スキーマ:接続ログ テーブル

この章では、接続データ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。「バージョン」欄は、示されている各テーブルでサポートされているデータベース アクセスのバージョンを示します。

表 7-1　　接続ログ 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
connection_log（7-1 ページ）	個別の接続。廃止されたテーブル **rna_flow** を置き換えます。	5.0+
connection_summary（7-15 ページ）	接続ログのサマリ。廃止されたテーブル **rna_flow_summary** を置き換えます。	5.0+
si_connection_log（7-19 ページ）	個別の接続。セキュリティ インテリジェンスに使用されます。	5.3+

connection_log

connection_log テーブルには、接続イベントに関する情報が格納されます。Firepower システムは、モニタ対象ホストとその他のホストの間で接続が確立されると接続イベントを生成します。このイベントには、モニタ対象トラフィックに関する詳細情報が含まれています。

connection_log テーブルは、Firepower システム バージョン 5.0 以降で廃止されたテーブル **rna_flow** を置き換えます。

詳細については、次の項を参照してください。

- connection_log のフィールド（7-2 ページ）
- connection_log の結合（7-15 ページ）
- connection_log のサンプル クエリ（7-15 ページ）

connection_log のフィールド

次の表に、**connection_log** 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 7-2　connection_log のフィールド

フィールド	説明
access_control_policy_name	接続をログに記録したアクセス コントロール ルール(またはデフォルト アクション)を含むアクセス コントロール ポリシー。
access_control_policy_UUID	接続をログに記録したアクセス コントロール ルール(またはデフォルト アクション)を含むアクセス コントロール ポリシーの UUID。
access_control_reason	アクセス コントロール ルールによって接続がログに記録された理由。次の 1 つまたは複数が表示されます。 • IP Block • IP Monitor • User Bypass • File Monitor • File Block • Intrusion Monitor • Intrusion Block • File Resume Block • File Resume Allow • File Custom Detection • SSL Block • DNS Block • DNS Monitor • URL Block • URL Monitor • HTTP Injection • Intelligent App Bypass • ログに記録された接続がない場合は空白
access_control_rule_action	アクセス コントロール ルールに関連付けられているアクション(またはデフォルト アクション):allow、block など。
access_control_rule_id	ルールの内部識別番号。
access_control_rule_name	接続をログに記録したアクセス コントロール ルール(またはデフォルト アクション)。
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) • unknown(システムが既知のサーバ フィンガープリントに基づいてサーバを識別できない場合) • 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)

表 7-2　connection_log のフィールド(続き)

