センサーのセットアップ

この章では、センサーのセットアップについて説明します。

センサーをネットワークに設置した後、**setup** コマンドを使用してセンサーを初期化する必要があります。**setup** コマンドを使用すると、ホスト名、IP インターフェイス、Telnet サーバ、Web サーバ ポート、アクセス コントロール リスト、時間設定、およびインターフェイスの割り当てと有効化など、センサーの基本的な設定を行います。センサーを初期化すると、ネットワーク経由でセンサーと通信できるようになります。その後、侵入防御を設定できます。

注意 Configuration >Sensor Setup in IDM を使用してセンサーをセットアップする前に、センサーを初期化する必要があります。手順については、P.1-6 の「センサーの初期化」を参照してください。

センサーを初期化したら、**Sensor Setup** でその他のネットワーク パラメータの変更と設定ができます。

この章は、次の項で構成されています。

ネットワーク設定の構成

この項では、ネットワークの設定を変更する方法について説明します。取り上げる事項は次のとおりです。

概要

Network パネルを使用して、センサーのネットワーク パラメータと通信パラメータを指定します。

（注）　**setup** コマンドを使用してセンサーを初期化すると、ネットワーク パラメータと通信パラメータの値が Network パネルに表示されます。これらのパラメータを変更する必要がある場合は、Network パネルで変更できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ネットワーク設定を構成するには、管理者である必要があります。

フィールド定義

Network パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Hostname**：センサーの名前。

  ホスト名は 1 ～ 64 文字の文字列で、^[A-Za-z0-9_/-]+$ に一致するパターンです。デフォルトは sensor です。ホスト名にスペースが含まれているか、または英数字が 64 文字を超えていると、エラー メッセージが表示されます。
- **IP Address**：センサーの IP アドレス。

  デフォルトは 10.1.9.201 です。
- **Network Mask**：IP アドレスに対応するマスク。

  デフォルトは 255.255.255.0 です。
- **Default Route**：デフォルトのゲートウェイ アドレス。

  デフォルトは 10.1.9.1 です。
- **FTP Timeout**：センサーと FTP サーバの通信中にタイムアウトになるまで FTP クライアントが待機する時間（秒単位）を設定します。

  有効な範囲は 1 ～ 86400 秒です。デフォルトは 300 秒です。
- **Web Server Settings**：Web サーバのセキュリティ レベルとポートを設定します。
  - **Enable TLS/SSL**：Web サーバの TLS と SSL をイネーブルにします。

デフォルトはイネーブルです。TLS と SSL をイネーブルにすることを強くお勧めします。

- **Web server port**：Web サーバが使用する TCP ポート。

  デフォルトは 443（HTTPS の場合）です。1 ～ 65535 以外の値を入力すると、エラー メッセージが表示されます。

- **Remote Access**：センサーのリモート アクセスをイネーブルにします。
  - **Enable Telnet**：Telnet によるセンサーへのリモート アクセスをイネーブルまたはディセーブルにします。

（注） Telnet は安全なアクセス サービスではないので、デフォルトでは使用不可です。

ボタンの機能：

- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

ネットワーク設定の構成

ネットワーク設定を構成するには、次の手順を実行します。

ステップ 1　管理者特権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 > Network** の順にクリックします。

Network パネルが表示されます。

ステップ 3　センサーのホスト名を編集するには、**Hostname** フィールドに新しい名前を入力します。

ステップ 4　センサーの IP アドレスを変更するには、**IP Address** フィールドに新しいアドレスを入力します。

ステップ 5　ネットワーク マスクを変更するには、**Network Mask** フィールドに新しいマスクを入力します。

ステップ 6　デフォルトのゲートウェイを変更するには、**Default Route** フィールドに新しいアドレスを入力します。

ステップ 7　FTP タイムアウトの時間を変更するには、**FTP Timeout** フィールドに新しい時間を入力します。

ステップ 8　TLS/SSL をイネーブルまたはディセーブルにするには、**Enable TLS/SSL** を選択または選択解除します。

（注） TLS/SSL を使用可能にすることを強くお勧めします。

（注） TLS と SSL は、Web ブラウザと Web サーバ間の暗号化通信を可能にするプロトコルです。TLS/SSL をイネーブルにした場合、`https://`*sensor_ip_address* を使用して IDM に接続します。TLS/SSL をディセーブルにした場合、`http://`*sensor_ip_address*`:`*port_number* を使用して IDM に接続します。

ステップ 9　Web サーバのポートを変更するには、**Web Server Port** フィールドに新しいポート番号を入力します。

（注）　Web サーバのポートを変更する場合、IDM に接続するときに、ブラウザの URL アドレスでポートを指定する必要があります。その場合、`https://`*sensor_ip_address:port_number*（`https://10.1.9.201:1040` など）の形式を使用します。

ステップ 10　リモート アクセスをイネーブルまたはディセーブルにするには、**Enable Telnet** を選択します。

（注）　Telnet は安全なアクセス サービスではないので、デフォルトでは使用不可です。ただし、安全なサービスである SSH が常にセンサーで実行されています。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 11　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

