スキーマ：相関テーブル

この章では、相関関連イベント（修復ステータスやホワイト リスト イベントなど）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 9-1　相関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
compliance_event（9-1 ページ）	相関イベント。このイベントは、アクティブな相関ポリシー内の相関ルールがトリガーされると生成されます。	4.10.x+
remediation_status（9-6 ページ）	修復ステータス イベント。このイベントは、アクティブな相関ポリシーによって応答として修復がトリガーされると生成されます。	4.10.x+
white_list_event（9-8 ページ）	ホワイト リスト イベント。このイベントは、アクティブなホワイト リスト コンプライアンス ポリシーでホワイト リストのコンプライアンスに準拠していないホストが検出されると、生成されます。	4.10.x+
white_list_violation（9-10 ページ）	ホワイト リスト違反。この違反は、ネットワーク上のホストが、アクティブなコンプライアンス ポリシーのコンプライアンス ホワイト リストにどのように違反しているかを追跡します。	4.10.x+

compliance_event

compliance_event テーブルには、Firepower Management Center により生成される相関イベントに関する情報が格納されます。

詳細については、次の項を参照してください。

- compliance_event のフィールド（9-2 ページ）
- compliance_event の結合（9-6 ページ）
- compliance_event のサンプル クエリ（9-6 ページ）

compliance_event のフィールド

このテーブルのフィールドの多くは、相関ルールをトリガーしたイベントのタイプに応じて空白になることがある点に注意してください。たとえば、システムで特定のアプリケーション プロトコルまたは特定のポートで稼働している Web アプリケーションが検出されたために、Firepower Management Center により相関イベントが生成される場合、その相関イベントには、侵入関連の情報は含まれません。また、このテーブルのフィールドは、Firepower システム の設定に基づいて空白になることもあります。たとえば Control ライセンスを所有していない場合、相関イベントにはユーザ アイデンティティ情報が含まれません。

バージョン 5.0 以降、Firepower システム は検出エンジンではなく、管理対象デバイス レベルでのネットワークおよびユーザ アクティビティの検出を記録することに注意してください。現在、**compliance_event** テーブルの detection_engine_name フィールドと detection_engine_uuid フィールドは空白だけを返し、これらのフィールドを結合するクエリはレコードを返しません。イベントが検出された場所に関する情報については、detection_engine_uuid フィールドではなく sensor_uuid フィールドを照会する必要があります。

次の表に、**compliance_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 9-2　compliance_event のフィールド

フィールド	説明
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の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。
description	相関イベントと、このイベントがどのように引き起こされたかに関する情報。
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_host_criticality	相関イベントに関連する宛先ホストにユーザが割り当てたホスト重要度:None、Low、Medium、または High
dst_host_type	宛先ホストのタイプ:Host、Router、Bridge、NAT Device、または Load Balancer
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 IP v 6 アドレスのバイナリ表現。
dst_os_product	宛先ホストのオペレーティング システムの名前。

表 9-2　compliance_event のフィールド(続き)

フィールド	説明
dst_os_vendor	宛先ホストのオペレーティング システムのベンダー。
dst_os_version	宛先ホストのオペレーティング システムのバージョン番号。
dst_port	イベント プロトコル タイプが TCP または UDP の場合にトラフィックを受信するホストのポート番号。プロトコル タイプが ICMP の場合は ICMP コード。
dst_rna_service	トリガーイベントに関連付けられている送信元ホストのアプリケーション プロトコル(判明している場合)。判明していない場合は、次のいずれかになります。 • none または空白:アプリケーション プロトコル トラフィックがありません。 • unknown:既知のサーバ フィンガープリントに基づいてサーバを識別できませんでした。 • pending:システムにさらに情報が必要です。
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、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。
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	宛先ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。
dst_user_name	宛先ユーザのユーザ名。
dst_user_phone	宛先ユーザの電話番号。
dst_vlan_id	宛先ホストの VLAN ID 番号(該当する場合)。
event_id	デバイスによって生成されたトリガー侵入イベントの識別番号。
event_time_sec	トリガー イベントの日時を示す UNIX タイムスタンプ。
event_time_usec	トリガー イベントのタイムスタンプのマイクロ秒単位の増分。
event_type	相関ルールをトリガーした基礎となるイベントのタイプ、または Firepower Management Center が相関イベントを生成する原因となった基礎となるイベントのタイプ値は次のとおりです。 • ids:侵入イベント トリガー • rna:検出イベント、ホスト入力イベント、接続イベント、またはトラフィック プロファイル変更トリガー • rua:ユーザ検出イベント トリガー • whitelist:コンプライアンス ホワイト リスト違反トリガー
host_event_type	イベント タイプ(New Host、Identity Conflict など)。
id	相関イベントの内部識別番号。

