イベントの表示

イベントビューアを使用すると、ASA（ASA-SM を含む）、FWSM および IPS デバイスからのイベントを選択してモニタリング、表示、および調査できます。イベントはビューに整理されます。重要なイベントを見つけるためにビューをフィルタリングまたは検索できます。必要に応じて、カスタマイズしたビューおよびフィルタを作成できます。または、アプリケーションに含まれる定義済みのビューを使用できます。

この章は次のトピックで構成されています。

Event Viewer 機能の概要

Event Viewer は、ASA および FWSM デバイス、ならびにセキュリティ コンテキストからの syslog（システム ログ）イベント、ならびに IPS デバイスおよび仮想センサーからの Secure Device Event Exchange（SDEE）イベントを対象にネットワークをモニタします。Event Viewer は、これらのイベントを収集し、収集したイベントを表示し、グループ化し、その詳細を調べるためのインターフェイスを備えています。

（注）　バージョン 4.5 以降、Security Manager では、syslog を 1 つのローカルコレクタと 2 つのリモートコレクタに転送できます。詳細については、[Event Management] ページを参照してください。

ヒント　Event Viewer および関連アプリケーションである Report Manager および Health and Performance Monitor は、ネットワーク内にある特定のタイプのシスコデバイスの動作モニタリングおよびトラブルシューティングに役立ちます。これらのアプリケーションでは、さまざまなイベントの相関付け、コンプライアンスレポート、長期的フォレンジック、またはシスコ製とシスコ製以外の両方のデバイスの統合モニタリングの機能は提供されません。

IPS イベントを処理する際、Cisco Security Manager の Report Manager コンポーネントはイベントを個別に報告します。 Cisco Security Manager のイベント ビューア コンポーネントにアラートが表示されます。イベント ビューア コンポーネントで、IPS Summarizer はイベントを単一のアラートにグループ化するため、IPS センサーが送信するアラートの数が減少します。

ヒント　Cisco IPS Manager Express（IME）と Cisco Security Manager は、まったく同じ方法ではイベントを要約しません。

ここでは、Event Viewer で簡易化できる主要なアクティビティについて簡単に説明します。

- 履歴ビュー　（2 ページ）
- リアルタイム ビュー　（3 ページ）
- ビューとフィルタ　（3 ページ）
- ポリシーのナビゲーション　（4 ページ）
- Event Viewer のアクセス コントロールについて　（5 ページ）
- Event Viewer のスコープおよび制限　（6 ページ）
- 詳細に解析される Syslog　（7 ページ）

履歴ビュー

履歴ビューは、選択した期間（たとえば、直前の 10 分間）に発生したイベントを表示するビューで、新規イベントが収集された場合でも表示内容は自動的には更新されません。より新しいイベントを表示するには、ビューをリフレッシュする必要があります。

Event Viewer で履歴ビューを使用する場合に考えられるさまざまな可能性の中から、次のアクティビティを見ていきます。

- **接続のトラブルシューティング**：ユーザーが特定のサーバーに到達できないというレポートが生成されたときには、そのユーザーの IP アドレスが送信元または宛先である場合に影響を与えるイベントをすべて表示するように履歴ビュー（たとえば、過去 10 分間）を設定できます。次に、表示された特定のイベントから、リソースに対するユーザーのアクセスを拒否するポリシーに進むことができます。

- **シグニチャの調整**：すべての IPS メッセージ、または特定のカテゴリに属するすべての IPS メッセージを表示するビューを設定すると、イベントが実際には誤検出であることを判別できます。次に、関連付けられたポリシーをクロス起動します。ホストを除外するようにシグニチャを調整するか、または問題のイベントでレポートされた重大度を低くします。

イベントアクションフィルタを作成して、アラートの処理方法を変更することも検討します。false positive の処理には、実際のシグニチャを編集するよりもイベントアクション フィルタを使用する方が良い場合がよくあります。詳細については、イベント アクション フィルタ ルールの管理に関するヒントを参照してください。

- **ポリシー展開の検証**：新規または変更したポリシーを展開したあとで、その特定のポリシーに対応するイベントを選択して、ポリシーが効果的に動作していることを確認する必要がある場合があります。たとえば、新規ポリシーによってトリガーされたファイアウォール拒否メッセージを特定できます。

リアルタイム ビュー

リアルタイム ビューには受信した状態のままのイベントが表示され、イベント テーブルがウォータフォール式に自動的に更新されます。「リアルタイム」という用語は正確な表現ではないことに注意してください。システム遅延をはじめとする要因により、真のリアルタイム システム応答は実現されません。

Event Viewer でリアルタイム ビューを使用する場合に考えられるさまざまな可能性の中から、次のアクティビティを見ていきます。

- **ほぼリアルタイムでの攻撃の**調査：特定の送信元 IP アドレスまたは送信元/宛先ペアの詳細を切り分けることで、監視対象デバイスに対する攻撃、または監視対象デバイスを通過している攻撃の詳細をイベントビューアで参照できます。
- **デバイスアクティビティの検証**：ネットワーク内のデバイスを調べて、デバイスの存在の有無、存在する場合にイベントを送信中であるかを判断できます。
- **脅威レベルの高いIPSイベントの表示**：特定の脅威レベルを超えるイベントをすべて表示するようにビューをフィルタ処理できます。IPS センサーを正しく調整すると、リアルタイム ビューで監視するイベントの流れが管理しやすくなります。

ビューとフィルタ

Event Viewer でイベントを表示するには、ビューを開きます。ビューは、フィルタおよび他のプロパティのセットです。これには、イベントのサブセットを定義できる色ルール、選択したカラムとその位置および幅、ならびにデフォルトの時間枠が含まれます。ビューによってイベント リストのスコープを制限できるため、検索内容をより簡単に見つけられます。

Event Viewer には多数の定義済みのビューがあります。定義済みのビューのフィルタ ルールは変更できませんが、ビューのコピーを作成して、コピーのフィルタ ルールを変更できます。作

成するビューはカスタム ビューと呼ばれます。詳細については、カスタム ビューの作成 （51 ページ）を参照してください。

Event Viewer を最大限活用するには、フィルタの使用が鍵となります。受信中のすべてのイベントから、必要とする情報だけを記載したビューを抽出できます。イベントリストを絞り込む（すでにフィルタリングされたイベントリストのフィルタリング）には、さまざまなフィルタリング方法が使用できます。次のリストに、一般的なフィルタリング機能を示します。詳細については、イベントのフィルタリングおよびクエリー （54 ページ）を参照してください。

- **時間フィルタ**：時間フィルタを使用すると、クライアントにロードするイベントを制限したり、イベントテーブルに表示されるイベントを制限したりできます。時間のフィルタリングでは、**直前の 1 時間**など定義済みの値を選択したり、日付と時刻で特定の時間範囲を指定したりできます。詳細については、イベントの時間範囲の選択 （54 ページ）を参照してください。
- **カラムフィルタ**：カラムフィルタを使用すると、イベントの特定の値に基づいてイベントをフィルタリングできます。たとえば、特定の送信元または宛先、あるいはその両方に対してフィルタリングできます。カラムによっては、値の範囲またはポリシーオブジェクトに対してもフィルタリングできます。カラムフィルタは、ビューに対するビュー設定の一部です。詳細については、カラムベース フィルタの作成 （56 ページ）を参照してください。
- **クイックフィルタ**：クイックフィルタを使用すると、イベントテーブルに一覧表示されたイベントに対してテキストベースのフィルタリングを実行できます。検索ではカラムを区別しません。いずれかのカラムに文字列が存在するイベントがすべて表示されます。フィルタのスコープを変更するには、[Quick Filter] ドロップダウン リスト（虫眼鏡として表示される）を使用します。詳細については、テキスト文字列に対するフィルタリング （60 ページ）を参照してください。
- **フィルタでのドリルダウン**：フィルタにさらに別のフィルタを集約すると選択性が高まり、要件を満たす特定のイベントまたはイベントセットが表示されるまで「ドリルダウン」できます。別のフィルタを選択するたびに、[Event Monitoring] ウィンドウの最上部にある [View Settings] ペインが更新されて、選択したビューの現在の集約フィルタ定義が表示されます。

ポリシーのナビゲーション

特定のイベントから、そのイベントを制御する Security Manager 内のポリシーにナビゲートできます。特定のポリシーから、そのポリシーに関連付けられたイベントに移動することもできます。詳細については、「Event Viewer からの Security Manager ポリシーの検索 （68 ページ）」および「Looking Up Events for a Cisco Security Manager Policy （70 ページ）」を参照してください。

Event Viewer のアクセス コントロールについて

ユーザ名に割り当てられたユーザ権限によって、Event Viewer で実行可能な操作が制御されます。ローカル ユーザまたは他のタイプの ACS 以外のアクセス コントロールを使用している場合は、すべてのユーザが Event Viewer にアクセスできます。ただし、次のアクセス制限が課されます。

- デバイスをモニタ対象として選択または選択解除するためには、システム管理者、ネットワーク管理者、またはアプルーバ権限を持っている必要があります。モニタするデバイスの選択 （42 ページ）を参照してください。
- Event Management の管理設定ページを変更するには、システム管理者権限を持っている必要があります。このページでは、Event Manager サービスの開始、停止、および設定 （37 ページ）および[Event Management] ページで説明するとおりに、サービスをイネーブルまたはディセーブルにしたり、ストレージの場所の設定やその他の設定を行います。

ACS を使用して Security Manager へのアクセスを制御する場合は、次も制御できます。

- View Event Viewer 権限を使用して、Event Viewer アプリケーションへのアクセスを制御できます。この権限を使用すると、特定のユーザによる Event Viewer へのアクセスを防げます。または、Report Manager へのアクセスを許可せずに Event Viewer へのアクセスを許可するロールを作成できます。すべてのデフォルト ACS ロールで Event Viewer を使用できます。
- [Modify] > [Manage Event Monitoring] 権限を使用して、デバイスのモニタリングをイネーブルまたはディセーブルにできるユーザを制御できます。モニタするデバイスの選択 （42 ページ）で説明するとおりに、デバイスをモニタ対象として選択するには、ユーザがこの権限を持っている必要があります。この権限を持つデフォルト ACS ロールは、システム管理者、ネットワーク管理者、アプルーバ、セキュリティ管理者、およびセキュリティ アプルーバです。
- ポリシー検索機能の使用を制御できます。ポリシー検索を実行するには、デバイスに対するデバイスの表示権限、およびファイアウォールまたは IPS ポリシーに対する表示権限もユーザが持っている必要があります。すべての権限を持っていないユーザーが一致ルールの検索を試みると、「Unable to Find Matching Rule」エラーが発生します。ポリシー検索の詳細については、Event Viewer からの Security Manager ポリシーの検索 （68 ページ）を参照してください。
- ユーザは、少なくともデバイスに対する表示権限がある場合にのみ、そのデバイスのイベントを表示できます。
- Event Management の管理設定ページへのアクセスを制御できます。このページでは、Event Manager サービスの開始、停止、および設定 （37 ページ）および[Event Management] ページで説明するとおりに、サービスをイネーブルまたはディセーブルにしたり、ストレージの場所の設定やその他の設定を行います。このページ（またはその他の管理設定ページ）にアクセスするには、ユーザは Admin 権限を持っている必要があります。ヘルプ デスクを除く、すべてのデフォルト ACS ロールでページを表示できますが、設定を変更できるのはシステム管理者だけです。

- カラム フィルタ（[Device]、[Source]、[Destination]、[Source Service]、および [Destination Service] カラムなど）に対するネットワーク/ホストおよびサービス ポリシー オブジェクトの使用を制御できます。ネットワーク/ホスト、ネットワーク/ホスト-IPv6、およびサービス オブジェクトをフィルタで使用するには、これらに対する適切なオブジェクトの表示権限をユーザが持っている必要があります。カラム フィルタの作成の詳細については、カラムベース フィルタの作成 （56 ページ）を参照してください。

Cisco Security Manager と Cisco Secure ACS との統合の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

Event Viewer のスコープおよび制限

次の表に、Event Viewer の機能面のスコープおよび制限について詳しく示します。

表 *1 : Event Viewer* のスコープおよび制限

項目	説明
デバイス サポート	次のタイプのデバイスから収集されたイベントを表示できます。Event Viewer は、次に示すソフトウェア リリースでテスト済みですが、より古いソフトウェア リリースで使用できる場合があります。 • **ASA デバイス（ASA-SM を含む）とセキュリティコンテキスト**：すべての 8.x リリース。 • **FWSM デバイスとセキュリティコンテキスト**：リリース 3.1.17、3.2.17、4.0.10、および 4.1.1 以降。 • **IPS デバイスと仮想センサー**：リリース 6.1 以降。 IPS サポートに IOS IPS は含まれません。
イベント データストアのサイズと場所	モニタ対象のデバイスから収集されたイベントを格納するために割り当てる場所とディスク スペースを制御できます。[Event Data Store Disk Size] に 90% と入力すると、最古のイベントから順に最新のイベントに置き換わります。 拡張ストレージまたはアーカイブの場所を接続したストレージ デバイス上に設定できます。Security Manager は、自動的に拡張ストレージにイベントをコピーします。過去のイベントを表示したときに、過去のイベントがローカル ディスクに存在しなくなっている場合には自動的に拡張ストレージから取得されます。 これらの設定の構成に関する詳細については、[Event Management] ページを参照してください。
イベントの制限	[Event Data Pagination Size] オプションを使用して、イベント テーブル内で一度に表示できるイベントの最大数を制御できます。このオプションの設定の詳細については、[Event Management] ページを参照してください。

項目	説明
ポリシー オブジェクト	カラム フィルタを作成する場合には、ネットワーク/ホストやサービス オブジェクトなど一部のタイプのポリシー オブジェクトを使用できます。 [表示（View）] > [ネットワークホストオブジェクトの表示（Show Network Host Objects）] を選択して、送信元および宛先カラムに IP アドレスではなくホストオブジェクト名を表示することもできます。このオプションは、デフォルトで選択されます。 IP アドレスからホスト名へのマッピングは、イベントの送信元および宛先だけでサポートされます。また、マッピングはホスト オブジェクトだけに適用されます。イベントの送信元または宛先がネットワーク オブジェクト、グループ オブジェクト、またはアドレス範囲オブジェクトに一致した場合は、Event Viewer ではオブジェクト名が表示されません。 **ヒント** そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
ビュー	単一の Event Viewer クライアントでは、最大 4 つの履歴ビューと 1 つのリアルタイム ビューを同時に開けます。
クライアント	1 台の Security Manager サーバーに対して、最大 5 つの Security Manager クライアントが同時にイベントビューアを開くことができ、Security Manager クライアントごとにイベントビューアのコピーを 1 つ開くことができます。

詳細に解析される Syslog

標準の syslog の構造と内容、およびそれぞれを構成する要素の詳細については、使用するデバイスおよびソフトウェア バージョンのシステム ログのマニュアルを参照してください。

マニュアルは、Cisco.com の次の場所にあります。

- ASA デバイス:
  http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html [英語]
- FWSM デバイス:
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_system_message_guides_list.html [英語]

ここに挙げられていない syslog は、未処理 syslog として表示されます。syslog の全内容が表示されるのは、詳細に解析される syslog だけです。

Security Manager で詳細に解析される syslog の詳細については、次の表を参照してください。

表 *2:* 詳細に解析される *Syslog*

syslog カテゴリ	syslog ID	syslog の合計数
フロー、セッション syslog	110002 ～ 110003、209003 ～ 209005、302003 ～ 302004、302009 ～ 302010、302012 ～ 302018、302020 ～ 302021、302035 ～ 302036、302303 ～ 302306、302033 ～ 302034、303002 ～ 302005、313001、313004、313005、313008、324000 ～ 324006、337001 ～ 337009、431001 ～ 431002、407001 ～ 407002、416001、418001 ～ 418002、419001 ～ 419003、424001 ～ 424002、450001、448001、609001 ～ 609002 （注） 302303 ～ 302306 の状態バイパス syslog は、イベントマネージャについてのみ詳細に解析されています。ただし、TCP、UDP、およびSCTP状態バイパス syslog のイベントマネージャのイベント説明には、「State-bypass」キーワードが表示されません。 （注） レポート、イベントからポリシー、およびポリシーからイベントは、状態バイパス syslog ではサポートされていません。	66
ボットネット	338001 ～ 338004、338101 ～ 338104、338201 ～ 338202、338301	11
ACL	106100、106023、106002、106006、106018	5
拒否されたファイアウォール	106001、106007、106008、106010 ～ 106017、106020 ～ 106022、106025 ～ 106027	17
アイデンティティファイアウォール	746003、746005、746010、746016	4
AAA	109001 ～ 109010、109012、109016 ～ 109020、109023 ～ 109029、109031 ～ 109035、113001 ～ 113025	53
検査	108002 ～ 108007、303004 ～ 303005、400000 ～ 400050、406001 ～ 406002、415001 ～ 415020、500001 ～ 500005、508001 ～ 508002、608001 ～ 608005、607001 ～ 607003、703001 ～ 703002、726001	99
NAT	201002 ～ 201006、201009 ～ 201013、202005、202011、305005 ～ 305012	20
IPSec VPN	402114 ～ 402122、602103 ～ 602104、602303 ～ 602304、702305、702307	15

syslog カテゴリ	syslog ID	syslog の合計数
フェールオーバー（HA）	101001 ～ 101005、102001、103001 ～ 103007、104001 ～ 104004、311001 ～ 311004、709001 ～ 709007、210001 ～ 210022（210008、210010 を除く）	48
SSL VPN	725001 ～ 725009、725012 ～ 725013、716001 ～ 716020、716023 ～ 716039、716041 ～ 716060、722001 ～ 722023、722026 ～ 722044、722046 ～ 722051、723001 ～ 723002、723009 ～ 723012、723014、724001 ～ 724004	128
Etherchannel	426001 ～ 426003	3
クラスタ	302022 ～ 302027	6

Event Viewer の概要

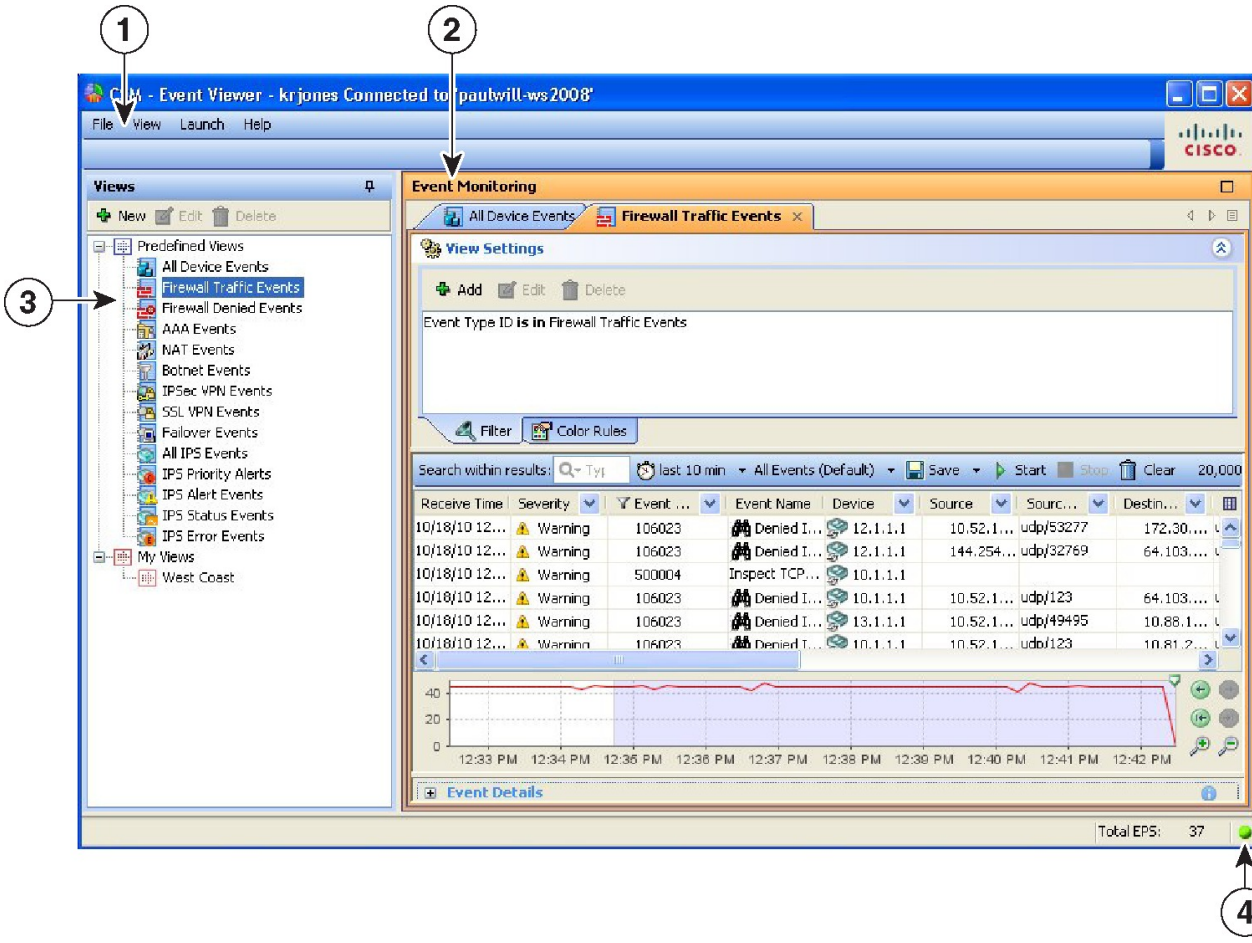
Event Viewer を使用すると、モニタ対象のファイアウォールおよび IPS デバイスから収集したイベントおよびアラートを表示できます。モニタ対象のデバイスの選択の詳細については、モニタするデバイスの選択 （42 ページ）を参照してください。

Event Viewer を起動するには、次のいずれかを実行します。

- Windows Start メニューから [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Security Managerクライアント（Cisco Security Manager Client）] > [イベントビューア（Event Viewer）] を選択するか（正確なコマンドパスは異なる場合があります）、デスクトップの [イベントビューア（Event Viewer）] アイコンをダブルクリックします。ログインを求められます。Cisco Security Manager クライアント アプリケーションの開始方法の詳細については、Security Manager クライアントへのログインおよび終了を参照してください。
- Configuration Manager または Report Manager アプリケーションから [起動（Launch）] > [イベントビューア（Event Viewer）] を選択するか、Configuration Manager ツールバーの [イベントビューア（Event Viewer）] ボタンをクリックします。Event Viewer が他のアプリケーションへのログインに使用したのと同じユーザ アカウントを使用して開かれます。

次の図と後続のリストに、Event Viewer の基本的要素について示します。

図 *1 : Event Viewer* のメイン ウィンドウ



次のリストに、メインの Event Viewer ウィンドウの詳細を示します。

- **（1）メニューバー**：イベントビューアでアクションを実行するための一般的なコマンドです。次のメニューが含まれます。
  - [File]：ビューでの操作に使用します。コマンドの詳細については、『Event Viewer の [File] メニュー （12 ページ）』を参照してください。
  - [View]：ビュー内での操作および一般的システム管理に使用します。コマンドの詳細については、『Event Viewer の [File] メニュー （12 ページ）』を参照してください。
  - [Launch]：Configuration Manager または Report Manager アプリケーションの開始に使用します。
  - [Help]：オンライン ヘルプの開始、または著作権とライセンス情報の表示に使用します。

- **（2）イベントモニタリングウィンドウ**：開いているビューが右ペインに表示されます。開いている各ビューは、別々のタブに示されます（最大 4 つの履歴ビューと 1 つのリアルタイム ビューが開けます）。このスペース内でビューを水平または垂直に配置する、また

は別のウィンドウにビューをフローティングもできることに注意してください。ビューの配置方法またはフローティング方法の詳細については、ビューのフローティングと配置（47 ページ）を参照してください。

[Event Monitoring] ウィンドウの数々の部分の詳細については、[Event Monitoring] ウィンドウ（17 ページ）を参照してください。

- **（3）ビューリスト**：左ペインはビューのリストです。ビューのリストでは、定義済みのビューとカスタム ビューが別々にフォルダに整理されます。カスタム ビューは [My Views] フォルダに一覧表示されます。最も簡単にビューを開く方法は、ビューをダブルクリックする方法です。これにより、現在開いているビューが置き換えられます。現在開いているビューと置き換えずにビューを開くには、ビューを右クリックし、[新しいタブで開く（Open in New Tab）] を選択します。ビューを開く方法の詳細については、ビューを開く（47 ページ）を参照してください。

