第 17 章：SecurID の使用方法

次の表を使用すると、情報をすぐに見つけることができます。

トピック	参照先
はじめに	はじめに（P.488）
インストールの前提条件	インストールの前提条件（P.489）
ネットワーク デバイスへのアクセス	ネットワーク デバイスへのアクセス（P.490）
SecurID トークンの追加	SecurID ソフトウェア トークンの追加（P.492）
SecurID を使用した NCM へのログイン	SecurID を使用したログイン（P.493）
SecurID のトラブルシューティング	SecurID のトラブルシューティング（P.496）

はじめに

RSA SecurID® ソリューションは、組織を保護するために、許可されたユーザだけにネットワーク リソースへのアクセス権が付与されることを保証できるように設計されています。一般に、SecurID は 2 つの部分から構成される認証方式で、物理ハードウェア コンポーネントと同様、パスワードおよび PIN を必要とします。ハードウェア コンポーネントは、そのパスコードを 60 秒ごとに変更します。一部のデバイス メーカーでは、ルータやスイッチにこの認証システムを組み込んでいます。SecurID の動作の詳細については、SecurID のマニュアルを参照してください。

（注）外部認証に SecurID を使用するように NCM を設定した場合、NCM プロキシに接続するときにシングル サインオン機能はイネーブルになりません。SecurID パスコードは再利用できないため、SecurID クレデンシャルを使用してもう一度認証する必要があります。

NCM は、セキュリティ性の高い、次の 2 要素認証の SecurID をサポートします。

- NCM にログインするユーザの認証
- NCM 経由のネットワーク デバイスへのアクセス

次の表に、SecurID のデバイス アクセス サポートを示します。

NCM へのアクセス	接続方式	SecurID のサポート
Web ユーザ インターフェイス	HTTP	○
SSH/Telnet プロキシ	SSH	×
	Telnet	○
API	RMI	×

（注）デバイス アクセスに SecurID ソフトウェア トークンを使用する場合は、ACEServer 管理者が、ソフトウェア トークンが「New Pin」モードでないことを確認する必要があります。このモードになっていると、デバイスへのアクセスは失敗します。接続方式として SSH を使用している場合は、接続する前に SSH クライアントでの SSH 鍵認証をディセーブルにします。

インストールの前提条件

NCM へのユーザ認証を行うには、次のことを確認してください。

- RSA からハードウェア トークンまたはソフトウェア トークンを購入している。
- ACEServer 5.2 が動作していて、NCM サーバからアクセス可能である。
- ACEServer 上にユーザを作成している。
- ACEServer 上で、NCM が動作しているホストが Agent Host として追加されている。
- Agent Host 設定で、エージェント タイプが「UNIX Agent」である。
- ACEServer 上にユーザを作成した。
- ACEServer ユーザにソフトウェア トークンを割り当てた。
- ユーザが Agent Host から接続できるようにした。

NCM でデバイスにアクセスするには、次のことを確認してください。

- NCM が Windows サーバで動作している。
- RSA ソフトウェア トークンのソフトウェアがインストールされている。
- ACEServer 5.2 が動作していて、デバイスからアクセス可能である。
- RSA からソフトウェア トークンを取得している。
- RSA ソフトウェア トークン アプリケーションを使用して、SecurID トークンを NCM サーバにインポートしている。
- ユーザにソフトウェア トークンを割り当てている。
- ACEServer にライセンスを追加している。
- ACEServer 上にユーザを作成している。
- ユーザにソフトウェア トークンを割り当てている。
- ユーザがデバイスに接続できるようにしている。
- トークンの PIN を設定している。
- NCM で、SecurID ユーザに対応するユーザを追加した。
- ユーザごとに一意のトークンを使用するか、トークンのプールを使用するかを選択した。
- トークンのプールを使用する場合、トークン プール ユーザ名を割り当てた。
- ユーザにトークンを割り当てた。
- Device Access 変数の User SecurID が「Exec」または「Enable」に設定された状態で、パスワード規則（またはデバイス固有のパスワード）を追加した。

