CHAPTER 23

センサーの初期化

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 を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センサーを初期化する方法について説明します。この章は、次の項で構成されています。

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。

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、IME 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。その後、続けて CLI の高度な設定を使用し、Telnet のイネーブル化、Web サーバの設定、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、IME の Startup Wizard を使用することもできます。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

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。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

詳細情報

- **setup** コマンドを使用して AIP SSM を初期化する手順については、「AIP SSM の高度なセットアップ」（P.23-17）を参照してください。
- **setup** コマンドを使用して IPS SSP を初期化する手順については、「IPS SSP の高度なセットアップ」（P.23-26）を参照してください。
- ASDM を使用して AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。
- **setup** コマンドを使用して AIM IPS を初期化する手順については、「AIM PS の高度なセットアップ」（P.23-15）を参照してください。
- **setup** コマンドを使用して NME IPS を初期化する手順については、「NME IPS の高度なセットアップ」（P.23-30）を参照してください。
- **setup** コマンドを使用して IDSM2 を初期化する手順については、「IDSM2 の高度なセットアップ」（P.23-21）を参照してください。

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

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

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 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 テキストを表示できます。ヘルプ テキストを表示するには、プロンプトで疑問符（**?**）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を問い合わせてきます。**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ています。

例 23-1 に、[System Configuration Dialog] の例を示します。

例 23-1　[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

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

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 キーを押すか、または Enter キーを押して 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。

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 キーを押して、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ように 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、および 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。デフォルト値は、開始時刻が 3 月の第 2 日曜日午前 2 時、終了時刻が 11 月の第 1 日曜日午前 2 時と指定します。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、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：どのデータも 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 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　設定を保存するには、**2** と入力します（または、**3** と入力して、CLI、IDM、または IME を使用した高度なセットアップに進みます）。

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

ステップ 12　センサーをリブートするには、**yes** と入力します。

ステップ 13　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）。

```
sensor# 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 14　証明書のフィンガープリントを書き留めます。このフィンガープリントは、Web ブラウザでこのアプライアンスに HTTPS を使用して接続したときに、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 15　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。これでセンサーの侵入防御設定を行う準備ができました。

詳細情報

- 最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。

ASDM での AIP SSC-5 のセットアップ

AIP SSC-5 の初期化では、他のセンサーのように IPS CLI で **setup** コマンドを実行する必要はありません。AIP SSC-5 は、ASDM から初期化できます。ASDM を起動すると、AIP SSC-5 の管理インターフェイスに接続され、次のデフォルト ネットワーク パラメータが設定されます。

- 管理 VLAN：VLAN 1
- 管理 IP アドレス：192.168.1.1/24

（注）　適応型セキュリティ アプライアンスのデフォルトの管理 IP アドレスは 192.168.1.1/24 です。

- ゲートウェイ：192.168.1.1
- ユーザ名およびパスワード：**cisco**

ASDM でデフォルト パラメータを変更するには、[Configuration] > [Device Setup] > [SSC Setup] を選択します。AIP SSC-5 で IPS のより高度な設定を行うには、[IPS] タブをクリックして IDM を起動するか、IPS CLI にログインします。

詳細情報

- ASDM の使用方法の詳細については、ASDM のマニュアルを参照してください。
- 最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

高度なセットアップ

この項では、基本的なセットアップに続けて CLI の Advanced Setup を使用し、さまざまな Cisco IPS プラットフォームの高度なセットアップを行う方法について説明します。内容は次のとおりです。

アプライアンスの高度なセットアップ

（注）　現在サポートされている Cisco IPS アプライアンスは、IPS 4240、IPS 4255、IPS 4260、および IPS 4270-20 です。

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のモデルによって異なりますが、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。

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）　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 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。現在のインターフェイス設定が表示されます

```
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 7　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）　次のオプションを使用して、インターフェイスを作成および削除できます。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いて、インターフェイスを VLAN で分割していない場合、追加の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 8　インライン VLAN ペアを追加するには、**2** と入力します。使用可能なインターフェイスのリストが表示されます。

