CHAPTER 21

NME IPS の設定

（注） すべての IPS プラットフォームで、許可される同時 CLI セッション数は 10 です。

この章では、NME IPS を設定し、IPS トラフィックの受信を準備する方法について説明します。これで、侵入防御を設定する準備が整います。この章は、次の内容で構成されています。

NME IPS の設定手順

NME IPS を設定するには、次のタスクを実行します。

1. インターフェイスを設定します。
2. NME IPS にログインします。
3. NME IPS を初期化します。

   setup コマンドを実行して NME IPS を初期化します。
4. NME IPS が侵入防御のためにトラフィックをキャプチャするように設定します。
5. サービス アカウントを作成します。

注意 サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用して新しいパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

6. ユーザの追加、信頼されるホストの追加など、その他の初期タスクを実行します。
7. 侵入防御を設定します。
8. グローバル相関を設定します。
9. NME IPS をスムーズに実行し続けるための管理タスクを実行します。
10. 新しいシグニチャ アップデートおよびサービス パックで IPS ソフトウェアをアップグレードします。
11. 必要な場合はブート ヘルパーとブートローダのイメージを再作成します。

詳細情報

- インターフェイスを設定する手順については、「NME IPS およびルータでのインターフェイスの設定」（P.21-4）を参照してください。
- NME IPS にログインする手順については、「NME IPS へのログイン」（P.2-8）を参照してください。
- NME IPS で **setup** コマンドを実行する手順については、「NME IPS の高度な設定」（P.3-24）を参照してください。
- サービス アカウントを作成する手順については、「サービス アカウントの作成」（P.4-22）を参照してください。
- センサーを設定する手順については、第 4 章「センサーのセットアップ」を参照してください。
- 侵入防御を設定する手順については、第 9 章「異常検出の設定」、第 7 章「イベント アクション規則の設定」、第 8 章「シグニチャの定義」、および第 14 章「Attack Response Controller でのブロッキングとレート制限の設定」を参照してください。
- グローバル相関を設定する手順については、第 10 章「グローバル相関の設定」を参照してください。
- センサーをスムーズに実行し続ける手順については、第 17 章「センサーの管理タスク」を参照してください。
- Cisco IPS ソフトウェアの入手の詳細については、「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 のイメージを再作成する手順については、「NME IPS システム イメージのインストール」（P.23-41）を参照してください。

インストールの検証とシリアル番号の確認

NME IPS のインストールを検証するには、特権 EXEC モードで **show inventory** コマンドを使用します。

（注） このコマンドを使用して、TAC とのトラブルシューティングで使用される NME IPS のシリアル番号を調べることもできます。シリアル番号は、SN: FHH1117001R のように PID 行に表示されます。

NME IPS のインストールを検証するには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

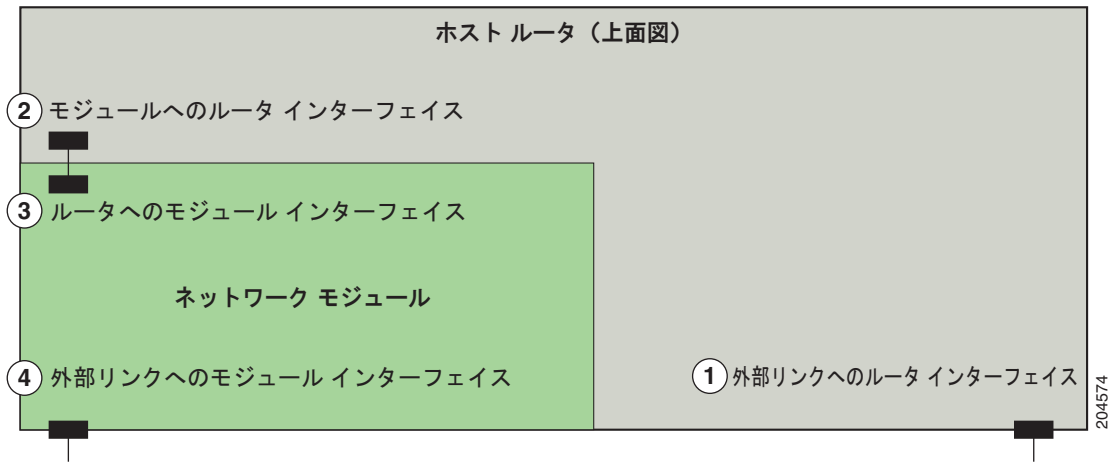
ステップ 3　NME IPS がルータ インベントリに含まれていることを確認します。

```
router# show inventory
NAME: "3845 chassis", DESCR: "3845 chassis"
PID: CISCO3845          , VID: V01 , SN: FTX1002C255

NAME: "c3845 Motherboard with Gigabit Ethernet on Slot 0", DESCR: "c3845 Motherboard with
Gigabit Ethernet"
PID: CISCO3845-MB       , VID: V03 , SN: FOC09514J4Y

NAME: "4 Port FE Switch on Slot 0 SubSlot 0", DESCR: "4 Port FE Switch"
PID: HWIC-4ESW          , VID: V01 , SN: FOC1102394U

NAME: "High Speed WAN Interface Card - 1 Port Gigabit Ethernet on Slot 0 SubSlot
 3", DESCR: "High Speed WAN Interface Card - 1 Port Gigabit Ethernet"
PID: HWIC-1GE-SFP       , VID: V01 , SN: FOC10164DAR

NAME: "1000BASE-T SFP", DESCR: "1000BASE-T SFP"
PID: SP7041             , VID: C  , SN: 00000MTC101608RB

NAME: "Cisco Intrusion Prevention System NM on Slot 2", DESCR: "Cisco Intrusion
Prevention System NM"
PID: NME IPS-K9         , VID: V01, SN: FHH1117001R


router#
```

