CHAPTER 41

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」（P.41-1）
- 「ロギングのライセンス要件」（P.41-5）
- 「ロギングの前提条件」（P.41-6）
- 「ガイドラインと制限事項」（P.41-6）
- 「ロギングの設定」（P.41-7）
- 「ログのモニタリング」（P.41-25）
- 「ロギングの機能履歴」（P.41-29）

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」（P.41-2）
- 「syslog メッセージの分析」（P.41-2）
- 「syslog メッセージ形式」（P.41-3）
- 「重大度」（P.41-3）
- 「メッセージ クラスと syslog ID の範囲」（P.41-4）
- 「syslog メッセージのフィルタリング」（P.41-4）
- 「ログ ビューアでのソート」（P.41-4）
- 「カスタム メッセージ リストの使用」（P.41-5）
- 「クラスタリングの使用」（P.41-5）

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 41-1 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 41-1 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 41-1　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。

ログ ビューアでのソート

すべての ASDM ログ ビューア（Real-Time Log Viewer、Log Buffer Viewer、および Latest ASDM Syslog Events Viewer）でメッセージをソートできます。複数のカラムでテーブルをソートするには、ソートの基準とする、最初のカラムのヘッダーをクリックし、**Ctrl** キーを押したまま、同時にソート

順に含める他のカラムのヘッダーをクリックします。時間順にメッセージをソートするには、日付と時刻のカラムを両方選択します。どちらか一方だけを選択した場合は、（時刻に関係なく）日付のみまたは（日付に関係なく）時刻のみでメッセージがソートされます。

Real-Time Log Viewer および Latest ASDM Syslog Events Viewer でメッセージをソートすると、記録された新しいメッセージは通常の表示位置となる一番上ではなく、ソートされた順序で表示されます。つまり、メッセージはその他のメッセージの中に混ざって表示されます。

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。

（注） クラスタの装置から syslog メッセージをモニタするには、モニタする各装置に対して ASDM セッションを開く必要があります。

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 [Syslog Server] ペインで個別のエントリを指定します。

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。
- アクセス リストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギング重大度がデバッグ（レベル 7）のアクセス リストに対しては、アクセス リストのログは生成されません。**logging list** コマンドのロギング重大度のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセス リスト コンフィギュレーションのロギング重大度をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体を変更する必要があります。

  次に、ロギング重大度がデバッグに変更されているため、アクセス リストのヒットが含まれていない **show running-config logging** コマンドの出力例を示します。

```
hostname# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  次に、アクセス リスト ヒットを含む **show running-config logging** コマンドの出力例を示します。

```
hostname# show running-config logging
```

```
logging enable
logging timestamp
logging buffered debugging
```

この場合、アクセス リスト コンフィギュレーションは変更せず、アクセス リスト ヒット数が次の例のように表示されます。

