CHAPTER 3

センサーの初期化

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。内容は次のとおりです。

初期化について

（注） **setup** コマンドは、管理者が使用する必要があります。

ネットワーク上にセンサーをインストールした後、**setup** コマンドを使用してそれを初期化し、ネットワーク経由で通信できるようにする必要があります。**setup** コマンドを使用して、基本的なセンサーの設定値を設定します。これには、ホスト名、IP インターフェイス、アクセス コントロール リスト、グローバル相関サーバ、および時間設定が含まれます。CLI で高度な設定を使用したまま、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。

簡単セットアップ モード

コンソール ケーブルを使用してセンサーに接続したときに、センサーの基本的なネットワーク設定値がまだ設定されていない場合、センサーは自動的に **setup** コマンドを呼び出します。次の条件では、センサーが自動セットアップを呼び出しません。

- すでに初期化が正常に完了している場合。
- センサーの復旧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の設定を正常に完了した後、ホスト設定をデフォルトに設定した場合。

setup コマンドを入力すると、システムのコンソール画面に 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。各プロンプトの隣のカッコ内の値は、最後に設定されたデフォルト値を表しています。

System Configuration Dialog

setup コマンドを入力すると、システムのコンソール画面に 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。

各プロンプトの隣のカッコ内の値は、現在の値です。

変更を行うオプションにたどり着くまで、System Configuration Dialog 全体に従います。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 を押します。

変更を中断し、System Configuration Dialog を最後まで実行せずに特権 EXEC プロンプトに戻るには、Ctrl キーを押した状態で C キーを押します。

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

変更が完了すると、セットアップ セッションで作成した設定が System Configuration Dialog に表示されます。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、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** と **no** のどちらかを入力する必要があります。

サマータイムは、recurring モードと date モードのどちらにも設定できます。recurring モードを選択した場合、開始日と終了日は週、曜日、月、および時刻に基づいたものになります。date モードを選択した場合、開始日と終了日は月、日、年、および時刻に基づいたものになります。disable を選択すると、サマータイムがオフになります。

（注）　System Configuration Dialog で日時を設定する必要があるのは、システムがアプライアンスであり、NTP を使用していない場合のみです。

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

例 3-1　System Configuration Dialog の例

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

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



Current time: Thu Jan 15 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 Collaboration?[yes]:
DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Collaboration?[yes]:
HTTP proxy server IP address[128.107.241.169]:
HTTP proxy server Port number[8080]:
Modify system clock settings?[no]: yes
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

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

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

センサーの基本的なセットアップ

setup コマンドを使用して基本的なセンサーのセットアップを行うことができ、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することができます。

setup コマンドを使用して基本的なセンサーのセットアップを行うには、次の手順に従います。

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 **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 インターフェイスの形式は、IP Address/Netmask,Gateway で *X.X.X.X/nn,Y.Y.Y.Y* のようになります。ここで、*X.X.X.X* はセンサーの IP アドレスを 32 ビット アドレスとして、ピリオド区切りの 4 つのオクテットで表したものです。また、*nn* はネットマスク内のビット数を指定し、*Y.Y.Y.Y* はデフォルトのゲートウェイを 32 ビット アドレスとして、ピリオド区切りの 4 つのオクテットで指定します。

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、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 とすると 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）が許可され、10.1.1.0/24 では 10.1.1.0 サブネット上の IP アドレス（10.1.1.0 ～ 10.1.1.255）のみが許可されます。アクセスをネットワーク全体でなく 1 つの IP アドレスだけに制限するには、32 ビットのネットマスクを使用します。たとえば、10.1.1.1/32 では 10.1.1.1 アドレスだけが許可されます。

c. アクセス リストに追加するすべてのネットワークを追加し終わるまでステップ b を繰り返したら、空の Permit 行で Enter を押して、次のステップに進みます。

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

b. HTTP プロキシ サーバを追加するには、**yes** と入力してから、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を使用するには、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。

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. サマータイムの設定値を修正するには、**yes** と入力します。

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

b. 米国のサマータイムのデフォルトを選択するには、**yes** と入力するか、**no** と入力して recurring、date、または disable 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指定します。

有効なエントリは、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。

有効なエントリは、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 日曜午前 2:00、終了時刻が 11 月の第 1 日曜日の午前 2:00 です。デフォルトのサマータイム オフセットは 60 分です。

g. サマータイム設定の終了月を指定します。

有効なエントリは、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。

有効なエントリは、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、[A-Za-z0-9()+:,_/-]+$ というパターンの 24 文字までの文字列です。

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。

協定世界時（UTC）からの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。

認証のある 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。そうでない場合は、認証なしの 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** を入力します。

- 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 : データが SensorBase ネットワークに提供されますが、潜在的に機密性の高いデータは除かれるため、送信されることはありません。
- Full : 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。これには、SensorBase Network への参加に付随する事項の説明があります。

ステップ 10　SensorBase Network に参加するには、**yes** と入力します。

```
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
exit
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** と入力して設定を保存します（または、**3** と入力し、CLI、IDM、または IME を使用した高度な設定を続行します）。

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

ステップ 12　**yes** と入力してセンサーをリブートします。

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（TLS に必要）を表示します。

