RSA Authentication Manager 6.1 for Windows
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 Windows Installation Guide』の内容を日本語に翻訳したものです。

第 1 版 日本語版：2005 年 9 月

P/N JS-ACE-6103

目次

はじめに

本書では、RSA Authentication Manager 6.1 for Windows 2000 と RSA Authentication Manager 6.1 for Windows 2003 をインストールする方法について説明します。

対象となる読者

本書は、Windows 2000 および Windows 2003 のセキュリティ システム管理者を対象としています。RSA Authentication Manager をインストールする管理者は、サーバ 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。

本書の内容を一般ユーザに公開しないでください。

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 6.1 for Windows 2000、RSA Authentication Manager 6.1 for Windows 2003、および RSA Authentication Manager 6.1 for UNIX は 1 枚の CD-ROM で提供されます。CD-ROM には、次のものも収録されています .

- RSA Authentication Manager 6.1 for Windows 2000/Windows 2003 のオンライン ヘルプ (英語版)
- Windows 2000/Windows 2003、および UNIX 用の英語版ドキュメント ファイル (PDF 形式)

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。

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。

オンライン ヘルプ

RSA Authentication Manager 6.1には詳細なオンライン ヘルプ システムが用意されており、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。Windows 2000 または Windows 2003 プラットフォームで Configuration Management アプリケーションを実行するか、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

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 台のプライマリと 1 台のレプリカ構成を 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。

- 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。

ライセンスとユーザ登録の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

システム要件

最小システム要件については、付録 C「Windows 2003 Server の最小システム要件」を参照してください。

サポートされるプラットフォーム

- サポートされる言語を実行している Microsoft Windows 2000 Server または Advanced Server (Service Pack 4)
- サポートされる言語を実行している Microsoft Windows 2003 Enterprise Server
- サポートされる言語を実行している Microsoft Windows 2003 Standard Server

サポートされる言語については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

必要なハードウェア

- Intel Pentium 266 MHz 以上のプロセッサ (Windows 2000 Server)
- Intel Pentium 733 MHz 以上のプロセッサ (Windows 2003 Server、Standard Edition または Enterprise Edition)
- 256 MB の物理メモリの他に、1,000 ユーザあたり +2 MB の物理メモリ
- 物理メモリの 2 倍のスワップ ファイル
- ローカル CD-ROM ドライブ
- NTFS ファイル システム
- 1024 × 768 ピクセル以上の解像度のディスプレイ

認証をできるだけ高速化するには、次のハードウェアをご使用ください。

- Intel Pentium 4 (3.2 GHz 以上) のデュアル プロセッサ
- プロセッサあたり 2048 MB の物理メモリ

必要なディスク容量

- RSA Authentication Manager ソフトウェア：200 MB
- 1,000 ユーザあたり 2 MB
- RSA Authentication Manager Remote Administration ソフトウェア：20 MB
- RSA Authentication Agent for Windows：5 MB

必要なディスク容量の詳細については、『RSA Authentication Manager 6.1 管理者ガイド』の各プラットフォームの「データベースのメンテナンス」の章を参照してください。

インストールに関する重要なガイドライン

- プライマリとレプリカのマシンは、RSA Authentication Manager 専用として使用してください。
- 各マシンの名前は、ネットワーク上の完全修飾ドメイン名でなければなりません。
- RSA Authentication Manager は、サポートされるオペレーティング システムにのみインストールしてください。
- 同じシステムに RSA Authentication Manager を 2 つ以上インストールすることはできません。
- RSA Authentication Manager ソフトウェアをネットワーク ドライブや FAT (File Allocation Table) パーティションにインストールすることはできません。
- RSA Authentication Manager をドメイン コントローラにインストールしないでください。
- 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サーバ コンソールにアクセスできるようにしてください。

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 6.0 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、6.0 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。

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

日本時間は時報で確認してください。117 に電話して確認できます。

メモ：NTP サービスを使用する場合は、プライマリでのみ有効にしてください。プライマリは、レプリカのタイム シンクロナイゼーションを自動的に維持します。

データベースで使用する言語の変更

RSA Authentication Manager データベースで使用する言語を変更するには、RSA Authentication Manager ソフトウェアが動作している Windows 2000 マシンまたは Windows 2003 マシンの言語とロケールを変更する必要があります。システムで使用する言語とロケールを指定するには、コントロール パネルの [地域のオプション] を使用します。言語を変更してから RSA Authentication Manager ソフトウェアを再インストールしてください。英語以外の言語を実行しているシステムの場合は、インストール プロセスからメッセージが表示され、適切な言語を選択できます。

注意：英語以外のシステムに RSA Authentication Manager をインストールした後、英語版に戻すことはできません。サポートされる日本語や ISO-Latin-1 言語から、サポートされる別の ISO-Latin-1 言語に変更する場合は、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。

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、『Readme』(**readme.pdf**) を確認してください。構成とインストールに関する重要な情報が記載されています。

アップグレードに必要なもの

- ❑ RSA Authentication Manager CD-ROM。
- ❑ サーバ マシンのディレクトリに格納されているライセンス ファイル。

重要：インストールを開始する前にライセンス ファイル (**sdti.cer**、**server.cer**、**server.key**、および **license.rec**) 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、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。

- ❑ 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：納品される各 RSA SecurID トークンには、トークン シード レコードが同梱されていますが、RSA Authentication Manager とトークン シード レコードは別のパッケージで納品されます。

- ❑ 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。
- ❑ マシンのローカル Administrator 権限。

必要な情報

- ❑ Windows 2003 または Windows 2000 マシンで使用されている言語とロケール、および使用する言語。サポートされる言語については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。
- ❑ 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。
- ❑ インストールするレプリカの名前と IP アドレス。

  プライマリのインストールの後にレプリカを定義します。レプリカを追加するには、付録 D「データベース ユーティリティ」で説明されているレプリカ管理ユーティリティを使用します。

操作

- ❑ インストールの前に、ライセンス ファイルのバックアップ コピーを作成します。オリジナルのライセンス ファイルとトークン シード レコードを安全な場所に保管してください。
- ❑ 標準インストールを実行するのか、サイレント インストールを実行するのかを指定します。サイレント インストールの場合、構成パラメータはコマンド ラインから指定します。