表 9-2　compliance_event のフィールド(続き)

フィールド	説明
impact	イベントの影響フラグ値。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) 相関ルールが侵入イベントによってトリガーされた場合にのみ設定します。
interface_egress_name	接続に関連付けられた入力インターフェイス。
interface_ingress_name	接続に関連付けられた出力インターフェイス。
policy_name	違反が発生した相関ポリシー。
policy_rule_name	ポリシー違反をトリガーした相関ルール。
policy_rule_uuid	相関ルールの固有識別子。
policy_time_sec	相関イベントが生成された日時を示す UNIX タイムスタンプ。
policy_uuid	相関ポリシーの固有識別子。
priority	相関イベントのプライオリティ。ユーザ インターフェイスで設定されます。このイベント プライオリティは、トリガーされたルールのプライオリティまたは違反が発生した相関ポリシーのプライオリティによって決まります。
protocol_name	イベントに関連付けられているプロトコル(使用可能な場合)。
protocol_num	IANA 指定のプロトコル番号(使用可能な場合)。
rna_event_type	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。
rua_event_type	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。
rule_generator_id	トリガー侵入イベントを生成したコンポーネントのジェネレータ ID 番号(GID)。
rule_message	相関ルールをトリガーした侵入イベントを説明するテキスト。ルールベースのイベントの場合、イベント 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_signature_id	イベントのシグニチャ ID(SID)。トリガー侵入イベントが生成される原因となった特定のルール、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_zone_egress_name	相関イベントの出力セキュリティ ゾーン。
security_zone_ingress_name	相関イベントの入力セキュリティ ゾーン。
sensor_address	コンプライアンス イベントをトリガーした基礎となる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	コンプライアンス イベントをトリガーした基礎となるイベントを生成した管理対象デバイス。
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)。

表 9-2　compliance_event のフィールド(続き)

フィールド	説明
src_host_criticality	コンプライアンス イベントに関連する送信元ホストにユーザが割り当てたホスト重要度:None、Low、Medium、または High。
src_host_type	送信元ホストのタイプ:Host、Router、Bridge、NAT Device、または Load Balancer。
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。
src_os_product	送信元ホストのオペレーティング システムの名前。
src_os_vendor	送信元ホストのオペレーティング システムのベンダー。
src_os_version	送信元ホストのオペレーティング システムのバージョン番号。
src_port	送信元ホストのポート番号。ICMP トラフィックの場合は ICMP タイプが表示されます。
src_rna_service	トリガーイベントに関連付けられている送信元ホストのアプリケーション プロトコル(判明している場合)。判明していない場合は、次のいずれかになります。 • none または空白:アプリケーション プロトコル トラフィックがありません。 • unknown:既知のサーバ フィンガープリントに基づいてサーバとアプリケーション プロトコルを識別できませんでした。 • pending:システムにさらに情報が必要です。
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。これは、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	送信元ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。
src_user_name	送信元ユーザのログイン ユーザ名。
src_user_phone	送信元ユーザの電話番号。
src_vlan_id	送信元ホストの VLAN 識別番号(該当する場合)。
user_event_type	トリガー ユーザ イベントのタイプ(New User Identity または User Login など)。

compliance_event の結合

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

表 9-3　compliance_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
dst_ipaddr または src_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

