Security Cloud Control Firewall Management イベントの表示

この章では、Security Cloud Control Firewall Management でライブイベントおよび過去のイベントを表示する方法について説明します。

ライブイベントを表示する

[ライブ（Live）]イベントページには、入力したフィルタおよび検索条件に一致する、直近500件のイベントが表示されます。[ライブ（Live）] ページに最大数である 500 のイベントが表示されており、さらに表示されるイベントが追加されると、Security Cloud Control は最新のライブイベントを表示し、最も古いライブイベントを [履歴（Historical）] イベントページに転送します。これにより、ライブイベントの総数が 500 に維持されます。この転送には、約 1 分を要します。フィルタリング基準を追加しない場合は、イベントを記録するように設定されたルールによって生成された最新の 500 のライブイベントがすべて表示されます。

イベントのタイムスタンプは UTC で表示されます。

ライブイベントが再生中か一時停止中かにかかわらず、フィルタリング基準を変更すると、イベント画面がクリアされ、収集プロセスが再開されます。

Security Cloud Control イベントビューアでライブイベントを表示するには、次の手順を実行します。

手順

ステップ 1 左側のペインで、**[イベントとログ（Events & Logs）]>[イベント（Events）]>[イベントロギング（Events Logging）]** を選択します。

ステップ 2 [ライブ（Live）] タブをクリックします。

次のタスク

次の関連情報を参照して、イベントを再生および一時停止する方法を確認します。

関連情報：

- ライブイベントの再生/一時停止 （2 ページ）
- 履歴イベントの表示 （3 ページ）
- イベントビューのカスタマイズ （4 ページ）

ライブイベントの再生/一時停止

ライブイベントのストリーミング中に「再生」または「一時停止」できます。ライブイベントが「再生中」の場合、Security Cloud Control は、イベントビューアで指定されたフィルタ基準に一致するイベントを受信順に表示します。イベントが一時停止された場合、ライブイベントの再生を再開するまで、Security Cloud Control はライブイベントページを更新しません。イベントの再生を再開すると、Security Cloud Control は、イベントの再生を再開した時点からライブページにイベントの入力を開始します。見逃したイベントが遡って再生されることはありません。

ライブイベントのストリーミングを再生または一時停止したかどうかにかかわらず、Security Cloud Control が受信したすべてのイベントを表示するには、[履歴（Historical）] タブをクリックします。

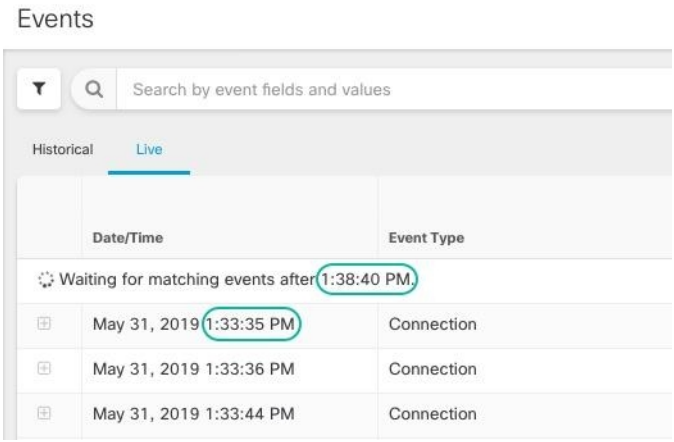
ライブイベントの自動一時停止

イベントを約 5 分間連続して表示した後、Security Cloud Control は、ライブイベントのストリーミングを一時停止しようとしていることを警告します。その時点で、リンクをクリックしてライブイベントのストリーミングをさらに 5 分間継続するか、ストリーミングを停止することができます。準備ができたら、ライブイベントのストリーミングを再開できます。

イベントの受信と報告

Secure Event Connector または Security Service Exchange がイベントを受信してから、Security Cloud Control がライブイベントビューアにイベントを投稿するまでに、わずかに遅れが生じる

場合があります。ライブページで遅延を確認できます。イベントのタイムスタンプは、イベントが Secure Event Connector または Security Service Exchange によって受信された時刻です。



履歴イベントの表示

[ライブ（Live）]イベントページには、入力したフィルタおよび検索条件に一致する、直近500件のイベントが表示されます。直近の 500 件より古いイベントは、[履歴（Historical）] イベントテーブルに転送されます。この転送には、約1分を要します。その後、保存したすべてのイベントをフィルタリングして、探しているイベントを見つけることができます。

履歴イベントを表示するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションウィンドウで **[イベントとログ（Events & Logs）] > [イベント（Events）] > [イベントロギング（Events Logging）]** を選択します。

ステップ 2 [履歴（Historic）] タブをクリックします。デフォルトでは、[履歴（Historic）] イベントテーブルを開くと、フィルタは過去 1 時間以内に収集されたイベントを表示するように設定されています。

イベントの属性は、Firepower Device Manager（FDM）または Adaptive Security Device Manager（ASDM）によって報告されるものとほぼ同じです。

- Firepower Threat Defense イベント属性の完全な説明については、『Cisco Firepower Threat Defense Syslog メッセージ』を参照してください。
- ASA イベント属性の詳細については、『Cisco ASA Series Syslog Messages』を参照してください。

イベントビューのカスタマイズ

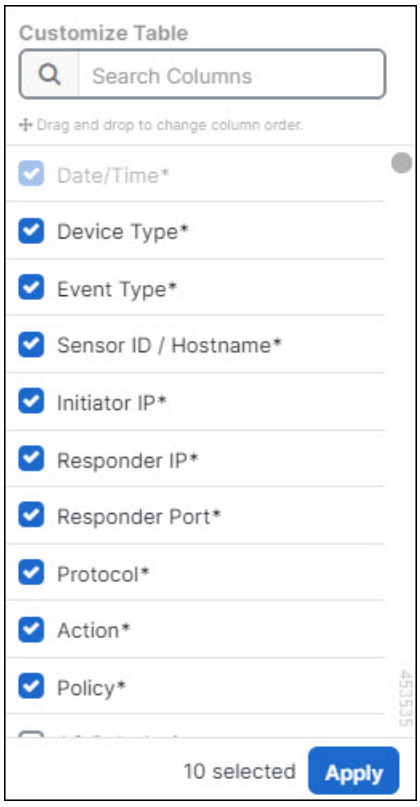
[イベントロギング（Event Logging）]ページに加えられた変更は、このページから移動して後で戻ったときに備えて自動的に保存されます。

（注） ライブイベントと履歴イベントビューの設定は同じです。イベントビューをカスタマイズすると、変更はライブビューと履歴ビューの両方に適用されます。

列の表示/非表示

ライブイベントと履歴イベントの両方のイベントビューを変更して、必要なビューに適用される列ヘッダーのみを含めることができます。列の右側にある列フィルタアイコン をクリックし、必要な列を選択または選択解除して、[適用（Apply）]をクリックします。

図 *1:* 列の表示/非表示



アスタリスクの付いた列は、デフォルトでイベントテーブル内に含まれますが、いつでも削除できます。

列の検索と追加

デフォルトリストに含まれていない列をさらに検索し、ライブイベントと履歴イベントの両方のイベントビューに追加できます。テーブルをカスタマイズして多くの列を追加すると、パフォーマンスが低下する可能性があるので注意してください。データの取得を高速化するために、使用する列の数は減らすようにしてください。

または、イベントの横にある [+] アイコンをクリックして展開し、非表示の列を表示します。

列の並べ替え

イベントテーブルの列を並べ替えることができます。列の右側にある列フィルタアイコン をクリックし、選択した列のリストを表示します。次に、列をドラッグアンドドロップして希望する順序に並べ替えます。ドロップダウンメニューのリストの一番上にある列が、イベントテーブルの左端の列として表示されます。

関連情報：

- [イベントロギング（Event Logging）] ページでのイベントのフィルタリング
- Security Analytics and Logging のイベント属性

イベントロギングページのカラムの表示および非表示

[イベントロギング（Event Logging）] ページには、構成済み ASA および FDM による管理 デバイスから Cisco Cloud に送信されたイベントが表示されます。

テーブルで表示/非表示ウィジェットを使用して、[イベントロギング（Event Logging）] ページの列を表示したり非表示にしたりできます。

手順

ステップ 1 左側のペインで、**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[イベントロギング（Events Logging）]** を選択します。

ステップ 2 テーブルの右端までスクロールし、列フィルタアイコン をクリックします。

ステップ 3 表示する列のチェックボックスをオンにし、非表示にする列のチェックボックスをオフにします。

列が再び表示されるか非表示にされるまで、表示するように選択した列がテナントにログインしている他のユーザーにも表示されます。

以下の表は、デフォルトの列ヘッダーについて説明しています。

カラム ヘッダ	説明
Date/Time	デバイスがイベントを生成した時間。デフォルトでは、イベントタイムスタンプはローカルタイムゾーンで表示されます。イベントのタイムスタンプをUTCで表示するには、イベントタイムスタンプのタイムゾーンの変更（11 ページ）を参照してください。
デバイスタイプ（Device Type）	ASA（適応型セキュリティアプライアンス） FTD（Firepower Threat Defense）

