CHAPTER 25

ファイアウォール サービス モジュールのモニタリング

この章では、Firewall Services Module（FWSM; ファイアウォール サービス モジュール）のためのロギングと Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の設定方法について説明します。Syslog メッセージの内容および Syslog メッセージのフォーマットについても説明します。

この章では、モニタリング、ロギング、および SNMP のコマンドやオプションについて包括的な説明は行いません。詳しい説明とその他のコマンドについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

この章では、次の内容について説明します。

Syslog メッセージの設定および管理

ここでは、ロギングの機能と設定について説明します。Syslog メッセージのフォーマット、オプション、変数についても説明します。ここでは、次の内容について説明します。

ロギングの概要

FWSM では、Syslog メッセージの監査証跡（許可および拒否されているネットワーク トラフィックの種類などのアクティビティを示す）の生成がサポートされており、システム ロギングを設定することもできます。

すべての Syslog メッセージには、デフォルトの重大度があります。必要に応じて、メッセージを新しい重大度に再割り当てすることができます。重大度を選択すると、そのレベルおよびより低いレベルのロギング メッセージが生成されます。より高いレベルのメッセージは生成されません。重大度が高く

なるほど、生成されるメッセージが増えます。ロギングおよび Syslog メッセージの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Log Messages*』を参照してください。

FWSM Syslog メッセージでは、FWSM のモニタリングやトラブルシューティングのための情報を得ることができます。ロギング機能を使用すると、次のことができます。

- ログに記録する Syslog メッセージの指定
- Syslog メッセージの重大度のディセーブル化または変更
- Syslog メッセージの重大度を色別で指定
- Syslog メッセージの簡単な説明をヒントとして表示
- Syslog メッセージの説明および推奨処置の指定
- Syslog メッセージの 1 つまたは複数の送信先の指定。これには、内部バッファ、1 台または複数台の Syslog サーバ、SNMP 管理ステーション、指定した電子メール アドレス、Telnet セッションや SSH セッションなどが含まれます。
- 重大度やメッセージ クラスなどによる、グループ内での Syslog メッセージの設定と管理
- バッファがいっぱいになった場合の、内部バッファの内容に対する処理方法の指定。バッファの上書き、FTP サーバへのバッファの内容の送信、内部フラッシュ メモリへの内容の保存などがあります。
- Syslog メッセージ全体、または Syslog メッセージのサブセットを、任意の出力先またはすべての出力先に送信。
- Syslog メッセージの重大度、Syslog メッセージのクラスに応じて、またはカスタム ログ メッセージ リストを作成することにより、どの場所にどの Syslog メッセージを送信するかをフィルタリング。

セキュリティ コンテキストおよびロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システムまたは管理コンテキストにログインし、それから別のコンテキストを変更する場合、セッション中に表示されるメッセージは現在のコンテキストに関連したメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの Syslog メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

FWSM は、それぞれのメッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の Syslog サーバに送信されるコンテキスト メッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。ロギング装置 ID のイネーブル化の詳細については、「Syslog メッセージへの装置 ID の記載」（P.25-16）を参照してください。

ロギングのイネーブル化およびディセーブル化

ここでは、FWSM でロギングをイネーブル化/ディセーブル化する方法について説明します。内容は次のとおりです。

設定された全出力先へのロギングのイネーブル化

次のコマンドによりロギングをイネーブルにできますが、ロギングされたメッセージを表示したり保存したりできるように、少なくとも 1 つの出力先を指定する必要もあります。出力先を指定していない場合、FWSM はイベント発生時に生成される Syslog メッセージを保存しません。

ログ出力先の設定の詳細については、「ログの出力先の設定」（P.25-4）を参照してください。

ロギングをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# logging enable
```

設定された全出力先へのロギングのディセーブル化

設定された全出力先へのロギングをディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# no logging enable
```

ログ設定の表示

実行中のログ設定を表示するには、次のコマンドを入力します。

```
hostname(config)# show logging
```

次に、**show logging** コマンドの出力例を示します。

```
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

ホストまたはネットワークのマッピング名の出力

Syslog メッセージでのホストまたはネットワークのマッピング名の出力をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# logging names
```

Syslog メッセージにホストまたはネットワークのマッピング名ではなく、IP アドレスを出力するには、次のコマンドを入力します。

```
hostname(config)# no logging names
```

次に、ホストまたはネットワークの IP アドレスのマッピング名を含む Syslog メッセージの例を示します。

```
hostname(config)# no logging names
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Name logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

次に、**logging names** コマンドが使用されたときに生成される Syslog メッセージの例を示します。

```
%FWSM-6-302013: Built outbound TCP connection 144547141745774540 for inside:client/42934
(client/42934) to outside:server/11223 (server/80)
```

次に、**no logging names** コマンドが使用されたときに生成される Syslog メッセージの例を示します。

```
%FWSM-6-302013: Built outbound TCP connection 144547141745774540 for
inside:172.149.1.1/42934 (172.149.1.1/42934) to outside:172.109.1.1/11223 (172.109.1.1/80)
```

ログの出力先の設定

ここでは、FWSM で生成されたログ メッセージの保存先と送信先を指定する方法について説明します FWSM で生成された Syslog メッセージを表示するには、ログの出力先を指定する必要があります。ログの出力先を指定せずにロギングをイネーブルにした場合、FWSM でメッセージは生成されますが、参照が可能な場所への保存は行われません。

ここでは、次の内容について説明します。

- 「Syslog サーバへの Syslog メッセージの送信」（P.25-4）
- 「電子メール アドレスへの Syslog メッセージの送信」（P.25-6）
- 「ASDM への Syslog メッセージの送信」（P.25-7）
- 「スイッチ セッション、Telnet セッション、または SSH セッションへの Syslog メッセージの送信」（P.25-8）
- 「ログ バッファへの Syslog メッセージの送信」（P.25-9）

Syslog サーバへの Syslog メッセージの送信

ここでは、Syslog サーバに Syslog メッセージを送信するように FWSM を設定する方法について説明します。

Syslog メッセージを Syslog サーバに送信するように FWSM を設定すると、Syslog メッセージをアーカイブしてサーバの空きディスク スペース以外の制約を受けないようにし、保存後にログ データを操作できるようになります。たとえば、特定タイプの Syslog メッセージがログに記録されたり、ログか

らデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

Syslog サーバでは、syslogd というプログラム（サーバ）を実行する必要があります。UNIX では、OS（オペレーティング システム）の一部として Syslog サーバを提供しています。Windows 95 および Windows 98 の場合、別のベンダーから syslogd サーバを入手してください。

（注） この手順で定義した Syslog サーバへのロギングを開始するには、すべての出力先へのロギングを必ずイネーブルにしてください。「設定された全出力先へのロギングのイネーブル化」（P.25-3）を参照してください。ロギングをディセーブルにするには、「設定された全出力先へのロギングのディセーブル化」（P.25-3）を参照してください。

Syslog メッセージを Syslog サーバに送信するように FWSM を設定する手順は、次のとおりです。

ステップ 1　Syslog メッセージを受信する Syslog サーバを指定するには、次のコマンドを入力します。

```
hostname(config)# logging host interface_name ip_address [tcp[/port] | udp[/port]]
[format emblem]
```

format emblem キーワードでは、Syslog サーバの EMBLEM フォーマットのロギングをイネーブルにします（UDP だけ）。

interface_name 引数には、Syslog サーバにアクセスするときのインターフェイスを指定します。

ip_address 引数には、Syslog サーバの IP アドレスを指定します。

tcp[*/port*] または **udp**[*/port*] 引数には、Syslog サーバに Syslog メッセージを送信するために FWSM で TCP または UDP を使用する必要があることを指定します。デフォルト プロトコルは UDP です。UDP または TCP のいずれかを使用して Syslog サーバにデータを送信するように FWSM を設定することはできますが、両方を使用するように設定することはできません。TCP を指定した場合、FWSM は Syslog サーバに障害が発生したために中断された Syslog メッセージ送信を検知します。UDP を指定した場合、Syslog サーバが動作可能かどうかに関係なく、FWSM は Syslog メッセージの送信を続行します。*port* 引数には、Syslog サーバが Syslog メッセージを待ち受けるポートを指定します。有効なポートの値は、どちらのプロトコルも 1025 ～ 65,535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

次に例を示します。