ビューのリストのペインで実行できるその他の操作の詳細については、ビューリスト （15 ページ）を参照してください。

- **（4）ステータス情報**：ステータスバーの右下部分には、現在の1 秒あたりのイベント（EPS）レートおよびモニタリングシステムの現在のヘルスを示すアイコンが表示されます。アラート ステータス アイコンをクリックして、過去 5 分の統計情報および現在のシステム アラートを表示するバブルを開きます。このビューから [Details] リンクをクリックして詳細情報を表示できます。バブルを閉じるには、アラート ステータス アイコンをもう一度クリックします。詳細については、Event Manager サービスの管理 （37 ページ）を参照してください。

（注） ステータスバーに表示される 1 秒あたりのイベント（EPS）情報は、2 秒ごとに受信されるイベントの数に基づいて計算されます。一方、タイムスライダーグラフに表示される EPS 情報は、選択した時間範囲で使用可能なすべてのイベントの集約を実行することによって計算されます。したがって、ステータスバーとタイムスライダーグラフに表示される数値が異なる場合があります。

次の例を参照してください。

ステータスバーの EPS 情報の表示例

時間 T1 で、イベント ビューア アプリケーションが 192 個のイベントを受信したとします。ステータスバーに表示される 1 秒あたりのイベント数（EPS）は、192 / 2 = 96 です。これは、Security Manager が 2 秒ごとにイベントを収集し、ステータスバーに 1 秒あたりのイベントを表示するためです。T1 + 2 秒で、イベント ビューア アプリケーションが 384 個のイベントを受信したとします。ステータスバーに表示される EPS は、（384 - 192）/2 = 96 になります。これは、現在の値と以前の値の差を 2 で割ったものです。

タイムスライダーグラフでの EPS 情報の表示例

Security Manager は、10 秒間隔で 1 秒あたりのイベントを保持します。たとえば、イベントビューア アプリケーションが 10 秒間隔で 352 個のイベントを受信した場合、EPS は 352 / 10 = 35 になります。この値は、Security Manager によって保持されます。次の 10 秒の間隔で、イベントビューアが 1056 のイベントを受信すると、EPS は（1056 – 352）/10 = 70 になり、これは Security Manager によって保持されます。

タイムスライダーグラフに値を表示する

タイムスライダーグラフには、開始時刻と終了時刻がある期間の情報が表示されます。指定された時間間隔で収集された 1 秒あたりのすべてのイベントが集計され、グラフにプロットされます。この例では、35 と 70 が 10 秒ごとに保存される値です。したがって、タイムスライダーグラフには EPS が 35 および 70 として表示されますが、これらはステータスバーに表示される値とは異なります。

Event Viewer の [File] メニュー

次の表に、Event Viewer の [File] メニューのコマンドを示します。

表 *3 : Event Viewer* の *[File]* メニュー

コマンド	説明
New View	新規カスタム ビューを作成します。名前および説明の入力を求められます。カスタム ビューの作成 （51 ページ）を参照してください。 または、ビューリストの [新規（+） （New (+)）] ボタンをクリックします。
Open View	新規タブにビューを開きます。開くビューを選択するように要求されます。最大で 4 つの履歴ビューと 1 つのリアルタイム ビューを開くことができます。ビューを開く （47 ページ）を参照してください。 **ヒント** ビューのリスト内でダブルクリックして、ビューを開いて表示されているビューと置き換えます。
Save	フィルタ（カスタム ビューの場合のみ）、ならびに選択したカラム、カラム幅、およびソート順序などのテーブル プリファレンス、時間範囲や色ルールなど、アクティブなビューに加えた変更を保存します。ビューの保存 （53 ページ）を参照してください。 定義済みのビューのフィルタ変更を保存する場合は、[Save As] を使用して新規カスタム ビューを作成する必要があります。
Save As	表示されているビューに加えた変更をカスタム ビューとして保存します。ビューの保存 （53 ページ）を参照してください。
Close View	表示されているビューを閉じます。

コマンド	説明
Close All Views	開かれているすべてのビューを閉じます。
終了（Exit）	Event Viewer を閉じます。Event Viewer を終了すると、開いているフローティング Event Viewer ウィンドウが閉じられます。

Event Viewer の [View] メニュー

次の表に、Event Viewer の [View] メニューのコマンドを示します。

表 *4 : Event Viewer* の *[View]* メニュー

コマンド	説明
[モード（Mode）]	イベントテーブルに表示するイベントを選択する時間間隔を指定します。サブメニューから次のオプションのいずれかを選択します。 • **last 10 minutes** • [過去 1 時間（last 1 hour）] • **last 12 hours** • **last 1 day** • **last 1 week** • **is today** • **is yesterday** • **[次の日（is on . . .**（カレンダーが開き、カレンダー上で単一の日付をクリックして指定できます） • [次の期間（is between）]（カレンダーが 2 つ開き、カレンダー上で開始と終了の日付と時刻を指定できます） • [リアルタイム（Real Time）]（イベントを受信した状態のまま表示するモードを設定します） または、ツールバーの [時間セレクタ（Time Selector）] コントロールをクリックして、同じオプションから選択します。イベント テーブル ツールバー （19 ページ）を参照してください。
Customize Column	イベント テーブルに表示するカラムを変更します。[Choose Columns to Display] ダイアログボックスが開き、表示するカラムを選択できます。使用可能なカラムの詳細については、イベント テーブルのカラム （22 ページ）を参照してください。

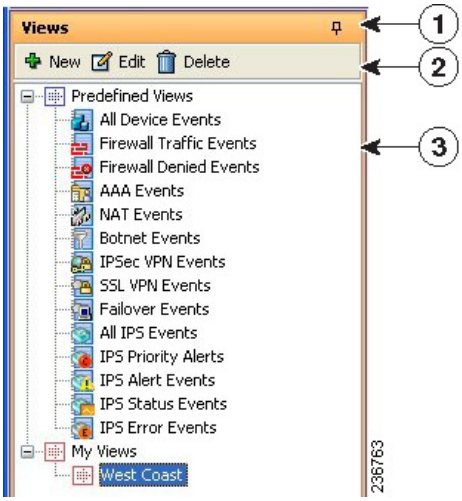
コマンド	説明
開始（Start）	イベントを取得して現在のビューのイベントテーブルを更新する作業を開始します。イベントテーブルには、[開始（Start）] をクリックしたときから時間モードの制限またはイベントテーブルの改ページ制限になるまでに受信したイベントが表示されます。 または、イベントテーブルツールバーの [開始（Start）] ボタンをクリックします。
停止（Stop）	イベント取得を停止します。イベントテーブルには、[停止（Stop）] をクリックするまでに受信したイベントが表示されます。 または、イベントテーブルツールバーの [停止（Stop）] ボタンをクリックします。
Show View Settings	[View Settings] ペインを開きます。ここには、現在のビューのフィルタおよび色設定が表示されます。このような設定は、[View Settings] ペインを使用して変更できます。 または、[View Settings] ペイン タイトル バー内のアイコン、テキスト、またはタイトルバーの右側の二重矢印などの任意の場所をクリックします。見出しをクリックすると、ペインが開閉します。
Show Event Details	[イベントの詳細（Event Details）]ペインを開き、選択されたイベントの詳細を表示します。 または、下記の手順も実行できます。 • [イベントの詳細（Event Details）]ペインのタイトルバーの左側にある展開アイコン（+）をクリックします。 • イベント テーブルのイベントをダブルクリックして、ポップアップ ウィンドウにイベントの詳細データを表示します。 ヒント [Event Details] ダイアログボックスから、イベント詳細を印刷したり、詳細の 1 行以上をクリップボードにコピーしたりできます。また、[Next] および [Previous] ボタンを使用して、イベントリスト全体をスクロールできます。
Manage Monitored Devices	いずれのデバイスまたはデバイス グループのイベントを Event Viewer に表示するかを選択できます。詳細については、モニタするデバイスの選択（42 ページ）を参照してください。 （注） デフォルトでは、Security Manager インベントリに追加されたすべての ASA、FWSM、または IPS デバイスが監視されます。
Show Event Store Disk Usage	使用されているディスク容量と保存されている最も古いイベントの経過時間を示すウィンドウが開きます。イベント データ ストア用のディスク スペースの使用率のモニタリング （44 ページ）を参照してください。

コマンド	説明
Show Network Host Objects	オンにすると、送信元または宛先IPアドレスの代わりにホストオブジェクト名が表示されます（使用可能な場合）。このオプションは、デフォルトで選択されます。 **ヒント** そのオブジェクトに関連付けられたIPアドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
Reset Layout	非表示にしていたか、または手動で拡大縮小していたビューのリストペインの幅を元の設定に戻します。

ビューリスト

Event Viewer メイン ウィンドウの左ペインには、次の図に示すように使用可能なビューのリストが表示されます。ビューは、フィルタおよび他のプロパティのセットです。これには、イベントのサブセットを定義できる色ルール、選択したカラムとその位置および幅、ならびにデフォルトの時間枠が含まれます。

図 *2:* イベントビューアのビューリスト



ビューのリストには、次のコントロールが含まれます。

- **（1）プッシュピンボタン**：ビューリストペインを開くか閉じるかを制御するには、プッシュピンアイコンをクリックします。ピンが垂直の場合、[Event Monitoring] ウィンドウ（右ペイン）を最大化しないかぎり、ビューのリストは開いたままになります。ピンが水平の場合、ビューのリストは左端に縮小されます。リストを開くには、左端のビューの見出しをクリックする必要があります。
- **（2）ツールバー**：ツールバーには次のボタンが含まれています。

- [新規（New）] ボタン：新規カスタムビューを作成するには、[新規（New）] ボタンをクリックします。ビューの名前および説明の入力を求められます。詳細については、カスタム ビューの作成 （51 ページ）を参照してください。
- [編集（Edit）] ボタン：選択したカスタムビューの名前または説明を変更するには、[編集（Edit）] ボタンをクリックします。カスタム ビューのみを編集できます。詳細については、カスタム ビューの名前または説明の編集 （52 ページ）を参照してください。
- [削除（Delete）] ボタン：選択したカスタムビューを削除するには、[削除（Delete）] ボタンをクリックします。カスタム ビューだけが削除できます。詳細については、カスタム ビューの削除 （53 ページ）を参照してください。

- **（3）ビューのリスト**：リストでは、定義済みのビューとカスタムビューが別々のフォルダに整理されます。カスタムビューは [マイビュー（My Views）] フォルダに一覧表示されます。最も簡単にビューを開く方法は、ビューをダブルクリックする方法です。これにより、現在開いているビューが置き換えられます。現在開いているビューと置き換えずにビューを開くには、ビューを右クリックし、[新しいタブで開く（Open in New Tab）] を選択します。ビューを開く方法の詳細については、ビューを開く （47 ページ）を参照してください。
- **右クリック ショートカット メニュー**：ビューで右クリックすると、実行可能な追加のコマンドのリストが表示されます。
  - [Open]：ビューを開いて現在アクティブなビューと置き換えます。現在アクティブなビューに保存されていない変更が含まれる場合は、変更の保存を求められます。ビューがすでに開いている場合は、最前面に移動されます。ビューを開く （47 ページ）を参照してください。
  - [Open in New Tab]：新規タブにビューを開きます。このため、既存の開いているビューは閉じません。ビューを開く （47 ページ）を参照してください。
  - [名前を付けて保存（Save As）]：ビューを新しいカスタムビューとして保存します。ビューの保存 （53 ページ）を参照してください。
  - [Edit]：カスタム ビューの名前と説明を編集します。カスタム ビューの名前または説明の編集 （52 ページ）を参照してください。
  - [Delete]：カスタム ビューを削除します。カスタム ビューの削除 （53 ページ）を参照してください。
  - [View Description]：ビューの説明を表示します。

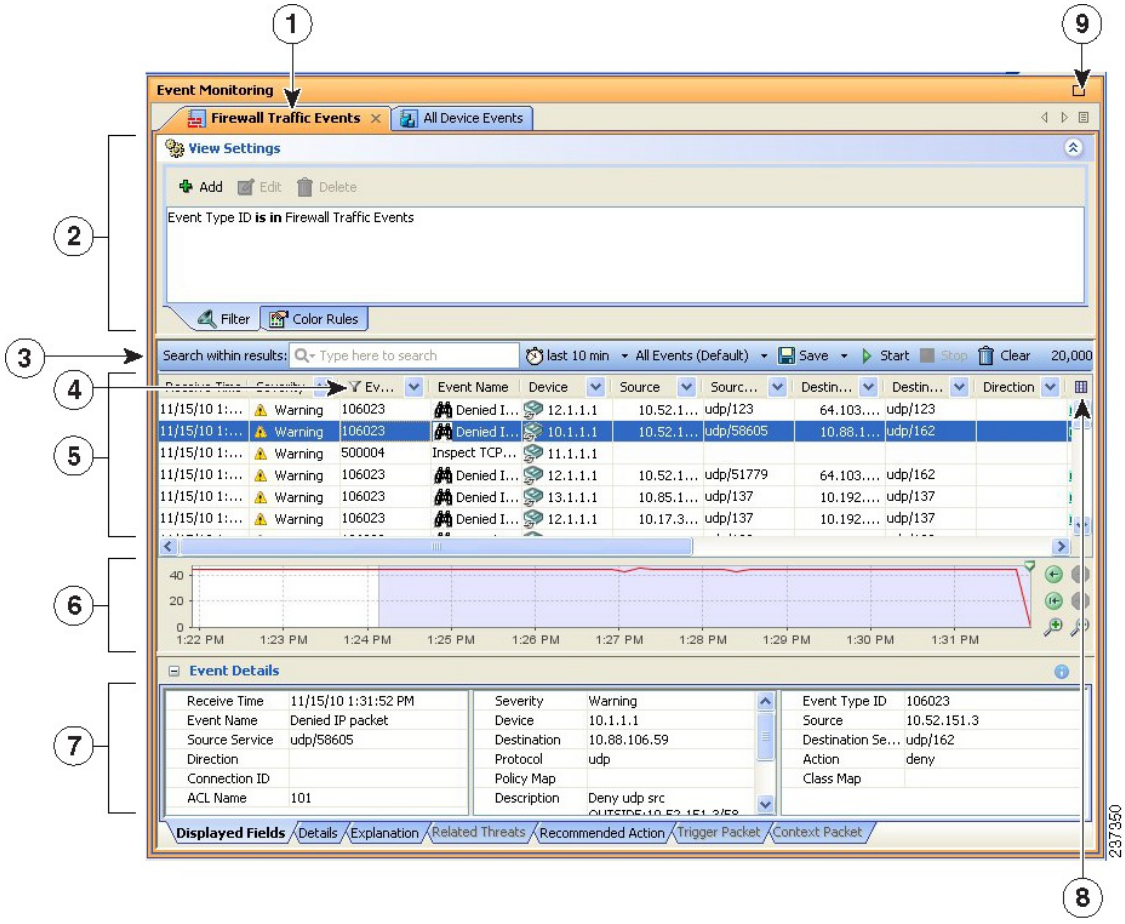
関連項目

- ビューとフィルタ （3 ページ）
- Event Viewer の概要 （9 ページ）
- ビューのフローティングと配置 （47 ページ）

[Event Monitoring] ウィンドウ

[イベント監視（Event Monitoring）] ウィンドウには、開いているイベントビューが表示されます。このウィンドウでビューの設定およびフィルタ イベントの分析ができます。

図 3 : [Event Monitoring] ウィンドウ



1	ビューのタブ。	6	時間スライダ。
2	[View Settings] ペイン。	7	[Event Details] ペイン。
3	イベント テーブル ツールバー。	8	[Column Selector] ボタン。
4	[Filtered Column] アイコン。	9	[Open View] スクロール ボタンとリスト。
5	イベント テーブル。		

[Event Monitoring] ウィンドウには、次の主要な要素が含まれています。

- **View tabs (1, 9)**：ビューを開くと、ウィンドウ内のタブとして示されます。ビューを変更するには、タブをクリックする、左右矢印ボタンをクリックしてタブ全体をスクロールする、または [Open View List] ボタンをクリックして目的のビューを選択する、のいずれか

を実行します。タブ名を右クリックし、適切なコマンドを選択して、ビューを並べて表示するまたは別のウィンドウにフローティングするように配置できます。詳細については、ビューのフローティングと配置 （47 ページ）を参照してください。

（注） 最大で 4 つの履歴ビューと 1 つのリアルタイム ビューを開くことができます。

- **View Settings pane (2)**：[ビューの設定（View Settings）] ペインを使用して、ビューで使用するカラムフィルタおよび色ルールを定義します。見出しの任意の場所をクリックするか、または [ビュー（View）] > [ビューの設定を表示（Show View Settings）] コマンドで切り替えて、ペインを開いたり閉じたりできます。

[View Settings] ペインには、[Filter] および [Color Rules] の 2 つのタブがあります。これらのタブは、ペインの下部に沿って表示されます。各タブ上で、タブの本体には現在のフィルタまたはルールが表示されます。ルールを変更するには、ルールを選択し、必要に応じてペインの上部に沿って表示される [Edit] または [Delete] ボタンをクリックします。新規ルールを作成するには、[Add] ボタンをクリックします。

カラムベース フィルタの作成 （56 ページ）で説明するとおりに、イベント テーブルのカラム フィルタリング コントロールを使用して、フィルタを追加することもできます。色ルールの詳細については、ビューの色ルールの設定 （50 ページ）を参照してください。

- **Event Table Toolbar (3)**：イベントテーブルの上部にあるツールバーには、テーブルに一覧表示されたイベントに明確に関連するショートカットボタンやその他のコントロールが含まれます。ツールバー コントロールの詳細については、イベント テーブル ツールバー （19 ページ）を参照してください。

- [Event Table (4, 5, 8)]：イベントテーブルには、フィルタ基準に一致するイベントが各行に 1 つ表示されます。これらのイベントは、プライマリまたは拡張データ ストアから取得される場合があります。明示的に拡張データ ストアからデータを要求する必要はありません。デバイスからのイベントを表示するには、そのデバイスに対するデバイスの表示権限を持っている必要があります。

イベント テーブルの表示のカスタマイズ （48 ページ）で説明するとおりに、イベント テーブルを構成しているカラムに対しては、非表示、サイズ変更、順序の並べ替え、およびソートが可能です。カラムの説明、および表示するカラムを選択する [Column Selector] ボタンの使用方法の詳細については、イベント テーブルのカラム （22 ページ）を参照してください。

カラムにフィルタが適用されている場合は、カラムの見出しにアイコンが表示されます。

- **Time Slider (6)**：履歴ビューの場合、時間スライダには、テーブル内に表示された時間の現在のスライス、およびイベントレート（/秒）が線形グラフとして表示されます。時間スライダの使用方法の詳細については、時間スライダ （32 ページ）を参照してください。

- **Event Details Pane (7)**：[イベント詳細（Event Details）] ペインには、現在選択されているイベントの詳細情報が表示されます。見出しの任意の場所をクリックするか、または [ビュー（View）] > [イベントの詳細を表示（Show Event Details）] コマンドで切り替えて、

ペインを開いたり閉じたりできます。詳細については、[Event Details] ペイン （33 ページ）を参照してください。

イベント テーブル ツールバー

次の図と表に、Event Viewer のイベント テーブルのすぐ上にあるツールバーの要素を示します。

表 5: イベント テーブル ツールバーの要素

コールアウト	名前	説明
1	[Search Within Results] フィールド （クイック フィルタ）	このツールは、クイックフィルタとも呼ばれます。この要素は、単語またはフレーズを検索し、検索スコープを特定のカラムに限定する場合に使用します。また、使用する検索語句で大文字と小文字を区別するかどうか、ワイルドカードを使用できるかどうか、および一致は部分一致か、大文字と小文字を区別するか、完全一致か、文字列内の任意の位置に含まれていればよいかを選択できます。この検索は、選択したビューおよびロードされたデータ内でだけ動作します。詳細については、テキスト文字列に対するフィルタリング （60 ページ）を参照してください。

コールアウト	名前	説明
2	Time Selector（モード） （[表示（View）] > [モード（Mode）]に相当）	時間セレクタは、次の手順を実行する場合に使用します。 • イベント テーブル ペインに表示するイベントを受信した時間に応じてフィルタリングします。イベントの時間範囲の選択 （54 ページ）を参照してください。 • リアルタイム ビューまたは履歴ビューから選択します。リアルタイム ビューと履歴ビュー間の切り替え （52 ページ）を参照してください。 • クライアントにロードする時間間隔を指定します。現在時刻から過去にさかのぼってイベントを表示するモードの 1 つを使用している場合は、ポインタをフィールドに重ねると、表示されたイベントの開始と終了時刻が表示されます。特定の時間間隔を使用している場合は、ツールバーに時間間隔が表示されます。
3	Events by IP Address Type Selector	イベントに含まれる IP アドレス タイプに基づいてリストをフィルタリングするために、[Events by IP Address Type Selector] を使用します。次のオプションがあります。 • [全てのイベント（All Events）]（デフォルト）：アドレスタイプに関係なくすべてのイベントを表示します。これがデフォルトのオプションです。 • [IPv4イベントのみ（IPv4 Events Only）]：イベントのすべてのアドレスがIPv4形式の場合にのみイベントを表示します。 • [IPv6イベントのみ（IPv6 Events Only）]：イベントの少なくとも1つのアドレスがIPv6形式の場合にのみイベントを表示します。 **ヒント** 選択は保存できません。次回ビューを開いたときにデフォルト以外が必要な場合は、再度オプションを選択する必要があります。

コールアウト	名前	説明
4	保存 （[ファイル（File）] > [保存（Save）] または [ファイル（File）] > [別名で保存（Save As）] に相当）	フィルタ（カスタムビューの場合のみ）、ならびに選択したカラム、カラム幅、およびソート順序などのテーブルプリファレンス、時間範囲や色ルールなど、現在のビューに加えた変更を保存するには、[保存（Save）] をクリックします。 または、下矢印をクリックし、[別名で保存（Save As）] を選択して変更を新規カスタムビューとして保存します。定義済みのビューのフィルタ変更を保存する場合は、[Save As] を使用して新規カスタム ビューを作成する必要があります。詳細については、カスタム ビューの作成 （51 ページ）を参照してください。
5	開始（Start） （[表示（View）] > [開始（Start）] に相当）	イベントテーブルにイベントリストをリロードまたは再起動するには、[開始（Start）] をクリックします。[Start] をクリックすると、テーブルを最初にロードしてから発生したすべてのイベントを取得します。
6	停止（Stop） （[表示（View）] > [停止（Stop）] に相当）	イベントテーブルのイベントリストを停止するには、[停止（Stop）] をクリックします。現在リアルタイム ビューである場合、時間セレクタは停止した時間だけでなく、ロードされている時間間隔も示します。また、[Stop] をクリックすると、クエリーが停止し、現在 Event Viewer にロードされているイベント セットが表示されます。
7	クリア（Clear）	イベントテーブルを空にするには、[クリア（Clear）] をクリックします。
8	[Event Enumerator] とメッセージ	ツールバーの右側に表示されている数値は、Event Viewer クライアントにロードされているイベント数です。この数はイベントがロードされるたびに増えていき、フィルタ条件と一致するイベントがすべて表示されるか、改ページ制限に達するか、どちらか少ない方で終了します。改ページ制限を変更した場合は（[Event Management] ページを参照）、Event Viewer を終了して再び開くことによって新規制限を有効にする必要があります。 クエリが拡張イベントストレージ領域からのイベントの取得を要求する場合は、「Data being fetched from extended store」などのメッセージが表示されます。拡張ストレージ領域からのイベントのフェッチは、通常、プライマリストレージ領域からイベントをフェッチするよりも時間がかかります。

イベント テーブルのカラム

次の表に、Event Viewer のビューに表示できるすべてのカラムをアルファベット順に一覧表示して説明します。イベント タイプによってイベント データが存在する場合と存在しない場合があるように、デバイスに適用できるカラムはデバイスによってさまざまです。

ビューを保存した場合は、選択したカラムとその順序が保持されて、次回ビューを開いたときに表示されます。開いている（またアクティブな）ビューに表示するカラムを選択するには、次のいずれかを実行します。

- （推奨の方法）。イベントテーブルのヘッダー行の右端の [列セレクタ（Column Chooser）] アイコンをクリックします（ [Event Monitoring] ウィンドウ （17 ページ）を参照）。[Choose Columns to Display] ダイアログボックスが開き、カラムがアルファベット順に一覧表示されます。列の選択または選択解除は、個別に、または [すべて選択（Select All）]/[すべて選択解除（Unselect All）] チェックボックスを使用して実行できます。また、[Revert] をクリックして、ビューのデフォルトのカラム選択に戻せます。
- [ビュー（View）] > [列のカスタマイズ（Customize Columns）] を選択します。
- 任意のカラムの見出しを右クリックし、カラムを個別に選択または選択解除します。または、[More] をクリックして、[View] > [Customize Columns] コマンドで使用したのと同じダイアログボックスを開きます。

