接続およびセキュリティ関連の接続イベント

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で検出された接続のログを生成できます。このログは接続イベントと呼ばれます。接続イベントには、セキュリティ関連の接続イベント（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ロックされた接続）が含まれます。

接続イベントには、一般に、次によって検出されたトランザクションが含まれます。

- アクセス コントロール ポリシー
- 復号ポリシー
- （プレフィルタまたはトンネルルールによってキャプチャされた）プレフィルタ ポリシー
- DNS ブロックリスト
- URL ブロックリスト
- ネットワーク（IP アドレス）ブロックリスト

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。

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関連の接続イベントの比較

セキュリティ関連の接続イベントは、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関連の接続イベントに同一の接続イベントがあります。セキュリティ関連の接続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関連の接続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、セキュリティ関連の接続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 Secure Firewall 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

NetFlow データ

接続の概要（グラフ用集約データ）

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、接続サマリーの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。

セキュリティ関連の接続イベント専用の接続サマリー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サマリーの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

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、サマリ内の接続がサマリ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関連の接続イベントフィールド

（注） 接続に関連付けられたイベントの検索に、接続/セキュリティ関連の接続イベントの検索ページは使用できません。

[アクセスコントロールポリシー（Access Control Policy）]（Syslog：ACPolicy）

接続をモニターしたアクセス コントロール ポリシー。

[アクセス制御ルール（Access Control Rule）]（Syslog：AccessControlRuleName）

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 つのモニター ルール。

接続が 1 つのモニター ルールに一致した場合、Secure Firewall Management Center は接続を処理したルールの名前を表示し、その後にモニター ルール名を表示します。接続が複数のモニター ルールに一致した場合、一致するモニター 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 つのモニター 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 モニター ルール（***N***Monitor Rules）] をクリックします。

[アクション（Action）]（Syslog：AccessControlRuleAction）

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ー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ー以外のアクセス 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、モニター 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、モニター 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 [モニター（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、またはユーザー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ロックされた接続。 • 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ーの 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ー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。
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。
（空白/空）	ルールに一致するのに十分なパケットが渡される前に接続が閉じられました。 侵入防御などのアクセス制御以外の機能によって接続がログに記録される場合にのみ発生します。

[アプリケーションプロトコル（Application Protocol）]（syslog：ApplicationProtocol）

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを抑制します。

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 カテゴリおよびタグ（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）

接続中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：Very High、High、Medium、Low、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。

[認証ソース（Authentication Source）]

使用されている認証のタイプに基づいて、次のいずれかの値が含まれます。

- パッシブ アイデンティティ エージェントの**パッシブ アイデンティティ ソース**
- キャプティブポータルとして設定された Azure AD（SAML）レルムの **SAML キャプティブポータル**

詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

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、関連するビジネスとの関連性があります。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。

[クライアントとクライアントバージョン（Client and Client Version）]（Syslog：Client、ClientVersion）

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 カテゴリおよびタグ（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。

Connection Counter（Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

Connection Instance ID（Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

ConnectionDuration(Syslog のみ)

このフィールドは syslog フィールドとしてのみ存在します。Secure Firewall Management Center の Web インターフェイスにはありません。（Web インターフェイスは、[最初のパケット（First Packet）] 列と [最後のパケット（Last Packet）] 列を使用してこの情報を伝送します。）

このフィールドは、接続の最後にロギングが発生した場合にのみ、値が備わっています。接続開始の syslog メッセージでは、このフィールドは出力されません。その時点では不明であるためです。

接続終了の syslog メッセージでは、このフィールどは最初のパケットと最後のパケットまでの秒数が表示されます。短時間の接続ではゼロになることがあります。たとえば、syslog のタイムスタンプが 12:34:56 で ConnectionDuration が 5 の場合、最初のパケットは 12:34:51 に検出されました。

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。同一の行が複数作成される制約を適用した後にのみ、[Count] フィールドが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。

ピアの復号（Decrypt Peer）

関連付けられた接続のパケットを復号する VPN ピアの IP アドレス（ピアの IKE アドレス）。

VPN ピアの IP アドレスを表示するには、接続の開始時と接続の終了時にログを記録するアクセス コントロール ポリシー ルールのログ設定を有効にする必要があります。復号されたトラフィックのアクセス コントロール ポリシーのバイパス（sysopt connection permit-vpn）オプションを有効にした場合、復号されたトラフィックの詳細を表示できません。

復号ポリシー（Syslog：SSLPolicy）

接続を処理した SSL ポリシー。

アクセス コントロール ポリシーの詳細設定で TLS サーバーのアイデンティティ検出が有効になっている場合で、そのアクセス コントロール ポリシーに関連付けられている復号ポリシーがない場合、このフィールドにはどの説明についても何も保持されません。

復号ルール（Syslog：SSLRuleName）

接続を処理した復号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ールール。接続がモニター ルールに一致した場合、フィールドには接続を処理したルールの名前が表示され、その後にモニター ルール名が表示されます。

検出タイプ（Syslog：DetectionType）

このフィールドには、クライアントアプリケーションの検出元が表示されます。[AppID] または [暗号化された可視性（Encrypted Visibility）] のいずれかです。

[宛先ポート/ICMPコード（Destination Port/ICMP Code）]（Syslog：個別のフィールド - DstPort、ICMPCode）

Secure Firewall Management Center のインターフェイスでは、これらの値は概要とグラフを抑制します。

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。

DestinationSecurityGroup（Syslog のみ）

このフィールドには、 **Destinationsecuritygrouptag**（使用可能な場合）の数値に関連付けられているテキスト値が保持されます。グループ名をテキスト値として使用できない場合、このフィールドには、[DestinationSecurityGroupTag] フィールドと同じ整数値が含まれます。

