スキーマ:検出イベントおよびネットワーク マップのテーブル

この章では、検出イベントと シスコ ネットワーク マップに関連するテーブル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。

Firepower システム は、ホストとネットワーク デバイスにより生成されるトラフィックをモニタし、継続的に検出イベントを生成します。

ネットワーク マップとは、検出イベントで報告されるネットワーク資産に関する情報のリポジトリです。ネットワーク マップには、検出された各ホストとネットワーク デバイスに関する情報(オペレーティング システム、サーバ、クライアント アプリケーション、ホスト属性、脆弱性など)が含まれています。

脆弱性は、ホストに被害を及ぼす可能性がある特定の侵害やエクスプロイトの記述です。シスコには独自の脆弱性データベース(VBD)があります。この VBD は Bugtraq データベースと MITRE の CVE データベースを相互参照します。また、ホスト入力機能を使用してサードパーティの脆弱性データをインポートできます。

ネットワーク マップでの特定のホストに関する情報は、ホストのタイプと、モニタ対象トラフィックで使用可能な情報によって異なる可能性があることに注意してください。

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をサポートしている Firepower システム のバージョンを示します。廃止されたテーブルは製品の現行バージョンでも引き続きサポートされていますが、今後もサポートを引き続き受けるために、廃止されたテーブルとフィールドを使用しないでおくことをシスコでは**強く**推奨します。

表 6-1　検出イベントおよびネットワーク マップの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
application_host_map（6-5 ページ）	モニタ対象ネットワークのホストで検出されたアプリケーション。	5.0+
application_ip_map（A-1 ページ）	モニタ対象ネットワークで検出されたアプリケーションに関連付けられているカテゴリ、タグ、生産性、およびリスク。	5.2+
application_ip_map（A-1 ページ）	モニタ対象ネットワークで検出されたアプリケーションに関連付けられているカテゴリ、タグ、生産性、およびリスク。 バージョン 5.2 で廃止置き換わるテーブル: **application_ip_map（A-1 ページ）**。	5.0-5.1.x
application_tag_map（6-10 ページ）	モニタ対象ネットワークで検出されたアプリケーションに関連付けられているタグ	5.0+
domain_control_information（6-12 ページ）	ドメイン階層情報	6.0+
network_discovery_event（6-12 ページ）	検出イベントおよびホスト入力イベント。	5.0+
rna_host（6-14 ページ）	モニタ対象ネットワークのホストの基本情報。	5.2+
rna_host_attribute（6-16 ページ）	モニタ対象ネットワークの各ホストに関連付けられているホスト属性。	5.2+
rna_host_client_app（6-17 ページ）	モニタ対象ネットワークのホストで検出されたクライアント アプリケーション。	5.2+
rna_host_client_app（6-17 ページ）	モニタ対象ネットワークのホストで検出された HTTP（Web ブラウザ）クライアント アプリケーションに関連付けられているペイロード。	5.2+
rna_host_ioc_state（6-23 ページ）	ホストの侵害状態が格納されます。	5.3+
rna_host_ip_map（6-27 ページ）	モニタ対象ネットワークのホストの MAC アドレスにホスト ID を相関付けます。	5.2+
rna_host_os（6-30 ページ）	モニタ対象ネットワークのホストで検出されたオペレーティング システム。	5.2+
rna_host_os_vulns（6-31 ページ）	モニタ対象ネットワークのホストに関連付けられている脆弱性。	5.2+
rna_host_protocol（6-33 ページ）	モニタ対象ネットワークのホストで検出されたプロトコル。	4.10.x+
rna_host_protocol（6-33 ページ）	プロトコルを検出した管理対象デバイスに関連するモニタ対象ネットワーク上のホスト。	5.2+
rna_host_service（6-36 ページ）	モニタ対象ネットワークのホストで検出されたサービス。	5.2+
rna_host_service_banner（6-38 ページ）	モニタ対象ネットワークのホストで検出されたサービスのサービス ベンダーとバージョン（「バナー」）をアドバタイズするネットワーク トラフィックのヘッダー。	5.2+
rna_host_service_info（6-39 ページ）	モニタ対象ネットワークのホストで検出されたサービスの詳細。	5.2+

表 6-1　検出イベントおよびネットワーク マップのテーブルのスキーマ（続き）

参照先	次の内容が格納されるテーブル	Version
rna_host_service_payload（6-43 ページ）	モニタ対象ネットワークのホストで検出されたサービスに関連付けられているペイロード。	5.2+
rna_host_service_subtype（6-45 ページ）	モニタ対象ネットワークのホストで検出されたサービスのサブ サービス。	5.2+
rna_host_service_vulns（6-47 ページ）	モニタ対象ネットワークのホストで検出されたサービスに関連付けられている脆弱性。	5.2+
rna_host_third_party_vuln（6-48 ページ）	モニタ対象ネットワークのホストに関連付けられているサードパーティの脆弱性。	5.2+
rna_host_third_party_vuln_bugtraq_id（6-50 ページ）	モニタ対象ネットワークのホストおよび Bugtraq データベース（`http://www.securityfocus.com/bid/`）の脆弱性に関連付けられているサードパーティの脆弱性。	5.2+
rna_host_third_party_vuln_cve_id（6-52 ページ）	モニタ対象ネットワークのホストおよび MITRE の CVE データベースの脆弱性に関連付けられているサードパーティの脆弱性。（`http://www.cve.mitre.org/`）。	5.2+
rna_host_third_party_vuln_rna_id（6-54 ページ）	モニタ対象ネットワークのホストおよび VDB の脆弱性に関連付けられているサードパーティの脆弱性。	5.2+
rna_ip_host（A-1 ページ）	モニタ対象ネットワークの IP ホストの基本情報。 バージョン 5.2 で廃止置き換わるテーブル **rna_host（6-14 ページ）**。	4.10.x-5.1.x
rna_ip_host_client_app（A-1 ページ）	モニタ対象ネットワークのホストで検出されたクライアント アプリケーション。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_client_app（6-17 ページ）**。	4.10.x-5.1.x
rna_ip_host_client_app_payload（A-1 ページ）	モニタ対象ネットワークの IP ホストで検出された HTTP（Web ブラウザ）クライアント アプリケーションに関連付けられているペイロード。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_client_app（6-17 ページ）**。	4.10.x-5.1.x
rna_ip_host_os（A-1 ページ）	モニタ対象ネットワークの IP ホストで検出されたオペレーティング システム。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_os（6-30 ページ）**。	4.10.x-5.1.x
rna_ip_host_os_vulns（A-1 ページ）	モニタ対象ネットワークの IP ホストに関連付けられている脆弱性。 バージョン 5.2 で廃止置き換わるテーブル：**rna_host_os_vulns（6-31 ページ）**。	4.10.x--5.1.x
rna_ip_host_sensor（A-1 ページ）	ホストを検出した管理対象デバイスに関連するモニタ対象ネットワーク上の IP ホスト。 バージョン 5.2 で廃止置き換わるテーブル：**rna_host_protocol（6-33 ページ）**。	5.0-5.1.x

表 6-1　検出イベントおよびネットワーク マップのテーブルのスキーマ(続き)

参照先	次の内容が格納されるテーブル	Version
rna_ip_host_service(A-1 ページ)	モニタ対象ネットワークの IP ホストで検出されたサービス。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_service(6-36 ページ)**。	4.10.x-5.1.x
rna_ip_host_service_banner(A-1 ページ)	モニタ対象ネットワークのホストで検出されたサービスのサービス ベンダーとバージョン(「バナー」)をアドバタイズするネットワーク トラフィックのヘッダー。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_service_banner(6-38 ページ)**。	4.10.x-5.1.x
rna_ip_host_service_info(A-1 ページ)	モニタ対象ネットワークの IP ホストで検出されたサービスの詳細。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_service_info(6-39 ページ)**。	4.10.x-5.1.x
rna_ip_host_service_payload(A-1 ページ)	モニタ対象ネットワークの IP ホストで検出されたサービスに関連付けられているペイロード。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_service_payload(6-43 ページ)**。	4.10.x-5.1.x
rna_ip_host_service_subtype(A-1 ページ)	モニタ対象ネットワークの IP ホストで検出されたサービスのサブサービス。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_service_subtype(6-45 ページ)**。	4.10.x-5.1.x
rna_ip_host_service_vulns(A-1 ページ)	モニタ対象ネットワークの IP ホストで検出されたサービスに関連付けられている脆弱性。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_service_vulns(6-47 ページ)**。	4.10.x-5.1.x
rna_ip_host_third_party_vuln(A-1 ページ)	モニタ対象ネットワークの IP ホストに関連付けられているサードパーティの脆弱性。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_third_party_vuln(6-48 ページ)**。	4.10.x-5.1.x
rna_ip_host_third_party_vuln_bugtraq_id(A-1 ページ)	モニタ対象ネットワークの IP ホストおよび Bugtraq データベース(`http://www.securityfocus.com/bid/`)の脆弱性に関連付けられているサードパーティの脆弱性。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_third_party_vuln_bugtraq_id(6-50 ページ)**。	4.10.x-5.1.x
rna_ip_host_third_party_vuln_cve_id(A-1 ページ)	モニタ対象ネットワークの IP ホストおよび MITRE の CVE データベースの脆弱性に関連付けられているサードパーティの脆弱性。(`http://www.cve.mitre.org/`)。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_third_party_vuln_cve_id(6-52 ページ)**。	4.10.x-5.1.x

