



## **Firepower System データベース アクセス ガイド**

バージョン 6.3

2019 年 4 月 10 日

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

### **Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

シスコは世界各国 200 箇所にオフィスを開設しています。

所在地、電話番号、FAX 番号

は以下のシスコ Web サイトをご覧ください。

([www.cisco.com/go/offices](http://www.cisco.com/go/offices)) をご覧ください。

**【注意】 シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。**

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合があります  
りますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2016 年 Cisco Systems, Inc. All rights reserved.



---

**CHAPTER 1****概要 1-11**

|                               |      |
|-------------------------------|------|
| バージョン 6.3 でのデータベース アクセスの重要な変更 | 1-11 |
| バージョン 6.3 の新規テーブルおよび変更されたテーブル | 1-11 |
| 前提条件                          | 1-12 |
| ライセンス                         | 1-12 |
| Firepower システム 機能と用語          | 1-12 |
| 通信ポート                         | 1-12 |
| クライアントシステム                    | 1-12 |
| クエリ アプリケーション                  | 1-13 |
| データベース クエリ                    | 1-13 |
| 最初に行う作業                       | 1-14 |

---

**CHAPTER 2****データベース アクセスのセットアップ 2-1**

|   |      |
|---|------|
| データベース ユーザ アカウントの作成                           | 2-1  |
| Firepower Management Center でのデータベース アクセスの有効化 | 2-2  |
| JDBC ドライバのダウンロード                              | 2-3  |
| クライアント SSL 証明書のインストール                         | 2-4  |
| サードパーティ アプリケーションを使用したデータベースへの接続               | 2-5  |
| カスタム プログラムを使用したデータベースへの接続                     | 2-7  |
| カスタム Java プログラムのサンプル コード                      | 2-7  |
| アプリケーションの実行                                   | 2-8  |
| データベースの照会                                     | 2-9  |
| サポートされている SHOW ステートメント構文                      | 2-10 |
| サポートされている DESCRIBE または DESC ステートメント構文         | 2-10 |
| サポートされている SELECT ステートメント構文                    | 2-11 |
| 結合の制約   | 2-12 |
| 使い慣れていない形式で保存されているデータの照会                      | 2-13 |
| パフォーマンス上の理由によるクエリの制限                          | 2-14 |
| クエリのヒント                                       | 2-15 |
| クエリのトラブルシューティング                               | 2-15 |
| サンプル クエリ                                      | 2-16 |

## CHAPTER 3

## スキーマ: システムレベルテーブル 3-1

|                        |      |
|------------------------|------|
| audit_log              | 3-1  |
| audit_log のフィールド       | 3-1  |
| audit_log の結合          | 3-2  |
| audit_log のサンプルクエリ     | 3-2  |
| fireamp_event          | 3-2  |
| fireamp_event のフィールド   | 3-3  |
| fireamp_event の結合      | 3-8  |
| fireamp_event のサンプルクエリ | 3-8  |
| health_event           | 3-9  |
| health_event のフィールド    | 3-9  |
| health_event の結合       | 3-10 |
| health_event のサンプルクエリ  | 3-10 |

## CHAPTER 4

## スキーマ: 侵入テーブル 4-1

|                                 |     |
|---------------------------------|-----|
| intrusion_event                 | 4-1 |
| intrusion_event のフィールド          | 4-2 |
| intrusion_event の結合             | 4-7 |
| intrusion_event のサンプルクエリ        | 4-7 |
| intrusion_event_packet          | 4-7 |
| intrusion_event_packet のフィールド   | 4-8 |
| intrusion_event_packet の結合      | 4-8 |
| intrusion_event_packet のサンプルクエリ | 4-8 |
| rule_message                    | 4-9 |
| rule_message のフィールド             | 4-9 |
| rule_message の結合                | 4-9 |
| rule_message のサンプルクエリ           | 4-9 |

## CHAPTER 5

## スキーマ: 統計情報追跡テーブル 5-1

|  |     |
|--|-----|
| 統計情報追跡テーブルについて                           | 5-2 |
| 統計情報追跡テーブルの保存特性                          | 5-3 |
| 統計情報テーブルの照会時の時間間隔の指定                     | 5-3 |
| app_ids_stats_current_timeframe          | 5-4 |
| app_ids_stats_current_timeframe のフィールド   | 5-5 |
| app_ids_stats_current_timeframe の結合      | 5-6 |
| app_ids_stats_current_timeframe のサンプルクエリ | 5-6 |
| app_stats_current_timeframe              | 5-6 |
| app_stats_current_timeframe のフィールド       | 5-7 |
| app_stats_current_timeframe の結合          | 5-8 |

|   |      |
|---|------|
| app_stats_current_timeframe のサンプルクエリ                  | 5-8  |
| compliance_events_stats_current_timeframe             | 5-8  |
| compliance_events_stats_current_timeframe のフィールド      | 5-9  |
| compliance_event_stats_current_timeframe の結合          | 5-9  |
| compliance_event_stats_current_timeframe のサンプルクエリ     | 5-9  |
| dns_query_stats_current_timeframe                     | 5-9  |
| dns_query_stats_current_timeframe のフィールド              | 5-10 |
| dns_query_stats_current_timeframe の結合                 | 5-10 |
| dns_query_stats_current_timeframe のサンプルクエリ            | 5-10 |
| geolocation_stats_current_timeframe                   | 5-11 |
| geolocation_stats_current_timeframe のフィールド            | 5-11 |
| geolocation_stats_current_timeframe の結合               | 5-12 |
| geolocation_stats_current_timeframe のサンプルクエリ          | 5-13 |
| ids_impact_stats_current_timeframe                    | 5-13 |
| ids_impact_stats_current_timeframe のフィールド             | 5-13 |
| ids_impact_stats_current_timeframe の結合                | 5-14 |
| ids_impact_stats_current_timeframe のサンプルクエリ           | 5-14 |
| interface_stats_current_timeframe                     | 5-14 |
| interface_stats_current_timeframe フィールド               | 5-15 |
| interface_stats_current_timeframe 結合                  | 5-15 |
| interface_stats_current_timeframe サンプルクエリ             | 5-15 |
| ip_reputation_stats_current_timeframe                 | 5-16 |
| ip_reputation_stats_current_timeframe のフィールド          | 5-16 |
| ip_reputation_stats_current_timeframe の結合             | 5-17 |
| ip_reputation_stats_current_timeframe のサンプルクエリ        | 5-17 |
| qos_rule_stats_current_timeframe                      | 5-17 |
| qos_rule_stats_current_timeframe フィールド                | 5-17 |
| qos_rule_stats_current_timeframe 結合                   | 5-18 |
| qos_rule_stats_current_timeframe サンプルクエリ              | 5-18 |
| session_stats_current_timeframe                       | 5-18 |
| session_stats_current_timeframe のフィールド                | 5-19 |
| session_stats_current_timeframe の結合                   | 5-19 |
| session_stats_current_timeframe のサンプルクエリ              | 5-19 |
| ssl_stats_current_timeframe                           | 5-20 |
| ssl_stats_current_timeframe のフィールド                    | 5-20 |
| ssl_stats_current_timeframe の結合                       | 5-22 |
| ssl_stats_current_timeframe のサンプルクエリ                  | 5-22 |
| storage_stats_by_disposition_current_timeframe        | 5-22 |
| storage_stats_by_disposition_current_timeframe のフィールド | 5-23 |

|  |      |      |
|--|------|------|
| storage_stats_by_disposition_current_timeframe の結合         | 5-23 |      |
| storage_stats_by_disposition_current_timeframe のサンプルクエリ    |      | 5-24 |
| storage_stats_by_file_type_current_timeframe               | 5-24 |      |
| storage_stats_by_file_type_current_timeframe のフィールド        | 5-24 |      |
| storage_stats_by_file_type_current_timeframe の結合           | 5-25 |      |
| storage_stats_by_file_type_current_timeframe のサンプルクエリ      |      | 5-25 |
| transmission_stats_by_file_type_current_timeframe          | 5-25 |      |
| transmission_stats_by_file_type_current_timeframe のフィールド   | 5-26 |      |
| transmission_stats_by_file_type_current_timeframe の結合      | 5-26 |      |
| transmission_stats_by_file_type_current_timeframe のサンプルクエリ |      | 5-26 |
| url_category_stats_current_timeframe                       | 5-27 |      |
| url_category_stats_current_timeframe のフィールド                | 5-27 |      |
| url_category_stats_current_timeframe の結合                   | 5-28 |      |
| url_category_stats_current_timeframe のサンプルクエリ              |      | 5-28 |
| url_reputation_stats_current_timeframe                     | 5-28 |      |
| url_reputation_stats_current_timeframe のフィールド              | 5-28 |      |
| url_reputation_stats_current_timeframe の結合                 | 5-29 |      |
| url_reputation_stats_current_timeframe のサンプルクエリ            |      | 5-29 |
| user_ids_stats_current_timeframe                           | 5-30 |      |
| user_ids_stats_current_timeframe のフィールド                    | 5-30 |      |
| user_ids_stats_current_timeframe の結合                       | 5-31 |      |
| user_ids_stats_current_timeframe のサンプルクエリ                  |      | 5-31 |
| user_stats_current_timeframe                               | 5-31 |      |
| user_stats_current_timeframe のフィールド                        | 5-32 |      |
| user_stats_current_timeframe の結合                           | 5-32 |      |
| user_stats_current_timeframe のサンプルクエリ                      |      | 5-32 |

## CHAPTER 6

## 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 6-1

|                               |      |     |
|-------------------------------|------|-----|
| application_host_map          | 6-5  |     |
| application_host_map のフィールド   | 6-6  |     |
| application_host_map の結合      | 6-6  |     |
| application_host_map のサンプルクエリ |      | 6-7 |
| application_info              | 6-7  |     |
| application_info のフィールド       | 6-8  |     |
| application_info の結合          | 6-9  |     |
| application_info のサンプルクエリ     |      | 6-9 |
| application_tag_map           | 6-10 |     |
| application_tag_map のフィールド    | 6-10 |     |
| application_tag_map の結合       | 6-11 |     |

|                                      |      |
|--------------------------------------|------|
| application_tag_map のサンプルクエリ         | 6-11 |
| domain_control_information           | 6-12 |
| domain_control_information のフィールド    | 6-12 |
| domain_control_information の結合       | 6-12 |
| domain_control_information のサンプルクエリ  | 6-12 |
| network_discovery_event              | 6-12 |
| network_discovery_event のフィールド       | 6-13 |
| network_discovery_event の結合          | 6-14 |
| network_discovery_event のサンプルクエリ     | 6-14 |
| rna_host                             | 6-14 |
| rna_host のフィールド                      | 6-14 |
| rna_host の結合                         | 6-15 |
| rna_host のサンプルクエリ                    | 6-16 |
| rna_host_attribute                   | 6-16 |
| rna_host_attribute のフィールド            | 6-16 |
| rna_host_attribute の結合               | 6-17 |
| rna_host_attribute のサンプルクエリ          | 6-17 |
| rna_host_client_app                  | 6-17 |
| rna_host_client_app のフィールド           | 6-18 |
| rna_host_client_app の結合              | 6-19 |
| rna_host_client_app のサンプルクエリ         | 6-20 |
| rna_host_client_app_payload          | 6-20 |
| rna_host_client_app_payload のフィールド   | 6-21 |
| rna_host_client_app_payload の結合      | 6-22 |
| rna_host_client_app_payload のサンプルクエリ | 6-23 |
| rna_host_ioc_state                   | 6-23 |
| rna_host_ioc_state のフィールド            | 6-24 |
| rna_host_ioc_state の結合               | 6-26 |
| rna_host_ioc_state のサンプルクエリ          | 6-26 |
| rna_host_ip_map                      | 6-27 |
| rna_host_ip_map のフィールド               | 6-27 |
| rna_host_ip_map の結合                  | 6-27 |
| rna_host_ip_map のサンプルクエリ             | 6-28 |
| rna_host_mac_map                     | 6-28 |
| rna_host_mac_map のフィールド              | 6-29 |
| rna_host_mac_map の結合                 | 6-29 |
| rna_host_mac_map のサンプルクエリ            | 6-29 |
| rna_host_os                          | 6-30 |
| rna_host_os のフィールド                   | 6-30 |

|                                   |      |
|-----------------------------------|------|
| rna_host_os の結合                   | 6-31 |
| rna_host_os のサンプルクエリ              | 6-31 |
| rna_host_os_vulns                 | 6-31 |
| rna_host_os_vulns のフィールド          | 6-32 |
| rna_host_os_vulns の結合             | 6-32 |
| rna_host_os_vulns のサンプルクエリ        | 6-33 |
| rna_host_protocol                 | 6-33 |
| rna_host_protocol のフィールド          | 6-33 |
| rna_host_protocol の結合             | 6-34 |
| rna_host_protocol のサンプルクエリ        | 6-34 |
| rna_host_sensor                   | 6-34 |
| rna_host_sensor のフィールド            | 6-35 |
| rna_host_sensor の結合               | 6-35 |
| rna_host_sensor のサンプルクエリ          | 6-35 |
| rna_host_service                  | 6-36 |
| rna_host_service のフィールド           | 6-36 |
| rna_host_service の結合              | 6-37 |
| rna_host_service のサンプルクエリ         | 6-37 |
| rna_host_service_banner           | 6-38 |
| rna_host_service_banner のフィールド    | 6-38 |
| rna_host_service_banner の結合       | 6-38 |
| rna_host_service_banner のサンプルクエリ  | 6-39 |
| rna_host_service_info             | 6-39 |
| rna_host_service_info のフィールド      | 6-40 |
| rna_host_service_info の結合         | 6-41 |
| rna_host_service_info のサンプルクエリ    | 6-42 |
| rna_host_service_payload          | 6-43 |
| rna_host_service_payload のフィールド   | 6-43 |
| rna_host_service_payload の結合      | 6-44 |
| rna_host_service_payload のサンプルクエリ | 6-45 |
| rna_host_service_subtype          | 6-45 |
| rna_host_service_subtype のフィールド   | 6-46 |
| rna_host_service_subtype の結合      | 6-46 |
| rna_host_service_subtype のサンプルクエリ | 6-46 |
| rna_host_service_vulns            | 6-47 |
| rna_host_service_vulns のフィールド     | 6-47 |
| rna_host_service_vulns の結合        | 6-48 |
| rna_host_service_vulns のサンプルクエリ   | 6-48 |
| rna_host_third_party_vuln         | 6-48 |



|   |      |
|---|------|
| rna_host_third_party_vuln のフィールド              | 6-49 |
| rna_host_third_party_vuln の結合                 | 6-50 |
| rna_host_third_party_vuln のサンプルクエリ            | 6-50 |
| rna_host_third_party_vuln_bugtraq_id          | 6-50 |
| rna_host_third_party_vuln_bugtraq_id のフィールド   | 6-51 |
| rna_host_third_party_vuln_bugtraq_id の結合      | 6-51 |
| rna_host_third_party_vuln_bugtraq_id のサンプルクエリ | 6-52 |
| rna_host_third_party_vuln_cve_id              | 6-52 |
| rna_host_third_party_vuln_cve_id のフィールド       | 6-53 |
| rna_host_third_party_vuln_cve_id の結合          | 6-53 |
| rna_host_third_party_vuln_cve_id のサンプルクエリ     | 6-54 |
| rna_host_third_party_vuln_rna_id              | 6-54 |
| rna_host_third_party_vuln_rna_id のフィールド       | 6-55 |
| rna_host_third_party_vuln_rna_id の結合          | 6-55 |
| rna_host_third_party_vuln_rna_id のサンプルクエリ     | 6-56 |
| rna_vuln                                      | 6-56 |
| rna_vuln のフィールド                               | 6-57 |
| rna_vuln の結合                                  | 6-58 |
| rna_vuln のサンプルクエリ                             | 6-59 |
| tag_info                                      | 6-59 |
| tag_info のフィールド                               | 6-59 |
| tag_info の結合                                  | 6-60 |
| tag_info のサンプルクエリ                             | 6-60 |
| url_categories                                | 6-60 |
| url_categories のフィールド                         | 6-60 |
| url_categories の結合                            | 6-60 |
| url_categories のサンプルクエリ                       | 6-61 |
| url_reputations                               | 6-61 |
| url_reputations のフィールド                        | 6-61 |
| url_reputations の結合                           | 6-61 |
| url_reputations のサンプルクエリ                      | 6-61 |
| user_ipaddr_history                           | 6-62 |
| user_ipaddr_history のフィールド                    | 6-62 |
| user_ipaddr_history の結合                       | 6-63 |
| user_ipaddr_history のサンプルクエリ                  | 6-64 |

**CHAPTER 7****スキーマ: 接続ログ テーブル** 7-1

|                       |     |
|-----------------------|-----|
| connection_log        | 7-1 |
| connection_log のフィールド | 7-2 |

|                             |      |      |
|-----------------------------|------|------|
| connection_log の結合          | 7-15 |      |
| connection_log のサンプルクエリ     |      | 7-15 |
| connection_summary          | 7-15 |      |
| connection_summary のフィールド   |      | 7-16 |
| connection_summary の結合      | 7-18 |      |
| connection_summary のサンプルクエリ |      | 7-19 |
| si_connection_log           | 7-19 |      |
| si_connection_log のフィールド    |      | 7-19 |
| si_connection_log の結合       | 7-31 |      |
| si_connection_log のサンプルクエリ  |      | 7-31 |

## CHAPTER 8

## スキーマ: ユーザ アクティビティ テーブル 8-1

|                               |     |     |
|-------------------------------|-----|-----|
| discovered_users              | 8-1 |     |
| discovered_users のフィールド       |     | 8-2 |
| discovered_users の結合          | 8-2 |     |
| discovered_users のサンプルクエリ     |     | 8-2 |
| user_discovery_event          | 8-3 |     |
| user_discovery_event のフィールド   |     | 8-3 |
| user_discovery_event の結合      | 8-4 |     |
| user_discovery_event のサンプルクエリ |     | 8-4 |
| user_ioc_state                | 8-5 |     |
| user_ioc_state フィールド          |     | 8-5 |
| user_ioc_state 結合             | 8-7 |     |
| user_ioc_state サンプルクエリ        |     | 8-7 |

## CHAPTER 9

## スキーマ: 関連テーブル 9-1

|                             |      |      |
|-----------------------------|------|------|
| compliance_event            | 9-1  |      |
| compliance_event のフィールド     |      | 9-2  |
| compliance_event の結合        | 9-6  |      |
| compliance_event のサンプルクエリ   |      | 9-6  |
| remediation_status          | 9-6  |      |
| remediation_status のフィールド   |      | 9-7  |
| remediation_status の結合      | 9-7  |      |
| remediation_status のサンプルクエリ |      | 9-7  |
| white_list_event            | 9-8  |      |
| white_list_event のフィールド     |      | 9-8  |
| white_list_event の結合        | 9-9  |      |
| white_list_event のサンプルクエリ   |      | 9-10 |
| white_list_violation        | 9-10 |      |

|                               |      |
|-------------------------------|------|
| white_list_violation のフィールド   | 9-10 |
| white_list_violation の結合      | 9-11 |
| white_list_violation のサンプルクエリ | 9-11 |

---

**CHAPTER 10****スキーマ:ファイルイベントテーブル** 10-1

file\_event 10-1

file\_event のフィールド 10-2

file\_event の結合 10-6

file\_event のサンプルクエリ 10-6

---

**APPENDIX A****廃止テーブル** A-1

---

**INDEX**





## 概要

Firepower システム® データベース アクセス機能により、シスコ Firepower Management Center では、JDBC SSL 接続をサポートしているサードパーティクライアントを使用して、侵入、検出、ユーザアクティビティ、相関、接続、脆弱性、アプリケーション、および URL 統計のデータベース テーブルを照会できます。

Crystal Reports、Actuate BIRT、JasperSoft iReport などの業界標準のレポート作成ツールを使用してクエリを作成し、送信することができます。また、独自のカスタム アプリケーションを設定してプログラム制御下にある シスコ データを照会することもできます。たとえば、侵入および ディスカバリ イベント データについて定期的にレポートしたり、アラート ダッシュボードをリフレッシュしたりするサプレットを構築することが可能です。

1 つのクライアントで複数の Firepower Management Center に接続できますが、それぞれへのアクセスを個別に設定する必要があることに注意してください。

接続するアプライアンスを決定する際には、シスコ アプライアンス上のデータベースを照会すると、使用可能なアプライアンス リソースが減少する点に注意してください。クエリを慎重に設計し、組織の優先度に対応した適切な時点でクエリを送信する必要があります。

詳細については、次の項を参照してください。

- [バージョン 6.3 でのデータベース アクセスの重要な変更 \(1-1 ページ\)](#)
- [前提条件 \(1-2 ページ\)](#)
- [最初に行う作業 \(1-4 ページ\)](#)

## バージョン 6.3 でのデータベース アクセスの重要な変更

Firepower システム展開をバージョン 6.1 からバージョン 6.3 にアップグレードする場合、次に示す変更にご注意ください。これらの変更の一部では、クエリを更新する必要があります。

### バージョン 6.3 の新規テーブルおよび変更されたテーブル

次の表に、バージョン 6.3 のデータベース アクセス テーブルに対する変更を示します。

表 1-1      でのテーブルの変更の概要バージョン 6.3

| テーブル               | 変更の説明        |
|--------------------|--------------|
| rule_documentation | テーブルが廃止されました |

## 前提条件

データベースアクセス機能を使用する前に、以降の項で説明する前提条件を満たしている必要があります。

- [ライセンス \(1-2 ページ\)](#)
- [Firepower システム 機能と用語 \(1-2 ページ\)](#)
- [通信ポート \(1-2 ページ\)](#)
- [クライアント システム \(1-2 ページ\)](#)
- [クエリ アプリケーション \(1-3 ページ\)](#)
- [データベース クエリ \(1-3 ページ\)](#)

## ライセンス

いずれかの シスコ ライセンスがインストールされている場合には、外部データベースを照会できます。ただし、一部のテーブルは、ライセンスされている機能に関連付けられています。これらのテーブルにデータが取り込まれるのは、関連付けられている機能を使用できるようにライセンスが設定されており、そのデータが生成されるように展開が適切に設定されている場合だけです。ライセンスされていない機能に関連付けられているテーブルを照会することはできません。ライセンスの詳細については、『*Firepower Management Center Configuration Guide*』の「Understanding Licensing」を参照してください。

## Firepower システム 機能と用語

このマニュアルの情報を理解するには、Firepower システム の機能と名称、そのコンポーネントの機能について理解しておく必要があります。これらのコンポーネントにより生成される各種 イベント データについて理解しておく必要があります。『*Firepower Management Center Configuration Guide*』では、聞き慣れない用語や製品固有の用語の定義を頻繁に確認できます。この構成ガイドには、このマニュアルで説明するフィールドのデータに関する追加情報も収録されています。

## 通信ポート

Firepower システム では、内外のアプライアンス間で通信を行い、ネットワーク展開内で特定の機能を有効にするために、特定のポートを使用する必要があります。

Firepower Management Center でデータベース アクセスを有効にすると、クライアントとアプライアンスの間で JDBC トラフィックを伝送する接続にポート 1500 と 2000 が使用されます。

## クライアント システム

Firepower システム データベースへの接続に使用するコンピュータに、Java ソフトウェア (Java Runtime Environment (JRE) と呼ばれます) または Java 仮想マシン (JVM) をインストールする必要があります。最新バージョンの Java を <http://java.com/> からダウンロードできます。

Firepower Management Center から、データベースへの接続に使用する JDBC ドライバ ファイルが含まれているパッケージをダウンロードして解凍する必要があります。このパッケージには、Firepower Management Center との暗号化通信用の SSL 証明書のインストールに使用する実行可能ファイルや、これらのユーティリティのその他のソース ファイルも含まれています。

また、ご使用のコンピュータで該当するシステム設定(環境変数など)を変更する方法も理解しておく必要があります。

## クエリ アプリケーション

Firepower システム データベースを照会するには、商用のレポート ツール(Actuate BIRT、JasperSoft iReport、または Crystal Reports など)や、JDBC SSL 接続をサポートするその他の任意のアプリケーション(カスタム アプリケーションを含む)を使用できます。このマニュアルでは、データベースに接続するために必要な情報(JDBC URL、ドライバ JAR ファイル、ドライバクラスなど)について説明します。ただし、JDBC SSL 接続の詳しい設定手順については、ご使用のレポート ツールのドキュメントを参照してください。

シスコには、RunQuery と呼ばれるサンプル コマンドライン Java アプリケーションもあります。このアプリケーションを使用して、データベース接続のテストやスキーマの表示を実行できるほか、基本クエリまたはアドホック クエリを手動で実行することができます。RunQuery のソース コードは、カスタム Java アプリケーションでデータベース接続を設定する際のリファレンスでもあります。RunQuery ソース コードは、Firepower Management Center からダウンロードする ZIP パッケージに含まれています。

RunQuery はサンプル クライアントであり、フル機能のレポート ツールではありません。シスコでは、データベース照会の主な手段として、このツールを使用しないことを強く推奨します。RunQuery の使用法については、ZIP パッケージに含まれている README ファイルを参照してください。

データベース アクセス機能が使用する JDBC 機能は次に示すものだけである点に注意してください。

- データベース メタデータ(スキーマ、バージョン、およびサポートされている機能などの情報を含みます)。
- SQL クエリの実行

データベース アクセスではその他の JDBC 機能(ストアド プロシージャ、トランザクション、バッチ コマンド、複数の結果セット、挿入/更新/削除機能など)は使用されません。

## データベース クエリ

データベースを照会するには、結合条件を使用した 1 つまたは複数のテーブルに対する SELECT ステートメントの記述方法と実行方法を理解している必要があります。

ユーザを支援するため、このマニュアルでは、サポートされている MySQL クエリの構文、Firepower システム データベース スキーマ、許可されている結合、およびクエリに関連するその他の重要な要件と制約事項について説明します。

# 最初に行う作業

[前提条件\(1-2 ページ\)](#)で説明する前提条件を満たしていることを確認したら、最初に Firepower Management Center に接続するようにクライアントシステムを設定できます。

[データベース アクセスのセットアップ\(2-1 ページ\)](#)では、アクセスを許可するようにアプライアンスを設定する方法、アプライアンスに接続するようにクライアントシステムを設定する方法、およびアプライアンスに接続するようにレポートアプリケーションを設定する方法について説明します。また、いくつかの基本的なクエリの手順と、サポートされている MySQL 構文について説明します。

このマニュアルの残りの部分には、データベースのスキーマと結合に関する情報とサンプルクエリを収録しており、次の章で構成されています。

- [スキーマ: システムレベルテーブル\(3-1 ページ\)](#)では、システムレベルテーブル(監査ログやヘルスイベントなど)のスキーマと結合について説明します。
- [スキーマ: 侵入テーブル\(4-1 ページ\)](#)では、侵入関連テーブルのスキーマと結合について説明します。
- [スキーマ: 統計情報追跡テーブル\(5-1 ページ\)](#)では、アプリケーション、URL、およびユーザ統計情報のテーブルのスキーマと結合について説明します。
- [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\(6-1 ページ\)](#)では、検出イベントとネットワーク マップ情報(ネットワーク資産に関する情報)が格納されているテーブルのスキーマと結合について説明します。
- [スキーマ: 接続ログ テーブル\(7-1 ページ\)](#)では、接続イベントと接続サマリ イベントの情報が格納されているテーブルのスキーマと結合について説明します。
- [スキーマ: ユーザ アクティビティ テーブル\(8-1 ページ\)](#)では、ユーザ検出およびアイデンティティ データが格納されているテーブルのスキーマと結合について説明します。
- [スキーマ: 相関テーブル\(9-1 ページ\)](#)では、相関関連テーブル(ホワイトリスト イベントおよび違反、修復ステータス データなど)のスキーマと結合について説明します。
- [スキーマ: ファイル イベント テーブル\(10-1 ページ\)](#)では、ファイル イベントが格納されているテーブルのスキーマと結合について説明します。





## データベース アクセスのセットアップ

データベースへの読み取り専用アクセスを取得するには、最初にアクセスを許可するようにアプライアンスを設定する必要があります。次に、JDBC ドライバをダウンロードし、アクセスするアプライアンスからの SSL 証明書を受け入れることで、アプライアンスに接続するクライアント システムを設定する必要があります。最後に、アプライアンスに接続するようにレポート アプリケーションを設定します。



コメント

データベース アクセスをセットアップする前に、[前提条件 \(1-2 ページ\)](#) で説明されている前提条件を満たす必要があります。

詳細については、次の項を参照してください。

- [データベース ユーザ アカウントの作成 \(2-1 ページ\)](#)
- [Firepower Management Center でのデータベースアクセスの有効化 \(2-2 ページ\)](#)
- [JDBC ドライバのダウンロード \(2-3 ページ\)](#)
- [クライアント SSL 証明書のインストール \(2-4 ページ\)](#)
- [サードパーティ アプリケーションを使用したデータベースへの接続 \(2-5 ページ\)](#)
- [カスタム プログラムを使用したデータベースへの接続 \(2-7 ページ\)](#)
- [データベースの照会 \(2-9 ページ\)](#)
- [クエリのトラブルシューティング \(2-15 ページ\)](#)
- [サンプル クエリ \(2-16 ページ\)](#)

## データベース ユーザ アカウントの作成

ライセンス:すべて

Firepower システム データベースへのアクセスを設定するには、最初にユーザ アカウントを作成し、Firepower システム データベースにアクセスするための権限をそのアカウントに割り当てる必要があります。この権限を付与するには、システム提供の External Database User ユーザ ロール、または組織が作成し、External Database User 権限が含まれているカスタム ユーザ ロールを、このアカウントに割り当てます。ユーザ アカウントの作成と、特定のユーザ ロールの権限の確認については、『*Firepower Management Center Configuration Guide*』を参照してください。



警告

**External Database Access** はグローバル権限です。**External Database Access** が付与されているユーザは、すべてのドメインに対して情報を照会できます。



ヒント

システム提供の Administrator ロールが割り当てられているユーザには、デフォルトで External Database User 権限が付与されています。

マルチドメイン型展開では、Admin アクセス権限があるドメインでユーザアカウントを作成できます。ただし、External Database User ロールはグローバルドメインレベルでのみ使用可能です。External Database User は、ドメインに関係なくすべてのイベントにアクセスできます。

## Firepower Management Center でのデータベースアクセスの有効化

ライセンス:すべて

外部データベース ユーザの作成後に、アプライアンスのデータベースへのアクセスを許可するように Firepower Management Center を設定する必要があります。また、アプライアンスでデータベース アクセス リストを設定し、外部データベースを照会するすべてのホスト IP アドレスを追加する必要があります。

データベース アクセスを有効にする方法:

アクセス:管理

- 
- ステップ 1 Firepower Management Center で [System] > [Configuration] を選択します。
- ステップ 2 左側の [External Database Access] をクリックします。  
[Database Settings] メニューが表示されます。
- ステップ 3 [Allow External Database Access] チェックボックスをオンにします。  
[アクセスリスト (Access List)] フィールドが表示されます。
- ステップ 4 サードパーティ アプリケーションの要件に応じて、[Server Hostname] フィールドに Firepower Management Center の完全修飾ドメイン名 (FQDN) または IPv4 アドレスを入力します。証明書をインストールするときに IPv6 アドレスを使用できないため、IPv6 アドレスは使用できません。  
FQDN を入力する場合は、クライアントが Firepower Management Center の FQDN を解決できることを確認する必要があります。IP アドレスを入力する場合は、クライアントがその IP アドレスを使用して Firepower Management Center に接続できることを確認する必要があります。
- ステップ 5 1 つ以上の IP アドレスからのデータベース アクセスを追加するため、[Add Hosts] をクリックします。  
[アクセスリスト (Access List)] フィールドに [IP アドレス (IP Address)] フィールドが表示されます。
- ステップ 6 [IP Address] フィールドでは、追加する IP アドレスに応じて次のいずれかを入力できます。
- 正確な IPv4 アドレス (192.168.1.101 など)
  - 正確な IPv6 アドレス (2001:DB8::4 など)

