式

ダンプリーダ ユーティリティは、CSV、HTML、TXT、XML、および XML2 という 5 種類の出力オプションをサポートします。これらの出力オプショについては、以下のセクションで詳しく説明します。

HTML

ダンプ ファイル データを Web ブラウザで表示するには、**dumpreader** コマンドに **HTML** 引数を指定します。次の例を参照してください。

```
dumpreader sdserv.dmp HTML dumpoutput
```

この例では、**sdserv.dmp** というダンプ ファイルが、カレント ディレクトリ (コマンドが実行されたディレクトリ) の下の **dumpoutput** サブディレクトリに、HTML 形式で出力されます。

output フォルダには、複数の HTML ファイル (サマリ ファイルの他に、ダンプ ファイル内のデータベース テーブルごとに 1 つずつのファイル) が格納されます。ディレクトリの内容を表示すると、サマリ ファイル名は次のような形式です。

```
dump_summary_04.01.03_11.40.37.html
```

この名前は、2003 年 4 月 1 日の 11:40:37 a.m. に出力が作成されたことを表します。

その他のファイルには、RSA Authentication Manager データベース スキーマ内のテーブル名に、同じ日付、時刻、拡張子が付いた名前が付けられます。次の例を参照してください。

```
SDUser_04.01.03_11.40.37.html
```

サマリ ファイルには、ダンプ ファイル内のすべてのデータベース テーブルへのリンクが含まれています。サマリ ファイル内の関連リンクをクリックすることで、対応するファイルをブラウザの中で表示できます。あるいは、ブラウザ (または HTML 対応の他のアプリケーション) の中でこれらのファイルを直接開くこともできます。

メモ：HTML 出力には、ダンプ ファイル内のデータのスキーマ バージョンも表示されます。これは、ファイルを作成した RSA Authentication Manager のリリースを表します。詳細については、99 ページの「RSA Authentication Manager の各リリースのスキーマのバージョン」を参照してください。

ダンプリーダ ユーティリティによる HTML 出力では、フィールド名とデータに含まれる特殊文字が解析され、次のような置換が行われます。

文字	置換後
>	&gt
<	&lt
&	&amp
"	&quot
[スペース]	

CSV

ダンプ ファイル データの形式を、サードパーティのスプレッドシートや他のプログラムに対応させるには、**dumpreader** コマンドに CSV 引数を指定します。次の例を参照してください。

```
dumpreader sdserv.dmp CSV dumpoutput
```

この例では、**sdserv.dmp** というダンプ ファイルが、カレント ディレクトリ (コマンドが実行されたディレクトリ) の下の **dumpoutput** サブディレクトリに、CSV 形式で出力されます。

output ディレクトリには、サマリ ファイルと、ダンプ ファイル内のデータベース テーブルごとに 1 つのファイルが格納されます。次の例を参照してください。

```
dump_summary_04.01.03_11.40.37.csv

SDAdministrativeRole_04.01.03_11.40.37.csv
SDAdministrator_04.01.03_11.40.37.csv
.
.
.
```

ダンプリーダ ユーティリティで CSV に出力する場合、データに含まれる特殊文字が解析され、カンマはスペースに置換されます。また、スペース文字の ASCII コード値 (10 進数の 32) より小さい ASCII コード値が割り当てられている記号も、スペースに置換されます。

XML

ダンプ ファイル データの形式を、サードパーティのレポート プログラム (Crystal Decisions 社の Crystal Reports など) に対応させるには、**dumpreader** コマンドに XML 引数を指定します。次の例を参照してください。

```
dumpreader sdserv.dmp XML dumpoutput -c
```

この例では、**sdserv.dmp** というダンプ ファイルが、XML コードが組み込まれた複数のテキスト ファイルに出力されます。これらのファイルは、カレント ディレクトリ (コマンドが実行されたディレクトリ) の下の **dumpoutput** サブディレクトリに保存されます。

output ディレクトリには、サマリ ファイルと、ダンプ ファイル内のデータベース テーブルごとに 1 つのファイルが格納されます。次の例を参照してください。

```
dump_summary_04.01.03_11.40.37.xml

SDAdministrativeRole_04.01.03_11.40.37.xml
SDAdministrator_04.01.03_11.40.37.xml
.
.
.
```

ファイル名は、ベース名と、ファイルが作成された正確な日付と時刻を表すタイムスタンプで構成されます。このため、ダンプリーダ ユーティリティを再実行しても、ファイルが上書きされることはありません。

ダンプリーダ ユーティリティによる XML 出力では、フィールド名とデータに含まれる特殊文字が解析され、次のような置換が行われます。

文字	置換後
>	&gt
<	&lt
&	&amp

XML2

ダンプ ファイルの内容を 1 つの XML エンコード ファイルに出力するには、XML2 オプションを使用します。次の例を参照してください。

```
dumpreader sdserv.dmp XML2 sdserv.xml -c
```

この例では、**sdserv.xml** という出力ファイルに、XML エンコード データベース テーブルと、そのテーブルに含まれるレコードが格納されます。**-c** オプションが指定されているため、テーブルは統合され、XML ファイルの中でアルファベット順に配置されます。

