接続イベントとセキュリティ インテリジェンス イベント

次のトピックでは、接続およびセキュリティ イベント テーブルを使用する方法について説明します。

接続イベントについて

システムは、管理対象デバイスが検出した接続のログを生成することができます。このログは接続イベントと呼ばれます。ルールやポリシーの設定を行うことで、ログに記録する接続の種類、接続をログに記録するタイミング、およびデータを保存する場所をきめ細かく制御できます。セキュリティインテリジェンスイベントは特殊な接続イベントで、レピュテーションベースのセキュリティインテリジェンス機能によってブラックリストに登録されている（ブロックされた）接続を表します。詳細については、接続ロギングを参照してください。

関連トピック

セキュリティ インテリジェンスについて

接続イベントとセキュリティ インテリジェンス イベントの比較

セキュリティ インテリジェンス イベントは、レピュテーションベースのセキュリティ インテリジェンス機能によりセッションがブラックリストに登録された（ブロックされた）ときに生成される接続イベントです。

ただし、すべてのセキュリティインテリジェンスイベントに同一の接続イベントがあります。セキュリティ インテリジェンス イベントは個別に表示して分析できます。また、システムはセキュリティ インテリジェンス イベントを個別に保存およびプルーニングします。

システムは、より多くのリソースを消費する評価を行う前に、セキュリティインテリジェンスを実施することに注意してください。接続がセキュリティインテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

（注） 本書では違うと明記されていない限り、接続イベントに関する情報は、セキュリティインテリジェンス イベントに関する情報でもあります。

NetFlow 接続

管理対象デバイスで収集された接続データを補うために、NetFlowエクスポータによってブロードキャストされたレコードを使用して接続イベントを生成できます。この方法が特に役立つのは、NetFlow エクスポータが、管理対象デバイスでモニタしているネットワークとは別のネットワークをモニタしている場合です。

システムは NetFlow レコードを単方向の接続終了イベントとして Firepower Management Center データベースに記録します。これらの接続に関して使用可能な情報は、アクセス コントロール ポリシーで検出された接続の情報とは若干異なります。NetFlow データと管理対象デバイス データの違いを参照してください。

関連トピック

Firepower システムの NetFlow データ

接続の概要（グラフ用集約データ）

Firepower システムは 5 分間隔で収集された接続データを集約し、接続の概要を作成します。この概要を使用して、接続グラフとトラフィック プロファイルがシステムで生成されます。必要に応じて、接続の概要データに基づいてカスタム ワークフローを作成できます。これは、個々の接続イベントに基づいたワークフローと同じように使用できます。

セキュリティ インテリジェンス イベント専用の接続の概要はないことに注意してください。ただし、対応する接続終了イベントは接続の概要データに集約できます。

集約するには、複数の接続が以下の状態である必要があります。

- 接続終了を表している
- 送信元と宛先の IP アドレスが同じで、応答側（宛先）のホストで同じポートを使用している
- 同じプロトコルを使用している（TCP または UDP）
- 同じアプリケーション プロトコルを使用している
- 同じ Firepower システム管理対象デバイスまたは同じ NetFlow エクスポータによって検出される

各接続の概要には、接続数など全トラフィック統計情報が含まれています。NetFlowエクスポータは単一方向接続を生成するので、接続の概要では、NetFlow データに基づく接続ごとに接続数が 2 ずつ増えます。

接続の概要には、概要内の集約された接続に関するすべての情報が含まれているわけではありませんので注意してください。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にクライアント情報は含まれません。

長時間接続

接続データを集約する 5 分間隔の 2 回以上に監視対象のセッションがまたがる場合、その接続は長時間接続と見なされます。接続サマリーで接続数を計算する際には、長時間接続が開始された 5 分間隔の回のみカウントします。

また、長時間接続において発信側と応答側が送信したパケット数とバイト数を計算する際は、システムは5分間隔の各回で実際に送信されたパケット数とバイト数を報告しません。代わりにシステムは、送信された合計パケット数と合計バイト数、接続の長さ、5 分間隔の各回で接続のどの部分が行われたかに基づいて、一定の送信速度を仮定し、値を推定します。

外部応答側からの統合接続サマリー

接続データの保存に必要なスペースを減らし、接続グラフのレンダリングを高速化するために、システムは次の場合に接続サマリーを統合します。

- 接続に関連するホストの 1 つが監視対象のネットワーク上にない場合
- 外部ホストの IP アドレス以外で、サマリー内の接続がサマリー集約条件を満たす場合

[分析（Analysis）] > [接続（Connections）] サブメニュー ページで接続サマリーを表示する場合や、接続グラフを使用する場合、システムは非モニタ対象ホストの IP アドレスの代わりに `external` と表示します。

この集約の結果として、外部応答側を含む接続サマリーまたはグラフから接続データのテーブル ビューにドリルダウンしようとすると（つまり、個別の接続データへのアクセス）、テーブル ビューには情報が何も表示されません。

接続およびセキュリティ インテリジェンス イベント フィールド

表形式およびグラフィカル ワークフローを使用して表示や検索ができる接続およびセキュリティ インテリジェンス イベントには、次に示すフィールドがあります。個別のイベントで利用可能な情報は、システムがいつ、なぜ、どのようにして接続を記録したかによって異なることに注意してください。

（注） 各セキュリティ インテリジェンス イベントには、同一の、個別に保存された接続イベントがあります。すべてのセキュリティ インテリジェンス イベントに、入力済みの [セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] フィールドがあります。

接続グラフは接続サマリーに基づいているため、接続サマリーを制約しているのと同じ条件が接続グラフを制約します。検索ページのアスタリスク（*）が付いたフィールドは、接続グラフおよび接続サマリーを制約します。無効な検索条件を使用して接続サマリーを検索し、カスタム ワークフローの接続サマリー ページを使用して結果を見る場合、無効な条件には適用不可（N/A）としてラベルが付けられ、取り消し線が引かれます。

全般情報（General Information）

アクセス コントロール ポリシー（Access Control Policy）

接続をモニタしたアクセス コントロール ポリシー。

アクセス コントロール ルール（Access Control Rule）

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニタ ルール。

接続が 1 つのモニタ ルールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。接続が複数のモニタ ルールに一致した場合、一致するモニタ ルールの数が表示されます（`Default Action + 2 Monitor Rules` など）。

接続に一致した最初の 8 つのモニタ ルールのリストをポップアップ ウィンドウに表示するには、[N モニタ ルール（*N*Monitor Rules）] をクリックします。