- IP アドレス範囲。
  - Firepower システムで IP アドレス範囲を使用する方法については、『*Firepower Management Center Configuration Guide*』の IP アドレス規則を参照してください。
- **any**(任意の IP アドレスを指定)

ステップ 7 [追加(Add)] をクリックします。

IP アドレスがデータベース アクセス リストに追加されます。

ステップ 8 必要に応じてデータベース アクセス リストのエントリを削除するには、削除アイコン(🗑️)をクリックします。

ステップ 9 [Save(保存)] をクリックします。

データベース アクセス設定が保存されます。

ステップ 10 次の項(JDBC ドライバのダウンロード)の順に進みます。

## JDBC ドライバのダウンロード

ライセンス:すべて

外部データベース ユーザを作成し、Firepower Management Center でデータベース アクセスを許可するように設定したら、JDBC ドライバをクライアントシステムにダウンロードします。データベースに接続するとき、この JDBC ドライバを使用する必要があります。

JDBC ドライバをダウンロードするには、次の手順を実行します。

アクセス:Admin

ステップ 1 Firepower Management Center で [System] > [Configuration] を選択します。

ステップ 2 左側の [External Database Access] をクリックします。

[Database Settings] メニューが表示されます。

ステップ 3 [Client JDBC Driver] の横にある [Download] をクリックし、ブラウザのプロンプトに従って **client.zip** パッケージをダウンロードします。

ステップ 4 ZIP パッケージを解凍します。場所を書きとめておきます。

パッケージのファイル構造を保持してください。

ドライバはその他のファイルとともに ZIP ファイル(**client.zip**)に含まれています。パッケージのディレクトリ構造は次のとおりです。

- **bin**:RunQuery と呼ばれるサンプルクライアントと、クライアントと Firepower Management Center の間での暗号化通信用証明書をインストールするときに使用する実行ファイルが含まれています。
- **lib**:JDBC ドライバ JAR ファイルが含まれています。
- **src:bin** ディレクトリ内の実行ファイルのソース コードが含まれています。

ステップ 5 次の項(クライアント SSL 証明書のインストール)の順に進みます。

## クライアント SSL 証明書のインストール

JDBC ドライバのダウンロード後に、システム提供プログラム InstallCert を使用して Firepower Management Center からの SSL 証明書を受け入れ、インストールします。クライアントシステムと Firepower Management Center は SSL 証明書認証を使用して安全に通信します。証明書を受け入れる場合、現在実行されている JRE の `security` ディレクトリ内のキーストア (`jssecacerts`) に証明書が追加されます。

```
$JAVA_HOME/jre[version]/lib/security
```

次に、Microsoft Windows と UNIX を実行しているコンピュータでのキーストアの一般的な場所を示します。

- C:\Program Files\Java\jre[version]\lib\security\jssecacerts
- /var/jre[version]/lib/security/jssecacerts



コメント

データベース アクセス機能にアクセスするために使用する予定の Java クエリ アプリケーションが異なる JRE を使用している場合は、その別の JRE の `security` ディレクトリにキーストアをコピーする必要があります。

**InstallCert を使用して SSL をインストールするには、次の手順を実行します。**

- ステップ 1 コンピュータでコマンドライン インターフェイスを開きます。
- ステップ 2 コマンドプロンプトから、ZIP パッケージの解凍時に作成された `bin` にディレクトリを変更します。
- ステップ 3 Firepower Management Center の SSL 証明書をインストールするには、次のように入力して Enter キーを押します。

```
java InstallCert defense_center
```

`defense_center` は Firepower Management Center の FQDN または IP アドレスです。InstallCert は IPv6 アドレスをサポートしていません。IPv6 ネットワークでは、解決可能なホスト名を使用する必要があります。

Microsoft Windows を実行しているコンピュータでは次の例に示すような出力が表示されます。

```
Loading KeyStore C:\Program Files\Java\jre6\lib\security...
Opening connection to defensecenter.example.com:2000...
Starting SSL handshake...
Subject GENERATION=server, T=vjdbc, O="シスコ, Inc.",
...
...
```

証明書を表示するように求められます。

- ステップ 4 オプションで、証明書を表示します。  
証明書を受け入れるように求められます。
- ステップ 5 証明書を受け入れます。

証明書が受け入れられると、Microsoft Windows を実行しているコンピュータから次の例のような出力が表示されます。

```
Added certificate to keystore 'C:\Program Files\Java\jre6\lib\security\jssecacerts'
using alias 'defensecenter.example.com-1'
```

Crystal Reports を使用する予定の場合は、キーストア (`jssecacerts`) の場所を書きとめておきます。この情報は、後で必要になります。

ステップ 6 次の選択肢があります。

- サードパーティアプリケーションを使用する場合は、次の項([サードパーティアプリケーションを使用したデータベースへの接続\(2-5 ページ\)](#))の手順に進みます。
- カスタムアプリケーションを使用する場合は、[カスタムプログラムを使用したデータベースへの接続\(2-7 ページ\)](#)の手順に進みます。

## サードパーティアプリケーションを使用したデータベースへの接続

証明書のインストール後、JDBC SSL 接続をサポートするサードパーティクライアントを使用して、Firepower Management Center でデータベースを照会できます。次の表に、クライアントと Firepower Management Center 間の接続を設定するために必要な情報を示します。

表 2-1 データベースアクセスクライアントの接続情報

| 情報                 | 説明  |
|--------------------|---|
| JDBC URL           | 次に示す JDBC URL によって Firepower システム データベースが識別されるため、クライアントの JDBC ドライバがそのデータベースとの接続を確立できます。<br><code>jdbc:vjdbc:rmi://defense_center:2000/VJdbc,eqe</code><br><code>defense_center</code> は Firepower Management Center の FQDN または IP アドレスです。   |
| JDBC ドライバ JAR ファイル | Firepower システム データベースへの接続を設定するときには次に示す JAR ファイルを使用する必要があります。 <ul style="list-style-type: none"> <li>• <code>vjdbc.jar</code></li> <li>• <code>commons-logging-1.1.jar</code></li> </ul> これらのファイルは、 <a href="#">JDBC ドライバのダウンロード(2-3 ページ)</a> の説明に従い <code>client.zip</code> ファイルをダウンロードして解凍した <code>lib</code> サブディレクトリにあります。 |
| JDBC ドライバクラス       | Firepower システム データベースへの接続を設定するときには次に示すドライバクラスを使用する必要があります。<br><code>com.sourcefire.vjdbc.VirtualDriver</code>   |
| ユーザ名とパスワード         | アプライアンスのデータベースに接続するには、External Database User 権限が付与されているユーザアカウントを使用します。詳細については、 <a href="#">データベースユーザアカウントの作成(2-1 ページ)</a> を参照してください。  |

以降のセクションでは、広く使用されている 3 つの業界標準レポート ツールを使用して、Firepower システム データベースに接続する際のヒントを説明します。これらのツールまたは他の Java ベースのアプリケーションのいずれを使用するかに関係なく、ご使用のレポート ツールのドキュメントで、JDBC SSL 接続の詳しい作成手順を参照してください。

### Crystal Reports

以下の情報は 32 ビット Windows 環境への Crystal Reports 2011 のインストールに適用されます。64 ビット Windows 環境を実行している場合はファイルパスが異なる可能性があります。

Crystal Reports 2011 が Firepower システム データベースに接続できるようにするには、次の操作が必要です。

- Firepower Management Center からダウンロードした JDBC ドライバ JAR ファイルを Crystal Reports クラスパスに追加します。Crystal Reports のデフォルトインストールの場合、次に示すファイルでクラスパス セクションを編集できます。  
C:\Program Files\SAP BusinessObjects\SAP Business Objects  
Enterprise XI 4.0\Java\CRConfig.xml
- クライアント SSL 証明書のインストール時に作成したキーストアを、適切な Crystal Reports セキュリティ ディレクトリにコピーします。Crystal Reports のデフォルトインストールの場合、ディレクトリは次のとおりです。  
C:\Program Files\SAP BusinessObjects\SAP Business Objects  
Enterprise XI 4.0\win32\_x86\jdk\jre\lib\security
- シスコ をデータベース名として使用し、Database Expert との新しい JDBC (JNDI) の接続を作成します。

### JasperSoft iReport

iReport が Firepower システム データベースに接続できるようにするには、次の操作が必要です。

- Firepower Management Center からダウンロードした JDBC ドライバ JAR ファイルを iReport クラスパスに追加します。
- Firepower Management Center からダウンロードした JDBC ドライバ JAR ファイルを使用して新しい JDBC ドライバを追加します。ドライバファイルの追加後は、iReport は新しいドライバクラスを検出するはずですが、
- 作成したドライバを使用して、新しいデータベース接続を作成します。

### Actuate BIRT

BIRT が Firepower システム データベースに接続できるようにするには、次の操作が必要です。

- [Generic JDBC Driver] テンプレートを使用してドライバ定義を追加します。
- [Generic JDBC] プロファイル タイプを使用して新しいデータベース接続を作成します。
- [JDBC Data Source] データ ソース タイプを使用してレポートのデータ ソースを作成します。

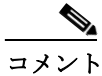


ヒント

新しい JDBC データ ソース プロファイルの作成時に シスコ ドライバ クラスを選択できない場合は、Firepower Management Center からダウンロードした JDBC ドライバ JAR ファイルを使用してドライバを追加します。

## カスタムプログラムを使用したデータベースへの接続

証明書をインストールしたら、カスタム Java レポート ツールが Firepower システム データベースを照会できるように設定できます。シスコ には、RunQuery という名前のサンプル Java コマンドラインアプリケーションがあります。このアプリケーションは、Firepower Management Center に含まれている JDBC ドライバを使用して必要な SSL 接続を確立します。RunQuery は、テーブルレコードとテーブルメタデータの両方を取得します。ソース コードは、Firepower Management Center からダウンロードした ZIP パッケージの `src` ディレクトリに含まれています。[JDBC ドライバのダウンロード\(2-3 ページ\)](#)を参照してください。



コメント

RunQuery はサンプル クライアントであり、フル機能のレポート ツールではありません。シスコ では、データベース照会の主な手段として、このツールを使用しないことを強く推奨します。RunQuery の使用方法については、ZIP パッケージに含まれている README ファイルを参照してください。

カスタム プログラムを使用したデータベースへの接続に関する詳細については、次の項を参照してください。

- [カスタム Java プログラムのサンプル コード\(2-7 ページ\)](#) : RunQuery アプリケーションがデータベース接続のセットアップとクエリの送信に使用する Java クラスとメソッドについて説明します。
- [アプリケーションの実行\(2-8 ページ\)](#) : Java アプリケーションを実行するための環境要件について説明します。

## カスタム Java プログラムのサンプルコード

RunQuery ソース コードでは、後述する関数が使用されます。次のコード例に、可能な実装方法の 1 つを示します。

### SSL プロバイダー接続の動的な設定

クライアントに SSL セキュリティ証明書をインストールしたら([クライアント SSL 証明書のインストール\(2-4 ページ\)](#)を参照)、プログラムで次の行を使用して JSSE プロバイダーを動的に登録できます。

```
Security.addProvider(new com.sun.net.ssl.internal.ssl.(Provider()));
```

### プログラムの JDBC ドライバの初期設定

`Class.forName()` メソッドを使用して Java アプリケーションに JDBC ドライバクラスを次のようにロードできます。

```
Class.forName("com.sourcefire.vjdbc.VirtualDriver").newInstance();
```

コマンドラインから起動するプログラムの場合は、ユーザが次のように JDBC クラスを指定できます。

```
java -Djdbc.drivers="com.sourcefire.vjdbc.VirtualDriver" program_name ...
```

`program_name` はプログラムの名前です。

### データベースへのプログラムの接続

プログラムがクエリを送信する前に、プログラムで JDBC 接続オブジェクトを取得する必要があります。接続を確立して接続オブジェクトを取得するには、次のように `DriverManager.getConnection` メソッドを使用します。

```
Connection conn = DriverManager.getConnection("jdbc:vjdbc:rmi://my_dc:2000/VJdbc,eqe",
    "user", "password");
```

`my_dc` は Firepower Management Center の FQDN または IP アドレス、`user` はデータベース アクセス ユーザ アカウント名、`password` はアカウント パスワードです。

### シスコ テーブルのデータの照会

クエリを送信し、取得したレコードを結果セットに割り当てるため、SQL クエリ オブジェクトを次のように作成します。

```
Statement stmt = conn.createStatement();
ResultSet rs = stmt.executeQuery("sql");
```

`sql` は SQL クエリです。サポートされている SQL 関数については、[データベースの照会 \(2-9 ページ\)](#) を参照してください。

### テーブル クエリの結果の作成

上記のクエリにより生成される結果セット (`rs`) から、次のようにフィールドを出力できます。

```
while(rs.next())
{
    for(int i=1; i<= md.getColumnCount(); i++)
    {
        System.out.print(rs.getString(i) + " ");
    }
    System.out.print("\n");
}
```

### スキーマ情報の取得

プログラムは、データベースのテーブルを次のようにリストできます。

```
DatabaseMetaData metaData = conn.getMetaData();
ResultSet tables = meta.getTables(null, null, null, null);
while (tables.next())
{
    System.out.println(tables.getString("TABLE_NAME"));
}
```

プログラムは、テーブルの列を次のようにリストできます。

```
ResultSet columns = metaData.getColumns(null, null, "table_name", null);
```

`table_name` は、データベース テーブルの名前です。

## アプリケーションの実行

アプリケーションを実行する前に、クライアント コンピュータの `CLASSPATH` を設定し、アプリケーションの JAR ファイルの場所と現在のディレクトリを組み込む必要があります。

[JDBC ドライバのダウンロード \(2-3 ページ\)](#) の説明に従ってデータベース アクセスの ZIP パッケージをダウンロードして解凍した場合は、`CLASSPATH` を次のように更新します。



**UNIX 環境でアプリケーションを実行するには:**

ステップ 1 次のコマンドを使用します。

```
export CLASSPATH=$CLASSPATH:.;path/lib/vjdbc.jar:path/lib/commons-logging-1.1.jar
```

*path* は、Firepower Management Center からダウンロードした ZIP パッケージを解凍したディレクトリパスです。

**Windows 7 環境でアプリケーションを実行するには:**

ステップ 1 [Computer] アイコンを右クリックして [Properties] を選択します。

[System] ウィンドウが表示されます。

ステップ 2 [Advanced System Settings] をクリックします。

[System Properties] ウィンドウが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [Environment Variables...] をクリックします。

[Environment Variables] ウィンドウが表示されます。

ステップ 5 **CLASSPATH** システム変数を選択して [Edit...] をクリックします。

[Edit System Variable] ウィンドウが表示されます。

ステップ 6 [Variable value:] フィールドに次を追加します。

```
.;path\bin;.;path\lib\vjjdbc.jar;.;path\lib\commons-logging-1.1.jar;.;path\lib
```

*path* は、Firepower Management Center からダウンロードした ZIP パッケージを解凍したディレクトリパスです。

ステップ 7 [OK] をクリックして、値を保存します。

[Environment Variables] ウィンドウが表示されます。

ステップ 8 [OK] をクリックして、値を保存します。これでアプリケーションを実行できます。

## データベースの照会

External Database Access はグローバル権限です。クエリで制限していない限り、結果はデータベース内のすべてのドメインを対象としています。

以降のセクションでは、サポートされているクエリの構文と、クエリに関連するその他の重要な要件および制約事項について説明します。

- サポートされている **SHOW** ステートメント構文(2-10 ページ)では、Firepower システム データベース照会のためにサポートされている MySQL **show** ステートメント構文について説明します。
- サポートされている **DESCRIBE** または **DESC** ステートメント構文(2-10 ページ)では、Firepower システム データベース照会のためにサポートされている MySQL **DESCRIBE** ステートメント構文について説明します。
- サポートされている **SELECT** ステートメント構文(2-11 ページ)では、Firepower システム データベース照会のためにサポートされている MySQL **select** ステートメント構文について説明します。

- [結合の制約\(2-12 ページ\)](#)では、Firepower システム データベース照会のためにサポートされている結合と、任意のテーブルに対して許可されている結合に関する情報の確認方法を説明します。
- [使い慣れていない形式で保存されているデータの照会\(2-13 ページ\)](#)では、使い慣れていない形式で保存されているデータ (UNIX タイムスタンプおよび IP アドレスを含む) に対してクエリを実行し、クエリが正常に完了し、予期しているとおりの結果が表示されるようにする方法について説明します。
- [パフォーマンス上の理由によるクエリの制限\(2-14 ページ\)](#)では、クエリに対する制約を適用する場合に、Firepower システム のパフォーマンスを低下させないための推奨事項について説明します。
- [クエリのヒント\(2-15 ページ\)](#)では、さまざまなアプライアンスで侵入イベントを照会する場合のヒントについて説明します。

スキーマの情報と許可されている結合については、以降の章を参照してください。

- [スキーマ: システムレベル テーブル\(3-1 ページ\)](#)
- [スキーマ: 侵入テーブル\(4-1 ページ\)](#)
- [スキーマ: 統計情報追跡テーブル\(5-1 ページ\)](#)
- [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\(6-1 ページ\)](#)
- [スキーマ: 接続ログ テーブル\(7-1 ページ\)](#)
- [スキーマ: ユーザ アクティビティ テーブル\(8-1 ページ\)](#)
- [スキーマ: 相関テーブル\(9-1 ページ\)](#)

## サポートされている SHOW ステートメント構文

**SHOW** ステートメントは、Firepower システム データベースのすべてのテーブルをリストします。Firepower システム データベースの照会に使用できる、サポートされている MySQL **SHOW** ステートメント構文を次に示します。

```
SHOW TABLES;
```

上記にない **SHOW** ステートメント構文はサポートされていません。

## サポートされている DESCRIBE または DESC ステートメント構文

Firepower システム データベースでは、**DESCRIBE** ステートメントを限定的に使用できます。Firepower システム データベースでは、**DESCRIBE** ステートメントの出力には列の名前と各列のデータのタイプだけがリストされます。Firepower システム データベースの照会に使用できる、サポートされている MySQL **DESCRIBE** ステートメント構文を次に示します。

```
DESCRIBE table_name;
```

Firepower システム データベースでは、これと同一のコマンド **DESC** もサポートされています。

```
DESC table_name;
```

表 2-2 サポートされている **DESCRIBE** ステートメントの構文

| 項目                      | 説明          |
|-------------------------|-------------|
| <code>table_name</code> | 照会するテーブルの名前 |

上記にない **DESCRIBE** ステートメント構文はサポートされていません。特に、Firepower システム データベース アクセス機能では次の要素はサポートされていません。

- INDEX FOR 句
- TABLE 句
- PROCEDURE 句

## サポートされている **SELECT** ステートメント構文

Firepower システム データベースの照会に使用できる、サポートされている MySQL **SELECT** ステートメント構文を次に示します。

```
SELECT
[ALL | DISTINCT]
[COUNT ( field ) | COUNT (*) ]

select_expr [, select_expr ...]

FROM table_references

[WHERE where_condition]

[GROUP BY { column_name | position } [ ASC | DESC ], ...]

[HAVING where_condition]

[ORDER BY { column_name | position } [ ASC | DESC ], ...]

[LIMIT { [offset,] row_count | row_count OFFSET offset}]
```

次の表に、上記の **SELECT** ステートメントの句と引数の必須構文について詳しく説明します。

表 2-3 サポートされている **SELECT** ステートメント構文

| 項目                 | 説明  |
|--------------------|---|
| select_expr        | {column_name [[AS] alias]   function(...) [[AS] alias]   aggregate_function(...) [[AS] alias]}  |
| column_name        | 照会するフィールドの名前  |
| 機能                 | {ABS   CAST   CEILING   CHAR_LENGTH   COALESCE   CONV   CHARACTER_LENGTH   CONCAT   CONVERT   COUNT   CURRENT_DATE   CURRENT_TIME   CURRENT_TIMESTAMP   EXTRACT   FLOOR   HEX   INET_ATON   INET_NTOA   INET6_ATON   INET6_NTOA   LEFT   LOWER   LPAD   MID   MOD   NULLIF   OCTET_LENGTH   POSITION   RIGHT   ROUND   SUBSTRING   SYSDATE   TIME   TIMESTAMP   TRIM   UPPER} |
| aggregate_function | {AVG   COUNT   COUNT(DISTINCT)   MAX   MIN   SUM}   |
| field              | 関数の実行対象フィールドの名前   |
| table_references   | 次のいずれかを入力します。 <ul style="list-style-type: none"> <li>• table_reference INNER JOIN table_reference join_condition</li> <li>• table_reference LEFT [OUTER] JOIN table_reference join_condition</li> </ul>   |
| table_reference    | table_name [[AS] alias]   |
| table_name         | 照会するテーブルの名前   |
| join_condition     | ON conditional_expr   |

表 2-3 サポートされている **SELECT** ステートメント構文(続き)

| 項目               | 説明  |
|------------------|---|
| conditional_expr | 結合に対応したフィールド値の等価比較。詳細については、 <a href="#">結合の制約(2-12 ページ)</a> を参照してください。  |
| where_condition  | 次のいずれかを入力します。 <ul style="list-style-type: none"> <li>• IS NULL または IS NOT NULL</li> <li>• NOT, !</li> <li>• BETWEEN ... AND ...</li> <li>• LIKE</li> <li>• =, !=, &lt;&gt;, &gt;, &gt;=, &lt;, &lt;=</li> </ul> |

サポートされている MySQL 構文の記述方法に慣れていない場合は、次の表でヒントを参照してください。

表 2-4 MySQL 構文の形式

| 記号   | 表記  | 意味           |
|------|-----|--------------|
| 角カッコ | [ ] | オプションの句または引数 |
| 波カッコ | { } | 必要な句または引数    |
| パイプ  |     | 句または引数の選択    |

上記にない **SELECT** ステートメント構文はサポートされていません。特に、Firepower システム データベース アクセス機能では次の要素はサポートされていません。

- **SELECT \***: フィールドを明示的に指定する必要があります。
- ユニオン
- サブクエリ
- **GROUP BY** 句の **WITH ROLLUP** 修飾子
- **INTO** 句
- **FOR UPDATE** 句

## 結合の制約

パフォーマンスおよびその他の実際的な理由から、Firepower システム データベースのテーブルに対して実行できる結合は限定されています。シスコでは、その結果がイベント分析に役立つ可能性のない結合は実行できません。

内部結合または左(外部)結合だけを実行できます。入れ子になった結合、クロス結合、自然結合、右(外部)結合、フル(外部)結合、および **USING** 句を使用した結合はサポートされていません。

スキーマに関するドキュメントでは、各テーブルでサポートされている結合が示されています。リストされていない結合はサポートされていません。たとえば、**compliance\_event** テーブルと **intrusion\_event** テーブルを **IP** アドレス フィールドで結合することはできません。これは、両方のテーブルに **IP** アドレス情報が含まれている場合でも同様です。また、廃止されたテーブルと廃止されたフィールドでの結合はリストされていません。

## 使い慣れていない形式で保存されているデータの照会

Firepower システム データベースでは、表示に適していない形式で一部のデータが保存されています。以降の項では、さまざまなフィールドに対してクエリを実行し、クエリが正常に完了し、預期しているとおりの結果が表示されるようにする方法について詳しく説明します。

- [IPv6 形式のアドレス \(2-13 ページ\)](#)
- [IPv4 アドレス \(2-13 ページ\)](#)
- [MAC アドレス \(2-13 ページ\)](#)
- [パケット データ \(2-14 ページ\)](#)
- [UNIX タイムスタンプ \(2-14 ページ\)](#)

### IPv6 形式のアドレス

Firepower システム データベースには、IPv6 アドレスがバイナリ形式で保存されます。結果を 16 進数形式で表示するには、`HEX()` 関数を使用します。特定の IPv6 アドレスのデータベースを照会するには、`UNHEX()` 関数を使用します。

たとえば、モニタ対象セッションに関する情報を含む `connection_log` テーブルを照会し、その照会を特定の IPv6 アドレスで制限するステートメントを次に示します。

```
SELECT HEX(initiator_ip), HEX(responder_ip), packets_sent, bytes_sent
FROM connection_log
WHERE initiator_ip = UNHEX('20010db80000000000000000000004321');
```

### IPv4 アドレス

Firepower システム データベースでは、IPv6 アドレスと同じフィールドに、IPv4 アドレスがバイナリ形式で保存されます。IPv6 アドレスと同様に、16 進数形式で表示する場合は `HEX()` 関数を使用します。データベースは RFC に準拠するためにビット 80 ~ 95 に 1 を取り込みますが、これによって無効な IPv6 アドレスが生成されます。たとえば IPv4 アドレス 10.5.15.1 は `000000000000000000000000FFFF0A050F01` として保存されます。

### MAC アドレス

Firepower システム データベースには、MAC アドレスがバイナリ形式で保存されます。結果を 16 進数形式で表示するには、`HEX()` 関数を使用します。

たとえば、次のステートメントは `rna_host_mac_map` テーブルを照会します。このテーブルには、IP アドレスでは識別されなかったホストとその MAC アドレスに関する情報が含まれており、照会で取得できるホストが最初の 5 つのホストに限定されます。

```
SELECT HEX(host_id), HEX(mac_address)
FROM rna_host_mac_map
LIMIT 5;
```

## パケットデータ

Firepower システム データベースは、侵入イベントのパケットデータをバイナリ形式で保存します。結果を 16 進数形式で表示するには、`HEX()` 関数を使用します。

たとえば、次のステートメントは `intrusion_event_packet` テーブルを照会し、特定イベントのパケットデータを取得します。

```
SELECT HEX(packet_data)
FROM intrusion_event_packet
WHERE event_id = 1234;
```

## UNIX タイムスタンプ

Firepower システム データベースではほとんどのタイムスタンプが UNIX タイムスタンプとして保存されます。UNIX タイムスタンプは、1970 年 1 月 1 日 00:00:00 (UTC) 以降の経過秒数を表します。現地時間で結果を表示するには、`FROM_UNIXTIME()` 関数を使用します。

たとえば、次のステートメントは `audit_log` テーブルを照会し、最大 25 件の結果を返します。このテーブルには、アプライアンスの Web インターフェイスでのユーザアクションがすべて記録されています。

```
SELECT FROM_UNIXTIME(action_time_sec), user, message
FROM audit_log
LIMIT 0, 25;
```

データベースのすべての時刻は UTC の時刻であることに注意してください。`CONVERT_TZ()` 関数を使用できますが、この関数は結果を UTC で返します。

一部のイベントには、マイクロ秒の精度が関連付けられている点に注意してください。UNIX タイムスタンプとマイクロ秒の増分を連結するには、`CONCAT()` 関数と `LPAD()` 関数を使用します。たとえば、次のステートメントは `intrusion_event` テーブルを照会します。

```
SELECT CONCAT(FROM_UNIXTIME(event_time_sec), '.', LPAD(event_time_usec, 6, '0')),
HEX(host_id),
rule_message
FROM intrusion_event
LIMIT 0, 25;
```

データベースに対し、特定の UNIX タイムスタンプのイベントを照会するには、`UNIX_TIMESTAMP()` 関数を使用します。

## パフォーマンス上の理由によるクエリの制限

Firepower システム データベース テーブルに対して実行できる結合はシステムにより制限されていますが、一部のコストがかかるクエリ (Firepower Management Center のパフォーマンスに悪影響を及ぼす可能性のあるクエリ) が許可されます。

したがって、大規模なテーブルの場合は結果セットを制限するようにします。戦略としては次のものがあります。

- 特定のリーフ ドメインにクエリを制限する
- 特定の時間範囲にクエリを制限する
- IP アドレスによりクエリを制限する
- **LIMIT** 句を使用する

展開によっては、多数のテーブルを照会する際に結果セットを制限する必要があることがあります。特に次のテーブルには、DC3000 での最大 1 億件のイベントを格納できます。

- **fireamp\_event**
- **intrusion\_event**
- **intrusion\_event\_packet**
- **connection\_log** (5.0 より古いバージョンでの名前: **rna\_flow**)
- **connection\_summary** (5.0 より古いバージョンでの名前: **rna\_flow\_summary**)

モニタ対象ネットワークでシステムが検出したホストの数によっては、ネットワーク マップ テーブルに対するクエリはコストが高くなることがあります。

## クエリのヒント

以降の項では、検出エンジンまたは侵入イベントを含むクエリを作成する場合に、固有の結果が得られるようにするためのヒントを示します。

### デバイス名

デバイス名は複数の Firepower Management Center 間で必ずしも一意である必要はありません。一意であるようにするには、特定のデバイス UUID をクエリに含めます。

### 侵入イベント

複数の管理対象デバイス上の侵入イベントに一意に一致するためには、**intrusion\_event** テーブルの次のフィールドをクエリに指定できます。

- `intrusion_event.event_id`
- `intrusion_event.event_time_sec`
- `intrusion_event.sensor_uuid`

## クエリのトラブルシューティング

1 つのクライアントへのアクセスを許可するように複数の Firepower Management Center を設定できますが、各システムを個別に設定する必要があります。各システムで使用可能な情報は複数の要因によって決まります。照会するデータがない場合、クエリから予期している結果が返されません。

以下に、クエリから結果が返されない原因のいくつかを示します。

- クエリの条件が細かすぎます。たとえば、クエリの時間範囲または IP アドレス範囲を調整する必要があります。
- イベント発生の原因となったネットワーク トラフィックによっては、イベントの一部のフィールドにデータが取り込まれないことがあります。たとえば、すべての接続イベントにペイロード情報が含まれているわけではありません。
- 照会するイベント タイプのログ記録を設定していませんでした。

- イベント保存を無効にしていました。
- ユーザがアクセスできないドメインを照会しようとしています。

イベントの生成方法とログ記録方法の詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

## サンプルクエリ

以降の項に収録されているサンプルクエリでは、データベースアクセス機能の使用法を示します。

- [ユーザの監査レコード \(2-16 ページ\)](#)
- [プライオリティおよび分類別の侵入イベント \(2-16 ページ\)](#)
- [侵入イベントおよびその関連ポリシー \(2-17 ページ\)](#)
- [検出されたホストのリスト \(2-17 ページ\)](#)
- [検出されたサーバのリスト \(2-17 ページ\)](#)
- [ネットワークのサーバの脆弱性 \(2-18 ページ\)](#)
- [オペレーティングシステムの概要 \(2-18 ページ\)](#)
- [ホストのオペレーティングシステムの脆弱性 \(2-18 ページ\)](#)
- [ホストの違反カウント \(2-19 ページ\)](#)



注意

展開によっては、一部のサンプルクエリの実行には非常にコストがかかることがあります。詳細については、「[パフォーマンス上の理由によるクエリの制限 \(2-14 ページ\)](#)」を参照してください。

### ユーザの監査レコード

次のクエリは、特定ユーザの監査ログのレコードをすべて返します。タイムスタンプは UTC で表示されます。

```
SELECT FROM_UNIXTIME(action_time_sec), user, message
FROM audit_log
WHERE user = 'eventanalyst';
```

### プライオリティおよび分類別の侵入イベント

次のクエリは、[Events By Priority and Classification] ワークフローの [Drilldown of Event]、[Priority]、[Classification] ビューを複製します。ユーザ設定でデフォルトの [Intrusion Events] ワークフローを変更していない場合、これが Firepower Management Center Web インターフェイスで [Analysis] > [Intrusion Events] を選択すると最初に表示されるページです。

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



## 侵入イベントおよびその関連ポリシー

次のクエリは、指定した週の侵入イベントをリストします。イベントごとに、関連する侵害ポリシー違反とルール分類が表示されます。

```
SELECT FROM_UNIXTIME(event_time_sec) AS event_time, event_id AS intrusion_event,
intrusion_event_policy_name AS policy, rule_classification AS classification
FROM intrusion_event
WHERE event_time_sec BETWEEN UNIX_TIMESTAMP('2011-10-01 00:00:00') AND
UNIX_TIMESTAMP('2011-10-07 23:59:59')
ORDER BY policy ASC;
```

