

RSA SecurID トークンによる認証

管理者へのメモ：この認証手順は、エンド ユーザに渡す前に必要に応じて変更してください。RSA SecurID Authenticator SID800 を導入する場合、エンド ユーザ向けの認証手順については、RSA Security Center のヘルプおよび『RSA Authenticator Utility 1.0 ユーザーズ クイック リファレンス』を参照してください。いずれも RSA Authenticator Utility 1.0 に同梱されています。

ここでは、ログイン時に使用する RSA SecurID トークンが割り当てられているものとして説明を進めています。

保護されたシステムにアクセスするには、次の 2 つの要素で構成される正しい RSA SecurID PASSCODE を入力する必要があります。

- ユーザの個人識別番号 (PIN)。PIN はユーザだけが知っているもので、記憶しておく必要があります。
- RSA SecurID トークンに現在表示されているトークンコード。トークンコードは、指定された間隔 (通常は 60 秒おき) で変化します。

操作の準備

次の情報を管理者に確認してください。

- システム生成 PIN を使用するのか、自分で PIN を作成する必要があるのか
- PIN の長さ (桁数)
- PIN が英数字なのか、数字だけなのか

New PIN モードの設定

二要素認証に必須の PIN がトークンに関連付けられていない場合は、New PIN モードになります。

New PIN モードのときに認証を受けるには

1. PASSCODE の指定が求められたら、RSA SecurID トークンに現在表示されているトークンコードを入力します。
2. 次のいずれかの操作を実行します。
 - システム生成 PIN を使用する場合：
表示される指示に従って、システム生成 PIN を使用することを指定します。PIN はメモに書き留めずに、記憶するようにしてください。
 - 自分で PIN を作成する場合：

- 自分で PIN を作成することを指定します。
 - 表示される指示に従って、PIN を入力します。
 - 確認のために PIN を再入力します。
3. 次のトークンコードが表示されるのを待ち、表示されたら、「スタンダード カード、キーホルダ、またはコンピュータに非接続の SID800 トークンによる認証」または「PINPAD による認証」の手順に従ってください。

スタンダード カード、キーホルダ、またはコンピュータに非接続の SID800 トークンによる認証

スタンダード カード、キーホルダ、またはコンピュータに非接続の SID800 トークンで認証を受けるには

PASSCODE の指定が求められたら、PIN に続けて、トークンに現在表示されているトークンコードを入力します。たとえば、PIN が 1234、現在のトークンコードが 800261 の場合は、「1234800261」と入力します。

メモ： RSA SecurID トークンコードを再利用することはできません。再びログインするには、次のトークンコードが表示されるまで待ってください。

PINPAD による認証

RSA SecurID PINPAD で認証を受けるには

1. PINPAD に PIN を入力し、PINPAD 下部の菱形 (◆) を押します。トークンに新しい PASSCODE が表示されます。トークンに新しい PASSCODE が表示されます。
2. 表示される指示に従って、PASSCODE を入力します。
3. PASSCODE が受け付けられたら、すぐに PINPAD の **P** を押してカードのメモリから PIN を消去します。

ネクスト トークンコード プロンプト

PASSCODE またはトークンコードを正しく入力しても、正当なトークン保有者であることを確認するために、次に表示されるトークンコード (ネクスト トークンコード) 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。

ネクスト トークンコード モードのときにスタンダード カード、キーホルダ、または SID800 トークンで認証を受けるには

トークンコードが変わるまで待ち、トークンコードが変わってから新しいトークンコードを入力します。トークンコードだけを入力してください。PIN を入力する必要はありません。

ネクスト トークンコードを正しく入力してもアクセスが許可されない場合は、システム管理者に連絡してください。

ネクスト トークンコード モードのときに PINPAD で認証を受けるには

1. PINPAD の **P** を押してカードのメモリから PIN を消去します。

2. トークンコードが変わるまで待ち、トークンコードが変わってから新しいトークンコードを入力します。トークンコードだけを入力してください。PIN を入力する必要はありません。

セキュリティ上の注意事項

不正なユーザに PIN を知られてしまったり、RSA SecurID トークンを盗まれてしまうと、不正なユーザが正当なユーザになりすます可能性があります。不正なユーザがとったアクションは、システムのセキュリティ ログ上では、正当なユーザがとったアクションとして扱われます。

ユーザ自身とシステム全体のセキュリティを保護するために、常に次の点に注意してください。

- 自分以外の人物に PIN を知られないようにしてください。
- 誰かに PIN を知られた可能性がある場合やトークンを紛失してしまった場合は、すみやかにセキュリティ管理者に報告してください。
- システムの標準ログオフ手順に従ってください。適切な手順でログオフしないと、システムに不正に侵入される危険があります。