CHAPTER 23

FWSM のモニタリング

この章では、FWSM のためのロギングと 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。システム ログ メッセージの内容とシステム ログ メッセージのフォーマットについても説明します。

この章は、モニタリングとロギングのコマンドやオプションについて包括的な説明をするものではありません。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。

この章で説明する内容は次のとおりです。

- SNMP の設定（p.23-2）
- ログの設定および管理（p.23-6）

SNMP の設定

ここでは、SNMP の使用方法について説明します。内容は次のとおりです。

- SNMP の概要（p.23-2）
- SNMP のイネーブル化（p.23-4）

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。

FWSM から 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）が送信されるように設定したり、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、MIB-II 準拠ブラウザを使用します。

表 23-1 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。

表 23-1　SNMP の MIB およびトラップのサポート

サポート対象の MIB またはトラップ	説明
SNMP コア トラップ	FWSM は、次のコア SNMP 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
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。 • システム
IF-MIB	セキュリティ アプライアンスは、次のテーブルの参照をサポートしています。 • ifTable • ifXTable
RFC1213-MIB	セキュリティ アプライアンスは、次のテーブルの参照をサポートしています。 • ip.ipAddrTable
SNMPv2-MIB	セキュリティ アプライアンスは、次の参照をサポートしています。 • snmp

表 23-1　SNMP の MIB およびトラップのサポート（続き）

サポート対象の MIB またはトラップ	説明
ENTITY-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。 • entPhysicalTable • entLogicalTable FWSM は、次のトラップの参照をサポートしています。 • config-change • fru-insert • fru-remove
CISCO-IPSEC-FLOW-MONITOR-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップの参照をサポートしています。 • start • stop
CISCO-REMOTE-ACCESS-MONITOR-MIB	FWSM は、MIB の参照をサポートしています。 FWSM は、次のトラップの参照をサポートしています。 • session-threshold-exceeded
CISCO-CRYPTO-ACCELERATOR-MIB	FWSM は、MIB の参照をサポートしています。
ALTIGA-GLOBAL-REG	FWSM は、MIB の参照をサポートしています。
Cisco Firewall MIB	FWSM は、次のグループの参照をサポートしています。 • cfwSystem この情報は、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 cfwSystem.cfwStatus です。
Cisco メモリ プール 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、FWSM 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 プロセス MIB	FWSM は、次のテーブルの参照をサポートしています。 • cpmCPUTotalTable
Cisco Syslog MIB	FWSM は、次のトラップをサポートしています。 • clogMessageGenerated この MIB は参照できません。

SNMP のイネーブル化

FWSM 上で実行される SNMP エージェントは、2 つの機能を実行します。

- NMS からの SNMP 要求への応答
- NMS へのトラップ（イベント通知）の送信

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　次のコマンドを入力して、FWSM で SNMP サーバがイネーブルになっていることを確認します。

```
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　次のコマンドを入力して、FWSM に接続できる NMS の IP アドレスを指定します。

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

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。

SNMP トラップは、デフォルトでは UDP ポート 162 上で送信されます。**udp-port** キーワードを使用すると、ポート番号を変更できます。

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。キーには、最大 32 文字の値を大文字と小文字を区別して指定します。スペースは入力できません。

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
```

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

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

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には、各機能タイプに対してこのコマンドを入力します。または、すべてのトラップをイネーブルにするには、**all** キーワードを入力します。

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**）。**snmp** キーワードを指定して、このコマンドの **no** 形式を使用すると、これらのトラップをディセーブルにすることができます。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化がリストアされます。

このコマンドを入力してトラップ タイプを指定しない場合、デフォルトは **syslog** となります（デフォルトの **snmp** トラップは、**syslog** トラップと一緒に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**

ipsec のトラップには、次のものがあります。

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

remote-access のトラップには、次のものがあります。

- **session-threshold-exceeded**

ステップ 6　次のコマンドを入力して、システム メッセージが NMS にトラップとして送信されるように設定します。

```
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　次のコマンドを入力して、NMS に送信されるシステム メッセージが生成されるように、ロギングをイネーブルにします。

```
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設定する例を示します。

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

ログの設定および管理

ここでは、ロギングの機能と設定について説明します。システム ログ 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。

- ロギングの概要（p.23-6）
- マルチコンテキスト モードでのロギング（p.23-7）
- ロギングのイネーブル化およびディセーブル化（p.23-7）
- ログの出力先の設定（p.23-9）
- 出力先に送信するシステム ログ メッセージのフィルタリング（p.23-19）
- ログ設定のカスタマイズ（p.23-22）
- システム ログ メッセージの内容（p.23-27）

ロギングの概要

FWSM のシステム ログでは、FWSM のモニタリングやトラブルシューティングのためのロギング情報が得られます。ロギングの設定は非常に柔軟性が高く、FWSM でのシステム ログ メッセージの処理方法に関して、さまざまな面からカスタマイズが可能です。