表 6-1　検出イベントおよびネットワーク マップのテーブルのスキーマ（続き）

参照先	次の内容が格納されるテーブル	Version
rna_ip_host_third_party_vuln_rna_id（A-1 ページ）	モニタ対象ネットワークの IP ホストおよび VDB の脆弱性に関連付けられているサードパーティの脆弱性。 バージョン 5.2 で廃止置き換わるテーブル **rna_host_third_party_vuln_rna_id（6-54 ページ）**。	4.10.x-5.1.x
rna_ip_host_user_history（A-1 ページ）	モニタ対象ネットワークの特定の IP ホストに対するユーザ アクティビティ。 バージョン 5.2 で廃止置き換わるテーブル **user_ipaddr_history（6-62 ページ）**。	4.10.x-5.1.x
rna_mac_host（A-1 ページ）	モニタ対象ネットワークの MAC ホスト（IP アドレスを持たないホスト）。	4.10.x-5.1.x
rna_mac_host_sensor（A-1 ページ）	ホストを検出した管理対象デバイスに関連するモニタ対象ネットワーク上の IP ホスト。	5.0-5.1.x
rna_mac_ip_map（A-2 ページ）	モニタ対象ネットワークの IP ホストの MAC アドレス。 バージョン 5.2 で廃止置き換わるテーブル：**rna_host_ip_map（6-27 ページ）**および **rna_host_mac_map（6-28 ページ）**。	4.10.x-5.1.x
rna_vuln（6-56 ページ）	シスコ VDB の脆弱性。	4.10.x+
tag_info（6-59 ページ）	検出されたアプリケーションを特徴付けるタグ。	5.0+
url_categories（6-60 ページ）	モニタ対象ネットワークのホストからアクセスされた URL を特徴付けるカテゴリ。	5.0+
url_reputations（6-61 ページ）	モニタ対象ネットワークのホストからアクセスされた URL を特徴付けるレピュテーション。	5.0+
user_ipaddr_history（6-62 ページ）	モニタ対象ネットワークの特定のホストに対するユーザ アクティビティ。	5.2+

application_host_map

application_host_map テーブルには、ネットワークで検出された各アプリケーションに関連付けられているカテゴリとタグ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。

- application_host_map のフィールド（6-6 ページ）
- application_host_map の結合（6-6 ページ）
- application_host_map のサンプル クエリ（6-7 ページ）

application_host_map のフィールド

次の表に、**application_host_map** テーブルでアクセスできるフィールドについて説明します。

表 6-2　application_host_map のフィールド

フィールド	説明
application_id	アプリケーションの内部識別番号。
application_name	ユーザ インターフェイスに表示されるアプリケーション名。
application_tag_id	このフィールドは廃止されており、null を返します。
business_relevance	ビジネスの生産性へのアプリケーションの関連度のインデックス(1 ～ 5)。1 は非常に低く、5 は非常に高いことを示します。
business_relevance_description	ビジネスとの関連度の説明(very low、low、medium、high、very high)。
host_id	ホストの ID 番号。
risk	アプリケーション リスクのインデックス(1 ～ 5)。1 は非常に低いリスク、5 は重大なリスクを示します。
risk_description	リスクの説明(very low、low、medium、high、critical)。

application_host_map の結合

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

表 6-3　application_host_map 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	app_ids_stats_current_timeframe.application_id application_info.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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 si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id

表 6-3　application_host_map の結合(続き)

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

application_host_map のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出されたアプリケーションに関する情報を返します。

```
SELECT host_id, application_id, application_name, business_relevance, risk
FROM application_host_map
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

application_info

application_info テーブルには、モニタ対象ネットワークのホストで検出可能なアプリケーションに関する情報が含まれています。

アプリケーションに関連付けられているタグのリストを **application_tag_map** テーブルから取得するには **application_id** で結合します。同様に、アプリケーションの関連カテゴリのリストを **application_host_map** から取得するには **application_id** で結合します。

詳細については、次の項を参照してください。

- application_info のフィールド(6-8 ページ)
- application_info の結合(6-9 ページ)
- application_info のサンプル クエリ(6-9 ページ)

application_info のフィールド

次の表に、**application_info** テーブルでアクセスできるフィールドについて説明します。

表 6-4　application_info のフィールド

フィールド	説明
application_description	アプリケーションの説明。
application_id	アプリケーションの内部識別番号。
application_name	ユーザ インターフェイスに表示されるアプリケーション名。
business_relevance	ビジネスの生産性に対するアプリケーションの関連度のインデックス(1 ～ 5)。1 は非常に低く、5 は非常に高いことを示します。
business_relevance_description	ビジネスとの関連度の説明(very low、low、medium、high、very high)。
domain_name	アプリケーションが検出されたドメインの名前。
domain_uuid	アプリケーション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。
is_client_application	検出されたアプリケーションがクライアントであるかどうかを示す true/false フラグ。
is_server_application	検出されたアプリケーションがサーバ アプリケーションであるかどうかを示す true/false フラグ。
is_web_application	検出されたアプリケーションが Web アプリケーションであるかどうかを示す true/false フラグ。
risk	アプリケーションの推定リスクのインデックス(1 ～ 5)。1 は非常に低いリスク、5 は重大なリスクを示します。
risk_description	リスクの説明(very low、low、medium、high、critical)。

application_info の結合

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

表 6-5　application_info 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_host_map.application_id app_ids_stats_current_timeframe.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id si_connection_log.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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

application_info のサンプル クエリ

次のクエリは、Global \ Company B \ Edge ドメイン内で検出された、host_id が 8 のアプリケーションのレコードを返します。

```
SELECT application_id, application_name, application_description, business_relevance,
risk
FROM application_info
WHERE application_id="8" AND domain_name= "Global \ Company B \ Edge";
```

application_tag_map

application_tag_map テーブルには、ネットワークで検出された各アプリケーションに関連付けられているタグ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。

- application_tag_map のフィールド（6-10 ページ）
- application_tag_map の結合（6-11 ページ）
- application_tag_map のサンプル クエリ（6-11 ページ）

application_tag_map のフィールド

次の表に、**application_tag_map** テーブルでアクセスできるフィールドについて説明します。

表 6-6　application_tag_map のフィールド

フィールド	説明
application_id	アプリケーションの内部識別番号。
application_name	ユーザ インターフェイスに表示されるアプリケーション。
domain_name	アプリケーションが検出されたドメインの名前。
domain_uuid	アプリケーション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。
tag_id	タグの内部識別番号。
tag_name	ユーザ インターフェイスに表示されるタグのテキスト。
tag_type	category または type のいずれか。

application_tag_map の結合

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

表 6-7　application_tag_map 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	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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 si_connection_log.application_protocol_name si_connection_log.application_protocol_id si_connection_log.client_application_id si_connection_log.web_application_id
tag_id	tag_info.tag_id

application_tag_map のサンプル クエリ

次のクエリは、指定されたアプリケーションに関連付けられているタグ レコードをすべて返します。

```
SELECT application_id, application_name, tag_id, tag_name

FROM application_tag_map

WHERE application_name="Active Directory";
```

domain_control_information

domain_control_information テーブルは、ドメインをその UUID にマップし、各ドメインの親ドメインの名前と UUID を示します。

詳細については、次の項を参照してください。

- domain_control_information のフィールド (6-12 ページ)
- domain_control_information の結合 (6-12 ページ)
- domain_control_information のサンプル クエリ (6-12 ページ)

domain_control_information のフィールド

次の表に、**domain_control_information** テーブルでアクセスできるフィールドについて説明します。

表 6-8　domain_control_information のフィールド

フィールド	説明
domain_name	ドメインの名前
domain_uuid	ドメインの UUID。これはバイナリで示されます。
parent_domain_name	親ドメインの名前 (該当する場合)。
parent_domain_uuid	親ドメインの UUID (該当する場合)。これはバイナリで示されます。

domain_control_information の結合

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

domain_control_information のサンプル クエリ

次のクエリは、すべてのドメイン名、ASCII 形式のドメイン UUID、およびその親ドメインを返します。