[DestinationSecurityGroupType] (Syslog のみ)

このフィールドには、セキュリティグループタグを取得した送信元が表示されます。

値	説明
インライン	送信元 SGT 値はパケットからのものです
Session Directory	送信元 SGT 値は、セッション ディレクトリ トピックによる ISE からのものです
SXP	送信元 SGT 値は SXP トピックによる ISE からのものです

宛先 SGT（Syslog：DestinationSecurityGroupTag）

接続に関係する宛先のセキュリティ グループ タグ（SGT）属性。

送信元 SGT 値は、[DestinationSecurityGroupType] フィールドで指定された送信元から取得されます。

[検出タイプ（Detection Type）]

このフィールドには、クライアントの検出元が表示されます。

デバイス

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを抑制します。

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。

DeviceUUID（Syslog のみ）

イベントを生成した ファイアウォール デバイスの一意の識別子。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

[DNSクエリ（DNS Query）]（Syslog：DNSQuery）

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

このフィールドには、DNS フィルタリングが有効になっている場合の URL フィルタリング一致のドメイン名も保持できます。この場合、[URL] フィールドは空白になり、[URL Category] フィールドと [URL Reputation] フィールドにはドメインに関連付けられた値が含まれます。

DNS フィルタリングの詳細については、DNS フィルタリング：DNS ルックアップ中の URL レピュテーションとカテゴリの識別（ベータ版）を参照してください。

[DNSレコードタイプ（DNS Record Type）]（Syslog：DNSRecordType）

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応答（DNS Response）]（Syslog：DNSResponseType）

問い合わせ時に接続でネーム サーバーに返された DNS レスポンス。

[DNSシンクホール名 （DNS Sinkhole Name）]（Syslog：DNS_Sinkhole）

システムが接続をリダイレクトしたシンクホール サーバーの名前。

DNS TTL（syslog：DNS_TTL）

DNS サーバーが DNS リソース レコードをキャッシュする秒数。

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 Firewall Management Center を設定したことがある場合に表示されます。

ピアの暗号化（Encrypt Peer）

関連付けられた接続のパケットを暗号化する VPN ピアの IP アドレス（ピアの IKE アドレス）。

VPN ピアの IP アドレスを表示するには、接続の開始時と接続の終了時にログを記録するアクセス コントロール ポリシー ルールのログ設定を有効にする必要があります。

EVE フィンガープリント（Syslog：EncryptedVisibilityFingerprint）

セッションの暗号化された可視化エンジン（EVE）によって検出されたTLSフィンガープリント。[Cisco Secure Firewallアプリケーション検出器（Cisco Secure Firewall Application Detectors）]ページで追加の詳細を表示するためのアクセス権は、現在、シスコ以外の電子メールアドレスを持つユーザーは利用できません。

EVE プロセス名（Syslog：EncryptedVisibilityProcessName）

暗号化された可視性エンジン（EVE）によって分析されたTLSクライアントhelloパケットのプロセスまたはクライアント。

EVE プロセス確実性スコア（Syslog：EncryptedVisibilityConfidenceScore）

暗号化された可視性エンジンが適切なプロセスを検出しているかを示す0ー100％の範囲内の信頼値。たとえば、プロセス名がFirefoxで、信頼スコアが80％の場合、エンジンが検出したプロセスがFirefoxであると80％信頼していることを示します。

EVE 脅威の確実性（Syslog：EncryptedVisibilityThreatConfidence）

暗号化された可視性エンジンによって検出されたプロセスに脅威が含まれる確率のレベル。このフィールドは、脅威信頼スコアの値に基づいて、帯域（[Very High]、[High]、[Medium]、[Low]、または[Very Low]）を示します。

EVE 脅威の確実性スコア（Syslog：EncryptedVisibilityThreatConfidenceScore）

暗号化された可視性エンジンによって検出されたプロセスに脅威が含まれていることを示す0ー100％の範囲内の信頼値。脅威信頼スコアが非常に高い場合（90%など）、[暗号化された可視性プロセス名（Encrypted Visibility Process Name）]フィールドには[マルウェア（Malware）]と表示されます。

エンドポイント ロケーション（Endpoint Location）

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

エンドポイントのプロファイル (Syslog:Endpoint Profile)

ISEで指定されたユーザーのエンドポイント デバイス タイプ。

Event Priority（Syslog のみ）

接続イベントが優先度の高いイベントであるかどうか。高優先度（`High`）イベントは、侵入、セキュリティインテリジェンス、ファイル、またはマルウェアイベントに関連付けられた接続イベントです。他のすべてのイベントは低優先度（`Low`）イベントです。

ファイル (Syslog: FileCount)

1つ以上のファイルイベントに関連付けられている接続で検出またはブロックされたファイル（マルウェア ファイルを含む）の数。

Secure Firewall Management Centerの Webインターフェイスでは、[ファイルの表示（View Files）]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。

[最初のパケットまたは最後のパケット（First Packet or Last Packet）]（Syslog：ConnectionDuration フィールドを参照）

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。

First Packet Time（Syslog のみ）

システムが最初のパケットを検出した時間。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

HTTP Referrer (Syslog: HTTPReferer)

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）。

HTTP 応答コード (Syslog:HTTPResponse)

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/出力インターフェイス（Ingress/Egress Interface）]（Syslog：IngressInterface、EgressInterface）

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。展開に非対称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ライン ペアに属する場合があります。

[入力/出力セキュリティ ゾーン（Ingress/Egress Security Zone）]（Syslog：IngressZone、EgressZone）

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。

入力仮想ルータ/出力仮想ルータ（Syslog：Ingressvrf、 EgressVRF）

仮想ルーティングを使用するネットワークにおける、トラフィックがネットワークに出入りするときに通過する仮想ルータの名前。

イニシエータ/Responder バイト (Syslog: InitiatorBytes、 ResponderBytes)

