CHAPTER 42

セキュリティ アプライアンスのモニタリング

この章では、セキュリティ アプライアンスをモニタリングする方法について説明します。この章は、次の項で構成されています。

SNMP の使用

この項では、SNMP を使用する方法について説明します。次の項目を取り上げます。

SNMP の概要

セキュリティ アプライアンスは、SNMP V1 および V2c でのネットワーク モニタリングに対するサポートを提供します。セキュリティ アプライアンスはトラップと SNMP 読み取りアクセスをサポートしますが、SNMP 書き込みアクセスはサポートしません。

セキュリティ アプライアンスからネットワーク管理ステーション（NMS）へトラップ（イベント通知）が送信されるように設定できるほか、NMS を使用してセキュリティ アプライアンス上にある MIB のブラウジングを行うこともできます。MIB は定義の集合であり、セキュリティ アプライアンスは各定義に対応する値のデータベースを保持しています。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（ブラウジング）するには、CiscoWorks for Windows またはその他の SNMP V1、MIB-II 互換ブラウザを使用してください。

表 42-1 は、セキュリティ アプライアンスでサポートされる MIB とトラップ、およびマルチ モードの場合に各コンテキストでサポートされる MIB とトラップを示しています。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） ソフトウェア バージョン 7.2(1)、8.0(2) 以降では、SNMP 情報は 5 秒おきにリフレッシュされます。結果として、連続するポーリングの間に少なくとも 5 秒間は待機することをお勧めします。

表 42-1　SNMP の MIB およびトラップのサポート

MIB またはトラップのサポート	説明
SNMP コア トラップ	セキュリティ アプライアンスは、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 • coldstart：セキュリティ アプライアンスがリロード後に動作しています。
MIB-II	セキュリティ アプライアンスは、次のグループおよびテーブルのブラウジングをサポートします。 • system
IF-MIB	セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。 • ifTable • ifXTable
RFC1213-MIB	セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。 • ip.ipAddrTable
SNMPv2-MIB	セキュリティ アプライアンスは、次のブラウジングをサポートします。 • snmp
ENTITY-MIB	セキュリティ アプライアンスは、次のグループおよびテーブルのブラウジングをサポートします。 • entPhysicalTable • entLogicalTable セキュリティ アプライアンスは、次のトラップのブラウジングをサポートします。 • config-change • fru-insert • fru-remove
CISCO-IPSEC-FLOW-MONITOR-MIB	セキュリティ アプライアンスは、MIB のブラウジングをサポートします。 セキュリティ アプライアンスは、次のトラップのブラウジングをサポートします。 • start • stop

表 42-1　SNMP の MIB およびトラップのサポート （続き）

MIB またはトラップのサポート	説明
CISCO-REMOTE-ACCESS-MONITOR-MIB	セキュリティ アプライアンスは、MIB のブラウジングをサポートします。 セキュリティ アプライアンスは、次のトラップのブラウジングをサポートします。 • session-threshold-exceeded
CISCO-CRYPTO-ACCELERATOR-MIB	セキュリティ アプライアンスは、MIB のブラウジングをサポートします。
ALTIGA-GLOBAL-REG	セキュリティ アプライアンスは、MIB のブラウジングをサポートします。
Cisco Firewall MIB	セキュリティ アプライアンスは、次のグループのブラウジングをサポートします。 • cfwSystem 情報は cfwSystem.cfwStatus です。これは、フェールオーバー ステータスに関連する情報であり、シングル コンテキストだけでなく、デバイス全体に関係します。
Cisco Memory Pool MIB	セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。 • 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 Process MIB	セキュリティ アプライアンスは、次のテーブルのブラウジングをサポートします。 • cpmCPUTotalTable
Cisco Syslog MIB	セキュリティ アプライアンスは、次のトラップをサポートします。 • clogMessageGenerated この MIB は参照できません。

SNMP のイネーブル化

セキュリティ アプライアンスで動作する 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、セキュリティ アプライアンスに接続できる NMS を識別するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、セキュリティ アプライアンスの SNMP サーバを確実にイネーブルにします。

```
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　セキュリティ アプライアンスに接続できる NMS の IP アドレスを識別するには、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]
```

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 UDP ポート 162 を使用して送信されます。ポート番号は **udp-port** キーワードを使用して変更できます。

