ファイアウォール デバイスでのロギング ポリシーの設定

ロギング機能では、NetFlow「コレクタ」のイネーブル化と管理、システムロギングのイネーブル化、ロギングパラメータの設定、イベントリスト（syslog フィルタ）の設定、宛先へのフィルタの適用、syslog メッセージの設定、syslog サーバーの設定、および電子メール通知パラメータの指定を行います。

[Logging Setup] ページを使用してロギングをイネーブルにし、ロギング パラメータを設定したあとで、[Event Lists] ページで（syslog のセットに対して）フィルタを設定します。このフィルタをロギング先に送信できます。[Logging Filters] ページでは、送信する syslog のロギング先を指定します。最後に、[Syslog] ページと [E-Mail] ページで syslog と電子メールを設定します。

この章は次のトピックで構成されています。

[NetFlow] ページ

NetFlow データ エクスポート用に設定されているデバイスは、そのデバイスのフローベースのトラフィック統計をキャプチャします。この情報は、デバイスから NetFlow コレクション サーバにユーザ データグラム プロトコル（UDP）データグラムの形式で定期的に送信されます。

[NetFlow] ページでは、選択したデバイスで NetFlow エクスポートをイネーブルにし、収集したフロー情報を送信する NetFlow「コレクタ」を定義および管理します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）]>[ロギング（Logging）] > [NetFlow]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [NetFlow]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ルール テーブルの使用
- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能

フィールド リファレンス

表 1 : [NetFlow] ページ

要素	説明
Enable Flow Export	オンになっている場合は、NetFlowデータエクスポートがイネーブルになります。
Template Export Interval	フロー情報がコレクタに送信される間隔（分単位）。この値は、1 ～ 3600 分で、デフォルトは 30 です。
アクティブ更新間隔（Active Refresh Interval）	アクティブ接続では、flow-updateイベント間の間隔を分単位で指定します。有効な値は、1 ～ 60 分です。デフォルト値は 1 分です。
遅延フロー作成（Delay Flow Create）	flow-create イベントの送信を指定した秒数遅らせます。値は 1 ～ 180 秒です。 この値が入力されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。設定されている遅延よりも前にフローが切断された場合は、flow-create イベントは送信されません。その代わりに拡張フロー ティアダウン イベントが送信されます。

要素	説明
Collectors table	現在定義されているNetFlowコレクタがリストされます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、[Add Collector]/[Edit Collector] ダイアログボックス（NetFlow） （3 ページ）が開きます。 （注） Cisco Security Manager では、ASA 9.6(4) から 9.7.0、および 9.8(2) 以降のデバイスに対する重複するNetflowコレクタは許可されません。デバイスの現在の設定を変更するか、重複している構成を削除します（**[プラットフォーム（Platform）] > [ロギング（Logging）] > [Netflow]**）。

[Add Collector]/[Edit Collector] ダイアログボックス（NetFlow）

[コレクタの追加（Add Collector）] および [コレクタの編集（Edit Collector）] ダイアログボックスを使用して、NetFlowの「コレクタ」を定義および編集します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add Collector]/[Edit Collector] ダイアログボックスは、[NetFlow] ページ （1 ページ）から開くことができます。

フィールド リファレンス

表 2 : [Add Collector]/[Edit Collector] ダイアログボックス

要素	説明
インターフェイス（Interface）	コレクタのアクセスに使用するデバイス インターフェイスの名前を入力または選択します。
コレクタ	NetFlow パケットの送信先のサーバの IP アドレスまたはネットワーク名を入力します。ネットワーク/ホストオブジェクトも選択できます。
UDP ポート（UDP Port）	NetFlow パケットの送信先の指定済みコレクタ上の UDP ポートを指定します。値の範囲は 1 ～ 65535 で、デフォルトは 2055 です。

組み込まれている Event Manager

Embedded Event Manager（EEM; 組み込みイベントマネージャ）を利用することで、問題をデバッグすることが可能になり、トラブルシューティング用に汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。

（注） Embedded Event Manager は、ASA 9.2(1) 以降でのみサポートされます。

サポートされるイベント

EEM は次のイベントをサポートします。

- Syslog：ASA は、syslog メッセージの ID を使用して、イベント マネージャ アプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベント マネージャ アプレット内で syslog メッセージの ID が重複することはできません。
- タイマー：タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベント マネージャ アプレットに対して一度だけ設定できます。各イベント マネージャ アプレットには最大で 3 つのタイマーがあります。3 種類のタイマーは次のとおりです。
  - ウォッチドッグ（定期的）タイマーは、アプレットアクションの完了後に指定された期間が経過するとイベント マネージャ アプレットをトリガーし、自動的にリスタートします。
  - カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベント マネージャアプレットを1回トリガーします。削除および再追加されない限りはリスタートしません。
  - 絶対（1 日 1 回）タイマーは、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は hh:mm:ss です。

各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを 1 つだけ設定できます。

- [なし（None）]：イベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。output コマンドの値に関係なく、action コマンドはクラッシュ情報ファイルを対象とします。出力は、show tech コマンドの前に生成されます。

（注） Syslog ID の範囲を使用するとき、およびタイマーを使用するときは注意が必要です。設定が正しくないと、ASA ループが発生し、アプレットが正常に実行されなくなる可能性があります。

アクションの設定

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先の設定

次の 3 つの場所のいずれかに action CLI コマンドの出力を送信できます。

- なし：デフォルトの設定です。出力を破棄します。
- コンソール：出力を ASA コンソールに送信します。
- ファイル：出力をファイルに送信します。次の 4 つのファイル オプションを使用できます。
  - 新規：イベント マネージャ アプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
  - 上書き：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。
  - 付加：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
  - ローテート：連のファイルを作成する：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

注意事項と制約事項

- シングル モードでだけサポートされています。マルチ コンテキスト モードではサポートされません。
- 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。
- EEM は、デバイスでロギング機能がイネーブルになっているかどうかに関係なくイネーブルになります。
- ASA の EEM 機能には、Cisco ルータにある EEM 機能のサブセットのみが含まれています。

- 通常、クラッシュ時は、ASA の状態は不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。
- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は none です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

Embedded Event Manager テーブルには、現在定義されているイベント マネージャ アプレットが一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。[Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス （6 ページ）が開きます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Embedded Event Manager]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Embedded Event Manager]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス （6 ページ）
- テーブル カラムおよびカラム見出しの機能

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログ ボックスを使用して、イベントマネージャアプレットを定義および編集します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックスは、組み込まれている Event Manager （4 ページ）から開くことができます。

フィールド リファレンス

表 *3 : [アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス*

要素	説明
名前	イベント マネージャ アプレットの一意の名前を入力します。名前にスペースを含めることはできず、32 文字未満にする必要があります。
説明	イベント マネージャ アプレットの説明を入力します。説明の長さは最大 256 文字です。
[構成] タブ	
クラッシュ情報	選択すると、ASA がクラッシュしたときにイベント マネージャ アプレットがトリガーされます。Output コマンドの値に関係なく、action コマンドはクラッシュ情報ファイルを対象とします。出力は、show tech コマンドの前に生成されます。 （注） ASA がクラッシュした場合、その状態は通常は不明です。一部の CLI コマンドは、この状態のときに実行するのは安全でない場合があります。
なし（None）	選択すると、イベント マネージャ アプレットを手動でトリガーできます。 （注） EEM アプレットの手動トリガーは、Cisco Security Manager ではサポートされていません。アプレットを手動でトリガーするには、FlexConfig を使用する必要があります。詳細については、FlexConfig の管理を参照してください。
Syslog テーブル	Syslog テーブルには、選択したアプレットに現在定義されている Syslog メッセージ ID が一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。[Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、[Syslog 設定の追加（Add Syslog Configuration）]/[Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックス （10 ページ）が開きます。
Absolute	絶対（1 日 1 回）タイマーイベントの設定。絶対タイマーが、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。 提供されたフィールドを使用して、時間、分、秒で時刻を入力します。時刻の範囲は 00:00:00（真夜中）から 23:59:59 です。