NME IPS ハードウェア インターフェイス

図 21-1 に、内部および外部の通信に使用されるルータ インターフェイスと NME IPS インターフェイスを示します。ルータ インターフェイスは Cisco IOS CLI で設定し、NME IPS インターフェイスは IPS CLI、IDM、IME、または CSM で設定できます。

図 21-1　NME IPS インターフェイスとルータ インターフェイス



1	外部リンクへのルータ インターフェイス Cisco IOS CLI を使用して標準のルータ設定を行います。
2	NME IPS へのルータ インターフェイス（ids-sensor x/0） Cisco IOS CLI を使用して、NME IPS の IP アドレスとデフォルトのゲートウェイ ルータを設定します。
3	ルータへの NME IPS インターフェイス（GigabitEthernet0/1） Cisco IOS CLI を使用して、インラインまたは無差別でインターフェイスを設定します。
4	外部リンクへの NME IPS インターフェイス（Management0/1） IPS CLI、IDM、IME、または CSM を使用して、コマンド/コントロール インターフェイスを設定します。

NME IPS およびルータでのインターフェイスの設定

ここでは、NME IPS とルータでインターフェイスを設定する方法について説明します。内容は次のとおりです。

NME IPS インターフェイスの設定手順

NME IPS とルータでインターフェイスを設定するには、次の手順に従います。

1. ルータで IPS コマンド/コントロール インターフェイスを設定し、NME IPS の IP アドレス、マスク、およびゲートウェイを設定します。
2. モニタリング インターフェイスをイネーブルにし、無差別またはインラインのいずれであるかを指定し、インターフェイスに ACL を割り当て、モジュールに障害が発生した場合にルータでトラフィックを処理する方法を指定し、モニタリング ACL（任意）を作成します。
3. 設定を保存します。

詳細情報

- IDS-Sensor インターフェイスでアンナンバード IP アドレスを設定する手順については、「ルータでの IDS-Sensor インターフェイスの設定」（P.21-6）を参照してください。
- モニタリング インターフェイスをイネーブルにする手順については、「ルータ インターフェイスでのモニタリングの設定」（P.21-7）を参照してください。

NAT の利点

NAT には次の利点があります。

- 内部ネットワークでプライベート IP アドレスを使用できます。プライベート IP アドレスは、インターネット上でルーティングできません。
- NAT はローカル IP アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際の IP アドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

詳細情報

ARC と NAT を連携させる方法については、「ARC および NAT」（P.21-5）を参照してください。

ARC および NAT

NAT を使用して、NME IPS への管理アクセスを確立する場合、NME IPS の ARC は、NME IPS の外部 IP アドレスを認識しません NME IPS への管理アクセスが、NME IPS が管理しているデバイスによって中断されないようにするには、ブロッキング デバイスを追加するたびに、NME IPS の NAT アドレスを宣言する必要があります。