セッション イニシエータが送信したバイトまたはセッション レスポンダが受信したバイトの総数。

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。

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 IP（Initiator/Responder IP）]（Syslog：SrcIP、DstIP）

Secure Firewall Management Center のインターフェイスでは、これらの値は概要とグラフを抑制します。

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）。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（26 ページ）も参照してください。

Secure Firewall Management Center の Web インターフェイスでは、ホストアイコンは接続がブロックされる原因となった IP アドレスを示します。

プレフィルタポリシーによってブロックされるか、または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、イニシエータとレスポンダの 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。

[イニシエータ/レスポンダのパケット数（Initiator/Responder Packets）]（Syslog：InitiatorPackets、ResponderPackets）

セッション イニシエータが送信したバイトまたはセッション レスポンダが受信したパケットの総数。

[イニシエータユーザー（Initiator User）]（Syslog：User）

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを制限します。

セッション イニシエータにログインしていたユーザー。このフィールドに [認証なし（No Authentication）] が入力されている場合、ユーザー 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。

該当する場合、ユーザー名の前には `<realm>\` が付いています。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意（26 ページ）も参照してください。

検査期間（Syslog：InspectionMicroseconds）

接続に関連付けられたパケットを検査するのにかかったミリ秒単位の時間。この期間は、最初のパケットの受信から検査プロセス完了までの時間で測定されます。この値は、各接続のパケットの検査に費やされる完全な処理時間を決定するのに役立ちます。

検査パケット（Syslog：InspectedPacketCount）

特定の接続で検査されたパケットの合計数。

[侵入イベント（Intrusion Events）]（syslog：IPSCount）

接続に関連付けられた侵入イベント（ある場合）の数。

Secure Firewall Management Center の Web インターフェイスでは、[侵入イベントの表示（View Intrusion Events）] アイコン（）はイベントのリストにリンクしています。

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。

MITRE ATT&CK

イベント中の任意の時点での ATT&CK フレームワークにおける攻撃の進行状況を示す進行状況グラフ。新しいペインでの拡張ビューをサポートし、MITRE の戦術、手法、および進行状況グラフの詳細を表示できます。

- 進行状況グラフをクリックすると、イベントの MITRE ATT&CK の詳細が表示されます。[MITRE ATT&CK] ウィンドウには、戦術、手法、サブ手法、および MITRE ページへのリンクが表示されます。
- 詳細を表示するウィンドウで、[詳細（Details）] をクリックすると、手法の一般的な説明が表示されます。

[NAT Source/Destination IP (Syslog: NAT_InitiatorIP, NAT_ResponderIP)]

セッションのイニシエータまたはレスポンダの NAT 変換後の IP アドレス。

[NAT Source/Destination Port (Syslog: NAT_InitiatorPort, NAT_ResponderPort)]

セッションのイニシエータまたはレスポンダの NAT 変換後のポート。

[NetBIOSドメイン（NetBIOS Domain）]（Syslog：NetBIOSDomain）

セッションで使用された NetBIOS ドメイン。

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。

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。

[ネットワーク分析ポリシー（Network Analysis Policy）]（Syslog：NAPPolicy）

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）。

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。

[元のクライアントのIP（Original Client IP）]（Syslog：originalClientSrcIP）

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。

その他のエンリッチメント

拡張ビューをサポートするイベントに関連付けられた非 MITRE 情報。

プレフィルタ ポリシー (Syslog:Prefilter Policy)

接続を処理したプレフィルタ ポリシー。

プロトコル (Syslog:Protocol)

Secure Firewall Management Center の Web インターフェイスは、次のようになります。

- この値は概要とグラフを抑制します。
- このフィールドは検索フィールドとしてのみ使用できます。

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。

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 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 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。

QUIC セッション ID

ファイアウォール内の QUIC 接続を一意に識別する 64 ビットの内部セッション識別子。

QUIC ストリーム ID

QUIC 接続内のストリームを一意に識別する 62 ビットのストリーム識別子。

[理由（Reason）]（Syslog：AccessControlRuleReason）

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 （26 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。

[参照先ホスト（Referenced Host）]（Syslog：ReferencedHost）

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。

SecIntMatchingIP(Syslog のみ)

どの IP アドレスが一致しているか。

有効な値：**None**、**Destination**、または**Source**。

[セキュリティコンテキスト（Security Context）]（Syslog：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。

[Security Intelligence Category (Syslog: URLSICategory, DNSSICategory , IPReputationSICategory)]

接続でブロックされた URL、ドメイン、または IP アドレスを表すか、またはそれを含む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、ブロックリスト、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、監視に関連する TID カテゴリ、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。

Secure Firewall Management Center の Web インターフェイスでは、DNS、ネットワーク（IP アドレス）、および URL セキュリティ インテリジェンスの接続イベントは 1 つのカテゴリ フィールドに結合されます。syslog メッセージでは、それらのイベントはタイプ別に固有です。

セキュリティ関連の接続イベントには、セキュリティ インテリジェンス イベントやその他の接続イベント（侵入イベントやマルウェアイベントをトリガーしたものなど）が含まれます。[セキュリティ インテリジェンスの概要（Security Intelligence Summary）] ワークフローには、すべてのセキュリティ インテリジェンス イベントがカテゴリや数ごとに表示されます。セキュリティ インテリジェンス カテゴリのないイベントは、グループ化され、数とのみ表示されます。

