RSA® SecurID® Software Token 2.2 for Android クイック スタート

はじめに

RSA SecurID Software Token 2.2 for Android をご利用いただき、ありがとうございます。この製品は、Android スマートフォン / タブレットを RSA SecurID 認証デバイスとして機能させるための認証ソフトウェアです。

アプリケーションを使用するには、ソフトウェア トークンをインポートする必要があります。アプリケーションでは、60 秒または 30 秒ごとに新しいトークンコードが生成されます。現在のトークンコードを使用して、SecurID で保護されているリソース、たとえば、企業 VPN にアクセスします。ソフトウェア トークンが SecurID PIN を必要とする場合、PIN とトークンコードを組み合わせたパスコードを使用します。トークンコードまたはパスコードが OTP（ワン タイム パスワード）です。

このドキュメントでは、Token アプリケーションのインストール方法、ソフトウェア トークンのインポート方法と使用方法について説明します。最大 10 個のソフトウェア トークンをデバイスにインポートできます。各トークンは 1 つずつインポートする必要があります。

Token アプリケーションのインストール

Google Play（Play ストア）からアプリケーション（無料）をインストールします。

アプリケーションをインストールするには、以下の手順に従います。

1. デバイスがインターネットに接続されていることを確認します。
2. アプリケーションの一覧で、**Google Play** または **Play ストア**のアイコンをタップします。
3. ［**検索**］をタップしてキーワード「**RSA SecurID**」を入力します。
4. ［**RSA SecurID Software Token**］を選択します。
5. ［**インストール**］をタップします。
   アプリケーションに必要になる権限が、デバイスに一覧表示されます。
6. ［**OK**］をタップするとダウンロードが開始されます。
   ステータス アイコンに、ダウンロードの進行状況が表示されます。ダウンロードが完了すると、通知アイコンがステータス バーに表示されます。［通知］ウィンドウにもアプリケーションが表示されます。

Token アプリケーションの起動

アプリケーションを起動するには、以下の手順に従います。

1. アプリケーションの一覧で、Token アイコンをタップします。
2. 使用許諾契約書を確認し、［**私は使用許諾契約書の条項に同意します**］を選択します。［**続行**］をタップします。

次のステップ

使用許諾契約書に同意した後、ソフトウェア トークンのインポートが可能になります。

- 管理者がデバイス ID の確認を求めてきた場合は、セクション？デバイス ID のメール送信？に進んでください。
- 管理者がデバイス ID の確認を求めずに、ソフトウェア トークンを送信してきた場合は、セクション？ソフトウェアトークンのインポート？に進んでください。

デバイス ID のメール送信

管理者は、トークンを送信する前に、デバイス ID の確認を求めてくることがあります。デバイス ID は、ソフトウェア トークンをデバイスにバインドして、ソフトウェア トークンが他のデバイスで使用できないようにします。デバイスのメール アカウントがセットアップされていることを確認します。管理者のメール アドレスを入手します。

デバイス ID をメールで送信するには、以下の手順に従います。

1. ようこそ画面で、［**デバイス ID**］をタップします。
2. 次のいずれかの操作を実行します。
   - ［**デバイス ID をメール**］をタップして、デバイス ID を本文に含んだメールを開きます。
   - ［**デバイス ID のコピー**］をタップして、デバイス ID をコピーします。
3. メール オプションを選択した場合は、管理者のメール アドレスを［**To:（宛先）**］フィールドに入力して、メールを送信します。
4. ？ソフトウェアトークンのインポート？に進みます

追加トークンのためのデバイス ID のメール送信

追加のソフトウェア トークンをリクエストし、管理者がこれらをバインドするためのデバイス ID を求めてきた場合、ユーザーはリクエストのたびにデバイス ID を送信する必要があります。デバイス ID は、［情報］画面に表示されます。

追加トークンのためにデバイス ID をメールで送信するには、以下の手順に従います。

1. ［**情報**］をタップします。
2. 次のいずれかの操作を実行します。
   - ［**デバイス ID**］＞［**デバイス ID をメール**］をタップして、デバイス ID を本文に含んだメールを開きます。
   - ［**デバイス ID**］＞［**デバイス ID のコピー**］をタップして、デバイス ID をコピーします。
3. メール オプションを選択した場合は、管理者のメール アドレスを［**To:（宛先）**］フィールドに入力して、メールを送信します。
4. ？ソフトウェアトークンのインポート？に進みます

RSA® SecurID® Software Token 2.2 for Android クイック スタート

ソフトウェアトークンのインポート

ユーザーは、添付ファイルまたは URL リンクの形式でメールによってソフトウェア トークンを受信します。あるいは、管理者は、ユーザーが QR コード？をスキャンするよう設定する場合もあります。また管理者の設定によっては、プロンプトが表示され、次のいずれかを入力する必要があります。