詳細情報

- ARC の詳細については、第 14 章「Attack Response Controller でのブロッキングとレート制限の設定」を参照してください。
- ブロッキング デバイスを追加するたびに NME IPS NAT アドレスを設定する手順については、次の手順を参照してください。
  - 「センサーで Cisco ルータを管理する設定」（P.14-23）
  - 「Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するセンサーの設定」（P.14-26）
  - 「センサーで Cisco ファイアウォールを管理する設定」（P.14-28）

ルータでの IDS-Sensor インターフェイスの設定

NME IPS インターフェイスを設定するには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

ステップ 4　CEF スイッチング パスをイネーブルにします。

```
router> configuration terminal
router(config)# ip cef
router(config)#
```

ステップ 5　ループバック インターフェイスを作成します。

```
router(config)# interface loopback 0
router(config-if)#
```

ステップ 6　ループバック インターフェイスに IP アドレスとネットマスクを割り当てます。

```
router(config-if)# ip address 10.99.99.99 255.255.255.255
router(config-if)# exit
router(config)#
```

（注）　NME IPS とのセッションを確立するには、NME IPS の内部インターフェイスに IP アドレスを割り当てる必要があります。ルータ内の他のインターフェイスに割り当てられているネットワークと重複しないネットワークを選択してください。

ステップ 7　アンナンバード ループバック インターフェイスを IDS-Sensor インターフェイスに割り当てます。この例ではスロット 1 を使用します。

```
router(config)# interface ids-sensor 1/0
router(config-if)# ip unnumbered Loopback 0
router(config-if)#
```

ステップ 8　ポートをアクティブにします。

```
router(config-if)# no shutdown
router(config-if)#
```

ステップ 9　コンフィギュレーション モードを終了します。

```
router(config-if)# end
```

ステップ 10　設定を NVRAM に書き込みます。

```
router# write memory
Building configuration
[OK]
```

これで、NME IPS を初期化し、侵入防御を設定する準備が整いました。

詳細情報

- ルータから NME IPS へのセッションの接続と終了の詳細については、「セッションの確立」（P.21-8）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 の高度な設定」（P.3-24）を参照してください。
- 侵入防御を設定する手順については、次の IPS ガイドを参照してください。
  - 『*Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 7.0*』
  - 『*Cisco Intrusion Prevention System Manager Express Configuration Guide for IPS 7.0*』
  - 『*Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.0*』

ルータ インターフェイスでのモニタリングの設定

モニタするルータ インターフェイスを設定するには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　（任意）ルータのモニタリング アクセス リストを設定します。

```
router(config)# access-list 101 permit tcp any eq www any
```

標準アクセス リストを設定し、どの種類のトラフィックを検査するかのフィルタリングにそのリストを適用できます。ACL が一致すると、その ACL に対してトラフィックは検査されません。この例では、HTTP トラフィックの検査だけをバイパスします。**access-list** コマンドのオプションの詳細については、『Cisco IOS Command Reference』を参照してください。

ステップ 4　インライン モードまたは無差別モードのいずれかでインターフェイスのモニタリングをイネーブルにし、アクセス リストを関連付けます。

```
router(config)# interface monitored_interface
router(config-if)# ids-service-module monitoring {inline | promiscuous} access-list 101
router(config-if)# exit
router(config)#
```

（注）　インターフェイスにアクセス リストを関連付けることによって、NME IPS に送信されるトラフィックがさらに制御されます。

ステップ 5　（インライン モードで）ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

ステップ 6　（インライン モードで）ルータが、モジュールの障害時にトラフィック検査を処理する方法を指定します。

```
router(config)# interface ids-sensor 1/0
```

```
router(config-if)# service-module {fail-close | fail-open}
router(config-if)#
```

デフォルトはフェールオープンです。

（注）　**fail-close** オプションでは、NME IPS に障害が発生した場合に、ルータがトラフィックを通過させません。**fail-open** オプションでは、NME IPS に障害が発生した場合に、ルータはトラフィックを通過させますが、IPS による検査は実行されません。

ステップ 7　コンフィギュレーション モードを終了します。

```
router(config-if)# exit
router(config)# exit
router#
```

ステップ 8　設定を NVRAM に書き込みます。

```
router# write memory
Building configuration
[OK]
```

