CHAPTER 15

SNMP の設定

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在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、SNMP を設定す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。

注意 センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして **request-snmp-trap** も選択する必要があります。

SNMP について

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

SNMP は、簡易な要求および応答プロトコルです。ネットワーク管理システムが要求を発行し、管理対象デバイスが応答を返します。この動作は、4 つのプロトコル動作、Get、GetNext、Set、および Trap の 1 つを使用することにより実現されます。

SNMP によるモニタ用にセンサーを設定できます。SNMP は、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。

SNMP トラップを送信するようにセンサーを設定できます。SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

トラップで指示される通知には次の利点があります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。イベントのトラップと呼ばれるメッセージを送信することで、この処理を行います。

イベントの受信後、マネージャはイベントを表示し、イベントに基づいてアクションを実行できます。たとえば、マネージャは、エージェントを直接ポーリングするか、他の関連デバイス エージェントをポーリングしてイベントについて理解を深められます。

（注） トラップで指示される通知は、重要でない SNMP 要求を除外することによって、ネットワーク リソースおよびエージェント リソースの大幅な節約をもたらします。ただし、SNMP ポーリングを完全には排除できません。SNMP 要求は、検出とトポロジ変更に必要です。また、管理対象デバイス エージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

SNMP の設定

注意 センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして **request-snmp-trap** も選択する必要があります。

サービス通知サブモードで一般的な SNMP パラメータを設定します。

オプション

次のオプションが適用されます。

- **default**：値をシステムのデフォルト設定に戻します。
- **enable-set-get {true | false}**：オブジェクト ID（OID）の **get** および **set** をイネーブルにします。
- **no**：エントリまたは選択の設定を削除します。
- **read-only-community**：SNMP エージェントに読み取り専用のコミュニティ名を指定します。デフォルトは public です。
- **read-write-community**：SNMP エージェントに読み書き可能なコミュニティ名を指定します。デフォルトは private です。
- **snmp-agent-port**：SNMP エージェントがリッスンするポートを指定します。デフォルトの SNMP ポート番号は 161 です。
- **snmp-agent-protocol**：SNMP エージェントが通信に使用するプロトコルを指定します。デフォルト プロトコルは UDP です。
- **system-contact**：このセンサーの連絡先情報を指定します。system-contact オプションは、SNMPv2-MIB::sysContact.0 値を変更します。
- **system-location**：センサーの場所を指定します。system-location オプションは、SNMPv2-MIB::sysLocation.0 値を変更します。

SNMP の一般的なパラメータの設定

SNMP の一般的なパラメータを設定するには、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 CLI にログインします。

ステップ 2　通知サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service notification
ips-ssp(config-not)#
```

ステップ 3　SNMP 管理ワークステーションがセンサー SNMP エージェントに要求を発行できるように、SNMP をイネーブルにします。

```
ips-ssp(config-not)# enable-set-get true
```

ステップ 4　SNMP エージェントパラメータを指定します。これらの値はセンサー SNMP エージェントのコミュニティ名を設定します。コミュニティ名は、SNMP 照会の強力でない認証に使用されるプレーン テキストのパスワード メカニズムです。

a. 読み取り専用のコミュニティ ストリングを割り当てます。読み取り専用のコミュニティ名には、SNMP エージェントに対する照会用のパスワードを指定します。

```
ips-ssp(config-not)# read-only-community PUBLIC1
```

b. 読み書き可能なコミュニティ ストリングを割り当てます。読み書き可能なコミュニティ名には、SNMP エージェントに対する **set** 用のパスワードを指定します。

```
ips-ssp(config-not)# read-write-community PRIVATE1
```

（注）　管理ワークステーションは、センサーにある、センサー SNMP エージェントに対して SNMP 要求を送信します。管理ワークステーションが要求を発行して、コミュニティ ストリングがセンサーのものと一致しない場合、センサーは要求を拒否します。

c. センサーの連絡先ユーザ ID を割り当てます。

```
ips-ssp(config-not)# system-contact BUSINESS
```

d. センサーの場所を入力します。

```
ips-ssp(config-not)# system-location AUSTIN
```

e. センサー SNMP エージェントのポートを入力します。

```
ips-ssp(config-not)# snmp-agent-port 161
```

（注）　ポートまたはプロトコルを変更する場合は、センサーをリブートする必要があります。

f. センサー SNMP エージェントが使用するプロトコルを指定します。

```
ips-ssp(config-not)# snmp-agent-protocol udp
```

（注）　ポートまたはプロトコルを変更する場合は、センサーをリブートする必要があります。

ステップ 5　設定を確認できます。

