RSA Authentication Agent 7.1 for Microsoft Windows リリースノート

2012 年 2 月

はじめに

本書では、RSA® Authentication Agent 7.1 for Microsoft Windows の新機能について説明します。また、既知の問題の回避策についても説明します。ソフトウェアをインストールする前に、本書を必ずお読みください。本書は次のセクションで構成されています。

本リリースノートは更新される場合があります。最新版 (英語) は、RSA SecurCare Online (**https://knowledge.rsasecurity.com**) からダウンロードできます。

本リリースの新機能

本リリースでは、次の新機能および機能拡張が加えられました。

マルチドメイン (ユニバーサル) ユーザグループのサポート。Authentication Agent では、マルチドメイングループを含むすべての Windows グループがサポートされます。ユーザおよびグループは同じフォレストに存在している必要があります。

ユーザプリンシパル名 (UPN) によるログオンのサポート。ユーザは、UPN を使用してログインできるようになりました。UPN 形式では、インターネットのメールアドレスの UserName@Example.RSA.com のように名前を指定します。

エージェントの配布の簡素化。以前のリリースでは、32 ビットおよび 64 ビットのオペレーティングシステムで別々のバージョンの Authentication Agent が必要でした。本リリースでは、サポート対象のすべてのオペレーティングシステムの 32 ビットおよび 64 ビット版の両方で単一の Agent を展開できます。

単一のバージョンですべての製品機能をサポート。

- 本バージョンでは、現在出荷されているすべてのバージョンの Microsoft Windows で、制御および管理機能が統一されています。これまでのバージョンでは、Vista 以前と以後のシステムでは制御および管理機能がそれぞれ異なっていました。
- 本リリースでは、現在出荷されているすべてのバージョンの Microsoft Windows で、RSA SecurID 800 トークンの接続がサポートされます。

ユーザの簡易切り替えのサポート。ユーザの簡易切り替え機能に対応している Windows オペレーティングシステムであれば、Authentication Agent でもこの機能がサポートされます。ユーザの簡易切り替え機能を使用すると、複数のユーザアカウントが、同時にコンピュータにログオンできます。

リモートデスクトッププロトコル (RDP) セッションのサポート。ユーザは、SecurID を使用して RDP セッションにログオンできるようになりました。

構成の変更。RSA Authentication Agent 6.1、6.4、7.0 ユーザインターフェースで設定可能であった構成のいくつかが、グループポリシーオブジェクトテンプレートでのみ設定できるようになりました。これらの変更の詳細については、以下を参照してください。

- 『*RSA Authentication Manager 7.1 for Microsoft Windows インストールおよび管理ガイド*』の第 1 章「概要」
- 『*RSA Authentication Agent 7.1 for Microsoft Windows グループポリシーオブジェクトテンプレートガイド*』の第 2 章「ユーザ設定と Agent サポート」

製品使用時の推奨事項

本セクションでは、Authentication Agent を正しくお使いいただくための推奨事項について説明します。

- 「Server」および「Workstation」の Windows サービスは常に実行している必要があります。サービスが中断された場合には、コンピュータを再起動してプロセスを再起動するようにユーザに指示します。
- [New PIN] または [Next Tokencode] モードで作業しているユーザは、これらのダイアログの操作を速やかに完了する必要があります。[New PIN] または [Next Tokencode] ダイアログがタイムアウトした場合には、CTRL+ALT+DEL を押して、もう一度やり直すようにユーザに指示してください。
- 『*インストールおよび管理ガイド*』で指示されているようにプッシュ型のインストールを実行します。たとえば、Microsoft Systems Management Server (SMS) を使用して、MSI をユーザのコンピュータに自動インストールします。Remote Desktop セッションを使用したプッシュ操作は、推奨されません。
- 自動登録を使用している場合には、Authentication Manager サーバの Authentication Agent ホストレコードに代替 IP アドレスを追加しないでください。