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、セキュリティ アプライアンスと NMS の間の共有秘密情報です。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
```

ステップ 5　セキュリティ アプライアンスでトラップを 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)# snmp-server enable traps [all | syslog | snmp [trap] [...] |
entity [trap] [...] | ipsec [trap] [...] | remote-access [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。

デフォルトのコンフィギュレーションでは、すべての **snmp** トラップがイネーブルです（**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 のトラップは次のとおりです。

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

entity のトラップは次のとおりです。

- **config-change**
- **fru-insert**
- **fru-remove**

ipsec のトラップは次のとおりです。

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

リモート アクセスのトラップは次のとおりです。

- **session-threshold-exceeded**

ステップ 6　システム 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て、生成されたシステム メッセージを 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 enable
```

次の例では、内部インターフェイス上のホスト 192.168.3.2 から要求を受信するようにセキュリティ アプライアンスを設定します。

```
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
```

ログの設定と管理

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

セキュリティ アプライアンスのシステム ログにより、セキュリティ アプライアンスのモニタリングおよびトラブルシューティングで必要な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。

- ログに記録するシステム ログ メッセージを指定する。
- システム ログ メッセージの重大度をディセーブルにするか、または変更する。
- システム ログ メッセージを送信する場所を 1 つ以上指定する。送信先には、内部バッファ、1 つ以上の syslog サーバ、ASDM、SNMP 管理ステーション、指定された電子メール アドレス、Telnet および SSH セッションなどがあります。
- システム ログ メッセージを、メッセージの重大度やクラスなどのグループで設定および管理する。
- 内部バッファがいっぱいになった場合に、そのバッファの内容に対して実行する処理を指定する。バッファを上書きするか、バッファの内容を FTP サーバに送信するか、または内容を内部のフラッシュ メモリに保存できます。

出力先のいずれかまたはすべてに対して、すべてのシステム ログ メッセージを送信するか、またはシステム ログ メッセージのサブセットを送信するように選択できます。いずれのシステム ログ メッセージをいずれの場所に送信するかをフィルタできます。これは、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って、またはカスタム ログ メッセージのリストを作成することで実行できます。

マルチ コンテキスト モードでのロギング

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 メッセージなどのシステム 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。

セキュリティ アプライアンスは、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、「システム ログ メッセージにデバイス ID を含める」（P.42-20）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、セキュリティ アプライアンス 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。出力先が指定されない場合、セキュリティ アプライアンスは、イベントが発生したとき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.42-7）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
```

ログの出力先の設定

この項では、セキュリティ アプライアンスにより生成されたログ 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。セキュリティ アプライアンスが生成し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すると、セキュリティ アプライアンスはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。

この項では、次のトピックについて取り上げます。

Syslog サーバへのシステム ログ メッセージの送信

この項では、セキュリティ アプライアンスを設定してログを syslog サーバに送信する方法について説明します。

ログを syslog サーバに送信するようにセキュリティ アプライアンスを設定すると、サーバで使用可能なディスク スペースを上限にしてログをアーカイブし、保存後にログ データを操作できます。たとえば、特定タイプのシステム ログ 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.42-6）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.42-6）を参照してください。

セキュリティ アプライアンスを設定して syslog サーバにシステム ログ メッセージを送信するには、次の手順を実行します。

ステップ 1　ログを受信する 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 キーワードは、syslog サーバでの EMBLEM 形式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*] 引数を使用して、システム ログ メッセージを syslog サーバに送信するためにセキュリティ アプライアンスで TCP または UDP を使用するように指定します。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セキュリティ アプライアンス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 を指定すると、セキュリティ アプライアンスは、syslog サーバでの障害やログ送信の中断を検出します。UDP を指定すると、セキュリティ アプライアンスは、syslog サーバが動作しているかどうかに関係なく、ログの送信を続けます。*port* 引数には、syslog サーバがシステム ログ メッセージをリッスンす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 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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

message_list 引数には、syslog サーバに送信するシステム ログ メッセージを特定するカスタマイズされたメッセージ 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.42-18）を参照してください。

次の例では、セキュリティ アプライアンスが重大度 3（エラー）以上のシステム ログ メッセージすべてを syslog サーバに送信するように指定しています。セキュリティ アプライアンス 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
```

ほとんどの 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 に到着することを想定しています。

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 host** *interface_name server_ip* [**tcp**/port] [**permit-hostdown**]

