RSA SecurID for Microsoft Windows
プランニング ガイド 1.1

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 / またはその他の国における RSA Security Inc. の登録商標または商標です。本文中に記載されている製品名、およびサービス名は各社の商標あるいは登録商標です。

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。

本書は英語版マニュアル「RSA SecurID for Microsoft Windows Planning 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 11 月

P/N JS - AGT - 6002

目次

はじめに

本書 (「RSA SecurID for Microsoft Windows プランニング ガイド 1.1」) は、RSA SecurID for Microsoft Windows を社内で活用するための概要と基本構造を説明します。RSA SecurID for Microsoft Windows は、RSA Authentication Manager 6.1 と RSA Authentication Agent 6.1 for Microsoft Windows を組み合わせて、Windows セキュリティを、時間ベースの RSA SecurID トークンの強力な二要素認証で強化します。

対象となる読者

本書は、ネットワーク管理者およびセキュリティ管理者、システム インテグレータ、情報技術担当者を対象としています。本書を他のユーザには公開しないでください。

マニュアル

マニュアルおよび製品サポート情報、さらにマニュアルに記載されていない最新のテクニカル情報に関しては、*RSA Authentication Agent 6.1 for Microsoft Windows Readme* を参照してください。Readme ファイルは、**readme.html** というファイル名で RSA Authentication Agent 6.1 for Microsoft Windows .zip ファイルのルートディレクトリに存在します。

サポートおよびサービス

RSA SecurCare オンライン	**https://knowledge.rsasecurity.com**

1 イントロダクション

RSA SecurID for Microsoft Windows は、時間ベースの RSA SecurID トークンの二要素認証を使用して Windows セキュリティを強化するマルチ コンポーネント ソリューションです。このソリューションは、RSA Authentication Agent 6.1 for Microsoft Windows、RSA Authentication Agent 5.3 for Web、および RSA Authentication Manager 6.1 を連携して使用します。

このソリューションにおいて、RSA Authentication Agent 6.1 for Microsoft Windows は、ユーザに RSA SecurID パスコードの入力を要求します。それにより Windows デスクトップへの認証や保護されているドメイン リソースおよびドメイン クライアント コンピュータへのアクセスや、Microsoft ネットワークへのリモート接続の開始などが可能となります。

RSA Authentication Agent 5.3 for Web を使用している企業の場合、ユーザがその企業の Web リソースにアクセスするには、RSA SecurID パスコードによる認証が必要です。ユーザが保護されているリソースにアクセスしようとするか、またはリモート接続を開始しようとすると、Authentication Agent は、保護されているリソースへのアクセス リクエストを途中で捕らえて Microsoft Windows パスワードのプロンプトの代わりに、RSA SecurID パスコードの入力をユーザに促します。その際、システムの構成によっては、Microsoft Windows パスワードのプロンプトと RSA SecurID パスコードのプロンプトの両方が表示されることもあります。Authentication Agent は、ユーザのログイン情報を検証するために、RSA Authentication Manager に送信します。

RSA Authentication Manager は、ユーザ認証アカウントのリポジトリです。管理者は、ユーザ アカウントを手動で作成するか、あるいは既存の Active Directory や LDAP データベースからインポートすることができます。認証時に Authentication Manager が受け取ったログオン情報が、サーバ内のデータベースのユーザ レコードと一致すると、ユーザは認証を受けて保護されているリソースにアクセスすることができます。

本書は、RSA Authentication Agent 6.1 for Microsoft Windows を中心に説明します。RSA Authentication Agent 6.1 に関する詳細は、「RSA Authentication Manager 6.1 管理者ガイド」を参照してください。RSA Authentication Agent 5.3 for Web に関する詳細は、*「RSA Authentication Agent 5.3 for Web Installation and Configuration Guide」*を参照してください。

RSA SecurID for Microsoft Windows の特徴

セキュアなリソース保護

RSA SecurID for Microsoft Windows は、二要素認証を用いて Windows パスワード セキュリティを強化します。二要素認証は、特許を取得したタイム シンクロナイズ テクノロジおよびアルゴリズムであり、セキュアであることが長期にわたり証明されています。

RSA SecurID 認証はパスワードのみの保護よりも強力です。RSA SecurID 認証は、ユーザの所持物 (RSA SecurID トークンコード) とユーザが知っている情報 (RSA SecurID PIN) を組み合わせて使用するからです。ユーザが保護されているリソースにアクセスしようとすると、RSA Authentication Agent はそのユーザに RSA SecurID パスコードを要求し、検証するためにそれを RSA Authentication Manager に送信します。権限のあるユーザは保護されているリソースにアクセスすることができ、権限のないユーザはアクセスが拒否されます。

以下の表は、RSA Authentication Manager がどのリソースを保護するかを説明します。

保護されるリソース	説明
ローカル Windows デスクトップ	ローカル認証は、RSA SecurID パスコード (ユーザの PIN の後にトークンコードを連結したもの) の入力をユーザに要求して、ローカル Windows デスクトップに対してユーザを認証します。詳細は 15 ページの「ローカル認証」を参照してください。
ドメイン リソースとドメイン クライアント デスクトップ	ドメイン認証は、RSA SecurID パスコードの入力をドメイン ユーザに要求して、ドメイン クライアント コンピュータ上の Windows デスクトップと保護されているドメインのリソースへのアクセスに対してユーザを認証します。詳細は 16 ページの「ドメイン認証」を参照してください。
ネットワーク リソースへのリモート接続	リモート認証は、保護されているネットワークへリモート接続を開始する前に、RSA SecurID パスコードの入力をユーザに要求します。詳細は 16 ページの「リモート認証」を参照してください。
ネットワーク リソースへのリモート ワイヤレス接続	ワイヤレス認証は、保護されているネットワークへリモート接続を開始する前に、RSA SecurID パスコードの入力をユーザに要求します。詳細は 19 ページの「ワイヤレス認証」を参照してください。
一般的 Windows オペレーション	RSA Authentication Manager はターミナル サーバにログオンする際、一般的 Windows オペレーションに RSA SecurID プロテクションを追加します。そして、Windows の **net use** と **runas** コマンドを発行して、保護されたネットワークにドライバをマッピングします。詳細は、20 ページの「一般的 Windows オペレーションのための RSA SecurID 認証」を参照してください。

簡素化された認証プロセス

Windows パスワードの統合を設定すると、Microsoft Windows パスワードが RSA SecurID ログオン プロセスに組み込まれます。パスワードの統合方法にもよりますが、初回のオンライン認証 (オンライン接続で認証を受ける) でユーザが Windows ログオン パスワードを入力すると、次にパスワード入力を求めるのは、パスワード期限が切れるとき (たとえば、90 日後、あるいはセキュリティ ポリシに基づいた期間) とすることができます。それ以外の認証時には、ユーザは RSA SecurID パスコードのみを入力します。詳細は、21 ページの「Windows パスワードの統合」を参照してください。

オフライン認証機能により、RSA SecurID 認証は拡張されて、RSA Authentication Manager に接続できない状況でもコンピュータおよびドメイン リソースを保護する認証プロセスの一貫性が保たれるようになります。オンラインでもオフラインであっても、ユーザは同じ方法で認証されます。詳細は、22 ページの「オフライン認証」を参照してください。

認証要求オプションの指定

管理者は、どのユーザに対し RSA SecurID パスコードの入力要求するかを指定することで、Windows リソースの保護される程度を決定します。管理者は RSA Authentication Agent による認証要求を構成できます。

- すべてのユーザ
- あるグループのユーザ
- 指定されたグループのメンバーを除くすべてのユーザ

RSA Authentication Agent はデフォルトの Windows グループ (たとえば、ドメイン ユーザまたはダイヤルイン ユーザ) 、あるいは Windows コンピュータ管理インターフェイスで管理者自身が作成したグループを使用することができます。

詳細は、20 ページの「認証要求の対象にするユーザの選定計画」を参照してください。

RSA RADIUS Server

RSA SecurID for Microsoft Windows ソリューションは RSA RADIUS Server を包含しています。RADIUS サーバは、RSA EAP Protected One Time Password (OTP) (EAP 32) をサポートする RSA Authentication Manager と一緒に出荷されています。また、RSA RADIUS Server は RSA Security EAP (EAP 15) を継続的にサポートします。

リモート認証ソリューションに RSA RADIUS Server を組み入れると、リモート サーバは RSA Authentication Manager を必要としなくなります。詳細は 16 ページの「リモート認証」を参照してください。

複数のトークンタイプのサポート

RSA Authentication Agent 6.1 for Microsoft Windows は以下の認証機器タイプをサポートします。

- RSA SecurID キーホルダ
- RSA SecurID スタンダード カード
- RSA SecurID PIN パッド
- RSA SecurID ソフトウェア トークン
- RSA SecurID Authenticator SID800

注記 : RSA SecurID ソフトウェア トークンを使用すると、ユーザは RSA SecurID PIN だけでネットワークにログオンできるため、他のタイプのトークンを使用する場合と比べてセキュリティ レベルが低くなります。
他の認証機器タイプは、ユーザに PIN とパスコードの入力を要求するか、RSA SecurID Authenticator SID800 を使用して物理的に認証機器をコンピュータに接続し次に PIN を入力する、のどちらかを要求します。さらに、ソフトウェアトークンがコンピュータに保存されるため、ユーザがコンピュータの前から離れる際、自分のトークンを削除することはできません。
トークンがインストールされるコンピュータのデスクトップに、ソフトウェア トークンを使用してログオンすることはできませんが、デスクトップにログオン後は (たとえば、保護されたドメインリソースに認証する)、それらのソフトウェア トークンを使用することはできます。

使いやすくなった各種機能

以下の機能おける RSA Authentication Agent 6.1 for Microsoft Windows の使いやすさを説明します。

RSA Security Center。RSA Authentication Agent 6.1 for Microsoft Windows は管理者およびユーザ用のグラフィカル ユーザ インターフェイスとして RSA Security Center を装備しています。

他の主な RSA Security 製品との統合。RSA Authentication Agent は RSA Authenticator Utility など他の主な RSA Security 製品と統合されます。これらの製品を一緒にインストールすることにより、RSA SecurID 認証に RSA SecurID Authenticator SID800 の使用が可能となります。RSA Authentication Agent と RSA Authenticator Utility は、グラフィカル ユーザ インターフェイス (RSA Security Center) を共有します。

PIN だけのアンロック。RSA Authentication Agent では、ユーザが完全なパスコードに代わり PIN だけで保護されているコンピュータ上のワークステーションに、アンロックできる構成オプションを装備しています。管理者として、この機能を有効および無効にできます。また、この機能のタイムアウト期間も設定できます。タイムアウト期間の終了後に、ユーザは完全なパスコードを入力してワークステーションをアンロックする必要があります。管理者は RSA Security Center (Authentication Agent のための構成インタフェース) で機能を構成し、タイムアウト期間を設定します。詳細は、ヘルプ トピック「Windows ログオン設定とは」を参照してください。

一般的 Windows オペレーションの RSA SecurID 認証。RSA Authentication Agent は Windows **net use** と **runas** コマンドに RSA SecurID 認証を追加します。さらに、Authentication Agent はユーティリティ **RSA Net Use** と **RSA RunAS** を含んでいます。これらのユーティリティは、Windows **net use** または **runas** ユーティリティをエミュレートしますが、より簡単な RSA SecurID 認証プロセスを提供します。

カスタマイズ オプション

以下の方法で RSA Authentication Agent 6.1 for Microsoft Windows をカスタマイズできます。

- ログオン プロンプトで「 your own company branding」を使用します。
- ログオン プロンプトでパスワードかパスコードのどちらを要求するか、を指定します。

詳細は、「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「RSA Authentication Manager 6.1 for Microsoft Windows をカスタマイズする」の章を参照してください。

エマージェンシー アクセス

RSA Authentication Agent 6.1 for Microsoft Windows では各種のエマージェンシー アクセス方法を提供します。使用するアクセス方法は、状況よって異なります。日常で起こりえる状況と、各状況に適用される方法を以下の表に示します。

状況	エマージェンシー アクセス方法
オンライン ユーザのトークンの紛失	• 固定パスワード • ワンタイム パスワード
オフライン ユーザのトークンの紛失	オフライン エマージェンシー トークン コード

状況	エマージェンシー アクセス方法
オンライン ユーザの PIN の失念	管理者ヘルプ デスクによる PIN のリセット
オフライン ユーザの PIN の失念	オフライン エマージェンシー パスコード
オフライン コンピュータへの管理アクセス	• 管理者アカウントの免除 • 予約パスワード

詳細は、23 ページの「エマージェンシー アクセスの計画」を参照してください。

ログの一元化

RSA Authentication Agent 6.1 for Microsoft Windows は、RSA Authentication Manager データベースにすべての認証イベントを集約して記録します。オフライン認証により生成された認証イベントは、ローカル コンピュータに一時的に記録されます。オフライン ユーザがオンラインになったときに、オフライン認証レコードを RSA Authentication Manager データベースのセントラル ログに転送するように RSA Authentication Manager を構成することが推奨されています。

容易な配布

管理者は、クライアント コンピュータへの配布用に構成した Microsoft Installer (.msi) インストール パッケージを作成することで、RSA Authentication Agent 6.1 for Microsoft Windows を効率良くクライアント コンピュータに配信することができます。たとえば、管理者は、自分が選択した認証ソリューションに応じて、保護されている環境のすべてのクライアント コンピュータに、RSA Authentication Agent のコンポーネントをインストールしなければなりません。インストール パッケージを作成すると、この作業の負荷が減少します。詳細は、58 ページの「インストール手法の計画」を参照してください。

サポートするプラットフォームとシステム要件

RSA Authentication Agent 6.1 for Microsoft Windows

RSA Authentication Agent 6.1 for Microsoft Windows は以下のプラットフォームをサポートします。

サーバ	クライアント	ターミナル サーバ
• Windows Server 2003 Standard • Windows Server 2003 SBS • Windows 2000 Professional • Windows 2000 Server	• Windows Server 2003 Standard • Windows 2003 Server SBS • Windows 2000 Professional • Windows 2000 Server • Windows XP Professional SP2 • Windows XP Tablet SP2	• Windows Terminal Server • Citrix MetaFrame XPs

