CHAPTER 3

IPS SSP の初期化

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降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、**setup** コマンドを使用して IPS SSP を初期化する方法について説明します。次のような構成になっています。

- 「初期化について」（P.3-1）
- 「簡易セットアップ モード」（P.3-2）
- 「System Configuration Dialog」（P.3-2）
- 「センサーの基本的なセットアップ」（P.3-4）
- 「IPS SSP の高度なセットアップ」（P.3-7）
- 「初期化の確認」（P.3-12）

初期化について

（注） **setup** コマンドを使用するには、管理者である必要があります。

IPS SSP をネットワーク上に設置した後、それを **setup** コマンドで初期化して、ネットワーク経由で通信できるようにする必要があります。**setup** コマンドを使用して初期化するまで、IDM または IME を使用して IPS SSP を設定することはできません。

setup コマンドでは、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、センサーの基本設定を設定できます。続けて CLI の高度な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行うことができます。あるいは、IDM または IME で Startup Wizard を使用することもできます。

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 ライセンスを取得している必要があります。グローバル相関機能の統計情報について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。

簡易セットアップ モード

コンソール ケーブルを使用してセンサーに接続したとき、センサーの基本的なネットワーク設定がまだ設定されていなければ、センサーは自動的に **setup** コマンドをコールします。次の状態では、センサーは自動セットアップをコールしません。

- すでに初期化が正常に完了している場合。
- センサーを復元またはダウンロードした場合。
- 自動セットアップを使用してセンサーを正常に設定した後にホスト設定をデフォルトに設定した場合。

setup コマンドを入力すると、システムのコンソール画面に対話形式のダイアログ、System Configuration Dialog が表示されます。System Configuration Dialog に従って設定プロセスを進めます。各プロンプトの隣に表示されるカッコ内の値は、最後に設定された値で、デフォルト値として使用されます。

System Configuration Dialog

setup コマンドを入力すると、システムのコンソール画面に対話形式のダイアログ、System Configuration Dialog が表示されます。System Configuration Dialog に従って設定プロセスを進めます。

各プロンプトの隣に表示されるカッコ内の値は、現在の値を示しています。

変更するオプションにたどり着くまで、System Configuration Dialog を進めます。変更しない項目のデフォルト設定を受け入れるには、**Enter** を押します。

System Configuration Dialog を中断して変更を行わずに EXEC プロンプトに戻るには、Ctrl を押した状態で C を押します。

System Configuration Dialog では、プロンプトごとにヘルプ テキストも提供されます。ヘルプ テキストにアクセスするには、プロンプトで **?** を入力します。

変更を最後まで行うと、セットアップ セッション中に作成した設定が System Configuration Dialog によって表示されます。さらに、この設定を使用するかどうかも確認されます。**yes** を入力すると、設定が保存されます。**no** を入力すると、設定は保存されずにプロセスが再開されます。このプロンプトにはデフォルトがありません。**yes** か **no** を入力する必要があります。

繰り返しモードまたは日付モードのいずれかでサマータイムを設定できます。繰り返しモードを選択すると、開始日と終了日は、週、曜日、月、および時刻に基づきます。日付モードを選択すると、開始日と終了日は、月、曜日、年、および時刻に基づきます。ディセーブルを選択すると、サマータイムはオフになります。

（注）　システムがアプライアンスで、なおかつ NTP を使用していない場合は、System Configuration Dialog で日付と時刻のみを設定します。

（注）　System Configuration Dialog は対話型のダイアログです。デフォルトの設定が表示されます。

例 3-1 に、System Configuration Dialog の例を示します。

例 3-1　System Configuration Dialog の例

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Wed Nov 11 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.0.2.0/24,255.255.0]:
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Global Correlation?[no]:
DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Global Correlation?[no]:
HTTP proxy server IP address[128.107.241.169]:
HTTP proxy server Port number[8080]:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
```

```
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances.We do not collect the data content of traffic
or other sensitive business or personal information.All data is aggregated and sent via
secure HTTP to the Cisco SensorBase Network servers in periodic intervals.All data shared
with Cisco will be anonymous and treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
* Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs.promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
* Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

センサーの基本的なセットアップ

setup コマンドを使用してセンサーの基本的なセットアップを実施し、その後に CLI、IDM、または IME を使用してセンサーのセットアップを完了させることができます。

setup コマンドを使用してセンサーの基本的なセットアップを実施するには、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次のようにセンサーにログインします。

