CHAPTER 12

SSH と証明書の設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上でサポートされています。ASA 8.3(*x*) では、サポートされていません。

この章では、センサーに SSH と証明書を設定する方法について説明します。次の事項について説明します。

SSH について

SSH は、高性能な認証機能とセキュアでないチャネル経由でのセキュアな通信を提供します。SSH は、センサーへの接続を暗号化し、キーを提供することで、正しいセンサーに接続されているかを検証可能にします。SSH はまた、ブロッキングのためにセンサーが接続する他のデバイスへの認証済み暗号化アクセスも提供します。

SSH は、次のいずれか、または両方を使用してホストやネットワークを認証します。

- パスワード
- ユーザ RSA 公開キー

SSH は、次の危険からの保護を提供します。

- IP スプーフィング：リモート ホストが、信頼できる別のホストからのものと見せかけてパケットを送信すること。

（注）　ローカル ネットワーク上に存在するスプーフィング実行者（外部に対しローカルのルータを装うことができる）に対しても、SSH は保護を提供できます。

- IP ソース ルーティング：あるホストが、他の信頼できるホストか来た IP パケットを偽装すること。
- DNS スプーフィング：ネーム サーバ レコードを偽造する攻撃者。
- 中間ホストによるクリア テキスト パスワードや他のデータのインターセプト。
- 中間ホスト使用者によるデータの操作。
- X 認証データと X11 サーバへのスプーフィングされた接続のリスニングをもとにした攻撃。

（注）　SSH では、パスワードがクリア テキストで送られることはありません。

許可キーの設定

このセクションでは、センサーに許可キーを設定する方法について説明します。次の事項について説明します。

- 「[Authorized Keys] ペイン」（P.12-2）
- 「[Authorized Keys] ペインのフィールド定義」（P.12-3）
- 「[Add Authorized Key]/[Edit Authorized Key] ダイアログボックスのフィールド定義」（P.12-3）
- 「許可キーの定義」（P.12-3）

[Authorized Keys] ペイン

（注）　許可キーの追加や編集を行うには、管理者である必要があります。オペレータ権限やビューア権限で許可キーの追加や編集を試みると、「Delivery Failed」メッセージが表示されます。

RSA 認証を使用してローカル SSH サーバにログインできるよう、クライアントに公開キーを定義するには、[Authorized Keys] ペインを使用します。[Authorized Keys] ペインには、センサーへのアクセスが許可された SSH クライアントすべての公開キーが表示されます。表示できるのは自分のキーだけです。他のユーザのキーは表示できません。

センサーにログインできる各ユーザには、そのユーザがログインする際に使用する各クライアントにより収集された許可キーのリストが割り当てられています。SSH を使用してセンサーにログインするときは、パスワードの代わりに RSA 認証を使用できます。

公開キーの定義には、秘密キーを保存するクライアントで RSA キー生成ツールを使用します。生成された公開キーを 3 つの数字（係数の長さ、公開指数、公開係数）の組み合わせとして表示し、これらの数字を [Authorized Keys] ペインのフィールドに入力します。

[Authorized Keys] ペインのフィールド定義

[Authorized Keys] ペインには、次のようなフィールドがあります。

- [ID]：キーを識別する一意のストリング（1 ～ 256 文字）。ID がスペースを含むか 256 文字を超える英数字の場合は、エラー メッセージが表示されます。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。範囲外の長さを指定すると、エラー メッセージが表示されます。
- [Public Exponent]：データを暗号化するために RSA アルゴリズムで使用されます。有効な範囲は 3 ～ 2147483647 です。範囲外の指数を指定すると、エラー メッセージが表示されます。
- [Public Modulus]：データを暗号化するために RSA アルゴリズムで使用されます。公開係数は、1 ～ 2048 個の数字ストリング（係数は、(2 ^ length) < modulus < (2 ^ (length + 1))）です。係数が範囲外であるか、数字ではなく文字を使用すると、エラー メッセージが表示されます。数値は、^[0-9][0-9]*$ のパターンと一致する必要があります。

[Add Authorized Key]/[Edit Authorized Key] ダイアログボックスのフィールド定義

[Add Authorized Key]/[Edit Authorized Key] ダイアログボックスには、次のフィールドがあります。

- [ID]：キーを識別する一意のストリング（1 ～ 256 文字）。ID がスペースを含むか 256 文字を超える英数字の場合は、エラー メッセージが表示されます。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。範囲外の長さを指定すると、エラー メッセージが表示されます。
- [Public Exponent]：データを暗号化するために RSA アルゴリズムで使用されます。有効な範囲は 3 ～ 2147483647 です。範囲外の指数を指定すると、エラー メッセージが表示されます。
- [Public Modulus]：データを暗号化するために RSA アルゴリズムで使用されます。公開係数は、1 ～ 2048 個の数字ストリング（係数は、(2 ^ length) < modulus < (2 ^ (length + 1))）です。係数が範囲外であるか、数字ではなく文字を使用すると、エラー メッセージが表示されます。数値は、^[0-9][0-9]*$ のパターンと一致する必要があります。