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 カテゴリ を参照してください。

Source Device

Secure Firewall Management Center の Web インターフェイスでは、この値は概要とグラフを抑制します。

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。

[送信元ポート/ICMPタイプ（Source Port/ICMP Type）]（Syslog：SrcPort、ICMPType）

Secure Firewall Management Center のインターフェイスでは、これらの値は概要とグラフを抑制します。

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。

SourceSecurityGroup（Syslog のみ）

このフィールドには、[SourceSecurityGroupTag]（使用可能な場合）の数値に関連付けられているテキスト値が保持されます。グループ名をテキスト値として使用できない場合、このフィールドには、[SourceSecurityGroupTag] フィールドと同じ整数値が含まれます。タグは、インラインデバイス（送信元SGT名が指定されていない）またはISE（送信元を指定している）から取得できます。

SourceSecurityGroupType (Syslog のみ)

このフィールドには、セキュリティグループタグを取得した送信元が表示されます。

値	説明
インライン	送信元 SGT 値はパケットからのものです
Session Directory	送信元 SGT 値は、セッション ディレクトリ トピックによる ISE からのものです
SXP	送信元 SGT 値は、SXP トピックによる ISE からのものです

送信元 SGT（Syslog：SourceSecurityGroupTag）

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）属性の数値表現。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。

TLS 実際のアクション（Syslog：SSLActualAction）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

システムは、検索ワークフローページの **TLS 状態** フィールドにフィールド値を表示します。

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。

アクション	説明
ブロック/リセット付きブロック（Block/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）	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）	置換された公開キーによる自己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（既知のキー）	既知の秘密キーを使用して復号された着信接続を表します。
デフォルトアクション	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	システムが復号化しなかった接続を表します。

TLS 証明書情報（Syslog：SSLCertificate）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

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）
- 有効期間の開始/終了（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）

TLS 証明書状態（Syslog：SSLServerCertStatus）

これは、証明書ステータスSSLルールの条件を設定した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ルールと一致する場合、次のサーバ証明書のステータス値の1つ以上がこのフィールドに表示されます。

- 自己署名
- 有効
- 署名が無効です
- 発行者が無効です
- 期限切れ
- 不明
- まだ有効ではありません
- 破棄

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。

TLS 暗号スイート（Syslog：SSSLCipherSuite）

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。暗号スイートの値の指定については、 https://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 TLS 暗号化

このフィールドは、Cisco Secure Firewall Management Center の Web インターフェイスで検索フィールドとしてのみ使用できます。

yes または **no** を [SSL] 検索フィールドに入力することで、TLS/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。

TLS 想定アクション（Syslog：SSLExpectedAction）

Secure Firewall Management Center の Web インターフェイスでは、このフィールドは検索フィールド専用です。

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。

TLS **の実際のアクション**に一覧された任意の値を入力します。

TLS 失敗の理由（Syslog：SSLFlowStatus）

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match

- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- 未完了のハンドシェイク（Incomplete Handshake）
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローページの **TLS 状態** フィールドに表示されます。

TLS フローエラー

エラーが TLS/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）]。

TLS フローフラグ

暗号化された接続の最初の 10 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。。

管理対象デバイスが過負荷の状態になっている場合は、OVER_SUBSCRIBED というメッセージが表示されます。詳細については、TLS/SSL オーバーサブスクリプションのトラブルシューティングを参照してください。

TLS フローメッセージ

次のキーワードは、暗号化トラフィックが TLS/SSL ハンドシェイク時にクライアントとサーバー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

- SERVER_NAME_MISMATCH

  セッションで表示されるサーバー証明書には、宛先ドメイン名に対応しない共通名または SAN 値があります。

- CERTIFICATE_CACHE_HIT

  宛先ドメイン名に一致する証明書がキャッシュ内で見つかりました。

- CERTIFICATE_CACHE_MISS

  宛先ドメイン名に一致する証明書がキャッシュ内で見つかりませんでした。

アプリケーションで TLS/SSL ハートビート エクステンションが使用されている場合は、HEARTBEAT というメッセージが表示されます。詳細については、TLS ハートビートについてを参照してください。

TLS セッション ID（Syslog：SSLSessionID）

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

TLS 状態

暗号化された接続を記録した **TLS の実際のアクション**（SSL ルール、デフォルトのアクションまたは、復号化できないトラフィックアクション）に関連付けられたアクション。[ロック（Lock）] 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、TLS/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。

システムが暗号化された接続の復号化に失敗した場合、実行された **TLS の実際のアクション**（復号化できないトラフィック アクション）および **TLS 失敗の理由** 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 [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。

暗号化された接続の SSL ハンドシェイクが未完了であり、システムがトラフィックの復号に失敗した場合、TLS **状態** フィールドに「不明（未完了のハンドシェイク）」と表示されます。

このフィールドを検索するときは、**TLS の実際のアクション** および **SSL 失敗の理由** の値を 1 つ以上を入力して、システムが処理した暗号化されたトラフィック、または復号化に失敗したトラフィックを表示します。

TLS サブジェクト/発行元国

このフィールドは Secure Firewall Management Center の Web インターフェイスのみで、検索フィールドとしてのみ使用できます。

暗号化証明書に関連付けられている件名または発行者の国に関する 2 文字の ISO 3166-1 アルファ 2 国コード。

TLS チケット ID（Syslog：SSLTicketID）

TLS/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。

SSLURLCategory（syslog のみ）

暗号化接続でアクセスされた URL の URL カテゴリ

このフィールドは syslog フィールドとしてのみ存在します。Secure Firewall Management Center の Web インターフェイスでは、このフィールドの値が URL カテゴリ列に組み込まれます。