RSA Authentication Agent for Web for IIS との相互運用性

RSA Authentication Agent 7.1 for Microsoft Windows および RSA Authentication Agent for Web for IIS は両方とも、RSA Authentication API を利用します。RSA Authentication Manager と通信するために、RSA Authentication API は設定ファイルとノードシークレットを必要とします。Authentication Agent for Windows および Authentication Agent for Web は、これらのファイルを別の場所に保存しています。同一マシン上にインストールされた両方の Authentication Agent が Authentication Manager と通信できるように、別々の場所に保存されるこれらのファイルが常に同じ内容である必要があります。

設定ファイルとノードシークレットは、以下の場所に保存されています。

- Authentication Agent for Windows のインストール環境 :**<<Program Files>>¥Common Files¥RSA Shared¥Auth Data**
- Authentication Agent for Web のインストール環境 :**<<Windows>>¥System 32**

ノードシークレットロードユーティリティを使用している場合、両方の場所にノードシークレットをロードできます。Authentication Agent for Windows または Authentication Agent for Web のいずれかを使用してテスト認証を行い、ノードシークレットが自動生成される場合、もう一方の Authentication Agent の保存場所にそのノードシークレットをコピーする必要があります。

Authentication Agent for Windows および Authentication Agent for Web は、以下の Windows レジストリ設定の下にあるレジストリキーを共有します。
HKEY_LOCAL_MACHINE¥SOFTWARE¥SDTI¥ACECLIENT。この場所に保存される設定は、トレースログおよび IP アドレスの上書きの制御に使用されます。両方の Authentication Agent は、同じレジストリの場所を使用し、デフォルトのレジストリ設定は、最初にインストールされる製品によってインストールされます。これらの設定は共有されるため、一方の Authentication Agent で設定が変更されると、その変更はもう一方の Authentication Agent にも自動的に反映されます。たとえば、Authentication Agent for Windows の RSA Control Center を使用して IP アドレスの上書きを変更する場合、Authentication Agent for Web の Control Panel アプリケーションを使用して変更する必要はありません。また、共有される設定は、いずれかの Authentication Agent をアンインストールしても削除されません。両方の Authentication Agent をアンインストールする場合は、レジストリ設定を手動で削除する必要があります。

次の手順で、1 台のコンピュータで Authentication Agent for Windows および Authentication Agent for Web の両方をインストールおよび使用すること推奨します。

始める前に

ノードシークレットの形式が最近変更されました。Authentication Agent for Windows では、新しい形式のノードシークレットを使用します。相互運用性のため、インストールした Authentication Agent for Web のバージョンでも、新しい形式を使用する必要があります。Authentication Agent for Web のバージョン 7.1 では、新しいノードシークレットの形式が使用されます。バージョン 7.1 より前の Authentication Agent for Web をインストールしている場合には、**RSA カスタマサポート**に問い合わせて新しいノードシークレットの形式をサポートするための適切なパッチを入手してください。

Authentication Agent for Windows と Authentication Agent for Web の相互運用性を確保するには、次の手順を実行します。

1. Authentication Agent for Web をインストールし、テスト認証を実行します。詳細は、『*RSA Authentication Agent for Web for IIS Installation and Configuration Guide*』を参照してください。
2. Authentication Agent for Windows をインストールします。詳細は、『*RSA Authentication Agent for Microsoft Windows インストールおよび管理ガイド*』を参照してください。

   重要：次の手順を完了するまでは、Authentication Agent for Windows でテスト認証を試行しないでください。

3. コマンドプロンプトを開いて、/O オプションを指定して **XCOPY** コマンドを実行し、**<<Windows>>¥System32** から **<<Program Files>>¥Common Files¥RSA Shared¥Auth Data** にノードシークレットをコピーします。/O オプションによって、ファイルの所有権とアクセスコントロールリスト (ACL) の情報もコピーされます。次のように入力します。

   XCOPY C:¥Windows¥System32¥securid "C:¥Program Files¥Common Files¥RSA Shared¥Auth Data¥" /O

   重要：COPY コマンドや Windows Explorer を使用して、ノードシークレットファイルをコピーしないでください。ノードシークレットは機密性が高いため、所有権と ACL 情報をコピーする必要があります。