```
hostname(config)# logging host dmz1 192.168.1.5
```

出力先として複数の Syslog サーバを指定する場合は、指定する Syslog サーバごとに個別にコマンドを入力します。

ステップ 2　Syslog サーバに送信する Syslog メッセージを指定するには、次のコマンドを入力します。

```
hostname(config)# logging trap {severity_level | message_list}
```

severity_level 引数には、Syslog サーバに送信するメッセージの重大度を指定します。重大度の番号（0 ～ 7）または名前を指定できます。重大度の名前については、「重大度」（P.25-20）を参照してください。たとえば、重大度を 3 に設定した場合、FWSM は重大度が 3、2、1、0 の Syslog メッセージを送信します。

message_list 引数には、Syslog サーバに送信する Syslog メッセージを識別するカスタム メッセージ リストを指定します。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによる Syslog メッセージのフィルタリング」（P.25-14）を参照してください。

次に、FWSM が重大度 3（error）以上の Syslog メッセージをすべて Syslog サーバに送信するよう指定する例を示します。FWSM は、重大度が 3、2、1 のメッセージを送信します。

```
hostname(config)# logging trap errors
```

ステップ 3　（任意）必要に応じて、次のコマンドを入力して、ロギング ファシリティをデフォルトの 20 以外の値に設定します。

```
hostname(config)# logging facility number
```

大部分の UNIX システムでは Syslog メッセージがファシリティ 20 で届くことを想定しています。

```
hostname(config)# logging
```

ステップ 4　（任意）TCP Syslog サーバがダウンした場合でもトラフィックの伝送を続行するには、次のコマンドを入力します。

hostname(config)# **logging permit-hostdown**

permit-hostdown キーワードでは、TCP ベースの Syslog サーバに対して新しいネットワーク アクセス セッションを許可します。

電子メール アドレスへの Syslog メッセージの送信

FWSM の Syslog メッセージの一部またはすべてを、電子メール アドレスに送信するよう設定することができます。電子メールで送信される場合、Syslog メッセージは電子メール メッセージの件名行に表示されます。このため、このオプションでは、critical、alert、および emergency など、重大度の高い Syslog メッセージを管理者に通知するように設定することをお勧めします。

（注）　この手順で定義した電子メール アドレスへのロギングを開始するには、すべての出力先へのロギングを必ずイネーブルにしてください。「設定された全出力先へのロギングのイネーブル化」（P.25-3）を参照してください。ロギングをディセーブルにするには、「設定された全出力先へのロギングのディセーブル化」（P.25-3）を参照してください。

出力先として電子メール アドレスを指定する手順は、次のとおりです。

ステップ 1　1 つまたは複数の電子メール アドレスに送信する Syslog メッセージを指定するには、次のコマンドを入力します。

```
hostname(config)# logging mail {severity_level | message_list}
```

severity_level 引数には、電子メール アドレスに送信するメッセージの重大度を指定します。重大度の番号（0 ～ 7）または名前を指定できます。重大度の名前については、「重大度」（P.25-20）を参照してください。たとえば、重大度を 3 に設定した場合、FWSM は重大度が 3、2、1、0 の Syslog メッセージを送信します。

message_list 引数には、電子メール アドレスに送信する Syslog メッセージを識別するカスタム メッセージ リストを指定します。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによる Syslog メッセージのフィルタリング」（P.25-14）を参照してください。

次に、以前に **logging list** コマンドで設定した「high-priority」という名前の *message_list* を使用する例を示します。

```
hostname(config)# logging mail high-priority
```

ステップ 2　Syslog メッセージを電子メール アドレスに送信する際に使用する送信元の電子メール アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# logging
from-address email_address
```

次に例を示します。

```
hostname(config)# logging from-address xxx-001@example.com
```

ステップ 3　Syslog メッセージを電子メール アドレスに送信する際に使用する受信者の電子メール アドレスを指定します。受信者のアドレスを 5 つまで設定できます。各受信者を個別に入力する必要があります。

受信者のアドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# logging recipient-address e-mail_address [severity_level]
```

重大度を指定しなかった場合、デフォルトの重大度が使用されます（エラー状態：重大度 3）。

次に例を示します。

```
hostname(config)# logging recipient-address admin@example.com
```

ステップ 4　Syslog メッセージを電子メール アドレスに送信する際に使用する SMTP サーバを指定するには、次のコマンドを入力します。

```
hostname(config)# smtp-server ip_address
```

次に例を示します。

```
hostname(config)# smtp-server 10.1.1.1
```

ASDM への Syslog メッセージの送信

Syslog メッセージを ASDM に送信するように FWSM を設定できます。FWSM は、ASDM への送信を待つ Syslog メッセージのためにバッファ領域を確保し、メッセージが発生するとバッファに保存します。ASDM ログ バッファは、内部ログ バッファとは別のバッファです。内部ログ バッファの詳細については、「ログ バッファへの Syslog メッセージの送信」（P.25-9）を参照してください。

ASDM のログ バッファがいっぱいになると、FWSM は新しい Syslog メッセージのためにバッファを確保するため、最も古い Syslog メッセージを削除します。ASDM ログ バッファに保持される Syslog メッセージの数を制御するために、バッファのサイズを変更できます。

ここでは、次の内容について説明します。

- 「ASDM ロギングの設定」（P.25-7）
- 「ASDM のログ バッファの消去」（P.25-8）

ASDM ロギングの設定

（注）　この手順で定義した ASDM へのロギングを開始するには、すべての出力先へのロギングを必ずイネーブルにしてください。「設定された全出力先へのロギングのイネーブル化」（P.25-3）を参照してください。ロギングをディセーブルにするには、「設定された全出力先へのロギングのディセーブル化」（P.25-3）を参照してください。

出力先として ASDM を指定する手順は、次のとおりです。

ステップ 1　ASDM に送信する Syslog メッセージを指定するには、次のコマンドを入力します。

```
hostname(config)# logging asdm {severity_level | message_list}
```

severity_level 引数には、ASDM に送信するメッセージの重大度を指定します。重大度の番号（0 ～ 7）または名前を指定できます。重大度の名前については、「重大度」（P.25-20）を参照してください。たとえば、重大度を 3 に設定した場合、FWSM は重大度が 3、2、1、0 の Syslog メッセージを送信します。

message_list 引数には、ASDM に送信する Syslog メッセージを識別するカスタム メッセージ リストを指定します。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによる Syslog メッセージのフィルタリング」（P.25-14）を参照してください。

次に、ロギングをイネーブルにして、ASDM のログ バッファに重大度 0、1、2 の Syslog メッセージを送信する例を示します。

```
hostname(config)# logging asdm 2
```

ステップ 2　ASDM のログ バッファに保存可能な Syslog メッセージの数を指定するには、次のコマンドを入力します。

```
hostname(config)# logging asdm-buffer-size num_of_msgs
```

num_of_msgs には、FWSM が ASDM のログ バッファに保存する Syslog メッセージの数を指定します。

次に、ASDM のログ バッファ サイズを 200 Syslog メッセージに設定する例を示します。

```
hostname(config)# logging asdm-buffer-size 200
```

ASDM のログ バッファの消去

ASDM ログ バッファの現在の内容を消去するには、次のコマンドを入力します。