ロギング機能を使用すると、次のことができます。

- 記録するシステム ログ メッセージの指定
- システム ログ メッセージの重大度のディセーブル化または変更
- システム ログ 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、ASDM、SNMP 管理ステーション、指定した電子メール アドレス、Telnet および 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、グループ内でのシステム ログ メッセージの設定と管理
- バッファが一杯になってラップアラウンドした場合の、内部バッファの内容に対する処理方法の指定。バッファの内容を FTP サーバに送信したり、内容を内部フラッシュ メモリに保存したりするよう FWSM を設定できます。
- ログ ファイルを FTP サーバに送信
- ログ ファイルを内部フラッシュ メモリに保存
- システム ログ メッセージのリモート モニタリング。Adaptive Security Device Manager（ASDM）、Telnet、SSH セッションを使用するか、または内部ログ バッファの内容を Web ブラウザにダウンロードすることによって行います。

システム ログ メッセージ全体、またはシステム ログ 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することができます。システム ログ メッセージの重大度、システム ログ メッセージのクラスにより、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、どこにどのシステム ログ メッセージを送信するかをフィルタリングできます。

マルチコンテキスト モードでのロギング

各セキュリティ コンテキストに独自の設定があるように、各セキュリティ コンテキストには独自のロギング設定とシステム メッセージ ログがあります。セキュリティ コンテキスト用のメッセージ ログには、そのコンテキストのためにイネーブル化された機能に関するメッセージが含まれます。たとえば、コンテキスト ログには、そのコンテキストのセキュリティ ポリシー、ルーティング、設定変更に関するメッセージが含まれます。シングル コンテキスト モードで動作するセキュリティ アプライアンスと同様に、セキュリティ コンテキストのロギングはデフォルトではイネーブルになっていません。セキュリティ コンテキストのためにログを保持するには、セキュリティ コンテキストにアクセスしてロギングを設定する必要があります。同様に、セキュリティ コンテキストのログ メッセージを表示するには、セキュリティ コンテキストにアクセスする必要があります。

システムまたは admin コンテキストにログインして別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するものだけです。

システム実行スペースで生成されるシステム メッセージ（フェールオーバー メッセージを含む）が、admin コンテキストで生成されたメッセージと一緒に、admin コンテキストに表示されます。admin コンテキストでロギングを設定してイネーブルにした場合、システム実行スペースで発生するメッセージは、自動的に admin コンテキスト メッセージに追加されます。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。

各メッセージにセキュリティ コンテキストのロギング装置 ID を記述するようにロギングを設定できます。このように設定した場合、各メッセージに、メッセージが作成されたコンテキストの名前が記述されます。admin コンテキストのロギング装置 ID をイネーブルにすると、システム実行スペースで生成されたメッセージには「system」という装置 ID が使用され、admin コンテキストで生成されたメッセージには装置 ID としてコンテキスト名が使用されます。ロギング装置 ID のイネーブル化の詳細については、「システム ログ メッセージへの装置 ID の記載」（p.23-23）を参照してください。

セキュリティ コンテキストの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』の「Enabling Multiple Context Mode」の章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 の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（p.23-7）
- 設定された全出力先へのロギングのディセーブル化（p.23-8）
- ログ設定の表示（p.23-8）

設定された全出力先へのロギングのイネーブル化

次の手順でロギングは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システム ログ 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.23-9）を参照してください。

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　次のコマンドを入力して、コンフィギュレーション モードにアクセスします。

```
hostname># config t
```

ステップ 2　次のコマンドを入力して、ロギングを開始します。

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

ステップ 3　次のコマンドを入力して、イネーブルになっているロギングのタイプを表示します。

```
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp 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
```

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
```

show logging コマンドの出力内容は、次のようになります。

```
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
```

ステータス行エントリの定義は、次のとおりです。

ロギング ステータス行	説明
System Log logging	システム ロギング全体のステータス
Facility	Syslog サーバに送信されたシステム ログ メッセージに使用されたロギング ファシリティ
Timestamp logging	システム ログ メッセージにタイムスタンプが記録されるかどうかを示します。
Standby logging	イネーブルにすると、フェールオーバーの発生時にフェールオーバー スタンバイ FWSM のシステム ログ メッセージの同期を維持します。
Deny Conn when Queue Full	イネーブルにすると、ログ キューがいっぱいになったときにすべてのトラフィックを拒否します。
Monitor logging	コンソールのロギングが Telnet または SSH セッションを通して表示可能かどうかを示します。
Buffer logging	内部ログ バッファがログ出力先としてイネーブルになっているかどうかを示します。
Trap logging	1 台または複数台の Syslog サーバへのログの送信がイネーブルになっているかどうかを示します。
History logging	SNMP 管理ステーションへのログの送信がイネーブルになっているかどうかを示します。
Device ID	システム ログ メッセージに装置 ID が記述されるかどうかを示します。
Mail logging	1 つまたは複数の電子メール アドレスへのログの送信がイネーブルになっているかどうかを示します。
ASDM logging	ASDM へのログの送信がイネーブルになっているかどうかを示します。

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。内容は次のとおりです。

- ログの出力先の概要（p.23-9）
- 出力先としての Syslog サーバの指定（p.23-10）
- 出力先としての電子メール アドレスの指定（p.23-12）
- 出力先としての ASDM の指定（p.23-13）
- Telnet セッションを使用したログの表示（p.23-15）
- 出力先としてのログ バッファの指定（p.23-16）

ログの出力先の概要

FWSM で生成されたログを表示するには、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。

FWSM では、ログの送信先として次の場所を設定できます。

- 1 台または複数の Syslog サーバ

- 1 つまたは複数の電子メール アドレス
- ASDM
- Telnet セッション
- 内部ログ バッファ

出力先としての Syslog サーバの指定

ここでは、FWSM のログの出力先として Syslog サーバを設定する方法について説明します。

FWSM のログを Syslog サーバに送信するよう設定すると、ログ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、特定のタイプのシステム ログ メッセージがロギングされたときに実行されるアクションを指定したり、ログからデータを抽出して、レポートのためにレコードを別のファイルに保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりすることができます。

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。

FWSM では、UDP または TCP を使用してデータを Syslog サーバに送信するよう設定することができますが、両方を同時に使用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ログ送信を検知します。UDP を指定した場合、FWSM は Syslog サーバが動作可能かどうかに関係なく、ログの送信を続行します。

ログ メッセージにタイムスタンプが必要であれば、ロギング タイムスタンプをイネーブルにすることができます。Syslog サーバへのログ送信に UDP を選択した場合、Syslog サーバの EMBLEM フォーマットのロギングをイネーブルにすることができます。

FWSM でシステム ログ メッセージを Syslog サーバに送信するよう設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ログを受信する Syslog サーバを指定します。

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

ここで

format emblem — 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 のみ）。

interface_name **—** Syslog サーバが常駐するインターフェイスを指定します。

port **—** Syslog サーバがシステム ログ 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。以前にコマンドを入力したときに使用した *port* と *protocol* の値を表示するには、**show running-config logging** コマンドを使用して一覧からコマンドを探します。TCP プロトコルは 6、UDP プロトコルは 17 としてリストに表示されます。

ip_address **—** Syslog サーバの IP アドレスを指定します。

tcp — FWSM が Syslog サーバへのシステム ログ メッセージの送信に TCP を使用するよう指定します。

udp — FWSM が Syslog サーバへのシステム ログ メッセージの送信に UDP を使用するよう指定します。

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 サーバを指定するには、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　次のコマンドを入力して、Syslog サーバに送信するシステム ログ メッセージを指定します。