```
SELECT domain_name, uuid_btoa(domain_uuid), parent_domain_name
FROM domain_control_information;
```

network_discovery_event

network_discovery_event テーブルには、検出イベントとホスト入力イベントに関する情報が格納されます。Firepower システム は、(新しいネットワーク機能を検出したか、または以前に識別されたネットワーク資産の変更を検出することで) モニタ対象ネットワークで変更を検出すると、検出イベントを生成します。Firepower システム は、ユーザがネットワーク資産を追加、変更、または削除することでネットワーク マップを手動で変更すると、ホスト入力イベントを生成します。

network_discovery_event 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_events** 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。

- network_discovery_event のフィールド（6-13 ページ）
- network_discovery_event の結合（6-14 ページ）
- network_discovery_event のサンプル クエリ（6-14 ページ）

network_discovery_event のフィールド

次の表に、**network_discovery_event** テーブルでアクセスできるフィールドについて説明します。

表 6-9　network_discovery_event のフィールド

フィールド	説明
confidence	Firepower システム によりサービスを識別するために割り当てられた信頼度（0 ～ 100）。
description	イベントの説明。
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。
event_id	イベントの内部識別番号。
event_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。
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。
event_type	イベントのタイプ。New Host や Identity Conflict など。
ip_address	このフィールドは廃止されており、null を返します。
ipaddr	イベントに関連するホストの IPv4 または IP v 6 アドレスのバイナリ表現。
mac_address	イベントに関連するホストの MAC アドレス。
mac_vendor	イベントに関連するホストの NIC ハードウェアのベンダー。
port	イベントをトリガーしたネットワーク トラフィックが使用していたポート。
sensor_address	検出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	検出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）。
user_dept	ホストの最終ログイン ユーザが所属する部門。
user_email	ホストの最終ログイン ユーザの電子メールアドレス。
user_first_name	ホストの最終ログイン ユーザの名前。
user_id	ホストの最終ログイン ユーザの内部識別番号。
user_last_name	ホストの最終ログイン ユーザの姓。
user_last_seen_sec	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。
user_last_updated_sec	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。
user_name	ホストの最終ログイン ユーザのユーザ名。
user_phone	ホストの最終ログイン ユーザの電話番号。

network_discovery_event の結合

次の表に、**network_discovery_event** 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 6-10　network_discovery_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

network_discovery_event のサンプル クエリ

次のクエリは、特定の期間内の検出イベント レコードを返します。このレコードには、ユーザ、検出デバイス名、タイムスタンプ、ホスト IP アドレスなどが含まれます。

```
SELECT sensor_name, event_time_sec, event_time_usec, event_type, ipaddr, user_id,
hex(mac_address), mac_vendor, port, confidence FROM network_discovery_event
WHERE event_time_sec
BETWEEN UNIX_TIMESTAMP("2013-01-01 00:00:00") AND UNIX_TIMESTAMP("2013-01-01 23:59:59")
ORDER BY event_time_sec DESC, event_time_usec DESC;
```

rna_host

rna_host テーブルには、管理対象ネットワークのホストの基本情報が格納されます。

バージョン 5.2 以降、このテーブルは **rna_ip_host** 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。

- rna_host のフィールド（6-14 ページ）
- rna_host の結合（6-15 ページ）
- rna_host のサンプル クエリ（6-16 ページ）

rna_host のフィールド

次の表に、**rna_host** テーブルでアクセスできるフィールドについて説明します。

表 6-11　rna_host のフィールド

フィールド	説明
criticality	ホストの重要度（None、Low、Medium、または High）。
domain_name	ホストが検出されたドメインの名前。
domain_uuid	ホス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。
hops	ホストから、そのホストを検出した管理対象デバイスまでのネットワーク ホップ数。
host_id	ホストの ID 番号。

表 6-11　rna_host のフィールド(続き)

フィールド	説明
host_name	ホストの名前。
host_type	ホストのタイプ:Host、Router、Bridge、NAT Device、または Load Balancer。
jailbroken	モバイル デバイスのオペレーティング システムがジェイルブレイクされているかどうかを示す true/false フラグ。
last_seen_sec	システムがホスト アクティビティを最後に検出した日時を示す UNIX タイムスタンプ。
mobile	検出されたホストがモバイル デバイスであるかどうかを示す true/false フラグ。
netbios_name	ホストの NetBIOS 名の文字列。
notes	ホストの Notes ホスト属性の内容。
vlan_id	VLAN 識別番号(該当する場合)。
vlan_priority	VLAN タグに含まれるプライオリティ値。
vlan_type	VLAN タグを含むカプセル化パケットのタイプ。 • 0:イーサネット • 1:トークン リング

rna_host の結合

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

表 6-12　rna_host 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
host_id	application_host_map.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host のサンプル クエリ

次のクエリは、Global \ Company B \ Edge ドメイン内の 25 件の **rna_host** レコードを、ホストのタイプに基づいて並べ替えて返します。このレコードには、ホスト ID、VLAN ID、ホストが最後に認識された時点、およびホストのタイプなどが含まれています。

```
SELECT host_id, vlan_id, last_seen_sec, host_type
FROM rna_host
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY host_type
LIMIT 0, 25;
```

rna_host_attribute

rna_host_attribute テーブルには、モニタ対象ネットワーク内の各ホストに関連付けられているホスト属性に関する情報が格納されます。これは、廃止された **rna_ip_host_attribute** テーブルを置き換えるテーブルです。

詳細については、次の項を参照してください。

- rna_host_attribute のフィールド（6-16 ページ）
- rna_host_attribute の結合（6-17 ページ）
- rna_host_attribute のサンプル クエリ（6-17 ページ）

rna_host_attribute のフィールド

次の表に、**rna_host_attribute** テーブルでアクセスできるフィールドについて説明します。

表 6-13　rna_host_attribute のフィールド

フィールド	説明
attribute_name	ホスト属性。Host Criticality や Default White List など。
attribute_value	ホスト属性の値。
host_id	ホストの ID 番号。

rna_host_attribute の結合

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

表 6-14　rna_host_attribute 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
host_id	application_host_map.host_id rna_host.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_attribute のサンプル クエリ

次のクエリは、選択されたホスト ID に関連付けられているすべてのホスト属性と値を返します。

```
SELECT attribute_name, attribute_value

FROM rna_host_attribute

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app

rna_host_client_app テーブルには、モニタ対象ネットワークのホストで検出されたクライアント アプリケーションに関する情報が格納されます。これは、廃止された **rna_ip_host_client_app** テーブルを置き換えるテーブルです。

詳細については、次の項を参照してください。

- rna_host_client_app のフィールド（6-18 ページ）
- rna_host_client_app の結合（6-19 ページ）
- rna_host_client_app のサンプル クエリ（6-20 ページ）

rna_host_client_app のフィールド

次の表に、**rna_ip_host_client_app** テーブルでアクセスできるフィールドについて説明します。

表 6-15　rna_host_client_app のフィールド

フィールド	説明
application	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。
application_protocol_id	検出されたアプリケーション プロトコルの内部 ID。
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)
application_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。
client_application_id	アプリケーションが識別可能な場合、アプリケーションの内部識別番号。
client_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)。 • 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)。
hits	クライアント アプリケーションが検出された回数。
host_id	ホストの ID 番号。
last_used_sec	システムがアプリケーション アクティビティを最後に検出した日時を示す UNIX タイムスタンプ。
version	ホストで検出されたアプリケーションのバージョン。

rna_host_client_app の結合

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

表 6-16　rna_host_client_app 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
host_id および application_protocol_id および client_application_id および version	次のセット： rna_host_client_app_payload.host_id rna_host_client_app_payload.application_protocol_id rna_host_client_app_payload.client_application_id rna_host_client_app_payload.version

表 6-16　rna_host_client_app の結合(続き)

