CHAPTER 10

スキーマ：ファイル イベント テーブル

この章では、ファイル イベントのスキーマとサポートされている結合について説明します。詳細については、次の表に示す項を参照してください。

表 10-1　ファイル イベント テーブルのスキーマ

参照先	次の内容が格納されるテーブル	Version
file_event（10-1 ページ）	モニタ対象ネットワーク内でファイル転送が検出されると生成されるファイル イベント。	5.1.1+

次に示すテーブルは使用可能ですが、シスコ では現在、これらのテーブルでの検索がサポートされていません。

- `file_categories`
- `file_rules`
- `file_types`
- `file_type_rule_map`
- `file_type_category_map`

file_event

`file_event` テーブルには、Firepower Management Center により生成されるファイル イベントに関する情報が格納されます。モニタ対象ネットワークでファイル転送が検出されるたびに、新しいファイル イベントが生成されます。AMP for Firepower によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイント ベースのマルウェア イベントには、対応するファイル イベントはありません。また、ファイル イベントには AMP for Endpoints 関連のフィールドはありません。

詳細については、次の項を参照してください。

- file_event のフィールド（10-2 ページ）
- file_event の結合（10-6 ページ）
- file_event のサンプル クエリ（10-6 ページ）

file_event のフィールド

file_event テーブルには、モニタ対象ネットワークを通過する際に検出されたファイルに関する情報が格納されます。各ファイル イベントを接続イベントに相関付けることができます。ファイルとファイル転送の詳細(ファイルの名前、サイズ、送信元、宛先、および方向、ファイルの SHA256 ハッシュ、ファイルを検出したデバイス、ファイルがマルウェアとして見なされるかどうか、など)が記録されます。

表 10-2　file_event のフィールド

フィールド	説明
action	ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 • 1:検出 • 2:ブロック • 3:マルウェア クラウド ルックアップ • 4:マルウェア ブロック • 5:マルウェア ホワイトリスト • 6:クラウド ルックアップ タイムアウト
application_id	ファイル転送を使用するアプリケーションにマップされている ID 番号。
application_name	次のいずれかです。 • 接続で使用されたアプリケーションの名前。 • pending または unknown(システムがアプリケーションを識別できない場合)。 • 空白(接続にアプリケーション情報がない場合)
archived	ファイルがアーカイブされているかどうかを示します。
cert_valid_end_date	接続で使用された SSL 証明書が有効ではなくなった時点を示す UNIX タイムスタンプ。
cert_valid_start_date	接続で使用された SSL 証明書の発行時点を示す UNIX タイムスタンプ。
client_application_id	クライアント アプリケーションの内部識別番号(該当する場合)。
client_application_name	クライアント アプリケーションの名前(該当する場合)。
connection_sec	ファイル イベントに関連付けられている接続イベントの UNIX タイムスタンプ(00:00:00 01/01/1970 からの経過秒数)。
counter	同じ秒数で発生した複数のイベントを区別するために使用されるイベント固有のカウンタ。
direction	ファイルのアップロードとダウンロードのいずれが行われたか。現時点では、この値はプロトコルに完全に依存しています(例えば接続が HTTP の場合はダウンロード)。

表 10-2　file_event のフィールド(続き)

フィールド	説明
disposition	ファイルのマルウェア ステータス。有効な値は次のとおりです。 • CLEAN:ファイルはクリーンであり、マルウェアが含まれていない。 • UNKNOWN:ファイルにマルウェアが含まれているかどうかが不明である。 • MALWARE:ファイルにマルウェアが含まれている。 • UNAVAILABLE:ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しなかった。 • CUSTOM SIGNATURE:ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理された。
domain_name	イベントが検出されたドメインの名前。
domain_uuid	イベントが検出されたドメインの UUID。これはバイナリで示されます。
dst_continent_name	宛先ホストが位置する地域の名前 **:不明 na:北米 as:アジア af:アフリカ eu:欧州 sa:南米 au:オーストラリア an:南極
dst_country_id	宛先ホストの国のコード。
dst_country_name	宛先ホストの国の名前。
dst_ip_address_v6	バージョン 5.2 で廃止されたフィールド。すべてのクエリに対して null を返します。
dst_ipaddr	トリガー イベントに関連する宛先ホストの IP アドレスのバイナリ表現。
dst_port	接続の宛先のポート番号。
event_description	イベント タイプに関連付けられている追加イベント情報。
event_id	イベント識別番号。
file_name	検出されたファイルの名前。この名前には、UTF-8 文字を使用できます。
file_sha	ファイルの SHA256 ハッシュ
file_size	検出されたファイルのサイズ(バイト単位)。
file_type	検出または検疫されたファイルのファイル タイプ。
file_type_category	ファイル カテゴリの説明
file_type_category_id	ファイル カテゴリの数値 ID。
file_type_id	ファイル タイプにマップされている ID 番号。
http_response_code	イベントで HTTP 要求に対して返された応答コード。
instance_id	イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。