RSA Authentication Agent 6.1 for Microsoft Windows を正常にインストールするには、使用するシステムが以下の要件を満たす必要があります。また、リソースの使用状況にもよりますが、システム リソースを増強するとパフォーマンスが改善されることがあります。

- 733 MHz 以上の Pentium プロセッサ
- 256 MB の RAM
- 50 MB の空きディスク スペース
- TCP/IP ネットワーキング

その他の要件は、「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「システム要件と準備」を参照してください。

RSA Authentication Agent 5.3 for Web

サポートするプラットフォーム

RSA Authentication Agent 5.3 for Web は、以下のプラットフォームで稼動するには制限があります。

- IIS (Internet Information Services) 6.0 をインストールした Windows Server 2003、Standard and Enterprise Editions
- Service Pack 4 および IIS (Internet Information Services) 5.0 をインストールした Windows 2000 Server

メモ：コンピュータが、RSA Authentication Manager のプライマリやレプリカとなることはありません。同じコンピュータで IIS と RSA Authentication Manager の両方を実行すると、パフォーマンスは減少するかもしれません。

ホスト システム要件

システムは以下の要件を最低限満たす必要があります。

- Intel Pentium 以上
- 32 MB の RAM
- 10 MB の空きディスク スペース
- TCP/IP ネットワーキング
- Web サーバ ディレクトリを含むディスク パーティションは NTFS パーティションでなければなりません。FAT ファイル システムはサポートされません。
- SSL (Secure Sockets Layer) 証明書

  (たとえばベリサインのような) 認証局から SSL 証明書を入手する方法に関する情報は、下記のベリサイン Web サイトを参照してください。**http://www.verisign.com**.
- ユーザ アクセスがプロキシ サーバを経由して Web ページを保護した場合、プロキシは cookies の通過をサポートしなければなりません。

クライアント システム要件

ブラウザ サポート。保護されている Web ページにアクセスするには、ユーザは次のいずれかの Web ブラウザをコンピュータにインストールします。

- Microsoft Internet Explorer 5.5 または 6.0

- Netscape Navigator 7.2

メモ：機密保護目的のため、ブラウザのキャッシングを無効にするようユーザに指示してください。

ワイヤレス サポート。ワイヤレス アクセス プロトコル経由の RSA SecurID Web 認証は、WAP 1.1 および 1.2.1 仕様で対応している以下の機能が必要になります。

- cookies のキャッシング
- WML Document Type Definition (DTD) バージョン 1.1

RSA SecurID ユーザは、cookie を受け入れるようにブラウザを設定しておく必要があります。さらに、ユーザは、フォームの利用、および Persistent Client State HTTP Cookie が利用できる Web ブラウザを使用する必要があります。

Microsoft Exchange Server ActiveSync のサポート。RSA Authentication Agent 5.3 for Web は Microsoft Exchange Server 2003 ActiveSync 上で稼動するには制限があります。

追加のシステム要求

RSA Authentication Agent 5.3 for Web は、RSA Authentication Manager （以前の RSA ACE/Server）5.2 以降と関連して作動します。Web エージェント管理者は RSA Authentication Manager システムとその各機能に精通している必要があります。

また、RSA Authentication Manager 管理者は Authentication Manager データベースにユーザを登録し、かつトークンが送信されたことを確認してください。

メモ：マルチホーム サーバのファイルを保護するために、Web エージェント ソフトウェアを使用する場合、RSA Authentication Manager データベースの付加的 IP アドレスを考慮する必要があります。RSA Authentication Manager 管理者は、Authentication Agent ホストで使用する各追加 IP アドレスに対してセカンダリ ノードを定義しなければなりません。また、IP アドレスのオーバライドを指定する必要があります。RSA ACE/Agent for Windows 6.0 以前を使用している場合、RSA Authentication Agent コントロール パネルの［**高度な設定**］タブのオーバライドを指定します。RSA Authentication Agent 6.1 for Microsoft Windows を使用している場合、RSA Security Center の ［高度な 設定］ページのオーバライドを指定します。オーバライド アドレスはサーバ データベースの Authentication Agent ホストに指定されたネットワーク アドレスと一致する必要があります。セカンダリ ノードの定義方法に関する説明は、RSA Authentication Manager のマニュアルを参照してください。

詳細は、「RSA Authentication Agent 5.3 for Web Installation and Configuration Guide」を参照してください。

RSA Authentication Manager 6.1

サポートするプラットホーム

RSA Authentication Manager 6.1 は、以下のプラットフォームで稼動するには制限があります。

- サポートする言語に対応している Microsoft Windows 2000 Server もしくは Advanced Server (Service Pack 4)
- サポートする言語に対応している Microsoft Windows 2003 Enterprise Server

- サポートする言語に対応している Microsoft Windows 2003 Standard Server

サポートする言語に関する情報は、「RSA Authentication Manager 6.1 管理者 ガイド」を参照してください。

ハードウェア要件

RSA Authentication Manager 6.1 を正常にインストールするには、使用するシステムが以下の要件を最低限満たす必要があります。

- Intel Pentium 266 MHz プロセッサ以上 (Windows 2000 Server)
- Intel Pentium 733 MHz プロセッサ以上 (Windows 2003 Server、Standard もしくは Enterprise Edition)
- 物理メモリ 256 MB 以上、さらに 1,000 ユーザごとに 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 ドライブ
- NTFS ファイル システム
- 解像度 800 x 600 ピクセル以上を表示できるモニタ ディスプレイ

可能な最高認証レートを実現するには、以下の要件を満たす必要があります。

- Dual Intel Pentium 4 (3.2 GHz 以上の) プロセッサ
- プロセッサあたり 2048 MB の物理メモリ

ディスク スペース要件

使用するシステムが以下の要件を最低限満たす必要があります。

- RSA Authentication Manager ソフトウェア用に 200 MB
- 1,000 ユーザごとに 2 MB の追加ディスク スペース
- RSA Authentication Manager Remote Administration ソフトウェア用に 20 MB
- RSA Authentication Agent for Windows 用に 5 MB

ディスク スペース要件に関する詳細は、「RSA Authentication Manager 6.1 for Windows インストール ガイド」の「データベース メンテナンス」を参照してください。

2 論理的な配置計画

論理的な配置とは、ユーザのビジネス環境においてソフトウェアをどのように使用するかということです。ソフトウェアをインストールする前に配置を論理的に計画することで、企業のニーズに適した実装を円滑に行うことができます。たとえば、管理者は以下の内容を決定する必要があります。

- 配置する認証ソリューション
- 使用するエマージェンシー アクセスの方法
- ユーザ認証のプロセス (たとえば、オンライン / オフラインに関わらずユーザ認証方法は同じにする、または、ユーザにパスワードと RSA SecurID パスコードの両方を入力させる、それとも RSA SecurID パスコードのみを入力させる、などを決定します)

本章では、これらの課題とその他の重要な課題について説明します。

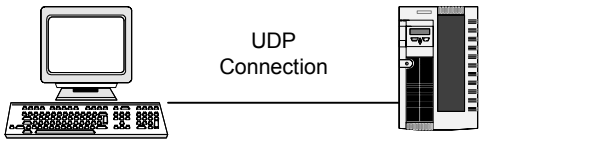
配置する認証ソリューションの選択に関する計画

管理者は、単一の認証ソリューションを配置することも、または複数のソリューションを組み合わせて配置することもできます。配置する認証ソリューションは、どのリソースを保護するかに基づきます。

このセクションでは、各認証ソリューションを総括します。

ローカル認証

ローカル認証コンポーネントは、RSA SecurID パスコードの入力をユーザに要求して、Windows デスクトップへの認証を行います。以下の図は、ローカル認証プロセスを示しています。



User's Computer

Component:
Local Authentication Client

RSA Authentication Manager

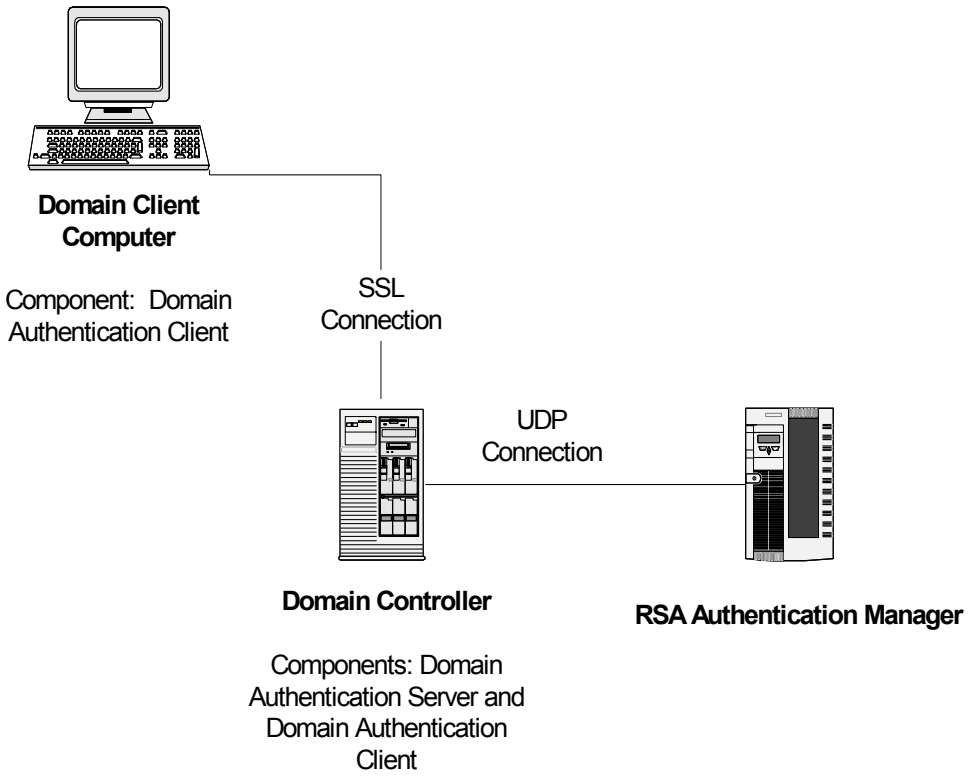
詳細は、41 ページの「ローカル認証を配置する」を参照してください。

ドメイン認証

ドメイン認証コンポーネントは、ドメイン アカウントを使用してるドメイン クライアントコンピュータやドメイン リソースへのアクセスを認証するため、RSA SecurID パスコードの入力をユーザに要求します。RSA Authentication Agent は、ユーザが以下のアクティビティのいずれかを実行する際に、有効な RSA SecurID パスコードの入力プロンプトを表示します。

- ドメインへのログオン
- ドメインのネットワーク ドライブをマウントする
- Windows **net use** または **runas** コマンドで保護されているドメインにアクセスする

以下の図は、ドメイン認証のプロセスを示しています。



詳細は、43 ページの「ドメイン認証を配置する」を参照してください。

リモート認証

リモート認証コンポーネントは、ユーザが VPN クライアントやポストダイヤル ターミナル ウィンドウを使ってネットワークへリモート接続を開始する前に、RSA SecurID パスコードの入力をユーザに要求して認証を行います。

