CHAPTER 4

IPS SSP 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、IPS SSP のセットアップについて説明します。次の事項について説明します。

- 「初期設定の概要」（P.4-1）
- 「ネットワークの設定」（P.4-2）
- 「[Allowed Hosts/Networks] の設定」（P.4-5）
- 「時刻の設定」（P.4-7）
- 「認証およびユーザの設定」（P.4-14）

初期設定の概要

ネットワークに設置した IPS SSP に、ネットワークを介して通信できるようにするには、**setup** コマンドを使用して初期設定する必要があります。**setup** コマンドを使用して IPS SSP を初期設定するまでは、IDM を設定できません。

setup コマンドによって、ホスト名、IP インターフェイス、アクセス コントロール リスト、グローバル相関サーバ、時刻設定などの基本センサー設定を行います。これに続いて CLI で拡張セットアップを使用して、Telnet のイネーブル化、Web サーバの設定、および仮想センサーとインターフェイスの割り当てとイネーブル化を実行できます。または、IDM の Startup Wizard を使用することもできます。

詳細情報

IPS SSP の初期設定手順については、第 18 章「IPS SSP の初期化」を参照してください。

ネットワークの設定

ここでは、ネットワーク設定の変更方法について説明します。次の事項について説明します。

- 「[Network] ペイン」（P.4-2）
- 「[Network] ペインのフィールド定義」（P.4-2）
- 「ネットワークの設定」（P.4-3）

[Network] ペイン

（注）　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。

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 パラメータおよび通信パラメータの値が [Network] ペインに表示されます。これらのパラメータの値は、必要に応じて [Network] ペインで変更できます。

[Network] ペインのフィールド定義

[Network] ペインには次のフィールドが表示されます。

- [Network Settings]：センサーのネットワーク パラメータをイネーブルにします。
  - [Hostname]：センサーの名前。ホスト名は、^[A-Za-z0-9_/-]+$ のパターンと一致する 1 ～ 64 文字のストリングにすることができます。デフォルトは sensor です。名前にスペースが含まれる場合、または名前が 64 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。
  - [IP Address]：センサーの IP アドレス。デフォルトは 192.168.1.2 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 ゲートウェイ アドレス。デフォルトは 192.168.1.1 です。
- [DNS/Proxy Settings]：グローバル相関をサポートする HTTP プロキシ サーバと DNS サーバのいずれかを設定できます。
  - [HTTP Proxy Server]：プロキシ サーバの IP アドレスを入力できます。ネットワークでプロキシを使用する場合、プロキシ サーバを使用してグローバル相関の更新をダウンロードする必要がある場合があります。
  - [HTTP Proxy Port]：プロキシ サーバのポート番号を入力できます。
  - [DNS Primary]：プライマリ DNS サーバの IP アドレスを入力できます。
  - [DNS Secondary]：セカンダリ DNS サーバの IP アドレスを入力できます。
  - [DNS Tertiary]：ターシャリ DNS サーバの IP アドレスを入力できます。

    DNS サーバを使用する場合、グローバル相関の更新が成功するには、DNS サーバを 1 台以上設定する必要があり、このサーバに到達できる必要があります。他の DNS サーバは、バックアップ サーバとして設定できます。DNS クエリーは、リストの最初のサーバに送信されます。このサーバが到達不能な場合、DNS クエリーは設定されている次の DNS サーバに送信されます。

注意　グローバル相関が機能するには、DNS サーバと HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル相関更新サーバへのアクセスについてだけサポートされています。

- HTTP、FTP、Telnet、CLI、およびその他のオプション
  - [Web Server Port] : Web サーバが使用する TCP ポート。デフォルトは HTTPS の 443 です。

    （注）　1 ～ 65535 の範囲の値を入力すると、エラー メッセージが表示されます。

  - [Enable TLS/SSL on HTTP] : Web サーバで TLS および SSL をイネーブルにします。デフォルトではイネーブルです。

    （注）　TLS および SSL はイネーブルにしておくことを強く推奨します。

  - [FTP Timeout] : センサーが FTP サーバと通信する場合に FTP クライアントがタイムアウトになるまでの秒数を設定します。有効な値の範囲は 1 ～ 86400 秒です。デフォルトは 300 秒です。
  - [Enable Telnet] : センサーへのリモート アクセスで Telnet をイネーブルまたはディセーブルにします。