カラム ヘッダ	説明
イベントタイプ	

カラム ヘッダ	説明
	この複合列には、以下のいずれかを含めることができます。 • **FTD イベントタイプ** • 接続（Connection）：アクセスコントロールルールからの接続イベントを表示します。 • ファイル（File）：アクセスコントロールルールのファイルポリシーによって報告されたイベントを表示します。 • 侵入（Intrusion）：アクセスコントロールルールの侵入ポリシーによって報告されたイベントを表示します。 • マルウェア（Malware）：アクセスコントロールルールのマルウェアポリシーによって報告されたイベントを表示します。 • [ASAイベントタイプ（ASA Event Types）]：これらのイベントタイプは、syslog または NetFlow イベントのグループを表します。syslog ID または NetFlow ID が含まれているグループの詳細については、『ASA イベントタイプ』を参照してください。 • 解析されたイベント（Parsed Events）：解析された syslog イベントには、他の syslog イベントよりも多くのイベント属性が含まれており、Security Cloud Control はそれらの属性に基づいて検索結果をより迅速に返すことができます。解析されたイベントはフィルタリングカテゴリではありませんが、解析されたイベント ID は、[イベントタイプ（Event Types）] 列に斜体で表示されます。斜体で表示されていないイベント ID は解析されていません。 • ASA NetFlow イベント ID：ASAからのすべての NetFlow（NSEL）イベン

カラム ヘッダ	説明
	トがここに表示されます。
センサーID/ホスト名（Sensor ID / Hostname）	センサー ID は、イベントを Security Service Exchange または Secure Event Connector に送信する IP アドレスです。 これは通常、Threat Defense または ASA の管理インターフェイスです。
[イニシエータ IP（Initiator IP）]	これは、ネットワークトラフィックの送信元の IP アドレスです。イニシエータ アドレス フィールドの値は、イベントの詳細の InitiatorIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
レスポンダ IP（Responder IP）	これは、パケットの宛先 IP アドレスです。宛先アドレスフィールドの値は、イベントの詳細の ResponderIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
ポート	セッション**レスポンダ**が使用するポートまたは ICMP コードです。宛先ポートの値は、イベントの詳細の **ResponderPort** の値に対応します
プロトコル	これは、イベントのプロトコルを表します。

カラム ヘッダ	説明
操作	ルールによって定義されたセキュリティアクションを指定します。入力する値は、検索対象と完全に一致する必要がありますが、大文字小文字は関係ありません。各イベントタイプ（接続、ファイル、侵入、マルウェア、syslog、および NetFlow）に異なる値を入力します。 • 接続イベントタイプの場合、フィルタは AC_RuleAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。 • ファイルイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。 • 侵入イベントタイプの場合、フィルタは InLineResult 属性で一致を検索します。それらの値は、Allowed、Blocked、Trusted の可能性があります。 • マルウェアイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、クラウド ルックアップ タイムアウトである可能性があります。 • syslog および NetFlow イベントタイプの場合、フィルタは Action 属性で一致を検索します。
ポリシー	イベントをトリガーしたポリシーの名前です。名前は ASA および FDM による管理デバイスによって異なります。

関連情報：

[イベントロギング（Event Logging）]ページを使用したイベントの検索とフィルタリング （12 ページ）

イベントタイムスタンプのタイムゾーンの変更

Security Cloud Control の [イベントロギング（Event Logging）] ページで、イベントタイムスタンプのタイムゾーン表示を変更します。

手順

ステップ 1 左側のペインで **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択します。

ステップ 2 [イベントロギング（Event Logging）] ページの右上にある [UTC時間（UTC Time）] ボタンまたは [ローカル時間（Local Time）] ボタンをクリックすると、選択したタイムゾーンのイベントタイムスタンプが表示されます。

デフォルトでは、イベントタイムスタンプはローカルタイムゾーンで表示されます。

カスタマイズ可能なイベントフィルタ

Secure Logging Analytics（SaaS）のお客様は、頻繁に使用するカスタムフィルタを作成して保存できます。

フィルタの要素は、設定時にフィルタのタブに保存されます。[イベントロギング（Event Logging）] ページに戻るたびに、これらの検索機能を使用できます。テナントの他の Security Cloud Control ユーザーは使用できません。複数のテナントを管理している場合、別のテナントでは使用できません。

（注） フィルタのタブで作業しているときにフィルタ条件を変更すると、加えられた変更はカスタムフィルタのタブに自動的に保存されることに注意してください。

手順

ステップ 1 メインメニューから **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択します。

ステップ 2 値の [検索（Search）] フィールドをクリアします。

ステップ 3 イベントテーブルの上にある青いプラスボタンをクリックして、[表示（View）] タブを追加します。フィルタ表示には、名前を付けるまで、[表示1（View 1）]、[表示2（View 2）]、[表示3（View 3）] のようにラベルが付けられます。

ステップ 4 ビューのタブを選択します。

ステップ 5 フィルタバーを開き、カスタムフィルタに必要なフィルタ属性を選択します。「[イベントロギング（Event Logging）] ページを使用したイベントの検索とフィルタリング （12 ページ）」を参照してください。カスタムフィルタにはフィルタ属性のみが保存されることに注意してください。

ステップ 6 [イベントロギング（Event Logging）] テーブルに表示する列をカスタマイズします。列の表示と非表示については、「イベントロギングページのカラムの表示および非表示 （5 ページ）」を参照してください。

ステップ 7 [表示X（View X）] ラベルの付いたフィルタタブをダブルクリックし、名前を変更します。

ステップ 8 （オプション）カスタムフィルタを作成したので、[検索（Search）] フィールドに検索条件を追加することにより、カスタムフィルタを変更せずに、[イベントロギング（Event Logging）] ページに表示される結果を微調整できます。「[イベントロギング（Event Logging）] ページを使用したイベントの検索とフィルタリング （12 ページ）」を参照してください。

[イベントロギング（Event Logging）] ページを使用したイベントの検索とフィルタリング

特定のイベントの履歴イベントテーブルとライブイベントテーブルの検索とフィルタ処理は、Security Cloud Control で他の情報を検索してフィルタ処理する場合と同様に機能します。フィルタ条件を追加すると、Security Cloud Control は [イベントロギング（Event Logging）] ページに表示される内容を制限し始めます。検索フィールドに検索条件を入力して、特定の値を持つイベントを検索することもできます。フィルタリングと検索のメカニズムを組み合わせると、検索はイベントのフィルタリング後に表示される結果の中から、入力した値を見つけようとします。

イベントログの検索を実行するオプションは次のとおりです。

- [イベントロギング（Events Logging）] ページを使用したイベントの検索 （20 ページ）
- バックグラウンドでの履歴イベントの検索 （21 ページ）

ライブイベントのフィルタリングは、履歴イベントの場合と同じように機能しますが、ライブイベントは時刻でフィルタリングできない点が異なります。

次のフィルタリング方法について説明します。

- ライブまたは履歴イベントのフィルタ処理 （13 ページ）
- NetFlow イベントのみフィルタ処理 （15 ページ）
- ASA または FDM による管理 デバイスの Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない （15 ページ）
- フィルタ要素の結合 （15 ページ）

ライブまたは履歴イベントのフィルタ処理

この手順では、イベントフィルタリングを使用して、[イベントロギング（Event Logging）] ページでイベントのサブセットを表示する方法について説明します。特定のフィルタ条件を繰り返し使用する場合は、カスタマイズしたフィルタを作成して保存できます。詳細については、「カスタマイズ可能なイベントフィルタ」を参照してください。

手順

ステップ 1 ナビゲーションバーで、**[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択します。

ステップ 2 [履歴（Historical）] タブまたは [ライブ（Live）] タブをクリックします。

ステップ 3 フィルタアイコン（ ）をクリックします。ピンアイコン（ ）をクリックして、[フィルタ（Filter）] ペインを開いた状態でピン留めします。

ステップ 4 保存されているフィルタ要素がない [表示（View）] タブをクリックします。

ステップ 5 フィルタリングするイベントの詳細を選択します。

- [FTDイベント（FTD Events）] :
  - 接続（Connection）：アクセスコントロールルールからの接続イベントを表示します。
  - ファイル（File）：アクセスコントロールルールのファイルポリシーによって報告されたイベントを表示します。
  - 侵入（Intrusion）：アクセスコントロールルールの侵入ポリシーによって報告されたイベントを表示します。
  - マルウェア（Malware）：アクセスコントロールルールのマルウェアポリシーによって報告されたイベントを表示します。
- ASAイベント（ASA Events）：これらのイベントタイプは、syslog または NetFlow イベントのグループを表します。