（注） Linux または Solaris システムで SecurID を使用している場合は、NCM への認証のみがサポートされます。

ネットワーク デバイスへのアクセス

SecurID を使用するデバイスに NCM を使用して接続する機能は、Windows システムだけでサポートされます。NCM からデバイスにアクセスする場合は、ソフトウェア トークンのソフトウェアおよびライセンスを RSA からダウンロードする必要があります。FOBS およびピンパッドなどのハードウェア トークン ライセンスは使用できません。

ソフトウェア トークンのソフトウェアは、RSA の Web サイトからダウンロードできます。NCM がインストールされている Windows システムに、必ずこのソフトウェアをインストールしてください。また、通常の SecurID メカニズムを使用して、この Windows システムにソフトウェア トークン ライセンスをインポートする必要もあります。

（注）ACEServer と NCM が動作しているサーバは、時刻が同期している必要があります。ソフトウェア トークンは、時刻の差を明確に感知します。2 つのサーバの時刻が 1 分以上ずれると、生成されたパスコードは失敗します。両方のサーバで NTP を使用すると、クロックを正確に保つことができます。

NCM は、SecurID を使用している場合は、デバイスへのアクセスを監視して、所定のトークンコードが 2 回使用されないようにします。これは、SecurID デバイス アクセスを使用する場合に、NCM でのアクティビティが低速になる可能性があることを意味します。これに対処するために、NCM には、複数のソフトウェア トークン シードをシステムにロードする機能が用意されています。次のいずれかのトークン管理モードを使用できます。

- ユーザ単位 : 各 NCM ユーザには、対応するソフトウェア トークン シードが 1 つ以上あります。このモードでは、各デバイス アクセスは、タスクまたは Telnet プロキシ接続を開始したユーザに対応するシード（複数可）だけを使用します。システム内のすべてのユーザに、有効なソフトウェア トークンを割り当てることをお勧めします。
  - Home ページの My Workplace で、My Settings をクリックします。My Workspace ページが開きます。
  - My Profile タブをクリックします。My Profile ページが開きます。My Profile ページのフィールドについては、P.219 の「My Profile ページのフィールド」を参照してください。

  （注）SecurID トークンの追加または更新については、P.492 の「SecurID ソフトウェア トークンの追加」を参照してください。

- プール : 汎用ソフトウェア トークン シードのプールが NCM に提供され、最高のパフォーマンスを実現するために可能な限り効率的に使用されます。
  - Admin の下のメニューバーで、Administrative Settings を選択し、Configuration Mgmt をクリックします。Configuration Management ページが開きます。
  - Device Access タブをクリックします。Device Access ページが開きます。このページでは、SecurID デバイス アクセスを設定できます。詳細については、P.64 の「Device Access ページのフィールド」を参照してください。

ソフトウェア シードが NCM にロードされると、特定のデバイスまたはデバイス セットを、RSA SecurID 認証を経由して管理するように指定できます。特定のデバイスへの SecurID アクセスをイネーブルにするには、次の手順を実行します。

1. Devices の下のメニューバーで、Inventory をクリックします。管理されているすべてのデバイスのリストが表示されます。
2. SecurID アクセスをイネーブルにするデバイスをクリックします。Device Details ページが開きます。
3. Action カラムで、Edit をクリックします。Edit Device ページが開きます。詳細については、P.120 の「New Device ページのフィールド」を参照してください。
4. Show Device Access Settings（デバイス固有の設定）リンクまでスクロール ダウンしてクリックします。
5. Setting ドロップダウン メニューから UseSecurID を選択して、Value に *exec* または *enable* と入力します。SecurID を Exec モードで使用する場合は、*exec* と入力します。*exec* を使用すると、Exec モード（通常、デバイスにログインしたときの最初のモード）がイネーブルになります。SecurID を Exec モードと Enable モードの両方で使用する場合は、*enable* と入力します。
6. Save Device ボタンをクリックします。