フィールド	説明
bytes_recv	セッション レスポンダが送信した合計バイト数。
bytes_sent	セッション イニシエータが送信した合計バイト数。
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	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)。 • 空白(接続にクライアント アプリケーション情報がない場合)。
client_application_version	クライアント アプリケーションのバージョン。
connection_type	接続情報の検出ソース。次のいずれかを行います。 • rna:シスコ デバイスで検出された場合 • netflow:NetFlow 対応デバイスによりエクスポートされる場合
counter	接続イベントに関連する侵入イベントのカウンタ。
dns_ttl	DNS レスポンスの存続期間(秒単位)。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
dns_response	DNS 応答。有効な値は次のとおりです。 • 0:NoError — エラーなし • 1:FormErr — フォーマット エラー • 2:ServFail — サーバ障害 • 3:NXDomain — 存在していないドメイン • 4:NotImp — 未実装 • 5:Refused — クエリ拒否 • 6:YXDomain — 名前が存在してはならない状況で存在している • 7:YXRRSet — RR セットが存在してはならない状況で存在している • 8:NXRRSet — 存在しているべき RR セットが存在していない • 9:NotAuth — 未承認 • 10:NotZone — 名前がゾーンに含まれていない • 16:BADSIG — TSIG 署名失敗 • 17:BADKEY — キーが認識されない • 18:BADTIME — 時間範囲外の署名 • 19:BADMODE — 不適切な TKEY モード • 20:BADNAME — 重複するキー名 • 21:BADALG — サポートされていないアルゴリズム • 22:BADTRUNC — 不適切な切り捨て • 3841(NXDOMAIN):ファイアウォールからの NXDOMAIN 応答 • 3842:SINKHOLE — ファイアウォールからのシンクホール応答
domain_name	セッションのドメインの名前。
domain_uuid	セッションのドメインの UUID。これはバイナリで示されます。
endpoint_profile	接続エンドポイントで使用されるデバイスのタイプの名前。
file_count	セッションで Snort によって識別されたファイルの数。セッションで識別されるファイルごと 1 件のレコードが生成されます。
first_packet_sec	セッションの最初のパケットが検出された日時を示す UNIX タイムスタンプ。
flow_id	接続の内部識別番号。
http_response_code	接続での HTTP 要求に対する応答コード。
hostname_in_query	接続が DNS クエリの場合に使用されるホスト名。
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。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
initiator_continent_name	セッションを開始した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
initiator_country_id	セッションを開始したホストの国のコード。
initiator_country_name	セッションを開始したホストの国の名前。
initiator_ip	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。
initiator_ip_address	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。
initiator_ipaddr	セッションを開始したホストの IP アドレスのバイナリ表現。
initiator_ipv4	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。
initiator_port	セッション イニシエータが使用するポート。
initiator_user_dept	イニシエータ ホストの最終ログイン ユーザが所属する部門。
initiator_user_email	イニシエータ ホストの最終ログイン ユーザの電子メールアドレス。
initiator_user_first_name	イニシエータ ホストの最終ログイン ユーザの名前。
initiator_user_id	イニシエータ ホストの最終ログイン ユーザの内部識別番号。
initiator_user_last_name	イニシエータ ホストの最終ログイン ユーザの姓。
initiator_user_last_seen_sec	イニシエータ ホストの最終ログイン ユーザのユーザ アクティビティを Firepower システム が最後に検出した日時を示す UNIX タイムスタンプ。
initiator_user_last_updated_sec	イニシエータ ホストの最終ログイン ユーザのユーザ レコードを Firepower システム が最後に更新した日時を示す UNIX タイムスタンプ。
initiator_user_name	イニシエータ ホストの最終ログイン ユーザのユーザ名。
initiator_user_phone	イニシエータ ホストの最終ログイン ユーザの電話番号。
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	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。
ioc_count	接続で検出された侵害の痕跡の数。
ips_event_count	侵入イベントのしきい値に達するまでに、接続で生成された侵入イベントの数。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
last_packet_sec	セッションの最後のパケットが検出された日時を示す UNIX タイム スタンプ。
location_ip	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
monitor_rule_id_1	接続に関連付けられている 1 番目のモニタ ルールの ID。この ID は、monitor_rule_name_1 に格納されている名前に関連付けられています。
monitor_rule_id_2	接続に関連付けられている 2 番目のモニタ ルールの ID。この ID は、monitor_rule_name_2 に格納されている名前に関連付けられています。
monitor_rule_id_3	接続に関連付けられている 3 番目のモニタ ルールの ID。この ID は、monitor_rule_name_3 に格納されている名前に関連付けられています。
monitor_rule_id_4	接続に関連付けられている 4 番目のモニタ ルールの ID。この ID は、monitor_rule_name_4 に格納されている名前に関連付けられています。
monitor_rule_id_5	接続に関連付けられている 5 番目のモニタ ルールの ID。この ID は、monitor_rule_name_5 に格納されている名前に関連付けられています。
monitor_rule_id_6	接続に関連付けられている 6 番目のモニタ ルールの ID。この ID は、monitor_rule_name_6 に格納されている名前に関連付けられています。
monitor_rule_id_7	接続に関連付けられている 7 番目のモニタ ルールの ID。この ID は、monitor_rule_name_7 に格納されている名前に関連付けられています。
monitor_rule_id_8	接続に関連付けられている 8 番目のモニタ ルールの ID。この ID は、monitor_rule_name_8 に格納されている名前に関連付けられています。
monitor_rule_name_1	接続に関連付けられている 1 番目のモニタ ルールの名前。この名前は、monitor_rule_id_1 に格納されている ID に関連付けられています。
monitor_rule_name_2	接続に関連付けられている 2 番目のモニタ ルールの名前。この名前は、monitor_rule_id_2 に格納されている ID に関連付けられています。
monitor_rule_name_3	接続に関連付けられている 3 番目のモニタ ルールの名前。この名前は、monitor_rule_id_3 に格納されている ID に関連付けられています。
monitor_rule_name_4	接続に関連付けられている 4 番目のモニタ ルールの名前。この名前は、monitor_rule_id_4 に格納されている ID に関連付けられています。
monitor_rule_name_5	接続に関連付けられている 5 番目のモニタ ルールの名前。この名前は、monitor_rule_id_5 に格納されている ID に関連付けられています。
monitor_rule_name_6	接続に関連付けられている 6 番目のモニタ ルールの名前。この名前は、monitor_rule_id_6 に格納されている ID に関連付けられています。
monitor_rule_name_7	接続に関連付けられている 7 番目のモニタ ルールの名前。この名前は、monitor_rule_id_7 に格納されている ID に関連付けられています。
monitor_rule_name_8	接続に関連付けられている 8 番目のモニタ ルールの名前。この名前は、monitor_rule_id_8 に格納されている ID に関連付けられています。
netbios_domain	接続で使用された NetBIOS ドメイン。
netflow_dst_as	宛先の NetFlow 自律システム番号、起点またはピア
netflow_dst_mask	Netflow 宛先アドレス プレフィックス マスク。
netflow_dst_tos	パケットが宛先から送信元に流れる場合の IP ヘッダーのタイプ オブ サービス(ToS)。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
netflow_snmp_in	送信元から宛先へ流れるパケットが使用するインターフェイスの ID。
netflow_snmp_out	宛先から送信元へ流れるパケットが使用するインターフェイスの ID。
netflow_src_as	送信元の NetFlow 自律システム番号、起点またはピア
netflow_src_mask	Netflow 送信元アドレス プレフィックス マスク。
netflow_src_tos	パケットが送信元から宛先に流れる場合の IP ヘッダーのタイプ オブ サービス(ToS)。
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。
original_client_continent_name	セッションを最初に開始した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 このフィールドは接続にプロキシが存在する場合に使用されます。
original_client_country_id	セッションを最初に開始したホストの国コード。このフィールドは接続にプロキシが存在する場合に使用されます。
original_client_country_name	セッションを最初に開始したホストの国名。このフィールドは接続にプロキシが存在する場合に使用されます。
original_client_ipaddr	セッションを最初に開始したホストの IP アドレスのバイナリ表現。このフィールドは接続にプロキシが存在する場合に使用されます。
packets_recv	セッションを開始したホストが受信したパケットの総数。
packets_sent	セッションを開始したホストが送信したパケットの総数。
prefilter_policy_name	侵入イベントを生成したプレフィルタ ポリシーの名前。
prefilter_policy_UUID	侵入イベントを生成したプレフィルタ ポリシーの UUID。
prefilter_rule_id	プレフィルタ/トンネル ルールの整数の ID。
prefilter_rule_name	プレフィルタ/トンネル ルールの名前。
protocol_name	接続で使用されたプロトコルの名前。
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。
qos_applied_interface_name	QoS が適用されたインターフェイスの名前。
qos_dropped_bytes_recv	QoS によりドロップされたレスポンダ バイト数。
qos_dropped_bytes_sent	QoS によりドロップされたイニシエータ バイト数。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
qos_dropped_packets_recv	QoS によりドロップされたレスポンダ パケット数。
qos_dropped_packets_sent	QoS によりドロップされたイニシエータ パケット数。
qos_policy_name	QoS ポリシーの名前。
qos_policy_uuid	QoS ポリシーの UUID。
qos_rule_id	QoS ルールの整数の ID。
qos_rule_name	QoS ルールの名前。
responder_continent_name	セッション イニシエータに対して応答したホストの所在地の地域の名前。 **: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
responder_country_id	セッション イニシエータに対して応答したホストの国のコード。
responder_country_name	セッション イニシエータに対して応答したホストの国の名前。
responder_ip	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。
responder_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。
responder_ipaddr	セッション イニシエータに対して応答したホストの IPv4 または IP v 6 アドレスのバイナリ表現。
responder_ipv4	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。
responder_port	セッション レスポンダが使用するポート。
responder_user_dept	セッション イニシエータに対して応答したホストの最終ログイン ユーザの所属部門。
responder_user_email	セッション イニシエータに対して応答したホストの最終ログイン ユーザの電子メールアドレス。
responder_user_first_name	セッション イニシエータに対して応答したホストの最終ログイン ユーザの名前。
responder_user_id	セッション イニシエータに対して応答したホストの最終ログイン ユーザの内部識別番号。
responder_user_last_name	セッション イニシエータに対して応答したホストの最終ログイン ユーザの姓。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
responder_user_last_seen_sec	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ アクティビティを Firepower システム が最後に検出した日時を示す UNIX タイムスタンプ。
responder_user_last_updated_sec	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ レコードを Firepower システム が最後に更新した日時を示す UNIX タイムスタンプ。
responder_user_name	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ名。
responder_user_phone	セッション イニシエータに対して応答したホストの最終ログイン ユーザの電話番号。
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_group	ネットワーク トラフィック グループの ID 番号。
security_intelligence_category	接続に関連付けられているセキュリティ インテリジェンス カテゴリ。
security_intelligence_ip	セキュリティ インテリジェンスによりモニタされる、接続に関連付けられている IP アドレスが、送信元 IP(src)と宛先 IP(dst)のいずれであるか。
security_zone_egress_name	接続イベントの出力セキュリティ ゾーン。
security_zone_ingress_name	接続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	セッションをモニタ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)。
sinkhole	シンクホール オブジェクトに関連付けられているリビジョン UUID。
source_device	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。
src_device_ip	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_device_ipaddr	次のいずれかを行います。 • 接続データをエクスポートした NetFlow 対応デバイスの IP アドレスのバイナリ表現。 • 0(シスコ 管理対象デバイスにより検出される接続の場合)。
src_device_ipv4	• 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。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
ssl_actual_action	SSL ルールに基づいて接続に対して実行されたアクション。ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは異なることがあります。有効な値は次のとおりです。 • 不明 • Do Not Decrypt • ブロック(Block) • Block With Reset • Decrypt (Known Key) • Decrypt (Replace Key) • Decrypt (Resign)
ssl_cipher_suite	SSL 接続で使用される暗号スイート。値は 10 進形式で格納されます。値によって示される暗号スイートについては、 www.iana.org/assignments/tls-parameters/tls-parameters. xhtml を参照してください。
ssl_expected_action	SSL ルールに基づいて接続に対して実行する必要があるアクション。有効な値は次のとおりです。 • *不明* • *Do Not Decrypt* • *ブロック(Block)* • *Block With Reset* • *Decrypt (Known Key)* • *Decrypt (Replace Key)* • *Decrypt (Resign)*

