ロギングの設定

この章では、ASA および ASASM のログを設定して管理する方法について説明します。次の項目を取り上げます。

ロギングに関する情報

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、ログの保護された長期ストレージを提供します。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

ASA のシステム ログにより、ASA 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して、次の操作を実行できます。

- ログに記録する syslog メッセージを指定する。
- syslog メッセージの重大度をディセーブルにする、または変更する。
- syslog メッセージの送信場所を 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。
- syslog 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。
- syslog の生成にレート制限を適用するかどうかを指定する。
- 内部ログ バッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュ メモリに保存する）を指定する。

- 場所、重大度、クラス、またはカスタム メッセージ リストを基準に syslog メッセージをフィルタリングする。

この項は、次の内容で構成されています。

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 コンテキストまたは管理コンテキストにログインし、他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メッセージだけです。

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

ASA および ASASM 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。

syslog メッセージの分析

次に、さまざまな syslog メッセージを確認することで取得できる情報タイプの例を示します。

- ASA および ASASM のセキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA および ASASM のセキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA または ASA サービス モジュールに対して発生している攻撃が表示されます。
- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザ認証とコマンドの使用により、セキュリティ ポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。

- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

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

```
%ASA Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

ASA	ASA および ASASM が生成するメッセージの syslog メッセージ ファシリティ コード。この値は常に ASA です。
Level	1 ～ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。詳細については、表 36-1 を参照してください。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。

重大度

表 36-1 に、syslog メッセージの重大度の一覧を示します。ASDM ログ ビューアで重大度を区別しやすくするために、重大度のそれぞれにカスタム カラーを割り当てることができます。syslog メッセージの色の設定を行うには、[Tools] > [Preferences] > [Syslog] タブを選択するか、ログ ビューアで、ツールバーの [Color Settings] をクリックします。

表 36-1　syslog メッセージの重大度

レベル番号	重大度	説明
0	**emergencies**	システムを使用できません。
1	**alert**	すぐに措置する必要があります。
2	**critical**	深刻な状況です。
3	**error**	エラー状態です。
4	**warning**	警告状態です。
5	**notification**	正常ですが、注意を必要とする状況です。
6	**informational**	情報メッセージです。
7	**debugging**	デバッグ メッセージです。

（注） ASA および ASASM は、重大度 0（emergencies）の syslog メッセージを生成しません。このレベルは、UNIX の syslog 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、ASA では使用されません。

メッセージ クラスと syslog ID の範囲

各クラスに関連付けられている syslog メッセージ クラスと syslog メッセージ ID の範囲のリストについては、syslog メッセージ ガイドを参照してください。

syslog メッセージのフィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ASA および ASASM を設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

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

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージのクラス（ASA および ASASM の機能領域と同等）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。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 ASA または ASASM を設定することもできます。

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- **logging class** コマンドを使用して、syslog メッセージの 1 つのカテゴリ全体の出力先を指定する。
- **logging list** コマンドを使用して、メッセージ クラスを指定するメッセージ リストを作成する。

syslog メッセージのクラスは、タイプごとに syslog メッセージを分類する方法の 1 つであり、ASA および ASASM 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。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog 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 syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージの生成時にオブジェクトが未知の場合、特定の *heading* = *value* の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*、Username = *user*、IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたは L2L ピアのパブリック IP アドレスです。

カスタム メッセージ リストの使用

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

たとえば、メッセージ リストを使用して次の操作を実行できます。

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

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

クラスタリングの使用