デバイス（またはデバイス グループ）が SecurID アクセスに設定され、かつソフトウェア シードが入力されていた場合、NCM は、デバイスにアクセスする必要があるたびに、正しい時間制限付きのトークンコードを自動的に生成します。

また、RSA SecurID 認証による管理のためのネットワーク パスワード規則をデバイスにセットアップすることもできます。詳細については、P.132 の「Device Password Rule ページのフィールド」を参照してください。その後、上記のステップ 4、5、および 6 を実行します。

SecurID ソフトウェア トークンの追加

SecurID ソフトウェア トークンを追加するには、次の手順を実行します。

1. RSA ソフトウェア トークン アプリケーションを使用して、NCM が動作するサーバにトークンをインポートします。
2. NCM Home ページの My Workspace/My Settings で、My Profile タブをクリックします。My Profile ページが開きます。
3. ページ下部の SecurID セクションで、Manage Software Token ライセンスのリンクをクリックします。View SecurID Tokens ページが開きます。このページでは、ログインしたユーザに関連付けられているソフトウェア トークンのライセンスを表示、追加、または更新できます。このライセンスは、SecurID クレデンシャルを必要とするようにデバイスが設定されている場合に、そのデバイスにログインするために使用されます。
4. Add Token リンクをクリックします。New SecurID Tokens ページが開きます。ユーザごとに、単一ソフトウェア トークンまたは汎用ソフトウェア トークンのプールを追加できます。

（注）Administration の下の Users オプションをクリックし、次にそのユーザの Edit オプションをクリックして、Manage Software Token ライセンスのリンクに移動することもできます。

New SecurID Tokens ページ

フィールド	説明 / アクション
SecurID User	ACEServer 上のトークンに割り当てられているユーザ名を入力します。
Software Token Serial Number	トークンのシリアル番号を入力します（ゼロを詰める）。
PIN	ACE/Server からの発行時に PIN がトークンに設定されている場合は、ここに PIN を入力します（**注**：PIN を更新する場合は、ここも更新する必要があります）。
Confirm PIN	確認のため、PIN を再度入力します。
Password	ACE/Server からの発行時に、PIN ではなくパスワードがトークンに設定されている場合は、ここにパスワードを入力します

作業が終了したら、必ず Save をクリックしてください。

SecurID を使用したログイン

RSA SecurID を外部認証メカニズムとして指定できます。詳細については、P.97 の「User Authentication ページのフィールド」を参照してください。

（注）*sdconf.rec* ファイルを、RSA SecurID ACE サーバから NCM サーバ（たとえば、*C:\WINDOWS\SYSTEM32\sdconf.rec*）にインストールする必要があります。このファイルに、NCM が SecurID にアクセスするために必要な接続情報が指定されています。インストールが完了したら、NCM Management Engine を再起動する必要があります。NCM Management Engine を再起動する方法については、P.113 の「サービスの開始と停止」を参照してください。

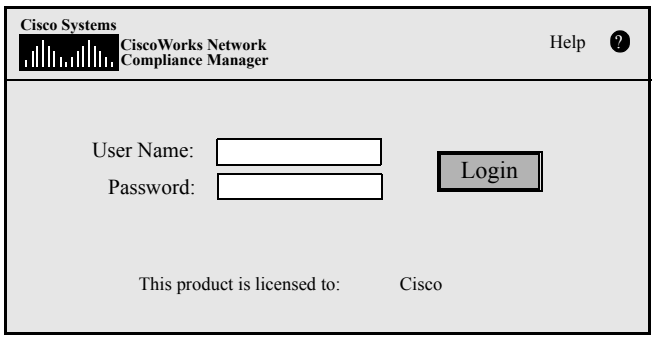
トークンが New Pin モードの場合、SecurID を使用して NCM にログインするには、次の 2 つの方法があります。