要素	説明
カウントダウン	カウントダウン（ワンショット）タイマーイベントを設定します。カウントダウンタイマーは、指定された期間が経過するとイベント マネージャ アプレットを 1 回トリガーします。削除および再追加されない限りはリスタートしません。 期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
ウォッチドッグ	ウォッチドッグ（定期的）タイマーイベントを設定します。ウォッチドッグタイマーは、アプレットアクションの完了後に指定された期間が経過するとイベントマネージャアプレットをトリガーし、自動的にリスタートします。 期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
出力	アクションからの出力を送信するための特定の宛先を設定するには、使用可能な出力宛先オプションのいずれかを選択します。 • なし：（デフォルト）出力を破棄します。 • コンソール：出力を ASA コンソールに送信します。 • ファイル：出力をファイルに送信します。[アクション（Action）] リストでファイルオプションを選択します。

要素	説明
操作	次の 4 つのファイル オプションを使用できます。 • 新規：イベントマネージャアプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。ファイル名は eem-applet-timestamp.log というフォーマットで、applet はイベントマネージャ アプレットの名前、timestamp は YYYYMMDD-hhmmss 形式の日付型タイムスタンプです。 • 上書き：イベントマネージャアプレットが呼び出されるたびに、指定されたファイルを上書きします。[ファイルの場所（File Location）] および [ファイル名（File Name）] フィールドを使用して、ファイルの詳細を指定します。 • 付加：イベントマネージャアプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。[ファイルの場所（File Location）] および [ファイル名（File Name）] フィールドを使用して、ファイルの詳細を指定します。 • ローテート：イベントマネージャアプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。[ファイル数（File Count）] フィールドでローテーションするファイルの数を指定します（有効な値の範囲は 2 から 100）。 新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数で示されます。ファイル名の形式は、eem-applet-x.log です。ここで、applet はアプレットの名前、x はファイル番号を示しています。
ファイルの場所（File Location）	出力ファイルの場所を指定します。ローテーションは、FTP、TFTP、および SMB のターゲットファイルを使用する場合もあります。
ファイル名	出力ファイルのファイル名を指定します。
ファイル数	「ローテート」が選択されたアクションの場合、ローテーションするファイル数を指定します。 新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数で示されます。有効なローテーションの値の範囲は 2 ～ 100 です。ファイル名の形式は、eem-applet-x.log です。ここで、applet はアプレットの名前、x はファイル番号を示しています。
[Action] タブ	

要素	説明
アクション テーブル	アクションテーブルには、選択したアプレットに現在定義されているアクションが一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。[Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、アクション構成の追加および編集ダイアログボックス （11 ページ）が開きます。

[Syslog 設定の追加（Add Syslog Configuration）]/[Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックス

[Syslog 設定の追加（Add Syslog Configuration）] および [Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックスを使用して、イベントマネージャアプレットの Syslog メッセージ ID を設定します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[Syslog 設定の追加（Add Syslog Configuration）] および [Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックスには、[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス （6 ページ）からアクセスできます。

フィールド リファレンス

表 *4 : [Syslog* 設定の追加（*Add Syslog Configuration*）*]/[Syslog* 設定の編集（*Edit Syslog Configuration*）*]* ダイアログボックス

要素	説明
ID	単一の syslog メッセージまたは syslog メッセージの範囲を入力します。指定された個々の syslog メッセージまたは syslog メッセージの範囲に一致する syslog メッセージが発生すると、イベント マネージャ アプレットがトリガーされます。 （注） syslog メッセージ ID を 2 回入力したり、1 つのイベント マネージャ アプレット内で重複させることはできません。
発生回数	（任意）[発生回数（Occurrences）] フィールドに、イベント マネージャ アプレットを呼び出すために syslog メッセージが発生する必要がある回数を入力します。デフォルトの発生回数は 0 秒ごとに 1 回です。有効な値は、1 ～ 4294967295 です。
Period	（任意）[期間（Period）] フィールドに、アクションを呼び出すために syslog メッセージが発生しなければならない許容時間（秒数）を入力します。この値によって、イベント マネージャ アプレットが設定された期間に 1 回呼び出される際の最大の間隔が制限されます。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

アクション構成の追加および編集ダイアログボックス

[アクション設定の追加（Add Action Configuration）]および[アクション設定の編集（Edit Action Configuration）]ダイアログボックスを使用して、イベントマネージャアプレットのアクションを設定します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[アクション設定の追加（Add Action Configuration）]および[アクション設定の編集（Edit Action Configuration）]ダイアログボックスには、[アプレットの追加（Add Applet）]および[アプレットの編集（Edit Applet）] ダイアログボックス （6 ページ）からアクセスできます。

フィールド リファレンス

表 *5:* アクション構成の追加および編集ダイアログボックス

要素	説明
序数 ID（Ordinal ID）	[序数ID（Ordinal ID）]フィールドに一意のシーケンス番号を入力します。有効なシーケンス番号の範囲は 0 ～ 4294967295 です。アクション設定を追加する場合、デフォルトで、序数 ID は使用されている最大序数 ID より 1 つ大きくなります。
CLI	CLI コマンドを [CLI] フィールドに入力します。このコマンドは、特権レベル 15（最高）を持つユーザーとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。

[E-Mail Setup] ページ

[E-Mail Setup] ページ（PIX 7.0/ASA のみ）では、送信元電子メールアドレスと、電子メールとして送信する指定済み syslog メッセージの受信者のリストを設定します。宛先電子メール アドレスに送信される syslog メッセージを重大度でフィルタできます。テーブルには、どのエントリが設定されているかが表示されます。

宛先電子メール アドレスに使用される syslog 重大度フィルタは、このセクションで選択した重大度と [Logging Filters] ページ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 フィルタのうち、より高い方になります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [電子メールセットアップ（E-Mail Setup）]**を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [電子メールセット**

アップ（**E-Mail Setup**）**]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *6 : [E-Mail Setup]* ページ

要素	説明
Source Email Address	syslog が電子メールとして送信されるときに送信元アドレスとして使用される電子メール アドレスを入力します。
[Destination Address] テーブル	現在定義されている、syslog メッセージの電子メール受信者がリストされます。 [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、このリストを管理します。[Add Row] ボタンおよび [Edit Row] ボタンを使用すると、[Add Email Recipient]/[Edit Email Recipient] ダイアログボックス （12 ページ）が開きます。

[Add Email Recipient]/[Edit Email Recipient] ダイアログボックス

[Add Email Recipient]/[Edit Email Recipient] ダイアログボックスでは、syslog メッセージを含む電子メールを送信する宛先アドレスを設定します。重大度に応じて送信するメッセージを制限できます。