詳細情報

- 無差別モードの詳細については、「無差別モードの設定」（P.6-17）を参照してください。
- インライン インターフェイス モードの詳細については、「インライン インターフェイス モードの設定」（P.6-19）を参照してください。

セッションの確立

NME IPS には外部コンソール ポートがないため、ルータで **service-module ids-sensor** *slot*/*port* **session** コマンドを発行するか、ルータへの Telnet 接続を、NME IPS ポート番号に対応するスロット番号で開始すると、NME IPS のコンソールにアクセスできるようになります。外部コンソール ポートがないことは、初期ブート設定がルータを通じてのみ可能であることを意味します。

service-module ids-sensor *slot*/*port* **session** コマンドを発行すると、NME IPS との間にコンソール セッションが作成されます。このセッションで任意の IPS コンフィギュレーション コマンドを発行できます。セッションでの作業を完了し、IPS CLI を終了すると、Cisco IOS CLI に戻ります。

session コマンドを使用すると、IDS-Sensor インターフェイスの IP アドレスを使用して逆方向の Telnet 接続が開始されます。IDS-Sensor インターフェイスは、NME IPS とルータの間のインターフェイスです。**session** コマンドを起動する前に、IDS-Sensor インターフェイスに IP アドレスを割り当てる必要があります。ルーティング可能な IP アドレスを割り当てると、IDS-Sensor インターフェイス自体が攻撃に対して脆弱になることがあります。これは、NME IPS がルーティング可能な IP アドレスによってネットワーク上に露出する（ルータの外部で NME IPS と通信できる）ためです。この脆弱性に対応するには、IDS-Sensor インターフェイスにアンナンバード IP アドレスを割り当てます。これにより、NME IPS IP アドレスは、ルータと NME IPS の間でローカルにのみ使用され、NME IPS との間にセッションを確立する目的のために分離されます。

（注）　アプリケーション ソフトウェアをインストールするか、モジュールのイメージを再作成する前に、ブートローダを始動するセッションを開始します。ソフトウェアのインストール後、アプリケーションを始動するセッションを開始します。

注意　モジュールにセッション接続し、大量のコンソール転送を実行した場合、ホスト コンソール インターフェイス速度が 115200/bps 以上に設定されていない限り、文字トラフィックが失われることがあります。速度が 115200/bps に設定されていることを確認するには、**show running config** コマンドを使用します。

詳細情報

IDS-Sensor インターフェイスを設定する手順については、「ルータでの IDS-Sensor インターフェイスの設定」（P.21-6）を参照してください。

セッションの開閉

（注）　ルータから NME IPS を初期化する必要があります（**setup** コマンドを実行します）。ネットワークを設定すると、SSH と Telnet を使用できるようになります。

NME IPS からモジュールとのセッションを確立するには、**service-module ids-sensor** *slot*/*port* **session** コマンドを使用します。Ctrl キーと Shift キーを押した状態で 6 を押してから、x キーを押して、セッション プロンプトをルータ プロンプトに戻します。NME IPS プロンプトからルータ プロンプトに戻ります。空白行で Enter を押して、セッション プロンプト（これもルータ プロンプト）に戻ります。ルータ コマンドの実行後にセッションに戻る場合にだけ、ルータとのセッションを一時停止する必要があります。NME IPS セッションに戻る予定がない場合は、セッションを一時停止する代わりに、セッションを閉じる必要があります。

セッションを閉じる場合は、NME IPS CLI から完全にログアウトします。新しいセッション接続では、ログインのためにユーザ名とパスワードが必要です。一時停止したセッションでは、CLI にログインしたままになります。**session** コマンドで接続した場合は、ユーザ名とパスワードを入力せずに、同じ CLI に戻ることができます。

（注）　Telnet クライアントには多くの種類があります。クライアントによっては、Ctrl キーを押した状態で 6 を押してから x キーを押す必要があります。制御文字は、^^、Ctrl-^、または ASCII 値 30（16 進数では 1E）で表されます。

注意　**disconnect** コマンドを使用してセッションを終了しても、そのセッションは残ります。この開いている状態のセッションは、残った接続を利用しようとしている人間に悪用されるおそれがあります。

NME IPS とのセッションを開始および閉じるには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　NME IPS のステータスをチェックし、動作していることを確認します。

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..
```

```
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             NME IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.195
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