（注）　デフォルトのユーザ名とパスワードはどちらも **cisco** です。

ステップ 2　センサーに初めてログインしたとき、デフォルトのパスワードを変更するよう求められます。パスワードは最低 8 文字で、強力なパスワードにする必要があります。辞書にある単語は使用しないでください。パスワードを変更すると、基本セットアップが開始されます。

ステップ 3　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 4　ホスト名を指定します。ホスト名は 64 文字までの文字列で、大文字と小文字が区別されます。数字、「_」、および「-」は使用できますが、スペースは使用できません。デフォルトは sensor です。

ステップ 5　IP インターフェイスを指定します。IP インターフェイスは、*X.X.X.X/nn*,*Y.Y.Y.Y*（IP アドレス / ネットマスク , ゲートウェイ）の形式になります。ここで、*X.X.X.X* はセンサーの IP アドレスを示し、ピリオドで区切られた 4 つのオクテットで記述される 32 ビット アドレスです。*nn* はネットマスクのビット数を示します。*Y.Y.Y.Y* はデフォルト ゲートウェイを示し、ピリオドで区切られた 4 つのオクテットで記述される 32 ビット アドレスです。

ステップ 6　**yes** を入力してネットワーク アクセス リストを修正します。

a. エントリを削除する場合は、エントリの番号を入力して Enter を押します。そうでない場合は、Enter を押して Permit 行に移動します。

b. アクセス リストに追加するネットワークの IP アドレスおよびネットマスクを入力します。

たとえば、10.0.0.0/8 は 10.0.0.0 ネットワーク上のすべての IP アドレス（10.0.0.0 ～ 10.255.255.255）を許可します。10.1.1.0/24 は 10.1.1.0 サブネット上の IP アドレス（10.1.1.0 ～ 10.1.1.255）のみを許可します。ネットワーク全体ではなく、単一 IP アドレスへのアクセスを許可する場合は、32 ビットのネットマスクを使用します。たとえば、10.1.1.1/32 は 10.1.1.1 アドレスのみを許可します。

c. アクセス リストに追加するすべてのネットワークが追加されるまで、ステップ b を繰り返します。その後、空の permit 行で Enter を押して次のステップに進みます。

ステップ 7　グローバル相関が動作するには、DNS サーバまたは HTTP プロキシ サーバを設定する必要があります。

a. **yes** を入力して DNS サーバを追加し、DNS サーバの IP アドレスを入力します。

b. **yes** を入力して HTTP プロキシ サーバを追加し、HTTP プロキシ サーバの IP アドレスとポート番号を入力します。

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 ライセンスを所有している必要があります。グローバル相関機能の統計情報について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、アップデート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。

ステップ 8　**yes** を入力して、システム クロック設定を修正します。

a. **yes** を入力して、サマータイム設定を修正します。

（注）　サマータイムは、DST とも呼ばれます。サマータイムを採用していない地域の場合は、ステップ m に進みます。

b. **yes** を入力して米国サマータイム デフォルトを選択します。あるいは、**no** を入力し、recurring、date、または disable を選択してサマータイム設定の設定方法を指定します。デフォルトは recurring です。

c. recurring を選択した場合は、サマータイム設定の開始月を指定します。有効な値は january、february、march、april、may、june、july、august、september、october、november、december です。デフォルトは march です。

d. サマータイム設定の開始週を指定します。有効な値は first、second、third、fourth、fifth、last です。デフォルトは second です。

e. サマータイム設定の開始曜日を指定します。有効な値は sunday、monday、tuesday、wednesday、thursday、friday、saturday です。デフォルトは sunday です。

f. サマータイム設定の開始時刻を指定します。デフォルトは 02:00:00 です。

（注）　デフォルトの定期的なサマータイム パラメータはアメリカ合衆国の時間帯用です。デフォルト値では、開始時刻が 3 月の第 2 日曜日の午前 2:00、終了時刻が 11 月の第 1 日曜日の午前 2:00 です。デフォルトのサマータイム オフセットは 60 分です。

g. サマータイム設定の終了月を指定します。有効な値は january、february、march、april、may、june、july、august、september、october、november、december です。デフォルトは november です。

h. サマータイム設定の終了週を指定します。有効な値は first、second、third、fourth、fifth、last です。デフォルトは first です。