アクション（Action）

接続をロギングした設定に関連付けられているアクション。

セキュリティ インテリジェンスによってモニタされている接続の場合、そのアクションは、接続によってトリガーされる最初のモニタ以外のアクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続と関連付けられたアクションが [モニタ（Monitor）] になることはありません。ただし、モニタ ルールに一致する接続の相関ポリシー違反をトリガーする可能性があります。

アクション	説明
許可（Allow）	アクセス コントロールによって明示的に許可された、またはユーザがインタラクティブ ブロックをバイパスしたために許可された接続。

アクション	説明
ブロック（Block）、リセットしてブロック（Block with reset）	次を含むブロックされた接続： • プレフィルタ ポリシーによってブロックされたトンネルおよびその他の接続 • セキュリティ インテリジェンスによってブラックリストに載せられた接続 • SSL ポリシーによってブロックされた暗号化接続 • 侵入ポリシーによってエクスプロイトがブロックされた接続 • ファイル ポリシーによってファイル（マルウェアを含む）がブロックされた接続。 システムが侵入またはファイルをブロックする接続では、アクセス コントロールの許可ルールを使用してディープ インスペクションを呼び出す場合にも、システムはブロックを表示します。
高速パス（Fastpath）	プレフィルタ ポリシーによって高速パスが適用された暗号化されていないトンネルおよびその他の接続。
インタラクティブ ブロック（Interactive Block）、リセット付きインタラクティブ ブロック（Interactive Block with reset）	システムがインタラクティブ ブロック ルールを使用してユーザの HTTP 要求を最初にブロックしたときにログに記録された接続。システムにより表示される警告ページでユーザがクリックスルーすると、そのセッションでログに記録されるその後の接続に許可アクションが付きます。
信頼（Trust）	アクセス コントロールによって信頼された接続。デバイス モデルに応じて、システムは信頼された TCP 接続を別にログに記録します。信頼されている接続のロギング を参照してください。
デフォルト アクション（Default Action）	アクセス コントロール ポリシーのデフォルト アクションによって処理される接続。

接続（Connections）

接続サマリーに含まれる接続数。長時間接続（複数回の接続サマリー間隔にまたがる接続）の場合、最初の接続サマリー間隔の分だけ増加します。[接続（Connections）] 条件を使用した検索で意味のある結果を表示するには、接続サマリー ページを持つカスタム ワークフローを使用する必要があります。

メンバー数（Count）

各行に表示される情報に一致する接続数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。カスタム ワークフローを作成し、ドリルダウン ページに [カウント（Count）] カラムを追加しない場合、各接続は個別に表示され、パケット数とバイト数は合計されません。

エンドポイント ロケーション（Endpoint Location）

ISE で指定された、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレス。

エンドポイント プロファイル（Endpoint Profile）

ISE で指定されたユーザのエンドポイント デバイス タイプ。

最初のパケットまたは最後のパケット（First Packet or Last Packet）

セッションの最初または最後のパケットが検出された日時。

イニシエータ/レスポンダ バイト（Initiator/Responder Bytes）

セッション イニシエータまたはセッション レスポンダが送信した合計バイト数。

イニシエータ/レスポンダ パケット（Initiator/Responder Packets）

セッション イニシエータが送信した合計パケット数。

イニシエータ ユーザ（Initiator User）（サマリーおよびグラフを制約）

セッション イニシエータにログインしていたユーザ。このフィールドに [認証なし（No Authentication）] が入力されている場合、ユーザ トラフィックは次のようになります。

- 関連付けられたアイデンティティ ポリシーがないアクセス コントロール ポリシーに一致しました。
- アイデンティティ ポリシーのいずれのルールにも一致しませんでした。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。

ネットワーク分析ポリシー（Network Analysis Policy）

イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ある場合）。

プレフィルタ ポリシー（Prefilter Policy）

接続を処理したプレフィルタ ポリシー。

理由（Reason）

多くの場合に接続がロギングされた 1 つまたは複数の原因。完全なリストについては、接続イベントの理由 （17 ページ）を参照してください。

IP ブロック、DNS ブロック、および URL ブロックの理由による接続には、固有のイニシエータ レスポンダ ペアごとに 15 秒のしきい値があります。システムがこれらのいずれかの接続をブロックした後、イベントを生成した時点から 15 秒の間、この 2 つのホスト間

で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、接続イベントを生成しません。

セキュリティ コンテキスト（Security Context）

ASA FirePOWER でマルチ コンテキスト モードで処理される接続で、トラフィックが通過した仮想ファイアウォール グループを特定するメタデータ。

セキュリティ グループ タグ（Security Group Tag）

接続に関係するパケットのセキュリティ グループ タグ（SGT）属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

セキュリティ インテリジェンスのカテゴリ（Security Intelligence Category）

接続でブラックリストに記載された IP アドレスを表すか、もしくはそれを含む、ブラックリストに記載されたオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワーク オブジェクトまたはグループ、ブラックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、またはインテリジェンス フィードのカテゴリのいずれかの名前にすることができます。

インテリジェンス フィードのカテゴリの詳細については、セキュリティ インテリジェンス オプション を参照してください。

TCP フラグ（TCP Flags）

NetFlow データから生成された接続において、接続で検出された TCP フラグ。このフィールドを検索する場合は、TCP フラグのカンマ区切りリストを入力することで、これらのフラグが *1* つ以上あるすべての接続が表示されます。

時刻（Time）

システムが接続を接続サマリーに集約するために使用した 5 分間隔の終了時刻。このフィールドは検索できません。

トラフィック（KB）（Traffic (KB)）（検索のみ）

接続で送信されたデータの総量（キロバイト単位）。

合計パケット（Total Packets）（検索のみ）

接続で送信された合計パケット数。

トンネル/プレフィルタ ルール（Tunnel/Prefilter Rule）

トンネル ルール、プレフィルタ ルール、または接続を処理したプレフィルタ ポリシーのデフォルト アクション。

Networking

宛先ポート/ICMP コード（Destination Port/ICMP Code）（サマリーおよびグラフを制約）

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。

DNS クエリ（DNS Query）

ドメイン名を検索するために接続でネーム サーバに送信された DNS クエリ。

DNS レコード タイプ（DNS Record Type）

接続で送信された DNS クエリを解決するために使用された DNS リソース レコードのタイプ。

DNS レスポンス（DNS Response）

問い合わせ時に接続でネーム サーバに返された DNS レスポンス。

DNS シンクホール名（DNS Sinkhole Name）

システムが接続をリダイレクトしたシンクホール サーバの名前。

DNS TTL

DNS サーバが DNS リソース レコードをキャッシュする秒数。

HTTP 応答コード（HTTP Response Code）

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。

入力/出力セキュリティ ゾーン（Ingress/Egress Security Zone）

接続に関連付けられた入力または出力のセキュリティ ゾーン。

再区分されたカプセル化接続では、元の入力セキュリティ ゾーンの代わりに、割り当てたトンネル ゾーンが入力フィールドに表示されます。出力フィールドは空白です。

イニシエータ/レスポンダ IP（Initiator/Responder IP）（サマリーおよびグラフを制約）

セッション イニシエータまたはレスポンダの IP アドレス（および DNS 解決が有効化されている場合はホスト名）。ブラックリストに記載された接続でブラックリストに記載された IP アドレスを識別できるように、ブラックリストに記載された IP アドレスの横のアイコンは見た目が少し異なります。