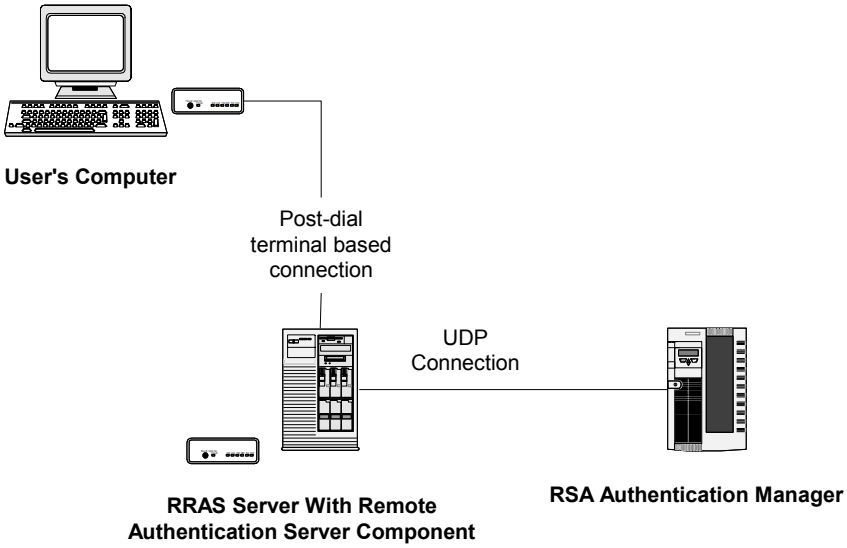
以下の環境タイプにおいてリモート認証が配置できます。

- Non-EAP
- EAP
  - RADIUS サーバを使用しない
  - RADIUS サーバを使用する

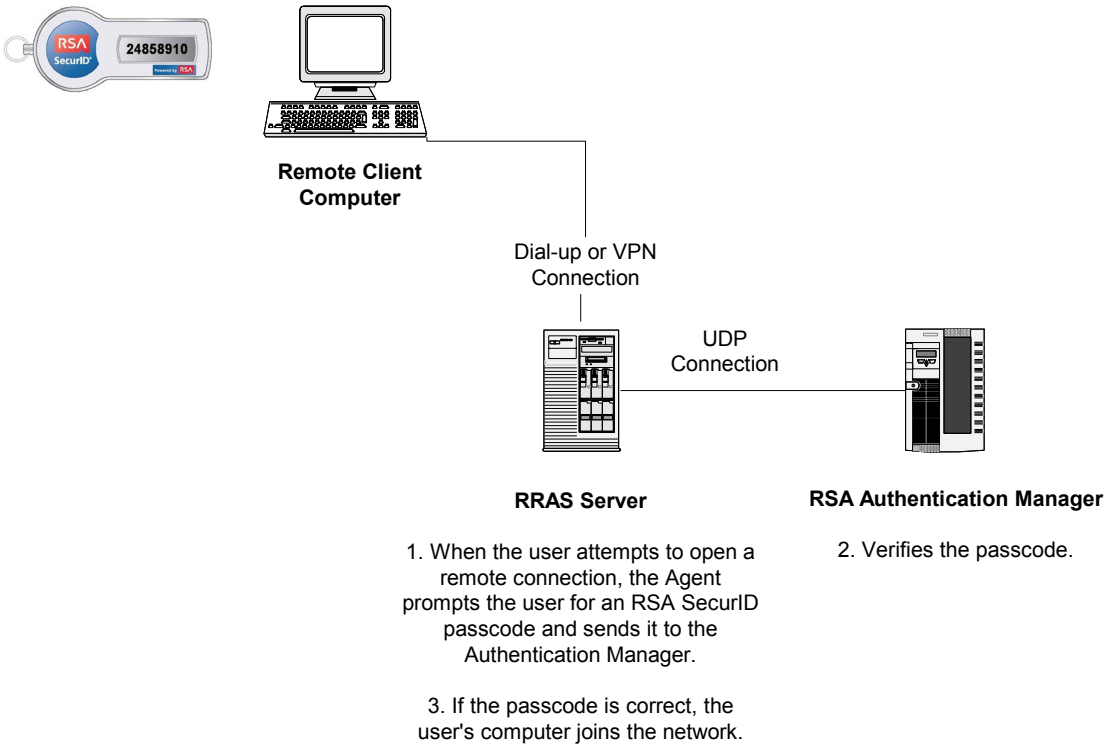
- ワイヤレス PEAP

以下の図は、各環境タイプにおける認証プロセスを示しています。

EAP を使用しないリモート認証

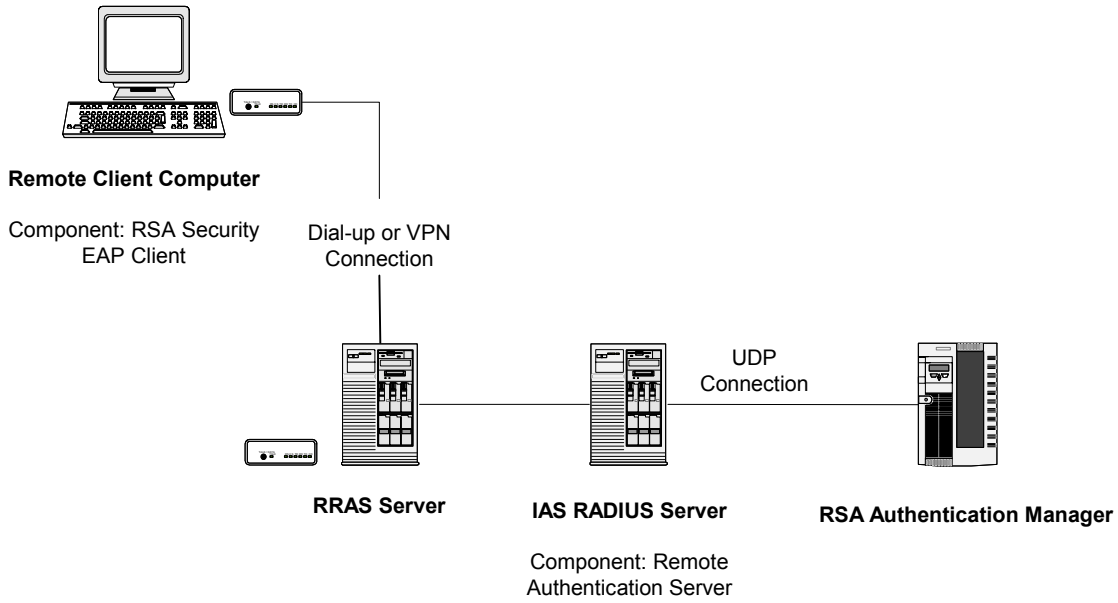


RADIUS サーバを使用しない EAP を使ったリモート認証



RADIUS サーバを使用する EAP を使ったリモート認証

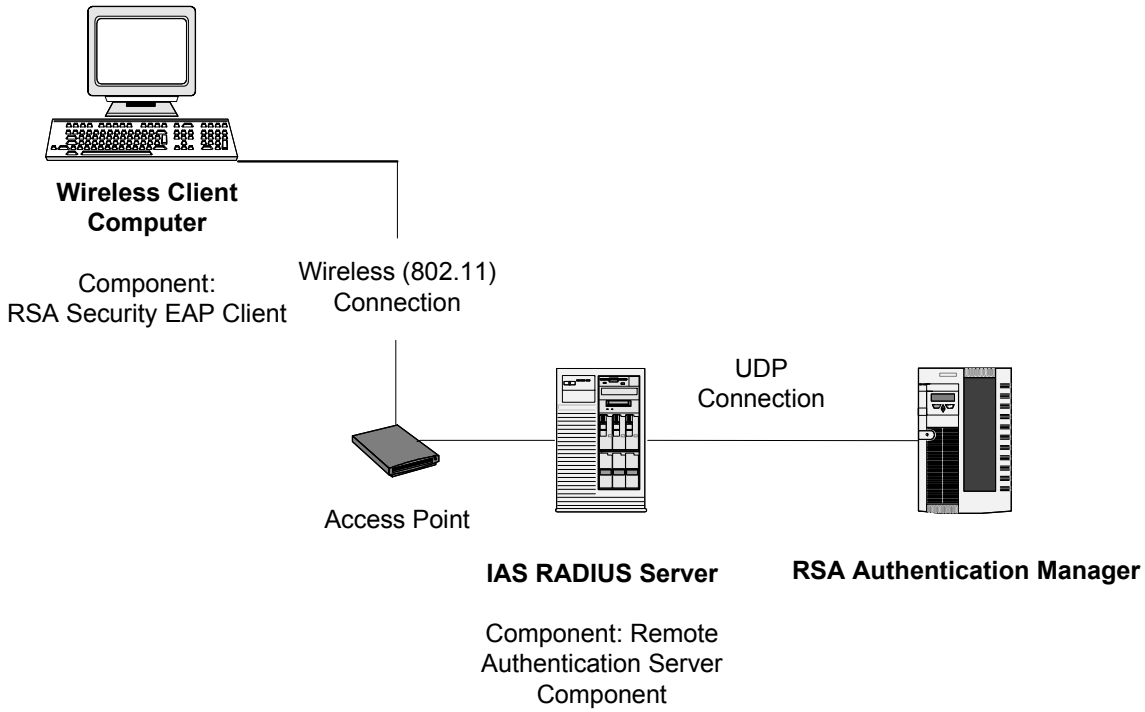
認証プロセスを図解するため、RADIUS サーバおよび RSA Authentication Manager は別々のコンピュータで表示します。実際の環境では、1 台のコンピュータに両方をインストールできます。また、Microsoft IAS RADIUS Server か RSA RADIUS Server のどちらかを使用できます。RSA RADIUS Server は RSA Authentication Manager 6.1 と一緒に出荷されます。Microsoft IAS RADIUS Server と RSA RADIUS Server の詳しい情報は、45 ページの「リモート認証を配置する」を参照してください。



ワイヤレス認証

ワイヤレス認証は、企業ネットワークへのワイヤレス接続を開始する前に、RSA SecurID パスコードの入力をユーザに要求して認証を行います。

以下の図は、ワイヤレス認証プロセスを示しています。認証プロセスを図解するため、RADIUS サーバ、および RSA Authentication Manager は別々のコンピュータで表示します。実際の環境では、1 台のコンピュータに両方をインストールできます。また、Microsoft IAS RADIUS Server か RSA RADIUS Server のどちらか、あるいは両方を組合せて使用できます。RSA RADIUS Server は RSA Authentication Manager 6.1 と一緒に出荷されます。



以下のどちらかを使用してワイヤレス認証を配置できます。

- RSA EAP - Protected OTP
- PEAP

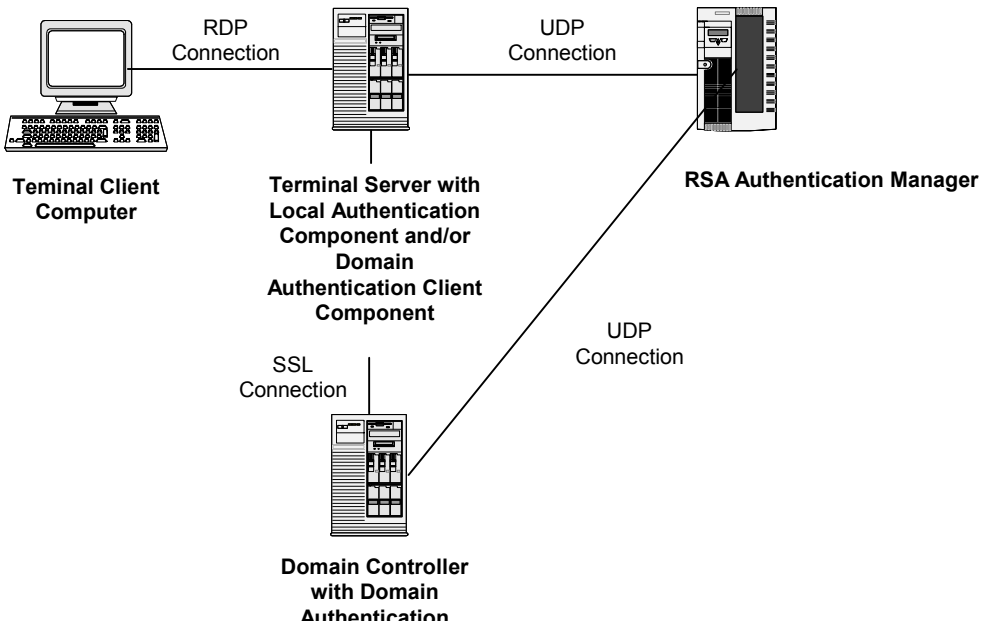
RSA EAP - Protected OTP を使用することにより、PEAP や TTLS と同様に、認証証明書や追加トンネリングが不要となります。

詳しい情報は、53 ページの「ワイヤレス認証を配置する」を参照してください。

一般的 Windows オペレーションのための RSA SecurID 認証

一般的 Windows オペレーションのための RSA SecurID 認証では、ユーザへの RSA SecurID パスコードの入力要求により、保護されているネットワークへのドライブマップや、ターミナルサーバへの認証、代替ユーザとして保護されたネットワークへの認証などを行います。

以下の図は、ターミナルサーバからネットワークにアクセスするための認証プロセスを示しています。



認証要求の対象にするユーザの選定計画

管理者は、どのユーザに RSA SecurID パスコードの入力要求するかを指定することで、Windows リソースが保護される程度を決定します。
管理者は、RSA Authentication Agent による認証要求を構成できます。

- すべてのユーザ
- あるグループのユーザ
- 指定されたグループのメンバーを除くすべてのユーザ

RSA Authentication Agent は、デフォルトの Windows グループ (たとえば、ドメイン ユーザまたはダイヤルインユーザ) 、あるいは Windows コンピュータ管理インターフェイスで管理者が作成したグループを使用することができます。

デフォルトの Windows グループ以外のグループを使用する場合、RSA Authentication Agent を構成する前にそれらのグループを作成する必要があります。グループの作成方法は、Windows のドキュメントを参照してください。認証要求をどのユーザに行うかを指定する方法は、ヘルプ トピック「RSA SecurID で認証要求するユーザおよびグループを指定する」を参照してください。

ユーザ認証の計画

Windows パスワードの統合

Windows パスワードの統合を設定すると、Microsoft Windows パスワードが RSA SecurID ログオン プロセスに組み込まれます。Windows パスワードはユーザの認証データと一緒に RSA Authentication Manager データベースに格納されます。また、オフライン認証のため、オフライン データにも格納されます。

パスワード統合を使用する方法の 1 つは、初回のオンライン認証 (オンライン接続で認証を受ける) の際、ユーザに Windows ログオン パスワードの入力要求し、ユーザのパスワード期限切れるときに (たとえば、90 日後、あるいはセキュリティポリシーに基づいた期間)、再度パスワードの入力を要求します。ユーザが新しいパスワードを作成すると、RSA Authentication Manager はそのパスワードを取得して、RSA Authentication Manager データベース内のユーザ レコードにパスワードを格納します。以降の認証では、ユーザは RSA SecurID パスコードのみを入力します。RSA Authentication Agent は、RSA Authentication Manager から Windows パスワードを取得して、それを Windows ログオン プロセスに送信するので、ユーザはパスワードを入力する必要がありません。パスワードが期限切れとなる場合、ユーザはシステムから新しいパスワードを作成するプロンプトを受信します。通常、新しいパスワードを作成するためには、再度古いパスワードを入力しなければなりませんが、パスワード期限満了プロンプトでは自動的に期限切れパスワードを記入します。そのため、最初のパスワード入力後、ユーザは初回のパスワードを覚えておく必要はありません。

もう 1 つの統合方法としては、ドメイン環境の場合、Windows ログオン パスワードを含む認証を初めてユーザが行ったときに、管理者は Active Directory に格納されているそのユーザのパスワードを長く、複雑なものに変更できます。Active Directory は、パスワードの変更をドメイン コントローラに通知します。RSA Authentication Manager は、ドメイン コントローラから新しいパスワードを取得して、それを RSA Authentication Manager データベースのユーザアカウントに格納します。そのユーザの次回の認証時に、RSA Authentication Agent は、Windows パスワードを RSA Authentication Manager から取得して、それを Windows ログオン プロセスに送信します。ユーザは新しいパスワードを見ることはありませんので、パスワードを覚えたり、パスワードを書き留めたりする必要はありません。企業のセキュリティ ポリシーにより定期的にパスワードの変更が必要である場合、ユーザが新しいパスワードを要求されるときには、期限切れのパスワードは RSA Authentication Agent が提示します。ユーザが期限切れのパスワードを入力する必要はありません。その結果、パスワードの統合は、ヘルプデスクへの問い合わせ数の減少、およびパスワードの失念や危殆化による生産性の低下を軽減し、管理コストの削減につながります

詳しい説明は、「RSA Autehtication Agent 6.1 インストレーション& アドミニストレーション ガイド」第 1 章「概要」の「Windows パスワードの統合」のセクションを参照してください。

オフライン認証

オフライン認証は、RSA Authentication Manager に接続できない状況でも、保護されたコンピュータおよびドメイン リソースに RSA SecurID 認証を拡張する認証プロセスです。オンラインでもオフラインであっても、ユーザは同じ方法で認証されます。