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	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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_service_info.application_protocol_id rna_host_service_payload.web_application_id

rna_host_client_app のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出されたクライアント アプリケーションに関する情報を返します。

```
SELECT host_id, client_application_id, client_application_name, version, hits,
application_protocol_id, application_protocol_name, last_used_sec
FROM rna_host_client_app
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_client_app_payload

rna_host_client_app_payload テーブルには、モニタ対象ネットワークで検出されたホストの Web アプリケーションに関連付けられている HTTP トラフィックのペイロードに関する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。

- rna_host_client_app_payload のフィールド(6-21 ページ)
- rna_host_client_app_payload の結合(6-22 ページ)
- rna_host_client_app_payload のサンプル クエリ(6-23 ページ)

rna_host_client_app_payload のフィールド

次の表に、**rna_host_client_app_payload** テーブルでアクセスできるフィールドについて説明します。

表 6-17　rna_host_client_app_payload のフィールド

フィールド	説明
application	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。
application_protocol_id	検出されたアプリケーション プロトコルの内部 ID（使用可能な場合）。クライアント アプリケーションと Web アプリケーションの両方の特性を持つトラフィックの場合、client_application_id フィールドと web_application_id フィールドの両方に同じ値が入っています。
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）
application_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。
client_application_id	クライアント アプリケーションの内部識別番号。
client_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）。 • 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）。
host_id	ホストの ID 番号。
payload_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。
payload_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。
version	ホストで検出された Web アプリケーションのバージョン。
web_application_id	Web アプリケーションの内部識別番号（使用可能な場合）。クライアント アプリケーションと Web アプリケーションの両方の特性を持つトラフィックの場合、client_application_id フィールドと web_application_id フィールドの両方に同じ値が入っています。
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）。

rna_host_client_app_payload の結合

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

表 6-18　rna_host_client_app_payload 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
次のセット: host_id, application_protocol_id, client_application_id, version	次のセット: rna_host_client_app.host_id rna_host_client_app.application_protocol_id rna_host_client_app.client_application_id rna_host_client_app.version

表 6-18　rna_host_client_app_payload の結合（続き）

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
client_application_id または web_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_id rna_host_service_info.application_protocol_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

rna_host_client_app_payload のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出された Web アプリケーションに関する情報を返します。

```
SELECT host_id, web_application_id, web_application_name, version,
client_application_id, client_application_name
FROM rna_host_client_app_payload
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_ioc_state

rna_host_ioc_state テーブルには、モニタ対象ネットワークのホストの IOC 状態が格納されます。

詳細については、次の項を参照してください。

- rna_host_ioc_state のフィールド（6-24 ページ）
- rna_host_ioc_state の結合（6-26 ページ）
- rna_host_ioc_state のサンプル クエリ（6-26 ページ）

rna_host_ioc_state のフィールド

次の表に、**rna_host_ioc_state** テーブルでアクセスできるフィールドについて説明します。

表 6-19　rna_host_ioc_state のフィールド

フィールド	説明
first_seen	侵害が最初に検出された時点を示す UNIX タイムスタンプ。
first_seen_sensor_address	侵害を最初に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。
first_seen_sensor_name	侵害を最初に検出した管理対象デバイス。
host_id	ホストの ID 番号。
ioc_category	侵害のカテゴリ。有効な値は次のとおりです。 • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
ioc_description	侵害の説明

表 6-19　rna_host_ioc_state のフィールド(続き)

フィールド	説明
ioc_event_type	侵害のイベント タイプ。有効な値は次のとおりです。 • Adobe Reader launched shell • Dropper Infection Detected by AMP for Endpoints • Excel Compromise Detected by AMP for Endpoints • Excel launched shell | • Impact 1 Intrusion Event — attempted-admin • Impact 1 Intrusion Event — attempted-user • Impact 1 Intrusion Event — successful-admin • Impact 1 Intrusion Event — successful-user • Impact 1 Intrusion Event — web-application-attack • Impact 2 Intrusion Event — attempted-admin • Impact 2 Intrusion Event — attempted-user • Impact 2 Intrusion Event — successful-admin • Impact 2 Intrusion Event — successful-user • Impact 2 Intrusion Event — web-application-attack • Intrusion Event — exploit-kit • Intrusion Event — malware-backdoor • Intrusion Event — malware-CnC • Java Compromise Detected by AMP for Endpoints • Java launched shell • PDF Compromise Detected by AMP for Endpoints • PowerPoint Compromise Detected by AMP for Endpoints • PowerPoint launched shell • QuickTime Compromise Detected by AMP for Endpoints • QuickTime launched shell • Security Intelligence Event — CnC • Suspected Botnet Detected by AMP for Endpoints • Threat Detected by AMP for Endpoints — Subtype is 'executed' • Threat Detected by AMP for Endpoints — Subtype is not 'executed' • Threat Detected in File Transfer — Action is not 'block' • Word Compromise Detected by AMP for Endpoints • Word launched shell
ioc_id	侵害の一意の ID 番号。
is_disabled	この侵害が無効にされていたかどうか。
last_seen	この侵害が最後に検出された時点を示す UNIX タイムスタンプ。

表 6-19　rna_host_ioc_state のフィールド(続き)

フィールド	説明
last_seen_sensor_address	侵害を最後に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。
last_seen_sensor_name	侵害を最後に検出した管理対象デバイス。

rna_host_ioc_state の結合

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

表 6-20　rna_host_ioc_state 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_ioc_state のサンプル クエリ

次のクエリは、指定された期間内の最大 25 件のホストとその ioc を返します。

```
SELECT host_id, ioc_id
FROM rna_host_ioc_state
WHERE first_seen
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY ioc_id DESC
LIMIT 0, 25;
```

rna_host_ip_map

rna_host_ip_map テーブルは、モニタ対象ネットワーク内のホストの IP アドレスにホスト ID を相関付けます。

詳細については、次の項を参照してください。

- rna_host_ip_map のフィールド（6-27 ページ）
- rna_host_ip_map の結合（6-27 ページ）
- rna_host_ip_map のサンプル クエリ（6-28 ページ）

rna_host_ip_map のフィールド

次の表に、**rna_host_ip_map** テーブルでアクセスできるフィールドについて説明します。

表 6-21　rna_host_ip_map のフィールド

フィールド	説明
host_id	ホストの ID 番号。
ipaddr	ホストの IP アドレスのバイナリ表現。

rna_host_ip_map の結合

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

表 6-22　rna_host_ip_map 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

表 6-22　rna_host_ip_map の結合(続き)

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	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr user_ipaddr_history.ipaddr white_list_event.ipaddr

rna_host_ip_map のサンプル クエリ

次のクエリは、選択されたホストの MAC 情報を返します。

```
SELECT host_id
FROM rna_host_ip_map
WHERE HEX(ipaddr) = "00000000000000000000FFFF0A0A0A04";
```

rna_host_mac_map

rna_host_mac_map テーブルは、モニタ対象ネットワーク内のホストの MAC アドレスにホスト ID を相関付けます。

詳細については、次の項を参照してください。

- rna_host_mac_map のフィールド(6-29 ページ)
- rna_host_mac_map の結合(6-29 ページ)
- rna_host_mac_map のサンプル クエリ(6-29 ページ)

rna_host_mac_map のフィールド

次の表に、**rna_host_mac_map** テーブルでアクセスできるフィールドについて説明します。

表 6-23　rna_host_mac_map のフィールド

フィールド	説明
host_id	ホストの ID 番号。
mac_address	ホストの MAC アドレス。
mac_vendor	検出されたホストのネットワーク インターフェイスのベンダー。

rna_host_mac_map の結合

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

表 6-24　rna_host_mac_map 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_mac_map のサンプル クエリ

次のクエリは、host_id が 8 のホストの MAC 情報を返します。

```
SELECT HEX(mac_address)
FROM rna_host_mac_map
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_os

rna_host_os テーブルには、モニタ対象ネットワークのホストで検出されたオペレーティング システム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。

- rna_host_os のフィールド(6-30 ページ)
- rna_host_os の結合(6-31 ページ)
- rna_host_os のサンプル クエリ(6-31 ページ)

rna_host_os のフィールド

次の表に、**rna_host_os** テーブルでアクセスできるフィールドについて説明します。

表 6-25　rna_host_os のフィールド

フィールド	説明
confidence	Firepower システム によりオペレーティング システムを識別するために割り当てられた信頼度(0 ～ 100)。
created_sec	システムがホスト アクティビティを最初に検出した日時を示す UNIX タイムスタンプ。
host_id	ホストの ID 番号。
last_seen_sec	システムがホスト アクティビティを最後に検出した日時を示す UNIX タイムスタンプ。
os_uuid	ホストで検出されたオペレーティング システムの固有識別子。UUID は、Firepower システム データベース内のオペレーティング システムの名前、ベンダー、およびバージョンにマップされます。
product	ホストで検出されたオペレーティング システム。
source_type	ホストのオペレーティング システムのアイデンティティ ソース。 • User:Web ユーザ インターフェイスからデータを入力したユーザの名前 • Application:ホスト入力機能を使用して別のアプリケーションからインポートされた • Scanner:Nmap、またはシステム ポリシーによって追加された別のスキャナ • rna:Firepower システム により検出(検出イベント、ポート一致、またはパターン一致のいずれかにより検出)。 • NetFlow:NetFlow 対応デバイスによってデータがエクスポートされた
vendor	ホストで検出されたオペレーティング システムのベンダー。
version	ホストで検出されたオペレーティング システムのバージョン。

rna_host_os の結合

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

表 6-26　rna_host_os 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os のサンプル クエリ

次のクエリは、host_id が 8 のホストのオペレーティング システムに関する情報を返します。

