セキュリティイベントの Syslog メッセージ

- セキュリティイベントの Syslog メッセージの ID （1 ページ）
- 侵入イベントのフィールドの説明 （2 ページ）
- 接続およびセキュリティ インテリジェンス イベントのフィールドの説明 （6 ページ）
- ファイルおよびマルウェアイベントのフィールドの説明 （18 ページ）
- セキュリティイベントの Syslog メッセージの履歴 （25 ページ）

セキュリティイベントの Syslog メッセージの ID

- 430001：侵入イベント

  この ID はリリース 6.3 で導入されました。

- 430002：接続の開始時に記録された接続イベント

  この ID はリリース 6.3 で導入されました。

- 430003：接続の終了時に記録された接続イベント

  この ID はリリース 6.3 で導入されました。

- 430004：ファイルイベント

  これらのイベントの Syslog サポートはリリース 6.4 で導入されました。

- 430005：ファイルマルウェアイベント

  これらのイベントの Syslog サポートはリリース 6.4 で導入されました。

侵入イベントのフィールドの説明

（注） リリース 6.3 以降、空の値または不明な値を持つフィールドは Syslog メッセージに含まれません。

AccessControlRuleName

このフィールドはリリース 6.5 以降の該当する侵入イベントの Syslog メッセージに含まれます。

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています。

次の場合、このフィールドは空になります（または、syslog メッセージの場合は省略されます）。

- [関連付けられたルールなし/デフォルトアクションなし（No associated rule/default action）] : 侵入インスペクションがアクセス コントロール ルールにもデフォルト アクションにも関連付けられていない場合。たとえば、パケットがデフォルトの侵入ポリシーによって検査された場合などです。
- [関連付けられている接続イベントなし（No associated connection event）] : セッションに記録された接続イベントがデータベースから消去されている場合。たとえば、接続イベントに侵入イベントよりも高いターンオーバーがある場合などです。

ACPolicy

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効になっている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 ポリシー。

ApplicationProtocol

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィック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。

Classification

イベントを生成したルールが属する分類。

Client

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニタ対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

Connection Counter

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定の侵入イベントに関連付けられた接続イベントを識別できます。

Connection Instance ID

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定の侵入イベントに関連付けられた接続イベントを識別できます。

DstIP

侵入イベントに関連する受信ホストが使用する IP アドレス。

DstPort

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

EgressInterface

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列には入力されません。

EgressZone

イベントをトリガーとして使用したパケットの出力セキュリティゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

First Packet Time （FirstPacketSecond）

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定の侵入イベントに関連付けられた接続イベントを識別できます。

GID

ジェネレータ ID。イベントを生成したコンポーネントの ID。

HTTPResponse

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。

ICMPCode

「**DstPort**」を参照してください。

ICMPType

「**SrcPort**」を参照してください。

IngressInterface

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブ インターフェイスの場合、このインターフェイスの列だけに入力されます。

IngressZone

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーンまたはトンネル ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

InlineResult

このフィールドはバージョン 6.3 で Syslog を介して使用できるようになりました。

このフィールドは次の値を持ちます。

- **`Dropped`**：インライン展開環境でパケットがドロップされる場合
- **`Would have dropped`**：インライン展開環境でパケットをドロップするように侵入ポリシーが設定されていればパケットがドロップされた場合

パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

IntrusionPolicy

このフィールドはバージョン 6.4 で Syslog を介して使用できるようになりました。

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

MPLS_Label

このフィールドはバージョン 6.3 で追加されました。

侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

Message

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハード コーディングされています。

ジェネレータおよび Snort ID（GID と SID）と SID バージョン（改訂）はカッコで囲んだコロン区切りの数字形式で各メッセージの末尾に付加されます（GID:SID:version）。例：**`(1:36330:2)`**。

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（ある場合）。

このフィールドには、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

NumIOC

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。

Priority

Cisco Talos Intelligence Group（Talos） で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高（high）]、[中（medium）]、および [低（low）] です。

Protocol

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポートプロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

Revision

イベントの生成に使用された署名のバージョン。

Sensor UUID

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定の侵入イベントに関連付けられた接続イベントを識別できます。

SID

イベントを生成したルールの署名 ID（Snort ID ともいう）

SSLActualAction

システムが暗号化されたトラフィックに適用したアクション。

SrcIP

侵入イベントに関連する送信ホストが使用する IP アドレス。

SrcPort

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

User

送信元ホストにログインしている既知のユーザのユーザ ID。

リリース 6.5 以降： 該当する場合、ユーザ名の前には `<realm>\` が付いています。

VLAN_ID

このフィールドはバージョン 6.3 で追加されました。

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

WebApplication

侵入イベントをトリガーとして使用したトラフィックで検出された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。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムは代わりに一般的な Web ブラウジング指定を提供します。