compliance_event のサンプル クエリ

次のクエリは、1 週間の相関イベント レコードを最大 25 件返します。これらのレコードには、イベント時刻、送信元と宛先の IP アドレス、送信元と宛先のポート、ポリシー情報などのイベント情報が含まれています。

```
SELECT event_id, policy_time_sec, impact, blocked, src_ipaddr, dst_ipaddr, src_port,
dst_port, description, policy_name, policy_rule_name, priority, src_host_criticality,
dst_host_criticality, security_zone_egress_name, security_zone_ingress_name,
sensor_name, interface_egress_name, interface_ingress_name
FROM compliance_event WHERE event_type!="whitelist"
AND policy_time_sec
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
domain_name= "Global \ Company B \ Edge"
ORDER BY policy_time_sec
DESC LIMIT 0, 25;
```

remediation_status

remediation_status テーブルには、修復イベントに関する情報が格納されます。修復イベントは、Firepower Management Center が相関ポリシー違反に対応して修復を開始すると生成されます。

詳細については、次の項を参照してください。

- remediation_status のフィールド (9-7 ページ)
- remediation_status の結合 (9-7 ページ)
- remediation_status のサンプル クエリ (9-7 ページ)

remediation_status のフィールド

次の表に、**remediation_status** 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 9-4　remediation_status のフィールド

フィールド	説明
id	違反が発生し、修復をトリガーした相関ポリシーの識別番号。
policy_name	違反が発生し、修復をトリガーした相関ポリシー。
policy_rule_name	修復をトリガーした特定の相関ルール。
policy_rule_uuid	相関ルールの固有識別子。
policy_time_sec	修復をトリガーした相関イベントの生成日時を示す UNIX タイムスタンプ。
policy_uuid	相関イベントをトリガーした相関ポリシーの固有識別子。
remediation_name	開始された修復。
remediation_time_sec	Firepower Management Center により修復が開始された日時を示す UNIX タイムスタンプ。
status_text	修復の開始時に発生した事象を説明するメッセージ(「successful completion of remediation」など)。

remediation_status の結合

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

remediation_status のサンプル クエリ

次のクエリは、特定の日付より前に生成された最大 25 件のレコードを返します。これらのレコードには修復のステータスに関する情報(修復のタイムスタンプ、ステータス メッセージなど)が含まれます。

```
SELECT policy_time_sec, remediation_time_sec, remediation_name, policy_name,
policy_rule_name, status_text

FROM remediation_status WHERE remediation_time_sec <= UNIX_TIMESTAMP("2011-10-01
00:00:00")

ORDER BY policy_time_sec

DESC LIMIT 0, 25;
```

white_list_event

white_list_event テーブルにはホワイト リスト イベントが格納されます。ホワイト リスト イベントは、ホストがアクティブなホワイト リスト コンプライアンス ポリシーのホワイト リストに準拠していないことがシステムにより検出されると生成されます。

バージョン 5.0 以降、Firepower システム は検出エンジンではなく、管理対象デバイス レベルでのネットワークおよびユーザ アクティビティの検出を記録することに注意してください。**white_list_event** テーブルの detection_engine_name フィールドと detection_engine_uuid フィールドは null だけを返し、またこれらのフィールドを結合するクエリはレコードを返しません。detection_engine_uuid フィールドの代わりに sensor_uuid フィールドを照会すると、同等の情報が返されます。

詳細については、次の項を参照してください。

- white_list_event のフィールド (9-8 ページ)
- white_list_event の結合 (9-9 ページ)
- white_list_event のサンプル クエリ (9-10 ページ)

white_list_event のフィールド

次の表に、**white_list_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 9-5　white_list_event のフィールド

フィールド	説明
description	ホワイト リスト違反の説明。
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。
host_criticality	ホワイト リストに準拠していないホストに対してユーザが割り当てた重要度 ([None]、[Low]、[Medium]、または [High])。
host_type	ホストのタイプ：Host、Router、Bridge、NAT Device、または Load Balancer。
id	ホワイト リスト イベントの内部固有識別子。
ip_address	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。
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。
ipaddr	準拠していないホストの IP アドレスのバイナリ表現。
os_product	オペレーティング システムの製品名。
os_vendor	オペレーティング システムのベンダー。
os_version	オペレーティング システムのバージョン番号。
policy_name	ホワイト リストを含む違反コンプライアンス ポリシー。
policy_time_sec	イベントが生成された日時を示す UNIX タイムスタンプ。
policy_uuid	ホワイトリスト イベントを含むコンプライアンス ポリシーの固有識別子。
port	サービス ホワイト リスト違反をトリガーしたイベント (非準拠サービスの結果として違反が発生した場合) に関連付けられているポート (存在する場合)。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

