# ログ

この章では、システム メッセージを記録して、トラブルシューティングに使用する方法について説明します。



## ロギングの概要

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、簡単な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、ログ用の保護された長期ストレージを提供します。ログは、ルーチンの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、Secure Firewall ASA のモニタリングおよびトラブルシューティングに必要な情報が得られます。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無効化または変更する。
- 次のような syslog メッセージ送信先を 1 つ以上指定する。
  - 内部バッファ
  - 1 台以上の syslog サーバ
  - ASDM
  - SNMP 管理ステーション

- 指定の電子メール アドレス
- コンソール
- Telnet および SSH セッション。

- 重大度レベルやメッセージ クラスなどによる、グループ内での syslog メッセージを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、重大度レベル、クラス、またはカスタム メッセージ リストにより、syslog メッセージをフィルタリングする。

# 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、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの 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 は、各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 サーバー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 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 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 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。
- ユーザー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の記号（%）で始まり、次のように構造化されています。

```
%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 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。 |
| レベル | 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。 |
| *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、またはユーザー名が含まれていることがあります。 |

# 重大度

次の表に、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 メッセージの色設定を行うには、[ツール（Tools）]>[設定（Preferences）]>[Syslog（Syslog）] タブを選択するか、またはログ ビューア自体のツールバーで [色の設定（Color Settings）] をクリックします。

**表 *1 : Syslog* メッセージの重大度**

| レベル番号 | 重大度 | 説明 |
|---|---|---|
| **0** | **emergencies** | システムが使用不可能な状態です。 |

| レベル番号 | 重大度 | 説明 |
|---|---|---|
| **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**（通告） | 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。<br>問題をデバッグするときに、このレベルで一時的にのみログに記録します。このログレベルでは、非常に多くのメッセージが生成される可能性があるため、システムパフォーマンスに影響を与える可能性があります。 |

（注） ASA は、重大度 0（緊急）の syslog メッセージを生成しません。

# syslog メッセージ 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、Secure Firewall ASA 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 クラス（機能エリアと同等）

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 Secure Firewall ASA を設定することもできます。

# syslog メッセージ クラス

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。

- syslog メッセージのカテゴリ全体の出力場所を指定します。
- メッセージ クラスを指定するメッセージ リストを作成します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

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 メッセージ生成時にオブジェクトが不明な場合、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レイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

**表 *2 : syslog* メッセージのクラスおよび関連付けられているメッセージ *ID* 番号**

| クラス | 定義 | Syslog メッセージ ID 番号 |
|---|---|---|
| auth | ユーザ認証 | 109、113 |
| — | アクセス リスト | 106 |
| — | アプリケーション ファイアウォール | 415 |
| bridge | トランスペアレント ファイアウォール | 110、220 |
| ca | PKI 証明機関 | 717 |
| citrix | Citrix クライアント | 723 |
| — | クラスタリング | 747 |
| — | カード管理 | 323 |
| config | コマンド インターフェイス | 111、112、208、308 |
| csd | セキュアなデスクトップ | 724 |
| cts | Cisco TrustSec | 776 |

| クラス | 定義 | Syslog メッセージ ID 番号 |
|---|---|---|
| dap | ダイナミック アクセス ポリシー | 734 |
| eap、eapoudp | ネットワーク アドミッション コントロール用の EAP または EAPoUDP | 333、334 |
| eigrp | EIGRP ルーティング | 336 |
| email | 電子メール プロキシ | 719 |
| — | 環境モニタリング | 735 |
| ha | フェールオーバー | 101、102、103、104、105、210、311、709 |
| — | Identity-Based ファイアウォール | 746 |
| ids | 侵入検知システム | 400、733 |
| — | IKEv2 ツールキット | 750、751、752 |
| ip | IP スタック | 209、215、313、317、408 |
| ipaa | IP アドレスの割り当て | 735 |
| ips | 侵入防御システム | 400、401、420 |
| — | IPv6 | 325 |
| — | ボットネット トラフィック フィルタリング | 338 |
| — | ライセンシング | 444 |
| mdm-proxy | MDM プロキシ | 802 |
| nac | ネットワーク アドミッション コントロール | 731、732 |
| nacpolicy | NAC ポリシー | 731 |
| nacsettings | NAC ポリシーを適用するための NAC 設定 | 732 |
| — | ネットワーク アクセス ポイント | 713 |
| np | ネットワーク プロセッサ | 319 |
| — | NP SSL | 725 |
| ospf | OSPF ルーティング | 318、409、503、613 |
| — | パスワードの暗号化 | 742 |
| — | Phone Proxy | 337 |