ステップ 3　ルータから NME IPS へのセッションを開きます。

```
router# service-module ids-sensor 1/0 session
Trying 10.89.148.195, 2322 ... Open
```

ステップ 4　モジュール セッションを終了または一時停止して、閉じます。

- `sensor# exit`

（注）　IPS CLI のサブモードを開始している場合は、すべてのサブモードを終了する必要があります。センサーのログイン プロンプトが表示されるまで、**exit** と入力します。

注意　セッションを適切に終了しないと、残っているセッションを別のユーザが乗っ取ることが可能になります。Cisco IOS セッションを完全に終了するには、必ず `router#` プロンプトで **exit** と入力してください。

- NME IPS との間のセッションを一時停止し、閉じるには、Ctrl キーと Shift キーを押した状態で 6 を押します。すべてのキーから指を離してから、x キーを押します。

（注）　セッションでの作業が終了したら、ルータに戻ってセッション（IPS アプリケーション）とモニタ対象のルータ インターフェイスの間の関連付けを確立する必要があります。

ステップ 5　ルータから接続解除します。

```
router# disconnect
```

ステップ 6　Enter を押して接続解除を確認します。

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

詳細情報

NME IPS を初期化する手順については、「NME IPS の高度な設定」（P.3-24）を参照してください。

NME IPS のステータスの表示

NME IPS のステータスと統計情報を表示するには、特権 EXEC モードで、**service-module ids-sensor** *slot/port* **status** コマンドを使用します。

NME IPS のステータスを表示するには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　NME IPS のステータスを表示します。

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version:  7.0(4)E4
  Model:             NME IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.195
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

ハートビート リセットのイネーブル化とディセーブル化

NME IPS のハートビートをリセットするには、特権 EXEC モードで、**service-module ids-sensor** *slot/port* **heartbeat reset {enable | disable}** コマンドを使用します。

NME IPS がフェールセーフ モードでブートされるか、アップグレード中の場合、**service-module ids heartbeat-reset** コマンドを使用するとプロセス中のリブートを防止できます。アップグレード中にハートビート リセットをイネーブルのままにした場合、NME IPS ハートビートが失われることがあります。

NME IPS ハートビートが失われた場合、ルータは、NME IPS に fail-open または fail-close の設定オプションを適用し、NME IPS へのトラフィックの送信を停止し、NME IPS をエラー状態に設定します。ルータは、NME IPS でハードウェア リセットを実行し、ハートビートが再確立されるまで NME IPS をモニタします。

（注）　ハートビート リセットをディセーブルにすると、システム イメージのインストール中に（このプロセスに非常に長い時間がかかる場合）、ルータによるモジュールのリセットが防止されます。

NME IPS のハートビートをリセットするには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ハートビート リセットのステータスを確認します。

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled
```

ステップ 4　NME IPS でハートビートをディセーブルにするには、次のコマンドを実行します。

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```

ステップ 5　NME IPS でハートビートを再びイネーブルにするには、次のコマンドを実行します。

```
router# service-module ids-sensor 1/0 heartbeat-reset enable
```

詳細情報

- NME IPS をアップグレードする手順については、「センサーのアップグレード」（P.23-2）を参照してください。
- NME IPS システム イメージをインストールする手順については、「NME IPS システム イメージのインストール」（P.23-41）を参照してください

NME IPS のリブート、リセット、およびシャットダウン

ここでは、NME IPS をシャットダウンする場合と方法について説明します。次の項目について説明します。

NME IPS ステータス モニタリング

NME IPS は RBCP を使用して、そのステータスをモニタします。RBCP は、SensorApp ではなく、NME IPS のメイン アプリケーションによってモニタされます。NME IPS のメイン アプリケーションに障害が発生した場合、RBCP ハートビート応答は NME IPS から返されません。ルータで、NME IPS に障害が発生したと判断された場合、RBCP を通じて **reload** コマンドが発行され、NME IPS で Linux カーネルがリブートされます。NME IPS の修復を試みている間、ルータは設定したフェールオーバー処理によって決定されるモードで動作します。

SensorApp の処理は停止する場合がありますが、NME IPS のメイン アプリケーションは、RBCP パケットの処理を続けます。この場合、NME IPS に対して設定したバイパス設定に従って、IPS CLI、IDM、または IME により、パケットが処理されます。

次のような 2 つの状況で、NME IPS はシャットダウンされます。

- ハードウェアまたはソフトウェアのエラーにより障害が発生した場合。ルータは、RBCP ハートビートの損失を通じて、これを検出できます。
- **reload** または **shutdown** コマンド。

詳細情報

- SensorApp の詳細については、「SensorApp」（P.A-25）を参照してください。
- ソフトウェア バイパスの詳細については、「インライン バイパス モードの設定」（P.6-38）を参照してください。

NME IPS のリブート、リセット、およびシャットダウン

NME IPS のリブート、リセット、およびシャットダウンを行うには、特権 EXEC モードで、**service-module ids-sensor** *slot/port* [**reload | reset | shutdown**] コマンドを使用します。

NME IPS のリブート、リセット、およびシャットダウンを行うには、次の手順に従います。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　NME IPS でオペレーティング システムを正常に停止し、リブートするには、次のコマンドを実行します。