プレフィルタ ポリシーによってブロックされるか、高速パスが適用されたプレーン テキストのパススルー トンネルでは、これらの IP アドレスはトンネル エンドポイント（トンネルの両側のネットワーク デバイスのルーテッド インターフェイス）を表します。

クライアントのオリジナル IP（Original Client IP）

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

プロトコル（Protocol）（サマリーおよびグラフを制約、検索のみ）

接続に使用されるトランスポート プロトコルです。特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。

送信元ポート/ICMP タイプ（Source Port/ICMP Type）（サマリーおよびグラフを制約）

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。

VLAN ID（Admin. VLAN ID）

接続をトリガーしたパケットに関連付けられている最内部 VLAN ID。

位置情報（GeoLocation）

イニシエータ/レスポンダ国（Initiator/Responder Country）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた国。システムにより、国旗のアイコンと、国の ISO 3166-1 alpha-3 国番号が表示されます。国旗アイコンの上にポインタを移動すると、国の完全な名称が表示されます。

イニシエータ/レスポンダ大陸（Initiator/Responder Continent）

ルーティング可能な IP が検出された場合の、セッション イニシエータまたはレスポンダの IP アドレスに関連付けられた大陸。

クライアントのオリジナル国（Original Client Country）

元のクライアントの IP アドレスが属する国。この値を取得するために、システムは元のクライアント IP アドレスを X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから抽出し、それを地理位置情報データベース（GeoDB）を使用して国にマップします。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

Device

デバイス（Device）（サマリーおよびグラフを制約）

接続を検出した管理対象デバイス。または、NetFlow データから生成された接続の場合は、データを処理した管理対象デバイス。

ドメイン（Domain）

接続を検出した管理対象デバイスのドメイン。または、NetFlow データから生成された接続の場合は、データを処理した管理対象デバイスのドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。

入力/出力インターフェイス（Ingress/Egress Interface）

接続に関連付けられた入力または出力のインターフェイス。展開に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイスセットに属する場合があります。

SSL

SSL の実際の動作（SSL Actual Action）（検索のみ）

システムがSSLポリシーの暗号化トラフィックに適用したアクション。システムにより、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドにフィールド値が表示されます。

アクション	説明
ブロック（Block）/ リセットしてブロック（Block With Reset）	ブロックされた暗号化接続を表します。
復号（再署名）（Decrypt (Resign)）	再署名サーバ証明書を使用して復号された発信接続を表します。
復号（キーの交換）（Decrypt (Replace Key)）	置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。
復号（既知のキー）（Decrypt (Known Key)）	既知の秘密キーを使用して復号化された着信接続を表します。
デフォルトアクション（Default Action）	接続がデフォルト アクションによって処理されたことを示します。
復号しない（Do not Decrypt）	システムが復号しなかった接続を表します。

SSL 証明書ステータス（SSL Certificate Status）

これは、認証ステータスのSSLルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックがSSLルールに一致すると、このフィールドに次のサーバの証明書のステータス値の 1 つ以上が表示されます。

- 自署（Self Signed）
- 有効（Valid）
- 署名が無効（Invalid Signature）
- 発行元が無効（Invalid issuer）
- 期限切れ
- 不明
- まだ有効ではない（Not Valid Yet）
- 失効（Revoked）

復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [未チェック（Not Checked）] と表示されます。

SSL 証明書情報（SSL Certificate Information）（検索のみ）

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSL 暗号スイート（SSL Cipher Suite）

接続を暗号化するのに使用される暗号スイートを表すマクロ値。暗号スイート値の指定については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。

接続に適用された SSL 暗号化（SSL Encryption applied to the connection）（検索のみ）

yes または **no** を [SSL（SSL）] 検索フィールドに入力することで、SSL 暗号化された接続または暗号化されていない接続が表示されます。

SSL 予想アクション（SSL Expected Action）（検索のみ）

有効な SSL ルールで指定された、暗号化トラフィックに適用されると予想されるアクション。[SSL の実際の動作（SSL Actual Action）] にリストされている値を入力します。

SSL 失敗理由（SSL Failure Reason）

システムが暗号化されたトラフィックの復号に失敗した理由：

- 不明

- 不一致（No Match）
- Success
- キャッシュされていないセッション（Uncached Session）
- 不明な暗号スイート（Unknown Cipher Suite）
- サポートされていない暗号スイート（Unsupported Cipher Suite）
- サポートされていない SSL バージョン（Unsupported SSL Version）
- 使用された SSL 圧縮（SSL Compression Used）
- パッシブ モードで復号化できないセッション（Session Undecryptable in Passive Mode）
- ハンドシェイク エラー（Handshake Error）
- 復号エラー（Decryption Error）
- 保留中のサーバ名カテゴリの検索（Pending Server Name Category Lookup）
- 保留中の共通名カテゴリの検索（Pending Common Name Category Lookup）
- 内部エラー（Internal Error）
- 使用不可能なネットワーク パラメータ（Network Parameters Unavailable）
- 無効なサーバ証明書の処理（Invalid Server Certificate Handle）
- 使用不可能なサーバ証明書フィンガープリント（Server Certificate Fingerprint Unavailable）
- サブジェクト DN をキャッシュできない（Cannot Cache Subject DN）
- 発行元 DN をキャッシュできない（Cannot Cache Issuer DN）
- 不明な SSL バージョン（Unknown SSL Version）
- 使用不可能な外部証明書リスト（External Certificate List Unavailable）
- 使用不可能な外部証明書フィンガープリント（External Certificate Fingerprint Unavailable）
- 無効な内部証明書リスト（Internal Certificate List Invalid）
- 使用不可能な内部証明書リスト（Internal Certificate List Unavailable）
- 使用不可能な内部証明書（Internal Certificate Unavailable）
- 使用不可能な内部証明書フィンガープリント（Internal Certificate Fingerprint Unavailable）
- 使用不可能なサーバ証明書の検証（Server Certificate Validation Unavailable）
- サーバ証明書の検証エラー（Server Certificate Validation Failure）
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL フロー エラー（SSL Flow Error）

