セキュリティ アプライアンスのロギングの設定

この章では、セキュリティ アプライアンスのロギングの設定および管理に使用するコマンドについて説明します。また、システム ログ メッセージの形式と、リモート管理およびモニタ ツールについても説明します。

この章では、ロギング コマンドおよびオプション全体についての総合的な説明は行いません。詳細な説明と、その他のロギング コマンドについては、『*Cisco Security Appliance Command Reference*』を参照してください。

ここでは、次の項目について説明します。

ロギングの概要

システム メッセージ ロギング機能は、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に関するロギング情報を表示します。ロギング設定は非常に柔軟性があり、セキュリティ アプライアンスのメッセージ処理をさまざまな局面でカスタマイズできます。

システム メッセージのロギング機能を使用すると、次の処理が可能になります。

- ログに記録するメッセージの指定。
- メッセージの重大度のディセーブル化または変更。
- メッセージの送信先（複数も可）の指定。たとえば、コンソール、内部バッファ、1 つまたは複数の syslog サーバ、ASDM、SNMP 管理ステーション、特定の電子メール アドレス、Telnet セッション、SSH セッションを指定できます。
- グループ（重大度やメッセージ クラスによる）でのメッセージの設定および管理。
- バッファがいっぱいになり、バッファ ラップが発生した場合の、内部バッファの内容の処理方法の設定。バッファの内容を FTP サーバに送信するか、またはフラッシュに保存するかにセキュリティ アプライアンスを設定できます。
- ASDM、Telnet および 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る、リモートでのシステム メッセージのモニタリング。

ロギング コマンドのほとんどは、設定モードで入力されます。設定モードにするには、**configure terminal** コマンドを入力します。

セキュリティ アプライアンスによって生成されたログを表示するには、出力先を設定する必要があります。送信するメッセージは全部か、または一部か、出力先は全部か、または任意の箇所かという選択ができます。メッセージの重大度によって、メッセージのクラスによって、またはメッセージ リストを作成することによって、送信するメッセージとその送信先を限定することができます。メッセージ リストを作成すると、送信する複数のメッセージに対してシステム ログ メッセージ宛先を 1 つでも複数でも自由に指定できます。

多くのロギング コマンドでは、コマンドを適用するメッセージを特定するために、重大度しきい値を指定する必要があります。重大度の値は 0 から 7 で、レベル番号が小さいほど重大なエラーとなります。重大度は数値またはキーワードで指定します（表 1-6 を参照）。レベルを指定すると、セキュリティ アプライアンスによってコマンドがそのレベル以下のメッセージに適用されます。たとえば、重大度 3 を指定するコマンドを入力すると、そのコマンドの結果は重大度 1、2、および 3 のメッセージに適用されます。

（注） セキュリティ アプライアンスでは、重大度が 0（emergencies）のメッセージは生成されません。このレベルは、UNIX システム ログ メッセージ機能との互換性のために、**logging** コマンドで指定できますが、セキュリティ アプライアンスでは使用されません。

一部のログおよびロギング コマンドでは、**format emblem** オプションをサポートします。EMBLEM システム ログ メッセージの形式は、Cisco IOS ソフトウェア フォーマットと整合するように設計されており、CiscoWorks 管理アプリケーションとも互換性があります。

（注） システム　メッセージはすべてがエラー状態を示すわけではありません。正常なイベントを報告したり、設定変更をログに記録したりするだけのメッセージもあります。

基本ロギング コマンド

ロギング コマンドの一般的な使用方法には、ロギングの開始、ロギングの停止、メッセージの重大度の変更、メッセージのディセーブル化、および設定変更の復元などがあります。ここでは、次の項目について説明します。

ロギングのイネーブル化およびディセーブル化

次のコマンドは、ロギングをイネーブルにするため、ログを表示するため、およびコンフィギュレーション設定値を表示するために使用します。

目的	コマンド	説明
ロギングのイネーブル化およびディセーブル化	**logging enable**	すべての出力先へのシステム ログ メッセージの送信をイネーブルにします。 ログを表示するには、ロギングの出力先を設定する必要があります。 （注）　**logging on** コマンドは、下位互換性のためにそのままサポートされています。
	no logging enable	すべての出力先へのロギングをディセーブルにします。
ログおよびコンフィギュレーション設定値の表示	**show logging**	システム ログ メッセージ バッファの内容と現在のロギング設定をリストで表示します。 （注）　システム ログ メッセージ バッファの内容を表示できるようにするには、まずバッファ出力先を設定する必要があります。 詳細については、P.1-8 の「ロギング バッファの設定および管理」を参照してください。

重大度の変更またはメッセージのディセーブル化

次のコマンドは、個々のメッセージの重大度を変更するため、および個々のメッセージをディセーブルにするために使用します。重大度の表は、P.1-22 の「重大度」を参照してください。