（注） [Description]、[Event Name]、[Receive Time] 以外のほとんどのカラムに、フィルタリング機能があります。詳細については、 カラムベース フィルタの作成 （56 ページ）を参照してください。

表 *6 : Event Viewer* のカラムの説明

カラムのラベル	説明
AAA Group	AAA グループ ポリシー。
AAA Server	ユーザのアクセス要求を処理するサーバ。認証、許可、アカウンティングを実行します。
AAA ユーザ（AAA User）	AAA ユーザ名。
ACE Hash1 ACE Hash2	アクセス コントロール リスト エントリ（ACE）のハッシュコード 1 とハッシュコード 2。 syslog 106023 イベントおよび 106100 イベントからポリシー検索を正常に完了するには、ハッシュ コードが必要です。このようなハッシュ コードは、Security Manager を使用して設定を展開した場合にだけ使用できます。
ACL Name	アクセス コントロール リスト（ACL）の名前または ID。

カラムのラベル	説明
Action	フローに対して実行されるアクション。たとえば、終了や拒否。
アラート詳細（Alert Details）	アラートに関する詳細。
アプリ名	イベントを発生させているアプリケーションの名前。
App Stop Reason	アプリケーションがシャットダウンされた方法と理由に関する説明。
アプリケーションバージョン	イベントを発生させているアプリケーションのバージョン。
Attack Relevance Rating	攻撃とその対象となる宛先との関連性を示すために使用される数値。
Backplane Interface	バックプレーンインターフェイス。バックプレーンインターフェイスが物理インターフェイスと異なる場合にだけ識別されます。
Botnet Category	ドメイン名がブロックリストに掲載されている理由を示すカテゴリ。たとえば、ボットネット、トロイの木馬、スパイウェアなど。
Botnet Domain	動的なフィルタデータベースに登録されていて、トラフィックの宛先となったドメイン名または IP アドレス。ブロック リスト、許可リスト、またはグレーリストに追加できます。
Build Time	ソフトウェアが構築された日付と時刻。
Build Type	構築のタイプ。通常、これは「リリース」または「デバッグ」などの語句です。アプリケーションのビルダーの ID である場合もあります。
Byte Count	接続のデータ転送のバイト数。
Call Id	このパケットが属するセッションのピアのコール ID。
クラスマップ	クラスマップ名。
接続期間（Connection Duration）	接続のライフタイム。
Connection ID	接続の一意の識別子。
Connection Limit	接続またはセッションの最大数。
Connection Termination Value	接続終了の要因。バージョンが正しくない、ペイロードタイプが無効であるなど。

カラムのラベル	説明
Current Connection Count	現在の接続の数。
説明	syslog の場合は未処理メッセージが表示され、IPS の場合はイベントの説明が表示されます。
[接続先（Destination）]	トラフィック宛先（ASA および FWSM の場合）または攻撃目標（IPS の場合）の IP アドレスまたはホスト名。複数の値を取ることができ、IPv4 または IPv6 アドレスを含められます。 [View] > [Show Network Host Objects] が選択されて、宛先 IP アドレスと一致するホストオブジェクトが定義されている場合は、ホスト オブジェクト名が表示されます。 **ヒント** そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
Destination Context Data	アラートがトリガーされた直前および直後に送信されたデータを示すコンテキストバッファ。ターゲットから供給されたストリーム データを Base64 でエンコードした表現。
Destination FQDN	宛先 IP アドレスの完全修飾ドメイン名（ある場合）。
Destination Interface	宛先インターフェイス。 Etherchannel アラート（426001 ～ 426003）の場合は、このイベントが発生した Etherchannel インターフェイスの名前。[Source Interface] カラムにメンバ インターフェイスが識別されます。
Destination Locality	侵入で指定されたとおりに、ターゲットアドレスが特定のネットワークの内側に存在するか、外側に存在するか。
Destination OS	ターゲットのオペレーティングシステム情報。
Destination OS Relevance	宛先ターゲット OS 値の関連性を示す数値。
Destination OS Source	ターゲット OS データの情報元。使用できる値は learned、imported、または configured です。
Destination Service	宛先ポート。複数の値になることがあります。
Destination User Identity	トラフィック宛先のユーザ名（存在する場合）。
デバイス	イベントの送信元。通常はデバイス ID です。 Not Available と識別されたデバイスは、Security Manager インベントリから削除されています。

カラムのラベル	説明
Device Identifier	ASA デバイスのクラスタの場合、イベントのソースノードの ID です。これは、[Server Setup] ページの [Syslogデバイス IDを有効にする（Enable Syslog Device ID）] 設定に基づいています。 [デバイスID（Device Identifier）] を使用して、生成された syslog をフェールオーバーデバイスでフィルタリングできます。フェールオーバーが発生した場合、syslog メッセージを生成したフェールオーバーデバイスの IP アドレスがここに表示されます。ただし、Cisco Security Manager で管理されているフェールオーバーデバイスによって生成された syslog メッセージの場合、[デバイスID（Device Identifier）] 列は空白になります。 （注） [ツール（Tools）] > [Cisco Security Manager管理（Cisco Security Manager Administration）] の [イベント管理（Event Management）] ページで、[フェールオーバースタンバイデバイスからのsyslogを処理（Process Syslogs from Failover Standby Device）] チェックボックスをオンにします。 クラスタは、複数のノードを持つ単一のデバイスとして Security Manager によって管理されます。したがって、すべてのノードのイベントはクラスタ仮想 IP にマップされ、Event Viewer にクラスタ仮想 IP と共に表示されます。[デバイスID（Device Identifier）] を使用して、ノードの特定のクラスタメンバーにより生成された syslog をフィルタリングできます。
方向	トラフィックの方向。inbound または outbound です。
イベント ID（Event ID）	内部で各イベントに割り当てられる一意の連続番号。
Event Name	イベントに付けられたユーザにわかりやすい名前。
Event Summary	サマリーアラートであり、特性が共通する 1 つ以上のアラートを表したものです。数値は、「initialAlert」属性値との一致により、最後のサマリーアラート以降にシグニチャが発行された回数を示します。
イベント タイプ ID	ASA または FWSM の場合は Syslog ID です。 IPS の場合は次のいずれかになります。 • [Sig ID] と [Sub-Sig ID] の組み合わせ（IPS アラート イベントの場合） • IPS ステータス（IPS ステータス イベントの場合） • IPS エラー（IPS エラー イベントの場合）

カラムのラベル	説明
Execution State	アプリケーションの実行ステータス。
Final Alert	サマリーアラートに適用され、特性が共通する1つ以上のアラートを表したものです。このアラートが、 initialAlert 属性に同じ値を含む最後のイベントアラートであるかどうかを示します。
Generation Time	デバイスのローカルイベント生成時刻を表します（IPS イベントでのみ使用可能）。
Global Correlation Audit Mode	アラートが監査モード処理で処理されたかどうか（true または false）。
Global Correlation Deny Attacker	リスク レーティングを算出した結果、内部オーバーライドを超えたために、攻撃者拒否アクションが発生した（または発生することになっていた）のかどうかを示す true または false。
Global Correlation Deny Packet	リスク レーティングを算出した結果、内部オーバーライドを超えたために、パケット拒否アクションが発生した（または発生することになっていた）のかどうかを示す true または false。
Global Correlation Modified Risk Rating	リスク レーティングのためにレピュテーション リスク デルタを追加して、リスク レーティングを調整したかどうかを示す true または false。
グローバル相関その他のオーバーライド（Global Correlation Other Overrides）	リスク レーティングを算出した結果、オーバーライドしきい値を超えたために、他に防御アクションが講じられたかどうかを示す true または false。
Global Correlation Risk Delta	レピュテーション スコアにより、リスク レーティングをどのくらい増やしたかを示す 0 ～ 99 の値。監査モードがイネーブルになっている場合は、監査モードがイネーブルでないと、リスク レーティングをどのくらい調整することになったかを示します。
ヒット カウント（Hit Count）	設定された時間間隔で ACL エントリによってフローが許可または拒否された回数。ASA または FWSM が特定のフローに対して最初の syslog メッセージを生成すると、値が 1 となります。 （注） 画面間を移動した後に ACL ポリシーページに移動すると、すべての ACL ルールについて、[HitCount] および [LastHitTime] の値にそれぞれ [0] および [なし（Never）] が表示されます。実際の [HitCount] および [LastHitTime] の値を取得するには、ACL ポリシーページの [ヒットカウントの更新（Refresh Hit Count）] ボタンをクリックします。値はデータベースから取得され、すべての ACL ルールに表示されます。

カラムのラベル	説明
Hit Count Info	ACL ヒットカウント情報（例：First hit）。
ホスト ID（Host ID）	イベントを発生させたホストのグローバルに一意な識別子。
ICMP コード（ICMP Code）	ICMP タイプのコード。たとえば、ICMP タイプ 3 およびコード 0 はネット到達不能であり、コード 1 はホスト到達不能です。
ICMP Type	ICMP メッセージのタイプ。たとえば、宛先到達不能の場合は3、エコーの場合は 8 です。
初期アラート（Initial Alert）	このフィールドはサマリーアラートに適用され、特性が共通する 1 つ以上のアラートを表したものです。値 initialAlertは、特性（sigid/subsigid）が同じでサマリー アラートではない最後の evIdsAlert のイベント ID です。
Ip Log ID	iplog ドキュメントを（ホスト範囲とともに）一意に識別する IP ログ識別子。
IpLog Address	IP ログに関連付けられた IPv4 または IPv6 アドレス。
IpLog Alert Reference	ログの開始をトリガーした evAlert イベントのグローバル イベント ID。
IpLog Begin Time	ログ ドキュメントに現在使用できる時間範囲の開始。
IpLog Bytes Captured	キャプチャされた総バイト数。キャプチャされたパケットの中には、メモリ制限のためにログからすでに削除されているものもあることに注意してください。
IpLog Bytes Remaining	ログが終了するまでの残りバイト数。
IpLog End Time	ログ ドキュメントに現在使用できる時間範囲の終了。
IpLog残り時間（分）（IpLog Minutes Remaining）	ログが終了するまでの残り分数。
IpLogキャプチャされたパケット（IpLog Packets Captured）	キャプチャおよび記録されたパケットの総数。
IpLog Packets Remaining	ログが終了するまでの残りパケット数。
IpLog Status	ログ ステータスを表す文字列。
IPS Category	SEE イベント カテゴリ。
IPS User	操作を開始しているユーザのユーザ名。

カラムのラベル	説明
License Limit	ライセンスの最大数。
List Name	ドメイン名が記載されているリスト、管理者許可リスト、ブロックリスト、または IronPort リスト。
ログイン アクション（Login Action）	発生したログインアクション：loggedIn、loggedOut、または loginFailed。
Malicious Host	悪意のあるホストのホスト名。
Malicious IP	悪意のあるデバイスの IP アドレス。
Max Connection	NAT 接続の最大数。
MaxEmbryonic Connection	初期接続の最大数。
NAT Destination	変換された（NAT されたとも呼ばれる）宛先 IP アドレス。 変換された宛先のホスト名。
NAT Destination Service	変換された（または NAT された）宛先ポート。
NAT Global IP	グローバルアドレス。IPv4 または IPv6 アドレスを含められます。
NAT Source	変換された（または NAT された）送信元 IP アドレス。IPv4 または IPv6 アドレスを含められます。 変換された送信元のホスト名。
NAT Source Service	変換された（または NAT された）送信元ポート。
NAT Type	ネットワークアドレス変換のタイプ（例：[スタティック（Static）] または [ダイナミック（Dynamic）]）。
New Time	デバイス クロックが変更された時刻。
New Version	アップグレードインストール後のシステム ソフトウェア バージョン。
番号	現在表示されているイベント（行）の数これは単純な連番であり、イベントの内容とは関係ありません。イベントのタイプの情報については、[Event ID] および [Event Name] フィールドを参照してください。
Old Time	変更前のデバイス クロック時間。
Old Version	アップグレードアンインストール前のシステム ソフトウェア バージョン。
Operation Successful	操作が正常に実行されたかどうかを示します。

カラムのラベル	説明
Package File	自動的にダウンロードされてインストールされるパッケージファイルの名前。
Physical Interface	物理インターフェイス。物理インターフェイスが [Interface] カラムの対応する値と異なる場合にだけ識別されます。
ポリシー マップ	ポリシー マップ名。
Protocol	Level-3 プロトコルまたは Level-4 プロトコル。
プロトコルバージョン	プロトコル バージョン。
Protocol (Non L3)	イベントに示された Level-3 または Level-4 以外のプロトコル。たとえば、TACACS、RADIUS、FTP、または H245。
理由	特定のイベントに関連付けられた理由。たとえば、接続のティアダウンが関連付けの理由の場合があります。
Receive Time	イベントが Security Manager によって受信された時刻。
レピュテーション	-10.0 ～ +10.0 で示される攻撃者のレピュテーションスコア。スコアが低い（負の値が大きい）ほど、ホストが悪意のあるホストである可能性が高くなります。
Result Status	操作が正常に完了したかどうかを示す操作のステータス。
Risk Rating	イベントに関連付けられたリスクを計算した値。
[グループでのロール（Role in Group）]	ASA ロードバランシンググループのこのメンバーのロール（[グループ（Group）]、[制御（Control）]、または [データ（Data）]）。
セキュリティコンテキスト	対応する [Interface] カラムに指定された名前付きインターフェイスが関連付けられているセキュリティ コンテキスト。
Sensor Event ID	イベントのシリアル番号。発信元ホストのスコープ内で一意であることが保証されています。
重大度	ファイアウォールまたは IPS の重大度値。
SIA Event Name	[SIA Service Name] フィールドで識別されたサービスに対して発生したイベント。
SIA Service Name	このイベントが発生した Service Insertion Architecture（SIA）サービスの名前。
Sig Details	レポートされたシグニチャの詳細。トリガーされて、アラートの生成を引き起こしたシグニチャです。

カラムのラベル	説明
Sig ID	Sig ID 値は、アラート発信者がアクティビティを特定するために使用されます。この値により、アクティビティにあらかじめ定義されているシグニチャを識別できます。
Signature Version	アラートの生成に使用されたシグニチャ定義のバージョン。
ソース	トラフィック送信元（ASA および FWSM の場合）または攻撃者（IPS の場合）の IP アドレスまたはホスト名。複数の値を取ることができ、IPv4 または IPv6 アドレスを含められます。 [View] > [Show Network Host Objects] が選択されて、送信元 IP アドレスと一致するホスト オブジェクトが定義されている場合は、ホスト オブジェクト名が表示されます。 **ヒント** そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
Source Context Data	アラートがトリガーされた直前および直後に送信されたデータを示すコンテキスト バッファ。攻撃者から供給されたストリーム データを Base64 でエンコードした表現。
Source FQDN	送信元 IP アドレスの完全修飾ドメイン名（ある場合）。
送信元インターフェイス（Source Interface）	送信元インターフェイス。 Etherchannel アラート（426001 ～ 426003）の場合は、このイベントが発生した Etherchannel バンドルの一部であるインターフェイスの名前。[Destination Interface] カラムに Etherchannel インターフェイスが識別されます。
Source Locality	攻撃者のアドレスが、侵入検知デバイスの設定で指定された特定のネットワークの内側に存在するか、外側に存在するかを識別します。
送信元サービス（Source Service）	送信元ポート。
Source User Identity	トラフィック送信元に関連付けられているユーザ名（ある場合）。
SSO サーバー	シングル サインオン（SSO）サーバ名。
SSO Server Type	シングル サインオン（SSO）サーバ タイプ。たとえば、SiteMinder。
Sub SigId	サブシグニチャ ID 値。シグニチャ ID（sigId）とともに、アラート発信者がアクティビティを特定するために使用されます。

カラムのラベル	説明
Summary Type	サマリーアラートのすべてのアラートに共通する特性を定義します。
Target Value Rating	アラートで特定したターゲットに関連付けられているアセット値。
脅威レベル	脅威度が関連付けられている場合に、次の値のいずれかが表示されます。none、very-low、low、moderate、high、または very-high。
Threat Rating	イベントの脅威レーティング（ある場合）。
タイム ゾーン	発信元ホストがある場所の現地タイムゾーン。
Translated Call ID	このパケットが属するセッションのピアの変換済みコール ID。
Trigger Packet	アラートをトリガーした単一の完全なパケット（base64 バイナリ形式）。
Truncated	イベントに含まれるトリガーパケットが切り捨てられているかどうか。
トンネル タイプ	VPN トンネル タイプ。
タイプ（Type）	AAA タイプ。authentication、authorization、accounting など。
Upgrade Name	アンインストールされたアップグレード パッケージの名前。
URI	自動アップグレード サーバ ディレクトリの URI。
UTC Offset	センサー現地時間の offset 属性は、発信元ホストがある現地時間に変換するために UTC 時間に追加する必要がある分数を示します。
仮想センサー	イベントに関連付けられた仮想センサーの名前。
VLAN Id	アラートをトリガーしたアクティビティにかかわるパケットに関連付けられた VLAN 番号。
[VPNグループ（VPN Group）]	VPN グループ ポリシー。
VPN IPSec SPI	IPSec セキュリティ パラメータ インデックス。
VPN User	VPN ユーザ名。
Watchlist Delta	アラートに関連付けられたアクティビティの送信元がウォッチリストに記載されているために、リスク レーティングに付加された値。

時間スライダ

時間スライダは、履歴ビューの使用中にイベント テーブルの下にあります。リアルタイム ビューでは使用されません。次の図に、時間スライダを示します。右側の改ページコントロールについては、図 4 : 時間スライダの要素 （32 ページ） で説明します。

図 4: 時間スライダの要素

時間スライダは、次の操作を実行する場合に使用できます。

- サーバでの Events Per Second（EPS）傾向を表示します。必要なタイム フレームの期間の EPS 傾向がより良く表示されるように、右側のコントロールを使用してズームインまたはズームアウトできます。

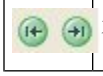
ウィンドウ内に時間範囲を配置するために、時間スライダの背景をクリックしてドラッグすることもできます。背景を動かしても選択した時間範囲に影響はありません。

- イベントテーブル内に表示するイベントの時間のスライスを選択します。選択には、垂直スライダを動かすか、改ページコントロールを使用します。垂直スライダの位置は、イベントテーブルに表示される最新のイベントを決定します。時間のスライスを変更するたびに、その期間に一致するイベントがイベント テーブルにリロードされます。

イベント テーブルに表示されるイベントの時間範囲は、選択した時間間隔によって決まります。詳細については、イベントの時間範囲の選択 （54 ページ）を参照してください。

次の表に、時間スライダの右側の改ページコントロールについて説明します。

表 7: 時間スライダのページ送りボタン

要素	説明
	前のページ（前方）および次のページ（後方）。ページのサイズは、選択した時間モードによって異なります。 （注） たとえば、前方から後方というようにページ コントロールを交互に使用すると、イベント テーブルでのソート順序が逆になります。つまり、最新のイベントが、テーブルの上から下、または下から上の順に並びます。
	先頭ページ（最前方）および最終ページ（最後方）。

要素	説明
	ズームイン（表示される合計時間間隔が短くなります）およびズームアウト（表示される時間間隔が長くなります）。 ズームしても、イベントテーブルの内容は変更されません。青色の影付きの領域は、イベント テーブルに現在表示されている時間間隔を示します。

[Event Details] ペイン

[Event Details] ペイン（ [Event Monitoring] ウィンドウ （17 ページ）に示す）には、単一のイベント内に含まれる情報が表示されます。この情報はペイン内の複数のタブに表示され、その内容はデータを解析する Event Viewer のイベントおよび機能の豊富さによって異なります。コンポーネントには、次のものがあります。

- [表示されるフィールド（Displayed Fields）] タブ：イベントテーブルに表示されるフィールドを表示します。
- [詳細（Details）] タブ：選択したイベントに使用できるすべてのフィールドを表示します。フィールドは、アルファベット順になっています。
- [説明（Explanation）] タブ：このイベントタイプの概要を表示します。
- [関連する脅威（Related Threats）] タブ：イベントと相関関係にある脅威を表示します（IPS イベントのみ）。
- [推奨アクション（Recommended Action）] タブ：このタイプのイベントに対する推奨事項を表示します（Syslogs のみ）。
- [トリガーパケット（Trigger Packet）] タブ：トリガーパケットデータを表示します（IPS イベントのみ）。
- [コンテキストパケット（Context Packet）] タブ：送信元（攻撃者）および宛先（ターゲット）のコンテキストパケットデータを表示します（IPS イベントのみ）。
- [メモ（Notes）]：メモを追加して、後で特定のシグネチャに戻って、自分や他のユーザーがシグネチャやイベントに追加した内容を確認できるようにします。詳細については、[Signatures] ページを参照してください。

（注） ここで追加したメモは、Configuration Manager をクロス起動したときにも保持されます。

（注） 特定のシグネチャに対するイベントが複数ある場合、1 つのイベントに注釈を付けると、そのシグネチャに関連するすべてのイベントに注釈が付けられます。

イベント管理の準備

デバイスから生成されたイベントを表示する場合は、事前にそのデバイスを Event Viewer で機能するように設定する必要があります。

時間の同期

標準のネットワーク管理では、時差およびネットワークデバイス同期が考慮されます。そのために通常、ネットワーク タイム プロトコル（NTP）サーバが使用されます。Event Viewer は、時間基準を統一すると最も使いやすくなります。ただし、Security Manager がイベントを受け取った時刻（[Receive Time]）を表示できるほか、IPS デバイスの場合にはデバイスがイベントを生成した時刻（[Generation Time]）を表示できます。

可能な場合は常に、同じ NTP サーバでモニタリングしている Security Manager サーバおよびデバイスを設定します。

クライアントが開かれたときの Security Manager サーバーのクロックと Security Manager クライアントのクロックの違いは、イベントデータをサーバー時間からクライアント時間に変換/マッピングするときに考慮されます。たとえば、Security Manager サーバーの時間が進んで時差が動的に変化する場合、サーバーから取得されたデータには更新されたタイムスタンプが表示されますが、クライアントが開かれたときに、クライアントは引き続き、サーバーの時間とクライアントの時間に基づいて時差をマッピングします。このような状況では、サーバーでの時間の変化に対応する短い時間だけ、イベントビューアにデータが表示されません。このため、Security Manager サーバーのクロックの変更は、頻度を減らし、影響が最も少ない時間に行うことをお勧めします。

イベント管理のための ASA と FWSM デバイスの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

イベントビューアまたは syslog イベントを分析する他のアプリケーションを使用して ASA（ASA-SM を含む）または FWSM デバイスから生成されたイベントを表示する場合は、事前に syslog メッセージを生成および送信するようにそのデバイスでロギングポリシーを設定する必要があります。

（注） 仮想 IP アドレスを持つクラスタデバイス（Security Manager バージョン 4.4 以降）が Security Manager と仮想デバイスの両方で設定されている場合、そのデバイスを追加できます。

ヒント　デバイスごとに適切なロギング設定を指定できますが、ネットワーク内の複数の ASA または FWSM デバイスで同じロギング設定を使用することになる場合もあります。この項では個々のデバイスを設定する方法について説明しますが、共有ポリシーを作成して複数のデバイスに割り当てることもできます。共有ポリシーの設定と割り当ての詳細については、新しい共有ポリシーの作成およびポリシー ビューにおけるポリシー割り当ての変更を参照してください。

ここで説明するロギング設定のほか、ファイアウォール ポリシーまたは ACL ポリシー オブジェクトにアクセス コントロール エントリを設定した場合にはそのエントリごとにロギングを設定することもできます。デフォルトでは拒否されたアクセスだけがログに記録されますが、ログに記録する情報が増えるように ACL ロギング オプションを設定できます。

（注）　マルチ コンテキスト モードでコンテキストからイベントを確実にレポートするには、Cisco Event Viewer は各コンテキストの管理インターフェイスの IP アドレスを必要とします。

ステップ 1　（デバイスビュー）ASA もしくは FWSM デバイスまたはセキュリティコンテキストを選択してから、ポリシーセレクタで [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。

ポリシーで、[ロギングの有効化（Enable Logging）] を選択します。必要に応じて他のオプションを設定できます。オプションの詳細については、[Logging Setup] ページを参照してください。

ステップ 2　[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。

Security Manager サーバーの IP アドレスを syslog サーバーテーブルに追加します。UDP プロトコルを使用するようにサーバを設定します。Security Manager Administration の[Event Management] ページで別のポートを設定しないかぎり、デフォルト ポート 514 が適切なポートです。