```
ips-ssp(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   error-filter: error|fatal <defaulted>
   enable-detail-traps: false <defaulted>
   enable-notifications: false <defaulted>
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: public <defaulted>
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
ips-ssp(config-not)#
```

ステップ 6　通知サブモードを終了します。

```
ips-ssp(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

アクションをシグニチャに割り当てる手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。

SNMP トラップの設定

注意　センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして **request-snmp-trap** も選択する必要があります。

サービス通知サブモードで SNMP トラップを設定します。

オプション

次のオプションが適用されます。

- **enable-detail-traps {true | false}**：サイズの制限がない詳細トラップの送信をイネーブルにします。他のトラップはスパース モード（484 バイト未満）で送信されます。
- **enable-notifications {true | false}**：イベント通知をイネーブルにします。
- **error-filter {warning | error | fatal}**：SNMP トラップを生成するエラーを決定します。SNMP トラップは、フィルタに一致するすべての evError イベントについて生成されます。デフォルトはエラーおよび重大です。
- **trap-community-name**：トラップの宛先を定義する際に名前を指定しない場合は、トラップを送信する際に使用されるコミュニティ名を指定します。

- **trap-destinations**：シグニチャ アクションから生成されたエラー イベントおよびアラート イベントを送信する宛先を定義します。
  - **trap-community-name**：トラップを送信する際に使用されるコミュニティ名を指定します。コミュニティ名を指定しない場合は、一般トラップのコミュニティ名が使用されます。
  - **trap-port**：SNMP トラップを送信するポート番号を指定します。

SNMP トラップの設定

SNMP トラップを設定するには、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 CLI にログインします。

ステップ 2　通知サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service notification
ips-ssp(config-not)#
```

ステップ 3　SNMP トラップをイネーブルにします。

```
ips-ssp(config-not)# enable-notifications true
```

ステップ 4　SNMP トラップ用に次のパラメータを指定します。

a. SNMP トラップを介して通知するエラー イベントを指定します。

```
ips-ssp(config-not)# error-filter {error | warning | fatal}
```

（注） **error-filter [error | warning | fatal]** コマンドには、エラー、警告、および重大トラップが含まれます。このコマンドは重大度に基づいてトラップをフィルタ処理します（除去しません）。

b. 詳細 SNMP トラップが必要かどうかを指定します。

```
ips-ssp(config-not)# enable-detail-traps true
```

c. 詳細トラップに含めるコミュニティ ストリングを入力します。

```
ips-ssp(config-not)# trap-community-name TRAP1
```

ステップ 5　センサーがこれらのトラップを送信する管理ワークステーションを認識するように、SNMP トラップ宛先のパラメータを指定します。

a. SNMP 管理ステーションの IP アドレスを入力します。

```
ips-ssp(config-not)# trap-destinations 10.0.0.0
```

b. SNMP 管理ステーションの UDP ポートを入力します。デフォルトは 162 です。

```
ips-ssp(config-not-tra)# trap-port 162
```

c. トラップ コミュニティ ストリングを入力します。

```
ips-ssp(config-not-tra)# trap-community-name AUSTIN_PUBLI
```

（注） コミュニティ ストリングはトラップに含まれていて、複数のエージェントから複数のトラップ タイプを受信する場合に役立ちます。たとえば、ルータまたはセンサーはトラップを送信できるので、コミュニティ ストリング内にルータまたはセンサーを特別に識別するものを入れておくと、コミュニティ ストリングに基づいてトラップをフィルタ処理できます。

ステップ 6　設定を確認できます。

```
ips-ssp(config-not-tra)# exit
ips-ssp(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 1)
   -----------------------------------------------
      ip-address: 10.1.1.1
      -----------------------------------------------
         trap-community-name: AUSTIN_PUBLIC default:
         trap-port: 161 default: 162
      -----------------------------------------------
   -----------------------------------------------
   error-filter: warning|error|fatal default: error|fatal
   enable-detail-traps: true default: false
   enable-notifications: true default: false
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: PUBLIC1 default: public
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
ips-ssp(config-not)#
```

ステップ 7　通知サブモードを終了します。

```
ips-ssp(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

アクションをシグニチャに割り当てる手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。

サポート対象 MIB

センサーでは、次のプライベート MIB がサポートされています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

（注） MIB II はセンサーで使用できますが、シスコではサポートしていません。一部の要素が正確でないことがわかっています（たとえば、センシング インターフェイスの IF MIB からのパケット カウントなど）。MIB II の要素を使用できますが、シスコでは、それらがすべて正確な情報を提供することを保証していません。シスコは、リストにあるその他の MIB を完全サポートしていますし、それらの出力も正確です。

これらのプライベートの Cisco MIB は、次の URL の [SNMP v2 MIBs] という見出しの下で確認できます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml