



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を説明します。この章は、次の項で構成されています。

- [概要 \(P.9-2\)](#)
- [System Configuration Dialog \(P.9-2\)](#)
- [センサーの初期化 \(P.9-3\)](#)
- [初期化の確認 \(P.9-10\)](#)

概要

センサーをネットワークに設置した後、**setup** コマンドを使用してセンサーを初期化する必要があります。**setup** コマンドを使用すると、ホスト名、IP インターフェイス、Telnet サーバ、Web サーバポート、アクセスコントロールリスト、時間設定、およびインターフェイスの割り当てと有効化など、センサーの基本的な設定を行います。センサーを初期化すると、ネットワーク経由でセンサーと通信できるようになります。その時点で、侵入防御を設定する準備が整います。

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 という対話型のダイアログが表示されます。この System Configuration Dialog によって、設定プロセスの手順が示されます。

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。

変更を行わず、System Configuration Dialog 全体を実行しないで EXEC プロンプトに戻るには、**Ctrl+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を表示できます。ヘルプテキストにアクセスするには、プロンプトで疑問符 (?) を押します。

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尋ねるメッセージが表示されます。**yes** を入力すると、その設定が保存されます。**no** を入力すると、設定は保存されずに、プロセスが再度開始されます。このプロンプトにはデフォルトはありません。**yes** または **no** を入力する必要があります。

サマータイムは、**recurring** モードまたは **date** モードのいずれかで設定できます。**recurring** モードを選択すると、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。

System Configuration Dialog では、デフォルトの仮想センサー vs0 を編集できます。仮想センサーには、混合モードとインライン ペアの両方またはどちらかを割り当てることができます。またこれは、割り当てられたインターフェイスを使用可能にします。セットアップが完了すると、仮想センサーはトラフィックを監視するように設定されています。



(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。

センサーの初期化

センサーを初期化するには、次の手順を実行します。

ステップ 1 管理者特権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。

- シリアル接続、またはモニタとキーボードを使用して、アプライアンスにログインします。



(注) IDS-4215、IPS-4240、または IPS-4255 では、モニタとキーボードは使用できません。

- IDS-2 とのセッション：

— Catalyst ソフトウェアの場合：

```
cat6k> enable
cat6k> (enable) session module_number
```

— Cisco IOS ソフトウェアの場合：

```
switch# session slot slot_number processor 1
```

- NM-CIDS とのセッション：

```
router# service-module IDS-Sensor slot_number/port_number session
```

- AIP SSM とのセッション：

```
asa# session 1
```



(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。



注意

パスワードを忘れた場合はセンサー イメージの再作成が必要なこともあります（『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照）。ただし、管理者特権を持つ別のユーザがいる場合を除きます。別の管理者がログインして、パスワードを忘れたユーザに新しいパスワードを割り当てることができます。または、サポートのためにサービス アカウントを作成している場合には、TAC でパスワードを作成してもらうことができます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。

パスワードを変更すると、`sensor#` プロンプトが表示されます。

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。



(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。

```
--- 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 Configuration:
```

```
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
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
```

```
Current time: Wed May 5 10:25:35 2004
```

ステップ 4 Space キーを押して次の質問を表示します。

```
Continue with configuration dialog? [yes]:
```

一度に 1 ページずつ表示するには Space キーを押します。一度に 1 行ずつ表示するには **Enter** キーを押します。

ステップ 5 `yes` を入力して続行します。

ステップ 6 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「-」は有効ですが、スペースは入力できません。デフォルトは `sensor` です。

ステップ7 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。ここでの X.X.X.X (X は 0 ~ 255) 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 はネットマスクの番号です。Y.Y.Y.Y (Y は 0 ~ 255) 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8 Telnet サーバのステータスを指定します。

Telnet サービスは `disable` または `enable` に設定できます。デフォルトは `disable` です。

ステップ9 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 サーバポートを変更した場合は、IDM への接続時にブラウザの URL アドレスでそのポートを指定する必要があります。指定する形式は `https://sensor_ip_address:port` (たとえば、`https://10.1.9.201:1040`) 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、暗号化は無効になりません。

ステップ10 `yes` を入力してネットワーク アクセス リストを修正します。

- a. エントリを削除する場合は、エントリの番号を入力して **Enter** 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。

IP ネットワーク インターフェイスは、IP アドレス/ネットマスク (X.X.X.X/nn) の形式で指定します。ここでの X.X.X.X (X は 0 ~ 255) 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、そのネットワークのネットマスクの番号です。

たとえば、`10.0.0.0/8` は 10.0.0.0 ネットワーク上のすべての IP アドレス (10.0.0.0 ~ 10.255.255.255) を許可し、`10.1.1.0/24` は 10.1.1.0 サブネット上の IP アドレス (10.1.1.0 ~ 10.1.1.255) だけを許可します。

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

- c. アクセスリストに追加するネットワークの入力がすべて終わるまで、ステップ b を繰り返します。
- d. 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 11 システムクロックの設定値を修正するには、**yes** を入力します。

- a. NTP を使用する場合は **yes** を入力します。

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。手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring the Sensor to Use an NTP Server as its Time Source」を参照してください。

- b. サマータイム設定を修正するには、**yes** を入力します。



(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 n に進みます。

- c. サマータイムの設定方法を指定するには、**recurring**、**date**、または **disable** を入力します。

デフォルトは **recurring** です。

- d. **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。

デフォルトは **april** です。

- e. 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 **first** です。

- f. 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。

デフォルトは **sunday** です。

- g. 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。デフォルト値は、開始時刻が 4 月の第 1 日曜日午前 2 時、終了時刻が 10 月の第 4 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。

