CHAPTER 18

IPS SSP の初期化

（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、**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。次の事項について説明します。

初期設定の概要

（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。

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。

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すると、センサーの基本的なネットワーク設定が済んでいない場合は、センサーにより自動的に **setup** コマンドが呼び出されます。次の場合、自動セットアップは呼び出されません。

- 初期化が正常に完了している場合。
- センサーをリカバリまたはダウングレードした場合。
- 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でホストの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 コンソール画面に System Configuration Dialog と呼ばれる対話形式のダイアログが表示されます。System Configuration Dialog に従って設定プロセスを進めます。各プロンプトの横のカッコ内には、最後に設定されたデフォルト値が表示されます。

System Configuration Dialog

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

各プロンプトの横のカッコ内には、現在の値が表示されます。

変更するオプションに到達するまで System Configuration Dialog 全体を実行する必要があります。変更しない項目でデフォルト設定を受け付ける場合は、Enter キーを押します。

変更を中断し、System Configuration Dialog を最後まで実行せずに EXEC プロンプトに戻るには、Ctrl+C を押します。

System Configuration Dialog では、各プロンプトのヘルプ テキストも表示できます。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。

変更が完了したら、セットアップ セッション中に作成した設定が System Configuration Dialog に表示されます。また、この設定を使用するかどうかも尋ねられます。**yes** を入力すると、その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、プロセスが再度開始されます。このプロンプトにはデフォルトはありません。**yes** または **no** を入力する必要があります。

サマータイムは、Recurring モードまたは Date モードのいずれかで設定できます。Recurring モードを選択した場合は、開始日および終了日は、週、日、月、および時間に基づいて設定します。Date モードを選択すると、開始日および終了日は、月、日、年、および時間に基づいて設定します。Disable を選択すると、サマータイムがオフになります。

（注）　システムがアプライアンスで NTP を使用していない場合は、System Configuration Dialog で日付と時間を設定するだけで済みます。

（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ています。

例 18-1 に、System Configuration Dialog の例を示します。

例 18-1　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[192.168.1.2/24,192.168.1.1]:
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

センサーの基本的なセットアップは **setup** コマンドを使用して実行できます。その後、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します。

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行するには、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両方とも **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、基本的な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、スペースは受け付けられません。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、IP アドレス/ネットマスク,ゲートウェイ（*X.X.X.X/nn,Y.Y.Y.Y*）の形式で指定します。ここで、*X.X.X.X* は、32 ビット アドレスのセンサーの IP アドレスを、ピリオドで区切った 4 つのオクテットで指定しています。*nn* はネットマスクのビット数を指定しています。*Y.Y.Y.Y* は、32 ビット アドレスのデフォルト ゲートウェイを、ピリオドで区切った 4 つのオクテットで指定しています。

ステップ 6　**yes** と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** を押すか、または **Enter** を押して Permit 行に進みます。

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、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）だけを許可します。ネットワーク全体ではなく、1 つの IP アドレスへのアクセスを許可する場合は、32 ビット ネットマスクを使用します。たとえば、10.1.1.1/32 は、アドレス 10.1.1.1 だけを許可します。

c. アクセス リストに追加するネットワークの追加がすべて終わるまで、ステップ b を繰り返します。その後、空白の Permit 行で **Enter** を押して次の手順に進みます。

ステップ 7　グローバル相関が動作するためには、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** と入力して DNS サーバを追加してから、DNS サーバの IP アドレスを入力します。

b. **yes** と入力して HTTP プロキシ サーバを追加してから、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。

ステップ 8　システム クロックの設定値を修正するには、**yes** と入力します。

a. サマータイム設定を修正するには、**yes** と入力します。

（注）　サマータイムは DST とも呼びます。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** と入力して、デフォルトのアメリカ合衆国のサマータイムを選択します。または、**no** と入力して、Recurring、Date、または Disable のいずれかを選択し、サマータイム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入力します。有効な入力は、january、february、march、april、may、june、july、august、september、october、november、および 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、および 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。有効な入力は、sunday、monday、tuesday、wednesday、thursday、friday、および 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 時に指定されています。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。有効な入力は、january、february、march、april、may、june、july、august、september、october、november、および 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、および 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。有効な入力は、sunday、monday、tuesday、wednesday、thursday、friday、および 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。ゾーン名は、最長で 24 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ 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. システムの時間帯を修正するには、**yes** と入力します。

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. 標準時間帯オフセットを指定します。協定世界時（UTC）からの標準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** と入力します。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。認証されていない NTP を選択することもできます。