ダンプリーダ ユーティリティによる XML2 出力の場合、特殊文字の解析は行われません。検出されたダンプ ファイル データが、そのまま出力されます。

TXT

ダンプ ファイルの内容を構造化テキスト ファイルに出力するには、TXT オプションを使用します。次の例を参照してください。

```
dumpreader sdserv.dmp TXT sdserv.txt -c
```

この例では、**sdserv.txt** という出力ファイル内のデータは単純なテキストであり、テキスト エディタ (**emacs** など) で表示できる形式です。**-c** オプションが指定されているため、テーブルは統合され、テキスト ファイルの中でアルファベット順に配置されます。

ダンプリーダ ユーティリティによる TXT 出力の場合、特殊文字の解析は行われません。検出されたダンプ ファイル データが、そのまま出力されます。

スキーマ フィールド名の相違

ダンプリーダ ユーティリティからの出力を使用するには、RSA Authentication Manager データベース スキーマ (データベース テーブルとそのテーブルに含まれるレコード) を理解している必要があります。

ダンプ ファイルの相違を含めて、データベース スキーマの詳細は、ヘルプと、『Administration Toolkit Reference Guide』(**authmgr_admin_toolkit.pdf**) に記載されています。

メモ：ダンプ ファイル内のいくつかのデータベース フィールド名は、実際のデータベース スキーマ内の対応するフィールド名とは異なります。これは、以前のバージョンのダンプ ファイルとの下位互換性を維持するためです。詳細については、次の「RSA Authentication Manager の各リリースのスキーマのバージョン」を参照してください。

RSA Authentication Manager の各リリースのスキーマのバージョン

RSA Authentication Manager データベース スキーマは、製品のライフ サイクルの中で変化してきました。次の表は、ダンプ ファイルに含むことができるスキーマ バージョンを示しています。

RSA ACE/Server バージョン	スキーマ バージョン
5.2	19.00.00
5.1	18.00.00
5.0	17.00.00
4.1	16.00.00
4.0	14.00.00
3.31	12.00.00
3.2	12.00.00
3.1	11.00.00
3.0.1	10.00.00

ダンプリーダ ユーティリティのトラブルシューティング

ダンプリーダ ユーティリティは、ダンプ ファイル、ユーザ入力、およびその他の問題を検出し、各種のエラー メッセージを生成します。このセクションでは、ダンプリーダのエラー メッセージをアルファベット順に示し、その内容を説明します。ダンプリーダ ユーティリティのコマンド構文の詳細については、94 ページの「ダンプリーダ ユーティリティの使用」を参照してください。

メモ：コマンドの詳しい使い方を画面上に表示するには、引数を指定せずに **dumpreader** コマンドを実行します。

Invalid number of parameters. See the usage summary. (パラメータの個数が正しくありません。コマンドの使い方を確認してください)

コマンド ラインに 1 つ以下、または 5 つ以上の引数が指定されています。

Invalid command line parameter. See the usage summary. (コマンド ラインのパラメータが正しくありません。コマンドの使い方を確認してください)

3 つまたは 4 つの引数が指定されていますが、その 3 番目または 4 番目の引数が **-c** ではありません。

Invalid format. See the usage summary. (形式が正しくありません。コマンドの使い方を確認してください)

形式を指定するパラメータが次のいずれでもありません。

```
CSV
HTML
XML
XML2
TXT
```

Could not open dump file. (ダンプ ファイルを開けません)

指定したダンプ ファイルを開くことができません。指定したダンプ ファイル名が間違っているか、ダンプ ファイルが壊れているか、またはファイルを開くための適切なアクセス権が与えられていない可能性があります。

Could not read schema version from the dump file. (ダンプ ファイルからスキーマ バージョンを読み込めません)

ダンプ ファイルからバージョン情報を読み込めません。ダンプ ファイルが壊れている可能性があります。

Could not consolidate table information. (テーブル情報を結合できません)

大規模なダンプ ファイルの出力を結合しようとして、メモリ不足になりました。もっと多くのメモリが搭載されているマシンかスワップ領域が大きいマシンを使用してください。または、**-c** オプションを指定せずに **dumpreader** コマンドを実行します。

Invalid file format. (ファイル形式が正しくありません)

ダンプ ファイルを読み込めません。ファイルが壊れているか、別のタイプのファイルに間違って .dmp 拡張子が指定されている可能性があります。

Could not open output file. (出力ファイルを開けません)

指定した出力形式が XML2 または TXT で、出力ファイルまたはパス名に書き込み保護が設定されているか、またはディスクが満杯です。

Could not write tag into the output file. (出力ファイルにタグを書き込めません)

指定した出力形式が XML2 または TXT で、ディスクが満杯か、削除されているか、壊れているために、出力ファイルを作成できません。

Could not read field from dump file. (ダンプ ファイルからフィールドを読み込めません)

ダンプ ファイルから情報を読み込めません。ファイルが壊れているか、ファイルが保存されているメディアが壊れている可能性があります。

Could not create output file for the table <*table name*>. (テーブル <*table name*> の出力ファイルを作成できません)

CSV、HTML、または XML 出力ファイルを作成できません。出力ディレクトリが存在しないか書き込み保護が設定されている、またはディスクが削除されているか満杯です。