CS-MARS など他のイベント管理アプリケーションを使用している場合には、そのサーバもこのポリシーに追加します。

（注）　必要に応じてEMBLEMメッセージフォーマットを使用できます。従来のフォーマットもEMBLEMフォーマットもサポートされています。CS-MARS では EMBLEM がサポートされないため、CS-MARS サーバには EMBLEM フォーマットのメッセージを送信しないでください。

syslog サーバ ポリシーのオプションの詳細については、[Syslog Servers] ページを参照してください。

ステップ 3　タイムスタンプを syslog メッセージに追加する、メッセージの重大度を変更する、特定のメッセージの生成を抑止するなど、デフォルト以外の syslog サーバー設定を行う場合は、[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [サーバーのセットアップ（Server Setup）] ポリシーを設定します。詳細については、[Server Setup] ページを参照してください。

ステップ 4 （任意）[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）] ポリシーでは、syslog サーバーに送信されるメッセージの種類を微調整できます。このポリシーの詳細については、[Logging Filters] ページおよび[Edit Logging Filters] ダイアログボックスを参照してください。

次に、このポリシーを設定するためのヒントを示します。

- ロギングフィルタを追加するときには、[ロギング先（Logging Destination）] に [Syslogサーバー（Syslog Servers）] を選択します。
- メッセージ重大度に基づいて簡単なフィルタを作成したり、イベント クラスに基づいてはるかに複雑なフィルタを設定したりできます。イベントクラスを使用する場合は、[ロギングフィルタ（Logging Filters）] ポリシーで直接設定を行うことも、[イベントリスト（Event Lists）] ポリシーで個別にイベントリストを設定することもできます（[Event Lists] ページを参照）。

ステップ 5 （任意）メッセージの重大度またはメッセージ番号で時間間隔あたりに生成されるメッセージの数量を制限するように、[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）] ポリシーを設定できます。これにより、syslog サーバのフラッディングを回避するのが容易になります。[Rate Limit] ページを参照してください。

ステップ 6 （任意、ただし推奨）ASA デバイスのネットワーク タイム プロトコル サーバーを指定するように、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP] ポリシーを設定できます。NTP を使用すると、日付と時刻情報の一貫性を確保して容易にイベントを相関付けることができます。Security Manager サーバに使用するのと同じ NTP サーバを指定します。異なるサーバを使用する場合は、それらのサーバが同期されていることを確認してください。[NTP] ページを参照してください。

イベント管理のための IPS デバイスの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IPS デバイスから生成されたイベントを Event Viewer を使用して表示する場合は、事前に Security Manager サーバがそのデバイスにアクセスできるようにそのデバイスで [Allowed Hosts] ポリシーを設定する必要があります。[Allowed Hosts] ポリシーでは設定へのアクセスも許可するように Security Manager を設定する必要があるため、IPS デバイスがすでに正しく設定されている可能性があります。また、ネットワーク タイム プロトコル（NTP）も設定する必要があります。

IPS デバイスで効率よくイベントを管理できるように、デバイス ビューで IPS デバイスに対して次のポリシーを設定します。

- [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）] > [許可されたホスト（Allowed Hosts）] : （必須）Security Manager サーバーをテーブルに追加します。Security Manager サーバをそのホスト IP アドレス（たとえ

ば、10.100.10.10）で特定するか、または Security Manager サーバが存在するネットワーク（たとえば、10.100.10.0/24）を指定できます。

デバイスで CS-MARS など他のイベント管理アプリケーションを使用している場合は、そのサーバもポリシーに必ず追加します。

Allowed Hosts ポリシーの設定の詳細については、許可ホストの識別を参照してください。

- [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]：（推奨）日付と時刻情報の一貫性を確保して容易にイベントを相関付けることができるように、Security Manager サーバーに使用するのと同じ NTP サーバーを設定します。異なるサーバを使用する場合は、それらのサーバが同期されていることを確認してください。詳細については、NTP サーバの識別を参照してください。

ヒント　デバイスごとに適切な許可ホストおよび NTP 設定を指定できますが、ネットワーク内の複数の IPS デバイスで同じ設定を使用することになる場合もあります。この項では個々のデバイスを設定する方法について説明しますが、ポリシーの共有バージョンを作成して複数のデバイスに割り当てることもできます。共有ポリシーの設定と割り当ての詳細については、新しい共有ポリシーの作成およびポリシー ビューにおけるポリシー割り当ての変更を参照してください。

Event Manager サービスの管理

Event Manager サービスにより、Event Viewer アプリケーションを使用できるようになります。Event Viewer を機能させるには、このサービスを開始する必要があります。サービスの機能全体を設定および管理するために実行できるタスクがいくつかあります。

ここでは、次の内容について説明します。

Event Manager サービスの開始、停止、および設定

Event Viewer または Report Manager を使用するには、Event Manager サービスが動作中である必要があります。

Security Manager をインストールすると、『Installation Guide for Cisco Security Manager』に記載のとおり、サーバーが最小メモリ要件を満たさない場合を除き、Event Manager サービスは自

動的にイネーブルになります。最小メモリ要件を満たさないシステム上でもサービスを手動で開始できますが、満足できるパフォーマンスが得られない場合があります。主な要因は、管理対象のデバイスの数と各デバイスのイベント生成速度です。

ヒント　[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）] ページで [イベント管理の有効化（Enable Event Management）] オプションが選択されているにもかかわらず、[起動（Launch）] > [イベントビューア（Event Viewer）] を選択したときにイベントビューアが使用不可能であるというメッセージが表示される場合は、イベントビューアサービスを再起動してみてください。まず、[Enable] オプションの選択を解除し、[Save] をクリックします。サービスが停止するまで待ちます。次に、[Enable] オプションを選択し、[Save] をクリックし、サービスが再び開始されるまで待機します。その後、Event Viewer を再度開いてみます。

次の手順では、Event Manager サービスを開始、停止、および設定する方法について説明します。

関連項目

- イベント データ ストア用のディスク スペースの使用率のモニタリング （44 ページ）

ステップ 1　（イベントビューアではなく）メインの [Security Manager] ウィンドウで、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択します。

ステップ 2　次のいずれかを実行します。

- Event Manager サービスをイネーブルまたは開始するには、[イベント管理の有効化（Enable Event Management）] を選択します。
- Event Manager サービスをディセーブルまたは停止するには、[イベント管理の有効化（Enable Event Management）] の選択を解除します。

イベント データ ストアの場所と最大サイズ、デバイスがイベントを送信する必要のある syslog ポート、改ページサイズ（これにより、イベントテーブルにロードされるイベントの最大数が決まります）など、他の設定も変更できます。拡張イベント ストレージの場所を設定して、プライマリ保管場所を拡張することもできます。これらの設定の詳細については、[Event Management] ページを参照してください。

（注）　バージョン 4.5 以降、Security Manager では、syslog を 1 つのローカルコレクタと 2 つのリモートコレクタに転送できます。詳細については、[Event Management] ページを参照してください。

ステップ 3　[保存（Save）] をクリックして変更を保存します。

[Enable Event Management] オプションを変更した場合、Event Manager サービスを起動または停止してもよいかどうかの確認が求められます。[はい（Yes）] をクリックするとサービスがすぐに開始または停止し、進捗インジケータが表示され、変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。

改ページサイズを除く他の設定を変更する場合は、Event Manager サービスをいったん停止してから再起動する必要があります。進捗インジケータが表示されます。

Event Manager サービスのモニタリング

Event Manager サービスは、着信 syslog メッセージを処理し、モニタ対象の IPS デバイスから SDEE アラートを取得します。処理されるデータ量は、ネットワーク アクティビティによって異なります。ネットワーク内で生成される Events Per Second（EPS）がサービスによって処理できるよりも大きい時間がある可能性があります。この場合、サービスはスロットルモードに移行してイベントを選択的にドロップします。

サービスのステータスをモニタして輻輳を特定し、発生する問題に対処できます。サービスのステータスは、Event Viewer の概要 （9 ページ）に示すように、Event Viewer のステータスバーの右下隅のアイコンに表示されます。[Total EPS] は、サービスに発生している現在の Events Per Second のレートを示します。アラート ステータス アイコンの色は次を示します。

- 緑色の点：問題はありません。すべてのイベントが正常に処理されています。
- 黄色の点：警告がいくつかあります。たとえば、重大度レベルが低いイベントがドロップされた場合。
- オレンジ色の点：より深刻な問題があります。たとえば、重大度レベルが低いおよび中程度のイベントがドロップされた場合。
- 赤い色の点：クリティカルな状況です。たとえば、重大度レベルが高いイベントがドロップされた、または syslog ポートもしくはイベント データ ストアの場所に問題があるなど、システムに重大な問題がある場合。
- ネットワーク ワイヤの切断：Event Manager サービスが意図的にまたはサーバ問題によってディセーブルになっています。イベントは保存または取得されません。これが意図的ではない場合は、Event Manager サービスの開始、停止、および設定 （37 ページ）で説明するとおりに、Event Manager サービスを再起動します。

詳細情報を表示するには、アラート ステータス アイコンをクリックします。バブルが開いて、過去 5 分の概要統計情報が表示されます。統計情報には、受信およびドロップしたイベント数や、ある場合はイベント サーバ アラート メッセージが含まれます。アラート ステータス アイコンをもう一度クリックしてバブルを閉じます。

バブルが開いているときに、バブル内の [詳細（Details）] リンクをクリックしてより詳細な情報を表示できます。[Details] リンクをクリックすると、[Event Statistics Details] ダイアログボックスが開いて、次の情報が表示されます。

- **[Last 5 Minutes Statistics]**：
  - [受信済みイベント数（Events Received）]：サービスが過去 5 分間に受信した syslog イベントおよび取得した SDEE アラートの総数。

- [ドロップ済みイベント数（Events Dropped）]：輻輳が原因でサービスでドロップする必要があったイベントまたはアラートの総数。この数は、モニタ対象のデバイスからのドロップだけを示します。このため、通常の状況では、この数は0である必要があります。0以外の数の場合は、サービスがスロットルモードであることを示すため、[Event Server Alerts] セクションのメッセージを確認します。
- [監視対象外デバイスからのイベント数（Events from Unmonitored Devices）]：監視対象として選択されていないデバイスからサーバーに送信されたsyslogメッセージ数（モニタするデバイスの選択　（42 ページ）を参照）。

モニタ対象外のデバイスからのイベントは常にドロップされますが、サービスに負荷をかけます。最後に検出されたモニタ対象外のデバイスのIPアドレスが表示されます。このIPアドレスを使用してメッセージの送信元を判別します。その後、そのデバイスを監視対象デバイスのリストに追加する必要があるか、またはCisco Security Managerサーバーをsyslogサーバーリストから削除するようにデバイスの設定を変更する必要があるか判断できます。

メッセージを送信しているデバイスがネットワーク外にある場合は、このsyslogトラフィックがネットワーク内に入ってくることを防ぐようにファイアウォール設定を調整します。

- **[Status Information]**：
  - [秒単位の合計イベント数（EPS）（Total Events Per Second (EPS)）]：イベントを現在処理しているレート。この測定には、ドロップされたイベントは含まれません。
  - [使用されているイベントバッファ（Event Buffer Used）]：イベントの処理に現在使用されている共有イベントバッファのパーセンテージ。バーは、スロットルレベルを示すために次のとおり色分けされます。

緑色：スロットル モードではありません。

黄色：重大度が低いイベントがドロップされました。

オレンジ色：重大度が低いおよび中程度のイベントがドロップされました。

赤色：重大度が高いイベントがドロップされました。

- [イベントサーバーのアラート（Event Server Alerts）]：これらのメッセージには、対処する必要がある特定のステータス問題が表示されます。表示される可能性のあるメッセージと有効なソリューションについては、表 8 : Event Manager ステータス メッセージ　（41 ページ）を参照してください。
- [コピー（Copy）]ボタン：情報をクリップボードにコピーするには、[コピー（Copy）]ボタンをクリックします。コピーした情報にはHTMLマークアップが含まれます。情報は、HTML ファイルに貼り付けできます。

表 *8 : Event Manager* ステータス メッセージ

アラート メッセージ	アラート レベル	有効なアクション
UDP port <514> could not be acquired, therefore syslog events cannot be collected.	高い	示されたポートを外部アプリケーションがすでに使用している可能性があります（デフォルト syslog ポートは 514）。その外部アプリケーションを停止する必要がある場合があります。**netstat -ao | findstr 514** などの netstat コマンドを使用して、プロセスの PID を識別できます。
The event data store location does not exist, therefore events cannot be stored.	高い	Security Manager の管理設定で設定されたイベント データ ストアの場所が存在しないか、その場所に対して必要な読み取り/書き込み権限が Security Manager サーバにありません。場所の設定の詳細については、[Event Management] ページを参照してください。
Low severity events are being dropped.	低い	イベントが非常に高いレートで受信されたか、システムに高い負荷がかかっているかのいずれかです。 デバイスが過度にイベントを頻繁に送信しているかどうかを特定するには、[All Device Events] ビューを開いてリアルタイム ビューと履歴ビュー間の切り替え （52 ページ） で説明するとおりに、リアルタイム モードに切り替えます。 サーバに高い負荷がかかっているかどうかを特定するには、サーバで Windows にログインして Task Manager または他のツールを使用して Security Manager 以外にシステムに高い負荷をかけているアプリケーションがあるかどうかを確認します。可能であれば、そのアプリケーションをディセーブルにするか停止します。問題が頻繁に発生する場合は、サーバから他のアプリケーションをアンインストールすることを検討します。
Low and medium severity events are being dropped.	中規模	
All events are being dropped.	高い	

アラート メッセージ	アラート レベル	有効なアクション
Events from unknown devices are being received.	低い	モニタするデバイスの選択 （42 ページ）で説明するとおりに、モニタ対象に選択されていないデバイスから syslog イベントが Security Manager サーバに送信されました。これらのデバイスは、モニタリングでサポートされていないデバイス タイプの可能性があり、また Security Manager インベントリにも入っていない可能性があります。 メッセージは、これらのデバイスに対する EPS レートによって異なります。重大度が低いメッセージの場合は、EPS レートが 500 ～ 5,000 であることを示します。中程度の場合は、EPS レートが 5,000 ～ 10,000 であることを示します。高い場合は、EPS レートが 10,000 を超えることを示します。 [最後の5分間の統計（Last 5 Minutes Statistics）] の [監視対象外デバイスからのイベント数（Events from Unmonitored Devices）] 統計情報には、これらのイベントの数および最後のサポート対象外デバイスの IP アドレスが表示されます。モニタ対象にデバイスを選択するか、Security Manager サーバのアドレスを削除するように、デバイスの syslog ポリシーを変更します。複数のモニタ対象外のデバイスがメッセージを送信している場合は、手順を繰り返す必要があります。
Events from unknown devices are being received at a high rate.	中規模	
Events from unknown devices are being received at a very high rate.	高い	

モニタするデバイスの選択

Security Manager データベースに追加されたすべての ASA および FWSM デバイスならびにセキュリティ コンテキスト、ならびに IPS デバイスおよび仮想センサーは、Event Viewer で自動的にモニタ対象に選択されます。

（注） マルチ コンテキスト モードでコンテキストからイベントを確実にレポートするには、Cisco Event Viewer は各コンテキストの管理インターフェイスの IP アドレスを必要とします。

バージョン 4.17 以降、Cisco Security Manager は非管理インターフェイスからもイベントを受け取りますが、次の制限があります。

- 静的 IP アドレスインターフェイスのみがサポートされています。

- Syslog のクラスタープール IP 範囲が使用されるため、クラスターデバイスからのイベントは表示されません。
- Syslog サーバー設定の展開後にのみ、非管理インターフェイス IP を取得するようデバイス イベント マネージャに通知されます。したがって、最初のイベントドロップが発生する可能性があります。
- この拡張機能は、syslog リレーサービスではサポートされていません。

デバイスで Event Viewer を使用しない場合は、そのデバイスをモニタ対象から除外できます。Security Manager サーバを syslog サーバとして使用するように ASA もしくは FWSM デバイスまたはセキュリティ コンテキストを設定していない場合は、デバイスまたはセキュリティ コンテキストからイベントを受信することはいずれにせよないことに注意してください。このため、モニタしない ASA または FWSM の選択を解除する必要はありません。

ヒント　Event Viewer では Cisco IOS IPS デバイスをモニタできません。

関連項目

- デバイス インベントリへのデバイスの追加
- イベント管理のための ASA と FWSM デバイスの設定　（34 ページ）
- イベント管理のための IPS デバイスの設定　（36 ページ）

ステップ 1　イベントビューアで、**[表示（View）] > [監視対象デバイスの管理（Manage Monitored Device）]** を選択して、[監視対象デバイスの管理（Manage Monitored Devices）] ダイアログボックスを開きます。

デバイス リストには、Security Manager インベントリ内のデバイスのうち、表示権限があるすべてのデバイスが表示されます。権限がないデバイスは表示されません。選択できる対象が、表示されたデバイスにかぎられます。いずれのデバイスに対しても選択または選択解除する権限がない場合は、リストは読み取り専用となりデバイスをモニタ対象に選択できません。アクセス権限の詳細については、Event Viewer のアクセス コントロールについて　（5 ページ）を参照してください。

ステップ 2　Event Viewer でイベントをモニタするデバイスだけが選択されていることを確認します。モニタしないデバイスの選択を解除します。

デバイス グループに属するすべてのデバイスの選択ステータスを変更する場合は、そのグループを選択または選択解除します。

ステップ 3　[OK] をクリック

Event Viewer で変更が有効になるまで待機することが必要になる場合があります。

イベント データ ストア用のディスク スペースの使用率のモニタリング

Event Manager サービスは、指定された量のディスク スペースをプライマリおよび拡張イベント データ ストアに使用します。これにより、サービスが原因でサーバ コンピュータまたは拡張保管場所が過負荷になることが確実になくなります。プライマリおよび拡張イベントデータ ストアのサイズは、[Event Management] ページの説明に従い、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）]** ページで設定します。

プライマリと拡張の両方の場所で、割り当てたスペースの90％が使用された場合、新しいデータにスペースを空けるためにストレージから最も古いイベントデータが削除されます。設定した場合は、データはプライマリ ストアから拡張ストアにコピーされます。ほとんどの場合、プライマリ ストレージから削除されたイベントは、循環によって拡張ストレージからなくなるまで拡張保管場所から引き続きクエリーに使用できます（プライマリから拡張データ ストアへのコピーのタイミングは、Events Per Second（EPS）レート、プライマリ ストアの拡張ストアに対する相対的サイズ、および拡張ストアにすでにコピーされたプライマリ データのパーセンテージを含む、多数の要因に依存します）。

イベントビューアで **[表示（View）] > [イベントストアディスク使用率の表示（Show Event Store Disk Usage）]** を選択して、割り当てたスペースのうち現在使用されている量と、最も古いイベントの経過時間をモニターできます。情報は円グラフで表示され、各場所の使用領域と未使用領域が GB 単位で示されます。各場所に現在保存されている最も古いイベントについても示されます。

この情報を参考にして、各場所に割り当てたスペースの増減を判断できます。

ヒント いずれかの場所のサイズを小さくしたときに、その新しいサイズが現在の使用量を下回っている場合は、新たに設定した目標のサイズに達するまで、最も古いイベントから順にすぐに削除されます。

イベント データ ストアのアーカイブまたはバックアップと復元

イベント データ ストアは、標準の Security Manager データベース バックアップには付属していません。イベント データ ストアをアーカイブまたはバックアップする場合は、プライマリまたは拡張のいずれの場所でも、それぞれの作業を別々に実行する必要があります。バックアップは必要に応じて復元できます。

ここでは、イベント データ ストアのバックアップと復元に必要な手順について説明します。

ヒント Event Manager サービスをディセーブルにすると、イベントがデータ ストアに書き込まれないため、バックアップ プロセスまたは復元プロセス中に生成されたイベントが失われることになります。

ステップ 1 イベント データ ストアをバックアップするには、次の手順を実行します。

a) Security Manager クライアントで、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択します。

b) イベント データ ストア フォルダの名前を特定します。フォルダは、[イベントデータストアの場所（Event Data Store Location）] フィールドに表示されています。デフォルトは *NMSROOT***MDC\eventing\database** で、NMSROOT はインストールディレクトリ（通常は C:\Program Files\CSCOpx）です。

拡張データ ストアをバックアップする場合は、[Extended Data Store Location] フィールドにその場所が指定されます。

c) [Enable Event Management] チェックボックスをオフにして、Event Manager サービスを停止します。[保存（Save）] をクリックして変更を保存します。サービスを停止するかどうかの確認が求められます。[はい（Yes）] をクリックし、サービスが停止したことが通知されるまで待ちます。

d) Security Manager の外部に、*NMSROOT***MDC\eventing\config\collector.properties** ファイルおよびイベントデータ ストア フォルダのコピーを作成します。そのコピーを別のサーバに保存して、ハードウェア障害が発生した場合にバックアップとして使用できるようにします。

拡張データ ストアもバックアップする場合は、そのフォルダもコピーします。

e) Security Manager クライアントの [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [イベント管理（Event Management）] ページで、[イベント管理の有効化（Enable Event Management）] チェックボックスをオンにし、[保存（Save）] をクリックします。サービスを開始するかどうかの確認が求められます。[はい（Yes）] をクリックし、サービスが開始されたことが通知されるまで待ちます。

ステップ 2 イベントデータ ストアを復元するには、次の点を除き、データのバックアップに使用したときと同じプロセスを使用します。

- 既存のイベント データ ストアのコピーを作成するのではなく、イベント データ ストアがある場所にバックアップをコピーします。このとき、まず既存のデータを削除してから、バックアップ データをコピーすることもできます。ただし、データ ストアのサイズ制限を超えていないかぎり、バックアップ データと既存のデータを混在させることができます（データストアの制限は、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [イベント管理（Event Management）] ページで設定されます）。

（注） 新旧のデータを混在できるは、collector.properties の既存のコピーを保持している（つまり、まだこのファイルを復元していない）場合で、かつ新旧のデータが同じサーバからのものである場合だけです。複数の異なるサーバからのデータ ストアはマージできません。

- Security Manager の再インストールを必要としたハードウェア障害または他のイベントから回復している場合を除き、collector.properties は復元しないでください。

イベントビューアの使用

モニタ対象のデバイスが関与するネットワーク問題のトラブルシューティングに役立てるために Event Viewer を使用します。ビューおよびフィルタリングを使用して、問題を分析し、原因と有効な対応策を特定することに役立てます。

ここでは、次の内容について説明します。

イベント ビューの使用方法

Event Viewer でイベントを表示するには、ビューを開きます。ビューは、フィルタおよび他のプロパティのセットです。これには、イベントのサブセットを定義できる色ルール、選択したカラムとその位置および幅、ならびにデフォルトの時間枠が含まれます。ビューによってイベント リストのスコープを制限できるため、検索内容をより簡単に見つけられます。

ここでは、次の内容について説明します。

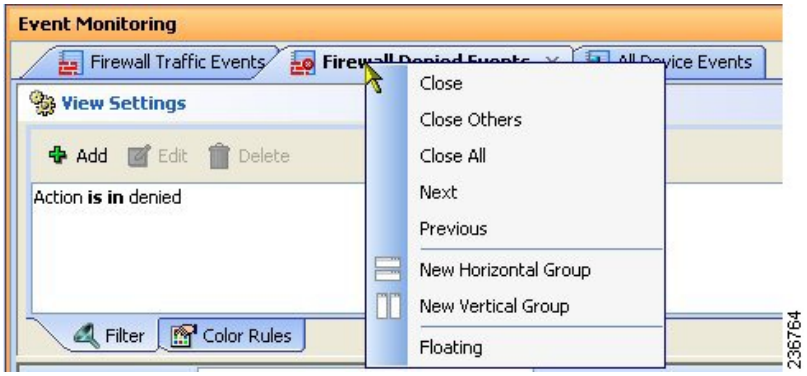
ビューを開く

Event Viewer では、最大 4 つの履歴ビューと 1 つのリアルタイム ビューが開けます。ビューを開くと、Event Viewer はビュー設定および時間範囲を使用してイベント データ ストアからイベントを取得してイベント テーブルに表示します。

- ビューを開いて現在アクティブで開いているビューと置き換えるには、Event Viewer で次のいずれかを実行します。
  - ビューのリストでビューをダブルクリックします。
  - ビューのリストでビューを右クリックして、[開く（Open）] を選択します。
- 新規タブにビューを開くには、次のいずれかを実行します。
  - メニュー バーで **[ファイル（File）] > [ビューを開く（Open View）]** を選択します。[Open a View] ダイアログボックスが開きます。このダイアログボックスは基本的にビューのリストと同じです。ビューを選択して、[OK] をクリックします。
  - ビューのリストでビューを右クリックして、[新しいタブで開く（Open In New Tab）] を選択します。