  イベントの詳細については、「Security Cloud Control イベントタイプ」を参照してください。
  - 解析されたイベント（Parsed Events）：解析された syslog イベントには、他の syslog イベントよりも多くのイベント属性が含まれており、Security Cloud Control はそれらの属性に基づいて検索結果をより迅速に返すことができます。解析されたイベントはフィルタリングカテゴリではありませんが、解析されたイベント ID は、[イベントタイプ（Event Types）] 列に斜体で表示されます。斜体で表示されていないイベント ID は解析されていません。
- 時間範囲（Time Range）：[開始時刻（Start time）] または [終了時刻（End time）] フィールドをクリックして、表示する期間の開始時刻と終了時刻を選択します。タイムスタンプは、コンピュータのローカル時間で表示されます。

- アクション（Action）：ルールによって定義されたセキュリティアクションを指定します。入力する値は、検索対象と完全に一致する必要がありますが、大文字小文字は関係ありません。各イベントタイプ（接続、ファイル、侵入、マルウェア、syslog、および NetFlow）に異なる値を入力します。
  - 接続イベントタイプの場合、フィルタは AC_RuleAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。
  - ファイルイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、Allow、Block、Trust の可能性があります。
  - 侵入イベントタイプの場合、フィルタは InLineResult 属性で一致を検索します。それらの値は、Allowed、Blocked、Trusted の可能性があります。
  - マルウェアイベントタイプの場合、フィルタは FileAction 属性で一致を検索します。それらの値は、クラウドルックアップ タイムアウトである可能性があります。
  - syslog および NetFlow イベントタイプの場合、フィルタは Action 属性で一致を検索します。
- [センサーID/ホスト名（Sensor ID / Hostname）]：センサー ID は、イベントを Secure Event Connector または Security Service Exchange に送信する管理 IP アドレスです。

  FDM による管理デバイスの場合、センサー ID は通常、デバイスの管理インターフェイスの IP アドレスです。
- **IP アドレス**
  - イニシエータ（Initiator）：ネットワークトラフィックの送信元の IP アドレスです。イニシエータアドレス フィールドの値は、イベントの詳細の InitiatorIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
  - レスポンダ（Responder）：パケットの宛先 IP アドレスです。宛先アドレスフィールドの値は、イベントの詳細の ResponderIP フィールドの値に対応します。10.10.10.100 などの単一のアドレス、または 10.10.10.0/24 などの CIDR 表記で定義されたネットワークを入力できます。
- **ポート**
  - イニシエータ（Initiator）：セッションイニシエータが使用するポートまたは ICMP タイプ。送信元ポートの値は、イベントの詳細の InitiatorPort の値に対応します（範囲の追加：開始ポートと終了ポートと、イニシエータとレスポンダの間または両方のスペース）。
  - レスポンダ（Reponder）：セッションレスポンダが使用するポートまたは ICMP コード。宛先ポートの値は、イベントの詳細の ResponderPort の値に対応します
- NetFlow：ASA NetFlow イベントは、syslog イベントとは異なります。NetFlow フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの「NetFlow イベント ID」は、Cisco ASA NetFlow 実装ガイド [英語] で定義されています。

ステップ 6 （任意）[表示（View）] タブの側をクリックして、フィルタをカスタムフィルタとして保存します。

NetFlow イベントのみフィルタ処理

この手順では、ASA NetFlow イベントのみを検索します。

手順

ステップ 1 左側のメニューから**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[イベントロギング（Events Logging）]** を選択します。

ステップ 2 フィルタアイコン をクリックして、開いた状態でフィルタをピン留めします。

ステップ 3 [Netflow] ASA イベントフィルタをオンにします。

ステップ 4 他のすべての ASA イベントフィルタをオフにします。

[イベントロギング（Event Logging）] テーブルには、ASA NetFlow イベントのみが表示されます。

ASA または FDM による管理 デバイスの Syslog イベントをフィルタリングするが、ASA NetFlow イベントはフィルタリングしない

この手順では、syslog イベントのみを検索します。

手順

ステップ 1 左側のペインで、**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[イベントロギング（Events Logging）]** を選択します。

ステップ 2 フィルタアイコン をクリックして、開いた状態でフィルタをピン留めします。

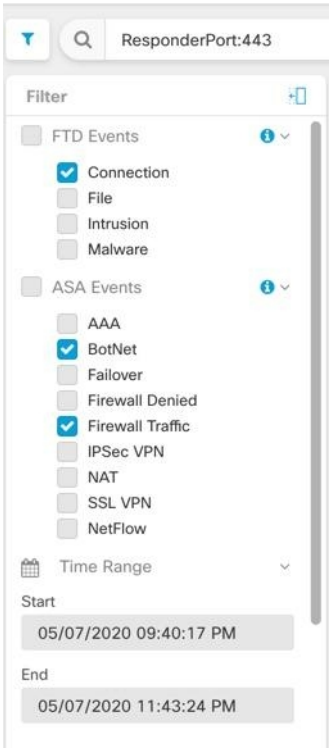
ステップ 3 [フィルタ（Filter）]ペインの一番下までスクロールし、[NetFlowイベントを含める（Include NetFlow Events）] フィルタが**オフ**になっていることを確認します。

ステップ 4 [ASAイベント（ASA Events）] フィルタツリーまでスクロールして戻り、[NetFlow] ボックスが**オフ**になっていることを確認します。

ステップ 5 ASA または FTD フィルタ条件の残りを選択します。

フィルタ要素の結合

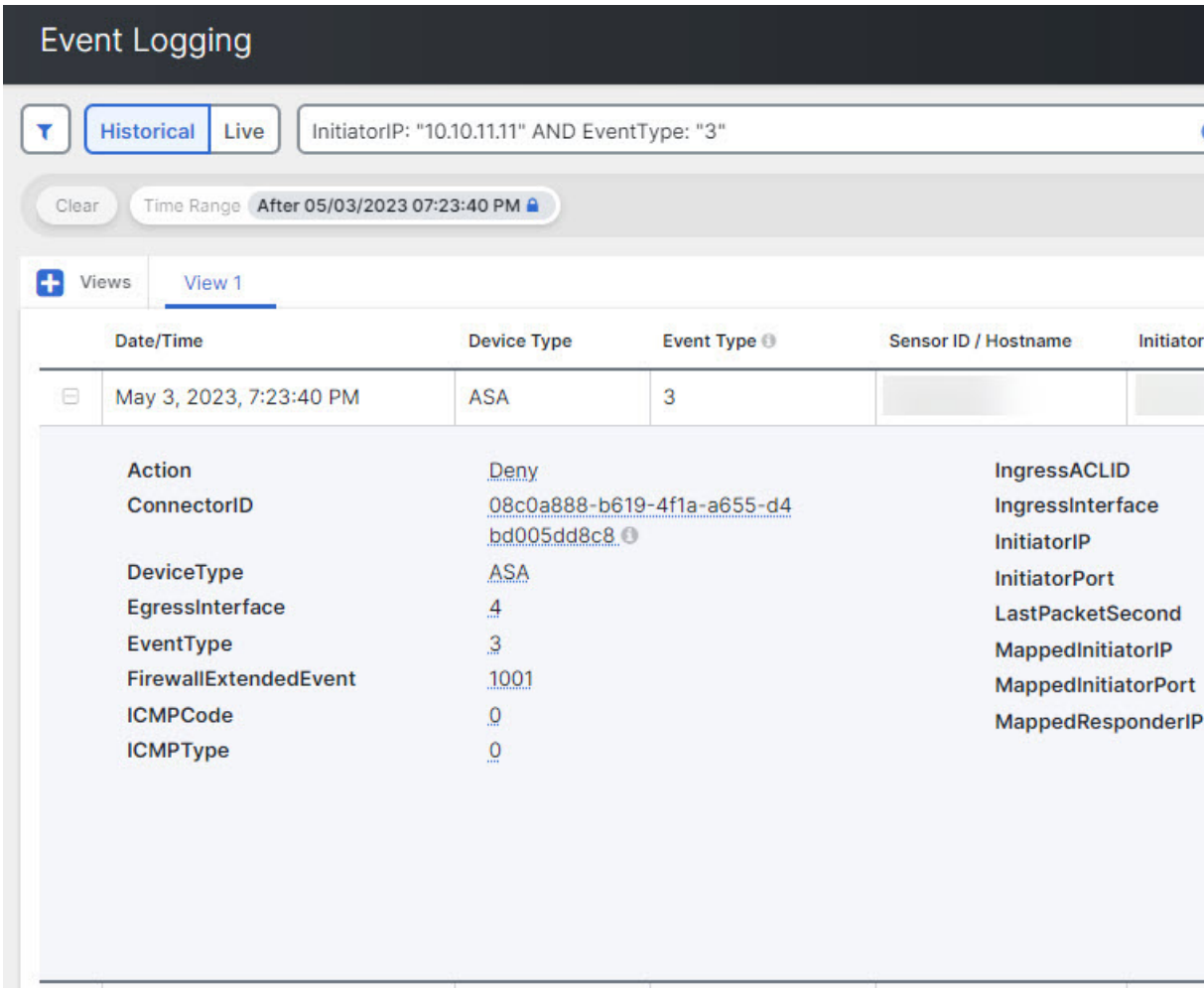
イベントのフィルタリングは、通常、Security Cloud Control の標準フィルタリングルールに従います。フィルタリングカテゴリには「かつ（AND）」が適用され、カテゴリ内の値は「または（OR）」が適用されます。フィルタをユーザー独自の検索条件と組み合わせることもできます。ただし、イベントフィルタの場合は、デバイスイベントフィルタにも「または」が適用されます。たとえば、フィルタで次の値が選択されているとします。