    （注）　Telnet はセキュアなアクセス サービスではないため、デフォルトでは無効になっています。

  - [Allow Password Recovery] : パスワードの回復をイネーブルにします。デフォルトではイネーブルです。

詳細情報

グローバル相関の詳細については、第 11 章「グローバル相関の設定」を参照してください。

ネットワークの設定

注意　グローバル相関機能が動作するには、有効なセンサー ライセンスが必要です。グローバル相関機能の統計情報は引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

ネットワークを設定するには、次の手順に従ってください。

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] > [Network] を選択します。

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 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　グローバル相関をサポートする 1 台の HTTP プロキシ サーバまたは 1 台以上の DNS サーバを設定するには、[HTTP Proxy Server] フィールドに HTTP プロキシ サーバの IP アドレスを入力し、[HTTP Proxy Port] フィールドにポート番号を入力するか、または [DNS Primary] フィールドに DNS サーバの IP アドレスを入力します。

DNS サーバを使用する場合、グローバル相関の更新が成功するには、DNS サーバを 1 台以上設定する必要があり、このサーバに到達できる必要があります。他の DNS サーバは、バックアップ サーバとして設定できます。DNS クエリーは、リストの最初のサーバに送信されます。このサーバが到達不能な場合、DNS クエリーは設定されている次の DNS サーバに送信されます。

注意　グローバル相関が機能するには、DNS サーバと HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル相関更新サーバへのアクセスについてだけサポートされています。

グローバル相関をオンにしない場合、次の [Warning] ダイアログボックスで [OK] をクリックします。

```
DNS or HTTP proxy is required for グローバル相関 inspection and reputation filters, but no
DNS or proxy servers are defined. Do you want to continue?
```

ステップ 8　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した場合は、IDM へ接続するときに、ブラウザの URL アドレス内でポートを指定する必要があります。その場合、使用する URL は https://*sensor_ip_address*:*port_number* という形式です（https://10.1.9.201:1040 など）。

ステップ 9　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 on HTTP] チェック ボックスをオンにします。

（注）　TLS/SSL は有効にしておくことを強く推奨します。

（注）　TLS および SSL は、Web ブラウザと Web サーバの間の暗号化通信を可能にするプロトコルです。TLS/SSL がイネーブルの場合、https://*sensor_ip_address* を使用して IDM に接続します。TLS/SSL がディセーブルの場合、http://*sensor_ip_address*:*port_number* を使用して IDM に接続します。

ステップ 10　FTP タイムアウトの秒数を変更するには、[FTP Timeout] フィールドに新しい秒数を入力します。デフォルトは 300 秒です。

ステップ 11　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] チェック ボックスをオンにします。

（注）　Telnet はセキュアなアクセス サービスではないため、デフォルトでは無効になっています。ただし、センサー上でセキュアなサービスである SSH が常時実行されています。

ステップ 12　パスワードの回復を有効にするには、[Allow Password Recovery] チェック ボックスをオンにします。

（注）　パスワードの回復はイネーブルにすることを強く推奨します。イネーブルにしないと、パスワードの問題が発生した場合に、アクセスできるようにするために、センサーのイメージを再作成する必要があります。

ヒント　変更を取り消すには、[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。

（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。

詳細情報

グローバル相関の詳細については、第 11 章「グローバル相関の設定」を参照してください。

[Allowed Hosts/Networks] の設定

ここでは、許可ホストおよびネットワークをシステムに追加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。

- 「[Allowed Hosts/Networks] ペイン」（P.4-5）
- 「[Allowed Hosts/Network] ペインおよび [Add and Edit Allowed Host] ダイアログボックスのフィールドの定義」（P.4-6）
- 「[Allowed Hosts/Networks] の設定」（P.4-6）

[Allowed Hosts/Networks] ペイン

（注）　許可ホストおよび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。

setup コマンドを使用してセンサーを初期化すると、許可ホスト パラメータの値が [Allowed Hosts/Networks] ペインに表示されます。これらのパラメータの値は、必要に応じて [Allowed Hosts/Networks] ペインで変更できます。[Allowed Hosts/Networks] ペインを使用して、センサーへのアクセスを許可するホストまたはネットワークを指定します。デフォルトでは、リストにはエントリはなく、したがって、ホストを追加するまで、ホストはアクセスを許可されません。

（注） 許可ホスト リストには、ASDM、IDM、IME、Cisco Security Manager などの管理ホスト、および Cisco Security MARS 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、または削除するときは、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。