```
hostname(config)# access-list global line 1 extended permit icmp any host 4.2.2.2 log
debugging interval 1 (hitcnt=7) 0xf36b5386
hostname(config)# access-list global line 2 extended permit tcp host 10.1.1.2 any eq
www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
hostname(config)# access-list global line 3 extended permit ip any any (hitcnt=543)
0x25f9e609
```

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.41-7）
- 「出力先の設定」（P.41-8）

（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、次の手順を実行します。

ステップ 1　ASDM で、次のいずれかを選択してください。

- **[Home] > [Latest ASDM Syslog Messages] > [Enable Logging]**
- **[Configuration] > [Device Management] > [Logging] > [Logging Setup]**
- **[Monitoring] > [Real-Time Log Viewer] > [Enable Logging]**
- **[Monitoring] > [Log Buffer] > [Enable Logging]**

ステップ 2　[Enable logging] チェックボックスをオンにして、ロギングをオンにします。

次の作業

「出力先の設定」（P.41-8）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」（P.41-9）
- 「FTP の設定」（P.41-10）
- 「ロギングに使用するフラッシュ メモリの設定」（P.41-10）
- 「syslog メッセージの設定」（P.41-11）
- 「syslog ID 設定の編集」（P.41-11）
- 「非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力」（P.41-12）
- 「内部ログ バッファへの syslog メッセージの送信」（P.41-13）
- 「内部ログ バッファをフラッシュ メモリに保存する」（P.41-13）
- 「ASDM Java Console による記録されたエントリの参照とコピー」（P.41-14）
- 「電子メール アドレスへの syslog メッセージの送信」（P.41-14）
- 「電子メール受信者の追加または編集」（P.41-15）
- 「リモート SMTP サーバの設定」（P.41-15）
- 「ASDM での syslog メッセージの表示」（P.41-16）
- 「ロギングの宛先へのメッセージ フィルタの適用」（P.41-16）
- 「ロギング フィルタの適用」（P.41-17）
- 「メッセージ クラスと重大度フィルタの追加または編集」（P.41-17）
- 「syslog メッセージ ID フィルタの追加または編集」（P.41-18）
- 「コンソール ポートへの syslog メッセージの送信」（P.41-18）
- 「Telnet または SSH セッションへの syslog メッセージの送信」（P.41-18）
- 「カスタム イベント リストの作成」（P.41-19）
- 「syslog サーバへの EMBLEM 形式の syslog メッセージの生成」（P.41-20）
- 「syslog サーバ設定の追加または編集」（P.41-20）
- 「他の出力先への EMBLEM 形式の syslog メッセージの生成」（P.41-21）
- 「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.41-21）
- 「ロギング キューの設定」（P.41-21）
- 「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」（P.41-22）
- 「セキュア ロギングのイネーブル化」（P.41-22）
- 「非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力」（P.41-23）

- 「syslog メッセージへの日付と時刻の出力」（P.41-23）
- 「syslog メッセージのディセーブル化」（P.41-23）
- 「syslog メッセージの重大度の変更」（P.41-24）
- 「syslog メッセージ生成のレート制限」（P.41-24）
- 「個々の syslog メッセージに対するレート制限の割り当てまたは変更」（P.41-24）
- 「syslog メッセージのレート制限の追加または編集」（P.41-25）
- 「syslog 重大度に対するレート制限の編集」（P.41-25）

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。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。

ステップ 2　[Enable logging] チェックボックスをオンにして、メイン ASA に対するロギングを有効にします。

ステップ 3　[Enable logging on the failover standby unit] チェックボックスをオンにして、スタンバイ ASA に対するロギングを有効にします（可能な場合）。

ステップ 4　[Send debug messages as syslogs] チェックボックスをオンにして、すべてのデバッグ トレース出力がシステム ログにリダイレクトされるようにします。このオプションがイネーブルになっている場合、syslog メッセージはコンソールには表示されません。そのため、デバッグ メッセージを表示するには、コンソールでロギングをイネーブルにし、デバッグ syslog メッセージ番号および重大度レベルの宛先としてコンソールを設定する必要があります。使用する syslog メッセージ番号は、**711001** です。この syslog メッセージに対するデフォルトの重大度レベルは、[Debugging] です。

ステップ 5　[Send syslogs in EMBLEM format] チェックボックスをオンにして、EMBLEM 形式をイネーブルにします。これにより、syslog サーバを除くロギングの宛先すべてに対して EMBLEM 形式が使用されます。

ステップ 6　ロギング バッファがイネーブルの場合に syslog メッセージが保存される内部ログ バッファのサイズを、[Buffer Size] フィールドで指定します。バッファの空き容量がなくなると、FTP サーバまたは内部フラッシュ メモリにログを保存していない限り、メッセージは上書きされます。デフォルトのバッファ サイズは 4096 バイトです。有効な範囲は 4096 ～ 1048576 です。

ステップ 7　バッファ内のデータが上書きされる前に、それらを FTP サーバに保存する場合は、[Save Buffer To FTP Server] チェックボックスをオンします。バッファ内のデータが上書きされるようにする場合は、このチェックボックスをオフにします。

ステップ 8　[Configure FTP Settings] をクリックして、FTP サーバを指定し、バッファ内のデータを保存する際に使用する FTP パラメータを設定します。詳細については、「FTP の設定」（P.41-10）を参照してください。

ステップ 9　バッファ内のデータが上書きされる前に、それらを内部フラッシュ メモリに保存する場合は、[Save Buffer To Flash] チェックボックスをオンにします。

（注）　このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。

ステップ 10　[Configure Flash Usage] をクリックし、ロギングに使用する内部フラッシュ メモリの最大容量、および最低限維持すべき空き容量を KB 単位で指定します。このオプションをイネーブルにすると、メッセージが格納されるデバイス ディスク上に、「syslog」という名前のディレクトリが作成されます。詳細については、「ロギングに使用するフラッシュ メモリの設定」（P.41-10）を参照してください。

（注）　このオプションは、単一ルーテッド モードまたはトランスペアレント モードでだけ使用できます。

ステップ 11　[Queue Size] フィールドで、ASA または ASASM に表示するシステム ログのキュー サイズを指定します。

FTP の設定

ログ バッファの内容の保存に使用する FTP サーバのコンフィギュレーションを指定するには、次の手順を実行します。

ステップ 1　[Enable FTP client] チェックボックスをオンにして、FTP クライアントのコンフィギュレーションをイネーブルにします。