（注）　ネットワーク設定を変更すると、センサーへの接続が中断し、新しいアドレスでの再接続が必要になることがあります。

許可されたホストの設定

この項では、許可されたホストをシステムに追加する方法について説明します。取り上げる事項は次のとおりです。

概要

Allowed Hosts パネルを使用して、センサーへのアクセスを許可されたホストまたはネットワークを指定します。

（注）　**setup** コマンドを使用してセンサーを初期化すると、許可されたホストのパラメータ値が Allowed Hosts パネルに表示されます。これらのパラメータを変更する必要がある場合は、Allowed Hosts パネルで変更できます。

デフォルトでは、リストには何もエントリがないため、ホストを追加するまで許可されたホストはありません。

（注）　許可されたホストのリストに、ASDM、IDM、IDS MC などの管理ホスト、および IDS Security Monitor などのモニタリング ホストを追加する必要があります。追加しないと、センサーと通信できません。

注意　許可ホストを追加、編集、削除するときは、センサーのリモート管理に使用する IP アドレスを削除しないように注意してください。

サポートされているユーザ ロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

許可されたホストとネットワークを設定するには、管理者である必要があります。

フィールド定義

この項では、許可されたホストのフィールド定義を示します。取り上げる事項は次のとおりです。

Allowed Hosts パネル

Allowed Hosts パネルには、次のフィールドがあります。

フィールドの説明：

- **IP Address**：ホストがセンサーへのアクセスを許可する IP アドレス。
- **Network Mask**：ホストの IP アドレスに対応するマスク。

ボタンの機能：

- **Add**：Add Allowed Host ダイアログボックスを開きます。
  このダイアログボックスでは、許可されたホストのリストにホストまたはネットワークを追加できます。
- **Edit**：Edit Allowed Host ダイアログボックスを開きます。
  このダイアログボックスでは、このホストまたはネットワークに関連付けられた値を変更できます。
- **Delete**：許可されたホストのリストからホストまたはネットワークを削除します。
- **Apply**：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。
- **Reset**:作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Allowed Host ダイアログボックス

Add and Edit Allowed Host ダイアログボックスには、次のフィールドがあります。

フィールドの説明：

- **IP Address**：ホストがセンサーへのアクセスを許可する IP アドレス。
- **Network Mask**：ホストの IP アドレスに対応するマスク。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

許可されたホストの設定

センサーへのアクセスが許可されたホストとネットワークを指定するには、次の手順を実行します。

ステップ 1　管理者特権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 > Allowed Hosts** の順にクリックします。

Allowed Hosts パネルが表示されます。

ステップ 3　**Add** をクリックして、ホストまたはネットワークをリストに追加します。

Add Allowed Hosts ダイアログボックスが表示されます。

許可されたホストは最大 512 台追加できます。

ステップ 4　**IP Address** フィールドにホストまたはネットワークの IP アドレスを入力します。

入力した IP アドレスが既存のリストのエントリに含まれている場合、エラー メッセージが表示されます。

ステップ 5　ホストまたはネットワークのネットワーク マスクを **Network Mask** フィールドに入力するか、またはドロップダウン リストからネットワーク マスクを選択します。

IDM では、IP アドレスがホストであるかネットワークであるかに関係なく、必ずネットマスクを指定する必要があります。ネットマスクを指定しないと、`Network Mask is not valid` というエラーが表示されます。

また、ネットワーク マスクが IP アドレスと一致しない場合も、エラー メッセージが表示されます。

ステップ 6　**OK** をクリックします。

新しいホストまたはネットワークが、Allowed Hosts パネルにある許可されたホストのリストに表示されます。

ステップ 7　許可されたホストのリストにある既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Allowed Host ダイアログボックスが表示されます。

ステップ 8　**IP Address** フィールドで、ホストまたはネットワークの IP アドレスを編集します。

ステップ 9　**Network Mask** フィールドで、ホストまたはネットワークのネットワーク マスクを編集します。

ステップ 10　**OK** をクリックします。

編集されたホストまたはネットワークが、Allowed Hosts パネルの許可されたホストのリストに表示されます。

ステップ 11　リストからホストまたはネットワークを削除するには、ホストまたはネットワークを選択して **Delete** をクリックします。

削除されたホストは、Allowed Hosts パネルの許可されたホストのリストに表示されなくなります。

注意　ホストを削除すると、それ以降のホストからのネットワーク接続は、すべて拒否されます。

ヒント　変更を元に戻すには、**Reset** をクリックします。

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

SSH の設定

SSH は強力な認証を提供し、安全ではないチャネル上の通信を安全なものにします。

SSH は、センサーへの接続を暗号化し、正しいセンサーに接続中であることを検証できるように鍵を提供します。また、SSH は、ブロッキング目的で、センサーが接続しているその他のデバイスに対しても認証済みで暗号化されたアクセスを提供します。