## 検出されたホストのリスト

次のクエリは、ネットワークで検出されたすべての MAC ホスト (IP アドレスのないホスト) のホスト ネットワーク マップでの基本情報と、各 NIC のハードウェア ベンダーを返します。

```
SELECT HEX(mac_address), mac_vendor, host_type, FROM_UNIXTIME(last_seen_sec)
FROM rna_mac_host;
```

次のクエリは、IP アドレスを MAC アドレスにマップします。

```
SELECT HEX(ipaddr), HEX(mac_address), HEX(host_id)
FROM rna_host_ip_map LEFT JOIN rna_host_mac_map on
rna_host_ip_map.host_id=rna_host_mac_map.host_id;
```

## 検出されたサーバのリスト

次のクエリは、2つの関連するテーブルを結合し、ネットワークで検出されたサーバを、その属性の多くとともにリストとして返します。これは、Firepower Management Center の Web インターフェイスでサーバのテーブルビューに表示される内容に似ています。

```
SELECT FROM_UNIXTIME(s.last_used_sec), HEX(s.host_id), s.port, s.protocol, s.hits,
i.service_name, i.vendor, i.version, i.source_type, s.confidence
FROM AS s
LEFT JOIN rna_ip_host_service_info AS i ON (s.host_id = i.host_id AND s.port = i.port AND
s.protocol =
i.protocol);
```

このクエリは、データベースアクセスが必要なため、host\_id、port、および protocol のセットでテーブルを左結合する点に注意してください。[rna\\_host\\_service の結合 \(6-37 ページ\)](#) および [rna\\_host\\_service\\_info の結合 \(6-41 ページ\)](#) を参照してください。

## ネットワークのサーバの脆弱性

次のクエリは、2つの脆弱性関連テーブルを結合し、特定のホストで検出された有効なサーバ関連の脆弱性と、各脆弱性がネットワーク上で悪用可能であるかどうかのリストを示します。

```
SELECT h.rna_vuln_id, v.title, v.remote
FROM rna_host_service_vulns AS h
LEFT JOIN rna_vuln AS v ON (h.rna_vuln_id = v.rna_vuln_id)
WHERE h.ip_address = INET_ATON('10.10.10.4')
AND h.invalid = 0;
```

このクエリは、[rna\\_host\\_service\\_vulns\(6-47 ページ\)](#)と [rna\\_vuln の結合\(6-58 ページ\)](#)で必要なため、[rna\\_vuln\\_id](#) でテーブルを左結合する点に注意してください。

## オペレーティングシステムの概要

次のクエリは、[Operating System Summary] ワークフローで [Summary of OS Names] ページを複製します。ユーザ設定でデフォルトのワークフローを変更していない場合、これが **Firepower Management Center Web** インターフェイスで [Analysis] > [Hosts] を選択し、次に [Hosts] を選択すると最初に表示されるページです。

```
SELECT vendor, product, count(*) AS total
FROM rna_host_os
GROUP BY vendor, product
ORDER BY total DESC;
```

## ホストのオペレーティングシステムの脆弱性

次のクエリは、2つの脆弱性関連テーブルを結合し、特定のホストで検出された有効なオペレーティングシステム関連の脆弱性と、各脆弱性がネットワーク上で悪用可能であるかどうかのリストを示します。

```
SELECT h.rna_vuln_id, v.title, v.remote
FROM rna_host_os_vulns AS h
LEFT JOIN rna_vuln AS v ON (h.rna_vuln_id = v.rna_vuln_id)
WHERE h.host_id = UNHEX('9610B6E6F1784DA4B39BEA7A210AAD68')
AND h.invalid = 0;
```

このクエリは、データベースアクセスで必要なため、[rna\\_vuln\\_id](#) でテーブルを左結合する点に注意してください。[rna\\_host\\_os\\_vulns\(6-31 ページ\)](#)および [rna\\_vuln の結合\(6-58 ページ\)](#)を参照してください。

## ホストの違反カウント

次のクエリは、[Host Violation Count] ワークフローで [Host Violation Count] ページを複製します。ユーザ設定でデフォルトの [Compliance White List Violations] ワークフローを変更していない場合、これが Firepower Management Center Web インターフェイスで [Analysis] > [Correlation] > [White List Violations] を選択すると最初に表示されるページです。

```
SELECT host_id, HEX(host_id), white_list_name, count(*) AS total
FROM white_list_violation
GROUP BY host_id, white_list_name
ORDER BY total DESC;
```





## スキーマ:システムレベル テーブル

この章では、システムレベルの機能(監査、アプライアンスヘルスマニタ、マルウェア検出、およびセキュリティ更新のログ記録など)のスキーマとサポートされている結合について説明します。詳細については、次の表に示す項を参照してください。

表 3-1 システムレベル 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                      | バージョン   |
|---|-------------------------------------|---------|
| <a href="#">audit_log (3-1 ページ)</a>     | アプライアンスの Web インターフェイスとのユーザインタラクション。 | 4.10.x+ |
| <a href="#">fireamp_event (3-2 ページ)</a> | AMP for Endpoints マルウェア検出および検疫イベント。 | 5.1+    |
| <a href="#">health_event (3-9 ページ)</a>  | モニタ対象アプライアンスのヘルス ステータス イベント。        | 4.10.x+ |

### audit\_log

**audit\_log** テーブルには、Firepower システム ユーザと Web インターフェイスのインタラクションに関する情報が格納されます。監査ログにはローカル アプライアンスのレコードだけが格納され、管理対象アプライアンスのレコードは格納され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。

- [audit\\_log のフィールド \(3-1 ページ\)](#)
- [audit\\_log の結合 \(3-2 ページ\)](#)
- [audit\\_log のサンプル クエリ \(3-2 ページ\)](#)

### audit\_log のフィールド

次の表に、**audit\_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 3-2 **audit\_log** のフィールド

| フィールド           | 説明  |
|-----------------|---|
| action_time_sec | アプライアンスにより監査レコードが生成された日時を示す UNIX タイムスタンプ。 |
| domain_name     | ユーザがログインしたドメインの名前。                        |
| domain_uuid     | ユーザがログインしたドメインの UUID。これはバイナリで示されます。       |

表 3-2 audit\_log のフィールド(続き)

| フィールド     | 説明  |
|-----------|---|
| message   | ユーザが実行した操作。                                   |
| source    | Web インターフェイス ユーザのホストの IP アドレス(ドット形式 10 進表記法)。 |
| subsystem | 監査レコードが生成されたときにユーザがたどったメニューパス。                |
| user      | 監査イベントをトリガーしたユーザのユーザ名。                        |

## audit\_log の結合

audit\_log テーブルに対して結合を実行することはできません。

## audit\_log のサンプルクエリ

次のクエリは、最大 25 件の最新監査ログ エントリを、時刻でソートし、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT from_unixtime(action_time_sec)
AS Time, user, subsystem, message, source, count(*)
AS Total
FROM audit_log
GROUP BY source, subsystem, user, message
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY source DESC;
```

## fireamp\_event

fireamp\_event テーブルには、AMP for Endpoints により検出されたマルウェア イベントと、AMP for Firepower により検出されたネットワーク ベースのイベントに関する情報が格納されます。これらのイベントには、クラウド内で検出または検疫されたマルウェア、検出方法、マルウェアの影響を受けるホストとユーザに関する情報が含まれています。個々のマルウェア イベントに関するその他の情報は、イベントの生成方法と生成理由に応じて異なります。

AMP for Firepower はネットワーク トラフィックでマルウェア ファイルを検出することから、ネットワーク ベースのマルウェア イベントには、ファイルの送信に使用された接続に関する、ポート、アプリケーションプロトコル、および送信元 IP アドレスの情報が含まれます。

AMP for Endpoints 展開からインポートされたマルウェア イベントと IOC には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報(ファイルパス、呼び出し元クライアントアプリケーションなど)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。

- [fireamp\\_event のフィールド\(3-3 ページ\)](#)
- [fireamp\\_event の結合\(3-8 ページ\)](#)
- [fireamp\\_event のサンプルクエリ\(3-8 ページ\)](#)

## fireamp\_event のフィールド

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

表 3-3 `fireamp_event` のフィールド

| フィールド                                | 説明   |
|--------------------------------------|--|
| <code>application_id</code>          | ファイル転送を実行するアプリケーションにマップされている ID 番号。  |
| <code>application_name</code>        | 転送を実行するアプリケーションの名前。  |
| <code>cert_valid_end_date</code>     | 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。  |
| <code>cert_valid_start_date</code>   | 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。   |
| <code>client_application_id</code>   | クライアントアプリケーションの内部識別番号(該当する場合)。   |
| <code>client_application_name</code> | クライアントアプリケーションの名前(該当する場合)。   |
| <code>cloud_name</code>              | マルウェア イベントの発生元クラウドサービスの名前。各 <code>cloud_name</code> 値には <code>cloud_uuid</code> 値が関連付けられています。  |
| <code>cloud_uuid</code>              | マルウェア イベントの発生元クラウドサービスの内部の固有 ID。各 <code>cloud_uuid</code> 値には <code>cloud_name</code> 値が関連付けられています。  |
| <code>connection_sec</code>          | マルウェア イベントに関連付けられている接続イベントの UNIX タイムスタンプ(00:00:00 01/01/1970 からの経過秒数)。   |
| <code>counter</code>                 | 同じ秒数で発生した複数のイベントを区別するために使用されるイベント固有のカウンタ。  |
| <code>detection_name</code>          | 検出されたマルウェアまたは検疫されたマルウェアの名前。  |
| <code>detector_type</code>           | マルウェアを検出したディテクタ。各 <code>detector_type</code> 値には <code>detector_type_id</code> 値が関連付けられています。有効な表示値とその関連 ID を次に示します。 <ul style="list-style-type: none"> <li>• ClamAV:128</li> <li>• ETHOS:8</li> <li>• SPERO:32</li> <li>• SHA:4</li> <li>• Tetra:64</li> </ul>         |
| <code>detector_type_id</code>        | マルウェアを検出した検出テクノロジーの内部 ID。各 <code>detector_type_id</code> 値には <code>detector_type</code> 値が関連付けられています。有効な表示値とその関連タイプを次に示します。 <ul style="list-style-type: none"> <li>• 4:SHA</li> <li>• 8:ETHOS</li> <li>• 32:SPERO</li> <li>• 64:Tetra</li> <li>• 128:ClamAV</li> </ul> |

表 3-3 fireamp\_event のフィールド(続き)

| フィールド              | 説明  |
|--------------------|---|
| direction          | <p>ファイルのアップロードとダウンロードのいずれが行われたかを示す値。次のいずれかの値になります。</p> <ul style="list-style-type: none"> <li>ダウンロード</li> <li>Upload</li> </ul> <p>現時点では、この値はプロトコルに依存しています(例えば接続が HTTP の場合はダウンロード)。</p>   |
| disposition        | <p>ファイルのマルウェア ステータス。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>CLEAN: ファイルはクリーンであり、マルウェアが含まれていない。</li> <li>UNKNOWN: ファイルにマルウェアが含まれているかどうか不明である。</li> <li>MALWARE: ファイルにマルウェアが含まれている。</li> <li>UNAVAILABLE: ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しなかった。</li> <li>CUSTOM SIGNATURE: ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理された。</li> </ul> |
| domain_name        | イベントが検出されたドメインの名前。  |
| domain_uuid        | イベントが検出されたドメインの UUID。これはバイナリで示されます。   |
| dst_continent_name | <p>宛先ホストが位置する地域の名前</p> <p>** : 不明</p> <p>na : 北米</p> <p>as : アジア</p> <p>af : アフリカ</p> <p>eu : 欧州</p> <p>sa : 南米</p> <p>au : オーストラリア</p> <p>an : 南極</p>  |
| dst_country_id     | 宛先ホストの国のコード。  |
| dst_country_name   | 宛先ホストの国の名前。   |
| dst_ip_address_v6  | このフィールドは廃止されており、null を返します。   |
| dst_ipaddr         | 接続の宛先の IPv4 または IPv6 アドレスのバイナリ表現。   |
| dst_port           | 接続の宛先のポート番号。  |
| endpoint_user      | シスコ クラウドによりイベントが検出された場合に シスコ AMP for Endpoints エージェントにより判別されるユーザ。このユーザは LDAP に関連付けられておらず、discovered_users テーブルに表示されません。   |
| event_description  | イベント タイプに関連付けられている追加イベント情報。   |
| event_id           | マルウェア イベントの内部固有 ID。   |



表 3-3 fireamp\_event のフィールド(続き)

| フィールド            | 説明   |
|------------------|--|
| event_subtype    | <p>マルウェア検出につながったアクション。各 event_subtype 値には event_subtype_id 値が関連付けられています。有効な表示値とその関連 ID を次に示します。</p> <ul style="list-style-type: none"> <li>• Create:1</li> <li>• Execute:2</li> <li>• Move:22</li> <li>• Scan:4</li> </ul>   |
| event_subtype_id | <p>マルウェア検出につながったアクションの内部 ID。各 event_subtype_id 値には event_subtype 値が関連付けられています。有効な表示値とその関連サブタイプを次に示します。</p> <ul style="list-style-type: none"> <li>• 1:作成</li> <li>• 2:実行</li> <li>• 4:スキャン</li> <li>• 22:移動</li> </ul>   |
| event_type       | <p>マルウェア イベントのタイプ。各 event_type 値には event_type_id 値が関連付けられています。有効な表示値とその関連 ID を次に示します。</p> <ul style="list-style-type: none"> <li>• Blocked Execution:553648168</li> <li>• Cloud Recall Quarantine:553648155</li> <li>• Cloud Recall Quarantine Attempt Failed:2164260893</li> <li>• Cloud Recall Quarantine Started:553648147</li> <li>• Cloud Recall Restore from Quarantine:553648154</li> <li>• Cloud Recall Restore from Quarantine Failed:2164260892</li> <li>• Cloud Recall Restore from Quarantine Started:553648146</li> <li>• FireAMP IOC:1107296256</li> <li>• Quarantine Failure:2164260880</li> <li>• Quarantined Item Restored:553648149</li> <li>• Quarantine Restore Failed:2164260884</li> <li>• Quarantine Restore Started:553648150</li> <li>• Scan Completed, No Detections:554696715</li> <li>• Scan Completed With Detections:1091567628</li> <li>• Scan Failed:2165309453</li> <li>• Scan Started:554696714</li> <li>• Threat Detected:1090519054</li> <li>• Threat Detected in Exclusion:553648145</li> <li>• Threat Detected in Network File Transfer:1</li> <li>• Threat Detected in Network File Transfer (Retrospective):2</li> <li>• Threat Quarantined:553648143</li> </ul> |

表 3-3 fireamp\_event のフィールド(続き)

| フィールド              | 説明  |
|--------------------|---|
| event_type_id      | <p>マルウェア イベント タイプの内部 ID。各 event_type_id 値には event_type 値が関連付けられています。有効な表示値とその関連タイプを次に示します。</p> <ul style="list-style-type: none"> <li>553648143:Threat Quarantined</li> <li>553648145:Threat Detected in Exclusion</li> <li>553648146:Cloud Recall Restore from Quarantine Started</li> <li>553648147:Cloud Recall Quarantine Started</li> <li>553648149:Quarantined Item Restored</li> <li>553648150:Quarantine Restore Started</li> <li>553648154:Cloud Recall Restore from Quarantine</li> <li>553648155:Cloud Recall Quarantine</li> <li>553648168:Blocked Execution</li> <li>554696714:Scan Started</li> <li>554696715:Scan Completed, No Detections</li> <li>1090519054:Threat Detected</li> <li>1091567628:Scan Completed With Detections</li> <li>1107296256:FireAMP IOC</li> <li>2164260880:Quarantine Failure</li> <li>2164260893:Cloud Recall Quarantine Attempt Failed</li> <li>2164260884:Quarantine Restore Failed</li> <li>2164260892:Cloud Recall Restore from Quarantine Failed</li> <li>2165309453:Scan Failed</li> </ul> |
| file_name          | 検出または検疫されたファイルの名前。この名前には、UTF-8 文字を使用できます。   |
| file_path          | 検出または検疫されたファイルのファイルパス。ファイル名は含まれません。このパスには、UTF-8 文字を使用できます。  |
| file_sha           | 検出または検疫されたファイルの SHA-256 ハッシュ値。  |
| file_size          | 検出または検疫されたファイルのサイズ(バイト単位)。  |
| file_timestamp     | 検出または検疫されたファイルの作成タイムスタンプ。   |
| file_type          | 検出または検疫されたファイルのファイルタイプ。   |
| file_type_id       | 検出または検疫されたファイルのファイルタイプの内部 ID。   |
| http_response_code | イベントで HTTP 要求に対して返された応答コード。   |
| instance_id        | イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。  |
| ioc_count          | イベントで検出された侵害の痕跡の数。  |
| parent_file_name   | 検出が行われたときに、検出または検疫されたファイルにアクセスしたファイルの名前。  |
| parent_file_sha    | 検出が行われたときに、検出または検疫されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。  |
| policy_uuid        | イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する識別番号。   |

表 3-3 fireamp\_event のフィールド(続き)

| フィールド                        | 説明  |
|------------------------------|---|
| retroactive_disposition      | 特性が更新されている場合のファイルの特性。特性が更新されていない場合、このフィールドには disposition フィールドと同じ値が格納されます。有効な値は disposition フィールドと同じです。   |
| 得点                           | 動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値(0 ~ 100)。   |
| security_context             | トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の説明。システムがこのフィールドにデータを設定するのは、マルチ コンテキストモードの ASA FirePOWER デバイスの場合だけです。 |
| sensor_address               | イベントを生成したデバイスの IP アドレス。   |
| sensor_id                    | イベントを生成したデバイスの ID。  |
| sensor_name                  | イベントレコードを生成した管理対象デバイスのテキスト名。接続デバイスではなくレポート デバイス自体を参照するイベントの場合、このフィールドは null です。                           |
| sensor_uuid                  | 管理対象デバイスの固有識別子( <code>fireamp_event.sensor_name</code> が null の場合は 0)。                                    |
| src_continent_name           | 送信元ホストが位置する地域の名前<br>**: 不明<br>na: 北米<br>as: アジア<br>af: アフリカ<br>eu: 欧州<br>sa: 南米<br>au: オーストラリア<br>an: 南極  |
| src_country_id               | 送信元ホストの国のコード。   |
| src_country_name             | 送信元ホストの国の名前。  |
| src_ip_address_v6            | バージョン 5.2 で廃止されたフィールド。すべてのクエリに対して null を返します。   |
| src_ipaddr                   | 接続元の IPv4 または IPv6 アドレスのバイナリ表現。   |
| src_port                     | 接続元のポート番号。  |
| ssl_issuer_common_name       | SSL 証明書の発行元の共通名。これは一般に証明書発行元のホストとドメイン名ですが、その他の情報が含まれていることもあります。   |
| ssl_issuer_country           | SSL 証明書の発行元の国。  |
| ssl_issuer_organization      | SSL 証明書の発行元の組織。   |
| ssl_issuer_organization_unit | SSL 証明書の発行元の組織単位。   |
| ssl_serial_number            | 発行元 CA によって割り当てられた SSL 証明書のシリアル番号。  |
| ssl_subject_common_name      | SSL 証明書の件名共通名。これは通常、証明書件名のホストとドメイン名ですが、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。  |

表 3-3 fireamp\_event のフィールド(続き)

| フィールド                         | 説明   |
|-------------------------------|--|
| ssl_subject_organization_unit | SSL 証明書の件名の組織単位。   |
| threat_name                   | 脅威の名前。   |
| timestamp                     | マルウェア イベント生成時のタイムスタンプ。   |
| url                           | 接続元の URL。  |
| user_id                       | ファイルを送信または受信したホストの最終ログイン ユーザの内部識別番号。このユーザは <b>discovered_users</b> テーブルに含まれています。 |
| username                      | ファイルを送信または受信したホストの最終ログイン ユーザの名前。   |
| web_application_id            | Web アプリケーションの内部識別番号(該当する場合)。   |
| web_application_name          | Web アプリケーションの名前(該当する場合)。   |

## fireamp\_event の結合

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

表 3-4 fireamp\_event の結合

| このテーブルで結合に使用するフィールド             | 結合できるフィールド   |
|---------------------------------|--|
| dst_ipaddr<br>または<br>src_ipaddr | rna_host_ip_map.ipaddr<br>user_ipaddr_history.ipaddr |

## fireamp\_event のサンプルクエリ

次のクエリは、指定されたユーザに関連付けられている 25 件のマルウェア イベントを、timestamp の昇順にソートして返します。

```
SELECT event_id, timestamp, src_ipaddr, dst_ipaddr, username, cloud_name, event_type,
event_subtype, event_description, detection_name, detector_type, file_name,
parent_file_name
FROM fireamp_event
WHERE username="username" ORDER BY timestamp ASC
LIMIT 25;
```

## health\_event

**health\_event** テーブルには、Firepower システム によって生成されたヘルス イベントに関する情報が格納されます。

詳細については、次の項を参照してください。

- [health\\_event のフィールド \(3-9 ページ\)](#)
- [health\\_event の結合 \(3-10 ページ\)](#)
- [health\\_event のサンプル クエリ \(3-10 ページ\)](#)

## health\_event のフィールド

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

表 3-5 **health\_event** のフィールド

| フィールド          | 説明  |
|----------------|---|
| description    | 関連するヘルス モジュールがヘルス イベントを生成した条件の説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには [Unable to Execute] というラベルが付けられます。  |
| domain_name    | イベントが検出されたドメインの名前。  |
| domain_uuid    | イベントが検出されたドメインの UUID。これはバイナリで示されます。   |
| event_time_sec | Firepower Management Center によりヘルス イベントが生成された日時を示す UNIX タイムスタンプ。  |
| id             | イベントの内部識別番号。  |
| module_name    | イベントを生成したヘルス モジュールの名前。  |
| sensor_name    | イベント レコードを生成した管理対象デバイスのテキスト名。接続デバイスではなくレポート デバイス自体を参照するヘルス イベントの場合、このフィールドは <b>null</b> です。   |
| sensor_uuid    | 管理対象デバイスの固有識別子 (sensor_name が null の場合は 0)。   |
| status         | sensor_uuid で識別されるアプライアンスについて報告されたヘルス モニタ ステータス。値は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>red</b>: 重大ステータス。アプライアンス上の 1 つ以上のヘルス モジュールが制限を超え、問題が解決されていません。</li> <li>• <b>yellow</b>: 警告ステータス。アプライアンス上の 1 つ以上のヘルス モジュールが制限を超え、問題が解決されていません。</li> <li>• <b>green</b>: 通常ステータス。アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作しています。</li> <li>• <b>recovered</b>: アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作しています。これには、前に重大または警告状態だったモジュールも含まれます。</li> <li>• <b>disabled</b>: アプライアンスが無効またはブラックリストに追加されているか、現在到達不能であるか、または正常性ポリシーがアプライアンスに適用されていません。</li> <li>• <b>error</b>: アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行されていません。</li> </ul> |

表 3-5 health\_event のフィールド(続き)

| フィールド | 説明   |
|-------|--|
| units | ヘルス テストの結果の測定単位。たとえば%(ディスク使用量のパーセンテージ)。    |
| value | ヘルス テストの結果の単位数。例えば 80 % の場合 value は 80 です。 |

## health\_event の結合

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

## health\_event のサンプルクエリ

次のクエリは、定義された時間枠内にログに記録された最大 25 件の最新のヘルス イベントを、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT module_name, FROM_UNIXTIME(event_time_sec)
AS event_time, description, value, units, status, sensor_name
FROM health_event
WHERE event_time_sec AND domain_name= "Global \ Company B \ Edge"
BETWEEN UNIX_TIMESTAMP("2011-10-01 00:00:00")
AND UNIX_TIMESTAMP("2011-10-07 23:59:59")
ORDER BY event_time DESC
LIMIT 0, 25;
```



## スキーマ:侵入テーブル

この章では、侵入イベント、侵入イベントをトリガーしたパケット、および関連するルールメッセージのスキーマとサポートされている結合について説明します。

詳細については、次の表に示す項を参照してください。

表 4-1 侵入テーブルのスキーマ

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

### intrusion\_event

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



ヒント

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

詳細については、次の項を参照してください。

- [intrusion\\_event](#) のフィールド (4-2 ページ)
- [intrusion\\_event](#) の結合 (4-7 ページ)
- [intrusion\\_event](#) のサンプルクエリ (4-7 ページ)

## intrusion\_event のフィールド

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

表 4-2 `intrusion_event` のフィールド

| フィールド                                   | 説明  |
|---|---|
| <code>access_control_policy_name</code> | 侵入イベントを生成した侵入ポリシーに関連付けられているアクセス コントロール ポリシー。アクセス コントロール ポリシー名とアクセス コントロール ルール名の組み合わせは、Firepower Management Center で一意である点に注意してください。   |
| <code>access_control_policy_UUID</code> | 侵入イベントを生成した侵入ポリシーに関連付けられているアクセス コントロール ポリシーの UUID。  |
| <code>access_control_rule_id</code>     | 侵入イベントを生成した侵入ポリシーに関連付けられているアクセス コントロール ルールの内部識別番号。  |
| <code>access_control_rule_name</code>   | 侵入イベントを生成した侵入ポリシーに関連付けられているアクセス コントロール ルールの名前。アクセス コントロール ルールの名前は、1つのポリシー内では固有であるが、異なるポリシー間では固有ではない点に注意してください。  |
| <code>application_protocol_id</code>    | アプリケーション プロトコルの内部識別番号。  |
| <code>application_protocol_name</code>  | 次のいずれかになります。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)</li> <li>pending(システムがさらにデータを必要としている場合)</li> <li>空白(接続にアプリケーション情報がない場合)</li> </ul>   |
| <code>blocked</code>                    | 侵入イベントをトリガーしたパケットの処理を示す値。 <ul style="list-style-type: none"> <li>0:パケットはドロップされなかった</li> <li>1:パケットはドロップされた(インライン型、スイッチ型、またはルーティング型展開)</li> <li>2:侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開で設定されているデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。</li> </ul> |
| <code>client_application_id</code>      | 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。   |
| <code>client_application_name</code>    | 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。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)</li> <li>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)。</li> <li>null(接続にアプリケーション情報がない場合)</li> </ul>              |
| <code>connection_sec</code>             | 侵入イベントに関連付けられている接続イベントの UNIX タイムスタンプ(00:00:00 01/01/1970 からの経過秒数)。  |
| <code>counter</code>                    | 特定の秒で発生した接続イベントごとに増加する番号。これは、同じ秒で発生した複数の接続イベントを区別するために使用されます。   |



表 4-2 intrusion\_event のフィールド(続き)

| フィールド                     | 説明  |
|---------------------------|---|
| detection_engine_name     | バージョン 5.0 で廃止されたフィールド。すべてのクエリに対して null を返します。   |
| detection_engine_uuid     | バージョン 5.0 で廃止されたフィールド。すべてのクエリに対して null を返します。   |
| domain_name               | イベントのために指定されたドメインの名前。   |
| domain_uuid               | イベントのために指定されたドメインの UUID。これはバイナリで示されます。  |
| dst_continent_name        | 宛先ホストが位置する地域の名前<br>**:不明<br>na:北米<br>as:アジア<br>af:アフリカ<br>eu:欧州<br>sa:南米<br>au:オーストラリア<br>an:南極   |
| dst_country_id            | 宛先ホストの国のコード。  |
| dst_country_name          | 宛先ホストの国の名前。   |
| dst_ip_address            | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。  |
| dst_ip_address_v6         | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。  |
| dst_ipaddr                | トリガー イベントに関連する宛先ホストの IPv4 または IPv6 アドレスのバイナリ表現。   |
| dst_port                  | 次のいずれかを行います。 <ul style="list-style-type: none"> <li>イベントプロトコルタイプが TCP または UDP の場合は宛先ポート番号</li> <li>イベントプロトコルタイプが ICMP の場合は ICMP コード。</li> </ul> |
| dst_user_dept             | 宛先ユーザの所属部門。   |
| dst_user_email            | 宛先ユーザの電子メールアドレス。  |
| dst_user_first_name       | 宛先ユーザの名前。   |
| dst_user_id               | 宛先ユーザの内部識別番号。宛先ユーザとは、侵入イベント発生前に宛先ホストにログインしていた最終ユーザです。   |
| dst_user_last_name        | 宛先ユーザの姓。  |
| dst_user_last_seen_sec    | システムが宛先ユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。  |
| dst_user_last_updated_sec | システムが宛先ユーザのレコードを最後に更新した日時を示す UNIX タイムスタンプ。  |
| dst_user_name             | 宛先ユーザのユーザ名。   |

表 4-2 intrusion\_event のフィールド(続き)

| フィールド                        | 説明   |
|------------------------------|--|
| dst_user_phone               | 宛先ユーザの電話番号。  |
| event_id                     | イベントの内部識別番号。Firepower Management Center でイベントを一意に識別します。  |
| event_time_sec               | イベント パケットがキャプチャされた日時を示す UNIX タイムスタンプ。  |
| event_time_usec              | イベントのタイムスタンプのマイクロ秒単位の増分。マイクロ秒単位の精度を使用できない場合、この値は 0 です。   |
| http_response_code           | イベントで HTTP 要求に対して返された応答コード。  |
| icmp_code                    | イベントが ICMP トラフィックの場合は ICMP コード。イベントが ICMP トラフィックから生成されたものではない場合は null。   |
| icmp_type                    | イベントが ICMP トラフィックの場合は ICMP タイプ。イベントが ICMP トラフィックから生成されたものではない場合は null。   |
| impact                       | イベントの影響フラグ値。整数値は次のとおりです。 <ul style="list-style-type: none"> <li>• 1: レッド(脆弱)</li> <li>• 2: オレンジ(脆弱の可能性あり)</li> <li>• 3: イエロー(現在は脆弱でない)</li> <li>• 4: ブルー(不明なターゲット)</li> <li>• 5: グレー(不明な影響)</li> </ul> |
| instance_id                  | イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。   |
| interface_egress_name        | 発信トラフィックのインターフェイスの名前。  |
| interface_ingress_name       | 着信トラフィックのインターフェイスの名前。  |
| intrusion_event_policy_uuid  | 侵入イベントをトリガーした侵入ポリシーの固有識別子。   |
| intrusion_event_policy_name  | 侵入イベントを生成した侵入ポリシー。   |
| ioc_count                    | イベントで検出された侵害の痕跡の数。   |
| network_analysis_policy_name | 侵入イベントを生成した侵入ポリシーに関連付けられているネットワーク分析ポリシー。   |
| network_analysis_policy_UUID | 侵入イベントを生成した侵入ポリシーに関連付けられているネットワーク分析ポリシーの UUID。   |
| priority                     | イベントに関連付けられているルール分類のプライオリティ。ルールのプライオリティはユーザ インターフェイスで設定されます。   |
| protocol_name                | 侵入イベントに関連付けられているトラフィック プロトコルのテキスト名。  |
| protocol_num                 | プロトコルの IANA 番号。IANA 番号のリストは <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> にあります。   |
| reviewed                     | 侵入イベントが確認済みとしてマークされているかどうか。 <ul style="list-style-type: none"> <li>• 1: 確認済み</li> <li>• 0: 未確認</li> </ul>  |
| rule_classification          | 侵入イベントに関連付けられているルール分類の説明。通常、イベントをトリガーしたルールによって検出された攻撃を説明します。例: A Network Trojan was Detected.  |
| rule_classification_id       | 侵入イベントに関連付けられているルール分類の識別番号。  |