4. Authentication Agent for Windows のテスト認証を実行します。詳細は、『*RSA Authentication Agent for Microsoft Windows インストールおよび管理ガイド*』を参照してください。

Secured by RSA Certified Partner Solution 製品との相互運用性

RSA Authentication Agent 7.1 for Microsoft Windows を Secured By RSA Certified Partner Solution 製品と使用する場合には、**Secured by RSA Certified Partner Solutions** のサイトにアクセスしてください。このサイトには、実装ガイドおよび使用法や互換性に関する情報が掲載されています。

パッケージ内容

RSA Authentication Agent は、**RSA Authentication Agents for Microsoft Windows** から入手できます。

RSA Authentication Agent 7.1 のフォルダには、次のフォルダおよびファイルが含まれます。

フォルダ / ファイル	説明
Configuration Wizard	このフォルダには設定ウィザードの実行ファイル (**ConfigWizard.exe**) が含まれています。設定ウィザードは、インストーラをカスタマイズしたり、複数コンピュータにデプロイする場合に使用できます。
x86 および x64	これらのフォルダには、RSA Authentication Agent 7.1 を 32 ビットおよび 64 ビットのコンピュータにローカルでインストールするための Windows インストーラパッケージが含まれています。

フォルダ / ファイル	説明
Language Packs	このフォルダには英語版の製品をインストールした後にインストールする日本語言語パックが含まれています。日本語版のオペレーティングシステムを使用し、標準の英語版製品をインストールした後に、日本語言語パックをインストールした場合は、ユーザインタフェースおよびヘルプが日本語で表示されます。詳細については、『*インストールおよび管理ガイド*』を参照してください。
Licenses	このフォルダには、RSA の使用許諾契約 (RSA_License_Agreement.doc) が含まれています。
Policy Templates	このフォルダには、認証設定を管理するためのグループポリシーオブジェクト (GPO) の管理テンプレートが含まれています。
Node Secret Load Utility	このフォルダには、RSA SecurID 認証を実行する前に Authentication Manager サーバから Authentication Agent コンピュータにノードシークレットを安全にコピーするためのノードシークレットロードユーティリティ (**agent_nsload.exe**) が含まれています。 注 : ノードシークレットロードユーティリティは、ノードシークレットを確立するためには必須ではありません。詳細については、『*インストールおよび管理ガイド*』を参照してください。
Documentation	このフォルダには製品ドキュメントが含まれています。詳細については、次のセクション「ドキュメントとアプリケーションヘルプ」を参照してください。

ドキュメントとアプリケーションヘルプ

製品ドキュメントは、次の Web サイトから入手できます。

- **RSAAuthentication Agent for Microsoft Windows**
- **RSA SecurCare Online**。RSA Authentication Agent 7.1 for Microsoft Windows の製品ドキュメントのページに、各ドキュメントのファイルへのリンクが掲載されています。

次のドキュメントは、RSA Authentication Agent 7.1 パッケージに含まれており、**¥documentation** ディレクトリに保存されています。

ドキュメント

タイトル	ファイル名
RSA Authentication Agent 7.1 for Microsoft Windows インストールおよび管理ガイド	**auth_agent71_install_admin_guide.pdf**
RSA Authentication Agent 7.1 for Microsoft Windows グループポリシーオブジェクトテンプレートガイド	**auth_agent71_gpo_template_guide.pdf**

RSA Authentication Agent 7.1 for Microsoft Windows には次のヘルプがインストールされます。

アプリケーションヘルプ

タイトル	ファイル名
RSA Authentication Agent (SecurID) ヘルプ	RSA Control Center からこのヘルプにアクセスできます。
(日本語) RSA Authentication Agent (SecurID) ヘルプ	RSA Control Center からこのヘルプにアクセスできます。日本語版のオペレーティングシステムを使用し、標準の英語版製品をインストールした後に、日本語言語パックをインストールした場合は、ユーザインタフェースおよびヘルプが日本語で表示されます。