| クラス | 定義 | Syslog メッセージ ID 番号 |
|---|---|---|
| rip | RIP ルーティング | 107、312 |
| rm | Resource Manager | 321 |
| — | Smart Call Home | 120 |
| 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 |
| snmp | SNMP | 212 |
| — | ScanSafe | 775 |
| ssl | SSL スタック | 725 |
| svc | SSL VPN クライアント | 722 |
| sys | システム | 199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741 |
| — | 脅威の検出 | 733 |
| tre | トランザクション ルール エンジン | 780 |
| — | UC-IME | 339 |
| tag-switching | サービス タグ スイッチング | 779 |
| vm | VLAN マッピング | 730 |
| 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 |
| vpnc | VPN クライアント | 611 |
| vpnfo | VPN フェールオーバー | 720 |
| vpnlb | VPN ロード バランシング | 718 |
| — | VXLAN | 778 |
| webfo | WebVPN フェールオーバー | 721 |
| webvpn | WebVPN および AnyConnect クライアント | 716 |
| — | NAT および PAT | 305 |

# ログ ビューアのメッセージのソート

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

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 メッセージのリストで、次の条件のいずれかまたはすべてを使用して syslog メッセージのグループを指定します。

- 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

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。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。メッセージリストの2つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

# クラスタ

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、モニターリング、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 サーバーは、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ーするには、モニター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。

# ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

### IPv6 のガイドライン

- IPv6 がサポートされます。Syslog は、TCP または UDP を使用して送信できます。
- syslog 送信用に設定されたインターフェイスが有効であること、IPv6 対応であること、および syslog サーバが指定インターフェイス経由で到達できることを確認します。
- Ipv6 を介したセキュア ロギングはサポートされていません。

### その他のガイドライン

- syslog サーバでは、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 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。
- Secure Firewall ASA 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、Secure Firewall ASA 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 サーバーを指定するには、各 syslog サーバーの **[Syslog Server]** ペインで、個別のエントリを指定します。
- スタンドバイ デバイスでは、TCP 上での syslog の送信はサポートされません。
- トランスポートプロトコルとして TCP を使用する場合、メッセージが失われないように syslog サーバーへの接続が 4 つ開きます。syslog サーバーを使用して非常に多数のデバイスからメッセージを収集する場合、接続オーバーヘッドの合計がサーバーに対して大きすぎる場合は、代わりに UDP を使用します。
- 2 つの異なるリストまたはクラスを異なる syslog サーバーまたは同じ場所に割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。ただし、マルチ コンテキスト モードでは、コンテキストごとに 4 サーバーに制限されています。

- syslog サーバは、Secure Firewall ASA 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスが ICMP 到達不能メッセージを拒否し、同じサーバに syslog を送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバーがクラッシュしないようにするため、syslog 313001、313004、および 313005 の生成を抑制します。
- syslog の UDP 接続の数は、ハードウェア プラットフォームの CPU の数と、設定する syslog サーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定する syslog サーバの数を乗算した値と同じになります。たとえば各 syslog サーバでは次のようになります。
  - Firepower 4110 では最大 22 の UDP syslog 接続が可能です。
  - Firepower 4120 では最大 46 の UDP syslog 接続が可能です。

  これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは2分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。
- 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も変更する必要があります。

  ロギング重大度がデバッグに変更されたため、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次に示します。

```
ciscoasa# 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。

```
ciscoasa# 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。

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

```
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- Secure Firewall ASA が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。
- syslog サーバーから受信したサーバー証明書には、[拡張キーの使用（Extended Key Usage）] フィールドに「ServAuth」が含まれている必要があります。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

# ロギングの設定

ここでは、ロギングの設定方法について説明します。

## ロギングの有効化

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。

**手順**

**ステップ 1** ASDM で、次のいずれかを選択します。

- **[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。

## 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ーリング用に 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 サーバー、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。