オフライン認証を有効にすると、RSA Authentication Agent が RSA Authentication Manager と接続したときに、Authentication Manager がオフラインデータを生成し、それを Authentication Agent コンピュータにダウンロードします。Authentication Agent コンピュータは、RSA Authentication Manager への次回のオンライン接続時に、オフライン データの受信を開始します。たとえば、41 ページの「ローカル認証を配置する」で説明されている認証テストを実行した場合、Authentication Manager への認証を行いますが、2 回実行して Authentication Manager への認証に成功すると、Authentication Manager はオフラインデータを生成し、ダウンロードします。ローカルユーザ認証がオフラインで行われる場合、Authentication Agent は、ユーザのコンピュータに格納されているオフラインデータを照会して、ユーザの認証情報を検証します。ユーザの認証情報が正しければ、ユーザは保護されているリソースへのアクセスが許可されます。

ドメイン認証で保護されているコンピュータへのオフライン認証を有効にする場合も、同じプロセスで行われます。ドメインコントローラは、RSA Authentication Manager への 2 度目のオンライン認証が行われたときに、オフラインデータの受信を開始します。ユーザがドメイン認証サーバホスト上でオンライン認証に 2 回成功すると、ドメイン認証クライアントは、RSA Authentication Manager への最初のオンライン認証時に、オフライン データの受信を開始します。これ以降、RSA Authentication Manager とドメイン コントローラ間で接続できない状況でも、ドメイン ユーザは、ドメインへアクセスの認証を行うことができます。さらに、ドメインユーザは、ドメイン クライアントとドメイン コントローラが接続できない状況でも、ドメイン アカウントを使用してローカル デスクトップへのアクセス認証を行うことも可能です。

オフライン認証の構成とその有効 / 無効の切り替えは、RSA Authentication Manager Database Administration Application を使用します。システム全体のオフライン認証の構成とその有効 / 無効の切り替えは、個々のエージェント単位やユーザのグループ単位で設定することができます。Authentication Manager がシステム全体もしくはグループのユーザに対して生成するオフライン データの量を指定することができます。たとえば、営業グループのために RSA Authentication Manager の生成するオフライン日数を 7 日間と構成した場合、営業グループのすべてのオフラインユーザは 7 日間のオフライン日数を得ることになります。

詳しい説明は、「RSA Authetication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「オフライン認証」の章を参照してください。さらに、*「RSA Authentication Manager 6.1 管理者ガイド」*の「エージェントとエージェントホスト上でのアクティブ化」の章で「オフライン認証と Windows パスワード統合のセットアップ」を参照してください。

エマージェンシー アクセスの計画

エマージェンシー アクセスにより、トークンの紛失、PIN の失念や、オフライン日数を使い果たした、といういずれの場合でも、ユーザや管理者が保護されているリソースにアクセスすることができます。以下の表は、エマージェンシー アクセス方法の説明と、各方法の説明が記載されている箇所を示しています。

オンラインユーザを対象

エマージェンシー アクセス方法	説明	使用できるソリューション	特徴	説明の記載箇所
ワンタイム パスワード	保護されている自分のコンピュータへのアクセスを、(トークンコードの紛失時などに) トークンコードなしでユーザに許可する	• ローカル • ドメイン	• RSA Authentication Manager によって生成されます • 1 回の認証のみ有効です • ユーザの RSA SecurID PIN と組み合わせて使用する必要があります	*「RSA Authentication Manager 6.1 管理者ガイド」* の章「認証のためのユーザの登録」の「紛失トークンをテンポラリパスワードで代替する」を参照してください。
固定パスワード	保護されている各自のコンピュータへのアクセスを、(トークンコードの紛失時などに) トークンコードなしでユーザに許可する	• ローカル • ドメイン	• RSA Authentication Manager 管理者が作成します • そのユーザの「lost token status」が変更されるまで有効です • オフラインユーザのオフラインエマージェンシートークンコードと同様の機能を持たせることができます (たとえば、トークンを無くしたユーザが、オンラインとオフラインの両方で機能する同一パスワードを使用することが可能です) • ユーザの RSA SecurID PIN と組み合わせて使用する必要があります	「RSA Authentication Manager 6.1 管理者ガイド」の章「認証のためのユーザの登録」の「紛失トークンをテンポラリパスワードで代替する」を参照してください。

オンラインユーザを対象

エマージェンシーアクセス方法	説明	使用できるソリューション	特徴	説明の記載箇所
オフラインエマージェンシートークンコード	保護されている自分のコンピュータへのアクセスを、(トークンコードの紛失時などに) トークンコードなしでユーザに許可する	• ローカル • ドメイン	• ユーザの RSA SecurID PIN と組み合わせて使用する必要があります • ユーザの次回のオンライン認証時に変更します • 指定した期限で期限が切れます • オンラインユーザの固定パスワードと同様の機能を持たせることができます (たとえば、トークンを紛失したユーザが、オンラインとオフラインの両方で機能する同一パスワードを使用することができます)	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「概要」の章の「エマージェンシー アクセス」を参照してください。
オフラインエマージェンシーパスコード	保護されている各自のコンピュータへのアクセスを、PIN またはトークンコードなしてユーザに許可する (たとえば、ユーザが PIN を失念した、PIN が危殆化した、またはオフライン日数を使い果たしたときなどに使用できます)	• ローカル • ドメイン	• New PIN が必要です • ユーザの次回のオンライン認証時に変更します • 指定した期限で期限が切れます	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「概要」の章の「エマージェンシー アクセス」を参照してください。

管理者を対象				
エマージェンシーアクセス方法	**説明**	**使用できるソリューション**	**特徴**	**説明の記載箇所**
予約パスワード	管理者は、パスコードの入力無しで、ユーザのコンピュータをそのユーザ本人として認証することができるようになります	ローカル	• 各エージェントホスト上で管理者が設定します • 使用期限はありません	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「ローカル認証を構成する」の章の「予約パスワードを設定する」を参照してください。
管理者アカウントの免除	管理者が、保護されているコンピュータへの認証時に、パスワードのみの入力で済むようになります	• ローカル • ドメイン	• エージェントをインストールするときに、インストールを実行している管理者に対して作成されます • 各エージェントホストに対して作成されます • Window パスワードセキュリティのみで保護されます • ユーザ名ではなく、Well-Known Security Identifier (SID) によるアカウントで識別されます	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の「概要」の章の「管理者アカウントの免除」を参照してください。

RSA Authentication Manager データベースの準備

管理者は、RSA SecurID パスコード入力を要求するすべてのユーザを、RSA SecurID ユーザとして RSA Authentication Manager データベースに登録する必要があります。管理者は、RSA Authentication Manager データベースにユーザ レコードを手動で追加するか、あるいは既存の Active Directory や LDAP データベースを使用することができます。ユーザ レコードをインポートするには、RSA Authentication Manager データベースに登録するユーザ名が、Active Directory データベース内のユーザ名と一致する必要があります。詳細は、*「RSA Authentication Manager 6.1 管理者ガイド」*の「認証のためのユーザ登録」の章の「LDAP ユーザ データのインポート」を参照してください。

ユーザ レコードのインポートに使用できる既存のデータベースが無い場合は、RSA SecurID Web Express を使用してレコードを迅速に登録することができます。RSA SecurID Web Express を使用すると、ユーザ自身の要求によりユーザ トークンをアクティブ化ができるようになり、Authentication Manager データベースへのユーザ レコードの追加処理が自動で行われます。このとき、ユーザは自分のアカウントも Authentication Manager データベースに新規に作成します。詳細は、RSA SecurID Web Express ソフトウェアに同梱されている *「RSA SecurID Web Express Planning Guide」*を参照してください。また、RSA Authentication Manager ソフトウェアに同梱されている *「RSA Authentication Manager 6.1 Deployment Guide」*も参照してください。このガイドでは、RSA SecurID 認証デバイスの配置に関するガイドラインが説明されています。

Windows パスワードの統合を使用する場合は、RSA Authentication Manager データベースに登録するユーザ名を、Windows ユーザ名と一致させる必要があります。

ユーザを準備する

RSA Authentication Manager データベースにユーザを追加して、有効なトークンを配置した後、管理者はユーザに認証の手続きとユーザ トークンの使い方を説明する必要があります。
情報に関しては以下を参照してください。

- 「RSA Authentication Manager 6.1 Deployment Guide」の「Planning Communication With End Users」
- 「Authenticating with an RSA SecurID Token」

これらのガイドは、RSA Authentication Manager ソフトウェアに同梱されています。

ヘルプデスク管理者を用意する

ユーザは、ヘルプデスク管理者に連絡して、エマージェンシー アクセスコードやトークン紛失時パスワードを入手します。したがって、管理者は、認証処理および エマージェンシー アクセス方法について、ヘルプデスク管理者の教育計画を考える必要があります。
詳細は、「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の付録 E の「ユーザへの説明事項」を参照してください。また、RSA Authentication Manager ソフトウェアに同梱されている「RSA Authentication Manager 6.1 管理者 ガイド」および「RSA SecurID トークンによる認証」を参照してください。

3 論理配置サンプル シナリオ

この章では RSA SecurID for Microsoft Windows の配置に関する実用的なシナリオを提示します。各シナリオでは、Windows 環境においてビジネス ニーズを満たすソフトウェアの使い方が提示されます。シナリオは、従業員 50 人の小規模企業と従業員 2,000 人の中規模企業を例にしたものです。

シナリオ 1: 小規模の企業

従業員 50 人の企業を管理すると想定します。企業の待遇として、全従業員は週に一日自宅で作業します。従業員の一部は、出張中に作業することもあります。従業員がオフィスから離れた場所で作業するときは、ネットワークからオフラインになります。従業員は、オフィスから離れた場所で作業するために、ファイルをネットワークからラップトップにコピーします。オフィスから離れているときには、従業員は、Microsoft Outlook Web Access を使用して仕事用の電子メール アカウントをチェックします。

オフィスでは、従業員は企業ドメインへログオンします。従業員は、ユーザ名と Microsoft Windows パスワードを入力してログオンします。企業ポリシにより、従業員は、パスワードを 90 日ごとに変更する必要があります。従業員の大半は、簡単に思い出せる (したがって、誰でも簡単に推測できる) パスワードを使用しています。従業員の中にはパスワードだけではなく、どれがセキュリティを満たさないか、または会社によって確立されたコンプライアンス ポリシを書き留める人もいます。

従業員は、自分のコンピュータへのソフトウェアのインストールに関与していません。これらの作業は管理者が行います。

以下の表は、この企業の必要性 (ニーズ) と RSA SecurID for Microsoft Windows が提供する事項を示しています。

企業の必要性	RSA SecurID for Microsoft Windows が提供する事項
ドメイン リソースを保護する、セキュアで信頼できる手法	• ドメインリソー スへの RSA SecurID 二要素保護 • RSA Authentication Manager への接続不能の場合でも、ドメイン リソースへの RSA SecurID 二要素保護を拡張する方法
簡単でありながら、セキュアなユーザの認証方法	• ユーザがパスコードのみを要求されるように、Microsoft Windows のパスワードと RSA SecurID ログオンを統合する方法 • オンライン認証とオフライン認証で同一である一貫した認証プロセス
自宅で作業するユーザに RSA SecurID 認証プロセスを提供する方法	ネットワーク経由で RSA Authentication Manager に接続していないコンピュータへの認証まで、RSA SecurID 二要素認証を拡張する方法
リモート アクセス可能な Web リソースを保護するセキュアな方法	Web リソース向けの RSA SecurID 二要素保護

以下の表は、このシナリオで RSA SecurID 認証を適用できる場所、必要なコンポーネント、およびインストールする場所を示しています。

ドメイン リソース	
コンポーネント	**インストールする場所**
ドメイン認証サーバ コンポーネント	ドメイン コントローラ ホスト
ドメイン認証クライアント コンポーネント	ドメイン クライアント コンピュータおよびドメイン コントローラ ホスト

Web リソース	
コンポーネント	**インストールする場所**
Web Agent 5.3 サーバ コンポーネント	Web サーバ ホスト

考察

このシナリオでは、ドメイン認証、Windows パスワード統合、およびオフライン認証を組み合わせ、オフィスで作業するユーザとオフィスを離れて作業するユーザの両方に一貫した認証を確実に実施します。

オフィス内におけるドメイン認証は、RSA SecurID パスコードの入力をユーザに要求することで、企業ドメインのリソースおよび Windows デスクトップへのアクセス認証を行います。有効なパスコードを入力したユーザのみがアクセスを許可されます。オフライン認証では、ドメイン コントローラが一時的に RSA Authentication Manager と通信不能になっても、ユーザがドメインに認証できるため、より高い信頼性を得ることができます。

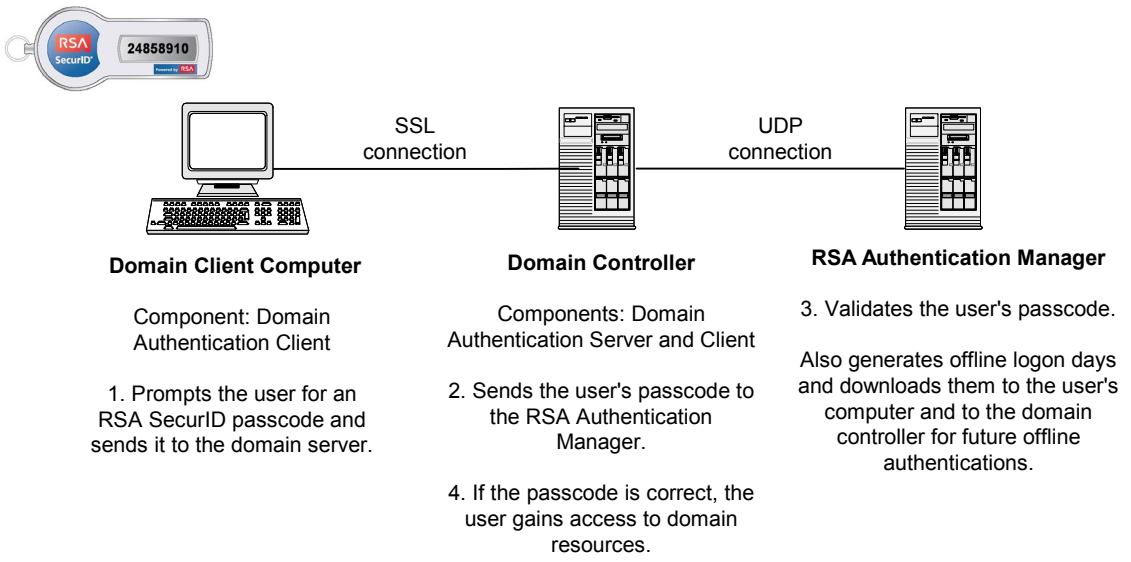
オフライン認証を追加すると、オフィスを離れて作業しているユーザに対しても同じ認証プロセスが行われるように RSA SecurID 認証機能が拡張します。ドメイン アカウントを使用してオフラインで認証を実行するには、ユーザは RSA SecurID パスコードを入力する必要があります。