```
hostname(config)# clear logging asdm
```

スイッチ セッション、Telnet セッション、または SSH セッションへの Syslog メッセージの送信

スイッチから FWSM にログインする場合、Telnet セッションを使用して接続されます。そのため、Telnet または SSH セッションへのロギングを設定するのと同じ方法で、スイッチ セッションへのロギングを設定します。

Telnet または SSH セッションで Syslog メッセージを表示するには、次の 2 つの手順を実行する必要があります。

1. Telnet または SSH セッションに送信するメッセージの指定
2. 現在のセッションの Syslog メッセージの表示

ここでは、次の内容について説明します。

- 「Telnet および SSH セッションのロギングの設定」（P.25-9）
- 「現在のセッションの Syslog メッセージの表示」（P.25-9）

Telnet および SSH セッションのロギングの設定

（注）　この手順で定義した Telnet または SSH へのロギングを開始するには、すべての出力先へのロギングを必ずイネーブルにしてください。「設定された全出力先へのロギングのイネーブル化」（P.25-3）を参照してください。ロギングをディセーブルにするには、「設定された全出力先へのロギングのディセーブル化」（P.25-3）を参照してください。

Telnet または SSH セッションに送信するメッセージを指定するには、次のコマンドを入力します。

```
hostname(config)# logging monitor {severity_level | message_list}
```

severity_level 引数には、セッションに送信するメッセージの重大度を指定します。重大度の番号（0 ～ 7）または名前を指定できます。重大度の名前については、「重大度」（P.25-20）を参照してください。たとえば、重大度を 3 に設定した場合、FWSM は重大度が 3、2、1、0 の Syslog メッセージを送信します。

message_list 引数には、セッションに送信する Syslog メッセージを識別するカスタム メッセージ リストを指定します。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによる Syslog メッセージのフィルタリング」（P.25-14）を参照してください。

現在のセッションの Syslog メッセージの表示

現在のセッションのロギングをイネーブルにする手順は、次のとおりです。

ステップ 1　FWSM にログインしたあとに、次のコマンドを入力して、現在のセッションのロギングをイネーブルにします。

```
hostname# terminal monitor
```

このコマンドにより、現在のセッションでだけロギングがイネーブルになります。ログアウトしたあとに再度ログインする場合は、このコマンドを再入力する必要があります。

ステップ 2　現在のセッションのロギングをディセーブルにするには、次のコマンドを入力します。

```
hostname(config)# terminal no monitor
```

ログ バッファへの Syslog メッセージの送信

出力先として設定すると、ログ バッファは Syslog メッセージの一時保存場所として機能します。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになった場合、バッファを別の場所に保存するように FWSM を設定していないかぎり、新しいメッセージが生成されると古いメッセージは上書きされます。

ここでは、次の内容について説明します。

出力先としてのログ バッファのイネーブル化

（注）　この手順で定義したバッファへのロギングを開始するには、すべての出力先へのロギングを必ずイネーブルにしてください。「設定された全出力先へのロギングのイネーブル化」（P.25-3）を参照してください。ロギングをディセーブルにするには、「設定された全出力先へのロギングのディセーブル化」（P.25-3）を参照してください。

ログの出力先としてログ バッファをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# logging buffered {severity_level | message_list}
```

severity_level 引数には、バッファに送信するメッセージの重大度を指定します。重大度の番号（0 ～ 7）または名前を指定できます。重大度の名前については、「重大度」（P.25-20）を参照してください。たとえば、重大度を 3 に設定した場合、FWSM は重大度が 3、2、1、0 の Syslog メッセージを送信します。

message_list 引数には、バッファに送信する Syslog メッセージを識別するカスタム メッセージ リストを指定します。カスタム メッセージ リストの作成方法の詳細については、「カスタム メッセージ リストによる Syslog メッセージのフィルタリング」（P.25-14）を参照してください。

たとえば、重大度が 1 と 2 のメッセージをログ バッファに保存するよう指定するには、次のいずれかのコマンドを入力します。

```
hostname(config)# logging buffered critical
```

または

```
hostname(config)# logging buffered level 2
```

message_list オプションには、ログ バッファに保存するメッセージの選択基準を記述したメッセージ リストの名前を指定します。

```
hostname(config)# logging buffered notif-list
```

ログ バッファの表示

ログ バッファを表示するには、次のコマンドを入力します。

```
hostname(config)# show logging
```

ログ バッファ サイズの変更

デフォルトのログ バッファ サイズは 4 KB です。ログ バッファのサイズを変更するには、次のコマンドを入力します。

```
hostname(config)# logging buffer-size bytes
```

bytes 引数には、ログ バッファに使用するメモリの容量（バイト単位）を設定します。たとえば、8192 を指定した場合、FWSM によってログ バッファに 8 KB のメモリが使用されます。

次に、FWSM でログ バッファに 16 KB のメモリを使用するよう指定する例を示します。

```
hostname(config)# logging buffer-size 16384
```

フラッシュ メモリへの、いっぱいになったログ バッファの自動保存

この設定を行わない場合、FWSM はメッセージを連続的にログ バッファに送信し、バッファがいっぱいになると古いメッセージは上書きされます。Syslog メッセージの履歴が必要な場合、バッファがいっぱいになるたびにバッファの内容を別の出力先に送信するように FWSM を設定できます。バッファの内容は、内部フラッシュ メモリまたは FTP サーバに保存できます。

バッファの内容を別の場所に保存するとき、FWSM は次のようなデフォルトのタイムスタンプ フォーマットを使用した名前でログ ファイルを作成します。

LOG-YYYY-MM-DD-HHMMSS.TXT

YYYY は年、*MM* は月、*DD* は日、*HHMMSS* は時刻（時、分、秒）です。

FWSM は、ログ バッファの内容を内部フラッシュ メモリまたは FTP サーバに書き込んでいる間も、ログ バッファへの新しいメッセージの保存を続行します。

バッファがいっぱいになるたびにログ バッファのメッセージを内部フラッシュ メモリに保存するよう指定するには、次のコマンドを入力します。

```
hostname(config)# logging flash-bufferwrap
```

FTP サーバへの、いっぱいになったログ バッファの自動保存

バッファの保存の詳細については、「内部フラッシュ メモリへのログ バッファの現在の内容の保存」セクションを参照してください。

バッファがいっぱいになるたびにログ バッファのメッセージを FTP サーバに保存するよう指定する手順は、次のとおりです。

ステップ 1　バッファがいっぱいになるたびにログ バッファの内容を FTP サーバに送信する FWSM の機能をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# logging ftp-bufferwrap
```

ステップ 2　FTP サーバを識別するには、次のコマンドを入力します。

```
hostname(config)# logging ftp-server server path username password
```

server 引数には、外部 FTP サーバの IP アドレスを指定します。

path 引数には、ログ バッファのデータを保存する FTP サーバへのディレクトリ パスを指定します。このパスは、FTP ルート ディレクトリへの相対パスです。

username 引数には、FTP サーバにログインできるユーザ名を指定します。

password 引数には、指定したユーザ名のパスワードを指定します。

次に例を示します。

```
hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
```

内部フラッシュ メモリへのログ バッファの現在の内容の保存

バッファの内容は、いつでも内部フラッシュ メモリに保存できます。ログ バッファの現在の内容を内部フラッシュ メモリに保存するには、次のコマンドを入力します。

```
hostname(config)# logging savelog [savefile]
```

たとえば、次のコマンドは、ログ バッファの内容を「latest-logfile.txt」というファイル名で内部フラッシュ メモリに保存します。

```
hostname(config)# logging savelog latest-logfile.txt
```

ログ バッファの内容の消去

ログ バッファの内容を削除するには、次のコマンドを入力します。