表 4-2 intrusion\_event のフィールド(続き)

| フィールド                      | 説明  |
|----------------------------|---|
| rule_generator             | 侵入イベントを生成したコンポーネント。生成コンポーネントは、ルールエンジン、デコーダ、またはプリプロセッサです。  |
| rule_generator_id          | 侵入イベントを生成した rule_generator で指定されているコンポーネントのジェネレータ ID (GID)。   |
| rule_message               | イベントを説明するテキスト。ルールベースの侵入イベントの場合、メッセージはルールから生成されます。デコーダベースおよびプリプロセッサベースのイベントの場合、メッセージはハードコーディングされています。            |
| rule_revision              | 侵入イベントに関連付けられているルールのリビジョン番号。  |
| rule_signature_id          | 侵入イベントのシグニチャ ID (SID)。侵入イベントが生成される原因である特定のルール、デコーダ メッセージ、またはプリプロセッサ メッセージを識別します。                                |
| security_context           | トラフィックが通過したセキュリティ コンテキスト (仮想ファイアウォール) の説明。マルチコンテキスト モードの ASA FirePOWER デバイスでは、システムはこのフィールドにのみ入力することに注意してください。   |
| security_zone_egress_name  | ポリシー違反をトリガーした侵入イベントの出力セキュリティゾーン。  |
| security_zone_ingress_name | ポリシー違反をトリガーした侵入イベントの入力セキュリティゾーン。  |
| sensor_address             | イベントを生成した管理対象デバイスの IP アドレス。形式は <i>ipv4_address</i> , <i>ipv6_address</i> です。                                    |
| sensor_name                | 侵入イベントを生成した管理対象デバイスの名前。   |
| sensor_uuid                | 管理対象デバイスの固有識別子 (sensor_name が null の場合は 0)。   |
| src_continent_name         | 宛先ホストが位置する地域の名前<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>an : 南極 |
| src_country_id             | 宛先ホストの国のコード。  |
| src_country_name           | 宛先ホストの国の名前。   |
| src_ip_address             | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。  |
| src_ip_address_v6          | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。  |
| src_ipaddr                 | トリガー イベントに関連する送信元ホストの IPv4 または IPv6 アドレスのバイナリ表現。  |

表 4-2 intrusion\_event のフィールド(続き)

| フィールド                     | 説明  |
|---------------------------|---|
| src_port                  | 次のいずれかを行います。 <ul style="list-style-type: none"> <li>イベントプロトコルタイプが TCP または UDP の場合は送信元ポート番号</li> <li>イベントプロトコルタイプが ICMP の場合は ICMP タイプ。</li> </ul>  |
| src_user_dept             | 送信元ユーザの所属部門。  |
| src_user_email            | 送信元ユーザの電子メールアドレス。   |
| src_user_first_name       | 送信元ユーザの名前。  |
| src_user_id               | 送信元ユーザの内部識別番号。送信元ユーザとは、侵入イベント発生前に送信元ホストにログインしていた最終ユーザです。  |
| src_user_last_name        | 送信元ユーザの姓。   |
| src_user_last_seen_sec    | システムが送信元ユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。   |
| src_user_last_updated_sec | 送信元ユーザのレコードの最終更新日時を示す UNIX タイムスタンプ。   |
| src_user_name             | 送信元ユーザのユーザ名。  |
| src_user_phone            | 送信元ユーザの電話番号。  |
| vlan_id                   | 侵入イベントをトリガーしたパケットに関連付けられている最も内側の VLAN の識別番号。  |
| web_application_id        | 侵入イベントで使用された Web アプリケーションの内部識別番号(該当する場合)。   |
| web_application_name      | 侵入イベントで使用された Web アプリケーション(該当する場合)。次のいずれかになります。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)</li> <li>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)。</li> <li>空白(接続に HTTP トラフィックがない場合)。</li> </ul> |

## intrusion\_event の結合

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

表 4-3 `intrusion_event` の結合

| このテーブルで結合に使用するフィールド  | 結合できるフィールド  |
|--|---|
| application_protocol_id<br>または<br>client_application_id<br>または<br>web_application_id | application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>rna_host_service_payload.web_application_id |
| dst_ipaddr<br>または<br>src_ipaddr  | rna_host_ip_map.ipaddr<br>user_ipaddr_history.ipaddr  |

## intrusion\_event のサンプルクエリ

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

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

## intrusion\_event\_packet

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

詳細については、次の項を参照してください。

- [intrusion\\_event\\_packet のフィールド \(4-8 ページ\)](#)
- [intrusion\\_event\\_packet の結合 \(4-8 ページ\)](#)
- [intrusion\\_event\\_packet のサンプルクエリ \(4-8 ページ\)](#)

## intrusion\_event\_packet のフィールド

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

表 4-4 `intrusion_event_packet` のフィールド

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

## intrusion\_event\_packet の結合

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

## intrusion\_event\_packet のサンプルクエリ

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

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

## rule\_message

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

詳細については、次の項を参照してください。

- [rule\\_message のフィールド \(4-9 ページ\)](#)
- [rule\\_message の結合 \(4-9 ページ\)](#)
- [rule\\_message のサンプル クエリ \(4-9 ページ\)](#)

## rule\_message のフィールド

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

表 4-5 **rule\_message** のフィールド

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

## rule\_message の結合

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

## rule\_message のサンプル クエリ

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

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

■ rule\_message





## スキーマ:統計情報追跡テーブル

この章では、アプリケーションと URL の統計情報追跡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。これらのテーブルには、次の統計情報が収集されます。

- アクセス コントロールと侵入イベント(アプリケーション別およびユーザ別)
- 帯域幅の使用状況と接続に関する決定(アプリケーション別およびユーザ別)
- 帯域幅の使用状況と接続に関する決定(URL レピュテーション(リスク)別および URL のビジネス関連度別)

各テーブルの詳細情報へのリンクについては、次の表を参照してください。

表 5-1 アプリケーションと URL の統計情報のテーブル

| 参照先   | 次の統計情報が格納されるテーブル  | Version |
|---|---|---------|
| <a href="#">app_ids_stats_current_timeframe (5-4 ページ)</a>           | アクセス コントロール アクティビティおよび侵入からの保護アクティビティ(アプリケーション別およびアプリケーション属性の範囲別)                              | 5.0+    |
| <a href="#">app_stats_current_timeframe (5-6 ページ)</a>               | トラフィック ボリュームとシステム アクセス コントロール アクティビティ(接続の許可また拒否)(アプリケーション別およびアプリケーション属性の範囲別)                  | 5.0+    |
| <a href="#">compliance_events_stats_current_timeframe (5-8 ページ)</a> | コンプライアンスおよびホワイトリスト イベント   | 6.0+    |
| <a href="#">dns_query_stats_current_timeframe (5-9 ページ)</a>         | DNS クエリ   | 6.0+    |
| <a href="#">geolocation_stats_current_timeframe (5-11 ページ)</a>      | アクセス コントロール アクティビティ(ロケーション別)。   | 5.2+    |
| <a href="#">ids_impact_stats_current_timeframe (5-13 ページ)</a>       | 影響レベル別の侵入イベントの統計情報(ブロックされた接続とドロップされた可能性のある接続)。  | 5.1.1+  |
| <a href="#">interface_stats_current_timeframe (5-14 ページ)</a>        | インターフェイスの統計情報。  | 6.1 以降  |
| <a href="#">ip_reputation_stats_current_timeframe (5-16 ページ)</a>    | 指定されたセキュリティ インテリジェンス カテゴリの IP アドレス、URL、および DNS ドメインに対する要求に関連付けられている帯域幅使用状況と接続に関する統計情報が格納されます。 | 6.0+    |
| <a href="#">qos_rule_stats_current_timeframe (5-17 ページ)</a>         | トリガーされるサービス ルールの品質の統計情報とその適用方法が含まれます。   | 6.1 以降  |

表 5-1 アプリケーションと URL の統計情報のテーブル(続き)

| 参照先  | 次の統計情報が格納されるテーブル  | Version |
|--|---|---------|
| <a href="#">session_stats_current_timeframe</a> (5-18 ページ)                   | すべての接続の統計情報が格納されます。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。                   | 5.2+    |
| <a href="#">ssl_stats_current_timeframe</a> (5-20 ページ)                       | SSL 接続の統計情報が格納されます。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。                   | 5.4+    |
| <a href="#">storage_stats_by_disposition_current_timeframe</a> (5-22 ページ)    | 特性に基づくファイルの統計情報が格納されます。統計情報は、バイト数、特性、センサー、および時刻に基づいて抽出できます。               | 5.3+    |
| <a href="#">storage_stats_by_file_type_current_timeframe</a> (5-24 ページ)      | ファイルタイプに基づくファイルの統計情報が格納されます。統計情報は、バイト数、ファイルタイプ、センサー、および時刻に基づいて抽出できます。     | 5.3+    |
| <a href="#">transmission_stats_by_file_type_current_timeframe</a> (5-25 ページ) | ファイルタイプに基づく接続の統計情報が格納されます。統計情報は、バイト数、接続、ファイルタイプ、センサー、および時刻に基づいて抽出できます。    | 5.3+    |
| <a href="#">tunnel_session_stats_current_timeframe</a>                       | このテーブルのルックアップは現在サポートされていません。  | 6.1 以降  |
| <a href="#">url_category_stats_current_timeframe</a> (5-27 ページ)              | 要求された Web サイトのカテゴリ別のトラフィック ボリュームとシステム アクセス コントロール アクティビティ (接続の許可また拒否)     | 5.0+    |
| <a href="#">url_reputation_stats_current_timeframe</a> (5-28 ページ)            | 要求された Web サイトのレピュテーション別のトラフィック ボリュームとシステム アクセス コントロール アクティビティ (接続の許可また拒否) | 5.0+    |
| <a href="#">user_ids_stats_current_timeframe</a> (5-30 ページ)                  | ユーザ別のアクセス コントロール アクティビティと侵入からの保護アクティビティ。                                  | 5.0+    |
| <a href="#">user_stats_current_timeframe</a> (5-31 ページ)                      | ユーザ別のトラフィック ボリュームとシステム アクセス コントロール アクティビティ (接続の許可また拒否)                    | 5.0+    |

## 統計情報追跡テーブルについて

テーブルの名前の末尾に、データの時間枠を示す `current_day`、`current_month`、または `current_year` が付きます。たとえば、`app_ids_stats_current_timeframe` は、`app_stats_current_day`、`app_stats_current_month`、および `app_stats_current_year` となります。`app_stats_current_year` テーブルには 360 日分の統計情報が格納され、`current_month` テーブルには 30 日分の統計情報が格納されます。

Firepower Management Center は、ネットワーク内の管理対象デバイスから未加工のカウンタを受信するたびに、3 種類のテーブルをすべて更新しますが、更新間隔は徐々に広がります。`current_day` テーブルの間隔が最も狭く (テーブルに応じて 15 秒または 5 分)、`current_year` テーブルでは間隔が最も広がります (24 時間)。詳細については、[統計情報追跡テーブルの保存特性](#) (5-3 ページ) を参照してください。

## 統計情報追跡テーブルの保存特性

重要な詳細について、次の表を参照してください。

表 5-2 統計情報テーブルの保存特性

| テーブルタイプ       | 間隔(精度)   | 保存期間                              |
|---------------|--|-----------------------------------|
| current_day   | 次のテーブルでは 15 秒:<br>app_ids_stats_current_timeframe および<br>user_ids_stats_current_timeframe  | 過去 24 時間のすべての間隔に、現在の<br>間隔を加算した期間 |
|               | 次のテーブルでは 5 分:<br>app_stats_current_timeframe、<br>user_stats_current_timeframe、<br>url_category_stats_current_timeframe、および<br>url_reputation_stats_current_timeframe | 過去 24 時間のすべての間隔に、現在の<br>間隔を加算した期間 |
| current_month | 1 時間   | 過去 30 日分の時間に現在の時間を加算<br>した期間      |
| current_year  | 24 時間  | 過去 360 日に当日を加算した期間                |

保存間隔はその開始時刻により定義されます。たとえば、**current\_month** テーブルには 10:00:00 ~ 10:59:59 までの間のカウントが、タイムスタンプが 10:00:00 の 1 つのレコードとして格納されます。1 日の開始時刻は 00:00:00、終了時刻は 23:59:59 であることに注意してください。間隔の開始時刻は UNIX タイムスタンプ (GMT) として保存されます。

## 統計情報テーブルの照会時の時間間隔の指定

クエリで有効な時間間隔は、テーブルと、クエリの `time_start_sec` フィールドの両方によって定義されます。

たとえば SQL ステートメントに `time_start_sec = 6:00:00` と指定されている場合、間隔はテーブルのタイプに応じて次のように異なります。

- **current\_day** テーブル: 6:00:00 ~ 6:00:14 (15 秒のテーブルの場合) または 6:00:00 ~ 6:04:59 (5 分のテーブルの場合)。
- **current\_month** テーブル: 6:00:00 ~ 6:59:59。
- **current\_year** テーブル: 0:00:00 ~ 翌日の 23:59:59。

データを取得する最も簡単な方法は、間隔の開始時刻を指定する方法です。たとえば **app\_ids\_stats\_current\_day** テーブルから取得する場合は、次のいずれかを指定します。

```
00:00:00
00:00:15
00:00:30
23:59:45
```

クエリに含まれているタイムスタンプが、間隔の開始時刻と異なる場合、システムでは要求が次のように変更されます。

- 開始時刻を最も近い間隔の時刻に繰り上げます。
- 終了時刻を最も近い間隔の時刻に繰り下げます。

たとえば次のクエリでは開始時刻が繰り上げられます。

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 12:30:00");
```

これは以下と同じです:

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec = UNIX_TIMESTAMP("2011-12-01 01:00:00");
```

複数の間隔からなる範囲でクエリを実行する場合は、間隔の開始時刻が繰り上げられ、終了時刻が繰り下げられます。次に例を示します。

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 12:59:00") and
UNIX_TIMESTAMP("2011-12-10 16:28:00");
```

これは次のように変更されます。

```
SELECT application_id
FROM app_ids_stats_current_month
WHERE start_time_sec BETWEEN UNIX_TIMESTAMP("2011-12-10 13:00:00") and
UNIX_TIMESTAMP("2011-12-12 16:00:00");
```

クエリ間隔がテーブルの時間枠を超えて延長される場合、通常は別のテーブルから追加データを取得できますが、その別のテーブルのデータの精度がより粗いことがあります。たとえば、過去2日間の帯域幅使用状況を取得するには、**current\_day** テーブル(精度は5分)から昨日分の結果を取得できますが、**current\_month**(時間単位)または **current\_year**(日単位)から昨日のみの統計情報を取得することもできます。

## app\_ids\_stats\_current\_timeframe

**app\_ids\_stats\_current\_timeframe** テーブルには、モニタ対象ネットワークのアプリケーションアクティビティと侵入イベントに関する統計情報が格納されます。統計情報は、検出されるアプリケーション、アプリケーションタイプ(アプリケーションプロトコル、クライアントアプリケーション、または Web アプリケーション)、およびアプリケーションのリスクとビジネスとの関連度に基づいて抽出できます。これらのテーブルでは、侵入ポリシー違反が原因でブロックされた接続と、推定される侵入の影響も追跡されます。

**current\_day**、**current\_month**、および **current\_year** 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

**app\_ids\_stats\_current\_timeframe** テーブルの詳細については、次に示す項を参照してください。

- **app\_ids\_stats\_current\_timeframe** のフィールド(5-5 ページ)
- **app\_ids\_stats\_current\_timeframe** の結合(5-6 ページ)
- **app\_ids\_stats\_current\_timeframe** のサンプルクエリ(5-6 ページ)

## app\_ids\_stats\_current\_timeframe のフィールド

次の表に、`app_ids_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-3 `app_ids_stats_current_timeframe` のフィールド

| フィールド                                       | 説明  |
|---|---|
| <code>application_id</code>                 | アプリケーションの内部識別番号。  |
| <code>application_name</code>               | 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。  |
| <code>blocked</code>                        | 侵入ポリシーの違反が原因でブロックされた接続の数。   |
| <code>business_relevance</code>             | 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。  |
| <code>business_relevance_description</code> | ビジネスとの関連度の説明 ( <code>very low</code> , <code>low</code> , <code>medium</code> , <code>high</code> , <code>very high</code> )。 |
| <code>domain_name</code>                    | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>                    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>impact_level_1</code>                 | アプリケーションについて記録された影響レベル 1(脆弱)の侵入イベントの数。  |
| <code>impact_level_2</code>                 | 影響レベル 2(脆弱な可能性あり)の侵入イベントの数。   |
| <code>impact_level_3</code>                 | 影響レベル 3(ホストは現在脆弱ではない)の侵入イベントの数  |
| <code>impact_level_4</code>                 | 影響レベル 4(ターゲットが不明)の侵入イベントの数。   |
| <code>impact_level_5</code>                 | 影響レベル 5(不明な脆弱性)の侵入イベントの数。   |
| <code>is_client_application</code>          | 検出されたアプリケーションがクライアントアプリケーションであるかどうかを示す <code>true/false</code> フラグ。   |
| <code>is_server_application</code>          | 検出されたアプリケーションがアプリケーションプロトコルであるかどうかを示す <code>true/false</code> フラグ。  |
| <code>is_web_application</code>             | 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 <code>true/false</code> フラグ。  |
| <code>netmap_num</code>                     | 統計情報が収集されたドメインの Netmap ID。  |
| <code>risk</code>                           | 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。  |
| <code>risk_description</code>               | 推定リスクの説明 ( <code>very low</code> , <code>low</code> , <code>medium</code> , <code>high</code> , <code>critical</code> )。      |
| <code>sensor_address</code>                 | 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 <code>ipv4_address</code> , <code>ipv6_address</code> です。                                      |
| <code>sensor_id</code>                      | イベントを提供したデバイスの ID。  |
| <code>sensor_name</code>                    | 侵入イベントを生成した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>                    | 管理対象デバイスの固有識別子( <code>sensor_name</code> が <code>null</code> の場合は 0)。   |
| <code>start_time_sec</code>                 | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定(5-3 ページ)</a> を参照してください。                                    |
| <code>would_have_dropped</code>             | 侵入ポリシーがインライン型展開でパケットをドロップするように設定されている場合にドロップされるパケットの数。  |

## app\_ids\_stats\_current\_timeframe の結合

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

表 5-4 `app_ids_stats_current_timeframe` 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      | <a href="#">application_info.application_id</a><br><a href="#">application_host_map.application_id</a><br><a href="#">application_tag_map.application_id</a><br><a href="#">rna_host_service_info.application_protocol_id</a><br><a href="#">rna_host_client_app_payload.web_application_id</a><br><a href="#">rna_host_client_app_payload.client_application_id</a><br><a href="#">rna_host_client_app.client_application_id</a><br><a href="#">rna_host_client_app.application_protocol_id</a><br><a href="#">rna_host_service_payload.web_application_id</a> |

## app\_ids\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、`app_ids_stats_current_month` テーブルから最大 25 件のアプリケーション レコードを返します。各レコードには、特定の時間間隔におけるアプリケーションのブロックされた接続数と侵入イベント数が含まれます。

```
SELECT from_unixtime(start_time_sec), sum(blocked)
FROM app_ids_stats_current_day
WHERE start_time_sec = unix_timestamp("2013-12-15");
```

## app\_stats\_current\_timeframe

`app_stats_current_timeframe` テーブルには、アプリケーション別、およびトラフィックをモニタするデバイス別の帯域幅使用状況とアクセス コントロール アクション(接続の許可または拒否)に関する統計情報が格納されます。これらの統計情報は、アプリケーションのビジネスとの関連度、推定リスク、およびタイプに基づいてフィルタリングできます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`app_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [app\\_stats\\_current\\_timeframe](#) のフィールド (5-7 ページ)
- [app\\_stats\\_current\\_timeframe](#) の結合 (5-8 ページ)
- [app\\_stats\\_current\\_timeframe](#) のサンプルクエリ (5-8 ページ)

## app\_stats\_current\_timeframe のフィールド

次の表に、`app_stats_current_timeframe` 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 5-5 `app_stats_current_timeframe` のフィールド

| フィールド                                       | 説明  |
|---|---|
| <code>application_id</code>                 | アプリケーションの内部識別番号。  |
| <code>application_name</code>               | 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。  |
| <code>business_relevance</code>             | 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。   |
| <code>business_relevance_description</code> | ビジネスとの関連度の説明 ( <code>very low</code> 、 <code>low</code> 、 <code>medium</code> 、 <code>high</code> 、 <code>very high</code> )。 |
| <code>bypass</code>                         | 遅延が原因でのバイパスが可能なパケットの数。  |
| <code>bytes_in</code>                       | 指定された期間中のアプリケーションの着信トラフィックのバイト数。  |
| <code>bytes_out</code>                      | 指定された期間中のアプリケーションの発信トラフィックのバイト数。  |
| <code>connections_allowed</code>            | 許可された接続の数。  |
| <code>connections_denied</code>             | アクセス コントロール ポリシーの違反が原因で拒否された接続の数。   |
| <code>domain_name</code>                    | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>                    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>is_client_application</code>          | 検出されたアプリケーションがクライアント アプリケーションであるかどうかを示す <code>true/false</code> フラグ。  |
| <code>is_server_application</code>          | 検出されたアプリケーションがアプリケーション プロトコルであるかどうかを示す <code>true/false</code> フラグ。   |
| <code>is_web_application</code>             | 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 <code>true/false</code> フラグ。  |
| <code>netmap_num</code>                     | 統計情報が収集されたドメインの Netmap ID。  |
| <code>qos_dropped_bytes_in</code>           | QoS によりドロップされた着信バイト数。   |
| <code>qos_dropped_bytes_out</code>          | QoS によりドロップされた発信バイト数。   |
| <code>risk</code>                           | 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。   |
| <code>risk_description</code>               | 推定リスクの説明 ( <code>very low</code> 、 <code>low</code> 、 <code>medium</code> 、 <code>high</code> 、 <code>critical</code> )。      |
| <code>sensor_address</code>                 | トラフィックをモニタしていた管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code> 、 <code>ipv6_address</code> です。                                 |
| <code>sensor_id</code>                      | トラフィックを検出した管理対象デバイスの内部識別番号。   |
| <code>sensor_name</code>                    | トラフィックを検出した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>                    | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が <code>null</code> の場合は 0)。  |
| <code>start_time_sec</code>                 | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。                             |
| <code>would_bypass</code>                   | バイパス対象であったが検査されたパケットの数。   |



## app\_stats\_current\_timeframe の結合

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

表 5-6 `app_stats_current_timeframe` の結合

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

## app\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、Firepower Management Center に接続しているすべての管理対象デバイスで、1 日間においてビジネスの関連度が低くリスクが高いアプリケーションに関連付けられている着信トラフィック ロードおよび発信トラフィック ロードを返します。

```
SELECT start_time_sec, sum(bytes_in), sum(bytes_out)
FROM app_stats_current_day
WHERE business_relevance <= 2
AND risk >= 4 AND start_time_sec = unix_timestamp("2013-12-15");
```

## compliance\_events\_stats\_current\_timeframe

`compliance_stats_events_current_timeframe` テーブルには、特定の時間枠におけるコンプライアンスおよびホワイトリスト イベントの数に関する統計情報が格納されます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`compliance_events_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [compliance\\_events\\_stats\\_current\\_timeframe のフィールド\(5-9 ページ\)](#)
- [compliance\\_event\\_stats\\_current\\_timeframe の結合\(5-9 ページ\)](#)
- [compliance\\_event\\_stats\\_current\\_timeframe のサンプルクエリ\(5-9 ページ\)](#)



## compliance\_events\_stats\_current\_timeframe のフィールド

次の表に、`compliance_events_stats_current_timeframe` 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 5-7 `compliance_events_stats_current_timeframe` のフィールド

| フィールド                          | 説明  |
|--------------------------------|---|
| <code>domain_name</code>       | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>       | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>netmap_num</code>        | 統計情報が収集されたドメインの Netmap ID。  |
| <code>priority_0_events</code> | 特定の時間枠内に検出されたプライオリティ 0 のイベント。   |
| <code>priority_1_events</code> | 特定の時間枠内に検出されたプライオリティ 1 のイベント。   |
| <code>priority_2_events</code> | 特定の時間枠内に検出されたプライオリティ 2 のイベント。   |
| <code>priority_3_events</code> | 特定の時間枠内に検出されたプライオリティ 3 のイベント。   |
| <code>priority_4_events</code> | 特定の時間枠内に検出されたプライオリティ 4 のイベント。   |
| <code>priority_5_events</code> | 特定の時間枠内に検出されたプライオリティ 5 のイベント。   |
| <code>rule</code>              | イベントをトリガーしたホワイトリストのルール。このルールが空の場合、イベントはコンプライアンス イベントです。   |
| <code>start_time_sec</code>    | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## compliance\_event\_stats\_current\_timeframe の結合

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

## compliance\_event\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、1 日間におけるプライオリティ 0、1、および 2 のイベントと、関連するホワイトリストルールを、ドメインを基準に並べ替えて返します。

```
SELECT domain_name, priority_0_events, priority_1_events, priority_2_events, rule
FROM compliance_event_stats_current_day
ORDER BY domain_name DESC;
```

## dns\_query\_stats\_current\_timeframe

`dns_query_stats_current_timeframe` テーブルには、DNS クエリの統計情報が格納されます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性 \(5-3 ページ\)](#) を参照してください。

`dns_query_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [dns\\_query\\_stats\\_current\\_timeframe](#) のフィールド (5-10 ページ)
- [dns\\_query\\_stats\\_current\\_timeframe](#) の結合 (5-10 ページ)
- [dns\\_query\\_stats\\_current\\_timeframe](#) のサンプルクエリ (5-10 ページ)

## dns\_query\_stats\_current\_timeframe のフィールド

次の表に、`dns_query_stats_current_timeframe` 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 5-8 `dns_query_stats_current_timeframe` のフィールド

| フィールド                            | 説明  |
|----------------------------------|---|
| <code>bytes_in</code>            | 指定された期間中の着信トラフィックのバイト数。   |
| <code>bytes_out</code>           | 指定された期間中の発信トラフィックのバイト数。   |
| <code>connections_allowed</code> | 指定された DNS クエリで許可された接続の数。  |
| <code>connections_denied</code>  | アクセス コントロール ポリシー違反が原因で、指定された DNS クエリで拒否された接続の数。   |
| <code>dns_record_type</code>     | DNS クエリで使用される DNS ルックアップのタイプ。   |
| <code>domain_name</code>         | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>         | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>sensor_address</code>      | トラフィックをモニタしていた管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code> , <code>ipv6_address</code> です。     |
| <code>sensor_id</code>           | トラフィックを検出した管理対象デバイスの内部識別番号。   |
| <code>sensor_name</code>         | トラフィックを検出した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>         | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が null の場合は 0)。   |
| <code>start_time_sec</code>      | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## dns\_query\_stats\_current\_timeframe の結合

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

## dns\_query\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、1 日間における各センサーの DNS レコード タイプに関連付けられている接続の数を、センサー名でソートし、ドメインを `Global \ Company B \ Edge` に限定して返します。

```
SELECT sensor_name, dns_record_type, sum(connections_allowed), sum(connections_denied)
FROM dns_query_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

## geolocation\_stats\_current\_timeframe

`geolocation_stats_timeframe` テーブルには、ロケーション レベルに基づく侵入イベントに関する統計情報が格納されます。統計情報は、影響レベル、デバイス、およびパケットの処理方法に基づいて抽出できます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`geolocation_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- `geolocation_stats_current_timeframe` のフィールド(5-11 ページ)
- `geolocation_stats_current_timeframe` の結合(5-12 ページ)
- `geolocation_stats_current_timeframe` のサンプル クエリ(5-13 ページ)

## geolocation\_stats\_current\_timeframe のフィールド

次の表に、`geolocation_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-9 `geolocation_stats_current_timeframe` のフィールド

| フィールド                              | 説明  |
|------------------------------------|---|
| <code>bytes_from</code>            | セッション レスポンダが送信した合計バイト数。   |
| <code>bytes_to</code>              | セッション イニシエータが送信した合計バイト数。  |
| <code>destination_continent</code> | 宛先ホストが位置する地域の名前<br>**: 不明<br>na: 北米<br>as: アジア<br>af: アフリカ<br>eu: 欧州<br>sa: 南米<br>au: オーストラリア<br>an: 南極 |
| <code>destination_country</code>   | 宛先ホストの国のコード。  |
| <code>domain_name</code>           | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>           | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>flows_allowed</code>         | 許可されたフローの数。   |
| <code>flows_denied</code>          | アクセス コントロール ポリシーの違反が原因で拒否されたフローの数。  |
| <code>netmap_num</code>            | 統計情報が収集されたドメインの Netmap ID。  |
| <code>sensor_address</code>        | 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> です。                |

表 5-9 geolocation\_stats\_current\_timeframe のフィールド(続き)

| フィールド            | 説明   |
|------------------|--|
| sensor_id        | イベントを提供したデバイスの ID。   |
| sensor_name      | 侵入イベントを生成した管理対象デバイスの名前。  |
| sensor_uuid      | 管理対象デバイスの固有識別子 (sensor_name が null の場合は 0)。  |
| source_continent | 送信元ホストが位置する地域の名前<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>an : 南極                     |
| source_country   | 送信元ホストの国のコード。  |
| start_time_sec   | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。  |
| xff_continent    | 接続にプロキシが存在する場合は、最初の送信元ホストが位置する地域の名前。<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>an : 南極 |
| xff_country      | 接続にプロキシが存在する場合は、最初の送信元ホストの国コード。  |

## geolocation\_stats\_current\_timeframe の結合

geolocation\_stats\_current\_timeframe テーブルに対して結合を実行することはできません。

## geolocation\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、当日における最初の 25 件のアジアからの接続イベントの送信元の国とセンサー名を、ドメインを Global \ Company B \ Edge に限定して返します。

```
SELECT sensor_name, source_continent
FROM geolocation_stats_current_year
WHERE destination_continent='as' and domain_name= "Global \ Company B \ Edge"
LIMIT 20;
```

## ids\_impact\_stats\_current\_timeframe

`ids_impact_stats_timeframe` テーブルには、影響レベルに基づく侵入イベントに関する統計情報が格納されます。統計情報は、影響レベル、デバイス、およびパケットの処理方法に基づいて抽出できます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`ids_impact_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [ids\\_impact\\_stats\\_current\\_timeframe のフィールド\(5-13 ページ\)](#)
- [ids\\_impact\\_stats\\_current\\_timeframe の結合\(5-14 ページ\)](#)
- [ids\\_impact\\_stats\\_current\\_timeframe のサンプルクエリ\(5-14 ページ\)](#)

## ids\_impact\_stats\_current\_timeframe のフィールド

次の表に、`ids_impact_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-10 `ids_impact_stats_current_timeframe` のフィールド

| フィールド                       | 説明   |
|-----------------------------|--|
| <code>blocked</code>        | 侵入ポリシーの違反が原因でブロックされた接続の数。  |
| <code>domain_name</code>    | 統計情報のために指定されたドメインの名前。  |
| <code>domain_uuid</code>    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。   |
| <code>impact_level_1</code> | アプリケーションについて記録された影響レベル 1(脆弱)の侵入イベントの数。   |
| <code>impact_level_2</code> | 影響レベル 2(脆弱な可能性あり)の侵入イベントの数。  |
| <code>impact_level_3</code> | 影響レベル 3(ホストは現在脆弱ではない)の侵入イベントの数   |
| <code>impact_level_4</code> | 影響レベル 4(ターゲットが不明)の侵入イベントの数。  |
| <code>impact_level_5</code> | 影響レベル 5(不明な脆弱性)の侵入イベントの数。  |
| <code>netmap_num</code>     | 統計情報が収集されたドメインの Netmap ID。   |
| <code>sensor_address</code> | 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> です。 |

表 5-10 ids\_impact\_stats\_current\_timeframe のフィールド(続き)

| フィールド              | 説明  |
|--------------------|---|
| sensor_id          | イベントを提供したデバイスの ID。  |
| sensor_name        | 侵入イベントを生成した管理対象デバイスの名前。   |
| sensor_uuid        | 管理対象デバイスの固有識別子 (sensor_name が null の場合は 0)。   |
| start_time_sec     | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |
| would_have_dropped | 侵入ポリシーがインライン型展開でパケットをドロップするように設定されている場合にドロップされるパケットの数。                                      |