許可キーの定義

許可キーを定義する手順は次のとおりです。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [SSH] > [Authorized Keys] と選択し、[Add] をクリックして公開キーをリストに追加します。最大 50 の SSH 公開キーを追加できます。

ステップ 3　[ID] フィールドに、キーを識別するための一意の ID を入力します。

ステップ 4　[Modulus Length] フィールドに、整数を入力します。

係数の長さは、係数の有効ビット数で表します。RSA キーの強度は、係数のサイズに依存します。係数のビット数が多いほど、キーは強力になります。

（注）　係数の長さ、公開指数、公開係数がわからない場合、秘密キーの保存先となるクライアント上で RSA キー生成ツールを使用します。生成された公開キーを 3 つの数のセット（係数の長さ、公開指数、公開係数）として表示し、ステップ 4 ～ 6 でこれらの数を入力します。

ステップ 5　[Public Exponent] フィールドに、整数を入力します。RSA アルゴリズムでは、公開指数を使用してデータが暗号化されます。公開指数の有効範囲は、3 ～ 2147483647 の数です。

ステップ 6　[Public Modulus] フィールドに値を入力します。公開係数は、数字ストリング値（係数は、(2 ^ length) < modulus < (2 ^ (length + 1))）です。RSA アルゴリズムでは、公開係数を使用してデータが暗号化されます。

ヒント　変更を廃棄して [Add Authorized Key] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 7　[OK] をクリックします。[Authorized Keys] ペインの許可キー リストに新しいキーが表示されます。

ステップ 8　許可キー リストにある既存のエントリを編集するには、エントリを選択して [Edit] をクリックします。

ステップ 9　[Modulus Length] フィールド、[Public Exponent] フィールド、[Public Modulus] フィールドを編集します。

注意　エントリの作成後は、[ID] フィールドを変更できません。

ヒント　変更を廃棄して [Edit Authorized Key] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 10　[OK] をクリックします。[Authorized Keys] ペインの許可キー リストに編集したキーが表示されます。

ステップ 11　公開キーをリストから削除するには、キーを選択し、[Delete] ボタンをクリックします。削除したキーが [Authorized Keys] ペインの許可キー リストから消えます。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 12　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

既知のホスト キーの設定

ここでは、既知のホスト キーの設定方法について説明します。次の事項について説明します。

[Known Host Keys] ペイン

（注）　既知のホスト キーの追加や編集を行うには、管理者である必要があります。

[Known Host Keys] ペインを使用して、センサーが管理するブロッキング デバイス、および更新のダウンロードやファイルのコピーに使用される SSH（SCP）サーバに公開キーを定義します。[Known Host Keys] ペインの設定に必要な情報を取得するために、各デバイスとサーバから公開キーを入手することが必要です。公開キーを正しいフォーマットで取得できない場合、[Add Known Host Keys] ダイアログボックスの [Retrieve Host Key] をクリックします。

IDM は、IP アドレスで指定されたホストから既知のホスト キーの取得を試行します。成功した場合、IDM がキーを [Add Known Host Key] ペインに読み込みます。

（注）　[Retrieve Host Key] が使用可能なのは、[Add] ダイアログボックスだけです。IP アドレスが無効な場合、エラー メッセージが表示されます。

[Known Host Keys] ペインのフィールド定義

[Known Host Keys] ペインには、次のようなフィールドがあります。

- [IP Address]：追加するキーに対応するホストの IP アドレス。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。範囲外の長さを指定すると、エラー メッセージが表示されます。
- [Public Exponent]：データを暗号化するために RSA アルゴリズムで使用されます。有効な範囲は 3 ～ 2147483647 です。範囲外の指数を指定すると、エラー メッセージが表示されます。
- [Public Modulus]：データを暗号化するために RSA アルゴリズムで使用されます。公開係数は、1 ～ 2048 個の数字ストリング（係数は、(2 ^ length) < modulus < (2 ^ (length + 1))）です。係数が範囲外であるか、数字ではなく文字を使用すると、エラー メッセージが表示されます。数値は、^[0-9][0-9]*$ のパターンと一致する必要があります。

