



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 \(1 ページ\)](#)
- [接続イベントとセキュリティ インテリジェンス イベントのフィールド \(4 ページ\)](#)
- [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 \(30 ページ\)](#)
- [デバイス サマリー ページの表示 \(35 ページ\)](#)

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。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 (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 (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
- SSL 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 ブラックリスト
- URL ブラック リスト
- ネットワーク (IP アドレス) ブラックリスト

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 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) 本書では違ふ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 エクスポート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 エクスポートが、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、複数の接続が次のとおりでなければなりません。

- 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 エクスポート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 エクスポート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（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。

接続イベントとセキュリティインテリジェンス イベントのフィールド



(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。

Access Control Policy (Syslog: ACPolicy)

接続をモニタしたアクセス コントロール ポリシー。

アクセス制御ルール (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、Firepower Management Center は接続を処理したルールの名前を表示し、その後モニター 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 (NMonitor Rules)] をクリックします。

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、モニター ルールに一致する接続の関連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)	<p>次を含むブロックされた接続：</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>
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。The system logs trusted TCP connections differently depending on the device model.
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。

アプリケーション プロトコル (Syslog: ApplicationProtocol)

In the Firepower Management Center web interface, this value constrains summaries and graphs.

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するリスク：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のバージョン (Syslog:クライアント、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。

[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。

[Sensor UUID]、[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、接続イベントを一意に識別できます。

[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。

[Sensor UUID]、[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、接続イベントを一意に識別できます。

ConnectionDuration(Syslog のみ)

このフィールドはのみ存在する syslog フィールド;として存在しない、Firepower Management Center Web インターフェイス。(Web インターフェイスは、最初のパケットと最後のパケットの列を使用してこの情報を伝達します)。

このフィールドは、接続の終了時にロギングが発生した場合にのみ、値があります。開始-接続の Syslog メッセージのこのフィールドは、出力、これはその時点で知られませんでした。

エンド-接続の Syslog メッセージには、このフィールドは、最初のパケットと最後のパケットは、ゼロに短時間の接続があります間の秒数を示します。たとえば、syslog のタイムス

タンブは 12時 34分: 56 と、ConnectionDuration は 5、し、最初のパケットが観察された 12時 34分: 51 にします。

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。

宛先ポート/ICMP コード (Syslog: フィールド - DstPort、ICMPCode を分離)

Firepower Management Center Web インターフェイスでは、これらの値がサマリー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。

Device

In the Firepower Management Center web interface, this value constrains summaries and graphs.

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。

DNS クエリ (Syslog: DNSQuery)

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 レコードの種類 (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 (Syslog: DNSResponseType)

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 (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 サーバの名前。

DNS の TTL (Syslog: 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。

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。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

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。

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

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。

ファイル (Syslog: FileCount)

(マルウェア ファイルを含む) ファイルの数は、検出または1つまたは複数のファイル イベントに関連付けられている接続でブロックします。

In the Firepower Management Center web interface, the view files icon () links to a list of files. 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 (Syslog: ConnectionDuration | フィールドを参照してください)

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。

[Sensor UUID]、[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、接続イベントを一意に識別できます。

HTTP Referrer (Syslog: HTTPReferer)

接続で検出されたHTTPトラフィックの要求URLの参照元を示すHTTP参照元 (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: 要求に対する応答)

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/出カインターフェイス (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。

セキュリティ ゾーンの入力/出力 (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。

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

The total number of bytes transmitted by the session initiator or received by the session responder.

イニシエータ/レスポンド大陸 (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ドの IP アドレスに関連付けられた大陸。

イニシエータ/レスポンド国 (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ドの 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。

Initiator/Responder IP (Syslog: SrcIP, DstIP)

In the Firepower Management Center web interface, these values constrain summaries and graphs.

The IP address (and host name, if DNS resolution is enabled) of the session initiator (source IP address) or responder (destination IP address).

In the Firepower Management Center web interface, host icons next to blacklisted IP addresses look slightly different so that you can identify the blacklisted IP address in a blacklisted connection.

For plaintext, passthrough tunnels either blocked or fastpathed by the prefilter policy, source and destination IP addresses represent the tunnel endpoints—the routed interfaces of the network devices on either side of the tunnel.

イニシエータ/応答側パケット (Syslog: InitiatorPackets、 ResponderPackets)

The total number of packets transmitted by the session initiator or received by the session responder.