Could not write table name into the output file. (出力ファイルにテーブル名を書き込めません)

XML2 または TXT 形式で、出力ファイルにテーブル名を書き込めません。ディスクが満杯か、壊れているか、または削除されている可能性があります。

Could not write the close record tag into the output file. (出力ファイルに終了レコード タグを書き込めません)

XML2 または TXT 出力ファイルに書き込むことができません。ディスクが満杯か、壊れているか、または削除されている可能性があります。

Internal error. Dump file might be corrupt. (内部エラー。ダンプ ファイルが壊れている可能性があります)

ダンプ ファイルから予期せぬデータが検出されました。ダンプ ファイルが壊れている可能性があります。

Could not add field to the table. (テーブルにフィールドを追加できません)

XML、HTML、または CSV 出力ファイル内で、テーブルに新しいフィールドを定義できません。これは通常、メモリの問題です。メモリまたはスワップ領域を増やして、もう一度試してください。

Could not write the open record tag into the output file. (出力ファイルに開始レコード タグを書き込めません)

XML2 または TXT 出力ファイルに情報を書き込むことができません。ディスクが満杯か、壊れているか、または削除されている可能性があります。

Could not write field data into the output file. (出力ファイルにフィールド データを書き込めません)

出力ファイル (すべての形式) に情報を書き込むことができません。ディスクが満杯か、壊れているか、または削除されている可能性があります。

E トラブルシューティング

RSA Authentication Manager 配布メディアまたはインストール ソフトウェアに関する問題が生じた場合は、この付録で、症状や表示されたエラー メッセージに該当するセクションを参照してください。この付録の説明やトラブルシューティングのヒントを参照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。問い合わせ先については、8 ページの「サポートとサービス」を参照してください。

配布メディア

CD-ROM マウント コマンドを実行すると、「unknown command (不明なコマンドです)」エラー メッセージが表示される

CD-ROM のデバイス名は、ホストに応じて異なります。CD-ROM ドライブをマウントしようとしたときに「unknown command (不明なコマンドです)」というエラー メッセージが表示される場合は、オペレーティング システムのマニュアルを参照してください。

“Cannot create administrator. Use an empty database.” (管理者を作成できません。空のデータベースを使用してください)

ulimit が非常に小さい値に設定されている AIX システムで、**root** でない人が RSA Authentication Manager をインストールしようとすると、このエラー メッセージが表示されます。ulimit fsize の値は 4194303 以上に設定する必要があります。システム パラメータの必要最低限の値と、値の変更方法については、付録 B「カーネル パラメータの変更」を参照してください。

sdsetup が動作しない、または終了する

ディスク容量が十分でないために発生するエラー

アップグレード時にディスク容量に関する問題が発生した場合は、新規インストールに移行する前にログ データベースを消去してください。その結果、新規インストール用にディスク容量が確保されます。詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の「データベースのメンテナンス (UNIX)」の章を参照してください。

“You must be root in order to run sdsetup... .” (sdsetup を実行するには root でなければなりません)

sdsetup を実行している管理者の UID が 0 でない場合、次のメッセージが表示されます。

```
You must be root in order to run 'sdsetup.' Please 'su' to
root or log out and log in as root. (sdsetup を実行するには root
でなければなりません。su コマンドを実行して root になるか、いったんログ
アウトしてから root でログインしてください )
```

root でログオンしている場合は、このメッセージは表示されません。**su** コマンドに "-" 引数を指定せずに **root** になった場合、プラットフォームによってはこのエラーが発生することがあります。

インストールを停止し、**root** でログオンするか、次の **su** コマンドを使用して **root** になります。

```
su  -  root
```

その後、再び **sdsetup** を実行してください。

“Error - The sdserv [*log*] database is currently busy - exiting.” (エラー - sdserv [log] データベースは現在使用中です。終了します)

このエラー メッセージが表示され、インストール プログラムが中断した場合は、RSA Authentication Manager データベース ブローカが実行されているか、または正しくシャットダウンされていません。

インストールを続行するには、Authentication Manager プログラムが実行されていないことを確認してください。次に、Authentication Manager プログラム ファイルが格納されているディレクトリから、レポート作成ユーティリティを停止します。次のコマンドを入力します。

```
ACEUTILS/rptconnect stop
```

データベース ブローカとサービスを停止するには、次のコマンドを入力します。

```
ACEPROG/aceserver stop
ACEPROG/sdconnect stop
```

データベース ブローカが既に停止しているというエラー メッセージが表示される場合は、***ACEDATA*** ディレクトリにデータベース ロック ファイル (**sdserv.lk** または **sdlog.lk**) があるかどうかを確認してください。このファイルがある場合は、システム スタートアップ ファイルから **sdconnect clean** を実行することによって、問題を解決できる可能性があります。

