スキーマ:侵入テーブル

この章では、侵入イベント、侵入イベントをトリガーしたパケット、および関連するルール メッセージ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 4-1　侵入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
intrusion_event（4-1 ページ）	侵入イベント（エクスプロイトの日時とタイプ、および攻撃の攻撃元と標的に関するコンテキスト情報など）。	4.10.x+
intrusion_event_packet（4-7 ページ）	侵入イベントをトリガーした 1 つ以上のパケットの内容。	4.10.x+
rule_message（4-9 ページ）	侵入イベントのルール メッセージ（関連付けられているジェネレータ ID（GID）、シグニチャ ID（SID）、およびバージョン データなどを含む）。	4.10.x+
（4-9 ページ）	ルールに関する情報（攻撃シナリオ、影響を受けるシステム、およびルールの作成時点と作成者に関する情報など）。	5.2+

intrusion_event

intrusion_event テーブルには、Firepower システム により特定された侵入の可能性に関する情報が格納されます。可能性のある侵入ごとに、イベントと関連レコードがデータベースに生成されます。このレコードには、エクスプロイトの日時とタイプ、アクセス コントロール ポリシーとルール、侵入ポリシーとルール、および攻撃の攻撃元と標的に関するその他のコンテキスト情報が含まれています。

ヒント　パケットベースのイベントの場合、イベントをトリガーした 1 つ以上のパケットのコピーも使用可能になります。intrusion_event_packet のサンプル クエリ（4-8 ページ）を参照してください。

詳細については、次の項を参照してください。

- intrusion_event のフィールド（4-2 ページ）
- intrusion_event の結合（4-7 ページ）
- intrusion_event のサンプル クエリ（4-7 ページ）

intrusion_event のフィールド

次の表に、**intrusion_event** テーブルでアクセスできるデータベース フィールドについて説明します。

表 4-2　intrusion_event のフィールド

フィールド	説明
access_control_policy_name	侵入イベントを生成した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。アクセス コントロール ポリシー名とアクセス コントロール ルール名の組み合わせは、Firepower Management Center で一意である点に注意してください。
access_control_policy_UUID	侵入イベントを生成した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 ポリシーの UUID。
access_control_rule_id	侵入イベントを生成した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 ルールの内部識別番号。
access_control_rule_name	侵入イベントを生成した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 ルールの名前。アクセス コントロール ルールの名前は、1 つのポリシー内では固有であるが、異なるポリシー間では固有ではない点に注意してください。
application_protocol_id	アプリケーション プロトコルの内部識別番号。
application_protocol_name	次のいずれかになります。 • アプリケーションの名前(確実な識別が可能な場合) • pending(システムがさらにデータを必要としている場合) • 空白(接続にアプリケーション情報がない場合)
blocked	侵入イベントをトリガーしたパケットの処理を示す値。 • 0:パケットはドロップされなかった • 1:パケットはドロップされた(インライン型、スイッチ型、またはルーティング型展開) • 2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開で設定されているデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。
client_application_id	侵入イベントで使用されたクライアント アプリケーションの内部識別番号。
client_application_name	侵入イベントで使用されたクライアント アプリケーション(使用可能な場合)。次のいずれかになります。 • アプリケーションの名前(確実な識別が可能な場合) • 汎用クライアント名(システムがクライアント アプリケーションを検出したが、特定のアプリケーションであることを識別できない場合)。 • null(接続にアプリケーション情報がない場合)
connection_sec	侵入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	特定の秒で発生した接続イベントごとに増加する番号。これは、同じ秒で発生した複数の接続イベントを区別するために使用されます。

表 4-2　intrusion_event のフィールド(続き)

フィールド	説明
detection_engine_name	バージョン 5.0 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。
detection_engine_uuid	バージョン 5.0 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。
domain_name	イベントのために指定されたドメインの名前。
domain_uuid	イベントのために指定されたドメインの 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	バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。
dst_ip_address_v6	バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。
dst_ipaddr	トリガー イベントに関連する宛先ホストの IPv4 または IPv6 アドレスのバイナリ表現。
dst_port	次のいずれかを行います。 • イベント プロトコル タイプが TCP または UDP の場合は宛先ポート番号 • イベント プロトコルタイプが ICMP の場合は ICMP コード。
dst_user_dept	宛先ユーザの所属部門。
dst_user_email	宛先ユーザの電子メール アドレス。
dst_user_first_name	宛先ユーザの名前。
dst_user_id	宛先ユーザの内部識別番号。宛先ユーザとは、侵入イベント発生前に宛先ホストにログインしていた最終ユーザです。
dst_user_last_name	宛先ユーザの姓。
dst_user_last_seen_sec	システムが宛先ユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。
dst_user_last_updated_sec	システムが宛先ユーザのレコードを最後に更新した日時を示す UNIX タイムスタンプ。
dst_user_name	宛先ユーザのユーザ名。