ビューのフローティングと配置

一度に最大 4 つの履歴ビューと 1 つのリアルタイム ビューが開けます。複数のビューを開いている場合は、Event Viewer のメインウィンドウの右ペインにタブウィンドウとして開かれています。複数のエリアがある場合は、最後に使用したエリア（「タブグループ」）内に開かれています。ウィンドウを配置するコマンドは、次の図に示すようにビュー ウィンドウのタブを右クリックすると表示されます。



必要に応じてビュー ウィンドウを配置するには多くのオプションがあります。たとえば、2 つのビューを並べて比較する、またはビューを閉じずにメイン ウィンドウから削除する必要がある場合があります。

目的の表示にするために、次の方法を使用してビュー ウィンドウを配置できます。

- ビューのフローティング：ビューを閉じずに Event Viewer のメインウィンドウからビューを削除するには、ビューのタブを右クリックして、[フローティング（Floating）] を選択します。ビューは独自のウィンドウに移動されます。

ビューをすでにフローティングしている場合は、[フローティング先（Floating to）] を選択して、すでにフローティングされているウィンドウの 1 つを選択できます。ビューはそのウィンドウ内の新規タブになります。

- ビューのドッキング：フローティングビューを Event Viewer のメインウィンドウに戻すには、ビューのタブを右クリックして、[ドッキング（Docking）] を選択します。
- 並べて比較のためにビューを水平または垂直に配置：ビューをフローティングせずに、簡単に比較できるようにビューを垂直または水平に配置するには、ビューのタブを右クリックして、[新規横方向グループ（New Horizontal Group）] または [新規縦方向グループ（New Vertical Group）] を選択します。これらのコマンドは、現在のタブ付きグループを選択されたレイアウトに分割します。これらのコマンドを使用するには、少なくとも 2 つのビューが開いている必要があります。3 つ以上のビューが開いていて、ビューのすべてを別のウィンドウに開く場合は、コマンドを複数回使用する必要があります。
- 異なるタブグループへのビューの移動：開いているビューがいくつかあり、ビューを水平または垂直なグループに配置している場合に、グループ間でビューを移動するには、ビューのタブを右クリックして、[次のタブグループに移動（Move to Next Tab Group）] または [前のタブグループに移動（Move to Previous Tab Group）] を選択します。コマンドは、このような移動が可能なようにビューが配置されている場合にだけ表示されます。
- グループの方向の変更：水平と垂直間でレイアウトを切り替えるには、ビューのタブを右クリックして、[タブグループの方向を変更（Change Tab Groups Orientation）] を選択します。

イベント テーブルの表示のカスタマイズ

イベント テーブルの定義済みまたはカスタム ビューの表示を要件を満たすようにカスタマイズできます。これらの変更は、定義済みのビューでも保存できます。

イベント テーブルをカスタマイズするために、次の手順を実行できます。

- 一覧表示されるイベントのタイプを制限するために、カラム フィルタを作成します。フィルタを定義するには、カラムベース フィルタの作成 （56 ページ）で説明するとおりにカラムの見出しの下矢印を使用します。
- 重大度に基づいてイベントを強調表示するには、ビューの色ルールの設定 （50 ページ）で説明するとおりに色ルールを作成します。
- テーブルに表示するカラムを変更するには、イベント テーブルのカラム （22 ページ）で説明するとおりにテーブルの見出し行の右側にある [Column Selector] アイコンをクリックします。
- カラムの幅を変更するには、カラムの見出しの右端をクリックし、目的のサイズにドラッグします。

- カラムの順序を変更するには、カラムの見出しをクリックし、カラムを目的の位置にドラッグします。
- カラムでイベント リストをソートするには、カラムの見出しをクリックします。カラム ソートは、昇順、降順、およびデフォルト順（イベント受信時刻順）が3回のクリック サイクルに基づいて実行されます。
- ビューセレクタおよび[イベントモニタリング（Event Monitoring）] ウィンドウの幅をデフォルト値にリセットするには、**[表示（View）]>[レイアウトのリセット（Reset Layout）]** を選択します。
- 送信元および宛先カラムが IP アドレスまたはホスト オブジェクト名のいずれを表示するかを 送信元/宛先 IP アドレスとホスト オブジェクト名間の切り替え （49 ページ）で説明するとおりに変更します。

関連トピック：

- カスタム ビューの作成 （51 ページ）
- ビューの保存 （53 ページ）

送信元/宛先 IP アドレスとホスト オブジェクト名間の切り替え

送信元および宛先 IP アドレスを表示できます。または、送信元または宛先 IP アドレスに一致するオブジェクトのホスト オブジェクト名を表示できます。デフォルトでは、Event Viewer はホスト オブジェクト名がある場合にはホスト オブジェクト名を表示します。

IPアドレスからホスト名へのマッピングは、イベントの送信元および宛先だけでサポートされます。また、マッピングはホスト オブジェクトだけに適用されます。イベントの送信元または宛先がネットワーク オブジェクト、グループ オブジェクト、またはアドレス範囲オブジェクトに一致した場合は、Event Viewer ではオブジェクト名が表示されません。

オブジェクトのタイプおよび内容を明らかにします。たとえば、これはホストタイプがネットワーク/ホストオブジェクトの場合だけ機能するのか、つまり、オブジェクトの単一値のホストバージョンか、単一値のグループオブジェクトの場合に機能するのか、またはネットワークか範囲オブジェクトの場合に機能するかなど。

送信元/宛先 IP アドレスとホスト オブジェクト名間で切り替えるには、次の手順を実行します。

- 送信元または宛先 IP アドレスに一致するオブジェクトのホストオブジェクト名を表示するには、[表示（View）] > [ネットワークホストオブジェクトの表示（Show Network Host Objects）] を選択します。このオプションは、デフォルトで選択されます。

ヒント そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。

（注） IP アドレスからホスト オブジェクト名へのキャッシュは、Event Viewer の起動時に作成されます。新規ホスト オブジェクトを定義した場合は、これらの変更をデータベースに送信し、次に Event Viewer を閉じて再起動してこれらのマッピングが使用されるようにする必要があります。

- 送信元および宛先カラム内の IP アドレスを表示するには、[表示（View）] > [ネットワークホストオブジェクトの表示（Show Network Host Objects）] の選択を解除します。

ビューの色ルールの設定

色ルールを使用して、イベントテーブル内に表示されるイベントをイベントの重大度に基づいて色分けできます。色分けを使用すると、最も必要なイベントの識別が簡単にできます。

色ルールを編集して、選択的に色ルールをイネーブルおよびディセーブルにできます。これにより、色ルールを削除せずにオンおよびオフにできます。

ヒント 色ルールは、定義済みビューとカスタム ビューの両方に対して設定できます。ただし、色ルールはビュー間で共有できません。すべての色ルールは、ビューに一意です。同じルールを複数のビューに適用する場合は、各ビューでルールを再作成する必要があります。

色ルールを定義し、イネーブルにするには、次の手順を実行します。

ステップ 1 色ルールを定義するビューを開きます（ビューを開く （47 ページ）を参照）。

ステップ 2 [ビューの設定（View Settings）] ペインで [色ルール（Color Rules）] タブをクリックします（[Event Monitoring] ウィンドウ （17 ページ）を参照）。

ステップ 3 次のいずれかを実行します。

- 新規ルールを追加するには、[追加（Add）] ボタンをクリックします。[Add Color Rule] ダイアログボックスで次のとおりルールを設定します。
  - [有効化（Enable）] を選択してルールをアクティブにします。
  - [シビラティ（重大度）（Severity）] リストから、ルールを適用するシビラティ（重大度）レベルを選択します。
  - [フォアグラウンド（Foreground）]（テキストの色）、[バックグラウンド（Background）]、および [フォントタイプ（Font Type）]（太字またはイタリック体）コントロールを使用して、テーブル内でのシビラティ（重大度）の表示方法を定義します。[Preview Text] エリアには、ルールがどのように表示されるかが示されます。
- ルールを編集するには、ルールを選択し、[編集（Edit）] 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、[削除（Delete）] ボタンをクリックします。

カスタム ビューの作成

カスタム ビューは、ビュー設定でフィルタを定義するビューです。カスタム ビューを使用すると、モニタリングおよび分析のためにエリアを正確に特定するようにフィルタ ルールを設定できます。カスタム ビューはプライベートなものであり、ユーザ間で共有できません。

カスタム ビューの作成には、最初からビューを作成、または既存のビューから作成の2つの方法があります。

- 定義済みカラム フィルタのないカスタム ビューを作成するには、次のいずれかを実行します。
  - メニューバーで [ファイル（File）] > [新規ビュー（New View）] を選択する。
  - ビューのリストの上の [新規（New）] ボタンをクリックする。

次に、ビューの名前および任意でビューの説明を入力して、[OK] をクリックします。ビューは、ビューのリストの [My Views] フォルダに追加されます。

- 既存のビューに基づいてカスタム ビューを作成するには、次のいずれかを実行します。
  - もとにする目的のビューを開いて、イベントテーブルツールバーの [保存（Save）] ボタンの下矢印をクリックして、[名前を付けて保存（Save As）] を選択、またはメニューバーで [ファイル（File）] > [名前を付けて保存（Save As）] を選択します。
  - ビューのリストでもとにする目的のビューを右クリックして、[名前を付けて保存（Save As）] を選択します。

次に、ビューの名前および任意でビューの説明を入力して、[OK] をクリックします。ビューは、ビューのリストの [My Views] フォルダに追加されます。新規ビューは、もとにするビューと同じフィルタを持ちます。

（注） ビュー名は、最大128文字で、英数字、スペース、ハイフン（-）、アンダースコア（_）、プラス記号（+）、ピリオド、およびアンド記号（&）を使用できます。説明には、最大1024 文字を使用できます。

新規ビューを作成したら、既存のビューと同じ方法でそのビューをカスタマイズできます。

- ビュー設定でフィルタを定義します。カラムベース フィルタの作成 （56 ページ）を参照してください。
- ビュー設定で色ルールを定義します。ビューの色ルールの設定 （50 ページ）を参照してください。

- イベントテーブルで表示するカラムを選択します。イベントテーブルのカラム （22ページ）を参照してください。
- イベント テーブルの表示をカスタマイズします。イベント テーブルの表示のカスタマイズ （48 ページ） を参照してください。

関連項目

- ビューとフィルタ （3 ページ）
- イベント テーブル ツールバー （19 ページ）
- カスタム ビューの名前または説明の編集 （52 ページ）
- カスタム ビューの削除 （53 ページ）

カスタム ビューの名前または説明の編集

カスタムビューの名前、またはカスタムビューの説明を変更するには、次のいずれかの手順を実行します。

- ビューリストでカスタムビューを選択して、リストの上にある [編集（Edit）] ボタンをクリックします。
- ビューリストでカスタムビューを右クリックして、[編集（Edit）] を選択します。

次に、カスタムビューの名前または説明に必要な変更を加えて、[OK] をクリックします。

（注） ビュー名は、最大128文字で、英数字、スペース、ハイフン（-）、アンダースコア（_）、プラス記号（+）、ピリオド、およびアンド記号（&）を使用できます。説明には、最大1024 文字を使用できます。

定義済みのビューの名前または説明は変更できません。

リアルタイム ビューと履歴ビュー間の切り替え

リアルタイムまたは履歴期間のいずれかを使用する任意のビューに対してイベントテーブルを更新できます。リアルタイムビューには、受信した状態のままのイベントが表示されます。一方、履歴ビューには、イベントテーブルツールバーの [スタート（Start）] ボタンをクリックするまで更新されないイベントのスタティックリストが表示されます。

開いているビューで、リアルタイムと履歴期間の間を切り替えるには、次の手順を実行します。

- リアルタイムでイベントを表示するには、[表示（View）] > [モード（Mode）] > [リアルタイム（Real Time）] を選択、またはイベントテーブルツールバーの [時間セレクタ（Time Selector）] コントロールをクリックして、[リアルタイム（Real Time）] を選択します。

ツールバーのコントロールの場所を見つけるには、イベント テーブル ツールバー （19 ページ）を参照します。

- 履歴期間のイベントを表示するには、[表示（View）]>[モード（Mode）] メニューから、またはイベントテーブルツールバーの [時間セレクタ（Time Selector）] コントロールから、目的のタイムフレームを選択します。[Real Time] 以外のオプションすべてが履歴ビューです。詳細については、イベントの時間範囲の選択 （54 ページ）を参照してください。

ビューの保存

ビューの設定を編集した場合は、変更が持続するように設定を保存する必要があります。ビューを保存すると、フィルタ（カスタム ビューの場合のみ）、選択したカラム、カラム幅、およびソート順序などのテーブル プリファレンス、時間範囲、および色ルールの変更が保存されます。定義済みのビューのフィルタを変更する場合は、[Save As] を使用して新規カスタム ビューを作成する必要があります。

- ビューの変更を保存するには、Event Viewer で次のいずれかを実行します。
  - メニューバーから **[ファイル（File）] > [保存（Save）]** を選択する。
  - イベントテーブルツールバーで [保存（Save）] ボタンをクリックする。

変更の保存を確認するように求められます。

- 新規カスタム ビューとして変更を保存するには、次のいずれかを実行して [Save View As] ダイアログボックスを開きます。
  - メニューバーから **[ファイル（File）] > [名前を付けて保存（Save As）]** を選択する。
  - イベントテーブルツールバーの [保存（Save）] ボタンの下矢印をクリックして、[名前を付けて保存（Save As）] を選択する。
  - ビューのリストでビューを右クリックして、[名前を付けて保存（Save As）] を選択する。

次に、ビューの名前および任意でビューの説明を入力して、[OK] をクリックします。ビューは、ビューのリストの [My Views] フォルダに追加されます。

（注） ビュー名は、最大 128 文字で、英数字、スペース、ハイフン（-）、アンダースコア（_）、プラス記号（+）、ピリオド、およびアンド記号（&）を使用できます。説明には、最大 1024 文字を使用できます。

カスタム ビューの削除

カスタム ビューは削除できますが、定義済みのビューは削除できません。カスタム ビューを削除するには、次のいずれかを実行します。

- ビューのリストでカスタムビューを選択して、リストの上にある [削除（Delete）]（ゴミ箱）ボタンをクリックします。
- ビューのリストでカスタムビューを右クリックして、[削除（Delete）] を選択します。

削除の確認が求められます。

イベントのフィルタリングおよびクエリー

イベントテーブルに表示されるイベントのフィルタリングには多くのオプションがあります。適切な時間範囲を選択する、特定のカラムの要素をフィルタリングする、またはテキスト文字列を検索することによってもイベントのリストを絞り込めます。

ここでは、次の内容について説明します。

イベントの時間範囲の選択

イベントテーブルツールバーの [時間セレクタ（Time Selector）] コントロール、またはそれに相当する [表示（View）] > [モード（Mode）] コマンドを使用して、イベントを表示するための時間範囲を選択します。イベントテーブルには、選択した時間範囲内に発生したイベントだけが一覧表示されます。ツールバーの [Time Selector] コントロールの場所を見つけるには、イベント テーブル ツールバー （19 ページ）を参照します。

ヒント 履歴ビューの場合、時間はワークステーションに設定された時間ではなく、サーバの時間に基づいています。

時間範囲を変更すると、選択した範囲内のイベントを表示するようにイベント テーブルがリロードされます。履歴ビューの場合、[開始（Start）] をクリックして、またはイベント テーブルのリフレッシュ （56 ページ）で説明したその他のアクションを実行して、イベントリストをリフレッシュできます。

時間範囲のオプションは、次のとおりです。

- 現在時刻から過去にさかのぼってイベントを表示するには、次のいずれかの期間を選択します。[過去 10 分間（last 10 minutes）]、[過去 1 時間（last 1 hour）]、[過去 12 時間（last 12 hours）]、[過去 1 日間（last 1 day）]、または [過去 1 週間（last 1 week）] です。
- 今日または昨日のイベントを表示するには、必要に応じて [今日（today）] または [昨日（yesterday）] を選択します。
- 特定の日のイベントを表示するには、[次の日（is on）] を選択し、表示されたカレンダーからその日付を選択します。
- 特定の日付と時刻の範囲のイベントを表示するには、[次の期間（is between）] を選択し、表示されたカレンダーから範囲の最初および最後の日付と時刻を選択します。
- リアルタイム イベントを表示するには、[Real Time] を選択します。

フィルタリングと時間スライダの使用方法

時間スライダの垂直スライダ コントロールを使用すると、イベント テーブルに表示されるイベントの開始時刻を変更できます。これは、イベントの場所を特定し、そのおおよその発生時刻を確認するときに特に便利です。

時間スライダの操作の詳細については、時間スライダ （32 ページ）を参照してください。

時間スライダを使用してフィルタリングを使いやすくするには、次の手順を実行します。

ステップ 1 履歴ビューを開く、またはツールバーの Time Selector を使用する、または **[表示（View）]>[モード（Mode）]** コマンドを使用して、[過去10分間（Last 10 Minutes）] など適切な時間範囲を選択します。詳細については、イベントの時間範囲の選択 （54 ページ）を参照してください。

ステップ 2 調査するイベントのおおよその時刻に垂直スライダを移動します。

イベント テーブルがリロードされて、垂直スライダで指定した時刻とそれ以前に発生したイベントが表示されます。この時間範囲は時間スライダで共有され、選択した時間の長さは Time Selector で選択した時間の長さに基づきます（たとえば、[過去10分間（Last 10 Minute）] ビューの場合は 10 分間。または、[の間にある（is between）] ビューで選択した時間と同じ長さ）。時間範囲は [Time Selector] コントロールに、たとえば次のように示されます。

ステップ 3 これで、イベントの場所を特定するために、次のいずれかを実行できます。

- カスタム カラム フィルタを適用します。カラムベース フィルタの作成 （56 ページ）を参照してください。
- テキスト文字列を検索するには、クイック フィルタを使用します。テキスト文字列に対するフィルタリング （60 ページ）を参照してください。
- イベント テーブルをスクロールするか、またはイベント テーブルのページを切り替えます。
- 時間スライダのページ コントロールを使用して、時間範囲を前方または後方にリセットします。詳細については、時間スライダ （32 ページ）を参照してください。

（注） 時間スライダでページを切り替えるときに前方または後方に移動する距離は、設定されているモード（時間範囲）またはイベント テーブルが保持できるイベントの数によって決まります。垂直スライダの位置は、イベント テーブルにロードされた最新のイベントを示します。

イベント テーブルのリフレッシュ

「過去 10 分」など履歴モードを使用している場合、表示される最新のイベントは時間範囲を選択した時刻またはビューを開いた時刻に対応しています。同様に、リアルタイム モードを使用していて [Stop] をクリックした場合、イベント テーブルにはイベント ストリームを停止したあとに到着したイベントは含まれません。

イベントテーブルに一覧表示されたイベントをリフレッシュして、現在の選択された時間範囲のイベントにするには、次のいずれかを実行します。

- ツールバーで [開始（Start）] をクリックするか、**[表示（View）] > [開始（Start）]** を選択します。イベントテーブルは、現在の選択された時間範囲に基づいてリフレッシュされます。リアルタイム ビューの場合は、イベント ストリームが再開します。
- ツールバーの日時セレクタを使用するか、**[表示（View）] > [モード（Mode）]** コマンドを使用して、異なる時間範囲を選択します。
- イベント テーブルの下にある時間スライダの垂直スライダまたは改ページ コントロールを使用して、異なる時間のスライスを選択します。これらのコントロールの使用の詳細については、時間スライダ （32 ページ）を参照してください。

カラムベース フィルタの作成

Event Viewer で特定のカラムの内容に基づいてイベント テーブルをフィルタリングできます。カラム フィルタは、ビュー設定に含まれているフィルタのタイプで、ビューの基本的内容を定義します。カラムフィルタを適用するたびに、新しく選択されたフィルタが含まれるようにビューに対するビュー設定が更新されます。新規フィルタをビュー定義の一部として持続させるには、ビューを閉じる前に保存する必要があります。

カラム フィルタを定義するには、次のとおり多くの方法があります。

- [ビュー設定（View Settings）] ペインで [追加（Add）] ボタンをクリックします。まず、フィルタのもとにするカラムの選択を求められます。[OK] をクリックすると、フィルタの作成を求められます。
- [ビュー設定（View Settings）] ペインでフィルタを選択して、[編集（Edit）] ボタンをクリックしてフィルタを変更します。
- イベント テーブルでカラムの見出しの下矢印ボタンをクリックして、ドロップダウン リストから次のいずれかを選択します。
  - 特定のエントリ。ドロップダウン リストには、テーブルに一覧表示されたイベントに現在表示されているすべての値が含まれています。

- [(All)]。このカラムからフィルタを削除するには、[(All)] を選択します。イベントテーブルは、他のフィルタ基準を満たすイベントを表示するように更新されます。
- [(Custom)]。複数の値もしくは負の値を持つ場合がある、または現在のイベント テーブルのカラムに現在は含まれていないデータに基づく場合があるフィルタを作成するには、[(Custom)] を選択します。[(Custom)] を選択することは、[View Settings] ペインで直接フィルタを作成することと基本的に同じです。

- イベントテーブルで値を右クリックして、[この値でフィルタリング（Filter This Value）] を選択します。このアクションは、ドロップダウン リストからカラムに対して値を選択することと同じ結果になります。

他に、[この値以外でフィルタリング（Filter Not This Value）] を選択して、値を除外するフィルタを作成できます。

- イベントテーブルで値を右クリックして、[イベントからフィルタを作成（Create Filter from Event）] を選択します。含める特定のカラムを選択するように求められます。右クリックしたカラムは当初は選択されていますが、選択を解除できます。

次の手順では、カラムのドロップダウンリストから単純に値を選択しない、カスタム カラム ベース フィルタを構築する方法を説明します。

ヒント

- カラム フィルタは累積的です。ビューのイベントテーブルにイベントが表示されるには、そのイベントがすべてのカラムフィルタ基準を満たす必要があります。論理和を取ったカラムフィルタのセットは作成できません。
- カラムによっては、ネットワーク/ホストまたはサービス ポリシー オブジェクトを選択してフィルタ基準を定義できます。ポリシーオブジェクトを選択すると、フィルタを簡素化できます。ただし、フィルタでポリシーオブジェクトが選択できるようにするには、オブジェクトがデータベースにコミットされている必要があります。フィルタリング目的で新規オブジェクトを作成する場合は、Event Viewer でフィルタ作成を試みる前に、変更を Configuration Manager に必ず送信します（また、Workflow モードをアプルーバで使用している場合は、変更を承認します）。

ポリシーオブジェクトの使用中は、デバイスレベルのオーバーライドがオブジェクトに対して定義されているかどうかがフィルタリングによって認識されます。たとえば、10.10.10.10 を含むネットワーク/ホスト オブジェクトを使用し、デバイス A がアドレスを 10.10.10.12 に変更するオーバーライドを保持している場合は、デバイス A からのイベントはイベントが 10.10.10.12 と一致する場合にだけリストに表示されます。オーバーライドを保持しないデバイスの場合は、イベントは 10.10.10.10 と一致する必要があります。さらに、デバイス A が 10.10.10.10 と一致するイベントを保持している場合は、イベントがデバイスレベルのオーバーライドと一致しないため、イベントは一覧表示されません。つまり、ポリシーオブジェクトを使用するとデバイスごとに異なる結果となるため、ポリシー定義により厳密に一致することになります。

組織がユーザ アクセスの制御に ACS を使用している場合は、ネットワーク/ホスト、ネットワーク/ホスト -IPv6、およびサービス オブジェクトをフィルタで使用するために適切なオブジェクトの表示権限を持っている必要があります。

