CHAPTER 16

NM-CIDS の設定

この章では、NM-CIDS をセットアップして、トラフィックの受信を準備するために実行する必要のあるタスクについて説明します。これを行うと、侵入検出を設定できるようになります。

（注） NM-CIDS はインライン モードでは動作せず、混合モードでのみ動作します。したがって、侵入防御は設定できません。

この章は、次の項で構成されています。

コンフィギュレーション シーケンス

NM-CIDS を設定するには、次のタスクを実行します。

1. ルータに IDS インターフェイスを設定します。

   手順については、P.16-3 の「IDS センサー インターフェイスのルータへの設定」を参照してください。

2. NM-CIDS にログインします。

   手順については、P.16-5 の「NM-CIDS セッションの確立」を参照してください。

3. NM-CIDS を初期化します。

   setup コマンドを実行して NM-CIDS を初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

4. トラフィックを取り込んで侵入検出分析を行うように NM-CIDS を設定します。

   手順については、P.16-7 の「パケット キャプチャの設定」を参照してください。

5. サービス アカウントを作成します。

   手順については、P.4-16 の「サービス アカウントの作成」を参照してください。

6. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

7. 侵入検出を設定します。

   手順については、第 6 章「イベント アクション ルールの設定」、第 7 章「シグニチャの定義」、および第 10 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

8. 管理タスクを実行して NM-CIDS が円滑に動作し続けるようにします。

   手順については、第 13 章「センサーの管理タスク」および第 16 章「管理タスク」を参照してください。

9. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

   詳細については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

10. 必要に応じて、ブート ヘルパーとブート ローダーのイメージを再作成します。

    手順については、P.17-23 の「NM-CIDS システム イメージのインストール」を参照してください。

IDS センサー インターフェイスのルータへの設定

NM-CIDS には外部コンソール ポートはありません。NM-CIDS へのコンソール アクセスは、ルータで **service-module ids-module** *slot_number*/**0 session** コマンドを発行した場合、または NM-CIDS スロットに対応するポート番号でルータへの Telnet 接続を開始した場合にイネーブルになります。外部コンソール ポートがないことは、初期ブートアップ コンフィギュレーションはルータ経由でのみ可能であることを意味します。

service-module ids-sensor *slot_number*/**0 session** コマンドを発行する場合は、NM-CIDS とのコンソール セッションを作成します。NM-CIDS で、どのような IPS コンフィギュレーション コマンドでも発行できます。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 コマンドは、IDS センサー インターフェイスの IP アドレスを使用して、逆 Telnet 接続を開始します。IDS センサー インターフェイスは、NM-CIDS 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には、事前に IDS センサー インターフェイスに IP アドレスを割り当てておく必要があります。ルーティング可能な IP アドレスを割り当てると、ID センサー インターフェイス自体が攻撃に対して脆弱になります。この脆弱性に対処するために、ループバック IP アドレスを IDS センサー インターフェイスに割り当てます。

NM-CIDS インターフェイスを設定するには、次の手順を実行します。

ステップ 1　NM-CIDS スロット番号をルータに設定します。

```
router # show interfaces ids-sensor slot_number/0
```

（注） **show run** コマンドを使用することもできます。「IDS-Sensor」とスロット番号を検索します。

（注） Cisco IOS では、NM-CIDS に「IDS-Sensor」という名前が付けられています。この例では、スロット番号は 1 で、ポートは 1 つしかないので、ポート番号は 0 です。

ステップ 2　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)# exit
```

ステップ 3　ループバック インターフェイスを作成します。

```
router# configure terminal
router(config)# interface loopback 0
```

ステップ 4　IP アドレスとネットマスクをループバック インターフェイスに割り当てます。

```
router(config-if)# ip address 10.16.0.0 255.255.0.0
```

（注）　NM-CIDS の内部インターフェイスに IP アドレスを割り当てて、NM-CIDS に対してセッションを開始する必要があります。ルータにある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ます。このアドレスは NM-CIDS へのアクセスに使用しないので、実 IP アドレスである必要はありません。

ステップ 5　番号未指定のループバック インターフェイスを IDS センサー 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
```