表 9-5　white_list_event のフィールド(続き)

フィールド	説明
priority	ホワイト リスト イベントのプライオリティ。ユーザ インターフェイスで設定されます。
protocol_name	イベントに関連付けられているプロトコル(使用可能な場合)。
protocol_num	IANA 指定のプロトコル番号(使用可能な場合)。
rna_service	ホワイト リスト違反をトリガーしたサービス(使用可能な場合)。
sensor_address	トラフィックを検出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	ホワイト リスト イベントを生成したデバイス。
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)。
user_dept	ユーザの所属部門。
user_email	ユーザの電子メール アドレス。
user_first_name	ユーザの名前。
user_id	イベント発生前にホストにログインしていた最終ユーザの内部 ID 番号。
user_last_name	ユーザの姓。
user_last_seen_sec	システムが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。
user_last_updated_sec	ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。
user_name	ユーザのログイン ユーザ名。
user_phone	ユーザの電話番号。
vlan_id	VLAN 識別番号(該当する場合)。
white_list_name	違反が発生したホワイト リスト。
white_list_uuid	ホワイト リストの固有識別子。

white_list_event の結合

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

表 9-6　white_list_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
ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

white_list_event のサンプル クエリ

次のクエリは、指定された時点よりも前に生成されたレコードを最大 25 件返します。これらのレコードには、ホワイト リスト イベントに関する情報（コンプライアンス ポリシー名、イベント生成時点のタイムスタンプ、ホワイト リストの名前など）が含まれます。

```
SELECT policy_name, policy_time_sec, ipaddr, user_name, port, description,
white_list_name, priority, host_criticality, sensor_name

FROM white_list_event WHERE policy_time_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00")

ORDER BY policy_time_sec DESC LIMIT 0, 25;
```

white_list_violation

white_list_violation テーブルは、コンプライアンス ホワイト リスト違反を追跡します。この違反は、ネットワーク上のホストが、アクティブなコンプライアンス ポリシーのコンプライアンス ホワイト リストにどのように違反しているかを追跡します。

詳細については、次の項を参照してください。

- white_list_violation のフィールド（9-10 ページ）
- white_list_violation の結合（9-11 ページ）
- white_list_violation のサンプル クエリ（9-11 ページ）

white_list_violation のフィールド

次の表に、**white_list_violation** 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 9-7　white_list_violation のフィールド

フィールド	説明
host_id	ホワイト リストに違反するホストの ID 番号。
info	ホワイト リスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。 ホワイト リストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらなのかも示されます。
ip_address	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。
port	サービス ホワイト リスト違反をトリガーしたイベント（非準拠サービスの結果として違反が発生した場合）に関連付けられているポート（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。
protocol_name	イベントに関連付けられているプロトコル。

表 9-7　white_list_violation のフィールド(続き)

フィールド	説明
type	ホワイト リスト違反のタイプ。非準拠が原因で違反が発生したかどうかを示します。 • オペレーティング システム(os) • サービス(service) • クライアント アプリケーション(client app) • プロトコル(protocol)
violation_time_sec	違反がログに記録された日時を示す UNIX タイムスタンプ。
white_list_name	違反が発生したホワイト リスト。
white_list_uuid	ホワイト リストの固有識別子。

white_list_violation の結合

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

white_list_violation のサンプル クエリ

次のクエリは、ホワイト リスト違反に関する情報(ホワイト リストに違反するホストの IP アドレス、違反が発生したホワイト リストの名前、違反の数など)を含むレコードを最大 25 件返します。

```
SELECT host_id, white_list_name, count(*)
FROM white_list_violation
GROUP BY white_list_name, host_id
ORDER BY white_list_name
DESC LIMIT 0, 25;
```