表 4-2　intrusion_event のフィールド(続き)

フィールド	説明
dst_user_phone	宛先ユーザの電話番号。
event_id	イベントの内部識別番号。Firepower Management Center でイベントを一意に識別します。
event_time_sec	イベント パケットがキャプチャされた日時を示す UNIX タイムスタンプ。
event_time_usec	イベントのタイムスタンプのマイクロ秒単位の増分。マイクロ秒単位の精度を使用できない場合、この値は 0 です。
http_response_code	イベントで HTTP 要求に対して返された応答コード。
icmp_code	イベントが ICMP トラフィックの場合は ICMP コード。イベントが ICMP トラフィックから生成されたものではない場合は null。
icmp_type	イベントが ICMP トラフィックの場合は ICMP タイプ。イベントが ICMP トラフィックから生成されたものではない場合は null。
impact	イベントの影響フラグ値。整数値は次のとおりです。 • 1:レッド(脆弱) • 2:オレンジ(脆弱の可能性あり) • 3:イエロー(現在は脆弱でない) • 4:ブルー(不明なターゲット) • 5:グレー(不明な影響)
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。
interface_egress_name	発信トラフィックのインターフェイスの名前。
interface_ingress_name	着信トラフィックのインターフェイスの名前。
intrusion_event_policy_uuid	侵入イベントをトリガーした侵入ポリシーの固有識別子。
intrusion_event_policy_name	侵入イベントを生成した侵入ポリシー。
ioc_count	イベントで検出された侵害の痕跡の数。
network_analysis_policy_name	侵入イベントを生成した侵入ポリシーに関連付けられているネットワーク分析ポリシー。
network_analysis_policy_UUID	侵入イベントを生成した侵入ポリシーに関連付けられているネットワーク分析ポリシーの UUID。
priority	イベントに関連付けられているルール分類のプライオリティ。ルールのプライオリティはユーザ インターフェイスで設定されます。
protocol_name	侵入イベントに関連付けられているトラフィック プロトコルのテキスト名。
protocol_num	プロトコルの IANA 番号。IANA 番号のリストは http://www.iana.org/assignments/protocol-numbers にあります。
reviewed	侵入イベントが確認済みとしてマークされているかどうか。 • 1:確認済み • 0:未確認
rule_classification	侵入イベントに関連付けられているルール分類の説明。通常、イベントをトリガーしたルールによって検出された攻撃を説明します。例:A Network Trojan was Detected.
rule_classification_id	侵入イベントに関連付けられているルール分類の識別番号。

表 4-2　intrusion_event のフィールド(続き)

フィールド	説明
rule_generator	侵入イベントを生成したコンポーネント。生成コンポーネントは、ルール エンジン、デコーダ、またはプリプロセッサです。
rule_generator_id	侵入イベントを生成した rule_generator で指定されているコンポーネントのジェネレータ ID(GID)。
rule_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、メッセージはルールから生成されます。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、メッセージはハード コーディングされています。
rule_revision	侵入イベントに関連付けられているルールのリビジョン番号。
rule_signature_id	侵入イベントのシグニチャ ID(SID)。侵入イベントが生成される原因である特定のルール、デコーダ メッセージ、またはプリプロセッサ メッセージを識別します。
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。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。
security_zone_egress_name	ポリシー違反をトリガーした侵入イベントの出力セキュリティ ゾーン。
security_zone_ingress_name	ポリシー違反をトリガーした侵入イベントの入力セキュリティ ゾーン。
sensor_address	イベントを生成した管理対象デバイスの IP アドレス。形式は *ipv4_address,ipv6_address* です。
sensor_name	侵入イベントを生成した管理対象デバイスの名前。
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)。
src_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
src_country_id	宛先ホストの国のコード。
src_country_name	宛先ホストの国の名前。
src_ip_address	バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。
src_ip_address_v6	バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。
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。

表 4-2　intrusion_event のフィールド(続き)

