



ロギングの設定

ロギング機能では、ロギングをイネーブルにしてログ情報の処理方法を指定できます。ログ表示機能では、リアルタイムでシステム ログ メッセージを表示できます。ログ表示機能の詳細については、[第 41 章「ロギングのモニタリング」](#)を参照してください。

ロギングの概要

セキュリティ アプライアンスは、アクティビティ（許可または拒否されたネットワーク トラフィックのタイプなど）を説明するシステム ログ メッセージの監査証跡の生成をサポートし、システム ロギングの設定を可能にします。

すべてのシステム ログ メッセージには、デフォルトの重大度レベルが設定されています。メッセージには、必要に応じて新しい重大度レベルを再割り当てできます。重大度レベルを選択するとき、そのレベルから下位のレベルへのロギング メッセージが生成されます。上位レベルからのメッセージは含まれません。重大度レベルが高いほど、含まれるメッセージは多くなります。ロギングおよびシステム ログ メッセージの詳細については、『*Cisco Security Appliance System Log Messages Guide*』を参照してください。

ロギングのセキュリティ コンテキスト

各セキュリティ コンテキストは、ロギング コンフィギュレーションがあり、メッセージを生成します。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たシステム ログ メッセージにはフェールオーバー メッセージが含まれており、管理コンテキストで生成されたメッセージとともに管理コンテキストで表示されます。システム実行スペースで、ロギングを設定したり、ロギング情報を表示したりすることはできません。

各メッセージにコンテキスト名を表示するようにセキュリティ アプライアンスを設定できます。単一の `syslog` サーバに送信されるコンテキスト メッセージを区別するのに役立ちます。この機能を使用すると、管理コンテキストで生成されたメッセージとシステムで生成されたメッセージを判別できます。システム実行スペースから送信されたメッセージはデバイス ID `system` を使用し、管理コンテキストから送信されたメッセージはデバイス ID として管理コンテキスト名を使用します。デバイス ID を使用するには、[P.15-7 の「Advanced Syslog Configuration」](#)を参照してください。

ログिंगの使用

セキュリティ コンテキストを定義したら、**Configuration > Device Management > Logging** を選択します。Logging では、次の操作を実行できます。

-
- ステップ 1** Logging Setup ペインで、ログングをイネーブルにし、ログング パラメータを設定します。詳細については、[P.15-3 の「Logging Setup」](#) を参照してください。
 - ステップ 2** Syslog Setup ペインでは、syslog サーバに送信されるシステム ログ メッセージにファシリティのコードを含めるように設定したり、各メッセージにタイムスタンプを含めるように指定したり、メッセージの重大度レベルを表示または変更したり、メッセージを抑止したりします。詳細については、[P.15-6 の「Syslog Setup」](#) を参照してください。
 - ステップ 3** E-Mail Setup ペインで、通知を目的として電子メールで送信されるシステム ログ メッセージを指定します。詳細については、[P.15-6 の「Syslog Setup」](#) を参照してください。
 - ステップ 4** Event Lists ペインで、記録するメッセージを指定するイベントのカスタム リストを作成します。ここで作成したリストは、ログ フィルタのセットアップ時に使用されます。詳細については、[P.15-10 の「Event Lists」](#) を参照してください。
 - ステップ 5** Logging Filters ペインで、各ログの宛先に送信されるメッセージのフィルタリングに使用する基準を指定します。フィルタの作成に使用する基準とは、重大度レベル、メッセージクラス、メッセージ ID、またはイベントリストです。詳細については、[P.15-13 の「Logging Filters」](#) を参照してください。
 - ステップ 6** Rate Limit ペインで、指定した時間間隔に生成可能なメッセージ数を制限します。詳細については、[P.15-17 の「Rate Limit」](#) を参照してください。
 - ステップ 7** Syslog Server ペインで、セキュリティ アプライアンスがシステム ログ メッセージを送信する syslog サーバを 1 つ以上指定します。詳細については、[P.15-20 の「Syslog サーバ」](#) を参照してください。
 - ステップ 8** SMTP ペインで、ASDM が電子メール アラートと通知メッセージを送信する宛先となる SMTP サーバを 1 つ以上指定します。詳細については、[P.15-21 の「SMTP」](#) を参照してください。
-