```
hostname(config)# logging trap {severity_level (1-7) | message_list}
```

ここで

severity_level — Syslog サーバに送信するメッセージの重大度を指定します。たとえば、レベルの設定を 3 にすると、FWSM はレベルが 3、2、1、および 0 のシステム ログ メッセージを送信します。数字（2 など）か名前（critical など）のどちらかを指定できます。

メッセージの重大度の詳細については、「重大度」（p.23-28）を参照してください。

message_list — Syslog サーバに送信するシステム ログ 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 リストによるシステム ログ メッセージのフィルタリング」（p.23-21）を参照してください。

次に、FWSM が重大度 3（errors）以上のシステム ログ 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　サーバに送信するシステム ログ メッセージに装置 ID を記述する場合は、次のコマンドを入力します。

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

Syslog サーバに送信されるシステム ログ メッセージに、指定した装置 ID（指定したインターフェイスのホスト名と IP アドレス、または文字列）が記述されます。

ステップ 4　必要に応じて、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（大部分の UNIX システムではシステム ログ 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）。

ロギング ファシリティの設定を変更するには、次のコマンドを入力します。

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

次に例を示します。

```
hostname(config)# logging facility 16
```

ステップ 5　次のコマンドを入力して、設定の変更を確認します。

```
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
```

出力先としての電子メール アドレスの指定

FWSM のシステム ログ 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。電子メールで送信した場合、システム ログ メッセージは電子メール メッセージの件名の行に表示されます。このため、このオプションは、critical、alert、emergency など重大度の高いシステム ログ メッセージを管理者に通知する場合に設定することを推奨します。

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システム ログ メッセージを指定します。システム ログ メッセージの重大度またはシステム ログ メッセージ リスト変数を使用して、送信するシステム ログ メッセージを指定します。

送信するシステム ログ 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 {message_list | severity_level}
```

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　次のコマンドを入力して、システム ログ 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　システム ログ 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]
```

次に例を示します。

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

（注）　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）。

ステップ 4　次のコマンドを入力して、システム ログ 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 サーバを指定します。

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

次に例を示します。

```
hostname(config)# smtp-server smtp-host-1
```

出力先としての ASDM の指定

FWSM では、システム ログ メッセージを ASDM に送信するよう設定することができます。

FWSM は、ASDM への送信を待つシステム ログ 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 のログ バッファは、内部ログ バッファとは異なります。内部ログ バッファの詳細については、「ログ バッファの概要」（p.23-16）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 は新しいシステム ログ メッセージのためにバッファを確保するため、最も古いシステム ログ メッセージを削除します。ASDM のログ バッファに保存されるシステム ログ メッセージの数を制御するには、バッファのサイズを変更します。

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　次のコマンドを入力して、ASDM に送信するシステム ログ メッセージを指定します。

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

コマンド オプションは次のとおりです。

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルの設定を 3 にすると、FWSM はレベルが 3、2、1、および 0 のシステム ログ メッセージを生成します。次のように、数字または名前を指定できます。 • **0** または **emergencies** — システム使用不能 • **1** または **alerts** — 早急に処置が必要 • **2** または **critical** — クリティカル状態 • **3** または **errors** — エラー • **4** または **warnings** — 警告 • **5** または **notifications** — 正常だが注意が必要な状態 • **6** または **informational** — 情報 • **7** または **debugging** — デバッグ メッセージ、log FTP コマンド、および WWW URL
message_list	ASDM のログ バッファに送信するシステム ログ メッセージを識別するリストを指定します。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 リストによるシステム ログ メッセージのフィルタリング」（p.23-21）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 のシステム ログ 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　次のようにグローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用して、ASDM のログ バッファに保存可能なシステム ログ メッセージの数を指定します。

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

num_of_msgs に、FWSM が ASDM のログ バッファに保存するシステム ログ 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 システム ログ メッセージに設定する例を示します。

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

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
```