```
hostname(config)# clear logging buffer
```

Syslog メッセージのフィルタリング

ここでは、出力先に送信される Syslog メッセージを指定する方法について説明します。内容は次のとおりです。

メッセージのフィルタリングの概要

生成される Syslog メッセージは、特定の Syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ある出力先にすべての Syslog メッセージを送信し、別の出力先には Syslog メッセージのサブセットを送信するように FWSM を設定できます。

具体的には、Syslog メッセージが次の基準に従って出力先に転送されるように、FWSM を設定できます。

- Syslog メッセージの ID 番号
- Syslog メッセージの重大度
- Syslog メッセージのクラス（FWSM の機能領域と同等）

これらの基準をカスタマイズするには、「ログの出力先の設定」（P.25-4）で出力先を設定する場合に指定できるメッセージ リストを作成します。

あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するように FWSM を設定することもできます。

たとえば、重大度が 1、2、3 の Syslog メッセージをすべて内部ログ バッファに送信したり、クラスが「ha」の Syslog メッセージをすべて特定の Syslog サーバに送信したり、「high-priority」という名前のメッセージ リストを作成して、問題をシステム管理者に通知するために電子メール アドレスに送信したりするように FWSM を設定することができます。

クラスによる Syslog メッセージのフィルタリング

Syslog メッセージのクラスは、タイプごとに Syslog メッセージを分類する方法の 1 つであり、FWSM の機能に相当します。たとえば、「auth」クラスはユーザ認証を示します。

ここでは、次の内容について説明します。

メッセージ クラスの概要

ロギング クラスでは、1 つのコマンドで Syslog メッセージのカテゴリ全体の出力先を指定できます。

Syslog メッセージのクラスは次の 2 つの方法で使用できます。

- **logging class** コマンドを発行して、Syslog メッセージのカテゴリ全体の出力先を指定します。
- メッセージ クラスを指定する **logging list** コマンドを使用して、メッセージ リストを作成します。手順については、「カスタム メッセージ リストによる Syslog メッセージのフィルタリング」（P.25-14）を参照してください。

特定のクラスに属する Syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、400 で始まる Syslog メッセージ ID はすべて、ids クラスに関連しています この IDS 機能に関連付けられた Syslog メッセージの範囲は、400400 ～ 400415 です。

指定の出力先へのクラス内の全メッセージの送信

クラス内のすべてのメッセージを出力先のタイプに送信するように設定した場合、この設定によって、特定の出力先コマンドの設定が上書きされます。たとえば、重大度 7 のメッセージをログ バッファに送信するように指定し、さらに重大度 3 の ha クラス メッセージをログ バッファに送信するように指定した場合、後の設定が優先されます。

設定した出力先に Syslog メッセージ クラス全体を送信するように FWSM を設定するには、次のコマンドを入力します。

```
hostname(config)# logging class message_class {buffered | history | mail | monitor | trap}
[severity_level]
```

message_class 引数には、指定の出力先に送信する Syslog メッセージのクラスを指定します。Syslog メッセージ クラスの一覧については、表 25-1 を参照してください。

buffered、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスの Syslog メッセージの出力先を指定します。**history** キーワードは、SNMP でのロギングをイネーブルにします。**monitor** キーワードは、Telnet および SSH でのロギングをイネーブルにします。**trap** キーワードは、Syslog サーバへのロギングをイネーブルにします。コマンド ライン エントリごとに出力先を 1 つ指定してください。クラスを複数の出力先に送信するよう指定する場合は、出力先ごとに個別にコマンドを入力します。

severity_level 引数では、重大度を指定することにより、出力先に送信される Syslog メッセージをさらに制限します。メッセージの重大度の詳細については、「重大度」（P.25-20）を参照してください。

次に、クラス「ha」（ハイ アベイラビリティ：フェールオーバーともいう）に関する重大度が 1（alert）の Syslog メッセージをすべて内部ロギング バッファに送信するように指定する例を示します。

```
hostname(config)# logging class ha buffered alerts
```

表 25-1 に、Syslog メッセージ クラス、および各クラスに関連付けられている Syslog メッセージ ID の範囲を示します。

表 25-1　Syslog メッセージのクラスおよび関連するメッセージ ID 番号

クラス	定義	Syslog メッセージ ID 番号
auth	ユーザ認証	109、113
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
config	コマンド インターフェイス	111、112、208、308

表 25-1　Syslog メッセージのクラスおよび関連するメッセージ ID 番号 （続き）

クラス	定義	Syslog メッセージ ID 番号
e-mail	電子メール プロキシ	719
ha	フェールオーバー（ハイ アベイラビリティ）	101、102、103、104、210、311、709
ip	IP スタック	209、215、313、317、408
NP	ネットワーク プロセッサ	319
ospf	OSPF ルーティング	318、409、503、613
rip	RIP ルーティング	107、312
rm	リソース マネージャ	321
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711

カスタム メッセージ リストによる Syslog メッセージのフィルタリング

カスタム メッセージ リストを作成して、送信する Syslog メッセージとその出力先を柔軟に制御できます。カスタム Syslog メッセージ リストでは、重大度、メッセージ ID、Syslog メッセージ ID の範囲、メッセージ クラスのいずれかまたはすべてを基準として、Syslog メッセージのグループを指定できます。

たとえば、メッセージ リストを使用して、次のことを実行できます。

- 重大度が 1 および 2 の Syslog メッセージを選択し、1 つ以上の電子メール アドレスに送信する。
- メッセージ クラス（「ha」など）に関連付けられたすべての Syslog メッセージを選択し、内部バッファに保存する。

メッセージ リストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンド エントリで行う必要があります。メッセージ選択基準が重複するメッセージ リストを作成することもできます。メッセージ リストの 2 つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

ログ バッファに保存するメッセージを選択するために FWSM が使用するカスタム リストを作成する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、メッセージ選択基準を含むメッセージ リストを作成します。

```
hostname(config)# logging list name {level level [class message_class] |
message start_id[-end_id]}
```

name 引数には、リストの名前を指定します。重大度の名前を Syslog メッセージ リストの名前として使用しないでください。使用が禁止された名前には、「emergency」、「alert」、「critical」、「error」、「warning」、「notification」、「informational」、および「debugging」があります。また、ファイル名の最初に、これらの用語の最初の 3 文字を使用しないでください。たとえば、「err」という文字で始まるファイル名を使用しないでください。

level *level* 引数には、重大度を指定します。重大度の番号（0 ～ 7）または名前を指定できます。重大度の名前については、「重大度」（P.25-20）を参照してください。たとえば、重大度を 3 に設定した場合、FWSM は重大度が 3、2、1、0 の Syslog メッセージを送信します。

class *message_class* 引数には、特定のメッセージ クラスを指定します。クラス名のリストについては、表 25-1（P.25-13）を参照してください。

message *start_id*[**-***end_id*] 引数には、個々の Syslog メッセージ ID 番号または番号の範囲を指定します。

次に、重大度が 3 以上のメッセージをログ バッファに保存するよう指定する、「notif-list」という名前のメッセージ リストを作成する例を示します。

```
hostname(config)# logging list notif-list level 3
```

ステップ 2　（任意）リストにさらにメッセージ選択基準を追加する場合は、前の手順と同じコマンドを入力して、既存のメッセージ リストの名前と追加する基準を指定します。リストに追加する基準ごとに、個別にコマンドを入力します。

次に、メッセージ リストに基準を追加する例を示します。追加する基準は、メッセージ ID 番号の範囲、およびメッセージ クラス「ha」（ハイ アベイラビリティ：フェールオーバー）です。

```
hostname(config)# logging list notif-list 104024-105999
hostname(config)# logging list notif-list level critical
hostname(config)# logging list notif-list level warning class ha
```

上記の例では、指定した基準に一致する Syslog メッセージが出力先に送信されます。リストに含めるための Syslog メッセージの基準は、次のとおりです。

- 範囲が 104024 ～ 105999 の Syslog メッセージ ID
- 重大度が critical 以上のすべての Syslog メッセージ（emergency、alert、または critical）
- 重大度が warning 以上のすべての ha クラスの Syslog メッセージ（emergency、alert、critical、error、または warning）

Syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。Syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

ログ設定のカスタマイズ

ここでは、ロギング設定を微調整するためのオプションについて説明します。内容は次のとおりです。

ロギング キューの設定

FWSM のメモリ内には、設定された出力先への送信を待機している Syslog メッセージをバッファするために割り当てられる、固定された数のブロックがあります。必要なブロックの数は、Syslog メッセージ キューの長さと、指定した Syslog サーバの数によって異なります。

指定された出力先に送信する前に FWSM がキューに保持できる Syslog メッセージの数を指定するには、次のコマンドを入力します。