表 7-2　connection_log のフィールド(続き)

フィールド	説明
ssl_flow_flags	暗号化接続のデバッグ レベル フラグ。有効な値は次のとおりです。 • 0x00000001:NSE_FLOW__VALID — 他のフィールドを有効にするために設定する必要があります • 0x00000002:NSE_FLOW__INITIALIZED — 内部構造が処理可能です • 0x00000004:NSE_FLOW__INTERCEPT — SSL セッションが代行受信されました • 0x40000000:CH_CIPHERS_MODIFIED — client hello で暗号が変更されています。 • 0x80000000:CH_CURVES_MODIFIED — client hello で暗号曲線が変更されています。 • 0x100000000:CH_TLS_DOWNGRADED — クライアント側の接続の TLS バージョンがダウングレードされました。 • 0x200000000:CH_SESSION_ID_ZEROED — client hello でセッション ID が削除されました。 • 0x400000000:CH_SESSION_TICKET_ZEROED — client hello のセッション チケットが削除されました。 • 0x800000000:CH_EXTENSION_REMOVED — TLS 拡張子が client hello から削除されました。 • 0x1000000000:CH_ALPN_MODIFIED — client hello の ALPN 拡張子が変更されました。 • 0x2000000000:CH_PADDING_MODIFIED — client hello の padding 拡張子が変更されました。 • 0x4000000000:CH_MISMATCH — client hello の時間で使用されるキャッシュ済みのサーバ証明書が変更されました。 • 0x8000000000:CH_ALPN_HAS_H2 — client hello の ALPN 拡張子に HTTP/2 が追加されました。 • 0x10000000000:SH_ALPN_HAS_H2 — server hello の ALPN 拡張子に HTTP/2 が追加されました。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
ssl_flow_messages	SSL ハンドシェイク時にクライアントとサーバ間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001:NSE_MT__HELLO_REQUEST • 0x00000002:NSE_MT__CLIENT_ALERT • 0x00000004:NSE_MT__SERVER_ALERT • 0x00000008:NSE_MT__CLIENT_HELLO • 0x00000010:NSE_MT__SERVER_HELLO • 0x00000020:NSE_MT__SERVER_CERTIFICATE • 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080:NSE_MT__CERTIFICATE_REQUEST • 0x00000100:NSE_MT__SERVER_HELLO_DONE • 0x00000200:NSE_MT__CLIENT_CERTIFICATE • 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800:NSE_MT__CERTIFICATE_VERIFY • 0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000:NSE_MT__CLIENT_FINISHED • 0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000:NSE_MT__SERVER_FINISHED • 0x00010000:NSE_MT__NEW_SESSION_TICKET • 0x00020000:NSE_MT__HANDSHAKE_OTHER • 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000:NSE_MT__APP_DATA_FROM_SERVER