コンソール ポートへのシステム ログ メッセージの送信

この項では、セキュリティ アプライアンスを設定してログをコンソール ポートに送信する方法について説明します。

（注）　この手順で定義するコンソール ポートへのロギングを開始するには、すべての出力先で確実にロギングを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.42-6）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.42-6）を参照してください。

コンソール ポートに送信するシステム 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 console {severity_level | message_list}
```

severity_level 引数には、コンソール ポート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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

message_list 引数には、コンソール ポートに送信するシステム ログ メッセージを特定するカスタマイズされたメッセージ 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.42-18）を参照してください。

次の例では、セキュリティ アプライアンスが重大度 3（エラー）以上のシステム ログ メッセージすべてを syslog サーバに送信するように指定しています。セキュリティ アプライアンスは、重大度が 3、2、および 1 のメッセージを送信します。

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

電子メール アドレスへのシステム ログ メッセージの送信

セキュリティ アプライアンスを設定して、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 アドレスに送信できます。電子メールで送信される場合、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、重大度の高いシステム ログ 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.42-6）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.42-6）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 つ以上の電子メール アドレスに送信されるようにシステム 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 {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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

message_list 引数には、電子メール アドレスに送信するシステム ログ メッセージを特定するカスタマイズされたメッセージ 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.42-18）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　電子メール アドレスにシステム ログ メッセージを送信するときに使用する送信元電子メール 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　電子メールにシステム ログ メッセージを送信するときに使用する宛先の電子メール 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　電子メールの宛先にシステム ログ メッセージを送信するときに使用する 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 へのシステム ログ メッセージの送信

セキュリティ アプライアンスを設定して、ASDM にシステム ログ メッセージを送信できます。セキュリティ アプライアンスは、ASDM に送信されるのを待っているシステム ログ メッセージのためにバッファ領域を取り分け、メッセージが生成されるとその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 バッファへのシステム ログ メッセージの送信」（P.42-13）を参照してください。

ASDM ログ バッファがいっぱいになると、セキュリティ アプライアンスは最も古いシステム ログ メッセージを削除して、新しいシステム ログ メッセージのためのバッファ領域を確保します。ASDM ログ バッファに保持されるシステム ログ メッセージの数を制御するため、バッファのサイズを変更できます。

この項では、次のトピックについて取り上げます。

- 「ASDM ロギングの設定」（P.42-11）
- 「ASDM のログ バッファの消去」（P.42-12）

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.42-6）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.42-6）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 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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

message_list 引数には、ASDM に送信するシステム ログ メッセージを特定するカスタマイズされたメッセージ 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.42-18）を参照してください。

次の例では、ロギングをイネーブルにして、重大度が 0、1、および 2 のシステム ログ メッセージを ASDM ログ バッファに送信する方法を示しています。

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

ステップ 2　ASDM ログ バッファで保持するシステム 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 asdm-buffer-size num_of_msgs
```

num_of_msgs 引数には、セキュリティ アプライアンスが ASDM ログ バッファで保持するシステム ログ メッセージの数を指定します。

次の例は、ASDM ログ バッファのサイズをシステム ログ メッセージ 200 件分に設定する方法を示しています。

```
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
```

Telnet または SSH セッションへのシステム ログ メッセージの送信

Telnet または SSH セッションでシステム ログ 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を指定する。
2. 現在のセッションでログを表示する。

この項では、次のトピックについて取り上げます。

- 「Telnet および SSH セッションのロギングの設定」（P.42-12）
- 「現在のセッションでのシステム ログ メッセージの表示」（P.42-13）

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.42-6）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.42-6）を参照してください。

Telnet セッションまたは 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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

message_list 引数には、セッションに送信するシステム ログ メッセージを特定するカスタマイズされたメッセージ 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.42-18）を参照してください。

現在のセッションでのシステム ログ メッセージの表示

ステップ 1　セキュリティ アプライアンスにログインした後、次のコマンドを入力して、現在のセッションで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　現在のセッションで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 バッファへのシステム ログ メッセージの送信

出力先として設定されている場合、ログ バッファはシステム ログ メッセージの一時的な保存場所となります。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とき、つまりバッファ ラップが発生した場合は、セキュリティ アプライアンスがいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