syslog メッセージは、クラスタリング環境でのアカウンティング、モニタリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイムスタンプおよびデバイス ID を含むヘッダー フィールドを制御できます。syslog サーバは、syslog ジェネレータを識別するためにデバイス ID を使用します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

ロギングのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ロギングの前提条件

ロギングには次の前提条件があります。

- syslog サーバは syslogd というサーバ プログラムを実行する必要があります。Windows（Windows 95 および Windows 98 を除く）では、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 の場合は、別のベンダーから syslogd サーバを入手する必要があります。
- ASA または ASASM が生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギン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、ASA および ASASM 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。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数の syslog サーバを指定する場合は、syslog サーバごとに新しいコマンドを入力します。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。
- ASA は、シングル コンテキスト モードの **logging host** コマンドで 16 の syslog サーバの設定をサポートします。マルチ コンテキスト モードでは、この制限はコンテキストごとに 4 台のサーバです。

ロギングの設定

この項では、ロギングを設定する方法について説明します。次の項目を取り上げます。

- 「ロギングのイネーブル化」（P.36-6）
- 「出力先の設定」（P.36-7）

（注） 最小コンフィギュレーションは、ASA および ASASM で syslog メッセージを処理するために実行する操作および要件によって異なります。

ロギングのイネーブル化

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。

コマンド	目的
logging enable **例：** `hostname(config)# logging enable`	ロギングをイネーブルにします。ロギングをディセーブルにするには、**no logging enable** コマンドを入力します。

次の作業

「出力先の設定」（P.36-7）を参照してください。

出力先の設定

トラブルシューティングおよびパフォーマンスのモニタリング用に syslog メッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部 syslog サーバ、ASDM、SNMP 管理ステーション、コンソール ポート、指定した電子メール アドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

この項は、次の内容で構成されています。

外部 syslog サーバへの syslog メッセージの送信

外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

外部 syslog サーバに syslog メッセージを送信するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**logging host** *interface_name syslog_ip* [**tcp**[*/port*] | **udp**[*/port*] [**format emblem**]] **例：** `hostname(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem`	syslog サーバにメッセージを送信するように、ASA および ASASM を設定します。 **format emblem** キーワードは、UDP 限定で syslog サーバでの EMBLEM 形式ロギングをイネーブルにします。*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。*syslog_ip* 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*] キーワードと引数のペアは、ASA および ASASM は、syslog サーバに syslog メッセージを送信するために TCP または UDP を使用する必要があることを指定します。 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 ASA 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。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。 TCP を指定すると、ASA および ASASM は syslog サーバの障害を検出し、セキュリティ保護として、ASA および ASA サービス モジュール を経由する接続をブロックします。TCP syslog サーバへの接続に関係なく新しい接続を許可するには、手順 3 を参照してください。UDP を指定すると、ASA および ASASM は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 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。
ステップ 2	**logging trap** {*severity_level* | *message_list*} **例：** `hostname(config)# logging trap errors`	syslog サーバに送信する syslog メッセージを指定します。重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASA および ASASM は、重大度が 3、2、および 1 の syslog メッセージを送信します。syslog サーバに送信する syslog メッセージを特定したカスタム メッセージ リストを指定することもできます。

	コマンド	目的
ステップ 3	**logging permit-hostdown** **例：** `hostname(config)# logging permit-hostdown`	（任意）TCP 接続された syslog サーバがダウンした場合、新しい接続をブロックする機能をディセーブルにします。ASA または ASASM が syslog メッセージを TCP ベースの syslog サーバに送信するように設定されている場合、および syslog サーバがダウンしているかログ キューがいっぱいの場合、新しい接続はブロックされます。新しい接続は、syslog サーバがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。ログ キューの詳細については、「ロギング キューの設定」（P.36-16）を参照してください。
ステップ 4	**logging facility** *number* **例：** `hostname(config)# logging facility 21`	（任意）ロギング ファシリティを 20 以外の値に設定します。これは、ほとんどの UNIX システムで想定されています。

内部ログ バッファへの syslog メッセージの送信

一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定する必要があります。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、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 ASA および ASASM を設定していない限り、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。syslog メッセージを内部ログ バッファに送信するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**logging buffered** {*severity_level* | *message_list*}
	