```
hostname(config)# logging queue message_count
```

message_count 変数には、処理待ちの Syslog メッセージを Syslog メッセージ キューに保持する数を指定します。デフォルトは 512 Syslog メッセージです。0（ゼロ）を設定すると、Syslog メッセージの数は無制限になります。つまり、キュー サイズの制約が、利用可能なブロック メモリだけになります。

キューおよびキュー統計情報を表示するには、次のコマンドを入力します。

```
hostname(config)# show logging queue
```

Syslog メッセージへの日付と時刻の追加

Syslog メッセージの生成日時を Syslog メッセージに記載するように指定するには、次のコマンドを入力します。

```
hostname(config)# logging timestamp
```

Syslog メッセージへの装置 ID の記載

非 EMBLEM フォーマットの Syslog メッセージに装置 ID を記載するように FWSM を設定するには、次のコマンドを入力します。

```
hostname(config)# logging device-id {context-name | hostname | ipaddress interface_name |
string text}
```

Syslog メッセージには、1 つの装置 ID タイプだけを指定できます。

context-name キーワードは、現在のコンテキストの名前を装置 ID として使用することを示します（マルチコンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**システム**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

hostname キーワードは、FWSM のホスト名をデバイス ID として使用するように指定します。

ipaddress *interface_name* 引数を指定すると、*interface_name* として指定したインターフェイスの IP アドレスがデバイス ID として使用されます。**ipaddress** キーワードを使用すると、Syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された FWSM のインターフェイス IP アドレスとなります。このキーワードにより、デバイスから送信されるすべての Syslog メッセージに単一の一貫したデバイス ID を指定できます。

string *text* 引数を指定すると、入力したテキスト文字列がデバイス ID として使用されます。この文字列には、最大 16 文字を指定できます。空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

（注）　イネーブルにすると、装置 ID は EMBLEM フォーマットの Syslog メッセージや SNMP トラップに表示されません。

次に、セキュリティ アプライアンスのロギング装置 ID をイネーブルにする例を示します。

```
hostname(config)# logging device-id hostname
```

次に、セキュリティ アプライアンスのセキュリティ コンテキストのロギング装置 ID をイネーブルにする例を示します。

```
hostname(config)# logging device-id context-name
```

EMBLEM フォーマットの Syslog メッセージの生成

UDP 経由で Syslog サーバに送信される Syslog メッセージに EMBLEM フォーマットを使用するには、次のコマンドを入力して、Syslog サーバを出力先として設定するときに **format emblem** オプションを指定します。

```
hostname(config)# logging host interface_name ip_address {tcp[/port] | udp[/port]}
[format emblem]
```

interface_name および *IP_address* には Syslog メッセージを受信する Syslog サーバを指定します。**tcp**[*/port*] および **udp**[*/port*] は使用するプロトコルとポートを示します。**format emblem** は、Syslog サーバに送信するメッセージに対して EMBLEM フォーマットをイネーブルにします。

セキュリティ アプライアンスでは、Syslog メッセージの送信に UDP および TCP プロトコルを使用できますが、EMBLEM フォーマットをイネーブルにできるのは、UDP 経由で送信されるメッセージだけです。デフォルトのプロトコルおよびポートは、UDP および 514 です。

次に例を示します。

```
hostname(config)# logging host interface_1 122.243.006.123 udp format emblem
```

EMBLEM 形式の Syslog メッセージを Syslog サーバ以外に送信するには、次のコマンドを入力します。

```
hostname(config)# logging emblem
```

Syslog サーバの詳細については、「Syslog サーバへの Syslog メッセージの送信」（P.25-4）を参照してください。

Syslog メッセージのディセーブル化

セキュリティ アプライアンスで特定の Syslog メッセージが生成されないようにするには、次のコマンドを入力します。

```
hostname(config)# no logging message message_number
```

次に例を示します。

```
hostname(config)# no logging message 113019
```

ディセーブルにした Syslog メッセージを再度イネーブルにするには、次のコマンドを入力します。

```
hostname(config)# logging message message_number
```

次に例を示します。

```
hostname(config)# logging message 113019
```

ディセーブルにした Syslog メッセージのリストを表示するには、次のコマンドを入力します。

```
hostname(config)# show logging message
```

ディセーブルにしたすべての Syslog メッセージのロギングを再度イネーブルにするには、次のコマンドを入力します。

```
hostname(config)# clear config logging disabled
```

Syslog メッセージの重大度の変更

Syslog メッセージのロギング レベルを指定するには、次のコマンドを入力します。

```
hostname(config)# logging message message_ID level severity_level
```

次に、Syslog メッセージ 113019 の重大度を 4（warning）から 5（notification）に変更する例を示します。

```
hostname(config)# logging message 113019 level 5
```

Syslog メッセージのロギング レベルをデフォルトのレベルに戻すには、次のコマンドを入力します。

```
hostname(config)# no logging message message_ID level current_severity_level
```

次に、Syslog メッセージ 113019 の重大度をデフォルトの 4（warning）に戻す例を示します。

```
hostname(config)# no logging message 113019 level 5
```

特定のメッセージの重大度を表示するには、次のコマンドを入力します。

```
hostname(config)# show logging message message_ID
```

重大度が変更された Syslog メッセージのリストを表示するには、次のコマンドを入力します。

```
hostname(config)# show logging message
```

変更したすべての Syslog メッセージの重大度をデフォルトに戻すには、次のコマンドを入力します。

```
hostname(config)# clear configure logging level
```

次の例の一連のコマンドは、**logging message** コマンドにより、Syslog メッセージのイネーブル化と、Syslog メッセージの重大度の両方を制御する方法を示しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Syslog メッセージに使用する内部フラッシュ メモリの容量の変更

ログ バッファの内容を内部フラッシュ メモリに保存するよう FWSM を設定するには、次の 2 つの方法があります。

- バッファがいっぱいになるたびにログ バッファの内容が内部フラッシュ メモリに保存されるようロギングを設定する。
- コマンドを入力して、ログ バッファの現在の内容をただちに内部フラッシュ メモリに保存するよう FWSM に指示する。

デフォルトでは、FWSM は、内部フラッシュ メモリの最大 1 MB をログ データに使用できます。FWSM でのログ データの保存のために解放する必要がある内部フラッシュ メモリのデフォルトの最低容量は、3 MB です。

内部フラッシュ メモリの空き容量が、内部フラッシュ メモリに保存するログ ファイルのために設定された最小限の容量を下回る場合、FWSM は最も古いログ ファイルを削除し、その新しいログ ファイルが保存されたとしても最小限の容量が確保されるようにします。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリがまだ制限を下回る場合、FWSM で新しいログ ファイルを保存できません。

Syslog メッセージに利用できる内部フラッシュ メモリの容量の設定を変更する手順は、次のとおりです。

ステップ 1　ログ ファイルの保存に利用できる内部フラッシュ メモリの最大容量を指定するには、次のコマンドを入力します。

```
hostname(config)# logging flash-maximum-allocation kbytes
```

kbytes には、ログ ファイルの保存に使用可能な内部フラッシュ メモリの最大容量（KB 単位）を指定します。

次に、ログ ファイルのために使用できる内部フラッシュ メモリの最大容量を約 1.2 MB に設定する例を示します。

```
hostname(config)# logging flash-maximum-allocation 1200
```

ステップ 2　FWSM でのログ ファイルの保存のために解放する必要がある内部フラッシュ メモリの最低容量を指定するには、次のコマンドを入力します。