この項では、次のトピックについて取り上げます。

- 「出力先としてのログ バッファのイネーブル化」（P.42-13）
- 「ログ バッファの表示」（P.42-14）
- 「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」（P.42-14）
- 「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」（P.42-15）
- 「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」（P.42-15）
- 「ログ バッファの内容の消去」（P.42-15）

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.42-6）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.42-6）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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

message_list 引数には、バッファに送信するシステム ログ メッセージを特定するカスタマイズされたメッセージ 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.42-18）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、セキュリティ アプライアンスによってログ バッファに 8 KB のメモリが使用されます。

次に、セキュリティ アプライアンス 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

特に設定されていない限り、セキュリティ アプライアンスは、メッセージを継続的にログ バッファ宛てに送信し、バッファがいっぱいになると古いメッセージを上書きします。ログの履歴を残しておきたい場合は、セキュリティ アプライアンスでバッファがいっぱいになるたびに、その内容を別の場所に送信するように設定します。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、セキュリティ アプライアンス 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* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

セキュリティ アプライアンスは、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 ラップが発生するたびにログ バッファのメッセージが内部フラッシュ メモリに保存され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 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」を参照してください。

バッファ ラップが発生するたびにログ バッファのメッセージが FTP サーバに保存されるように指定するには、次の手順を実行します。

ステップ 1　バッファ ラップが発生するたびに、セキュリティ アプライアンスでログ バッファの内容を FTP サーバ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 ftp-bufferwrap
```

ステップ 2　FTP 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 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 ディレクトリに対する相対パスです。

username 引数には、FTP サーバへのロギングで有効な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]
```

次の例では、latest-logfile.txt というファイル名で、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。

```
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
```

システム ログ メッセージのフィルタリング

この項では、出力先に送信するシステム ログ メッセージの指定方法について説明します。次の項目を取り上げます。

メッセージのフィルタリングの概要

生成されるシステム ログ メッセージは、特定のシステム ログ 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、セキュリティ アプライアンスを設定して、すべてのシステム ログ メッセージを 1 つの出力先に送信し、それらのシステム ログ メッセージのサブセットを別の出力先にも送信することができます。

具体的には、システム ログ 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、セキュリティ アプライアンスを設定できます。

- 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（セキュリティ アプライアンスの機能領域と同等）

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.42-7）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セキュリティ アプライアンスを設定することもできます。

たとえば、セキュリティ アプライアンスを設定して、重大度が 1、2、および 3 のシステム ログ メッセージすべてを内部ログ バッファに送信したり、「ha」クラスのシステム ログ メッセージすべてを特定の syslog サーバに送信したり、あるいは「high-priority」という名前のメッセージのリストを作成し、潜在的な問題についてシステム管理者に電子メールで通知したりできます。

クラスを基準としたシステム 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は、タイプごとにシステム ログ メッセージを分類する方法の 1 つであり、セキュリティ アプライアンスの機能に相当します。たとえば、「vpnc」クラスは VPN クライアントを意味します。

この項では、次のトピックについて取り上げます。

- 「メッセージ クラスの概要」（P.42-16）
- 「指定の出力先へのクラス内の全メッセージの送信」（P.42-17）

メッセージ クラスの概要

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

システム ログ 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、システム ログ メッセージの 1 つ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。この方法については、「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.42-18）を参照してください。

特定のクラスに属するすべてのシステム ログ メッセージの ID 番号は、最初の 3 桁が同じです。たとえば、611 で始まるすべてのシステム ログ メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられているシステム ログ メッセージの範囲は、611101 ～ 611323 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、レベル 7 のメッセージがログ バッファに送信されるように指定されているときに、レベル 3 の ha クラスのメッセージもログ バッファに送信されるように指定する場合は、後者のコンフィギュレーションが優先されます。