ステップ 2　[Server IP Address] フィールドで、FTP サーバの IP アドレスを指定します。

ステップ 3　[Path] フィールドで、保存済みログ バッファ データの格納先となる FTP サーバ上のディレクトリ パスを指定します。

ステップ 4　FTP サーバへログインするためのユーザ名を、[Username] フィールドに指定します。

ステップ 5　FTP サーバへログインするためのユーザ名に関連付けられたパスワードを、[Password] フィールドに指定します。

ステップ 6　[Confirm Password] フィールドに再度パスワードを入力し、[OK] をクリックします。

ロギングに使用するフラッシュ メモリの設定

ログ バッファの内容を内部フラッシュ メモリに保存する場合の制限事項を指定するには、次の手順を実行します。

ステップ 1　[Maximum Flash to Be Used by Logging] フィールドで、ロギングに使用できる内部フラッシュ メモリの最大容量を、KB 単位で指定します。

ステップ 2　[Minimum Free Space to Be Preserved] フィールドで、最低限維持すべき内部フラッシュ メモリの空き容量を、KB 単位で指定します。内部フラッシュメモリがこの制限値に近づくと、新しいログが保存されなくなります。

ステップ 3　[OK] をクリックして、このダイアログボックスを閉じます。

syslog メッセージの設定

syslog メッセージを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Setup] を選択します。

ステップ 2　[Facility code to include in syslogs] ドロップダウン リストから、syslog サーバでメッセージを保存する際の基準として使用するシステム ログ ファシリティを選択します。デフォルトは LOCAL(4)20 です。これは、ほとんどの UNIX システムで必要となるコードです。ただし、ネットワーク デバイス間では 8 つのファシリティが共用されているため、システム ログではこの値を変更しなければならない場合があります。

ステップ 3　送信される各 syslog メッセージに日時を追加する場合は、[Include timestamp in syslogs] チェックボックスをオンにします。

ステップ 4　[Show] ドロップダウン リストから、[Syslog ID] テーブルに表示する情報を選択します。使用可能なオプションは、次のとおりです。

- すべての syslog メッセージ ID が [Syslog ID] テーブルに一覧表示されるよう指定する場合は、[Show all syslog IDs] を選択します。
- 明示的にディセーブルにした syslog メッセージ ID だけ [Syslog ID] テーブルに表示されるよう指定する場合は、[Show disabled syslog IDs] を選択します。
- 重大度レベルがデフォルトのレベルから変更された syslog メッセージ ID だけ [Syslog ID] テーブルに表示されるよう指定する場合は、[Show syslog IDs with changed logging] を選択します。
- 重大度レベルが変更された syslog メッセージ ID および明示的にディセーブルになった syslog メッセージ ID だけ [Syslog ID] テーブルに表示されるよう指定する場合は、[Show syslog IDs that are disabled or with a changed logging level] を選択します。

ステップ 5　[Syslog ID Setup] テーブルには、その設定内容を基づいて、syslog メッセージのリストが表示されます。変更する個々のメッセージ ID またはメッセージ ID の範囲を選択します。選択したメッセージ ID は、ディセーブルにすることも、その重大度レベルを変更することもできます。リストから複数のメッセージ ID を選択する場合は、その範囲の先頭にあたる ID を選択し、Shift キーを押しながらその範囲の最後にあたる ID をクリックします。

ステップ 6　syslog メッセージにデバイス ID が含まれるよう設定する場合は、[Advanced] をクリックします。詳細については、「syslog ID 設定の編集」（P.41-11）および「非 EMBLEM 形式の syslog メッセージへのデバイス ID の出力」（P.41-12）を参照してください。

syslog ID 設定の編集

syslog メッセージの設定を変更するには、次の手順を実行します。

（注）　[Syslog ID(s)] フィールドは表示専用です。この領域に表示される値は、[Syslog Setup] ペインにある [Syslog ID] テーブルで選択されたエントリにより決まります。

ステップ 1　[Disable Message(s)] チェックボックスをオンにして、[Syslog ID(s)] リストに ID が表示されている syslog メッセージをディセーブルにします。

ステップ 2　[Logging Level] ドロップダウン リストから、[Syslog ID(s)] リストに ID が表示されている syslog メッセージのうち、送信する syslog メッセージの重大度レベルを選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3　[OK] をクリックして、このダイアログボックスを閉じます。

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、次の手順を実行します。

ステップ 1　[Enable syslog device ID] チェックボックスをオンにして、非 EMBLEM 形式の syslog メッセージすべてにデバイス ID が含まれるように指定します。

ステップ 2　次のいずれかのオプションを選択して、どのようなデバイス ID を使用するかを指定します。

- ASA のホスト名
- インターフェイス IP アドレス

  選択した IP アドレスに対応するインターフェイス名を、ドロップダウン リストから選択します。

  クラスタリングを使用する場合は、[In an ASA cluster, always use master's IP address for the selected interface] をオンにします。
- 文字列

  [User-Defined ID] フィールドに、ユーザ独自の英数文字列を入力します。
- ASA クラスタ名

ステップ 3　[OK] をクリックして、このダイアログボックスを閉じます。

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。

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。

ステップ 1　syslog メッセージを内部ログ バッファに送信する方法を指定するには、次のいずれかを選択してください：

- **[Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]**
- **[Configuration] > [Device Management] > [Logging] > [Logging Filters]**

ステップ 2　内部ログ バッファを空にするには、[Monitoring] > [Logging] > [Log Buffer] > [View] を選択します。次に、[Log Buffer] ペインで、[File] > [Clear Internal Log Buffer] を選択します。

ステップ 3　内部ログ バッファのサイズを変更するには、[Configuration] > [Device Management] > [Logging] > [Logging Setup] を選択します。デフォルトのバッファ サイズは 4 KB 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。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。

ステップ 4　別の場所に新しいメッセージを保存するには、次のオプションから 1 つを選択します。

- 内部フラッシュ メモリに新しいメッセージを送信するには、[Flash] チェックボックスをオンにし、[Configure Flash Usage] をクリックします。[Configure Logging Flash Usage] ダイアログボックスが表示されます。
  - **a.** ロギングに使用するフラッシュ メモリの最大容量を KB で指定します。
  - **b.** ロギングをフラッシュ メモリに保持する最小空き領域量を KB で指定します。
  - **c.** [OK] をクリックして、このダイアログボックスを閉じます。
- FTP サーバに新しいメッセージを送信するには、[FTP Server] チェックボックスをオンにし、[Configure FTP Settings] をクリックします。[Configure FTP Settings] ダイアログボックスが表示されます。