表 7-2　connection_log のフィールド(続き)

フィールド	説明
ssl_flow_status	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 'Unknown' • 'No Match' • 'Success' • 'Uncached Session' • 'Unknown Cipher Suite' • 'Unsupported Cipher Suite' • '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' • 'Invalid Action'
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。

表 7-2　connection_log のフィールド(続き)

フィールド	説明
ssl_issuer_organization_unit	SSL 証明書の発行元の組織単位。
ssl_policy_action	ルールが一致しない場合のためにポリシーで設定されているデフォルト アクション。
ssl_policy_name	接続を処理した SSL ポリシーの ID 番号。
ssl_policy_reason	SSL ポリシーが SSL セッションをログに記録した理由。
ssl_rule_action	SSL ルールに対しユーザ インターフェイスで選択されたアクション(allow、block など)。
ssl_rule_name	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
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_server_name	SSL Client Hello でサーバ名に指定された名前。
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。
ssl_url_category	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
ssl_version	接続の暗号化に使用された SSL または TLS プロトコル バージョン。
tcp_flags	セッションで検出された TCP フラグ。
url	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(使用可能な場合)。
url_category	モニタ対象ホストによって要求された URL のカテゴリ。
url_reputation	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。次のいずれかが必要です。 • 1:高リスク • 2:疑わしいサイト • 3:セキュリティ リスクのある無害なサイト • 4:無害なサイト • 5:既知
web_application_id	Web アプリケーションの内部識別番号。
web_application_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)。 • 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)。

connection_log の結合

次の表に、**connection_log** テーブルを使用して実行できる結合について説明します。

表 7-3　connection_log 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
initiator_ipaddr または responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

connection_log のサンプル クエリ

次のクエリは、**connection_log** テーブルから最大 25 件の接続イベント レコードを、パケットのタイムスタンプに基づいて降順にソートして返します。

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation

FROM connection_log

WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00" ) ORDER BY
first_packet_sec