URLを参照してください。

TLS バージョン（Syslog：SSLVersion）

接続の暗号化に使用された TLS/SSL プロトコル バージョン。

- 不明
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2
- TLSv1.3

[TCPフラグ（TCP Flags）]（Syslog：TCPFlags）

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。

TLS クライアント SNI（Syslog： SSLServerName）

このフィールドには、TLS **ClientHello** メッセージの Server Name Indication（SNI）値が表示されます。TLS **ClientHello** メッセージの SNI 値は、クライアントが接続しようとしているホスト名を示します。

[合計パケット数（Total Packets）]

このフィールドは検索フィールドとしてのみ使用できます。

接続で送信された合計パケット数。

[トラフィック（KB）（Traffic (KB)）]

このフィールドは検索フィールドとしてのみ使用できます。

接続で送信されたデータの総量（キロバイト単位）。

トンネル/プレフィルタ ルール (Syslog:Tunnel または 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。

[URL、URLカテゴリ、およびURLレピュテーション（URL, URL Category, and URL Reputation）]（syslog：URL、URLCategory および SSLURLCategory、URLReputation）

セッション中にモニター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）。

URL カテゴリとレピュテーションを表示するイベントでは、該当する URL ルールをアクセス コントロール ポリシーに含め、[URL] タブに URL カテゴリと URL レピュテーションを使用してルールを設定する必要があります。

URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

[URL] 列が空で、DNS フィルタリングが有効になっている場合、[DNS Query] フィールドにドメインが表示され、[URL Category] と [URL Reputation] の値がドメインに適用されます。

システムが TLS/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 TLS/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。

上記は **SSLURLCategory** も参照してください。

[ユーザーエージェント（User Agent）]（Syslog：UserAgent）

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

[VLAN ID]（Syslog：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。

VPN Action

接続に関連付けられた VPN アクション。

値は以下のとおりです。

- [暗号化（Encrypt）]：VPN は、ログに記録された接続のトラフィックを暗号化します。接続を暗号化する VPN ピアの IP アドレスを確認するには、[暗号化ピア（Encrypt Peer）] 列を参照してください。

- [復号（Decrypt）]：VPNは、ログに記録された接続のトラフィックを復号します。接続を復号するVPNピアのIPアドレスを確認するには、[復号ピア（Decrypt Peer）]列を参照してください。
- [VPNルーティング（VPN Routing）]：トラフィックはVPNトンネルを通過します。VPNは、接続の開始時に復号を実行し、接続の終了時に暗号化を実行します。接続を暗号化および復号するVPNピアのIPアドレスを確認すには、[暗号化ピア（Encrypt Peer）]列および[復号ピア（Decrypt Peer）]列を参照してください。

Webアプリケーション (Syslog: WebApplication)

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 と一致しなかった場合は、そのトラフィックがアドバタイズメントトラフィックなどの参照先のトラフィックの可能性があります。システムが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（使用可能な場合）を保存し、そのアプリケーションを Web アプリケーションとしてリストします。

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 カテゴリおよびタグ（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。

Zero Trustアプリケーション

エンドユーザーがアクセスを要求したアプリケーションの名前。

Zero Trustアプリケーショングループ

ルールに一致したアプリケーションがアプリケーショングループの一部である場合のアプリケーショングループの名前。

Zero Trustアプリケーションホスト

アプリケーションにアクセスするためにユーザーデバイスが要求したIPアドレスまたはホスト名。

Zero Trustアプリケーションポリシー

Cisco Zero Trustアプリケーションポリシーと一致したルールの名前。

Zero Trust発信元ユーザー

プライベートアプリケーションへのアクセスを要求したユーザーデバイスの固有ID。

Zero Trustプロキシ

ネットワークトラフィックをインターセプトしたCisco Zero Trustプロキシのドメイン名。

Zero Trustルール

接続要求と一致するルールの名前。

Zero Trustステータス

要求が成功したか失敗したかを示す Cisco Zero Trust アクセス要求の状態。

Zero Trustトンネル ID

Cisco Zero Trust アクセス中に Secure Client および Firewall Threat Defense デバイス間で確立されたトンネルの固有 ID。ユーザーは、セッション内で同じトンネルを使用して複数のプライベート アプリケーションにアクセスできます。

接続およびセキュリティ関連の接続イベントのフィールドについて

Secure Firewall Management Center の Web インターフェイスでは、[分析（Analysis）] > [接続（Connections）] サブメニューのテーブル形式とグラフィカルなワークフローを使用して、接続イベントとセキュリティ関連の接続イベントを表示したり検索することができます。

（注） 各セキュリティ関連の接続イベントには、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関連の接続イベントには、自動入力される [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。

個別のイベントで使用可能な情報は、システムがいつ、なぜ、どのようにして接続をログに記録したかによって異なります。

検索の制約

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。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。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。

syslog フィールド

ほとんどのフィールドは Secure Firewall Management Center Web インターフェイス内のほか、syslog メッセージとしても表示されます。同等にリストされている syslog のないフィールドは、syslog メッセージでは使用可能できません。いくつかのフィールドは（前述のように）syslog のみであり、その他のいくつかのフィールドは syslog メッセージ内の個別のフィールドですが、Web インターフェイス内では統合されたフィールドか、その逆です。

イニシエータ/レスポンダ、送信元/接続先、および送信者/受信者フィールドに関する注意

表 *1*: 用語の比較

フィールド	イベントタイプ	説明
イニシエータ/レスポンダ	接続	接続のイニシエータ/レスポンダ。 接続のイニシエータは、侵入の送信元またはマルウェアファイルの送信者と同じである必要はありません。
Source/Destination	Intrusion	攻撃の送信元/接続先。 侵入イベントの送信元は、接続のイニシエータまたはレスポンダです。
送信者/受信者 （Sending..., Receiving...）	ファイル、マルウェア	ファイルまたはマルウェアの送信者/受信者。 ファイルはアップロードまたはダウンロードされる可能性があるため、ファイルの送信者は必ずしも接続のイニシエータではありません。