エラーが SSL セッション中に発生した場合はエラー名および 16 進数コード。エラーが発生しない場合は [成功（Success）]。

SSL フロー フラグ（SSL Flow Flags）

暗号化された接続の最初の 10 個のデバッグ レベル フラグ。ワークフロー ページでは、すべてのフラグを表示するには、省略記号（**...**）をクリックします。

SSL フロー メッセージ（SSL Flow Messages）

次のキーワードは、暗号化トラフィックが SSL ハンドシェイク時にクライアントとサーバ間で交換される指定されたメッセージタイプに関連付けられていることを示します。詳細については、http://tools.ietf.org/html/rfc5246を参照してください。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

SSL ポリシー（SSL Policy）

接続を処理した SSL ポリシー。

SSL ルール（SSL Rule）

接続を処理した SSL ルールまたはデフォルト アクションと、その接続に一致した最初のモニタ ルール。接続が 1 つのモニタ ルールに一致した場合、Firepower Management Center は接続を処理したルールの名前を表示し、その後にモニタ ルール名を表示します。

SSL セッション ID（SSL Session ID）

SSL ハンドシェイク時にクライアントとサーバ間でネゴシエートされた 16 進数セッション ID。

SSL ステータス（SSL Status）

暗号化された接続を記録した、[SSL の実際の動作（SSL Actual Action）]（SSL ルール、デフォルト アクション、または復号できないトラフィック アクション）に関連したアクション。ロック アイコン（  ）は、SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力することで、システムが処理した、または復号に失敗した暗号化トラフィックが表示されます。

SSL 件名/発行者の国（SSL Subject/Issuer Country）（検索のみ）

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

SSL チケット ID（SSL Ticket ID）

SSL ハンドシェイク時に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSL バージョン（SSL Version）

接続の暗号化に使用された SSL または TLS プロトコル バージョン。

- 不明
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TSLv1.2

Application

アプリケーション プロトコル（Application Protocol）（サマリーおよびグラフを制約）

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

アプリケーション プロトコル カテゴリとタグ（Application Protocol Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

アプリケーションのリスク（Application Risk）

接続で検出されたアプリケーショントラフィックに関連付けられたリスク。「非常に高い（Very High）」、「高（High）」、「中（Medium）」、「低（Low）」、「非常に低い（Very Low）」のいずれかとなります。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーショントラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

クライアントおよびクライアント バージョン（Client and Client Version）

接続で検出されたクライアントのクライアント アプリケーションとバージョン。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に「client」という語を付加して FTP client などと表示します。

クライアント カテゴリとタグ（Client Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

HTTP リファラ（HTTP Referrer）

接続で検出された HTTP トラフィックの要求 URL のリファラを示す HTTP リファラ（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

参照ホスト（Referenced Host）

接続のプロトコルが HTTP または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

ユーザ エージェント（User Agent）

接続で検出された HTTP トラフィックから取得したユーザ エージェント文字列アプリケーションの情報。

Web アプリケーション（Web Application）

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web ブランジング（Web Browsing）] と表示されます。

Web アプリケーションのカテゴリとタグ（Web Application Category and Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

URL

URL、URL カテゴリ、および URL レピュテーション（URL, URL Category, and URL Reputation）

セッション中にモニタ対象のホストによって要求された URL と、関連付けられたカテゴリおよびレピュテーション（利用できる場合）。

システムが SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL証明書に基づいてトラフィックを識別します。したがってSSLアプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

NetFlow

NetBIOS ドメイン（NetBIOS Domain）

セッションで使用された NetBIOS ドメイン。

NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）

NetFlow データから生成された接続の場合、接続のトラフィックの送信元または宛先に対する、Border Gateway Protocol の自律システム番号。

NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）

NetFlowデータから生成された接続の場合、送信元または宛先のIPアドレスに、送信元と宛先のプレフィックス マスクが追加されたもの。

NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlow エクスポータから出たときの Type of Service（TOS）バイトの設定。

NetFlow SNMP 入出力（NetFlow SNMP Input/Output）

NetFlow データから生成された接続の場合、接続トラフィックが NetFlow 対応デバイスに入ったか、NetFlowエクスポータから出た際のインターフェイスのインターフェイスインデックス。

ソース デバイス（Source Device）（サマリーおよびグラフを制約）

接続の生成に使用されたデータをブロードキャストする NetFlow エクスポータの IP アドレス。管理対象デバイスによって接続が検出された場合、このフィールドには`Firepower`と表示されます。

QoS

QoS がドロップされたイニシエータのバイト数（QoS-Dropped Initiator Bytes）/QoS がドロップされたレスポンダのバイト数（QoS-Dropped Responder Bytes）

レート制限によりセッション イニシエータまたはセッション レスポンダからドロップされたバイト数。

QoS がドロップされたイニシエータのパケット数（QoS-Dropped Initiator Packets）/QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）

レート制限によりセッション イニシエータまたはセッション レスポンダからドロップされたパケット数。

QoS が適用されたインターフェイス（QoS-Applied Interface）

レート制限された接続で、レート制限を適用するインターフェイスの名前。

QoS ポリシー（QoS Policy）

接続のレートを制限する QoS ポリシー。

QoS ルール（QoS Rule）

接続のレートを制限する QoS ルール。

関連イベント（Associated Events）

接続に関連付けられたイベントの検索に、接続やセキュリティ インテリジェンスのイベントの検索ページは使用できません。

ファイル（Files）

接続に関連付けられたファイル イベント（ある場合）。ファイルの表示アイコン（  ）は、ファイルのリストにリンクしています。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