宛先電子メール アドレスに使用される syslog 重大度フィルタは、このセクションで選択した重大度と [Logging Filters] ページ （17 ページ）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 フィルタのうち、より高い方になります。

ナビゲーション パス

[Add Email Recipient]/[Edit Email Recipient] ダイアログボックスには、[E-Mail Setup] ページ（11 ページ）からアクセスできます。

フィールド リファレンス

表 *7 : [Add Email Recipient]/[Edit Email Recipient]* ダイアログボックス

要素	説明
Destination Email Address	選択したタイプの syslog メッセージの受信電子メール アドレスを入力します。

要素	説明
[Syslog Severity] リスト	この受信者に電子メールで送信する syslog の重大度を選択します。選択した重大度以上のメッセージが送信されます。メッセージの重大度レベルについては、ログ レベル （33 ページ）を参照してください。

[Event Lists] ページ

[Event Lists] ページ（PIX 7.0+/ASA のみ）では、ロギングに対する syslog メッセージ フィルタのセットを定義します。[Logging Setup] ページでロギングをイネーブルにし、グローバル ロギング パラメータを設定したあとで、このページを使用して、さまざまなロギング先に送信される syslog メッセージのフィルタに使用するイベント リストを設定します（[Logging Filters] ページ （17 ページ）で、イベント リストのロギング先を指定します）。

[Event Lists] テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、エントリを管理します。[Add Row] および [Edit Row] を使用すると、[Add Event List]/[Edit Event List] ダイアログボックス （15 ページ）が開きます。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [イベント リスト（Event Lists）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [イベント リスト（Event Lists）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Logging Setup] ページ （22 ページ）
- ロギング設定の設定 （21 ページ）

セージ クラスおよび関連するメッセージ ID 番号

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 *8 :* セージ クラスおよび関連するメッセージ *ID* 番号

クラス	定義（Definition）	メッセージ ID 番号
auth	ユーザ認証	109、113

クラス	定義（Definition）	メッセージ ID 番号
ブリッジ	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
config	コマンド インターフェイス	111、112、208、308
電子メール（e-mail）	電子メール プロキシ	719
ha	フェールオーバー（ハイアベイラビリティ）	101、102、103、104、210、311、709
ids	侵入検知システム	400、401、415
ip	IP スタック	209、215、313、317、408
np	ネットワーク プロセッサ	319
ospf	OSPF ルーティング	318、409、503、613
rip	RIP ルーティング	107、312
rm	Resource Manager	321
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
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711
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
webvpn	Web ベースの VPN	716

[Add Event List]/[Edit Event List] ダイアログボックス

[Add Event List]/[Edit Event List] ダイアログボックスでは、イベント リストを作成または編集し、イベント リスト フィルタに含める syslog メッセージを指定します。

次の基準を使用して、イベント リストを定義できます。

- クラスと重大度
- メッセージ ID

クラスは、関連する syslog メッセージの特定のタイプを表します。たとえば、クラス auth は、ユーザ認証に関連するすべての syslog メッセージを表します。

重大度は、ネットワークの通常機能におけるイベントの相対的な重要性に基づいて syslog を分類します。最も高い重大度は [緊急（Emergency）] で、利用可能なリソースがないことを意味します。最も低い重大度は [デバッグ（Debugging）] で、すべてのネットワーク 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、個々のメッセージを一意に識別する数値です。単一のメッセージ ID または ID の範囲をイベント リストで指定できます。

ナビゲーション パス

[Add Event List]/[Edit Event List] ダイアログボックスには、[Event Lists] ページ （13 ページ）からアクセスできます。

フィールド リファレンス

表 9 : [Add Event List]/[Edit Event List] ダイアログボックス

要素	説明
Event List Name	このイベント リストを一意に識別する名前を入力します。
Event Class/Severity Filters	このテーブルには、このイベント リストに対して定義されているイベント クラスと重大度レベル フィルタがリストされます。 エントリを管理するには、このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用します。[Add Row] および [Edit Row] を使用すると、[Add/Edit Syslog Class] ダイアログボックス （16 ページ）が開きます。
Message ID Filters	このテーブルには、このイベント リストに対して定義されているメッセージ ID フィルタがリストされます。 エントリを管理するには、このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用します。[Add Row] および [Edit Row] を使用すると、[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス （16 ページ）が開きます。

[Add/Edit Syslog Class] ダイアログボックス

[Add Syslog Class]/[Edit Syslog Class] ダイアログボックスでは、イベント クラスおよび関連する重大度レベルをイベント リスト フィルタとして指定します。

クラスによって、関連する特定のタイプの syslog メッセージが表されるため、syslog を個別に選択する必要はありません。たとえば、クラス auth は、ユーザ認証に関連するすべての syslog メッセージを表します。

重大度は、ネットワークの通常機能におけるイベントの相対的な重要性に基づいて syslog を分類します。最も高い重大度は [緊急（Emergency）] で、利用可能なリソースがないことを意味します。最も低い重大度は [デバッグ（Debugging）] で、すべてのネットワーク イベントに関する詳細情報を提供します。

ナビゲーション パス

[Add Syslog Class]/[Edit Syslog Class] ダイアログボックスには、[Add Event List]/[Edit Event List] ダイアログボックス （15 ページ）からアクセスします。

関連項目

- [Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス （16 ページ）
- [Event Lists] ページ （13 ページ）

フィールド リファレンス

表 10 : [Add/Edit Syslog Class] ダイアログボックス

要素	説明
イベント クラス	目的のイベント クラスを選択します。イベント クラスについては、セージ クラスおよび関連するメッセージ ID 番号 （13 ページ）を参照してください。
重大度	目的のメッセージ重大度レベルを選択します。重大度レベルについては、ログ レベル （33 ページ）を参照してください。

[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス

[Syslog メッセージ ID フィルタの追加（Add Syslog Message ID Filter）]/[Syslog メッセージ ID フィルタの編集（Edit Syslog Message ID Filter）] ダイアログボックスでは、Syslog メッセージ ID、または ID の範囲をイベントリストフィルタとして指定します。

ナビゲーション パス

[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックスには、[Add Event List]/[Edit Event List] ダイアログボックス （15 ページ）からアクセスできます。

関連項目

- [Add/Edit Syslog Class] ダイアログボックス （16 ページ）
- [Event Lists] ページ （13 ページ）

フィールド リファレンス

[メッセージ ID（Message IDs）]：Syslog メッセージ ID または ID の範囲を入力します。範囲を指定するには、ハイフンを使用します（101001-101010 など）。メッセージ ID は、100000 ～ 999999 である必要があります。

メッセージ ID および対応するメッセージは、適切な製品の『System Log Message』ガイドにリストされています。これらのガイドには、cisco.com からアクセスできます。

PIX ファイアウォール

- http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html

ASA

- http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html

FWSM

- http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

[Logging Filters] ページ

[Logging Filters] ページでは、[Event Lists] ページを使用して設定されているイベント リスト（syslog フィルタ）、または [Edit Logging Filters] ページを使用して指定する syslog メッセージだけのためのロギング先を設定します。特定のイベント クラスまたはすべてのイベント クラスからの syslog メッセージは、[Edit Logging Filters] ページを使用して選択できます。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング フィルタ（Logging Filters）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング フィルタ（Logging Filters）] を選択します。[ロギング フィルタ（Logging Filters）] を右クリックしてポリシーを作成するか、または共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- ロギング設定の設定 （21 ページ）