```
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。

フィンガープリントは、Web ブラウザで HTTPS を使用してこのアプライアンスに接続するとき、証明書の信頼性を確認するために必要です。

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 IPS ソフトウェアを入手する手順については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）を参照してください。

高度な設定

ここでは、さまざまな Cisco IPS プラットフォームの CLI で高度な設定をさらに続ける方法について説明します。次のような構成になっています。

アプライアンス用の高度な設定

（注） 新しいサブインターフェイスの追加は、2 段階のプロセスです。最初に、仮想センサー設定を編集するときのインターフェイスを準備します。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応じて変更されますが、プロンプトはすべてのモデルに対して同じです。

アプライアンスの高度な設定を続行するには、次の手順に従います。

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　高度な設定にアクセスするために、**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　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

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

ステップ 6　インターフェイスと仮想センサーの設定を修正するために **yes** と入力すると、現在のインターフェイスの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　インターフェイスの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、インターフェイスの作成および削除ができます。仮想センサーの設定で、仮想センサーにインターフェイスを割り当てます。インターフェイスに無差別モードを使用し、それらを 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 ペアを追加し、利用可能なインターフェイスのリストを表示するには、**2** と入力します。

注意　新しい VLAN ペアは、仮想センサーに自動的には追加されません。

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

ステップ 9　たとえば、インライン VLAN ペアを GigabitEthernet0/0 に追加するには、**1** を入力します。

```
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 と 2 の番号を入力します。

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

ステップ 12　Enter を押すと、使用可能なインターフェイスのメニューに戻ります。

（注）　プロンプトで値を入力せずに復帰を入力すると、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 GigabitEthernet0/1 をインライン VLAN ペア用に設定できます。

ステップ 13　Enter を押して、トップ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 ペアを追加し、それらのオプションを表示するには、**4** を入力します。

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

ステップ 15　ペアの名前、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 を押して、トップ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 を押して、トップ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　**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 19　**2** を入力して、仮想センサーの設定 vs0 を修正します。

```
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　**3** を入力して、インライン VLAN ペア GigabitEthernet0/0:1 を追加します。

ステップ 21　**4** を入力して、インライン インターフェイス ペア NewPair を追加します。

ステップ 22　Enter を押して、トップ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 を押して、トップ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止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。この保護が必要ない場合は、自動脅威防止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　**yes** と入力して、すべての仮想センサーで自動脅威防止をディセーブルにします。

ステップ 26　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を終了します。

```
The following configuration was entered.
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name 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　**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 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　**yes** と入力してリブートを続行します。

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 IPS ソフトウェアを入手する手順については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）を参照してください。

AIM IPS の高度な設定

AIM IPS の高度な設定を続行するには、次の手順に従います。

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 との間にセッションを確立します。

```
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　高度な設定にアクセスするために、**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　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

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

ステップ 6　**yes** と入力して、インターフェイスおよび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あるという警告が表示されることがあり、その場合は仮想センサーの設定を修正できません。スペースバーを押すと、次のメニューが表示されます。

```
[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であるという警告が表示された場合は、**2** を入力して、これまでの設定を保存し、セットアップを終了します。その後、再びセットアップを開始し、インターフェイスおよび仮想センサーのメニューに戻るまで Enter を押してください。

ステップ 7　**2** を入力して、仮想センサーの設定を修正します。

```
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　**2** を入力して、仮想センサー vs0 の設定を編集します。

```
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　**1** を入力して、GigabitEthernet0/1 を仮想センサー vs0 に追加します。

```
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 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止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。この保護が必要ない場合は、自動脅威防止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　**yes** と入力して、すべての仮想センサーで自動脅威防止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 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　**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 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　**yes** と入力してリブートを続行します。

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 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手順については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）を参照してください。

AIP SSM の高度な設定

AIP SSM の高度な設定を続行するには、次の手順に従います。

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 との間に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。

ステップ 3　高度な設定にアクセスするために、**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　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

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

ステップ 6　**yes** と入力して、インターフェイスおよび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　インターフェイスの設定を編集するには、**1** と入力します。

（注）　AIP SSM にインターフェイスを設定する必要はありません。Modify interface default-vlan 設定は無視してください。AIP SSM の場合、仮想センサー間のトラフィックの分離は、他のセンサーの場合とは異なる方法で設定します。

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

ステップ 8　Enter を押して、トップ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　**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] GigabitEthernet0/1
Add Interface:
```

ステップ 11　**1** を入力して、GigabitEthernet0/1 を仮想センサー vs0 に追加します。

（注） ASA 7.2 以前では、1 つの仮想センサーがサポートされます。GigabitEthernet0/1 を割り当てられた仮想センサーは、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に使用されます。GigabitEthernet0/1 を 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ることもできます。

（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ます。ASA 7.2.3 では、パケットを特定の仮想センサーに送信したり、デフォルトの仮想センサーによってモニタされるパケットを送信したりできます。デフォルトの仮想センサーは、GigabitEthernet0/1 を割り当てた仮想センサーです。GigabitEthernet0/1 を 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ることもできます。

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

ステップ 13　**3** を入力して仮想センサーを作成します。