Telnet セッションを使用したログの表示

Telnet セッションで Syslog メッセージを表示する手順は、次のとおりです。

ステップ 1　インターフェイス内部のホストから FWSM へのアクセスを許可するための FWSM の設定をまだ行っていない場合、次の手順で設定します。

a. 次のコマンドを入力して、IP アドレスとインターフェイス名を指定します。

```
hostname(config)# telnet ip_address [subnet_mask] [if_name]
```

たとえば、ホストの IP アドレスが 192.168.1.2 の場合、コマンドは次のようになります。

```
hostname(config)# telnet 192.168.1.2 255.255.255.255
```

b. 応答がない場合に FWSM がセッションを切断するまでの Telnet セッションの待ち時間を、デフォルトの 5 分より大きな値に設定します。15 分以上に設定するのが望ましいです。設定方法は次のとおりです。

```
hostname(config)# telnet timeout 15
```

ステップ 2　ホストで Telnet を起動し、FWSM の内部インターフェイスを指定します。

Telnet の接続時に、FWSM で次のようなプロンプトが表示されます。

```
FWSM passwd
```

ステップ 3　Telnet のパスワードを入力します。デフォルトのパスワードは、**cisco** です。

ステップ 4　次のコマンドを入力して、コンフィギュレーション モードを開始します。

```
hostname(config)# enable
(Enter your password at the prompt)

hostname(config)# configure terminal
```

ステップ 5　次のコマンドを入力して、メッセージ ロギングを開始します。

```
hostname(config)# logging monitor level (1-7)
```

ステップ 6　次のコマンドを入力して、この Telnet セッションにログを送信します。

```
hostname(config)# terminal monitor
```

このコマンドにより、現在の Telnet セッションでのみロギングがイネーブルになります。**logging monitor** コマンドはすべての Telnet セッションのロギングに関する設定を行いますが、**terminal monitor**（および **terminal no monitor**）コマンドは個々の Telnet セッションのロギングを制御します。

ステップ 7　ホストに ping を実行するか、または Web ブラウザを起動することにより、イベントをトリガーします。

Telnet セッション ウィンドウに Syslog メッセージが表示されます。

ステップ 8　完了したら、次のコマンドでこの機能をディセーブルにします。

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

出力先としてのログ バッファの指定

ここでは、FWSM でシステム ログ メッセージを内部ログ バッファに保存するよう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。

- 出力先としてのログ バッファのイネーブル化（p.23-16）
- ログ バッファがいっぱいになった場合の動作の指定（p.23-17）
- 内部フラッシュ メモリへのログ バッファの内容の保存（p.23-18）
- ログ バッファの内容の消去（p.23-18）

ログ バッファの概要

出力先として設定すると、ログ バッファはシステム ログ 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、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。ログ メッセージを保存するには、バッファがいっぱいになるたびにバッファの内容を FTP サーバや内部フラッシュ メモリに保存するよう FWSM を設定して、古いメッセージが上書きされないようにすることができます。

ログ バッファのサイズは、バッファが一杯になる前にバッファに保存できるメッセージの数によって決まります。デフォルトのログ バッファ サイズは 4 KB です。

ログ バッファを出力先としてイネーブルにする場合、保存するメッセージも指定できます。指定しなければ、メッセージの生成時にすべてのメッセージがログ バッファに保存されます。FWSM で保存するメッセージの選択を行うとき、重大度や、カスタム メッセージ リストで指定する基準に基づいて設定することができます。保存するメッセージの制限の詳細については、「出力先に送信するシステム ログ メッセージのフィルタリング」（p.23-19）を参照してください。

出力先としてのログ バッファのイネーブル化

ログの出力先としてログ バッファをイネーブルにし、オプションのログ バッファ設定値を設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、FWSM でのシステム ログ メッセージのログ バッファへの保存をイネーブルにし、ログ バッファに保存するメッセージを指定します。

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

level は保存するメッセージの重大度、*message_list* はログ バッファに保存するメッセージを選択するために使用するカスタム リストの名前です。

level オプションには、数値（3 など）または名前（error など）で重大度を指定します。どちらを指定しても、その重大度以上のメッセージが選択されます。つまり、重大度 3 を選択した場合、重大度が 3、2、1 のメッセージがログ バッファに保存されます。

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
```

logging list コマンドを使用してカスタム メッセージ リストを作成することができます。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 リストによるシステム ログ メッセージのフィルタリング」（p.23-21）を参照してください。

ステップ 2　（任意）次のコマンドを入力して、ログ バッファのサイズを変更します。

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

bytes オプションにはログ 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 と指定すると、FWSM はログ バッファに 8 KB のメモリを使用します。

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
```