スタートアップ ファイルに次のコマンドを入力します。

```
ACEPROG/sdconnect clean
```

その後、Authentication Manager を再起動し、再び **sdsetup** を実行します。

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。

sdsetup が既に実行されている

sdsetup を起動したときに次のメッセージが表示されることがあります。

```
A copy of sdsetup is currently running or was abnormally
terminated. Please conclude the running copy before starting
another. If you shelled from sdsetup, you may return by
typing 'exit.' (sdsetup のコピーが実行されているか、または異常終了しています。実行中のコピーを終了してから、別のコピーを起動してください。sdsetup からシェルを起動している場合は、「exit」と入力して戻ります )
```

sdsetup の別のコピーが動作していないのにこのメッセージが表示される場合は、**sdsetup.running** ファイルを削除してください。

カレント ワーキング ディレクトリに **sdsetup.running** ファイルがあると、このメッセージが表示されます。他のユーザが **sdsetup** を実行しているか、以前にインストールを中断したときに、このファイルが残されている可能性があります。**sdsetup** を実行しているユーザがいない場合のみ、カレント ワーキング ディレクトリから **sdsetup.running** ファイルを削除してください。

インストール後のエラー

ホスト名を解決できない

ネーム サーバを使用していて、RSA Authentication Manager プライマリまたはレプリカのホスト名を解決できない場合は、Authentication Manager のプライマリ ホスト名 (**ブート名**とも呼びます) がそのマシンのエイリアス リストの先頭に指定されていることを確認してください。

“Unable to set ulimit to 4194303, errno=1...” (ulimit を 4194303 に設定できません)

ulimit が非常に小さい値に設定されている AIX システムで、**root** でない人が RSA Authentication Manager プログラムを実行しようとすると、このエラー メッセージが表示されます。ulimit fsize の値は 4194303 以上に設定する必要があります。システムでこの値を変更する方法については、付録 B「カーネル パラメータの変更」を参照してください。

“BROKER 0: Unable to find server... in file SERVICES...” (BROKER 0: SERVICES ファイルにサーバが指定されていません)

sdconnect を実行しようとすると、このメッセージが表示されることがあります。16 ページの「インストール前の操作」に示されているように、**/etc/services** にサービス名とポート番号が追加されていることを確認してください。

“This account does not have permission to access the server database” (このアカウントには、サーバ データベースにアクセスする権限がありません)

sdconnect を実行しようとすると、このメッセージが表示されることがあります。ファイルのアクセス権が正しく設定されていることを確認してください。**sdconnect** を実行するには、root または RSA Authentication Manager ファイル オーナとしてログオンする必要があります。

アクセス権が正しく設定されている場合は、付録 B「カーネル パラメータの変更」に示されているようにUNIXカーネル パラメータが設定されていることを確認してください。いくつかのカーネル パラメータの値を大きくしなければならない可能性があります。

TACACS+ のトラブルシューティング

TACACS+ デバイス上で認証できない場合は、次の手順を実行してください。

TACACS+ デバイスでの認証の問題を解決するには

1. **sdadmin** を実行して RSA Authentication Manager 監査証跡レポートを調べ、認証の失敗に関する情報を確認します。
2. エージェント ホストとAuthentication Manager間の物理的な接続に異常がないことを確認します。
3. **aceserver** が実行されていることを確認します。
4. TACACS+ デーモン (**sdtacplusd**) が実行されており、**root** がデーモンを所有していることを確認します。
5. **sdinfo** を実行して、Authentication Manager 上の **sdconf.rec** を表示します。TACACS+ が有効であることを確認します。有効でない場合は、TACACS をサポートできません。TACACS+を有効にするには、第5章「RSA Authentication ManagerのTACACS+サポート」の説明に従って **sdsetup -config** を実行します。
6. Authentication Managerの**ace/data**サブディレクトリに引数ファイル(**sdtacplus.arg**)があることを確認します。
7. **.arg** ファイルに指定されている構成ファイルが存在することを確認します。
8. **sdadmin** の [List Agent Hosts] オプションを使用して、プライマリとレプリカが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ことを確認します。登録されていない場合、TACACS エージェント ホストからの認証は失敗し、Authentication Manager の監査証跡に「Agent Host Not Found (エージェント ホストが見つかりませんでした)」が記録されます。
9. 問題を解決するためにより多くの情報が必要な場合は、**syslog** デーモンをオンにして、TACACS サーバによって記録されたメッセージを確認します。Authentication Manager マシンでデーモンのディレクトリ (通常は **/usr/etc** または **/usr/sbin**) に移動し、「syslogd」と入力します。*syslog* 構成ファイルのセットアップ方法については、UNIX man page で **syslogd** を参照してください。**ACE/Server** というプレフィックスから始まるメッセージも含めて、**syslog** メッセージについての説明は、Cisco Systems 社のマニュアルを参照してください。
10. NAS (Network Access Server) 上で TACACS デバッグ オプションを実行します。この操作を実行するには、**enable** モードにする必要があります。デバッグできるコマンドを表示するには、次のコマンドを入力します。

    ```
    debug ?
    ```

    デバッグできる *command_name* を選択し、次のように入力してください。

    ```
    debug command_name
    ```

    次の例を参照してください。

    ```
    debug tacacs
    ```

    この場合、NAS から TACACS の「Access control debugging is on (アクセス制御のデバッグはオンです)」という確認メッセージが表示されます。