```
hostname(config)# logging flash-minimum-free kbytes
```

kbytes には、FWSM で新しいログ ファイルを保存するために空いている必要のある内部フラッシュ メモリの最低容量（KB 単位）を指定します。

次に、FWSM で新しいログ ファイルを保存するために内部フラッシュ メモリに 4,000 KB の最低空き容量が必要であるという指定を行う例を示します。

```
hostname(config)# logging flash-minimum-free 4000
```

Syslog メッセージの概要

ここでは、セキュリティ アプライアンスで生成される Syslog メッセージの内容について説明します。内容は次のとおりです。

- 「Syslog メッセージのフォーマット」（P.25-20）

- 「重大度」（P.25-20）

Syslog メッセージのフォーマット

Syslog メッセージは、パーセント記号（%）から始まり、次のような構造になっています。

```
%FWSM Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

FWSM	セキュリティ アプライアンスで生成されるメッセージの Syslog メッセージ ファシリティ コードを示します。この値は常に FWSM です。
Level	1 ～ 7 を指定します。レベルは、Syslog メッセージで記述される状態の重大度に対応します。値が小さいほど、重大な状況です。詳細については、表 25-2 を参照してください。
Message_number	Syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状態を説明する文字列です。Syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。変数フィールドおよびその説明のリストについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Log Messages*』を参照してください。

重大度

表 25-2 に、Syslog メッセージの重大度の一覧を示します。

表 25-2　Syslog メッセージの重大度

レベル番号	level キーワード	説明
0	emergency	システムが使用不能です。
1	alert	即時のアクションが必要です。
2	critical	クリティカル条件。
3	error	エラー条件。
4	warning	警告条件。
5	notification	正常だが注意を要する状態。
6	informational	情報メッセージ
7	debugging	デバッグ中にだけ表示

（注）　セキュリティ アプライアンスは、重大度 0（emergency）の Syslog メッセージは生成しません。このレベルは、UNIX システム ログ機能との互換性のために **logging** コマンドで提供されますが、セキュリティ アプライアンスでは使用されません。

SNMP の設定

ここでは、SNMP の設定方法について説明しますが、すべての SNMP MIB およびトラップについて包括的な説明は提供していません。MIB およびイベント通知の詳細情報については、付録 D「MIB と CLI コマンドの対応」を参照してください。

内容は次のとおりです。

SNMP の概要

FWSM は、SNMP v1 および v2c を使用したネットワーク モニタをサポートしています。FWSM では、トラップおよび SNMP リード アクセスはサポートされますが、SNMP ライト アクセスはサポートされません。

Network Management Station（NMS; ネットワーク管理ステーション）にトラップ（イベント通知）を送信するように FWSM を設定したり、NMS を使用して FWSM 上の MIB（管理情報ベース）を参照できます。MIB は定義の集合で、FWSM は各定義の値のデータベースを保持します。MIB を参照するには、NMS から SNMP get 要求を発行します。SNMP トラップを受信して、MIB を参照するには、CiscoWorks for Windows またはその他の SNMP V1 や V2、MIB-II 準拠ブラウザを使用します。

表 25-3 に、サポート対象の MIB、FWSM のトラップ、およびマルチモードの各コンテキストのトラップを示します。Cisco MIB は、次の Web サイトからダウンロードできます。

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

ダウンロードした MIB を、NMS 用にコンパイルします。

（注）　パフォーマンス低下の原因になる場合があるため、SNMP を使用してデータを取得する頻度を制限します。また、リソース使用状況データを効率的に収集するために、コンテキスト単位でポーリングをスケジューリングします。

表 25-3　SNMP の MIB およびトラップのサポート

MIB およびトラップ	説明
CISCO-CRYPTO-ACCELERATOR-MIB	FWSM は、MIB の参照をサポートしています。
• CISCO-ENTITY-MIB • CISCO-ENTITY-ALARM-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-ENTITY-REDUNDANCY-MIB	FWSM は、次のグループおよびテーブルの参照をサポートしています。 • entLogicalTable • entPhysicalTable FWSM は、次のトラップを送信します。 • alarm-asserted • alarm-cleared • config-change • fru-insert • fru-remove • redun-switchover

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-IP-PROTOCOL-FILTER-MIB	FWSM は、次のテーブルの参照をサポートしています。 • cippfIpProfileTable • cippfIpFilterExtTable • cippfIpFilterStatsTable • cippfIpFilterTable 次に、**show access-list** コマンドで表示されるエントリを、cippfIpfilterTable オブジェクトおよび cippfIpfilterStatsTable オブジェクトでの SNMP 操作により取得する例を示します。

```
!
interface Vlan50
 nameif inside
 security-level 100
 ip address 50.0.0.2 255.0.0.0
!
interface Vlan60
 nameif outside
 security-level 0
 ip address 60.0.0.2 255.0.0.0
!
snmp-server host outside 60.0.0.1 community public version 2c
udp-port 161
!

hostname# show access-list
access-list aaa line 1 extended permit tcp any any eq www
(hitcnt=0) 0xe0998155

snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 returns as

SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.3.97.97.97 = INTEGER: 2
<<<< 2 means extended access-list
SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.1.1 = STRING: "aaa"
SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.2.1 = STRING: "aaa"
SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.1.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.2.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.3.97.97.97.1 = INTEGER:
2
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.3.97.97.97.1 = INTEGER:
1
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.3.97.97.97.1 =
Hex-STRING: 00 00 00 00  <-- denotes src network
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.3.97.97.97.1 =
Hex-STRING: 00 00 00 00  <-- denotes src network mask
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.3.97.97.97.1 =
Hex-STRING: 00 00 00 00  <-- denotes dest network
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.3.97.97.97.1 =
Hex-STRING: 00 00 00 00  <-- denotes dest network mask
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.3.97.97.97.1 = INTEGER:
6  <-- 6 stands for tcp protocol number
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.3.97.97.97.1 =
Gauge32: 0  <-0 means any port
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.3.97.97.97.1 =
Gauge32: 0  <-0 means any port.
SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.3.97.97.97.1 =
Gauge32: 80 <- www translates to 80
```

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-IP-PROTOCOL-FILTER-MIB（続き）	SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.3.97.97.97.1 = Gauge32: 0 <- 0 means any port. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.3.97.97.97.1 = INTEGER: 2 <- 2 means log for ACL is disabled. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.3.97.97.97.1 = INTEGER: 1 <- 1 means ACL log enabled. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.3.97.97.97.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.3.97.97.97.1 = Counter64: 0 <<<< 0 is current ACL hit counter for ACL 'aaa' ここで、「3.97.97.97」は、ASCII 文字のアクセス リスト名を示します。アクセス リスト名「aaa」は、97.97.97 に変換されます。ここで、「97」は ASCII 文字「a」に相当します。「3」は ASCII リスト名の文字番号を示します。 次に、ネットワーク オブジェクト グループを使用した、拡張されていないアクセス リストの例を示します。このリストは、SNMP 操作により取得できます。個々のアクセス リストのヒット カウントは、SNMP OID の「cipppfIpFilterHits」で集約および表示されます。 ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! object-group network src-network network-object 50.1.1.1 255.255.255.255 network-object 50.1.1.2 255.255.255.255 network-object 50.1.1.3 255.255.255.255 object-group network dest-network network-object 60.1.1.1 255.255.255.255 network-object 60.1.1.2 255.255.255.255 network-object 60.1.1.3 255.255.255.255 access-list aaa extended permit tcp object-group src-network object-group dest-network ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname(config)# **show access-list**