ログ バッファがいっぱいになった場合の動作の指定

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 バッファに記録し、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。ログ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 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
```

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　次のコマンドを入力して、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します。

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

ステップ 2　次のコマンドを入力して、FTP サーバの詳細を指定します。

```
hostname(config)# logging ftp-server {server_address | server_hostname} path username
password
```

ここで

server_address — 外部 FTP サーバの IP アドレスを指定します。

server_hostname — 外部 FTP サーバのホスト名を指定します。

path — ログ バッファ データを保存する FTP サーバのディレクトリ パスを指定します。このパスは FTP の root ディレクトリへの相対パスです。例：`/security_appliances/syslogs/appliance107`

username — FTP サーバにログインできるユーザ名を指定します。

password — 指定したユーザ名のパスワードを指定します。

次に、サーバ名に「logserver-352」、パスに「/syslogs」、ユーザ名に「logsupervisor」、パスワードに「1luvMy10gs」を指定するコマンドの例を示します。

```
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
```

内部フラッシュ メモリへのログ バッファの内容の保存

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]
```

次に、ログ バッファの現在の内容を「latest-logfile.txt」という名前で内部フラッシュ メモリに保存する例を示します。

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

ログ バッファの内容の消去

ログ バッファの内容を消去するには、次のコマンドを入力します。

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

出力先に送信するシステム ログ メッセージのフィルタリング

ここでは、特定の出力先へ送信するシステム ログ 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（p.23-19）
- クラスによるシステム ログ メッセージのフィルタリング（p.23-19）
- カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング（p.23-21）

メッセージのフィルタリングの概要

特定の出力先に特定のシステム ログ メッセージだけが送信されるように、生成されたシステム ログ メッセージをフィルタリングすることができます。たとえば、ある出力先にすべてのシステム ログ メッセージを送信し、別の出力先にはシステム ログ 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。

特に、システム ログ メッセージが 1 つの出力先に送信されるように、FWSM で次の項目を設定します。

- システム ログ メッセージの ID 番号
- システム ログ メッセージの重大度
- システム ログ メッセージのクラス（FWSM の機能領域に相当）
- 作成するシステム ログ メッセージ リスト

たとえば、重大度が 1、2、3 のシステム ログ 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」のシステム ログ 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。

クラスによるシステム ログ メッセージのフィルタリング

システム ログ メッセージのクラスを使用して、FWSM の機能に相当するタイプごとに、システム ログ メッセージを分類することができます。たとえば、「vpnc」クラスは VPN クライアントを示します。

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

システム メッセージ クラスは、2 通りの方法で使用できます。

- **logging class** コマンドを発行して、システム ログ メッセージのカテゴリ全体の出力先を指定します。
- システム ログ メッセージのカスタム リストの作成時に *message_class* 変数を使用して、システム ログ メッセージのクラス全体をカスタム リストに含めます。

特定のクラス内のシステム ログ メッセージはすべて、システム ログ メッセージ ID 番号の先頭 3 桁が同じになります。たとえば、611 で始まるシステム ログ メッセージ ID はすべて、vpnc（VPN クライアント）クラスに関連しています。VPN クライアント機能に関連するシステム ログ メッセージは、611,101 ～ 611,323 です。

指定の出力先へのクラス内の全メッセージの送信

設定した出力先にシステム ログ メッセージ クラス全体を送信するよう 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 | console | history | mail |
monitor | trap} [severity_level]
```

ここで

message_class — 指定の出力先に送信するシステム ログ メッセージのクラスを指定します。システム ログ メッセージ クラスの一覧については、表 23-2 を参照してください。

buffered | console | history | mail | monitor | trap — このクラスのシステム ログ メッセージを送信する出力先を指定します。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 — 重大度を指定することにより、出力先に送信するシステム ログ 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.23-28）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（警告）のシステム ログ 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指定する例を示します。

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

表 23-2 に、システム ログ メッセージのクラスと、各クラスに関連するシステム ログ メッセージ ID の範囲を示します。

表 23-2　システム ログ 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	システム ログ メッセージの ID 番号
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
rip	RIP ルーティング	107、312
auth	ユーザ認証	109、113
bridge	透過ファイアウォール	110、220
config	コマンド インターフェイス	111、112、208、308
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711
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
ip	IP スタック	209、215、313、317、408
snmp	SNMP	212
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPSec	316、320、402、404、501、602、702、713、714、715
ospf	OSPF ルーティング	318、409、503、613
np	ネットワーク プロセッサ	319
rm	リソース マネージャ	321
ids	Intrusion Detection System（IDS; 侵入検知システム）	400、401、415
vpnc	VPN クライアント	611

表 23-2　システム ログ 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	システム ログ メッセージの ID 番号
ca	PKI 認定機関	717
電子メール	電子メール プロキシ	719
vpnlb	VPN 負荷分散	718
vpnfo	VPN フェールオーバー	720

カスタム メッセージ リストによるシステム ログ メッセージのフィルタリング

カスタム メッセージ リストを作成すると、出力先に送信するシステム ログ メッセージの管理を柔軟に行えます。カスタム システム ログ メッセージ リストでは、基準の一部または全部を使用して、システム ログ メッセージのグループを指定します。基準となるのは、重大度、メッセージ ID、システム メッセージ ID の範囲、メッセージ クラスです。

たとえば、メッセージ リストを使用して次のことができます。

- 重大度が 1 および 2 のシステム ログ メッセージを選択して 1 つまたは複数の電子メール アドレスに送信
- メッセージ クラス（「ha」など）に関連するシステム ログ メッセージを選択して内部バッファに保存

メッセージ リストには、メッセージ選択の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可能です。メッセージ リストの 2 つの基準によって同一のメッセージが選択される場合でも、メッセージのロギングは 1 回しか行われません。

（注）　システム ログ メッセージ リストの名前として重大度の名前を使用しないでください。使用が禁止された *message_list* の名前には、「emergencies」、「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。

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 {message_list | [severity_level | message_class |
message_ID | range_of_IDs]}
```