[Add Known Host Key]/[Edit Known Host Key] ダイアログボックスのフィールド定義

[Add Known Host Key]/[Edit Known Host Key] ダイアログボックスには、次のフィールドがあります。

- [IP Address]：追加するキーに対応するホストの IP アドレス。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。範囲外の長さを指定すると、エラー メッセージが表示されます。
- [Public Exponent]：データを暗号化するために RSA アルゴリズムで使用されます。有効な範囲は 3 ～ 2147483647 です。範囲外の指数を指定すると、エラー メッセージが表示されます。
- [Public Modulus]：データを暗号化するために RSA アルゴリズムで使用されます。公開係数は、1 ～ 2048 個の数字ストリング（係数は、(2 ^ length) < modulus < (2 ^ (length + 1))）です。係数が範囲外であるか、数字ではなく文字を使用すると、エラー メッセージが表示されます。数値は、^[0-9][0-9]*$ のパターンと一致する必要があります。

既知のホスト キーの定義

既知のホスト キーを定義する手順は次のとおりです。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [SSH] > [Known Host Keys] と選択し、[Add] をクリックして既知のホスト キーをリストに追加します。

ステップ 3　[IP Address] フィールドに、キーの追加対象となるホストの IP アドレスを入力します。

ステップ 4　[Retrieve Host Key] をクリックします。IDM は、ステップ 3 で入力した IP アドレスのホストからのキー取得を試行します。取得に成功した場合、ステップ 8 に進みます。失敗した場合、ステップ 5 ～ 7 を実行します。

注意　取得したキーが指定したアドレスに対して正しいか検証し、サーバ IP アドレスがスプーフィングされていないことを確認します。

ステップ 5　[Modulus Length] フィールドに、整数を入力します。係数の長さは、係数の有効ビット数で表します。RSA キーの強度は、係数のサイズに依存します。係数のビット数が多いほど、キーは強力になります。

ステップ 6　[Public Exponent] フィールドに、整数を入力します。RSA アルゴリズムでは、公開指数を使用してデータが暗号化されます。

ステップ 7　[Public Modulus] フィールドに値を入力します。公開係数は、数字ストリング値（係数は、(2 ^ length) < modulus < (2 ^ (length + 1))）です。RSA アルゴリズムでは、公開係数を使用してデータが暗号化されます。

ヒント　変更を廃棄して [Add Known Host Key] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 8　[OK] をクリックします。新しいキーが [Known Host Keys] ペインの既知のホスト キーのリストに表示されます。

ステップ 9　許可キー リストにある既存のエントリを編集するには、エントリを選択して [Edit] をクリックします。

ステップ 10　[Modulus Length] フィールド、[Public Exponent] フィールド、[Public Modulus] フィールドを編集します。

注意　エントリの作成後は、[ID] フィールドを変更できません。

ヒント　変更を廃棄して [Edit Known Host Key] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 11　[OK] をクリックします。編集したキーが [Known Host Keys] ペインの既知のホスト キーのリストに表示されます。

ステップ 12　公開キーをリストから削除するには、キーを選択し、[Delete] ボタンをクリックします。削除したキーが [Known Host Keys] ペインの既知のホスト キーのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 13　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

センサー キーの生成

このセクションでは、センサー キーの取得方法について説明します。次の項目を取り上げます。

- 「[Sensor Key] ペイン」（P.12-7）
- 「[Sensor Key] ペインのフィールド定義」（P.12-7）
- 「センサー SSH ホスト キーの表示と生成」（P.12-7）

[Sensor Key] ペイン

（注）　センサー SSH ホスト キーを生成するには、管理者である必要があります。

サーバでは、その身元を証明する手段として SSH ホスト キーが使用されます。クライアントは、既知のキーを見つけると、正しいサーバに接続したと認識します。センサーでは、初回起動時に SSH ホスト キーが生成されます。これは [Sensor Key] ペインに表示されます。[Generate Key] をクリックして、キーを新しいキーに置き換えます。

[Sensor Key] ペインのフィールド定義

[Sensor Key] ペインに、センサー SSH ホスト キーが表示されます。[Generate Key] を押して、新しいセンサー SSH ホスト キーを生成します。

センサー SSH ホスト キーの表示と生成

注意　これ以降は、既存のキーの代わりに新しいキーが使用されるため、引き続き正常に接続するためには、リモート システム上にある既知ホストのテーブルを新しいホスト キーで更新する必要があります。

センサー SSH ホスト キーの表示と生成を行うには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [SSH] > [Sensor Key] と選択します。センサー SSH ホスト キーが表示されます。