2 RSA Authentication Manager のインストール

この章では、1 台のプライマリと 1 台以上のレプリカを新規にインストールする方法について説明します。

プライマリの新規インストール

重要：各マシンの名前は、ネットワーク上の完全修飾ドメイン名でなければなりません。

プライマリに RSA Authentication Manager を新規インストールするには

1. 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。

   メモ：RSA RADIUS サーバは、Authentication Manager とともに自動的にインストールされます。**RSA RADIUS Administration.msi** は使用しないでください。
3. [Select 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。[Primary RSA Authentication Manager] を選択します。
4. 画面の指示に従ってインストールを完了します。
5. ライセンス ファイル (**sdti.cer**、**server.cer**、**server.key**、および **license.rec**) のバックアップコピーを作成し、CD-ROM に保存します。

   重要：ライセンス ファイルは、インストール中に変更されます。したがって、ディレクトリ内のライセンス ファイルが消失したり、壊れたりした場合、再びアクセスするには変更されたライセンス ファイルが必要です。
6. RSA Authentication Manager プロセスを起動します。操作手順については、14 ページの「RSA Authentication Manager プロセスの起動と停止」を参照してください。

サイレント モードでプライマリに RSA Authentication Manager を新規インストールするには

1. 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. 次のコマンドを入力して、インストールを開始します。

```
setup.exe /s /v"/q /l* log file TYPE=PRIMARY LICPATH=path to
license file [LANG=language] [INSTALLDIR=installation
directory]"
```

log file には、ログファイルへの完全修飾パスを指定し、*斜体*の部分にはそれぞれ適切な値を指定します。

メモ：コマンドを入力するときは、必要な引用符を忘れずに指定してください。

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、インストールでデフォルト値が使用されます。

省略可能なプロパティ	指定可能な値	デフォルト値
LANG	ENG、SPA、TCH など	ENG
INSTALLDIR	インストール ディレクトリの完全修飾パス	[Program Files] > [RSA Security] > [RSA Authentication Manager]

たとえば、デフォルト値を使用してプライマリを新規インストールするには、次のように入力します。

```
setup.exe /s /v"/q /l* c:¥log.txt TYPE=PRIMARY
LICPATH=d:¥license_files"
```

3. ライセンス ファイル (**sdti.cer**、**server.cer**、**server.key**、および **license.rec**) のバックアップコピーを作成し、CD-ROM に保存します。

重要：ライセンス ファイルは、インストール中に変更されます。したがって、ディレクトリ内のライセンス ファイルが消失したり、壊れたりした場合、再びアクセスするには変更されたライセンス ファイルが必要です。

4. RSA Authentication Manager プロセスを起動します。操作手順については、14 ページの「RSA Authentication Manager プロセスの起動と停止」を参照してください。

RSA Authentication Manager プロセスの起動と停止

すべての RSA Authentication Manager プロセスの起動と停止は、[RSA Authentication Manager Control Panel] から行います。

プライマリですべてのRSA Authentication Managerプロセスを起動または停止するには

1. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。
2. [RSA Auth Mgr Control Panel] ツリーで [Start & Stop RSA Authentication Manager Services] をクリックします。
3. [Service Management] で以下の操作を行います。
   - すべてのサービスを起動するには、[Start Services] の [Start All] をクリックします。
   - すべてのサービスを停止するには、[Stop Services] の [Stop All] をクリックします。

データベースへのトークン シード レコードの追加

プライマリに RSA Authentication Manager を新規インストールした場合は、データベースにトークン シード レコードはなく、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 つあるだけです。

ここでトークン シード レコードをインポートすると、管理者のユーザ レコードを作成し、トークンを割り当てることができます。トークン レコードをインポートしない場合は、データベースを管理できるのはソフトウェアをインストールしたユーザだけになり、プライマリのマシン上でローカルに管理することだけが可能です。

トークン シード レコードのインポートと、データベースへのユーザの追加の詳細については、RSA Authentication Manager のオンライン ヘルプを参照してください。

RSA Authentication Manager データベースにトークン シード レコードを追加するには

1. プライマリにローカルの Administrator としてログオンします。
2. トークン シード レコードが保存されているメディアを適切なドライブに挿入します。
3. [スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Host Mode] の順にクリックします。
4. [Token] メニューの [Import Tokens] を選択します。
5. 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。または [Open] ボタンをクリックして場所を参照します。
6. [OK] をクリックします。
7. [OK] をクリックしてダイアログ ボックスを閉じます。
   新しいトークン レコードが **sdserv** データベースに追加されます。

トークンが正しくインポートされたことを確認するには

1. [Token] > [List Tokens] の順にクリックします。
2. [List Tokens] ダイアログ ボックスの [List to Screen]、[List All Tokens]、[All Algorithms] チェックボックスをオンにし、[OK] をクリックします。
   トークン レポートにデータベース内のすべてのトークンの一覧が表示されます。
3. トークン レポートを閉じるには、[Exit] をクリックします。

Push DB によるレプリカへの初期データベースのプッシュ

Push DB (レプリカへの初期データベースのプッシュ) は、RSA Authentication Manager データベース ファイルをレプリカに自動的に配布する方法です。

- プライマリで Push DB 機能が有効な場合は、***ACEDATA*¥replica_package¥license¥** ディレクトリをレプリカ マシンにコピーします。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 機能が無効な場合は、***ACEDATA*¥replica_package¥** ディレクトリをレプリカ マシンにコピーします。

デフォルトでは、Push DB は有効に設定されています。Push DB を無効にするには、次の手順を実行します。無効にしない場合は、次の「新規レプリカの追加とインストール」に進みます。

Push DB を無効にするには

1. RSA Authentication Manager Administration を起動します。
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。

ステップ 3 で逆の操作を行うと、いつでもこの機能を有効にできます。

次の「新規レプリカの追加とインストール」に進みます。

新規レプリカの追加とインストール

新規レプリカを追加およびインストールするには

1. プライマリの [RSA Authentication Manager Control Panel] ですべてのサービスを停止します。操作手順については、14 ページの「RSA Authentication Manager プロセスの起動と停止」を参照してください。
2. プライマリで、[スタート] > [プログラム] > [RSA Security] > [RSA Authentication Manager Configuration Tools] > [RSA Authentication Manager Replica Management] の順にクリックして、レプリカ管理ユーティリティを起動します。

   メモ : レプリカを実行している場合やデータベース ブローカを停止していない場合、使用できるボタンは [Details] ボタンだけで、サーバのリストの上に [READ ONLY Access to database] が表示されます。