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	説明
コンテンツ制限（Content Restriction）	セーフサーチ機能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）]	システムは検査を行わず、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しました。DNS ブロックの理由は、DNS ルール アクションに応じて、Block、Domain not found、または Sinkhole のアクションとペア化されます。
DNS モニタ	システムが、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が、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した。

理由	説明
エレファントフロー	接続は、エレファントフローと見なすのに十分な大きさです。このフローは、システム全体のパフォーマンスに影響を与えるのに十分な大きさです。デフォルトでは、エレファントフローとは1GB/10秒を超えるフローです。**system support elephant-flow-detection** コマンドを使用して、Firewall Threat Defense CLI でエレファントフローを識別するためのバイトしきい値と時間しきい値を調整できます。詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンス [英語] を参照してください。 （注） フローは、バイトと時間の両方のしきい値を超えた場合にのみ、エレファントフローと見なされます。 カスタムダッシュボードを作成して、エレファントフローと他の相互に関連するメトリック（Snort、システム、物理コアなどの CPU メトリックなど）を関連付けることができます。詳細については、「システムモニタリングとトラブルシューティング」の章を参照してください。
エレファントフローの除外（Elephant Flow Exempted）	エレファントフローが検出され、それが、修復から除外する必要があるフローに関して定義されている L4 ACL ルールに一致する場合。
Encrypted Visibility ブロック	Encrypted Visibility Engine がブロックした接続。
Encrypted Visibility IoC	Encrypted Visibility Engine が接続イベントに対して、高い、または非常に高いマルウェア確実性レベルで検出した Indications of Compromise (IoC) イベント。IoC イベントは、悪意のあるクライアントを使用してホストから生成された暗号化セッションに対してトリガーされます。悪意のあるホストの IP アドレス、MAC アドレス、OS 情報などの情報と、不審なアクティビティのタイムスタンプを表示できます。
Encrypted Visibility 免除	Encrypted Visibility Engine ブロックアクションをバイパスできる接続。
ファイル ブロック	接続に、システムが送信を阻止するファイルまたはマルウェア ファイルが含まれていました。[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	接続に、システムが送信を阻止するカスタム検出リストにあるファイルが含まれていました。
ファイル モニタ	システムが、接続に特定のタイプのファイルを検出しました。

理由	説明
ファイル再開許可	ファイル伝送が、元はファイル ブロック ルールまたはマルウェア ファイル ブロック 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）]	ファイル伝送が、元はファイル検出ルールまたはマルウェア クラウド ルックアップ 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。
[侵入ブロック（Intrusion Block）]	Snort3 エンジン：「ドロップするはず」の結果がある場合、接続イベントの理由は「侵入ブロック」ではなく空白です。「ドロップするはず」のイベントは、入力される接続イベントの理由に関して「許可」と同じように扱われます。
侵入モニタ	システムが、接続でエクスプロイト（侵入ポリシー違反）を検出しましたがブロックしませんでした。これは、トリガーされた侵入ルールの状態が Generate Events に設定されている場合に発生します。
IP ブロック	システムが検査する前に、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しました。IP ブロックの理由は、必ず、Block のアクションとペア化されます。
IP モニタ	システムが、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が、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した。
SSL ブロック（SSL Block）	システムが TLS/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）]	システムが検査する前に、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しました。URL ブロックの理由は、必ず、Block のアクションとペア化されます。

理由	説明
URL モニタ	システムが、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が、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した。
ユーザ バイパス	最初にユーザーの HTTP 要求をブロックしましたが、ユーザー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。[ユーザーバイパス（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。
保留中のルールの照合（Pending Rule Match）	ルールの評価が完了する前に接続が終了し、その接続中に一致するルールがありませんでした。システムは、この接続を、評価および「許可」アクションに関する保留中のルールとともにログに記録します。

接続イベント フィールドの入力の要件

接続イベント、セキュリティ関連接続イベント、または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。

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が伴ってません（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。

（注） セキュリティ関連の接続イベントには、セキュリティ インテリジェンス イベントやその他の接続イベント（侵入イベントやマルウェアイベントをトリガーしたものなど）が含まれます。[セキュリティ インテリジェンスの概要（Security Intelligence Summary）] ワークフローは、セキュリティ インテリジェンス カテゴリを持たないセキュリティ関連の接続イベントをグループ化し、[セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）] の値なしでカウントを表示します。

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ーの 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）]（SGT）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。

- TLS/SSL 関連のフィールドには、復号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 Secure Firewall 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）。
- URL カテゴリとレピュテーションを表示する接続イベントでは、該当する URL ルールをアクセス コントロール ポリシーに含め、[URL] タブに URL カテゴリと URL レピュテーションを使用してルールを設定する必要があります。URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

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）]：システム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、TLS/SSL関連のフィールドには、復号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	○	×	○	○
アクセスコントロール ルール（Access Control Rule）	○	×	○	○
Action	○	×	○	○
アプリケーション プロトコル	○	○	利用可能な場合	あり
アプリケーション プロトコル カテゴリとタグ（Application Protocol Category & Tag）	○	×	利用可能な場合	あり
Application Risk	○	×	利用可能な場合	○
ビジネス関連性	○	×	利用可能な場合	○
クライアント	○	×	利用可能な場合	あり
クライアントカテゴリとタグ（Client Category & Tag）	○	×	利用可能な場合	あり
Client Version	○	×	利用可能な場合	あり
Connections	○	○	×	○
Count	○	○	○	○
宛先ポート/ICMP タイプ（Destination Port/ICMP Type）	○	○	○	○
宛先 SGT（Destination SGT）	○	×	○	○