[Allowed Hosts/Network] ペインおよび [Add and Edit Allowed Host] ダイアログボックスのフィールドの定義

[Allowed Hosts/Networks] ペインおよび [Add and Edit Allowed Host] ダイアログボックスには、次のフィールドが表示されます。

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

[Allowed Hosts/Networks] の設定

センサーへのアクセスを許可するホストおよび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] > [Allowed Hosts/Networks] を選択し、[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。最大で 512 の許可ホストを追加できます。

ステップ 3　[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。IP アドレスが既存のリスト エントリの一部としてすで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 4　[Network Mask] フィールドに、ホストまたはネットワークのネットワーク マスクを入力するか、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 アドレスであるか、ネットワーク アドレスであるかに関係なく、ネットマスクを常に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にも、エラー メッセージが表示されます。

ヒント 変更を廃棄して [Add Allowed 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。[Allowed Hosts/Networks] ペイン内のリストに、新しいホストまたはネットワークが表示されます。

ステップ 6　リスト内の既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 7　[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 8　[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。

ヒント　変更を廃棄して [Edit Allowed 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 9　[OK] をクリックします。[Allowed Hosts/Networks] ペイン内のリストに、編集済みのホストまたはネットワークが表示されます。

ステップ 10　ホストまたはネットワークをリストから削除するには、ホストまたはネットワークを選択し、[Delete] をクリックします。[Allowed Hosts/Networks] ペイン内のリストからホストが削除されます。

注意　ホストを削除すると、それ以降そ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　変更を破棄するには、[Reset] をクリックします。

ステップ 11　[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。

時刻の設定

ここでは、時刻源および IPS SSP について説明します。次の事項について説明します。

- 「[Time] ペイン」（P.4-7）
- 「時刻源および IPS SSP」（P.4-8）
- 「IPS SSP クロックと適応型セキュリティ アプライアンス クロックの同期化」（P.4-8）
- 「IPS SSP と NTP サーバの同期化の確認」（P.4-8）
- 「[Time] ペインのフィールドの定義」（P.4-9）
- 「[Configure Summertime] ダイアログボックスのフィールドの定義」（P.4-10）
- 「センサーの時刻の設定」（P.4-10）
- 「センサーの時刻の修正」（P.4-12）
- 「Cisco ルータを NTP サーバにする設定」（P.4-13）
- 「イベントのクリア」（P.4-14）

[Time] ペイン

（注）　時刻を設定するには、管理者である必要があります。

[Time] ペインを使用して、センサーのローカル日付、時刻、時間帯、サマータイム（DST）、およびセンサーで時刻源として NTP サーバを使用するかどうかを設定します。

（注）　センサー時刻源として NTP サーバを使用することを推奨します。

時刻源および IPS SSP

IPS SSP 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 UTC（グリニッジ標準時）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。IPS SSP を初期化するとき、時間帯およびサマータイムを設定します。
IPS SSP で時刻を設定するには、次の 2 つの方法があります。

- IPS SSP のクロックは、インストール先の適応型セキュリティ アプライアンスのクロックと自動的に同期されます。これはデフォルトです。
- 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 IPS SSP を設定できます。

（注） NTP サーバを使用することを推奨します。認証付き NTP または認証のない NTP を使用できます。認証付き NTP の場合は、NTP サーバの IP アドレス、NTP サーバのキー ID、および NTP サーバのキー値が必要です。初期設定中に NTP をセットアップすることも、CLI、IDM、IME、または ASDM を使用して、後から NTP を設定することもできます。

詳細情報

- NTP を設定する手順については、「ネットワークの設定」（P.4-3）を参照してください。
- Cisco ルータを NTP サーバとして設定する手順については、「Cisco ルータを NTP サーバにする設定」（P.4-13）を参照してください。

IPS SSP クロックと適応型セキュリティ アプライアンス クロックの同期化

IPS SSP を起動するたび、および適応型セキュリティ アプライアンスのクロックが設定されるたびに、そのシステム クロックが親シャーシのクロック（適応型セキュリティ アプライアンス）と同期化されます。時間が経過すると、IPS SSP クロックと適応型セキュリティ アプライアンス クロックの間に差異が発生します。差異は、1 日あたり数秒に及ぶことがあります。この問題を回避するには、IPS SSP クロックと適応型セキュリティ アプライアンス クロックの両方を外部の NTP サーバと同期させます。NTP サーバに IPS SSP クロックのみ同期させた場合、または適応型セキュリティ アプライアンス シャーシ クロックのみ同期させた場合、時刻の差異が発生します。