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-IP-PROTOCOL-FILTER-MIB（続き）	access-list mode auto-commit access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list aaa; 9 elements access-list aaa line 1 extended permit tcp object-group src-network object-group dest-network 0x705bc913 <---- only exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.1 (hitcnt=0) 0xcb224dc0 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.2 (hitcnt=0) 0x324aa638 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.3 (hitcnt=0) 0xca52e993 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.1 (hitcnt=0) 0xa45db454 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.2 (hitcnt=0) 0xd69df47f <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.3 (hitcnt=0) 0xb06956a6 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.1 (hitcnt=0) 0xcd7aeba4 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.2 (hitcnt=0) 0x3210272d <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.3 (hitcnt=0) 0xa2b03187 <---- not exposed snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.3.97.97.97 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.3.97.97.97.1 = INTEGER: 6 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.3.97.97.97.1 = STRING: "src-network" <--- source network object group name SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.3.97.97.97.1 = STRING: "dest-network" <-- destination network object-group name.. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.3.97.97.97.1 = ""

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-IP-PROTOCOL-FILTER-MIB（続き）	SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.3.97.97.97.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.3.97.97.97.1 = Counter64: 0 <-- aggregated ACL hit counter 次に、**show ipv6 access-list** コマンドで表示されるアクセス リスト エントリが SNMP 操作により取得および表示される例を示します。 interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ipv6 address 2000:400:3:1::100/64 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ipv6 address 2001:400:3:1::100/64 ! ! ipv6 access-list allow_ipv6 permit tcp any any eq www ! access-group allow_ipv6 in interface inside access-group allow_ipv6 in interface outside ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! FWSM# show ipv6 access-list ipv6 access-list allow_ipv6; 1 elements ipv6 access-list allow_ipv6 line 1 permit tcp any any eq www (hitcnt=0) 0xfabbda56 snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 returns as SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.10.97.108.108.111.119.95.105.112.118.54 = INTEGER: 3 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.1.3 = STRING: "allow_ipv6" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.2.3 = STRING: "allow_ipv6" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.1.3 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.2.3 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.10.97.108.108.111.119.95.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.10.97.108.108.111.119.95.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.10.97.108.108.111.119.95.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.10.97.108.108.111.119.95.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 95.105.112.118.54.1 = Gauge32: 0

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-IP-PROTOCOL-FILTER-MIB（続き）	SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.10.97.108.108.111.119.95.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.10.97.108.108.111.119.95.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.10.97.108.108.111.119.95.105.112.118.54.1 = INTEGER: 6 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.10.97.108.108.111.119. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.10.97.108.108.111.119.95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.10.97.108.108.111.119.95.105.112.118.54.1 = Gauge32: 80 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.10.97.108.108.111.119.95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.10.97.108.108.111.119.95.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.10.97.108.108.111.119.95.105.112.118.54.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.10.97.108.108.111.119.95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.10.97.108.108.111.119.95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.10.97.108.108.111.119.95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.10.97.108.108.111.119.95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.10.97.108.108.111.119.95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.10.97.108.108.111.119.95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.10.97.108.108.111.119.95.105.112.118.54.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.10.97.108.108.111.119.95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.10.97.108.108.111.119.95.105.112.118.54.1 = Counter64: 0 **（注）** どちらのアクセス リストでも SNMP クエリーを実行できません。 オブジェクト グループを使用するため、拡張されているアクセス リスト エントリでは SNMP クエリーを実行できません。SNMP クエリーは、オブジェクト グループを使用する、拡張されていないアクセス リストに対してだけ実行できます。SNMP クエリーは、オブジェクト グループを使用するアクセス リストの収集されたアクセス リスト ヒット カウンタに対してだけ実行できます。アクセス リストでオブジェクト グループを使用するため、拡張されたアクセス リスト エントリでは、ヒット カウントに対して SNMP クエリーを実行できません。 113 文字以上で設定されたアクセス リスト名では、SNMP クエリーを実行できません。

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-FIREWALL-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のグループの参照をサポートしています。 • cfwSystem cfwSystem.cfwStatus の情報は、単一コンテキストではなく装置全体のフェールオーバー ステータスに関する情報です。 FWSM は、次のテーブルの参照をサポートしています。 • cfwConnectionStatTable
CISCO-IPSEC-FLOW-MONITOR-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップを送信します。 • start • stop
CISCO-L4L7-RESOURCE-LIMIT-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップの参照をサポートしています。 • limit-reached • rate-limit-reached FWSM は、次のテーブルの参照をサポートしています。 • ciscoL4L7ResourceLimitTable • ciscoL4L7ResourceRateLimitTable
CISCO-MEMORY-POOL-MIB	FWSM は、次のテーブルの参照をサポートしています。 • ciscoMemoryPoolTable：このテーブルに保存されるメモリ使用状況は、セキュリティ アプライアンスの汎用プロセッサだけに適用され、ネットワーク プロセッサには適用されません。
CISCO-NAT-EXT-MIB	FWSM は、MIB の参照をサポートしています。
CISCO-PROCESS-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のテーブルの参照をサポートしています。 • cpmCPUTotalTable FWSM は、次のトラップを送信します。 • rising threshold
CISCO-REMOTE-ACCESS-MONITOR-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップを送信します。 • session-threshold-exceeded
CISCO-SYSLOG-MIB	FWSM は、次のトラップを送信します。 • clogMessageGenerated この MIB は参照できません。

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
CISCO-UNIFIED-FIREWALL-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のグループの参照をサポートしています。 • cufwUrlFilterGlobals：このグループは、グローバル URL フィルタリング統計情報を提供します。
IF-MIB	FWSM は、次のテーブルの参照をサポートしています。 • ifTable • ifXTable

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明

IP-FORWARD-MIB	FWSM は、テーブル inetCidrRouteTable の参照をサポートしています。
	次に、**show route** コマンドで表示されるエントリを SNMP 操作により取得する例を示します。
	`!`
	`interface Vlan50`
	`nameif inside`
	`security-level 100`
	`ip address 50.0.0.2 255.0.0.0`
	`!`
	`interface Vlan60`
	`nameif outside`
	`security-level 0`
	`ip address 60.0.0.2 255.0.0.0`
	`!`
	`snmp-server host outside 60.0.0.1 community public version 2c udp-port 161`
	`!`
	
	`hostname# show route`
	`50.0.0.0 255.0.0.0 is directly connected, inside`
	`60.0.0.0 255.0.0.0 is directly connected, outside`
	
	inetCidrRouteTable からの SNMP 要求が、次を返します。
	`snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.2.1.4.24.7 returns`
	
	`IP-MIB::ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1`
	`<---- ifindex`
	`IP-MIB::ip.24.7.1.7.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2`
	`<---- Inindex`
	`IP-MIB::ip.24.7.1.8.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 3`
	`<---- refer local`
	`IP-MIB::ip.24.7.1.8.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 3`
	`<---- refer local`
	`IP-MIB::ip.24.7.1.9.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2`
	`<---- 2 means local or connected route`
	`IP-MIB::ip.24.7.1.9.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2`
	`<---- 2 means local or connected route`
	`IP-MIB::ip.24.7.1.10.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0`
	`IP-MIB::ip.24.7.1.10.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0`
	`IP-MIB::ip.24.7.1.11.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0`
	`IP-MIB::ip.24.7.1.11.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0`
	`IP-MIB::ip.24.7.1.12.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 0`
	`<--- primary metric 0 for connected route`
	`IP-MIB::ip.24.7.1.12.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 0`
	`<--- primary metric 0 for connected route`
	`IP-MIB::ip.24.7.1.13.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.13.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.14.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.14.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.15.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.15.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.16.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.16.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1`
	`IP-MIB::ip.24.7.1.17.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1`
	`<----- 1 means route is active`
	`IP-MIB::ip.24.7.1.17.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1`
	`<----- 1 means route is active`

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明

IP-FORWARD-MIB（続き）	inetCidrRouteTable から SNMP OID の「inetCidrRouteIfIndex」を取得する SNMP 要求の場合は、次のように入力します。
	
	`snmpget 60.0.0.2 -c public -v 2c ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 returns as`
	