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**）
デバイス	○	○	○	○
ドメイン（Domain）	○	○	○	○
DNS クエリ（DNS Query）	○	×	○	○
DNS レコードタイプ（DNS Record Type）	○	×	○	○
DNS レスポンス（DNS Response）	○	×	○	○
DNS シンクホール名（DNS Sinkhole Name）	○	×	○	○
DNS TTL	○	×	○	○
Egress Interface	○	×	○	○
Egress Security Zone	○	×	○	○
エンドポイントロケーション（Endpoint Location）	○	×	○	○
エンドポイント プロファイル	○	×	○	○
ファイル	○	×	×	○
First Packet	○	○	○	○
HTTP リファラ（HTTP Referrer）	○	×	×	○
HTTP 応答コード（HTTP Response Code）	○	×	○	○
Ingress Interface	○	×	○	○
入力セキュリティゾーン（Ingress Security Zone）	○	×	○	○
Initiator Bytes	○	○	有用でない	yes
Initiator Country	○	×	○	○
イニシエータ IP（Initiator IP）	○	○	○	○

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**）
イニシエータパケット（Initiator Packets）	○	○	有用でない	yes
Initiator User	○	○	○	○
Intrusion Events	○	×	×	○
侵入ポリシー（Intrusion Policy）	○	×	○	○
IOC（侵害の兆候）（IOC (Indication of Compromise)）	○	×	○	○
最後のパケット（Last Packet）	○	○	×	○
NetBIOS Domain	○	×	○	○
NetFlow 送信元/宛先の自律システム（NetFlow Source/Destination Autonomous System）	×	○	×	○
NetFlow 送信元/宛先のプレフィックス（NetFlow Source/Destination Prefix）	×	○	×	○
NetFlow 送信元/宛先 TOS（NetFlow Source/Destination TOS）	×	○	×	○
NetFlow SNMP 入出力（NetFlow SNMP Input/Output）	×	○	×	○
ネットワーク分析ポリシー（Network Analysis Policy）	○	×	○	○
クライアントのオリジナル国（Original Client Country）	○	×	○	○
Original Client IP	○	×	○	○
プレフィルタポリシー（Prefilter Policy）	○	×	○	○

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 が適用されたインターフェイス（QoS-Applied Interface）	○	×	×	○
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バイト数（QoS-Dropped Responder Bytes）	○	×	×	○
QoS がドロップされたレスポンダのパケット数（QoS-Dropped Responder Packets）	○	×	×	○
QoS ポリシー	○	×	×	○
QoS ルール（QoS Rule）	○	×	×	○
理由	○	×	○	○
参照ホスト（Referenced Host）	○	×	×	○
Responder Bytes	○	○	有用でない	yes
Responder Country	○	×	○	○
Responder IP	○	○	○	○
Responder Packets	○	○	有用でない	yes
Security Context（ASA のみ）	○	×	○	○
セキュリティ インテリジェンスのカテゴリ	○	×	○	○
Source Device	○	○	○	○

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**）
Source Port/ICMP Type	○	○	○	○
送信元 SGT（Source SGT）	○	×	○	○
SSL Certificate Status	○	×	×	○
SSL Cipher Suite	○	×	×	○
SSL Flow Error	○	×	×	○
SSL Flow Flags	○	×	×	○
SSL Flow Messages	○	×	×	○
復号ポリシー	○	×	×	○
復号ルール	○	×	×	○
SSL セッション ID	○	×	×	○
SSL Status	○	×	×	○
SSL Version	○	×	×	○
TCP Flags	×	○	×	○
時刻	○	○	×	○
トンネル/プレフィルタルール（Tunnel/Prefilter Rule）	○	×	○	○
URL	○	×	利用可能な場合	あり
URL カテゴリ	○	×	利用可能な場合	あり
URLレピュテーション（URL Reputation）	○	×	利用可能な場合	あり
ユーザエージェント（User Agent）	○	×	×	○
VLAN ID	○	×	○	○

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**）
Web アプリケーション	○	×	利用可能な場合	あり
Web アプリケーションのカテゴリとタグ（Web Application Category & Tag）	○	×	利用可能な場合	あり

接続およびセキュリティ関連の接続イベントテーブルの使用

Secure Firewall Management Center を使用して、接続イベントまたはセキュリティ関連の接続イベントのテーブルを表示することができます。ここでユーザーは、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。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

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）] > [セキュリティ関連のイベント（Security-Related 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。
- データソース：データがセキュリティ分析とロギング（オンプレミス）を使用してリモートで保存されていて、データソースを変更する正当な理由がある場合は、データソースを選択します。このオプションに関する重要な情報については、Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Secure Firewall Management Center での作業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関連の接続イベントフィールド （4 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、デフォルトでこれらのフィールドは非表示にされています。表示されるフィールドを変更するには、任意の列名の [列の無効化（Disable Column）] ✕ をクリックしてフィールド選択ツールを表示します。

- 追加情報：システムの外部にある利用可能なソース内のデータを表示するには、イベント値を右クリックします。表示されるオプションはデータ タイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。詳細については、Web ベースのリソースを使用したイベントの調査を参照してください。
- 外部インテリジェンス：イベントに関する情報を収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査を参照してください。

