センサーの初期化

内容

この章では、**setup** コマンドを使用してセンサー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。

初期化について

センサーをネットワークに設置したら、**setup** コマンドを使用してセンサーを初期化し、ネットワーク経由でセンサーが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センサーを初期化するまでは、IDM または IME を使用してセンサーの設定を行うことはできません。

setup コマンドを使用して、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、時間設定など、センサーの基本的な設定を行います。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。**setup** コマンドにセンサーを設定したら、IDM または IME のネットワーク設定を変更できます。

（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。

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、センサーが自動的に **setup** コマンドを呼び出します。この時点では、センサーの基本的なネットワーク設定はまだ行われていません。次の条件下では、センサーは自動セットアップの呼び出しを行いません。

- 初期化がすでに正常に完了している場合。
- センサーの回復またはダウングレードを行った場合。
- 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、ホスト コンフィギュレーションをデフォルトにした場合。

setup コマンドを入力すると、システムのコンソール画面に [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。前回設定されたデフォルト値は、各プロンプトの横のカッコ内に表示されます。

システム設定ダイアログ

setup コマンドを入力すると、システムのコンソール画面に [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。現在の値は、各プロンプトの横のカッコ内に表示されます。

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。変更しない項目のデフォルト設定を使用するには、Enter 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] は、プロンプトごとにヘルプ テキストも提示します。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。

変更が完了すると、[System Configuration Dialog] はセットアップ セッション中に作成されたコンフィギュレーションを表示させます。また、この設定を使用するかどうかを問い合わせてきます。**yes** を入力すると、コンフィギュレーションが保存されます。**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** 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] モードを選択すると、開始日および終了日は、週、日、月、および時間がベースになります。[date] モードを選択すると、開始日および終了日は、月、日、年、および時間がベースになります。[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ます。

例 B-1 に、[System Configuration Dialog] の例を示します。

例 B-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]:
```

詳細情報

IDM のグローバル相関機能の詳細については、「グローバル相関の設定」を参照してください。IME については、「グローバル相関の設定」を参照してください。CLI については、「グローバル相関の設定」を参照してください。

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行うことができます。その後、続けて 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行うことができます。その後、続けて 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　センサーへの初回ログインでは、デフォルト パスワードの変更を求められます。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します。

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 アドレスで、ピリオドで区切った 4 つのオクテットで記述されています。*nn* はネットマスクのビット数です。*Y.Y.Y.Y* は、32 ビット アドレスのデフォルト ゲートウェイで、ピリオドで区切った 4 つのオクテットで記述されています。

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指定します。

（注） 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 アドレスだけ（10.1.1.0 ～ 10.1.1.255）を許可します。ネットワーク全体ではなく単一の 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 10.1.1.1 のアドレスだけを許可します。

c. アクセス リストに追加するネットワークをすべて入力し終わるまで、ステップ b を繰り返します。終わったら、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 動作するように DNS サーバまたは HTTP プロキシ サーバをグローバル相関に対して設定する必要があります。

a. **yes** を入力すると、DNS サーバが追加されます。その後、続けて DNS サーバの IP アドレスを入力します。

b. **yes** を入力すると、HTTP プロキシ サーバが追加されます。その後、続けて HTTP プロキシ サーバの IP アドレスおよび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、有効なセンサーの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。

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. 米国のサマータイムのデフォルトを選択するには、**yes** と入力します。または、サマータイムの設定方法を指定するには、**no** と入力して [recurring]、[date]、または [disable] を選択します。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。有効な値は、january、february、march、april、may、june、july、august、september、october、november および december です。デフォルト値は 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。デフォルトは値 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、および saturday です。デフォルト値は sunday です。

f. サマータイム設定の開始時刻を指定します。デフォルト値は 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 日曜午前 2 時、終了時刻が 11 月の第一日曜日の午前 2 時です。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 および december です。デフォルト値は 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、および saturday です。デフォルト値は sunday です。

j. サマータイム設定の終了時刻を指定します。デフォルト値は 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）。デフォルト値は 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. 標準時の時間帯のオフセットを指定します。UTC からの標準時間帯の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。または、認証されていない NTP を選択できます。

ステップ 9　SensorBase Network Participation に参加するには、**off**、**partial**、または **full** と入力します。

- [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、送信されません。
- [Full]：除外された攻撃者 / 攻撃対象者の 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 の免責事項が表示されます。ここでは、SensorBase Network に参加する際に必要なものが示されます。

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

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24, 192.168.1.1
host-name sensor
telnet-option disabled
sshv1-fallback 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 10.10.1.2 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方法」（P.C-1）を参照してください。
- HTTPS を使用して IDM にログインするための手順については、「IDM へのログイン」を参照してください。
- センサーの侵入防御を設定する手順については、次のガイドを参照してください。
  - *『Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 7.2』*
  - *『Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.2』*
  - *『Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.2』*

高度なセットアップ

ここでは、センサーの CLI で高度なセットアップを継続する方法について説明します。ここで説明する内容は、次のとおりです。

• 「ASA 5585-X IPS SSP の高度な設定」（P.B-17）

アプライアンスの高度な設定

（注） 現在サポートされている Cisco IPS アプライアンスは、IPS 4345、IPS 4360、IPS 4510、および IPS 4520 です。

（注） 新しいサブインターフェイスの追加は、2 つのステップからなるプロセスです。まず、仮想センサーの設定を編集するときにインターフェイスを分類します。次に、どのインターフェイスとサブインターフェイスをどの仮想センサーに割り当てるかを選択します。

インターフェイスは、アプライアンス モデルによって変わりますが、プロンプトはすべてのモデルで同じです。続けてアプライアンスの高度なセットアップを行うには、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アプライアンスにログインします。

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。高度なセットアップにアクセスするためのメニューに進むには、**Enter** キーまたはスペースバーを押します。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

ステップ 4　Telnet サーバのステータスを指定します。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　SSHv1 フォールバックの設定を指定します。デフォルトではディセーブルになっています。

ステップ 6　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） 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なりません。

ステップ 7　**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、現在のインターフェイス設定を参照します。

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Promiscuous:
   GigabitEthernet0/0
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3

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

 Virtual Sensor: vs1
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs2
```

```
  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 8　インターフェイス設定を編集するには、**1** と入力します。

（注）　次のオプションでは、インターフェイスの作成および削除を実行できます。インターフェイスを仮想センサーの設定に含まれる仮想センサーに割り当てます。インターフェイスに無差別モードを使用して、VLAN で分割しない場合、追加設定は必要ありません。

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

ステップ 9　インライン VLAN ペアを追加し、使用可能なインターフェイスのリストを表示するには、**2** を入力します。

注意　新しい VLAN ペアが仮想センサーに自動的に追加されることはありません。