SSH は、次のいずれか 1 つまたは複数を使用して、ホストまたはネットワークを認証します。

- Password
- ユーザ RSA 公開鍵

SSH は次のものからネットワークを保護します。

- IP スプーフィング：リモート ホストは、別の信頼できるホストから送信されたかのように偽装してパケットを送信します。

  SSH は、外部へのルータであるかのように偽装する可能性のあるローカル ネットワーク上のスプーファーを阻止します。
- IP ソース ルーティング：ホストは別の信頼できるホストから送信されたかのように IP パケットを偽装します。
- DNS スプーフィング：攻撃者がネーム サーバ レコードを偽造します。
- 中間ホストによるクリア テキスト パスワードとその他のデータの傍受
- 中間ホストを支配する攻撃者によるデータの操作
- X 認証データの傍受と X11 サーバへの偽装接続に基づく攻撃

（注）　SSH はパスワードをクリア テキストで送信することは決してありません。

この項で取り上げる事項は次のとおりです。

許可鍵の定義

この項では、公開鍵の定義方法について説明します。取り上げる事項は次のとおりですます。

概要

Authorized Keys パネルを使用して、RSA 認証によってローカル SSH サーバへのログインが許可されるクライアントの公開鍵を定義できます。Authorized Keys パネルには、センサーへのアクセスが許可されたすべての SSH クライアントの公開鍵が表示されます。

センサーにログインできる各ユーザは、そのユーザがログインする各クライアントから収集した許可鍵のリストを持ちます。SSH を使用してセンサーにログインするときは、パスワードを使用する代わりに RSA 認証を使用できます。

秘密鍵を保存するクライアントで RSA 鍵生成ツールを使用します。次に、生成された公開鍵を 3 つの数字のセット（Key Modulus Length、Public Exponent、Public Modulus）として表示し、これらの数字を Authorized Keys パネルの該当するフィールドに入力します。

表示できるのは自分の鍵だけで、他のユーザの鍵は表示できません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

許可鍵を追加したり編集したりするには、管理者である必要があります。オペレータ特権またはビューア特権で許可鍵の追加または編集を試みると、`Delivery Failed` メッセージが表示されます。

フィールド定義

この項では、許可鍵のフィールド定義を示します。取り上げる事項は次のとおりです。

- Authorized Keys パネル（P.2-9）
- Add and Edit Authorized Key ダイアログボックス（P.2-10）

Authorized Keys パネル

Authorized Keys パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **ID**：鍵を識別する一意の文字列（1 ～ 256 文字）。

  ID にスペースが含まれているか、または英数字が 256 文字を超えていると、エラー メッセージが表示されます。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。

  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。

  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。

  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **Add**：Add Authorized Key ダイアログボックスを開きます。

  このダイアログボックスでは、新しい許可鍵を追加できます。
- **Edit**：Edit Authorized Key ダイアログボックスを開きます。

  このダイアログボックスでは、この許可鍵に関連付けられた値を変更できます。
- **Delete**：リストから許可鍵を削除します。
- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Authorized Key ダイアログボックス

Add and Edit Authorized Key ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **ID**：鍵を識別する一意の文字列（1 ～ 256 文字）。
  ID にスペースが含まれているか、または英数字が 256 文字を超えていると、エラー メッセージが表示されます。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。
  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。
  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。
  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

許可鍵の定義

公開鍵を定義するには、次の手順を実行します。

ステップ 1　管理者特権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 > SSH > Authorized Keys** の順にクリックします。

Authorized Keys パネルが表示されます。

ステップ 3　**Add** をクリックして、公開鍵をリストに追加します。

Add Authorized Key ダイアログボックスが表示されます。

最大 50 個の SSH 許可鍵を追加できます。

ステップ 4　**ID** フィールドに、許可鍵を識別するための一意の ID を入力します。

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、係数の有意ビットの数です。RSA 鍵の強度は、係数のサイズに依存します。係数のビット数が多いほど、鍵は強力になります。

（注）　係数の長さ、公開指数、および公開係数が不明の場合は、秘密鍵を常駐させるクライアント上で RSA 鍵生成ツールを使用します。生成された公開鍵を 3 つの数字セット（係数の長さ、公開指数、および公開係数）として表示し、ステップ 5 ～ 7 でこれらの数字を入力します。

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。公開指数の有効値は、3 ～ 2147483647 です。

ステップ 7　**Public Modulus** フィールドに値を入力します。

公開係数は文字列値です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。

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　変更を元に戻すには、**Reset** をクリックします。

ステップ 8　**OK** をクリックします。

Authorized Keys パネルの許可鍵リストに、新しい鍵が表示されます。

ステップ 9　許可鍵リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Authorized Key ダイアログボックスが表示されます。

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

注意　エントリを作成した後は、**ID** フィールドは変更できません。

ステップ 11　**OK** をクリックします。

Authorized Keys パネルの許可鍵リストに、編集された鍵が表示されます。

ステップ 12　公開鍵をリストから削除するには、それを選択して **Delete** をクリックします。

削除された鍵は、Authorized Keys パネルの許可鍵リストに表示されなくなります。

ヒント　**Reset** をクリックして、変更を削除します。

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

既知のホスト鍵の定義

この項では、既知のホスト鍵を定義する方法について説明します。取り上げる事項は次のとおりです。

概要

Known Host Keys パネルを使用して、センサーが管理するブロッキング デバイスの公開鍵と、アップダートのダウンロードまたはファイルのコピーに使用される SSH（SCP）サーバの公開鍵を定義します。Known Host Keys パネル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鍵の報告を受ける必要があります。公開鍵を正しい形式で取得できない場合は、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。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