ステップ 6　ポートをアクティブにします。

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

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)# end
```

ステップ 8　コンフィギュレーションを NVRAM に書き込みます。

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

NM-CIDS セッションの確立

この項では、ルータと NM-CID 間にセッションを確立する方法について説明します。取り上げる事項は次のとおりです。

NM-CIDS に対するセッションの開始

ルータから NM-CIDS へのセッションを確立するには、**session** コマンドを使用します。**Ctrl+Shift+6** キーを押し、その後 **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。つまり、NM-CIDS 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** キーを押して、セッション プロンプト、つまり NM-CIDS プロンプトに戻ります。ルータ コマンドを実行後、セッションに戻る場合は、NM-CIDS へのセッションを中断するだけにします。NM-CIDS セッションに戻る予定がない場合は、セッションを中断するのではなく、セッションを閉じます。

セッションを閉じると、NM-CIDS CLI から完全にログアウトされて、新規セッションを接続するには、ログインするためにユーザ名とパスワードが必要です。セッションの中断では、CLI にログインした状態のままになっています。**session** コマンドで接続すると、同じ CLI に戻ることができ、ユーザ名もパスワードも指定する必要はありません。

（注） Telnet クライアントはさまざまです。場合によっては、**Ctrl+6+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 1E）として指定されます。

注意 **disconnect** コマンドを使用してセッションをそのままにしておくと、セッションは動作状態のままです。開いているセッションは、まだ動作中の接続を利用しようと考える人物によって、不正利用される可能性があります。

NM-CIDS へのセッションをオープンおよびクローズするには、次の手順を実行します。

ステップ 1　ルータから NM-CIDS へのセッションを開きます。

```
router# service-module ids-sensor 1/0 session
Trying 10.16.0.0, 2033 ... Open
```

ステップ 2　**Ctrl+Shift+6** キーを押し、その後 **x** キーを押して、ルータ プロンプトに戻って、NM-CIDS セッションを中断します。

ステップ 3　空白行で **Enter** キーを押して、NM-CIDS プロンプトに戻ります。

ステップ 4　NM-CIDS セッションを終了します。

```
nm-cids# exit
```

（注）　IPS CLI のサブモードにいる場合は、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 ログイン プロンプトが表示されるまで、**exit** を入力します。

セッションを適切に閉じることができないと、まだ動作中の接続が他人に不正利用される可能性があります。Router# プロンプトで必ず **exit** と入力して、Cisco IOS セッションを完全に閉じてください。

ステップ 5　NM-CIDS へのセッションを中断して閉じるには、**Ctrl+Shift** キーを押した状態で **6** キーを押します。すべてのキーを放してから、**x** キーを押します。

（注）　セッションを終了したら、ルータに戻って、セッション（IPS アプリケーション）と監視するルータ インターフェイスとの間の関連付けを確立する必要があります。

ステップ 6　ルータから切断します。

```
router# disconnect
```

ステップ 7　**Enter** キーを押して切断を確認します。

```
router# Closing connection to 10.16.0.0 [confirm] <Enter>
```

NM-CIDS への Telnet 接続

NM-CIDS スロットに対応するポート番号で、直接ルータに Telnet で接続することもできます。P.16-3 の「IDS センサー インターフェイスのルータへの設定」でループバック 0 インターフェイスを設定するときに割り当てたアドレスを使用します。

ポート番号は、「2001 + 32 × スロット番号」という式で決定されます。

たとえば、スロット 1 の場合、ポート番号は 2033、スロット 2 の場合は 2065、などとなります。

Telnet を使用してポート 2033 へのセッションを起動するには、次のように入力します。

```
router# telnet 10.16.0.0 2033
```

パケット キャプチャの設定

パケット モニタリングには、ルータ上で目的のインターフェイス（サブインターフェイスを含む）をイネーブルにする必要があります。監視対象のインターフェイスまたはサブインターフェイスは必要な数だけ選択できます。これらのインターフェイスで送信されるパケットおよび受信されるパケットは、検査のために NM-CIDS に転送されます。インターフェイスは、ルータ CLI（Cisco IOS）を使用してイネーブルまたはディセーブルにします。

（注）　ルータで暗号化を行っている場合、NM-CIDS は、ルータに着信するパケットは復号化後、およびルータから発信するパケットは暗号化前に、受信します。

NM-CIDS にパケット キャプチャを設定するには、次の手順を実行します。

ステップ 1　ルータ コンソールにログインします。

ステップ 2　インターフェイス コンフィギュレーションを表示します。

```
router# show run
```

ステップ 3　監視するインターフェイスまたはサブインターフェイス（たとえば、FastEthernet0/0）を確認します。

（注）　監視するインターフェイスまたはサブインターフェイスは複数選択できますが、一度に編集できるインターフェイスは 1 つだけです。

ステップ 4　グローバル コンフィギュレーション モードに入ります。

```
router# configure terminal
```

ステップ 5　インターフェイスまたはサブインターフェイスを指定します。

```
router(config)# interface FastEthernet0/0
```

（注）　トラフィックは、ルータの 1 つのインターフェイスから着信します。

ステップ 6　ネットワーク トラフィックを NM-CIDS にコピーするようにインターフェイスを設定します。