詳細情報

IPS SSP での時刻修正の詳細については、「センサーの時刻の修正」（P.4-12）を参照してください。

IPS SSP と NTP サーバの同期化の確認

Cisco IPS では、無効な NTP キー値や ID など、誤った NTP 設定はセンサーに適用できません。誤った設定を適用しようとすると、エラー メッセージが表示されます。NTP 設定を確認するには、**show statistics host** コマンドを使用してセンサーの統計情報を収集します。[NTP statistics] セクションには、NTP サーバとセンサーの同期に関するフィードバックなどの NTP 統計情報が表示されます。

NTP 設定を確認するには、次の手順に従ってください。

ステップ 1　センサーにログインします。

ステップ 2　ホストの統計情報を生成します。

```
sensor# show statistics host
     ...
```

```
NTP Statistics
        remote           refid      st t when poll reach   delay   offset  jitter
    11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
    LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
   ind assID status  conf reach auth condition  last_event cnt
     1 10372  f014   yes   yes   ok     reject   reachable  1
     2 10373  9014   yes   yes  none    reject   reachable  1
   status = Not Synchronized
...
```

ステップ 3　数分後にホストの統計情報を再度生成します。

```
sensor# show statistics host
...
NTP Statistics
        remote           refid      st t when poll reach   delay   offset  jitter
   *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
    LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
   ind assID status  conf reach auth condition  last_event cnt
     1 10372  f624   yes   yes   ok   sys.peer   reachable  2
     2 10373  9024   yes   yes  none    reject   reachable  2
   status = Synchronized
```

ステップ 4　状態が引き続き `Not Synchronized` の場合は、NTP サーバの管理者に相談して、NTP サーバが正しく設定されていることを確認してください。

[Time] ペインのフィールドの定義

[Time] ペインには次のフィールドが表示されます。

- [Sensor Local Date]：センサーの現在の日付。デフォルト値は 1970 年 1 月 1 日です。日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]：センサーの現在の時刻（hh:mm:ss）。デフォルト値は 00:00:00 です。時間、分、または秒が範囲外の場合、エラー メッセージが表示されます。

（注）　センサーが日付および時刻のフィールドをサポートしていない場合、またはセンサーで NTP 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です。

- [Standard Time Zone]：時間帯名および UTC オフセットを設定できます。
  - [Zone Name]：サマータイムが有効でないときの現地時間帯。デフォルトは UTC です。事前定義済みの 37 セットの時間帯から選択するか、^[A-Za-z0-9()+:,_/-]+$ というパターンと一致する一意の名前（24 文字）を作成することができます。
  - [UTC Offset]：現地時間帯オフセット（分単位）。デフォルトは 0 です。事前定義済みの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設定されます。

（注）　時間帯オフセットを変更するには、センサーをリブートする必要があります。

- [NTP Server]：時刻源として NTP サーバを使用するようにセンサーを設定できます。
  - [IP Address]：NTP サーバの IP アドレス（NTP サーバを使用してセンサーの時刻を設定する場合）。
  - [Authenticated NTP]：キーおよびキー ID の必要な認証付きの NTP を使用できます。

  - [Key] : NTP MD5 キー タイプ。
  - [Key ID] : NTP サーバでの認証に使用するキーの ID（1 ～ 65535）。範囲外のキー ID を指定すると、エラー メッセージが表示されます。
  - [Unauthenticated NTP] : NTP を使用でき、認証は必要ありません。したがって、キーやキー ID も必要ありません。
- [Summertime] : サマータイム設定をイネーブルにすること、および設定することができます。
  - [Enable Summertime] : 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。デフォルトではディセーブルです。

[Configure Summertime] ダイアログボックスのフィールドの定義

[Configure Summertime] ダイアログボックスには、次のフィールドがあります。

- [Summer Zone Name] : サマータイム ゾーン名。デフォルトは UTC です。事前定義済みの 37 セットの時間帯から選択するか、^[A-Za-z0-9()+:,_/-]+$ というパターンと一致する一意の名前（24 文字）を作成することができます。
- [Offset] : サマータイム中に加える分数。デフォルトは 60 です。事前定義済みの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設定されます。