- [Edit Logging Filters] ダイアログボックス （19 ページ）

フィールド リファレンス

表 *11 : [Logging Filters]* ページ

要素	説明
Logging Destination	このフィルタに一致するメッセージが送信されるロギング先の名前がリストされます。ロギング先は次のとおりです。 • [内部バッファ（Internal Buffer）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスの内部バッファにパブリッシュされます。 • [コンソール（Console）]。このフィルタと一致するメッセージは、コンソール ポート接続にパブリッシュされます。 • [Telnetセッション（Telnet Sessions）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスに接続されている Telnet セッションにパブリッシュされます。 • [Syslogサーバー（Syslog Servers）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog サーバー（Syslog Servers）] ページで指定された syslog サーバーにパブリッシュされます。 • [電子メール（E-Mail）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）] > [ロギング（Logging）] > [電子メール設定（E-mail Setup）]（PIX7.0/ASA のみ）ページで指定された受信者にパブリッシュされます。 • [SNMPトラップ（SNMP Trap）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] ページで指定された SNMP 管理ステーションにパブリッシュされます。 • [ASDM]。このフィルタと一致するメッセージは、いずれかの ASDM セッションにパブリッシュされます。
Syslogs From All Event Classes	フィルタする重大度、使用するイベント リスト、またはロギングがすべてのイベント クラスからディセーブルにされているかどうかがリストされます。イベント クラスについては、セージ クラスおよび関連するメッセージ ID 番号 （13 ページ）を参照してください。
Syslogs From Specific Event Classes	フィルタとして設定されているイベント クラスと重大度がリストされます。イベント クラスについては、セージ クラスおよび関連するメッセージ ID 番号 （13 ページ）を参照してください。重大度レベルについては、 ログ レベル （33 ページ）を参照してください。

[Edit Logging Filters] ダイアログボックス

[Edit Logging Filters] ダイアログボックスでは、ロギング先のフィルタを編集します。syslog は、すべてまたは特定のイベント クラスから設定するか、特定のロギング先に対してディセーブルにできます。

ナビゲーション パス

[Edit Logging Filters] ダイアログボックスには [Logging Filters] ページからアクセスできます。[Logging Filters] ページの詳細については、[Logging Filters] ページ （17 ページ）を参照してください。

関連項目

- ロギング設定の設定 （21 ページ）
- [Logging Filters] ページ （17 ページ）

フィールド リファレンス

表 *12 : [Edit Logging Filters]* ダイアログボックス

要素	説明
Logging Destination list	このフィルタのロギング先を指定します。 • [内部バッファ（Internal Buffer）]。このフィルタと一致するメッセージは、セキュリティアプライアンスの内部バッファにパブリッシュされます。 • [コンソール（Console）]。このフィルタと一致するメッセージは、コンソール ポート接続にパブリッシュされます。 • [Telnetセッション（Telnet Sessions）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスに接続されている Telnet セッションにパブリッシュされます。 • [Syslogサーバー（Syslog Servers）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslogサーバー（Syslog Servers）] ページで指定された syslog サーバーにパブリッシュされます。 • [電子メール（E-Mail）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）]>[ロギング（Logging）]>[電子メール設定（E-mail Setup）]（PIX7.0/ASA のみ）ページで指定された受信者にパブリッシュされます。 • [SNMPトラップ（SNMP Trap）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）]>[SNMP] ページで指定された SNMP 管理ステーションにパブリッシュされます。 • [ASDM]。このフィルタと一致するメッセージは、いずれかの ASDM セッションにパブリッシュされます。
Syslog from All Event Classes	
Filter on severity option	ロギング メッセージの重大度をフィルタします。
Filter on severity list	フィルタするロギング メッセージのレベルを指定します。
Use event list option	イベント リストを使用することを指定します。
Use event list	使用するイベント リストを指定します。イベント リストは [Event Lists] ページ （13 ページ）で定義されています。
Disable logging option	選択した宛先へのすべてのロギングをディセーブルにします。

要素	説明
Syslog from Specific Event Classes (PIX7.0)	
イベント クラス	イベント クラスと重大度を指定します。イベント クラスには、1 つまたはすべての使用可能なアイテムが含まれます。イベント クラスについては、 セージ クラスおよび関連するメッセージ ID 番号 （13 ページ）を参照してください。
重大度	ロギング メッセージのレベルを指定します。重大度レベルについては、ログ レベル （33 ページ）を参照してください。

ロギング設定の設定

[Logging Setup] ページでは、セキュリティ アプライアンスでのシステム ロギングをイネーブルにしたり、他のロギング オプションを設定したりできます。これらのオプションには、セキュリティ アプライアンスおよびフェールオーバー装置に関するロギングのイネーブル化、基本的なログ フォーマットと詳細、および内部バッファをパージする前の長期保管デバイス、FTP サーバ、またはフラッシュへのロギングが含まれます。

関連項目

- [Logging Setup] ページ （22 ページ）

ステップ 1 [プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslog]>[ロギングの設定（Logging Setup）] を選択して、[ロギングの設定（Logging Setup）] ページを表示します。

ステップ 2 [ロギングの有効化（Enable Logging）] をオンにします。

このオプションは、セキュリティ アプライアンスでのロギングをイネーブルにします。

ステップ 3 このセキュリティアプライアンスとペアになっているフェールオーバー装置上でロギングをイネーブルにするには、[スタンバイフェールオーバー装置でのロギングを有効にする（Enable logging on the standby failover unit）] チェックボックスをオンにします。

ステップ 4 EMBLEM フォーマットをイネーブルにするには、またはデバッグ メッセージを syslog メッセージの一部として送信するには、対応するチェックボックスをオンにします。

EMBLEM をイネーブルにする場合は、UDP プロトコルを使用して syslog メッセージをパブリッシュする必要があります。TCP とは互換性がありません。

ステップ 5 内部バッファをクリアする前に、あとで処理するために内部バッファ データを FTP サーバに書き込むには、次の手順を実行します。

a) [FTPサーバーバッファラップ（FTP Server Buffer wrap）] をオンにします。
b) FTP サーバーの IP アドレスを [IPアドレス（IP Address）] フィールドに入力します。
c) FTP サーバーへのログインに使用するアカウントのユーザー名を [ユーザー名（User Name）] フィールドに入力します。

d) ファイルを保存するパスを、FTP ルートに関連した [パス（Path）] フィールドに入力します。
e) ユーザ名の認証に使用されるパスワードを入力および確認します。

ステップ 6 内部バッファをクリアする前に、あとで処理するために内部バッファ データをフラッシュに書き込むには、次の手順を実行します。

a) [フラッシュ（Flash）] をオンにします。
b) 内部バッファ データのストレージに割り当てる最大メモリ量を指定します。
c) フラッシュ ドライブに残す必要のある最小空きメモリを指定します。内部バッファからのデータを書き込むとき、この最小値を維持できないと、容量要件を満たすためにメッセージが切り詰められます。

ステップ 7 ASDM クライアントで表示するためにアプライアンス上に維持する最大キューサイズを指定するには、[メッセージキューのサイズ（メッセージ数）（Message Queue Size (Messages)）] フィールドにその値を入力します。

[Logging Setup] ページ

[Logging Setup] ページでは、セキュリティ アプライアンスでのシステム ロギングをイネーブルにしたり、他のロギング オプションを設定したりできます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング設定（Logging Setup）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング設定（Logging Setup）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 13 : [Logging Setup] ページ