Logging Setup

Logging Setup ペインでは、セキュリティ アプライアンスでのシステム ログインをイネーブルにして、スタンバイ装置がログインを引き継ぐかどうか、デバッグ メッセージを送信するかどうか、EMBLEM 形式を使用するかどうかなど、一般ログイン パラメータを指定できます。また、内部ログ バッファやセキュリティ アプライアンスのログイン キューのデフォルト設定も変更できます。このペインにアクセスするには、**Configuration > Device Management > Logging > Logging Setup** を選択します。

フィールド

- **Enable logging** : メイン セキュリティ アプライアンスのログインをオンにします。
- **Enable logging on the failover standby unit** : 使用可能な場合は、スタンバイ セキュリティ アプライアンスのログインをオンにします。
- **Send debug messages as syslog** : すべてのデバッグ トレース出力をシステム ログにリダイレクトします。このオプションがイネーブルになっている場合、システム ログ メッセージはコンソールに表示されません。したがって、デバッグ メッセージを表示するには、コンソールでログインをイネーブルにし、デバッグ システム ログ メッセージ番号および重大度レベルの宛先として設定する必要があります。使用するシステム ログ メッセージ番号は、**711001** です。このシステム ログ メッセージのデフォルトの重大度レベルは **debug** です。
- **Send syslog in EMBLEM format** : syslog サーバ以外のすべてのログの宛先に使用するため、EMBLEM 形式をイネーブルにします。
- **Buffer Size** : ログイン バッファがイネーブルになっている場合に、システム ログ メッセージが保存される内部ログ バッファのサイズを指定します。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、バッファがいっぱいになったとき、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。指定できる範囲は、**4096 ~ 1048576** バイトです。
- **Save Buffer To FTP Server** : 上書きされる前にバッファの内容を FTP サーバに保存するには、このチェックボックスをオンにします。バッファの内容の上書きを許可するには、このチェックボックスをオフにします。
- **Configure FTP Settings** : FTP サーバを示し、バッファの内容の保存に使用する FTP パラメータを設定します。
- **Save Buffer To Flash** : 上書きされる前にバッファの内容を内部フラッシュ メモリに保存するには、このチェックボックスをオンにします。



(注) このオプションは、ルーテッドまたは透過シングルモードでのみ使用できます。

- **Configure Flash Usage** : ログインのために内部フラッシュ メモリで使用される最大容量および維持する最小空き容量を KB で指定します。このオプションをオンにすると、「syslog」という名前のディレクトリが、メッセージの格納先のデバイス ディスクに作成されます。



(注) このオプションは、ルーテッドまたは透過シングルモードでのみ使用できます。

- **Queue Size** : セキュリティ アプライアンスで表示されるシステム ログのキュー サイズを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

詳細情報

- P.15-4 の「Configure FTP Settings」を参照してください。
- P.15-5 の「Configure Logging Flash Usage」を参照してください。

Configure FTP Settings

Configure FTP Settings ダイアログボックスでは、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できます。

フィールド

- Enable FTP client : 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。
- Server IP Address : FTP サーバの IP アドレスを指定します。
- Path : 保存されたログ バッファの内容を格納する FTP サーバへのディレクトリ パスを指定します。
- Username : FTP サーバにログインするためのユーザ名を指定します。
- Password : FTP サーバに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指定します。
- Confirm Password : パスワードを確認します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Configure Logging Flash Usage

Configure Logging Flash Usage ダイアログボックスでは、ログ バッファの内容を内部フラッシュ メモリに保存するときの制限を指定できます。

フィールド

- **Maximum Flash to Be Used by Logging** : ログ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 で指定します。
- **Minimum Free Space to Be Preserved** : 保持する内部フラッシュ メモリの容量を、KB で指定します。内部フラッシュメモリが制限値に近づくと、新しいログが保存されなくなります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	—	—