目的	コマンドの構文	説明
メッセージの重大度の変更	**logging message** *message_number* **level** *severity_level* **no logging message** *message_number* **level** *severity_level*	特定のシステム ログ メッセージの重大度を設定します。
	show logging message	デフォルトの設定が修正されたシステム ログ メッセージ（異なる重大度が割り当てられたメッセージおよびディセーブルにされたメッセージ）のリストを表示します。
	clear config logging level	すべてのロギング重大度の変更をデフォルトにリセットします。
メッセージのディセーブル化	**no logging message** *message_number*	特定のシステム ログ メッセージをディセーブルにします。
	logging message *message_number*	ディセーブル状態のメッセージのロギングを再開します。
	show logging message	デフォルトの設定が修正されたシステム ログ メッセージ（異なる重大度が割り当てられたメッセージおよびディセーブルにされたメッセージ）のリストを表示します。
	clear config logging disabled	以前にディセーブルにされたメッセージすべてのロギングを再度イネーブルにします。

コンフィギュレーション設定値のデフォルト値への復元

次のコマンドは、すべての設定オプションをそれぞれのデフォルト値にリセットするために使用します。

目的	コマンドの構文	説明
ロギング コンフィギュレーション設定値のデフォルト値への復元	**clear configure logging**	すべてのロギング コンフィギュレーション設定値をそれぞれのデフォルト値に戻します。このコマンドは、すべてのコンフィギュレーション設定値、たとえば、メッセージ重大度の変更、ディセーブル状態のメッセージ、バッファ ラップ オプション、およびフラッシュ オプションに影響を与えます。

システム ログ メッセージ出力先の指定および管理

セキュリティ アプライアンスは、システム ログ メッセージをさまざまな出力先に送信するように設定できます。また、個々のシステム ログ メッセージまたはメッセージ グループを指定して、送信するシステム ログ メッセージとその出力先を限定することもできます。

出力先には、次のものがあります。

- 内部バッファ
- 1 つまたは複数の syslog サーバ
- 1 つまたは複数の電子メール宛先
- ASDM (Adaptive Security Device Manager)
- Telnet および SSH セッション
- コンソール
- SNMP 管理ステーション

ここでは、次の項目について説明します。

出力先を設定および管理するコマンド

次のコマンドは、セキュリティ アプライアンスが送信するシステム ログ メッセージの出力先を指定するために使用します。

表 1-1　ログ出力先を設定するコマンド

出力先	コマンドの構文	説明
内部バッファ	**logging buffered** *message_list*|*severity_level* **no logging buffered** *message_list*|*severity_level*	システム ログ メッセージを内部バッファに保存します。バッファに送信するメッセージは、*message_list* 変数および *severity_level* 変数で限定できます。 **show logging** コマンドを使用してバッファの内容を表示します。 内部バッファを設定および管理するときに使用するコマンドの詳細については、P.1-8 の「ロギング バッファの設定および管理」を参照してください。

表 1-1　ログ出力先を設定するコマンド（続き）

出力先	コマンドの構文	説明
システム ログ メッセージ サーバ	**logging host** *interface_name ip_address* **[tcp**[*/port*] | **udp**[*/port*]] **[format emblem]** **no logging host** *interface_name ip_address* **[tcp**[*/port*] | **udp**[*/port]*] **[format emblem]**	システム ログ メッセージを受信するホストを指定します（syslog サーバ）。セキュリティ アプライアンスは、UDP または TCP でメッセージを送信します。デフォルトのプロトコルおよびポートは UDP/514 です。デフォルト TCP ポート（指定されている場合）は 1468 です。**format emblem** オプションによって EMBLEM フォーマット設定がイネーブルにされます（UDP のみ）。
	logging trap *message_list*|*severity_level* **no logging trap** *message_list*|*severity_level*	システム ログ メッセージを syslog サーバに送信できるようにします（サーバを識別するには **logging host** コマンドを参照）。 *severity_level* を 1 から 7 に設定するか、または重大度名を入力します。*message_list* 変数で送信されるメッセージを指定することもできます。
	logging facility *number* **no logging facility** *number*	syslog サーバのロギング ファシリティを設定します。デフォルトは 20 です。
電子メール アドレス	**logging mail** *message_list*|*severity_level* **no logging mail** *message_list*|*severity_level*	システム ログ メッセージを 1 つまたは複数の電子メール受信側に送信することを指定します。送信するシステム ログ メッセージを指定するには、*message_list* 変数または *severity_level* 変数を使用します。
	logging recipient-address **no logging recipient-address**	システム ログ メッセージを電子メール宛先に送信する場合に使用する受信側電子メール アドレスを指定します。最大 5 つの受信側アドレスが設定できます。受信側はそれぞれ新規コマンド エントリで指定します。
	logging from-address **no logging from-address**	システム ログ メッセージを電子メール宛先に送信する場合に使用する送信元電子メール アドレス。
コンソール	**logging console** *message_list* | *severity_level* **no logging console** *message_list* | *severity_level*	システム ログ メッセージが、発生したときにセキュリティ アプライアンス コンソール（tty）に表示されるようにします。 *severity_level* を 1 から 7 に設定するか、または重大度名を使用します。*message_list* 変数で送信されるメッセージを指定することもできます。 このコマンドは、問題をデバッグしている場合、またはネットワークの負荷が最小の場合に使用します。パフォーマンスを低下させることがあるので、ネットワークの使用率が高いときは使用しないでください。