  - **a.** [Enable FTP Client] チェックボックスをオンにします。
  - **b.** 表示されたフィールドに、FTP サーバ IP アドレス、パス、ユーザ名、パスワードを入力します。
  - **c.** パスワードを確認し、[OK] をクリックしてこのダイアログボックスを閉じます。

内部ログ バッファをフラッシュ メモリに保存する

内部ログ バッファをフラッシュ メモリに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Internal Log Buffer to Flash] の順に選択します。

[Enter Log File Name] ダイアログボックスが表示されます。

ステップ 2　最初のオプションを選択し、LOG-YYYY-MM-DD-hhmmss.txt 形式のデフォルト ファイル名でログ バッファを保存します。

ステップ 3　2 番目のオプションを選択し、そのログ バッファのファイル名を指定します。

ステップ 4　ログ バッファのファイル名を入力して [OK] をクリックします。

ASDM Java Console による記録されたエントリの参照とコピー

ASDM Java コンソールを使用して、ASDM エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。

ASDM Java Console にアクセスするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [ASDM Java Console] の順に選択します。

ステップ 2　仮想マシンのメモリ統計を表示するには、コンソールで **m** と入力します。

ステップ 3　ガーベージ コレクションを実行するには、コンソールで **g** と入力します。

ステップ 4　メモリの使用状況を監視するには、Windows Task Manager を開き **asdm_launcher.exe** ファイルをダブルクリックします。

（注）　メモリ割り当ての最大値は 256 MB です。

ステップ 5　続行するには、ファイアウォール コンフィギュレーション ガイドの “Monitoring Performance” section on page 63-12 を参照してください。

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。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [E-Mail Setup] を選択します。

ステップ 2　syslog メッセージを電子メールとして送信する際に、その送信元アドレスとして使用する電子メール アドレスを、[Source E-Mail Address] フィールドに指定します。

ステップ 3　[Add] をクリックして、指定した syslog メッセージの受信者の電子メール アドレスを入力します。詳細については、「電子メール受信者の追加または編集」（P.41-15）を参照してください。

ステップ 4　その受信者に送信する syslog メッセージの重大度レベルを、ドロップダウン リストから選択します。宛先の電子メール アドレスに対して適用される syslog メッセージの重大度フィルタにより、指定された重大度レベル以上のメッセージが送信されます。[Logging Filters] ペインで指定されたグローバル フィルタも、各電子メール受信者に適用されます。詳細については、「ロギング フィルタの適用」（P.41-17）を参照してください。

ステップ 5　[Edit] をクリックして、この受信者へ送信する syslog メッセージの現在の重大度を変更します。詳細については、「電子メール受信者の追加または編集」（P.41-15）を参照してください。

ステップ 6　[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 7　以降の手順については、「リモート SMTP サーバの設定」（P.41-15）を参照してください。

電子メール受信者の追加または編集

電子メールの受信者および重大度を追加または編集するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [E-mail Setup] を選択します。

ステップ 2　[Add] または [Edit] をクリックして、[Add/Edit E-Mail Recipient] ダイアログボックスを表示します。

ステップ 3　宛先の電子メール アドレスを入力し、ドロップダウン リストから syslog 重大度を選択します。重大度レベルは次のように定義されています。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

（注）　宛先電子メール アドレスへのメッセージをフィルタリングする場合は、[Add/Edit E-Mail Recipient] ダイアログボックスで指定した重大度と、[Logging Filters] ペインですべての電子メール受信者に対して設定したグローバル フィルタの重大度のうち、上位にある方が使用されます。

ステップ 4　[OK] をクリックして、このダイアログボックスを閉じます。

追加または修正されたエントリが [E-mail Recipients] ペインに表示されます。

ステップ 5　[Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

リモート SMTP サーバの設定

特定のイベントに対する電子メール アラートおよび通知の送信先となるリモート SMTP サーバを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Logging] > [SMTP] を選択します。

ステップ 2　プライマリ SMTP サーバの IP アドレスを入力します。

ステップ 3　（任意）スタンバイ SMTP サーバの IP アドレスを入力し、[Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

ASDM での syslog メッセージの表示

ASDM に送信された最新の syslog メッセージを表示するには、[Home] > [Latest ASDM Syslog Messages] を選択します。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メッセージ用に領域を確保する設定は、ASDM のデフォルト設定です。

ロギングの宛先へのメッセージ フィルタの適用

ロギングの宛先にメッセージ フィルタを適用するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Logging Filters] を選択します。

ステップ 2　フィルタを適用するロギングの宛先の名前を選択します。選択できるロギングの宛先は次のとおりです。

- ASDM
- コンソール ポート
- 電子メール
- 内部バッファ
- SNMP サーバ
- Syslog サーバ
- Telnet または SSH セッション

このほか、2 番目のカラム [Syslogs From All Event Classes] と 3 番目のカラム [Syslogs From Specific Event Classes] でも選択操作を行います。2 番目のカラムでは、ロギングの宛先へのメッセージをフィルタリングする場合に使用する重大度やイベント クラスが表示されるほか、すべてのイベント クラスに対してロギングをディセーブルにするかを選択することもできます。3 番目のカラムには、選択したロギングの宛先へのメッセージをフィルタリングする場合に使用するイベント クラスが表示されます。詳細については、「メッセージ クラスと重大度フィルタの追加または編集」（P.41-17）および「syslog メッセージ ID フィルタの追加または編集」（P.41-18）を参照してください。

ステップ 3　**[Edit]** をクリックして、[Edit Logging Filters] ダイアログボックスを表示します。フィルタを適用、編集、またはディセーブルにする手順については、「ロギング フィルタの適用」（P.41-17）を参照してください。

ロギング フィルタの適用

フィルタを適用するには、次の手順を実行します。

ステップ 1　重大度レベルに基づいて syslog メッセージのフィルタリングを行う場合は、[Filter on severity] オプションを選択します。

ステップ 2　イベント リストに基づいて syslog メッセージのフィルタリングを行う場合は、[Use event list] オプションを選択します。

ステップ 3　選択した宛先に対するロギングをすべてディセーブルにする場合は、[Disable logging from all event classes] オプションを選択します。

ステップ 4　[New] をクリックして、新しいイベント リストを追加します。新しいイベント リストを追加する手順については、「カスタム イベント リストの作成」（P.41-19）を参照してください。