```
router(config-if)# ids-service-module monitoring
```

（注）　モニタリングを停止するには、**no ids-service-module monitoring** コマンドを使用します。

ステップ 7　インターフェイス モードを終了します。

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

ステップ 8　監視するインターフェイスまたはサブインターフェイスそれぞれに対して、ステップ 3 ～ 6 を繰り返します。

ステップ 9　グローバル コンフィギュレーション モードを終了します。

```
router(config)# exit
```

ステップ 10　NM-CIDS がネットワーク トラフィックを分析していることを確認します。

a. NM-CIDS 上の外部インターフェイスに対して Telnet セッションまたは SSH セッションを開きます。

（注）　SSH には、許可されたホストが必要です。手順については、P.4-36 の「既知のホストリストへのホストの追加」を参照してください。

b. NM-CIDS にログインします。

c. インターフェイス統計情報を表示して、モニタリング インターフェイスが動作していることを確認します。

```
nm-cids# show interface clear
nm-cids# show interface
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 23
   Total Bytes Received = 1721
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 2
   Total Bytes Transmitted = 120
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
```

d. ステップ c を繰り返して、カウンタが徐々に増加していることを確認します。増加していることは、NM-CIDS がネットワーク トラフィックを受信していることを示します。

カウンタが増加しない場合は、ステップ 3 ～ 6 を適切に実行し、**setup** コマンドで NM-CIDS を初期化したときに、FastEthernet0/0 が仮想センサーに追加されていることを確認します。

管理タスク

この項では、NM-CIDS のリブート方法および Cisco IPS ソフトウェアのステータスの確認方法について説明します。

この項では、次のトピックについて説明します。

NM-CIDS のシャットダウン、リロード、およびリセット

Cisco IOS には、NM-CIDS を制御する **shutdown** コマンド、**reload** コマンド、および **reset** コマンドが用意されています。

- **shutdown**：オペレーティング システムを適切に終了させます。

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

注意　ルータから NM-CIDS を取り外す前に、必ず **shutdown** コマンドを実行してください。**shutdown** コマンドを実行せずに NM-CIDS を取り外すと、データの消失、またはハードディスク ドライブの破損を招く可能性があります。

- **reload**：NM-CIDS 上のオペレーティング システムを適切に停止してリブートします。

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

- **reset**：NM-CIDS 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回復するために使用されます。

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

次の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 hard disc!
Do you want to reset?[confirm]
```

注意　ハードディスク ドライブのデータが失われるのは、最初に NM-CIDS をシャットダウンせずに **reset** コマンドを発行した場合だけです。NM-CIDS がまだ正常に動作している場合は、**reset** コマンドでなく、**reload** コマンドを使用します。その他の状況の場合は、**reset** コマンドを使用しても安全です。

Cisco IPS ソフトウェアのステータスの確認

ルータで動作している Cisco IPS のステータスを確認するには、**status** コマンドを使用します。

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

表示される出力の例を次に示します。

```
Router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 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 Detection System Network Module
Software version: 5.0(1)S42
Model: NM-CIDS
Memory: 254676 KB
Mgmt IP addr:     xx.xx.xx.xx
Mgmt web ports:    443
Mgmt TLS enabled: true
```

サポートされている Cisco IOS コマンド

service-module ids-sensor *slot_number*/**0** Cisco IOS コマンドが新しく NM-CIDS をサポートするようになりました。スロット番号は異なることがありますが、ポートは常に 0 です。

次のオプションが適用されます。

- 特権モード EXEC
  - **service-module ids-sensor** *slot_number*/**0 reload**

    オペレーティング システムを NM-CIDS にリロードします。
  - **service-module ids-sensor** *slot_number*/**0 reset**

    NM-CIDS に対してハードウェア リセットを行います。
  - **service-module ids-sensor** *slot_number*/**0 session**

    session コマンドを使用して、IPS コンソールにアクセスできるようになります。
  - **service-module ids-sensor** *slot_number*/**0 shutdown**

    NM-CIDS で動作している IPS アプリケーションをシャットダウンします。

注意　シャットダウンを正常に行わずに NM-CIDS を取り外すと、ハードディスク ドライブの破損を招く可能性があります。NM-CIDS アプリケーションが正常にシャットダウンされると、NM-CIDS の取り外しが可能になったことを示すメッセージが Cisco IOS によって表示されます。

  - **service-module ids-sensor** *slot_number*/**0 status**

    Cisco 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。
- インターフェイス モードの設定 (config-if)
  - **ids-service-module monitoring**

    指定したインターフェイス（またはサブインターフェイス）上で IPS モニタリングをイネーブルにできます。指定したインターフェイス上の着信パケットと発信パケットの両方が、モニタリングのために転送されます。