表 10-2　file_event のフィールド(続き)

フィールド	説明
netmap_num	イベントが検出されたドメインの Netmap ID。
policy_uuid	イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する識別番号。
sandboxed	ファイルが動的分析のために送信されているかどうかを示します。値は次のとおりです。 • Sent for Analysis • Failed to Send • File Size is Too Small • File Size is Too Large • Sent for Analysis • Analysis Complete • Failure (Network Issue) • Failure (Rate Limit) • Failure (File Too Large) • Failure (File Read Error) • Failure (Internal Library Error) • File Not Sent, Disposition Unavailable • Failure (Cannot Run File) • Failure (Analysis Timeout) • File Not Supported
得点	動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ～ 100)。
security_context	トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の説明。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスの場合だけです。
sensor_address	イベントを提供したデバイスの IP アドレスのバイナリ表現。
sensor_id	イベントを提供したデバイスの ID。
sensor_name	イベント レコードを生成した管理対象デバイスのテキスト名。接続デバイスではなくレポート デバイス自体を参照するイベントの場合、このフィールドは null です。
sensor_uuid	管理対象デバイスの固有識別子(sensor_name が null の場合は 0)。
signature_processed	ファイルの署名が処理されたかどうかを示します。

表 10-2　file_event のフィールド(続き)

フィールド	説明
src_continent_name	送信元ホストが位置する地域の名前 **:不明 na:北米 as:アジア af:アフリカ eu:欧州 sa:南米 au:オーストラリア an:南極
src_country_id	送信元ホストの国のコード。
src_country_name	送信元ホストの国の名前。
src_ip_address_v6	バージョン 5.2 で廃止されたフィールド。すべてのクエリに対して null を返します。
src_ipaddr	トリガー イベントに関連する送信元ホストの IPv4 または IPv6 アドレスのバイナリ表現。
src_port	接続元のポート番号。
ssl_issuer_common_name	SSL 証明書の発行元の共通名。これは一般に証明書発行元のホストとドメイン名ですが、その他の情報が含まれていることもあります。
ssl_issuer_country	SSL 証明書の発行元の国。
ssl_issuer_organization	SSL 証明書の発行元の組織。
ssl_issuer_organization_unit	SSL 証明書の発行元の組織単位。
ssl_serial_number	発行元 CA によって割り当てられた SSL 証明書のシリアル番号。
ssl_subject_common_name	SSL 証明書の件名共通名。これは一般に証明書の件名のホストとドメイン名ですが、その他の情報が含まれていることもあります。
ssl_subject_country	SSL 証明書の件名の国。
ssl_subject_organization	SSL 証明書の件名の組織。
ssl_subject_organization_unit	SSL 証明書の件名の組織単位。
storage	ファイルの保存ステータス。値は次のとおりです。 • File Stored • Unable to Store File • File Size is Too Large • File Size is Too Small • Unable to Store File • File Not Stored, Disposition Unavailable
threat_name	脅威の名前。
timestamp	ファイル タイプを識別するために十分なファイルが送信された時点を示す UNIX タイムスタンプ。

表 10-2　file_event のフィールド(続き)

フィールド	説明
url	ファイル送信元の URL。
user_id	宛先ユーザの内部識別番号。宛先ユーザとは、イベント発生前に宛先ホストにログインした最終ユーザです。
username	user_id に関連付けられている名前。
web_application_id	Web アプリケーションの内部識別番号(該当する場合)。
web_application_name	Web アプリケーションの名前(該当する場合)。

file_event の結合

次の表に、**file_event** テーブルで実行できる結合について説明します。

表 10-3　file_event の結合

このテーブルで結合に使用するフィールド	結合できるフィールド
application_id	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

file_event のサンプル クエリ

次のクエリは、特性が CLEAN ではない最大 10 件のファイル イベントと、アプリケーション名、接続情報、およびファイルの名前を返します。

```
SELECT file_event.application_name, file_event.connection_sec, file_event.counter,
file_event.file_name
FROM file_event
WHERE file_event.disposition != "CLEAN" limit 10;
```