接続およびセキュリティ インテリジェンス イベントのフィールドの説明

（注） リリース 6.3 以降、空の値または不明な値を持つフィールドは Syslog メッセージに含まれません。

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。
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。

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 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）。

AccessControlRuleReason

接続がロギングされた 1 つまたは複数の原因（使用可能な場合）。

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。

ACPolicy

接続をモニタしたアクセス コントロール ポリシー。

ApplicationProtocol

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。

クライアント

接続で検出されたクライアント アプリケーション。

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。

ClientVersion

接続で検出されたクライアント アプリケーションのバージョン（使用可能な場合）。

Connection Counter

このフィールドはリリース 6.4.0.4 で追加されました。

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、接続イベントを識別できます。

Connection Instance ID

このフィールドはリリース 6.4.0.4 で追加されました。

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、接続イベントを識別できます。

ConnectionDuration

このフィールドはバージョン 6.3 で導入されました。

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。

DestinationSecurityGroup

このフィールドはリリース 6.5 で導入されました。

接続に関係する宛先のセキュリティグループ。

このフィールドと [DestinationSecurityGroupTag] は、名前と値のペアです。対応する **DestinationSecurityGroupTag** フィールドが値を持つ場合でも、このフィールドは不明である可能性があります。

SourceSecurityGroup と **SourceSecurityGroupTag** のフィールド定義も参照してください。

DestinationSecurityGroupTag

このフィールドはリリース 6.5 で導入されました。

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。SGT は、信頼ネットワーク内のトラフィック宛先の権限を指定します。

DestinationSecurityGroup とこのフィールドは、名前と値のペアです。対応する DestinationSecurityGroup フィールドの値が不明な場合でも、このフィールドは値を持つ可能性があります。

「**SourceSecurityGroupTag**」も参照してください。

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_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。

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。

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。

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。

DNSSICategory

「**URLSICategory**」を参照してください。

DstIP

セッションレスポンダの IP アドレス（宛先 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）。

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、送信元と宛先の 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。

DstPort

セッション レスポンダが使用するポート。

EgressInterface

接続に関連付けられた出力インターフェイス。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。

EgressVRF

このフィールドのサポートはバージョン 6.6 で追加されました。

仮想ルーティングおよびフォワーディングを使用するネットワークでは、トラフィックがネットワークから出るときに通過する仮想ルータの名前。

EgressZone

接続に関連付けられた出力セキュリティ ゾーン。

再ゾーン化されたカプセル化接続の場合、出力フィールドは空白になります。

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。

Event Priority

このフィールドはリリース 6.5 で追加されました。

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。

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。

First Packet Time

このフィールドはリリース 6.4.0.4 で追加されました。

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、接続イベントを識別できます。

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）。

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。

ICMPCode

セッションレスポンダが使用する ICMP コード。

ICMPType

セッションイニシエータが使用する ICMP タイプ。

IngressInterface

接続に関連付けられた入力インターフェイス。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。

IngressZone

接続に関連付けられた入力セキュリティ 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。

InitiatorBytes

セッション イニシエータが送信した合計バイト数。

InitiatorPackets

セッション イニシエータが送信した合計パケット数。

IPReputationSICategory

「**URLSICategory**」を参照してください。

IPSCount

接続に関連付けられた侵入イベント（ある場合）の数。

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）。

NetBIOSDomain

セッションで使用された NetBIOS ドメイン。

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。

Prefilter Policy

接続を処理したプレフィルタ ポリシー。

Protocol

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。

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。

ResponderBytes

セッションレスポンダが受信した合計バイト数。

ResponderPackets

セッションレスポンダが受信した合計パケット数。

SecIntMatchingIP

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**。

セキュリティ グループ（Security Group）

リリース 6.5 では、このフィールドが **SourceSecurityGroupTag** フィールドに置き換えられ、**SourceSecurityGroup**、**DestinationSecurityGroupTag**、および **DestinationSecurityGroup** の新しいフィールドが導入されました。

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。

Sensor UUID

このフィールドはリリース 6.4.0.4 で追加されました。

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、接続イベントを識別できます。

SourceSecurityGroup

このフィールドはリリース 6.5 で追加されました。

接続に関係する送信元のセキュリティグループ。

このフィールドと [SourceSecurityGroupTag] は、名前と値のペアです。対応する **SourceSecurityGroupTag** フィールドが値を持つ場合でも、このフィールドは不明である可能性があります。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（送信元を指定する）から取得できます。