ここで

message_list — メッセージ選択基準を含むリストの名前を指定します。

severity_level — 指定した重大度のメッセージをすべてログ バッファに保存するよう指定します。

message_class — 指定したメッセージ クラスに関連するメッセージをすべてログ バッファに保存するよう指定します。

message_ID — 個々のシステム ログ メッセージ ID 番号を指定します。

range_of_IDs ― メッセージ ID 番号の範囲（例：103401-103599）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。メッセージ クラスの詳細については、「クラスによるシステム ログ メッセージのフィルタリング」（p.23-19）を参照してください。

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

上記の例では、指定した基準に一致するシステム ログ メッセージがログ バッファに送信されます。リストに含めるためのシステム ログ メッセージの基準は、次のとおりです。

- 範囲が 100100 ～ 100110 のシステム ログ メッセージ ID
- 重大度が critical レベル以上のすべてのシステム ログ メッセージ（emergency、alert、または critical）
- 重大度が warning レベル以上のすべての VPN クラスのシステム ログ メッセージ（emergency、alert、critical、error、または warning）

これらの条件のいずれかを満たしたシステム ログ メッセージがロギングされます。1 つのシステム ログが複数の条件を満たしている場合でも、メッセージのロギングは 1 回しか行われません。

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（p.23-22）
- システム ログ メッセージへの日付および時刻の記載（p.23-23）
- システム ログ メッセージへの装置 ID の記載（p.23-23）
- EMBLEM フォーマットのシステム ログ メッセージの生成（p.23-24）
- システム ログ メッセージのディセーブル化（p.23-24）
- システム ログ メッセージの重大度の変更（p.23-25）
- ログに使用する内部フラッシュ メモリの容量の変更（p.23-26）

ロギング キューの設定

セキュリティ アプライアンスには、指定の出力先への送信を待つ間、システム ログ メッセージをバッファリングしておくためのメモリの固定ブロックがあります。必要なブロック数は、システム ログ メッセージ キューの長さと、指定された Syslog サーバの数によって決まります。

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システム ログ 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、処理待ちのシステム ログ メッセージをシステム ログ 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 システム ログ メッセージです。0（ゼロ）を設定すると、システム ログ 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 メモリのみとなります。

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
```

システム ログ メッセージへの日付および時刻の記載

システム ログ メッセージの生成日時をシステム ログ 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
```

システム ログ メッセージへの装置 ID の記載

非 EMBLEM フォーマットのシステム ログ 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}
```

ここで

context-name — 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 モードで動作している FWSM にのみ適用されます）。

hostname — FWSM のホスト名を装置 ID として使用するよう指定します。

ipaddress *interface_name* **—** *interface_name* に指定したインターフェイスの IP アドレスを装置 ID として使用するよう指定します。

ipaddress オプションを使用すると、システム ログ メッセージの送信元のインターフェイスに関係なく、その装置 ID が指定された FWSM のインターフェイス IP アドレスになります。このキーワードが、装置から送信されるすべてのシステム ログ メッセージのための統一された装置 ID になります。

string *text* **—** *text* オプションに入力された文字を装置 ID として使用するよう指定します。文字列は 16 文字まで入力可能です。*text* には、スペースと以下の文字は使用できません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（より小さい）
- >（より大きい）
- ?（クエスチョン マーク）

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

次に、FWSM 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、FWSM 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
```

マルチコンテキスト モードで admin コンテキストのロギング装置 ID をイネーブルにすると、システム実行スペースで生成されたメッセージには「**system**」という装置 ID が使用され、admin コンテキストで生成されたメッセージには装置 ID として admin コンテキスト名が使用されます。

EMBLEM フォーマットのシステム ログ メッセージの生成

Syslog サーバ以外の出力先に送信するシステム ログ 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ます。

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

UDP 経由で Syslog サーバに送信されるシステム ログ メッセージに EMBLEM フォーマットを使用するには、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。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]
```

ここで

interface_name および *IP_address* にはシステム ログ 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、システム ログ 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のみです。デフォルトのプロトコルおよびポートは、UDP/514 です。

次に例を示します。

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

システム ログ メッセージのディセーブル化

FWSM で特定のシステム ログ 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
hostname(config)#
```

次に例を示します。

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

ディセーブルにしたシステム ログ 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
hostname(config)#
```

ディセーブルにしたシステム ログ 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システム ログ 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
```

システム ログ メッセージの重大度の変更

システム ログ 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、システム ログ メッセージ ID 113019 の重大度を 4（warnings）から 5（notifications）に変更する例を示します。

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

システム ログ 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)# logging message message_ID level severity_level
```

次に、システム ログ メッセージ ID 113019 の重大度をデフォルトの 4（warnings）に戻す例を示します。

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

重大度が変更されたシステム ログ 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
```