このシナリオでは、Web リソースの保護に RSA Authentication Agent 5.3 for Web を使用します。オフライン ユーザが、Microsoft Outlook Web Access を使用して電子メール アカウントへのアクセスを試行すると、Authentication Agent がユーザに RSA SecurID パスコードの入力を要求します。認証済みユーザのみが企業の電子メール アカウントへのアクセスを許可されます。

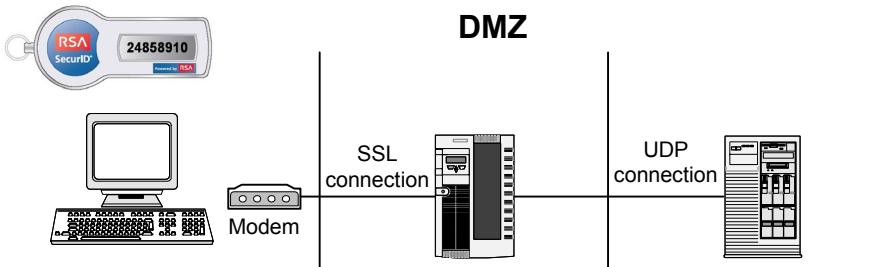
このシナリオでは、Windows パスワード統合により Windows パスワードのセキュリティを強化するとともに認証プロセスを簡略化します。たとえば、ユーザの初回ログオン以降であれば、管理者は Active Directory に格納されているそのユーザのパスワードを長く、複雑なものに変更できます。Active Directory は、パスワードの変更をドメイン コントローラに通知します。RSA Authentication Manager は、ドメイン コントローラから新しいパスワードを取得して、それを RSA Authentication Manager データベースのユーザ アカウントに格納します。そのユーザの次回の認証時に、RSA Authentication Agent は、Windows パスワードを RSA Authentication Manager から取得して、それを Windows ログオン プロセスに送信します。ユーザは新しいパスワードを見ることはありませんので、パスワードを覚えたり、またパスワードを書き留めたりする必要はありません。

この企業では、管理者が一般従業員のためにソフトウェアをインストールして構成するので、管理者はユーザのコンピュータにアクセスする必要があります。これを容易にするために、全員へのパスコード要求から管理者を除外することもできます。これは、管理者用の Windows グループを作成し、このグループのメンバー以外のユーザ全員に対して認証要求を実施するようにします。

以下の図は、オフィスで作業するユーザのオンライン セットアップを示しています。



以下の図は、自宅で作業するユーザのセットアップを示しています。



DMZ

Domain Client Computer

Component: Domain Authentication Client

1. Prompts the user for an RSA SecurID passcode and validates the passcode against locally stored offline logon data.

2. If the passcode is correct, the user gains access to the local desktop.

Web Server

Component: RSA Authentication Agent 5.3 and Outlook Web Access

3. For accessing e-mail through Outlook Web Access, prompts the user for an RSA SecurID passcode and sends it to the RSA Authentication Manager.

5. If the passcode is correct, the user gains access to his or her e-mail account.

RSA Authentication Manager

4. Verifies the user's passcode and sends verification status to the web server.

シナリオ 2: 中規模の企業

従業員を 2,000 人雇っている企業に勤めているとします。企業のリソースは、北米ドメインと欧州ドメインの 2 つのドメインに分割されています。各ドメインには、それぞれ 2 台のドメインコントローラが存在します。

研究所にある 3 台のコンピュータを除くコンピュータは、全てネットワークにオンライン接続しています。研究所のコンピュータには機密データを含むファイルが存在するので、承認された数人の従業員のみにアクセスを限定します。

RRAS 企業の従業員の 20 % は、IPSec VPN (Internet Protocol Security Virtual Private Network) および Windows Terminal Services for Siebel を使用してリモートでカスタマアカウント情報の状況確認を行う販売員です。パイロットグループは、ワイヤレス接続を使用してリモート接続します。システム管理者は、RRAS を使用してリモート接続します。

企業の必要性	RSA SecurID for Microsoft Windows が提供する事項
ドメイン リソースを保護するセキュアな方法	• ドメイン リソースへの RSA SecurID 二要素保護 • RSA Authentication Manager への接続不能の場合でも、ドメイン リソースへの RSA SecurID 二要素保護を拡張する方法
ネットワークに接続していないコンピュータに対して RSA SecurID 認証を拡張する方法	• ローカル コンピュータへの RSA SecurID 二要素保護 • RSA Authentication Manager を介してネットワークに接続していないコンピュータに向けて RSA SecurID 二要素認証を拡張する方法
リモート アクセス可能なドメインリソースを保護するセキュアな方法	リモート アクセス可能なリソースの RSA SecurID 二要素保護
簡単でありながら、セキュアなユーザの認証方法	• ユーザがパスコードのみを要求されるように、Microsoft Windows のパスワードと RSA SecurID ログオンを統合する方法 • オンライン認証とオフライン認証で同一である認証プロセス
RSA Authentication Agent クライアント ソフトウェアを効率良くインストールして構成する方法	Microsoft Installer (.msi) のサポート

以下の表は、このシナリオで RSA SecurID 認証を適用できる場所、必要なコンポーネント、およびインストールする場所を示しています。

ドメイン リソース

コンポーネント	インストールする場所
ドメイン認証サーバ コンポーネント	ドメイン コントローラ
ドメイン認証クライアント コンポーネント	• ドメイン コントローラ • ドメイン クライアント コンピュータ

ローカル コンピュータ

コンポーネント	インストールする場所
ローカル認証クライアント コンポーネント	• ネットワークに接続していない研究用コンピュータ • オフサイト コンピュータ

リモート接続

コンポーネント	インストールする場所
リモート認証サーバコンポーネント	RRAS サーバ

ワイヤレス接続

コンポーネント	インストールする場所
リモート認証サーバ コンポーネント	RADIUS サーバ
RSA EAP クライアント コンポーネント	ドメイン リソースへのリモート アクセスに使用される全コンピュータ

ターミナル エミュレーション セッション

コンポーネント	インストールする場所
• ローカル認証コンポーネント • ドメイン認証コンポーネント	ターミナル サーバ

ディスカッション

ドメインとドメイン クライアント コンピュータ

このシナリオにおいて、ドメイン認証は、RSA SecurID パスコードの入力をユーザに要求して、企業ドメインへのアクセスの認証を行います。また RSA SecurID パスコードの再認証なしで、ユーザが保護されたドメイン間を横断できるようにドメイン認証を構成することができます。

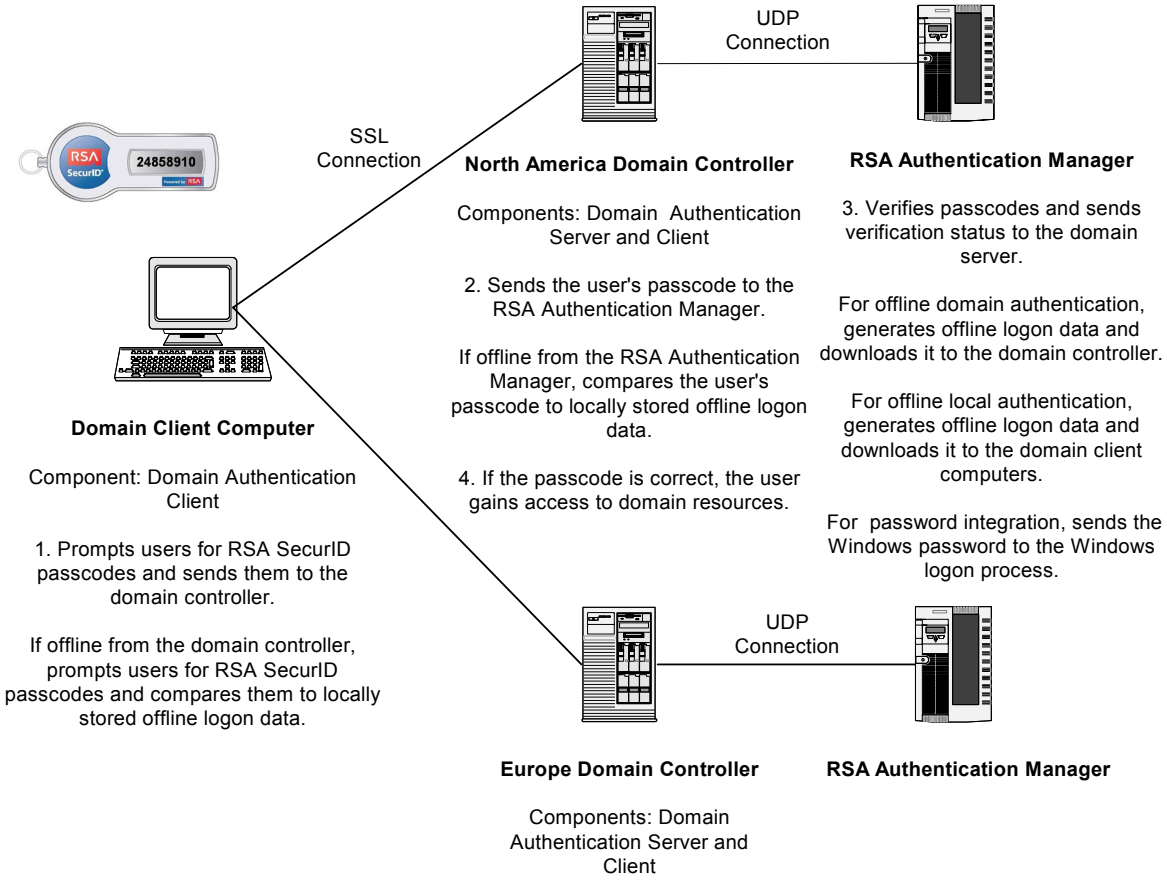
また、保護および非保護のドメイン間の認証を構成できます。非保護のドメイン内を横断するユーザは RSA SecurID パスコードの入力を要求されません。保護されているドメイン内を横断するユーザは RSA SecurID パスコードの入力を要求されます。

オフライン認証により、ドメイン コントローラが一時的に RSA Authentication Manager と切断していても、ユーザはドメイン認証を行うことができます。また、クライアントがドメイン コントローラから切断された場合 (たとえば、ユーザが機内または自宅から作業している場合) にも、ユーザがドメイン アカウントを使用して、ドメイン クライアント デスクトップへの認証が可能です。

ドメイン クライアント コンピュータの Windows パスワード統合を有効にすると、Windows パスワードのセキュリティを強化するとともに認証プロセスを簡略化することが可能となります。たとえば、ユーザの初回ログオン以降であれば、管理者は Active Directory に格納されているそのユーザのパスワードを長く複雑なものに変更できます。Active Directory は、パスワードの変更をドメイン コントローラに通知します。RSA Authentication Manager は、ドメイン コントローラから新しいパスワードを取得して、それを RSA Authentication Manager データベースのユーザ アカウントに格納します。そのユーザの次回の認証時に、RSA Authentication Agent は、Windows パスワードを RSA Authentication Manager から取得して、それを Windows ログオン プロセスに送信します。ユーザは新しいパスワードを見ることはありませんので、パスワードを覚えたり、もしくはパスワードを書き留めたりする必要はありません。RSA SecurID パスコードの再認証なしで、ユーザが保護されたドメイン間を横断できるようにドメイン認証を構成することができます。

詳細は、43 ページの「ドメイン認証を配置する」を参照してください。また、「インストール&アドミニストレーションガイド」の「ドメイン認証を構成する」の章の「クロスドメイン認証を構成する」を参照してください。

以下の図は、このシナリオにおけるドメイン認証のセットアップを示しています。



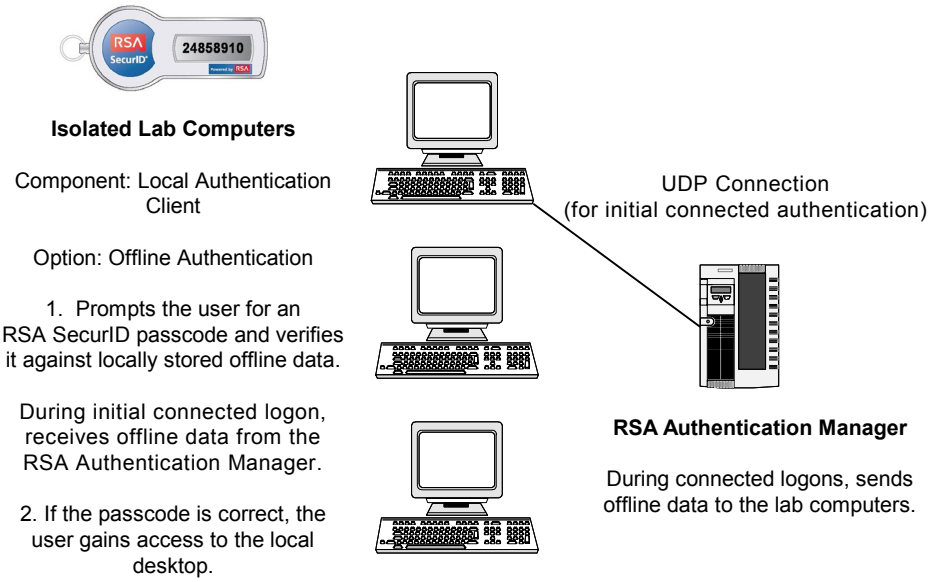
ネットワークに接続していないコンピュータ

このシナリオでは、ローカル認証とオフライン認証を組み合わせ、ネットワークに接続していない 3 台の研究用コンピュータへ RSA SecurID 認証を拡張しています。また、Windows ログオン パスワードを RSA SecurID 認証プロセスに統合して Windows パスワードの統合化を行い、認証プロセスを簡略化しています。