侵入イベント（Intrusion Events）

接続に関連付けられた侵入イベント（ある場合）。侵入イベントの表示アイコン（  ）は、イベントのリストにリンクしています。

接続イベントの理由

接続イベントの [理由（Reason）] フィールドには、次の状況で接続がロギングされた理由が表示されます。

理由（Reason）	説明
コンテンツ制限（Content Restriction）	セーフサーチまたはYouTube EDU機能のいずれかに関連したコンテンツ制限を実施するために、パケットが変更されました。
DNS ブロック（DNS Block）	ドメイン名とセキュリティインテリジェンスデータに基づいて、インスペクションなしで接続が拒否されました。[DNS ブロック（DNS Block）] の理由は、DNS ルール アクションに応じて、[ブロック（Block）]、[ドメインが見つかりません（Domain not found）]、[シンクホール（Sinkhole）] のアクションと対として組み合わされます。
DNS モニタ（DNS Monitor）	システムはドメイン名とセキュリティインテリジェンスデータに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
ファイル ブロック（File Block）	ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いでいます。[ファイル ブロック（File Block）] の理由は必ず [ブロック（Block）] アクションと対として組み合わされます。
ファイル カスタム検出（File Custom Detection）	カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いでいます。
ファイル モニタ（File Monitor）	システムが接続において特定のファイルの種類を検出しました。
ファイル復帰許可（File Resume Allow）	ファイル送信がはじめに [ファイル ブロック（Block Files）] ルールまたは [マルウェア ブロック（Block Malware）] ファイル ルールによってブロックされました。ファイルを許可する新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に再開しました。この理由はインライン展開のみで表示されます。
ファイル復帰ブロック（File Resume Block）	ファイル送信がはじめに [ファイル検出（Detect Files）] ルールまたは [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ファイル ルールによって許可されました。ファイルをブロックする新しいアクセス コントロール ポリシーが展開された後、HTTP セッションが自動的に停止しました。この理由はインライン展開のみで表示されます。
インテリジェント アプリケーション バイパス（Intelligent App Bypass）	インテリジェント アプリケーション バイパス（IAB）モード： • アクションが [信頼（Trust）] の場合、IAB はバイパス モードでした。一致するトラフィックは、追加のインスペクションなしで通過しました。 • アクションが [許可（Allow）] の場合、IAB はテスト モードでした。一致するトラフィックは、追加のインスペクションに使用できました。

理由（Reason）	説明
侵入ブロック（Intrusion Block）	接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずでした。[侵入ブロック（Intrusion Block）] の理由は、ブロックされたエクスプロイトの場合は[ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
侵入モニタ（Intrusion Monitor）	接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [イベントを生成する（Generate Events）] に設定されている場合に発生します。
IP ブロック（IP Block）	IP アドレスとセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[IP ブロック（IP Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
IP モニタ（IP Monitor）	システムは IP アドレスとセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
SSL ブロック（SSL Block）	システムが SSL インスペクション設定に基づいて暗号化接続をブロックしました。[SSL ブロック（SSL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
URL ブロック（URL Block）	URL とセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続が拒否されました。[URL ブロック（URL Block）] の理由は必ず [ブロック（Block）] のアクションと対として組み合わされます。
URL モニタ（URL Monitor）	システムは URL とセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、システムは接続を拒否するのではなくモニタするように設定されています。
ユーザ バイパス（User Bypass）	最初にユーザの HTTP 要求をブロックしましたが、ユーザのクリックによって警告ページからサイトを表示しました。[ユーザ バイパス（User Bypass）] の理由は必ず [許可（Allow）] のアクションと対として組み合わされます。

接続イベント フィールドの入力の要件

接続イベント、セキュリティ インテリジェンス イベント、接続サマリーで利用可能な情報は、いくつかの要因によって異なります。

アプライアンス モデルおよびライセンス

多くの機能は、ターゲット デバイスで特定のライセンス付与対象の機能を有効にしなければ使用できません。また、一部のモデルでしか使用できない機能も多くあります。

たとえば、NGIPSv デバイスは SSL インスペクションをサポートしません。これらのデバイスは暗号化されたトラフィックを検査できないため、記録される接続イベントには暗号化された接続に関する情報は含まれていません。

トラフィックの特性

システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、イニシエータ ホストに関連付けられているユーザがいない、またはプロトコルが DNS、HTTP、または HTTPS ではない接続で検出される参照先ホストがいない可能性があります。

発信元/検出方法：トラフィック ベースの検出と NetFlow

NetFlow 専用フィールドを除き、NetFlow レコードで利用可能な情報は、トラフィック ベースの検出によって生成される情報よりも限定されます。NetFlowデータと管理対象デバイスデータの違いを参照してください。

評価ステージ

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。

たとえば、システムは、さらなるリソース集中型評価を行う前に、セキュリティ インテリジェンスを強制します。接続がセキュリティ インテリジェンスによってブロックされた場合、結果として生成されるイベントには、その後の評価によってシステムで収集されることになっていた情報（ユーザ ID など）が含まれません。

ロギング方法：接続の開始または終了

システムが接続の検出時にその接続の開始または終了（またはその両方）をログに記録できるかどうかは、システムがその接続をどのように検出して処理するように設定されているかによって異なります。

接続開始イベントには、セッション期間にわたってトラフィックを調査して判別しなければならない情報を伴っていません（送信されたデータの合計量や、接続の最終パケットのタイムスタンプなど）。また、接続開始イベントにセッションのアプリケーションや URL トラフィックに関する情報が伴っている保証もなく、セッションの暗号化に関する詳細は含まれていません。通常、ブロックされる接続については、接続開始イベントのログへの記録が唯一のオプションになります。

接続イベント タイプ：個々またはサマリー

接続サマリーには、集約された接続に関連付けられたすべての情報が含まれているわけではありません。たとえば、接続の概要に集約される接続にはクライアント情報が使用されないため、概要にはクライアント情報は含まれません。

接続グラフは、接続終了ログのみを使用する接続サマリーのデータに基づいていることに注意してください。接続開始データだけをロギングするようにシステムが設定されている場合、接続グラフと接続サマリーのイベント ビューにはデータが表示されません。

その他の設定

接続のロギングに影響するその他の設定には以下のものが含まれますが、これらに限定されるわけではありません。

- Active Directory ドメイン コントローラで認証するユーザに関連付けられている接続では、ISE が設定されている場合にのみ、ISE 関連のフィールドにデータが入力されます。接続イベントには、LDAP、RADIUS、RSA ドメイン コントローラで認証するユーザの ISE データは含まれません。
- [セキュリティ グループ タグ（Security Group Tag）] フィールドにデータが入力されるのは、ISE をアイデンティティ ソースとして設定した場合、またはカスタム SGT ルール条件を追加した場合のみです。
- プレフィルタ関連のフィールド（セキュリティ ゾーン フィールドのトンネル ゾーン情報を含む）には、プレフィルタ ポリシーで処理される接続の場合にのみ、データが入力されます。
- SSL 関連のフィールドには、SSL ポリシーで処理される暗号化接続の場合にのみ、データが入力されます。トラフィックの復号化が必要ない場合、Do Not Decrypt ルールの操作を使用して、フィールドの値を表示することができます。
- ファイル情報フィールドには、ファイル ポリシーと関連付けられたアクセス コントロール ルールによってログに記録される接続の場合にのみ、データが入力されます。
- 侵入情報フィールドには、侵入ポリシーに関連付けられているアクセス コントロール ルールあるいはデフォルト アクションによってログに記録される接続の場合にのみ、データが入力されます。
- QoS 関連のフィールドには、レート制限が適用される接続の場合にのみ、データが入力されます。
- [理由（Reason）] フィールドには、特定の場合にのみデータが入力されます（ユーザがインタラクティブ ブロック設定をバイパスしている場合など）。
- [ドメイン（Domain）] フィールドが表示されるのは、マルチテナンシー用に Firepower Management Center を設定した場合のみです。
- アクセス コントロール ポリシーの詳細設定では、HTTP セッションのモニタ対象ホストによって要求された URL ごとにシステムが接続ログに保存する文字数を制御できます。この設定を使用して URL のロギングを無効化する場合、システムは接続ログで個々の URL を表示しませんが、カテゴリとレピュテーションデータは参照できます（存在する場合）。