管理専用アクセスが有効になっているインターフェイスで syslog ロギングを設定した場合、データプレーン関連のログ（syslog ID 302015、302014、106023、および 304001）はドロップされて syslog サーバーに到達しません。これらの syslog メッセージがドロップされるのは、

データパス ルーティング テーブルに管理インターフェイスのルーティングがないためです。したがって、設定するインターフェイスで管理専用アクセスが無効になっていることを確認してください。

## 外部 syslog サーバーへの syslog メッセージの送信

外部syslogサーバー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ときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

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

### 手順

**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、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 サーバー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、syslog メッセージを保存する内部ログ バッファのサイズを指定します。バッファの空き容量がなくなると、FTPサーバー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 サーバーに保存する場合は、[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 サーバーを指定し、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。

**ステップ 9** [Save Buffer To Flash] チェックボックスをオンにして、上書きする前に内部フラッシュ メモリにバッファの内容を保存します。

（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。

（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** ASA で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 サーバー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。

### 手順

**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** FTP サーバーの IP アドレスを指定します。

**ステップ 3** 保存されるログ バッファ コンテンツの格納先となる FTP サーバー上のディレクトリ パスを指定します。

**ステップ 4** FTP サーバーにログインするためのユーザー名を指定します。

**ステップ 5** FTP サーバーへログインするためのユーザー名に関連付けられたパスワードを指定します。

**ステップ 6** パスワードを確認し、[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。

### 手順

**ステップ 1** 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指定します（KB 単位）。

**ステップ 2** 維持する内部フラッシュ メモリの容量を指定します（KB 単位）。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、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

## セキュア ロギングの有効化

### 手順

**ステップ 1** **[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 サーバーを選択し、[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。

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。

**ステップ 5** （任意） [Reference Identity] に、syslog サーバーから受信した証明書に対する RFC 6125 参照 ID チェックをイネーブルにする参照 ID オブジェクトを名前で指定します。

参照 ID オブジェクトについて詳しくは、参照 ID の設定を参照してください。

## syslog サーバーに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバーへの 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。

### 手順

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

IPv6 を介した syslog の送信がサポートされています。

**ステップ 2** [Add] をクリックして、新しい syslog サーバを追加します。

[Add Syslog Server] ダイアログボックスが表示されます。

（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 サーバーの数は最大で 4 です（合計で 16 まで）。

**ステップ 3** syslog サーバーがビジー状態の場合、ASA 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。

**ステップ 4** [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、syslog サーバーがダウンしている場合にすべてのトラフィックを許可するように設定します。

ASA では、TCP 接続された syslog サーバーに syslog メッセージを送信するように設定されている場合、syslog サーバーに障害が発生すると、セキュリティ保護のために ASA を経由する新しい接続をブロックします。syslog サーバーが動作していない場合でも新しい接続を許可するには、このチェックボックスをオンにします。

UDP を指定すると、ASA は、syslog サーバー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、次の手順を実行します。

### 手順

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

**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。

## syslog サーバーの設定の追加または編集

syslog サーバー設定を追加または編集するには、次の手順を実行します。

### 手順

**ステップ 1** syslogサーバー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 サーバーとの通信に使用する IP アドレスを入力します。

syslog サーバーが 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 サーバーにデータを送信するように ASA および ASASM を設定することができます。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。

警告 TCP を指定すると、ASA は syslog サーバーの障害を検出したときに、セキュリティ上の理由で ASA を経由する新しい接続をブロックします。syslog サーバーに障害が発生しても新しい接続を許可するには、syslog サーバーに送信する EMBLEM 形式の syslog メッセージの生成 （14 ページ）のステップ 4 を参照してください。

**ステップ 3** syslog サーバーにおいて、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 サーバーへの接続が 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。

## 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、ASA 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。

### 手順

**ステップ 1** 次のいずれかのオプションを選択して、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。

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

**ステップ 2** **[Monitoring]** > **[Logging]** > **[Log Buffer]** > **[View]** の順に選択します。次に [Log Buffer] ペインで **[File]** > **[Clear Internal Log Buffer]** の順に選択して、内部ログ バッファを空にします。

**ステップ 3** **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** の順に選択して、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。

ASA 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 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て、[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。
  1. 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。
  2. 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。