```
SELECT vendor, product, version, source_type, confidence
FROM rna_host_os
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_os_vulns

rna_host_os_vulns テーブルには、モニタ対象ネットワーク内のホストに関連付けられている脆弱性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。

- rna_host_os_vulns のフィールド（6-32 ページ）
- rna_host_os_vulns の結合（6-32 ページ）
- rna_host_os_vulns のサンプル クエリ（6-33 ページ）

rna_host_os_vulns のフィールド

次の表に、**rna_host_os_vulns** テーブルでアクセスできるフィールドについて説明します。

表 6-27　rna_host_os_vulns のフィールド

フィールド	説明
host_id	ホストの ID 番号。
invalid	脆弱性がホストで有効であるかどうかを示す値。 • 0:脆弱性が有効 • 1:脆弱性が無効
rna_vuln_id	脆弱性の内部識別番号。

rna_host_os_vulns の結合

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

表 6-28　rna_host_os_vulns 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
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_os_vulns のサンプル クエリ

次のクエリは、host_id が 8 のホストのオペレーティング システムの脆弱性を返します。

```
SELECT rna_vuln_id, invalid
FROM rna_host_os_vulns
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_protocol

rna_host_protocol テーブルには、モニタ対象ネットワークのホストで検出されたプロトコル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。

- rna_host_protocol のフィールド（6-33 ページ）
- rna_host_protocol の結合（6-34 ページ）
- rna_host_protocol のサンプル クエリ（6-34 ページ）

rna_host_protocol のフィールド

次の表に、**rna_host_protocol** テーブルでアクセスできるフィールドについて説明します。

表 6-29　rna_host_protocol のフィールド

フィールド	説明
host_id	ホストの ID 番号。
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。
layer	プロトコルを実行しているネットワーク層（Network または Transport）。
mac_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。
mac_vendor	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。
protocol_name	ホストが使用するトラフィック プロトコル。
protocol_num	プロトコルの IANA 指定のプロトコル番号。

rna_host_protocol の結合

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

表 6-30　rna_host_protocol 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_protocol のサンプル クエリ

次のクエリは、host_id が 8 のホストのプロトコル レコードをすべて返します。

```
SELECT protocol_num, protocol_name
FROM rna_host_protocol
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_sensor

rna_host_sensor テーブルには、モニタ対象ネットワーク内のホスト IP アドレスが格納され、各アドレスを検出した管理対象デバイスが示されています。

rna_host_sensor テーブルは、Firepower システム バージョン 5.2 以降で廃止されたテーブル **rna_ip_host_sensor** 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。

- rna_host_sensor のフィールド（6-35 ページ）
- rna_host_sensor の結合（6-35 ページ）
- rna_host_sensor のサンプル クエリ（6-35 ページ）

rna_host_sensor のフィールド

次の表に、**rna_host_sensor** テーブルでアクセスできるフィールドについて説明します。

表 6-31　rna_host_sensor のフィールド

フィールド	説明
host_id	ホストの ID 番号。
sensor_address	検出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	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)。

rna_host_sensor の結合

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

表 6-32　rna_host_sensor 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_sensor のサンプル クエリ

次のクエリは、最大 25 件のホストと、それらのホストを検出したセンサーを **rna_host_sensor** テーブルから返します。

```
SELECT host_id, sensor_address, sensor_name

FROM rna_host_sensor

LIMIT 0, 25;
```

rna_host_service

rna_host_service テーブルには、ネットワーク ポートとトラフィック プロトコルの組み合わせによりモニタ対象ネットワークのホストで検出されたサービスに関する一般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。

- rna_host_service のフィールド（6-36 ページ）
- rna_host_service の結合（6-37 ページ）
- rna_host_service のサンプル クエリ（6-37 ページ）

rna_host_service のフィールド

次の表に、**rna_host_service** テーブルでアクセスできるフィールドについて説明します。

表 6-33　rna_host_service のフィールド

フィールド	説明
confidence	Firepower システム によりサーバを識別するために割り当てられた信頼度（0 ～ 100）。
hits	サーバが検出された回数。
host_id	ホストの ID 番号。
last_used_sec	システムが最後にサーバ アクティビティを検出した日時を示す UNIX タイムスタンプ。
port	サーバで使用されるポート。
protocol	トラフィック プロトコル：TCP または UDP。

rna_host_service の結合

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

表 6-34　rna_host_service 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
次のセット: host_id port protocol	次のセット: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 次のセット: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol 次のセット: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service のサンプル クエリ

次のクエリは、host_id が 8 のホストについて検出された、最初の 25 件のサーバ レコードを返します。

```
SELECT hits, protocol, port, confidence

FROM rna_host_service

WHERE HEX(host_id) = "00000000000000000000000000000008"

LIMIT 0, 25;
```

rna_host_service_banner

rna_ip_host_service_banner テーブルには、ネットワーク トラフィックからのヘッダー情報が格納されます。このヘッダー情報は、モニタ対象ネットワークのホストのサーバのベンダーとバージョン(「バナー」)をアドバタイズします。ネットワーク検出ポリシーの [Capture Banners] オプションを有効にしていない場合は、Firepower システム はサーバ バナーを保存しない点に注意してください。

詳細については、次の項を参照してください。

- rna_host_service_banner のフィールド(6-38 ページ)
- rna_host_service_banner の結合(6-38 ページ)
- rna_host_service_banner のサンプル クエリ(6-39 ページ)

rna_host_service_banner のフィールド

次の表に、**rna_host_service_banner** テーブルでアクセスできるフィールドについて説明します。

表 6-35　rna_host_service_banner のフィールド

フィールド	説明
バナー	サーバのバナー(そのサーバについて検出された最初のパケットの最初の 256 バイト)。
host_id	ホストの ID 番号。
port	サーバで使用されるポート。
protocol	トラフィック プロトコル:TCP または UDP。

rna_host_service_banner の結合

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

表 6-36　rna_host_service_banner 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
次のセット: host_id port protocol	次のセット: rna_host_service.host_id rna_host_service.port rna_host_service.protocol 次のセット: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol 次のセット: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

表 6-36　rna_host_service_banner の結合(続き)

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_banner のサンプル クエリ

次のクエリは、host_id が 8 のホストのサーバ バナーを返します。

```
SELECT port, protocol, banner
FROM rna_host_service_banner
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_info

rna_host_service_info テーブルには、モニタ対象ネットワークのホストで検出されたサーバに関する詳細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。

- rna_host_service_info のフィールド(6-40 ページ)
- rna_host_service_info の結合(6-41 ページ)
- rna_host_service_info のサンプル クエリ(6-42 ページ)

rna_host_service_info のフィールド

次の表に、**rna_host_service_info** テーブルでアクセスできるフィールドについて説明します。

表 6-37　rna_host_service_info のフィールド

フィールド	説明
application_id	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空白を返します。
application_protocol_id	検出されたアプリケーション プロトコルの内部 ID(使用可能な場合)。
application_protocol_name	次のいずれか: • アプリケーション プロトコルの名前(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)
business_relevance	ビジネスの生産性に対するアプリケーションの関連度のインデックス(1 ～ 5)。1 は非常に低く、5 は非常に高いことを示します。
business_relevance_ description	ビジネスとの関連度の説明(very low、low、medium、high、very high)。
created_sec	システムが最初にアプリケーション プロトコルを検出した日時を示す UNIX タイムスタンプ。
host_id	ホストの ID 番号。
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。
last_used_sec	システムが最後にサーバ アクティビティを検出した日時を示す UNIX タイムスタンプ。
port	サーバで使用されるポート。
protocol	トラフィック プロトコル:TCP または UDP。
risk	アプリケーション リスクのインデックス(1 ～ 5)。1 は非常に低いリスク、5 は非常に高いリスクを示します。
risk_description	リスクの説明(very low、low、medium、high、very high)。
service_info_id	サーバの内部識別番号。
service_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。
source_type	サーバのアイデンティティ ソース: • User:Web ユーザ インターフェイスからデータを入力したユーザの名前 • Application:ホスト入力機能を使用して別のアプリケーションからインポートされた • Scanner:NMAP により追加されたか、または送信元タイプが Scanner でホスト入力機能からインポートされた • rna:Firepower システム により検出(検出イベント、ポート一致、またはパターン一致のいずれかにより検出)。 • NetFlow:NetFlow 対応デバイスによってデータがエクスポートされた

表 6-37　rna_host_service_info のフィールド(続き)

フィールド	説明
vendor	ホストのサーバのベンダー。
version	ホストで検出されたサーバのバージョン。

rna_host_service_info の結合

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

表 6-38　rna_host_service_info 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	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_application_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

表 6-38　rna_host_service_info の結合(続き)

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id
次のセット: host_id および port および protocol	次のセット: rna_host_service.host_id rna_host_service.port rna_host_service.protocol 次のセット: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 次のセット: rna_host_service_payload.host_id rna_host_service_payload.port rna_host_service_payload.protocol

rna_host_service_info のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出されたアプリケーション プロトコルに関する情報を返します。