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 9　インライン VLAN ペアを GigabitEthernet0/0 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 10　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 11　VLAN 1 および VLAN 2 の数を入力します。

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

ステップ 12　Enter キーを押して使用可能なインターフェイスの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、インライン VLAN ペアのもう 1 つのインターフェイス（GigabitEthernet0/1 など）を設定できます。

ステップ 13　Enter キーを押して、最上位レベルのインターフェイス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 14　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 15　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 16　Enter キーを押して、最上位レベルのインターフェイス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 17　Enter キーを押して、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 18　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 19　仮想センサーの設定 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 20　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 21　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 22　Enter キーを押して、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 23　Enter キーを押して、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 24　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 25　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 26　Enter キーを押して、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
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 27　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 28　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 29　リブートを続行するには、**yes** と入力します。

ステップ 30　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

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

AIM PS の高度なセットアップ

続けて AIM IPS 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 AIM IPS のセッションを開始します。

```
router# service-module ids-sensor 0/0 session
Trying 10.1.9.1, 2322 ... Open


sensor login: cisco
Password: ********
```

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　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）　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 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。

分析エンジンが初期化中で、現在仮想センサーの設定を修正できないという警告が表示される場合があります。Space キーを押して、次のメニューを表示します。

```
[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.

Enter your selection[2]:
```

分析エンジンが初期化中という警告が表示された場合は、**2** と入力してここまでの設定を保存し、セットアップを終了します。その後、セットアップを再開し、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るまで Enter キーを押します。

ステップ 7　仮想センサーの設定を修正するには、**2** と入力します。

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 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　仮想センサー vs0 の設定を編集するには、**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] GigabitEthernet0/1
Add Interface:
```

ステップ 9　仮想センサー vs0 に GigabitEthernet0/1 を追加するには、**1** と入力します。

```
Add Interface: 1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
   GigabitEthernet0/1

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

ステップ 10　Enter キーを押して、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 11　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 12　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 aim-ips
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 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
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 13　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 14　AIM IPS をリブートします。

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

ステップ 15　リブートを続行するには、**yes** と入力します。

ステップ 16　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、AIM IPS に侵入防御を設定する準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

AIP SSM の高度なセットアップ

続けて AIP SSM 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 AIP SSM のセッションを開始します。

```
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。

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）　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 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: GigabitEthernet0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 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　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）　AIP SSM 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 AIP SSM を設定します。

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

ステップ 8　Enter キーを押して、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 9　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 10　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] GigabitEthernet0/1
Add Interface:
```

ステップ 11　仮想センサー vs0 に GigabitEthernet0/1 を追加するには、**1** と入力します。

（注）　ASA 7.2 以前では、1 つ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 アプライアンスから着信するパケットのモニタリングには、GigabitEthernet0/1 が割り当てられた仮想センサーが使用されます。GigabitEthernet0/1 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。

（注）　IPS 6.0 以降を実行する ASA 7.2.3 以降では、複数の仮想センサーがサポートされています。ASA 7.2.3 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、GigabitEthernet0/1 が割り当てられている仮想センサーです。GigabitEthernet0/1 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 12　Enter キーを押して、メインの仮想センサー メニューに戻ります。

ステップ 13　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 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　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 16　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 17　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 18　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）　GigabitEthernet0/1 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。

（注）　ASA 7.2 以前では、1 つ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 アプライアンスから着信するパケットのモニタリングには、GigabitEthernet0/1 が割り当てられた仮想センサーが使用されます。GigabitEthernet0/1 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。

（注）　IPS 6.0 を実行する ASA 7.2.3 以降では、複数の仮想センサーがサポートされています。ASA 7.2.3 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、GigabitEthernet0/1 が割り当てられている仮想センサーです。GigabitEthernet0/1 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。

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   GigabitEthernet0/1

  [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 キーを押して、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 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、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 21　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 aip-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 GigabitEthernet0/1
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　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 23　AIP SSM をリブートします。