研究用コンピュータでオフライン認証を有効にするには、各コンピュータから Windows ログオン パスワードと RSA SecurID パスコードの両方を入力して、初期オンライン認証を 2 回 (たとえば、テスト認証を 1 回また実際の認証を 1 回) ネットワークに接続して実施する必要があります。2 回目の認証時に、RSA Authentication Manager は、オフラインデータを作成して各研究用コンピュータにダウンロードします。各研究用コンピュータの Windows ログオン パスワードは、そのコンピュータのオフライン データに含まれています。以降のオフライン認証時には、ローカル認証コンポーネントは、ユーザに RSA SecurID パスコードのみを要求します。コンピュータで稼動している Authentication Agent が、ローカル コンピュータに保存されているオフラインデータと入力されたパスコードを比較します。パスコードが正しければ、ユーザは研究用コンピュータ デスクトップへのアクセスが許可されます。さらにオフライン データを取得するには、定期的に、各ユーザは研究用コンピュータにオフライン アクセスすることが必要であり、そしてオンライン認証しなければなりません。

ローカル認証についての詳細は、41 ページの「ローカル認証を配置する」を参照してください。

以下の図は、このシナリオにおける研究用コンピュータのセットアップを示しています。



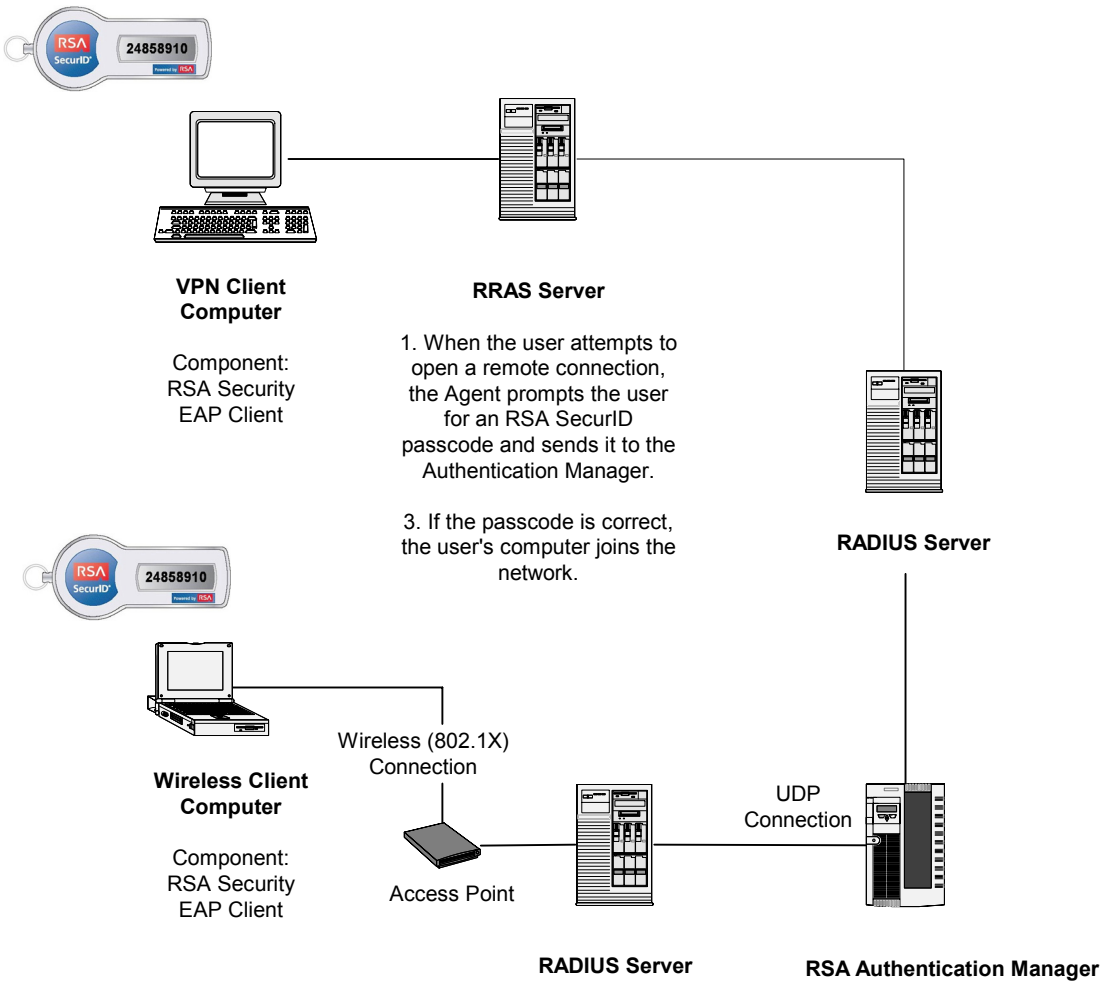
リモートおよびワイヤレス接続

このシナリオでは、リモート認証により、ユーザは、企業ドメインへのリモート接続を開始する前に、RSA SecurID パスコードで認証を行うことが要求されます。

リモート認証により、販売員は、アカウント データへアクセスする前に認証を要求されます。そして、管理者は、RRAS サーバへアクセスする前に (たとえば、管理作業を行う前に) 認証を要求されます。ワイヤレス認証により、パイロット グループは、ワイヤレス接続を開始する前にパスコードでの認証を要求されます。

リモート認証についてのもっと詳しい情報は、45 ページの「リモート認証を配置する」、ワイヤレス認証についての詳細は、53 ページの「ワイヤレス認証を配置する」を参照してください。

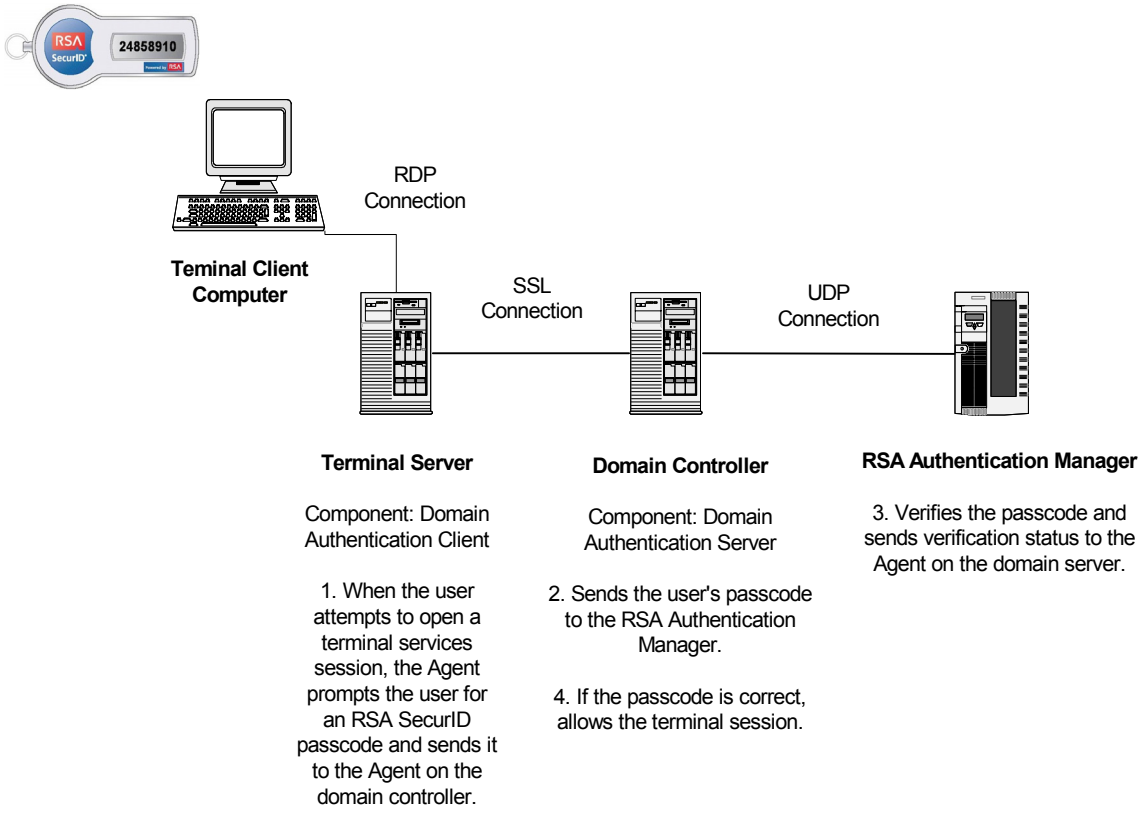
以下の図は、このシナリオにおけるリモートおよびワイヤレス アクセスのセットアップを示しています。



ターミナル サービス セッション

ターミナル サーバでのドメイン認証を有効にすると、Windows Terminal Services for Siebel を使用する販売員は、カスタマー アカウント情報へアクセスする前に、RSA SecurID パスコードで認証を行うことが要求されます。これを容易にするには、RSA Authentication Agent ドメイン認証クライアント コンポーネントをターミナル サーバにインストールします。

以下の図は、ターミナル サービス ユーザのセットアップを示しています。



4 物理的な配置計画

物理的な配置では、インストールするソフトウェア コンポーネントと、それらのインストール先を決定します。本章では、以下の内容について説明します。

- 各認証ソリューションを配置する基本的な手順
- インストールする必要があるコンポーネントの選択と、インストールする場所の決定
- ソフトウェアのインストールに関するオプション

インストールするコンポーネントとインストール先に関する計画

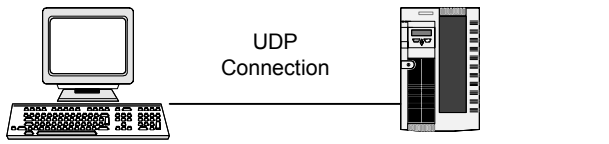
このセクションでは各認証ソリューションを手動で配置するための基本的な手順を説明します。配置するソリューションによっては、サイレント インストールを作成するとより短時間で配置することができます。詳細は、58 ページの「インストール手法の計画」を参照してください。

ローカル認証を配置する

以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager	セキュアなコンピュータ
ローカル認証クライアント コンポーネント	RSA SecurID で保護する各コンピュータ

以下の図は、ローカル認証のセットアップを示しています。



User's Computer **RSA Authentication Manager**

Component:
Local Authentication Client

以下の表は、ローカル認証を配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」のどこに記載されているかを示しています。

配置手順	「RSA Authentication Agent 6.1 インストレーション&アドミニストレーションガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 をインストールしてセットアップします。	「システム要件と準備」の章

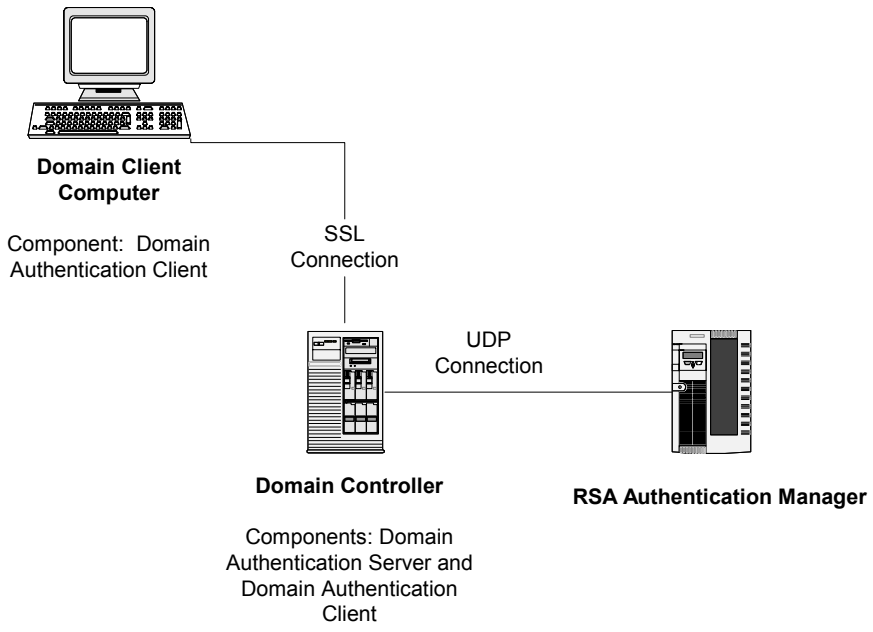
配置手順	「RSA Authentication Agent 6.1 インストレーション&アドミニストレーションガイド」の詳細情報の記載場所
2. Microsoft Windows 認証要求グループを作成します。	「システム要件と準備」の章の「RSA SecurID 認証要求の対象ユーザ グループの作成」
3. 保護する各コンピュータにローカル認証クライアント コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
4. IP アドレスの割り当てに DHCP (Dynamic Host Configuration Protocol) を使用している場合、ユーザの保護されているコンピュータに Automated Agent Host Registration and Update utility をインストールして構成します。	付録の「エージェント ホストを RSA Authentication Manager データベースに自動登録する」
5. RSA Security Center を起動します。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 4 : RSA Security Center を起動する」
6. 認証環境の状態を確認して認証テストを行います。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 5 : 認証環境の状態を確認する」および「ステップ 6 : 認証テスト」
7. ローカル認証を構成します。	「ローカル認証を構成する」の章

ドメイン認証を配置する

以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Certificate Utility	物理的にセキュアなコンピュータ
RSA Authentication Manager	セキュアなコンピュータ
ドメイン認証サーバ コンポーネント	RSA SecurID で保護する各ドメイン コントローラ
ドメイン認証クライアント コンポーネント	• RSA SecurID で保護する各ドメイン コントローラ • RSA SecurID で保護する各ドメイン クライアント コンピュータ

以下の図は、ドメイン インストールのセットアップを示しています。



以下の表は、ドメイン認証を配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」のどこに記載されているかを示しています。

配置手順	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 をインストールしてセットアップします。	「システム要件と準備」の章
2. Microsoft Windows 認証要求グループをドメイン コントローラに作成します。	「システム要件と準備」の章の「RSA SecurID 認証要求の対象ユーザ グループの作成」