	例：
	`hostname(config)# logging buffered critical`
	
	`hostname(config)# logging buffered level 2`
	
	`hostname(config)# logging buffered notif-list`
		一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定します。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とき、つまりバッファ ラップが発生した場合は、ASA および ASASM 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。内部ログ バッファを空にするには、**clear logging buffer** コマンドを入力します。

ステップ 2	**logging buffer-size** *bytes* **例：** `hostname(config)# logging buffer-size 16384`	内部ログ バッファのサイズを変更します。デフォルトのバッファ サイズは 4 KB です。
ステップ 3	次のいずれかのオプションを選択します。	

コマンド	目的
logging flash-bufferwrap **例：** hostname(config)# logging flash-bufferwrap	バッファの内容を別の場所に保存するとき、ASA および ASASM は、次のタイムスタンプ形式を使用する名前でログ 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。 ASA および ASASM は、新しいメッセージを引き続き内部ログ バッファに保存し、いっぱいになったログ 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 ftp-bufferwrap **例：** hostname(config)# logging ftp-bufferwrap	バッファの内容を別の場所に保存するとき、ASA および ASASM は、次のタイムスタンプ形式を使用する名前でログ 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。 ASA および ASASM は、新しいメッセージを引き続き内部ログ バッファに保存し、いっぱいになったログ バッファの内容を FTP サーバに保存します。
logging ftp-server *server path username password* **例：** hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs	ログ バッファの内容を保存する FTP サーバを指定します。*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* 引数は、指定したユーザ名に対するパスワードを示します。
logging savelog [*savefile*] **例：** hostname(config)# logging savelog latest-logfile.txt	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。

電子メール アドレスへの syslog メッセージの送信

syslog 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。

	コマンド	目的
ステップ 1	**logging mail** {*severity_level* | *message_list*} **例：** `hostname(config)# logging mail high-priority`	電子メール アドレスに送信する syslog メッセージを指定します。電子メールで送信される場合、syslog メッセージは電子メール メッセージの件名行に表示されます。このため、このオプションでは、critical、alert、および emergency など、重大度の高い syslog メッセージを管理者に通知するように設定することをお勧めします。
ステップ 2	**logging from-address** *email_address* **例：** `hostname(config)# logging from-address xxx-001@example.com`	電子メール アドレスに syslog 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 アドレスを指定します。
ステップ 3	**logging recipient-address** *e-mail_address [severity_level]* **例：** `hostname(config)# logging recipient-address admin@example.com`	電子メール アドレスに syslog 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。
ステップ 4	**smtp-server** *ip_address* **例：** `hostname(config)# smtp-server 10.1.1.1`	電子メール アドレスに syslog メッセージを送信するときに使用する SMTP サーバを指定します。

ASDM への syslog メッセージの送信

syslog メッセージを ASDM に送信するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**logging asdm** {*severity_level* | *message_list*} **例：** hostname(config)# logging asdm 2	ASDM に送信する syslog メッセージを指定します。ASA または ASASM は、ASDM への送信を待つ syslog メッセージのためにバッファ領域を確保し、メッセージが発生するとバッファに保存します。ASDM ログ バッファは、内部ログ バッファとは別のバッファです。ASDM のログ バッファがいっぱいになると、ASA または ASASM は最も古い syslog メッセージを削除し、新しい syslog メッセージ用にバッファ領域を確保します。最も古い syslog メッセージを削除して新しい syslog メッセージのためのスペースを確保するのは、ASDM のデフォルト設定です。ASDM ログ バッファに保持される syslog メッセージの数を制御するために、バッファのサイズを変更できます。
ステップ 2	**logging asdm-buffer-size** *num_of_msgs* **例：** hostname(config)# logging asdm-buffer-size 200	ASDM ログ バッファに保持される syslog メッセージの数を指定します。ASDM ログ バッファの現在の内容を空にするには、**clear logging asdm** コマンドを入力します。

コンソール ポートへの syslog メッセージの送信

syslog メッセージをコンソール ポートに送信するには、次のコマンドを入力します。

コマンド	目的
logging console {*severity_level* | *message_list*} **例：** hostname(config)# logging console errors	コンソール ポートに送信する syslog メッセージを指定します。

SNMP サーバへの syslog メッセージの送信

SNMP サーバへの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。

コマンド	目的