```
SELECT host_id, application_protocol_name, version, vendor, created_sec, last_used_sec,
business_relevance, risk

FROM rna_host_service_info

WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_payload

rna_host_service_payload テーブルには、モニタ対象ネットワーク内のホストにより関連付けられている Web アプリケーションに関する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。

- rna_host_service_payload のフィールド(6-43 ページ)
- rna_host_service_payload の結合(6-44 ページ)
- rna_host_service_payload のサンプル クエリ(6-45 ページ)

rna_host_service_payload のフィールド

次の表に、**rna_host_service_payload** テーブルでアクセスできるフィールドについて説明します。

表 6-39　rna_host_service_payload のフィールド

フィールド	説明
application_id	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。
application_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。
host_id	ホストの ID 番号。
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。
payload_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。
payload_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。
port	サーバで使用されるポート。
protocol	トラフィック プロトコル:TCP または UDP。
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。 • Web 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)。

rna_host_service_payload の結合

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

表 6-40　rna_host_service_payload 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
web_application_id	app_ids_stats_current_timeframe.application_id application_info.application_id application_host_map.application_id application_tag_map.application_id app_stats_current_timeframe.application_id connection_log.application_protocol_id connection_log.client_application_id connection_log.web_application_id connection_summary.application_protocol_id si_connection_log.application_protocol_name si_connection_log.client_application_id si_connection_log.web_application_id file_event.application_id intrusion_event.application_protocol_id intrusion_event.client_application_id intrusion_event.web_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
次のセット: host_id port protocol	次のセット: rna_host_service.host_id rna_host_service.port rna_host_service.protocol 次のセット: rna_host_service_banner.host_id rna_host_service_banner.port rna_host_service_banner.protocol 次のセット: rna_host_service_info.host_id rna_host_service_info.port rna_host_service_info.protocol

表 6-40　rna_host_service_payload の結合（続き）

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_vulns.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_payload のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出された Web アプリケーションに関する情報を返します。

```
SELECT host_id, web_application_id, web_application_name, port, protocol
FROM rna_host_service_payload
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_subtype

rna_host_service_subtype テーブルには、モニタ対象ネットワークのホストで検出されたサーバのサブサーバに関する情報が格納されています。

詳細については、次の項を参照してください。

- rna_host_service_subtype のフィールド（6-46 ページ）
- rna_host_service_subtype の結合（6-46 ページ）
- rna_host_service_subtype のサンプル クエリ（6-46 ページ）

rna_host_service_subtype のフィールド

次の表に、**rna_host_service_subtype** テーブルでアクセスできるフィールドについて説明します。

表 6-41　rna_host_service_subtype のフィールド

フィールド	説明
host_id	ホストの ID 番号。
port	サーバで使用されるポート。
protocol	トラフィック プロトコル:TCP または UDP。
service_name	次のいずれかになります。 • トリガー イベントに関連付けられているホストのサーバ。 • none または空白(識別のためのデータが使用できない場合) • pending(追加データが必要な場合) • 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)
source_type	サーバのアイデンティティ ソース: • User:Web ユーザ インターフェイスからデータを入力したユーザの名前 • Application:ホスト入力機能を使用して別のアプリケーションからインポート • Scanner:NMAP により追加されたか、または送信元タイプが Scanner でホスト入力機能からインポート • rna:Firepower システムにより検出(検出イベント、ポート一致、またはパターン一致のいずれかにより検出) • NetFlow:NetFlow 対応デバイスによってエクスポートされたデータ
sub_service_name	ホストで検出されたサブサーバ。
sub_service_vendor	ホストで検出されたサブサーバのベンダー。
sub_service_version	ホストで検出されたサブサーバのバージョン。
vendor	ホストで検出されたサーバのベンダー。
version	ホストで検出されたサーバのバージョン。

rna_host_service_subtype の結合

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

rna_host_service_subtype のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出されたすべてのサブサーバ レコードを返します。

```
SELECT host_id, service_name, version, sub_service_name, sub_service_version,
sub_service_vendor
FROM rna_host_service_subtype
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_service_vulns

rna_host_service_vulns テーブルには、モニタ対象ネットワーク内のホストで検出されたサーバにマップされている脆弱性に関する情報が格納されています。

詳細については、次の項を参照してください。

- rna_host_service_vulns のフィールド（6-47 ページ）
- rna_host_service_vulns の結合（6-48 ページ）
- rna_host_service_vulns のサンプル クエリ（6-48 ページ）

rna_host_service_vulns のフィールド

次の表に、**rna_host_service_vulns** テーブルでアクセスできるフィールドについて説明します。

表 6-42　rna_host_service_vulns のフィールド

フィールド	説明
application_id	ホストで実行されているアプリケーション プロトコルの内部識別番号。
application_name	ユーザ インターフェイスに表示されるアプリケーション プロトコル名。
host_id	ホストの ID 番号。
invalid	アプリケーション プロトコルを実行しているホストで脆弱性が有効であるかどうかを示す値。 • 0:脆弱性が有効 • 1:脆弱性が無効
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	サーバで使用されるポート。
protocol	トラフィック プロトコル:TCP または UDP。
rna_vuln_id	脆弱性の内部識別番号。
service_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。
vendor	ホストで検出されたサーバのベンダー。
version	ホストで検出されたサーバのバージョン。

rna_host_service_vulns の結合

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

表 6-43　rna_host_service_vulns 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
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_payload.host_id rna_host_third_party_vuln_bugtraq_id.host_id rna_host_third_party_vuln_cve_id.host_id rna_host_third_party_vuln_rna_id.host_id rna_host_third_party_vuln.host_id

rna_host_service_vulns のサンプル クエリ

次のクエリは、host_id が 8 のホストで検出されたすべてのサーバ脆弱性に関する情報を返します。

```
SELECT host_id, rna_vuln_id, vendor, service_name, version, invalid FROM
rna_host_service_vulns
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln

rna_host_third_party_vuln テーブルには、モニタ対象ネットワーク内のホストに関連付けられているサードパーティの脆弱性に関する情報が含まれています。このテーブルの情報は、ホスト入力機能によってインポートされるサードパーティの脆弱性データによって決定されることに注意してください。

詳細については、次の項を参照してください。

- rna_host_third_party_vuln のフィールド（6-49 ページ）
- rna_host_third_party_vuln の結合（6-50 ページ）
- rna_host_third_party_vuln のサンプル クエリ（6-50 ページ）

rna_host_third_party_vuln のフィールド

次の表に、**rna_host_third_party_vuln** テーブルでアクセスできるフィールドについて説明します。

表 6-44　rna_host_third_party_vuln のフィールド

フィールド	説明
description	脆弱性に関する説明。
host_id	ホストの ID 番号。
invalid	脆弱性がホストで有効であるかどうかを示す値。 • 0:脆弱性が有効 • 1:脆弱性が無効
name	脆弱性のタイトル。
port	ポート番号（脆弱性が、特定のポートで検出された関連アプリケーションまたはサーバに関連付けられている場合）。
protocol	トラフィック プロトコル（TCP または UDP）（そのプロトコルを使用するアプリケーションに脆弱性が関連付けられている場合）。
source	脆弱性のソース。
third_party_vuln_id	脆弱性に関連付けられた識別番号。

rna_host_third_party_vuln の結合

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

表 6-45　rna_host_third_party_vuln 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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln のサンプル クエリ

次のクエリは、host_id が 8 のホストのサードパーティの脆弱性に関する情報を返します。