3. プライマリのデータベースにレプリカを追加します。レプリカ マシン名には完全修飾コンピュータ名を入力する必要があります。操作手順については、オンライン ヘルプの「Adding a Replica to the Database」を参照してください。
4. プライマリでレプリカ パッケージを作成します。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。操作手順については、オンライン ヘルプの「Creating a Replica Package」を参照してください。
5. 次のいずれかの操作を実行します。
   - プライマリで Push DB 機能が有効な場合は、**¥¥RSA Authentication Manager¥data¥replica_package¥license** ディレクトリをレプリカ マシンにコピーします。
   - プライマリでが Push DB 機能が無効な場合は、**¥¥RSA Authentication Manager¥data¥replica_package** ディレクトリをレプリカ マシンにコピーします。

6. [RSA Authentication Manager Control Panel] を使用して、プライマリを起動します。
7. レプリカをインストールします。操作手順については、次の「レプリカに RSA Authentication Manager ソフトウェアをインストールするには」を参照してください。
8. [RSA Authentication Manager Control Panel] を使用して、レプリカを起動します。

重要：プライマリとレプリカの間の初期接続を確立し、レプリカに適切なデータベースがあることをプライマリが確認できるようにするには、プライマリが動作している必要があります。

レプリカに RSA Authentication Manager ソフトウェアをインストールするには

重要：各サーバ マシンの名前はすべて小文字でなければならず、ネットワーク上の完全修飾コンピュータ名であることが必要です。

1. 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。

   メモ：RSA RADIUS サーバは、Authentication Manager とともに自動的にインストールされます。**RSA RADIUS Administration.msi** は使用しないでください。
3. [Select 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。[Replica RSA Authentication Manager] 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、プライマリからコピーしたレプリカ パッケージを参照し、[Next] をクリックします。
5. 画面の指示に従ってインストールを完了します。

インストールするレプリカごとに、この手順を繰り返してください。

サイレント モードでレプリカに RSA Authentication Manager ソフトウェアをインストールするには

重要：各サーバ マシンの名前はすべて小文字で、ネットワーク上の完全修飾コンピュータ名であることが必要です。

1. 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. 次のコマンドを入力して、インストールを開始します。

   ```
   setup.exe /s /v"/q /l* log file TYPE=REPLICA LICPATH=path to
   Replica Package [INSTALLDIR=installation directory]"
   ```

   log file には、ログファイルへの完全修飾パスを指定し、*斜体*の部分にはそれぞれ適切な値を指定します。

   メモ：コマンドを入力するときは、必要な引用符を忘れずに指定してください。

INSTALLDIR 引数は省略可能です。ディレクトリ パスを指定しないと、[Program Files] > [RSA Security] > [RSA Authentication Manager] にインストールされます。

たとえば、デフォルト値を使用してレプリカを新規インストールするには、次のように入力します。

```
setup.exe /s /v"/q /l* c:¥log.txt TYPE=REPLICA
LICPATH=c:¥replica_package"
```

3. インストールするレプリカごとに、この手順を繰り返してください。

次のステップ

- Remote Administration ソフトウェアをインストールまたはアップグレードするには、第 3 章「Remote Administration ソフトウェアのインストールとアップグレード」を参照してください。
- ブラウザベースのアドミニストレーション アプリケーションである Quick Admin をインストールまたはアップグレードするには、第 5 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。

3 Remote Administration ソフトウェアのインストールとアップグレード

Remote Administration ソフトウェアを使用すると、RSA Authentication Manager データベースをリモート管理できます。RSA Authentication Manager Host Mode は、プライマリまたはレプリカから実行でき、RSA Authentication Manager Remote Administration ソフトウェアを実行している他のマシンから実行することもできます。

メモ：Remote Administration アプリケーションを使用して変更できるのは、プライマリのデータベースだけです。レプリカ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。

インストール / アップグレードのチェックリスト

操作を開始する前に、次のチェックリストを使用して、RSA Authentication Manager ソフトウェアのアップグレード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確認してください。

- ❑ Windows 2000 Professional Server、Windows 2000 Advanced Server (Service Pack 4)、Windows XP Pro、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。
- ❑ 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。
- ❑ Windows マシンの言語とロケール、および使用する言語。
- ❑ リモート マシンのローカル 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。

さらに、標準インストールを実行するのか、サイレント インストールを実行するのかを指定します。サイレント インストールの場合、構成パラメータはコマンド ラインから指定します。

Remote Administration の新規インストール

メモ：Remote Administration ソフトウェアは、RSA Authentication Manager 6.1 のインストールまたはアップグレード時に、デフォルトでプライマリまたはレプリカにインストールされます。ただし、レプリカ データベースへのリモート アドミニストレーション接続は読み取り専用です。

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

1. 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。

   メモ：RSA RADIUS サーバは、Authentication Manager とともに自動的にインストールされます。**RSA RADIUS Administration.msi** は使用しないでください。
3. [Select 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。
4. **sdconf.rec**ファイルと**server.cer**ファイルが格納されているディレクトリを参照し、[Next] をクリックします。
5. 画面の指示に従ってインストールを完了します。
6. 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。

インストールの終了後、リモート アドミニストレーションを行うことができるようにプライマリを構成する手順については、『RSA Authentication Manager 6.1 管理者ガイド』の「Remote Administration」の章を参照してください。

サイレント モードで Remote Administration ソフトウェアをインストールするには

1. 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. 次のコマンドを入力して、インストールを開始します。

   ```
   setup.exe /s /v"/q /l* log file TYPE=REMOTE LICPATH=path to
   server.cer and sdconf.rec"
   ```

   log file には、ログファイルへの完全修飾パスを指定し、*斜体*の部分にはそれぞれ適切な値を指定します。

   メモ：コマンドを入力するときは、必要な引用符を忘れずに指定してください。

   たとえば、Remote Administration をインストールするには、次のように入力します。

   ```
   setup.exe /s /v"/q /l* c:¥log.txt TYPE=REMOTE
   LICPATH=c:¥license_files"
   ```

3. 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。

インストールの終了後、リモート アドミニストレーションを行うことができるようにプライマリを構成する手順については、『RSA Authentication Manager 6.1 管理者ガイド』の「Remote Administration」の章を参照してください。

Remote Administration のアップグレード

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

1. 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 ManagerCD-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. [Upgrade] 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 this installation] チェックボックスをオンにし、[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。