既知のホスト鍵を追加したり編集したりするには、管理者である必要があります。

フィールド定義

この項では、既知のホスト鍵のフィールド定義を示します。取り上げる事項は次のとおりです。

Known Host Keys パネル

Known Host Keys パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：鍵を追加するホストの IP アドレス。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。
  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。
  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。
  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **Add**：Add Known Host Key ダイアログボックスを開きます。
  このダイアログボックスで、新しい既知のホスト鍵を追加できます。
- **Edit**：Edit Known Host Key ダイアログボックスを開きます。
  このダイアログボックスで、この既知のホスト鍵に関連付けられた値を変更できます。
- **Delete**：リストから既知のホスト鍵を削除します。
- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Known Host Key ダイアログボックス

Add and Edit Known Host Key ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：鍵を追加するホストの IP アドレス。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。
  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。
  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。
  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **Retrieve Host Key**：IDM は、IP アドレスで指定されたホストから既知のホスト鍵を取得しようとします。取得に成功した場合、IDM は取得したホスト鍵を Add Known Host Key パネルに入力します。
  Add ダイアログボックスでのみ使用できます。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。
- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

既知のホスト鍵の定義

既知のホスト鍵を設定するには、次の手順を実行します。

ステップ 1　管理者特権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 > SSH > Known Host Keys** の順にクリックします。

Known Host Keys パネルが表示されます。

ステップ 3　**Add** をクリックして、既知のホスト鍵をリストに追加します。

Add Known Host Key ダイアログボックスが表示されます。

ステップ 4　**IP Address** フィールドに、鍵を追加するホストの IP アドレスを入力します。

ステップ 5　**Retrieve Host Key** をクリックします。

Device Manager は、ステップ 3 で入力した IP アドレスのホストから鍵を取得しようとします。取得が成功した場合、ステップ 8 に進みます。取得が失敗した場合、ステップ 5 ～ 7 を実行してください。

注意　取得した鍵が指定されたアドレスに適していることを確認し、サーバの IP アドレスがスプーフィングされてないことを確認します。

ステップ 6　**Modulus Length** フィールドに整数を入力します。

係数の長さは、係数の有意ビットの数です。RSA 鍵の強度は、係数のサイズに依存します。係数のビット数が多いほど、鍵は強力になります。

ステップ 7　**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 8　**Public Modulus** フィールドに値を入力します。

公開係数は文字列値です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。

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　変更を元に戻すには、**Reset** をクリックします。

ステップ 9　**OK** をクリックします。

Known Host Keys パネルの既知のホスト鍵リストに、新しい鍵が表示されます。

ステップ 10　許可鍵リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Authorized Key ダイアログボックスが表示されます。

ステップ 11　**Modulus Length**、**Public Exponent**、および **Public Modulus** フィールドを編集します。

注意　エントリを作成した後は、**ID** フィールドは変更できません。

ステップ 12　**OK** をクリックします。

Known Host Keys パネルの既知のホスト鍵リストに、編集された鍵が表示されます。

ステップ 13　公開鍵をリストから削除するには、それを選択して **Delete** をクリックします。

削除された鍵は、Known Host Keys パネルの既知のホスト鍵リストに表示されなくなります。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 14　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

センサー SSH ホスト鍵の表示と生成

この項では、センサー SSH ホスト鍵を表示および生成する方法を説明します。取り上げる事項は次のとおりです。

概要

サーバは SSH ホスト鍵を使用して、ID を証明します。クライアントは、既知の鍵を見つけると、正しいサーバに接続したことを認識します。

センサーでは、最初に起動したときに SSH ホスト鍵が生成されます。この SSH ホスト鍵は Sensor Key パネルに表示されます。**Generate Key** をクリックして、この鍵を新しい鍵に置換します。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサー SSH ホスト鍵を生成するには、管理者である必要があります。

フィールド定義

Sensor Key パネルにセンサー SSH ホスト鍵が表示されます。**Generate Key** ボタンによって新しいセンサー SSH ホスト鍵が生成されます。

センサー SSH ホスト鍵の表示と生成

センサー SSH ホスト鍵の表示と生成を行うには、次の手順を実行します。

ステップ 1　管理者特権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 > SSH > Sensor Key** の順にクリックします。