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

- [Off]：いずれのデータも SensorBase ネットワークに提供されません。
- [Partial]：データは SensorBase ネットワークに提供されますが、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るため送信されません。
- [Full]：すべてのデータは、除外する攻撃者や攻撃対象の IP アドレスを除き、SensorBase ネットワークに提供されます。

SensorBase Network Participation の免責事項が表示されます。ここでは、SensorBase Network に参加することに伴う注意事項が説明されます。

ステップ 10　**yes** と入力して SensorBase Network に参加します。

```
The following configuration was entered.
service host
network-settings
host-ip 10.89.143.126/24,10.89.143.254
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（または **3** を入力し、CLI を使用して拡張セットアップを続行します）。

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

ステップ 12　時間設定を変更した場合は、**yes** と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方法については、「Cisco IPS ソフトウェアの入手」（P.20-2）を参照してください。

IPS SSP 拡張セットアップ

注意　IPS SSP には、4 種類のポート（コンソール、管理、GigabitEthernet、10GE）があります。IPS SSP の右前面パネルにあるコンソール ポートと管理ポートは、IPS ソフトウェアを使用して設定および制御します。IPS SSP の左前面パネルにある GigabitEthernet ポートと 10GE ポートは、IPS ソフトウェアではなく、ASA ソフトウェアを使用して設定および制御します。ただし、IPS SSP をリセットまたはシャットダウンした場合は、GigabitEthernet ポートと 10GE ポートもリンク ダウンします。スケジュールされたメンテナンスの時間帯は IPS SSP をリセットまたはシャットダウンして、これらのポートがリンク ダウンする影響を最小化する必要があります。

IPS SSP の拡張セットアップを続行するには、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、IPS SSP のセッションに入ります。

```
asa# session 1
```

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** と入力して拡張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です。

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://ips_ssp_ip_address:port` という形式です（`https://10.1.9.201:1040` など）。

（注）　デフォルトでは、Web サーバは TLS および SSL の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はなりません。

ステップ 6　**yes** と入力して、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の設定を編集します。

（注）　IPS SSP 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 の設定は無視してください。IPS SSP での仮想センサー間のトラフィックの分離設定は、その他のセンサーとは異なります。

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

ステップ 8　**Enter** を押してトップレベル インターフェイスの仮想センサー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の設定を編集します。

```
  [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** を入力して仮想センサー vs0 に PortChannel0/0 を追加します。

（注）　複数の仮想センサーがサポートされています。適応型セキュリティ アプライアンスでは、パケットを特定の仮想センサーに誘導するか、またはパケットを送信して、デフォルトの仮想センサーによりパケットをモニタすることができます。デフォルトの仮想センサーは、PortChannel0/0 を割り当てたセンサーです。PortChannel0/0 は vs0 に割り当てることを推奨しますが、必要であれば別の仮想センサーに割り当ててもかまいません。

ステップ 12　**Enter** を押してメインの仮想センサー 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　（任意）仮想センサーの名前と説明を入力します。

（注）　ステップ 14 ～ 18 は任意です。複数の仮想センサーが必要な場合のみ要求されます。

```
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　（任意）**1** を入力して、既存の異常検出設定である 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　（任意）**2** を入力して、シグニチャ定義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　（任意）シグニチャ定義設定の名前として **newSig** と入力します。

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

ステップ 18　（任意）**1** を入力して、既存のイベント アクション規則の設定である 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は、新しい仮想センサーに割り当てるように促されます。

```
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および仮想センサーの設定メニューを終了します。

```
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** と入力します。

（注）　センサーには、リスク レーティングの高い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ためのオーバーライドが組み込まれています。この保護が不要な場合は、自動的な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** と入力してすべての仮想センサーで自動的な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 10.1.9.201/24,10.1.9.1
host-name ips-ssp
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** と入力してリブートを続行します。

ステップ 25　リブートしたら、IPS SSP にログインして自己署名 X.509 証明書を表示します（TLS で必要です）。

```
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。フィンガープリントは、Web ブラウザを使用して HTTPS でこの IPS SSP に接続した際に、証明書の信頼性を確認するために必要です。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

ASA ソフトウェアの詳細については、次の URL 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 が初期化されている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 10.89.131.17/23,10.89.130.1
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
ips-ssp#
```

（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 証明書を表示します（TLS で必要です）。

```
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。フィンガープリントは、Web ブラウザを使用してこの IPS SSP に接続した際に、証明書の信頼性を確認するために必要です。

詳細情報

IPS SSP へのログイン方法については、第 19 章「IPS SSP へのログイン」を参照してください。