既知の問題

本セクションでは、RSA Authentication Agent 7.1 for Microsoft Windows の既知の問題と回避策について説明します。

RSA SecurID 800 トークンの USB 接続が断続的になる。
トラッキング番号：AAWIN-1954、AAWIN-1859
問題：SecurID 800 トークンの背面のシリアルコードの下に製造コードが記載されています。製造コードの先頭文字は、A、C、または D であり、通常はその後に数値が続きます。USB 接続が断続的になる問題は、製造コードが A、A2、A8、および A9 のトークンで発生する可能性があります。また、Windows Vista コンピュータがスリープモードから復帰するときにも発生する可能性があります。
回避策：SecurID 800 を取り外して、再度挿入します。SecurID 800 は、USB アダプタやエクステンダではなく、コンピュータの USB ポートに必ず直接接続してください。SecurID 800 を USB ポートに接続しなくても、PIN とトークンコードを手で入力して認証することもできます。

RSA Control Center のアイコンが接続されている RSA SecurID 800 のステータスを正しく表示しない場合がある。
トラッキング番号：AAWIN-1953
問題：RSA Control Center アイコンの右上に青のプラス記号が表示されていれば、USB ポートに接続されているトークンを RSA Control Center が認識していることを表します。64 ビット コンピュータに RSA Authentication Client と RSA Authentication Agent の両方がインストールされた環境で、RSA Authentication Client をアンインストールすると、ユーザがトークンを接続してもアイコンに青のプラス記号が表示されない場合があります。
回避策：RSA Authentication Client を 64 ビットコンピュータでアンインストールして再インストールする場合には、RSA Authentication Agent のインストールを修復する必要があります。

64 ビットの Vista を使用しているユーザが、システムをロック解除するときに不正な PIN を入力した場合、[その他のユーザ] タイルを使用してログオンする必要がある場合がある。
トラッキング番号：AAWIN-1948
問題：[Unlock with SecurID PIN] 機能を有効にしている 64 ビットの Vista コンピュータにログオンし、コンピュータをロック解除するときに不正な PIN を入力した場合、通常使用している認証タイルを使用してログオンできなくなる場合があります。
回避策：[その他のユーザ] タイルを使用してログオンしてください。

Windows XP のローカル管理者が、リモートユーザを強制的にログオフできない場合がある。
トラッキング番号：AAWIN-1947
問題：Windows XP コンピュータを複数のリモートユーザが利用しており、[Unlock with an RSA SecurID PIN] 機能が有効になっている場合に、リモートユーザが接続されている RSA SecurID 800 を使用してシステムをロックした場合、ローカルの管理者は、リモートユーザを強制的にログオフできなくなる場合があります。
回避策：複数のリモートユーザが利用する Windows XP コンピュータでは [Unlock with SecurID PIN] 機能を有効にしないでください。

トレースのレベルやトレースファイルを書き込む場所を変更する場合には、コンピュータを再起動する必要がある。
トラッキング番号：AAWIN-1933
問題：トラブルシューティング目的で、トレースログファイルを書き込むように RSA Control Center で設定できます。通常は、RSA のカスタマサポートから指示されない限り、トレースを有効にすることはありません。たとえば、トレースのレベルを verbose (詳細) から error (エラー) に変更した場合、この変更を有効にするためにコンピュータを再起動する必要があります。また、トレースファイルを書き込む場所を変更する場合も、コンピュータを再起動する必要があります。
回避策：トレースのレベルやトレースファイルを書き込む場所を変更する場合には、コンピュータを再起動してください。詳細については、『*RSA Authentication Agent 7.1 for Microsoft Windows インストールおよび管理ガイド*』の「トレースの有効化」を参照してください。

ローカル管理者が Windows のコントロール パネルからインストールされている Authentication Agent を変更すると、致命的なエラーが発生する可能性がある。
トラッキング番号：AAWIN-1909
問題：サイレントモードで Authentication Agent がインストールされた場合、ローカル管理者がコントロール パネルからインストール済みの Authentication Agent を変更しようとすると、致命的なエラーが発生する場合があります。
回避策：新しい MSI パッケージを作成し、次のコマンドを使用してインストールします。
msiexec /qn /i "RSA Authentication Agent.msi" ADDLOCAL=ALL REINSTALLMODE=vomus REINSTALL=LAC
MSI パッケージの作成とデプロイの手順については、『*RSA Authentication Agent 7.1 for Microsoft Windows インストールおよび管理ガイド*』の第 3 章 「RSA Authentication Agent のインストール」を参照してください。