メモ: X ターミナルを使用している場合、デバッグ ログを表示するには、「terminal monitor」と入力します。

また、**sdtacplus.arg** ファイルの中でも、TACACS+ デーモンのデバッグを指定できます。.arg ファイル内の **-d** オプションのコメントを解除し、RSA Authentication Manager を再起動してください。TACACS+ デバッグ ログが **var/tmp/tacplus.log** に格納されます。

認証セッションがタイムアウトする

Cisco Systems 社の TACACS+ ファームウェアでは、30 秒のインアクティビティ タイムアウトが設定されています。このタイムアウトによって、ネクスト トークンコード操作が妨げられる可能性があります。ネクスト トークンコードが表示されるのを待っている間に、新たなタイムアウトが発生するのを回避するには、キーボードの任意の文字キーを押し、Backspace キーで削除してから ENTER キーを押すようにユーザに指示します。

RSA Authentication Manager ログ メッセージ

Agent Host Not Found *Agent Host = server's IP address* (エージェント ホストを検出できません、エージェント ホスト = サーバの IP アドレス)

デフォルトの **utmp** と **wtmp** は、**var/adm/tacacs** ディレクトリに格納されています。構成ファイルに **-h** が設定されている場合、Authentication Manager はすべての TACACS エージェント ホストに対して個別に **wtmp** ファイルを作成します。これらのファイル名は、**wtmp** ファイル **sdtac_wtmp** にホスト名を連結して作成されます。たとえば、ログオンがエージェント ホスト *panama* から行われた場合、**wtmp** エントリは **sdtac_wtmp** と **sdtac_wtmp.panama** に作成されます。

TACACS Enable Not Authorized (TACACS Enable モードが許可されていません)

グローバル管理者または指定のエージェント ホストの管理者以外のユーザが NAS 上で Enable モードを開始しようとすると、このメッセージが表示されます。

TACACS Enable Succeeded (TACACS Enable モードが正常に開始されました)

エージェント ホストの管理者が Enable モードを開始しました。

TACACS Fail with TACACS passwd (TACACS パスワードでの TACACS ログインに失敗しました)

ログオンしているユーザが、正しいUNIX形式のパスワードを入力できませんでした。

TACACS Login with TACACS passwd (TACACS パスワードを使用して TACACS ログインに成功しました)

トークンの所有者以外の人がローカルUNIXパスワード ファイルに対して認証されました。

F

SAM データベースからのユーザ レコードの作成

RSA Authentication Manager データベースのセットアップを支援するために、2 つのユーティリティが提供されています。これらのユーティリティを使用すると、Windows システムの既存の SAM (Security Account Manager) データベースから RSA Authentication Manager データベースにユーザを移動できます。

- **dumpsamusers.exe**。Windows でのみ実行され、1 つ以上の SAM データベースからユーザ レコードを読み取り、カンマ区切りのフラット ファイルに書き込みます。各レコードには、1 人のユーザのログオン名、ファースト ネーム、およびラスト ネームが含まれます。
- **loadsamusers**。UNIX 上で実行され、フラット ファイルから読み込んで解析し、ファイル内の各ユーザに対して、ファイルから検出した 3 つの情報アイテムを含むレコードを Authentication Manager データベースに作成します。

dumpsamusers は Windows でのみ動作するので、RSA Authentication Manager for UNIX と共にインストールされるのは **loadsamusers** だけです。ネットワークに Windows システムがあり、SAM ファイルのユーザ情報をダンプして **loadsamusers** でロードする場合は、RSA Authentication Manager のインストール CD-ROM から **dumpsamusers.exe** のコピーを直接取り出すことができます。Windows 用のインストール処理全体を行う必要はありません。**dumpsamusers.exe** ファイルは、CD-ROM の **aceserv¥nt_i386** ディレクトリにあります。この付録では、Windows システム上で **dumpsamusers** を実行していることを前提にしています。

転送処理を完全に自動化することはできません。Windows では、SAM データベースのファースト ネーム フィールドとラスト ネーム フィールドは個別に提供されません。これらは 1 つのフル ネーム フィールドとして提供され、このフィールドの使い方に制限はありません。引数を指定することで、最初のフィールドがファースト ネームなのかラスト ネームなのかを **dumpsamusers** に示すことができます。それでも、さまざまな矛盾が発生します。出力ファイルを手動で編集してこれらの矛盾を取り除かないと、**loadsamusers** は正しく動作しません。

メモ : LDAP ディレクトリからユーザ レコードを作成するユーティリティも提供されています。詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の「認証のためのユーザの登録」の章およびオンライン ヘルプの「Manage LDAP Users」を参照してください。

dumpsamusers.exe による SAM ユーザ レコードの抽出

dumpsamusers ユーティリティは Windows コマンド プロンプトから実行してください。

構文

```
dumpsamusers [server(s)...]-lf | -fl outfile
```

引数

[*server(s)...*]	ネットワークに接続している 1 つ以上のサーバの名前。各名前はスペースで区切り、先頭に 2 つの ¥ を付けます (たとえば **¥¥system1 ¥¥system2**)。この引数は省略可能です。省略すると、コマンドはユーティリティが実行されるシステムにのみ影響します。
-lf または **-fl**	SAM データベースに格納されているユーザ名の順序を指定します。“lf” (last, first) (2 つの名前がカンマで区切られる場合) と “fl” (first last) (カンマを使用しない場合) のいずれかを指定できます。
outfile	ユーザ レコードが書き込まれる出力ファイルを指定します。

