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 （19 ページ）
- セキュリティイベントの Syslog メッセージの履歴 （26 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）。

- 関連ルール/デフォルトアクションなし：侵入インスペクションは、アクセス制御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ません。たとえば、システムが適用するルールを決定する前に通過する必要があるパケットを処理するために指定された侵入ポリシーによってパケットが検査された場合が該当します。(このポリシーは、アクセス制御ポリシーの [詳細（Advanced）] タブで指定されます。)
- [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ー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。

このフィールドはリリース 6.5 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。

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、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。

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、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。

DeviceUUID

このフィールドはリリース 6.5 で追加されました。

イベントを生成した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、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。

（FirstPacketSecond）

このフィールドはリリース 6.5 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。

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、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。HTTP 要求の成功と失敗の理由を示します。

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。

（注） このフィールドは、IPS ルールが「ドロップして生成する」に設定されている場合にのみ使用できます。

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。

メッセージ

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。

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

接続を開始したホストの IP アドレスに関連付けられたユーザー名。エクスプロイトの送信元ホストである場合とそうでない場合があります。このユーザー値は、通常、ネットワーク上のユーザーだけに知らされます。

リリース 6.5 以降： 該当する場合、ユーザー名の前には `<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。

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）。

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

接続をモニターしたアクセス 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。

Client

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）。

このフィールドはリリース 6.5 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。

[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。

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

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。

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。

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）数値属性。

リリース 6.6 では、この値は [DestinationSecurityGroupType] フィールドで指定されたソースから取得されます。

リリース 6.5 では、この値は ISE（SXP またはユーザーセッションのいずれか）から取得されます。

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

このフィールドはリリース 6.6 で導入されました。

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

DeviceUUID

このフィールドはリリース 6.5 で追加されました。

イベントを生成した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_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

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。

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。

リリース 6.7 以降（実験段階の機能として）：

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。

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 サーバーに返された 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、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。

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ーのエンドポイント デバイス タイプ。

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`）のイベントは、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。

このフィールドはリリース 6.5 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。

[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。

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。ステータスコードは、HTTP 要求の成功や失敗の理由を示します。

HTTP レスポンスコードの詳細については、RFC 2616（HTTP）の「Section 10」を参照してください。

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。

Ingressvrf

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に入るときに通過する仮想ルータの名前。

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）。

NAT_InitiatorIP, NAT_ResponderIP

このフィールドのサポートはバージョン 7.1 で追加されました。

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_InitiatorPort, NAT_ResponderPort

このフィールドのサポートはバージョン 7.1 で追加されました。

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。

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 アドレスが一致しているか。

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

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。

SourceSecurityGroup

このフィールドはリリース 6.5 で導入されました。

接続に関係する送信元のセキュリティグループ。

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。

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。

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

SourceSecurityGroupType

このフィールドはリリース 6.6 で導入されました。

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

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、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。

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/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）（Decrypt (Resign)）]	再署名サーバー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ー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）

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
- 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）

SSLPolicy

接続を処理した SSL ポリシー。

リリース 6.7 以降： 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 SSL ポリシーがない場合、このフィールドにはどの SSL イベントについても何も保持されません。

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。

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ー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。

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ーのホスト名。

SSLSessionID

TLS/SSL ハンドシェイク時にクライアントとサーバー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ー対象のホストによって要求された URL。

リリース 6.7 以降（実験段階の機能として）：

[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。

URLCategory

セッション中にモニター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）。

リリース 6.7 以降（実験段階の機能として）：

[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。

URLReputation

セッション中にモニター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）。

リリース 6.7 以降（実験段階の機能として）：

[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。

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。

User

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。

リリース 6.5 以降： 該当する場合、ユーザー名の前には `<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ー 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ーに依存するクライアントアプリケーション。

このフィールドはリリース 6.5 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。

[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、特定の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を一意に識別できます。

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、特定の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を一意に識別できます。

DeviceUUID

このフィールドはリリース 6.5 で追加されました。

イベントを生成した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、特定の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を一意に識別できます。

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）。

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、特定の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を一意に識別できます。