このフィルタを使用すると、Security Cloud Control では、Firewall Threat Defenseデバイスの接続イベント**または** ASA の BotNet イベント**または**ファイアウォール トラフィック イベント、**かつ**時間範囲内の 2 つの時間の間に発生したイベント、**かつ** ResponderPort 443 も含むイベントが表示されます。時間範囲内の履歴イベントでフィルタリングできます。ライブイベントページには常に最新のイベントが表示されます。

特定の属性：値ペアの検索

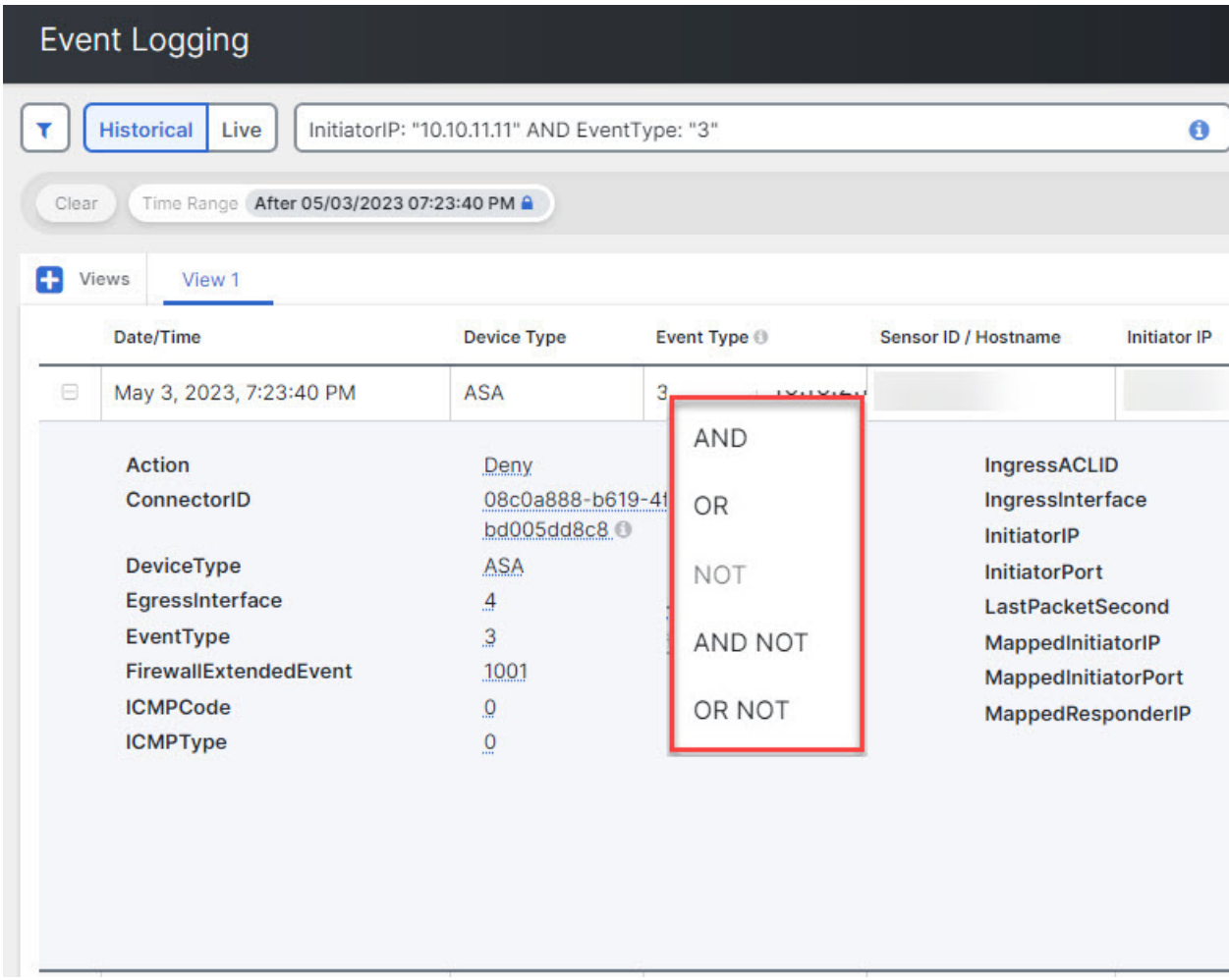
検索フィールドにイベント属性と値を入力することで、ライブイベントや過去のイベントを検索できます。これを行う最も簡単な方法は、イベントログテーブルで、検索する属性をクリックすることです。Security Cloud Control によってその属性が検索フィールドに入力されます。クリックできるイベントは、マウスのカーソルを合わせると青色になります。次に例を示します。



この例では、イニシエータ IP（InitiatorIP）の値である 10.10.11.11 にマウスのカーソルを合わせてクリックすることにより、検索が開始されています。「InitiatorIP」とその値が検索文字列に追加されています。次に、イベントタイプの値である 3 にマウスのカーソルが合わされてクリックされ、検索文字列に追加されています。このとき、Security Cloud Control によって AND が追加されています。そのため、この検索の結果は、10.10.11.11 から開始された、「かつ」イベントタイプが 3 のイベントのリストになります。

上の例で、値 3 の横にある虫眼鏡に注目してください。この虫眼鏡にマウスのカーソルを合わせ、AND、OR、AND NOT、OR NOT 演算子を選択して、検索に追加する値とともに指定することもできます。

次の例では「OR」が選択されています。この検索の結果は、10.10.11.11 から開始された、「または」イベントタイプが 106023 のイベントのリストになります。検索フィールドが空のときにテーブルの値を右クリックした場合は、他の値がないため、「以外（NOT）」しか使用できないことに注意してください。



マウスのカーソルを合わせると青色で強調表示される値は、検索文字列に追加できます。

AND、OR、NOT、AND NOT、OR NOT フィルタ演算子

検索文字列で使用される「AND」、「OR」、「NOT」、「AND NOT」、および「OR NOT」の動作は次のとおりです。

AND

すべての属性を含むイベントを検索するには、フィルタ文字列で AND 演算子を使用します。AND 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、TCP プロトコルを含んだ、「かつ」イニシエータ IP アドレス（InitiatorIP）10.10.10.43 から開始された、「かつ」イニシエータポート（InitiatorPort）59614 から送信されたイベントが検索されます。AND ステートメントを追加するたびに、基準を満たすイベントの数が少なくなることが予期されます。

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

OR

いずれかの属性を含むイベントを検索するには、フィルタ文字列で OR 演算子を使用します。OR 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、TCP プロトコルを含んだ、「または」イニシエータ IP アドレス（InitiatorIP）10.10.10.43 から開始された、「または」イニシエータポート（InitiatorPort）59614 から送信されたイベントがイベントビューアに表示されます。OR ステートメントを追加するたびに、基準を満たすイベントの数が多くなることが予期されます。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

NOT

特定の属性を持つイベントを除外するには、検索文字列の先頭でのみ、これを使用します。たとえば、次の検索文字列では、InitiatorIP が 192.168.25.3 のイベントが結果から除外されます。

```
NOT InitiatorIP: "192.168.25.3"
```

AND NOT

特定の属性を含むイベントを除外するには、フィルタ文字列で AND NOT 演算子を使用します。AND NOT 演算子は、検索文字列の先頭では使用できません。

たとえば、次のフィルタ文字列では、イニシエータ IP アドレス（InitiatorIP）が 192.168.25.3 のイベントが表示されますが、それらのうち、レスポンダ IP アドレス（ResponderIP）が 10.10.10.1 のものは表示されません。

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

NOT と AND NOT を組み合わせて、複数の属性を除外することもできます。たとえば、次のフィルタ文字列では、InitiatorIP が 192.168.25.3 のイベントと ResponderIP が 10.10.10.1 のイベントが除外されます。