表 1-1　ログ出力先を設定するコマンド（続き）

出力先	コマンドの構文	説明
コンソールへの Telnet または SSH セッション	**logging monitor** *message_list* | *severity_level* **no logging monitor** *message_list* | *severity_level*	Telnet または SSH でセキュリティ アプライアンスコンソールにアクセスしているときに、システム ログ メッセージが発生した場合、そのメッセージが表示されるようにします。 *severity_level* を 1 から 7 に設定するか、または重大度名を指定します。詳細については、表 1-6 を参照してください。*message_list* 変数で送信されるメッセージを指定することもできます。 Telnet または SSH セッションを使用してメッセージを表示するには、Telnet または SSH セッションを確立し、**logging monitor** コマンドを入力し、次に **terminal monitor** コマンドを入力します。
ASDMASDM	**logging asdm** *message_list*|*severity_level* **no logging asdm** *message_list*|*severity_level*	指定されたメッセージを ASDM に送信します。
	show logging asdm	ASDM システム ログ メッセージ バッファの内容を表示します。
	logging asdm-buffer-size *num_of_messages* **no logging asdm-buffer-size** *num_of_messages*	ASDM システム ログ メッセージ バッファに保存されるメッセージ数を指定します。その後メッセージは ASDM に送信されます。 このコマンドの **no** 形式を使用すると、バッファ サイズがデフォルト値の 100 にリセットされます。
	clear logging asdm	ASDM システム ログ メッセージ バッファをクリアします。
SNMP 管理ステーション	**logging history** *message_list*|*severity_level* **no logging history** *message_list*|*severity_level*	SNMP のシステム ログ メッセージをイネーブルにします。 *severity_level* を 1 から 7 に設定するか、または重大度名を設定します。詳細については、表 1-6 を参照してください。*message_list* 変数で送信されるメッセージを指定することもできます。詳細については、**logging list** コマンドを参照してください。 次のコマンドを使用して、セキュリティ アプライアンスに SNMP をセット アップします。 **snmp-server host** [*if_name*] *ip_addr* **snmp-server location** *text* **snmp-server contact** *text* **snmp-server community** *key* **snmp-server enable** *traps* SNMP コマンドの使用方法の詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

ロギング キューの設定および管理

セキュリティ アプライアンスではメモリに一定数のブロックが設けられており、システム ログ メッセージのバッファ用に割り当てることができます。必要なブロック数は、メッセージ キューの長さ、および指定された syslog ホスト数によって決まります。

次のコマンドは、処理を待機する間に、ロギング キューに保存できるメッセージ数を変更するために使用します。

目的	コマンドの構文	説明
ロギング キューのサイズの変更	**logging queue** *msg_count* **no logging queue** *msg_count*	処理を待機する間に、メッセージ キューに保持できるシステム ログ メッセージ数を指定します。デフォルトのメッセージ数は 512 です。メッセージ数を制限しないと指定するには、0（ゼロ）を設定します。
キュー統計情報の表示	**show logging queue**	次のコマンドは、キュー統計情報を表示するために使用します。

ロギング バッファの設定および管理

ロギング メッセージをセキュリティ アプライアンスで内部に保存するには、出力先として内部バッファを指定する必要があります。

セキュリティ アプライアンスに次の設定を行うには、次のコマンドを使用します。

- syslog を内部でバッファに保存。
- バッファのサイズを指定。
- 内部バッファがラップするとき（つまり、バッファがいっぱいのとき）、セキュリティ アプライアンスが内部バッファの内容を処理する方法の指定。内部バッファの内容は、フラッシュまたは FTP サーバに保存できます。

表 1-2　ロギング バッファを設定するコマンド

目的	コマンドの構文	説明
システム ログ メッセージのバッファへの保存を指定	**logging buffered** *message_list*| *severity_level* **no logging buffered** *message_list*| *severity_level*	システム ログ メッセージを内部バッファに保存します。 特定タイプのメッセージのみを内部バッファに保存する場合は、*message_list* オプションまたは *severity_level* オプションを使用します。
ロギング バッファの内容の消去	**clear logging buffer**	バッファの内容を消去します。

表 1-2　ロギング バッファを設定するコマンド（続き）

目的	コマンドの構文	説明
使用するフラッシュ量の指定	**logging flash-minimum-free** *kbytes* **no logging flash-minimum-free** *kbytes* **logging flash- maximum-allocation** *kbytes* **no logging flash- maximum-allocation** *kbytes*	システム ログ メッセージを保存するためにロギング コマンドで使用できるフラッシュ量を指定します。このコマンドは、**logging flash-bufferwrap** コマンドおよび **logging-savelog** コマンドに適用されます。 **flash-minimum-free** オプションは、常に利用できるように空けておく最小フラッシュ領域量を指定する（KB 単位）ために使用します。 **flash-maximum-allocation** オプションは、システム ログ メッセージの保存に使用できる最大フラッシュ領域量を指定する（KB 単位）ために使用します。 （注）　**logging flash** に関連するコマンドは、単一モードの場合のみ有効です。
バッファ ラップをフラッシュに保存	**logging flash-bufferwrap** **no logging flash-bufferwrap**	イネーブル状態の場合、バッファ ラップ（つまり、バッファがいっぱい）のとき、バッファの内容がフラッシュに保存されます。
現行バッファ内容のフラッシュへの保存	**logging savelog** *filename*	システム ログ メッセージ バッファの内容を、指定されたファイル名のファイルで、フラッシュに保存します。 ファイル名が指定されていない場合、デフォルトのタイムスタンプ形式がファイル名に使用されます。 このコマンドは、特権 EXEC モード コマンドです。
バッファ ラップの FTP サーバへの送信	**logging ftp-bufferwrap** **no logging ftp-bufferwrap**	メッセージ バッファがいっぱいの場合、バッファの内容が設定された FTP サーバに送信されます。 **logging ftp-server** コマンドで FTP サーバを設定します。
	logging ftp-server *ftp_server path username password* **no logging ftp-server** *ftp_server path username password*	FTP サーバを設定します。FTP サーバについての必要な情報を指定するには、次に示すオプションを使用します。 • *ftp-server*：外部 FTP サーバ名または IP アドレス。 • *path*：システム ログ メッセージを保存する FTP サーバ上のディレクトリ パス。 • *username*：FTP サーバへのユーザ ログイン。 • *password*：username のパスワード。