logging history [*logging_list* | *level*] **例：** hostname(config)# logging history errors	SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定します。SNMP ロギングをディセーブルにするには、**no logging history** コマンドを入力します。

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**logging monitor** {*severity_level* | *message_list*} **例：** `hostname(config)# logging monitor 6`	Telnet または SSH セッションに送信する syslog メッセージを指定します。
ステップ 2	**terminal monitor** **例：** `hostname(config)# terminal monitor`	現在のセッションへのロギングだけをイネーブルにします。一度ログアウトして再び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。現在のセッションへのロギングをディセーブルにするには、**terminal no monitor** コマンドを入力します。

カスタム イベント リストの作成

カスタム イベント リストを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**logging list** *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[**-***end_id*]} **例：** `hostname(config)# logging list notif-list level 3`	内部ログ バッファに保存されるメッセージの選択基準を指定します。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。 *name* 引数には、リストの名前を指定します。**level** *level* キーワードと引数のペアは、重大度を指定します。**class** *message_class* キーワードと引数のペアは、特定のメッセージ クラスを指定します。**message** *start_id*[**-***end_id*] キーワードと引数のペアは、個々の syslog メッセージ番号または番号の範囲を指定します。 **（注）** 重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベント リスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベント リスト名は使用しないでください。

ステップ 2	**logging list** *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[**-***end_id*]}
	
	例：
	`hostname(config)# logging list notif-list message 104024-105999`
	
	`hostname(config)# logging list notif-list level critical`
	
	`hostname(config)# logging list notif-list level warning class ha`
		（任意）リストにメッセージの選択基準をさらに追加します。前回の手順で使用したものと同じコマンドを入力し、既存のメッセージ リストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。
		
		• ID が 104024 ～ 105999 の範囲の syslog メッセージ。
		• 重大度が critical 以上（emergency、alert、または critical）のすべての syslog 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 syslog メッセージ。
		
		（注） syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

syslog サーバへの EMBLEM 形式の syslog メッセージの生成

syslog サーバへの EMBLEM 形式の syslog メッセージを生成するには、次のコマンドを入力します。

コマンド	目的
logging host *interface_name ip_address* {**tcp**[*/port*] | **udp**[*/port*]} [**format emblem**] **例：** `hostname(config)# logging host interface_1 127.0.0.1 udp format emblem`	EMBLEM 形式の syslog メッセージを、UDP のポート 514 を使用して syslog サーバに送信します。 **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 限定）。*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***]** キーワードと引数のペアは、syslog サーバに syslog メッセージを送信するために ASA および ASASM で TCP を使用するか、UDP を使用するかを指定します。 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 ASA および ASASM 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。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。 複数の **logging host** コマンドを使用して、追加サーバを指定できます。それらすべてで syslog メッセージが受信されます。2 つ以上のロギング サーバを設定する場合は、必ず、すべてのロギング サーバにおいて、ロギングの重大度の上限を warnings にしてください。 TCP を指定すると、ASA または ASASM は syslog サーバの障害を検出し、セキュリティ保護として ASA を経由する新しい接続をブロックします。UDP を指定すると、ASA または ASASM は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 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。 **（注）**　TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次のコマンドを入力します。

コマンド	目的
logging emblem **例：** `hostname(config)# logging emblem`	syslog サーバ以外の出力先（たとえば、Telnet または SSH セッション）に EMBLEM 形式の syslog メッセージを送信します。

ログを記録可能な内部フラッシュ メモリの容量の変更

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

	コマンド	目的
ステップ 1	**logging flash-maximum-allocation** *kbytes* **例：** `hostname(config)# logging flash-maximum-allocation 1200`	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します。デフォルトでは、ASA は、内部フラッシュ メモリの最大 1 MB をログ データに使用できます。ASA および ASASM 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、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、ASA または ASASM は最も古いログ ファイルを削除し、その新しいログ ファイルが保存されたとしても最小限の容量が確保されるようにします。削除するファイルがなかったり、古いファイルすべてを削除しても最小限の容量を確保できなかったりする場合、ASA または ASASM はその新しいログ ファイルを保存できません。