ステップ 5　ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 6　ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 7　[Add] をクリックして、イベント クラスおよび重大度レベルを追加し、[OK] をクリックします。

ダイアログボックスの上部には、フィルタに対して選択したロギングの宛先が表示されます。

メッセージ クラスと重大度フィルタの追加または編集

メッセージのフィルタリングに使用するメッセージ クラスおよび重大度レベルを追加または編集するには、次の手順を実行します。

ステップ 1　ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 2　ドロップダウン リストから、ロギング メッセージの重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 3　選択が終了したら、[OK] をクリックします。

syslog メッセージ ID フィルタの追加または編集

syslog メッセージ ID フィルタを作成または編集する手順については、「syslog ID 設定の編集」（P.41-11）を参照してください。

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、次の手順を実行します。

ステップ 1　ASDM で、次のオプションから 1 つを選択します。

- **[Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]**
- **[Configuration] > [Device Management] > [Logging] > [Logging Filters]**

ステップ 2　[Logging Destination] カラムでコンソールを選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3　コンソール ポートに送信する syslog メッセージを指定するには、すべてのイベント クラスから syslog を選択するか、または特定のイベント クラスから syslog を選択します。

ステップ 4　以降の手順については、「ロギング フィルタの適用」（P.41-17）を参照してください。

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。

ステップ 1　ASDM で、次のいずれかを選択してください。

- **[Home] > [Latest ASDM Syslog Messages] > [Configure ASDM Syslog Filters]**
- **[Configuration] > [Device Management] > [Logging] > [Logging Filters]**

ステップ 2　[Logging Destination] カラムの Telnet および SSH のセッションを選択し、[Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3　Telnet または SSH セッションに送信する syslog メッセージを指定するには、すべてのイベント クラスから syslog を選択するか、または特定のイベント クラスから syslog を選択します。

ステップ 4　以降の手順については、「ロギング フィルタの適用」（P.41-17）を参照してください。

ステップ 5　現在のセッションでのみロギングをイネーブルにするには、[Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択します。

ステップ 6　[Enable Logging] チェックボックスをチェックし、[Apply] をクリックします。

カスタム イベント リストの作成

イベント リストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（SNMP サーバなど）に送信されるイベントのカスタム リストを作成するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Event Lists] を選択します。

ステップ 2　[Add] をクリックして、[Add Event List] ダイアログボックスを表示します。

ステップ 3　[Name] フィールドに、イベント リストの名前を入力します。スペースは使用できません。

ステップ 4　[Event Class/Severity] 領域で、[Add] をクリックし、[Add Class and SeverityFilter] ダイアログボックスを表示します。

ステップ 5　ドロップダウン リストからイベント クラスを選択します。使用できるイベント クラスは、使用しているデバイス モードによって異なります。

ステップ 6　ドロップダウン リストから重大度レベルを選択します。重大度レベルは次のとおりです。

- Emergency（レベル 0、システムが使用不能）

（注）　重要度レベル 0 を使用することはお勧めできません。

- Alert（レベル 1、即時対処が必要）
- Critical（レベル 2、クリティカル条件）
- Error（レベル 3、エラー条件）
- Warning（レベル 4、警告条件）
- Notification（レベル 5、正常だが顕著な条件）
- Informational（レベル 6、情報メッセージのみ）
- Debugging（レベル 7、デバッグ メッセージのみ）

ステップ 7　[OK] をクリックして、このダイアログボックスを閉じます。

ステップ 8　[Message ID Filters] 領域で、[Add] をクリックし、[Add Syslog Message ID Filter] ダイアログボックスを表示します。

ステップ 9　[Message IDs] フィールドに、フィルタに含める syslog メッセージ ID または syslog メッセージ ID の範囲（101001 ～ 199012 など）を入力します。

ステップ 10　[OK] をクリックして、このダイアログボックスを閉じます。

目的のイベントがリストに表示されます。このエントリを変更する場合は、[Edit] をクリックします。

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、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Syslog Server] を選択します。

ステップ 2　syslog サーバを新たに追加する場合は、[Add] をクリックし、[Add Syslog Server] ダイアログボックスを表示します。既存の syslog サーバの設定を変更する場合は、[Edit] をクリックして、[Edit Syslog Server] ダイアログボックスを表示します。

（注）　1 つのセキュリティ コンテキストに対して設定できる syslog サーバの数は最大で 4 です（合計で 16 まで）。

ステップ 3　syslog サーバがビジー状態の場合、ASA または ASASM でキューに入れることができるメッセージ数を指定します。値がゼロの場合は、キューに入れられるメッセージ数が無制限になります。

[Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンにして、いずれかの syslog サーバがダウンした場合にすべてのトラフィックを制限するかどうかを指定します。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。

ステップ 4　以降の手順については、「syslog サーバ設定の追加または編集」（P.41-20）を参照してください。

syslog サーバ設定の追加または編集

syslog サーバ設定を追加または編集するには、次の手順を実行します。

ステップ 1　syslog サーバとの通信に使用するインターフェイスを、ドロップダウン リストから選択します。

ステップ 2　syslog サーバとの通信に使用する IP アドレスを入力します。

syslog サーバが ASA または ASASM との通信に使用するプロトコル（TCP または UDP）を選択します。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。

ステップ 3　syslog サーバにおいて、ASA または ASASM との通信に使用されるポート番号を入力します。

ステップ 4　[Log messages in Cisco EMBLEM format (UDP only)] チェックボックスをオンにして、シスコの EMBLEM 形式でメッセージをログに記録するかどうかを指定します（プロトコルとして UDP が選択されている場合に限る）。

ステップ 5　[Enable secure logging using SSL/TLS (TCP only)] チェックボックスをオンにして、syslog サーバへの接続が SSL/TLS over TCP の使用により保護され、syslog メッセージの内容が暗号化されるよう指定します。

ステップ 6　[OK] をクリックして設定を完了します。

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、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択します。