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。

- FTP サーバー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。

  1. [Enable FTP Client] チェックボックスをオンにします。
  2. 表示されたフィールドに、FTP サーバー IP アドレス、パス、ユーザー名、パスワードを入力します。
  3. 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 バッファのフラッシュへの保存

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。

### 手順

**ステップ 1** **[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。

## ログの記録で使用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。

### 手順

**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ます。

**ステップ 3** [Logging to Internal Buffer] 領域の [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** ログインに使用できるフラッシュ 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1MBをログデータに使用できます。ASA 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に保存されているログファイルにより、内部フラッシュメモリの空き容量が設定された最小限の容量を下回ってしまう場合、ASAは最も古いログファイルを削除し、新しいログファイルの保存後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い場合、または古いファイルをすべて削除しても空きメモリの容量が最小限の容量を下回っている場合、ASA 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、[Configure Logging Flash Usage] ダイアログボックスを閉じます。

### 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。

**手順**

**ステップ 1** **[Tools]** > **[ASDM Java Console]** の順に選択します。

**ステップ 2** コンソールで **m** と入力して、仮想マシンのメモリ統計情報を表示します。

**ステップ 3** コンソールで **g** と入力して、ガベージ コレクションを実行します。

**ステップ 4** Windows タスク マネージャを開き、**asdm_launcher.exe** ファイルをダブルクリックして、メモリ使用量を監視します。

（注） メモリ割り当ての最大値は 256 MB です。

## 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。

**手順**

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

**ステップ 2** 電子メール メッセージとして送信される syslog メッセージの送信元アドレスとして使用する電子メール アドレスを指定します。

**ステップ 3** [追加（Add）] をクリックして、指定した syslog メッセージの受信者の新しい電子メール アドレスを入力します。

**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。

**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。

**ステップ 6** [OK] をクリックして、[Add E-mail Recipient] ダイアログボックスを閉じます。

## 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。

### 手順

**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、[Add/Edit E-Mail Recipient] 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 サーバーの設定

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 サーバーを設定するには、次の手順を実行します。

**手順**

**ステップ 1** **[Configuration]** > **[Device Setup]** > **[Logging]** > **[SMTP]** の順に選択します。

**ステップ 2** プライマリ SMTP サーバーの IP アドレスを入力します。

**ステップ 3** （任意）スタンバイ SMTP サーバーの 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。

## 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。

**手順**

**ステップ 1** 次のいずれかのオプションを選択します。

- **[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** すべてのイベント クラスまたは特定のイベント クラスのいずれかから syslog を選択して、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。

## 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。

**手順**

**ステップ 1** 次のいずれかのオプションを選択します。

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

**ステップ 2** [Logging Destination] カラムの [Telnet and SSH Sessions] 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** すべてのイベント クラスまたは特定のイベント クラスのいずれかから syslog を選択して、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 4** **[Configuration]** > **[Device Management]** > **[Logging]** > **[Logging Setup]** の順に選択して、現在のセッションのロギングだけをイネーブルにします。

**ステップ 5** [Enable logging] チェックボックスをオンにし、[Apply] をクリックします。

# syslog メッセージの設定

## 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。

### 手順

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

**ステップ 2** ファイル メッセージのベースとして使用する syslog サーバーのシステム ログ機能を選択します。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** [Include timestamp in syslogs] チェックボックスをオンにして、送信される各 syslog メッセージに日付と時刻を追加します。

[Timestamp Format] ドロップダウンを使用して、レガシー（mm: dd: yyyy hh: mm: ss）または RFC 5424（yyyy: Dd: mmTHH: Mm: ssz）形式を選択します。

**ステップ 4** ログイン試行が失敗した場合に無効なユーザー名を syslog メッセージに表示する場合は、[Hide username if its validity cannot be determined] チェックボックスをオフにします。デフォルト設定では、ユーザー名が無効な場合、または有効かどうか不明な場合、ユーザー名は非表示です。たとえば、ユーザーが誤ってユーザー名の代わりにパスワードを入力した場合、結果として生成される syslog メッセージで「ユーザー名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザー名を表示することもできます。

**ステップ 5** [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。

- [Syslog ID] テーブルにすべての syslog メッセージ ID を表示するように指定するには、[Show all syslog IDs] を選択します。
- [Syslog ID] テーブルに明示的にディセーブルにした syslog メッセージ ID だけを表示するように指定するには、[Show disabled syslog IDs] を選択します。
- [Syslog ID] テーブルにデフォルト値から変更された重大度を含む syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs with changed logging] を選択します。