ステップ 3　新しいセンサー SSH ホスト キーを生成するには、[Generate Key] をクリックします。ダイアログボックスに次の警告が表示されます。

```
Generating a new SSH host key requires you to update the known hosts tables on remote
systems with the new key so that future connections succeed. Do you want to continue?
```

ステップ 4　[OK] をクリックして続行します。新しいホスト キーが生成され、古いホスト キーが削除されます。ステータス メッセージに、キー更新が成功したことが表示されます。

証明書について

Cisco IPS は、IDM を実行する Web サーバを含んでいます。管理ステーションは、この Web サーバに接続します。ブロッキング転送センサーも、マスター ブロッキング センサーの Web サーバに接続します。この Web サーバでは、セキュリティを確保するため、SSL プロトコルに似た TLS という暗号化プロトコルが使用されます。Web ブラウザでは、`https://ip_address` で始まる URL が入力されると、それに対する応答として、TLS プロトコルまたは SSL プロトコルによりホストとの間で暗号化セッションのネゴシエーションが行われます。

注意　Web ブラウザでは、初めてのネゴシエーションが行われる際、この時点ではまだ CA に対する信頼が確立されていないため、IDM から提示される証明書は拒否されます。

（注）　IDM は、デフォルトで TLS および SSL の使用がイネーブルになっています。TLS および SSL を使用することを強く推奨します。

TLS による暗号化セッションのネゴシエーション プロセスは、クライアントとサーバとが協調して何度もデータをやり取りすることから、「ハンドシェイク」と呼ばれます。サーバからクライアントへ証明書が送信されると、クライアントでは、この証明書に対して、次の 3 つのテストが実行されます。

1. 証明書に記載されている発行元は信頼できるか。

   各 Web ブラウザには、出荷される時点で、信頼されているサードパーティ CA のリストが組み込まれています。証明書に記載されている発行元が、ブラウザにより信頼されている CA のリストに含まれていれば、この最初のテストでは問題なしと判断されます。

2. その日の日付が、証明書の有効期間内にあるか。

   それぞれの証明書には、有効期間を表す 2 つの日付が記載された [Validity] フィールドがあります。その日の日付がこの期間内に該当すれば、この 2 番目のテストでは問題なしと判断されます。

3. 証明書に記載されているサブジェクトの共通名が、URL ホスト名と一致するか。

   URL ホスト名が、サブジェクトの共通名と比較されます。一致すれば、この 3 番目のテストでは問題なしと判断されます。

Web ブラウザから IDM に接続しようとすると、センサーは独自の証明書を発行しますが（センサーが自分自身の CA）、ブラウザにより信頼されている CA のリストにはセンサーが含まれていないため、返された証明書は無効と見なされます。

ブラウザにエラー メッセージが表示された場合の対処方法としては、次の 3 つの選択肢が考えられます。

- サイトへの接続を即座に解除する。
- その他の Web ブラウザ セッション用に証明書を受け入れる。
- 証明書に記載されている発行元を Web ブラウザの信頼 CA リストに追加して、有効期間が経過するまで証明書を信頼する。

最も簡単な方法は、発行元を永続的に信頼することです。ただし、発行元を追加する前に必ず、アウトオブバンド方式を使用して、証明書のフィンガープリントを検証します。これにより、センサーになりすました攻撃者による被害を回避できます。Web ブラウザに表示される証明書のフィンガープリントが、センサーのフィンガープリントと一致するかどうかを確認してください。

注意　センサーの組織名またはホスト名を変更した場合は、センサーの次回リブート時に新しい証明書が生成されます。Web ブラウザから IDM への次回接続時には、手動上書きダイアログボックスが表示されます。この場合は、Internet Explorer および Firefox で、証明書フィンガープリントの検証を再度実行する必要があります。

詳細情報

証明書の検証の詳細については、「CA の検証」（P.1-8）を参照してください。

信頼できるホストの設定

ここでは、信頼できるホストの設定方法について説明します。次の事項について説明します。

[Trusted Hosts] ペイン

（注）　信頼できるホストを追加するには、管理者である必要があります。

[Trusted Hosts] ペインを使用して、マスター ブロッキング センサーの証明書、およびセンサーが更新のダウンロードに使用する TLS サーバと SSL サーバの証明書を追加します。CSA MC など、センサーが通信する外部製品インターフェイスの IP アドレスの追加にも使用できます。

[Trusted Hosts] ペインには、追加されたすべての信頼できるホスト証明書が一覧表示されます。証明書は、IP アドレスを入力することにより追加できます。IDM は証明書を取得し、そのフィンガープリントを表示します。フィンガープリントを受け入れると、証明書に対する信頼が確立されます。リストでは、エントリの追加と削除を行えますが、エントリの編集は行えません。