サイレント モードで Remote Administration ソフトウェアをアップグレードするには

1. 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. 次のコマンドを入力して、アップグレードを開始します。

   ```
   setup.exe /s /v"/q /l* log file TYPE=REMOTE LICPATH=path to
   server.cer and sdconf.rec UPGRADE=1"
   ```

   log file には、ログファイルへの完全修飾パスを指定し、*斜体*の部分にはそれぞれ適切な値を指定します。

   メモ：コマンドを入力するときは、必要な引用符を忘れずに指定してください。

   たとえば、Remote Administration をアップグレードするには、次のように入力します。

   ```
   setup.exe /s /v"/q /l* c:¥log.txt TYPE=REMOTE
   LICPATH=c:¥license_files UPGRADE=1"
   ```

リモート管理するサーバの追加

Remote Administration ソフトウェアが動作しているマシンから別のデータベースを管理する必要がある場合は、リモート管理するサーバを追加します。

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] > [プログラム] > [RSA Security] > [RSA Authentication Manager Control Panel] の順にクリックします。
2. [RSA Authentication Manager Control Panel] メニューの [Add & Remove Remote Administration] をクリックします。
3. 右側のパネルで、[Add] をクリックします。
4. **sdconf.rec**ファイルと**server.cer**ファイルの場所を指定し、[OK]をクリックします。
5. 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 マシンとプライマリの **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。

メモ：Remote Administration のリストからサーバを削除するには、そのレルムのすべての管理セッションを停止した後、ステップ 3 で削除するサーバを選択し、[Remove] をクリックします。

Remote Administration からサーバを削除するには

1. 適用可能なレルムですべての管理セッションをシャットダウンします。
2. [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。
3. [RSA Authentication Manager Control Panel] メニューの [Add & Remove Remote Administration] をクリックします。

右側のパネルで、削除するサーバを選択し、[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)。

リモートから管理しているレルムのすべてのサーバに対して、同じ範囲のポート番号を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. [RSA Authentication Manager Control Panel] を使用して、RSA Authentication Manager とデータベース ブローカを停止します。
2. **RSA Authentication Manager¥rdbms32** ディレクトリに、**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。
3. 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 ]
   ```

   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、次のように指定します。

   ```
   -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。

   メモ：Windows システムの場合、最小ポート番号として 3000 未満の値は指定できません。

   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。
4. RSA Authentication Manager を再起動します。

4 RSA Authentication Manager 6.1 へのアップグレード

RSA Authentication Manager 6.1 へのアップグレードは、RSA ACE/Server 5.1 以上 (およびパッチ バージョン)、および RSA Authentication Manager 6.0 以上 (およびパッチ バージョン) から行うことができます。

アップグレード前のチェックリスト

重要 : 現在、RSA RADIUS サーバを使用していて、RSA RADIUS 6.1 へ移行する場合は、プライマリ サーバとレプリカ サーバ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。
- ❑ システム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。
- ❑ 既存のプライマリ サーバの **sdserv** および **sdlog** 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 : 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。操作手順については、29 ページの「RSA ACE/Server 5.1 または 5.2 サービス、または RSA Authentication Manager 6.0 サービスの起動と停止」を参照してください。

- ❑ プライマリおよびレプリカでのローカル 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。新しいライセンスを購入した場合は、新しいライセンス ファイル。

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。

さらに、標準アップグレードを実行するのか、サイレント アップグレードを実行するのかを指定します。サイレント アップグレードの場合、構成パラメータはコマンド ラインから指定します。

プライマリのアップグレード前の準備

重要：アップグレードを実行する前に、プライマリ サーバとレプリカ サーバのローカル 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、マシンがロックされることがあります。操作手順については、RSA Authentication Agent のマニュアルを参照してください。

プライマリのアップグレードの準備をするには

1. RSA ACE/Server 5.1 または 5.2 プライマリ サーバ、または RSA Authentication Manager 6.0 プライマリ サーバで RSA ACE/Server サービスを停止します。操作手順については、29 ページの「RSA ACE/Server 5.1 または 5.2 サービス、または RSA Authentication Manager 6.0 サービスの起動と停止」を参照してください。

   アップグレードするサーバでサービスが動作している間は、ソフトウェアをアップグレードできません。さらに、[Automatic RSA ACE/Server startup] をオフにする必要があります。

2. すべての RSA ACE/Server プロセスまたは RSA Authentication Manager プロセスを停止した後、***ACEDATA*** ディレクトリをコピーすることによって、データベース ファイル、ライセンス ファイル、および構成ファイルのバックアップ コピーを作成します。

   メモ：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。

   データのバックアップの詳細については、『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 (Windows)」の章を参照してください。

3. マシンを再起動します。

マシンを再起動すると、プライマリをアップグレードできる状態になります。

プライマリのアップグレード

メモ：以前のバージョンの RSA ACE/Server と同じ場所に RSA Authentication Manager 6.1 をインストールすることはできません。新しいデフォルトの場所は、**<*drive*>:¥Program Files¥RSA Security¥RSA Authentication Manager** です。

プライマリをアップグレードするには

1. プライマリ 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. **aceserv¥windows¥** ディレクトリの **setup.exe** をダブルクリックします。
3. [Upgrade] 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 this installation] チェックボックスをオンにし、[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。

5. レプリカを追加する予定がない場合にのみ、プライマリの [RSA Authentication Manager Control Panel] から RSA Authentication Manager サービスを起動します。

プライマリのアップグレードはこれで完了です。

サイレント モードでプライマリをアップグレードするには

1. プライマリ 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. 次のコマンドを入力して、アップグレードを開始します。

   ```
   setup.exe /s /v"/q /l* log file TYPE=PRIMARY LICPATH=path to
   license files UPGRADE=1"
   ```

   log file には、ログファイルへの完全修飾パスを指定し、*斜体*の部分にはそれぞれ適切な値を指定します。

   メモ：コマンドを入力するときは、必要な引用符を忘れずに指定してください。

   たとえば、プライマリをアップグレードするには、次のように入力します。

   ```
   setup.exe /s /v"/q /l* c:¥log.txt TYPE=PRIMARY
   LICPATH=d:¥license_files UPGRADE=1"
   ```

3. マシンを再起動します。
4. レプリカを追加する予定がない場合にのみ、プライマリの [RSA Authentication Manager Control Panel] から RSA Authentication Manager サービスを起動します。