出力ファイルの編集

dumpsamusers は次の規則に従って名前を解析します。

- 順序が “lf” (last, first) の場合は、カンマの前の部分がラスト ネームであり、カンマの後の部分がファースト ネームであると解釈されます。
- 順序が “fl” (first last) の場合は、最後のスペースの後の部分がラスト ネームであり、その前の部分がファースト ネームであると解釈されます。

ミドル イニシャルが使用されている場合は、**dumpsamusers** はこれらの規則に従って、ミドル イニシャルをファースト ネームの一部であると解釈します。姓が 2 つの部分に分かれている場合は、変則的になる可能性があります。たとえば、姓の後に称号が続く場合や、名前ではなく説明が指定されているエントリなどがその例です。次の表は、“fl” (first last) の場合の例を示しています。

レコードから検出された名前	解析された ファースト ネーム	ラスト ネーム
Anne Van Ostkamp	Anne Van	Ostkamp
Robert F. Martin III	Robert F. Martin	III
John Daly Jr.	John Daly	Jr.
Development Group	Development	Group

“lf” (last, first) の方が問題は少ないのですが、それでも問題がないわけではありません。たとえば、称号の前にカンマが使用されている “Brown, Thomas G., Sr.” の場合、“Brown, Thomas G.”がファースト ネームで、“Sr.”がラスト ネームとして解析されます。どちらの順序を使用する場合も、「Development Group」などの記述は問題です。

単純な “last, first” や “first last” のパターンだけで、ユーティリティがすべての場合を区別し、対応することはできないので、**loadsamusers** を実行する前に、**dumpsamusers** の出力ファイルを確認し、編集する必要があります。ファイルは ASCII 形式であり、すべてのフィールドにラベルが付いています。ほとんどの場合、変更が必要なのは一部のレコードだけです。

loadsamusers.exe による RSA Authentication Manager ユーザ レコードの作成

loadsamusers ユーティリティは UNIX コマンド プロンプトから実行します。

loadsamusers ユーティリティは RSA Authentication Manager Administration Toolkit の機能の一部を利用するので、次の条件が適用されます。

- RSA Authentication Manager 環境変数を設定する必要があります。

  この環境変数が正しく設定されるように、**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。
- **loadsamusers** の起動時にデータベース ブローカが実行されている必要があります。
- **apidemon** プログラムも格納されているディレクトリから **loadsamusers** を実行する必要があります。これらの 2 つのプログラムが格納されるデフォルト ディレクトリは ***ACEUTILS*/toolkit** です。

構文

```
loadsamusers infile [-i | -b] [outfile] [-g group]
```

引数

infile	入力ファイル (**dumpsamuser**) を指定します。
-i または **-b**	ユーティリティを対話型プロセス (-i) として起動するか、バッチ プロセス (-b) として起動するかを指定します。この引数は省略可能です。デフォルトは対話モードです。レコードに無効な文字 (全角文字など) が含まれている場合は、置換文字列の入力が求められます。バッチ モードでは、このようなレコードはインポートされず、その一覧が表示されます。ログオンの重複など、致命的でないエラーも表示されます。出力ファイルが指定されている場合は (次の引数を参照)、そのファイルに書き込まれます。
outfile	致命的でないエラーを含むレコードの一覧 (前の引数を参照) が書き込まれる出力ファイルを指定します。この引数は省略可能です。省略すると、レコードの一覧は画面に表示されます。
-g *group*	RSA Authentication Manager グループを指定します。このコマンドで追加されるすべてのユーザが、このグループに割り当てられます。指定したグループが存在しない場合は、自動的に作成されます。この引数は省略可能です。省略すると、ユーザはグループに割り当てられません。

loadsamusers プログラムは、ロードできないレコードを検出したときに終了するように設計されています。その時点までにロードされたユーザは、Authentication Manager データベースにそのまま残ります。

G 最小システム要件 (Solaris 9)

この付録では、RSA Authentication Manager が正しく動作するために最低限必要な Solaris 9 のコンポーネントについて説明します。操作に先立ち、13 ページの「インストールに関する重要なガイドライン」を参照してください。

システムを適切に最小化するためには、Solaris 9 を新規インストールすることをお勧めします。コア コンポーネント クラスタを選択し、次のパッケージを追加します。

- SUNWlibC
- SUNWlibCx

Solaris サービスの最小構成

オペレーティング システムをインストールしたら、システム構成と、予定しているマシンの使用環境に応じて、特定のパッケージを削除できます。システムに現在含まれているパッケージを表示するには、**pkginfo** コマンドを使用します。パッケージを削除するには、**pkgrm** コマンドを使用します。

Sun SPARC SunFire プロセッサ上で動作する Solaris 9 の最小構成要件は次のとおりです。

ハードウェア

- SUNWced
- SUNWcedx
- SUNWdmfex
- SUNWeridx
- SUNWged
- SUNWgedx
- SUNWhmd
- SUNWhmdx
- SUNWqfed
- SUNWqfedx
- SUNWpd
- SUNWpdx