メッセージのグループの管理

セキュリティ アプライアンスには、システム ログ メッセージをグループとして設定および管理できるようにするメカニズムがいくつか用意されています。このメカニズムには、メッセージ重大度、メッセージ クラス（メッセージ ソース）、または作成するカスタム メッセージが含まれます。このメカニズムを使用すると、1 つのコマンドを入力して、小規模メッセージ グループにも大規模メッセージ グループにも適用することが入力できます。

次にメッセージ グループの管理の例をいくつか示します。

- 重大度 1、2、および 3 のメッセージすべてを内部バッファにロギングする。
- 「ha」クラスのメッセージすべてを特定の syslog サーバに送信する。
- 「high-priority」という名前のメッセージ リストを作成し、そのリストにあるメッセージを電子メール アドレスに送信して、システム管理者に問題を通知する。

logging class コマンドを使用すると、あるカテゴリのシステム メッセージ全体の出力先を 1 つのコマンドで指定できます。クラスは、セキュリティ アプライアンスの機能エリアに関連付けられているメッセージのカテゴリです。たとえば、「vpnc」クラスは VPN クライアントを示します。

1 つのコマンドを入力して、関連する機能エリアに関連付けられているメッセージすべてにそのコマンドを適用する場合は、*message_class* 変数を使用します。

メッセージ ID 番号は、メッセージ番号の最初の 3 桁で参照されます。たとえば、611 には番号 611101 から 611323 までのシステム メッセージすべてが含まれます。このメッセージのグループは、vpnc （VPN クライアント）クラスに関連付けられています。

次のコマンドは、メッセージ リストを作成するため、および複数のメッセージ グループを 1 つの出力先に送信するために使用します。

表 1-3　メッセージのグループを管理するコマンド

コマンド / オプション	構文	説明
logging list	**logging list** *message_list* **level** *severity_level* [**class** *message_class*] **no logging list** *message_list* **level** *severity_level* [**class** *message_class*]	カスタムのメッセージ リストを作成します。*message_list* は、作成するリストを識別するために選定する名前です。 **（注）** メッセージ　リストの名前に重大度の名前を使用しないでください。*message_list* 名には、「emergencies」、「alert」、「critical」、「error」、「warning」、「notification」、「informational」、および「debugging」は使用できません。 これらの単語は、最初の 3 文字でも、ファイル名の先頭には使用しないでください。たとえば、「err」で始まるファイル名は使用しないでください。
	logging list *message_list* **level** *severity_level* [**class** *message_class*] **no logging list** *message_list* **level** *severity_level* [**class** *message_class*]	この構文オプションは、指定された重大度を持つ特定のクラス内のメッセージすべてを含むメッセージ リストを作成するために使用します。
	logging list *message_list* **message** *syslog_id* - [*syslog_id2*] **no logging list** *message_list* **message** *syslog_id - [syslog_id2]*	この構文オプションは、ある範囲のメッセージ ID 番号を含むメッセージ リストを作成するために使用します。

表 1-3　メッセージのグループを管理するコマンド（続き）

コマンド / オプション	構文	説明
ロギング クラス	**logging class** *message_class* **buffered** | **console** | **history** | **mail** | **monitor** |**trap** | *severity_level* **no logging class** *message_class* **buffered** | **console** | **history** | **mail** | **monitor** |**trap** | *severity_level*	そのクラスに関連するメッセージすべてを指定された出力先に送信します。出力先に送信するメッセージ数をさらに限定するには、重大度しきい値を指定します。

メッセージ クラス変数の値

表 1-4 に、メッセージ クラスと各クラスのメッセージ ID 範囲をリストで示しています。

表 1-4　メッセージ クラスと関連メッセージ ID 番号

クラス	定義	メッセージ 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	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 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

システム ログ メッセージの内容および形式の修正

次のコマンドは、次の処理を行うようにセキュリティ アプライアンスを設定するために使用します。

- すべてのシステム ログ メッセージにデバイス ID を含める。
- すべてのシステム ログ メッセージにタイムスタンプを含める。
- システム ログ メッセージに EMBLEM フォーマットを使用する。