Syslog Setup

Syslog Setup ペインでは、syslog サーバを宛先とするメッセージにファシリティ コードを含めるように設定し、システム ログ メッセージにタイムスタンプを含める必要があるかどうかを決定できます。また、メッセージの重大度レベルを変更したり、記録しないメッセージを抑止したりもできます。このペインにアクセスするには、**Configuration > Device Management > Logging > Syslog Setup** を選択します。

フィールド

- **Facility code to include in syslogs** : syslog サーバのシステム ログ ファシリティを、ファイル メッセージの基本として使用するよう指定します。デフォルトは LOCAL(4)20 で、ほとんどの UNIX システムで想定されているコードです。ただし、ネットワーク デバイスでは使用可能な 8 つのファシリティを共有しているため、システム ログのこの値を変更しなければならない場合があります。
- **Include timestamp in syslogs** : 送信されるすべてのシステム ログ メッセージに日付と時刻を含めます。
- **Syslog ID Setup** : Syslog ID テーブルに表示される情報を選択します。オプションは次のように定義されています。
 - **Show all syslog IDs** : Syslog ID テーブルで、システム ログ メッセージ ID のリスト全体を表示するように指定します。
 - **Show suppressed syslog IDs** : Syslog ID テーブルで、明示的に抑止されたシステム ログ メッセージ ID のみを表示するように指定します。
 - **Show syslog IDs with changed logging** : Syslog ID テーブルで、デフォルト値から変更された重大度レベルを持つシステム ログ メッセージ ID のみを表示するように指定します。
 - **Show syslog IDs that are suppressed or with a changed logging level** : Syslog ID テーブルで、重大度レベルが変更されたシステム ログ メッセージ ID と、明示的に抑止されたシステム ログ メッセージ ID のみを表示するように指定します。
- **Syslog ID Table** : Syslog ID Table View にある設定に基づいてシステム ログ メッセージのリストを表示します。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 の抑止またはその重大度レベルの変更のいずれかを行えます。リスト内の複数のメッセージ ID を選択するには、範囲の最初の ID を選択し、Shift キーを押した状態で範囲の最後の ID をクリックします。
- **Advanced** : システム ログ メッセージにデバイス ID を含めるように設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

- P.15-7 の「[Edit Syslog ID Settings](#)」を参照してください。
- P.15-7 の「[Advanced Syslog Configuration](#)」を参照してください。

Edit Syslog ID Settings

Edit Syslog ID Settings ダイアログボックスでは、選択したシステム ログ メッセージの重大度レベルを変更したり、選択したシステム ログ メッセージの抑止を指定したりできます。

フィールド

- Syslog ID(s) : 表示のみ。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で決まります。
- Suppress Message(s) : Syslog ID リストに表示されるシステム ログ メッセージ ID のメッセージを抑止するには、このチェックボックスをオンにします。
- Logging Level : Syslog ID リストに表示されるシステム ログ メッセージ ID に送信される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)
 - 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、デバッグ中のみ表示)

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Advanced Syslog Configuration

セキュリティ アプライアンスが非 EMBLEM 形式のシステム ログ メッセージにデバイス ID を含めるように設定できます。システム ログ メッセージに、1 つのタイプだけのデバイス ID を指定できます。デバイス ID は、適応型セキュリティ アプライアンスのホスト名、インターフェイス IP アドレス、コンテキスト、またはテキスト文字列で指定できます。

Advanced Syslog Configuration ダイアログボックスでは、システム ログ メッセージにデバイス ID を含めるかどうかを決定できます。この機能がイネーブルになっている場合、デバイス ID がすべての非 EMBLEM 形式のシステム ログ メッセージに含まれます。

フィールド

- Enable Syslog Device ID : デバイス ID をすべての非 EMBLEM 形式のシステム ログ メッセージに含めるように指定します。
- Hostname : デバイス ID としてホスト名を使用するように指定します。
- IP Address : デバイス ID としてインターフェイスの IP アドレスを使用するように指定します。
 - Interface Name : 指定した IP アドレスに対応するインターフェイス名を指定します。
- String : デバイス ID としてユーザ定義の文字列を使用するように指定します。
 - User-defined ID : 英数字のユーザ定義文字列を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