設定された出力先にシステム ログ メッセージ クラス全体が送信されるようにセキュリティ アプライアンスを設定するには、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]
```

message_class 引数には、指定した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 42-2 を参照してください。

buffered、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスのシステム ログ 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 エントリあたり 1 つの出力先を指定します。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 引数には重大度を指定し、出力先に送信されるシステム 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.42-24）を参照してください。

次の例では、重大度が 1（alert）で ha（ハイ アベイラビリティ、またはフェールオーバー）クラスに関連するすべてのシステム ログ メッセージが内部のロギング バッファに送信されるように指定しています。

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

表 42-2 に、システム ログ メッセージ クラスおよび各クラスに関連付けられたシステム ログ メッセージ ID の範囲を示します。

表 42-2　システム ログ メッセージのクラスと関連するメッセージの 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	トランスペアレント 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

表 42-2　システム ログ メッセージのクラスと関連するメッセージの ID 番号 （続き）

クラス （続き）	定義	システム ログ メッセージの ID 番号
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	侵入検知システム	400、401、415
vpnc	VPN クライアント	611
webvpn	Web ベースの VPN	716
ca	PKI 認証局	717
e-mail	電子メール プロキシ	719
vpnlb	VPN ロード バランシング	718
vpnfo	VPN フェールオーバー	720
npssl	NP SSL	725

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 リストを作成して、送信するシステム ログ 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 システム ログ メッセージ リストでは、重大度、メッセージ ID、システム ログ メッセージ ID の範囲のいずれかまたはすべてを基準として使用して、またはメッセージ クラスごとに、システム ログ 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 リストを次に利用できます。

- 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、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システム ログ 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、各メッセージ選択基準に新しいコマンド エントリを 1 つずつ追加する必要があります。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。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 セキュリティ アプライアンス 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。重要度の名前をシステム ログ メッセージ リストの名前として使用しないでください。使用禁止の名前は、「emergencies」、「alert」、「critical」、「error」、「warning」、「notification」、「informational」、および「debugging」です。同様に、ファイル名の先頭でこれらの単語の最初の 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.42-24）を参照してください。たとえば重大度を 3 に設定すると、セキュリティ アプライアンスは、重大度が 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。

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 42-2（P.42-17）を参照してください。

message *start_id*[**-***end_id*] 引数には、個々のシステム ログ 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 メッセージが出力先に送信されるように指定しています。リストに追加されるシステム ログ メッセージの基準として、次の条件が指定されています。

- ID が 104024 ～ 105999 の範囲のシステム ログ メッセージ
- 重大度が critical 以上（emergency、alert、または critical）のすべてのシステム ログ メッセージ
- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての ha クラスのシステム ログ メッセージ

システム ログ 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。システム ログ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。説明する項目は次のとおりです。

- 「ロギング キューの設定」（P.42-19）
- 「システム ログ メッセージに日付と時刻を含める」（P.42-20）
- 「システム ログ メッセージにデバイス ID を含める」（P.42-20）
- 「EMBLEM 形式でのシステム ログ メッセージの生成」（P.42-21）
- 「システム ログ メッセージのディセーブル化」（P.42-21）
- 「システム ログ メッセージの重大度の変更」（P.42-22）
- 「ログを記録可能な内部フラッシュ メモリの容量の変更」（P.42-23）

ロギング キューの設定

Cisco ASA のメモリ内には、設定された出力先に送信されるのを待機しているシステム ログ メッセージをバッファするために割り当てることができる、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、システム ログ メッセージ キューの長さおよび指定した syslog サーバの数によって異なります。

設定された出力先に送信されるまでの間、セキュリティ アプライアンスのキューで待機できるシステム 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、処理されるまでの間、システム ログ メッセージ キューで待機できるシステム ログ メッセージの数を指定します。デフォルトは 512 件のシステム ログ メッセージです。0（ゼロ）はシステム ログ メッセージの数が無制限であることを示し、使用可能なブロック メモリのサイズがキュー サイズの上限になることを意味します。

キューおよびキューの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 メッセージに日付と時刻を含める

システム ログ メッセージに、システム ログ メッセージが生成された日付と時刻を含め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 メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式のシステム ログ メッセージに含めるようにセキュリティ アプライアンスを設定するには、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}
```

システム ログ メッセージには、1 つのタイプのデバイス ID 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、セキュリティ アプライアンス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、システム ログ 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 は指定されたセキュリティ アプライアンス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システム ログ 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。文字列の長さは、最大で 16 文字です。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、EMBLEM 形式のシステム ログ メッセージや SNMP トラップにデバイス ID は表示されません。