表 1-5　メッセージの内容および形式を修正するコマンド

目的	コマンドの構文	説明
システム ログ メッセージにデバイス ID を含める	**logging device-id {hostname | ipaddress** *if_name* **| string** *text*} **no logging device-id {hostname | ipaddress** *if_name* **| string** *text*}	イネーブル状態の場合、セキュリティ アプライアンスは、EMBLEM フォーマットでないシステム ログ メッセージすべてにデバイス ID を表示します。 **ipaddress** オプションを使用すると、デバイス ID は、メッセージが送信されたインターフェイスに関係なく、指定したセキュリティ アプライアンスインターフェイスの IP アドレスとなります。このオプションの使用により、そのデバイスから送信されるメッセージすべてに、1 つの同じデバイス ID が割り当てられます。 **（注）** イネーブル状態の場合、デバイス ID は EMBLEM フォーマットのメッセージまたは SNMP トラップには表示されません。
システム ログ メッセージにタイムスタンプを含める	**logging timestamp** **no logging timestamp**	イネーブル状態の場合、セキュリティ アプライアンスはすべてのシステム ログ メッセージにタイムスタンプを表示します。
EMBLEM フォーマットを使用するようにシステム ログ メッセージを修正	**logging emblem** **no logging emblem**	イネーブル状態の場合、システム ログ メッセージが EMBLEM フォーマットで表示されます。 **（注）** このコマンドは、syslog ホストに送信されるシステム ログ メッセージには影響しません。ホスト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、**logging host** コマンドを使用します。

ロギング コマンド例

ここでは、**logging** コマンドの使用方法を示す例をステップごとに説明します。ここでは、次の項目について説明します。

ロギングのイネーブル化

次の手順ではロギングをイネーブルにしますが、ログ メッセージを表示するには出力先も指定する必要があります。詳細については、P.1-15 の「システム ログ メッセージの出力先の設定」を参照してください。

ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　コンフィギュレーション モードを表示するには、次のコマンドを入力します。

```
enable
(Enter your password at the prompt)
configure terminal
```

ステップ 2　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。

```
logging enable
```

ステップ 3　ロギング レベルを変更するには、次のコマンドを入力します。

logging *output_destination severity_level* (1-7)

有効な *output_destination* 値は、**asdm**、**console**、**buffered**、**history**、**mail**、**monitor**、および **trap** です。

ステップ 4　ロギング設定を表示するには、次のコマンドを入力します。

```
show all
```

ロギング出力のテスト

ステップ 1　コンフィギュレーション モードを表示するには、次のコマンドを入力します。

```
enable
(Enter your password at the prompt)
configure terminal
```

ステップ 2　コンソールへのログ メッセージの送信を開始するには、次のコマンドを入力します。

```
logging console 7
quit
```

このテストでは、次のシステム ログ メッセージが生成されます。

```
111005: End configuration: OK
```

このメッセージは、コンフィギュレーション モードを終了したことを示しています。「111005」はメッセージ ID 番号です（このメッセージの詳細については、第 2 章「システム ログ メッセージ」を参照してください）。

ステップ 3　コンソール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。

```
configure terminal
no logging console 7
quit
```

（注）　テストには、**logging console** コマンドのみを使用してください。進行中のシステム ログ メッセージの出力先にコンソールを使用すると、システム パフォーマンスが低下することがあります。セキュリティ アプライアンスが実際の動作環境にある場合、メッセージの保存には **logging buffered** コマンド、メッセージの表示には **show logging** コマンド、**logging buffered** コマンドで表示されたメッセージの消去には **clear logging buffer** コマンドのみを使用してください。

システム ログ メッセージの出力先の設定

ここでは、システム ログ メッセージを任意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方法について説明します。セキュリティ アプライアンスには、次のように、システム ログ メッセージを送信する出力先がいくつか用意されています。

- 内部バッファ
- 1 つまたは複数の syslog サーバ
- 1 つまたは複数の電子メール アドレス
- ASDM （Monitoring タブを使用）
- SNMP 管理ステーション
- Telnet および SSH セッション
- tty コンソール

ここでは、次の項目について説明します。

システム ログ メッセージのバッファへの送信

システム ログ メッセージをバッファに送信するには、次の手順を実行します。次の例では、バッファに送信する複数のメッセージを指定するプロセスを簡単にするために、まずメッセージ リストを作成します。

ステップ 1　指定の重大度を持つメッセージまたはメッセージ　クラスを含むメッセージ　リストを作成するには、次のコマンドを入力します。

logging list *message_list* | **level** *severity_level* [**class** *message_class*]

ここで、*message_list* は作成するファイルの名前、*severity_level* はリストに含めるメッセージの重大度、*message_class* はリストに含めるメッセージのカテゴリです。

次に例を示します。

```
logging list my_critical_messages level 2
```

（注）　メッセージ リストのファイル名に重大度の名前を使用しないでください。

ステップ 2　作成したメッセージ リストにメッセージを追加するには、次のコマンドを入力します。

logging list *message_list* **message** *syslog_id-syslog_id2*

ここで、*message_list*　　は、修正するメッセージのリストが格納されているファイル名で、*syslog_id-syslog_id2* はリストに追加するメッセージ ID 番号の範囲です。