Sensor Key パネルが表示されます。

センサー SSH ホスト鍵が表示されます。

ステップ 3　新しいセンサー SSH ホスト鍵を生成するには、**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?
```

注意　新しい鍵で既存の鍵を置換するため、以後の接続が成功するようにリモート システムの既知のホスト テーブルを新しいホスト鍵で更新する必要があります。

ステップ 4　**OK** をクリックして続行します。

新しいホスト鍵が生成され、古いホスト鍵が削除されます。

ステータス メッセージに鍵の更新が成功したことが表示されます。

証明書の設定

センサーと証明書の詳細については、P.1-18 の「IDM と証明書」を参照してください。この項で取り上げる事項は次のとおりです。

信頼できるホストの追加

この項では、信頼できるホストを追加する方法について説明します。取り上げる事項は次のとおりです。

概要

Trusted Hosts パネルを使用して、マスター ブロッキング センサーの証明書と、このセンサーがアップデート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。

Trusted Hosts パネルには、追加したすべての信頼できるホスト証明書のリストが表示されます。IP アドレスを入力することにより、証明書を追加できます。IDM は証明書を取得して、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、証明書が信頼されます。リストにエントリを追加したり、リストからエントリを削除したりできますが、エントリを編集することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

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。

フィールド定義

この項では、信頼できるホストのフィールド定義を示します。取り上げる事項は次のとおりです。

Trusted Hosts パネル

Trusted Hosts パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：信頼できるホストの IP アドレス。
- **MD5**：Message Digest 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するアルゴリズムです。

- **SHA1**：Secure Hash Algorithm。
  SHA1 は、暗号メッセージ ダイジェスト アルゴリズムです。

ボタンの機能：

- **Add**：Add Trusted Host ダイアログボックスを開きます。
  このダイアログボックスでは、新しい信頼できるホストを追加できます。
- **View**：View Trusted Host ダイアログボックスを開きます。
  このダイアログボックスでは、信頼できるホストに関連付けられた証明書データを表示できます。
- **Delete**：リストから信頼できるホストを削除します。
- **Apply**：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。
- **Reset**:作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add Trusted Host ダイアログボックス

Add Trusted Host ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **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。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

信頼できるホストの追加

信頼できるホストを追加するには、次の手順を実行します。

ステップ 1　管理者特権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 > Trusted Hosts** の順にクリックします。

Trusted Hosts パネルが表示されます。

ステップ 3　**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。

Add Trusted Host ダイアログボックスが表示されます。

ステップ 4　**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 5　センサーが 443 以外のポートを使用している場合は、**Port** フィールドにポート番号を入力します。

ステップ 6　**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。この新しい信頼できるホストは、Trusted Hosts パネル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が、ダイアログボックスに示されます。

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

信頼できるホストの追加が成功したかどうかのステータスが、ダイアログボックスに示されます。

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

ステップ 7　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を比較して、フィンガープリントが正しいことを検証します。ステップ 7 を参照してください。両方の値が一致しない場合、その信頼できるホストをすぐに削除してください。ステップ 8 を参照してください。

ステップ 8　信頼できるホストのリストにある既存のエントリを表示するには、それを選択して **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。このダイアログボックスで表示されるデータは、読み取り専用です。

ステップ 9　**OK** をクリックします。

ステップ 10　信頼できるホストをリストから削除するには、それを選択して **Delete** をクリックします。

削除された信頼できるホストは、Trusted Hosts パネル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　変更を元に戻すには、**Reset** をクリックします。

ステップ 11　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

サーバ証明書の表示と生成

この項では、サーバ証明書を表示および生成する方法を説明します。取り上げる事項は次のとおりです。

概要

Server Certificate パネルに、センサー サーバ X.509 の証明書が表示されます。このパネルで、新しいサーバの自己署名付き X.509 証明書を生成できます。証明書は、センサーを最初に起動したときに生成されます。**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　センサーの IP アドレスが証明書に含まれます。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。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

サーバ証明書を生成するには、管理者である必要があります。

フィールド定義

Server Certificate パネルに、センサー サーバ X.509 の証明書が表示されます。**Generate Certificate** をクリックすると、新しいセンサー X.509 証明書が生成されます。

サーバ証明書の表示と生成

センサー サーバ X.509 証明書の表示と生成を行うには、次の手順を実行します。

ステップ 1　管理者特権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** の順にクリックします。

Server Certificate パネルが表示されます。

センサー サーバ X.509 証明書が表示されます。

ステップ 3　新しいセンサー サーバ X.509 証明書を生成するには、**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?
```

注意　新しいフィンガープリントを書き込みます。後で接続したとき、またはセンサーを信頼できるホストとして追加するときに、Web ブラウザに表示されるフィンガープリントを確認する必要があります。センサーがマスター ブロッキング センサーの場合は、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 センサーの、信頼できるホスト テーブルを更新する必要があります。

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、古いサーバ証明書が削除されます。

時刻の設定

この項では、時刻源とセンサーについて説明します。取り上げる事項は次のとおりです。

概要

Time パネルを使用して、日付、時刻、時間帯、サマータイム（DST）を設定し、センサーが時刻源に NTP サーバを使用するかどうかを設定します。

（注）　センサーの時刻源として NTP サーバを使用する方法を推奨します。

時刻源およびセンサー

センサーには、信頼できる時刻源が必要です。すべてのイベント（アラート）に、正しい Coordinated Universal Time（UTC; 世界標準時）と現地時間のタイムスタンプが必要です。タイムスタンプがないと、攻撃の後でログを正しく分析できません。センサーを初期化するときに、時間帯とサマータイム設定をセットアップします。詳細については、P.1-6 の「センサーの初期化」を参照してください。

センサーに時刻を設定する方法を要約して示します。

- アプライアンスの場合
  - **clock set** コマンドを使用して、時刻を設定する。これがデフォルトの方法です。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Manually Setting the System Clock」を参照してください。
  - NTP を使用する。