E-Mail Setup

E-Mail Setup ペインでは、通知目的の電子メール メッセージとして送信される、指定したシステム ログ メッセージの受信者リストとともに、送信元電子メール アドレスもセットアップできます。宛先電子メール アドレスに送信されるシステム ログ メッセージは、重大度レベルでフィルタリングできます。テーブルには、どのエントリの作成が完了しているかが表示されます。このペインにアクセスするには、**Configuration > Device Management > Logging > E-Mail Setup** を選択します。

宛先電子メール アドレスへのメッセージのフィルタリングに使用されるシステム ログ メッセージの重大度レベルは、Logging Filters ペインですべての電子メール受信者に対して設定されたグローバルフィルタに比べ、ここで選択した方がより高くなっています。

宛先電子メール アドレスに使用されるシステム ログ 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。

フィールド

- **Source E-Mail address** : 電子メール メッセージとして送信されるシステム ログ メッセージの送信元アドレスとなる電子メール アドレスを指定します。
- **Destination E-Mail Address** : 指定したシステム ログ メッセージの受信者の電子メール アドレスを指定します。
- **Syslog Severity** : この受信者に送信されるシステム ログ メッセージの重大度レベルを指定します。指定した重大度またはそれ以上の重大度を持つメッセージが送信されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

- P.15-9 の「[Add/Edit E-Mail Recipients](#)」を参照してください。
- P.15-9 の「[SMTP](#)」を参照してください。
- P.15-13 の「[Logging Filters](#)」を参照してください。

Add/Edit E-Mail Recipients

Add/Edit E-Mail Recipient ダイアログボックスでは、指定した重大度を持つシステム ログ メッセージを電子メール メッセージとして送信する、宛先電子メールアドレスをセットアップできます。

宛先電子メール アドレスへのメッセージのフィルタリングに使用される重大度レベルは、Logging Filters ペインですべての電子メール受信者に対して設定されたグローバル フィルタに比べ、ここで選択した方がより高くなっています。

フィールド

- Destination E-Mail Address : 選択したシステム ログ メッセージの受信者の電子メールアドレスを指定します。
- Syslog Severity : この受信者に送信されるシステム ログ メッセージの重大度レベルを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

SMTP

SMTP ペインでは、アラートなど、発生した重要イベントを電子メールで通知する SMTP クライアントをイネーブルまたはディセーブルにできます。追加できるのは SMTP サーバの IP アドレスで、オプションとしてバックアップ SMTP サーバの IP アドレスも設定できます。ASDM は IP アドレスが有効かどうかを検証しないので、アドレスは必ず正確に入力してください。このペインにアクセスするには、**Configuration > Properties > Logging > Email Setup** を選択します。

フィールド

- Remote SMTP Server : プライマリ SMTP サーバとセカンダリ SMTP サーバを設定します。
- Primary Server IP Address : SMTP サーバの IP アドレスを指定します。
- Secondary Server IP Address (オプション) : バックアップ SMTP サーバの IP アドレスを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Event Lists

Event Lists ペインでは、どのシステム ログ メッセージが特定の宛先に送信されるのかを選択するときには使用する、イベントのカスタム リストを作成できます。ロギングをイネーブルにし、Logging Setup ペインを使用してロギング パラメータを設定したら、Event Lists ペインでイベントのリストを 1 つ以上作成します。これらのイベント リストは、イベントの各リストのロギングの宛先を指定する場合に Logging Filters ペインで使用します。このペインにアクセスするには、**Configuration > Device Management > Logging > Event Lists** を選択します。

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。

- メッセージ クラス
- 重大度
- メッセージ ID

メッセージ クラスは、各メッセージのクラスを個々に指定するのではなく、メッセージのクラス全体を指定できるようにする、セキュリティ アプライアンスの機能に関連したシステム ログ メッセージのグループです。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、**auth** クラスを使用します。