## ids\_impact\_stats\_current\_timeframe の結合

ids\_impact\_stats\_current\_timeframe テーブルに対して結合を実行することはできません。

## ids\_impact\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、当日における最初の 25 件の blocked イベントと would\_have\_dropped イベントを、ドメインを Global \ Company B \ Edge に限定して返します。

```
SELECT blocked, would_have_dropped
FROM ids_impact_stats_current_year
WHERE domain_name= "Global \ Company B \ Edge"
LIMIT 25;
```

## interface\_stats\_current\_timeframe

Interface\_stats\_current\_timeframe テーブルには、特定のインターフェイスに関する統計情報が含まれます。

current\_day、current\_month、および current\_year 統計情報テーブルについては、[統計情報追跡テーブルの保存特性 \(5-3 ページ\)](#) を参照してください。

interface\_stats\_current\_timeframe テーブルの詳細については、次に示すセクションを参照してください。

- [interface\\_stats\\_current\\_timeframe フィールド \(5-15 ページ\)](#)
- [interface\\_stats\\_current\\_timeframe 結合 \(5-15 ページ\)](#)
- [interface\\_stats\\_current\\_timeframe サンプルクエリ \(5-15 ページ\)](#)

## interface\_stats\_current\_timeframe フィールド

次の表で、`interface_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-11 `interface_stats_current_timeframe` フィールド

| フィールド                                  | 説明  |
|--|---|
| <code>connections_allowed</code>       | 許可された接続の数。  |
| <code>connections_denied</code>        | 侵入ポリシーの違反が原因でブロックされた接続の数。   |
| <code>domain_name</code>               | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>               | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>egress_bytes</code>              | 出力バイト数。   |
| <code>ingress_bytes</code>             | 入力バイト数。   |
| <code>interface_name</code>            | インターフェイスの名前。  |
| <code>interface_uuid</code>            | インターフェイスの UUID。   |
| <code>netmap_num</code>                | 統計情報が収集されたドメインの Netmap ID。  |
| <code>qos_dropped_egress_bytes</code>  | QoS によりドロップされた出力バイト数。   |
| <code>qos_dropped_ingress_bytes</code> | QoS によりドロップされた入力バイト数。   |
| <code>sensor_address</code>            | 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> です。    |
| <code>sensor_id</code>                 | イベントを提供したデバイスの ID。  |
| <code>sensor_name</code>               | 侵入イベントを生成した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>               | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が <code>null</code> の場合は 0)。                      |
| <code>start_time_sec</code>            | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## interface\_stats\_current\_timeframe 結合

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

## interface\_stats\_current\_timeframe サンプルクエリ

次のクエリは、当日における最初の 25 件の `blocked` イベントと `would_have_dropped` イベントを、ドメインを `Global \ Company B \ Edge` に限定して返します。

```
SELECT blocked, would_have_dropped
FROM ids_impact_stats_current_year
WHERE domain_name= "Global \ Company B \ Edge"
LIMIT 25;
```

## ip\_reputation\_stats\_current\_timeframe

`ip_category_stats_current_timeframe` テーブルには、指定されたセキュリティ インテリジェンス カテゴリの IP アドレス、URL、および DNS ドメインへの要求に関連付けられている帯域幅使用状況と接続に関する統計情報が格納されます。クエリの対象を、トラフィックをモニタしていた管理対象デバイスに制限することもできます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`ids_impact_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- `ip_reputation_stats_current_timeframe` のフィールド(5-16 ページ)
- `ip_reputation_stats_current_timeframe` の結合(5-17 ページ)
- `ip_reputation_stats_current_timeframe` のサンプル クエリ(5-17 ページ)

## ip\_reputation\_stats\_current\_timeframe のフィールド

次の表に、`ip_reputation_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-12 `ip_reputation_stats_current_timeframe` のフィールド

| フィールド                            | 説明   |
|----------------------------------|--|
| <code>bytes_in</code>            | 指定された期間中の着信トラフィックのバイト数。  |
| <code>bytes_out</code>           | 指定された期間中の発信トラフィックのバイト数。  |
| <code>connections_allowed</code> | 指定された IP で許可された接続の数。   |
| <code>connections_denied</code>  | アクセス コントロール ポリシー違反が原因で、指定された IP で拒否された接続の数。  |
| <code>domain_name</code>         | 統計情報のために指定されたドメインの名前。  |
| <code>domain_uuid</code>         | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。   |
| <code>name</code>                | セキュリティ インテリジェンスの名前(例:「URL Malware」)。   |
| <code>sensor_address</code>      | 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> です。                           |
| <code>sensor_id</code>           | イベントを提供したデバイスの ID。   |
| <code>sensor_name</code>         | 侵入イベントを生成した管理対象デバイスの名前。  |
| <code>sensor_uuid</code>         | 管理対象デバイスの固有識別子( <code>sensor_name</code> が <code>null</code> の場合は 0)。  |
| <code>start_time_sec</code>      | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定(5-3 ページ)</a> を参照してください。                         |
| <code>type</code>                | エントリの情報のタイプ。有効な値は次のとおりです。<br>0: ネットワーク インテリジェンス統計情報。<br>1: DNS セキュリティ インテリジェンス統計情報。<br>2: URL セキュリティ インテリジェンス統計情報。 |



## ip\_reputation\_stats\_current\_timeframe の結合

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

## ip\_reputation\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、当日における最初の 25 件の接続(受信バイト数と送信バイト数、接続数、接続のタイプ、およびセンサーを表示)を、ドメインを Global \ Company B \ Edge に限定し、ドメインを基準に並べ替えて返します。

```
SELECT uuid_btoa(domain_uuid), domain_name, type, name, bytes_in, bytes_out,
connections_allowed, connections_denied, sensor_name
FROM ip_reputation_stats_current_day
ORDER BY domain_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
LIMIT 25;
```

## qos\_rule\_stats\_current\_timeframe

`Qos_rule_stats_current_timeframe` テーブルには、トリガーされるサービス ルールの品質と適用方法に関する統計情報が含まれています。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性 \(5-3 ページ\)](#) を参照してください。

`qos_rules_stats_current_timeframe` テーブルの詳細については、次に示すセクションを参照してください。

- [qos\\_rule\\_stats\\_current\\_timeframe フィールド \(5-17 ページ\)](#)
- [qos\\_rule\\_stats\\_current\\_timeframe 結合 \(5-18 ページ\)](#)
- [qos\\_rule\\_stats\\_current\\_timeframe サンプルクエリ \(5-18 ページ\)](#)

## qos\_rule\_stats\_current\_timeframe フィールド

次の表で、`qos_rule_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-13 `qos_rule_stats_current_timeframe` フィールド

| フィールド                        | 説明                                     |
|------------------------------|--|
| <code>deploy_revision</code> | QoS ポリシーのリビジョン UUID。                   |
| <code>domain_name</code>     | 統計情報のために指定されたドメインの名前。                  |
| <code>domain_uuid</code>     | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。 |
| <code>netmap_num</code>      | 統計情報が収集されたドメインの Netmap ID。             |

表 5-13 qos\_rule\_stats\_current\_timeframe フィールド(続き)

| フィールド                 | 説明  |
|-----------------------|---|
| qos_dropped_bytes_in  | QoS によりドロップされた着信バイト数。   |
| qos_dropped_bytes_out | QoS によりドロップされた発信バイト数。   |
| qos_policy_id         | QoS ポリシーの UUID。   |
| qos_policy_name       | QoS ポリシーの名前。  |
| qos_rule_id           | QoS ルールの整数の ID。   |
| qos_rule_name         | QoS ルールの名前。   |
| 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 <i>ipv4_address, ipv6_address</i> です。                        |
| sensor_id             | イベントを提供したデバイスの ID。  |
| sensor_name           | イベントを生成した管理対象デバイスの名前。   |
| sensor_uuid           | 管理対象デバイスの固有識別子 ( <i>sensor_name</i> が null の場合は 0)。   |
| start_time_sec        | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## qos\_rule\_stats\_current\_timeframe 結合

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

## qos\_rule\_stats\_current\_timeframe サンプルクエリ

次のクエリは、当日における QoS ルール、QoS ポリシー名、QoS ルール名、およびセンサー名でドロップされた発着信バイト数を、センサー名の降順で、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT qos_dropped_bytes_in, qos_dropped_bytes_in, qos_policy_name, qos_rule_name,
sensor_name
FROM qos_rule_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

## session\_stats\_current\_timeframe

`session_stats_timeframe` テーブルには、すべての接続の統計情報が格納されます。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性 \(5-3 ページ\)](#) を参照してください。

`session_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [session\\_stats\\_current\\_timeframe](#) のフィールド (5-19 ページ)
- [session\\_stats\\_current\\_timeframe](#) の結合 (5-19 ページ)
- [session\\_stats\\_current\\_timeframe](#) のサンプルクエリ (5-19 ページ)

## session\_stats\_current\_timeframe のフィールド

次の表に、`session_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-14 `session_stats_current_timeframe` のフィールド

| フィールド                            | 説明  |
|----------------------------------|---|
| <code>bytes_in</code>            | 指定された期間中の着信トラフィックのバイト数。   |
| <code>bytes_out</code>           | 指定された期間中の発信トラフィックのバイト数。   |
| <code>connections_allowed</code> | 指定された URL カテゴリで許可された接続の数。   |
| <code>connections_denied</code>  | アクセス コントロール ポリシー違反が原因で、指定された URL カテゴリで拒否された接続の数。  |
| <code>domain_name</code>         | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>         | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>id</code>                  | このフィールドは使用されず、常に 0 を返します。   |
| <code>sensor_address</code>      | 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> です。    |
| <code>sensor_id</code>           | イベントを提供したデバイスの ID。  |
| <code>sensor_name</code>         | 侵入イベントを生成した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>         | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が null の場合は 0)。                                   |
| <code>start_time_sec</code>      | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## session\_stats\_current\_timeframe の結合

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

## session\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、当日における各センサーで拒否された接続と許可された接続の数を、`sensor_name` の降順で、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT sensor_name, sensor_id connections_denied, connections_allowed
FROM session_stats_current_day
ORDER BY sensor_name DESC
WHERE domain_name= "Global \ Company B \ Edge";
```

## ssl\_stats\_current\_timeframe

`ssl_stats_current_timeframe` テーブルには、SSL 接続の統計情報が格納されます。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`ssl_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [ssl\\_stats\\_current\\_timeframe のフィールド\(5-20 ページ\)](#)
- [ssl\\_stats\\_current\\_timeframe の結合\(5-22 ページ\)](#)
- [ssl\\_stats\\_current\\_timeframe のサンプルクエリ\(5-22 ページ\)](#)

## ssl\_stats\_current\_timeframe のフィールド

次の表に、`ssl_stats_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-15 `ssl_stats_current_timeframe` のフィールド

| フィールド  | 説明  |
|--|---|
| <code>block</code>                                       | リセットなしでドロップされた SSL セッションの数。                             |
| <code>block_with_reset</code>                            | リセットありでドロップされた SSL セッションの数。                             |
| <code>cached_session</code>                              | セッション キャッシュ内で見つかった SSL セッションの数。                         |
| <code>cannot_determine_verdict</code>                    | SSL ルールの評価中に発生したハンドシェイク エラーの数。                          |
| <code>cert_expired</code>                                | 証明書が期限切れであった SSL セッションの数。                               |
| <code>cert_invalid_issuer</code>                         | 証明書発行元が無効であったか、または Trusted CA リストで見つからなかった SSL セッションの数。 |
| <code>cert_invalid_signature</code>                      | 証明書に無効なシグニチャが含まれていた SSL セッションの数。                        |
| <code>cert_not_checked</code>                            | 証明書が検査されなかった SSL セッションの数。                               |
| <code>cert_not_yet_valid</code>                          | 証明書が有効ではなかった SSL セッションの数。                               |
| <code>cert_revoked</code>                                | 証明書が失効していた SSL セッションの数。                                 |
| <code>cert_self_signed</code>                            | 証明書が自己署名されていた SSL セッションの数。                              |
| <code>cert_unknown</code>                                | 証明書ステータスが不明だった SSL セッションの数。                             |
| <code>cert_valid</code>                                  | 証明書が有効だった SSL セッションの数。                                  |
| <code>cert_validation_cache_hit</code>                   | 証明書が検証キャッシュ内で見つかった回数。                                   |
| <code>cert_validation_cache_miss</code>                  | 証明書が検証キャッシュ内で見つからなかった回数。                                |
| <code>decrypt_resign_self_signed</code>                  | 自己署名証明書を使用する SSL セッションが復号化/再署名方式を使用して復号化された回数。          |
| <code>decrypt_resign_self_signed_replace_key_only</code> | 自己署名証明書を使用する SSL セッションが、キー置換のみの複合化/再署名方式を使用して復号化された回数。  |
| <code>decrypt_resign_signed_cert</code>                  | 自己署名証明書を使用する SSL セッションが復号化/再署名方式を使用して復号化された回数。          |
| <code>decrypt_with_known_key</code>                      | SSL セッションが既知のキー方式を使用して復号化された回数。                         |

表 5-15 ssl\_stats\_current\_timeframe のフィールド(続き)

| フィールド                                 | 説明  |
|---------------------------------------|---|
| decryption_error                      | 復号化中にエラーが発生した SSL セッションの数。  |
| domain_name                           | 統計情報のために指定されたドメインの名前。   |
| domain_uuid                           | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| do_not_decrypt                        | SSL セッションが検出されたが復号化されなかった回数。  |
| handshake_error                       | SSL ルールの評価前に発生したハンドシェイク エラーの数。  |
| netmap_num                            | 統計情報が収集されたドメインの Netmap ID。  |
| orig_cert_cache_hit                   | 元の証明書がキャッシュ内で見つかった回数。   |
| orig_cert_cache_miss                  | 元の証明書がキャッシュ内で見つからなかった回数。  |
| resigned_cert_cache_hit               | 再署名証明書がキャッシュ内で見つかった回数。  |
| resigned_cert_cache_miss              | 再署名証明書がキャッシュ内で見つからなかった回数。   |
| 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 <i>ipv4_address</i> , <i>ipv6_address</i> です。                |
| sensor_id                             | イベントを提供したデバイスの ID。  |
| sensor_name                           | イベントを生成した管理対象デバイスの名前。   |
| sensor_uuid                           | 管理対象デバイスの固有識別子 ( <i>sensor_name</i> が null の場合は 0)。   |
| session_cache_hit                     | SSL セッション ID またはチケットがキャッシュで見つかった回数。   |
| session_cache_miss                    | SSL セッション ID またはチケットがキャッシュで見つからなかった回数。  |
| session_incorrectly_identified_as_ssl | SSL を使用するものとして誤って指定されていたセッションの数。  |
| ssl_compression                       | SSL 圧縮を使用したセッションの数。   |
| ssl_sessions_decrypted                | 正常に復号化された SSL セッションの数。  |
| ssl_sessions_not_decrypted            | 正常に復号化されなかった SSL セッションの数。   |
| ssl_sessions_reused_by_id             | SSL セッションが ID を再利用した回数。   |
| ssl_sessions_reused_by_ticket         | SSL セッションがチケットを再利用した回数。   |
| ssl_sessions_with_errors              | エラーが発生した SSL セッションの数。   |
| ssl_v20                               | SSL バージョン 2.0 を使用する SSL セッションの数。  |
| ssl_v30                               | SSL バージョン 3.0 を使用する SSL セッションの数。  |
| ssl_version_unknown                   | 不明なバージョンの SSL を使用する SSL セッションの数。  |
| start_time_sec                        | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |
| tls_v10                               | TLS バージョン 1.0 を使用する SSL セッションの数。  |
| tls_v11                               | TLS バージョン 1.1 を使用する SSL セッションの数。  |
| tls_v12                               | TLS バージョン 1.2 を使用する SSL セッションの数。  |
| total_ssl_sessions                    | 検出された SSL セッションの総数。   |
| uncached_session                      | ID またはチケットのキャッシュ ミスにより復号化できなかった回数。  |

表 5-15 ssl\_stats\_current\_timeframe のフィールド(続き)

| フィールド                         | 説明                                       |
|-------------------------------|--|
| undecryptable_in_passive_mode | デバイスがパッシブモードであるために復号化できなかった SSL セッションの数。 |
| unknown_cipher_suite          | 不明な暗号スイートを使用する SSL セッションの数。              |
| unsupported_cipher_suite      | 既知であるがサポートされていない暗号スイートを使用する SSL セッションの数。 |

## ssl\_stats\_current\_timeframe の結合

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

## ssl\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、当日における各センサーの SSL セッションの数、復号化されたセッションの数、復号化されなかったセッションの数、パッシブモードで復号化できなかったセッションの数を、`sensor_name` の降順で、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT sensor_name, total_ssl_sessions, ssl_sessions_decrypted,
ssl_sessions_not_decrypted, undecryptable_in_passive_mode
FROM ssl_stats_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

## storage\_stats\_by\_disposition\_current\_timeframe

`storage_stats_by_disposition_timeframe` テーブルには、保存ファイルの統計情報が格納されません。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`storage_stats_by_disposition_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [storage\\_stats\\_by\\_disposition\\_current\\_timeframe のフィールド\(5-23 ページ\)](#)
- [storage\\_stats\\_by\\_disposition\\_current\\_timeframe の結合\(5-23 ページ\)](#)
- [storage\\_stats\\_by\\_disposition\\_current\\_timeframe のサンプルクエリ\(5-24 ページ\)](#)

## storage\_stats\_by\_disposition\_current\_timeframe のフィールド

次の表に、`storage_stats_by_disposition_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-16 `storage_stats_by_disposition_current_timeframe` のフィールド

| フィールド                       | 説明   |
|-----------------------------|--|
| <code>bytes_written</code>  | ファイルのサイズ(バイト単位)。   |
| <code>disposition</code>    | ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• CLEAN: ファイルはクリーンであり、マルウェアが含まれていない。</li> <li>• UNKNOWN: ファイルにマルウェアが含まれているかどうか不明である。</li> <li>• MALWARE: ファイルにマルウェアが含まれている。</li> <li>• UNAVAILABLE: ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しなかった。</li> <li>• CUSTOM SIGNATURE: ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理された。</li> </ul> |
| <code>domain_name</code>    | 統計情報のために指定されたドメインの名前。  |
| <code>domain_uuid</code>    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。   |
| <code>netmap_num</code>     | 統計情報が収集されたドメインの Netmap ID。   |
| <code>number_dropped</code> | ドロップされたこの特性のファイルの数。  |
| <code>number_stored</code>  | 保存されたこの特性のファイルの数。  |
| <code>sensor</code>         | ファイルを検出したデバイスの ID。   |
| <code>sensor_address</code> | 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 <code>ipv4_address, ipv6_address</code> です。   |
| <code>sensor_name</code>    | 侵入イベントを生成した管理対象デバイスの名前。  |
| <code>sensor_uuid</code>    | 管理対象デバイスの固有識別子( <code>sensor_name</code> が null の場合は 0)。   |
| <code>start_time_sec</code> | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定(5-3 ページ)</a> を参照してください。   |

## storage\_stats\_by\_disposition\_current\_timeframe の結合

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



## storage\_stats\_by\_disposition\_current\_timeframe のサンプルクエリ

次のクエリは、当日における各センサーでドロップされたファイルの数と保存されたファイルの数を、sensor\_name の降順で、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT sensor_name, number_dropped, number_stored
FROM storage_stats_by_disposition_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY sensor_name DESC;
```

## storage\_stats\_by\_file\_type\_current\_timeframe

**storage\_stats\_by\_file\_type\_current\_timeframe** テーブルには、ファイルタイプ別の保存ファイルの統計情報が格納されます。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。

**current\_day**、**current\_month**、および **current\_year** 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

**storage\_stats\_by\_file\_type\_current\_timeframe** テーブルの詳細については、次に示す項を参照してください。

- [storage\\_stats\\_by\\_file\\_type\\_current\\_timeframe のフィールド\(5-24 ページ\)](#)
- [storage\\_stats\\_by\\_file\\_type\\_current\\_timeframe の結合\(5-25 ページ\)](#)
- [storage\\_stats\\_by\\_file\\_type\\_current\\_timeframe のサンプルクエリ\(5-25 ページ\)](#)

## storage\_stats\_by\_file\_type\_current\_timeframe のフィールド

次の表に、**storage\_stats\_by\_file\_type\_current\_timeframe** 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-17 **storage\_stats\_by\_file\_type\_current\_timeframe** のフィールド

| フィールド          | 説明   |
|----------------|--|
| bytes_written  | ファイルのサイズ(バイト単位)。   |
| domain_name    | 統計情報のために指定されたドメインの名前。  |
| domain_uuid    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。                                       |
| file_type      | 検出または検疫されたファイルのファイルタイプ。  |
| file_type_id   | ファイルタイプにマップされている ID 番号。  |
| netmap_num     | 統計情報が収集されたドメインの Netmap ID。   |
| number_dropped | ドロップされたこのタイプのファイルの数。   |
| number_stored  | 保存されたこのタイプのファイルの数。   |
| sensor         | ファイルを検出したデバイスの ID。   |
| 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 <i>ipv4_address</i> 、 <i>ipv6_address</i> です。 |



表 5-17 storage\_stats\_by\_file\_type\_current\_timeframe のフィールド(続き)

| フィールド          | 説明  |
|----------------|---|
| sensor_name    | 侵入イベントを生成した管理対象デバイスの名前。   |
| sensor_uuid    | 管理対象デバイスの固有識別子(sensor_name が null の場合は 0)。  |
| start_time_sec | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## storage\_stats\_by\_file\_type\_current\_timeframe の結合

session\_stats\_current\_timeframe テーブルに対して結合を実行することはできません。

## storage\_stats\_by\_file\_type\_current\_timeframe のサンプルクエリ

次のクエリは、当日における各センサーでドロップされたファイルの数と保存されたファイルの数を、file\_type の降順で、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT sensor_name, number_dropped, number_stored, file_type
FROM storage_stats_by_file_type_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY file_type DESC;
```

## transmission\_stats\_by\_file\_type\_current\_timeframe

transmission\_stats\_by\_file\_type\_current\_timeframe テーブルには、ファイルタイプ別の保存ファイルの統計情報が格納されます。統計情報は、バイト数、接続、センサー、および時刻に基づいて抽出できます。

current\_day、current\_month、および current\_year 統計情報テーブルについては、[統計情報追跡テーブルの保存特性 \(5-3 ページ\)](#) を参照してください。

transmission\_stats\_by\_file\_type\_current\_timeframe テーブルの詳細については、次に示す項を参照してください。

- [transmission\\_stats\\_by\\_file\\_type\\_current\\_timeframe のフィールド \(5-26 ページ\)](#)
- [transmission\\_stats\\_by\\_file\\_type\\_current\\_timeframe の結合 \(5-26 ページ\)](#)
- [transmission\\_stats\\_by\\_file\\_type\\_current\\_timeframe のサンプルクエリ \(5-26 ページ\)](#)

## transmission\_stats\_by\_file\_type\_current\_timeframe のフィールド

次の表に、`transmission_stats_by_file_type_current_timeframe` 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。このタイプのすべてのテーブルには同じフィールドが含まれています。

表 5-18 `transmission_stats_by_file_type_current_timeframe` のフィールド

| フィールド                       | 説明  |
|-----------------------------|---|
| <code>bytes_sent</code>     | 送信バイト数。   |
| <code>domain_name</code>    | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>file_type</code>      | 検出または検疫されたファイルのファイルタイプ。   |
| <code>file_type_id</code>   | ファイルタイプにマップされている ID 番号。   |
| <code>netmap_num</code>     | 統計情報が収集されたドメインの Netmap ID。  |
| <code>number_dropped</code> | ドロップされたこのタイプのファイルの数。  |
| <code>number_sent</code>    | 送信されたこのタイプのファイルの数。  |
| <code>sensor</code>         | ファイルを検出したデバイスの ID。  |
| <code>sensor_address</code> | 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 <code>ipv4_address, ipv6_address</code> です。                  |
| <code>sensor_name</code>    | 侵入イベントを生成した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>    | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が null の場合は 0)。                                   |
| <code>start_time_sec</code> | 測定間隔開始日時を示す UNIX タイムスタンプ。詳細については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |

## transmission\_stats\_by\_file\_type\_current\_timeframe の結合

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

## transmission\_stats\_by\_file\_type\_current\_timeframe のサンプルクエリ

次のクエリは、当日における各センサーでドロップされた接続の数と送信された接続の数を、`file_type` の降順で、Global \ Company B \ Edge ドメインに限定して返します。

```
SELECT sensor_name, number_dropped, number_sent, file_type
FROM transmission_stats_by_file_type_current_day
WHERE domain_name= "Global \ Company B \ Edge"
ORDER BY file_type DESC;
```

## url\_category\_stats\_current\_timeframe

`url_category_stats_current_timeframe` テーブルには、指定された URL カテゴリの URL に対する要求に関連付けられている帯域幅使用状況と接続に関する統計情報が格納されます。クエリの対象を、トラフィックをモニタしていた管理対象デバイスに制限することもできます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`url_category_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [url\\_category\\_stats\\_current\\_timeframe のフィールド\(5-27 ページ\)](#)
- [url\\_category\\_stats\\_current\\_timeframe の結合\(5-28 ページ\)](#)
- [url\\_category\\_stats\\_current\\_timeframe のサンプルクエリ\(5-28 ページ\)](#)

## url\_category\_stats\_current\_timeframe のフィールド

次の表に、`url_category_stats_current_timeframe` 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 5-19 `url_category_stats_current_timeframe` のフィールド

| フィールド                            | 説明   |
|----------------------------------|--|
| <code>bytes_in</code>            | 指定された期間中の着信トラフィックのバイト数。  |
| <code>bytes_out</code>           | 指定された期間中の発信トラフィックのバイト数。  |
| <code>category</code>            | URL のカテゴリ。   |
| <code>connections_allowed</code> | 指定された URL カテゴリで許可された接続の数。  |
| <code>connections_denied</code>  | アクセスコントロールポリシー違反が原因で、指定された URL カテゴリで拒否された接続の数。   |
| <code>domain_name</code>         | 統計情報のために指定されたドメインの名前。  |
| <code>domain_uuid</code>         | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。   |
| <code>netmap_num</code>          | 統計情報が収集されたドメインの Netmap ID。   |
| <code>sensor_address</code>      | トラフィックをモニタしていた管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code> 、 <code>ipv6_address</code> です。    |
| <code>sensor_id</code>           | トラフィックを検出した管理対象デバイスの内部識別番号。  |
| <code>sensor_name</code>         | トラフィックをモニタする管理対象デバイス。  |
| <code>sensor_uuid</code>         | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が <code>null</code> の場合は 0)。                           |
| <code>start_time_sec</code>      | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定(5-3 ページ)</a> を参照してください。 |

## url\_category\_stats\_current\_timeframe の結合

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

## url\_category\_stats\_current\_timeframe のサンプルクエリ

次のクエリは最大 25 件の URL カテゴリ レコードを返します。各レコードには、指定された間隔における関連する着信トラフィックと発信トラフィックのバイト数、および許可された接続と拒否された接続が含まれています。このクエリは Games カテゴリと Global \ Company B \ Edge ドメインに限定されます。

```
SELECT category, sensor_name, sensor_address, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied
FROM url_category_stats_current_year
WHERE category="Games" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```

## url\_reputation\_stats\_current\_timeframe

`url_reputation_stats_current_timeframe` テーブルには、指定されたレピュテーションの URL に対する要求に関連付けられている帯域幅使用状況と接続に関する統計情報が格納されます。クエリ結果を、トラフィックをモニタしていた管理対象デバイスに制限することもできます。

`current_day`、`current_month`、および `current_year` 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

`url_reputation_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- [url\\_reputation\\_stats\\_current\\_timeframe のフィールド\(5-28 ページ\)](#)
- [url\\_reputation\\_stats\\_current\\_timeframe の結合\(5-29 ページ\)](#)
- [url\\_reputation\\_stats\\_current\\_timeframe のサンプルクエリ\(5-29 ページ\)](#)

## url\_reputation\_stats\_current\_timeframe のフィールド

次の表に、`url_reputation_stats_current_timeframe` 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 5-20 `url_reputation_stats_current_timeframe` のフィールド

| フィールド                            | 説明                                |
|----------------------------------|-----------------------------------|
| <code>bytes_in</code>            | 指定された期間中の着信トラフィックのバイト数。           |
| <code>bytes_out</code>           | 指定された期間中の発信トラフィックのバイト数。           |
| <code>connections_allowed</code> | 許可された接続の数。                        |
| <code>connections_denied</code>  | アクセス コントロール ポリシーの違反が原因で拒否された接続の数。 |
| <code>domain_name</code>         | 統計情報のために指定されたドメインの名前。             |

表 5-20 url\_reputation\_stats\_current\_timeframe のフィールド(続き)

| フィールド          | 説明  |
|----------------|---|
| domain_uuid    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| netmap_num     | 統計情報が収集されたドメインの Netmap ID。  |
| reputation     | 要求された URL に関連付けられているリスク。次のいずれかが必要です。 <ul style="list-style-type: none"> <li>• High risk</li> <li>• Suspicious site</li> <li>• Benign site with security risks</li> <li>• Benign site</li> <li>• Well known</li> <li>• Risk unknown</li> </ul> |
| sensor_address | トラフィックをモニタしていた管理対象デバイスの IP アドレス。形式は <i>ipv4_address, ipv6_address</i> です。   |
| sensor_id      | トラフィックをモニタしていた管理対象デバイスの内部識別番号。  |
| sensor_name    | トラフィックをモニタしてい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 ( <i>sensor_name</i> が null の場合は 0)。   |
| start_time_sec | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。   |

## url\_reputation\_stats\_current\_timeframe の結合

url\_reputation\_stats\_current\_timeframe テーブルに対して結合を実行することはできません。

## url\_reputation\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、url\_reputation\_stats\_current\_month テーブルから最大 25 件の URL レピュテーション レコードを返します。各レコードには、測定間隔中の着信トラフィックと発信トラフィックのバイト数、および許可された接続と拒否された接続が含まれています。このクエリは High risk レピュテーションと Global \ Company B \ Edge ドメインに限定されます。

```
SELECT sensor_name, sensor_address, reputation, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied
FROM url_reputation_stats_current_year
WHERE reputation="High risk" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```

## user\_ids\_stats\_current\_timeframe

`user_ids_stats_current_timeframe` テーブルは、ユーザ別のアクセス フィルタリングの統計情報と影響の統計情報が格納されるラウンドロビンテーブルです。

このタイプの `current_day`、`current_month`、および `current_year` テーブルについては、[統計情報追跡テーブルの保存特性 \(5-3 ページ\)](#) を参照してください。

ラウンドロビン統計情報テーブルの使用法については、[統計情報追跡テーブルについて \(5-2 ページ\)](#) を参照してください。

`user_ids_stats_current_timeframe` テーブルの詳細については、次に示す項を参照してください。

- `user_ids_stats_current_timeframe` のフィールド (5-30 ページ)
- `user_ids_stats_current_timeframe` の結合 (5-31 ページ)
- `user_ids_stats_current_timeframe` のサンプルクエリ (5-31 ページ)

## user\_ids\_stats\_current\_timeframe のフィールド

次の表に、`user_ids_stats_current_timeframe` 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 5-21 `user_ids_stats_current_timeframe` のフィールド

| フィールド                       | 説明  |
|-----------------------------|---|
| <code>blocked</code>        | 侵入ポリシーの違反が原因でブロックされた接続の数。   |
| <code>domain_name</code>    | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>    | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>impact_level_1</code> | ユーザについて記録された影響レベル 1 (脆弱) の侵入イベントの数。   |
| <code>impact_level_2</code> | ユーザについて記録された影響レベル 2 (脆弱な可能性あり) の侵入イベントの数。   |
| <code>impact_level_3</code> | ユーザについて記録された影響レベル 3 (ホストは現在脆弱ではない) の侵入イベントの数。   |
| <code>impact_level_4</code> | ユーザについて記録された影響レベル 4 (不明なターゲット) の侵入イベントの数。   |
| <code>impact_level_5</code> | ユーザについて記録された影響レベル 5 (不明な脆弱性) の侵入イベントの数。   |
| <code>netmap_num</code>     | 統計情報が収集されたドメインの Netmap ID。  |
| <code>sensor_address</code> | トラフィックをモニタしていた管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code> 、 <code>ipv6_address</code> です。     |
| <code>sensor_id</code>      | トラフィックを検出した管理対象デバイスの内部識別番号。   |
| <code>sensor_name</code>    | トラフィックを検出した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>    | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が null の場合は 0)。   |
| <code>start_time_sec</code> | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |
| <code>user_id</code>        | ホストの最終ログインユーザの内部識別番号。   |

表 5-21 user\_ids\_stats\_current\_timeframe のフィールド(続き)

| フィールド              | 説明   |
|--------------------|--|
| username           | ホストの最終ログイン ユーザのユーザ名。                                   |
| would_have_dropped | 侵入ポリシーがインライン型展開でパケットをドロップするように設定されている場合にドロップされるパケットの数。 |

## user\_ids\_stats\_current\_timeframe の結合

user\_ids\_stats\_current\_timeframe テーブルに対して結合を実行することはできません。

## user\_ids\_stats\_current\_timeframe のサンプルクエリ

次のクエリは、user\_ids\_stats\_current\_month テーブルから最大 25 件のユーザ レコードを返します。各レコードには、Global \ Company B \ Edge ドメインでの選択された username のブロックされた接続の数と侵入イベントの数が含まれます。