- SecurID の System PIN の使用
- SecurID の新規 PIN の使用

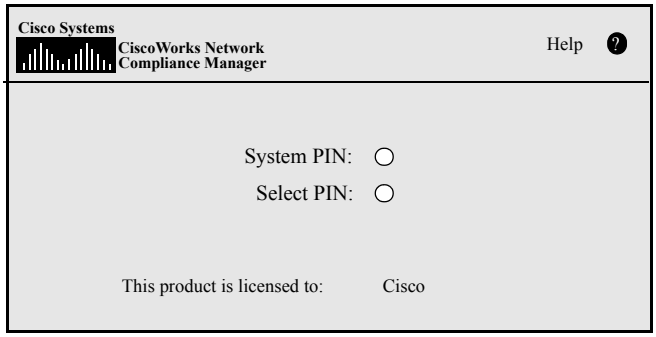
RSA のログイン手順では、必ず、新規 PIN によるユーザの再認証が要求されます。

NCM ログイン プロンプトで、次の操作を行います（下図を参照）。

1. NCM ユーザ名を入力します。
2. Password フィールドにパスコードを入力します。
3. Login をクリックします。



System PIN または新規 PIN のいずれかの使用を求めるプロンプトを表示するように SecurID システムが設定されている場合は、次のページが開きます。



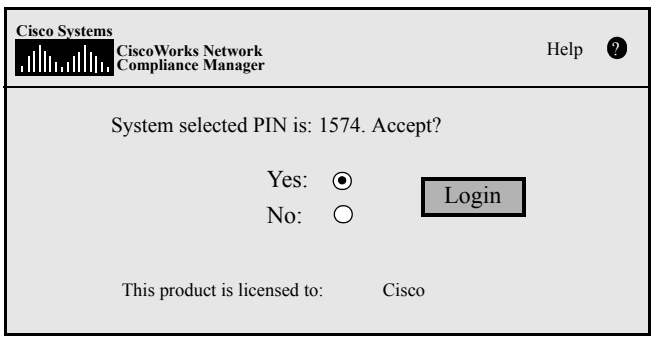
System PIN をクリックする場合は、P.494 の「ログイン方式 1：System PIN の使用」を参照してください。Select PIN をクリックする場合は、P.495 の「ログイン方式 2：新規 PIN の使用」を参照してください。

（注）System PIN または新規 PIN のいずれかの使用を求めるプロンプトを表示するように SecurID システムが設定されていない場合は、SecurID システムの設定に応じて、「ログイン方式 1」または「ログイン方式 2」のいずれかを参照してください。

ログイン方式 1：System PIN の使用

ログイン ページで、次の操作を行います。

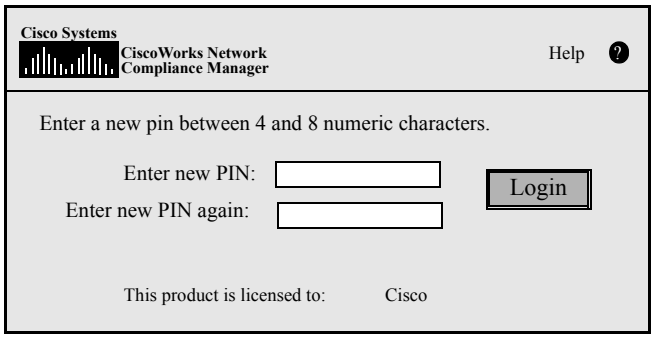
1. System PIN をクリックします（P.464 を参照）。SecurID から System PIN を取得した後、Yes をクリックします（下図を参照）。
2. Login をクリックします。
3. しばらく待ち、次のトークンコードでログインするように要求するプロンプトが表示されます。



ログイン方式 2：新規 PIN の使用

ログイン ページで、次の操作を行います。

1. Select PIN をクリックします（P.403 を参照）。
2. 新規 PIN を 2 回入力します（下図を参照）。
3. Login をクリックします。PIN が PIN パラメータを順守しているかどうかが確認されます。



SecurID のトラブルシューティング

I. SecurID を使用して NCM にログインできない場合は、RSA 管理者にお問い合せください。

II. デバイス アクセスに SecurID を使用する場合は、変更検出の Syslog User Identification オプションをオフにすることをお勧めします。オフにしない場合、Snapshot Task Failed メッセージが表示されることがあります。