重大度レベルは、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログ メッセージを分類します。最も高い重大度レベルは **emergency** で、リソースが使用不能になっていることを表します。最も低い重大度レベルは **debugging** で、各ネットワーク イベントに関する詳細情報を提供します。

メッセージ ID は、各メッセージを一意に識別する数値です。システム ログ メッセージの範囲を識別するには、101001-101010 など、イベント リストのメッセージ ID を使用できます。

フィールド

- **Name** : イベント リストの名前を一覧表示します。
- **Event Class/Severity** : ロギング メッセージのイベント クラスおよび重大度レベルを一覧表示します。イベント クラスは次のとおりです。
 - **All** : すべてのイベント クラス
 - **auth** : ユーザ認証
 - **bridge** : 透過ファイアウォール
 - **ca** : PKI の認証局
 - **config** : コマンド インターフェイス
 - **ha** : フェールオーバー
 - **ips** : 侵入防御サービス
 - **ip** : IP スタック
 - **np** : ネットワーク プロセッサ
 - **ospf** : OSPF ルーティング
 - **rip** : RIP ルーティング
 - **rm** : リソース マネージャ
 - **session** : ユーザ セッション
 - **snmp** : SNMP
 - **sys** : システム

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)
- **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、デバッグ中のみ表示)
- Message IDs : フィルタに含めるシステム ログ メッセージ ID または ID の範囲 (101001-101010 など) を一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

- [P.15-11 の「Add/Edit Event List」](#) を参照してください。
- [P.15-12 の「Add/Edit Syslog Message ID Filter」](#) を参照してください。
- [P.15-13 の「Logging Filters」](#) を参照してください。

Add/Edit Event List

Add/Edit Event List ダイアログボックスでは、ログの宛先に送信するメッセージを指定する場合に使用できるイベント リストを作成または編集できます。メッセージ クラスおよび重大度レベル、またはメッセージ ID に基づいてメッセージをフィルタリングするイベント リストを作成できます。

メッセージ クラスは、適応型セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。イベント リストを作成するとき、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できます。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、`auth` クラスを使用します。

重大度レベルは、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログ メッセージを定義します。最も高い重大度レベルは `emergency` で、リソースが使用不能になっていることを表します。最も低い重大度レベルは `debugging` で、各ネットワーク イベントに関する詳細情報を提供します。

メッセージ ID は、各メッセージを一意に識別する数値です。システム ログ メッセージの範囲を識別するには、101001-101010 など、イベント リストのメッセージ ID を使用できます。

フィールド

- Name : イベント リストの名前を入力します。
- Event Class : イベント クラスを一覧表示します。イベント クラスは次のとおりです。
 - All : すべてのイベント クラス
 - auth : ユーザ認証
 - bridge : 透過ファイアウォール
 - ca : PKI の認証局
 - config : コマンド インターフェイス

- ha : フェールオーバー
 - ips : 侵入防御サービス
 - ip : IP スタック
 - np : ネットワーク プロセッサ
 - ospf : OSPF ルーティング
 - rip : RIP ルーティング
 - rm : リソース マネージャ
 - session : ユーザ セッション
 - snmp : SNMP
 - sys : システム
- Severity : ログिंग メッセージのレベルを一覧表示します。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)
 - 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、デバッグ中のみ表示)
 - Message IDs Filters : フィルタに含めるシステム ログ メッセージ ID またはシステム ログ メッセージ ID の範囲 (101001-101010 など) を一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add/Edit Syslog Message ID Filter

Add/Edit Syslog Message ID Filter ダイアログボックスでは、イベント リストに含める 1 つ以上のシステム ログ メッセージ ID を指定できます。

フィールド

- Message IDs : 記録するシステム ログ メッセージ ID または ID の範囲を指定します。範囲を指定するには、ハイフンを使用します (101001-101010 など)。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Logging Filters