変更したすべてのシステム ログ 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 config logging level
hostname(config)#
```

次の例の一連のコマンドは、**logging message** コマンドにより、システム ログ メッセージのイネーブル化と、システム ログ 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)
```

ログに使用する内部フラッシュ メモリの容量の変更

ログ バッファの現在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 はログ データ用に最大 1 MB の内部フラッシュ メモリを使用できます。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 メモリへのログ ファイルの保存により、内部フラッシュ メモリの空き容量が、設定された最低限度を下回ると、新しいログ ファイルを保存しても最低限のメモリの空き容量が確保されるよう、FWSM は古いログ ファイルを削除します。削除するファイルがない場合、または古いファイルをすべて削除しても空き容量が最低限度以上にならない場合は、FWSM は新しいログ ファイルを保存できません。

ログ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　次のコマンドを入力して、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します。

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

kbytes 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）です。

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　次のコマンドを入力して、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 4000 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
```

システム ログ メッセージの内容

ここでは、FWSM で生成されるシステム ログ 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。

- システム ログ メッセージのフォーマット（p.23-27）
- 重大度（p.23-28）
- システム ログ メッセージで使用される変数（p.23-28）
- logging コマンドのリスト（p.23-31）

システム ログ メッセージのフォーマット

システム ログ メッセージは、パーセント記号（%）で始まり、構成内容は次のとおりです。

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

フィールドの内容は次のとおりです。

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システム ログ 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。レベルは、システム ログ 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 23-3 を参照してください。
Message_number	システム ログ メッセージを示す 6 桁の一意の数値
Message_text	状態を説明する文字列。システム ログ メッセージのこの部分には、IP アドレス、ポート番号、ユーザ名が含まれることがあります。表 23-4 に、変数フィールドとその情報のタイプを示します。

重大度

表 23-3 に、システム ログ メッセージの重大度を示します。

表 23-3　システム ログ メッセージの重大度

レベル番号	レベル キーワード	説明
0	**emergencies**	システム使用不能
1	**alert**	早急に処置が必要
2	**critical**	クリティカル状態
3	**error**	エラー状態
4	**warning**	警告状態
5	**notification**	正常だが注意が必要な状態
6	**informational**	情報メッセージ
7	**debugging**	デバッグ中のみ表示

（注）　FWSM は、重大度 0（emergencies）のシステム ログ 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。

システム ログ メッセージで使用される変数

システム ログ メッセージでは、よく変数が使用されます。表 23-4 に、システム ログ メッセージの説明のためにこのガイドで使用する変数を示します。1 つのシステム ログ メッセージでしか使用しない変数は、このリストに示していません。

表 23-4　システム ログ メッセージの変数フィールド

変数	情報のタイプ
acl_ID	ACL の名前
bytes	バイト数
code	システム ログ メッセージから返される、エラー原因またはエラー発生源（システム ログ メッセージによって異なる）を示す 10 進数
command	コマンド名
command_modifier	*command_modifier* は、次のいずれかの文字列です。 • cmd（この文字列の場合、コマンドに修飾子はありません） • clear • no • show
connections	接続数

表 23-4　システム ログ メッセージの変数フィールド（続き）

変数	情報のタイプ
connection_type	接続タイプ： • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • UDP 経由 • ルート • RTP • RTCP
dec	10 進数
dest_address	パケットの宛先アドレス
dest_port	宛先ポート番号
device	メモリ ストレージ装置。フロッピー ディスク、内部フラッシュ メモリ、TFTP、フェールオーバー スタンバイ ユニット、コンソール端末など
econns	初期接続の数
elimit	**static** または **nat** コマンドで指定された初期接続の数
filename	タイプ セキュリティ アプライアンス イメージ、ASDM ファイル、コンフィギュレーションのファイル名
ftp-server	外部 FTP サーバの名前または IP アドレス
gateway_address	ネットワーク ゲートウェイの IP アドレス
global_address	グローバル IP アドレス、セキュリティ レベルの低いインターフェイスのアドレス
global_port	グローバル ポート番号
hex	16 進数
inside_address	内部（ローカル）IP アドレス、セキュリティ レベルの高いインターフェイスのアドレス
inside_port	内部ポート番号
interface_name	インターフェイスの名前
IP_address	*n.n.n.n* 形式の IP アドレス。*n* は 1 ～ 255 の整数
MAC_address	MAC アドレス
mapped_address	変換された IP アドレス
mapped_port	変換されたポート番号
message_class	FWSM の機能領域に対応付けられたシステム ログ メッセージのカテゴリ
message_list	システム ログ メッセージの ID 番号、クラス、重大度などを記述した、ユーザが作成するファイルの名前
message_number	システム ログ メッセージの ID
nconns	スタティックまたは xlate テーブルに許可された接続の数
netmask	サブネット マスク
number	数値。形式はシステム ログ メッセージによって異なります。
octal	8 進数