```
router# service-module ids-sensor 1/0 reload
Do you want to proceed with the reload?[confirm]
```

ステップ 4　NME IPS でハードウェアをリセットするには、次のコマンドを実行します。

```
router# service-module ids-sensor 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
```

（注）　NME IPS には、永続的なストレージ デバイスとして機能するコンパクト フラッシュ デバイスが搭載されています（ハードディスク ドライブではありません）。

注意　データが失われるのは、NME IPS をシャットダウンせずに **reset** コマンドを実行した場合だけです。それ以外の状況では、安全に **reset** コマンドを使用できます。

ステップ 5　NME IPS で実行中のアプリケーションをシャットダウンするには、次のコマンドを実行します。

```
router# service-module ids-sensor 1/0 shutdown
Trying 10.10.10.1, 2129 ...Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor1/0 shutdown complete
```

新しいコマンドと変更されたコマンド

（注）　その他の Cisco IOS ソフトウェア コマンドについては、Cisco.com（http://www.cisco.com/en/US/products/ps6441/index.html）の『*Cisco IOS Release 12.4(20)T Command Reference*』を参照してください。

ここでは、次の Cisco IOS の新しいコマンドと変更されたコマンド、および NME IPS を設定するために使用する特定のコマンドについて説明します。次の項目について説明します。

interface ids-sensor

IPS センサー インターフェイスを設定し、config-if モードを開始するには、config モードで **interface ids-sensor** コマンドを使用します。モジュールの障害時にルータでトラフィック検査を処理する方法を指定するには、config-if モードで **service-module** コマンドを使用します。デフォルトはフェール オープンです。

interface ids-sensor *slot/port*

ip {address | unnumbered}

service-module {*fail-close* | *fail-open*}

構文の説明

slot	NME IPS のルータ シャーシ スロットの数。
/port	NME IPS のポート番号。 （注）　*slot* 引数と *unit* 引数の間には、スラッシュ記号が必要です。
ids-sensor	センサーの IPS インターフェイス。
ip address	インターフェイスの IP アドレスを設定します。
ip unnumbered	明示的な IP アドレスなしで、IP アドレス処理をイネーブルにします。
service-module fail-close	NME IPS は、すべてのトラフィックをドロップします。
service-module fail-open	NME IPS は、すべてのトラフィックを通過させますが、トラフィック検査は実行しません（デフォルト）。

注意　**ip** コマンドに関連付けられている 57 のサブコマンドがありますが、このモジュールに対してサポートされているサブコマンドは、**ip address** と ip **unnumbered** の 2 つだけです。その他のサブコマンドのいずれかをイネーブルにすると、予期せぬ動作が発生することがあります。

デフォルト

デフォルトは**フェールオープン**です。

コマンド モード

Config

Config-if

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが追加されました。

使用上のガイドライン

interface ids-sensor *slot/port* コマンドでは、config-if モードを開始し、IPS センサー スロットおよびポートを設定できます。NME IPS で、スロットの値は、ルータでモジュールが取り付けられている物理的な場所を判定することによって指定され、ポート番号は 0 です。

例

次の例は、**interface IDS-Sensor** コマンドを使用して、スロット 1、ポート 0 で、NME IPS の config-if モードを開始する方法を示しています。