Logging Filters ペインでは、メッセージフィルタをログの宛先に適用できます。ログの宛先に適用されたフィルタにより、その宛先に送信するメッセージが選択されます。メッセージクラスおよび重大度レベルに従ってメッセージをフィルタリングしたり、Event Lists ペインで作成可能なイベント リストを使用したりできます。このペインにアクセスするには、**Configuration > Device Management > Logging > Logging Filters** を選択します。

フィールド

- **Logging Destination** : フィルタを適用できるログिंगの宛先の名前を一覧表示します。ログिंगの宛先は次のとおりです。
 - コンソール
 - セキュリティ アプライアンス
 - Syslog サーバ
 - SNMP トラップ
 - 電子メール
 - 内部バッファ
 - Telnet セッション
- **Syslogs From All Event Classes** : 重大度、またはログの宛先へのメッセージのフィルタリングに使用するイベント クラスを一覧表示するか、すべてのイベント クラスに対してログिंगをディセーブルにするかどうかを指定します。
- **Syslogs From Specific Event Classes** : ログの宛先へのメッセージのフィルタリングに使用するイベント クラスを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

- P.15-13 の「[Edit Logging Filters](#)」を参照してください。
- P.15-12 の「[Add/Edit Syslog Message ID Filter](#)」を参照してください。
- P.15-15 の「[Add/Edit Class and Severity Filter](#)」を参照してください。
- P.15-10 の「[Event Lists](#)」を参照してください。

Edit Logging Filters

Edit Logging Filters ダイアログボックスでは、各ログの宛先へのフィルタの適用、すでにログの宛先に適用されているフィルタの編集、またはログの宛先に対するフィルタのディセーブル化を行うことができます。メッセージクラスおよび重大度レベルに従ってメッセージをフィルタリングしたり、Event Lists ペインで作成可能なイベント リストを使用したりできます。

フィールド

- Logging Destination : このフィルタに対してログギングの宛先を指定します。
- Filter on severity : 重大度レベルに従って、システム ログ メッセージをフィルタリングします。
 - Filter on severity : フィルタリングを行うシステム ログ メッセージのレベルを指定します。
- Use event list : このフィルタへのイベント リストの使用を指定します。
 - Use event : 使用するイベント リストを指定します。
- New : 新しいイベント リストを追加できます。
- Disable logging from all event classes : 選択した宛先へのすべてのログギングをディセーブルにします。
- Event Class : イベント クラスを指定します。イベント クラスは次のとおりです。
 - All : すべてのイベント クラス
 - auth : ユーザ認証
 - bridge : 透過ファイアウォール
 - ca : PKI の認証局
 - config : コマンド インターフェイス
 - ha : フェールオーバー
 - ips : 侵入防御サービス
 - ip : IP スタック
 - np : ネットワーク プロセッサ
 - ospf : OSPF ルーティング
 - rip : RIP ルーティング
 - rm : リソース マネージャ
 - session : ユーザ セッション
 - snmp : SNMP
 - sys : システム
- Severity : ログギング メッセージのレベルを指定します。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)
 - 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、デバッグ中のみ表示)

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add/Edit Class and Severity Filter

Add/Edit Class and Severity Filter ダイアログボックスでは、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指定できます。

メッセージクラスは、適応型セキュリティ アプライアンスの機能に関連するシステム ログ メッセージのグループです。イベント リストを作成するとき、各メッセージを個々に指定するのではなく、メッセージのクラス全体を指定できます。たとえば、ユーザ認証に関連したすべてのシステム ログ メッセージを選択するには、`auth` クラスを使用します。

重大度レベルは、ネットワークの通常機能でのイベントの相対重要性に基づいて、システム ログを定義します。最も高い重大度レベルは `emergency` で、リソースが使用不能になっていることを表します。最も低い重大度レベルは `debugging` で、各ネットワーク イベントに関する詳細情報を提供します。