プライマリのアップグレードはこれで完了です。

レプリカのアップグレード前の準備

レプリカのアップグレードの準備をするには

1. プライマリからレプリカへレプリカ パッケージをコピーします。
2. ***ACEDATA*¥replica_package¥** ディレクトリをレプリカ マシンの ***ACEDATA*** 以外のディレクトリにコピーします。

   メモ：プライマリで Push DB 機能が有効な場合は、***ACEDATA*¥replica_package¥license** ディレクトリを、レプリカ マシンの ***ACEDATA*** 以外のディレクトリにコピーする必要があります。レプリカをインストールし、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。

3. レプリカですべての RSA ACE/Server サービスまたは RSA Authentication Manager サービスとを停止します。操作手順については、29 ページの「RSA ACE/Server 5.1 または 5.2 サービス、または RSA Authentication Manager 6.0 サービスの起動と停止」を参照してください。

   アップグレードするサーバでサービスが動作している間は、ソフトウェアをアップグレードできません。さらに、[Automatic RSA ACE/Server startup] をオフにする必要があります。
4. ***ACEDATA*** ディレクトリをコピーすることによって、データベース ファイル、ライセンス ファイル、および構成ファイルのバックアップ コピーを作成します。

メモ：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。

RSA Authentication Manager データのバックアップの詳細については、『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 (Windows)」の章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には

1. レプリカ 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. [Upgrade] 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 this installation] チェックボックスをオンにし、[Next] をクリックします。
4. レプリカ パッケージの場所を指定し、[Next] をクリックします。
5. 画面の指示に従ってインストールを完了します。
6. レプリカ サーバで RSA Authentication Manager サービスを再起動します。

メモ：レプリカが起動すると、Push DB が有効な場合は、プライマリがレプリカにデータベースをプッシュします。

レプリカのアップグレードはこれで完了です。

サイレント モードでレプリカをアップグレードするには

1. レプリカ 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. 次のコマンドを入力して、アップグレードを開始します。

```
setup.exe /s /v"/q /l* log file TYPE=REPLICA LICPATH=path to
Replica Package UPGRADE=1"
```

log file には、ログファイルへの完全修飾パスを指定し、*斜体*の部分にはそれぞれ適切な値を指定します。

メモ：コマンドを入力するときは、必要な引用符を忘れずに指定してください。

たとえば、レプリカをアップグレードするには、次のように入力します。

```
setup.exe /s /v"/q /l* c:¥log.txt TYPE=REPLICA
LICPATH=c:¥replica_package UPGRADE=1"
```

3. レプリカで RSA Authentication Manager サービスを再起動します。

メモ：レプリカが起動すると、Push DB が有効な場合は、プライマリがレプリカにデータベースをプッシュします。

レプリカのアップグレードはこれで完了です。

RSA ACE/Server 5.1 または 5.2 サービス、または RSA Authentication Manager 6.0 サービスの起動と停止

プライマリですべての RSA ACE/Server 5.1 または 5.2 サービス、または RSA Authentication Manager 6.0 サービスを停止するには

重要：すべてのリモート管理者にまもなくシャットダウンすることを通知します。

1. [スタート]>[設定]>[コントロール パネル]の順にクリックし、[RSA ACE/Server] アイコンをダブルクリックします。
2. [RSA ACE/Server] で [Stop] をクリックします。
3. 「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。
4. [RSA ACE/Server] ダイアログ ボックスの [OK] をクリックします。

[Automatic RSA ACE/Server startup] チェックボックスがオンの場合は、オフにします。

5 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

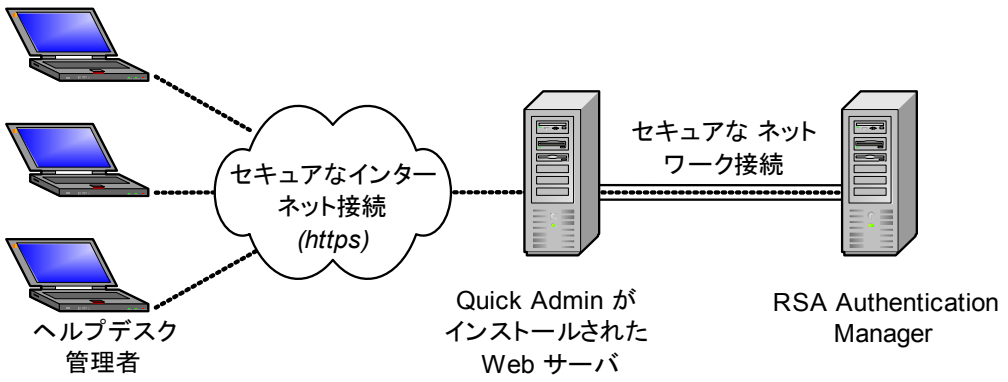
Quick Admin は以下で構成されています。

- 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、39 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、39 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、39 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、39 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. 34 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. 37 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、47 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、44 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

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
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 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、プライマリでテスト変換を実行します。操作手順については、52 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. プライマリをアップグレードします。操作手順については、26 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、プライマリで完全な変換を実行します。操作手順については、52 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 (1 つまたは複数) をアップグレードします。操作手順については、27 ページの「レプリカのアップグレード前の準備」、および 28 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。

テスト変換を実行するには

1. 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. 6.1 より前のバージョンのプライマリ RSA Authentication Manager Host Mode で、[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	52 ページの「完全な変換の実行」の説明を参照して、プログラム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

UNIX から Windows への RSA Authentication Manager の転送

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

1. Windows マシンに RSA Authentication Manager を新規インストールします。手順については、13 ページの「プライマリの新規インストール」を参照してください。

   インストールの終了後、Windows マシンのデータベースには、RSA Authentication Manager 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 UNIX プライマリで、次のコマンドを入力して **aceserver** を停止します。

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

3. サーバ データベースのダンプ ファイルを作成します。次のコマンドを入力します。

   ```
   ./sddump -s
   ```

   sdserv.dmp というファイルがカレント ディレクトリに作成されます。

4. Windows システムに **¥dump** ディレクトリを作成します。

5. RSA Authentication Manager が動作している UNIX 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 **RSA Authentication Manager¥data** ディレクトリにコピーしないでください。

Windows 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**

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。
   - [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 Auth Mgr Control Panel] メニューで [Start & Stop RSA Auth Mgr Services] をクリックします。
   - [Start Services] の下の [Stop All] をクリックします。