    アプライアンスは、NTP 同期時刻源から時刻を取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に NTP をアプライアンスにセットアップすることも、CLI、IDM、または ASDM を通して NTP を設定することもできます。

    （注）　NTP 同期時刻源を使用する方法を推奨します。

- IDSM-2 の場合
  - IDSM-2　は、自動的にその時計をスイッチ時刻と同期させることができる。これがデフォルトの方法です。

    （注）　UTC 時刻は、スイッチと IDSM-2 の間で同期が取られます。時間帯とサマータイム設定は、スイッチと IDSM-2 間で同期が取られません。

注意　スイッチと IDSM-2 の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイム設定が IDSM-2 とスイッチとで一致していない場合、IDSM2 の現地時間は不正確になる可能性があります。

- NTP を使用する。

  IDSM-2 は、その時刻を NTP 同期時刻源から取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に NTP を使用するように IDSM-2 を設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

  （注）　NTP 同期時刻源を使用する方法を推奨します。

- NM-CIDS の場合
  - NM-CIDS は、自動的にその時計を取り付け先（親ルータ）のルータ シャーシの時計と同期させることができる。これがデフォルトの方法です。

    （注）　UTC 時刻は、親ルータと NM-CIDS の間で同期が取られます。時間帯とサマータイム設定は、親ルータと NM-CIDS の間で同期が取られません。

注意　親ルータと NM-CIDS の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイムの設定が NM-CIDS とルータとで一致していない場合、NM-CIDS の現地時間は不正確になる可能性があります。

- NTP を使用する。

  NM-CIDS は、その時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に NM-CIDS を NTP を使用するように設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

  （注）　NTP 同期時刻源を使用する方法を推奨します。

- AIP SSM の場合
  - AIP SSM は、自動的にその時計を取り付け先の ASA の時計と同期させることができる。これがデフォルトの方法です。

    （注）　UTC 時刻は、ASA と AIP SSM の間で同期が取られます。時間帯とサマータイム設定は、ASA と AIP SSM の間で同期が取られません。

注意　ASA と AIP SSM の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイムの設定が AIP SSM と ASA とで一致していない場合、AIP SSM の現地時間は不正確になる可能性があります。

- NTP を使用する。

  AIP SSM は、その時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に AIP SSM を NTP を使用するように設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

（注）　NTP 同期時刻源を使用する方法を推奨します。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

時刻設定を設定するには、管理者である必要があります。

フィールド定義

この項では、時刻のフィールド定義を示します。取り上げる事項は次のとおりです。

- Time パネル（P.2-23）
- Configure Summertime ダイアログボックス（P.2-24）

Time パネル

Time パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Sensor Local Date**：センサー上の現在の日付。

  デフォルトは 1970 年 1 月 1 日です。日付の値が月の範囲外の場合、エラー メッセージが表示されます。

- **Sensor Local Time**：センサー上の現在の時刻（hh:mm:ss）。

  デフォルトは 00:00:00 です。時間、分、または秒が範囲外の場合はエラー メッセージが表示されます。

（注）　センサーが日付フィールドや時刻フィールドをサポートしていない場合、またはセンサー上で NTP 設定を設定していない場合、これらのフィールドはディセーブルになっています。

- **Standard Time Zone**：時間帯の名前と UTC オフセットを設定します。
  - **Zone Name**：サマータイムが実施されていない場合のローカル時間帯。

    デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24　文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
  - **UTC Offset**：ローカル時間帯のオフセット（分単位）。

    デフォルトは 0 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。
- **NTP Server**：センサーが時刻源として NTP サーバを使用するように設定します。
  - **IP Address**：NTP サーバを使用してセンサー上の時刻を設定する場合、NTP サーバの IP アドレス。
  - **Key**：NTP MD5 鍵タイプ。
  - **Key ID**：NTP サーバ上で認証に使用される鍵の ID（1 ～ 65535）。

    鍵 ID が範囲外の場合は、エラー メッセージが表示されます。
- **Summertime**：サマータイム設定をイネーブルにし、その設定をします。
  - **Enable Summertime**：ここをクリックすると、サマータイム モードがイネーブルになります。

    デフォルトはディセーブルです。

ボタンの機能：

- **Configure Summertime**：ここをクリックすると、Configure Summertime ダイアログボックスが開きます。

  Configure Summertime ダイアログボックスを開くことができるのは、**Enable Summertime** を選択した場合のみです。
- **Apply**：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。

  Time パネル上のその他の設定（NTP、サマータイム、標準時間帯の設定など）が変更された場合、**Apply** がイネーブルになります。**Apply** は、日付と時刻を除く、Time パネル上のすべてのフィールドに対応しています。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。
- **Apply Time to Sensor**：センサー上の日付と時刻を設定します。

  Apply Time to Sensor は日付と時刻を変更した場合にのみ、イネーブルになります。変更した日付と時刻をセンサーに保存する場合は、**Apply Time to Sensor** をクリックする必要があります。

Configure Summertime ダイアログボックス

Configure Summertime ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Summer Zone Name**：サマータイム時間帯の名前。

  デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
- **Offset**：サマータイム中に付加する時間数。