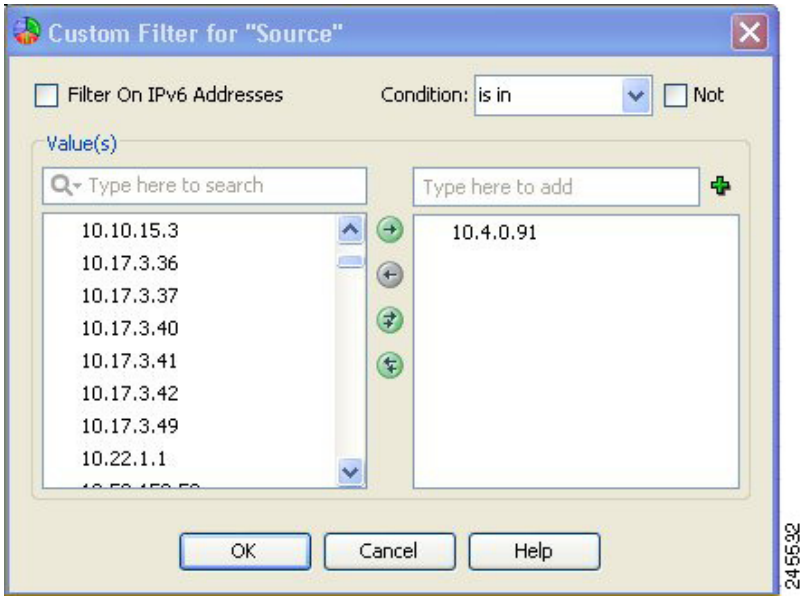
- すべてではありませんが、ほとんどのカラムの内容に対してフィルタリングできます。カラムに下矢印がない場合は、そのカラムに対してはフィルタリングできません。たとえば、[Description]、[Event Name]、[Generation Time]、または [Receive Time] に対してはフィルタリングできません。
- フィルタアイコン（じょうご）はフィルタリングされたカラムの見出しに表示されます。
- 使用可能なカラムの詳細については、イベント テーブルのカラム （22 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- [ビュー設定（View Settings）] ペインで [追加（Add）] ボタンをクリックします。[Add Custom Filter to a Column] ダイアログボックスが開きます。フィルタのもとにするカラムを選択して、[OK] をクリックします。
- [ビュー設定（View Settings）] ペインで、変更するフィルタを選択して [編集（Edit）] ボタンをクリックします。
- ドロップダウンリストからカラムに対して [（カスタム）（(Custom)）] を選択します。
- 目的のカラムに含まれる任意のセルを右クリックして、[カスタムフィルタ（Custom Filter）] を選択します。

選択したカラムに対して [Custom Filter] ダイアログボックスが開きます。

ステップ 2 [Custom Filter] ダイアログボックスで目的の値を選択します。次の図に、[Source] カラムに対するこのダイアログボックスの一般的な例を示します。



次に、[Custom Filter] ダイアログボックスに表示される可能性のあるコントロールについて説明します。すべてのカラムに対してすべてのコントロールが表示されるわけではありません。

- [使用可能な項目（Available Items）] と [選択された項目（Selected Items）] のリスト：ほとんどの場合、項目を選択するには、使用可能な値が含まれる左側のリストで項目を強調表示してから、右矢印をクリックして選択された値のリストに移動します。複数の値を選択できます。右側のリストはフィルタリングする値を定義します。

使用可能な値のカラムに一覧表示される項目は、イベントテーブルに一覧表示されたイベントに現在表示されている値によって決定されます。アドレスおよびサービスフィールドの場合は、ポリシーオブジェクトもリストに含まれます。使用可能な値がたくさんある場合は、リストの上にある編集ボックスに目的の値を入力して検索できます。入力するとリストがフィルタリングされます。Q の横にある下矢印をクリックして、一致する検索文字列の評価方法を変更します。

次の方法を使用して、値の選択または選択解除をすることもできます。

- 選択された値のリストの上にある編集ボックスに項目を入力して、+ ボタンをクリックします。この方法は、使用可能な値が多数ある場合、または現在のイベントリストにない値に対してフィルタリングする場合に役立ちます。
- 他方のリストに移動する、一方のリストの項目をダブルクリックします。
- 選択に関係なく、すべての項目を移動するには、二重矢印のボタンをクリックします。

（注） 限られた場合ですが、[Custom Filter] ダイアログボックスに単一のリストが含まれる場合があります。たとえば、[Event Type ID] および [Device] カラムに対する [Custom Filter] ダイアログボックスには単一のセレクタが含まれます。この場合、項目の隣にあるチェックボックスを使用して選択します。フォルダを選択すると、フォルダ内のすべての項目が選択されます。

- [IPv6アドレスに対するフィルタリング（Filter on IPv6 Addresses）]：アドレスを含むカラムの場合、このオプションを使用して、使用可能な値のカラムの IPv4 アドレスと IPv6 アドレスおよびネットワーク/ホストオブジェクトを切り替えて一覧表示します。単一のビュー内では、IPv4 アドレスまたは IPv6 アドレスのいずれかに対してフィルタリングできますが、両方に対してはできません。
- [条件（Condition）]、[次ではない（Not）]：選択された項目に適用する条件を定義します。通常は、[次に含まれる（is in）] です。

ネガティブ条件を作成して、選択された値で定義されるイベントをイベントテーブルに含めないようにするには、[Not] オプションを選択します。

ステップ 3 [OK] をクリック

ビュー設定は、新規フィルタが含まれるように更新されます。また、イベントテーブルは、すべてのフィルタを満たすイベントだけを表示するように更新されます。

特定のイベントの値に基づいたフィルタリング

イベント内に含まれる情報、またはイベント内の単一のセルに基づいて新規にフィルタを作成できます。そのためには、右クリックしてフィルタ コマンドを選択します。フィルタ コマンドを使用してフィルタリングする場合、カラムフィルタがビュー設定に追加されます。次を実行できます。

- 選択したイベントの複数の値に基づいてフィルタを作成するには、[イベントからフィルタを作成（Create Filter from Event）] を選択し、ダイアログボックスからフィルタリングする値を選択します。ダイアログボックスには、テーブルに表示されたカラムだけが一覧表示されます。現在の値はカッコで囲まれて表示されます。カラムの説明については、イベント テーブルのカラム （22 ページ）を参照してください。
- セルの値だけに対してフィルタリングするには、セルを右クリックして、[この値でフィルタリング（Filter This Value）] を選択します。
- セルの値だけに対してフィルタリングするには、セルを右クリックして、[この値以外でフィルタリング（Filter Not this Value）] を選択します。すべての空のセルを含む、このカラムの選択された値を含まないすべてのイベントがテーブルに表示されます。
- 送信元、送信元サービス、宛先、および宛先サービスに基づいて、選択したイベントのフローに対してフィルタリングするには、[このフローをフィルタリング（Filter This Flow）] を選択します。

テキスト文字列に対するフィルタリング

イベント内のテキスト文字列を検索するには、クイック フィルタを使用します。検索キーワードを入力すると、イベントテーブルから一致しないイベントが自動的に除外されます。すべてのカラムを検索できます（デフォルト）。または特定のカラムを選択して検索できます。

次の図に、イベント テーブル ツールバーの右側にあるクイック フィルタを示します（イベント テーブル ツールバー （19 ページ）を参照）。

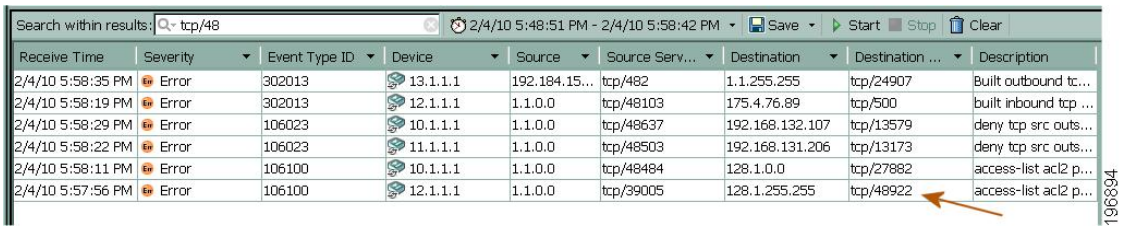
検索を実行するには、単に検索文字列を入力します。文字列の評価方法を変更するには、編集ボックスの左側の [Q]（虫眼鏡）の隣にある下矢印をクリックします。次のコントロールを使用して、検索スコープを制限できます。

- カラム名：特定のカラムを選択して、そのカラム内だけを検索します。テーブルに現在表示されているすべてのカラムがリストに含まれています。デフォルトでは、すべてのカラムを検索します。
- 大文字と小文字の区別：一致の選択時に大文字を考慮するかどうかを制御するには、[大文字小文字の区別あり（Case sensitive）] または [大文字小文字の区別なし（Case insensitive）] を選択します。デフォルトでは、大文字と小文字の区別なしです。
- ワイルドカードの使用：次の文字をワイルドカードとして評価するには、[ワイルドカードを使用（Use Wild Cards）] を選択します。
  - *（アスタリスク）：0 文字以上と一致します。
  - ?（疑問符）：1 文字と一致します。
- 一致方法：セル内で検索文字列が存在する場所を指定するために、次から 1 つを選択します。

- [Match from start]：文字列は、セルの先頭にある必要があります。
- [Match exactly]：セルには、すべての検索文字列、かつ検索文字列だけが含まれている必要があります。
- [Match anywhere]：文字列は、セル内の任意の場所に存在できます。

検索文字列を削除するには、単にクイック フィルタ編集ボックスから検索文字列を削除します。

たとえば、tcp/48 で始まるポートに関連するイベントを検索するには、**tcp/48** をクイックフィルタに入力します。次の図で、6 つを除いてすべてのイベントがフィルタリングによってテーブルから除外されたことに注意してください。この例では、検索文字列は、最初の 5 つのイベントでは [Source Service] カラムで見つかりましたが、6 番めのイベントでは [Destination Service] カラムで見つかりました。宛先サービスだけが重要なことが事前にわかっている場合は、クイック フィルタ ドロップダウン リストから [接続先サービス（Destination Service）] を選択すると、テーブルに最後のイベントだけが表示されます。



フィルタのクリア

イベントテーブルにフィルタを適用すると、一致しないイベントは表示されません。一致しないイベントを表示する必要がある場合があります。この場合、異なるフィルタ（またはフィルタなし）を適用する異なるビューを開くか、現在のビューからフィルタをクリアします。

フィルタをクリアすると、フィルタ定義がビュー設定から削除されますが、変更は [保存（Save）] をクリックするまで永続化されません。したがって、ビュー設定を再定義せずに、フィルタを一時的に削除できます。

フィルタを一度に 1 つずつ、またはすべてのフィルタをクリアできます。

- 単一のフィルタをクリアするには、次のいずれかを実行します。
  - [表示設定（View Settings）] ペインでフィルタを選択して、[削除（Delete）] をクリックします。
  - フィルタリングされた列のドロップダウンリストから [（すべて）（(All)）] を選択します。
  - フィルタリングされた列を右クリックして、[このフィルタをクリア（Clear This Filter）] を選択します。
- すべてのフィルタをクリアするには、イベントテーブル内で右クリックして、[すべてのフィルタをクリア（Clear All Filters）] を選択します。

特定のイベントに対する操作の実行

イベントテーブル内の単一のイベントに対して、次のような操作をさまざまな方法で実行できます。

- **右クリック**：イベントテーブルの単一のイベントを右クリックすると、そのイベントで使用できるコマンドを含むコンテキストメニューが開きます。右クリック メニューから実行可能な操作の詳細については、次の項を参照してください。
  - イベント コンテキスト（右クリック）メニュー （62 ページ）
  - 単一のイベントの詳細の参照 （67 ページ）
  - イベント レコードのコピー （67 ページ）
  - ビューの保存 （53 ページ）
  - 特定のイベントの値に基づいたフィルタリング （59 ページ）

（注） イベントビューアで有効な IPv4 アドレスの上にマウスを置くと、その IP アドレスの IP インテリジェンスツールを起動できます。IP インテリジェンスツールは、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS 情報など、IPv4 アドレスに関するさまざまな情報を提供します。IP インテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence）を参照してください。

- **イベントの選択**：イベントテーブルの単一のイベントをクリックすると、そのイベントが強調表示され、[イベントの詳細（Event Details）] ペインにその特定のイベントの詳細が表示されます。別のイベントを選択するには **Ctrl** キーを押した状態で選択し、ある範囲のイベントを選択するには **Shift** キーを押した状態で選択します。
- **イベントのダブルクリック**：イベントテーブルの単一のイベントをダブルクリックすると、[イベントの詳細（Event Details）] ダイアログボックスが開き、読みやすい形式でイベント情報が表示されます。[Event Details] ダイアログボックスでは、表示された詳細を印刷できます。または、詳細の一部またはすべてを他のプログラムに貼り付けるためにクリップボードにコピーできます。[Next] および [Previous] ボタンを使用してイベント テーブルに一覧表示されたイベント全体をスクロールできます。属性の意味の詳細については、イベント テーブルのカラム （22 ページ）を参照してください。

または、イベントを右クリックし、[すべての詳細を表示（Show All Details）] を選択して [イベントの詳細（Event Details）] ダイアログボックスを開くこともできます。

イベント コンテキスト（右クリック）メニュー

イベント テーブルのイベントを右クリックすると、コンテキスト メニューが表示され、選択したイベントに使用できるコマンドが提供されます。使用可能なコマンドの特定のリストは、右クリックしたイベントのタイプおよび特定のセルによって異なります。次の表に、使用可能なコマンドすべてについて説明します。

（注） 以下にリストされている右クリックオプションに加えて、イベントビューアで有効なIPv4アドレスの上にマウスを置くと、そのIPアドレスのIPインテリジェンスツールも起動できます。IPインテリジェンスツールは、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS情報など、IPv4アドレスに関するさまざまな情報を提供します。IPインテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence）を参照してください。

表 *9:* イベント コンテキスト メニュー

コマンド	説明
Clear This Filter	このカラムに定義されたフィルタを削除します。このコマンドが使用できるのは、フィルタリングされたカラムのセルを右クリックした場合だけです。 フィルタはビュー設定から削除されます。変更を持続させるには、ビューを保存する必要があります。
Clear All Filters	ビュー設定からすべてのフィルタを削除します。このコマンドが使用できるのは、少なくとも1つのカラム フィルタがある場合だけです。 変更を持続させるには、ビューを保存する必要があります。
Filter This Value Filter Not This Value	右クリックしたセルの値に基づいてカラムフィルタを作成します。値に基づいて、ポジティブまたはネガティブ フィルタを作成できます。 ビュー設定は新規フィルタで更新されて、このカラムの既存のフィルタがあればそのフィルタと置き換えられます。変更を持続させるには、ビューを保存する必要があります。
Create Filter from Event	選択したイベントの値に基づいて一連のカラムフィルタを作成します。含める特定のカラムを選択するように求められます。右クリックしたカラムは当初は選択されていますが、選択を解除できます。 ビュー設定は新規フィルタで更新されて、選択したカラムの既存のカラムフィルタはすべて置き換えられます。変更を確定させるには、ビューを保存する必要があります。
カスタム フィルタ（Custom Filter）	カラムベース フィルタの作成 （56 ページ）で説明するとおりに、カスタム カラム フィルタを作成します。 ビュー設定は新規フィルタで更新されて、選択したカラムの既存のフィルタはすべて置き換えられます。変更を確定させるには、ビューを保存する必要があります。

コマンド	説明
Filter This Flow	特定のトラフィック フローに関連するイベントを示すカラムベース フィルタのセットを作成します。フィルタリングされるカラムは、送信元および送信元サービス、ならびに宛先および宛先サービスです。 ビュー設定は新規フィルタで更新されて、選択したカラムの既存のフィルタはすべて置き換えられます。変更を確定させるには、ビューを保存する必要があります。
Show IPLogs	外部パケットアナライザ ツールを使用して、IPS アラート イベントに対して IP ログを開きます。パケット アナライザがインストールされていて、*.pcap ファイル拡張子に関連付けられている必要があります。
Show All Details	イベントに対する [Event Details] ダイアログボックスが開き、読みやすい形式ですべてのイベント情報が表示されます。詳細を印刷またはクリップボードにコピーすることもできます。 この詳細は、イベント テーブルの下の [Event Details] ペインに表示される詳細と同じです。
Copy commands	次のコマンドを使用して、イベントデータをクリップボードにコピーできます。その後、データを使用するためにスプレッドシートまたは他のプログラムに貼り付けられます。詳細については、イベント レコードのコピー（67 ページ）を参照してください。 • [セルのコピー（Copy Cell）]：右クリックしたセルの内容をクリップボードにコピーします。 • [選択されたイベントをコピー（Copy Selected Events）]：すべての選択された（強調表示された）イベントの内容をクリップボードにコピーします。 • [すべてのイベントをコピー（Copy All Events）]：すべての一覧表示されたイベントの内容をクリップボードにコピーします。 このコマンドは、イベントテーブルを管理可能な数のイベントにフィルタリングした場合にだけ役立ちます。
Save Selected Events as HTML Save All Events as HTML Save Selected Events as CSV Save All Events as CSV	イベントテーブルに一覧表示されたすべてのイベント、またはすべての選択された（強調表示された）イベントをワークステーションのHTMLまたは Comma-Separated Values（CSV; カンマ区切り値）ファイルに保存します。エクスポートファイルのフォルダ選択およびファイル名の入力を求められます。 詳細については、ファイルへのイベントの保存 （68 ページ）を参照してください。

コマンド	説明
Go To Policy	Configuration Manager のデバイスのポリシー設定でこのイベントを生成したポリシーを検索します。このコマンドは、[Event Name] セルに双眼鏡アイコンが表示されるイベントに対してだけ使用できます。詳細については、 Event Viewer からの Security Manager ポリシーの検索 （68 ページ）を参照してください。
パケット キャプチャ	パケット キャプチャ ツールが開き、デバイス上でのパケット キャプチャに対する条件が定義できます。
Ping and TraceRoute	ping、TraceRoute、および NS ルックアップ ツールが開き、これらのアプリケーションをイベントの送信元デバイスで使用できます。詳細については、ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析を参照してください。

コマンド	説明

Tune Signature	選択したイベントに関連付けられたシグネチャを有効または無効にしたり、デバイスまたは共有ポリシーに割り当てられているシグネチャの基本リスクレーティングを変更したりできる [IPSシグネチャのクイック調整（IPS Signature Quick Tune）] ダイアログボックスを開きます。
	
	シグネチャを調整するには、チケットを作成するか、開く必要があります。詳細については、アクティビティ/チケットの操作を参照してください。
	
	シグネチャの基本リスクレーティング値。この値は、忠実度評価と重大度係数を掛け合わせたものを 100 で割る（忠実度評価 X 重大度係数 /100）ことによって計算されます。この値は読み取り専用です。直接変更できません。基本リスクレーティングを変更するには、重大度と忠実度の値を変更する必要があります。
	
	• 重大度：シグネチャによってレポートされる重大度レベル（[High]、[Medium]、[Low]、または [Informational]）。
	  • High = 100
	  • Medium = 75
	  • Low = 50
	  • Informational = 25
	
	• 忠実度：忠実度評価、または Signature Fidelity Rating（SFR; シグネチャの忠実度評価）は、ターゲットに関する具体的な情報がない場合のシグネチャの実行忠実度に関連付ける重みを示します。この評価には、0 ～ 100 の任意の数字を指定できます。100 は、シグニチャの信頼性が最も高いことを意味します。
	
	シグネチャを有効または無効にするか、基本リスクレーティングを変更した後、変更をデバイスに反映させるために、Configuration Manager を使用して設定をデバイスに再展開する必要があります。このような変更はリアルタイムのイベントにのみ影響し、過去のイベントには影響しません。設定の展開の詳細については、展開についてを参照してください。

IPS シグネチャ クイック チューン ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

選択したイベントに関連付けられたシグネチャを有効または無効にしたり、デバイスまたは共有ポリシーに割り当てられているシグネチャの基本リスクレーティングを変更したりするに

は、[IPSシグネチャのクイック調整（IPS Signature Quick Tune）] ダイアログボックスを使用します。

ナビゲーション パス

イベントビューアで、行（イベント）を右クリックし、[シグネチャの調整（Tune Signature）] をクリックします。詳細については、イベント コンテキスト（右クリック）メニュー （62 ページ）を参照してください。

単一のイベントの詳細の参照

各イベントには、多くの別々のフィールドに特定の情報が多数含まれています。通常、これらのフィールドのサブセットはイベントテーブルに表示します。イベントの全詳細を表示する必要がある場合は、次のいずれかを使用します。

- [イベントの詳細（Event Details）] ペイン：イベントを選択して、イベントテーブルの下にある [イベントの詳細（Event Details）] ペインを開きます。このペインを開くには、[イベントの詳細（Event Details）] タイトル行の任意の場所をクリックするか、メニューから [表示（View）] > [イベントの詳細の表示（Show Event Details）] を選択します。[Event Details] ペインでは、情報がタブに整理されます。このペインの詳細については、[Event Details] ペイン （33 ページ）を参照してください。
- [イベントの詳細（Event Details）] ダイアログボックス：このダイアログボックスを開くには、イベントをダブルクリックするか、イベントを右クリックして、[すべての詳細を表示（Show All Details）] を選択します。情報は、フラットなリストで表示され、[Event Details] ペインの [Details] タブに表示される情報が示されます。属性の意味の詳細については、イベント テーブルのカラム （22 ページ）を参照してください。

[Event Details] ダイアログボックスには、次のコントロールが含まれています。

- [Print] ボタン：情報を印刷するには、このボタンをクリックします。プリンタを選択するプロンプトが表示されます。
- [コピー（Copy）] ボタン：このボタンの下矢印をクリックして [すべての行（All Rows）] または [選択した行（Selected Rows）] を選択します。情報がクリップボードにコピーされます。情報は別のアプリケーションに貼り付けられます。テーブルで少なくとも 1 行を選択した場合にだけ、[Selected Rows] コマンドが機能することに注意してください。
- [Next]、[Previous] ボタン：イベント テーブルに現在表示されているイベント全体をスクロールするには、このボタンをクリックします。[Next] で上に、[Previous] で下にテーブル内を移動します。

イベント レコードのコピー

単一のイベント、複数のイベント、すべてのイベント、さらに単一のセルの内容をクリップボードにコピーできます。その後、スプレッドシートや電子メール メッセージなどの別のアプリケーションに情報を貼り付けられます。

イベント テーブルで次の手順を実行できます。

- [選択したイベントのコピー（Copy selected events）]：1 つ以上の選択したイベントをコピーするには、イベントテーブル内で右クリックして、[選択したイベントをコピー（Copy Selected Events）] を選択します。いずれのイベントを右クリックするかは重要ではありません。テーブル内で選択された（強調表示された）イベントがコピーされます。

イベントをクリックして選択します。さらに別のイベントを選択するには **Ctrl** キーを押した状態で選択し、ある範囲のイベントを選択するには **Shift** キーを押した状態で選択します。

- **単一のセルの内容のコピー**：1 つのイベント内の単一のセルの内容をコピーするには、セルを右クリックして、[セルのコピー（Copy Cell）] を選択しますテーブル内で複数のイベントが選択されている場合は、セルの内容をコピーできません。
- **すべてのイベントのコピー**：イベント テーブルに表示されているすべてのイベントをコピーするには、テーブル内の任意の場所で右クリックして、[すべてのイベントのコピー（Copy All Events）] を選択します。

ファイルへのイベントの保存

イベントをクリップボードにコピーして別のアプリケーションに貼り付ける代わりに、イベントを HTML または Comma-Separated Values（CSV; カンマ区切り値）ファイルに直接保存できます。HTML ファイルは情報を表示する場合に便利です。一方で、CSV ファイルはスプレッドシート アプリケーションで開いて詳細分析およびレポート生成に使用できます。

イベント データを保存すると、フォルダの選択およびファイル名の入力を求められます。

イベント テーブルで次の手順を実行できます。

- **選択したイベントの保存**：1 つ以上の選択したイベントを保存するには、イベントテーブル内で右クリックして、[選択したイベントをHTMLとして保存（Save Selected Events as HTML）] または [選択したイベントをCSVとして保存（Save Selected Events as CSV）] のいずれかを選択します。いずれのイベントを右クリックするかは重要ではありません。テーブル内で選択された（強調表示された）イベントが保存されます。

イベントをクリックして選択します。さらに別のイベントを選択するには **Ctrl** キーを押した状態で選択し、ある範囲のイベントを選択するには **Shift** キーを押した状態で選択します。

- **すべてのイベントの保存**：イベントテーブルに表示されているすべてのイベントを保存するには、テーブル内の任意の場所で右クリックして、[選択したイベントをHTMLとして保存（Save Selected Events as HTML）] または [選択したイベントをCSVとして保存（Save Selected Events as CSV）] のいずれかを選択します。

Event Viewer からの Security Manager ポリシーの検索

Event Viewer では、イベントが IPS シグニチャ ポリシーまたは明示的なアクセス ルールに関連する特定のアクション（アクセスの拒否など）から生成されたものである場合、そのイベント自体から関連するシグニチャまたはアクセス ルールを迅速に特定できます。

ポリシー検索を実行する主な理由は、ポリシーが生成しているイベントに基づいてポリシーを調整することです。たとえば、アクセスルールにより、実際には許可すべきトラフィックがドロップされることがあります。イベントが表示中であるため、そのイベントを発生させているポリシーがあることがわかります。数回のクリックで、そのイベントから再設定する必要があるポリシーにたどり着くことができます。