ステップ 2	**logging flash-minimum-free** *kbytes* **例：** `hostname(config)# logging flash-minimum-free 4000`	ASA または ASASM でログ 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指定します。

ロギング キューの設定

ロギング キューを設定するには、次のコマンドを入力します。

コマンド	目的
logging queue *message_count* **例：** `hostname(config)# logging queue 300`	設定された出力先に送信されるまでの間、ASA および ASASM がそのキューに保持できる syslog メッセージの数を指定します。ASA および ASASM のメモリ内には、設定された出力先への送信を待機している syslog メッセージをバッファするために割り当てられる、固定された数のブロックがあります。必要なブロックの数は、syslog メッセージ キューの長さと、指定した syslog サーバの数によって異なります。デフォルトのキューのサイズは 512 syslog メッセージです。キューのサイズは、使用可能なブロック メモリのサイズが上限です。有効値は 0 ～ 8192 メッセージです。値はプラットフォームによって異なります。ロギング キューが 0 に設定されている場合、プラットフォームに応じて、キューは設定可能な最大サイズ（8192 メッセージ）になります。プラットフォームごとの最大キュー サイズは次のとおりです。 • ASA-5505：1024 • ASA-5510：2048 • 他のすべてのプラットフォーム：8192

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべての syslog メッセージを指定した出力先に送信するには、次のコマンドを入力します。

コマンド	目的
logging class *message_class* {**buffered** | **console** | **history** | **mail** | **monitor** | **trap**} [*severity_level*] **例：** `hostname(config)# logging class ha buffered alerts`	指定した出力先コマンドでコンフィギュレーションを上書きします。たとえば、重大度 7 のメッセージが内部ログ バッファに送信されるように指定し、重大度 3 の ha クラスのメッセージが内部ログ バッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。**buffered**、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスの syslog メッセージの出力先を指定します。**history** キーワードは、SNMP でのロギングをイネーブルにします。**monitor** キーワードは、Telnet および SSH でのロギングをイネーブルにします。**trap** キーワードは、syslog サーバへのロギングをイネーブルにします。コマンドライン エントリあたり 1 つの出力先を指定します。1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに新しいコマンドを入力します。

セキュア ロギングのイネーブル化

セキュア 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。

コマンド	目的
logging host *interface_name syslog_ip* [**tcp**/port | **udp**/*port*] [**format emblem**] [**secure**] **例：** `hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure`	セキュア ロギングをイネーブルにします。 *interface_name* 引数には、syslog サーバが常駐する *インターフェイスを指定します。syslog_ip* 引数*には*、syslog サーバの IP アドレスを指定します。*port* 引数には、syslog サーバが syslog メッセージをリスンするポート（TCP または UDP）を指定します。**tcp** キーワードは、ASA または ASASM が TCP を使用して syslog メッセージを syslog サーバに送信するように指定します。**udp** キーワードは、ASA または ASASM が UDP を使用して syslog メッセージを syslog サーバに送信するように指定します。**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。**secure** キーワードは、リモート ロギング ホストへの接続で、TCP の場合にだけ SSL/TLS を使用するように指定します。 **（注）** セキュア ロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。

非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次のコマンドを入力します。

コマンド	目的

logging device-id {**cluster-id** |**context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}
 	
例：
`hostname(config)# logging device-id hostname`
 	
`hostname(config)# logging device-id context-name`
	デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるように ASA または ASASM を設定します。syslog 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デバイス ID として使用するように指定します（マルチ コンテキスト モードだけに適用）。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。
	
	（注） ASA クラスタでは、常に、選択したインターフェイスのマスター ユニットの IP アドレスを使用します。
	
	cluster-id キーワードがデバイス ID としてクラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。**hostname** キーワードは、ASA 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* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。**string** *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。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 syslog 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。

syslog メッセージへの日付と時刻の出力

syslog メッセージに日付と時刻を含めるには、次のコマンドを入力します。

コマンド	目的
logging timestamp hostname(config)# logging timestamp **例：** hostname(config)# logging timestamp LOG-2008-10-24-081856.TXT	syslog メッセージにメッセージが生成された日付と時刻が含まれるように指定します。syslog メッセージから日付と時刻を削除するには、**no logging timestamp** コマンドを入力します。

syslog メッセージのディセーブル化

指定した syslog 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。

コマンド	目的