要素	説明
Enable Logging	メイン セキュリティ アプライアンスのロギングをオンにします。
Enable Logging on the Failover Standby Unit	スタンバイ セキュリティ アプライアンスが使用可能な場合は、そのロギングをオンにします。

要素	説明
Send syslogs in EMBLEM format（PIX7.x+、ASA、FWSM 3.x+）	すべてのロギング先に対する EMBLEM フォーマット ロギングをイネーブルにします。EMBLEM を有効にする場合は、UDP プロトコルを使用して syslog メッセージをパブリッシュする必要があります。EMBLEM は TCP と互換性がありません。 （注） この設定は、CS-MARS と互換性がありません。
Send debug messages as syslogs（PIX7.x+、ASA、FWSM 3.x+）	すべてのデバッグ トレース出力を syslog にリダイレクトします。このオプションが有効になっている場合、syslog 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、コンソールでロギングを有効にし、デバッグ syslog メッセージ番号とログ レベルの宛先として設定する必要があります。使用される syslog メッセージ番号は 711011 です。この syslog のデフォルトロギングレベルは [デバッグ（debug）] です。
Memory Size of Internal Buffer (bytes)	ロギング バッファがイネーブルになっている場合に syslog が保存される内部バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。有効な範囲は 4096 ～ 1048576 です。
Specify FTP Server Information（PIX7.x+、ASA、FWSM 3.x+）	
FTP Server Buffer Wrap	バッファの内容を上書きする前に FTP サーバに保存するには、このボックスをオンにし、次のフィールドに必要な宛先情報を入力します。FTP 設定を削除するには、このオプションを選択解除します。
IPアドレス	FTP サーバの IP アドレスを入力します。
ユーザー名	FTP サーバに接続するときに使用するユーザ名を入力します。
パス（Path）	バッファの内容を保存するパスを FTP ルートからの相対で入力します。
Password/Confirm	FTP サーバへのユーザ名の認証に使用されるパスワードを入力および確認します。
Specify flash size	
フラッシュ	バッファの内容を上書きする前にフラッシュ 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。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。

要素	説明
Maximum flash to be used by logging (KB)	ロギング用のフラッシュ メモリで使用する最大容量を指定します（KB単位）。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。
Minimum free space to be preserved (KB)	フラッシュ メモリに保持する最小空き容量を指定します（KB単位）。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。
ASDM Logging（PIX7.x+、ASA、FWSM 3.x+）	
Message Queue Size	ASDM で表示する syslog のキュー サイズを指定します。

レート制限レベルの設定

[レート制限（Rate Limit）]ページでは、特定のタイプ（「アラート」または「クリティカル」）のログメッセージの最大数、および特定の期間内に生成できる特定の Syslog ID のメッセージを指定します。ロギング レベルごと、および Syslog メッセージ ID ごとに個別の制限を指定できます。設定が競合する場合は、Syslog メッセージ ID の制限が優先されます。

特定の期間内の特定の Syslog メッセージ ID に対して生成できるメッセージの最大数を指定するには、[Add/Edit Rate Limited Syslog Message] ダイアログボックス （27 ページ）を使用します。

特定の期間内の特定の Syslog ロギング レベルに対して生成できるメッセージの最大数を指定するには、[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （26 ページ）を使用します。

関連項目

- [Rate Limit] ページ （25 ページ）

次の手順に従って、メッセージ ロギングのレート制限を管理します。

ステップ 1 [Rate Limit] ページにアクセスするには、次のいずれかを実行します。

- （デバイス ビュー）デバイス ポリシー セレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 Syslog ロギング レベルのレート制限を追加、編集、および削除します。

- 一定の期間内に特定のロギング レベルに対して生成できるメッセージの最大数を指定するには、[Syslog ロギング レベルのレート制限（Rate Limits for Syslog Logging Levels）] テーブルの下にある [行の追加

（Add Row）] ボタンをクリックして、[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （26 ページ）を開きます。ロギング レベルを選択し、レート制限を定義します。

- 特定のロギングレベルのレート制限を編集するには、[Syslogロギングレベルのレート制限（Rate Limits for Syslog Logging Levels）] テーブルの適切なエントリを選択し、テーブルの下にある [行の編集（Edit Row）] ボタンをクリックして、[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス（26 ページ）を開きます。必要に応じてレート制限を変更します。
- [Syslogロギングレベルのレート制限（Rate Limits for Syslog Logging Levels）] テーブルからレート制限エントリを削除するには、そのエントリを選択し、テーブルの下にある [行の削除（Delete Row）] ボタンをクリックします。確認ダイアログボックスが表示される場合があります。[OK] をクリックしてエントリを削除します。

ステップ 3 メッセージ ID に従ってログ メッセージの制限を追加、編集、および削除します。

- 特定の期間内に特定メッセージ ID に対して生成できるメッセージの最大数を指定するには、[個別にレート制限されたSyslogメッセージ（Individually Rate Limited Syslog Messages）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックして、[Add/Edit Rate Limited Syslog Message] ダイアログボックス （27 ページ）を開きます。Syslog メッセージ ID を選択し、レート制限を定義します。
- 特定の Syslog メッセージ ID のレート制限を編集するには、[個別にレート制限されたSyslogメッセージ（Individually Rate Limited Syslog Messages）] テーブルの適切なエントリを選択し、テーブルの下にある [Edit Row] ボタンをクリックして、[Add/Edit Rate Limited Syslog Message] ダイアログボックス（27 ページ）を開きます。必要に応じてレート制限を変更します。
- [個別にレート制限されたSyslogメッセージ（Individually Rate Limited Syslog Messages）] テーブルからメッセージ制限エントリを削除するには、そのエントリを選択し、テーブルの下にある [行の削除（Delete Row）] ボタンをクリックします。確認ダイアログボックスが表示される場合があります。[OK] をクリックしてエントリを削除します。

[Rate Limit] ページ

[Rate Limit] ページでは、特定の期間内に生成する必要のある特定のタイプ（たとえば、アラートやクリティカル）のログ メッセージの最大数を指定できます。ロギング レベルごと、および Syslog メッセージ ID ごとに制限を指定できます。設定が異なる場合は、Syslog メッセージ ID の制限が優先されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ロギング設定の設定　（21 ページ）
- [Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス　（26 ページ）
- [Add/Edit Rate Limited Syslog Message] ダイアログボックス　（27 ページ）

フィールド リファレンス

表 14 : [Rate Limit] ページ

要素	説明
[Rate Limits for Syslog Logging Levels] テーブル	
ログ レベル（Logging Level）	レート制限を指定する Syslog ロギング レベル。
No. of Messages	指定された時間に送信できる、指定されたタイプのメッセージの最大数。
Interval (seconds)	レート制限カウンタがリセットされるまでの秒数。
[Individually Rate Limited Syslog Messages] テーブル	
syslog ID	レート制限を指定する Syslog メッセージの識別番号。
No. of Messages	指定された時間に送信できる、指定された ID を持つメッセージの最大数。
Interval (seconds)	レート制限カウンタがリセットされるまでの秒数。

[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス

[Add Rate Limit for Syslog Logging Levels]/[Edit Rate Limit for Syslog Logging Levels] ダイアログボックスを使用して、特定の期間内に生成する必要のある特定のログ レベルのログ メッセージの最大数を指定できます。ロギング レベルごと、または syslog メッセージ ID ごとに制限を指定できます（[Add/Edit Rate Limited Syslog Message] ダイアログボックス　（27 ページ）を参照）。設定が異なる場合、レート制限された syslog メッセージレベルの設定がレート制限のロギング レベルの設定を上書きします。