i. サマータイム設定の終了曜日を指定します。有効な値は sunday、monday、tuesday、wednesday、thursday、friday、saturday です。デフォルトは sunday です。

j. サマータイム設定の終了時刻を指定します。デフォルトは 02:00:00 です。

k. DST ゾーンを指定します。ゾーン名には、[A-Za-z0-9()+:,_/-]+$ のパターンを持つ 24 文字までの文字列を使用できます。

l. サマータイム オフセットを指定します。協定世界時（UTC）からのサマータイム オフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。デフォルトは 60 です。

m. **yes** を入力してシステム時間帯を修正します。

n. 標準時の時間帯名を指定します。ゾーン名には 24 文字までの文字列を使用できます。

o. 標準時の時間帯オフセットを指定します。UTC からの標準時の時間帯オフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。デフォルトは 0 です。

p. NTP を使用する場合は、**yes** を入力します。認証された NTP を使用するには、NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。これらがこの時点で存在しない場合は、後で NTP を設定できます。あるいは、未認証の NTP を選択することもできます。

ステップ 9　**off**、**partial**、または **full** を入力して、SensorBase Network Participation に参加します。

- off : SensorBase ネットワークにデータは提供されません。
- partial : SensorBase ネットワークにデータが提供されます。ただし、潜在的に機密性が高いと見なされるデータは、フィルタリングによって除外され、送信されません。
- full : 除外指定した攻撃者 / 攻撃対象の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

SensorBase Network Participation の注意事項が表示されます。これには、SensorBase ネットワークに参加することにより何が起こるかが説明されています。

ステップ 10　**yes** を入力して、SensorBase ネットワークに参加します。

```
The following configuration was entered.
service host
network-settings
host-ip 192.0.2.0/24,255.255.255.0
host-name sensor126
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
day-of-week sunday
```

```
    time-of-day 02:00:00
    exit
    end-summertime
    month november
    week-of-month first
    day-of-week sunday
    time-of-day 02:00:00
    exit
    exit
    ntp-option enabled
    ntp-keys 1 md5-key 8675309
    ntp-servers 10.89.143.92 key-id 1
    exit
    service global-correlation
    network-participation full
    exit


    [0] Go to the command prompt without saving this config.
    [1] Return to setup without saving this config.
    [2] Save this configuration and exit setup.
    [3] Continue to Advanced setup.
```

ステップ 11　**2** を入力して設定を保存します（あるいは、**3** を入力して、CLI を使用した高度なセットアップを続けて行います）。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 12　時刻設定を変更した場合は、**yes** を入力してセンサーをリブートします。

詳細情報

最新の IPS ソフトウェアを入手する手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

IPS SSP の高度なセットアップ

注意　IPS SSP は、4 種類のポート（コンソール、管理、GigabitEthernet、および 10GE）を備えています。コンソール ポートと管理ポート（IPS SSP の右前面パネル上にある）は、IPS ソフトウェアによって設定および制御を行います。GigabitEthernet ポートと 10GE ポート（IPS SSP の左前面パネル上にある）は、IPS ソフトウェアではなく、ASA ソフトウェアによって設定および制御を行います。ただし、IPS SSP をリセットまたはシャットダウンするときは、GigabitEthernet ポートと 10GE ポートもリンクダウンします。これらのポートに対するリンク ダウンの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンはスケジュールされたメンテナンス期間中に行う必要があります。

IPS SSP の高度なセットアップを続けて行うには、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 IPS SSP へのセッションを確立します。

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1.Escape character sequence is 'CTRL-^X'.
```

```
login: cisco
Password:
Last login: Fri Jan 14 04:14:54 from 10.77.25.187
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, xport, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S.laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.
asa#
```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　**3** を入力して、高度なセットアップにアクセスします。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトではディセーブルになっています。

ステップ 5　Web サーバ ポートを指定します。Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　Web サーバは、デフォルトで TLS/SSL 暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** を入力して、インターフェイスと仮想センサーの設定を修正します。

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel 0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 7　**1** を入力して、インターフェイス設定を編集します。

（注）　IPS SSP 上でインターフェイスを設定する必要はありません。[Modify interface default-vlan] 設定は無視します。IPS SSP の場合、仮想センサー間のトラフィックの分離は、他のセンサーとは異なる方法で設定されます。