- h. 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。

デフォルトは **october** です。

- i. 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 **last** です。

- j. 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。

デフォルトは **sunday** です。

- k. サマータイム設定の終了時刻を指定します。

- l. 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。
- m. サマータイム オフセットを指定します。
世界標準時 (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 0 です。
- n. システムの時間帯を修正するには、**yes** を入力します。
- o. 標準時の時間帯名を指定します。
ゾーン名は 24 文字までの文字列です。
- p. 標準時のオフセットを指定します。
デフォルトは 0 です。
世界標準時 (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)。

ステップ 12 **yes** を入力して、仮想センサーの設定を修正します (vs0)。

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: GigabitEthernet0/1
Unused:
  GigabitEthernet2/1
  GigabitEthernet2/0
Promiscuous:
  GigabitEthernet0/0
Inline:
  None
Inline VLAN Pair:
  None
```

ステップ 13 混合インターフェイスまたはモニタリング インターフェイスを追加するには、**yes** と入力します。

ステップ 14 たとえば `GigabitEthernet0/1` のように、追加するインターフェイスを入力します。

ステップ 15 **yes** と入力して、インライン インターフェイス ペアを追加します (プラットフォームがインライン インターフェイス ペアをサポートしている場合だけ表示されます)。

- a. インライン インターフェイス ペアの名前を入力します。
- b. インライン インターフェイス ペアの説明を入力します。
デフォルトは、`Created via setup by user <yourusername>` です。
- c. インライン ペアの最初のインターフェイスの名前 **interface1** を入力します。
- d. インライン ペアの 2 番目のインターフェイスの名前 **interface2** を入力します。
- e. a ~ d のステップを繰り返して、さらにインライン インターフェイス ペアを追加するか、**Enter** を押して次のオプションに進みます。

ステップ 16 **yes** と入力して、インライン VLAN ペアを追加します（プラットフォームがインライン VLAN ペアをサポートしている場合だけ表示されます）。

インライン VLAN ペアに使用できるインターフェースのリストが、次のように表示されます。

```
Available Interfaces:
[1] GigabitEthernet0/0
[2] GigabitEthernet2/0
[3] GigabitEthernet2/1
```

ステップ 17 さらに分割してインライン VLAN ペアにするインターフェースの番号を入力します。

そのインターフェースの現在のインライン VLAN ペア設定が、次のように表示されます。

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

- a. 追加するサブインターフェースの番号を入力します。
- b. インライン VLAN ペアの説明を入力します。
- c. 最初の VLAN 番号 (vlan1) を入力します。
- d. 2 番目の VLAN 番号 (vlan2) を入力します。
- e. a ~ d のステップを繰り返して、このインターフェース上にさらにインライン VLAN ペアを追加するか、**Enter** を押して次のオプションに進みます。

ステップ 18 別のインターフェースをさらに分割するには、**yes** と入力します。インライン VLAN ペアの追加を終了するには、**no** と入力するか、**Enter** を押します。

設定した内容が次のオプションと共に表示されます。

```
[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.
```

ステップ 19 **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 20 システムの日付と時刻を修正するには、**yes** を入力します。



(注) このオプションは、モジュールでは使用できません。また NTP が設定されている場合も使用できません。このモジュールは、設置されているルータまたはスイッチ、あるいは設定済みの NTP サーバから時刻を取得します。

- a. 現地日付を入力します (yyyy-mm-dd)。
- b. 現地時間を入力します (hh:mm:ss)。

ステップ 21 センサーをリブートします。

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

ステップ 22 `yes` を入力してリブートを続行します。

ステップ 23 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 24 証明書のフィンガープリントを書き留めます。

この情報は、Web ブラウザでこのセンサーへ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 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。

最新版のソフトウェアを入手する方法については、P.10-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。最新のソフトウェア アップデートを適用する方法は Readme で説明されています。

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。

初期化の確認

`setup` コマンドを実行した後で、センサーが正しく初期化されたことを確認する必要があります。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。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Logging In to the Sensor」を参照してください。

ステップ2 設定を表示します。

```

sensor# show configuration
generating current config:
! -----
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! -----
display-serial
! -----
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! -----
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit

```

```

exit
! -----
service logger
exit
! -----
service network-access
exit
! -----
service notification
exit
! -----
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
! -----
service ssh-known-hosts
exit
! -----
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SgGS Ib3DQEBBQUAMFcx CzAJBgNVBAYTA1VTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ2l2Y28gU3lzdGVtcywgSW5jLjESM
BAGA1UECXMJUU1NNLU1QUzEwMRyYwFAYDVQQDEw0xMC44OS4xNDkuMjE1MIGfMA0GCsqGS Ib3DQEBAQUAA
4GNADCBiQKBgQC0obDuZOE Pudw63Rlt8K1YsymzR/D9Rlcnad/U0gjAQGfcUh3sG3TXPQewon1fh0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANMf4zPcPCAORJ6DMQHFj44A+3tMZWsC

```

```

yaod23S1oYOxx7v5puPDYn3IQIDAQABMA0GCSqGSIB3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVWHji12vBLo+biULJG95hbTF1qO+ba3R6nPD3tepgx5zTdOr2onn1FHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ11AQDiogskdCs4ax1tB4SbEU5y1tkKgcwWEdJpbbNHzpoRsRICfM3H1OEwN
exit
! -----
service web-server
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。

この情報は、Web ブラウザでこのセンサーへ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。