Initiator User (Syslog: User)


Firepower Management Centerサマリーとグラフに Web インターフェイス、この値が制限されます。

セッション イニシエータにログインしていたユーザ。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。

侵入イベント (Syslog: IPSCount)

The number of intrusion events, if any, associated with the connection.

In the Firepower Management Center web interface, the view intrusion events icon () links to a list of events.

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。

NetBIOS ドメイン (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 エクスポート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 エクスポートから出たときの Type of Service (TOS) バイトの設定。

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 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。

プレフィルタ ポリシー (Syslog: プレフィルタ ポリシー)

接続を処理したプレフィルタ ポリシー。

プロトコル (Syslog: プロトコル)

In the Firepower Management Center web interface:

- This value constrains summaries and graphs.
- This field is available only as a search field.

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ドのバイト数 (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ド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ドのパケット数 (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ド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。

理由 (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 \(20 ページ\)](#) 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ドペアごとに 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。

ホストの参照 (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 アドレスが一致します。

有効な値:なし、宛先、または送信元。

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。

セキュリティ グループ タグ (Syslog:セキュリティ グループ)

接続に関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 カテゴリ (Syslog: URLSICategory、 DNSSICategory、 IPReputationSICategory、)

The name of the blacklisted object that represents or contains the blacklisted URL, domain, or IP address in the connection. 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、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。

Firepower Management Center Web インターフェイス、DNS、ネットワーク (IP アドレス)、および URL のセキュリティ インテリジェンス接続のイベントが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によって特定です。

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。

[Sensor UUID] (Syslog のみ)

イベントを生成した Firepower デバイスの一意の識別子。

[Sensor UUID]、[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、接続イベントを一意に識別できます。

Source Device

In the Firepower Management Center web interface, this value constrains summaries and graphs.

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 エクスポートの 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 (Syslog: SrcPort、 ICMPType)

In the Firepower Management Center web interface, these values constrain summaries and graphs.

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。

SSL Actual Action (Syslog: SSLActualAction)

In the Firepower Management Center web interface, this field is a search field only.

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。

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 (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)]	システムが復号化しなかった接続を表します。

SSL 証明書情報 (Syslog: SSLCertificate)

In the Firepower Management Center web interface, this field is a search field only.

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 Certificate Status (Syslog: SSLServerCertStatus)

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)]
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- Unknown
- 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 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)

このフィールドは、Firepower 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 (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。

SSL 期待アクション (Syslog: SSLExpectedAction)

In the Firepower Management Center web interface, this field is a search field only.

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
- 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 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 [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。On a workflow page, to view all flags, click the ellipsis (...).

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。

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 TLS/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

アプリケーションで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、TLS/SSL 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。

SSL ポリシー (Syslog: SSLPolicy)

接続を処理した SSL ポリシー。

SSL ルール (Syslog: SSLRuleName)

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。If the connection matched a Monitor rule, the field displays the name of the rule that handled the connection, followed by the Monitor rule name.

SSLServerName(Syslog のみ)

This field exists ONLY as a syslog field; it does not exist in the Firepower Management Center web interface.

Hostname of the server with which the client established an encrypted connection.

SSL 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、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 Subject/Issuer Country

このフィールドはでのみ使用可能なFirepower Management CenterWeb インターフェイス、および [検索] フィールドとしてのみ。

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。

SSL 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 Only)

URL categories for the URL visited in the encrypted connection.

このフィールドはのみ存在する syslog フィールド; として Firepower Management Center URL カテゴリ列で Web インターフェイス、このフィールドに値が含まれています。

URLを参照してください。

SSL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

TCP フラグ (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。

Total Packets

This field is available only as a search field.