関連トピック

NetFlow データと管理対象デバイス データの違い

接続イベント フィールドで利用可能な情報

このトピックの表に、システムが接続およびセキュリティインテリジェンスのフィールドに値を読み込むことができるタイミングを示します。表の列は、次のイベントタイプを示しています。

- [発信元：直接（Origin: Direct）]：Firepower システムの管理対象デバイスで検出および処理される接続を表すイベント。
- [発信元：NetFlow（Origin: NetFlow）]：NetFlow エクスポータでエクスポートされる接続を表すイベント。
- [ロギング：開始（Logging: Start）]：開始時にログに記録される接続を表すイベント。
- [ロギング：終了（Logging: End）]：終了時にログに記録される接続を表すイベント。

表内の「はい（yes）」は、システムが接続イベント フィールドに値を読み込む必要があることを意味するものではなく、読み込むことができることを意味します。システムは、ネットワーク トラフィック内に存在する（および検出可能な）情報だけを報告します。たとえば、SSL 関連のフィールドには、SSL ポリシーによって処理される暗号化された接続のレコードについてのみ値が読み込まれます。

接続イベント フィールド	発信元：直接（Origin: Direct）	発信元：NetFlow（Origin: NetFlow）	ロギング：開始（Logging: Start）	ロギング：終了（Logging: End）
アクセス コントロール ポリシー（Access Control Policy）	Yes	No	Yes	Yes
アクセス コントロール ルール（Access Control Rule）	Yes	No	Yes	Yes
操作（Action）	Yes	No	Yes	Yes
アプリケーション プロトコル	Yes	Yes	利用可能な場合	Yes
アプリケーション プロトコル カテゴリとタグ（Application Protocol Category & Tag）	Yes	No	利用可能な場合	Yes
アプリケーションのリスク（Application Risk）	Yes	No	利用可能な場合	Yes
ビジネスとの関連性（Business Relevance）	Yes	No	利用可能な場合	Yes
クライアント（Client）	Yes	No	利用可能な場合	Yes

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
クライアント カテゴリとタグ（Client Category & Tag）	Yes	No	利用可能な場合	Yes
クライアント バージョン（Client Version）	Yes	No	利用可能な場合	Yes
接続（Connections）	Yes	Yes	No	Yes
メンバー数（Count）	Yes	Yes	Yes	Yes
宛先ポート/ICMP タイプ（Destination Port/ICMP Type）	Yes	Yes	Yes	Yes
Device	Yes	Yes	Yes	Yes
ドメイン（Domain）	Yes	Yes	Yes	Yes
DNS クエリ（DNS Query）	Yes	No	Yes	Yes
DNS レコード タイプ（DNS Record Type）	Yes	No	Yes	Yes
DNS レスポンス（DNS Response）	Yes	No	Yes	Yes
DNS シンクホール名（DNS Sinkhole Name）	Yes	No	Yes	Yes
DNS TTL	Yes	No	Yes	Yes
出力インターフェイス（Egress Interface）	Yes	No	Yes	Yes
出力セキュリティ ゾーン（Egress Security Zone）	Yes	No	Yes	Yes
エンドポイント ロケーション（Endpoint Location）	Yes	No	Yes	Yes
エンドポイント プロファイル（Endpoint Profile）	Yes	No	Yes	Yes
ファイル（Files）	Yes	No	No	Yes
最初のパケット（First Packet）	Yes	Yes	Yes	Yes

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
HTTP リファラ（HTTP Referrer）	Yes	No	No	Yes
HTTP 応答コード（HTTP Response Code）	Yes	No	Yes	Yes
入力インターフェイス（Ingress Interface）	Yes	No	Yes	Yes
入力セキュリティ ゾーン（Ingress Security Zone）	Yes	No	Yes	Yes
イニシエータ バイト数（Initiator Bytes）	Yes	Yes	有用でない	Yes
イニシエータの国（Initiator Country）	Yes	No	Yes	Yes
イニシエータ IP（Initiator IP）	Yes	Yes	Yes	Yes
イニシエータ パケット（Initiator Packets）	Yes	Yes	有用でない	Yes
イニシエータ ユーザ（Initiator User）	Yes	Yes	Yes	Yes
侵入イベント（Intrusion Events）	Yes	No	No	Yes
侵入ポリシー（Intrusion Policy）	Yes	No	Yes	Yes
IOC（侵害の兆候）（IOC (Indication of Compromise)）	Yes	No	Yes	Yes
最後のパケット（Last Packet）	Yes	Yes	No	Yes
NetBIOS ドメイン（NetBIOS Domain）	Yes	No	Yes	Yes
NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）	No	Yes	No	Yes

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）	No	Yes	No	Yes
NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）	No	Yes	No	Yes
NetFlow SNMP 入出力（NetFlow SNMP Input/Output）	No	Yes	No	Yes
ネットワーク分析ポリシー（Network Analysis Policy）	Yes	No	Yes	Yes
クライアントのオリジナル国（Original Client Country）	Yes	No	Yes	Yes
クライアントのオリジナル IP（Original Client IP）	Yes	No	Yes	Yes
プレフィルタ ポリシー（Prefilter Policy）	Yes	No	Yes	Yes
QoS が適用されたインターフェイス（QoS-Applied Interface）	Yes	No	No	Yes
QoS がドロップされたイニシエータのバイト数（QoS-Dropped Initiator Bytes）	Yes	No	No	Yes
QoS がドロップされたイニシエータのパケット数（QoS-Dropped Initiator Packets）	Yes	No	No	Yes
QoS がドロップされたレスポンダのバイト数（QoS-Dropped Responder Bytes）	Yes	No	No	Yes
QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）	Yes	No	No	Yes