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
```

EMBLEM 形式でのシステム ログ メッセージの生成

- syslog サーバ以外の宛先に送信されるシステム ログ メッセージで EMBLEM 形式を使用するには、次のコマンドを入力します。

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

- UDP を使用して syslog サーバに送信されるシステム ログ メッセージで EMBLEM 形式を使用するには、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。syslog サーバに関する詳細情報については、「Syslog サーバへのシステム ログ メッセージの送信」（P.42-7）を参照してください。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]
  ```

  interface_name および *ip_address* でシステム ログ メッセージを受信する syslog サーバを指定し、**tcp**[*/port*] および **udp**[*/port*] で使用するプロトコルとポートを指定し、**format emblem** で syslog サーバに送信されるメッセージの EMBLEM 形式をイネーブルにします。

  Cisco ASA は、UDP または TCP プロトコルを使用してシステム ログ メッセージを送信できますが、EMBLEM 形式をイネーブルにできるのは UDP を使用して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とポートは UDP と 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

- セキュリティ アプライアンスで特定のシステム 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
  ```

  次に例を示します。

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

- ディセーブルされたシステム 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
  ```

- ディセーブルにされたシステム 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
  ```

- ディセーブルにされ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
  ```

  次の例では、ID が 113019 のシステム ログ メッセージの重大度を 4（warnings）から 5（notifications）に変更しています。

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

- 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 レベルにリセットするには、次のコマンドを入力します。

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

  次の例では、ID が 113019 のシステム ログ メッセージの重大度をデフォルト値の 4（warnings）に変更しています。

  ```
  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
  ```

- 重大度が変更されているシステム 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
  ```

- 変更されたすべてのシステム ログ メッセージの重大度をそれぞれのデフォルトにリセットするには、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、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)
```

ログを記録可能な内部フラッシュ メモリの容量の変更

セキュリティ アプライアンスでは、次の 2 つの方法で、ログ バッファの内容を内部フラッシュ メモリに保存できます。

- バッファ ラップが発生するたびにログ 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にロギングを設定する
- セキュリティ アプライアンスに命令してログ バッファの現在の内容をすぐに内部フラッシュ メモリに保存させるコマンドを入力する

デフォルトでは、セキュリティ アプライアンスは、内部フラッシュ メモリの最大 1 MB をログ データのために使用できます。セキュリティ アプライアンスでログ データを保存するために必要な内部フラッシュ メモリの最小空き容量は、デフォルトで 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、セキュリティ アプライアンスは最も古いログ 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メモリ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、セキュリティ アプライアンスで新しいログ ファイルを保存できません。

ログの記録で使用可能な内部フラッシュ メモリの容量設定を変更するには、次の手順を実行します。

ステップ 1　ログ ファイルの保存で使用可能な内部フラッシュ 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 では、ログ ファイルの保存で使用可能な内部フラッシュ メモリの最大容量をキロバイト単位で指定します。

次の例では、ログ ファイル用に使用可能な内部フラッシュ メモリの最大容量を約 1.2 MB に設定しています。

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

ステップ 2　セキュリティ アプライアンスでのログ 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 では、セキュリティ アプライアンスで新しいログ ファイルを保存するために必要な内部フラッシュ メモリの最小空き容量をキロバイト単位で指定します。

次の例では、セキュリティ アプライアンスで新しいログ ファイルを保存できるように、内部フラッシュ メモリの最小空き容量として 4000 KB を確保する必要があるように指定しています。

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

システム ログ メッセージの概要

この項では、セキュリティ アプライアンスが生成するシステム ログ メッセージの内容について説明します。説明する項目は次のとおりです。

システム ログ メッセージの形式

システム ログ 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。

```
%PIX|ASA  Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

PIX|ASA	Cisco ASA が生成す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 PIX|ASA です。
Level	1 ～ 7。レベルは、システム ログ メッセージに記述されている状況の重大度を示します。値が小さいほど、重大な状況です。詳細については、「表 42-3」を参照してください。
Message_number	システム ログ メッセージを特定する 6 桁の一意の番号。
Message_text	状態を説明する文字列です。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、またはユーザ名が含まれていることがあります。

重大度

表 42-3 に、システム ログ メッセージの重大度の一覧を示します。

表 42-3　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**	システムが使用不能です。
1	**alert**	即時のアクションが必要です。
2	**critical**	危険な状態です。
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（emergencies）のシステム ログ メッセージを生成しません。このレベルは、UNIX システムのログ機能との互換性を保つために **logging** コマンドで使用できますが、Cisco ASA では使用されません。