接続で送信された合計パケット数。

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: トンネルまたはプレフィルタールール)

トンネルルール、プレフィルタールール、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 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 エージェント (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。

Web アプリケーション (Syslog: web アプリケーション)

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 ブラウジング (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。

接続とセキュリティ インテリジェンス イベントのフィールドについて

Firepower 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 インテリジェンス イベントを表示したり、検索できます。



- (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。

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 Firepower 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 のみのフィールドですが、その他のいくつかは、syslog メッセージ内の個別のフィールドが Web インターフェイス内に統合されたフィールド、またはその逆のフィールドです。

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、バ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せられます。
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せられます。
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。

理由 (Reason)	説明
[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： <ul style="list-style-type: none"> • 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)	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せられます。
[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せられます。
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 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せられます。

理由 (Reason)	説明
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せられます。
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せられます。

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 TLS/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、接続サマリーに接続を集約する際にクライアント情報は使用されないため、サマリーに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。
- TLS/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 エクスポート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、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	はい	いいえ	はい	はい
アクセス コントロール ルール (Access Control Rule)	はい	いいえ	はい	はい
Action	はい	いいえ	はい	はい
アプリケーション プロトコル	はい	はい	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)	はい	いいえ (No)	利用可能な場 合	yes
アプリケーションのリスク (Application Risk)	はい	いいえ (No)	利用可能な場 合	yes
ビジネス関連性	はい	いいえ (No)	利用可能な場 合	yes
クライアント	はい	いいえ (No)	利用可能な場 合	yes
クライアント カテゴリとタグ (Client Category & Tag)	はい	いいえ (No)	利用可能な場 合	yes
Client Version	はい	いいえ (No)	利用可能な場 合	yes
Connections	はい	はい	いいえ	はい
Count	はい	はい	はい	はい
宛先ポート/ICMP タイプ (Destination Port/ICMP Type)	はい	はい	はい	はい
デバイス	はい	はい	はい	はい
ドメイン (Domain)	はい	はい	はい	はい
DNS クエリ (DNS Query)	はい	いいえ	はい	はい
DNS レコード タイプ (DNS Record Type)	はい	いいえ	はい	はい

接続イベント フィールド	発信元：直接 (Origin: Direct)	発信元： NetFlow (Origin: NetFlow)	ログギング：開 始 (Logging: Start)	ログギング：終 了 (Logging: End)
DNS レスポンス (DNS Response)	はい	いいえ	はい	はい
DNS シンクホール名 (DNS Sinkhole Name)	はい	いいえ	はい	はい
DNS TTL	はい	いいえ	はい	はい
Egress Interface	はい	いいえ	はい	はい
Egress Security Zone	はい	いいえ	はい	はい
エンドポイント ロケーション (Endpoint Location)	はい	いいえ	はい	はい
エンドポイント プロファイル	はい	いいえ	はい	はい
ファイル	はい	いいえ	いいえ	はい
First Packet	はい	はい	はい	はい
HTTP リファラ (HTTP Referrer)	はい	いいえ	いいえ	はい
HTTP 応答コード (HTTP Response Code)	はい	いいえ	はい	はい
Ingress Interface	はい	いいえ	はい	はい
入力セキュリティゾーン (Ingress Security Zone)	はい	いいえ	はい	はい
Initiator Bytes	はい	はい	有用でない	yes
Initiator Country	はい	いいえ	はい	はい
イニシエータ IP (Initiator IP)	はい	はい	はい	はい
イニシエータ パケット (Initiator Packets)	はい	はい	有用でない	yes
Initiator User	はい	はい	はい	はい
Intrusion Events	はい	いいえ	いいえ	はい

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)
侵入ポリシー (Intrusion Policy)	はい	いいえ	はい	はい
IOC (侵害の兆候) (IOC (Indication of Compromise))	はい	いいえ	はい	はい
最後のパケット (Last Packet)	はい	はい	いいえ	はい
NetBIOS Domain	はい	いいえ	はい	はい
NetFlow 送信元/宛先の自律システム (NetFlow Source/Destination Autonomous System)	いいえ	はい	いいえ	はい
NetFlow 送信元/宛先のプレフィックス (NetFlow Source/Destination Prefix)	いいえ	はい	いいえ	はい
NetFlow 送信元/宛先 TOS (NetFlow Source/Destination TOS)	いいえ	はい	いいえ	はい
NetFlow SNMP 入出力 (NetFlow SNMP Input/Output)	いいえ	はい	いいえ	はい
ネットワーク分析ポリシー (Network Analysis Policy)	はい	いいえ	はい	はい
クライアントのオリジナル国 (Original Client Country)	はい	いいえ	はい	はい
Original Client IP	はい	いいえ	はい	はい
プレフィルタ ポリシー (Prefilter Policy)	はい	いいえ	はい	はい
QoS が適用されたインターフェイス (QoS-Applied Interface)	はい	いいえ	いいえ	はい
QoS がドロップされたイニシエータのバイト数 (QoS-Dropped Initiator Bytes)	はい	いいえ	いいえ	はい