```
router(config)# interface ids-sensor 1/0
router(config-if)#
```

次の例は、**ip unnumbered** サブコマンドとともに **interface ids-sensor** コマンドを使用して、ルータ コマンドおよび制御インターフェイスを指定する方法を示しています。

```
router(config)# interface ids-sensor 1/0
router(config-if)# ip unnumbered router_command_and_control_interface
router(config-if)#
```

次の例は、ハードウェアの障害時に、すべてのトラフィックはモジュールを通過するが、トラフィック検査は実行しないように、**service-module fail-open** コマンドを使用して NME IPS を設定する方法を示しています。

```
router(config)# interface ids-sensor 1/0
router(config-if)# service-module fail-open
router(config-if)#
```

関連コマンド

コマンド	説明
interface *interface_name*	モニタする必要があるインターフェイスを指定します。

interface *interface_name*

config-if モードを開始するには、無差別モードまたはインライン モードでモニタリング用にインターフェイスを設定し、インライン モニタリングに標準 ACL または拡張 ACL を適用し、config モードで **interface** *interface_name* コマンドを使用します。

interface *interface_name*

ids-service-module monitoring {**promiscuous** | **inline**} **access-list** *number*

構文の説明

interface_name	モニタされるルータ インターフェイスの名前。
ids-service-module	インターフェイスに IPS を設定します。

monitoring	NME IPS がトラフィックを検査する方法を指定します。
promiscuous	NME IPS が、無差別モードでトラフィックを検査するかどうかを指定します。
inline	NME IPS が、インライン モードでトラフィックを検査するかどうかを指定します。
access-list	検査するインターフェイスに、番号付き ACL または拡張 ACL を適用していることを指定します。
number	ACL の番号。

デフォルト

なし

コマンド モード

Config

Config-if

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが追加されました。

使用上のガイドライン

interface *interface_name* コマンドでは、config-if モードを開始し、インターフェイスに対してインライン モードまたは無差別モードで動作するようにルータを設定できます。

例

次の例は、**interface** コマンドを使用して config-if モードを開始し、ACL 101 を使用して GigabitEthernet0/0 のモニタリングを設定する方法を示しています。

```
router(config)# interface GigabitEthernet0/0
router(config-if)# ids-service-module monitoring inline access-list 101
router(config-if)#
```

関連コマンド

コマンド	説明
interface ids-sensor	IPS インターフェイスを設定します。

service-module ids-sensor

注意　ルータをリロードしたときに、NME IPS もリロードされます。NME IPS でデータの損失が生じないようにするには、**reload** コマンドを使用してルータをリブートする前に、**shutdown** コマンドを使用してモジュールを必ずシャットダウンしてください。

ハートビートが失われたときに、Cisco IOS software が NME IPS をリブートすることを防ぎ、モジュールに対してリブート、リセット、コンソール アクセスのイネーブル化、シャットダウン、統計情報の表示、ステータスのモニタを実行するには、特権 EXEC モードで **service-module ids-sensor** コマンドを使用します。

service-module ids-sensor *slot*/*port* {**heartbeat-reset** {**enable** | **disable**} **reload** | **reset** | **session** | **shutdown** | **status**}

構文の説明

slot	NME IPS のルータ シャーシ スロットの数。
/*port*	NME IPS のポート番号。 **（注）** *slot* 引数と *unit* 引数の間には、スラッシュ記号が必要です。
heartbeat-reset	ハートビート リセットをイネーブルまたはディセーブルにします。デフォルトではイネーブルになっています。 **（注）** ハートビート リセットをディセーブルにすると、システム イメージのインストール中に（このプロセスに非常に長い時間がかかる場合）、ルータによる NME IPS のリセットが防止されます。
reload	NME IPS のオペレーティング システムをスムーズに停止し、リブートします。
reset	NME IPS のハードウェアをリセットします。通常、このコマンドはシャットダウンから復旧するために使用します。
session	ルータからモジュールへのコンソール アクセスをイネーブルにします。
shutdown	NME IPS で実行中の IPS アプリケーションをシャットダウンします。
statistics	モジュールの統計情報を提供します。
status	IPS ソフトウェアのステータスに関する情報を提供します。

デフォルト

デフォルトは、**heartbeat enabled** です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが追加されました。

使用上のガイドライン

NME IPS がフェールセーフ モードでブートされるか、アップグレード中の場合、**service-module ids heartbeat-reset** コマンドを使用するとプロセス中のリブートを防止できます。アップグレード中にハートビート リセットをイネーブルのままにした場合、NME IPS ハートビートが失われることがあります。

NME IPS ハートビートが失われた場合、ルータは、NME IPS に fail-open または fail-close の設定オプションを適用し、NME IPS へのトラフィックの送信を停止し、NME IPS をエラー状態に設定します。ルータは、NME IPS でハードウェア リセットを実行し、ハートビートが再確立されるまで NME IPS をモニタします。

確認プロンプトが表示されたら、Enter を押してアクションを確認するか、n キーを押してキャンセルします。

例

次の例は、スロット 1、ポート 0 で、NME IPS のハートビートが失われた場合に、リセット アクションをディセーブルまたはイネーブルにする方法を示しています。

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```

次の例は、NME IPS で IDS ハートビートをイネーブルにする方法を示しています。