```
SELECT username, start_time_sec, blocked, impact_level_1, impact_level_2,
impact_level_3, impact_level_4, impact_level_5 FROM user_ids_stats_current_year
WHERE username="username" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```

## user\_stats\_current\_timeframe

user\_stats\_current\_timeframe テーブルには、ユーザ別の帯域幅使用状況とアクセス コントロール アクション(接続の許可または拒否)に関する統計情報が格納されます。クエリの対象を、トラフィックをモニタしていた管理対象デバイスに制限することもできます。

current\_day、current\_month、および current\_year 統計情報テーブルについては、[統計情報追跡テーブルの保存特性\(5-3 ページ\)](#)を参照してください。

詳細については、次の項を参照してください。

- [user\\_stats\\_current\\_timeframe のフィールド\(5-32 ページ\)](#)
- [user\\_stats\\_current\\_timeframe の結合\(5-32 ページ\)](#)
- [user\\_stats\\_current\\_timeframe のサンプルクエリ\(5-32 ページ\)](#)

## user\_stats\_current\_timeframe のフィールド

次の表に、`user_stats_current_timeframe` 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 5-22 `user_stats_current_timeframe` のフィールド

| フィールド                              | 説明  |
|------------------------------------|---|
| <code>bytes_in</code>              | 測定間隔におけるユーザの着信トラフィックのバイト数。  |
| <code>bytes_out</code>             | 測定間隔におけるユーザの発信トラフィックのバイト数。  |
| <code>connections_allowed</code>   | 測定間隔においてこのユーザに対して許可された接続数。  |
| <code>connections_denied</code>    | アクセス コントロール ポリシー違反が原因で、このユーザに対して拒否された接続の数。  |
| <code>domain_name</code>           | 統計情報のために指定されたドメインの名前。   |
| <code>domain_uuid</code>           | 統計情報のために指定されたドメインの UUID。これはバイナリで示されます。  |
| <code>netmap_num</code>            | 統計情報が収集されたドメインの Netmap ID。  |
| <code>qos_dropped_bytes_in</code>  | QoS によりドロップされた着信バイト数。   |
| <code>qos_dropped_bytes_out</code> | QoS によりドロップされた発信バイト数。   |
| <code>sensor_address</code>        | トラフィックをモニタしていた管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code> , <code>ipv6_address</code> です。     |
| <code>sensor_id</code>             | トラフィックを検出した管理対象デバイスの内部識別番号。   |
| <code>sensor_name</code>           | トラフィックを検出した管理対象デバイスの名前。   |
| <code>sensor_uuid</code>           | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が null の場合は 0)。   |
| <code>start_time_sec</code>        | 測定間隔の開始時刻を示す UNIX タイムスタンプ。開始時刻の指定については、 <a href="#">統計情報テーブルの照会時の時間間隔の指定 (5-3 ページ)</a> を参照してください。 |
| <code>user_id</code>               | トラフィックを生成したホストの最終ログイン ユーザの内部識別番号。   |
| <code>username</code>              | トラフィックを生成したホストの最終ログイン ユーザのユーザ名。   |

## user\_stats\_current\_timeframe の結合

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

## user\_stats\_current\_timeframe のサンプルクエリ

次のクエリは最大 25 件のユーザレコードを返します。各レコードには、`domain_name= "Global \ Company B \ Edge` ドメイン内での測定間隔中の着信トラフィックと発信トラフィックのバイト数、および許可された接続と拒否された接続が含まれています。

```
SELECT sensor_name, sensor_address, username, start_time_sec, bytes_in, bytes_out,
connections_allowed, connections_denied
FROM user_stats_current_year
WHERE username="username" AND domain_name= "Global \ Company B \ Edge"
LIMIT 0, 25;
```





## 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   |
|---|--|-----------|
| <a href="#">application_host_map</a> (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+      |
| <a href="#">application_ip_map</a> (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+      |
| <a href="#">application_ip_map</a> (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。<br>バージョン 5.2 で廃止置き換わるテーブル:<br><a href="#">application_ip_map</a> (A-1 ページ)。 | 5.0-5.1.x |
| <a href="#">application_tag_map</a> (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+      |
| <a href="#">domain_control_information</a> (6-12 ページ) | ドメイン階層情報   | 6.0+      |
| <a href="#">network_discovery_event</a> (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+      |
| <a href="#">rna_host</a> (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+      |
| <a href="#">rna_host_attribute</a> (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+      |
| <a href="#">rna_host_client_app</a> (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+      |
| <a href="#">rna_host_client_app</a> (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+      |
| <a href="#">rna_host_ioc_state</a> (6-23 ページ)         | ホストの侵害状態が格納されます。   | 5.3+      |
| <a href="#">rna_host_ip_map</a> (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+      |
| <a href="#">rna_host_os</a> (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+      |
| <a href="#">rna_host_os_vulns</a> (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+      |
| <a href="#">rna_host_protocol</a> (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+   |
| <a href="#">rna_host_protocol</a> (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+      |
| <a href="#">rna_host_service</a> (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+      |
| <a href="#">rna_host_service_banner</a> (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+      |
| <a href="#">rna_host_service_info</a> (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       |
|--|---|---------------|
| <a href="#">rna_host_service_payload(6-43 ページ)</a>             | 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+          |
| <a href="#">rna_host_service_subtype(6-45 ページ)</a>             | 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+          |
| <a href="#">rna_host_service_vulns(6-47 ページ)</a>               | 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+          |
| <a href="#">rna_host_third_party_vuln(6-48 ページ)</a>            | 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+          |
| <a href="#">rna_host_third_party_vuln_bugtraq_id(6-50 ページ)</a> | 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 ( <a href="http://www.securityfocus.com/bid/">http://www.securityfocus.com/bid/</a> ) 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+          |
| <a href="#">rna_host_third_party_vuln_cve_id(6-52 ページ)</a>     | 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。<br>( <a href="http://www.cve.mitre.org/">http://www.cve.mitre.org/</a> )。           | 5.2+          |
| <a href="#">rna_host_third_party_vuln_rna_id(6-54 ページ)</a>     | 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+          |
| <a href="#">rna_ip_host(A-1 ページ)</a>                           | モニタ対象ネットワークの IP ホストの基本情報。<br>バージョン 5.2 で廃止置き換わるテーブル <a href="#">rna_host(6-14 ページ)</a> 。  | 4.10.x-5.1.x  |
| <a href="#">rna_ip_host_client_app(A-1 ページ)</a>                | 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。<br>バージョン 5.2 で廃止置き換わるテーブル <a href="#">rna_host_client_app(6-17 ページ)</a> 。                                      | 4.10.x-5.1.x  |
| <a href="#">rna_ip_host_client_app_payload(A-1 ページ)</a>        | 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。<br>バージョン 5.2 で廃止置き換わるテーブル <a href="#">rna_host_client_app(6-17 ページ)</a> 。 | 4.10.x-5.1.x  |
| <a href="#">rna_ip_host_os(A-1 ページ)</a>                        | 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。<br>バージョン 5.2 で廃止置き換わるテーブル <a href="#">rna_host_os(6-30 ページ)</a> 。   | 4.10.x-5.1.x  |
| <a href="#">rna_ip_host_os_vulns(A-1 ページ)</a>                  | 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。<br>バージョン 5.2 で廃止置き換わるテーブル: <a href="#">rna_host_os_vulns(6-31 ページ)</a> 。  | 4.10.x--5.1.x |
| <a href="#">rna_ip_host_sensor(A-1 ページ)</a>                    | 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。<br>バージョン 5.2 で廃止置き換わるテーブル: <a href="#">rna_host_protocol(6-33 ページ)</a> 。                                 | 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      |
|--|--|--------------|
| <a href="#">rna_ip_host_service(A-1 ページ)</a>                     | 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_service(6-36 ページ)</a> 。   | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_service_banner(A-1 ページ)</a>              | 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 バンナーとバージョン(「バナー」)をアダプタイズするネットワーク トラフィックのヘッダー。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_service_banner(6-38 ページ)</a> 。  | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_service_info(A-1 ページ)</a>                | 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_service_info(6-39 ページ)</a> 。   | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_service_payload(A-1 ページ)</a>             | 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_service_payload(6-43 ページ)</a> 。  | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_service_subtype(A-1 ページ)</a>             | 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_service_subtype(6-45 ページ)</a> 。  | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_service_vulns(A-1 ページ)</a>               | 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_service_vulns(6-47 ページ)</a> 。  | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_third_party_vuln(A-1 ページ)</a>            | 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_third_party_vuln(6-48 ページ)</a> 。   | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_third_party_vuln_bugtraq_id(A-1 ページ)</a> | 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 ( <a href="http://www.securityfocus.com/bid/">http://www.securityfocus.com/bid/</a> ) 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。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_third_party_vuln_bugtraq_id(6-50 ページ)</a> 。 | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_third_party_vuln_cve_id(A-1 ページ)</a>     | 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。<br>( <a href="http://www.cve.mitre.org/">http://www.cve.mitre.org/</a> )。<br>バージョン 5.2 で廃止置き換わるテーブル<br><a href="#">rna_host_third_party_vuln_cve_id(6-52 ページ)</a> 。              | 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      |
|--|--|--------------|
| <a href="#">rna_ip_host_third_party_vuln_rna_id(A-1 ページ)</a> | 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。<br>バージョン 5.2 で廃止置き換わるテーブル <a href="#">rna_host_third_party_vuln_rna_id(6-54 ページ)</a> 。         | 4.10.x-5.1.x |
| <a href="#">rna_ip_host_user_history(A-1 ページ)</a>            | 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。<br>バージョン 5.2 で廃止置き換わるテーブル <a href="#">user_ipaddr_history(6-62 ページ)</a> 。                                     | 4.10.x-5.1.x |
| <a href="#">rna_mac_host(A-1 ページ)</a>                        | 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 |
| <a href="#">rna_mac_host_sensor(A-1 ページ)</a>                 | 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    |
| <a href="#">rna_mac_ip_map(A-2 ページ)</a>                      | モニタ対象ネットワークの IP ホストの MAC アドレス。<br>バージョン 5.2 で廃止置き換わるテーブル: <a href="#">rna_host_ip_map(6-27 ページ)</a> および <a href="#">rna_host_mac_map(6-28 ページ)</a> 。 | 4.10.x-5.1.x |
| <a href="#">rna_vuln(6-56 ページ)</a>                           | シスコ VDB の脆弱性。  | 4.10.x+      |
| <a href="#">tag_info(6-59 ページ)</a>                           | 検出されたアプリケーションを特徴付けるタグ。   | 5.0+         |
| <a href="#">url_categories(6-60 ページ)</a>                     | 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+         |
| <a href="#">url_reputations(6-61 ページ)</a>                    | 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+         |
| <a href="#">user_ipaddr_history(6-62 ページ)</a>                | 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  |
|---|---|
| <code>application_id</code>                 | アプリケーションの内部識別番号。  |
| <code>application_name</code>               | 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。  |
| <code>application_tag_id</code>             | このフィールドは廃止されており、 <code>null</code> を返します。   |
| <code>business_relevance</code>             | 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。  |
| <code>business_relevance_description</code> | ビジネスとの関連度の説明 ( <code>very low</code> 、 <code>low</code> 、 <code>medium</code> 、 <code>high</code> 、 <code>very high</code> )。 |
| <code>host_id</code>                        | ホストの ID 番号。   |
| <code>risk</code>                           | 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。  |
| <code>risk_description</code>               | リスクの説明 ( <code>very low</code> 、 <code>low</code> 、 <code>medium</code> 、 <code>high</code> 、 <code>critical</code> )。        |

## 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  |
|-----------------------------|---|
| <code>application_id</code> | <code>app_ids_stats_current_timeframe.application_id</code><br><code>application_info.application_id</code><br><code>application_tag_map.application_id</code><br><code>app_stats_current_timeframe.application_id</code><br><code>connection_log.application_protocol_id</code><br><code>connection_log.client_application_id</code><br><code>connection_log.web_application_id</code><br><code>connection_summary.application_protocol_id</code><br><code>file_event.application_id</code><br><code>intrusion_event.application_protocol_id</code><br><code>intrusion_event.client_application_id</code><br><code>intrusion_event.web_application_id</code><br><code>rna_host_service_info.application_protocol_id</code><br><code>rna_host_client_app_payload.web_application_id</code><br><code>rna_host_client_app_payload.client_application_id</code><br><code>rna_host_client_app.client_application_id</code><br><code>rna_host_client_app.application_protocol_id</code><br><code>rna_host_service_payload.web_application_id</code><br><code>si_connection_log.application_protocol_name</code><br><code>si_connection_log.client_application_id</code><br><code>si_connection_log.web_application_id</code> |

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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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<br>app_ids_stats_current_timeframe.application_id<br>application_tag_map.application_id<br>app_stats_current_timeframe.application_id<br>connection_log.application_protocol_id<br>connection_log.client_application_id<br>connection_log.web_application_id<br>si_connection_log.application_protocol_id<br>si_connection_log.application_protocol_name<br>si_connection_log.client_application_id<br>si_connection_log.web_application_id<br>connection_summary.application_protocol_id<br>file_event.application_id<br>intrusion_event.application_protocol_id<br>intrusion_event.client_application_id<br>intrusion_event.web_application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>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<br>application_info.application_id<br>application_host_map.application_id<br>app_stats_current_timeframe.application_id<br>connection_log.application_protocol_id<br>connection_log.client_application_id<br>connection_log.web_application_id<br>connection_summary.application_protocol_id<br>file_event.application_id<br>intrusion_event.application_protocol_id<br>intrusion_event.client_application_id<br>intrusion_event.web_application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>rna_host_service_payload.web_application_id<br>si_connection_log.application_protocol_name<br>si_connection_log.application_protocol_id<br>si_connection_log.client_application_id<br>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 IPv6 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> 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 ( <code>sensor_name</code> 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              | <code>rna_host_ip_map.ipaddr</code><br><code>user_ipaddr_history.ipaddr</code> |

## 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。 <ul style="list-style-type: none"> <li>0:イーサネット</li> <li>1:トークンリング</li> </ul> |

## 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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ip_map.host_id<br>rna_host_ioc_state.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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<br>rna_host.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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 \(6-20 ページ\)](#)

## rma\_host\_client\_app のフィールド

次の表に、`rma_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 `rma_host_client_app` のフィールド

| フィールド                                  | 説明   |
|--|--|
| <code>application</code>               | 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。  |
| <code>application_protocol_id</code>   | 検出されたアプリケーションプロトコルの内部 ID。  |
| <code>application_protocol_name</code> | 次のいずれかになります。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)</li> <li>pending(システムがさらにデータを必要としている場合)</li> <li>空白(接続にアプリケーション情報がない場合)</li> </ul>  |
| <code>application_type</code>          | 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。  |
| <code>client_application_id</code>     | 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。  |
| <code>client_application_name</code>   | 次のいずれかになります。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)。</li> <li>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)。</li> <li>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)。</li> </ul> |
| <code>hits</code>                      | クライアントアプリケーションが検出された回数。  |
| <code>host_id</code>                   | ホストの ID 番号。  |
| <code>last_used_sec</code>             | 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。  |
| <code>version</code>                   | 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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>rna_host_third_party_vuln.host_id |
| host_id<br>および<br>application_protocol_id<br>および<br>client_application_id<br>および<br>version | 次のセット:<br>rna_host_client_app_payload.host_id<br>rna_host_client_app_payload.application_protocol_id<br>rna_host_client_app_payload.client_application_id<br>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<br>または<br>client_application_id | app_ids_stats_current_timeframe.application_id<br>application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>app_stats_current_timeframe.application_id<br>connection_log.application_protocol_id<br>connection_log.client_application_id<br>connection_log.web_application_id<br>connection_summary.application_protocol_id<br>si_connection_log.application_protocol_name<br>si_connection_log.client_application_id<br>si_connection_log.web_application_id<br>file_event.application_id<br>intrusion_event.application_protocol_id<br>intrusion_event.client_application_id<br>intrusion_event.web_application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_service_info.application_protocol_id<br>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。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)</li> <li>pending(システムがさらにデータを必要としている場合)</li> <li>空白(接続にアプリケーション情報がない場合)</li> </ul>  |
| 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。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)。</li> <li>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)。</li> <li>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)。</li> </ul>     |
| 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。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)。</li> <li>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)。</li> <li>空白(接続に HTTP トラフィックがない場合)。</li> </ul> |

## 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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>rna_host_third_party_vuln.host_id |
| 次のセット:<br>host_id,<br>application_protocol_id,<br>client_application_id,<br>version | 次のセット:<br>rna_host_client_app.host_id<br>rna_host_client_app.application_protocol_id<br>rna_host_client_app.client_application_id<br>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<br>または<br>web_application_id | app_ids_stats_current_timeframe.application_id<br>application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>app_stats_current_timeframe.application_id<br>connection_log.application_protocol_id<br>connection_log.client_application_id<br>connection_log.web_application_id<br>connection_summary.application_protocol_id<br>si_connection_log.application_protocol_name<br>si_connection_log.client_application_id<br>si_connection_log.web_application_id<br>file_event.application_id<br>intrusion_event.application_protocol_id<br>intrusion_event.client_application_id<br>intrusion_event.web_application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>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   |
|--|--|
| <code>first_seen</code>                | 侵害が最初に検出された時点を示す UNIX タイムスタンプ。   |
| <code>first_seen_sensor_address</code> | 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 <code>ipv4_address, ipv6_address</code> です。  |
| <code>first_seen_sensor_name</code>    | 侵害を最初に検出した管理対象デバイス。  |
| <code>host_id</code>                   | ホストの ID 番号。  |
| <code>ioc_category</code>              | 侵害のカテゴリ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• CnC Connected</li> <li>• Exploit Kit</li> <li>• High Impact Attack</li> <li>• Low Impact Attack</li> <li>• Malware Detected</li> <li>• Malware Executed</li> <li>• Dropper Infection</li> <li>• Java Compromise</li> <li>• Word Compromise</li> <li>• Adobe Reader Compromise</li> <li>• Excel Compromise</li> <li>• PowerPoint Compromise</li> <li>• QuickTime Compromise</li> </ul> |
| <code>ioc_description</code>           | 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 | <p>侵害のイベント タイプ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Adobe Reader launched shell</li> <li>• Dropper Infection Detected by AMP for Endpoints</li> <li>• Excel Compromise Detected by AMP for Endpoints</li> <li>• Excel launched shell  </li> <li>• Impact 1 Intrusion Event – attempted-admin</li> <li>• Impact 1 Intrusion Event – attempted-user</li> <li>• Impact 1 Intrusion Event – successful-admin</li> <li>• Impact 1 Intrusion Event – successful-user</li> <li>• Impact 1 Intrusion Event – web-application-attack</li> <li>• Impact 2 Intrusion Event – attempted-admin</li> <li>• Impact 2 Intrusion Event – attempted-user</li> <li>• Impact 2 Intrusion Event – successful-admin</li> <li>• Impact 2 Intrusion Event – successful-user</li> <li>• Impact 2 Intrusion Event – web-application-attack</li> <li>• Intrusion Event – exploit-kit</li> <li>• Intrusion Event – malware-backdoor</li> <li>• Intrusion Event – malware-CnC</li> <li>• Java Compromise Detected by AMP for Endpoints</li> <li>• Java launched shell</li> <li>• PDF Compromise Detected by AMP for Endpoints</li> <li>• PowerPoint Compromise Detected by AMP for Endpoints</li> <li>• PowerPoint launched shell</li> <li>• QuickTime Compromise Detected by AMP for Endpoints</li> <li>• QuickTime launched shell</li> <li>• Security Intelligence Event – CnC</li> <li>• Suspected Botnet Detected by AMP for Endpoints</li> <li>• Threat Detected by AMP for Endpoints – Subtype is 'executed'</li> <li>• Threat Detected by AMP for Endpoints – Subtype is not 'executed'</li> <li>• Threat Detected in File Transfer – Action is not 'block'</li> <li>• Word Compromise Detected by AMP for Endpoints</li> <li>• Word launched shell</li> </ul> |
| 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 <code>ipv4_address</code> , <code>ipv6_address</code> 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             | <code>rna_host.host_id</code><br><code>rna_host_attribute.host_id</code><br><code>rna_host_protocol.host_id</code><br><code>rna_host_os_vulns.host_id</code><br><code>application_host_map.host_id</code><br><code>rna_host_client_app.host_id</code><br><code>rna_host_client_app_payload.host_id</code><br><code>rna_host_ip_map.host_id</code><br><code>rna_host_mac_map.host_id</code><br><code>rna_host_os.host_id</code><br><code>rna_host_sensor.host_id</code><br><code>rna_host_service.host_id</code><br><code>rna_host_service_banner.host_id</code><br><code>rna_host_service_info.host_id</code><br><code>rna_host_service_payload.host_id</code><br><code>rna_host_service_vulns.host_id</code><br><code>rna_host_third_party_vuln_bugtraq_id.host_id</code><br><code>rna_host_third_party_vuln_cve_id.host_id</code><br><code>rna_host_third_party_vuln_rna_id.host_id</code><br><code>rna_host_third_party_vuln.host_id</code> |

## 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 を関連付けます。

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             | <code>rna_host.host_id</code><br><code>rna_host_attribute.host_id</code><br><code>rna_host_protocol.host_id</code><br><code>rna_host_os_vulns.host_id</code><br><code>application_host_map.host_id</code><br><code>rna_host_client_app.host_id</code><br><code>rna_host_client_app_payload.host_id</code><br><code>rna_host_ioc_state.host_id</code><br><code>rna_host_mac_map.host_id</code><br><code>rna_host_os.host_id</code><br><code>rna_host_sensor.host_id</code><br><code>rna_host_service.host_id</code><br><code>rna_host_service_banner.host_id</code><br><code>rna_host_service_info.host_id</code><br><code>rna_host_service_payload.host_id</code><br><code>rna_host_service_vulns.host_id</code><br><code>rna_host_third_party_vuln_bugtraq_id.host_id</code><br><code>rna_host_third_party_vuln_cve_id.host_id</code><br><code>rna_host_third_party_vuln_rna_id.host_id</code><br><code>rna_host_third_party_vuln.host_id</code> |