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

特定の要素を除外する検索結果を含めるには、フィルタ文字列で OR NOT 演算子を使用します。OR NOT 演算子は、検索文字列の先頭では使用できません。

たとえば、次の検索文字列では、プロトコル（Protocol）が TCP のイベント、「または」InitiatorIP が 10.10.10.43 のイベント、「または」InitiatorPort が 59614 ではないイベントが検索されます。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

これは、(Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614") の検索と考えることもできます。

ワイルドカード検索

アスタリスク（*）を「属性：値」ペア検索の「値」フィールドでワイルドカードとして使用して、イベント内の結果を検索することができます。たとえば、次のフィルタ文字列では、

```
URL:*feedback*
```

属性フィールドが「URL」のイベントの文字列が検索され、「feedback」という文字列が含まれているイベントが表示されます。

関連情報：

- イベントロギングページのカラムの表示および非表示
- Security Analytics and Logging のイベント属性

[イベントロギング（Events Logging）] ページを使用したイベントの検索

ログに記録されたすべてのイベントを検索して必要な情報を見つけるには、[イベントロギング（Event Logging）] ページの検索機能とレポート機能を使用します。履歴イベントに関するレポートのみを生成できることに注意してください。

手順

ステップ 1 ナビゲーションバーで、**[イベントとログ（Events & Logs）] > [イベント（Events）] > [イベントロギング（Events Logging）]** を選択します。

ステップ 2 [履歴（Historical）] タブまたは [ライブ（Live）] タブをクリックします。

ステップ 3 検索バーに検索クエリを入力し、[検索（Search）] をクリックして検索を実行します。

または、検索ボックスをクリックして [サンプルフィルタ（Sample Filters）] のリストから選択し、イベントをすばやく検索します。サンプルフィルタを使用して、検索バーに検索クエリをすばやく入力し、特定のニーズに合わせて変更します。サンプルフィルタの使用に関する詳細については、サンプルフィルタを使用したイベントの検索 （21 ページ）を参照してください。

ステップ 4 （オプション）検索ページから離れている間にバックグラウンドで検索を実行し、レポートを生成するには、次の手順を実行します。

a) 検索クエリを入力し、[検索（Search）] ドロップダウンリストから [レポートのスケジュール設定（Schedule Report）] を選択します。

b) [Generate Report] をクリックします。

検索はキューに入れられ、完了すると通知されます。バックグラウンドで複数の検索を実行できます。

レポートのスケジュール設定の詳細については、バックグラウンドで検索レポートを生成するためのスケジュール （22 ページ）を参照してください

ステップ 5 （オプション）検索レポートを表示および管理する場合は、[レポート（Reports）] をクリックします。このビューから、次の操作を実行できます。

- [レポート（Reports）] ページでは、検索レポートを表示、ダウンロード、または削除できます。
- 1回限りのレポートを生成するか、定期レポートをスケジュール設定するには、[レポートのスケジュール設定（Schedule a Report）] をクリックします。

- 通知設定を表示または変更するには、[通知設定の表示（View Notification Settings）] をクリックして [通知設定（Notification Preferences）] ページに移動します。

次のタスク

定期検索が必要な場合は、任意の1回限りのレポートを定期レポートのスケジュールに変換できます。詳細については、バックグラウンドで検索レポートを生成するためのスケジュール（22 ページ）を参照してください。

サンプルフィルタを使用したイベントの検索

サンプルフィルタを使用すると、完全なクエリを入力せずに共通の検索クエリをすばやく作成できます。フィルタを選択し、特定のニーズに合わせてクエリパラメータを変更します。

手順

ステップ 1 **[Event Logging]** ページで、検索バーをクリックします。**[Sample Filters]** のリストが、検索バーの下に表示されます。

ステップ 2 ドロップダウンリストから、フィルタを選択します。検索バーに対応する検索クエリが自動的に入力されます。

ステップ 3 事前定義されたクエリの値を変更して検索を絞り込みます。

例

- 特定の Web サイトに関連するイベントを検索するには、**[Wildcard URL]** を選択します。検索バーに **URL**： **"*.sharepoint.com"** と表示されます。sharepoint.com を調査対象の他のドメインに変更できます。
- 特定のデバイスに関係するイベントを検索するには、**[Specific Host]** を選択します。検索バーに **InitiatorIP**： **"192.168.55.55" OR ResponderIP**： **"192.168.55.55"** と表示されます。192.168.55.55 をモニターするデバイスの IP アドレスに変更します。

ステップ 4 **[検索（Search）]** をクリックします。

バックグラウンドでの履歴イベントの検索

Security Cloud Control では、検索条件を定義し、その検索条件に基づいてイベントログを検索できます。[レポート（Reports）] 機能により、バックグラウンドでイベントログ検索を実行し、レポートを生成することができます。

設定した通知設定に基づいて、レポートの生成が完了したときに通知を受け取ります。

[レポート（Reports）]ページから、レポートを表示、ダウンロード、または削除できます。さらに、1 回限りのレポートまたは定期レポートのいずれかの生成をスケジュールすることもで

きます。[通知設定（Notification Settings）] ページに移動して、サブスクリプション オプションを表示または変更します。

バックグラウンドで検索レポートを生成するためのスケジュール

バックグラウンドで1回限りのイベントログ検索またはスケジュール済みのイベントログ検索を実行し、レポートを生成するには、[イベントロギング（Event Logging）] ページの [レポート（Report）] 機能を使用します。スケジュールされたレポートはいつでも変更またはキャンセルできます。また、1 回限りの検索クエリを繰り返し検索に変更することもできます。

（注）
- 履歴イベントに関するレポートの生成のみをスケジュールできます。
- 開始、完了、または失敗したレポートに関するアラートを取得することを選択できます。

検索をスケジュールしてレポートを生成するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションバーで、**[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択します。

ステップ 2 [履歴（Historical）] タブをクリックして履歴イベントを表示します。

ステップ 3 検索バーに検索クエリを入力します。

ステップ 4 [検索（Search）] ドロップダウンをクリックし、[レポートのスケジュール設定（Schedule Report）] を選択します。

ステップ 5 （オプション）レポートを識別するための名前を入力します。

ステップ 6 デフォルトでは、[今すぐレポートを生成（Generate report now）] チェックボックスはオンになっています。オンにすると、保存時にレポートの生成が開始されます。

ステップ 7 [繰り返しスケジュールの設定（Setup recurring schedule）] チェックボックスをオンにして、次の設定を行います。

- [ログの検索期間（Search Logs for the Last）]：遡って検索する期間を指定します。
- [頻度（Frequency）]：スケジュールされた検索を実行する頻度と、実行する時間を指定します。

ステップ 8 ウィンドウの下部で、スケジュールされた検索条件を確認します。[スケジュールおよび今すぐ生成（Schedule and Generate Now）] をクリックします。検索をすぐに開始することを選択しなかった場合は、[レポートのスケジュール設定（Schedule Report）] をクリックします。

次のタスク

スケジュールされた検索レポートは、Security Cloud Control によって自動的に削除されるまで、最大 7 日間表示できます。

検索レポートのダウンロード

検索結果とスケジュールクエリは、Security Cloud Control によって自動的に削除されるまで 7 日間保存されます。検索レポートのコピーを CSV 形式でダウンロードできます。

手順

ステップ 1 ナビゲーションバーで、**[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択します。

ステップ 2 [レポート（Reports）] をクリックします。

ステップ 3 **[Actions]** 列で、レポートの横にある **[Download]** をクリックして、レポートをダウンロードします。CSV 形式の検索レポートは、ローカルドライブのデフォルトの保存場所に自動的にダウンロードされます。

ステップ 4 （オプション）検索クエリを表示してレポートをダウンロードするには、次の手順を実行します。

a) **[Queries]** タブをクリックします。
b) レポートを展開して、検索クエリの詳細を表示します。
c) 表示してダウンロードするレポートの横にある **[View Reports]** をクリックします。
d) [Download] をクリックします。

Security Analytics and Logging のイベント属性

イベント属性の説明

Security Cloud Control によって使用されるイベント属性の説明は、Firepower Device Manager（FDM）および Adaptive Security Device Manager（ASDM）によって報告されるものとほぼ同じです。

- 適応型セキュリティアプライアンス（ASA）イベント属性の詳細については、「Cisco ASA シリーズ Syslog メッセージ」を参照してください。

一部の ASA syslog イベントは「解析」され、その他には、属性値ペアを使用してイベントログテーブルの内容をフィルタリングするときに使用できる追加の属性があります。syslog イベントのその他の重要な属性については、次の追加トピックを参照してください。

- 解析された ASA Syslog イベント
- 一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性
- Syslog イベントのイベント名属性
- 時間属性