no logging message *message_number* **例：** hostname(config)# no logging message 113019	ASA または ASASM が特定の syslog メッセージを生成しないように指定します。ディセーブル化された syslog メッセージを再度イネーブルにするには、**logging message** *message_number* コマンド（たとえば、**logging message 113019** など）を入力します。ディセーブル化されたすべての syslog メッセージのロギングを再度イネーブルにするには、**clear config logging disabled** コマンドを入力します。

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次のコマンドを入力します。

コマンド	目的
logging message *message_ID* **level** *severity_level* **例：** hostname(config)# logging message 113019 level 5	syslog メッセージの重大度を指定します。syslog メッセージの重大度をその設定にリセットするには、**no logging message** *message_ID* **level** *current_severity_level* コマンド（たとえば、**no logging message 113019 level 5** など）を入力します。変更されたすべての syslog メッセージの重大度をそれらの設定にリセットするには、**clear configure logging level** コマンドを入力します。

syslog メッセージ生成のレート制限

syslog メッセージの生成レートを制限するには、次のコマンドを入力します。

コマンド	目的
logging rate-limit {unlimited | {*num* [*interval*]}} message *syslog_id* | level *severity_level* **例：** hostname(config)# logging rate-limit 1000 600 level 6	指定された重大度（1 ～ 7）を、指定の時間内でメッセージセットまたは個々のメッセージ（出力先ではない）に適用します。レート制限は、すべての設定された出力先に送信されるメッセージの量に影響します。ロギングのレート制限をデフォルト値にリセットするには、**clear running-config logging rate-limit** コマンドを入力します。ロギングのレート制限をリセットするには、**clear configure logging rate-limit** コマンドを入力します。

ログのモニタリング

ログ バッファまたはリアルタイムでログをモニタし、システム パフォーマンスのモニタリングに役立つようにするには、次のいずれかのコマンドを入力します。

コマンド	目的
show logging	重大度を含む syslog メッセージを表示します。 **（注）** 表示できる syslog メッセージの最大数は、1000 です。これはデフォルト設定です。表示できる syslog メッセージの最大数は、2000 です。
show logging message	重大度が変更された syslog メッセージとディセーブル化された syslog メッセージの一覧を表示します。
show logging message *message_ID*	特定の syslog メッセージの重大度を表示します。
show logging queue	ロギング キューとキュー統計情報を表示します。
show logging rate-limit	拒否された syslog メッセージを表示します。
show running-config logging rate-limit	ロギングのレート制限の現在の設定を表示します。

例

次の例は、**show logging** コマンドで表示されるロギング情報を示しています。

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

ロギングの設定例

次の例は、syslog メッセージをイネーブルにするかどうかを制御する方法と、指定した syslog メッセージの重大度を制御する方法を示しています。

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

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

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

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

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

ロギングの機能履歴

表 36-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 36-2　ロギングの機能履歴

機能名	プラットフォーム リリース	機能情報
ロギング	7.0(1)	さまざまな出力先を通して ASA ネットワーク ロギング情報を提供します。ログ ファイルを表示して保存するオプションも含まれています。
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 **logging rate-limit** コマンドが導入されました。
ロギング リスト	7.2(1)	さまざまな基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために他のコマンドで使用されるロギング リストを作成します。 **logging list** コマンドが導入されました。

表 36-2　ロギングの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
セキュア ロギング	8.0(2)	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 **logging host** コマンドが変更されました。
ロギング クラス	8.0(4)、8.1(1)	ロギング メッセージの ipaa イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。
ロギング クラスと保存されたロギング バッファ	8.2(1)	ロギング メッセージの dap イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。 保存されたロギング バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアする追加サポート。 **clear logging queue bufferwrap** コマンドが導入されました。
パスワードの暗号化	8.3(1)	パスワードの暗号化に対するサポートが追加されました。 **logging ftp server** コマンドが変更されました。
拡張ロギングおよび接続ブロック	8.3(2)	TCP を使用するように syslog サーバを設定すると、syslog サーバを使用できない場合、ASA は、サーバが再び使用可能になるまで syslog メッセージを生成する新しい接続をブロックします（たとえば、VPN、ファイアウォール、カットスルー プロキシ接続）。この機能は、ASA のロギング キューがいっぱいのときにも新しい接続をブロックするように拡張されました。接続は、ロギング キューがクリアされると再開されます。 この機能は、Common Criteria EAL4+ に準拠するために追加されました。必要がない限り、syslog メッセージを送受信できないときは接続を許可することを推奨します。接続を許可するには、引き続き **logging permit-hostdown** コマンドを使用します。 **show logging** コマンドが変更されました。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。
クラスタリング	9.0(1)	ASA 5580 および 5585-X でのクラスタリング環境における syslog メッセージ生成のサポートが追加されました。 **logging device-id** コマンドが変更されました。