ナビゲーション パス

[Add Rate Limit for Syslog Logging Levels]/[Edit Rate Limit for Syslog Logging Levels] ダイアログボックスには、[Rate Limit] ページからアクセスできます。詳細については、[Rate Limit] ページ　（25 ページ）を参照してください。

関連項目

- ロギング設定の設定　（21 ページ）

- [Add/Edit Rate Limited Syslog Message] ダイアログボックス （27 ページ）
- [Rate Limit] ページ （25 ページ）

フィールド リファレンス

表 15 : [Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス

要素	説明
ログ レベル（Logging Level）	レート制限を指定する syslog ロギング レベル。
メッセージ数（Number of Messages）	指定された時間に送信できる、指定されたタイプのメッセージの最大数。
間隔（秒）	レート制限カウンタがリセットされるまでの秒数。

[Add/Edit Rate Limited Syslog Message] ダイアログボックス

[Add Rate Limited Syslog Message]/[Edit Rate Limited Syslog Message] ダイアログボックスを使用して、特定の期間内に生成できる特定の Syslog ID のログ メッセージの最大数を指定できます。syslog メッセージ ID ごと、またはロギング レベルごとに制限を指定できます（[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （26 ページ）を参照）。設定が異なる場合、レート制限された syslog メッセージレベルの設定がレート制限のロギング レベルの設定を上書きします。

ナビゲーション パス

[Add Rate Limited Syslog Message]/[Edit Rate Limited Syslog Message] ダイアログボックスには、[Rate Limit] ページからアクセスできます。詳細については、[Rate Limit] ページ （25 ページ）を参照してください。

関連項目

- ロギング設定の設定 （21 ページ）
- [Rate Limit] ページ （25 ページ）
- [Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （26 ページ）

フィールド リファレンス

表 16 : [Add/Edit Rate Limited Syslog Message] ダイアログボックス

要素	説明
syslog ID	レート制限を指定する syslog メッセージの識別番号。

要素	説明
メッセージ数（Number of Messages）	指定された時間に送信できる、指定された ID を持つメッセージの最大数。
間隔（秒）	レート制限カウンタがリセットされるまでの秒数。

Syslog サーバ設定の設定

一般的な Syslog サーバ設定を設定して、Syslog サーバに送信される Syslog メッセージに含めるファシリティ コードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

関連項目

- Syslog サーバの定義 （35 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）**[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）]** を選択して、[Server Setup] ページ （30 ページ）を開きます。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 必要に応じて基本的なメッセージ設定を変更します。

- syslog サーバーでデフォルトとは異なるファシリティが必要な場合は、[ファシリティ（Facility）] リストで必要なファシリティを選択します。
- メッセージが生成された日時をメッセージに含める場合は、[タイムスタンプを各 Syslog メッセージで有効にする（Enable Timestamp on Each Syslog Message）] を選択します。
  - ロギングタイムスタンプを rfc5424 形式で設定する場合は、[タイムスタンプ形式の有効化（rfc5424）（Enable Timestamp Format(rfc5424)）] を選択します。このオプションは、ASA 9.12.1 デバイス以降に適用されます。タイムスタンプの出力例：

例：

```
2003-08-24T05:14:15.000003-07:00
```

- デバイス識別子を syslog メッセージに追加する場合は（これはメッセージの先頭に配置されます）、[Syslogデバイス IDを有効にする（Enable Syslog Device ID）] を選択し、ID のタイプを選択します。

（注） ASA クラスタの場合、クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタブートストラップ設定で割り当てられたローカルユニット名をデバイス ID（クラスタ ID オプション） として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。コントロールユニットのインターフェイス IP アドレスをすべてのクラスタデバイスに使用するかどうかも指定できます。

- [インターフェイス（Interface）]：アプライアンスがメッセージの送信に使用するインターフェイスに関係なく、指定されたインターフェイスの IP アドレスを使用します。[選択（Select）] をクリックして、インターフェイスを識別するインターフェイスまたはインターフェイス ロールを選択します。インターフェイス ロールは、単一のインターフェイスにマッピングされる必要があります。

ASA クラスタの場合、コントロールユニットのインターフェイス IP アドレスをすべてのクラスタデバイスに使用するように指定するには、[インターフェイス名（Interface Name）] フィールドで対応するオプションを選択します。

- [ユーザ定義ID（User Defined ID）]：選択したテキスト文字列を使用します（最大 16 文字）。
- [ホスト名（Host Name）]：デバイスのホスト名を使用します。
- [クラスタID（Cluster ID）]：デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

ステップ 3 [Syslog Message] テーブルを使用して、特定の Syslog メッセージのデフォルト設定を変更します。デフォルト設定を変更する場合にだけ、このテーブルでルールを設定する必要があります。メッセージに割り当てられている重大度を変更したり、メッセージが生成されてないように（ディセーブル化）したりできます。

- ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add/Edit Syslog Message] ダイアログボックス （34 ページ）に入力します。

設定を変更するメッセージ番号を選択してから、新しいシビラティ（重大度）レベルを選択するか、[抑制（Suppressed）] を選択してメッセージの生成をディセーブルにします。通常は、重大度レベルの変更やメッセージのディセーブル化は行いませんが、必要に応じて両方のフィールドを変更できます。[OK] をクリックしてテーブルにルールを追加します。

メッセージ重大度レベルの詳細については、ログ レベル （33 ページ）を参照してください。

- ルールを編集するには、ルールを選択して [行の編集（Edit Row）] ボタンをクリックし、目的の変更を加えて [OK] をクリックします。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。
- NetFlow を使用している場合は、[NetFlowと同等のsyslogを無効化（Disable NetFlow Equivalent Syslogs）] ボタンをクリックして、NetFlow と同等の syslog メッセージの生成を簡単にディセーブルにできます。

これにより、メッセージが抑止されたメッセージとしてテーブルに追加されます。これらの同等の syslog メッセージがすでにテーブルにある場合、既存のルールは上書きされません。

Syslog リレー構成

Cisco Security Manager サーバーで受信したイベントに加えて、最大 2 台の外部/リモートコントローラ（syslog ホスト）にイベントを転送できます。syslog リレーは、UDP syslog プロトコルを使用して受信したメッセージを別の syslog ホストに転送します。

Cisco Security Manager サーバーから転送された syslog メッセージに、syslog メッセージの送信元 IP アドレスとして Cisco Security Manager サーバーの IP アドレスを含めるには、CLI コマンドでそのアドレスを有効にする必要があります。

1. CSCOpx\MDC\logrelay に移動し、logrelay.properties ファイルを開きます。
2. 次のように、ext1 と ext2 の値を false に設定します。

```
## Source Preservation
#logrelay.dp.txring.ext0.preserve.source=true logrelay.dp.txring.ext1.preserve.source=false
logrelay.dp.txring.ext2.preserve.source=false
```

（注） デフォルトでは、ext1 と ext2 を false に設定することにより、値はすべてのコレクタに対して true になります。Cisco Security Manager は、Cisco Security Manager IP を使用して syslog メッセージを送信します。この変更は、リモートコレクタに対してのみ実行でき、ローカルコレクタ（ext0）に対しては実行できません。