- 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（Host Profile）]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[侵害を受けたホスト（Compromised Host）]をクリックします。
- ユーザープロファイル：ユーザーID情報を表示するには、[ユーザーID（User Identity）]の隣に表示される[ユーザー（User）]アイコン、またはIOCに関連付けられているユーザーの場合は[レッドユーザー（Red User）]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（View Files）]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 （40 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）]列の[侵入イベント（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の表示 （41 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ロックさ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。ブロックではなく、接続をモニター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）]列の[有効なロック（Enabled Lock）]をクリックします。
- 制約：表示される列を制約するには、非表示にする列の見出しにある[閉じる（Close）]（✕）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：（セキュリティ関連の接続イベントテーブルのみ）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て、[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ー ルールのうち 1 つにドリル ダウンするには、[*N* モニター 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ー 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。
- [ページ間の移動（Navigate Between Pages）]：現在のワークフローで現在の制約を保持したままページ間を移動するには、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 ビュー間の移動（Navigate Between Event Views）]：他のイベント ビューに移動して関連するイベントを表示するには、[移動先（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

1 つまたは複数のアクセス コントロール 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、Secure Firewall Management Center はファイル表示（  ）を [ファイル（Files）] 列に表示します。ファイル表示の数字は、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。

- エンドポイント向け AMP によって検出されたマルウェア イベント（「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、それはユーザー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。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

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（View Files）] 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（File's View）] 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（Malware File's View）] 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（File's Trajectory）] 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向け AMP によって検出されたマルウェア 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。

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

接続に関連付けられた侵入イベントの表示

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。

始める前に

このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリスト ユーザーである必要があります。

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）] 列の [侵入イベント（Intrusion Events）] 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（Listed Event's View）] 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。

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

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 *2:* 暗号化接続の証明書の詳細

属性	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。
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。

属性	説明
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。

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

デバイス サマリー ページの表示

[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ー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、[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 エスカレーションの有効化

接続イベントとセキュリティ インテリジェンス イベントの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Cisco Zero Trust Access セッションの接続監視の改善	7.7.10	Any	Cisco Zero Trust アクセスセッションの接続イベントフィールドが導入され、Zero Trust アクセスインシデントをより効果的に監視および調査できるようになりました。 • Zero Trustアプリケーションホスト • Zero Trust発信元ユーザー • Zero Trustプロキシ • Zero Trustルール • Zero Trustステータス • Zero TrustトンネルID 新規/変更された画面：**[分析（Analysis）]** > **[接続ヘッダ（Connections Header）]** > **[イベント（Events）]**
新しい接続イベントの理由：エレファントフロー。	7.1	任意（Any）	接続イベントの理由 （26 ページ）を参照してください。
NAT 変換済み IP アドレスとポート	7.1	任意（Any）	接続およびセキュリティ インテリジェンス イベント テーブルに 4 つの新しいフィールドが追加されました。 • NAT 送信元 IP（NAT Source IP） • NAT 宛先 IP（NAT Destination IP） • NAT 送信元ポート（NAT Source Port） • NAT 宛先ポート（NAT Destination Port）

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
リモートに保存された特定のイベントを操作するときにデータソースを選択する機能	7.0	任意（Any）	ワークフローの履歴を参照してください。
DNS フィルタリング	7.0 6.7（ベータ機能）	任意（Any）	DNS フィルタ処理が有効な場合： • [DNSクエリ（DNS Query）] フィールドは、一致する DNS フィルタ処理に関連付けられたドメインを保留できます。 • [URL] フィールドが空で、[DNSクエリ（DNS Query）]、[URLカテゴリ（URL Category）]、および [URLレピュテーション（URL Reputation）] には値がある場合、イベントは DNS フィルタ処理機能によって生成され、カテゴリとレピュテーションが [DNSクエリ（DNS Query）] で指定されたドメインに適用されます。 • Cisco Secure Firewall Management Center デバイス構成ガイド の「*DNS* フィルタリングとイベント」も参照してください。
接続イベントのカスタムテーブル向けサポートの削除	6.6	任意（Any）	接続イベントのカスタムテーブルを作成することはできなくなりました。アップグレードした場合、接続イベントのカスタムテーブルのうちすでに存在していたものは引き続き利用可能ですが、常に結果は返されません。 他のタイプのカスタムテーブルに変更はありません。 新規/変更された画面：**[分析（Analysis）] > [詳細（Advanced）][カスタムテーブル（Custom Tables）]** Platform：Firewall Management Center
接続イベントを削除およびすべて削除する機能の削除	6.6	任意（Any）	[削除（Delete）] および [すべて削除（Delete All）] ボタンは、接続イベントテーブルページから削除されました。 すべての接続イベントを消去するには、データの消去とストレージを参照してください。 新規/変更された画面：**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** Platform：Firewall Management Center

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
VRF および SGT の新しいフィールド	6.6	任意（Any）	• 入力仮想ルータ（Syslog：IngressVRF） • 出力仮想ルータ（Syslog：EgressVRF） • [DestinationSecurityGroupType]（Syslog のみ） • [SourceSecurityGroupType]（Syslog のみ）
新規および変更されたセキュリティグループタグのフィールド	6.5	任意（Any）	Firewall Management Center web インターフェイスのフィールドに変更を加えます： • 変更されたフィールド：[Security Group Tag] が [Source SGT] になりました • 新しいフィールド：[Destination SGT] Syslog フィールドへの変更： • 変更されたフィールド： [SecurityGroup] は [SourceSecurityGroupTag] になりました • 新しいフィールド： • [SourceSecurityGroup] • DestinationSecurityGroup • DestinationSecurityGroupTag サポートされるプラットフォーム：Firewall Management Center、管理対象デバイス
新しい syslog フィールド：[Event Priority]	6.5	任意（Any）	このフィールドは、接続イベントが侵入、ファイル、マルウェア、またはセキュリティ インテリジェンス イベントに関連付けられている場合に、その接続イベントを高優先度として識別します。
Syslog の接続イベントの固有識別子	6.4.0.4	任意（Any）	[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] の各 syslog フィールドの情報を総合すると、接続イベントを識別できます。

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。