DESC, last_packet_sec DESC LIMIT 0, 25;
```

connection_summary

connection_summary テーブルには、接続サマリまたは集約された接続に関する情報が格納されます。Firepower システムは、5 分間隔で接続を集約します。接続を集約対象にするには、接続が次の条件に対応している必要があります。

- 同一の送信元の IP アドレスと宛先 IP アドレスである
- 同じプロトコルを使用している
- 同じアプリケーションを使用している
- 同じ管理対象デバイスにより検出されているか(Firepower での管理対象デバイスにより検出されたセッションの場合)、または同じ NetFlow 対応デバイスによりエクスポートされ、同じ管理対象デバイスにより処理されている

接続サマリの集約データには、イニシエータ ホストとレスポンダ ホストにより送信されたパケットとバイトの総数と、サマリに含まれる接続の数などがあります。

connection_summary テーブルは、Firepower システム バージョン 5.0 以降で廃止されたテーブル **rna_flow_summary** を置き換えます。

詳細については、次の項を参照してください。

- connection_summary のフィールド（7-16 ページ）
- connection_summary の結合（7-18 ページ）
- connection_summary のサンプル クエリ（7-19 ページ）

connection_summary のフィールド

次の表に、**connection_summary** 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 7-4　connection_summary のフィールド

フィールド	説明
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） • unknown（システムが既知のサーバ フィンガープリントに基づいてサーバを識別できない場合） • 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）
bytes_recv	セッション レスポンダが送信した合計バイト数。
bytes_sent	セッション イニシエータが送信した合計バイト数。
connection_type	接続情報の検出ソース。次のいずれかを行います。 • rna：シスコ デバイスで検出された場合 • netflow：NetFlow 対応デバイスによりエクスポートされる場合
domain_name	セッションのドメインの名前。
domain_uuid	セッションのドメインの UUID。これはバイナリで示されます。
flow_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。
id	接続サマリの内部識別番号。
initiator_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。
initiator_ipaddr	セッションを開始したホストの IP アドレスのバイナリ表現。
initiator_user_dept	イニシエータ ホストの最終ログイン ユーザが所属する部門。
initiator_user_email	イニシエータ ホストの最終ログイン ユーザの電子メールアドレス。
initiator_user_first_name	イニシエータ ホストの最終ログイン ユーザの名前。
initiator_user_id	イニシエータ ホストの最終ログイン ユーザの内部識別番号。

表 7-4　connection_summary のフィールド(続き)

フィールド	説明
initiator_user_last_name	イニシエータ ホストの最終ログイン ユーザの姓。
initiator_user_last_seen_sec	イニシエータ ホストの最終ログイン ユーザのユーザ アクティビティを Firepower システム が最後に検出した日時を示す UNIX タイムスタンプ。
initiator_user_last_updated_sec	イニシエータ ホストの最終ログイン ユーザのユーザ レコードを Firepower システム が最後に更新した日時を示す UNIX タイムスタンプ。
initiator_user_name	イニシエータ ホストの最終ログイン ユーザのユーザ名。
initiator_user_phone	イニシエータ ホストの最終ログイン ユーザの電話番号。
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。
netmap_num	接続が検出されたドメインの Netmap ID。
num_connections	サマリに含まれる接続の数。長時間接続(複数の接続サマリー間隔にわたる接続)の場合、最初の接続サマリー間隔の分だけ増加します。
original_client_ipaddr	セッションを最初に開始したホストの IP アドレスのバイナリ表現。このフィールドは接続にプロキシが存在する場合に使用されます。
packets_recv	セッション レスポンダが送信した合計パケット数。
packets_sent	セッション イニシエータが送信した合計パケット数。
protocol_name	集約セッションで使用されたプロトコルの名前。
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。
responder_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。
responder_ipaddr	集約されたセッションのイニシエータに応答したホストの IP アドレスのバイナリ表現。
responder_port	集約セッションでレスポンダが使用したポート。
responder_user_dept	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザの所属部門。
responder_user_email	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザの電子メールアドレス。
responder_user_first_name	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザの名前。
responder_user_id	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザの内部識別番号
responder_user_last_name	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザの姓。
responder_user_last_seen_sec	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザのユーザ アクティビティを Firepower システム が最後に検出した日時を示す UNIX タイムスタンプ。

表 7-4　connection_summary のフィールド(続き)

フィールド	説明
responder_user_last_updated_sec	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ レコードを Firepower システム が最後に更新した日時を示す UNIX タイムスタンプ。
responder_user_name	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザのユーザ名。
responder_user_phone	集約セッションのイニシエータに対して応答したホストの最終ログイン ユーザの電話番号。
security_zone_egress_name	接続イベントの出力セキュリティ ゾーン。
security_zone_ingress_name	接続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	集約セッションをモニタ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)。
source_device	送信元デバイスの ID。これは次のいずれかです。 • 接続のデータをエクスポートした NetFlow 対応デバイスの IP アドレス • Firepower:接続が シスコ管理対象デバイスにより検出された場合
start_time_sec	サマリーのセッション集約に使用される 5 分間の間隔の開始時点の日時を示す UNIX タイムスタンプ。

connection_summary の結合

次の表に、**connection_summary** テーブルを使用して実行できる結合について説明します。

表 7-5　connection_summary 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	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
initiator_ipaddr または responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

connection_summary のサンプル クエリ

次のクエリは、選択されたデバイスにより検出されたイベント サマリ レコードを最大 5 件返します。

```
SELECT initiator_ipaddr, responder_ipaddr, protocol_name, application_protocol_id,
source_device, sensor_name, sensor_address, packets_recv, packets_sent, bytes_recv,
bytes_sent, connection_type, num_connections