```
Available Interfaces
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

ステップ 10　インライン VLAN ペアを GigabitEthernet 0/0 に追加するには、**1** と入力します。たとえば、次のようになります。

```
Inline Vlan Pairs for GigabitEthernet0/0
   None
```

ステップ 11　サブインターフェイス番号と説明を入力します。

```
Subinterface Number:
Description[Created via setup by user asmith]:
```

ステップ 12　VLAN 1 および 2 の番号を入力します。

```
Vlan1[]: 200
Vlan2[]: 300
```

ステップ 13　**Enter** を押して、使用可能なインターフェイス メニューに戻ります。

（注）　プロンプトに値を入れずに改行すると、前のメニューに戻ります。

```
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
```

```
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

（注） この時点で、別のインターフェイス（たとえば、インライン VLAN ペアの場合は GigabitEthernet 0/1）を設定できます。

ステップ 14 **Enter** を押して、最上位レベルのインターフェイスの編集メニューに戻ります。

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

ステップ 15 インライン インターフェイス ペアを追加するには、**4** と入力します。次のオプションが表示されます。

```
Available Interfaces
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3
```

ステップ 16 ペア名、説明、およびペアにするインターフェイスを入力します。

```
Pair name: newPair
Description[Created via setup by user asmith:
Interface1[]: GigabitEthernet0/1
Interface2[]: GigabitEthernet0/2
Pair name:
```

ステップ 17 **Enter** を押して、最上位レベルのインターフェイスの編集メニューに戻ります。

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

ステップ 18 **Enter** を押して、最上位レベルの編集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 19 仮想センサーの設定を編集するには、**2** と入力します。

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

ステップ 20 仮想センサー設定 vs0 を修正するには、**2** と入力します。

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

```
No Interfaces to remove.

 Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/3
   [2] GigabitEthernet0/0
  Inline Vlan Pair:
   [3] GigabitEthernet0/0:1 (Vlans: 200, 300)
  Inline Interface Pair:
   [4] newPair (GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

ステップ 21　インライン VLAN ペア GigabitEthernet0/0:1 を追加するには、**3** と入力します。

ステップ 22　インライン インターフェイス ペア NewPair を追加するには、**4** と入力します。

ステップ 23　**Enter** を押して、最上位レベルの仮想センサー メニューに戻ります。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
   GigabitEthernet0/0:1 (Vlans: 200, 300)
  Inline Interface Pair:
   newPair (GigabitEthernet0/1, GigabitEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option: GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

ステップ 24　Enter を押して、最上位レベルのインターフェイスおよび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 25　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、パケットの拒否イベント アクションを高リスク評価のアラートに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 26　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

ステップ 27　Enter を押して、インターフェイスと仮想センサーの設定を終了します。

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option disabled
sshv1-fallback disabled
```

```
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 interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user asmith
vlan1 200
vlan2 300
exit
exit
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 GigabitEthernet0/1
interface2 GigabitEthernet0/2
exit
exit
service analysis-engine
virtual-sensor newVs
description Created via setup by user cisco
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/0
exit
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 1
logical-interface newPair
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 28　設定を保存するには、**2** と入力します。

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

ステップ 29　アプライアンスをリブートします。

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

ステップ 30　リブートを続行するには、**yes** と入力します。

ステップ 31　最新のサービス パックおよびシグニチャ アップデートを適用します。これでアプライアンスの侵入防御設定を行う準備ができました。

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方法」（P.C-1）を参照してください。
- HTTPS を使用して IDM にログインするための手順については、「IDM へのログイン」を参照してください。
- センサーの侵入防御を設定する手順については、次のガイドを参照してください。
  - *『Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 7.2』*
  - *『Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.2』*
  - *『Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.2』*

ASA 5500-X IPS SSP の高度な設定

続けて ASA 5500-X IPS SSP の高度なセットアップを行うには、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 へのセッションを確立します。

```
asa# session ips
```

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。高度なセットアップにアクセスするためのメニューに進むには、**Enter** キーまたはスペースバーを押します。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

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　SSHv1 フォールバックの設定を指定します。デフォルトではディセーブルになっています。

ステップ 6　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）　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なりません。

ステップ 7　**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 8　インターフェイス設定を編集するには、**1** と入力します。

（注）　ASA 5500-X IPS SSP には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 設定は無視する必要があります。仮想センサー間でトラフィックを分離する場合は、他のセンサーとは別に ASA 5500-X IPS SSP を設定します。

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

ステップ 9　Enter を押して、最上位レベルのインターフェイスおよび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 10　仮想センサーの設定を編集するには、**2** と入力します。

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

ステップ 11　仮想センサー vs0 の設定を修正するには、**2** と入力します。

```
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 12　仮想センサー vs0 に PortChannel 0/0 を追加するには、**1** と入力します。

（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のモニタリング対象にすることも、デフォルトの仮想センサーのモニタリング対象とすることもできます。デフォルトの仮想センサーは、PortChannel 0/0 が割り当てられている仮想センサーです。PortChannel 0/0 は vs0 に割り当てることを推奨しますが、必要なら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 13　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 14　仮想センサーを作成するには、**3** と入力します。

```
Name[]:
```

ステップ 15　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 16　既存の異常検出の設定 ad0 を使用するには、**1** と入力します。

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

ステップ 17　シグニチャ定義のコンフィギュレーション ファイルを作成するには、**2** と入力します。

ステップ 18　シグニチャ定義の設定名 **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 19　既存のイベント アクション規則の設定 rules0 を使用するには、**1** と入力します。

（注）　PortChannel 0/0 が vs0 に割り当てられていない場合、新しい仮想センサーに割り当てるようにプロンプトが表示されます。

```
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 20　Enter を押して、インターフェイスおよび仮想センサー設定メニューを終了します。

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

ステップ 21　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、パケットの拒否イベント アクションを高リスク評価のアラートに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 22　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name asa-ips
telnet-option disabled
sshv1-fallback 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 23　設定を保存するには、**2** と入力します。