ステップ 2　[Send syslogs in EMBLEM format] チェックボックスをオンにします。

ステップ 3　以降の手順については、「ロギング フィルタの適用」（P.41-17）を参照してください。

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。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択します。

ステップ 2　[Enable Logging] チェックボックスをオンにします。

ステップ 3　[Logging to Internal Buffer] 領域で、[Save Buffer to Flash] チェックボックスをオンにします。

ステップ 4　[Configure Flash Usage] をクリックします。

[Configure Logging Flash Usage] ダイアログボックスが表示されます。

ステップ 5　ログインに使用するフラッシュ メモリの最大容量を KB で入力します。

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 6　フラッシュ メモリにロギングするために維持する空き領域の最小容量を KB で入力します。

ステップ 7　[OK] をクリックして、このダイアログボックスを閉じます。

ロギング キューの設定

ロギング キューを設定するには、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Logging Setup] の順に選択します。

ステップ 2　[Enable Logging] チェックボックスをオンにします。

ステップ 3　[ASDM Logging] 領域で、設定された出力先に送信する前に ASA および ASASM が自分のキューに保持できる syslog メッセージの数を入力します。

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

ステップ 4　[OK] をクリックして、このダイアログボックスを閉じます。

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、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Logging Filters] の順に選択します。

ステップ 2　指定した出力先の設定オーバーライドするには、変更する出力先を選択してから [Edit] をクリックします。

[Edit Logging Filters] ダイアログボックスが表示されます。

ステップ 3　すべてのイベント クラスからの syslog または特定のイベント クラス領域からの syslog の設定を変更し、[OK] をクリックしてこのダイアログボックスを閉じます。

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。

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、出力先ごとに異なるフィルタリング オプションを選択します。

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、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Syslog Server] の順に選択します。

ステップ 2　セキュア ロギングをイネーブルにする syslog サーバを選択し、[Edit] をクリックします。

[Edit Syslog Server] ダイアログボックスが表示されます。

ステップ 3　[TCP] オプション ボタンをクリックします。

（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。

ステップ 4　[Enable secure syslog with SSL/TLS] チェックボックスをオンにして、[OK] をクリックします。

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、次の手順を実行します。

ステップ 1　ADSM で、[Configuration] > [Device Management] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration] の順に選択します。

ステップ 2　[Enable Syslog Device ID] チェックボックスをオンにします。

ステップ 3　[Device ID] 領域で、[Hostname]、[Interface IP Address]、または [String] オプション ボタンをクリックしてください。

- [Interface IP Address] オプションを選択した場合は、ドロップダウン リストで正しいインターフェイスが選択されていることを確認します。
- [String] オプションを選択した場合は、[User-Defined ID] フィールドにデバイス ID を入力します。文字列の長さは、最大で 16 文字です。

（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。

ステップ 4　[OK] をクリックして、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

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、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Syslog Setup] の順に選択します。

ステップ 2　[Syslog ID Setup] 領域で、[Include timestamp in syslogs] チェックボックスをオンにします。

ステップ 3　[Apply] をクリックして変更内容を保存します。

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、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Syslog Setup] の順に選択します。

ステップ 2　テーブルからディセーブルにする syslog を選択して、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3　[Disable Messages] チェックボックスをオンにし、[OK] をクリックします。

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、次の手順を実行します。

ステップ 1　ASDM で、[Configuration] > [Device Management] > [Logging] > [Syslog Setup] の順に選択します。

ステップ 2　重大度変更したい syslog をテーブルから選択して、[Edit] をクリックします。

[Edit Syslog ID Settings] ダイアログボックスが表示されます。

ステップ 3　適切な重大度を [Logging Level] ドロップダウン リストから選択し、[OK] をクリックします。

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、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Logging] > [Rate Limit] を選択します。

ステップ 2　レート制限を割り当てるロギング レベル（メッセージの重大度）を選択します。重大度レベルは次のように定義されています。

説明	重大度
Emergency	0：システムが使用不能
Alert	1：即時対処が必要
Critical	2：クリティカル条件
Error	3：エラー条件
Warning	4：警告条件
Notification	5：通常の状態だが、重要な状態
Informational	6：情報メッセージだけ
Debugging	7：デバッグ メッセージだけ

ステップ 3　送信されるメッセージの数が [No of Messages] フィールドに表示されます。また、選択したロギング レベルで送信できるメッセージ数を制限する際の基準となる時間間隔（秒単位）が [Interval (Seconds)] フィールドに表示されます。テーブルからロギング レベルを選択し、[Edit] をクリックして [Edit Rate Limit for Syslog Logging Level] ダイアログボックスを表示します。

ステップ 4　以降の手順については、「個々の syslog メッセージに対するレート制限の割り当てまたは変更」（P.41-24）を参照してください。

個々の syslog メッセージに対するレート制限の割り当てまたは変更

個々の syslog メッセージにレート制限を割り当てる、またはメッセージごとにレート制限を変更するには、次の手順を実行します。