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
QoS ポリシー（QoS Policy）	Yes	No	No	Yes
QoS ルール（QoS Rule）	Yes	No	No	Yes
理由（Reason）	Yes	No	Yes	Yes
参照ホスト（Referenced Host）	Yes	No	No	Yes
レスポンダ バイト数（Responder Bytes）	Yes	Yes	有用でない	Yes
レスポンダの国（Responder Country）	Yes	No	Yes	Yes
レスポンダ IP（Responder IP）	Yes	Yes	Yes	Yes
レスポンダ パケット（Responder Packets）	Yes	Yes	有用でない	Yes
セキュリティ コンテキスト（ASA のみ）（Security Context (ASA only)）	Yes	No	Yes	Yes
セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）	Yes	No	Yes	Yes
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	Yes	No	Yes	Yes
送信元デバイス（Source Device）	Yes	Yes	Yes	Yes
送信元ポート/ICMP タイプ（Source Port/ICMP Type）	Yes	Yes	Yes	Yes
SSL 証明書ステータス（SSL Certificate Status）	Yes	No	No	Yes
SSL 暗号スイート（SSL Cipher Suite）	Yes	No	No	Yes
SSL フロー エラー（SSL Flow Error）	Yes	No	No	Yes

接続イベント フィールド	発信元：直接（**Origin: Direct**）	発信元：**NetFlow**（**Origin: NetFlow**）	ロギング：開始（**Logging: Start**）	ロギング：終了（**Logging: End**）
SSL フロー フラグ（SSL Flow Flags）	Yes	No	No	Yes
SSL フロー メッセージ（SSL Flow Messages）	Yes	No	No	Yes
SSL ポリシー（SSL Policy）	Yes	No	No	Yes
SSL ルール（SSL Rule）	Yes	No	No	Yes
SSL セッション ID（SSL Session ID）	Yes	No	No	Yes
SSL ステータス（SSL Status）	Yes	No	No	Yes
SSL バージョン（SSL Version）	Yes	No	No	Yes
TCP フラグ（TCP Flags）	No	Yes	No	Yes
時刻（Time）	Yes	Yes	No	Yes
トンネル/プレフィルタ ルール（Tunnel/Prefilter Rule）	Yes	No	Yes	Yes
URL	Yes	No	利用可能な場合	Yes
URL カテゴリ（URL Category）	Yes	No	利用可能な場合	Yes
URL レピュテーション（URL Reputation）	Yes	No	利用可能な場合	Yes
ユーザ エージェント（User Agent）	Yes	No	No	Yes
VLAN ID（Admin. VLAN ID）	Yes	No	Yes	Yes
Web アプリケーション（Web Application）	Yes	No	利用可能な場合	Yes
Web アプリケーションのカテゴリとタグ（Web Application Category & Tag）	Yes	No	利用可能な場合	Yes

接続およびセキュリティインテリジェンスイベントテーブルの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

Firepower Management Center を使用して、接続イベントまたはセキュリティ インテリジェンス イベントのテーブルを表示することができます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

接続グラフにアクセスしたときに表示されるページは、使用するワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

接続またはセキュリティ インテリジェンス ワークフロー テーブルを使用すると、たくさんの一般的なアクションを実行できます。

ドリルダウン ページで接続イベントを制約する場合、同一のイベントからのパケット数とバイト数が合計されることに注意してください。ただし、カスタム ワークフローを使用しており、ドリルダウン ページに [カウント（Count）] カラムを追加していない場合、イベントは個別に表示され、パケット数とバイト数は合計されません。

システムが生成した接続イベントが 25 個を超えると、[接続イベント（Connection Events）] テーブル ビューに、使用可能なイベントのページ数ではなく、「1 of Many」と表示されます。

手順

ステップ 1 次のいずれかを選択します。

- **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**（接続イベントの場合）
- **[分析（Analysis）] > [接続（Connections）] > [セキュリティ インテリジェンス イベント（Security Intelligence Events）]**

（注） テーブルの代わりに接続グラフが表示された場合、ワークフロータイトルで [(ワークフローの切り替え)（(switch workflow)）] をクリックし、事前定義された [接続イベント（Connection Events）] ワークフローまたはカスタム ワークフローを選択します。事前定義されたすべての接続イベント（接続グラフを含む）は、接続のテーブル ビューで終了することに注意してください。

ステップ 2 次の選択肢があります。

- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更を参照してください。
- フィールド名：テーブルのカラムの内容について詳しく調べるには、接続およびセキュリティ インテリジェンス イベント フィールド （3 ページ）を参照してください。

  ヒント イベントのテーブル ビューでは、各アプリケーション タイプの [カテゴリ（Category）] および [タグ（Tag）] フィールド、NetFlow 関連のフィールド、SSL 関連のフィールドなど、いくつかのフィールドがデフォルトで非表示です。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。
- ユーザ プロファイル：ユーザ ID 情報を表示するには、ユーザ ID の横に表示されるユーザ アイコン（  または IOC に関連付けられたユーザのユーザ アイコン  ）をクリックします。
- ファイルおよびマルウェア：接続で検出されたまたはブロックされたマルウェアを含むファイルを表示するには、ファイルの表示アイコン（  ）をクリックし、接続で検出されたファイルとマルウェアの表示 （30 ページ）の説明に従って続行します。
- 侵入イベント：接続に関連付けられている侵入イベントを優先順位や影響とともに表示するには、[侵入イベント（Intrusion Events）] カラムの侵入イベント アイコン（  ）をクリックして、接続に関連付けられた侵入イベントの表示 （32 ページ）の説明に従って続行します。

  ヒント 1 つまたは複数の接続に関連付けられた侵入イベント、ファイル イベント、またはマルウェア イベントをすばやく表示するには、テーブルのチェックボックスを使用して接続を選択し、[ジャンプ（Jump to）] ドロップダウン リストから該当するオプションを選択します。セキュリティ インテリジェンスによりブラックリストに載せられている接続に関連するファイルまたは侵入が、アクセス制御ルールの評価の前にブロックされることによって、1 つも存在しない可能性があることに注意してください。ブラックリストではなく、接続をモニタするようにセキュリティ インテリジェンスを設定した場合に限り、セキュリティ インテリジェンス イベントに関するこの情報が表示されます。

- 証明書：接続を暗号化するために使用される利用可能な証明書についての詳細を表示するには、[SSL ステータス（SSL Status）] カラムの有効なロック アイコン（  ）をクリックします。

- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェックボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- イベントの削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。
- ドリル ダウン：ドリルダウン ページの使用を参照してください。