- パスワード
- アクティベーション コード

トークンのインポートを開始する前に、パスワードまたはアクティベーション コードが手元にあることを確認します。

受信したメールの指示に従って、次のいずれかのインポート手順を実施します。

メールの添付ファイル

メールの添付ファイルからソフトウェアトークンをインポートするには、以下の手順に従います。

1. デバイスのメールアプリケーションで、添付ファイル（ファイル拡張子は .sdtid）が挿入されたメールを開きます。
2. 添付ファイルをタップします。
3. プロンプトが表示されたら、パスワードを入力します。［**OK**］をタップします。
4. セキュリティ上の理由により、メールは削除してください。

URL リンク

メール内の URL リンクからソフトウェア トークンをインポートするには、以下の手順に従います。

1. デバイスのメールアプリケーションで、URL リンクが記載されたメッセージを開きます。
2. URL リンクをタップします。
3. プロンプトとして［アプリケーションを選択］が表示されたら、［**Token**］をタップします。
4. プロンプトが表示されたら、アクティベーション コードまたはパスワードを入力します。［**OK**］をタップします。
5. サーバ証明書の受け入れを承諾するように指示されたら、［**承諾**］をタップします。
6. セキュリティ上の理由により、メールは削除してください。

インポート URL オプション

URL リンクをタップしてトークンをインポートできない場合は、次の手動の手順を実施してください。

［インポート URL］オプションを使用してソフトウェア トークンをインポートするには、以下の手順に従います。

1. デバイスのメールアプリケーションで、URL リンクが記載されたメッセージを開きます。
2. URL リンクは、**http://127.0.0.1/securid** で始まります。リンクをホールドして、［コピー］オプションを選択します。
3. Token アプリに移動します。ようこそ画面で、［**トークンのインポート**］＞［**インポート URL**］をタップします。
4. テキスト フィールドをホールドして、［**貼り付け**］をタップします。
5. プロンプトが表示されたら、アクティベーション コードまたはパスワードを入力して、Enter キーをタップします。
6. サーバ証明書の受け入れを承諾するように指示されたら、［**承諾**］をタップします。
7. セキュリティ上の理由により、メールは削除してください。

注： 追加のトークンを手動でインポートするには、［**トークン リスト**］をタップしてから［**インポート URL**］をタップします。

QR コードのスキャン

管理者の指示に従ってトークン データを含む QR コードにアクセスし、次の手順に従って QR コードをキャプチャします。

QR コードをスキャンしてソフトウェア トークンをインポートするには、以下の手順に従います。

1. Token アプリに移動します。ようこそ画面で、［**トークンのインポート**］＞［**QR コードのスキャン**］をタップします。
2. QR コードの全体が明瞭に表示されていることを確認します。カメラを QR コードに向けてコードをキャプチャします。
3. プロンプトが表示されたら、アクティベーション コードまたはパスワードを入力して、［**OK**］をタップします。

注： QR コードをスキャンして追加のトークンをインポートするには、［**トークン リスト**］をタップしてから［**QR コードのスキャン**］をタップします。

PIN の設定

注： トークンが PIN を必要としない場合は、？保護されたリソースへの認証？に進みます。

開始する前に

インポートしたトークンによって、Token アプリケーションの起動時に、［PIN の入力］画面または［トークンコード］画面が表示されます。

次のいずれかの操作を実行します。

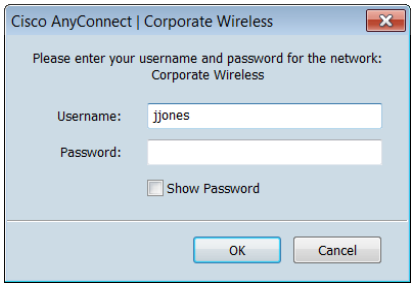
- ［PIN の入力］画面が表示されたら、セクション ?PIN の設定（PIN の入力画面）？に進んでください。
- ［トークンコード］画面が表示されたら、?PIN の設定（トークンコード画面）？に進んでください。

RSA® SecurID® Software Token 2.2 for Android
クイック スタート

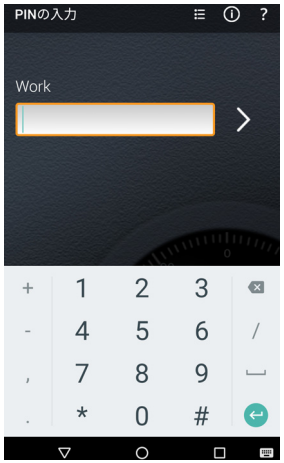
PIN の設定（PIN の入力画面）

［PIN の入力］画面から PIN を設定するには、以下の手順に従います（VPN の例）。

1. ユーザーの PC（またはユーザーのデバイス）から企業 VPN に接続します。
2. ユーザー名を入力して、ログオン画面を開いたままにします。



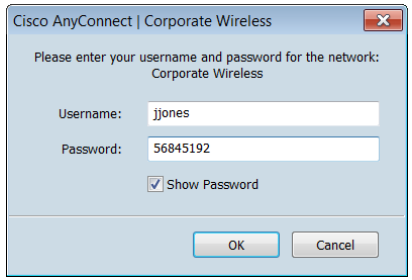
3. デバイスで Token アプリケーションを開始します。
4. ［PIN の入力］画面で **Enter** キーをタップするか、左にスワイプします。