[Server Setup] ページ

[Server Setup] ページでは、syslog サーバに送信される syslog メッセージに含めるファシリティコードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- Syslog サーバ設定の設定 （28 ページ）
- Syslog サーバの定義 （35 ページ）
- ロギング設定の設定 （21 ページ）
- ログ レベル （33 ページ）

フィールド リファレンス

表 *17 : [Server Setup]* ページ

要素	説明
Facility	アプライアンスが syslog サーバで定義されているメッセージに含める syslog ファシリティ コード。デフォルトは LOCAL4(20) です。これは UNIX システムで最も可能性の高いコードです。LOCAL0(16) ～ LOCAL7(23) のファシリティを選択できます。 Syslog ファシリティは、syslog データ ストリームを生成する各種ネットワーク デバイスを識別する必要のある集中 syslog モニタリング システムがある場合に役立ちます。ネットワーク デバイスは使用可能な 8 つのファシリティを共有するため、この値の変更が必要な場合があります。
Enable Timestamp on Each Syslog Message	メッセージが生成された日時を syslog メッセージに含めるかどうか。デフォルトでは、タイム スタンプは含められません。

要素	説明
Enable Syslog Device ID	EMBLEM 以外のフォーマットの syslog メッセージでデバイス ID を設定するかどうか。このオプションをオンにした場合は、次のいずれかをデバイス ID として使用することを選択します。これはすべての syslog メッセージの先頭に配置されます。 （注） ASA クラスタの場合、クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタブートストラップ設定で割り当てられたローカル ユニット名をデバイス ID（クラスタ ID オプション）として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。コントロール ユニットのインターフェイス IP アドレスをすべてのクラスタ デバイスに使用するかどうかも指定できます。 • [Interface]：選択したインターフェイスの IP アドレス。インターフェイスの名前を入力するか、あるいは [選択（Select）] をクリックしてリストから選択します（またはインターフェイスを指定するインターフェイス ロールを選択します）。適応型セキュリティ アプライアンスが外部サーバへのログ データの送信に使用するインターフェイスに関係なく、メッセージには、指定したインターフェイスの IP アドレスが含まれます。 インターフェイス ロールを選択する場合、そのロールはデバイス上の単一インターフェイスにマッピングされる必要があります。 ASA クラスタの場合、コントロール ユニットのインターフェイス IP アドレスをすべてのクラスタ デバイスに使用するように指定するには、[インターフェイス名（Interface Name）] フィールドで対応するオプションを選択します。 • [User Defined ID]：デバイス ID として定義するテキスト文字列。この文字列は最大 16 文字にできますが、次の特殊文字を含めることはできません。 & ’ " < > ? • [Host Name]：セキュリティ アプライアンスのホスト名。 • [Cluster ID]：デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

要素	説明
[Syslog Message] テーブル	このテーブルを使用して、特定の syslog メッセージの生成をイネーブルまたはディセーブルにしたり、メッセージの重大度レベルを変更したりします。生成されるメッセージ タイプが競合しないようにする場合、またはメッセージの重大度レベルを変更する場合は、このテーブルで何も設定する必要はありません。テーブルには、メッセージレベルを設定したメッセージ、および生成が抑止されているかどうか（テーブルの [true]）が表示されます。 • ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add/Edit Syslog Message] ダイアログボックス （34 ページ）に入力します。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[Delete Row] ボタンをクリックします。
[Disable NetFlow Equivalent Syslogs]/[Enable NetFlow Equivalent Syslogs]	NetFlow ロギングを使用している場合は、NetFlow メッセージと重複する syslog メッセージの生成をディセーブルにできます。[Disable] ボタンをクリックした場合、これらの重複する syslog メッセージが [Syslog Message] テーブルに抑止されたメッセージとして追加され、ボタンの名前が [Enable NetFlow Equivalent Syslogs] に変更されます。 [Enable] ボタンをクリックすると、重複する syslog メッセージがテーブルから削除され、抑止されなくなり、デバイスはこれらのメッセージの送信を再開します。ただし、[Disable] ボタンでリストに追加されたメッセージを手動で編集した場合、そのメッセージは [Enable] ボタンで削除されません。

ログ レベル

次の表で、ロギング レベルについて説明します。

表 *18 :* ログ レベル

ログ レベル（**Logging Level**）	タイプ	説明
[0]	Emergency	システムが使用不能です。システムが不安定であることを示すメッセージを生成します。
1	アラート	即時のアクションが必要です。即時の管理アクションを必要とするシステム整合性の問題を示すメッセージを生成します。
2	クリティカル	危険な状態です。クリティカルなシステムの問題を示すメッセージを生成します。

ログ レベル（**Logging Level**）	タイプ	説明
3	エラー	エラー条件。操作中のシステム エラーを示すメッセージを生成します。
4	警告	警告条件。システム警告を示すメッセージを生成します。たとえば、デバイスが正しく設定されていない可能性があります。
5	通知	正常だが注意を要する状態。通常は重大なイベントと見なされる正常な操作を示すメッセージを生成します。
6	Information	情報のみ。ネットワーク セッション レコードなど、通常の日常的なアクティビティであるシステム情報を示すメッセージを生成します。
7	Debugging	デバッグに役立つ syslog メッセージを生成します。また、FTP セッション中に発行されたコマンドおよび HTTP セッション中に要求された URL を示すログも生成します。すべての緊急事態、アラート、クリティカル、エラー、警告、通知、および情報メッセージを含みます。
-	無効	ロギングを行いません。

[Add/Edit Syslog Message] ダイアログボックス

[Add Syslog Message]/[Edit Syslog Message] ダイアログボックスでは、syslog メッセージのロギング レベルまたは抑止設定を変更します。

ナビゲーション パス

[Add Syslog Message]/[Edit Syslog Message] ダイアログボックスには、[Server Setup] ページ （30 ページ）からアクセスできます。

フィールド リファレンス

表 19 : [Add/Edit Syslog Message] ダイアログボックス

要素	説明
Syslog ID list	重大度レベルまたは抑止設定を変更するメッセージのメッセージ ログ ID。これらの値および対応するメッセージは、適切な製品の『System Log Message』ガイドに示されています。 **PIX ファイアウォール** http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html **ASA** http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html **FWSM** http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html （注） Cisco Security Manager 4.10 以降では、[Syslog ID] フィールドに syslog メッセージを入力できます。デバイスに対応する有効な syslog ID を入力してください。そうしないと、展開が失敗する可能性があります。
Logging Level list	メッセージに割り当てるロギング レベル。ロギング レベルと説明については、ログ レベル （33 ページ）を参照してください。 メッセージに割り当てるデフォルト レベルの使用を選択します（デフォルト）。
Suppressed	syslog メッセージの生成を抑止するかどうか。メッセージを抑止するとその生成がディセーブルになり、syslogs に表示されなくなります。
スタンバイでの Syslog の無効化（Disable Syslogs on Standby）	特定の syslog メッセージがスタンバイ ASA デバイスで生成されないようにするかどうか。この機能は ASA バージョン 9.4(1) から利用でき、Security Manager はバージョン 4.9 からこの機能をサポートします。

Syslog サーバの定義

[Syslog Servers] ページでは、セキュリティ アプライアンスが syslog メッセージを送信する syslog サーバを指定します。定義した syslog サーバを利用するには、[Logging Setup] ページを使用してロギングをイネーブルにし、[Logging Filters] ページを使用して宛先に適切なフィルタを設定する必要があります。

ヒント Security Manager Event Viewer を使用して ASA デバイスからイベントを表示する場合は、Security Manager サーバが syslog サーバとして定義されていることを確認してください。CS-MARS またはその他のアプリケーションを使用して syslog イベントを管理する場合はそれらのサーバをこのポリシーに含めてください。

セキュリティ アプライアンスで生成される syslog レコードを指示することで、レコードを処理および調査できます。

はじめる前に

ロギングをイネーブルにします。ロギング設定の設定 （21 ページ） を参照してください。

関連項目

- [Syslog Servers] ページ （37 ページ）
- [Add/Edit Syslog Server] ダイアログボックス （38 ページ）

ステップ 1 Select **Platform** > **Logging** > **Syslog** > **Syslog Servers** to display the Syslog Servers page.