次のタイプのイベントからポリシーを検索できます。

- ファイアウォール イベント：次の syslog メッセージのポリシーを検索できます。
  - 106023：IP パケットの拒否。
  - 106100：ACL による許可/拒否。
  - 302013：TCP の確立（TCP セッションの開始）。
  - 302015：UDP の確立（UDP セッションの開始）。
- IPS アラート イベント：有効なシグニチャ識別子およびサブシグニチャ識別子が設定されているすべての IPS イベント。

ヒントおよび注意事項

- IPv6 アドレスを含むイベントではファイアウォール ポリシーを検索できません。ただし、IPv6 アドレスの IPS ポリシーは検索できます。
- ポリシーが IP アドレスのみに基づいており、イベントを発生させたユーザ名に基づいていない場合、デバイスは Active Directory 内の IP アドレスを検索し、ユーザ名がその IP アドレスに関連付けられている場合、ユーザ名が syslog に追加されます。したがって、ポリシーにユーザ名が含まれていなくても、生成される syslog には含まれている可能性があります。ポリシーは宛先ユーザでは作成できないため、このフィールドはポリシーの検索時には使用されません。
- イベントが送信元 FQDN/宛先 FQDN に基づいて設定されたポリシーに対して生成された場合、生成される syslog には、デバイス障害のため FQDN が含まれません。こうした場合には、ポリシーの検索は機能しません。
- イベントがユーザ グループに基づいたポリシーに対して設定された場合には、syslog には、ユーザ グループではなくイベントを発生させた特定のユーザ名が含まれます。こうした場合には、ポリシーの検索は機能しません。
- syslog 106023 イベントおよび 106100 イベントからポリシー検索を正常に完了するには、ハッシュ コードが必要です。このようなハッシュ コードは、Security Manager を使用して設定を展開した場合にだけ使用できます。ポリシー検索が失敗した場合は、設定を（デバイスまたはファイルに）展開してから、ポリシー検索を再度試してみてください。
- フィルタをデバイスのポリシーテーブルに適用し、イベントを生成したルールまたはシグニチャが現在のビューからフィルタリングされている場合、Security Manager ではそれを強調表示できません。フィルタをクリアしてからやり直してください。

- アクセスルールの最後に配置された暗黙の **deny any** など、イベントが暗黙のルールによって生成された場合、Security Manager ではそのルールを強調表示できません。アクセス リストの最後に明示的な deny any ルールを作成するようにすると効果的です。
- ターゲット ポリシーは、デバイスが共有ポリシーを使用している場合も含め、常にデバイス ビューにあります。必要に応じてデバイス ビューを開いてポリシーを強調表示します。
- IPS シグニチャの場合、そのシグニチャがデフォルト シグニチャである場合には編集できないことがあります。
- アクセス ルールの場合、選択したルールがイベントの最適な一致となります。ルールに重複する部分があったり、ルールが冗長であったりすると、複数のルールが同じイベントを生成することがあります。このような場合、選択したルールを編集しても、後続のルールで同じアクションが実行される可能性があるため、イベントが完全には削除されないことがあります。アクセス ルール ツールを使用して、重複するルールを分析し、結合します。
- アクセス ルールの場合、セッション確立中に複数のルールがパケットを許可することがありますが、最初のルールだけが強調表示されます。
- 組織がアクセスの制御に ACS を使用している場合、ポリシー検索を実行するためには、デバイスに対するデバイスの表示権限、およびファイアウォールまたは IPS ポリシーに対する表示権限も持っている必要があります。ユーザがすべての権限を持っていない場合は、一致ルールの検索を試みたときに「Unable to Find Matching Rule」エラーが発生します。

ステップ 1 Event Viewer でイベントを右クリックし、[ポリシーに移動（Go To Policy）] を選択します。

ヒント テーブルで [Event Name] セルを確認することにより、イベントからポリシーを検索できるかどうかを識別できます。イベント名の前に双眼鏡アイコンがある場合は、ポリシーを検索できます。また、[Go To Policy] コマンドがグレーになっている場合、そのタイプのイベントではポリシーを検索できません。

ステップ 2 Security Manager は、デバイスの関連するアクセス ルールまたは IPS シグニチャを検索し、ポリシー テーブルで該当する項目を強調表示します。ここから、表示または変更するポリシーを編集できます。詳細な手順については、アクセス ルールの設定およびシグニチャの設定を参照してください。

変更内容は、更新した設定を送信し、展開するまで有効になりません。

Looking Up Events for a Cisco Security Manager Policy

特定のファイアウォール アクセス ルールまたは IPS シグネチャに関連するイベントをイベントビューアで検索できます。ヘルスとパフォーマンスのモニタで、特定のデバイスまたはサイト間トンネルに関連するイベントを検索することもできます。

イベントビューアがイベントを受信すると、イベントは解析され、「セッション化」されて、イベントバッファに書き込まれてから、データベースに書き込まれます。セッション化には 2

つの形式があります。セッション指向プロトコル（TCPなど）では、セッションには初期ハンドシェイクから接続のティアダウンまでが含まれます。セッションレス プロトコル（UDP など）では、セッションの開始時刻と終了時刻は、制限された時間内で追跡される最初と最後のパケットに基づきます。時間外のパケットは、他のセッションの一部と見なされます。

新しく受信したデータと完全に処理されたデータには違いがあるため、リアルタイムイベントまたは過去イベントのいずれも検索できます。

- [リアルタイム（Real-time）]：イベントをキャッシュ内に最大2分間保持するためセッション化には時間がかかります。そのため、リアルタイム イベント クエリーを使用して解析直後にイベントを表示し、受信した最新データへのアクセスを可能にします。
- 履歴（Historical）]：過去のイベントのレポートは、リアルタイムモニタリングで可能な期間よりも長期にわたる傾向を識別するのに役立ちます。過去のイベントの場合、[Result Format] は [All Matching Events] オプションであり、[Filter By Time] 値は過去 10 分に設定されます。

次の項では、イベント検索についてより詳細に説明します。

- アクセスルールのイベントの表示　（71 ページ）
- IPS シグニチャのイベントの表示　（73 ページ）
- HPM デバイスとサイト間 VPN のイベントの表示　（74 ページ）

アクセスルールのイベントの表示

Security Manager の [ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] ポリシーから、アクセスルールを選択し、イベントビューアの関連するイベント情報を表示できます。ルールに一致するリアルタイムまたは過去のイベントを表示できます。ASA（ASA-SM を含む）および FWSM デバイスのイベントを表示できます。

ファイアウォール アクセス ルールは、順序が付けられたリストまたは表の形式で提供されます。展開されると、このポリシーはAccess-Control List（ACL; アクセス コントロール リスト）となります。リスト内の各エントリは、Access-Control Entry（ACE; アクセス コントロール エントリ）と呼ばれます（詳細については、アクセス ルールについてを参照してください）。

パケットを転送するかドロップするかを決定するときに、デバイスは、リストされている順序で各アクセス ルールに照らしてパケットをテストします。アクセス ルールに対してロギングをイネーブルにすると、テストの結果はルールごとのログ設定に従って記録されます。ASA などの一部のデバイスでは、ロギングを明示的に設定しない場合でも、拒否されたアクセスのログ エントリが生成されます。ロギング オプションを含むアクセス ルールの作成の詳細については、アクセス ルールの設定を参照してください。

（[Advanced]/[Edit Options] ダイアログボックスで）ルールに対してロギングが有効な場合、イベントをログに記録するために、デバイスはイベントビューアにsyslogメッセージを送信します。このクエリーには、使用可能なキーワード情報などのアクセス ルール パラメータが含まれています。レポートされるイベントには、接続の設定およびティアダウンは含まれません。

ルール関連のイベントを表示するには、次の右クリック コマンドを使用します。

- **Show Events > Realtime**：このルールに一致するイベントのリアルタイムクエリ結果をイベントビューアに表示します。いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。
- **Show Events > Historical**：このルールに一致するイベントの履歴クエリ結果をイベントビューアに表示します。いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、履歴結果を変更できます。

アクセスルール イベント クエリの基準として、Security Manager からイベントビューアに次の情報が提供されます。

- [Device details]：ホスト名、ドメイン名、管理 IP アドレス、表示名などのデバイスに関する一般情報。
- [Source addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの送信元アドレス。
- [Destination addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの宛先アドレス。
- [Service]：プロトコルおよびポート情報。
- [イベントタイプ（Event Type）]：許可ルールの場合は「構築/ティアダウン/許可された IP 接続」、拒否ルールの場合は「セキュリティポリシーによってパケットを拒否」。

（注）

- 一度に照会できるアクセス ルールは 1 つだけです。
- セキュリティデバイスで NAT または PAT が設定されている場合、送信元アドレスと宛先アドレスは変換前および変換後のアドレスにそれぞれマッピングされ、Security Manager からイベントビューアにクエリーが送信されるときは変換後のアドレスが使用されます。インバウンド アクセス ルールの場合、宛先アドレスは変換前アドレスと見なされ、アウトバウンド アクセス ルールの場合、送信元アドレスは変換後アドレスと見なされます。
- 複数のサービス（UDP、TCP、ICMP など）でフィルタリングすると、正確な結果が得られない場合があります。この問題を回避するには、イベントビューアの起動後に一部のフィルタを削除します。
- ICMP サブタイプに基づくフィルタリングはサポートされていません。たとえば、ACE で「ICMP Echo」が稼働している場合、フィルタはプロトコル（ICMP）にのみ適用され、イベントビューアのタイプカラム（Echo）には適用されません。
- 「eq」、「neq」、「gt」、および「lt」のサービスポートは、イベントビューアへのクロス起動ではサポートされていません。

関連項目

- [Access Rules] ページ

• Looking Up Events for a Cisco Security Manager Policy （70 ページ）
• IPS シグニチャのイベントの表示 （73 ページ）
• HPM デバイスとサイト間 VPN のイベントの表示 （74 ページ）

IPS シグニチャのイベントの表示

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

着信トラフィックを設定済みのシグニチャと比較することにより、IPS デバイスによってネットワーク侵入が検出およびレポートされると、デバイス上で syslog メッセージが生成されます。デバイスが Security Manager によってモニタされている場合、シグニチャに関連付けられたログがデバイスから取得されたあと、イベントビューアでインシデントが生成されます。特定のシグニチャに関連付けられたイベントを検索すると、攻撃を迅速に識別し、デバイス設定を調整して侵入を最小限に抑えるか、または防止できます。

レポートされたネットワーク侵入イベントをイベントビューアで表示するには、Security Manager のデバイスのシグネチャポリシーで 1 つ以上のエントリを選択し、イベントビューアに移動してリアルタイムイベントおよび過去のイベントを表示します。

関連項目

• Looking Up Events for a Cisco Security Manager Policy （70 ページ）
• アクセスルールのイベントの表示 （71 ページ）
• HPM デバイスとサイト間 VPN のイベントの表示 （74 ページ）

ステップ 1 （デバイスビュー）IPS デバイスを選択して、[IPS]>[シグネチャ（Signatures）]>[シグネチャ（Signatures）] を選択し、[Signatures] ページを表示します。

ステップ 2 シグニチャテーブルで目的のエントリを右クリックするか、または複数のエントリを選択してそのうちの 1 つを右クリックし、[イベントの表示（Show Events）] メニューから次のコマンドのいずれかを選択します。

• [Realtime（リアルタイム）]：このシグニチャに一致するイベントのリアルタイムクエリ結果をイベントビューアに表示します。イベントビューアへのストリーミング中の未処理イベントを表示するには、このオプションを使用します。

いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

• [履歴（Historical）]：このシグニチャに一致するイベントの履歴クエリ結果をイベントビューアに表示します。

いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、結果を変更できます。

ヒント：

- シグニチャがディセーブルの場合、警告が表示され、イベント検索に進むかどうかが確認されます。
- タイプが Packet Data および Context Data のイベントはシグニチャ ルールによってトリガーされないため、これらのイベントはクエリー結果に表示されません。

HPM デバイスとサイト間 VPN のイベントの表示

Health and Performance Monitor から、監視対象デバイスのイベント、またはトンネルアップ/ダウンイベントが発生したサイト間 VPN のイベントにすばやくアクセスできます。

監視対象デバイスのイベントを表示するには、[すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[IPSデバイス（IPS Devices）]、[優先デバイス（Priority Devices）]、またはカスタムデバイス関連のビューからデバイスを選択し、デバイスの詳細領域で [概要（Summary）] タブを選択して、[イベントの表示（View Events）] ボタンをクリックします。イベントビューアが開き、[イベントモニタリング（Event Monitoring ）] ウィンドウに、選択したデバイスでフィルタリングされたイベントと、スライダバーで指定された期間が一覧表示されます。

トンネルのアップ/ダウンイベントが発生したサイト間 VPN の関連イベントを表示するには、次のいずれかを実行します。

- サイト間トンネルビューで、[ステータス（Status）] 列の [ダウン（Down）] 通知ハイパーリンクをクリックします。
- アラートビューで、トンネルアップ/ダウンアラートの [説明（Description）] 列のハイパーリンクをクリックします。

イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のアップ/ダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。

関連項目

- 正常性とパフォーマンスのモニタリングの準備
- Looking Up Events for a Cisco Security Manager Policy （70 ページ）
- アクセスルールのイベントの表示 （71 ページ）
- IPS シグニチャのイベントの表示 （73 ページ）

イベント分析の例

多種多様な手法を使用して、ネットワーク デバイスが生成したイベントを分析して対応できます。ここで示す例を参照すると、Security Manager の Event Viewer で実行できる操作の一部が理解しやすくなります。

ここでは、次の内容について説明します。

ヘルプ デスク：サーバへのユーザ アクセスがファイアウォールでブロックされている

この例では、ヘルプ デスクがサーバにアクセスできないユーザから電話を受けます。

ユーザがサーバにアクセスできない場合、次に示すように数多くの理由があります。

- ネットワークのサーバー側の問題。サーバーがダウンしている、ネットワーク接続が確立されていない、ポリシーによってサーバーのファイアウォールがアクティブにアクセスが禁止されているなど。
- ユーザとサーバ間のネットワーク クラウドの問題。ルーティングなど。
- ユーザーのネットワークの問題。ワークステーションの問題、ネットワーク接続に関する物理的な問題（ワイヤの破損など）、スイッチポートまたはワイヤレスアクセスポイントに関する問題、DNS ルックアップの失敗など。

Security Manager の Event Viewer では、このような問題を特定して解決することができません。ただし、制御しているファイアウォールがサーバへのアクセスをブロックしているかどうかはわかります。これにより、問題の発生源であるとしてファイアウォールを取り外すか、またはファイアウォールがアクセスをブロックしている場合には問題を修正したり、ポリシーに基づいてサーバがブロックされていることをユーザに通知したりできます。

この手順では、まずサーバへのアクセスがポリシーで拒否されていないことを確認し、ファイアウォールはサーバへのアクセスを許可する必要があるものと想定しています。

ステップ 1 ユーザにワークステーションおよびサーバの IP アドレスを確認します。

ステップ 2 イベントビューアを開きます。たとえば、Configuration Manager で **[起動（Launch）] > [イベントビューア（Event Viewer）]** を選択します。

ステップ 3 [ファイアウォールトラフィックイベント（[Firewall Traffic Events）] ビューをダブルクリックして開きます。必要に応じて、ワークステーションに関連する IPS イベントの有無も確認する場合は、[すべてのデバイスイベント（All Device Events）] ビューを使用できます。

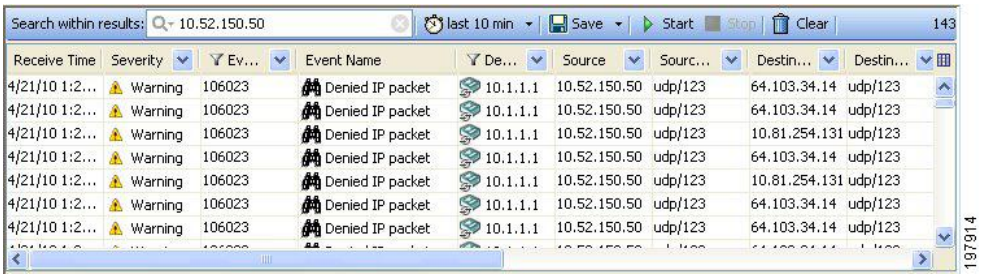
ヒント また、[ファイアウォール拒否イベント（Firewall Denied Events）] ビューを選択して、拒否されたイベントだけを表示できます。ただし、ユーザーのワークステーションに関連する他のイベントも確認することを推奨します。

ステップ 4 ユーザにサーバへのアクセスを再試行するように求めます。

ステップ 5 [開始（Start）] ボタンをクリックするか、または [表示（View）] > [開始（Start）] を選択し、イベントテーブルを更新して、最新のイベントを表示します。

ステップ 6 [結果内の検索（Search within Results）] ボックスにユーザーの IP アドレスを入力します。入力した内容に従ってイベントのリストがフィルタリングされ、いずれかのカラムに検索文字列が存在するイベントが表示されます。次の図のイベント リストには、過去 10 分間に発生した IP アドレス 10.52.150.50 に関するイベントがすべて表示されています。

図 *5：1* つの *IP* アドレスに限定したイベント リスト



ヒント また、[送信元（Source）] 列のドロップダウンリストから IP アドレス、および [宛先（Destination）] 列のドロップダウンリストからサーバーの IP アドレス（またはその逆）を選択して、関心のある送信元と宛先に関するイベントだけを表示できます。検索文字列ではイベントリストを十分に絞り込めないために分析が容易ではない場合には、カラム フィルタを使用します。

ステップ 7 ユーザーのワークステーションからサーバーに向かうトラフィック、またはサーバーからワークステーションに向かうトラフィックが拒否されたことを示すイベントを探します。syslog **106xxx** メッセージは、拒否アクションを示します。

テーブルでイベントを選択し、ウィンドウの一番下に [Event Details] ペインを開きます。このペインのタブには、メッセージ情報全体が表示され、わかりやすい説明と推奨するアクションが示されます。

ステップ 8 イベントがメッセージ **106023** または **106100** の場合は、接続を拒否しているアクセスルールを容易に特定して修正できます。テーブルで [Event Name] セルを確認することにより、イベントからポリシーを検索できるかどうかを識別できます。イベント名の前に双眼鏡アイコンがある場合は、ポリシーを検索できます。また、[Go To Policy] コマンドがグレーになっている場合、そのタイプのイベントではポリシーを検索できません。

ヒント アクセスリストの最後で暗黙の **deny any** ルールのためにトラフィックが拒否されている場合、Go To Policy コマンドではそのルールに移動できません。ルール検索のヒントについては、Event Viewer からの Security Manager ポリシーの検索 （68 ページ）を参照してください。

a) イベントを右クリックし、[Go To Policy] を選択します。ルールが選択された状態でデバイス ビューが表示されます。一致するルールが見つからない場合には通知されます。

b) 目的のアクセスが許可されるようにルールを変更します。そのためには単にルールを削除するだけでよい場合もあれば、具体的に宛先サーバとのトラフィックを許可する新規ルールを追加することが必要になる場合もあります（拒否ルールよりも上位に許可ルールを配置します）。組織のセキュリティポリシーによって、許容される変更が決まります。アクセス ルール ポリシーの設定の詳細については、アクセス ルールの設定を参照してください。

c) 更新した設定をデバイスに送信して展開します。展開プロセスの詳細については、Workflow 以外のモードでの設定の展開またはWorkflow モードでの設定の展開を参照してください。

展開が正常に完了するまで待機します。

ステップ 9 ユーザにサーバへのアクセスを再試行するように求めます。アクセスが再度拒否される場合は、イベントビューアで[開始（Start）]をクリックしてイベントリストを更新し、最新の拒否イベントを探します。

ヒント サーバとの通信を拒否するアクセス ルールが複数存在する場合もあります。アクセス ルール ポリシーは上から下に順に処理されるため、アクセスを阻止するルールを削除すると、それまで適用されていなかったルールが突然アクティブになることがあります。アクセス ルール ポリシーがきわめて長い場合には、ルールをいくつか順に削除していくことが必要になる場合があります。このほか、Rule Combiner ツールを使用して、アクセス ルール ポリシーを統合して簡素化する方法もあります。詳細については、ルールの結合を参照してください。

ステップ 10 ファイアウォールがアクセスをブロックしなくなるまで、アクセス拒否イベントの解決を続けます。

ヒント また、Packet Tracer ツールを使用して、ASA デバイスを経由してワークステーションからサーバに流れるトラフィックをシミュレートすることもできます。デバイスビューで、アクセスを拒否しているデバイスを右クリックし、[パケットトレーサ（Packet Tracer）] を選択します。詳細については、Packet Tracer を使用した ASA または PIX の設定の分析を参照してください。

すべてのイベントを解決したあとも、ユーザがサーバに到達できない場合、ファイアウォールはアクセスをブロックしているネットワーク要素の 1 つではないということになります。他の仲介ネットワーク デバイスを検討してみてください。トラフィックをブロックするアクセス ルールがルータに組み込まれていることなどが考えられます。

ボットネット アクティビティのモニタリングと軽減

Botnet Traffic Filter についての説明に従ってボットネット トラフィック フィルタリングを設定したあと、そのフィルタリングをモニタし、ネットワークで明らかになった問題の解決にあたることを推奨します。以降の項での説明に従って、Security Manager および ASDM を使用して、ボットネット アクティビティをモニタし、明らかになった問題を軽減できます。

- Adaptive Security Device Manager（ASDM）を使用したボットネット アクティビティのモニタリング （81 ページ）
- ボットネット トラフィックの軽減 （82 ページ）

対処可能なイベントであることを示す syslog メッセージについて

ボットネット トラフィック フィルタ イベントは、syslog メッセージ番号 338xxx を使用します。ただし、メッセージの中には単なる情報であり、メッセージに対するアクションが必要ないものもあります。

ボットネット イベントの syslog を表示するときには、次のメッセージ番号に特に注意してください。ブロックリストに掲載または許可されたトラフィックであることを示すメッセージの処理の詳細については、 ボットネット トラフィックの軽減 （82 ページ）を参照してください。syslog メッセージの詳細については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html で、ご使用の ASA ソフトウェアバージョンの Syslog メッセージ [英語] を参照してください。

- **338001 ～ 338004**：ASA がログに記録しているブロックリスト掲載のトラフィックを停止していないことを示します。進行中のボットネットアクティビティを停止する場合には、このようなメッセージに早急に対処する必要があります。
- **338005 ～ 338008**：ASA がログに記録し、ドロップしているブロックリスト掲載のトラフィックであることを示します。これは、トラフィックが廃棄ルールに該当したことを示します。したがって、ネットワークは保護されています。ただし、攻撃対象のコンピュータから感染を除去する必要があります。
- **338201、338202**：ASAがログに記録し、ドロップしていないグレーリスト掲載のトラフィックであることを示しますこのようなメッセージは、早急な対処を必要とするアクティブなボットネット接続であることを示す場合があります。
- **338203、338204**：ASAがログに記録し、ドロップしているグレーリスト掲載のトラフィックであることを示します。ネットワークは、このトラフィックから保護されています。ただし、グレーリスト掲載のサイトが正規のサイトである場合は、トラフィックがドロップされていること自体が早急の対処を必要とする問題であることがあります。グレーリスト掲載のアドレスが正規のアドレスであり、設定を再展開する場合は、スタティック データベースへのエントリの追加の説明に従ってそのアドレスを許可リストに追加できます。
- **338305 ～ 338307、338310**：ASA が動的なフィルタデータベースをダウンロードできませんでした。デバイスに DNS ルックアップを設定しており、Cisco Intelligence Security Operations Center にルーティング可能なネットワーク パスがあることを確認してください。Cisco Technical Support への問い合わせが必要になる場合があります。
- **338309**：ボットネット トラフィック フィルタ ライセンスが最新ではないため、動的なデータベースをダウンロードできません。適切なライセンスを購入してインストールしてください。ボットネット トラフィック フィルタ ライセンスは時間ベースであるため、有効なライセンスが期限切れになった可能性があります。

Security Manager の Event Viewer を使用したボットネットのモニタリング

Event Viewer アプリケーションを使用して、ASA デバイスが生成した syslog イベントをモニタできます。Event Viewer には、発生したばかりのボットネット イベントを表示する定義済みのビューがあります。