（注） 時間帯オフセットを変更するには、センサーをリブートする必要があります。

- [Start Time] : サマータイムの開始時刻設定。値は、hh:mm です。範囲外の時間または分を指定すると、エラー メッセージが表示されます。
- [End Time] : サマータイムの終了時刻設定。値は、hh:mm です。範囲外の時間または分を指定すると、エラー メッセージが表示されます。
- [Summertime Duration] : 期間を定期にするか、単一の日付にするかを設定できます。
  - [Recurring] : 期間は定期モードです。
  - [Date] : 期間は非定期モードです。
  - [Start] : 開始する週、曜日、月の設定。
  - [End] : 終了する週、曜日、月の設定。

センサーの時刻の設定

センサー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] > [Time] を選択します。

ステップ 3　[Sensor Local Date] で、ドロップダウン リストから現在の日付を選択します。日付とは、ローカル ホストの日付のことです。

ステップ 4　[Sensor Local Time] に、現在の時刻（hh:mm:ss）を入力します。時刻とは、ローカル ホストの時刻のことです。現在の時刻を表示する場合は、[Refresh] をクリックします。

注意　誤った時刻を指定すると、保存されているイベントに誤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。

（注）　NTP を設定した場合、モジュールの日付または時刻は変更できません。

ステップ 5　[Standard Time Zone] で、時間帯およびオフセットを設定します。

a.　[Zone Name] フィールドで、ドロップダウン リストから時間帯を選択するか、作成した時間帯を入力します。これは、サマータイムの時間が有効でないときに表示される時間帯です。

b.　[UTC Offset] フィールドに、UTC からのオフセット（分単位）を入力します。事前定義済みの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設定されます。

（注）　時間帯オフセットを変更するには、センサーをリブートする必要があります。

ステップ 6　NTP 同期を使用する場合は、[NTP Server] の下で次の内容を入力します。

- NTP サーバの IP アドレス（[IP Address] フィールド）。
- 認証付き NTP を使用する場合は、[Authenticated NTP] チェックボックスをオンにして、NTP サーバのキーを [Key] フィールドに入力し、NTP サーバのキー ID を [Key ID] フィールドに入力します。
- 認証なし NTP を使用する場合は、[Unauthenticated NTP] チェックボックスをオンにします。

（注）　NTP サーバを定義すると、センサーの時間はその 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、時間帯のパラメータおよびサマータイムのパラメータは有効です。

（注）　センサー時刻源として NTP サーバを使用することを推奨します。

ステップ 7　サマータイムをイネーブルにするには、[Enable Summertime] チェックボックスをオンにします。

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

ステップ 9　ドロップダウン リストから [Summer Zone Name] を選択するか、作成した名前を入力します。これは、サマータイムが有効な場合に表示される名前です。

ステップ 10　サマータイム期間中に時計を進める時間幅（分数）を、[Offset] フィールドに入力します。事前定義済みの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設定されます。

（注）　時間帯オフセットを変更するには、センサーをリブートする必要があります。

ステップ 11　サマータイム設定の適用を開始する時刻を、[Start Time] フィールドに入力します。

ステップ 12　サマータイム設定を解除する時刻を、[End Time] フィールドに入力します。

ステップ 13　[Summertime Duration] の下で、サマータイム設定を毎年特定の期間有効にするのか（recurring）、特定の日付で開始および終了するのか（date）を選択します。

a. [Recurring]：ドロップダウン リストから開始時間と終了時間を選択します。デフォルトは、3 月の第 2 日曜日と、11 月の第 1 日曜日です。

b. [Date]：ドロップダウン リストから開始時刻と終了時刻を選択します。デフォルトは、開始時刻、終了時刻とも 1 月 1 日です。

ヒント　変更を廃棄して [Configure Summertime] 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 14　[OK] をクリックします。

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 15　[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。

ステップ 16　時刻および日付の設定を変更した場合（ステップ 3 およびステップ 4）、[Apply Time to Sensor] をクリックして、センサーの時刻および日付の設定を保存する必要もあります。

センサーの時刻の修正

保存されているイベントには、その作成時刻がタイムスタンプとして記録されるため、時刻を正確に設定しないと、それらのイベントに対しても正確な時刻が記録されません。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。元のセンサー設定で時刻に誤って 8:00 p.m. を指定し、正しい時刻の 8:00 a.m. にエラーを訂正した場合、訂正した時刻は、さかのぼって設定されます。そのため、新しいイベントに古いイベントの時刻よりも過去の時刻が記録される場合があります。