```
Name[]:
```

ステップ 14　仮想センサーの名前と説明を入力します。

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

ステップ 15　**1** を入力して、既存の異常検出設定である 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　**2** を入力して、シグニチャ定義設定ファイルを作成します。

ステップ 17　シグニチャ定義設定ファイル名、**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　**1** を入力して、イベント アクション規則の既存の設定である rules0 を使用します。

（注）　GigabitEthernet0/1 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ます。GigabitEthernet0/1 を割り当てられた仮想センサーは、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に使用されます。GigabitEthernet0/1 を 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ることもできます。

（注）　IPS 6.0 を使用する ASA 7.2.3 以降では、複数の仮想センサーがサポートされます。ASA 7.2.3 では、パケットを特定の仮想センサーに送信したり、デフォルトの仮想センサーによってモニタされるパケットを送信したりできます。デフォルトの仮想センサーは、GigabitEthernet0/1 を割り当てた仮想センサーです。GigabitEthernet0/1 を 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ることもできます。

```
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 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止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。この保護が必要ない場合は、自動脅威防止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脅威防止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 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　**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　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　**yes** と入力してリブートを続行します。

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手順については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）を参照してください。

IDSM2 の高度な設定

IDSM2 の高度な設定を続行するには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して IDSM2 との間にセッションを確立します。

- 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　高度な設定にアクセスするために、**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　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

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

ステップ 6　**yes** と入力して、インターフェイスおよび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　インターフェイスの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、インターフェイスの作成および削除ができます。仮想センサーの設定で、仮想センサーにインターフェイスを割り当てます。インターフェイスに無差別モードを使用し、それらを 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 ペアが動作している場合、2 つの IDSM2 データ ポートはネイティブ VLAN のみ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。パケットは 802.1q ヘッダーを持たず、VLAN によって分離できません。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 8　**3** を入力して無差別 VLAN グループを追加します。

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

ステップ 9　**2** を入力し、次のように VLAN グループを GigabitEthernet0/8 に追加します。

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

a.　**10** を入力してサブインターフェイス 10 を追加します。

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

b.　**1** を入力して、未割り当てのすべての VLAN をサブインターフェイス 10 に割り当てます。

```
Subinterface Number:
```

c.　**9** を入力してサブインターフェイス 9 を追加します。

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

d.　**1-100** と入力して VLAN 1 ～ 100 をサブインターフェイス 9 に割り当てます。

（注）　これにより、VLAN 1 ～ 100 がサブインターフェイス 10 に含まれている未割り当ての VLAN から削除されます。

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

f. 空白のサブインターフェイス行で Enter を押し、VLAN グループに使用可能な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 を押して、トップ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 を押して、トップレベル 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　**2** を入力して、仮想センサーの設定を編集します。

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

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

ステップ 14　**2** を入力して、VLAN グループ GigabitEthernet0/8:10 を仮想センサー vs0 に追加します。

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

ステップ 15　Enter を押して、トップ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 を押して、トップ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 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止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。この保護が必要ない場合は、自動脅威防止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　**yes** と入力して、すべての仮想センサーで自動脅威防止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 IDSM2
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　**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 21　IDSM2 をリブートします。

```
IDSM2# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 22　**yes** と入力してリブートを続行します。

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 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手順については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）を参照してください。

NME IPS の高度な設定

NME IPS の高度な設定を続行するには、次の手順に従います。

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 との間にセッションを確立します。

```
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　高度な設定にアクセスするために、**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　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

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

ステップ 6　**yes** と入力して、インターフェイスおよび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あるという警告が表示されることがあり、その場合は仮想センサーの設定を修正できません。スペースバーを押すと、次のメニューが表示されます。

```
[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であるという警告が表示された場合は、**2** を入力して、これまでの設定を保存し、セットアップを終了します。その後、再びセットアップを開始し、インターフェイスおよび仮想センサーのメニューに戻るまで Enter を押してください。

ステップ 7　**2** を入力して、仮想センサーの設定を修正します。

```
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　**2** を入力して、仮想センサー vs0 の設定を編集します。

```
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　**1** を入力して、GigabitEthernet0/1 を仮想センサー vs0 に追加します。

```
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 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止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。この保護が必要ない場合は、自動脅威防止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止をディセーブルにするには、**yes** と入力します。そうでない場合は、Enter を押してデフォルトの no のままにします。

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name 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　**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 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　**yes** と入力してリブートを続行します。

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 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手順については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）を参照してください。

初期化の確認

センサーが初期化されたかどうかを確認するには、次の手順に従います。

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 Feb 09 12:03:44 2009
! ------------------------------
!Version 7.0(4)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S365.0   2008-10-31
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
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
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
!------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

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

ステップ 3　自己署名 X.509 証明書（TLS で必要）を表示します。

```
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 2 章「センサーへのログイン」を参照してください。