フィールド	説明
src_port	次のいずれかを行います。 • イベント プロトコル タイプが TCP または UDP の場合は送信元ポート番号 • イベント プロトコルタイプが ICMP の場合は ICMP タイプ。
src_user_dept	送信元ユーザの所属部門。
src_user_email	送信元ユーザの電子メール アドレス。
src_user_first_name	送信元ユーザの名前。
src_user_id	送信元ユーザの内部識別番号。送信元ユーザとは、侵入イベント発生前に送信元ホストにログインしていた最終ユーザです。
src_user_last_name	送信元ユーザの姓。
src_user_last_seen_sec	システムが送信元ユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。
src_user_last_updated_sec	送信元ユーザのレコードの最終更新日時を示す UNIX タイムスタンプ。
src_user_name	送信元ユーザのユーザ名。
src_user_phone	送信元ユーザの電話番号。
vlan_id	侵入イベントをトリガーしたパケットに関連付けられている最も内側の VLAN の識別番号。
web_application_id	侵入イベントで使用された 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	侵入イベントで使用された Web アプリケーション(該当する場合)。次のいずれかになります。 • アプリケーションの名前(確実な識別が可能な場合) • web browsing(システムがアプリケーション プロトコル HTTP を検出したが、特定の Web アプリケーションを検出できない場合)。 • 空白(接続に HTTP トラフィックがない場合)。

intrusion_event の結合

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

表 4-3　intrusion_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_protocol_id または client_application_id または web_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
dst_ipaddr または src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

intrusion_event のサンプル クエリ

次のクエリは、25 件の最も頻繁に発生した未確認の侵入イベント結果を、Count に基づいて降順にソートして返します。

```
SELECT rule_message, priority, rule_classification, count(*) as Count
FROM intrusion_event
WHERE reviewed="0"
GROUP BY rule_message, priority, rule_classification
ORDER BY Count DESCLIMIT 0, 25;
```

intrusion_event_packet

intrusion_event_packet テーブルには、侵入イベントをトリガーした 1 つ以上のパケットの内容に関する情報が格納されます。管理対象デバイスから Firepower Management Center へのパケット転送を禁止している場合、**intrusion_event_packet** テーブルにはデータが格納されません。

詳細については、次の項を参照してください。

- intrusion_event_packet のフィールド (4-8 ページ)
- intrusion_event_packet の結合 (4-8 ページ)
- intrusion_event_packet のサンプル クエリ (4-8 ページ)

intrusion_event_packet のフィールド

次の表に、**intrusion_event_packet** テーブルでアクセスできるデータベース フィールドについて説明します。

表 4-4　intrusion_event_packet のフィールド

フィールド	説明
detection_engine_name	バージョン 5.0 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。
detection_engine_uuid	バージョン 5.0 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。
domain_name	イベントのために指定されたドメインの名前。
domain_uuid	イベントのために指定されたドメインの UUID。これはバイナリで示されます。
event_id	イベントの識別番号。この ID は、特定の管理対象デバイスにおいて固有です。
linktype	パケットの外部レイヤの形式を示す内部キー。管理対象デバイスがパケットを正しく復号化するためにこのキーを使用します。リンク タイプ 1 だけがサポートされています。
netmap_num	イベントが検出されたドメインの Netmap ID。
packet_data	イベントをトリガーしたパケットの内容。
packet_time_sec	イベント パケットがキャプチャされた日時を示す UNIX タイムスタンプ。
packet_time_usec	イベントのタイムスタンプのマイクロ秒単位の増分。マイクロ秒単位の精度を使用できない場合、この値は 0 です。
sensor_address	イベントを生成した管理対象デバイスの IP アドレス。形式は *ipv4_address*,*ipv6_address* です。
sensor_name	侵入イベントを生成した管理対象デバイスの名前。
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）。

intrusion_event_packet の結合

intrusion_event_packet テーブルに対して結合を実行することはできません。

intrusion_event_packet のサンプル クエリ

次のクエリは、選択されたイベント ID に一致するすべてのパケットに関するパケット情報を返します。

```
SELECT event_id, packet_time_sec, sensor_address, packet_data
FROM intrusion_event_packet
WHERE event_id="1";
```

rule_message

rule_message テーブルは、侵入ルールのルール メッセージのマスタ リストです。各ルール メッセージにはその識別情報が付いています。

詳細については、次の項を参照してください。

- rule_message のフィールド(4-9 ページ)
- rule_message の結合(4-9 ページ)
- rule_message のサンプル クエリ (4-9 ページ)

rule_message のフィールド

次の表に、**rule_message** テーブルでアクセスできるデータベース フィールドについて説明します。

表 4-5　rule_message のフィールド

フィールド	説明
generator_id	ルールをトリガーするコンポーネントの GID。
message	トリガーされたルールに関連付けられているメッセージ。
rev_uuid	ルール リビジョンの固有識別子。
revision	ルールのリビジョン番号。
signature_id	アプライアンスのユーザ インターフェイスでレンダリングされるルールの識別番号。
uuid	ルールの固有識別子。

rule_message の結合

rule_message テーブルに対して結合を実行することはできません。

rule_message のサンプル クエリ

次のクエリは、GID が 1、SID が 1200 の侵入ルールの侵入ルール メッセージを返します。

```
SELECT generator_id, signature_id, revision, message
FROM rule_message
WHERE generator_id="1"
AND signature_id="1200";
```