たとえば、初期セットアップ中にセンサーを中部時間に設定し、さらにサマータイムをイネーブルにした場合、現地時間が 8:04 p.m. であれば、時刻は 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、21:00:23 CDT と表示された時計を見て誤りに気づいたとします。この場合、時刻を 9:00 a.m. に変更すれば、時計は 09:01:33 CDT と表示されます。ただし、UTC からのオフセットは変更されていないため、UTC 時刻は 14:01:33 UTC になります。この結果、タイムスタンプの問題が生じます。

イベント レコードにおけるタイムスタンプの整合性を維持するには、**clear events** コマンドを使用して、過去の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。

（注）　イベントは、個別には削除できません。

詳細情報

イベント ストアからイベントをクリアする手順については、「イベントのクリア」（P.4-14）を参照してください。

Cisco ルータを NTP サーバにする設定

センサーが NTP サーバを時刻源として使用するためには、センサーと NTP サーバの間に認証済みの接続が必要です。センサーがキーの暗号化のためにサポートしているのは、MD5 ハッシュ アルゴリズムのみです。Cisco ルータが NTP サーバとして動作するようにし、その内部クロックを時刻源として使用するには、次の手順を使用します。

注意　センサーの NTP 機能は、NTP サーバとして動作する Cisco ルータと互換性を持つように設計されています。センサーは他の NTP サーバとも連携できますが、テストまたはサポートされていません。

（注）　NTP サーバのキー ID とキー値を手元に用意してください。NTP サーバを時刻源として使用するようにセンサーを設定する場合、NTP サーバの IP アドレスと共にこれらが必要になります。

Cisco ルータが NTP サーバとして動作するように設定するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
router# configure terminal
```

ステップ 3　キー ID とキー値を作成します。

```
router(config)# ntp authentication-key key_ID md5 key_value
```

キー ID は、1 から 65535 までの数値です。キー値はテキスト（数字または文字）です。これは、後で暗号化されます。

例

```
router(config)# ntp authentication-key 100 md5 attack
```

（注）　センサーがサポートするのは MD5 キーのみです。

（注）　すでにルータにキーが存在する場合もあります。他のキーを確認するには、**show running configuration** コマンドを使用します。これらの値は、信頼できるキーとしてステップ 4 で使用されます。

ステップ 4　ステップ 3 で作成したキーを信頼できるキーとして指定（または既存のキーを使用）します。

```
router(config)# ntp trusted-key key_ID
```

信頼できるキーの ID は、ステップ 3 のキー ID と同じ数値です。

例

```
router(config)# ntp trusted-key 100
```

ステップ 5　センサーが通信するルータのインターフェイスを指定します。

```
router(config)# ntp source interface_name
```

例

```
router(config)# ntp source FastEthernet 1/0
```

ステップ 6　センサーに割り当てる NTP マスター ストラタム番号を指定します。