次に例を示します。

```
logging list my_critical_messages message 101001-102034
```

ステップ 3　作成したメッセージ リスト内のメッセージをバッファに送信するように指定するには、次のコマンドを入力します。

logging buffered *message_list*

ここで、*message_list* は、バッファに送信するメッセージのリストが格納されているファイル名です。

次に例を示します。

```
logging buffered my_critical_messages
```

システム ログ メッセージの Syslog サーバへの送信

メッセージをホストに送信する場合、メッセージは UDP か TCP を使用して送信されます。ホストでは、syslogd と呼ばれるプログラム（サーバと呼ばれる）が動作している必要があります。UNIX には、オペレーティング システムの一部として syslog サーバが用意されています。Windows 95 または Windows 98 の場合は、別のベンダーから syslog サーバを入手してください。

syslogd の設定手順については、『*Cisco Security Appliance Configuration Guide*』を参照してください。ロギング サーバに、特定のタイプのメッセージが記録された場合に実行するアクションを指定できます。たとえば、電子メールの送信、ログ ファイルへのレコードの保存、またはワークステーションでのメッセージの表示です。

syslog サーバにメッセージ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には、次の手順を実行します。

ステップ 1　メッセージを受信するホストを指定するには、次のコマンドを入力します。

logging host *if_name ip_address* [tcp*[/port]* | **udp**[*/port*]] [**format emblem**]

ここで、*if_name* はホストのインターフェイスの名前、*ip_address* はホストの IP アドレス、*port* はメッセージを送信する TCP または UDP のポート番号です。

次に例を示します。

```
logging host dmz1 192.168.1.5
```

複数のホストを指定できますが、ホストごとに別のコマンドを入力する必要があります。

ステップ 2　ロギング レベルを設定するには、次のコマンドを入力します。

```
logging trap severity_level (1-7)
```

ここで、*severity_level* は送信するメッセージの重大度です。

debugging (7) レベルを使用するのは、初期セットアップ時とテスト時だけにしてください。セットアップまたはテストの終了後は、レベルを **debugging** から **errors (3)** に変更して、実際の動作環境に移行してください。

ステップ 3　各メッセージにデバイス ID を含める場合は、次のコマンドを入力します。

```
logging device-id {hostname | ipaddress if_name | string text}
```

メッセージには、syslog サーバに送信されたメッセージに指定されたデバイス ID （指定されたインターフェイスのホスト名および IP アドレスまたは文字列のいずれか）が含まれています。

ステップ 4　必要に応じて、ロギング ファシリティにデフォルトの 20 以外の値を設定します。UNIX システムのほとんどは、ファシリティ 20 でメッセージが到着することを期待します。ロギング ファシリティを設定するには、次のコマンドを入力します。

```
logging facility number
```

システム ログ メッセージの電子メール アドレスへの送信

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には、次の手順を実行します。

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メッセージを指定します。メッセージ重大度変数またはメッセージ リスト変数を使用して、送信するメッセージを指定します。

この例では、前に **logging list** コマンドでセット アップした「high-priority」という名前を *message_list* に使用します。

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。

```
logging mail message_list|severity_level level
```

次に例を示します。

```
logging mail high-priority
```

ステップ 2　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場合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。

```
logging from-address email_address
```

次に例を示します。

```
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宛先に送信する場合に使用する受信側電子メール アドレスを指定します。最大 5 つの受信側アドレスが設定できます。各受信側は別々に入力する必要があります。

受信側アドレスを指定するには、次のコマンドを入力します。

logging recipient-address *e-mail_address* [**level** *severity_level*]

次に例を示します。

```
logging recipient-address admin@example.com
```

（注）　重大度が指定されていない場合、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　システム ログ メッセージを電子メール宛先に送信する場合に使用する SMTP サーバを指定するには、次のコマンドを入力します。

smtp-server *hostname*

次に例を示します。

```
smtp-server smtp-host-1
```

システム ログ メッセージの Telnet コンソール セッションへの送信

Telnet コンソール セッションでシステム ログ メッセージを表示するには、次の手順を実行します。

ステップ 1　まだ設定していない場合は、内部インターフェイスのホストがセキュリティ アプライアンスにアクセスできるように、セキュリティ アプライアンスを設定します。

a. 次のコマンドを入力します。

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、コマンドは次のとおりです。

```
telnet 192.168.1.2 255.255.255.255
```

b. セキュリティ アプライアンスがセッションを切断するまでの Telnet セッションのアイドル状態の許容時間を、デフォルトの 5 分より長い値に設定する必要もあります。適切な値は、短くても 15 分です。Telnet セッションのこの時間を設定するには、次のコマンドを入力します。

```
telnet timeout 15
```

ステップ 2　ホストで Telnet を開始して、セキュリティ アプライアンスの内部インターフェイスを指定します。

Telnet で接続ができると、セキュリティ アプライアンスによって `passwd:` というプロンプトが表示されます。

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

ステップ 4　コンフィギュレーション モードを表示するには、次のコマンドを入力します。

```
enable
(Enter your password at the prompt)
configure terminal
```

ステップ 5　メッセージ ロギングを開始するには、次のコマンドを入力します。

logging monitor *severity_level* (1-7)

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

```
terminal monitor
```

このコマンドでは、現在の Telnet セッションに対してのみロギングがイネーブルにされます。**logging monitor** コマンドでは、すべての Telnet セッションに対してロギング プリファレンスが設定され、一方 **terminal monitor**（および **terminal no monitor**）コマンドでは、個々の Telnet セッションそれぞれに対してのロギングが制御されます。

ステップ 7　ホストを ping するかまたは Web ブラウザを開始して、いくつかのメッセージを起動します。システム ログ メッセージが Telnet セッション ウィンドウに表示されます。

ステップ 8　完了した場合、この機能を次のコマンドでディセーブルにします。