デバイスにトークンコードが表示されます。

5. VPN ログオン画面で［**パスコード**］または［パスワード］フィールドにトークンコードを入力します。PIN を作成するダイアログが表示されます。PIN は必ず 4 桁から 8 桁までの数字を指定し、先頭をゼロ以外にします。
6. 新しい PIN を入力し、確認のため再入力します。VPN にパスコード プロンプトが表示されます。
7. デバイスで［**戻る**］ボタンをタップするか、右にスワイプして、［PIN の入力］画面に戻ります。
8. PIN を入力して、**Enter** キーをタップするか、左にスワイプして、パスコードを表示します。

9. VPN ログオン画面でパスコードを入力して［**OK**］をクリックします。

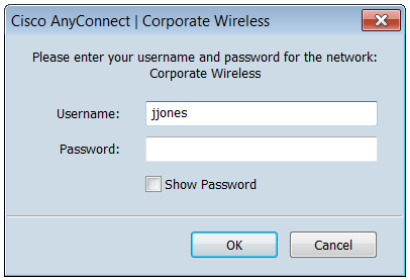


注： デバイス上の VPN クライアントを使用する場合は、アプリケーション メニューで［**コピー**］をタップしてパスコードをコピーし、このパスコードを VPN ログオン画面にペーストすることができます。

PIN の設定（トークンコード画面）

［トークンコード］画面から PIN を設定するには、以下の手順に従います（VPN の例）。

1. ユーザーの PC（またはユーザーのデバイス）から企業 VPN に接続します。
2. ユーザー名を入力して、ログオン画面を開いたままにします。



3. デバイスで Token アプリケーションを起動して、トークンコードを表示します。

4. VPN ログオン画面で［**パスコード**］または［パスワード］フィールドにトークンコードを入力します。PIN を作成するダイアログが表示されます。PIN は必ず 4 文字から 8 文字までの文字を指定し、先頭をゼロ以外にします。
5. 新しい PIN を入力し、確認のため再入力します。VPN にパスコード プロンプトが表示されます。
6. デバイスで［**ネクスト コード**］をタップします。
7. VPN ログオン画面に戻ります。［**パスコード**］または［パスワード］フィールドに PIN を入力します（この例では、PIN は 13867254 です）。PIN の右側にトークンコードを入力します。［**OK**］をクリックします。

保護されたリソースへの認証

次の手順に従って、コンピュータまたはデバイスから保護されたリソースへの認証を実行します。次の例では、コンピュータから保護されたリソースにアクセスします。

トークンの選択（必要な場合）

複数のソフトウェア トークンがあり、アクティブなトークンとは異なるトークンを使用する必要がある場合は、認証プロセスを開始する前に目的のトークンを選択します。

異なるトークンを選択するには、以下の手順に従います。

1. デバイスで Token アプリケーションを起動します。
2. ［**トークン リスト**］を選択します。
3. 目的のトークンの名前をタップします。これにより、トークンはアクティブ化されます。

認証

認証するには、次の手順に従います（VPN の例）。

1. 企業 VPN に接続します。
2. ユーザー名を入力して、ログオン画面を開いたままにします。
3. デバイスで Token アプリケーションを起動します。
4. 次のいずれかの操作を実行します。
   - ［PIN の入力］画面が表示されたら、PIN を入力して **Enter** キーをタップします。デバイスにパスコードが表示されます。VPN の［**パスコード**］（または［**パスワード**］）フィールドにパスコードを入力します。
   - トークンが PIN を必要とする場合に、Token アプリケーションに［トークンコード］画面が表示される場合、VPN の［**パスコード**］（または［**パスワード**］）フィールドに PIN を入力し、トークンコードを PIN の右側に入力します。
   - トークンが PIN を必要としない場合は、VPN の［**パスコード**］（または［**パスワード**］）フィールドにトークンコードを入力します。

ネクスト コードでの認証

ワン タイム パスワードを入力した後に、認証の完了のために、ネクスト コード（トークンコードまたはパスコード）の入力を求めるプロンプトが表示されることがあります。不正なワン タイム パスワードを連続して何度も入力した場合など、このプロンプトは、さまざまな理由で表示されます。ネクスト コードを要求する目的は、トークンが引き続き正当な所有者に所持されていることを確認することです。

ネクスト コードで認証するには、以下の手順に従います。

1. ネクスト コードを求めるプロンプトが表示されたら、デバイスの Token アプリケーションに戻ります。
2. ［**ネクスト コード**］をタップします。
3. 保護されたリソースの画面で、表示されたコードを入力します。

© 2010-2016 EMC Corporation. All Rights Reserved.
改訂：2016 年 11 月

本書に記載したその他の商品名およびサービスは各社の商標または登録商標です。