フィールド

- **Event Class** : イベント クラスを指定します。イベント クラスは次のとおりです。
 - `All` : すべてのイベント クラス
 - `auth` : ユーザ認証
 - `bridge` : 透過ファイアウォール
 - `ca` : PKI の認証局
 - `config` : コマンドインターフェイス
 - `ha` : フェールオーバー
 - `ips` : 侵入防御サービス
 - `ip` : IP スタック
 - `np` : ネットワーク プロセッサ
 - `ospf` : OSPF ルーティング
 - `rip` : RIP ルーティング
 - `rm` : リソース マネージャ
 - `session` : ユーザ セッション
 - `snmp` : SNMP
 - `sys` : システム
- **Severity** : ログメッセージのレベルを指定します。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)
 - `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、デバッグ中のみ表示)

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Add/Edit Syslog Message ID Filter

Add/Edit Syslog Message ID Filter ダイアログボックスでは、イベント リスト フィルタに含める個々のシステム ログ メッセージ ID または ID の範囲を指定できます。

フィールド

- Message IDs : システム ログ メッセージ ID または ID の範囲を指定します。範囲を指定するには、ハイフンを使用します (101001-101010 など)。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	システム
			コンテキスト	
•	•	•	•	—

Rate Limit

Rate Limit ペインでは、ファイアウォールが送信できるシステム ログ メッセージ数を指定できます。メッセージ ログイング レベルのレート制限を具体的に指定して、特定のメッセージのレートを制限することができます。レート レベルは、重大度レベルまたはメッセージ ID に適用されますが、宛先には適用されません。したがって、レート制限は、すべての設定済み宛先に送信されるメッセージの量に影響を与えます。このペインにアクセスするには、**Configuration > Device Management > Logging > Rate Limit** を選択します。

フィールド

Rate limits for syslog logging levels セクション

- **Logging Level** : メッセージの重大度レベルを一覧表示します。レベルは次のように定義されています。
 - Disabled (ログイングなし)
 - 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、デバッグ中のみ表示)
- **No of Messages** : 送信されるメッセージ数を表示します。メッセージ数を制限なしにするには、**Number of Messages** フィールドと **Time Interval** フィールドの両方を空白のままにします。
- **Interval (Seconds)** : このログイング レベルで送信できるメッセージ数を制限するのに使用される間隔を、秒数で表示します。メッセージ数を制限なしにするには、**Number of Messages** と **Time Interval** の両方を空白のままにします。
- **Edit** : **Edit Rate Limit** ダイアログボックスを開き、選択したログイング レベルのプロパティを編集するには、テーブルからログイング レベルを選択してここをクリックします。

Individually rate-limited syslog messages セクション

- **Syslog ID** : 制限されているシステム ログ メッセージの ID を表示します。
- **Logging Level** : メッセージの重大度レベルを表示します。重大度レベルのリストについては、[P.15-17 の「Rate limits for syslog logging levels セクション」](#)を参照してください。
- **No of Messages** : 指定された時間間隔に送信できるメッセージの最大数を表示します。
- **Interval (Seconds)** : システム ログ メッセージのレートの制限に使用される間隔を秒数で表示します。
- **Add** : 特定のメッセージのレートを制限します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

- P.15-18 の「[Edit Rate Limit for Syslog Logging Level](#)」を参照してください。
- P.15-18 の「[Add/Edit Rate Limit for Syslog Message](#)」を参照してください。

Edit Rate Limit for Syslog Logging Level

Edit Rate Limit for Syslog Logging Level ボックスでは、指定した時間間隔にファイアウォールが送信できるメッセージ数を制限できます。

フィールド

Rate limit for syslog logging levels セクション

- **Logging Level** : 選択したメッセージの重大度レベルを表示します。特定のメッセージ ID のレート制限を変更すると、ロギング レベルを指定できる場合があります。レベルは次のように定義されています。
 - Disabled (ロギングなし)
 - 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、デバッグ中のみ表示)
- **No of Messages** : このロギング レベルで送信可能なメッセージの最大数を指定します。
- **Time Interval (seconds)** : このロギングレベルでメッセージのレートを制限するときを使用される時間を、秒数で指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Add/Edit Rate Limit for Syslog Message

Add/Edit Rate Limit for Syslog Message ダイアログボックスでは、レート制限を特定のシステム ログメッセージに割り当てることができます。