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<br>compliance_event.src_ipaddr<br>connection_log.initiator_ipaddr<br>connection_log.responder_ipaddr<br>connection_summary.initiator_ipaddr<br>connection_summary.responder_ipaddr<br>fireamp_event.dst_ipaddr<br>fireamp_event.src_ipaddr<br>intrusion_event.dst_ipaddr<br>intrusion_event.src_ipaddr<br>network_discovery_event.ipaddr<br>si_connection_log.initiator_ipaddr<br>si_connection_log.responder_ipaddr<br>user_discovery_event.ipaddr<br>user_ipaddr_history.ipaddr<br>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) = "00000000000000000000000000000000FFFF0A0A0A04";
```

## 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 を関連付けます。

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             | <code>rna_host.host_id</code><br><code>rna_host_attribute.host_id</code><br><code>rna_host_protocol.host_id</code><br><code>rna_host_os_vulns.host_id</code><br><code>application_host_map.host_id</code><br><code>rna_host_client_app.host_id</code><br><code>rna_host_client_app_payload.host_id</code><br><code>rna_host_ioc_state.host_id</code><br><code>rna_host_ip_map.host_id</code><br><code>rna_host_os.host_id</code><br><code>rna_host_sensor.host_id</code><br><code>rna_host_service.host_id</code><br><code>rna_host_service_banner.host_id</code><br><code>rna_host_service_info.host_id</code><br><code>rna_host_service_payload.host_id</code><br><code>rna_host_service_vulns.host_id</code><br><code>rna_host_third_party_vuln_bugtraq_id.host_id</code><br><code>rna_host_third_party_vuln_cve_id.host_id</code><br><code>rna_host_third_party_vuln_rna_id.host_id</code><br><code>rna_host_third_party_vuln.host_id</code> |

## 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  |
|----------------------------|---|
| <code>confidence</code>    | 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)。   |
| <code>created_sec</code>   | 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。   |
| <code>host_id</code>       | ホストの ID 番号。   |
| <code>last_seen_sec</code> | 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。   |
| <code>os_uuid</code>       | 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。  |
| <code>product</code>       | ホストで検出されたオペレーティング システム。   |
| <code>source_type</code>   | 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。 <ul style="list-style-type: none"> <li>• <code>User:Web</code>: 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</li> <li>• <code>Application</code>: 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</li> <li>• <code>Scanner:Nmap</code>: 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</li> <li>• <code>rna:Firepower</code>: 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)。</li> <li>• <code>NetFlow:NetFlow</code>: NetFlow 対応デバイスによってデータがエクスポートされた</li> </ul> |
| <code>vendor</code>        | 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。  |
| <code>version</code>       | 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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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。 <ul style="list-style-type: none"> <li>0:脆弱性が有効</li> <li>1:脆弱性が無効</li> </ul> |
| 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         | <code>rna_vuln.bugtraq_id</code><br><code>rna_vuln.rna_vuln_id</code><br><code>rna_host_third_party_vuln_rna_id.rna_vuln_id</code><br><code>rna_host_third_party_vuln_cve_id.cve_id</code><br><code>rna_host_third_party_vuln_bugtraq_id.bugtraq_id</code>   |
| host_id             | <code>rna_host.host_id</code><br><code>rna_host_attribute.host_id</code><br><code>rna_host_protocol.host_id</code><br><code>application_host_map.host_id</code><br><code>rna_host_client_app.host_id</code><br><code>rna_host_client_app_payload.host_id</code><br><code>rna_host_ioc_state.host_id</code><br><code>rna_host_ip_map.host_id</code><br><code>rna_host_mac_map.host_id</code><br><code>rna_host_sensor.host_id</code><br><code>rna_host_service.host_id</code><br><code>rna_host_service_banner.host_id</code><br><code>rna_host_service_info.host_id</code><br><code>rna_host_service_payload.host_id</code><br><code>rna_host_third_party_vuln_bugtraq_id.host_id</code><br><code>rna_host_third_party_vuln_cve_id.host_id</code><br><code>rna_host_third_party_vuln_rna_id.host_id</code><br><code>rna_host_third_party_vuln.host_id</code> |



## 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<br>rna_host_attribute.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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   |
|-----------------------------|--|
| <code>host_id</code>        | ホストの ID 番号。  |
| <code>sensor_address</code> | 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 <code>ipv4_address</code> 、 <code>ipv6_address</code> です。 |
| <code>sensor_name</code>    | 管理対象デバイスの名前。   |
| <code>sensor_uuid</code>    | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が <code>null</code> 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  |
|----------------------|---|
| <code>host_id</code> | <code>rna_host.host_id</code><br><code>rna_host_attribute.host_id</code><br><code>rna_host_protocol.host_id</code><br><code>rna_host_os_vulns.host_id</code><br><code>application_host_map.host_id</code><br><code>rna_host_client_app.host_id</code><br><code>rna_host_client_app_payload.host_id</code><br><code>rna_host_ioc_state.host_id</code><br><code>rna_host_ip_map.host_id</code><br><code>rna_host_mac_map.host_id</code><br><code>rna_host_os.host_id</code><br><code>rna_host_service.host_id</code><br><code>rna_host_service_banner.host_id</code><br><code>rna_host_service_info.host_id</code><br><code>rna_host_service_payload.host_id</code><br><code>rna_host_service_vulns.host_id</code><br><code>rna_host_third_party_vuln_bugtraq_id.host_id</code><br><code>rna_host_third_party_vuln_cve_id.host_id</code><br><code>rna_host_third_party_vuln_rna_id.host_id</code><br><code>rna_host_third_party_vuln.host_id</code> |

## 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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>rna_host_third_party_vuln.host_id |
| 次のセット:<br>host_id<br>port<br>protocol | 次のセット:<br>rna_host_service_banner.host_id<br>rna_host_service_banner.port<br>rna_host_service_banner.protocol<br><br>次のセット:<br>rna_host_service_info.host_id<br>rna_host_service_info.port<br>rna_host_service_info.protocol<br><br>次のセット:<br>rna_host_service_payload.host_id<br>rna_host_service_payload.port<br>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:<br>host_id<br>port<br>protocol | 次のセット:<br><a href="#">rna_host_service.host_id</a><br><a href="#">rna_host_service.port</a><br><a href="#">rna_host_service.protocol</a><br><br>次のセット:<br><a href="#">rna_host_service_info.host_id</a><br><a href="#">rna_host_service_info.port</a><br><a href="#">rna_host_service_info.protocol</a><br><br>次のセット:<br><a href="#">rna_host_service_payload.host_id</a><br><a href="#">rna_host_service_payload.port</a><br><a href="#">rna_host_service_payload.protocol</a> |

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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>rna_host_service_vulns.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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: <ul style="list-style-type: none"> <li>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)</li> <li>pending (システムがさらにデータを必要としている場合)</li> <li>空白 (接続にアプリケーション情報がない場合)</li> </ul>   |
| 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: <ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> <li>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)。</li> <li>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</li> </ul> |



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<br>application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>app_stats_current_timeframe.application_id<br>connection_log.application_protocol_id<br>connection_log.client_application_id<br>connection_log.web_application_id<br>connection_summary.application_protocol_id<br>si_connection_log.application_protocol_name<br>si_connection_log.client_application_id<br>si_connection_log.web_application_id<br>file_event.application_id<br>intrusion_event.application_protocol_id<br>intrusion_event.client_application_id<br>intrusion_event.web_application_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_payload.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>rna_host_third_party_vuln.host_id |
| 次のセット:<br>host_id   | 次のセット:<br>rna_host_service.host_id  |
| および<br>port         | rna_host_service.port<br>rna_host_service.protocol  |
| および<br>protocol     | 次のセット:<br>rna_host_service_banner.host_id<br>rna_host_service_banner.port<br>rna_host_service_banner.protocol   |
|                     | 次のセット:<br>rna_host_service_payload.host_id<br>rna_host_service_payload.port<br>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   |
|-----------------------------------|--|
| <code>application_id</code>       | 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 <code>null</code> を返します。   |
| <code>application_name</code>     | 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 <code>null</code> を返します。   |
| <code>host_id</code>              | ホストの ID 番号。  |
| <code>ip_address</code>           | 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 <code>null</code> を返します。   |
| <code>payload_name</code>         | 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 <code>null</code> を返します。   |
| <code>payload_type</code>         | 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 <code>null</code> を返します。   |
| <code>port</code>                 | サーバで使用されるポート。  |
| <code>protocol</code>             | トラフィック プロトコル:TCP または UDP。  |
| <code>web_application_id</code>   | Web アプリケーションの内部識別番号。   |
| <code>web_application_name</code> | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• Web アプリケーションの名前(確実な識別が可能な場合)</li> <li>• <code>web browsing</code>(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)。</li> <li>• 空白(接続に HTTP トラフィックがない場合)。</li> </ul> |

## 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<br>application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>app_stats_current_timeframe.application_id<br>connection_log.application_protocol_id<br>connection_log.client_application_id<br>connection_log.web_application_id<br>connection_summary.application_protocol_id<br>si_connection_log.application_protocol_name<br>si_connection_log.client_application_id<br>si_connection_log.web_application_id<br>file_event.application_id<br>intrusion_event.application_protocol_id<br>intrusion_event.client_application_id<br>intrusion_event.web_application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id |
| 次のセット:<br>host_id<br>port<br>protocol | 次のセット:<br>rna_host_service.host_id<br>rna_host_service.port<br>rna_host_service.protocol<br><br>次のセット:<br>rna_host_service_banner.host_id<br>rna_host_service_banner.port<br>rna_host_service_banner.protocol<br><br>次のセット:<br>rna_host_service_info.host_id<br>rna_host_service_info.port<br>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             | <a href="#">rna_host.host_id</a><br><a href="#">rna_host_attribute.host_id</a><br><a href="#">rna_host_protocol.host_id</a><br><a href="#">rna_host_os_vulns.host_id</a><br><a href="#">application_host_map.host_id</a><br><a href="#">rna_host_client_app.host_id</a><br><a href="#">rna_host_client_app_payload.host_id</a><br><a href="#">rna_host_ioc_state.host_id</a><br><a href="#">rna_host_ip_map.host_id</a><br><a href="#">rna_host_mac_map.host_id</a><br><a href="#">rna_host_os.host_id</a><br><a href="#">rna_host_sensor.host_id</a><br><a href="#">rna_host_service.host_id</a><br><a href="#">rna_host_service_banner.host_id</a><br><a href="#">rna_host_service_info.host_id</a><br><a href="#">rna_host_service_vulns.host_id</a><br><a href="#">rna_host_third_party_vuln_bugtraq_id.host_id</a><br><a href="#">rna_host_third_party_vuln_cve_id.host_id</a><br><a href="#">rna_host_third_party_vuln_rna_id.host_id</a><br><a href="#">rna_host_third_party_vuln.host_id</a> |

## 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。 <ul style="list-style-type: none"> <li>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。</li> <li>none または空白 (識別のためのデータが使用できない場合)</li> <li>pending (追加データが必要な場合)</li> <li>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)</li> </ul>   |
| source_type         | サーバのアイデンティティ ソース: <ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> <li>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)</li> <li>NetFlow:NetFlow 対応デバイスによってエクスポートされたデータ</li> </ul> |
| 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  |
|-------------------------------|---|
| <code>application_id</code>   | 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。  |
| <code>application_name</code> | 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。   |
| <code>host_id</code>          | ホストの ID 番号。   |
| <code>invalid</code>          | 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。 <ul style="list-style-type: none"> <li>• 0:脆弱性が有効</li> <li>• 1:脆弱性が無効</li> </ul> |
| <code>ip_address</code>       | 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。   |
| <code>port</code>             | サーバで使用されるポート。   |
| <code>protocol</code>         | トラフィック プロトコル:TCP または UDP。   |
| <code>rna_vuln_id</code>      | 脆弱性の内部識別番号。   |
| <code>service_name</code>     | 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。   |
| <code>vendor</code>           | ホストで検出されたサーバのベンダー。  |
| <code>version</code>          | 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<br>rna_vuln.rna_vuln_id<br>rna_host_third_party_vuln_rna_id.rna_vuln_id<br>rna_host_third_party_vuln_cve_id.cve_id<br>rna_host_third_party_vuln_bugtraq_id.bugtraq_id  |
| host_id             | rna_host.host_id<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_payload.host_id<br>rna_host_third_party_vuln_bugtraq_id.host_id<br>rna_host_third_party_vuln_cve_id.host_id<br>rna_host_third_party_vuln_rna_id.host_id<br>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   |
|----------------------------------|--|
| <code>description</code>         | 脆弱性に関する説明。   |
| <code>host_id</code>             | ホストの ID 番号。  |
| <code>invalid</code>             | 脆弱性がホストで有効であるかどうかを示す値。 <ul style="list-style-type: none"><li>• 0:脆弱性が有効</li><li>• 1:脆弱性が無効</li></ul> |
| <code>name</code>                | 脆弱性のタイトル。  |
| <code>port</code>                | 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)。  |
| <code>protocol</code>            | 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)。                                    |
| <code>source</code>              | 脆弱性のソース。   |
| <code>third_party_vuln_id</code> | 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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>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。 <ul style="list-style-type: none"> <li>0:脆弱性が有効</li> <li>1:脆弱性が無効</li> </ul> |
| 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に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          | <a href="#">rna_vuln.bugtraq_id</a><br><a href="#">rna_vuln.rna_vuln_id</a><br><a href="#">rna_host_os_vulns.rna_vuln_id</a><br><a href="#">rna_host_service_vulns.rna_vuln_id</a> |

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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>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  |
|----------------------------------|---|
| <code>cve_id</code>              | 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。  |
| <code>description</code>         | 脆弱性に関する説明。  |
| <code>host_id</code>             | ホストの ID 番号。   |
| <code>invalid</code>             | 脆弱性がホストで有効であるかどうかを示す値。 <ul style="list-style-type: none"> <li>0:脆弱性が有効</li> <li>1:脆弱性が無効</li> </ul> |
| <code>ip_address</code>          | 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。   |
| <code>name</code>                | 脆弱性の名前またはタイトル。  |
| <code>port</code>                | 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)。   |
| <code>protocol</code>            | 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に関連付けられている場合)。                                   |
| <code>source</code>              | 脆弱性のソース。  |
| <code>third_party_vuln_id</code> | 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   |
|---------------------|--|
| <code>cve_id</code> | <a href="#">rna_vuln.bugtraq_id</a><br><a href="#">rna_vuln.rna_vuln_id</a><br><a href="#">rna_host_os_vulns.rna_vuln_id</a><br><a href="#">rna_host_service_vulns.rna_vuln_id</a> |

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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>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  |
|----------------------------------|---|
| <code>description</code>         | 脆弱性に関する説明。  |
| <code>host_id</code>             | ホストの ID 番号。   |
| <code>invalid</code>             | 脆弱性がホストで有効であるかどうかを示す値。 <ul style="list-style-type: none"> <li>0:脆弱性が有効</li> <li>1:脆弱性が無効</li> </ul> |
| <code>ip_address</code>          | 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。   |
| <code>name</code>                | 脆弱性の名前またはタイトル。  |
| <code>port</code>                | 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)。   |
| <code>protocol</code>            | 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)。                                   |
| <code>rna_vuln_id</code>         | 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。  |
| <code>source</code>              | 脆弱性のソース。  |
| <code>third_party_vuln_id</code> | 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   |
|--------------------------|--|
| <code>rna_vuln_id</code> | <a href="#">rna_vuln.bugtraq_id</a><br><a href="#">rna_vuln.rna_vuln_id</a><br><a href="#">rna_host_os.rna_vuln_id</a><br><a href="#">rna_host_service_vulns.rna_vuln_id</a> |

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<br>rna_host_attribute.host_id<br>rna_host_protocol.host_id<br>rna_host_os_vulns.host_id<br>application_host_map.host_id<br>rna_host_client_app.host_id<br>rna_host_client_app_payload.host_id<br>rna_host_ioc_state.host_id<br>rna_host_ip_map.host_id<br>rna_host_mac_map.host_id<br>rna_host_os.host_id<br>rna_host_sensor.host_id<br>rna_host_service.host_id<br>rna_host_service_banner.host_id<br>rna_host_service_info.host_id<br>rna_host_service_payload.host_id<br>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 <ul style="list-style-type: none"> <li>• 必須</li> <li>• Not Required</li> <li>• 不明</li> </ul>   |
| availability       | 脆弱性のエクスプロイトが可能な状況: <ul style="list-style-type: none"> <li>• Always</li> <li>• User Initiated</li> <li>• Time Dependent</li> <li>• 不明</li> </ul>   |
| 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 <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>  |
| 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: <ul style="list-style-type: none"> <li>• Configuration Error</li> <li>• Boundary Condition Error</li> <li>• Design Error</li> </ul>  |
| credibility        | 脆弱性の信頼度: <ul style="list-style-type: none"> <li>• Conflicting Reports</li> <li>• Conflicting Details</li> <li>• Single Source</li> <li>• Reliable Source</li> <li>• Multiple Sources</li> <li>• Vendor Confirmed</li> </ul> |
| 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。 <ul style="list-style-type: none"> <li>• No Exploit Required</li> <li>• Exploit Available</li> <li>• No Exploit Available</li> </ul>   |
| 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 rma\_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。 <ul style="list-style-type: none"> <li>TRUE</li> <li>FALSE</li> </ul>                          |
| 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。 <ul style="list-style-type: none"> <li>TRUE</li> <li>FALSE</li> </ul>                          |
| 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<br>または<br>bugtraq_id | <a href="#">rna_host_os_vulns.rna_vuln_id</a><br><a href="#">rna_host_service_vulns.rna_vuln_id</a><br><a href="#">rna_host_third_party_vuln_rna_id.rna_vuln_id</a><br><a href="#">rna_host_third_party_vuln_cve_id.cve_id</a><br><a href="#">rna_host_third_party_vuln_bugtraq_id.bugtraq_id</a> |

## 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。 <ul style="list-style-type: none"> <li>• category</li> <li>• tag</li> </ul> |

## 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。 <ul style="list-style-type: none"> <li>• 0: 認証は不要</li> <li>• 1: パッシブ認証、AD エージェント、または ISE セッション</li> <li>• 2: キャプティブ ポータルの正常な認証</li> <li>• 3: キャプティブ ポータルのゲスト認証</li> <li>• 4: キャプティブ ポータルの失敗認証</li> </ul> |
| 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<br>compliance_event.src_ipaddr<br>connection_log.initiator_ipaddr<br>connection_log.responder_ipaddr<br>connection_summary.initiator_ipaddr<br>connection_summary.responder_ipaddr<br>fireamp_event.dst_ipaddr<br>fireamp_event.src_ipaddr<br>intrusion_event.dst_ipaddr<br>intrusion_event.src_ipaddr<br>network_discovery_event.ipaddr<br>rna_host_ip_map.ipaddr<br>si_connection_log.initiator_ipaddr<br>si_connection_log.responder_ipaddr<br>user_discovery_event.ipaddr<br>white_list_event.ipaddr |
| user_id             | discovered_users.user_id<br>user_discovery_event.user_id<br>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) = "00000000000000000000000000000000FFFF0A0A0A04" AND start_time_sec >=  
UNIX_TIMESTAMP("2011-10-01 00:00:00");
```





## 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 |
|---|---|---------|
| <a href="#">connection_log (7-1 ページ)</a>      | 個別の接続。廃止されたテーブル <code>rna_flow</code> を置き換えます。            | 5.0+    |
| <a href="#">connection_summary (7-15 ページ)</a> | 接続ログのサマリ。廃止されたテーブル <code>rna_flow_summary</code> を置き換えます。 | 5.0+    |
| <a href="#">si_connection_log (7-19 ページ)</a>  | 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   |
|---|--|
| <code>access_control_policy_name</code> | 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。   |
| <code>access_control_policy_UUID</code> | 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。   |
| <code>access_control_reason</code>      | 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。 <ul style="list-style-type: none"> <li>• IP Block</li> <li>• IP Monitor</li> <li>• User Bypass</li> <li>• File Monitor</li> <li>• File Block</li> <li>• Intrusion Monitor</li> <li>• Intrusion Block</li> <li>• File Resume Block</li> <li>• File Resume Allow</li> <li>• File Custom Detection</li> <li>• SSL Block</li> <li>• DNS Block</li> <li>• DNS Monitor</li> <li>• URL Block</li> <li>• URL Monitor</li> <li>• HTTP Injection</li> <li>• Intelligent App Bypass</li> <li>• ログに記録された接続がない場合は空白</li> </ul> |
| <code>access_control_rule_action</code> | 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): <code>allow</code> 、 <code>block</code> など。  |
| <code>access_control_rule_id</code>     | ルールの内部識別番号。  |
| <code>access_control_rule_name</code>   | 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)。   |
| <code>application_protocol_id</code>    | アプリケーションプロトコルの内部識別番号。  |
| <code>application_protocol_name</code>  | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• アプリケーションの名前(確実な識別が可能な場合)</li> <li>• <code>unknown</code>(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)</li> <li>• <code>pending</code>(システムがさらにデータを必要としている場合)</li> <li>• 空白(接続にアプリケーション情報がない場合)</li> </ul>  |

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ド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。 <ul style="list-style-type: none"> <li>アプリケーションの名前(確実な識別が可能な場合)。</li> <li>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)。</li> <li>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)。</li> </ul> |
| 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。 <ul style="list-style-type: none"> <li>rna:シスコデバイスで検出された場合</li> <li>netflow:NetFlow 対応デバイスによりエクスポートされる場合</li> </ul>  |
| counter                    | 接続イベントに関連する侵入イベントのカウント。  |
| 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       | <p>DNS 応答。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0:NoError — エラーなし</li> <li>• 1:FormErr — フォーマットエラー</li> <li>• 2:ServFail — サーバ障害</li> <li>• 3:NXDomain — 存在していないドメイン</li> <li>• 4:NotImp — 未実装</li> <li>• 5:Refused — クエリ拒否</li> <li>• 6:YXDomain — 名前が存在してはならない状況で存在している</li> <li>• 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</li> <li>• 8:NXRRSet — 存在しているべき RR セットが存在していない</li> <li>• 9:NotAuth — 未承認</li> <li>• 10:NotZone — 名前がゾーンに含まれていない</li> <li>• 16:BADSIG — TSIG 署名失敗</li> <li>• 17:BADKEY — キーが認識されない</li> <li>• 18:BADTIME — 時間範囲外の署名</li> <li>• 19:BADMODE — 不適切な TKEY モード</li> <li>• 20:BADNAME — 重複するキー名</li> <li>• 21:BADALG — サポートされていないアルゴリズム</li> <li>• 22:BADTRUNC — 不適切な切り捨て</li> <li>• 3841(NXDOMAIN):ファイアウォールからの NXDOMAIN 応答</li> <li>• 3842:SINKHOLE — ファイアウォールからのシンクホール応答</li> </ul> |
| 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。<br>**: 不明<br>na: 北米<br>as: アジア<br>af: アフリカ<br>eu: 欧州<br>sa: 南米<br>au: オーストラリア<br>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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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 番目のモニター 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へ流れる場合の 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。<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>an : 南極<br>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 <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> 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ス 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ド 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。<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>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 IPv6 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 レスポンドが使用するポート。   |
| 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。 <ul style="list-style-type: none"> <li>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。</li> <li>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)。</li> </ul> |
| 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   | <p>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。</p> <ul style="list-style-type: none"> <li>不明</li> <li>Do Not Decrypt</li> <li>ブロック(Block)</li> <li>Block With Reset</li> <li>Decrypt (Known Key)</li> <li>Decrypt (Replace Key)</li> <li>Decrypt (Resign)</li> </ul> |
| ssl_cipher_suite    | <p>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、<br/> <a href="http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml">www.iana.org/assignments/tls-parameters/tls-parameters.xhtml</a> を参照してください。</p>   |
| ssl_expected_action | <p>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。</p> <ul style="list-style-type: none"> <li>不明</li> <li>Do Not Decrypt</li> <li>ブロック(Block)</li> <li>Block With Reset</li> <li>Decrypt (Known Key)</li> <li>Decrypt (Replace Key)</li> <li>Decrypt (Resign)</li> </ul>   |

表 7-2 connection\_log のフィールド(続き)

| フィールド          | 説明   |
|----------------|--|
| ssl_flow_flags | <p>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。</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 0x00000002:NSE_FLOW_INITIALIZED — 内部構造が処理可能です</li> <li>• 0x00000004:NSE_FLOW_INTERCEPT — SSL セッションが代行受信されました</li> <li>• 0x40000000:CH_CIPHERS_MODIFIED — client hello で暗号が変更されています。</li> <li>• 0x80000000:CH_CURVES_MODIFIED — client hello で暗号曲線が変更されています。</li> <li>• 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。</li> <li>• 0x200000000:CH_SESSION_ID_ZEROED — client hello でセッション ID が削除されました。</li> <li>• 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。</li> <li>• 0x800000000:CH_EXTENSION_REMOVED — TLS 拡張子が client hello から削除されました。</li> <li>• 0x1000000000:CH_ALPN_MODIFIED — client hello の ALPN 拡張子が変更されました。</li> <li>• 0x2000000000:CH_PADDING_MODIFIED — client hello の padding 拡張子が変更されました。</li> <li>• 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。</li> <li>• 0x8000000000:CH_ALPN_HAS_H2 — client hello の ALPN 拡張子に HTTP/2 が追加されました。</li> <li>• 0x10000000000:SH_ALPN_HAS_H2 — server hello の ALPN 拡張子に HTTP/2 が追加されました。</li> </ul> |

表 7-2 connection\_log のフィールド(続き)

| フィールド             | 説明   |
|-------------------|--|
| ssl_flow_messages | <p>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、<a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> を参照してください。</p> <ul style="list-style-type: none"> <li>• 0x00000001:NSE_MT__HELLO_REQUEST</li> <li>• 0x00000002:NSE_MT__CLIENT_ALERT</li> <li>• 0x00000004:NSE_MT__SERVER_ALERT</li> <li>• 0x00000008:NSE_MT__CLIENT_HELLO</li> <li>• 0x00000010:NSE_MT__SERVER_HELLO</li> <li>• 0x00000020:NSE_MT__SERVER_CERTIFICATE</li> <li>• 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE</li> <li>• 0x00000080:NSE_MT__CERTIFICATE_REQUEST</li> <li>• 0x00000100:NSE_MT__SERVER_HELLO_DONE</li> <li>• 0x00000200:NSE_MT__CLIENT_CERTIFICATE</li> <li>• 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE</li> <li>• 0x00000800:NSE_MT__CERTIFICATE_VERIFY</li> <li>• 0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC</li> <li>• 0x00002000:NSE_MT__CLIENT_FINISHED</li> <li>• 0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC</li> <li>• 0x00008000:NSE_MT__SERVER_FINISHED</li> <li>• 0x00010000:NSE_MT__NEW_SESSION_TICKET</li> <li>• 0x00020000:NSE_MT__HANDSHAKE_OTHER</li> <li>• 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT</li> <li>• 0x00080000:NSE_MT__APP_DATA_FROM_SERVER</li> </ul> |

表 7-2 connection\_log のフィールド(続き)

| フィールド                   | 説明  |
|-------------------------|---|
| ssl_flow_status         | <p>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。</p> <ul style="list-style-type: none"> <li>• 'Unknown'</li> <li>• 'No Match'</li> <li>• 'Success'</li> <li>• 'Uncached Session'</li> <li>• 'Unknown Cipher Suite'</li> <li>• 'Unsupported Cipher Suite'</li> <li>• 'Unsupported SSL Version'</li> <li>• 'SSL Compression Used'</li> <li>• 'Session Undecryptable in Passive Mode'</li> <li>• 'Handshake Error'</li> <li>• 'Decryption Error'</li> <li>• 'Pending Server Name Category Lookup'</li> <li>• 'Pending Common Name Category Lookup'</li> <li>• 'Internal Error'</li> <li>• 'Network Parameters Unavailable'</li> <li>• 'Invalid Server Certificate Handle'</li> <li>• 'Server Certificate Fingerprint Unavailable'</li> <li>• 'Cannot Cache Subject DN'</li> <li>• 'Cannot Cache Issuer DN'</li> <li>• 'Unknown SSL Version'</li> <li>• 'External Certificate List Unavailable'</li> <li>• 'External Certificate Fingerprint Unavailable'</li> <li>• 'Internal Certificate List Invalid'</li> <li>• 'Internal Certificate List Unavailable'</li> <li>• 'Internal Certificate Unavailable'</li> <li>• 'Internal Certificate Fingerprint Unavailable'</li> <li>• 'Server Certificate Validation Unavailable'</li> <li>• 'Server Certificate Validation Failure'</li> <li>• 'Invalid Action'</li> </ul> |
| 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。 <ul style="list-style-type: none"> <li>• 1:高リスク</li> <li>• 2:疑わしいサイト</li> <li>• 3:セキュリティ リスクのある無害なサイト</li> <li>• 4:無害なサイト</li> <li>• 5:既知</li> </ul>                   |
| 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。 <ul style="list-style-type: none"> <li>• アプリケーションの名前(確実な識別が可能な場合)。</li> <li>• 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)。</li> <li>• 空白(接続に HTTP トラフィックがない場合)。</li> </ul> |

## 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<br>または<br>client_application_id<br>または<br>web_application_id | application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>rna_host_service_payload.web_application_id |
| initiator_ipaddr<br>または<br>responder_ipaddr  | rna_host_ip_map.ipaddr<br>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せん。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 ホストとレスポンド 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。 <ul style="list-style-type: none"> <li>• アプリケーションの名前(確実な識別が可能な場合)</li> <li>• 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)</li> <li>• pending(システムがさらにデータを必要としている場合)</li> <li>• 空白(接続にアプリケーション情報がない場合)</li> </ul> |
| bytes_recv                | セッションレスポンド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。 <ul style="list-style-type: none"> <li>• rna: シスコ デバイスで検出された場合</li> <li>• netflow: NetFlow 対応デバイスによりエクスポートされる場合</li> </ul>  |
| 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 <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> 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 <code>ipv4_address</code> , <code>ipv6_address</code> 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 ( <code>sensor_name</code> 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。 <ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul> |
| 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                     | <code>application_info.application_id</code><br><code>application_host_map.application_id</code><br><code>application_tag_map.application_id</code><br><code>rna_host_service_info.application_protocol_id</code><br><code>rna_host_client_app_payload.web_application_id</code><br><code>rna_host_client_app_payload.client_application_id</code><br><code>rna_host_client_app.client_application_id</code><br><code>rna_host_client_app.application_protocol_id</code><br><code>rna_host_service_payload.web_application_id</code> |
| initiator_ipaddr<br>または<br>responder_ipaddr | <code>rna_host_ip_map.ipaddr</code><br><code>user_ipaddr_history.ipaddr</code>   |

## 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      | <p>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。</p> <ul style="list-style-type: none"> <li>• IP Block</li> <li>• IP Monitor</li> <li>• User Bypass</li> <li>• File Monitor</li> <li>• File Block</li> <li>• Intrusion Monitor</li> <li>• Intrusion Block</li> <li>• File Resume Block</li> <li>• File Resume Allow</li> <li>• File Custom Detection</li> <li>• SSL Block</li> <li>• DNS Block</li> <li>• DNS Monitor</li> <li>• URL Block</li> <li>• URL Monitor</li> <li>• HTTP Injection</li> <li>• Intelligent App Bypass</li> <li>• ログに記録された接続がない場合は空白</li> </ul> |
| 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。 <ul style="list-style-type: none"> <li>• アプリケーションの名前(確実な識別が可能な場合)</li> <li>• 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)</li> <li>• pending(システムがさらにデータを必要としている場合)</li> <li>• 空白(接続にアプリケーション情報がない場合)</li> </ul>   |
| bytes_recv                 | セッション レスポンド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    | <p>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。</p> <ul style="list-style-type: none"> <li>• アプリケーションの名前(確実な識別が可能な場合)</li> <li>• 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)。</li> <li>• 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)。</li> </ul>  |
| 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            | <p>接続情報の検出ソース。次のいずれかを行います。</p> <ul style="list-style-type: none"> <li>• rna:シスコ デバイスで検出された場合</li> <li>• netflow:NetFlow 対応デバイスによりエクスポートされる場合</li> </ul>  |
| 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               | <p>DNS 応答。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0:NoError — エラーなし</li> <li>• 1:FormErr — フォーマット エラー</li> <li>• 2:ServFail — サーバ障害</li> <li>• 3:NXDomain — 存在していないドメイン</li> <li>• 4:NotImp — 未実装</li> <li>• 5:Refused — クエリ拒否</li> <li>• 6:YXDomain — 名前が存在してはならない状況で存在している</li> <li>• 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</li> <li>• 8:NXRRSet — 存在しているべき RR セットが存在していない</li> <li>• 9:NotAuth — 未承認</li> <li>• 10:NotZone — 名前がゾーンに含まれていない</li> <li>• 16:BADSIG — TSIG 署名失敗</li> <li>• 17:BADKEY — キーが認識されない</li> <li>• 18:BADTIME — 時間範囲外の署名</li> <li>• 19:BADMODE — 不適切な TKEY モード</li> <li>• 20:BADNAME — 重複するキー名</li> <li>• 21:BADALG — サポートされていないアルゴリズム</li> <li>• 22:BADTRUNC — 不適切な切り捨て</li> <li>• 3841(NXDOMAIN):ファイアウォールからの NXDOMAIN 応答</li> <li>• 3842:SINKHOLE — ファイアウォールからのシンクホール応答</li> </ul> |
| 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。<br>**:不明<br>na:北米<br>as:アジア<br>af:アフリカ<br>eu:欧州<br>sa:南米<br>au:オーストラリア<br>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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの 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 番目のモニタールールの名前。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 番目のモニタールールの名前。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 番目のモニタールールの名前。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 番目のモニタールールの名前。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 番目のモニタールールの名前。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 番目のモニタールールの名前。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 番目のモニタールールの名前。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 番目のモニター 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へ流れる場合の 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。<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>an : 南極<br>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 <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> 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ス 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ス 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。<br>**: 不明<br>na: 北米<br>as: アジア<br>af: アフリカ<br>eu: 欧州<br>sa: 南米<br>au: オーストラリア<br>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 IPv6 アドレスのバイナリ表現。  |
| responder_port             | セッション レスポンスが使用するポート。   |
| 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)のいずれかであるか。  |
| 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。 <ul style="list-style-type: none"> <li>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。</li> <li>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)。</li> </ul> |

表 7-6 si\_connection\_log のフィールド(続き)

| フィールド               | 説明   |
|---------------------|--|
| ssl_actual_action   | <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 'Unknown'</li> <li>• 'Do Not Decrypt'</li> <li>• 'Block'</li> <li>• 'Block With Reset'</li> <li>• 'Decrypt (Known Key)'</li> <li>• 'Decrypt (Replace Key)'</li> <li>• 'Decrypt (Resign)'</li> </ul> |
| ssl_cipher_suite    | <p>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、<a href="http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml">www.iana.org/assignments/tls-parameters/tls-parameters.xhtml</a> を参照してください。</p>  |
| ssl_expected_action | <p>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。</p> <ul style="list-style-type: none"> <li>• 'Unknown'</li> <li>• 'Do Not Decrypt'</li> <li>• 'Block'</li> <li>• 'Block With Reset'</li> <li>• 'Decrypt (Known Key)'</li> <li>• 'Decrypt (Replace Key)'</li> <li>• 'Decrypt (Resign)'</li> </ul>  |
| ssl_flow_flags      | <p>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。</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 0x00000002:NSE_FLOW__INITIALIZED — 内部構造が処理可能です</li> <li>• 0x00000004:NSE_FLOW__INTERCEPT — SSL セッションが代行受信されました</li> </ul>   |

表 7-6 si\_connection\_log のフィールド(続き)

| フィールド             | 説明   |
|-------------------|--|
| ssl_flow_messages | <p>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、<a href="http://tools.ietf.org/html/rfc5246">http://tools.ietf.org/html/rfc5246</a> を参照してください。</p> <ul style="list-style-type: none"> <li>• 0x00000001:NSE_MT__HELLO_REQUEST</li> <li>• 0x00000002:NSE_MT__CLIENT_ALERT</li> <li>• 0x00000004:NSE_MT__SERVER_ALERT</li> <li>• 0x00000008:NSE_MT__CLIENT_HELLO</li> <li>• 0x00000010:NSE_MT__SERVER_HELLO</li> <li>• 0x00000020:NSE_MT__SERVER_CERTIFICATE</li> <li>• 0x00000040:NSE_MT__SERVER_KEY_EXCHANGE</li> <li>• 0x00000080:NSE_MT__CERTIFICATE_REQUEST</li> <li>• 0x00000100:NSE_MT__SERVER_HELLO_DONE</li> <li>• 0x00000200:NSE_MT__CLIENT_CERTIFICATE</li> <li>• 0x00000400:NSE_MT__CLIENT_KEY_EXCHANGE</li> <li>• 0x00000800:NSE_MT__CERTIFICATE_VERIFY</li> <li>• 0x00001000:NSE_MT__CLIENT_CHANGE_CIPHER_SPEC</li> <li>• 0x00002000:NSE_MT__CLIENT_FINISHED</li> <li>• 0x00004000:NSE_MT__SERVER_CHANGE_CIPHER_SPEC</li> <li>• 0x00008000:NSE_MT__SERVER_FINISHED</li> <li>• 0x00010000:NSE_MT__NEW_SESSION_TICKET</li> <li>• 0x00020000:NSE_MT__HANDSHAKE_OTHER</li> <li>• 0x00040000:NSE_MT__APP_DATA_FROM_CLIENT</li> <li>• 0x00080000:NSE_MT__APP_DATA_FROM_SERVER</li> </ul> |

表 7-6 si\_connection\_log のフィールド(続き)

| フィールド                   | 説明  |
|-------------------------|---|
| ssl_flow_status         | <p>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。</p> <ul style="list-style-type: none"> <li>• 'Unknown'</li> <li>• 'No Match'</li> <li>• 'Success'</li> <li>• 'Uncached Session'</li> <li>• 'Unknown Cipher Suite'</li> <li>• 'Unsupported Cipher Suite'</li> <li>• 'Unsupported SSL Version'</li> <li>• 'SSL Compression Used'</li> <li>• 'Session Undecryptable in Passive Mode'</li> <li>• 'Handshake Error'</li> <li>• 'Decryption Error'</li> <li>• 'Pending Server Name Category Lookup'</li> <li>• 'Pending Common Name Category Lookup'</li> <li>• 'Internal Error'</li> <li>• 'Network Parameters Unavailable'</li> <li>• 'Invalid Server Certificate Handle'</li> <li>• 'Server Certificate Fingerprint Unavailable'</li> <li>• 'Cannot Cache Subject DN'</li> <li>• 'Cannot Cache Issuer DN'</li> <li>• 'Unknown SSL Version'</li> <li>• 'External Certificate List Unavailable'</li> <li>• 'External Certificate Fingerprint Unavailable'</li> <li>• 'Internal Certificate List Invalid'</li> <li>• 'Internal Certificate List Unavailable'</li> <li>• 'Internal Certificate Unavailable'</li> <li>• 'Internal Certificate Fingerprint Unavailable'</li> <li>• 'Server Certificate Validation Unavailable'</li> <li>• 'Server Certificate Validation Failure'</li> <li>• 'Invalid Action'</li> </ul> |
| 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。 <ul style="list-style-type: none"> <li>• 1:高リスク</li> <li>• 2:疑わしいサイト</li> <li>• 3:セキュリティ リスクのある無害なサイト</li> <li>• 4:無害なサイト</li> <li>• 5:既知</li> </ul>                   |
| 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。 <ul style="list-style-type: none"> <li>• アプリケーションの名前(確実な識別が可能な場合)。</li> <li>• 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)。</li> <li>• 空白(接続に HTTP トラフィックがない場合)。</li> </ul> |