```
SELECT host_id, third_party_vuln_id, name, description, source, invalid
FROM rna_host_third_party_vuln
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_bugtraq_id

rna_host_third_party_vuln_bugtraq_id テーブルには、Bugtraq データベースの脆弱性にマップされ、モニタ対象ネットワーク内のホストに関連付けられているサードパーティの脆弱性に関する情報が格納されます。このテーブルのサードパーティ脆弱性データは、ホスト入力機能によってインポートされることに注意してください。

詳細については、次の項を参照してください。

- rna_host_third_party_vuln_bugtraq_id のフィールド（6-51 ページ）
- rna_host_third_party_vuln_bugtraq_id の結合（6-51 ページ）
- rna_host_third_party_vuln_bugtraq_id のサンプル クエリ（6-52 ページ）

rna_host_third_party_vuln_bugtraq_id のフィールド

次の表に、**rna_host_third_party_vuln_bugtraq_id** テーブルでアクセスできるフィールドについて説明します。

表 6-46　rna_host_third_party_vuln_bugtraq_id のフィールド

フィールド	説明
bugtraq_id	脆弱性に関連付けられている Bugtraq データベースの識別番号。
description	脆弱性に関する説明。
host_id	ホストの ID 番号。
invalid	脆弱性がホストで有効であるかどうかを示す値。 • 0:脆弱性が有効 • 1:脆弱性が無効
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。
name	脆弱性の名前またはタイトル。
port	ポート番号(脆弱性が、特定のポートで検出された関連アプリケーションまたはサーバに関連付けられている場合)。
protocol	トラフィック プロトコル(TCP または UDP)(そのプロトコルを使用するアプリケーションに脆弱性が関連付けられている場合)。
source	脆弱性のソース。
third_party_vuln_id	脆弱性に関連付けられているサードパーティの識別番号。

rna_host_third_party_vuln_bugtraq_id の結合

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

表 6-47　rna_host_third_party_vuln_bugtraq_id 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
bugtraq_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id

表 6-47　rna_host_third_party_vuln_bugtraq_id の結合(続き)

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_bugtraq_id のサンプル クエリ

次のクエリは、host_id が 8 のホストの BugTraq 脆弱性を返します。

```
SELECT host_id, third_party_vuln_id, bugtraq_id, name, description, source, invalid
FROM rna_host_third_party_vuln_bugtraq_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_cve_id

rna_host_third_party_vuln_cve_id テーブルには、MITRE の CVE データベースの脆弱性にマップされ、モニタ対象ネットワーク内のホストに関連付けられているサードパーティの脆弱性に関する情報が格納されます。このテーブルには、ホスト入力機能によってインポートされるサードパーティの脆弱性データが格納されていることに注意してください。

詳細については、次の項を参照してください。

- rna_host_third_party_vuln_cve_id のフィールド(6-53 ページ)
- rna_host_third_party_vuln_cve_id の結合(6-53 ページ)
- rna_host_third_party_vuln_cve_id のサンプル クエリ(6-54 ページ)

rna_host_third_party_vuln_cve_id のフィールド

次の表に、**rna_host_third_party_vuln_cve_id** テーブルでアクセスできるフィールドについて説明します。

表 6-48　rna_host_third_party_vuln_cve_id のフィールド

フィールド	説明
cve_id	MITRE の CVE データベースにおいて脆弱性に関連付けられている識別番号。
description	脆弱性に関する説明。
host_id	ホストの ID 番号。
invalid	脆弱性がホストで有効であるかどうかを示す値。 • 0:脆弱性が有効 • 1:脆弱性が無効
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。
name	脆弱性の名前またはタイトル。
port	ポート番号(脆弱性が、特定のポートで検出された関連アプリケーションまたはサーバに関連付けられている場合)。
protocol	トラフィック プロトコル(TCP または UDP)(そのプロトコルを使用するアプリケーションに脆弱性が関連付けられている場合)。
source	脆弱性のソース。
third_party_vuln_id	脆弱性に関連付けられた識別番号。

rna_host_third_party_vuln_cve_id の結合

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

表 6-49　rna_host_third_party_vuln_cve_id 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
cve_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id

表 6-49　rna_host_third_party_vuln_cve_id の結合(続き)

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_cve_id のサンプル クエリ

次のクエリは、host_id が 8 のホストの CVE 脆弱性を返します。

```
SELECT host_id, third_party_vuln_id, cve_id, name, description, source, invalid
FROM rna_host_third_party_vuln_cve_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_host_third_party_vuln_rna_id

rna_host_third_party_vuln_bugtraq_id テーブルには、Firepower システム脆弱性データベース(VDB)の脆弱性にマップされ、モニタ対象ネットワーク内のホストに関連付けられているサードパーティの脆弱性に関する情報が格納されています。このテーブルのサードパーティ脆弱性データは、ホスト入力機能によってインポートされることに注意してください。

詳細については、次の項を参照してください。

- rna_host_third_party_vuln_rna_id のフィールド(6-55 ページ)
- rna_host_third_party_vuln_rna_id の結合(6-55 ページ)
- rna_host_third_party_vuln_rna_id のサンプル クエリ(6-56 ページ)

rna_host_third_party_vuln_rna_id のフィールド

次の表に、**rna_host_third_party_vuln_rna_id** テーブルでアクセスできるフィールドについて説明します。

表 6-50　rna_host_third_party_vuln_rna_id のフィールド

フィールド	説明
description	脆弱性に関する説明。
host_id	ホストの ID 番号。
invalid	脆弱性がホストで有効であるかどうかを示す値。 • 0:脆弱性が有効 • 1:脆弱性が無効
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。
name	脆弱性の名前またはタイトル。
port	ポート番号(脆弱性が、特定のポートで検出された関連アプリケーションまたはサーバに関連付けられている場合)。
protocol	トラフィック プロトコル(TCP または UDP)(そのプロトコルを使用するアプリケーションに脆弱性が関連付けられている場合)。
rna_vuln_id	脆弱性を追跡するために シスコ が使用する脆弱性の識別番号。
source	脆弱性のソース。
third_party_vuln_id	脆弱性に関連付けられた識別番号。

rna_host_third_party_vuln_rna_id の結合

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

表 6-51　rna_host_third_party_vuln_rna_id 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
rna_vuln_id	rna_vuln.bugtraq_id rna_vuln.rna_vuln_id rna_host_os.rna_vuln_id rna_host_service_vulns.rna_vuln_id

表 6-51　rna_host_third_party_vuln_rna_id の結合(続き)

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
host_id	rna_host.host_id rna_host_attribute.host_id rna_host_protocol.host_id rna_host_os_vulns.host_id application_host_map.host_id rna_host_client_app.host_id rna_host_client_app_payload.host_id rna_host_ioc_state.host_id rna_host_ip_map.host_id rna_host_mac_map.host_id rna_host_os.host_id rna_host_sensor.host_id rna_host_service.host_id rna_host_service_banner.host_id rna_host_service_info.host_id rna_host_service_payload.host_id rna_host_service_vulns.host_id

rna_host_third_party_vuln_rna_id のサンプル クエリ

次のクエリは、host_id が 8 のホストのすべてのサードパーティ脆弱性と VDB ID を返します。

```
SELECT host_id, third_party_vuln_id, rna_vuln_id, name, description, source, invalid
FROM rna_host_third_party_vuln_rna_id
WHERE HEX(host_id) = "00000000000000000000000000000008";
```

rna_vuln

rna_vuln テーブルには、シスコ VDB の脆弱性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。

- rna_vuln のフィールド(6-57 ページ)
- rna_vuln の結合(6-58 ページ)
- rna_vuln のサンプル クエリ(6-59 ページ)

rna_vuln のフィールド

次の表に、**rna_vuln** テーブルでアクセスできるフィールドについて説明します。

表 6-52　rna_vuln のフィールド

フィールド	説明
authentication	この脆弱性のエクスプロイトに認証が必要であるかどうか • 必須 • Not Required • 不明
availability	脆弱性のエクスプロイトが可能な状況： • Always • User Initiated • Time Dependent • 不明
available_exploits	脆弱性に対して既知のエクスプロイトがあるかどうか • TRUE • FALSE
bugtraq_id	Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。
class	脆弱性のクラス： • Configuration Error • Boundary Condition Error • Design Error
credibility	脆弱性の信頼度： • Conflicting Reports • Conflicting Details • Single Source • Reliable Source • Multiple Sources • Vendor Confirmed
credit	脆弱性を報告したユーザまたは組織
ease	脆弱性のエクスプロイトの容易さ。 • No Exploit Required • Exploit Available • No Exploit Available
effect	脆弱性がエクスプロイトされた場合に発生する可能性のある影響の詳細。
entry_date	脆弱性がデータベースに登録された日付。
exploit	脆弱性のエクスプロイトを確認できる情報。