配置手順	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の詳細情報の記載場所
3. RSA Certificate Utility を物理的にセキュアなコンピュータにインストールします。	「システム要件と準備」の章の「ステップ 1 : Certificate Utility のインストール」
4. 証明書を作成します。	「システム要件と準備」の章の「ステップ 2 : 証明書の作成」
5. ドメイン認証サーバ コンポーネントをドメイン コントローラにインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
6. ドメイン認証クライアント コンポーネントを、保護されたドメインにアクセスする必要がある各クライアント コンピュータにインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
7. ドメイン コントローラ上で、RSA Security Center を起動して、ドメイン認証を構成します。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 4 : RSA Security Center を起動する」
8. 各ドメイン クライアント上で、RSA Security Center を起動して、ドメイン認証を構成します	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 4 : RSA Security Center を起動する」
9. 各ドメイン クライアントとドメイン コントローラ間の認証テストを行います。	「ドメイン認証を構成する」の章の「ステップ 2 : ドメイン認証をテストする」

リモート認証を配置する

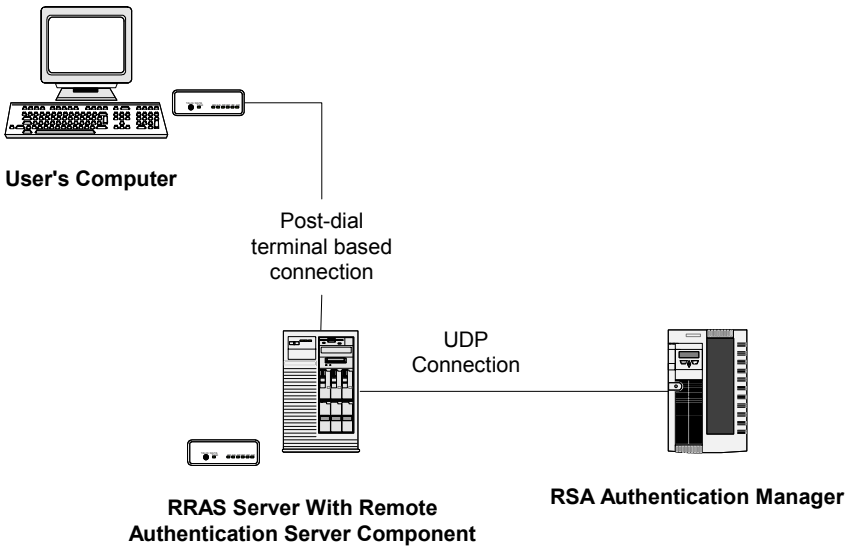
配置したいリモート認証ソリューションと同様に、自分の認証環境タイプによって、インストールするべき RSA Authentication Agent コンポーネントが決まります。EAP を使用するかどうか、どの RADIUS サーバを使用するかによって環境タイプが決定します。Microsoft IAS RADIUS Server か RSA RADIUS Server のどちらかを使用します。RSA RADIUS Server は RSA Authentication Manager と一緒に出荷されています。また、RSA RADIUS Server はリモート サーバの RSA Authentication Agent を必要としません。Microsoft IAS RADIUS Server ソリューションと RSA RADIUS Server ソリューションの両方は、OTP (RSA EAP Protected One Time Password) (EAP 32) をサポートします。さらに、RSA Security EAP(EAP15) もサポートします。

以下の図はこれらのリモート認証ソリューションのセットアップを示しています。

- EAP を使用しない
- RADIUS サーバを使用しない EAP
- Microsoft IAS RADIUS Server を使用する EAP
- RSA RADIUS Server を使用する EAP

EAP を使用しないリモート認証を配置する

以下の図は、この環境のセットアップを示しています。



以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager	セキュアなコンピュータ
リモート認証サーバ コンポーネント	RRAS サーバ

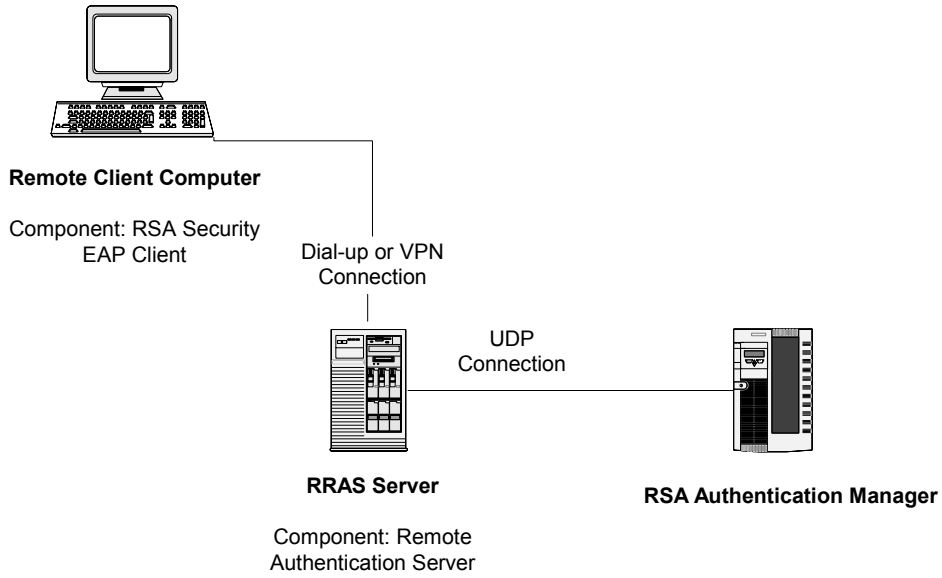
管理者は、EAP を使用する手法よりも、こちらの手法を使用したいと思う場合があります。なぜなら、この手法ではソフトウェアをクライアント コンピュータにインストールする必要がありません。

以下の表は、このリモート認証ソリューションを配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」のどこに記載されているかを示しています。R

配置手順	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーション ガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 をインストールしてセットアップします。	「システム要件と準備」の章
2. Microsoft Windows 認証要求グループを作成します。	「システム要件と準備」の章の「RSA SecurID 認証要求の対象ユーザグループの作成」
3. RRAS サーバにリモート認証サーバ コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
4. RSA Security Center を起動します。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 4 : RSA Security Center を起動する」
5. 認証環境の状態を確認して認証テストを行います。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 5 : 認証環境の状態を確認する」および「ステップ 6 : 認証テスト」
6. RRAS サーバに RSA Authentication Agent を構成します。	「リモート認証を構成する」の章の「EAP を使用しないリモート認証を配置する」

RADIUS サーバを使用しない EAP を使って、リモート認証を配置する

以下の図は、この環境のセットアップを示しています。



以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager 6.1	セキュアなコンピュータ
リモート認証サーバコンポーネント	RRAS サーバ
RSA Security EAP クライアントコンポーネント	RSA SecurID で保護する各クライアントコンピュータ

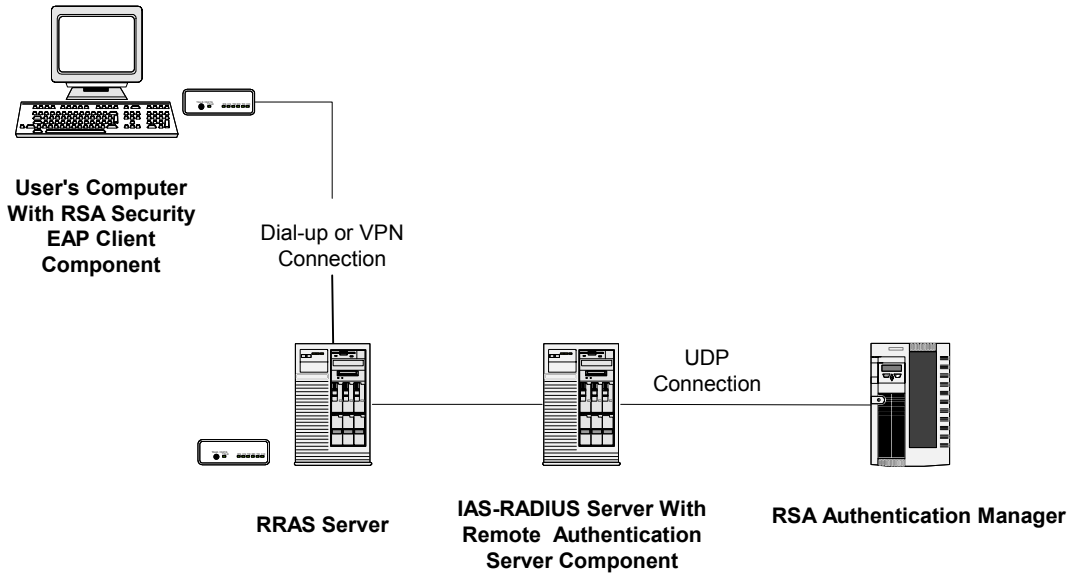
以下の表は、このリモート認証ソリューションを配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション&アドミニストレーションガイド」のどこに記載されているかを示しています。

配置手順	「RSA Authentication Agnet 6.1 インストレーション&アドミニストレーションガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 をインストールしてセットアップします。	「システム要件と準備」の章
2. Microsoft Active Directory にアクセス グループを作成します。	「リモート認証を構成する」の章の「RADIUS を使用しない EAP を使って、リモート認証を配置する」
3. RRAS サーバにリモート認証サーバ コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
4. RSA Security Center を起動します。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 4 : RSA Security Center を起動する」

配置手順	「RSA Authentication Agnet 6.1 インストレーション&アドミニストレーション ガイド」の詳細情報の記載場所
5. 認証環境の状態を確認して認証テストを行います。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 5 : 認証環境の状態を確認する」および「ステップ 6 : 認証テスト」
6. RSA Security EAP や RSA EAP - Protected OTP を使用するように RRAS サーバを構成します。	「リモート認証を構成する」の章の「RADIUS を使用しない EAP を使って、リモート認証を配置する」
7. 各リモートクライアントコンピュータに RSA Security EAP クライアントコンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
8. EAP を使用するようにリモートクライアントコンピュータを構成します。	「リモート認証を構成する」の章の「RADIUS を使用しない EAP を使って、リモート認証を配置する」
9. RRAS サーバに RSA Authentication Agent を構成します。	「リモート認証を構成する」の章の「RADIUS を使用しない EAP を使って、リモート認証を配置する」

Microsoft IAS RADIUS Server を使用する EAP を使って、リモート認証を配置する

以下の図は、この環境のセットアップを示しています。



以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager 6.1	セキュアなコンピュータ
リモート認証サーバ コンポーネント	Microsoft IAS Server
RSA Security EAP クライアント コンポーネント	各リモート クライアント コンピュータ

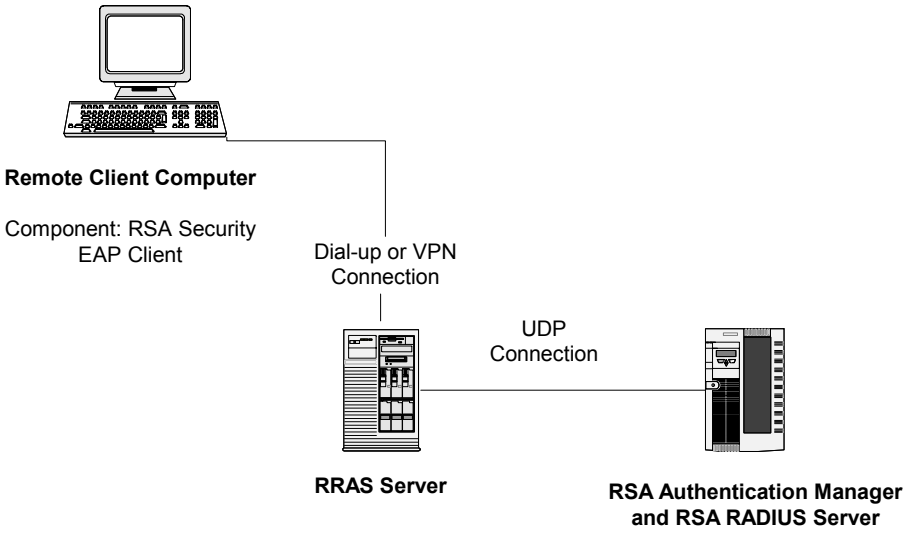
以下の表は、このリモート認証ソリューションを配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション&アドミニストレーションガイド」のどこに記載されているかを示しています。

配置手順	「RSA Authentication Agent 6.1 インストレーション&アドミニストレーション ガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 をインストールしてセットアップします。	「システム要件と準備」の章
2. Microsoft Active Directory にアクセス グループを作成します。	「リモート認証を構成する」の章の「Microsoft IAS RADIUS Server を使用する EAP を使って、リモート認証を配置する」
3. RADIUS を使用するように RRAS サーバを構成します	「リモート認証を構成する」の章の「Microsoft IAS RADIUS Server を使用する EAP を使って、リモート認証を配置する」

配置手順	「RSA Authentication Agent 6.1 インストレーション&アドミニストレーション ガイド」の詳細情報の記載場所
4. Microsoft IAS Server にリモート認証サーバ コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
5. RSA Security Center を起動します。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 4 : RSA Security Center を起動する」
6. 認証環境の状態を確認して認証テストを行います。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「ステップ 5 : 認証環境の状態を確認する」および「ステップ 6 : 認証テスト」
7. RSA Security EAP や RSA EAP - Protected OTP を使用するように Microsoft IAS Server を構成します。	「リモート認証を構成する」の章の「Microsoft IAS RADIUS Server を使用する EAP を使って、リモート認証を配置する」
8. 各リモート クライアント コンピュータに RSA Security EAP クライアント コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
9. EAP を使用するようにリモート クライアント コンピュータを構成します。	「リモート認証を構成する」の章の「Microsoft IAS RADIUS Server を使用する EAP を使って、リモート認証を配置する」
10. リモート サーバに RSA Authentication Agent を構成します。	「リモート認証を構成する」の章の「Microsoft IAS RADIUS Server を使用する EAP を使って、リモート認証を配置する」