ステップ 1　特定の syslog メッセージにレート制限を割り当てる場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 2　以降の手順については、「syslog メッセージのレート制限の追加または編集」（P.41-25）を参照してください。

ステップ 3　特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 4　以降の手順については、「syslog 重大度に対するレート制限の編集」（P.41-25）を参照してください。

syslog メッセージのレート制限の追加または編集

特定の syslog メッセージに対するレート制限を追加または変更するには、次の手順を実行します。

ステップ 1　特定の syslog メッセージに対するレート制限を追加する場合は、[Add] をクリックして、[Add Rate Limit for Syslog Message] ダイアログボックスを表示します。特定の syslog メッセージに対するレート制限を変更する場合は、[Edit] をクリックして、[Edit Rate Limit for Syslog Message] ダイアログボックスを表示します。

ステップ 2　レートを制限する syslog メッセージの ID を入力します。

ステップ 3　指定した時間内に送信できるメッセージの最大数を入力します。

ステップ 4　指定したメッセージのレートを制限する際の基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

（注）　メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

syslog 重大度に対するレート制限の編集

指定した syslog 重大度のレート制限を変更するには、次の手順を実行します。

ステップ 1　指定した重大度で送信可能なメッセージの最大数を指定します。

ステップ 2　指定した重大度のメッセージに対するレートを制限する基準となる時間間隔を秒単位で入力し、[OK] をクリックします。

選択したメッセージ重大度が表示されます。

（注）　メッセージ数を制限なしにする場合は、[Number of Messages] フィールドおよび [Time Interval] フィールドをともにブランクのままにします。

ログのモニタリング

この項では、次のトピックについて取り上げます。

- 「ログ ビューアを使用した syslog メッセージのフィルタリング」（P.41-26）

- 「フィルタリング設定の編集」（P.41-28）
- 「ログ ビューアを使用した特定のコマンドの実行」（P.41-28）

ログ バッファまたはリアルタイムでログをモニタリングし、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、次の手順を実行します。

ステップ 1　ASDM で、次のいずれかを選択してください。

- **[Monitoring] > [Logging] > [Log Buffer] > [View]**
- **[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]**

別のウィンドウのエラーを解決するために、[Real-Time Log Viewer] または [Log Buffer] ダイアログボックスに、メッセージの説明、追加の詳細、必要に応じた推奨処置が表示されます。

ステップ 2　以降の手順については、「ログ ビューアを使用した syslog メッセージのフィルタリング」（P.41-26）を参照してください。

ログ ビューアを使用した syslog メッセージのフィルタリング

Real-Time Log Viewer および Log Buffer Viewer の任意のカラムに対応する 1 つ以上の値に基づいて、syslog メッセージをフィルタリングできます。

ログ ビューアのいずれかを使用して syslog メッセージをフィルタリングするには、次の手順を実行します。

ステップ 1　次のいずれかを選択します。

- **[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]**
- **[Monitoring] > [Logging] > [Log Buffer] > [View]**

ステップ 2　[Real-Time Log Viewer] または [Log Buffer Viewer] ダイアログボックスのいずれかで、ツールバーの [Build Filter] をクリックします。

ステップ 3　[Build Filter] ダイアログボックスで、syslog メッセージに適用するフィルタリング基準を指定します。

a. [Date and Time] 領域で、リアルタイム、特定時刻、または時間範囲の 3 つのオプションの中から 1 つを選択します。特定時刻を選択した場合は、数値を入力してドロップダウン リストから時または分を選択し、時刻を指定します。時間範囲を選択した場合は、[Start Time] フィールドで、ドロップダウンの矢印をクリックしてカレンダーを表示します。ドロップダウン リストから開始日と開始時刻を選択し、[OK] をクリックします。[End Time] フィールドで、ドロップダウンの矢印をクリックしてカレンダーを表示します。ドロップダウン リストから終了日と終了時刻を選択し、[OK] をクリックします。

b. [Severity] フィールドに有効な重大度を入力します。または、[Severity] フィールドの右側で [Edit] アイコンをクリックします。[Severity] ダイアログボックスで、フィルタリングするリストの重大度をクリックします。重大度 1 ～ 7 を含めるには、[All] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。使用する正しい入力形式の詳細については、[Severity] フィールドの右側で [Info] をクリックしてください。

c. [Syslog ID] フィールドに有効な syslog ID を入力します。または、[Syslog ID] フィールドの右側で [Edit] アイコンをクリックします。[Syslog ID] ダイアログボックスで、ドロップダウン リストからフィルタリングの条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの

設定を [Build Filter] ダイアログボックスに表示します。[Delete] をクリックして、これらの設定を削除し、新しい設定を入力します。使用する正しい入力形式の詳細については、[Syslog ID] フィールドの右側で [Info] をクリックしてください。

d. [Source IP Address] フィールドに有効な送信元 IP アドレスを入力するか、または [Source IP Address] フィールドの右側で [Edit] アイコンをクリックします。[Source IP Address] ダイアログボックスで、1 つの IP アドレスまたは指定した IP アドレスの範囲を選択し、[Add] をクリックします。特定の IP アドレスまたは IP アドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。[Delete] をクリックして、これらの設定を削除し、新しい設定を入力します。使用する正しい入力形式の詳細については、[Source IP Address] フィールドの右側で [Info] をクリックしてください。

e. [Source Port] フィールドに有効な送信元ポートを入力するか、または [Source Port] フィールドの右側で [Edit] アイコンをクリックします。[Source Port] ダイアログボックスで、ドロップダウン リストからフィルタリングの条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。[Delete] をクリックして、これらの設定を削除し、新しい設定を入力します。使用する正しい入力形式の詳細については、[Source Port] フィールドの右側で [Info] をクリックしてください。

f. [Destination IP Address] フィールドに有効な宛先 IP アドレスを入力するか、または [Destination IP Address] フィールドの右側で [Edit] アイコンをクリックします。[Destination IP Address] ダイアログボックスで、1 つの IP アドレスまたは指定した IP アドレスの範囲を選択し、[Add] をクリックします。特定の IP アドレスまたは IP アドレスの範囲を除外するには、[Do not include (exclude) this address or range] チェックボックスをオンにします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。[Delete] をクリックして、これらの設定を削除し、新しい設定を入力します。使用する正しい入力形式の詳細については、[Destination IP Address] フィールドの右側で [Info] をクリックしてください。