FROM connection_summary

WHERE sensor_name='linden' limit 5;
```

si_connection_log

si_connection_log テーブルには、セキュリティ インテリジェンス イベントに関する情報が格納されます。Firepower システム は、セキュリティ インテリジェンスにより接続がブラックリストに追加またはモニタされるときに、セキュリティ インテリジェンス イベントを生成します。このイベントには、モニタ対象トラフィックに関する詳細情報が含まれています。

詳細については、次の項を参照してください。

- si_connection_log のフィールド(7-19 ページ)
- si_connection_log の結合(7-31 ページ)
- si_connection_log のサンプル クエリ(7-31 ページ)

si_connection_log のフィールド

次の表に、**si_connection_log** 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 7-6　si_connection_log のフィールド

フィールド	説明
access_control_policy_name	接続をログに記録したアクセス コントロール ルール(またはデフォルト アクション)を含むアクセス コントロール ポリシー。
access_control_policy_UUID	接続をログに記録したアクセス コントロール ルール(またはデフォルト アクション)を含むアクセス コントロール ポリシーの UUID。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
access_control_reason	アクセス コントロール ルールによって接続がログに記録された理由。次の 1 つまたは複数が表示されます。 • IP Block • IP Monitor • User Bypass • File Monitor • File Block • Intrusion Monitor • Intrusion Block • File Resume Block • File Resume Allow • File Custom Detection • SSL Block • DNS Block • DNS Monitor • URL Block • URL Monitor • HTTP Injection • Intelligent App Bypass • ログに記録された接続がない場合は空白
access_control_rule_action	アクセス コントロール ルールに関連付けられているアクション(またはデフォルト アクション):allow、block など。
access_control_rule_id	ルールの内部識別番号。
access_control_rule_name	接続をログに記録したアクセス コントロール ルール(またはデフォルト アクション)。
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) • unknown(システムが既知のサーバ フィンガープリントに基づいてサーバを識別できない場合) • 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)
bytes_recv	セッション レスポンダが送信した合計バイト数。
bytes_sent	セッション イニシエータが送信した合計バイト数。
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	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。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
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)。 • 空白(接続にクライアント アプリケーション情報がない場合)。
client_application_version	クライアント アプリケーションのバージョン。
connection_type	接続情報の検出ソース。次のいずれかを行います。 • rna:シスコ デバイスで検出された場合 • netflow:NetFlow 対応デバイスによりエクスポートされる場合
counter	接続イベントに関連する侵入イベントのカウンタ。
dns_ttl	DNS レスポンスの存続期間(秒単位)。
dns_response	DNS 応答。有効な値は次のとおりです。 • 0:NoError — エラーなし • 1:FormErr — フォーマット エラー • 2:ServFail — サーバ障害 • 3:NXDomain — 存在していないドメイン • 4:NotImp — 未実装 • 5:Refused — クエリ拒否 • 6:YXDomain — 名前が存在してはならない状況で存在している • 7:YXRRSet — RR セットが存在してはならない状況で存在している • 8:NXRRSet — 存在しているべき RR セットが存在していない • 9:NotAuth — 未承認 • 10:NotZone — 名前がゾーンに含まれていない • 16:BADSIG — TSIG 署名失敗 • 17:BADKEY — キーが認識されない • 18:BADTIME — 時間範囲外の署名 • 19:BADMODE — 不適切な TKEY モード • 20:BADNAME — 重複するキー名 • 21:BADALG — サポートされていないアルゴリズム • 22:BADTRUNC — 不適切な切り捨て • 3841(NXDOMAIN):ファイアウォールからの NXDOMAIN 応答 • 3842:SINKHOLE — ファイアウォールからのシンクホール応答
domain_name	セッションのドメインの名前。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
domain_uuid	セッションのドメインの UUID。これはバイナリで示されます。
endpoint_profile	接続エンドポイントで使用されるデバイスのタイプの名前。
file_count	セッションで Snort によって識別されたファイルの数。セッションで識別されるファイルごと 1 件のレコードが生成されます。
first_packet_sec	セッションの最初のパケットが検出された日時を示す UNIX タイムスタンプ。
http_response_code	接続での HTTP 要求に対する応答コード。
hostname_in_query	接続が DNS クエリの場合に使用されるホスト名。
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。
initiator_continent_name	セッションを開始したホストの所在地の地域の名前。 **: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
initiator_country_id	セッションを開始したホストの国のコード。
initiator_country_name	セッションを開始したホストの国の名前。
initiator_ipaddr	セッションを開始したホストの IP アドレスのバイナリ表現。
initiator_port	セッション イニシエータが使用するポート。
initiator_user_dept	イニシエータ ホストの最終ログイン ユーザが所属する部門。
initiator_user_email	イニシエータ ホストの最終ログイン ユーザの電子メールアドレス。
initiator_user_first_name	イニシエータ ホストの最終ログイン ユーザの名前。
initiator_user_id	イニシエータ ホストの最終ログイン ユーザの内部識別番号。
initiator_user_last_name	イニシエータ ホストの最終ログイン ユーザの姓。
initiator_user_last_seen_sec	イニシエータ ホストの最終ログイン ユーザのユーザ アクティビティを Firepower システム が最後に検出した日時を示す UNIX タイムスタンプ。
initiator_user_last_updated_sec	イニシエータ ホストの最終ログイン ユーザのユーザ レコードを Firepower システム が最後に更新した日時を示す UNIX タイムスタンプ。
initiator_user_name	イニシエータ ホストの最終ログイン ユーザのユーザ名。
initiator_user_phone	イニシエータ ホストの最終ログイン ユーザの電話番号。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
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	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。
ioc_count	接続で検出された侵害の痕跡の数。
ips_event_count	侵入イベントのしきい値に達するまでに、接続で生成された侵入イベントの数。
last_packet_sec	セッションの最後のパケットが検出された日時を示す UNIX タイムスタンプ。
location_ip	ISE と通信するインターフェイスの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。
monitor_rule_id_1	接続に関連付けられている 1 番目のモニタ ルールの ID。この ID は、monitor_rule_name_1 に格納されている名前に関連付けられています。
monitor_rule_id_2	接続に関連付けられている 2 番目のモニタ ルールの ID。この ID は、monitor_rule_name_2 に格納されている名前に関連付けられています。