ベース コンポーネント

- SUNWbip
- SUNWbzip
- SUNWcar
- SUNWcarx
- SUNWcs
- SUNWcsl
- SUNWcslx
- SUNWcsr
- SUNWcsu
- SUNWcsxu
- SUNWesu
- SUNWkvm
- SUNWkvmx
- SUNWlibC
- SUNWlibCx
- SUNWlibms
- SUNWlmsx
- SUNWnamos
- SUNWnamo
- SUNWswmt

用語集

ace/data、ace/prog、ace/rdbms、ace/utils、ace/examples サブディレクトリ
インストール プログラムによって作成されるサブディレクトリであり、RSA Authentication Manager データ、RSA Authentication Manager プログラム ファイル、Progress Software リレーショナル データベース管理システム ソフトウェア、レポート作成ユーティリティなどのユーティリティ、ドキュメント ファイルが格納されます。この 5 つのサブディレクトリは、インストール時に指定した RSA Authentication Manager トップレベル ディレクトリの下にあります。

***ACEDATA* ディレクトリ**
RSA Authentication Manager データ ディレクトリ。***ACEDATA*** は太字の斜体で示され、その位置には実際のディレクトリ名 (**/ace/data** など) を指定します。

***ACEDOC* ディレクトリ**
RSA Authentication Manager ドキュメント ディレクトリ。***ACEDOC*** は太字の斜体で示され、その位置には実際のディレクトリ名 (**/ace/doc** など) を指定します。

***ACEPROG* ディレクトリ**
RSA Authentication Manager プログラム ディレクトリ。***ACEPROG*** は太字の斜体で示され、その位置には実際のディレクトリ名 (**/ace/prog** など) を指定します。

aceserver
RSA Authentication Manager 製品の認証を実行するバックグラウンド Authentication Manager プロセス。

acesyncd
プライマリ / レプリカ通信を実現し、Authentication Manager データベースをプライマリとの間でレプリケートするバックグラウンド プロセス。

ACEUTILS ディレクトリ
RSA Authentication Manager ユーティリティ ディレクトリ。***ACEUTILS*** は太字の斜体で示され、その位置には実際のディレクトリ名 (**/ace/utils** など) を指定します。

***ACEUTILS* ディレクトリ**
RSA Authentication Manager ユーティリティ ディレクトリ。***ACEUTILS*** は太字の斜体で示され、その位置には実際のディレクトリ名 (**/top/ace/utils** など) を指定します。

license.rec
サイト固有の情報が格納されているファイル。ライセンス番号とカスタマ ID 番号、データベースに登録できるユーザとレプリカの数、トライアル ライセンスであるかどうかなどの情報が格納されています。

New PIN モード
トークンがこのモードになると、ユーザは RSA SecurID で保護されるシステムにアクセスするために、新しい PIN を受け取るか、作成する必要があります。

PASSCODE
ユーザの PIN と、ユーザのトークンに表示されるトークンコードの組み合わせ。

PIN
ユーザの個人識別番号。PIN は、RSA SecurID 二要素認証システムの要素の 1 つです。もう 1 つの要素はトークンコードです。

RADIUS プロファイル

RSA Authentication Manager ソフトウェアが RADIUS ユーザに PASSCODE を要求 (チャレンジ) する前に満たさなければならない必要条件のリスト。RADIUS サーバを通じて認証を受けるユーザは、RSA Authentication Manager データベースにプロファイルを登録しておく必要があります。

Remote Administration アプリケーション

リモート接続を通じて RSA Authentication Manager データベースの管理を可能にするアプリケーション。RSA Authentication Manager for UNIX データベースは、Windows NT、Windows 2000、Windows XP、または Windows 98 が動作しているマシンからリモート管理できます。Remote Administration アプリケーションは、グラフィカル ユーザ インタフェースを通じて RSA Authentication Manager データベースを管理できる方法であり、v3.0 以降に追加された管理機能にアクセスできる唯一の方法でもあります。

REP_ACE

レプリカ パッケージが格納されるディレクトリを指定する環境変数。REP_ACE が設定されていない場合、デフォルトにより、レプリカ パッケージは ACEDATA ディレクトリに作成されます。

RSA Authentication Agent

米 RSA Security 社が開発した製品であり、コンピュータやその他のデバイスにインストールされ、RSA Authentication Manager と共に動作して不正なアクセスを防止します。このコンピュータまたはデバイスに登録されているユーザは、正しい RSA SecurID PASSCODE を入力しない限り、アクセスが許可されません。