g. [Destination Port] フィールドに有効な宛先ポートを入力するか、または [Destination Port] フィールドの右側で [Edit] アイコンをクリックします。[Destination Port] ダイアログボックスで、ドロップダウン リストからフィルタリングの条件を選択し、[Add] をクリックします。[OK] をクリックして、これらの設定を [Build Filter] ダイアログボックスに表示します。[Delete] をクリックして、これらの設定を削除し、新しい設定を入力します。使用する正しい入力形式の詳細については、[Destination Port] フィールドの右側で [Info] をクリックしてください。

h. [Description] フィールドにフィルタリング テキストを入力します。このテキストには、正規表現を含む、1 つ以上の文字からなる任意の文字列を指定できます。ただし、セミコロンは有効な文字ではありません。また、この設定では大文字と小文字が区別されます。複数のエントリを指定する場合は、カンマで区切ります。

i. [OK] をクリックして、指定したフィルタリング設定をログ ビューアの [Filter By] ドロップダウン リストに追加します。フィルタ文字列は特定の形式に従います。FILTER: プレフィックスは、[Filter By] ドロップダウン リストに表示されるすべてのカスタム フィルタを示します。このフィールドにはランダムなテキストを入力することもできます。

次の表に、使用される形式の例を示します。

Build Filter の例	フィルタ文字列形式
Source IP = 192.168.1.1 または 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 ～ 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;

725001 ～ 725003 の範囲外の syslog ID	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

ステップ 4　syslog メッセージをフィルタリングするには、[Filter By] ドロップダウン リストでいずれかの設定を選択し、ツールバーで [Filter] をクリックします。この設定は、これ以降のすべての syslog メッセージにも適用されます。すべてのフィルタをクリアするには、ツールバーで [Show All] をクリックします。

（注）　[Build Filter] ダイアログボックスを使用して指定したフィルタは保存できません。これらのフィルタは、そのフィルタが作成された ASDM セッションのみで有効です。

フィルタリング設定の編集

[Build Filter] ダイアログボックスを使用して作成したフィルタリングを編集するには、次の手順を実行します。

次のいずれかを選択します。

- [Filter By] ドロップダウン リストで変更を入力して、フィルタを直接修正する。
- [Filter By] ドロップダウン リストでフィルタを選択し、[Build Filter] をクリックして [Build Filter] ダイアログボックスをクリックする。現在のフィルタリング設定を削除して新しい設定を入力するには、[Clear Filter] をクリックします。それ以外の場合は、表示された設定を変更して [OK] をクリックします。

  （注）　これらのフィルタリング設定は、[Build Filter] ダイアログボックスで定義されたフィルタのみに適用されます。

- フィルタリングを停止して、すべての syslog メッセージを表示するには、ツールバーで [Show All] をクリックします。

ログ ビューアを使用した特定のコマンドの実行

ログ ビューアのいずれかを使用して、**ping**、**traceroute**、**whois**、および **dns lookup** のコマンドを実行できます。

これらのコマンドのいずれかを実行するには、次の手順を実行します。

ステップ 1　次のいずれかを選択します。

- **[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]**
- **[Monitoring Logging] > [Log Buffer] > [View]**

ステップ 2　[Real-Time Log Viewer] または [Log Buffer] ペインから [Tools] をクリックし、実行するコマンドを選択します。または、表示された特定の syslog メッセージを右クリックしてコンテキスト メニューを表示し、実行するコマンドを選択します。

[Entering command] ダイアログボックスが表示され、選択したコマンドが自動的にドロップダウン リストに表示されます。

ステップ 3　選択した syslog メッセージの送信元 IP アドレスまたは宛先 IP アドレスのいずれかを [Address] フィールドに入力し、[Go] をクリックします。

指定した領域にコマンド出力が表示されます。

ステップ 4　[Clear] をクリックして出力を削除し、実行する別のコマンドをドロップダウン リストから選択します。必要に応じてステップ 3 を繰り返します。完了したら [Close] をクリックします。

ロギングの機能履歴

表 41-2 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 41-2　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。 次の画面が導入されました。[Configuration] > [Device Management] > [Logging] > [Logging Setup]。
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。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Rate Limit]。
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。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Event Lists]。
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。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Syslog Server]。
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。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Filters]。

表 41-2　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
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。 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。 次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Setup]。
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。
ログ ビューア	8.3(1)	送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。
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、[Configuration] > [Device Management] > [Logging] > [Syslog Servers] ペインで [Allow user traffic to pass when TCP syslog server is down] チェックボックスをオンのままにしておきます。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。 変更された ASDM 画面はありません。
syslog メッセージのフィルタリングとソート	8.4(1)	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージ フィルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、ASDM 設定ガイドを参照してください。 次の画面が変更されました。 [Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]。 [Monitoring] > [Logging] > [Log Buffer Viewer] > [View]。 この機能は、すべての ASA バージョンと相互運用性があります。
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。 次の画面が変更されました。 [Configuration] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration]。