自動登録機能がインストールされていないマシンでユーザが初めて認証した後に、RSA Control Center に利用可能なオフライン日数が不正に表示される。
トラッキング番号：AAWIN-1894
問題：[オフライン残り日数] フィールドには、利用可能なオフライン日数が数字および棒グラフで表示されます。自動登録機能がインストールされていないマシンでユーザが初めて認証した後に、棒グラフにはオフライン日数がゼロと不正に表示されます。数値は正しく表示されます。この問題は認証には影響はありません。
回避策：棒グラフに利用可能なオフライン日数を正しく表示するには、ユーザに再認証するように指示してください。再認証すると、RSA Control Center に利用可能なオフライン日数が正しく表示されます。

固定パスコードが割り当てられているユーザが、RSA Control Center からオフライン日数を更新できない。
トラッキング番号：AAWIN-1855
問題：固定パスコードが割り当てられているユーザは、RSA Control Center からオフライン日数を更新できません。
解決策：オフライン認証を必要とするユーザに固定パスコードを発行しないでください。

Authentication Agent の IP アドレス変更後に認証すると、RSA Authentication Manager 7.1 ログに無効なエラーメッセージが記録される。
トラッキング番号：AAWIN-1839
問題：自動登録が有効な Authentication Agent マシンの IP アドレスが変更された後に、その Authentication Agent からテスト認証を実行すると、RSA Authentication Manager 7.1 にエラーメッセージが不正に記録されます。「Offline Authentication Data Download Failed (オフライン認証データのダウンロードに失敗しました)」というエラーメッセージが記録されます。
回避策：このメッセージは無視してください。

インターネットに接続していないコンピュータに Authentication Agent をインストールする前に、信頼されるルート証明書に thawte Primary Root CA を手動でインストールする必要がある。
トラッキング番号：AAWIN-1801
問題：Authentication Agent には、信頼されるルート証明書として *thawte Primary Root CA* が必要です。コンピュータがインターネットに接続している場合には、この証明書は自動的に登録されます。
回避策：インターネットに接続していないコンピュータに Authentication Agent をインストールする前に、信頼されるルート証明書として *thawte Primary Root CA* をコンピュータアカウントにインストールする必要がある場合があります。詳細や手順については、**Microsoft サポート技術情報 (KB931125)** を参照してください。

ユーザが Windows パスワードを変更した場合、RSA SecurID PIN を使用してロック解除するには、一旦コンピュータをログオフしてから再認証する必要ある場合がある。
トラッキング番号：AAWIN-1791
問題：管理者は、認証済みのユーザがパスコードの代わりに PIN を使用してコンピュータのロック解除することを許可できます。管理者は、このオプションをグループポリシで設定できます。ユーザがログインした後に、Windows パスワードを変更し、その後にコンピュータをロックした場合、ユーザは PIN を使用してコンピュータをロック解除できなくなります。
回避策：PIN でコンピュータのロックを解除する機能を再度使えるようにするには、ユーザはコンピュータをログオフしてから、パスコードを使用して再認証する必要があります。

RSA Authentication Agent と RSA Authentication Client をインストールしてから、Authentication Client を削除すると、Cisco GINA チェーンが破損する。
トラッキング番号：AAWIN-1770
問題：Cisco VPN クライアント、RSA Authentication Agent、および RSA Authentication Client をインストールした場合、システムを再起動すると Cisco VPN 接続と RSA GINA が正しく表示されます。次に、RSA Authentication Client を削除して、システムを再起動すると、Microsoft GINA のみが表示されます。RSA Authentication Client を削除すると、Cisco GINA が破損し、Cisco GINA のレジストリ設定が不正にリセットされます。Authentication Client を削除すると、サードパーティの GINA チェーンのサポートも削除されるために、この問題が発生します。この問題は、Windows XP Pro SP3 および Windows Server 2003 のみで発生します。
回避策：Cisco GINA チェーンを元に戻すには、Windows レジストリ設定を手動で編集してから、変更が有効になるようにシステムを再起動する必要があります。次のようにレジストリ設定を編集します。