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

ステップ 24　リブートを続行するには、**yes** と入力します。

ステップ 25　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 AIP SSM の侵入防御設定を行う準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IDSM2 の高度なセットアップ

続けて IDSM2 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 IDSM2 のセッションを開始します。

- Catalyst ソフトウェア

```
console> enable
console> (enable) session module_number
```

- Cisco IOS ソフトウェア

```
router# session slot slot_number processor 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　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）　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 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: GigabitEthernet0/2
 Unassigned:
  Promiscuous:
   GigabitEthernet0/7
   GigabitEthernet0/8

 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　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）　次のオプションを使用して、インターフェイスを作成および削除できます。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いて、インターフェイスを VLAN で分割していない場合、追加の設定は必要ありません。

（注）　IDSM2 は、Add/Modify Inline Interface Pair Vlan Groups オプションをサポートしていません。インライン インターフェイス ペアを実行する場合、2 つの IDSM2 データ ポートが、ネイティブ VLAN だけを伝送するアクセス ポートまたはトランク ポートとして設定されます。パケットには 802.1q ヘッダーがなく、VLAN で分割できません。複数の VLAN をインラインでモニタするには、インライン VLAN ペアを使用してください。

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

ステップ 8　無差別 VLAN グループを追加するには、**3** と入力します。

```
Available Interfaces
  [1] GigabitEthernet0/7
  [2] GigabitEthernet0/8
Option:
```

ステップ 9　VLAN グループを GigabitEthernet0/8 に追加するには、**2** と入力します。

```
Promiscuous Vlan Groups for GigabitEthernet0/8
   None
Subinterface Number:
```

a. サブインターフェイス 10 を追加するには、**10** と入力します。

```
Subinterface Number: 10
Description[Created via setup by user asmith]:
Select vlans:
  [1] All unassigned vlans.
  [2] Enter vlans range.
Option:
```

b. 未割り当ての VLAN すべてをサブインターフェイス 10 に割り当てるには、**1** と入力します。

```
Subinterface Number:
```

c. サブインターフェイス 9 を追加するには、**9** と入力します。

```
Subinterface Number: 9
Description[Created via setup by user asmith]:
Vlans[]:
```

d. VLAN 1-100 をサブインターフェイス 9 に割り当てるには、**1-100** と入力します。

（注） この操作により、サブインターフェイス 10 に含まれている未割り当て VLAN から VLAN 1-100 が削除されます。

e. すべての VLAN グループを追加し終わるまで、ステップ c と d を繰り返します。

f. 空白の subinterface 行で Enter キーを押して、VLAN グループに使用できるインターフェイスのリストに戻ります。

```
  [1] GigabitEthernet0/7
  [2] GigabitEthernet0/8
Option:
```

ステップ 10　Enter キーを押して、最上位レベルのインターフェイス設定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] Modify interface default-vlan.
Option:
```

ステップ 11　Enter キーを押して、最上位レベルの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 12　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 vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

ステップ 13　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:
  Promiscuous:
   [1] GigabitEthernet0/7
```

ステップ 14　VLAN グループ GigabitEthernet0/8:10 を仮想センサー vs0 に追加するには、**2** と入力します。

```
Promiscuous Vlan Groups:
   [2] GigabitEthernet0/8:10  (Vlans: unassigned)
   [3] GigabitEthernet0/8:9  (Vlans: 1-100)
Add Interface:
```

ステップ 15　Enter キーを押して、最上位レベルの仮想センサー設定メニューに戻ります。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Promiscuous Vlan Groups:
   GigabitEthernet0/8:10  (Vlans: unassigned)
   GigabitEthernet0/8:9  (Vlans: 1-100)

  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

ステップ 16　Enter キーを押して、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 17　Enter キーを押して、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。

ステップ 18　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 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 19　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 idsm-2
telnet-option 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 GigabitEthernet0/8
admin-state enabled
subinterface-type vlan-group
subinterface 9
description Created via setup by user asmith
vlans range 1-100
exit
subinterface 10
description Created via setup by user asmith
vlans unassigned
exit
exit
exit
exit
service analysis-engine
virtual-sensor vs0
description Created via setup by user cisco
signature-definition sig0
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/8 subinterface-number 9
physical-interface GigabitEthernet0/8 subinterface-number 10
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
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 20　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 21　IDSM2 をリブートします。