詳細情報

外部製品インターフェイスの追加方法については、第 15 章「外部製品インターフェイスの設定」を参照してください。

[Trusted Hosts] ペインのフィールド定義

[Trusted Hosts] ペインには、次のようなフィールドがあります。

- [IP Address]：信頼できるホストの IP アドレス。

- [MD5] : メッセージ ダイジェスト 5 暗号化。MD5 は、メッセージの 128 ビット ハッシュの計算に使用されるアルゴリズムです。
- [SHA1] : Secure Hash Algorithm。SHA1 は、暗号学的メッセージ ダイジェスト アルゴリズムです。

[Add Trusted Host] ダイアログボックスのフィールド定義

[Add Trusted Host] ダイアログボックスには、次のようなフィールドがあります。

- [IP Address] : 信頼できるホストの IP アドレス。
- [Port] :（オプション）ホスト証明書を取得するポート番号を指定します。

信頼できるホストの追加

信頼できるホストを追加する手順は次のとおりです。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Certificates] > [Trusted Hosts] と選択し、[Add] をクリックして信頼できるホストをリストに追加します。

ステップ 3　[IP Address] フィールドに、追加する信頼できるホストの IP アドレスを入力します。

ステップ 4　443 以外のポートを使用する場合、[Port] フィールドにポート番号を入力します。

ヒント　変更を廃棄して [Add Trusted Host] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 5　[OK] をクリックします。IDM は、ステップ 3 で入力した IP アドレスのホストから証明書を取得します。新しい信頼できるホストが [Trusted Hosts] ペインの信頼できるホストのリストに表示されます。IDM がセンサーと通信中であることを知らせるダイアログボックスが表示されます。

```
Communicating with the sensor, please wait ...
```

信頼できるホストの追加に IDM が成功したか、ダイアログボックスにステータスが表示されます。

```
The new host was added successfully.
```

ステップ 6　表示される値と、直接端末接続またはコンソールなどで安全に取得した値とを比較することにより、そのフィンガープリントが正しいかどうかを検証します。不一致に気づいた場合、その信頼できるホストをただちに削除します。

ステップ 7　信頼できるホスト リストの既存のエントリを表示するには、エントリを選択して [View] をクリックします。[View Trusted Host] ダイアログボックスが表示されます。証明書データが表示されます。ダイアログボックスに表示されるデータは読み取り専用です。

ステップ 8　[OK] をクリックします。

ステップ 9　信頼できるホストをリストから削除するには、ホストを選択し、[Delete] ボタンをクリックします。その信頼できるホストが [Trusted Hosts] ペインの信頼できるホストのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 10　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

サーバ証明書の生成

ここでは、サーバ証明書の生成方法について説明します。次の事項について説明します。

[Server Certificate] ペイン

（注）　サーバ証明書を作成するには、管理者である必要があります。

[Server Certificate] パネルには、センサー サーバの X.509 証明書が表示されます。このペインから、新しいサーバ自己署名 X.509 証明書を生成できます。証明書は、センサーの初回起動時に生成されます。[Generate Certificate] をクリックして、新しいホスト証明書を生成します。

注意　証明書にはセンサーの IP アドレスが含まれます。センサーの IP アドレスを変更した場合は、新しい証明書を生成する必要があります。

[Server Certificate] ペインのフィールド定義

[Server Certificate] パネルには、センサー サーバの X.509 証明書が表示されます。[Generate Certificate] をクリックして、新しいセンサー X.509 証明書を生成します。

サーバ証明書の表示と生成

注意　新しいフィンガープリントを書き込みます。接続時に Web ブラウザの表示内容を確認する場合や、センサーを信頼できるホストとして追加する場合には、このフィンガープリントが必要になります。センサーがマスター ブロッキング センサーである場合は、マスター ブロッキング センサーにブロックを送信するリモート センサー上で、既知のホストのテーブルを更新する必要があります。

センサー サーバの X.509 証明書の表示と生成を行うには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して IDM にログインします。

ステップ 2　[Configuration] > [Sensor Setup] > [Certificate] > [Server Certificate] と選択します。センサー サーバの X.509 証明書が表示されます。

ステップ 3　センサー サーバの X.509 証明書を新しく生成するには、[Generate Certificate] をクリックします。ダイアログボックスに次の警告が表示されます。

```
Generating a new server certificate requires you to verify the new fingerprint the next
time you connect or when you add the sensor as a trusted host. Do you want to continue?
```

ステップ 4　[OK] をクリックして続行します。新しいサーバ証明書が生成され、これまでのサーバ証明書は削除されます。