RSA Authentication Agent ソフトウェア

RSA Authentication Agent およびサードパーティのエージェント ホストで認証ダイアログを実行するプログラム。

RSA SecurID ソフトウェア トークン

ネットワーク保護の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。

sdadmin

このプログラムを使用すると、TTY モード (キャラクタベース インタフェース) のプライマリ RSA Authentication Manager for UNIX でのみ、限定された管理作業を直接実行できます。v3.0 以降で追加された RSA Authentication Manager 管理機能は、Windows NT、Windows 2000、Windows XP、または Windows 98 の環境でリモートで実行される RSA Authentication Manager Host Mode アプリケーションを通じてのみ使用できます。

sdconf.rec

インストール プログラムによって作成される構成ファイル。エージェント ホストをインストールするときに、この構成ファイルをエージェント 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ていて、独自の構成レコードを持つサードパーティ デバイスの場合は不要です)。

sdinfo

このユーティリティを UNIX エージェント ホストで実行すると、システム構成レコード (**sdconf.rec**) のコピー (エージェント ホストにあるレコード) の情報が表示されます。このユーティリティを UNIX 版の Authentication Manager サーバで実行すると、構成情報とライセンス情報 (**sdconf.rec** と **license.rec** の内容) が表示されます。

sdlogmon

ログ レコード データベースにログ エントリが書き込まれたときに、そのログ エントリを画面上に表示するユーティリティ。

sdsetup

Authentication Manager システムをインストールおよび構成する RSA Authentication Manager プログラム。

sdshell

UNIX エージェント ホストでユーザの RSA SecurID 認証を要求するシェル。この UNIX エージェントには、NIS や DNS などのネーム サーバを使用する AIX エージェント ホストは含まれますが、**/etc/security/login.cfg** に定義されている認証方式を使用する AIX エージェント ホストは**含まれません**。

sdshell_adm

RSA SecurID PASSCODE を入力せずに、**su** コマンドを使用して簡単にアクセスしたいと考えているシステム管理者には、3 番目の認証シェルである **sdshell_adm** が提供されています。**sdshell** の代わりに **sdshell_adm** を使用できますが、推奨される方法ではありません。

sdshell_auth

ネーム サーバを使用しない AIX エージェント ホストで、ユーザを RSA SecurID で認証するためのシェル。これらのエージェント ホストでのユーザのプライマリ認証方式は “SecurID” であることが必要であり、**sdshell_auth** を実行するには RSA SecurID を **/etc/security/login.cfg** に定義する必要があります。

アクティング スレーブ

アクティング マスタが応答できない場合は、アクティング スレーブが旧バージョンの Agent 認証要求に応答します。

アクティング マスタ

旧バージョンの Agent の認証要求に応答するように構成されたアクティング マスタ。アクティング マスタは完全な機能を備えた v5.2 RSA ACE/Server です。

エージェント ホスト

不正なアクセスを防止するために、RSA Authentication Manager によって保護されているコンピュータまたはその他のデバイス。

自動移行

既存のマスタ Authentication Manager をプライマリにアップグレードする方法。マスタ Authentication Manager のデータベースは 5.2 データベースに自動的に移行されます。スレーブが含まれるシステムでアップグレードを実行する場合は、ローリング アップグレードを実行できます。

世界協定時 (UTC)

世界標準時。グリニッジ標準時とも呼びます。世界協定時は時報で確認します。

データベース ブローカ

RSA Authentication Manager データベースと、データベースにアクセスする RSA Authentication Manager プログラムとの間の接続を提供するプロセス。

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

トークンに表示されるコード。RSA SecurID PASSCODE は、トークンコードと PIN で構成されます。

二要素認証

RSA Authentication Manager システムで使用されている認証方式。ユーザは秘密の個人識別番号 (PIN) と、ユーザに割り当てられている RSA SecurID トークンで生成されたコードを入力する必要があります。PIN とトークンコードによって PASSCODE が構成されます。

ネクスト トークンコード モード

不正な PASSCODE を使用した認証試行が連続して実行されると、トークンはこのモードになります。このモードでは、ユーザが正しいコードを入力した後に、次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。そのコードも正しく入力できた場合だけ、アクセスが許可されます。

ノード シークレット

エージェント ホストと Authentication Manager だけが認識する擬似乱数データの文字列。エージェント ホストと Authentication Manager 間の通信を暗号化するために、ノード シークレットと他のデータの組み合わせが使用されます。

プライマリ Authentication Manager

アドミニストレーションを実行し、データベースの変更をレプリカにレプリケートする RSA Authentication Manager。

ユーザ パスワード

管理者の便宜上提供される特別な種類のトークン。ユーザは認証時に PASSCODE プロンプトに対してパスワードを入力できます。

レプリカ Authentication Manager

RSA SecurID 認証の実行が主要な機能である RSA Authentication Manager。

レプリカ パッケージ

レプリカをインストールするために必要なデータベース ファイルとライセンス ファイル。レプリカ パッケージは、プライマリでレプリカ管理ユーティリティを使用して作成します。ファイルは、***ACEDATA*** ディレクトリ内の **replica_package/database** ディレクトリと **replica_package/license** ディレクトリ、または REP_ACE で指定されるディレクトリに作成されます。

レルム

RSA Authentication Manager プライマリ (および 1 つ以上のレプリカ) と、そのデータベース、エージェント ホスト、ユーザ、トークン。

ローリング アップグレード

既存のマスタをプライマリにアップグレードし、スレーブをレプリカにアップグレードする方法。ローリング アップグレードの場合、既存のデータベースはデータを失うことなく v6.0 データベースに移行されます。認証サービスが停止することもありません。

索引