```
terminal no monitor
no logging monitor
```

システム ログ メッセージの SNMP 管理ステーションへの送信

ここでは、システム ログ メッセージを SNMP 管理ステーション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方法について説明します。次の項目について説明します。

SNMP 要求の受信

SNMP 管理ステーション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するには、次の手順を実行します。

ステップ 1　SNMP 管理ステーションの IP アドレスを設定するには、次のコマンドを入力します。

```
snmp-server host [if_name] ip_addr
```

ステップ 2　必要に応じて、次のコマンドでその他の snmp サーバ設定を指定します。

```
snmp-server location text
snmp-server contact text
snmp-server community key
```

詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

SNMP トラップの送信

セキュリティ アプライアンスから SNMP 管理ステーションにログ メッセージをトラップとして送信するには、次の手順を実行します。コールド スタート、リンク アップ、およびリンク ダウンの総称トラップは、すでに「SNMP 要求の受信」手順によってイネーブルにされています。

ステップ 1　SNMP トラップをイネーブルにするには、次のコマンドを入力します。

```
snmp-server enable traps
```

ステップ 2　ロギング レベルを設定するには、次のコマンドを入力します。

```
logging history severity_level (1-7)
```

debugging (7) レベルを使用するのは、初期セットアップ時とテスト時だけにしてください。セットアップまたはテストの終了後は、レベルを **debugging** からそれより低い値に変更して、実際の動作環境に移行してください。

ステップ 3　システム ログ メッセージのトラップの送信をディセーブルにするには、次のコマンドを入力します。