monitor_rule_id_3	接続に関連付けられている 3 番目のモニタ ルールの ID。この ID は、monitor_rule_name_3 に格納されている名前に関連付けられています。
monitor_rule_id_4	接続に関連付けられている 4 番目のモニタ ルールの ID。この ID は、monitor_rule_name_4 に格納されている名前に関連付けられています。
monitor_rule_id_5	接続に関連付けられている 5 番目のモニタ ルールの ID。この ID は、monitor_rule_name_5 に格納されている名前に関連付けられています。
monitor_rule_id_6	接続に関連付けられている 6 番目のモニタ ルールの ID。この ID は、monitor_rule_name_6 に格納されている名前に関連付けられています。
monitor_rule_id_7	接続に関連付けられている 7 番目のモニタ ルールの ID。この ID は、monitor_rule_name_7 に格納されている名前に関連付けられています。
monitor_rule_id_8	接続に関連付けられている 8 番目のモニタ ルールの ID。この ID は、monitor_rule_name_8 に格納されている名前に関連付けられています。
monitor_rule_name_1	接続に関連付けられている 1 番目のモニタ ルールの名前。この名前は、monitor_rule_id_1 に格納されている ID に関連付けられています。
monitor_rule_name_2	接続に関連付けられている 2 番目のモニタ ルールの名前。この名前は、monitor_rule_id_2 に格納されている ID に関連付けられています。
monitor_rule_name_3	接続に関連付けられている 3 番目のモニタ ルールの名前。この名前は、monitor_rule_id_3 に格納されている ID に関連付けられています。
monitor_rule_name_4	接続に関連付けられている 4 番目のモニタ ルールの名前。この名前は、monitor_rule_id_4 に格納されている ID に関連付けられています。
monitor_rule_name_5	接続に関連付けられている 5 番目のモニタ ルールの名前。この名前は、monitor_rule_id_5 に格納されている ID に関連付けられています。
monitor_rule_name_6	接続に関連付けられている 6 番目のモニタ ルールの名前。この名前は、monitor_rule_id_6 に格納されている ID に関連付けられています。
monitor_rule_name_7	接続に関連付けられている 7 番目のモニタ ルールの名前。この名前は、monitor_rule_id_7 に格納されている ID に関連付けられています。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
monitor_rule_name_8	接続に関連付けられている 8 番目のモニタ ルールの名前。この名前は、monitor_rule_id_8 に格納されている ID に関連付けられています。
netbios_domain	接続で使用された NetBIOS ドメイン。
netflow_dst_as	宛先の NetFlow 自律システム番号、起点またはピア
netflow_dst_mask	Netflow 宛先アドレス プレフィックス マスク。
netflow_dst_tos	パケットが宛先から送信元に流れる場合の IP ヘッダーのタイプ オブ サービス(ToS)。
netflow_snmp_in	送信元から宛先へ流れるパケットが使用するインターフェイスの ID。
netflow_snmp_out	宛先から送信元へ流れるパケットが使用するインターフェイスの ID。
netflow_src_as	送信元の NetFlow 自律システム番号、起点またはピア
netflow_src_mask	Netflow 送信元アドレス プレフィックス マスク。
netflow_src_tos	パケットが送信元から宛先に流れる場合の IP ヘッダーのタイプ オブ サービス(ToS)。
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。
original_client_continent_name	セッションを最初に開始した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 このフィールドは接続にプロキシが存在する場合に使用されます。
original_client_country_id	セッションを最初に開始したホストの国コード。このフィールドは接続にプロキシが存在する場合に使用されます。
original_client_country_name	セッションを最初に開始したホストの国名。このフィールドは接続にプロキシが存在する場合に使用されます。
original_client_ipaddr	セッションを最初に開始したホストの IP アドレスのバイナリ表現。このフィールドは接続にプロキシが存在する場合に使用されます。
packets_recv	セッションを開始したホストが受信したパケットの総数。
packets_sent	セッションを開始したホストが送信したパケットの総数。
prefilter_policy_name	侵入イベントを生成したプレフィルタ ポリシーの名前。
prefilter_policy_UUID	侵入イベントを生成したプレフィルタ ポリシーの UUID。
prefilter_rule_id	プレフィルタ/トンネル ルールの整数の ID。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
prefilter_rule_name	プレフィルタ/トンネル ルールの名前。
protocol_name	接続で使用されたプロトコルの名前。
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。
qos_applied_interface_name	QoS が適用されたインターフェイスの名前。
qos_dropped_bytes_recv	QoS によりドロップされたレスポンダ バイト数。
qos_dropped_bytes_sent	QoS によりドロップされたイニシエータ バイト数。
qos_dropped_packets_recv	QoS によりドロップされたレスポンダ パケット数。
qos_dropped_packets_sent	QoS によりドロップされたイニシエータ パケット数。
qos_policy_name	QoS ポリシーの名前。
qos_policy_uuid	QoS ポリシーの UUID。
qos_rule_id	QoS ルールの整数の ID。
qos_rule_name	QoS ルールの名前。
responder_continent_name	セッション イニシエータに対して応答したホストの所在地の地域の名前。 **: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
responder_country_id	セッション イニシエータに対して応答したホストの国のコード。
responder_country_name	セッション イニシエータに対して応答したホストの国の名前。
responder_ipaddr	セッション イニシエータに対して応答したホストの IPv4 または IP v 6 アドレスのバイナリ表現。
responder_port	セッション レスポンダが使用するポート。
responder_user_dept	セッション イニシエータに対して応答したホストの最終ログイン ユーザの所属部門。
responder_user_email	セッション イニシエータに対して応答したホストの最終ログイン ユーザの電子メールアドレス。
responder_user_first_name	セッション イニシエータに対して応答したホストの最終ログイン ユーザの名前。
responder_user_id	セッション イニシエータに対して応答したホストの最終ログイン ユーザの内部識別番号。
responder_user_last_name	セッション イニシエータに対して応答したホストの最終ログイン ユーザの姓。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
responder_user_last_seen_sec	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ アクティビティを Firepower システム が最後に検出した日時を示す UNIX タイムスタンプ。
responder_user_last_updated_sec	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ レコードを Firepower システム が最後に更新した日時を示す UNIX タイムスタンプ。
responder_user_name	セッション イニシエータに対して応答したホストの最終ログイン ユーザのユーザ名。
responder_user_phone	セッション イニシエータに対して応答したホストの最終ログイン ユーザの電話番号。
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_group	ネットワーク トラフィック グループの ID 番号。
security_intelligence_category	接続に関連付けられているセキュリティ インテリジェンス カテゴリ。
security_intelligence_ip	セキュリティ インテリジェンスによりモニタされる、接続に関連付けられている IP アドレスが、送信元 IP(src)と宛先 IP(dst)のいずれであるか。