一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性

一部の syslog イベントには、追加の属性「EventGroup」および「EventGroupDefinition」があります。属性:値のペアでフィルタ処理することにより、これらの追加属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。たとえば、イベントロギングテーブルの [検索（search）] フィールドに「`apfw:415*`」と入力して、アプリケーション ファイアウォール イベントをフィルタできます。

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

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
aaa/auth	ユーザ認証	109、113
acl/session	アクセスリスト/ユーザーセッション	106
apfw	アプリケーション ファイアウォール	415
ブリッジ	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
citrix	Citrix クライアント	723
clst	クラスタリング	747
cmgr	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	セキュアなデスクトップ	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
ipaa/envmon	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
idfw	Identity-Based ファイアウォール	746
ids	侵入検知システム	733
ids/ips	侵入検知システム/侵入防御システム	400
ikev2	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレスの割り当て	735
ips	侵入防御システム	401、420
ipv6	IPv6	325
l4tm	ブロックリスト、許可リスト、グレーリスト	338
lic	ライセンシング	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
vpn/nap	IKE と IPsec /ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
ospf	OSPF ルーティング	318、409、503、613
passwd	パスワードの暗号化	742
pp	Phone Proxy	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
sch	Smart Call Home	120
session	ユーザ セッション	108、201、202、204、302、303、304、314、405、406、407、500、502、607、608、609、616、620、703、710
session/natpat	ユーザーセッション/NAT および PAT	305
snmp	SNMP	212

EventGroup	EventGroupDefinition	Syslog メッセージ ID 番号（最初の 3 桁）
ssafe	ScanSafe	775
ssl/np ssl	SSL スタック/NP SSL	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
tre	トランザクション ルール エンジン	780
ucime	UC-IME	339
tag-switching	サービス タグ スイッチング	779
td	脅威の検出	733
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
vxlan	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN および AnyConnect クライアント	716
session/natpat	ユーザーセッション/NAT および PAT	305

Syslog イベントの EventName 属性

一部の syslog イベントには、追加の属性「EventName」があります。属性:値のペアでフィルタ処理することにより、EventName 属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。たとえば、[イベントロギング（Event Logging）] テーブルの検索フィールドに「**EventName:"Denied IP Packet"**」と入力することで、「Denied IP packet」のイベントをフィルタリングできます。

Syslog イベント ID とイベント名のテーブル

- AAA Syslog イベント ID とイベント名
- ボットネット Syslog イベント ID とイベント名
- フェールオーバー Syslog イベント ID とイベント名
- ファイアウォール拒否 Syslog イベント ID とイベント名
- ファイアウォール トラフィック Syslog イベント ID とイベント名
- アイデンティティ ベース ファイアウォール Syslog イベント ID とイベント名
- IPSec Syslog イベント ID とイベント名
- NAT Syslog イベント ID とイベント名
- SSL VPN Syslog イベント ID とイベント名

AAA Syslog イベント ID とイベント名

EventID	EventName
109001	AAA Begin
109002	AAA Failed
109003	AAA Server Failed
109005	Authentication Success
109006	認証に失敗
109007	Authorization Success
109008	「許可に失敗しました（Authorization Failed）」
109010	AAA Pending
109011	AAA Session Started
109012	AAA Session Ended
109013	AAA
109014	AAA Failed
109016	AAA ACL not found
109017	AAA Limit Reach
109018	AAA ACL Empty
109019	AAA ACL error

EventID	EventName
109020	AAA ACL error
109021	AAA error
109022	AAA HTTP limit reached
109023	AAA auth required
109024	「許可に失敗しました（Authorization Failed）」
109025	「許可に失敗しました（Authorization Failed）」
109026	AAA error
109027	AAA Server error
109028	AAA Bypassed
109029	AAA ACL error
109030	AAA ACL error
109031	認証に失敗
109032	AAA ACL error
109033	認証に失敗
109034	認証に失敗
109035	AAA Limit Reach
113001	AAA Session limit reach
113003	AAA overridden
113004	AAA Successful
113005	Authorization Rejected
113006	AAA user locked
113007	AAA User unlocked
113008	AAA successful
113009	AAA retrieved
113010	AAA Challenge received
113011	AAA retrieved

EventID	EventName
113012	認証成功
113013	AAA error
113014	AAA error
113015	認証を却下
113016	AAA Rejected
113017	AAA Rejected
113018	AAA ACL error
113019	AAA Disconnected
113020	AAA error
113021	AAA Logging Fail
113022	AAA Failed
113023	AAA reactivated
113024	AAA Client certification
113025	AAA Authentication fail
113026	AAA error
113027	AAA error

ボットネット **Syslog** イベント **ID** とイベント名

EventID	EventName
338001	Botnet Source Block List
338002	Botnet Destination Block List
338003	Botnet Source Block List
338004	Botnet Destination Block List
338101	Botnet Source Allow List
338102	Botnet destination Allow List
338202	Botnet destination Grey
338203	Botnet Source Grey
338204	Botnet Destination Grey

EventID	EventName
338301	Botnet DNS Intercepted
338302	Botnet DNS
338303	Botnet DNS
338304	Botnet Download successful
338305	Botnet Download failed
338306	Botnet Authentication failed
338307	Botnet Decrypt failed
338308	Botnet Client
338309	Botnet Client
338310	Botnet dyn filter failed

フェールオーバー Syslog イベント ID とイベント名

EventID	EventName
101001	Failover Cable OK
101002	Failover Cable BAD
101003	Failover Cable not connected
101004	Failover Cable not connected
101005	Failover Cable reading error
102001	Failover Power failure
103001	No response from failover mate
103002	Failover mate interface OK
103003	Failover mate interface BAD
103004	Failover mate reports failure
103005	Failover mate reports self failure
103006	Failover version incompatible
103007	Failover version difference
104001	Failover role switch
104002	Failover role switch

EventID	EventName
104003	Failover unit failed
104004	Failover unit OK
106100	Permit/Denied by ACL
210001	Stateful Failover error
210002	Stateful Failover error
210003	Stateful Failover error
210005	Stateful Failover error
210006	Stateful Failover error
210007	Stateful Failover error
210008	Stateful Failover error
210010	Stateful Failover error
210020	Stateful Failover error
210021	Stateful Failover error
210022	Stateful Failover error
311001	Stateful Failover update
311002	Stateful Failover update
311003	Stateful Failover update
311004	Stateful Failover update
418001	Denied Packet to Management
709001	Failover replication error
709002	Failover replication error
709003	Failover replication start
709004	Failover replication complete
709005	Failover receive replication start
709006	Failover receive replication complete
709007	Failover replication failure
710003	Denied access to Device

ファイアウォール拒否 Syslog イベント ID とイベント名

EventID	EventName
106001	Denied by Security Policy
106002	Outbound Deny
106006	Denied by Security Policy
106007	Denied Inbound UDP
106008	Denied by Security Policy
106010	Denied by Security Policy
106011	Denied Inbound
106012	Denied due to Bad IP option
106013	Dropped Ping to PAT IP
106014	Denied Inbound ICMP
106015	Denied by Security Policy
106016	Denied IP Spoof
106017	Denied due to Land Attack
106018	Denied outbound ICMP
106020	Denied IP Packet
106021	Denied TCP
106022	Denied Spoof packet
106023	Denied IP Packet
106025	Dropped Packet failed to Detect context
106026	Dropped Packet failed to Detect context
106027	Dropped Packet failed to Detect context
106100	Permit/Denied by ACL
418001	Denied Packet to Management
710003	Denied access to Device

ファイアウォール トラフィック Syslog イベント ID とイベント名

EventID	EventName
108001	Inspect SMTP

EventID	EventName
108002	Inspect SMTP
108003	Inspect ESMTP Dropped
108004	Inspect ESMTP
108005	Inspect ESMTP
108006	Inspect ESMTP Violation
108007	Inspect ESMTP
110002	No Router found
110003	Failed to Find Next hop
209003	Fragment Limit Reach
209004	Fragment invalid Length
209005	Fragment IP discard
302003	H245 Connection Start
302004	H323 Connection start
302009	Restart TCP
302010	Connection USAGE
302012	H225 CALL SIGNAL CONN
302013	Built TCP
302014	Teardown TCP
302015	Built UDP
302016	Teardown UDP
302017	Built GRE
302018	Teardown GRE
302019	H323 Failed
302020	Built ICMP
302021	Teardown ICMP
302022	Built TCP Stub
302023	Teardown TCP Stub
302024	Built UDP Stub