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）。

SHA_Disposition

ファイルの性質：

[クリーン（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。

[不明（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。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバー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ー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。

SSLCertificate

TLS/SSL サーバー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
- 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）

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、ユーザーがファイルをダウンロードした URL など。

User

接続を開始した IP アドレスに関連付けられているユーザー名。この IP アドレスがネットワークの外部にある場合、関連付けられているユーザー名は通常不明です。

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

ファイルイベントおよび Firepower デバイスによって生成されたマルウェアイベントの場合、このフィールドには、ID ポリシーまたは権限のあるログインによって決定されたユーザー名が表示されます。ID ポリシーがない場合、認証は必要ありませんと表示されます。

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
DNS フィルタ処理の更新	7.0 6.7（実験段階の機能）	DNS フィルタ処理が有効な場合： • DNSQuery 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、DNSQuery、URLCategory、および URLReputation 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 DNSQuery で指定されたドメインに適用されます。 • 詳細については、Management Center オンラインヘルプで DNS フィルタ処理とイベントに関する情報を参照してください。

機能	バージョン	詳細
SGT と VRF の新しい接続イベントフィールド	6.6	新しいセキュリティグループのフィールド： • DestinationSecurityGroupType • SourceSecurityGroupType 仮想ルーティングおよびフォーワディングフィールド： • IngressVRF • EgressVRF
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のフィールド： • 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	6.5	Syslog の [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。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。 詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ） および 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 （19 ページ） を参照してください。

機能	バージョン	詳細
侵入イベントのフィールドのリストに追加された IntrusionPolicy フィールド	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。
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は、完全修飾イベントとして使用できるようになりました。
セキュリティイベントのイベントタイプ ID	6.3	接続、セキュリティ インテリジェンス、および侵入イベントのメッセージには、メッセージヘッダーにイベントタイプ ID が含まれています。 詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
セキュリティ イベント メッセージに含まれる空の値と不明な値の省略	6.3	空の値または不明な値を持つフィールドは、接続、セキュリティ インテリジェンス、および侵入イベントの Syslog メッセージから省略されます。
ドキュメンテーションの改善	6.3	接続、セキュリティ インテリジェンス、および侵入イベントに関する Syslog フィールド名と説明の追加ドキュメント （この機能は、このリリースでは新規ではありません。）

機能	バージョン	詳細
Firepower（SFIMS）イベントログ形式	6.2.2	Apr 30 04:33:28 192.168.1.1 Apr 30 13:57:38 firepower SFIMS: Protocol: ICMP, SrcIP: 172.16.10.10, OriginalClientIP: ::, DstIP: 172.16.20.10, ICMPType: Echo Request, ICMPCode: 0, TCPFlags: 0x0, IngressInterface: inside, EgressInterface: outside, DE: Primary Detection Engine (e357206c-a9b0-11eb-93fe-a690508a381d), Policy: Default Allow All Traffic, ConnectType: Start, AccessControlRuleName: test, AccessControlRuleAction: Allow, Prefilter Policy: Unknown, UserName: No Authentication Required, Client: ICMP client, ApplicationProtocol: ICMP, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity, DNSResponseType: No Error, Sinkhole: Unknown, URLCategory: Unknown, URLReputation: Risk unknown
Firepower（NULL）イベントログ形式	6.6.3	Apr 30 02:07:02 192.168.1.1 2021-04-30T11:31:19Z firepower (null) %NGIPS-1-430002: EventPriority: Low, DeviceUUID: b2433c5c-a6a1-11eb-a6e7-be0b9833091f, InstanceID: 2, FirstPacketSecond: 2021-04-30T11:31:19Z, ConnectionID: 4, AccessControlRuleAction: Allow, SrcIP: 172.16.10.10, DstIP: 172.16.20.10, ICMPType: Echo Request, ICMPCode: No Code, Protocol: icmp, IngressInterface: inside, EgressInterface: outside, ACPolicy: Default Allow All Traffic, AccessControlRuleName: test, Client: ICMP client, ApplicationProtocol: ICMP, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity

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。