- **HKEY_LOCAL_MACHINE¥Cisco Systems¥VPN Client** の下で、**PreviousGinaPath** を **MSGina.dll** に設定します。
- **HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Winlogon** の下で、**GinaDLL** を **CSGina.dll** に設定します。

リモートデスクトップ接続から Authentication Agent をインストールすると、RSA SecurID のタイルが表示されない
トラッキング番号：AAWIN-1688
問題：リモートデスクトップ接続から Authentication Agent をインストールすると、ログオンしているユーザには、RSA SecurID のタイルではなく Microsoft パスワードのタイルが表示されます。
回避策：RSA SecurID のタイルを表示するには、マシンを再起動する必要があります。

接続した SecurID 800 を使用してリモートデスクトップ接続でログオンするユーザに PIN の入力が 2 回要求される。
トラッキング番号：AAWIN-1625
問題：接続した SecurID 800 を使用してリモートデスクトップ接続でログオンするユーザに PIN の入力が 2 回要求されます。この問題は、Windows XP および Windows Server 2003 で発生します。
回避策：PIN の入力を最初に要求されたら、入力する必要があります。再度要求されたら、デバイスのトークンコードが変更されるのを待ってから、PIN を入力する必要があります。

[新しい RSA SecurID PIN の設定] ダイアログボックスが、UAC (ユーザアカウント制御) ダイアログボックスの後ろに開く。
トラッキング番号：AAWIN-307
問題：ユーザがローカルの認証情報でコンピュータにログオンし、その後管理者権限が必要なアプリケーションにアクセスする必要が生じる場合があります。この時に使用する管理者アカウントが RSA SecurID パスコード認証の対象となっており、SecurID PIN をまだ作成していない場合、Authentication Agent は SecurID PIN の作成を指示するダイアログボックスを表示します。ただし、この [新しい RSA SecurID PIN の設定] ダイアログボックスが、Windows の UAC ダイアログボックスの後ろに開くため、ユーザは [新しい RSA SecurID PIN の設定] ダイアログボックスのフィールドにアクセスできません。
回避策：[新しい RSA SecurID PIN の設定] ダイアログボックスを Windows UAC ログオンダイアログボックスの後ろから移動します。これにより、選択項目やフィールドにアクセスして、PIN を設定できるようになります。

元のインストールディレクトリ以外のディレクトリに Authentication Agent を再インストールできない。
トラッキング番号：AAWIN-408
問題：設定ウィザード (**ConfigWizard.exe**) を使用して、独自の MSI パッケージを作成して、複数の環境にデプロイできます。その後、製品を再インストールする必要が生じた場合に、別のインストールパッケージを作成し、別のディレクトリにインストールしようとすると、インストールが失敗します。
回避策：Authentication Agent を再インストールする必要がある場合は、元のディレクトリと同じディレクトリにインストールしてください。インストールパッケージの名前には、製品のデフォルトの名前を使用するか、別の名前を指定できます。しかし、インストールパッケージに別の名前を指定した場合は、元のインストールパッケージがあったのと同じパスから、インストールパッケージを実行する必要があります。

初めてログオンしたコンピュータでインストールを実行すると、エラーメッセージが表示される
トラッキング番号：AAWIN-359
問題：管理者または標準ユーザとしてそれまでに一度もログオンしたことがないコンピュータで、RSA Authentication Agent をインストールしようとすると、［**OK**］をクリックして終了するように指示するアプリケーションエラーメッセージが表示されます。インストールを続行できません。
回避策：[**OK**] をクリックして、エラーメッセージを閉じてください。コンピュータを再起動し、再度ログオンします。これでコンピュータに RSA Authentication Agent をインストールできます。