RSA RADIUS Server を使用する EAP を使って、リモート認証を配置する

以下の図は、この環境のセットアップを示しています。



以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager 6.1	セキュアなコンピュータ
RSA RADIUS Server	RSA Authentication Manager と同等のコンピュータか、または RSA Authentication Manager とは別のコンピュータ
(オプション) ローカル認証クライアント	RSA RADIUS Server と同等のコンピュータ
RSA Security EAP クライアント コンポーネント	各リモートクライアント コンピュータ

メモ：RSA RADIUS Server を使用する EAP は RSA RADIUS Server ホストの Authentication Agent コンポーネントを必要としませんが、管理者は簡単なノード シークレットの管理方法を提供するためにローカル認証クライアント コンポーネントをインストールしたい場合があります。詳細は、「RSA Authentication Agent 6.1 インストーレーション&アドミニストレーションガイド」の「高度かつトラブルシューティングな設定を構成する」の章の「RSA RADIUS Server でノード シークレットを管理する」を参照してください。

以下の表は、このリモート認証ソリューションを配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション&アドミニストレーションガイド」のどこに記載されているかを示しています。

配置手順	「RSA Authentication Agent 6.1 インストレーション&アドミニストレーション ガイド」の詳細情報の記載場所
1. RSA RADIUS Server も伴う RSA Authentication Manager 6.1 をインストールしてセットアップします。	「システム要件と準備」の章
2. (オプション) RSA RADIUS Server コンピュータにローカル認証クライアント コンポーネントをインストールし、ローカル認証要求を **None** に設定します。	「高度かつトラブルシューティングな設定を構成する」の章の「RSA RADIUS Server でノード シークレット（Node Secret）を管理する」
3. RSA RADIUS Server を構成します。	「リモート認証を構成する」の章の「RSA RADIUS Server を使用する EAP を使って、リモート認証を配置する」
4. 各リモート クライアント コンピュータに RSA Security EAP クライアント コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
5. RSA RADIUS Server を使用するように RADIUS クライアントを構成します。	「リモート認証を構成する」の章の「RSA RADIUS Server を使用する EAP を使って、リモート認証を配置する」

配置手順	「RSA Authentication Agent 6.1 インストレーション&アドミニストレーション ガイド」の詳細情報の記載場所
6. EAP を使用するようにクライアント コンピュータを構成します。	「リモート認証を構成する」の章の「RSA RADIUS Server を使用する EAP を使って、リモート認証を配置する」

ワイヤレス認証を配置する

以下のタイプの環境でワイヤレス認証を配置することができます。

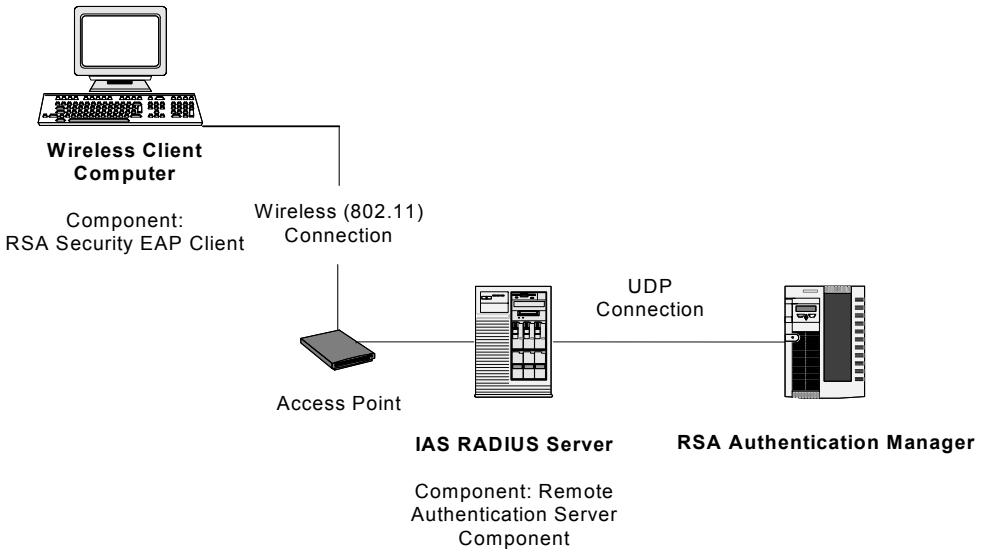
- RSA EAP - Protected OTP
- PEAP

RSA EAP - Protected OTP を使用することで、PEAP や TTLS のように、認証証明書および追加トンネリングが不要となります。

RSA RADIUS Server を使用する RSA EAP - Protected OTP を配置する

このセクションは RSA RADIUS Server を使用する RSA EAP - Protected OTP を使ったワイヤレス認証のセットアップについて説明していますが、Microsoft IAS RADIUS Server を使用するワイヤレス認証のセットアップにも当てはまります。詳しい情報は、「RSA Authentication Agent 6.1 インストレーション&アドミニストレーションガイド」の「ワイヤレス認証を構成する」の章の「RSA EAP - Protected OTP を使用するワイヤレス認証を配置する」を参照してください。

以下の図は、RSA RADIUS Server を使用するワイヤレス環境のセットアップを示しています。



以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager 6.1	セキュアなコンピュータ
RSA RADIUS Server	RSA Authentication Manager と同等のコンピュータか、または RSA Authentication Manager とは別のコンピュータ
(オプション) ローカル認証クライアント	RSA RADIUS Server と同等のコンピュータ
RSA Security EAP クライアント コンポーネント	各リモート クライアント コンピュータ

メモ：RSA RADIUS Server を使用する RSA EAP - Protected OTP は RSA RADIUS Server ホストの Authentication Agent コンポーネントを必要としませんが、管理者は簡単なノード シークレットの管理方法を提供するためにローカル認証クライアントコンポーネントをインストールしたい場合があります。詳細は、「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」の「高度かつトラブルシューティングな設定を構成する」の章の「RSA RADIUS Server でノード シークレットを管理する」を参照してください。

以下の表は、このリモート認証ソリューションを配置するための基本的な手順をまとめています。また、詳細情報が 「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」のどこに記載されているかを示しています。

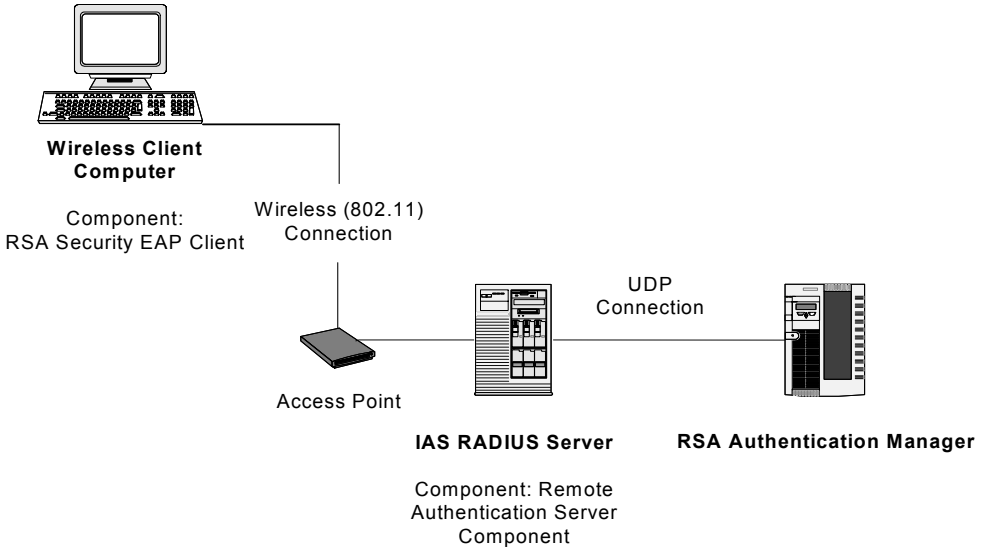
配置手順	「RSA Authentication Agnet 6.1 インストレーション & アドミニストレーションガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 と RSA RADIUS Server をインストールしてセットアップします。	「システム要件と準備」の章
2. (オプション) RSA RADIUS Server コンピュータにローカル認証クライアントコンポーネントをインストールし、ローカル認証要求を **None** に設定します。	「高度かつトラブルシューティングな設定を構成する」の章の「RSA RADIUS Server でノード シークレットを管理する」
3. RSA RADIUS Server を構成します。	「リモート認証を構成する」の章の「RSA RADIUS Server を使用する RSA EAP - Protected OTP を配置する」
4. ワイヤレス LAN 環境をセットアップします。	「リモート認証を構成する」の章の「RSA RADIUS Server を使用する RSA EAP - Protected OTP を配置する」
5. 各リモート クライアント コンピュータに RSA Security EAP クライアント コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章

配置手順	「RSA Authentication Agnet 6.1 インストレーション & アドミニストレーションガイド」の詳細情報の記載場所
6. クライアント コンピュータを構成します。	「リモート認証を構成する」の章の「RSA RADIUS Server を使用する RSA EAP - Protected OTP を配置する」

RSA RADIUS Server を使用する PEAP を配置する

このセクションは PEAP と RSA RADIUS Server を使ったワイヤレス認証のセットアップをまとめています。しかしながら、Microsoft IAS RADIUS Server を使用するワイヤレス認証のセットアップも可能です。詳細は、「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」の「ワイヤレス認証を構成する」の章の「PEAP を使用するワイヤレス認証を配置する」を参照してください。

以下の図は、RSA RADIUS Server を使用するワイヤレス環境のセットアップを示しています。



以下の表は、インストールする必要がある RSA Security コンポーネントとインストールする場所を示しています。

コンポーネント	場所
RSA Authentication Manager 6.1	セキュアなコンピュータ
RSA RADIUS Server	RSA Authentication Manager と同等のコンピュータか、または RSA Authentication Manager とは別のコンピュータ
(オプション) ローカル認証クライアント	RSA RADIUS Server と同等のコンピュータ
RSA Security EAP クライアント コンポーネント	各リモート クライアント コンピュータ

メモ：RSA RADIUS Server を使用する PEAP は RSA RADIUS Server ホストの Authentication Agent コンポーネントを必要としませんが、管理者は簡単なノード シークレットの管理方法を提供するためにローカル認証クライアントコンポーネントをインストールする場合があります。詳細は、「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」の「高度かつトラブルシューティングな設定を構成する」の章の「RSA RADIUS Server でノード シークレットを管理する」を参照してください。

以下の表は、このリモート認証ソリューションを配置するための基本的な手順をまとめています。また、詳細情報が「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」のどこに記載されているかを示しています。

配置手順	「RSA Authentication Agent 6.1 インストレーション & アドミニストレーションガイド」の詳細情報の記載場所
1. RSA Authentication Manager 6.1 と RSA RADIUS Server をインストールしてセットアップします。	「システム要件と準備」の章
2. (オプション) RSA RADIUS Server コンピュータにローカル認証クライアントコンポーネントをインストールし、ローカル認証要求を **None** に設定します。	「高度かつトラブルシューティングな設定を構成する」の章の「RSA RADIUS Server でノードシークレットを管理する」
3. ワイヤレス認証のための証明書を入手します。	「ワイヤレス認証を構成する」の章の「RSA RADIUS Server を使用する RSA EAP - Protected OTP を配置する」
4. RSA RADIUS Server を構成します。	「ワイヤレス認証を構成する」の章の「PEAP を使用するワイヤレス認証を配置する」
5. ワイヤレス LAN 環境をセットアップします。	「ワイヤレス認証を構成する」の章の「PEAP を使用するワイヤレス認証を配置する」
6. 各リモート クライアント コンピュータに RSA Security EAP クライアント コンポーネントをインストールします。	「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章
7. リモート クライアント コンピュータを構成します。	「ワイヤレス認証を構成する」の章の「PEAP を使用するワイヤレス認証を配置する」

インストール手法の計画

一部のソリューション（たとえば、ドメイン認証およびローカル認証）では、エージェント コンポーネントをすべてのユーザのコンピュータにインストールする必要があります。システム全体のコンピュータの数にもよりますが、この作業は多大な時間を必要とする可能性があります。そのため、RSA Authentication Agent 6.1 for Microsoft Windows では 2 つのインストール方法を提供しています。

- インタラクティブ インストール
- サインレント インストール

インタラクティブ インストール

各ドメインクライアント コンピュータでインストール ウィザードを実行して、インタラクティブ (対話型) インストールを実行します。その場合はインストール プロンプトに、設定情報を入力します。インタラクティブ インストールには、次の 2 種類のタイプがあります。

Typical。ドメイン認証クライアント コンポーネントをインストールします。

Custom。インストール作業者が選択したコンポーネントに従って、以下のコンポーネントの一部、またはすべてをインストールします。

- ローカル認証クライアント コンポーネント
- ドメイン認証サーバ コンポーネント
- ドメイン認証クライアント コンポーネント
- リモート認証サーバ コンポーネント
- RSA Security EAP クライアント

サインレント インストール

RSA Authentication Agent 6.1 for Microsoft Windows のインストール プロセスを速めるために、あらかじめ構成された .msi ネットワーク インストール パッケージを作成することができます。ネットワークでインストール パッケージを配付するか、またはネットワーク上の共有の場所にそのパッケージを置いておくことで、ユーザの介入が必要ない RSA Authentication Agent のサイレント インストールが可能となります。

デフォルトでは、インストール パッケージはドメイン認証クライアント コンポーネントだけをインストールします。ただし、デフォルトもしくはデフォルトに加えて他のエージェント コンポーネントのインストールを選択することもできます。すべてのコンポーネントの配置を計画していなくても、それらのコンポーネントを使用できるように後でインストールすることができます。

サインレント モード インストールを作成する

1. 弊社が提供しているファイルを使用して、ネットワーク インストール パッケージを作成します。
2. このインストールパッケージを、ネットワーク上の共有場所またはドメイン コントローラにコピーします。
3. 必要に応じて、インストール パッケージを編集してインストールをカスタマイズします。

デフォルトでは、インストール パッケージは、ドメイン認証クライアント コンポーネントをインストールします。ただし、インストールパッケージがその他の Authentication Agent コンポーネントをサイレント インストールするようにカスタマイズすることができます。

詳細は、「RSA Authentication Agent 6.1 インストレーション& アドミニストレーション ガイド」の「RSA Authentication Agent 6.1 for Microsoft Windows のインストール」の章の「サイレント モード インストールを作成する」を参照してください。

索引