EventID	EventName
302025	Teardown UDP Stub
302026	Built ICMP Stub
302027	Teardown ICMP Stub
302033	Connection H323
302034	H323 Connection Failed
302035	Built SCTP
302036	Teardown SCTP
303002	FTP file download/upload
303003	Inspect FTP Dropped
303004	Inspect FTP Dropped
303005	Inspect FTP reset
313001	ICMP Denied
313004	ICMP Drop
313005	ICMP Error Msg Drop
313008	ICMP ipv6 Denied
324000	GTP Pkt Drop
324001	GTP Pkt Error
324002	メモリ エラー
324003	GTP Pkt Drop
324004	GTP Version Not Supported
324005	GTP Tunnel Failed
324006	GTP Tunnel Failed
324007	GTP Tunnel Failed
337001	Phone Proxy SRTP Failed
337002	Phone Proxy SRTP Failed
337003	Phone Proxy SRTP Auth Fail
337004	Phone Proxy SRTP Auth Fail
337005	Phone Proxy SRTP no Media Session

EventID	EventName
337006	Phone Proxy TFTP Unable to Create File
337007	Phone Proxy TFTP Unable to Find File
337008	Phone Proxy Call Failed
337009	Phone Proxy Unable to Create Phone Entry
400000	IPS IP options-Bad Option List
400001	IPS IP options-Record Packet Route
400002	IPS IP options-Timestamp
400003	IPS IP options-Security
400004	IPS IP options-Loose Source Route
400005	IPS IP options-SATNET ID
400006	IPS IP options-Strict Source Route
400007	IPS IP Fragment Attack
400008	IPS IP Impossible Packet
400009	IPS IP Fragments Overlap
400010	IPS ICMP Echo Reply
400011	IPS ICMP Host Unreachable
400012	IPS ICMP Source Quench
400013	IPS ICMP Redirect
400014	IPS ICMP Echo Request
400015	IPS ICMP Time Exceeded for a Datagram
400017	IPS ICMP Timestamp Request
400018	IPS ICMP Timestamp Reply
400019	IPS ICMP Information Request
400020	IPS ICMP Information Reply
400021	IPS ICMP Address Mask Request
400022	IPS ICMP Address Mask Reply
400023	IPS Fragmented ICMP Traffic
400024	IPS Large ICMP Traffic

EventID	EventName
400025	IPS Ping of Death Attack
400026	IPS TCP NULL flags
400027	IPS TCP SYN+FIN flags
400028	IPS TCP FIN only flags
400029	IPS FTP Improper Address Specified
400030	IPS FTP Improper Port Specified
400031	IPS UDP Bomb attack
400032	IPS UDP Snork attack
400033	IPS UDP Chargen DoS attack
400034	IPS DNS HINFO Request
400035	IPS DNS Zone Transfer
400036	IPS DNS Zone Transfer from High Port
400037	IPS DNS Request for All Records
400038	IPS RPC Port Registration
400039	IPS RPC Port Unregistration
400040	IPS RPC Dump
400041	IPS Proxied RPC Request
400042	IPS YP server Portmap Request
400043	IPS YP bind Portmap Request
400044	IPS YP password Portmap Request
400045	IPS YP update Portmap Request
400046	IPS YP transfer Portmap Request
400047	IPS Mount Portmap Request
400048	IPS Remote execution Portmap Request
400049	IPS Remote execution Attempt
400050	IPS Statd Buffer Overflow
406001	Inspect FTP Dropped
406002	Inspect FTP Dropped

EventID	EventName
407001	Host Limit Reach
407002	Embryonic limit Reached
407003	Established limit Reached
415001	Inspect Http Header Field Count
415002	Inspect Http Header Field Length
415003	Inspect Http body Length
415004	Inspect Http content-type
415005	Inspect Http URL length
415006	Inspect Http URL Match
415007	Inspect Http Body Match
415008	Inspect Http Header match
415009	Inspect Http Method match
415010	Inspect transfer encode match
415011	Inspect Http Protocol Violation
415012	Inspect Http Content-type
415013	Inspect Http Malformed
415014	Inspect Http Mime-Type
415015	Inspect Http Transfer-encoding
415016	Inspect Http Unanswered
415017	Inspect Http Argument match
415018	Inspect Http Header length
415019	Inspect Http status Matched
415020	Inspect Http non-ASCII
416001	Inspect SNMP dropped
419001	Dropped packet
419002	Duplicate TCP SYN
419003	Packet modified
424001	Denied Packet

EventID	EventName
424002	Dropped Packet
431001	Dropped RTP
431002	Dropped RTCP
500001	Inspect ActiveX
500002	Inspect Java
500003	Inspect TCP Header
500004	Inspect TCP Header
500005	Inspect Connection Terminated
508001	Inspect DCERPC Dropped
508002	Inspect DCERPC Dropped
509001	Prevented No Forward Cmd
607001	Inspect SIP
607002	Inspect SIP
607003	Inspect SIP
608001	Inspect Skinny
608002	Inspect Skinny dropped
608003	Inspect Skinny dropped
608004	Inspect Skinny dropped
608005	Inspect Skinny dropped
609001	Built Local-Host
609002	Teardown Local Host
703001	H225 Unsupported Version
703002	H225 Connection
726001	Inspect Instant Message

アイデンティティ ベース ファイアウォール **Syslog** イベント **ID** とイベント名

EventID	EventName
746001	Import started

EventID	EventName
746002	Import complete
746003	Import failed
746004	Exceed user group limit
746005	AD Agent down
746006	AD Agent out of sync
746007	Netbios response failed
746008	Netbios started
746009	Netbios stopped
746010	Import user failed
746011	Exceed user limit
746012	User IP add
746013	User IP delete
746014	FQDN Obsolete
746015	FQDN resolved
746016	DNS lookup failed
746017	Import user issued
746018	Import user done
746019	Update AD Agent failed

IPSec Syslog イベント ID とイベント名

EventID	EventName
402114	Invalid SPI received
402115	Unexpected protocol received
402116	Packet doesn't match identity
402117	Non-IPSEC packet received
402118	Invalid fragment offset
402119	Anti-Replay check failure
402120	Authentication failure（認証失敗）
402121	Packet dropped
426101	cLACP Port Bundle

EventID	EventName
426102	cLACP Port Standby
426103	cLACP Port Moved To Bundle From Standby
426104	cLACP Port Unbundled
602103	Path MTU updated
602104	Path MTU exceeded
602303	New SA created
602304	SA deleted
702305	SA expiration - Sequence rollover
702307	SA expiration - Data rollover

NAT Syslog イベント ID とイベント名

EventID	EventName
201002	Max connection Exceeded for host
201003	Embryonic limit exceed
201004	UDP connection limit exceed
201005	FTP connection failed
201006	RCMD connection failed
201008	New connection Disallowed
201009	Connection Limit exceed
201010	Embryonic Connection limit exceeded
201011	接続制限の超過
201012	Per-client embryonic connection limit exceeded
201013	Per-client connection limit exceeded
202001	Global NAT exhausted
202005	Embryonic connection error
202011	Connection limit exceeded
305005	No NAT group found
305006	Translation failed
305007	Connection dropped
305008	NAT allocation issue
305009	NAT Created
305010	NAT teardown

EventID	EventName
305011	PAT created
305012	PAT teardown
305013	Connection denied

SSL VPN Syslog イベント ID とイベント名

EventID	EventName
716001	WebVPN Session Started
716002	WebVPN Session Terminated
716003	WebVPN User URL access
716004	WebVPN User URL access denied
716005	WebVPN ACL error
716006	WebVPN User Disabled
716007	WebVPN Unable to Create
716008	WebVPN Debug
716009	WebVPN ACL error
716010	WebVPN User access network
716011	WebVPN User access
716012	WebVPN User Directory access
716013	WebVPN User file access
716014	WebVPN User file access
716015	WebVPN User file access
716016	WebVPN User file access
716017	WebVPN User file access
716018	WebVPN User file access
716019	WebVPN User file access
716020	WebVPN User file access
716021	WebVPN user access file denied
716022	WebVPN Unable to connect proxy
716023	WebVPN session limit reached
716024	WebVPN User access error
716025	WebVPN User access error
716026	WebVPN User access error
716027	WebVPN User access error

EventID	EventName
716028	WebVPN User access error
716029	WebVPN User access error
716030	WebVPN User access error
716031	WebVPN User access error
716032	WebVPN User access error
716033	WebVPN User access error
716034	WebVPN User access error
716035	WebVPN User access error
716036	WebVPN User login successful
716037	WebVPN User login failed
716038	WebVPN User Authentication Successful
716039	WebVPN User Authentication Rejected
716040	WebVPN User logging denied
716041	WebVPN ACL hit count
716042	WebVPN ACL hit
716043	WebVPN Port forwarding
716044	WebVPN Bad Parameter
716045	WebVPN Invalid Parameter
716046	WebVPN connection terminated
716047	WebVPN ACL usage
716048	WebVPN memory issue
716049	WebVPN Empty SVC ACL
716050	WebVPN ACL error
716051	WebVPN ACL error
716052	WebVPN Session Terminated
716053	WebVPN SSO Server added
716054	WebVPN SSO Server deleted
716055	WebVPN Authentication Successful
716056	WebVPN Authentication Failed
716057	WebVPN Session terminated
716058	WebVPN Session lost
716059	WebVPN Session resumed