```
no snmp-server enable traps
```

特定のシステム ログ メッセージのディセーブル化およびイネーブル化

ここでは、システム ログ メッセージのディセーブル化および再イネーブル化の方法、およびディセーブル状態のシステム ログ メッセージの表示方法について説明します。ここでは、次の項目について説明します。

特定のシステム ログ メッセージのディセーブル化

特定のシステム ログ メッセージをディセーブルにするには、次のコマンドを入力します。

no logging message *message_number*

ここで、*message_number* はディセーブルにする特定のメッセージです。

ディセーブル状態のシステム ログ メッセージのリストの表示

ディセーブル状態のシステム 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。

show logging message

ディセーブル状態の特定システム ログ メッセージの再イネーブル化

ディセーブル状態のシステム 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。

logging message *message_number*

ここで、*message_number* は再イネーブル化する特定のメッセージです。

ディセーブル状態のシステム ログ メッセージすべての再イネーブル化

ディセーブル状態のシステム ログ メッセージをすべて再イネーブル化するには、次のコマンドを入力します。

clear config logging disabled

ログ メッセージの概要

ここでは、セキュリティ アプライアンスのシステム ログ メッセージの内容を説明します。ここでは、次の項目について説明します。

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（%）で始まり、次のような構造になっています。

%PIX|ASA-*Level*-*Message_number*: *Message_text*

次の説明を参照してください。

PIX|ASA	セキュリティ アプライアンスによって生成されたメッセージのメッセージ ファシリティ コードを識別します。この値は常に PIX|ASA です。
Level	1 ～ 7。レベルは、メッセージに記述された状態の重大度が反映されます。数値が小さいほど、重大度が高くなります。詳細については、表 1-6 を参照してください。
Message_number	メッセージを識別する固有の 6 桁の番号。
Message_text	状態を記述するテキスト文字列。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ることがあります。表 1-7 に、変数フィールドとその情報のタイプをリストで示しています。

（注）　セキュリティ アプライアンス シリアル コンソールで受信するシステム ログ メッセージには、メッセージのコード部分のみが含まれています。第 2 章「システム ログ メッセージ」のメッセージの説明には、重大度も記載されています。

重大度

表 1-6 に重大度をリストで示しています。

表 1-6　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。
1	**alert**	ただちに処置が必要。
2	**critical**	クリティカルな状態。
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**	情報メッセージのみ。
7	**debugging**	デバッグ中にのみ表示される。

付録 A「重大度別メッセージ リスト」に、各重大度で発生するメッセージをリストで示しています。

（注）　セキュリティ アプライアンスでは、重大度が 0（emergencies）のメッセージは生成されません。このレベルは、UNIX システム ログ メッセージ機能との互換性のために、**logging** コマンドで指定できますが、セキュリティ アプライアンスでは使用されません。

変数

ログ メッセージには変数が含まれていることがよくあります。表 1-7 に、ログ メッセージの説明のためにこのマニュアルで使用されている変数のほとんどをリストで示しています。1 つのログ メッセージにしか現れない変数の中には省略したものがあります。

表 1-7　システム ログ メッセージ内の変数フィールド

変数	情報のタイプ
acl_ID	ACL 名。
bytes	バイト数。
code	メッセージで返される 10 進数で、メッセージに応じて、エラーの原因または発生源を示します。
command	コマンド名。
command_modifier	*command_modifier* は、次の文字列のいずれかです。 • cmd （この文字列は、コマンドに修飾子がないことを意味します）。 • clear • なし • show
connections	接続数。
connection_type	接続タイプは次のとおりです。 • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • Via UDP • Route • 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 デバイス。たとえば、フロッピーディスク、フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末です。
econns	初期接続数。
elimit	**static** コマンドまたは **nat** コマンドで指定された初期接続数。

表 1-7　システム ログ メッセージ内の変数フィールド（続き）

変数	情報のタイプ
filename	セキュリティ アプライアンス イメージ、PDM ファイル、またはコンフィギュレーションの各タイプのファイル名。
ftp-server	外部 FTP サーバ名または IP アドレス。
gateway_address	ネットワーク ゲートウェイ IP アドレス。
global_address	グローバル IP アドレス。低セキュリティ レベル インターフェイス上のアドレス。
global_port	グローバル ポート番号。
hex	16 進数。
inside_address	内部（つまり、ローカル）IP アドレス。高セキュリティ レベル インターフェイス上のアドレス。
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 から 255 までの整数です。
MAC_address	MAC アドレス。
mapped_address	変換済み IP アドレス。
mapped_port	変換済みポート番号。
message_class	セキュリティ アプライアンスの機能エリアに関連付けられたメッセージのカテゴリ。
message_list	メッセージ ID 番号、メッセージ クラス、またはメッセージ重大度のリストを含む作成ファイルの名前。
message_number	メッセージ ID 番号。
nconns	static テーブルまたは xlate テーブルに許可された接続数。
netmask	サブネット マスク。
number	数。正確な形式は、ログ メッセージによって決まります。
octal	8 進数。
outside_address	外側（つまり、外部）IP アドレス。通常は、外部ルータの先のネットワークにある低セキュリティ レベル インターフェイス上のホストのアドレス。
outside_port	外部ポート番号。
port	TCP または UDP ポート番号。
privilege_level	ユーザ特権レベル。
protocol	パケットのプロトコル。たとえば、ICMP、TCP、または UDP。
real_address	Network Address Translation（NAT; ネットワーク アドレス変換）前の実 IP アドレス。
real_port	NAT 前の実ポート番号。
reason	メッセージの理由を記述するテキスト文字列。
service	パケットで指定されたサービス。たとえば、SNMP または Telnet。
severity_level	メッセージの重大度。
source_address	パケットのソース アドレス。
source_port	ソース ポート番号。
string	テキスト文字列（たとえば、ユーザ名）。

表 1-7　システム ログ メッセージ内の変数フィールド（続き）

変数	情報のタイプ
tcp_flags	TCP ヘッダー内のフラグ。たとえば、次に示すものです。 • ACK • FIN • PSH • RST • SYN • URG
time	*hh*:*mm*:*ss* 形式の時間。
url	URL。
user	ユーザ名。

他のリモート管理ツールおよびモニタ ツール

この項で説明するセキュリティ アプライアンスのオプションは、コマンド ライン以外のツールを使用して、リモートでセキュリティ アプライアンスをモニタするためのものです。ここでは、次の項目について説明します。

Cisco ASDM

Cisco Adaptive Security Device Manager （ASDM）は、ブラウザ ベースの設定ツールで、セキュリティ アプライアンスをグラフィックスを使用してセット アップ、設定、およびモニタできるように設計されており、セキュリティ アプライアンス コマンドライン インターフェイス（CLI）の詳しい知識は必要ありません。

Cisco Secure Policy Manager

Cisco Secure Policy Manager （CSPM）はセキュリティ ポリシー管理システムで、これを使用すると中心部からネットワーク全体のセキュリティ ポリシーを定義、配布、適用、および監査できます。CSPM により、境界アクセス コントロール、NAT、IDS、および IPSec ベース VPN などの複雑なネットワーク セキュリティ イベントの管理タスクが合理化されます。CSPM には、モニタ、イベント通知、および Web ベース レポート機能などのシステム監査機能が用意されています。

CSPM は、セキュリティ アプライアンスからシステム ログ メッセージを受信して、電子メール、ポケットベル、およびスクリプトなどの通知を指定された syslog に送ることができます。また、CSPM には、上位 10 ユーザや上位 10 Web サイトなどの syslog レポートも提供します。このレポートは、オンデマンドとスケジュール処理の両方で作成できます。レポートは、電子メールで送信することも、SSL 対応 Web ブラウザを使ってリモートで表示することもできます。

詳細については、次の Web サイトを参照してください。

http://www.cisco.com/go/policymanager

http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/index.htm

SNMP トラップ

セキュリティ アプライアンスのイベントは、SNMP を使用して報告できます。この機能を使用するには、Cisco SYSLOG MIB と Cisco SMI MIB を SNMP 管理ステーションにロードする必要があります。

Telnet

内部ホストから Telnet を使用して、セキュリティ アプライアンスにログインし、システムのステータスをモニタできます。IPSec がイネーブル状態の場合、外部ホストからコンソールにアクセスすることもできます。Telnet から **debug icmp trace** コマンドおよび **debug sqlnet** コマンドを使用して、ICMP （ping）トレースおよび SQL*Net アクセスを表示することができます。

Telnet コンソール セッションを使用すると、**logging monitor** コマンドおよび **terminal monitor** コマンドを使用してシステム ログ メッセージを表示することもできます（P.1-18 の「システム ログ メッセージの Telnet コンソール セッションへの送信」を参照）。