2. [スタート] > [RSA Security] > [RSA Authentication Manager Database Tools] > [Load] をクリックします (または **RSA Authentication Manager¥prog** ディレクトリで **sdload.exe** をダブルクリックします)。

   [RSA Authentication Manager Database Load] ダイアログ ボックスが表示されます。

3. [Server Database] チェックボックスをオンにして、サーバ ダンプ ファイルをロードすることを指定します。

4. [Server dump filename] ボックスに、ダンプ ファイルと **license.rec** ファイルのディレクトリを入力するか、その場所を参照します。
5. [Server Database Load Options] 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、62 ページページの「マージ ロジック」を参照してください。

6. [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。
7. [Close] をクリックします。

メモ：RSA Authentication ManagerUNIX マシンが RSA Authentication Manager 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 Replication Management] の順にクリックします。

C Windows 2003 Server の最小システム要件

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 Windows 2003 Server のコンポーネントについて説明します。操作に先立ち、10 ページに記載されている RSA Authentication Manager に関する「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。

メモ：RSA Authentication Manager のサービスとプロセスの詳細については、『RSA Authentication Manager 6.1 管理者ガイド』を参照してください。

システムを適切に最小化するためには、Windows 2003 Server を新規インストールすることをお勧めします。インストールでネットワーク インタフェース カード (NIC) を設定するときに、次の操作を実行します。

- [カスタム設定] を使用します。
- [インターネット プロトコル (TCP/IP)] 以外のすべての設定をアンインストールします。

NIC で DNS と WINS を構成する場合は、次の操作を実行します。

- 操作環境で DNS がサポートされていない場合は、[この接続のアドレスを DNS に登録する] チェックボックスをオフにします。
- [LMHOSTS の参照を有効にする] チェックボックスをオフにします。
- [WINS] タブの [NetBIOS Over TCP/IP を無効にする] チェックボックスをオンにします。
- システムが独立したワークグループのメンバであることを確認します。

インストールが完了したら、サービスを構成する必要があります。

Windows 2003 Server 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、次のサービスを [自動] に設定して、各サービスを開始します。

- DNS Client
- Event Log
- Logical Disk Manager
- Network Connections
- Plug & Play
- Protected Storage
- Remote Procedure Call
- Removable Storage
- Secondary Login Service
- Security Accounts Manager
- Windows Management Instrumentation

次のサービスを [手動] に設定して、各サービスを停止します。

- Uninterrupted Power Supplies
- Windows Installer
- Windows Time

その他の**すべて**のサービスは無効にします。

Windows 2003 Server Service Pack

Windows 2003 Server をインストールし、最小化した後で、適切な Service Pack とパッチをインストールできます。ただし、RSA Authentication Manager 6.1 は、最新のパッチに対して検証されていない可能性があります。このため、最新のパッチをインストールする場合は、事前に RSA セキュリティ正規販売代理店にご相談ください。

D データベース ユーティリティ

この付録では、インストールおよびアドミニストレーションに関連するデータベース 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。

ユーティリティ	目的
データベース ダンプ (**sddump.exe**)	サーバ データベースとログ データベースの内容をダンプし、ダンプ ファイル (**sdserv.dmp** と **sdlog.dmp**) を作成します。
データベース作成 (**sdnewdb.exe**)	ダンプ ファイルをロードするために必要な新しい空のデータベースを作成します。
データベース ロード (**sdload.exe**)	ダンプ ファイルを新しいデータベースにロードします。
データベース ダンプ リーダ (**dumpreader.exe**)	ダンプ ファイルの内容を業界標準の各種テキスト形式 (CSV、HTML、XML、TXT) に出力します。

データベース ダンプ ユーティリティとデータベース ロード ユーティリティには、インタフェース バージョンとコマンド ライン バージョンがあります。ダンプ ユーティリティとロード ユーティリティのコマンド ライン バージョンは、DOS プロンプトから実行できます。このバージョンは、特定のデータベース テーブルをダンプおよびロードできる追加機能を備えています。詳細については、62 ページの「DOS コマンドライン バージョンのダンプ ユーティリティとロード ユーティリティの使用」を参照してください。

メモ：この付録では、レプリカに関して多くの重要な機能を実行するレプリカ管理ユーティリティ (**sdrepmgmt_nt**) については説明していません。このユーティリティを使用すると、レプリカの追加と削除、新規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、レプリカからプライマリへの昇格を実行できます。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。

データベースのダンプ

データベースのダンプを作成するには

1. [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。

   [Authentication Manager Database Dump] ダイアログ ボックスが表示されます。

2. [Select Databases to Dump] の [Dump Log Database] チェックボックスと [Dump Server Database] チェックボックスをオンにします。

3. 関連するすべてのデルタ情報をダンプするには、[Options] の [Include delta tables in dump file] チェックボックスをオンにします。

[Allow database connections in multi-user mode] チェックボックスをオンにすると、データベースがアクティブな状態でもダンプを実行できます。すべての RSA Authentication Manager サービスが停止している場合は、このチェックボックスをオンにしてこのオプションを有効にできます。**停止していない** RSA Authentication Manager サービスがある場合は、このオプションはデフォルトで有効です。

メモ：アクティブなデータベースから作成されたダンプ ファイルには通常、他の管理作業によって発生するテンポラリ レコードが含まれます。マルチユーザ モードは、データベースの内容の確認や、ロード前のテストのためにダンプ ファイルを作成するときに限って使用することをお勧めします。

4. [Selective Dump] では、オプション ボタンを使用して、ダンプするデータの種類を指定できます。選択できるオプションは次のとおりです。
   - [By Group] を選択すると、特定のグループをダンプできます。グループの名前を入力してください。
   - [By User] を選択すると、特定のユーザをダンプできます。デフォルト ユーザ名を入力してください。
   - [By Token] を選択すると、特定のトークンをダンプできます。トークンのシリアル番号を入力してください。
5. [Disk Space Requirements] で、ディスクの空き容量がダンプに必要なディスク容量より多いことを確認します。[Output Directory] ボックスに、ダンプ ファイルを作成するディレクトリのパスを指定します。

   RSA Authentication Manager ソフトウェアが格納されているディレクトリ (通常は **ace**) 以外のパスを指定します。デフォルト ディレクトリにダンプ ファイルを作成する場合は、RSA Authentication Manager ソフトウェアをアンインストールする前に、ファイルを別の場所にコピーする必要があります。
6. [OK] をクリックします。