- [Syslog ID] テーブルに重大度が変更された syslog メッセージ ID と、明示的にディセーブルにされた syslog メッセージ ID だけを表示するように指定するには、[Show syslog IDs that are disabled or with a changed logging level] を選択します。

**ステップ 6** [Syslog ID Setup] テーブルには、その設定内容に基づいて、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 7** 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。

## 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。

### 手順

**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** [Syslog ID(s)] リストに表示される syslog メッセージ ID に送信するメッセージの重大度のロギング 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 [Edit Syslog ID Settings] 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。

**手順**

**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 control's IP address for the selected interface] チェックボックスをオンにします。
- 文字列

  英数字のユーザー定義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、[Advanced Syslog Configuration] ダイアログボックスを閉じます。

## syslog メッセージに日付と時刻を含める

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。

**手順**

**ステップ 1** **[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 メッセージの無効化

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。

手順

ステップ 1 **[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。

手順

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

ステップ 2 重大度を変更する 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。

## スタンバイ装置の syslog メッセージのブロック

スタンバイ装置で特定の syslog メッセージが生成されないようにするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Logging]** > **[Syslog Settings]** の順に選択します。

ステップ 2 テーブルの syslog ID を選択し、[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 スタンバイ装置で syslog メッセージが生成されないようにするには、[Disable messages on standby unit] チェックボックスをオンにします。

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。

## 非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

**ステップ 1** **[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ます。

- [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。

# 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 サーバーなど）に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

**ステップ 1** **[Configuration]** > **[Device Management]** > **[Logging]** > **[Event Lists]** の順に選択します。

**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** 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** [Add] をクリックして、[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、[Add Event List] ダイアログボックスを閉じます。

**ステップ 8** [Add] をクリックして、[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** 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、[Add Event List] 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。

# ロギング フィルタの設定

## 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。

**手順**

**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 サーバー
- Syslog サーバー

- 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。

**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 （27 ページ）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。

### 手順

**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。イベント リストを新たに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 （25 ページ）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。

## 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（22 ページ）を参照してください。

## 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。

### 手順

**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。

## 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。

### 手順

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

**ステップ 2** 指定した出力先の設定を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** [Syslogs from All Event Classes] または [Syslogs from Specific Event Classes] 領域のいずれかで設定を変更し、[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。

# syslog メッセージの生成レートの制限

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。

### 手順

**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。

- Emergency（レベル 0、システムが使用不能）
- 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** 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（30 ページ）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。

### 手順

**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メッセージに対するレート制限の追加または編集（30ページ）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（31 ページ）を参照してください。

## syslog メッセージに対する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。

### 手順

**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。

**手順**

**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。

# ログのモニターリング

ロギング ステータスの監視については、次のコマンドを参照してください。

- **[Monitoring] > [Logging] > [Log Buffer] > [View]**

  このペインでは、ログ バッファを表示できます。

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

  このペインでは、リアルタイムのログを表示できます。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

# 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

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。

### 手順

**ステップ 1** 次のいずれかのオプションを選択します。

- **[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、時間範囲の 3 つのオプションから 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、[Start Time] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。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] フィールドのドロップダウン矢印をクリックすると、カレンダーが表示されます。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。フィルタリングする重大度をリストでクリックします。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に関する詳細な情報については、[Severity] フィールドの右側にある [Info] アイコンをクリックします。

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] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウンリストからフィルタ対象の条件を選択し、[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。使用する正しい入力形式に関する詳細な情報については、[Syslog ID] フィールドの右側にある [Info] アイコンをクリックします。

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。単一の IP アドレスまたは IP アドレスの特定の範囲を選択し、[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て、[OK] をクリックし、[Build Filter] ダイアログボックスにこれらの設定を表示します。使用する正しい入力形式に関する詳細な情報については、[Source IP Address] フィールドの右側にある [Info] アイコンをクリックします。

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] フィールドの右側の [Edit] アイコンをクリックします。ドロップダウンリストからフィルタ対象の条件を選択し、[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。使用する正しい入力形式に関する詳細な情報については、[Source Port] フィールドの右側にある [Info] アイコンをクリックします。