security_zone_egress_name	接続イベントの出力セキュリティ ゾーン。
security_zone_ingress_name	接続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	セッションをモニタ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)。
sinkhole	シンクホール オブジェクトに関連付けられているリビジョン UUID。
src_device_ipaddr	次のいずれかを行います。 • 接続データをエクスポートした NetFlow 対応デバイスの IP アドレスのバイナリ表現。 • 0(シスコ 管理対象デバイスにより検出される接続の場合)。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
ssl_actual_action	SSL ルールに基づいて接続に対して実行されたアクション。 ルールに指定されているアクションが不可能なことがあるため、これは予期していたアクションとは 異なることがあります。有効な値は次のとおりです。 • 'Unknown' • 'Do Not Decrypt' • 'Block' • 'Block With Reset' • 'Decrypt (Known Key)' • 'Decrypt (Replace Key)' • 'Decrypt (Resign)'
ssl_cipher_suite	SSL 接続で使用される暗号スイート。値は 10 進形式で格納されます。値によって示される暗号スイートについては、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。
ssl_expected_action	SSL ルールに基づいて接続に対して実行される必要があるアクション。有効な値は次のとおりです。 • 'Unknown' • 'Do Not Decrypt' • 'Block' • 'Block With Reset' • 'Decrypt (Known Key)' • 'Decrypt (Replace Key)' • 'Decrypt (Resign)'
ssl_flow_flags	暗号化接続のデバッグ レベル フラグ。可能性あり値は次のとおりです。 • 0x00000001:NSE_FLOW__VALID — 他のフィールドを有効にするために設定する必要があります • 0x00000002:NSE_FLOW__INITIALIZED — 内部構造が処理可能です • 0x00000004:NSE_FLOW__INTERCEPT — SSL セッションが代行受信されました

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
ssl_flow_messages	SSL ハンドシェイク時にクライアントとサーバ間で交換されたメッセージ。詳細については、http://tools.ietf.org/html/rfc5246 を参照してください。 • 0x00000001:NSE_MT__HELLO_REQUEST • 0x00000002:NSE_MT__CLIENT_ALERT • 0x00000004:NSE_MT__SERVER_ALERT • 0x00000008:NSE_MT__CLIENT_HELLO • 0x00000010:NSE_MT__SERVER_HELLO • 0x00000020:NSE_MT__SERVER_CERTIFICATE • 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080:NSE_MT__CERTIFICATE_REQUEST • 0x00000100:NSE_MT__SERVER_HELLO_DONE • 0x00000200:NSE_MT__CLIENT_CERTIFICATE • 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800:NSE_MT__CERTIFICATE_VERIFY • 0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000:NSE_MT__CLIENT_FINISHED • 0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000:NSE_MT__SERVER_FINISHED • 0x00010000:NSE_MT__NEW_SESSION_TICKET • 0x00020000:NSE_MT__HANDSHAKE_OTHER • 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000:NSE_MT__APP_DATA_FROM_SERVER

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
ssl_flow_status	SSL フローのステータス。アクションが実行された理由、またはエラー メッセージが出された理由を示す値です。有効な値は次のとおりです。 • 'Unknown' • 'No Match' • 'Success' • 'Uncached Session' • 'Unknown Cipher Suite' • 'Unsupported Cipher Suite' • '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' • 'Invalid Action'
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。

表 7-6　si_connection_log のフィールド(続き)

フィールド	説明
ssl_issuer_organization_unit	SSL 証明書の発行元の組織単位。
ssl_policy_action	ルールが一致しない場合のためにポリシーで設定されているデフォルト アクション。
ssl_policy_name	接続を処理した SSL ポリシーの ID 番号。
ssl_policy_reason	SSL ポリシーが SSL セッションをログに記録した理由。
ssl_rule_action	SSL ルールに対しユーザ インターフェイスで選択されたアクション(allow、block など)。
ssl_rule_name	接続を処理した SSL ルールまたはデフォルト アクションの ID 番号。
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_server_name	SSL Client Hello でサーバ名に指定された名前。
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。
ssl_url_category	サーバ名と証明書の共通名から識別されるフローのカテゴリ。
ssl_version	接続の暗号化に使用された SSL または TLS プロトコル バージョン。
tcp_flags	セッションで検出された TCP フラグ。
url	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(使用可能な場合)。
url_category	モニタ対象ホストによって要求された URL のカテゴリ。
url_reputation	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。次のいずれかが必要です。 • 1:高リスク • 2:疑わしいサイト • 3:セキュリティ リスクのある無害なサイト • 4:無害なサイト • 5:既知
web_application_id	Web アプリケーションの内部識別番号。
web_application_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)。 • 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)。

si_connection_log の結合

次の表に、**si_connection_log** テーブルを使用して実行できる結合について説明します。

表 7-7　si_connection_log 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_name または application_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
initiator_ipaddr または responder_ipaddr	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr

si_connection_log のサンプル クエリ

次のクエリは、**si_connection_log** テーブルから最大 25 件の接続イベント レコードを、パケットのタイムスタンプに基づいて降順にソートして返します。

```
SELECT first_packet_sec, last_packet_sec, initiator_ipaddr, responder_ipaddr,
security_zone_ingress_name, security_zone_egress_name, initiator_port, protocol_name,
responder_port, application_protocol_id, client_application_id, web_application_id, url,
url_category, url_reputation

FROM si_connection_log

WHERE first_packet_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY
first_packet_sec

DESC, last_packet_sec DESC LIMIT 0, 25;
```