	`IP-MIB::ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1`
	
	（注） IPv6 ルート エントリでは SNMP クエリーを実行できません。
	
	show route コマンドで表示されるルート エントリ間に最大 3 分の遅延が発生する場合があり、このエントリに対して SNMP クエリーを実行することができます。

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明

IP-MIB	FWSM は、テーブル ipNetToPhysicalTable の参照をサポートしています。
	次に、**show arp** コマンドで表示されるエントリが SNMP 操作により取得される例を示します。
	`interface Vlan50`
	` nameif inside`
	` security-level 100`
	` ip address 50.0.0.2 255.0.0.0`
	`!`
	`interface Vlan60`
	` nameif outside`
	` security-level 0`
	` ip address 60.0.0.2 255.0.0.0`
	`!`
	`snmp-server host outside 60.0.0.1 community public version 2c udp-port 161`
	`!`
	
	`hostname# **show arp**`
	`inside 50.0.0.1 0004.23b3.9dea`
	`outside 60.0.0.1 000e.0c4e.f6cc`
	
	ipNetToPhysicalTable からの SNMP 要求の場合、次のように入力します。
	`snmpwalk 60.0.0.2 -c public -v 2c IP-MIB::ip.35 returns`
	
	`IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 = Hex-STRING: 00 04 23 B3 9D EA`
	`IP-MIB::ip.35.1.4.2.1.4.60.0.0.1 = Hex-STRING: 00 0E 0C 4E F6 CC`
	
	ipNetToPhysicalTable からの、特定の IP アドレスに対する SNMP 要求の場合、次のように入力します。
	
	`snmpwalk 60.0.0.2 -c public -v 2c IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 returns`
	
	`IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 = Hex-STRING: 00 04 23 B3 9D EA`
	
	ipNetToPhysicalTable オブジェクトは、ipNetToPhysicalIfIndex、ipNetToPhysicalNetAddressType、および ipNetToPhysicalNetAddress によって索引が作成されます。ここで、ipNetToPhysicalIfIndex は VLAN インターフェイス番号です。ipNetToPhysicalNetAddress オブジェクトは、MAC エントリを取得するための IP アドレスです。索引付き IP アドレスの MAC アドレスを取得するために、ipNetToPhysicalPhysAddress オブジェクトだけが ipNetToPhysicalTable から入力されます。
	（注） **show arp** コマンドで表示される ARP エントリ間に最大 3 分の遅延が発生する場合があり、このエントリに対して SNMP クエリーを実行することができます。

MIB-II	FWSM は、次のグループおよびテーブルの参照をサポートしています。 • system

表 25-3　SNMP の MIB およびトラップのサポート （続き）

MIB およびトラップ	説明
NAT-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップを送信します。 • packet-discard FWSM は、次のテーブルの参照をサポートしています。 • natAddrBindTable • natAddrPortBindTable
RFC1213-MIB	FWSM は、次のテーブルの参照をサポートしています。 • ip.ipAddrTable
SNMP コア トラップ	FWSM は、次の SNMP コア トラップを送信します。 • 認証：NMS が正しいコミュニティ ストリングを認証しなかったために SNMP 要求に失敗した場合 • リンクアップ：インターフェイスが「up」ステートに移行した場合 • リンクダウン：**nameif** コマンドを削除したりして、インターフェイスがダウンした場合 • コールドスタート：FWSM をリロードして実行した場合
SNMPv2-MIB	FWSM は、次の参照をサポートしています。 • snmp
TCP-MIB	FWSM は、次のテーブルの参照をサポートしています。 • tcpConnectionTable
UDP-MIB	FWSM は、次のテーブルの参照をサポートしています。 • udpEndpointTable

SNMP のイネーブル化

ここでは、FWSM で SNMP をイネーブルにする方法について説明します。FWSM 上で実行される SNMP エージェントは、次の 2 つの機能を実行します。

- NMS からの SNMP 要求に応答する。
- トラップ（イベント通知）を NMS に送信する。

SNMP エージェントをイネーブルにし、FWSM に接続できる NMS を指定する手順は、次のとおりです。

ステップ 1　FWSM 上の SNMP サーバを確実にイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# snmp-server enable
```

デフォルトでは、SNMP サーバはイネーブルです。

ステップ 2　FWSM に接続できる NMS の IP アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll]
[community text] [version {1 | 2c}] [udp-port port]
```

ここで、*interface_name* 引数には、NMS にアクセスするためのインターフェイスを指定します。

ip_address 引数には、NMS の IP アドレスを指定します。

NMS をトラップ受信またはブラウジング（ポーリング）だけに制限する場合には、**trap** または **poll** を指定します。デフォルトでは、NMS は両方の機能を実行します。

ポート番号を変更するには、**udp-port** キーワードを使用します。

ステップ 3　次のコマンドを入力して、コミュニティ ストリングを指定します。

```
hostname(config)# snmp-server community key
```

SNMP コミュニティ ストリングは、FWSM と NMS 間の共有シークレットです。キーは、大文字と小文字が区別される最大 32 文字の値です。スペースは使用できません。

ステップ 4　（任意）SNMP サーバの場所またはコンタクト情報を設定する場合には、次のコマンドを入力します。

```
hostname(config)# snmp-server {contact | location} text
```

ここで、*text* には、SNMP サーバの場所またはコンタクト情報を定義します。

ステップ 5　FWSM から NMS へのトラップ送信をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# snmp-server enable traps [all | syslog | snmp [trap] [...] |
cpu threshold [trap] | entity [trap] [...] | ipsec [trap] [...] | nat [trap] |
remote-access [trap] | resource [trap]]
```

機能タイプごとにこのコマンドを入力して、個々のトラップまたはトラップのセットをイネーブルにするか、**all** キーワードを入力してすべてのトラップをイネーブルにします。

デフォルト設定では、すべての SNMP トラップはイネーブルになっています（**snmp-server enable traps snmp authentication linkup linkdown coldstart**）。これらのトラップをディセーブルにするには、**snmp** キーワードを指定してこのコマンドの **no** 形式を使用します。ただし、**clear configure snmp-server** コマンドを使用すると、SNMP トラップのデフォルトのイネーブル状態に戻ります。

このコマンドを入力し、トラップ タイプを指定しない場合、デフォルトは **syslog** です。（デフォルトの **snmp** トラップは **syslog** トラップとともに引き続きイネーブルのままです）。

snmp のトラップには、次のものがあります。

- **authentication**
- **linkup**
- **linkdown**
- **coldstart**

entity のトラップには、次のものがあります。

- **config-change**
- **fru-insert**
- **fru-remove**
- **redun-switchover**
- **alarm-asserted**
- **alarm-cleared**

ipsec のトラップには、次のものがあります。

- **start**
- **stop**

nat のトラップには、次のものがあります。

- **packet-discard**

remote-access のトラップには、次のものがあります。

- **session-threshold-exceeded**

resource のトラップには、次のものがあります。

- **limit-reached**
- **rate-limit-reached**

cpu threshold のトラップには、次のものがあります。

- **rising**

cpu threshold rising トラップを受信するには、次のコマンドを入力して cpu threshold rising およびモニタリング値を指定する必要があります。

```
hostname(config)# cpu threshold rising threshold_value monitoring level
```

ステップ 6　Syslog メッセージをトラップとして NMS に送信できるようにするには、次のコマンドを入力します。

```
hostname(config)# logging history level
```

上記の **snmp-server enable traps** コマンドを使用して、**syslog** トラップをイネーブルにしておく必要があります。

ステップ 7　ロギングをイネーブルにし、あとで NMS に送信できる Syslog メッセージを生成するには、次のコマンドを入力します。

```
hostname(config)# logging enable
```

次に、FWSM が内部インターフェイス上でホスト 192.168.3.2 から要求を受信するように設定する例を示します。

```
hostname(config)# snmp-server host inside 192.168.3.2
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact Pat lee
hostname(config)# snmp-server community ohwhatakeyisthee
```