  デフォルトは 60 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。
- **Start Time**：サマータイム開始時刻の設定。

  値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- **End Time**：サマータイム終了時刻の設定。

  値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。

- **Summertime Duration**：サマータイム期間が毎年実施されるか、1 回だけの日付かを設定します。
  - **Recurring**：サマータイム期間は recurring（毎年実施される）モードです。
  - **Date**：サマータイム期間は、nonrecurring（毎年実施されない）モードです。
  - **Start**：開始の週、日、月の設定。
  - **End**：終了の週、日、月の設定。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

センサー上の時刻の設定

センサー上の時刻を設定するには、次の手順を実行します。

ステップ 1　管理者特権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 > Time** の順にクリックします。

Time パネルが表示されます。

ステップ 3　**Date** で、ドロップダウン ボックスから現在の時刻を選択します。

日付は、ローカル ホストの日付を示しています。

ステップ 4　**Time** で、現在の時刻（hh:mm:ss）を入力します。

時間は、ローカル ホストの時間を示しています。現在の時刻を表示するには、**Refresh** をクリックします。

注意　間違えて誤った時刻を指定すると、ストアされたイベントに間違ったタイムスタンプが設定されます。この場合は、イベントをクリアする必要があります。詳細については、P.2-27 の「センサー上の時刻の修正」を参照してください。

（注）　NTP を設定済みの場合、モジュール上の日付や時刻は変更できません。

ステップ 5　Standard Time Zone で次を実行します。

a. **Zone Name** フィールドのドロップダウン ボックスから時間帯を選択するか、または作成済みの時間帯を入力します。

これは、サマータイム時間が実施されていない場合に表示される時間帯です。

b. **UTC Offset** フィールドに、UTC のオフセットを分単位で入力します。

事前に定義された時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

ステップ 6　NTP 時刻同期を使用している場合は、**NTP Server** で次を入力します。

a. **IP Address** フィールドに NTP サーバの IP アドレスを入力する。

b. **Key** フィールドに NTP サーバの鍵を入力する。

c. **Key ID** フィールドに NTP サーバの鍵 ID を入力する。

（注）　NTP サーバを定義すると、センサーの時刻は NTP サーバによって設定されます。CLI の **clock set** コマンドを実行するとエラーが発生しますが、時間帯とサマータイムのパラメータは有効です。

ステップ 7　サマータイムをイネーブルにするには、Summertime で **Enable Summertime** を選択します。

ステップ 8　**Configure Summertime** をクリックします。

Configure Summertime ダイアログボックスが表示されます。

ステップ 9　ドロップダウン ボックスから Summer Zone Name を選択するか、または作成済みのサマータイム名を入力します。

これは、サマータイム時間が実施されている間に表示される時間帯名です。

ステップ 10　サマータイム中に付加する時間数を入力します。

事前に定義されたサマータイム時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

ステップ 11　**Start Time** フィールドに、サマータイム設定に適用する時刻を入力します。

ステップ 12　**End Time** フィールドに、サマータイム設定から削除する時刻を入力します。

ステップ 13　**Summertime Duration** で、サマータイム設定が毎年指定された日付に発生する（recurring）か、または指定された日付で開始および終了する（date）かを選択します。

a. Recurring：ドロップダウン ボックスから開始時刻と終了時刻を選択します。

デフォルトは 4 月の第 1 日曜日と 10 月の最終日曜日です。

b. Date：ドロップダウン ボックスから開始時刻と終了時刻を選択します。

開始および終了時刻のデフォルトは、1 月 1 日です。

ステップ 14　**OK** をクリックします。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 15　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

ステップ 16　時刻と日付の設定を変更した場合（ステップ 1 と 2）、**Apply Time to Sensor** の順にクリックして、変更した設定をセンサーに保存します。

センサー上の時刻の修正

イベントには発生時の時刻が刻印されるため、時刻を誤って設定した場合、保存されたイベントの時刻は不正確になります。

イベント ストアのタイムスタンプは、常に UTC 時刻に基づいています。イベント発生元になるセンサーのセットアップ中に、8:00 a.m. と間違えて 8:00 p.m. に時間を設定した場合、エラーを修正すると、修正された時間は過去に設定されます。新しいイベントが、古いイベントよりも古くなることがあります。

たとえば、初期セットアップ中にセンサーを中部時間でサマータイムが使用可能と設定し、現地時間が 8:04 p.m. だった場合、時間は 20:04:37 CDT として表示され、UTC からのオフセットは -5 時間になります（翌日の 01:04:37 UTC）。1 週間後の 9:00 a.m. に、時計が 21:00:23 CDT と表示され、エラーに気づいたとします。時間を 9:00 a.m. に変更すると、時計は 09:01:33 CDT と表示されます。UTC からのオフセットは変更されていないので、UTC 時間は 14:01:33 UTC になりますが、これがタイムスタンプの問題の原因になります。

イベント レコード上のタイムスタンプの整合性を保証するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブをクリアする必要があります。**clear events** コマンドの詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Clearing Events from the Event Store」を参照してください。

注意　イベントを個別に削除することはできません。

ユーザの設定

この項では、ユーザをシステムに追加する方法およびシステムから削除する方法について説明します。取り上げる事項は次のとおりです。

概要

IDM では、一度に複数のユーザがログインできます。ローカル センサーからユーザを作成および削除することができます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザは、ユーザが何を変更でき何を変更できないかを制御するロールに関連付けられます。

ユーザには、次の 4 つのロールがあります。

- ビューア：イベントの表示と設定ができますが、自分のユーザ パスワード以外の設定データは修正できません。
- オペレータ：すべてを表示でき、次のオプションを修正できます。
  - シグニチャ チューニング（優先順位、使用不可、使用可能）
  - 仮想センサーの定義
  - 管理対象ルータ
  - 自分のユーザ パスワード
- 管理者：すべてを表示でき、オペレータが修正できるすべてのオプションを修正でき、さらに次のオプションを修正できます。
  - センサーのアドレス設定
  - 設定エージェントまたはビュー エージェントとして接続できるホストのリスト
  - 物理検知インターフェイスの割り当て
  - 物理インターフェイスの制御をイネーブルまたはディセーブルにする
  - ユーザとパスワードの追加と削除
  - 新しい SSH ホスト鍵とサーバ証明書の生成
- サービス：サービス特権が付与されたユーザは、1 つのセンサーに 1 人だけ作成できます。サービス ユーザは、IDM にログインできません。サービス ユーザは、CLI ではなく bash シェルにログインします。

（注） サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。許可されるサービス アカウントは 1 つだけです。トラブルシューティング用には、サービス ロールのアカウントのみを作成してください。サービス アカウントを編集できるのは、管理者特権を持つユーザだけです。

注意 サービス アカウントを作成するかどうかは慎重に検討してください。サービス アカウントは、システムへのシェル アクセスを提供します。これにより、システムは脆弱になります。しかし、サービス アカウントを使用すると、管理者パスワードを喪失した場合に新規パスワードを作成することができます。状況を分析して、サービス アカウントをシステム上に存在させるかどうかを決定します。

サービス アカウントにログインすると、次の警告が表示されます。

```
********************** WARNING ************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and
troubleshooting purposes only. Unauthorized modifications
are not supported and will require this device to be
re-imaged to guarantee proper operation.
*******************************************************
```

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ユーザの追加と編集を行うには、管理者である必要があります。

フィールド定義

この項では、ユーザのフィールド定義を示します。取り上げる事項は次のとおりです。

- Users パネル（P.2-29）
- Add and Edit User ダイアログボックス（P.2-30）

Users パネル

Users パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Username**：ユーザ名。
  値は、1 ～ 64 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ に一致するパターンです。
- **Role**：ユーザ ロール。
  値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。
- **Status**：現在のユーザ アカウントのステータス（active、expired、または locked）を表示します。

ボタンの機能：

- **Add**：Add User ダイアログボックスを開きます。
  このダイアログボックスでは、新しいユーザをユーザ リストに追加できます。
- **Edit**：Edit User ダイアログボックスを開きます。
  このダイアログボックスでは、ユーザ リストにあるユーザを編集できます。
- **Delete**：ユーザ リストからユーザを削除します。
- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit User ダイアログボックス

Add and Edit User ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Username**：ユーザ名。
  有効な値は、1 ～ 64 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ に一致するパターンです。
- **User Role**：ユーザ ロール。
  有効な値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。
- **Password**：ユーザのパスワード。
  パスワードは 6 文字以上である必要があります。
- **Confirm Password**：パスワードを確認します。
  確認パスワードとユーザ パスワードが一致しない場合、エラー メッセージが表示されます。
- **Change the password to access the sensor**：ユーザのパスワードを変更します。
  Edit ダイアログボックスでのみ使用できます。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ユーザの設定

センサー上のユーザを設定するには、次の手順を実行します。

ステップ 1　管理者特権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 > Users** の順にクリックします。

Users パネルが表示されます。

ステップ 3　**Add** をクリックして、ユーザを追加します。

Add User ダイアログボックスが表示されます。

ステップ 4　**Username** フィールドにユーザ名を入力します。

ステップ 5　**User Role** フィールドのドロップダウン リストから、次のいずれかのユーザ ロールを選択します。

- 管理者
- オペレータ
- ビューア
- サービス

ステップ 6　**Password** フィールドに、そのユーザの新しいパスワードを入力します。

ステップ 7　**Confirm Password** フィールドで、そのユーザの新しいパスワードを確認します。

ステップ 8　**OK** をクリックします。

新しいユーザが、Users パネルのユーザ リストに表示されます。

ステップ 9　ユーザを編集するには、ユーザ リストにあるユーザを選択し、**Edit** をクリックします。

Edit User ダイアログボックスが表示されます。

ステップ 10　**Change the password to access the sensor** チェックボックスをオンにします。

ステップ 11　**User Role** フィールドと **Password** フィールドに必要な変更を行います。

ステップ 12　**OK** をクリックします。

編集したユーザが、Users パネルのユーザ リストに表示されます。

ステップ 13　ユーザをユーザ リストから削除するには、それを選択して **Delete** をクリックします。

削除されたユーザは、User パネルのユーザ リストに表示されなくなります。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 14　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。