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 がドロップされたイニシエータの パケット数 (QoS-Dropped Initiator Packets)	はい	いいえ	いいえ	はい
QoS がドロップされたレスポ ンダのバイト数 (QoS-Dropped Responder Bytes)	はい	いいえ	いいえ	はい
QoS がドロップされたレスポ ンダのパケット数 (QoS-Dropped Responder Packets)	はい	いいえ	いいえ	はい
QoS ポリシー	はい	いいえ	いいえ	はい
QoS ルール (QoS Rule)	はい	いいえ	いいえ	はい
理由	はい	いいえ	はい	はい
参照ホスト (Referenced Host)	はい	いいえ	いいえ	はい
Responder Bytes	はい	はい	有用でない	yes
Responder Country	はい	いいえ	はい	はい
Responder IP	はい	はい	はい	はい
Responder Packets	はい	はい	有用でない	yes
Security Context (ASA のみ)	はい	いいえ	はい	はい
セキュリティ グループ タグ (SGT)	はい	いいえ	はい	はい
セキュリティ インテリジェン スのカテゴリ	はい	いいえ	はい	はい
Source Device	はい	はい	はい	はい
Source Port/ICMP Type	はい	はい	はい	はい
SSL Certificate Status	はい	いいえ	いいえ	はい
SSL Cipher Suite	はい	いいえ	いいえ	はい

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 Flow Error	はい	いいえ	いいえ	はい
SSL Flow Flags	はい	いいえ	いいえ	はい
SSL Flow Messages	はい	いいえ	いいえ	はい
SSL ポリシー	はい	いいえ	いいえ	はい
SSL Rule	はい	いいえ	いいえ	はい
SSL セッション ID	はい	いいえ	いいえ	はい
SSL Status	はい	いいえ	いいえ	はい
SSL Version	はい	いいえ	いいえ	はい
TCP Flags	いいえ	はい	いいえ	はい
時刻	はい	はい	いいえ	はい
トンネル/プレフィルタ ルール (Tunnel/Prefilter Rule)	はい	いいえ	はい	はい
URL	はい	いいえ (No)	利用可能な場 合	yes
URL カテゴリ	はい	いいえ (No)	利用可能な場 合	yes
URLレピュテーション (URL Reputation)	はい	いいえ (No)	利用可能な場 合	yes
ユーザ エージェント (User Agent)	はい	いいえ	いいえ	はい
VLAN ID	はい	いいえ	はい	はい
Web アプリケーション	はい	いいえ (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)	はい	いいえ (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数	サポートされるドメイン数	アクセス
いずれか (Any)	いずれか (Any)	いずれか (Any)	いずれか (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。

ステップ 1 次のいずれかを選択します。

- [Analysis] > [Connections] > [Events] (接続イベントの場合)
- [Analysis] > [Connections] > [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、[接続イベントとセキュリティ インテリジェンス イベントのフィールド \(4 ページ\)](#) 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、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、TLS/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。

- トランザクション コンテキストと詳細：(所属する組織でイベント データを外部の Firepower システムに保存している場合) パケットや履歴データなど、イベントに関連する情報を調査するには、イベントの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、[を使用したイベント調査 Cisco Security Packet Analyzer](#) および [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。
- User Profile — To view user identity information, click the user icon that appears next to the user identity (📄), or for users associated with IOCs, (📄).
- 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 \(32 ページ\)](#) 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 \(34 ページ\)](#) 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、アクセスコントロール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 ログिंग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

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数	サポートされるドメイン数	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	いずれか (Any)	いずれか (Any)	Admin/Any Security Analyst


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、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。

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。
-

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数	サポートされるドメイン数	アクセス
Threat	Protection	いずれか (Any)	いずれか (Any)	Admin/Any Security Analyst

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 익스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。

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	説明
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。
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。
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。

属性	説明
Not Valid Before/After	証明書の有効期間。
Serial Number	発行元 CA によって割り当てられたシリアル番号。
Certificate Fingerprint	証明書の認証に使用する SHA ハッシュ値。
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数	サポートされるドメイン数	アクセス
いずれか (Any)	いずれか (Any)	いずれか (Any)	いずれか (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。

ステップ 1 [Overview] > [Summary] > [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](#)