フィールド

- **Syslog Message ID** : 制限するシステム ログ メッセージのメッセージ ID を指定します。
- **Number of Messages** : 指定された時間間隔にこのメッセージを送信できる最大回数を指定します。
- **Time Interval** : 指定したメッセージの制限に使用される時間を秒数で指定します。



(注) メッセージ数を制限なしにするには、Number of Messages フィールドと Time Interval フィールドの両方を空白のままにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

Syslog サーバ

Syslog Servers ペインでは、セキュリティ アプライアンスがシステム ログ メッセージを送信する syslog サーバを指定できます。定義した syslog サーバを使用するには、Logging Setup ペインを使用してロギングをイネーブルにし、Logging Filters ペインで使用可能な宛先をセットアップする必要があります。このペインにアクセスするには、**Configuration > Device Management > Logging > Syslog Server** を選択します。



(注) セキュリティ コンテキストにつき、最大 4 つの syslog サーバをセットアップできます。

フィールド

- **Interface** : syslog サーバとの通信に使用するインターフェイスを表示します。
- **IP Address** : syslog サーバとの通信に使用されるインターフェイスの IP アドレスを表示します。
- **Protocol/Port** : syslog サーバがセキュリティ アプライアンスとの通信に使用するプロトコルおよびポートを表示します。
- **EMBLEM** : メッセージをシスコ EMBLEM 形式 (Protocol/Port 設定で UDP が選択されている場合にのみ使用可能) で記録するかどうかを指定します。
- **Queue Size** : syslog サーバがビジー状態の場合、セキュリティ アプライアンス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、キューに入れられるメッセージ数に制限がないことを意味します。
- **Allow user traffic to pass when TCP syslog server is down** : syslog サーバがダウンしている場合に、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。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

詳細情報

- P.15-20 の「[Add/Edit Syslog Server](#)」を参照してください。
- P.15-3 の「[Logging Setup](#)」を参照してください。
- P.15-13 の「[Logging Filters](#)」を参照してください。

Add/Edit Syslog Server

Add/Edit Syslog Server ダイアログボックスでは、セキュリティ アプライアンスがシステム ログ メッセージを送信する syslog サーバを追加または編集できます。定義した syslog サーバを使用するには、Logging Setup ペインでロギングをイネーブルにし、Logging Filters ペインでログの宛先に特定のフィルタをセットアップする必要があります。



(注) コンテキストにつき、最大 4 つの syslog サーバをセットアップできます。

フィールド

- Interface : syslog サーバとの通信に使用するインターフェイスを指定します。
- IP Address : syslog サーバとの通信に使用する IP アドレスを指定します。
- Protocol : syslog サーバがセキュリティ アプライアンスとの通信に使用するプロトコル (TCP または UDP) を表示します。
- Port : syslog サーバがセキュリティ アプライアンスとの通信に使用するポートを指定します。
- Log messages in Cisco EMBLEM format (UDP only) : メッセージをシスコ EMBLEM 形式 (プロトコルとして UDP が選択されている場合にのみ使用可能) で記録するかどうかを指定します。
- Enable secure logging using SSL/TLS (TCP only) : syslog サーバへの接続が SSL/TLS over TCP の使用により保護され、システム ログ メッセージの内容が暗号化されることを指定します。



(注) PIX セキュリティ アプライアンスは、セキュア ログイング オプションをサポートしません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

SMTP

SMTP ペインでは、特定のイベントが発生したときに電子メールアラートと通知を送信する宛先となるリモート SMTP サーバの IP アドレスを設定できます。このペインにアクセスするには、**Configuration > Device Setup > Logging > SMTP** を選択します。

フィールド

- Primary Server IP Address : プライマリ SMTP サーバの IP アドレスを指定します。
- Secondary Server IP Address (オプション) : スタンバイ SMTP サーバの IP アドレスを指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォールモード		セキュリティ コンテキスト		
ルーテッド	透過	シングル	マルチ	
			コンテキスト	システム
•	•	•	•	—