   [RSA Authentication Manager Database Dump] ダイアログ ボックスに、ダンプ プロセスのステータスが表示されます。
7. 次のいずれかの操作を実行します。
   - ダンプ プロセスが終了したら、[Close] をクリックします。
   - ダンプ プロセスのステータス レポートを保存する場合は、[Save As] をクリックし、ファイル名とディレクトリを入力します。次に、[Save] をクリックし、[Close] をクリックします。

   [Output Directory] ボックスに指定したディレクトリに、ダンプ ファイル **sdserv.dmp** および **sdlog.dmp** が格納されます。61 ページの「ダンプ ファイルのロード」で説明するデータベース ロード プロセスでは、これらのダンプ ファイルと、**RSA Authentication Manager¥data** ディレクトリからコピーした **license.rec** ファイルが必要です。

これでダンプ プロセスは完了です。

データベースの新規作成

新しいデータベースを作成すると、既存のデータベース内のすべてのレコードが上書きされます。新しいデータベースにロードするダンプ ファイルに、少なくとも 1 つの管理者レコードが含まれていることを確認してください。

データベースを新規作成するには

1. RSA Authentication Manager プロセスが実行されていないことを確認します。
2. **RSA Authentication Manager¥prog** ディレクトリの **sdnewdb.exe** をダブルクリックします。
3. 新しい空の RSA Authentication Manager データベースを作成するには、[Log Database] チェックボックスと [Server Database] チェックボックスをオンにします。
4. [OK] をクリックします。

   プログラムが終了すると、新しいデータベースの作成に関する確認が求められます。

ダンプ ファイルのロード

ダンプ ファイルをロードするには

1. RSA Authentication Manager プロセスが実行されていないことを確認します。
2. **RSA Authentication Manager¥data** ディレクトリにダンプ ファイルをコピーします。
3. **RSA Authentication Manager¥prog** ディレクトリの **sdload.exe** をダブルクリックします。
4. [Server Database] チェックボックスと [Log Database] チェックボックスをオンにして、サーバ ダンプ ファイルとログ ダンプ ファイルをロードすることを指定します。
5. [Server dump filename] ボックスに、サーバ ダンプ ファイルの場所を入力します。別のレルムのデータベースをマージする場合は、**license.rec** ファイルの場所を入力します。または、[Browse] をクリックしてファイルの場所を選択します。
6. [Log dump filename] ボックスに、ログ ダンプ ファイルの場所を入力するか、または [Browse] をクリックしてファイルの場所を選択します。
7. [Server Database Load Options] で、次のチェックボックスを 1 つ以上オンにして、ロード操作に適用する条件を指定します。
   - [Server dump file has a different licence record than the current database] チェックボックスをオンにすると、別の RSA Authentication Manager のダンプ ファイルをロードしたり、別のレルムのダンプ ファイルを RSA Authentication Manager 6.1 データベースにマージしたりできます。
   - [Load delta records] チェックボックスをオンにすると、ダンプ ファイルと関連デルタ レコードがロードされます。

- [Commit loaded records only if all records are loaded successfully] チェックボックスをオンにすると、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。ダンプ ファイルが正しくロードされなかった場合は、データベースへの変更はコミットされません。
- [Merge records from server dump file with records in current database]チェックボックスをオンにすると、サーバ ダンプ ファイルのデータがデータベースに追加されます。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。

8. データベースにダンプ ファイルをロードするには、[OK] をクリックします。

マージ ロジック

[Merge records from server dump file with records in current database] チェックボックスをオンにすると、データベース内の情報が保持されます。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。ダンプ ファイル内の競合するシステム レコードは新しいデータベースにロードされないので注意してください。

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。

[Commit loaded records only if all records are loaded successfully] チェックボックスをオンにすると、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。

DOS コマンドライン バージョンのダンプ ユーティリティとロード ユーティリティの使用

データベース ダンプ ユーティリティとデータベース ロード ユーティリティには DOS コマンド ライン バージョンがあり、サーバ データベースの特定のテーブルをダンプしたり、ダンプ ファイルからサーバ データベースに特定のテーブルをロードしたりできます。ここでは、4 つのコマンド ライン ダンプ ユーティリティとロード ユーティリティについて説明します。

sdloadsrv

sdloadsrv ユーティリティでは、DOS コマンド ラインを使用して、サーバのダンプ ファイルをデータベースにロードできます。このコマンド ライン バージョンには、インタフェース バージョンのロード ユーティリティ (**sdload.exe**) にはない機能が追加されています。たとえば、サーバ ダンプ ファイルからテーブルを選択してロードできる機能などがあります。

次の表は、**sdloadsrv** 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
-d	*database name*	データベースのファイル名を指定します。ファイル名を指定しなかった場合のデフォルト値は **RSA Authentication Manager¥data¥sdserv** です。

オプション	引数	説明
-f	*filename*	ロード ファイルの名前を指定します。このオプションは必須です。
-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。
-m	なし	サーバ ダンプ ファイル (任意のバージョン) をプライマリ データベースにマージします。
-u	なし	v4.1 以前のダンプ ファイルをアップグレード モードでロードします。新しいデータベースにレプリカ テーブルが作成され、現在のシステムがプライマリとして追加されます。6.1 ダンプ ファイルを使用している場合は、このオプションは **-r** オプションと同じ動作をします。
-t	*table_list*	ダンプ ファイルから読み取られる各レコードの関連データで構成されるテーブルのリストを指定します。
-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サーバ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。v4.1 以前のダンプ ファイルを使用している場合は、このオプションは **-u** オプションと同じ動作をします。
-l	*licensefile*	ライセンス ファイルを指定します。
-c	なし	ダンプ ファイルが正しくロードされた場合のみ、データベースへの変更をコミットします。ダンプ ファイルが正しくロードされなかった場合は、データベースへの変更はコミットされません。
-v	なし	詳細な出力情報を表示します。

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。

sddumpsrv

sddumpsrv ユーティリティでは、DOS コマンド ラインを使用して、データベースからダンプ ファイルを作成できます。このコマンド ライン バージョンには、インタフェース バージョンのダンプ ユーティリティ **(sddump.exe)** にはない機能が追加されています。たとえば、サーバ データベースからテーブルを選択してダンプできる機能などがあります。