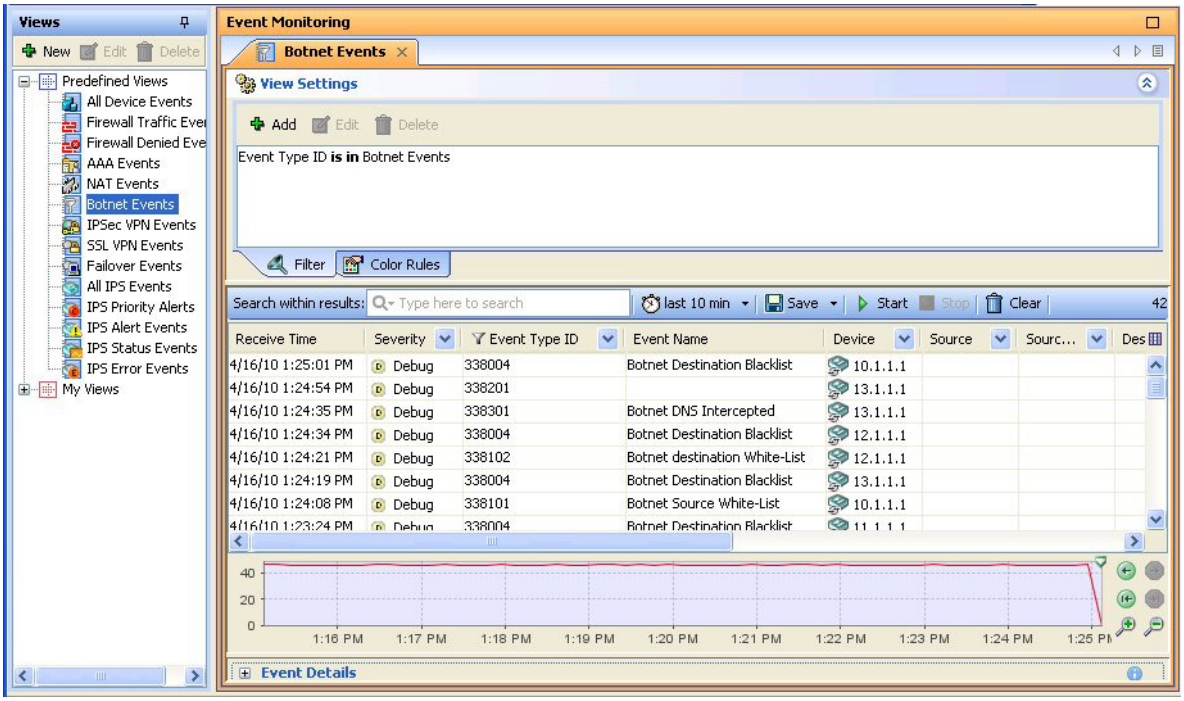
ボットネット メッセージはデバッグ重大度を知らせる情報であり、338xxx の番号が付与されています。

ヒント この手順では、Event Manager サービスがイネーブルになっていることを想定しています。そうでない場合は、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [イベント管理（Event Management）] ページを使用してイネーブルにします。

ステップ 1 イベントビューアを開きます。たとえば、Configuration Manager で **[起動（Launch）] > [イベントビューア（Event Viewer）]** を選択します。

ステップ 2 左ペインにある定義済みのビューのリストから、[ボットネットイベント（Botnet Events）] をダブルクリックします。ビューをダブルクリックしてアクティブにし、右ペインにロードする必要があります。ビューが開いていることを確認するには、右ペインでビューのタブ名が「Botnet Events」であることを確認します。次の図に、ボットネットイベントビューの一例を示します。

図 *6 : Security Manager の Event Viewer* へのボットネット イベント ビュー

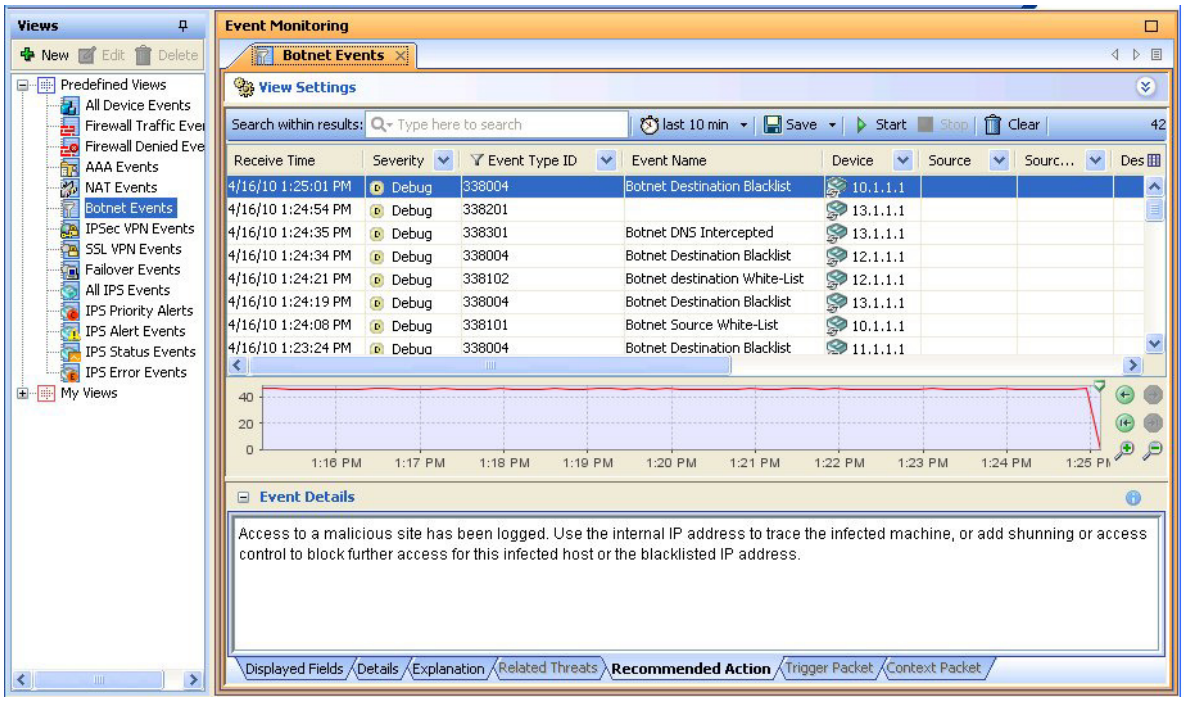


ステップ 3 特定のイベントの詳細を参照するには、テーブルでそのイベントを選択します。続いて、次の手順を実行します。

- イベントをダブルクリックして、読みやすい表形式で情報を表示します。
- ウィンドウの一番下に[イベントの詳細（Event Details）]セクションを開きます。詳細ペインには、イベントに関する情報がタブに編成されて表示されます。[Explanation] タブおよび[Recommended Action] タブには、イベントに関する情報と、イベントへの推奨の対処方法がわかりやすく示されています。

次の図に、Botnet Destination Blocklist メッセージ 338004 の [イベントの詳細（Event Details）] ペインを示します。この例には、推奨するアクションが表示されています。このメッセージの説明には、「This syslog message is generated when traffic to an IP address in the block list in the dynamic filter database appears.」（この syslog メッセージは、ダイナミック フィルタ データベース内のブロックリストの IP アドレスへのトラフィックが発生した場合に生成されます）とあります。このタイプのイベントの詳細については、ボットネット トラフィックの軽減 （82 ページ）を参照してください。

図 *7: Botnet Destination Blocklist* メッセージ *338004* に関するボットネットイベントの詳細



ステップ 4 イベント リストの対象を単一の ASA が生成したイベントに絞り込むには、[Device] カラムのドロップダウン矢印をクリックし、リストから目的のデバイスを選択します。リストの対象を複数の ASA に絞り込む場合は、ドロップダウン リストから [Custom] を選択し、表示されたダイアログボックスで目的のデバイスを選択します。

他のカラムに対するフィルタを使用して、リストを絞り込むこともできます。フィルタリングは、どのカラムでも同じように機能します。ドロップダウン リストから目的の値を選択するか、または [Custom] を選択してさらに複雑なカラム フィルタを作成します。

Security Manager の Report Manager を使用したボットネットのモニタリング

Report Managerアプリケーションを使用して、ボットネットアクティビティのレポートを生成できます。定義済みレポートがあり、上位の感染したホスト、上位のマルウェアポート、および上位のマルウェアサイトが示されます。これらのレポートの詳細については、ファイアウォール サマリー ボットネット レポートについてを参照してください。

ヒント　この手順では、Event Managerサービスがイネーブルになっていることを想定しています。そうでない場合は、[ツール（Tools）]>[Security Managerの管理（Security Manager Administration）]>[イベント管理（Event Management）]ページを使用してイネーブルにします。

ステップ1　Report Managerを開きます。そのためには、たとえば、Configuration Managerで[起動（Launch）]>[Report Manager]を選択します。

ステップ2　[システム（System）]>[FW]>[サマリーボットネット（Summary Botnet）]フォルダから目的のレポートを開きます。レポートを開くには、レポートをダブルクリックするか、レポートを右クリックして、[レポートを開く（Open Report）]を選択します。

ステップ3　（任意）目的の時間範囲およびデバイスを選択してレポートに含めるために、レポートをカスタマイズします。詳細については、レポート設定の編集を参照してください。

今後そのレポートを再生成するためにカスタム設定を保存するには、[名前を付けて保存（Save As）]をクリックしてカスタムレポートを作成します。詳細については、カスタム レポートの作成を参照してください。

ステップ4　[レポートの生成（Generate Report）]をクリックして収集した情報を取得して、グラフおよび表形式データで表示します。詳細については、レポートの起動と生成を参照してください。

定期的にレポートを生成する場合は、レポート スケジュールの設定で説明するとおりに、スケジュールを設定できます。

Adaptive Security Device Manager（ASDM）を使用したボットネット アクティビティのモニタリング

Adaptive Security Device Manager（ASDM）には、ボットネット レポート機能が含まれています。ASDMの読み取り専用バージョンがデバイス マネージャとしてSecurity Managerクライアントとともにインストールされ、Security Manager内からASDMを起動できます。

ヒント　完全な形の ASDM アプリケーションを別途インストールすることもできます。ただし、ASDM で実施した設定変更は、Security Manager ではアウトオブバンド変更であると見なされ、次回 Security Manager から設定を展開すると上書きされます。それでも ASDM を使用して設定変更を実施する必要がある場合は、その設定の Security Manager のビューが最新のものとなるように、Security Manager でデバイスに対するポリシーを再検出してください。

ステップ 1　Configuration Manager のデバイス ビューで ASA デバイスを選択します。

ステップ 2　**[起動（Launch）] > [Device Manager]** を選択して、ASA への ASDM 接続を開きます。設定変更が実施できないことが警告されます。[はい（Yes）] をクリックして続行します。

ステップ 3　ASDM で、次の領域のボットネット トラフィック フィルタ モニタリング情報を参照します。

- **[ホーム（Home）] > [ファイアウォールダッシュボード（Firewall Dashboard）]** には、ボットネット トラフィック フィルタの概要があります。
- **[モニタリング（Monitoring）] > [ボットネットトラフィックフィルタ（Botnet Traffic Filter）] > [レポート（Reports）]**には、上位のボットネットサイト、ポート、および感染したホストに関するチャートが含まれています。
- **[モニタリング（Monitoring）] > [ロギング（Logging）] > [ログバッファ（Log Buffer）]** には、syslog メッセージの履歴が表示されます。
- **[モニタリング（Monitoring）] > [ロギング（Logging）] > [リアルタイムログビューア（Real-Time Log Viewer）]** は、syslog メッセージが生成されたままの状態で表示されます。

ヒント　**[設定（Configure）] > [ボットネットトラフィックフィルタ（Botnet Traffic Filter）] > [ボットネットデータベース（Botnet Database）]**ページで、動的なデータベースを検索することもできます。このページではこのほか、手動でデータベースのダウンロードを開始したり、動的なデータベースを消去したりすることもできます。これらのアクションは、デバイスの設定を変更しません。Security Manager でポリシーを再検出する必要もありません。

ボットネット トラフィックの軽減

ボットネット トラフィックの軽減は、次の 2 つの手順からなります。

1. ネットワークからボットネット制御サイトへのトラフィックを停止する。
2. 攻撃対象のコンピュータから感染を除去する。

次の手順では、このプロセスをさらに詳しく説明します。

ステップ 1　好ましくないアドレスとの間でパケットがやり取りされていることを示すsyslogイベントが表示されます。一般には、メッセージ番号 338001 ～ 338008 または 338201 ～ 3382004 です。このようなメッセージの詳細

については、 対処可能なイベントであることを示す syslog メッセージについて （78 ページ）を参照してください。

ヒント メッセージ 338201 ～ 3382004 はグレーリスト掲載のトラフィックです。トラフィックを停止する前にまず、グレーリスト掲載のトラフィックが本当に好ましくないものであるかどうかを判断します。

ステップ 2 ボットネット トラフィックを停止します。

- メッセージ 338005 ～ 338008 および 338203 ～ 338204 は、ASA がトラフィックをすでにドロップしていることを示します。トラフィック分類ドロップルールは、ブロックリストまたはグレーリストに含まれているアドレスを対象とします。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化を参照してください。
- メッセージ 338001 ～ 338004 および 338201 ～ 338202 は、ASA がイベントをログに記録しているものの、トラフィックをドロップしていないことを示します。まずはこのトラフィックを停止する必要があります。

廃棄ルールのために ASA がまだボットネット トラフィックをドロップしていない場合には、ボットネット トラフィックを停止するためのオプションとして次のものが用意されています。

- （推奨の方法）。ボットネットサイトのドロップルールを設定し、設定を再展開します。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化を参照してください。
- （2 番目に推奨の方法）。SSH クライアントを使用して ASA にログインし、特権 EXEC モードを開始し、**shun** コマンドを使用してボットネットサイトとの間でやり取りされるトラフィックを阻止します。このコマンドは CLI ウィンドウで ASDM から発行することもできますが、Security Manager からは発行できません。shun コマンドは、トラフィックをブロックする永続的なルールを作成するものではありません。

たとえば、ボットネット サイトが 10.1.14.14 で、内部の感染したコンピュータが 10.100.10.10 である場合は、次のコマンドを発行します。最初のコマンドはボットネット コマンドセンターからの着信トラフィックをすべてブロックし、2つめのコマンドはボットネットサイトに感染したコンピュータからのトラフィックをブロックします。

shun 10.1.14.14

shun 10.100.10.10 10.1.14.14

- (Not recommended.) shun コマンドを推奨しますが、ボットネットサイトとの間でやり取りされるトラフィックを拒否する永続的なルールをインターフェイスのアクセス制御リスト（ACL）に作成することもできます。Cisco Security Manager でデバイスを選択した状態で、**[ファイアウォール（Firewall）] > [アクセスルール（Access Rule）]** を選択し、ルールを 2 つ作成します。1 つは宛先アドレスに関係なく、送信元アドレスであるボットネットサイトを拒否するルール、もう 1 つはボットネットサイトが宛先アドレスである送信元アドレスをすべて拒否するルールです。サービスの場合、すべてのトラフィックがブロックされるように IP を選択します。ルールを有効にするには、設定を展開する必要があります。

アクセス ルールを作成する方法は推奨しません。ボットネット サイトが一時的なものであるのに対して、永続的なルールを作成するためです。このタイプのネットワーク攻撃には、従来のアクセス ルールより

も、ボットネット トラフィック フィルタを使用してボットネット トラフィックを動的にブロックする方が適しています。

ステップ 3 感染したコンピュータに対するネットワーク アクセスをシャットダウンします。たとえば、コンピュータが接続されているスイッチポートを特定し、スイッチの CLI を使用してそのポートをシャットダウンします。問題のコンピュータが他にワイヤレスアクセスを備えている場合もあるため、ネットワーク アクセスを完全にシャットダウンするのは簡単な作業であるとはかぎりません。

ステップ 4 攻撃対象のコンピュータの所有者にそのコンピュータが感染していることを通知し、IT 担当者を派遣してコンピュータから感染を除去します。コンピュータから感染を除去するためのツールおよび手法については、このマニュアルでは取り上げません。

イベント テーブルからの false positive IPS イベントの削除

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

ある特定のパケットまたは一連のパケットが、IPS シグニチャに定義されている既知の攻撃プロファイルの特性に一致すると、IPS アプライアンスまたはサービス モジュール（IPS デバイス）がアラームをトリガーします。IPS が良性のアクティビティを悪意のあるアクティビティであるとレポートした場合、false positive（良性のトリガー）が発生します。各イベントの診断には人手の介入が必要であるため、false positive イベントの分析に時間をかけると、リソースが大量に消費されます。

悪意のあるアクティビティの検出に使用される IPS シグニチャの性質により、IPS の有効性を大幅に低下させたり、組織のコンピューティングインフラストラクチャ（ホストやネットワークなど）を大きく混乱させたりすることなく、false positive を完全に排除することはほぼ不可能です。IPS の展開時に独自に調整を実施すると、false positive が最小限に抑えられます。コンピューティング環境が変更されたとき（新規にシステムやアプリケーションを展開するときなど）には、定期的に再調整を実施する必要があります。IPS デバイスは柔軟な調整機能を備えており、定常状態の動作中に false positive が発生するのを最小限に抑えることができます。

false positive の一例が、ping スイープを実行してネットワーク検出マップを定期的に構築するネットワーク管理ステーションです。ping スイープは、ICMP Network Sweep with Echo シグニチャ（シグニチャ ID 2100）をトリガーします。このため、送信元アドレスがネットワーク管理ステーションの IP アドレスとなっている ICMP Network Sweep with Echo イベントは、実際には想定どおりの望ましいイベントです。

Event Viewer のイベント テーブルから false positive IPS イベントを削除するときには、次のオプションが用意されています。

- **既知の「クリーンな」ソースからイベントを除外します。**

イベントを除外すると、イベントが生成されなくなるのではなく、テーブルにイベントが表示されなくなります。イベントは引き続き使用できるため（フィルタを削除できます）、特定の

ネットワーク動作を調べるには除外されたホストからのアクティビティを確認する必要がある場合には、イベントを参照できます。

この手法の使用には、主に次の 2 つの欠点があります。

- イベントは引き続き生成されて、イベント ストアに追加されます。
- フィルタは、ホストからすべてのイベントを除外します。ホスト/シグニチャ ID のペアを除外する複雑なフィルタは作成できません。

次の手順では、クリーンであると識別した送信元からのイベントを除外する方法を示します。

- **false positive イベントの生成を阻止するイベント アクション フィルタ ルールを作成します。**

イベント アクション フィルタ ルールは、イベントの生成を阻止するための最も簡単な方法です。また、作業が難しくなるシグニチャの編集やカスタム シグニチャの作成にも、この方法を推奨します。イベント アクション フィルタ ルールでホストを除外すると、IPS デバイスはイベントをトリガーしても、アラームを生成せず、ログに記録を残しません。

ホストからすべてのイベントを全面的に除外するのではなく、特定のシグニチャを対象にできるため、良性であるとの確信があるイベントだけを排除できます。たとえば、次のイベント フィルタ ルールは、ネットワーク管理ステーション 10.100.15.75 の ICMP Network Sweep with Echo（2100）シグニチャから Produce Alert アクションを排除します。このネットワーク管理ホストが攻撃者アドレスであると見なされますが、実際にはイベント フィルタ ルールに指定されているアクションが、イベントから削除されるアクションです。他のアラート生成アクションを ICMP Network Sweep with Echo イベントに追加するイベント アクション オーバーライド ルールを作成する場合は、このルールでオーバーライドアクションも削除する必要があることに注意してください。

Name	Active	IDs	Subs	Attackers	Attack Ports	Victims	Victim Ports	Actions	RR	Stop
Local (1 Filter)										
NMS_Ping_Sweep	Yes	2100	0-255	10.100.15.75	0-65535	0.0.0.0-255.255.255.255	0-65535	Produce Alert	0-100	No

196055

イベント アクション フィルタ ルールの設定の詳細については、[Event Action Filters] ページを参照してください。

次の手順では、Event Viewer でフィルタリングを使用して、イベント リストから false positive を削除する方法を示します。ネットワーク/ホスト ポリシー オブジェクトを使用して、フィルタリングを実現します。

ヒント ネットワーク/ホスト オブジェクトを使用して送信元アドレス フィルタまたは宛先アドレス フィルタを作成すると、単にそのオブジェクトの内容を変更するだけでフィルタを更新できます。ビューに対してフィルタを追加または削除する必要はありません。利点にはもう 1 つ、イベント テーブルに現在表示されていないアドレスのフィルタをプロアクティブに作成できることがあります。Event Viewer の送信元/宛先カラム フィルタ コントロールには、イベント リストに現在掲載されているアドレスだけが一覧表示されます。

ステップ 1 クリーンなホストまたはネットワークの IP アドレスが含まれているネットワーク/ホスト ポリシー オブジェクトを作成します。

a) **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] ウィンドウを開きます（Policy Object Managerを参照）。
b) コンテンツテーブルから [ネットワーク/ホスト（Networks/Hosts）] を選択します。
c) ネットワーク/ホストポリシーオブジェクトのテーブルの下にある [行の追加（Add Row）]（+） ボタンをクリックし、オブジェクトタイプとして [グループ（Group）] を選択します。
d) [Add Network/Host Group] ダイアログボックスで IPS_Safe_Hosts などのオブジェクト名を入力します。
e) [IPv4アドレス情報の入力（Enter IPv4 Address Information）] を選択して、10.100.15.75 などの IP アドレスを入力します。
f) [追加>>（Add>>）] をクリックして IP アドレスを [グループ内のメンバー（Members in Group）] リストに追加します。
g) [OK] をクリックしてオブジェクトを作成します。
h) [閉じる（Close）] をクリックして、[Policy Object Manager] ウィンドウを閉じます。

ステップ 2 **[ファイル（File）] > [送信（Submit）]** を選択して、変更内容をデータベースに送信します（Workflow 以外のモード）。新規ポリシー オブジェクトだけでなく、すべての設定変更が送信されることに留意してください。

Workflow モードを使用している場合は、必要に応じてアクティビティを送信し、アクティビティの承認を得る必要があります。

ヒント Event Viewer では、データベースにすでに送信されたポリシー オブジェクトだけを表示できるため、そのオブジェクトを使用してフィルタを作成する場合は事前に変更内容を送信しておく必要があります。あとでポリシー オブジェクトを変更した場合には、そのオブジェクトの新規定義に使用しているフィルタの変更内容も送信する必要があります。

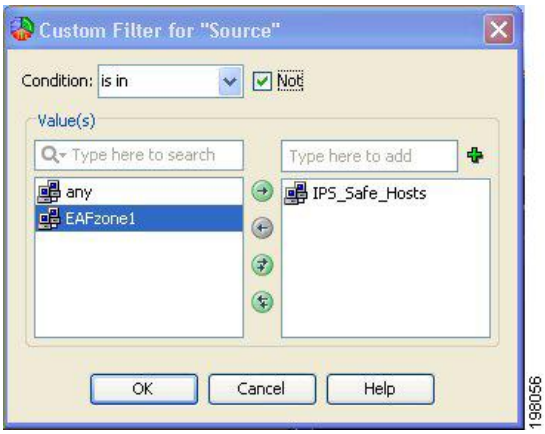
ステップ 3 **[起動（Launch）] > [イベントビューア（Event Viewer）]** を選択して、イベントビューア アプリケーションを開きます。

ステップ 4 ネットワーク管理ステーションを除外するカスタム ビューを作成します。

a) [すべてのIPSイベント（All IPS Events）] など、カスタムビューの土台として使用する定義済みのビューをダブルクリックします。[Views] リストでビューをダブルクリックすると、そのビューが開きます。更新するカスタム ビューがすでにある場合は、そのビューを開きます。
b) イベントテーブルで [ソース（Source）] 列のタイトルにある下向き矢印ボタンをクリックし、[カスタム（Custom）] を選択して [ソースのカスタムフィルタ（Custom Filter for Source）] ダイアログボックスを開きます。

ヒント：このダイアログボックスは、[設定の表示（View Settings）] ペインから開くこともできます。そのためには、[追加（Add）] ボタンをクリックし、[カスタムフィルタを列に追加（Add Custom Filter to a Column）] ダイアログボックスで [ソース（Source）] を選択し、[OK] をクリックします。

c) [Custom Filter for Source] ダイアログボックスで、作成したポリシー オブジェクトを選択し、右矢印ボタンをクリックしてそのオブジェクトを選択済みリストに移動します。また、[条件（Condition）] オプションの横にある [一致しない（Not）] オプションを選択します。次の図に、ダイアログボックスの内容を示します。



d) [OK] をクリックフィルタがビュー設定に追加され、テーブルからイベントを削除するために使用されます。

e) **[ファイル（File）] > [名前を付けて保存（Save As）]** を選択して、変更を新規カスタムビューとして保存します。ビューの名前と説明を入力するように求められます。それぞれ入力し、[OK] をクリックします。

次の図に、[All IPS Events] 定義済みビューから開始し、Filtered IPS Events という名前を指定した場合に、ビュー設定がどのようになるかを示します。

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。