ステップ 2 次のいずれかを実行します。

- 新しい syslog ターゲットを追加するには、[行の追加（Add Row）] ボタンをクリックします。
- 既存の syslog ターゲットを編集するには、その行のチェックボックスをオンにし、[行の編集（Edit Row）] ボタンをクリックします。

ステップ 3 [インタフェース（Interface）] フィールドで、インターフェイス名を入力または選択します。

リストには、現在のスコープに定義されているすべてのインターフェイスが表示されます。

ステップ 4 syslog サーバーの IP アドレスを [IPアドレス（IP Address）] フィールドで入力または選択します。

ステップ 5 UDP と TCP のいずれを使用するかを決定し、[Protocol] の下の適切なオプション ボタンをクリックします。

ステップ 6 セキュリティ アプライアンスが UDP または TCP syslog メッセージを送信するポートを入力します。ポートは、syslog サーバが受信するポートと同じである必要があります。

- TCP：1470（デフォルト）。TCP ポートは、セキュリティ アプライアンスの syslog サーバとだけ連携します。
- UDP：514（デフォルト）。

ステップ 7 EMBLEM フォーマットを使用して syslog メッセージを生成するには、[Cisco EMBLEMフォーマットのログメッセージ（Log messages in Cisco EMBLEM format）] チェックボックスをオンにします。

このオプションをイネーブルにするには、UDP プロトコルを選択してメッセージをこの syslog サーバにパブリッシュする必要があります。

ステップ 8 [OK] をクリック

定義が [Syslog Servers] テーブルに表示されます。

[Syslog Servers] ページ

[Syslog Servers] ページでは、セキュリティ アプライアンスが syslog メッセージを送信する syslog サーバを指定します。定義した syslog サーバを利用するには、[Logging Setup] ページを使用してロギングをイネーブルにし、[Logging Filters] ページを使用して宛先に適切なフィルタを設定する必要があります。

ヒント　Security Manager Event Viewer を使用して ASA デバイスからイベントを表示する場合は、Security Manager サーバが syslog サーバとして定義されていることを確認してください。CS-MARS またはその他のアプリケーションを使用して syslog イベントを管理する場合はそれらのサーバをこのポリシーに含めてください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [Syslogサーバー（Syslog Servers）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [Syslogサーバー（Syslog Servers）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- Syslog サーバの定義　（35 ページ）
- ロギング設定の設定　（21 ページ）

フィールド リファレンス

表 20 : [Syslog Servers] ページ

要素	説明
[Syslog Servers] テーブル	このデバイスが syslog メッセージを送信する syslog サーバ。テーブルには、サーバーにメッセージをパブリッシュするデバイスインターフェイス、サーバーの IP アドレス、syslog プロトコルとポート番号、およびメッセージが Cisco EMBLEM syslog フォーマットかどうかが表示されます。 コンテキストごとに設定できる syslog サーバは 4 つに制限されています。 • サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックし、 [Add/Edit Syslog Server] ダイアログボックス （38 ページ）に入力します。 • サーバーを編集するには、サーバーを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • サーバーを削除するには、サーバーを選択し、[行の削除（Delete Row）] ボタンをクリックします。
キュー サイズ	syslog サーバがビジーな場合にセキュリティ アプライアンスに syslog メッセージを格納するためのキューのサイズを指定します。最小は 1 メッセージです。デフォルトは 512 です。無制限の数のメッセージをキューに入れる場合は、0 を指定します（使用可能なブロック メモリによって制限されます）。
Allow user traffic to pass when TCP syslog server is down	TCP プロトコルを使用している 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。

[Add/Edit Syslog Server] ダイアログボックス

[Add Syslog Servers]/[Edit Syslog Servers] 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 syslog メッセージを送信する syslog サーバを追加または編集します。定義した syslog サーバを利用するには、[Logging Setup] ページを使用してロギングをイネーブルにし、[Logging Filters] ページを使用して宛先に適切なフィルタを設定する必要があります。

（注） コンテキストごとに設定できる syslog サーバは 4 つに制限されています。

ナビゲーション パス

[Add Syslog Servers] ダイアログボックスには、[Syslog Servers] ページからアクセスできます。[Syslog Servers] ページの詳細については、[Syslog Servers] ページ （37 ページ）を参照してください。

関連項目

- Syslog サーバの定義 （35 ページ）
- ロギング設定の設定 （21 ページ）

フィールド リファレンス

表 21 : [Add/Edit Syslog Server] ダイアログボックス

要素	説明
インターフェイス（Interface）	syslog サーバとの通信に使用するインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか、新しいオブジェクトを作成します。
IPアドレス	syslog サーバの IP アドレス。アドレスを定義するネットワーク/ホストポリシーオブジェクトの IP アドレスまたは名前を入力するか、[選択（Select）] をクリックしてネットワーク/ホストオブジェクトを選択します。 （注） Cisco Security Manager 4.13 以降、syslog サーバーで IPv6 アドレスがサポートされています。
プロトコル	syslog サーバで使用されるプロトコル（TCP または UDP）。UDP がデフォルトです。TCP ポートは、セキュリティ アプライアンスの syslog サーバとだけ連携します。 （注） EMBLEM フォーマットを使用する場合は、UDP を選択する必要があります。

要素	説明
[ポート（Port）]	セキュリティ アプライアンスが syslog メッセージを送信し、syslog サーバがそれらのメッセージを受信する TCP または UDP ポート。各プロトコルのデフォルト ポートは次のとおりです。 • TCP：1470 • UDP：514 ヒント　Security Manager サーバを syslog サーバとして定義している場合は、Security Manager Administration の[Event Management] ページにポート番号が表示されます。 （注）　Security Manager のインストールまたはアップグレード時に、Common Services syslog サービス ポートが 514 から 49514 に変更されます。あとで Security Manager がアンインストールされた場合、ポートは 514 に戻されません。
Log messages in Cisco EMBLEM format（UDP のみ）	メッセージを Cisco EMBLEM フォーマットでロギングするかどうか。syslog サーバでは UDP を使用する必要があります。 （注）　syslog サーバが Cisco Security MARS アプライアンスの場合は、このオプションを選択しないでください。Cisco Security MARS では、EMBLEM フォーマットが処理されません。
参照ID（Reference Identity）	バージョン 4.12 以降、Cisco Security Manager を使用すると、ポリシーオブジェクト セレクタから参照 ID ポリシーオブジェクト名を選択できます。 参照 ID は、ポートが TCP の場合にのみ有効になり、ポートが UDP の場合は無効になります。 詳細については、参照 IDを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。