  ヒント ロギングされた接続に一致した複数のモニタ ルールのうち 1 つにドリル ダウンするには、[*N* モニタ ルール（N Monitor Rules）] の値をクリックします。表示されるポップアップ ウィンドウで、接続イベントを抑制するために使用するモニタ ルールをクリックします。

- このページに移動する：ワークフロー ページのトラバーサル ツールを参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。

関連トピック

概要：ワークフロー
イベント ビュー設定の設定

接続で検出されたファイルとマルウェアの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威またはマルウェア	保護またはマルウェア	任意（Any）	任意（Any）	Admin/Any Security Analyst

1 つまたは複数のアクセス制御ルールにファイル ポリシーを関連付けると、システムは一致するトラフィックのファイル（マルウェアを含む）を検出できます。[分析（Analysis）] > [接続

（Connections）] メニュー オプションを使用して、各ルールによってロギングされた接続と関連付けられているファイル イベント（存在する場合）を確認します。ファイル リストの代わりに、Firepower Management Center はファイル表示アイコン（  ）を [ファイル（Files）] 列に表示します。アイコンの数字は、その接続で検出またはブロックされたファイル数（マルウェア ファイルを含む）を示します。

すべてのファイルおよびマルウェアイベントが接続に関連付けられるわけではありません。具体的には次のとおりです。

- エンドポイントベースのマルウェアイベントは、接続に関連付けられていません。これらのイベントは AMP for Endpoints 展開からインポートされます。
- IMAP に対応した電子メール クライアントの多くは単一 IMAP セッションを使用し、それはユーザがアプリケーションを終了したときに終了します。長時間接続はシステムによってロギングされますが、セッションでダウンロードされたファイルは、そのセッションが終了するまで接続に関連付けられません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [接続（Connections）] の順に移動して、関連するオプションを選択します。

ステップ 2 接続イベントテーブルを使用している場合、ファイル表示アイコン（  ）をクリックします。ポップアップ ウィンドウが表示され、接続で検出されたファイルのリストとともに、そのタイプと、該当する場合はマルウェア処理が示されます。

ステップ 3 次の選択肢があります。

- 表示：ファイル イベントのテーブル ビューを表示するには、ファイルの表示アイコン（）をクリックします。
- 表示：マルウェア イベントのテーブル ビューに詳細を表示するには、マルウェア ファイルの表示アイコン（  ）をクリックします。
- 追跡：ネットワークを経由するファイルの伝送を追跡するには、ファイルのトラジェクトリ アイコン（  ）をクリックします。
- 表示：接続で検出されたファイルまたはネットワーク ベースのマルウェア イベントすべての詳細を表示するには、[ファイルイベントの表示（View File Events）] または [マルウェア イベントの表示（View Malware Events）] をクリックします。

接続に関連付けられた侵入イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威	保護	任意（Any）	任意（Any）	Admin/Any Security Analyst

アクセス制御ルールまたはデフォルトアクションに侵入ポリシーを関連付けると、システムは一致するトラフィックのエクスプロイトを検出できます。[分析（Analysis）] > [接続（Connections）] メニュー オプションを使用して、ロギングされた接続と関連付けられている侵入イベント（存在する場合）、およびそれらのイベントの優先順位と影響を確認します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 [分析（Analysis）] > [接続（Connections）] の順に移動して、関連するオプションを選択します。

ステップ 2 接続イベント テーブルを使用する場合、[侵入イベント（Intrusion Events）] カラムの侵入イベント アイコン（  ）をクリックします。

ステップ 3 表示されるポップアップ ウィンドウで、以下のオプションを選択できます。

- パケット ビューで詳細を表示するには、リストされたイベントの表示アイコン（  ）をクリックします。
- [侵入イベントの表示（View Intrusion Events）] をクリックして、接続に関連付けられた侵入イベントすべての詳細を表示します。

暗号化接続の証明書の詳細

[分析（Analysis）]> [接続（Connections）] メニューを使用して、システムで処理される接続を暗号化するために使用される公開キー証明書（使用可能な場合）を表示できます。証明書には次の情報が含まれています。

表 *1:* 暗号化接続の証明書の詳細

属性（**Attribute**）	説明
件名/発行元共通名（Subject/Issuer Common Name）	証明書のサブジェクトまたは証明書発行元のホストおよびドメイン名。
件名/発行元組織（Subject/Issuer Organization）	証明書のサブジェクトまたは証明書発行元の組織。

属性（Attribute）	説明
件名/発行元組織ユニット（Subject/Issuer Organization Unit）	証明書のサブジェクトまたは証明書発行元の部門。
有効期間の開始/終了（Not Valid Before/After）	証明書の有効期間。
シリアル番号（Serial Number）	発行元 CA によって割り当てられたシリアル番号。
証明書フィンガープリント（Certificate Fingerprint）	証明書の認証に使用する SHA ハッシュ値。
公開キー フィンガープリント（Public Key Fingerprint）	証明書に含まれる公開キーの認証に使用する SHA ハッシュ値。

デバイス サマリー ページの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	任意（Any）	任意（Any）	カスタム（Custom）

[接続サマリー（Connection Summary）] ページは、接続イベントの検索によって制限されたカスタム ロールを持ち、[接続サマリー（Connection Summary）] ページへのメニュー ベースの明示的なアクセスを許可されたユーザにのみ表示されます。このページは、監視対象ネットワーク上のアクティビティをさまざまな条件で整理したグラフを表示します。たとえば [一定期間の接続数（Connections over Time）] グラフでは、選択した間隔における監視対象ネットワーク上の接続の合計数が表示されます。

接続グラフでできる操作と同じことが、接続サマリーのグラフでも、ほぼすべてできます。ただし、[接続の概要（Connection Summary）] ページのグラフは集約データに基づいているため、グラフの基になっている個々の接続イベントを調べることはできません。つまり、接続サマリーのグラフから接続データのテーブル ビューにドリルダウンすることはできません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[概要（Overview）] > [概要（Summary）] > [接続の概要（Connection Summary）]**を選択します。

ステップ 2 [デバイスの選択（Select Device）] リストから、サマリーを表示したいデバイスを選択するか、もしくはすべてのデバイスのサマリーを表示するために [すべて（All）] を選択します。

ステップ 3 グラフ接続の操作および分析を行うには、接続イベント グラフの使用方法の説明に従って続行します。

ヒント デフォルトの時間範囲に影響を与えずにさらに分析を行えるように接続グラフ分離するには、[表示（View）] をクリックします。

関連トピック

ユーザ ロールのエスカレーション