[DestinationSecurityGroup] と [DestinationSecurityGroupTag] も参照してください。

SourceSecurityGroupTag

リリース 6.5 では、**Security Group** フィールドがこのフィールドに置き換えられました。

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。

「**DestinationSecurityGroupTag**」も参加してください。

SrcIP

セッションイニシエータ の IP アドレス（送信元 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）。

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、送信元と宛先の 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。

SrcPort

セッション イニシエータが使用するポート。

SSLActualAction

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。

アクション	説明
[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。

SSLCertificate

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）

SSLExpectedAction

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。

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（Unknown）
- 不一致（No Match）
- 成功（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）

SSLPolicy

接続を処理した SSL ポリシー。

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。接続がモニタ 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 ルール名が表示されます。

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）]
- [有効（Valid）]
- [署名が無効（Invalid Signature）]
- [発行元が無効（Invalid issuer）]
- [期限切れ（Expired）]
- [不明（Unknown）]
- [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。

SSLServerName

クライアントが暗号化された接続を確立した相手側サーバのホスト名。

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。

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

暗号化接続でアクセスされた URL の URL カテゴリ

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。

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

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。

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。

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

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。

URLCategory

セッション中にモニタ対象ホストによって要求された URL のカテゴリ（使用可能な場合）。

URLReputation

セッション中にモニタ対象ホストによって要求された URL のレピュテーション（使用可能な場合）。

URLSICategory、DNSSICategory、IPReputationSICategory

接続でブラックリストに登録された URL、ドメイン、または IP アドレスを表すか、もしくはそれを含む、ブラックリストに登録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、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。

User

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。

リリース 6.5 以降： 該当する場合、ユーザ名の前には `<realm>\` が付いています。

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

このフィールドはバージョン 6.3 で Syslog を介して使用できるようになりました。

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。

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 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。

ファイルおよびマルウェアイベントのフィールドの説明

ファイルおよびマルウェアイベントの Syslog メッセージはリリース 6.4 で使用できるようになりました。

（注）

- 空の値または不明な値を持つフィールドはセキュリティイベントの Syslog メッセージに含まれません。ただし、「Unknown」または類似の値を持つ判定はファイルおよびマルウェアイベントのメッセージに含まれます。
- ファイルおよびマルウェアイベントのステータスフィールドの値には、初期ステータスのみが反映します。これらのフィールドは更新されません。

ApplicationProtocol

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーションプロトコル。

ArchiveDepth

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

ArchiveFileName

マルウェア ファイルが含まれていたアーカイブ ファイル（ある場合）の名前。

ArchiveFileStatus

調査中のアーカイブのステータス。次のいずれかの値になります。

- [保留中（Pending）]：アーカイブは調査中です
- [取得済み（Extracted）]：調査が問題なく正常に実行されました
- [失敗（Failed）]：システムのリソース不足のため調査に失敗しました。
- [深度の超過（Depth Exceeded）]：調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました
- [暗号化（Encrypted）]：部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています
- [調査できませんでした（Not Inspectable）]：部分的に正常に実行されましたが、ファイルは形式が不正であるか破損しています

ArchiveSHA256

マルウェア ファイルを含むアーカイブ ファイル（ある場合）の SHA-256 ハッシュ値。

Client

1 つのホストで実行され、ファイルを送信するためにサーバに依存するクライアント アプリケーション。

Connection Counter

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定のファイルおよびマルウェアイベントに関連付けられた接続イベントを識別できます。

Connection Instance ID

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定のファイルおよびマルウェアイベントに関連付けられた接続イベントを識別できます。

DstIP

接続に応答したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル受信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル送信者の IP アドレスです。

SrcIP も参照してください。

DstPort

DstIP で説明されている接続で使用されるポート。

FileAction

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

FileDirection

接続中にファイルがダウンロードされたか、またはアップロードされたか。値は次のとおりです。

- Download：ファイルは DstIP から SrcIP に転送されました。
- Upload：ファイルは SrcIP から DstIP に転送されました。

FileName

ファイルの名前。

FilePolicy

ファイルを検出したファイル ポリシー。

FileSandboxStatus

ファイルが動的分析のために送信されたかとその場合のステータスを示します。

FileSHA256

ファイルの SHA-256 ハッシュ値。

SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。
- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール

FileSize

The size of the file, in bytes.