```
  [1] Modify interface default-vlan.
Option:
```

ステップ 8　Enter を押して、インターフェイスと仮想センサーのトップレベルの設定メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 9　**2** を入力して、仮想センサー設定を編集します。

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

ステップ 10　**2** を入力して、仮想センサー vs0 の設定を修正します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel 0/0
Add Interface:
```

ステップ 11　**1** を入力して、PortChannel0/0 を仮想センサー vs0 に追加します。

（注）　複数の仮想センサーがサポートされます。適応型セキュリティ アプライアンスは、特定の仮想センサーにパケットを誘導することも、パケットを送信してデフォルトの仮想センサーにモニタさせることもできます。PortChannel0/0 を割り当てた仮想センサーがデフォルトの仮想センサーになります。PortChannel0/0 は vs0 に割り当てることを推奨しますが、必要に応じて、別の仮想センサーに割り当ててかまいません。

ステップ 12　Enter を押して、仮想センサーのメイン メニューに戻ります。

ステップ 13　**3** を入力して、仮想センサーを作成します。

```
Name[]:
```

ステップ 14　仮想センサーの名前と説明を入力します。

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

ステップ 15　**1** を入力して、既存の異常検出設定 ad0 を使用します。

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

ステップ 16　**2** を入力して、シグニチャ定義のコンフィギュレーション ファイルを作成します。

ステップ 17　シグニチャ定義設定の名前として **newSig** を入力します。

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

ステップ 18　**1** を入力して、既存のイベントアクション規則設定 rules0 を使用します。

（注）　PortChannel0/0 が vs0 に割り当てられていない場合、PortChannel0/0 をこの新しい仮想センサーに割り当てるよう求められます。

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

ステップ 19　Enter を押して、インターフェイスと仮想センサーの設定メニューに戻ります。

```
Modify default threat prevention settings?[no]:
```

ステップ 20　デフォルトの脅威防御設定を修正する場合は、**yes** を入力します。

（注）　このセンサーには、ハイ リスク レーティングのアラートにパケット拒否イベント アクションを追加する組み込みのオーバーライドが付属しています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 21　yes を入力して、すべての仮想センサー上の自動脅威防御をディセーブルにします。

```
The following configuration was entered.

service host
network-settings
host-ip 192.0.2.0/24,255.255.0
host-name ips-ssm
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
```

```
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 22　**2** を入力して設定を保存します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 23　IPS SSP をリブートします。

```
ips-ssp# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 24　**yes** を入力して、リブートを続行します。

ステップ 25　リブート後、センサーにログインし、自己署名 X.509 証明書（TLS で必要）を表示します。

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 26　証明書のフィンガープリントを書き留めます。Web ブラウザで HTTPS を使用してこの IPS SSP に接続する際に証明書の信頼性を確認するためにフィンガープリントが必要です。これで、IPS SSP に侵入防御を設定する準備ができました。

詳細情報

- IPS SSP 上の仮想センサー用にトラフィックを割り当てる手順については、「IPS SSP の仮想センサーの作成」（P.18-3）を参照してください。
- ASA ソフトウェアの詳細については、次の URL にある ASA のユーザ マニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

初期化の確認

IPS SSP の初期化が完了したことを確認するには、次の手順を実行します。

ステップ 1　IPS SSP にログインします。

ステップ 2　設定を表示します。

```
ips-ssp# show configuration
! ------------------------------
! Current configuration last modified Wed Jun 30 20:05:09 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S486.0   2010-04-29
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,255.255.0
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1006 0
alert-severity informational
exit
signatures 1102 0
alert-severity informational
exit
signatures 1104 0
alert-severity informational
exit
signatures 60000 0
promisc-delta 5
engine atomic-ip
exit
exit
exit
```

```
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

（注）　**more current-config** コマンドを使用して、設定を表示することもできます。

ステップ 3　自己署名 X.509 証明書（TLS で必要）を表示します。

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 4　証明書のフィンガープリントを書き留めます。Web ブラウザでこのセンサーに接続する際に証明書の信頼性を確認するためにフィンガープリントが必要です。

詳細情報

- IPS SSP へのログイン手順については、第 2 章「IPS SSP へのログイン」を参照してください。
- **more current-config** コマンドの使用手順については、「現在の設定の表示」（P.16-1）を参照してください。
- TLS フィンガープリントの詳細については、「TLS の設定」（P.4-39）を参照してください。