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。単一の IP アドレスまた

はIPアドレスの特定の範囲を選択し、[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。使用する正しい入力形式に関する詳細な情報については、[Destination IP Address]フィールドの右側にある[Info]アイコンをクリックします。

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]フィールドの右側の[Edit]アイコンをクリックします。ドロップダウン リストからフィルタ対象の条件を選択し、[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。使用する正しい入力形式に関する詳細な情報については、[Destination Port]フィールドの右側にある[Info]アイコンをクリックします。

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<br>Source Port = 67 | FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67; |
| Severity = Informational<br>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<br>Description = Built outbound | FILTER: srcIP=1.1.1.1;descr=Built outbound |

**ステップ 4** [Filter By]ドロップダウン リストの設定の1つを選択し、ツールバーの[Filter]をクリックして、syslogメッセージをフィルタリングします。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、ツールバーにある[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設定を編集するには、次の手順を実行します。

**手順**

次のいずれかのオプションを選択します。

- [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します。
- [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表示します。[Clear Filter] をクリックして、現在のフィルタ設定を削除し、新しい値を入力します。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。

- ツールバーの [Show All] をクリックすると、フィルタリングが停止し、すべての syslog メッセージが表示されます。

# ログ ビューアを使用した特定のコマンドの発行

いずれかのログ ビューアを使用して、**ping**、**traceroute**、**whois**、および **dns lookup** コマンドを発行できます。

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。

**手順**

**ステップ 1** 次のいずれかのオプションを選択します。

- **[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。

# ロギングの履歴

**表 *3:* ロギングの履歴**

| 機能名 | プラットフォームリリース | 説明 |
|---|---|---|
| Logging | 7.0(1) | さまざまな出力先を経由して 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。<br>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。<br>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。<br>次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Event Lists]。 |

| 機能名 | プラットフォームリリース | 説明 |
| --- | --- | --- |
| 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。<br>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。<br>次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Logging Filters]。 |
| 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。<br>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。<br>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。 |

| 機能名 | プラットフォームリリース | 説明 |
| --- | --- | --- |
| 拡張ロギングと接続ブロック | 8.3(2) | TCP を使用するように syslog サーバーを設定すると、syslog サーバーを使用できない場合、ASA はサーバー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。<br><br>この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも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にします。<br><br>414005、414006、414007、414008 の各 syslog メッセージが導入されました。<br><br>変更された ASDM 画面はありません。 |

| 機能名 | プラットフォームリリース | 説明 |
| --- | --- | --- |
| 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。<br>• 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。<br>• カスタム フィルタの作成。<br>• メッセージのカラムによるソート。詳細については、『ASDM 構成ガイド』を参照してください。<br>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。<br>次の画面が変更されました。<br>[Monitoring] > [Logging] > [Real-Time Log Viewer] > [View]。<br>[Monitoring] > [Logging] > [Log Buffer Viewer] > [View]。 |
| クラスタ | 9.0(1) | ASA 5580 および 5585-X のクラスタリング環境での syslog メッセージ生成のサポートが追加されました。<br>次の画面が変更されました。[Configuration] > [Logging] > [Syslog Setup] > [Advanced] > [Advanced Syslog Configuration]。 |
| スタンバイ装置の syslog のブロック | 9.4(1) | フェールオーバー コンフィギュレーションのスタンバイ装置で特定の syslog メッセージの生成をブロックするためのサポートを追加しました。<br>次の画面が変更されました。[Configuration] > [Device Management] > [Logging] > [Syslog Setup]。 |

| 機能名 | プラットフォームリリース | 説明 |
| --- | --- | --- |
| syslog サーバーのセキュアな接続のための参照 ID | 9.6(2) | TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 検証は、syslog サーバーサーバーへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。<br><br>次のページが変更されました。[ASDM Configuration] > [Remote Access VPN] > [Advanced] および [Configuration] > [Device Management] > [Logging] > [Syslog Servers -> Add or Edit] |
| syslog サーバーでの IPv6 アドレスのサポート | 9.7(1) | TCP と UDP 経由で syslog を記録、送信、受信するために、syslog サーバーを IPv6 アドレスで設定できるようになりました。<br><br>次の画面が変更されました。**[Configuration] > [Device Management] > [Logging] > [Syslog Servers] > [Add Syslog Server]** |