ファイルが完全に受信される前にシステムがファイルのタイプを特定した場合は、ファイルサイズが計算されない場合があります。

FileStorageStatus

イベントに関連付けられたファイルのストレージ ステータス：

Stored

関連するファイルが現在保存されているすべてのイベントを返します。

Stored in connection

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

Failed

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

syslog フィールドには、初期のステータスのみが含まれています。これらのステータスは変更後のステータスを反映するようには更新されません。

FileType

ファイルのタイプ（HTML や MSEXE など）。

First Packet Time

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、特定のファイルおよびマルウェアイベントに関連付けられた接続イベントを識別できます。

FirstPacketSecond

ファイルのダウンロード フローまたはアップロード フローが開始された時刻。

イベントが発生した時刻がメッセージ ヘッダーのタイムスタンプにキャプチャされます。

Protocol

接続に使用されたプロトコル（TCP や UDP など）。

Sensor UUID

このフィールドはリリース 6.4.0.4 で追加されました。

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、特定のファイルおよびマルウェアイベントに関連付けられた接続イベントを識別できます。

SHA_Disposition

ファイルの性質：

Clean

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

Custom Detection

ユーザがカスタム検出リストにファイルを追加したことを示します。

Malware

AMP クラウドでそのファイルがマルウェアとして分類された、ローカル マルウェア分析でマルウェアとして識別された、またはファイルポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

Unavailable

システムがAMPクラウドに問い合わせできなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

Unknown

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。

ファイルの後処理は、システムが AMP クラウドにクエリを実行したファイルについてのみ表示されます。

syslog フィールドには最初の後処理のみが反映されます。レトロスペクティブな判定を反映するようには更新されません。

SperoDisposition

SPERO 署名がファイル分析で使用されたかどうかを示します。有効な値：

- ファイルで実行された Spero の検出
- ファイルで実行されなかった Spero の検出

SrcIP

接続を開始したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル送信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル受信者の IP アドレスです。

DstIP も参照してください。

SrcPort

SrcIP で説明されている接続で使用されるポート。

SSLActualAction

システムが暗号化されたトラフィックに適用したアクション。

Block または Block with reset

ブロックされた暗号化接続を表します。

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。

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。

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。

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。

Do not Decrypt

システムが復号化しなかった接続を表します。

SSLCertificate

TLS/SSL サーバの証明書のフィンガープリント。

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（Unknown）
- 不一致（No Match）
- 成功（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）

ThreatName

検出されたマルウェアの名前。

ThreatScore

このファイルに関連付けられている最新の脅威スコア。これは、動的分析中に観察された悪意がある可能性がある動作に基づいた 0 ～ 100 の値です。

URI

ファイル トランザクションに関連付けられている接続の URI。たとえば、ユーザがファイルをダウンロードした URL など。

User

ファイルをダウンロードした内部ホストに関連付けられているユーザ名。

リリース 6.5 以降： 該当する場合、ユーザ名の前には `<realm>\` が付いています。

ファイルイベントおよびネットワーク向けAMPによって生成されたマルウェア イベントの場合、このユーザはネットワーク検出によって判別されます。ユーザは宛先ホストに関連付けられているため、内部ホストがマルウェア ファイルをアップロードしたマルウェア イベントにユーザは関連付けられません。

WebApplication

接続で検出されたHTTPトラフィックについて、内容を表すまたはURLを要求したアプリケーション。

セキュリティイベントの Syslog メッセージの履歴

機能	バージョン	詳細
SGTの新しい接続イベントフィールド	6.5	新しいセキュリティ グループ タグ フィールド： • SourceSecurityGroup • SourceSecurityGroupTag （Security Group フィールドがこれに置き換えられます） • DestinationSecurityGroup • DestinationSecurityGroupTag
新しい接続イベントフィールド：Event Priority	6.5	Event Priority フィールドが導入されました。
Syslog の接続イベントの固有識別子	6.4.0.4	Syslog の 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識別できます。これらのフィールドは、侵入、ファイル、およびマルウェアイベントの Syslog にも含まれます。
ファイルとマルウェアのイベントの syslog サポート	6.4	ファイルおよびマルウェアイベントのフィールドを Syslog を介して使用できるようになりました。
侵入イベントのフィールドのリストに IntrusionPolicy フィールドが追加された	6.4	侵入イベントの syslog が、イベントをトリガーした侵入ポリシーを指定するようになりました。

機能	バージョン	詳細
接続および侵入イベントのサポートが改善された	6.3	接続イベント、セキュリティインテリジェンスイベント、および侵入イベントが完全修飾イベントとして使用できるようになり、新しいイベントタイプ ID を持ちました。 これらのフィールドが、このガイドに記載されるようになりました。