outside_address	外部 IP アドレス。外部ルータを越えたネットワークの、通常はセキュリティ レベルの低いインターフェイス上に存在する Syslog サーバのアドレス

表 23-4　システム ログ メッセージの変数フィールド（続き）

変数	情報のタイプ
outside_port	外部ポート番号
port	TCP または UDP のポート番号
privilege_level	ユーザの権限レベル
protocol	パケットのプロトコル。ICMP、TCP、UDP など
real_address	Network Address Translation（NAT; ネットワーク アドレス変換）前の実際の IP アドレス
real_port	NAT の前の実際のポート番号
reason	システム ログ メッセージの理由を説明する文字列
service	パケットによって指定されるサービス。SNMP、Telnet など
severity_level	システム ログ メッセージの重大度
source_address	パケットの送信元アドレス
source_port	送信元ポート番号
string	文字列（ユーザ名など）
tcp_flags	TCP ヘッダーのフラグ • ACK • FIN • PSH • RST • SYN • URG
time	*hh*:*mm*:*ss* の形式の期間
url	URL
user	ユーザ名

logging コマンドのリスト

ここでは、システム ロギングの設定とモニタリングのために FWSM で利用できる logging コマンドのリストを紹介し、各コマンドを簡単に説明します。各コマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

表 23-5 に、FWSM でシステム ロギングの設定とモニタリングのために利用できるコマンドの一覧を示します。

表 23-5　logging コマンドのリスト

コマンド	説明
clear configure logging	ロギング コンフィギュレーションの設定をデフォルト値に戻します。
clear logging asdm	ASDM ログ バッファからすべてのシステム ログ メッセージを削除します。
clear logging buffer	システム ログ バッファからすべてのシステム ログ メッセージを削除します。
clear running-config logging rate-limit	ロギング レート リミットをデフォルトに戻します。
logging asdm	システム ログ メッセージの一部またはすべてを ASDM に送信するよう FWSM を設定します。
logging asdm-buffer-size	ASDM に送信されるのを待っているメッセージを格納しておくためのバッファのサイズを設定します。
logging buffered	システム ログ メッセージの一部またはすべてをシステム ログ バッファに保存するよう FWSM を設定します。
logging buffer-size	システム メッセージを格納しておくためのバッファのサイズを設定します。
logging class	指定したメッセージ クラスのすべてのメッセージが指定の出力先に送信されるよう指定します。
logging console	FWSM のコンソール セッション中にシステム ログ メッセージが表示されるようにします。
logging debug trace	デバッギング メッセージがシステム ログに保存されるようにします。
logging device-id	非 EMBLEM フォーマットのシステム ログ メッセージに装置 ID を記載するように FWSM を設定します。
logging emblem	Syslog サーバ以外の出力先に送信するシステム ログ メッセージに EMBLEM フォーマットを使用するよう FWSM を設定します。
logging enable	設定された全出力先へのロギングをイネーブルにします。
logging facility	システム メッセージ サーバに送信されるメッセージに使用するロギング ファシリティを指定します。
logging flash-bufferwrap	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 メモリに書き込まれるよう FWSM を設定します。
logging flash-maximum-allocation	FWSM がログ データを格納するために使用する内部フラッシュ メモリの最大容量を指定します。
logging flash-minimum-free	FWSM が新しいログ 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 メモリの最低容量を指定します。
logging from-adress	FWSM によって電子メール送信されるシステム ログ メッセージの送信元電子メール アドレスを指定します。
logging ftp-bufferwrap	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 FTP サーバに書き込まれるよう FWSM をイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** がイネーブルの場合に、FWSM からログ バッファ データを送信される FTP サーバの詳細を指定します。

表 23-5　logging コマンドのリスト（続き）

コマンド	説明
logging history	SNMP ロギングをイネーブルにし、SNMP サーバに送信されるメッセージを指定します。
logging host	ログの出力先として Syslog サーバを定義します。
logging list	特定の出力先に送信するメッセージをフィルタリングするためのメッセージ選択基準のリストを作成または編集します。
logging mail	FWSM から電子メールによってシステム ログ メッセージを送信するようにし、電子メールで送信するメッセージを指定します。
logging message	システム ログ メッセージの重大度の取り消しまたは変更を行います。
logging monitor	SSH および Telnet セッションでシステム ログ メッセージを表示するよう FWSM を設定します。
logging permit-hostdown	動作していない TCP ベースの Syslog サーバに対して、FWSM が新しいネットワーク アクセス セッションを許可するか拒否するかを指定します。
logging queue	設定した出力先に送信するために FWSM がシステム ログ キューに保持できるシステム ログ メッセージの数を指定します。
loggign rate limit	システム メッセージを生成するレートを制限します。
logging recipient-adress	FWSM によって電子メールで送信されるシステム ログ メッセージの受信者の電子メール アドレスを指定します。
logging savelog	現在のログ バッファの内容を内部フラッシュ メモリに保存します。
logging standby	フェールオーバー スタンバイ FWSM でこの FWSM のシステム ログ メッセージをログ出力先に送信するよう設定します。
logging timestamp	システム ログ メッセージにメッセージの生成日時を記載するよう指定します。
logging trap	FWSM から Syslog サーバに送信するシステム ログ メッセージを指定します。
remote access threshold	FWSM からのトラップの送信先となる、アクティブなリモート アクセス セッションの数を指定します。
show logging	現在のロギング設定と現在のシステム ログ内部バッファの内容を表示します。
show running-config logging	現在使用されているすべてのロギング コンフィギュレーションの設定を表示します。
show running config logging rate-limit	システム メッセージを生成するレートの制限を表示します。