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

ステップ 24　ASA 5500-X IPS SSP をリブートします。

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

ステップ 25　リブートを続行するには、**yes** と入力します。

ステップ 26　リブート後、センサーにログインし、自己署名 X.509 証明書を表示します（TLS で必要です）。

```
asa-ips# 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 27　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、HTTPS を使用して Web ブラウザでこの ASA 5500-X 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になります。

ステップ 28　最新のサービス パックおよびシグニチャ アップデートを適用します。これで、ASA 5500-X IPS SSP の侵入防御を設定する準備ができました。

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方法」（P.C-1）を参照してください。
- HTTPS を使用して IDM にログインするための手順については、「IDM へのログイン」を参照してください。
- センサーの侵入防御を設定する手順については、次のガイドを参照してください。
  - *『Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 7.2』*
  - *『Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.2』*
  - *『Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.2』*

ASA 5585-X IPS SSP の高度な設定

続けて ASA 5585-X IPS SSP の高度なセットアップを行うには、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 ASA 5585-X IPS SSP へのセッションを確立します。

```
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。高度なセットアップにアクセスするためのメニューに進むには、**Enter** キーまたはスペースバーを押します。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

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　SSHv1 フォールバックの設定を指定します。デフォルトではディセーブルになっています。

ステップ 6　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）　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なりません。

ステップ 7　**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:
   PortChannel0/0
```

```
 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 8　インターフェイス設定を編集するには、**1** と入力します。

（注）　ASA 5585-X IPS SSP には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 設定は無視する必要があります。仮想センサー間でトラフィックを分離する場合は、他のセンサーとは別に ASA 5585-X IPS SSP を設定します。

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

ステップ 9　Enter を押して、最上位レベルのインターフェイスおよび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 10　仮想センサーの設定を編集するには、**2** と入力します。

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

ステップ 11　仮想センサー vs0 の設定を修正するには、**2** と入力します。

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

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel0/0
Add Interface:
```

ステップ 12　仮想センサー vs0 に PortChannel 0/0 を追加するには、**1** と入力します。

（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のモニタリング対象にすることも、デフォルトの仮想センサーのモニタリング対象とすることもできます。デフォルトの仮想センサーは、PortChannel 0/0 が割り当てられている仮想センサーです。PortChannel 0/0 は vs0 に割り当てることを推奨しますが、必要なら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 13　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 14　仮想センサーを作成するには、**3** と入力します。

```
Name[]:
```

ステップ 15　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 16　既存の異常検出の設定 ad0 を使用するには、**1** と入力します。

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

ステップ 17　シグニチャ定義のコンフィギュレーション ファイルを作成するには、**2** と入力します。

ステップ 18　シグニチャ定義の設定名 **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 19　既存のイベント アクション規則の設定 rules0 を使用するには、**1** と入力します。

（注）　PortChannel 0/0 が vs0 に割り当てられていない場合、新しい仮想センサーに割り当てるようにプロンプトが表示されます。

```
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 20　Enter を押して、インターフェイスおよび仮想センサー設定メニューを終了します。

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

ステップ 21　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、パケットの拒否イベント アクションを高リスク評価のアラートに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 22　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name ips-ssm
telnet-option disabled
sshv1-fallback 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 23　設定を保存するには、**2** と入力します。

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

ステップ 24　ASA 5585-X 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 25　リブートを続行するには、**yes** と入力します。

ステップ 26　リブート後、センサーにログインし、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 27　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、HTTPS を使用して Web ブラウザでこの ASA 5585-X 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になります。

ステップ 28　最新のサービス パックおよびシグニチャ アップデートを適用します。これで、ASA 5585-X IPS SSP の侵入防御を設定する準備ができました。

詳細情報

HTTPS を使用して IDM にログインするための手順については、「IDM へのログイン」を参照してください。

初期化の確認

（注）　CLI 出力は、設定がどのように表示されるかを示した例です。オプションの設定選択、センサー モデル、およびインストールした IPS バージョンによって、正確に一致しません。

センサー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　センサーにログインします。

ステップ 2　設定を表示します。

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Fri Apr 19 19:01:05 2013
! ------------------------------
! Version 7.2(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S697.0   2013-02-15
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
inline-interfaces pair0
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
bypass-mode auto
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.106.133.159/23,10.106.132.1
```

```
host-name q4360-159
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
websession-inactivity-timeout 3600
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
logical-interface pair0
exit
exit
sensor#
```

（注） また、**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）。

```
sensor# show tls fingerprint
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 ブラウザでこのセンサーに接続した際に証明書の信頼性を確認するために必要になります。