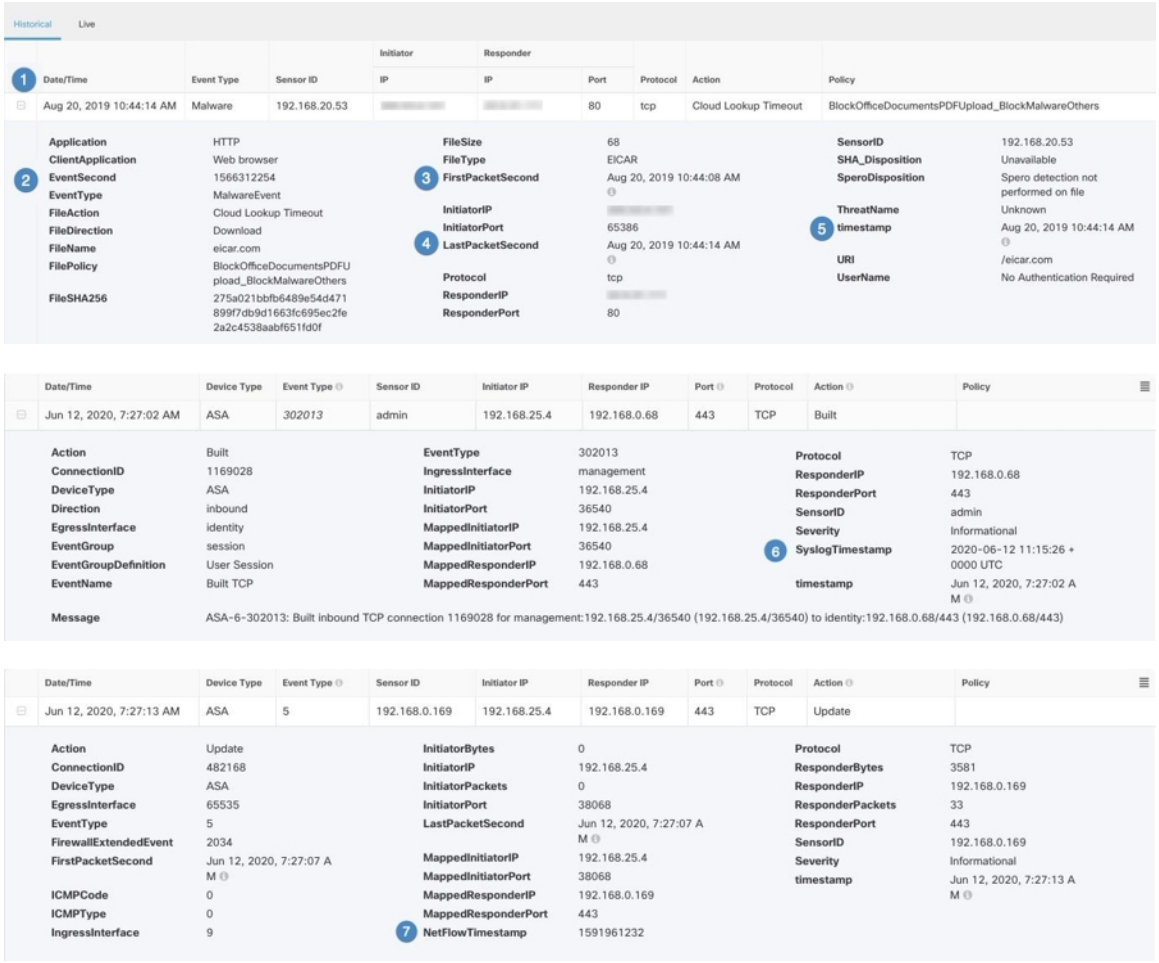
EventID	EventName
716060	WebVPN Session Terminated
722001	WebVPN SVC Connect request error
722002	WebVPN SVC Connect request error
722003	WebVPN SVC Connect request error
722004	WebVPN SVC Connect request error
722005	WebVPN SVC Connect update issue
722006	WebVPN SVC Invalid address
722007	WebVPN SVC Message
722008	WebVPN SVC Message
722009	WebVPN SVC Message
722010	WebVPN SVC Message
722011	WebVPN SVC Message
722012	WebVPN SVC Message
722013	WebVPN SVC Message
722014	WebVPN SVC Message
722015	WebVPN SVC invalid frame
722016	WebVPN SVC invalid frame
722017	WebVPN SVC invalid frame
722018	WebVPN SVC invalid frame
722019	WebVPN SVC Not Enough Data
722020	WebVPN SVC no address
722021	WebVPN Memory issue
722022	WebVPN SVC connection established
722023	WebVPN SVC connection terminated
722024	WebVPN Compression Enabled
722025	WebVPN Compression Disabled
722026	WebVPN Compression reset
722027	WebVPN Decompression reset
722028	WebVPN Connection Closed
722029	WebVPN SVC Session terminated
722030	WebVPN SVC Session terminated
722031	WebVPN SVC Session terminated

EventID	EventName
722032	WebVPN SVC connection Replacement
722033	WebVPN SVC Connection established
722034	WebVPN SVC New connection
722035	WebVPN Received Large packet
722036	WebVPN transmitting Large packet
722037	WebVPN SVC connection closed
722038	WebVPN SVC session terminated
722039	WebVPN SVC invalid ACL
722040	WebVPN SVC invalid ACL
722041	WebVPN SVC IPv6 not available
722042	WebVPN invalid protocol
722043	WebVPN DTLS disabled
722044	WebVPN unable to request address
722045	WebVPN Connection terminated
722046	WebVPN Session terminated
722047	WebVPN Tunnel terminated
722048	WebVPN Tunnel terminated
722049	WebVPN Session terminated
722050	WebVPN Session terminated
722051	WebVPN address assigned
722053	WebVPN Unknown client
723001	WebVPN Citrix connection Up
723002	WebVPN Citrix connection Down
723003	WebVPN Citrix no memory issue
723004	WebVPN Citrix bad flow control
723005	WebVPN Citrix no channel
723006	WebVPN Citrix SOCKS error
723007	WebVPN Citrix connection list broken
723008	WebVPN Citrix invalid SOCKS
723009	WebVPN Citrix invalid connection
723010	WebVPN Citrix invalid connection
723011	WebVPN citrix Bad SOCKS

EventID	EventName
723012	WebVPN Citrix Bad SOCKS
723013	WebVPN Citrix invalid connection
723014	WebVPN Citrix connected to Server
724001	WebVPN Session not allowed
724002	WebVPN Session terminated
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL handshake Started
725002	SSL Handshake completed
725003	SSL Client session resume
725004	SSL Client request Authentication
725005	SSL Server request authentication
725006	SSL Handshake failed
725007	SSL Session terminated
725008	SSL Client Cipher
725009	SSL Server Cipher
725010	SSL Cipher
725011	SSL Device choose Cipher
725012	SSL Device choose Cipher
725013	SSL Server choose cipher
725014	SSL LIB error
725015	SSL client certificate failed

Syslog イベントの時間属性

[イベントロギング（Event Logging）] ページのさまざまなタイムスタンプの目的を理解すると、関心のあるイベントをフィルタリングして見つけるのに役立ちます。



ケース	ラベル	説明
1	日時	Secure Event Connector（SEC）がイベントを処理した時刻。これは、ファイアウォールでそのトラフィックが検査された時刻と同じではない場合があります。タイムスタンプと同じ値。
2	EventSecond	LastPacketSecond と同じです。

ケース	ラベル	説明
3	FirstPacketSecond	接続が開かれた時刻。この時点で、ファイアウォールはパケットを検査します。 FirstPacketSecond の値は、LastPacketSecond から ConnectionDuration を差し引いて計算されます。 接続の開始時にログに記録される接続イベントの場合、FirstPacketSecond、LastPacketSecond、および EventSecond の値はすべて同じになります。
4	LastPacketSecond	接続が閉じた時刻。接続の最後に記録される接続イベントの場合、LastPacketSecond と EventSecond は等しくなります。
5	timestamp	Secure Event Connector（SEC）がイベントを処理した時刻。これは、ファイアウォールでそのトラフィックが検査された時刻と同じではない場合があります。[日時（Date/Time）] と同じ値。
6	syslog タイムスタンプ	「ロギングタイムスタンプ」が使用されている場合、syslog の開始時刻を表します。syslog にこの情報がない場合、SEC がイベントを受信した時刻が反映されます。
7	NetflowTimeStamp	ASA で、NetFlow パケットを埋めてフローコレクタに送信するのに十分なフローレコード/イベントの収集が終了した時刻。

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。