```
router(config)# ntp master stratum_number
```

例

```
router(config)# ntp master 6
```

NTP マスター ストラタム番号は、NTP 階層におけるサーバの相対的な位置を示します。1 ～ 15 までの番号を選択できます。どの番号を選択するかは、センサーに対して重要ではありません。

イベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアからイベントをクリアするには、次の手順を実行します。

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

ステップ 2　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　イベントをクリアする場合は、**yes** と入力します。

認証およびユーザの設定

ここでは、ユーザをシステムに追加する方法、およびユーザをシステムから削除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。

- 「[Authentication] ペイン」（P.4-14）
- 「[Authentication] ペインのフィールドの定義」（P.4-15）
- 「[Add and Edit User] ダイアログボックスのフィールドの定義」（P.4-15）
- 「ユーザ ロールについて」（P.4-15）
- 「サービス アカウントについて」（P.4-16）
- 「ユーザの追加、編集、削除およびアカウントの作成」（P.4-17）

[Authentication] ペイン

（注）　ユーザを追加および編集するには、管理者である必要があります。

IDM では、同時に複数のユーザがログインできます。ローカル センサーでは、ユーザの作成および削除を行えます。一度に 1 つのユーザ アカウントのみ変更できます。各ユーザは、その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ます。

[Authentication] ペインのフィールドの定義

[Authentication] ペインには次のフィールドが表示されます。

- [Username] : ユーザ名は ^[A-Za-z0-9()+:,_/-]+$ というパターンに従います。つまり、ユーザ名の先頭の 1 文字は英数字にする必要があり、A ～ Z（大文字または小文字）までの任意の英字、0 ～ 9 までの任意の数字、- および _ を含めることができます。またユーザ名は 1 ～ 64 文字使用できます。
- [Role] : ユーザ ロール。この値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。

（注）　Service のロールは、1 人のユーザのみ所有できます。

- [Status] : [active]、[expired]、[locked] など、現在のユーザ アカウント ステータスが表示されます。

[Add and Edit User] ダイアログボックスのフィールドの定義

[Add and Edit User] ダイアログボックスには、次のフィールドが表示されます。

- [Username] : ユーザ名は ^[A-Za-z0-9()+:,_/-]+$ というパターンに従います。つまり、ユーザ名の先頭の 1 文字は英数字にする必要があり、A ～ Z（大文字または小文字）までの任意の英字、0 ～ 9 までの任意の数字、- および _ を含めることができます。またユーザ名は 1 ～ 64 文字使用できます。
- [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。

（注）　Service のロールは、1 人のユーザのみ所有できます。

- [Password] : ユーザのパスワード。パスワードは、センサー管理者が [Passwords] ペインで設定する要件に準拠させる必要があります。
- [Confirm Password] : パスワードを確認できます。確認パスワードとユーザ パスワードと一致しない場合、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できます。[Edit] ダイアログボックスでのみ使用できます。

ユーザ ロールについて

ユーザ ロールは 4 種類あります。

- ビューア（Viewer）：設定およびイベントを表示できますが、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（Operator）：すべてのデータを表示できるほか、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、無効 / 有効）
  - 仮想センサー定義
  - 管理対象ルータ
  - 自分のユーザ パスワード
- 管理者（Administrator）：すべてのデータを表示できるほか、オペレータが修正できるすべてのオプションに加えて、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が許可されたホストのリスト
  - 物理的な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のイネーブル化またはディセーブル化
  - ユーザとパスワードの追加および削除
  - 新しい SSH ホスト キーおよびサーバ証明書の生成
- サービス（Service）：サービス権限を持つユーザはセンサーに 1 人だけ存在できます。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。

  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。サービス ロールを持つアカウントは、トラブルシューティングの目的でのみ作成してください。サービス アカウントを編集できるのは、管理者権限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、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

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.
*************************************************************************************
```

サービス アカウントについて

トラブルシューティングの際に使用する TAC 用のサービス アカウントを作成できます。センサーには複数のユーザがアクセスできますが、センサーに対するサービス権限を持てるのは 1 人のユーザだけです。サービス アカウントは、サポートの目的のためにのみ使用します。

サービス アカウントを作成した場合、root ユーザのパスワードは、サービス アカウントのパスワードに同期します。root でアクセスするには、サービス アカウントでログインしてから **su - root** コマンドを使用して root ユーザに切り替える必要があります。

注意　TAC の指示に基づく場合を除き、サービス アカウントを使用してセンサーに変更を加えないでください。サービス アカウントを使用してセンサーを設定すると、その設定は TAC のサポート対象外になります。サービス アカウントを使用してオペレーティング システムにサービスを追加すると、他の IPS サービスのパフォーマンスと機能に影響し、適切でなくなります。TAC は、追加のサービスが加えられたセンサーをサポートしません。

注意　サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

ユーザの追加、編集、削除およびアカウントの作成

センサー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] > [Authentication] を選択し、[Add] をクリックしてユーザを追加します。

ステップ 3　[Username] フィールドに、追加するユーザのユーザ名を入力します。

ステップ 4　[User Role] ドロップダウン リストから、次のユーザ ロールのいずれかを選択します。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）
- サービス（Service）

（注）　Service のロールは、1 人のユーザのみ所有できます。

ステップ 5　[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 6　[Confirm 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。

ヒント　変更を廃棄して [Add User] 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。[Users] ペイン内のユーザ リストに新しいユーザが表示されます。

ステップ 8　ユーザを編集するには、ユーザ リストでユーザを選択し、[Edit] をクリックします。

ステップ 9　[Username]、[User Role]、および [Password] フィールドを必要に応じて変更します。

ヒント　変更を廃棄して [Edit User] 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。[Users] ペイン内のユーザ リストに編集済みのユーザが表示されます。

ステップ 11　ユーザ リストからユーザを削除するには、ユーザを選択し、[Delete] をクリックします。[Users] ペイン内のユーザ リストからこのユーザが削除されます。

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。