```
idsm-2# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 22　リブートを続行するには、**yes** と入力します。

ステップ 23　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、IDSM2 に侵入防御を設定する準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）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 のコンソールおよび管理ポートは、IPS ソフトウェアによって設定および制御されます。また、ASA 5585-X GigabitEthernet および 10 GE ポートは、ASA ソフトウェアによって設定、制御および管理されます。ただし、IPS SSP をシャット ダウンまたはリセットした場合、ASA 5585-X ポートもリンク ダウンします。

続けて 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 SSP のセッションを開始します。

```
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,
export, 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　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）　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 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　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）　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 IPS SSP を設定します。

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

ステップ 8　Enter キーを押して、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 9　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 10　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 11　PortChannel0/0 を仮想センサー vs0 に追加するには、**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、PortChannel0/0 が割り当てられている仮想センサーです。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 12　Enter キーを押して、メインの仮想センサー メニューに戻ります。

ステップ 13　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 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を使用する場合にだけ必要です。

```
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）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 16　（任意）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 17　（任意）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 18　（任意）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）　PortChannel0/0 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 19　Enter キーを押して、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 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、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 21　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-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　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 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　リブートを続行するには、**yes** と入力します。

ステップ 25　リブート後、IPS SSP 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 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、HTTPS を使用して Web ブラウザでこの 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になります。

ステップ 27　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 IPS SSP の侵入防御設定を行う準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

NME IPS の高度なセットアップ

続けて NME IPS 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 NME IPS のセッションを開始します。

```
router# service-module ids-sensor 1/0 session
Trying 10.1.9.1, 2322 ... Open


sensor login: cisco
Password: ********
```

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　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）　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 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。分析エンジンが初期化中で、現在仮想センサーの設定を修正できないという警告が表示される場合があります。Space キーを押して、次のメニューを表示します。

```
[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.

Enter your selection[2]:
```

分析エンジンが初期化中という警告が表示された場合は、**2** と入力してここまでの設定を保存し、セットアップを終了します。その後、セットアップを再開し、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るまで Enter キーを押します。

ステップ 7　仮想センサーの設定を修正するには、**2** と入力します。

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/1
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 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　仮想センサー vs0 の設定を編集するには、**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] GigabitEthernet0/1
Add Interface:
```

ステップ 9　仮想センサー vs0 に GigabitEthernet0/1 を追加するには、**1** と入力します。

```
Add Interface: 1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
   GigabitEthernet0/1

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

ステップ 10　Enter キーを押して、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 11　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 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 12　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。または、Enter キーを押してデフォルトの no を受け入れます。

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name nme-ips
telnet-option enabled
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 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides
override-item-status Enabled
risk-rating-range 90-100
exit
exit

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

ステップ 13　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 14　NME IPS をリブートします。

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

ステップ 15　リブートを続行するには、**yes** と入力します。

ステップ 16　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、NME IPS に侵入防御を設定する準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

初期化の確認

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

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 Mon Nov 09 12:03:44 2009
! ------------------------------
! ! Version 7.1(1)E4
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S369.0   2009-09-29
! ------------------------------
service interface
exit
! ------------------------------
service authentication
password-strength
size 6
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 172.23.204.84/24,172.23.204.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server enabled
address 1.1.1.1
exit
dns-secondary-server enabled
address 2.2.2.2
exit
http-proxy proxy-server
address 1.1.1.1
port 1
exit
```

```
exit
time-zone-settings
offset -480
standard-time-zone-name PST
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
status
retired med-mem-retired
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） 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
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。

詳細情報

センサーにログインする手順については、第 22 章「センサーへのログイン」を参照してください。