RSA Authentication Agent 7.1 for Microsoft Windows の修復時または削除時に、「不明なプログラム」メッセージが UAC (ユーザアカウント制御) ダイアログボックスに表示される。
トラッキング番号：AAWIN-398
問題：RSA Authentication Agent を修復または削除する必要がある場合に、Windows Vista コンピュータで UAC (ユーザアカウント制御) を有効にすると、不明なプログラムがコンピュータにアクセスしようとしていることを表すメッセージが表示されます。このメッセージは、インストールプログラムでデジタル署名付きの Microsoft Windows インストーラパッケージが使用されている場合に表示されます。
回避策：UAC ダイアログボックスの [**許可 (Allow)**] をクリックして、修復または削除を続行してください。

ネットワークレベル認証を使用するリモートコンピュータにアクセスすると、複数の認証画面が表示される。
トラッキング番号：AAWIN-564
問題：リモート デスクトップ接続 6.1 は、Windows NLA (ネットワークレベル認証) を実装しています。リモートコンピュータに接続しようとした場合に、この機能が有効になっていると、リモート接続を確立する前に、認証画面が表示されます。NLA が有効な場合に、RSA SecurID 認証プロバイダを使用するリモートコンピュータに接続すると、リモートデスクトップ接続が完了する前に、2 つの認証画面が表示されます。1 つの認証画面はローカルコンピュータから開き、もう 1 つの認証画面はリモートコンピュータから開きます。これは、サードパーティの認証プロバイダを使用する場合の Microsoft のネットワークレベル認証の実装方法の制限によるものです。それぞれの認証画面にアカウント情報を入力し、認証が成功すれば、リモートコンピュータにアクセスできます。

注 : ネットワークレベル認証は、Windows Vista またはそれ以降のオペレーティングシステムの場合、デフォルトで有効です。Windows XP SP3 の場合、手動で有効にできます。ネットワークレベル認証の詳細については、Microsoft の Web サイトにアクセスしてください。

---

3 つのトークンを所有するユーザが最初のトークンで認証した後にログオフし、別のトークンで再ログオンすると、認証は成功するが、オフラインデータがダウンロードされず、RSA Authentication Agent Offline Local サービスが停止する。
トラッキング番号：AAWIN-650
問題：RSA Authentication Manager 7.1 SP4 でオフライン認証を有効にした場合に、ユーザに 3 つのトークンを割り当てると、最初のトークンを使用したユーザ認証とオフラインデータのダウンロードは成功します。しかし、ユーザがログオフし、他のトークンで認証を行うと、ユーザの認証は成功しますが、オフラインデータがダウンロードされず、RSA Authentication Agent Offline Local サービスが停止します。この問題は、RSA Authentication Manager 7.1 SP4 のみで発生します。
回避策：オフラインで認証する必要があるユーザに 3 つ目のトークンを割り当てないでください。

[クリア] をクリックしてオフラインデータをクリアしても、[クリア] ボタンが正しい表示に変更されない。
トラッキング番号：AAWIN-650
問題：RSA Security Center で [オフライン データ] セクションの [クリア] ボタンをクリックしても、[クリア] ボタンの表示が、オフラインデータがクリアされたことを表す表示に変更されません。ただし、オフラインデータはクリアされます。
回避策：回避策は不要です。

オフライン認証ポリシーで、ユーザに緊急コードの入力を要求するまでのオフライン認証の失敗許容回数を設定しても、Authentication Agent for Microsoft Windows ではこのポリシーが正しく処理されない。
トラッキング番号：AAWIN-635
問題：オフライン認証の失敗回数が一定数に達した場合に、緊急コードを入力することをユーザに要求するオフライン認証ポリシーを設定している場合、実際にはこのポリシーで設定されている半分の回数で、ユーザに緊急コードの入力が要求されます。
回避策：オフライン認証ポリシーに設定するオフライン認証の失敗許容回数を、実際の回数の 2 倍に設定してください。

サポートおよびサービス

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
RSA Secured Partner Solutions Directory	**www.rsasecured.com**

商標について

2012 年 2 月

日本語版初版 : 2012 年 6 月

P/N : JS-AGT-7104