表 6-52　rna_vuln のフィールド(続き)

フィールド	説明
impact	脆弱性の影響。これは侵入データ、検出イベント、および脆弱性アセスメントの間の相関に基づいて決定した影響レベルに対応しています。指定できる値は 1 ～ 10 です。10 が最も高い重大度です。脆弱性の影響度の値は、Bugtraq エントリの作成者が決定します。
ローカル	脆弱性がローカルでエクスプロイトされる必要があるかどうかを示します。 • TRUE • FALSE
long_description	脆弱性についての一般的な説明。
mitigation	脆弱性を緩和する方法を説明します。
modified_date	脆弱性の最終変更日(該当する場合)。
publish_date	脆弱性が公開された日付。
remote	脆弱性がネットワーク上でエクスプロイト可能であるかどうかを示します。 • TRUE • FALSE
rna_vuln_id	脆弱性を追跡するためにシステムで使用する シスコ の脆弱性 ID 番号。
scenario	攻撃者が脆弱性をエクスプロイトするシナリオの説明。
short_description	脆弱性の概要。
snort_id	Snort ID(SID)データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できると、その脆弱性は、侵入ルールの SID に関連付けられます。
solution	脆弱性に対する解決策。
technical_description	脆弱性に関する技術的な説明。
title	脆弱性のタイトル。

rna_vuln の結合

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

表 6-53　rna_vuln 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
rna_vuln_id または bugtraq_id	rna_host_os_vulns.rna_vuln_id rna_host_service_vulns.rna_vuln_id rna_host_third_party_vuln_rna_id.rna_vuln_id rna_host_third_party_vuln_cve_id.cve_id rna_host_third_party_vuln_bugtraq_id.bugtraq_id

rna_vuln のサンプル クエリ

次のクエリは、最大 25 件の脆弱性に関する情報を返します。これらのレコードは、当該脆弱性に基づいて生成されたイベントの数の順にソートされます。

```
SELECT rna_vuln_id, bugtraq_id, snort_id, title, publish_date, impact, remote, exploit,
long_description, technical_description, solution, count(*) as count
FROM rna_vuln
GROUP BY rna_vuln_id
ORDER BY rna_vuln_id DESC LIMIT 0, 25;
```

tag_info

tag_info テーブルには、ネットワークで検出されたアプリケーションに関連付けられているタグに関する情報が含まれています。アプリケーションには複数のタグが関連付けられていることがある点に注意してください。

詳細については、次の項を参照してください。

- tag_info のフィールド（6-59 ページ）
- tag_info の結合（6-60 ページ）
- tag_info のサンプル クエリ（6-60 ページ）

tag_info のフィールド

次の表に、**tag_info** テーブルでアクセスできるフィールドについて説明します。

表 6-54　tag_info のフィールド

フィールド	説明
domain_name	アプリケーションが検出されたドメインの名前。
domain_uuid	アプリケーション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。
tag_description	タグの説明。
tag_id	タグの内部 ID。
tag_name	ユーザ インターフェイスに表示されるタグのテキスト。
tag_type	次のいずれかが必要です。 • category • tag

tag_info の結合

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

表 6-55　tag_info 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
tag_id	application_tag_map.tag_id

tag_info のサンプル クエリ

次のクエリは、Global \ Company B \ Edge ドメイン内で選択されているタグ ID のアプリケーション タグ レコードを返します。

```
SELECT tag_id, tag_name, tag_type, tag_description

FROM tag_info

WHERE tag_id="100" AND domain_name= "Global \ Company B \ Edge";
```

url_categories

url_categories テーブルには、モニタ対象ネットワークのホストから要求される URL を特徴付けるカテゴリがリストされます。

詳細については、次の項を参照してください。

- url_categories のフィールド（6-60 ページ）
- url_categories の結合（6-60 ページ）
- url_categories のサンプル クエリ（6-61 ページ）

url_categories のフィールド

次の表では、**url_categories** テーブルのフィールドについて説明します。

表 6-56　url_categories のフィールド

フィールド	説明
category_description	URL カテゴリの説明。
category_id	URL カテゴリの内部識別番号。

url_categories の結合

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

url_categories のサンプル クエリ

次のクエリは、選択したカテゴリ ID のカテゴリ レコードを返します。

```
SELECT category_id, category_description
FROM url_categories
WHERE category_id="1";
```

url_reputations

url_reputations テーブルには、モニタ対象要求でホストから要求される URL を特徴付けるレピュテーションがリストされます。

詳細については、次の項を参照してください。

- url_reputations のフィールド（6-61 ページ）
- url_reputations の結合（6-61 ページ）
- url_reputations のサンプル クエリ（6-61 ページ）

url_reputations のフィールド

次の表では、**url_reputations** テーブルのフィールドについて説明します。

表 6-57　url_reputations のフィールド

フィールド	説明
reputation_description	レピュテーションの説明。
reputation_id	URL のレピュテーションの内部識別番号。

url_reputations の結合

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

url_reputations のサンプル クエリ

次のクエリは、特定のレピュテーション ID の URL レピュテーション情報を返します。

```
SELECT reputation_id, reputation_description
FROM url_reputations
WHERE reputation_id="1";
```

user_ipaddr_history

user_ipaddr_history テーブルには、モニタ対象ネットワーク内の特定のホストに対するユーザ アクティビティに関する情報が含まれます。

詳細については、次の項を参照してください。

- user_ipaddr_history のフィールド(6-62 ページ)
- user_ipaddr_history の結合(6-63 ページ)
- user_ipaddr_history のサンプル クエリ(6-64 ページ)

user_ipaddr_history のフィールド

次の表に、**user_ipaddr_history** テーブルでアクセスできるフィールドについて説明します。

表 6-58　user_ipaddr_history のフィールド

フィールド	説明
authentication_type	ユーザが使用する認証のタイプ。値は次のとおりです。 • 0:認証は不要 • 1:パッシブ認証、AD エージェント、または ISE セッション • 2:キャプティブ ポータルの正常な認証 • 3:キャプティブ ポータルのゲスト認証 • 4:キャプティブ ポータルの失敗認証
domain_name	ユーザが検出されたドメインの名前。
domain_uuid	ユーザ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。
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。
end_time_sec	ホストに異なるユーザがログインしていることを Firepower システム が検出した日時を示す UNIX タイムスタンプ。これにより、以前のユーザのセッションの推定される終了がマークされます。Firepower システム ではログオフが検出されないことに注意してください。
id	ユーザ履歴レコードの内部識別番号。
ipaddr	ホストの IP アドレスのバイナリ表現。
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。
start_time_sec	ユーザがホストにログインしたことを Firepower システム が検出した日時を示す UNIX タイムスタンプ。
security_group	ネットワーク トラフィック グループの ID 番号。
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。
user_id	ユーザの内部識別番号。
user_last_name	ユーザの姓。

表 6-58　user_ipaddr_history のフィールド(続き)

フィールド	説明
user_last_seen_sec	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。
user_last_updated_sec	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。
user_name	ユーザのユーザ名。
user_phone	ユーザの電話番号です。
user_rna_service	ユーザの検出時に使用されていたアプリケーション プロトコルの名前(使用可能な場合)。

user_ipaddr_history の結合

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

表 6-59　user_ipaddr_history 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	compliance_event.dst_ipaddr compliance_event.src_ipaddr connection_log.initiator_ipaddr connection_log.responder_ipaddr connection_summary.initiator_ipaddr connection_summary.responder_ipaddr fireamp_event.dst_ipaddr fireamp_event.src_ipaddr intrusion_event.dst_ipaddr intrusion_event.src_ipaddr network_discovery_event.ipaddr rna_host_ip_map.ipaddr si_connection_log.initiator_ipaddr si_connection_log.responder_ipaddr user_discovery_event.ipaddr white_list_event.ipaddr
user_id	discovered_users.user_id user_discovery_event.user_id rna_host_ioc_state.host_id

user_ipaddr_history のサンプル クエリ

次のクエリは、指定された開始タイムスタンプ以降の、選択された IP アドレスのユーザ アクティビティ レコードをすべて返します。

```
SELECT ipaddr, start_time_sec, end_time_sec, user_name, user_rna_service,
user_last_seen_sec, user_last_updated_sec

FROM user_ipaddr_history

WHERE HEX(ipaddr) = "00000000000000000000FFFF0A0A0A04" AND start_time_sec >=
UNIX_TIMESTAMP("2011-10-01 00:00:00");
```