1. Admin の下のメニューバーで、Administrative Settings を選択し、Configuration Mgmt をクリックします。Configuration Mgmt ページが開きます。
2. Change User Identification セクションの Syslog User Identification で、「Identify who made a configuration change from the syslog message text, if possible」チェックボックスをオフにします。
3. Change User Identification セクションの Auto-Create Users from Syslog で、「Create new users in NCM when the change author identified from syslog does not already exist (Auto-Create Users must be enabled)」チェックボックスをオフにします。
4. Save ボタンをクリックします。

III. 外部認証に失敗し、次に該当する場合は、NCM がローカル ユーザ クレデンシャルへのフォールバックを試行します。

- 外部認証サービスがダウンしている、またはアクセス不能である場合
- 外部認証方式を使用して正常にログインされなかったスタティック ユーザ アカウントの場合
- 組み込みの Admin ユーザ アカウントの場合

IV.RSA ACE/Agent クライアントと RSA ACE/Server との間の通信を認証するために、Node Secret ファイルが使用されます。ACE/Server ログ ファイルに次のようなメッセージがある場合は、NCM サーバの Node Secret ファイルを更新する必要があります。

```
07/12/2006 22:00:19U ----/core15.cisco.com       ---->/
07/12/2006 18:00:19L Node verification failed      ncmrsa.rduncm.cisco.com
```

Node Secret を作成するには、次の手順を実行します。

1. Agent Host --> Add（または Edit）Agent Host をクリックします。
2. Create Node Secret をクリックします。
3. Password ボックスにパスワードを入力し、その後 Confirm Password ボックスにパスワードを再度入力します。
4. Node Secret ファイルをデフォルトの名前でデフォルトのディレクトリに保存する場合は、OK をクリックします。Node Secret ファイルが、デフォルトの名前 *nodesecret.rec* でデフォルトのディレクトリに作成されます。デフォルトのディレクトリは、別のディレクトリを指定しない限り *ACEPROG* です。別のディレクトリを指定した場合でも、Database Administration アプリケーションを再起動するまではデフォルト ディレクトリのままです。ファイルを別の名前で保存する場合は、Browse をクリックします。Node Secret Filename Specification ダイアログボックスで、名前とディレクトリを変更し、Save をクリックします。

注：指定されたディレクトリに同じ名前の Node Secret ファイルが存在している場合、上書きするには Yes をクリックし、Node Secret Filename Specification ダイアログボックスに戻るには No をクリックします。Yes をクリックすると、指定した名前とディレクトリを使用して Node Secret ファイルが作成されます。

Add（または Edit）Agent Host ダイアログボックスで、Create Node Secret File ボタンは使用不可になっています。Node Secret Created が選択されています。

5. OK をクリックします。
6. 新しい Node Secret ファイルと Load Node Secret ユーティリティを Agent Host にコピーします。Load Node Secret ユーティリティによって、新しい Node Secret ファイルが Agent Host にロードされます。RSA Security では、ユーティリティ（agent_nsload）の 4 つのプラットフォーム固有バージョン（Windows、Solaris、HP-UX、および IBM AIX）が RSA Authentication Manager CD で提供されます。
7. Agent Host で、Load Node Secret ユーティリティを実行します。コマンドライン プロンプトで、`agent_nsload -f path -p password` と入力します（`path` は Node Secret ファイルのディレクトリの場所とファイル名で、`password` は Node Secret ファイルの保護に使用するパスワードです）。

注：ACE/Server が NCM サーバとは別のプラットフォーム上にある場合には、*agent_nsload* 実行ファイルの互換性がないことがあります。この場合は、RSA に問い合せて正しいバイナリを入手してください。また、場合によっては、RSA の dll が新しい Node Secret ファイルを特定できるように NCM サーバをリブートする必要があります。