```
router# service-module ids-sensor 1/0 heartbeat-reset enable
```

次の例は、**service-module ids** *slot*/*port* **status** コマンドを使用して、ハートビート リセットのステータスを表示する方法を示しています。

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled
```

次の例は、NME IPS でオペレーティング システムをスムーズに停止し、リブートする方法を示しています。

```
router# service-module ids-sensor 1/0 reload

Do you want to proceed with reload?[confirm]
```

次の例は、NME IPS でハードウェアをリセットする方法を示しています。警告が表示されます。

```
router# service-module ids-sensor 1/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose data on the NVRAM, nonvolatile file system or unsaved configuration!

Do you want to reset?[confirm]
```

次の例では、NME IPS オペレーティング システムへのコンソール アクセスがイネーブルになります。

```
router# service-module ids-sensor 1/0 session
```

次の例は、NME IPS で実行中の IPS アプリケーションをシャットダウンする方法を示しています。

```
router# service-module ids-sensor 1/0 shutdown

Trying 10.10.10.1, 2129 ... Open
%SERVICEMODULE-5-SHUTDOWN2:Service module IDS-Sensor 1/0 shutdown complete
```

次の例は、IPS ソフトウェア統計情報を表示する方法を示しています。

```
router# service-module ids-sensor 1/0 statistics
Module Reset Statistics:
CLI reset count = 1
  CLI reload count = 0
  Registration request timeout reset count = 1
  Error recovery timeout reset count = 1
  Module registration count = 7

The last IOS initiated event was a cli reset at 20:18:36.038 UTC Tue Jan 16 2007
```

次の例は、NME IPS の IPS ソフトウェアのステータスを表示する方法を示しています。

```
router# service-module ids-sensor 1/0 status
```

```
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait...
Service Module Version information received, Major ver = 1, Minor ver= 1

Cisco Systems Intrusion Prevention System Network Module
  Software version:  7.0(4)E4
  Model:             NME IPS
  Memory:            890996 KB
  Mgmt IP addr:      10.1.9.201
  Mgmt web ports:    443
  Mgmt TLS enabled:  true
```

関連コマンド

コマンド	説明
ids-service-module monitoring	特定のインターフェイスで IPS モニタリングをイネーブルにします。

service-module ids-sensor bootmode

NME IPS でフェールセーフ モードまたは通常ブート モードを開始するには、特権 EXEC モードで **service-module ids-sensor bootmode** コマンドを使用します。

service-module ids-sensor *slot*/*port* **bootmode** {**failsafe** | **normal**}

構文の説明

slot/	NME IPS のルータ シャーシ スロットの数。*slot* 引数と *port* 引数の間には、スラッシュ記号（/）が必要です。
port	NME IPS のポート番号。
failsafe	NME IPS でフェールセーフ ブート モードを開始します。
normal	NME IPS で通常ブート モードを開始します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

確認プロンプトが表示されたら、Enter を押してアクションを確認するか、n キーを押してキャンセルします。

例

次の例は、スロット 1、ポート 0 で、NME IPS のフェールセーフ ブート モードを開始する方法を示しています。

```
router# service-module ids-sensor 1/0 bootmode failsafe
```

次の例は、NME IPS で通常ブート モードをイネーブルにする方法を示しています。

```
router# service-module ids-sensor 1/0 bootmode normal
```

関連コマンド

コマンド	説明
ids-service-module monitoring	特定のインターフェイスで IDS モニタリングをイネーブルにします。