次の表は、**sddumpsrv** 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
-d	*database name*	データベースのファイル名を指定します。

オプション	引数	説明
-f	*filename*	ダンプ ファイルの名前を指定します。
-t	*table list*	ダンプ ファイルから読み取られる各レコードの関連データで構成されるテーブルのリストを指定します。
-p	なし	必要な親テーブルをダンプします。
-r	なし	レプリカ (デルタ) レコードをダンプします。
-m	なし	マルチユーザ モードでデータベースをダンプできます (データベース ブローカの実行中)。
-g	なし	グループ、グループ メンバ、ユーザ、およびトークンをダンプします。
-u	*login*	関連するデフォルト ログインに基づき、ユーザ レコードとトークンをダンプします。
-l	*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。

sdloadlog

sdloadlog ユーティリティでは、DOS コマンド ラインを使用して、ログ ダンプ ファイルをデータベースにロードできます。

次の表は、**sdloadlog** 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
-d	*database name*	データベースのファイル名を指定します。
-f	*filename*	ロード ファイルの名前を指定します。

sddumplog

sddumplog ユーティリティでは、DOS コマンド ラインを使用して、ログ データベースをダンプできます。

次の表は、**sddumplog** 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
-d	*dbname*	データベースのファイル名を指定します。
-f	*filename*	ロード ファイルの名前を指定します。

オプション	引数	説明
-m	なし	マルチユーザ モードでデータベースをダンプできます (データベース ブローカの実行中)。

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。

DOS コマンド プロンプト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、DOS コマンド プロンプトからのみ実行できます。

メモ: UNIX プラットフォーム バージョンのダンプリーダ 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 UNIX 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。

オプション	引数	説明
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。
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。このパラメータを指定しないと、出力は **stderr** (コンソール) に書き込まれます。パラメータが空で、二重引用符 (") で囲まれている場合は、**stdout** に出力されます。これも通常はコンソールです。
-c	なし	RSA Authentication Manger Administration 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です。これらのダンプ ファイルは、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。

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 のデータベース 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、70 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 Microsoft Excel のようなサードパーティ 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 フォルダには、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 フォルダには、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 (メモ帳など) 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) を理解していることが前提となります。

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、オンライン ヘルプと、『Administration Toolkit Reference Guide』を参照してください。

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
6.1	20.00.00
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。

メモ：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、65 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。また、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、出力ファイルに書き込めません。

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 SAM データベースからのユーザ レコードの作成

この付録では、Windows NT システムの既存の SAM (Security Accounts Manager) データベースから、Windows 2000 Server または Windows 2003 Server の RSA Authentication Manager データベースにユーザ情報を移動する際に使用する 2 つのユーティリティについて説明します。

ユーティリティ	目的
dumpsamusers.exe (Windows NT 専用)	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、カンマ区切りのテキスト ファイルに書き込みます。各レコードには、1 人のユーザのログイン名、ファースト ネーム、およびラスト ネームが含まれています。
loadsamusers.exe (Windows 2000 および Windows 2003 専用)	テキスト ファイルを読み込んで解析します。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 種類のデータを含むレコードを RSA Authentication Manager データベースに作成します。

転送処理を完全に自動化することはできません。Windows NT 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するので、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。

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 Windows 2000 または Windows 2003 コマンド プロンプトから実行します。このユーティリティでは RSA Authentication Manager Administration Toolkit の機能の一部を利用するので、**apidemon.exe** プログラムも格納されているディレクトリからこのユーティリティを起動する必要があります。また、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。

構文

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

引数

infile	入力ファイル、つまり **dumpsamusers** の出力ファイルを指定します。
-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。ログインの重複など、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。 **メモ：**この引数は大文字と小文字を区別します。

loadsamusers プログラムは、致命的なエラーを検出したとき、つまり、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、RSA Authentication Manager データベースにそのまま残ります。

F

RSA Authentication Manager のアンインストール

ソフトウェアをアンインストールする前に、すべての RSA Authentication Manager ファイルのバックアップを作成してください。RSA Authentication Manager データのバックアップの詳細については、『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 (Windows)」の章を参照してください。

RSA Authentication Manager をアンインストールするには

1. プライマリ サーバのすべての RSA Authentication Manager プロセスをシャットダウンします。操作手順については、14 ページの「RSA Authentication Manager プロセスの起動と停止」を参照してください。
2. [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。
3. インストールされているプログラムの一覧で [RSA Authentication Manager] を選択し、[削除] をクリックします。
4. [はい] をクリックします。
5. 画面の指示に従ってアンインストール プロセスを完了します。

用語集

Administration Toolkit
C または Tcl のカスタム アドミニストレーション アプリケーションの開発用ツールキット。Administration Toolkit (API Toolkit とも呼びます) には、RSA Authentication Manager データベースとの間で読み書きできる機能と実行ファイルが含まれています。

Configuration Management アプリケーション
プライマリまたはレプリカ上で、システム構成レコード ファイル **(sdconf.rec)** 内の情報を表示および編集するためのアプリケーション。ライセンス情報も表示されます。

license.rec
ライセンスの種類やライセンスに含まれるユーザ数など、サイト固有の情報が格納されているファイル。

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 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 Manager Host Mode
RSA Authentication Manager データベースを管理するためのアプリケーション。

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。

sdlog データベース
各認証要求の記録と、RSA Authentication Manager Host Mode アプリケーションを通じて実行された処理の記録が保存されるデータベース。ログ データベースとも呼びます。

sdserv データベース
システム パラメータ、トークン レコード、ユーザ レコード、およびエージェント ホスト情報を格納しているデータベース。サーバ データベースとも呼びます。

%SystemRoot%
Windows オペレーティング システムのルート ディレクトリ (**¥winnt** など)。

エージェント ホスト
RSA Authentication Agent ソフトウェアが動作しているコンピュータまたはその他のデバイス。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ます。エージェント ホストには、RSA Authentication Agent ソフトウェアが

動作しているデバイスに加えて、RSA Authentication Agent ソフトウェアが組み込まれているサードパーティ デバイス (コミュニケーション サーバ、ファイアウォール、ルータなど) も含まれます。

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 カードなど、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。

プライマリ

アドミニストレーションが行われる RSA Authentication Manager。プライマリはまた、データベースの変更をレプリカにレプリケートします。

レプリカ

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

レルム

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

索引