## 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<br>または<br>application_id<br>または<br>client_application_id<br>または<br>web_application_id | application_info.application_id<br>application_host_map.application_id<br>application_tag_map.application_id<br>rna_host_service_info.application_protocol_id<br>rna_host_client_app_payload.web_application_id<br>rna_host_client_app_payload.client_application_id<br>rna_host_client_app.client_application_id<br>rna_host_client_app.application_protocol_id<br>rna_host_service_payload.web_application_id |
| initiator_ipaddr<br>または<br>responder_ipaddr   | rna_host_ip_map.ipaddr<br>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;
```







## スキーマ: ユーザ アクティビティ テーブル

この章では、ユーザ アクティビティ および アイデンティティ イベントのスキーマとサポートされている結合について説明します。Firepower システム は、さまざまなユーザ ログイン (LDAP、POP3、IMAP、SMTP、AIM、SIP など) を追跡することでネットワークでのユーザ アクティビティを検出できます。

詳細については、次の表に示す項を参照してください。

表 8-1 ユーザ アイデンティティ 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 |
|--|-------------------------------------|---------|
| <a href="#">discovered_users (8-1 ページ)</a>     | システムにより検出されたユーザに関する情報。              | 5.0+    |
| <a href="#">user_discovery_event (8-3 ページ)</a> | ネットワーク上のユーザ アクティビティの詳細を示すユーザ検出イベント。 | 5.0+    |
| <a href="#">user_ioc_state (8-5 ページ)</a>       | ユーザの侵害状態が格納されます。                    | 6.2 以降  |

### discovered\_users

**discovered\_users** テーブルには、システムにより検出された各ユーザの詳細情報が格納されます。

**discovered\_users** テーブルは、Firepower システムのバージョン 5.0 以降で廃止されたテーブル **rua\_users** 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。

- [discovered\\_users のフィールド \(8-2 ページ\)](#)
- [discovered\\_users の結合 \(8-2 ページ\)](#)
- [discovered\\_users のサンプル クエリ \(8-2 ページ\)](#)

## discovered\_users のフィールド

次の表に、`discovered_users` 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 8-2 `discovered_users` のフィールド

| フィールド                         | 説明   |
|-------------------------------|--|
| <code>dept</code>             | ユーザの所属部門。  |
| <code>email</code>            | ユーザの電子メール アドレス。  |
| <code>first_name</code>       | ユーザの名前。  |
| <code>ip_address</code>       | このフィールドは廃止されており、すべてのクエリに対して <code>null</code> が返されます。      |
| <code>ipaddr</code>           | ユーザ ログインが検出されたホストの IPv4 または IPv6 アドレスのバイナリ表現。              |
| <code>last_name</code>        | ユーザの姓。   |
| <code>last_seen_sec</code>    | システムがユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。                   |
| <code>last_updated_sec</code> | ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。                             |
| <code>name</code>             | ユーザの名前。  |
| <code>phone</code>            | ユーザの電話番号。  |
| <code>rna_service</code>      | 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 <code>null</code> を返します。 |
| <code>user_id</code>          | ホストの最終ログイン ユーザの内部識別番号。                                     |

## discovered\_users の結合

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

表 8-3 `discovered_users` の結合

| 左結合できるフィールド          | 結合できる他のテーブルの結合タイプ  |
|----------------------|--|
| <code>user_id</code> | <code>user_discovery_event.user_id</code><br><code>user_ipaddr_history.user_id</code><br><code>user_ioc_state.user_id</code> |

## discovered\_users のサンプルクエリ

次のクエリは、指定された日時以降に生成された検出ユーザ レコードを最大 25 件まで返します。

```
SELECT user_id, ip_address, email, name, last_seen_sec, last_updated_sec
FROM discovered_users
WHERE last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00")
LIMIT 0, 25;
```

## user\_discovery\_event

`user_discovery_event` テーブルには、各ユーザ検出イベントのレコードが格納されます。

バージョン 5.0 以降、Firepower システム は検出エンジンではなく、管理対象デバイス レベルでのユーザアクティビティの検出を記録することに注意してください。このテーブルの `detection_engine_name` フィールドと `detection_engine_uuid` フィールドはそれぞれ、`sensor_name` フィールドと `sensor_uuid` フィールドに置き換えられました。これらのフィールドに対するクエリは、ユーザ検出イベントを生成した管理対象デバイスに関する情報を返します。

詳細については、次の項を参照してください。

- [user\\_discovery\\_event のフィールド \(8-3 ページ\)](#)
- [user\\_discovery\\_event の結合 \(8-4 ページ\)](#)
- [user\\_discovery\\_event のサンプルクエリ \(8-4 ページ\)](#)

## user\_discovery\_event のフィールド

次の表に、`user_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 8-4 `user_discovery_event` のフィールド

| フィールド                                  | 説明  |
|--|---|
| <code>application_protocol_id</code>   | 検出されたアプリケーションプロトコルの内部 ID。   |
| <code>application_protocol_name</code> | 次のいずれかになります。 <ul style="list-style-type: none"> <li>• 接続で使用されたアプリケーションの名前 (LDAP、POP3 など)</li> <li>• <code>pending</code> (システムで、何らかの理由でアプリケーションを識別できない場合)</li> <li>• 空白 (接続にアプリケーション情報がない場合)</li> </ul> |
| <code>description</code>               | 検出イベントのタイプが [Delete User Identity] または [User Identity Dropped] の場合は、ユーザ名。それ以外の場合は空白。  |
| <code>domain_name</code>               | ユーザが検出されたのドメインの名前。  |
| <code>domain_uuid</code>               | 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。  |
| <code>endpoint_profile</code>          | 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。   |
| <code>event_id</code>                  | 検出イベントの内部識別番号。  |
| <code>event_time_sec</code>            | 検出イベントの日時を示す UNIX タイムスタンプ。  |
| <code>event_type</code>                | 検出イベントのタイプ。New User Identity や User Login など。   |
| <code>ip_address</code>                | 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 <code>null</code> を返します。  |
| <code>ipaddr</code>                    | ユーザアクティビティが検出されたホストの IP アドレスのバイナリ表現。  |
| <code>location_ip</code>               | 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。  |
| <code>reported_by</code>               | ユーザログインを報告する Active Directory サーバの IPv4 アドレス、IPv6 アドレス、または NetBIOS 名。   |
| <code>security_group</code>            | ネットワークトラフィックグループの ID 番号。  |

表 8-4 user\_discovery\_event のフィールド(続き)

| フィールド                 | 説明   |
|-----------------------|--|
| sensor_address        | ユーザ検出イベントが検出された管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code> , <code>ipv6_address</code> です。 |
| sensor_name           | ユーザ検出イベントが検出された管理対象デバイスのテキスト名。   |
| sensor_uuid           | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> 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       | ユーザの名。   |
| 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        | ユーザの姓。   |
| user_last_seen_sec    | システムがユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。   |
| user_last_updated_sec | ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。   |
| user_name             | 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。   |

## user\_discovery\_event の結合

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

表 8-5 user\_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              | <code>rna_host_ip_map.ipaddr</code><br><code>user_ipaddr_history.ipaddr</code>   |
| user_id             | <code>discovered_users.user_id</code><br><code>user_ipaddr_history.user_id</code><br><code>user_ioc_state.user_id</code> |

## user\_discovery\_event のサンプルクエリ

次のクエリは、特定の日時以降に、選択された管理対象デバイスにより生成されたユーザ イベント レコードを最大 25 件まで返します。

```
SELECT event_time_sec, ipaddr, sensor_name, event_type, user_name, user_last_seen_sec,
user_last_updated_sec
FROM user_discovery_event
WHERE sensor_name = sensor_name
AND user_last_seen_sec >= UNIX_TIMESTAMP("2011-10-01 00:00:00") ORDER BY event_type ASC
LIMIT 0, 25;
```

## user\_ioc\_state

`user_ioc_state` テーブルには、モニタ対象ネットワークのユーザの 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。

- [user\\_ioc\\_state フィールド \(8-5 ページ\)](#)
- [user\\_ioc\\_state 結合 \(8-7 ページ\)](#)
- [user\\_ioc\\_state サンプル クエリ \(8-7 ページ\)](#)

## user\_ioc\_state フィールド

次の表で、`user_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 8-6 `user_ioc_state` フィールド

| フィールド                                  | 説明   |
|--|--|
| <code>first_seen</code>                | 侵害が最初に検出された時点を示す UNIX タイムスタンプ。   |
| <code>first_seen_sensor_address</code> | 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 <code>ipv4_address</code> , <code>ipv6_address</code> です。  |
| <code>first_seen_sensor_name</code>    | 侵害を最初に検出した管理対象デバイス。  |
| <code>user_id</code>                   | ユーザの ID 番号。  |
| <code>ioc_category</code>              | 侵害のカテゴリ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• CnC Connected</li> <li>• Exploit Kit</li> <li>• High Impact Attack</li> <li>• Low Impact Attack</li> <li>• Malware Detected</li> <li>• Malware Executed</li> <li>• Dropper Infection</li> <li>• Java Compromise</li> <li>• Word Compromise</li> <li>• Adobe Reader Compromise</li> <li>• Excel Compromise</li> <li>• PowerPoint Compromise</li> <li>• QuickTime Compromise</li> </ul> |
| <code>ioc_description</code>           | 侵害の説明  |

表 8-6 user\_ioc\_state フィールド(続き)

| フィールド          | 説明   |
|----------------|--|
| ioc_event_type | <p>侵害のイベント タイプ。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Adobe Reader launched shell</li> <li>• Dropper Infection Detected by AMP for Endpoints</li> <li>• Excel Compromise Detected by AMP for Endpoints</li> <li>• Excel launched shell  </li> <li>• Impact 1 Intrusion Event - attempted-admin</li> <li>• Impact 1 Intrusion Event - attempted-user</li> <li>• Impact 1 Intrusion Event - successful-admin</li> <li>• Impact 1 Intrusion Event - successful-user</li> <li>• Impact 1 Intrusion Event - web-application-attack</li> <li>• Impact 2 Intrusion Event - attempted-admin</li> <li>• Impact 2 Intrusion Event - attempted-user</li> <li>• Impact 2 Intrusion Event - successful-admin</li> <li>• Impact 2 Intrusion Event - successful-user</li> <li>• Impact 2 Intrusion Event - web-application-attack</li> <li>• Intrusion Event - exploit-kit</li> <li>• Intrusion Event - malware-backdoor</li> <li>• Intrusion Event - malware-CnC</li> <li>• Java Compromise Detected by AMP for Endpoints</li> <li>• Java launched shell</li> <li>• PDF Compromise Detected by AMP for Endpoints</li> <li>• PowerPoint Compromise Detected by AMP for Endpoints</li> <li>• PowerPoint launched shell</li> <li>• QuickTime Compromise Detected by AMP for Endpoints</li> <li>• QuickTime launched shell</li> <li>• Security Intelligence Event - CnC</li> <li>• Suspected Botnet Detected by AMP for Endpoints</li> <li>• Threat Detected by AMP for Endpoints - Subtype is 'executed'</li> <li>• Threat Detected by AMP for Endpoints - Subtype is not 'executed'</li> <li>• Threat Detected in File Transfer - Action is not 'block'</li> <li>• Word Compromise Detected by AMP for Endpoints</li> <li>• Word launched shell</li> </ul> |
| 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 8-6 user\_ioc\_state 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 <code>ipv4_address</code> , <code>ipv6_address</code> です。 |
| last_seen_sensor_name    | 侵害を最後に検出した管理対象デバイス。   |

## user\_ioc\_state 結合

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

表 8-7 user\_ioc\_state 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   |
|---------------------|--|
| user_id             | <code>discovered_users.user_id</code><br><code>user_ipaddr_history.user_id</code><br><code>user_discovery_event.user_id</code> |

## user\_ioc\_state 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 user_id, ioc_id
FROM user_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;
```







## スキーマ: 関連テーブル

この章では、関連関連イベント(修復ステータスやホワイト リスト イベントなど)のスキーマとサポートされている結合について説明します。詳細については、次の表に示す項を参照してください。

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

## compliance\_event

**compliance\_event** テーブルには、Firepower Management Center により生成される関連イベントに関する情報が格納されます。

詳細については、次の項を参照してください。

- [compliance\\_event のフィールド \(9-2 ページ\)](#)
- [compliance\\_event の結合 \(9-6 ページ\)](#)
- [compliance\\_event のサンプル クエリ \(9-6 ページ\)](#)

## compliance\_event のフィールド

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

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

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

表 9-2 compliance\_event のフィールド

| フィールド                 | 説明   |
|-----------------------|--|
| blocked               | 侵入イベントをトリガーしたパケットの処理を示す値。 <ul style="list-style-type: none"> <li>0: パケットはドロップされなかった</li> <li>1: パケットはドロップされた (インライン型、スイッチ型、またはルーティング型展開)</li> <li>2: 侵入ポリシーが、インライン型、スイッチ型、またはルーティング型展開のデバイスに適用されている場合は、イベントをトリガーしたパケットがドロップされている可能性がある。</li> </ul> |
| description           | 関連イベントと、このイベントがどのように引き起こされたかに関する情報。  |
| detection_engine_name | バージョン 5.0 で廃止されたフィールド。すべてのクエリに対して null を返します。  |
| detection_engine_uuid | バージョン 5.0 で廃止されたフィールド。すべてのクエリに対して null を返します。  |
| domain_name           | イベントが検出されたドメインの名前。   |
| domain_uuid           | イベントが検出されたドメインの UUID。これはバイナリで示されます。  |
| dst_host_criticality  | 関連イベントに関連する宛先ホストにユーザが割り当てたホスト重要度: None、Low、Medium、または High   |
| dst_host_type         | 宛先ホストのタイプ: Host、Router、Bridge、NAT Device、または Load Balancer   |
| dst_ip_address        | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。   |
| dst_ip_address_v6     | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。   |
| dst_ipaddr            | トリガー イベントに関連する宛先ホストの IPv4 または IPv6 アドレスのバイナリ表現。  |
| dst_os_product        | 宛先ホストのオペレーティング システムの名前。  |

表 9-2 compliance\_event のフィールド(続き)

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

表 9-2 compliance\_event のフィールド(続き)

| フィールド                      | 説明  |
|----------------------------|---|
| impact                     | <p>イベントの影響フラグ値。値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 1: レッド(脆弱)</li> <li>• 2: オレンジ(脆弱の可能性あり)</li> <li>• 3: イエロー(現在は脆弱でない)</li> <li>• 4: ブルー(不明なターゲット)</li> <li>• 5: グレー(不明な影響)</li> </ul> <p>関連ルールが侵入イベントによってトリガーされた場合にのみ設定します。</p> |
| interface_egress_name      | 接続に関連付けられた入力インターフェイス。   |
| interface_ingress_name     | 接続に関連付けられた出力インターフェイス。   |
| policy_name                | 違反が発生した関連ポリシー。  |
| policy_rule_name           | ポリシー違反をトリガーした関連ルール。   |
| policy_rule_uuid           | 関連ルールの固有識別子。  |
| policy_time_sec            | 関連イベントが生成された日時を示す UNIX タイムスタンプ。   |
| policy_uuid                | 関連ポリシーの固有識別子。   |
| priority                   | <p>関連イベントのプライオリティ。ユーザインターフェイスで設定されます。このイベントプライオリティは、トリガーされたルールのプライオリティまたは違反が発生した関連ポリシーのプライオリティによって決まります。</p>  |
| protocol_name              | イベントに関連付けられているプロトコル(使用可能な場合)。   |
| protocol_num               | IANA 指定のプロトコル番号(使用可能な場合)。   |
| rna_event_type             | バージョン 5.0 で廃止されたフィールド。すべてのクエリに対して null を返します。   |
| rua_event_type             | バージョン 5.0 で廃止されたフィールド。すべてのクエリに対して null を返します。   |
| rule_generator_id          | トリガー侵入イベントを生成したコンポーネントのジェネレータ ID 番号 (GID)。  |
| rule_message               | <p>関連ルールをトリガーした侵入イベントを説明するテキスト。ルールベースのイベントの場合、イベントメッセージはルールから生成されます。デコーダベースおよびプリプロセッサベースのイベントの場合、メッセージはハードコーディングされています。</p>   |
| rule_signature_id          | <p>イベントのシグニチャ ID (SID)。トリガー侵入イベントが生成される原因となった特定のルール、デコーダメッセージ、またはプリプロセッサメッセージを識別します。</p>  |
| security_zone_egress_name  | 関連イベントの出力セキュリティゾーン。   |
| security_zone_ingress_name | 関連イベントの入力セキュリティゾーン。   |
| sensor_address             | <p>コンプライアンス イベントをトリガーした基礎となるイベントを生成した管理対象デバイスの IP アドレス。形式は <code>ipv4_address</code>, <code>ipv6_address</code> です。</p>   |
| sensor_name                | <p>コンプライアンス イベントをトリガーした基礎となるイベントを生成した管理対象デバイス。</p>  |
| sensor_uuid                | 管理対象デバイスの固有識別子 ( <code>sensor_name</code> が null の場合は 0)。   |

表 9-2 compliance\_event のフィールド(続き)

| フィールド                     | 説明  |
|---------------------------|---|
| src_host_criticality      | コンプライアンス イベントに関連する送信元ホストにユーザが割り当てたホスト重要度: None、Low、Medium、または High。   |
| src_host_type             | 送信元ホストのタイプ: Host、Router、Bridge、NAT Device、または Load Balancer。  |
| src_ip_address            | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。  |
| src_ip_address_v6         | バージョン 5.2 で廃止されたフィールド。後方互換性を維持するため、このフィールドの値は null には設定されませんが、信頼できません。  |
| src_ipaddr                | トリガー イベントに関連する送信元ホストの IPv4 または IPv6 アドレスのバイナリ表現。  |
| src_os_product            | 送信元ホストのオペレーティング システムの名前。  |
| src_os_vendor             | 送信元ホストのオペレーティング システムのベンダー。  |
| src_os_version            | 送信元ホストのオペレーティング システムのバージョン番号。   |
| src_port                  | 送信元ホストのポート番号。ICMP トラフィックの場合は ICMP タイプが表示されます。   |
| src_rna_service           | トリガー イベントに関連付けられている送信元ホストのアプリケーションプロトコル(判明している場合)。判明していない場合は、次のいずれかになります。 <ul style="list-style-type: none"> <li>• none または空白: アプリケーションプロトコルトラフィックがありません。</li> <li>• unknown: 既知のサーバフィンガープリントに基づいてサーバとアプリケーションプロトコルを識別できませんでした。</li> <li>• pending: システムにさらに情報が必要です。</li> </ul> |
| src_user_dept             | 送信元ユーザの所属部門。  |
| src_user_email            | 送信元ユーザの電子メール アドレス。  |
| src_user_first_name       | 送信元ユーザの名前。  |
| src_user_id               | 送信元ユーザの内部識別番号。これは、イベント発生前に送信元ホストにログインしていた最終ユーザです。   |
| src_user_last_name        | 送信元ユーザの姓。   |
| src_user_last_seen_sec    | システムが送信元ユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。   |
| src_user_last_updated_sec | 送信元ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。   |
| src_user_name             | 送信元ユーザのログイン ユーザ名。   |
| src_user_phone            | 送信元ユーザの電話番号。  |
| src_vlan_id               | 送信元ホストの VLAN 識別番号(該当する場合)。  |
| user_event_type           | トリガー ユーザ イベントのタイプ(New User Identity または User Login など)。   |

## compliance\_event の結合

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

表 9-3 **compliance\_event** の結合

| このテーブルで結合に使用するフィールド             | 結合できるフィールド   |
|---------------------------------|--|
| dst_ipaddr<br>または<br>src_ipaddr | <a href="#">rna_host_ip_map.ipaddr</a><br><a href="#">user_ipaddr_history.ipaddr</a> |

## compliance\_event のサンプルクエリ

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

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

## remediation\_status

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

詳細については、次の項を参照してください。

- [remediation\\_status](#) のフィールド (9-7 ページ)
- [remediation\\_status](#) の結合 (9-7 ページ)
- [remediation\\_status](#) のサンプルクエリ (9-7 ページ)

## remediation\_status のフィールド

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

表 9-4 remediation\_status のフィールド

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

## remediation\_status の結合

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

## remediation\_status のサンプルクエリ

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

```
SELECT policy_time_sec, remediation_time_sec, remediation_name, policy_name,
policy_rule_name, status_text
FROM remediation_status WHERE remediation_time_sec <= UNIX_TIMESTAMP("2011-10-01
00:00:00")
ORDER BY policy_time_sec
DESC LIMIT 0, 25;
```

## white\_list\_event

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

バージョン 5.0 以降、Firepower システム は検出エンジンではなく、管理対象デバイス レベルでのネットワークおよびユーザ アクティビティの検出を記録することに注意してください。

**white\_list\_event** テーブルの `detection_engine_name` フィールドと `detection_engine_uuid` フィールドは `null` だけを返し、またこれらのフィールドを結合するクエリはレコードを返しませんが、`detection_engine_uuid` フィールドの代わりに `sensor_uuid` フィールドを照会すると、同等の情報が返されます。

詳細については、次の項を参照してください。

- [white\\_list\\_event のフィールド \(9-8 ページ\)](#)
- [white\\_list\\_event の結合 \(9-9 ページ\)](#)
- [white\\_list\\_event のサンプル クエリ \(9-10 ページ\)](#)

## white\_list\_event のフィールド

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

表 9-5 white\_list\_event のフィールド

| フィールド                              | 説明  |
|------------------------------------|---|
| <code>description</code>           | ホワイトリスト違反の説明。   |
| <code>detection_engine_name</code> | 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 <code>null</code> を返します。  |
| <code>detection_engine_uuid</code> | 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 <code>null</code> を返します。  |
| <code>host_criticality</code>      | ホワイトリストに準拠していないホストに対してユーザが割り当てた重要度 ([None]、[Low]、[Medium]、または [High])。                                    |
| <code>host_type</code>             | ホストのタイプ: Host、Router、Bridge、NAT Device、または Load Balancer。   |
| <code>id</code>                    | ホワイトリスト イベントの内部固有識別子。   |
| <code>ip_address</code>            | 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 <code>null</code> を返します。  |
| <code>ip_address_v6</code>         | 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 <code>null</code> を返します。  |
| <code>ipaddr</code>                | 準拠していないホストの IP アドレスのバイナリ表現。   |
| <code>os_product</code>            | オペレーティング システムの製品名。  |
| <code>os_vendor</code>             | オペレーティング システムのベンダー。   |
| <code>os_version</code>            | オペレーティング システムのバージョン番号。  |
| <code>policy_name</code>           | ホワイトリストを含む違反コンプライアンス ポリシー。  |
| <code>policy_time_sec</code>       | イベントが生成された日時を示す UNIX タイムスタンプ。   |
| <code>policy_uuid</code>           | ホワイトリスト イベントを含むコンプライアンス ポリシーの固有識別子。   |
| <code>port</code>                  | サービス ホワイトリスト違反をトリガーしたイベント (非準拠サービスの結果として違反が発生した場合)に関連付けられているポート (存在する場合)。他のタイプのホワイトリスト違反の場合、このフィールドは空白です。 |



表 9-5 white\_list\_event のフィールド(続き)

| フィールド                 | 説明   |
|-----------------------|--|
| priority              | ホワイト リスト イベントのプライオリティ。ユーザ インターフェイスで設定されます。                                     |
| protocol_name         | イベントに関連付けられているプロトコル(使用可能な場合)。  |
| protocol_num          | IANA 指定のプロトコル番号(使用可能な場合)。  |
| rna_service           | ホワイト リスト違反をトリガーしたサービス(使用可能な場合)。  |
| sensor_address        | トラフィックを検出した管理対象デバイスの IP アドレス。形式は <i>ipv4_address</i> , <i>ipv6_address</i> です。 |
| sensor_name           | ホワイト リスト イベントを生成したデバイス。  |
| sensor_uuid           | 管理対象デバイスの固有識別子 ( <i>sensor_name</i> が null の場合は 0)。                            |
| user_dept             | ユーザの所属部門。  |
| user_email            | ユーザの電子メール アドレス。  |
| user_first_name       | ユーザの名前。  |
| user_id               | イベント発生前にホストにログインしていた最終ユーザの内部 ID 番号。  |
| user_last_name        | ユーザの姓。   |
| user_last_seen_sec    | システムがユーザのログインを最後に報告した日時を示す UNIX タイムスタンプ。                                       |
| user_last_updated_sec | ユーザの情報の最終更新日時を示す UNIX タイムスタンプ。   |
| user_name             | ユーザのログイン ユーザ名。   |
| user_phone            | ユーザの電話番号。  |
| vlan_id               | VLAN 識別番号(該当する場合)。   |
| white_list_name       | 違反が発生したホワイト リスト。   |
| white_list_uuid       | ホワイト リストの固有識別子。  |

## white\_list\_event の結合

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

表 9-6 white\_list\_event の結合

| このテーブルで結合に使用するフィールド | 結合できるフィールド   |
|---------------------|--|
| ipaddr              | <a href="#">rna_host_ip_map.ipaddr</a><br><a href="#">user_ipaddr_history.ipaddr</a> |

## white\_list\_event のサンプルクエリ

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

```
SELECT policy_name, policy_time_sec, ipaddr, user_name, port, description,
white_list_name, priority, host_criticality, sensor_name
FROM white_list_event WHERE policy_time_sec <= UNIX_TIMESTAMP("2011-10-01 00:00:00")
ORDER BY policy_time_sec DESC LIMIT 0, 25;
```

## white\_list\_violation

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

詳細については、次の項を参照してください。

- [white\\_list\\_violation のフィールド \(9-10 ページ\)](#)
- [white\\_list\\_violation の結合 \(9-11 ページ\)](#)
- [white\\_list\\_violation のサンプルクエリ \(9-11 ページ\)](#)

## white\_list\_violation のフィールド

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

表 9-7 **white\_list\_violation** のフィールド

| フィールド         | 説明   |
|---------------|--|
| host_id       | ホワイト リストに違反するホストの ID 番号。   |
| info          | ホワイト リスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。<br>ホワイト リストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらなのかも示されます。 |
| ip_address    | バージョン 5.2 で廃止されたフィールド。すべてのクエリに対して null を返します。  |
| port          | サービス ホワイト リスト違反をトリガーしたイベント (非標準サービスの結果として違反が発生した場合) に関連付けられているポート (存在する場合)。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。                     |
| protocol_name | イベントに関連付けられているプロトコル。   |

表 9-7 white\_list\_violation のフィールド(続き)

| フィールド              | 説明   |
|--------------------|--|
| type               | ホワイト リスト違反のタイプ。非準拠が原因で違反が発生したかどうかを示します。 <ul style="list-style-type: none"><li>オペレーティング システム(os)</li><li>サービス(service)</li><li>クライアントアプリケーション(client app)</li><li>プロトコル(protocol)</li></ul> |
| violation_time_sec | 違反がログに記録された日時を示す UNIX タイムスタンプ。   |
| white_list_name    | 違反が発生したホワイト リスト。   |
| white_list_uuid    | ホワイト リストの固有識別子。  |

## white\_list\_violation の結合

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

## white\_list\_violation のサンプルクエリ

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

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





## スキーマ:ファイルイベント テーブル

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

表 10-1 ファイルイベント テーブルのスキーマ

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

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

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

### file\_event

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

詳細については、次の項を参照してください。

- [file\\_event のフィールド \(10-2 ページ\)](#)
- [file\\_event の結合 \(10-6 ページ\)](#)
- [file\\_event のサンプル クエリ \(10-6 ページ\)](#)

## file\_event のフィールド

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

表 10-2 file\_event のフィールド

| フィールド                   | 説明   |
|-------------------------|--|
| action                  | ファイル タイプに基づいてファイルに対して実行されたアクション。次のいずれかの値になります。 <ul style="list-style-type: none"> <li>• 1:検出</li> <li>• 2:ブロック</li> <li>• 3:マルウェア クラウド ルックアップ</li> <li>• 4:マルウェア ブロック</li> <li>• 5:マルウェア ホワイトリスト</li> <li>• 6:クラウドルックアップ タイムアウト</li> </ul> |
| application_id          | ファイル転送を使用するアプリケーションにマップされている ID 番号。  |
| application_name        | 次のいずれかです。 <ul style="list-style-type: none"> <li>• 接続で使用されたアプリケーションの名前。</li> <li>• pending または unknown(システムがアプリケーションを識別できない場合)。</li> <li>• 空白(接続にアプリケーション情報がない場合)</li> </ul>   |
| archived                | ファイルがアーカイブされているかどうかを示します。  |
| cert_valid_end_date     | 接続で使用された SSL 証明書が有効ではなくなった時点を示す UNIX タイムスタンプ。  |
| cert_valid_start_date   | 接続で使用された SSL 証明書の発行時点を示す UNIX タイムスタンプ。   |
| client_application_id   | クライアントアプリケーションの内部識別番号(該当する場合)。   |
| client_application_name | クライアントアプリケーションの名前(該当する場合)。   |
| connection_sec          | ファイル イベントに関連付けられている接続イベントの UNIX タイムスタンプ(00:00:00 01/01/1970 からの経過秒数)。  |
| counter                 | 同じ秒数で発生した複数のイベントを区別するために使用されるイベント固有のカウンタ。  |
| direction               | ファイルのアップロードとダウンロードのいずれが行われたか。現時点では、この値はプロトコルに完全に依存しています(例えば接続が HTTP の場合はダウンロード)。   |

表 10-2 file\_event のフィールド(続き)

| フィールド                 | 説明   |
|-----------------------|--|
| disposition           | ファイルのマルウェア ステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>CLEAN: ファイルはクリーンであり、マルウェアが含まれていない。</li> <li>UNKNOWN: ファイルにマルウェアが含まれているかどうか不明である。</li> <li>MALWARE: ファイルにマルウェアが含まれている。</li> <li>UNAVAILABLE: ソフトウェアから シスコ クラウドに対して、特性を確認する要求を送信できなかったか、または シスコ クラウド サービスが要求に応答しなかった。</li> <li>CUSTOM SIGNATURE: ファイルがユーザ定義のハッシュと一致するため、ユーザが指定した方法で処理された。</li> </ul> |
| domain_name           | イベントが検出されたドメインの名前。   |
| domain_uuid           | イベントが検出されたドメインの UUID。これはバイナリで示されます。  |
| dst_continent_name    | 宛先ホストが位置する地域の名前<br>** : 不明<br>na : 北米<br>as : アジア<br>af : アフリカ<br>eu : 欧州<br>sa : 南米<br>au : オーストラリア<br>an : 南極  |
| dst_country_id        | 宛先ホストの国のコード。   |
| dst_country_name      | 宛先ホストの国の名前。  |
| dst_ip_address_v6     | バージョン 5.2 で廃止されたフィールド。すべてのクエリに対して null を返します。  |
| dst_ipaddr            | トリガー イベントに関連する宛先ホストの IP アドレスのバイナリ表現。   |
| dst_port              | 接続の宛先のポート番号。   |
| event_description     | イベント タイプに関連付けられている追加イベント情報。  |
| event_id              | イベント識別番号。  |
| file_name             | 検出されたファイルの名前。この名前には、UTF-8 文字を使用できます。   |
| file_sha              | ファイルの SHA256 ハッシュ  |
| file_size             | 検出されたファイルのサイズ(バイト単位)。  |
| file_type             | 検出または検疫されたファイルのファイル タイプ。   |
| file_type_category    | ファイル カテゴリの説明   |
| file_type_category_id | ファイル カテゴリの数値 ID。   |
| file_type_id          | ファイル タイプにマップされている ID 番号。   |
| http_response_code    | イベントで HTTP 要求に対して返された応答コード。  |
| instance_id           | イベントを生成した管理対象デバイスの Snort インスタンスの数値 ID。   |

表 10-2 file\_event のフィールド(続き)

| フィールド               | 説明  |
|---------------------|---|
| netmap_num          | イベントが検出されたドメインの Netmap ID。  |
| policy_uuid         | イベントをトリガーしたアクセス コントロール ポリシーの固有識別子として機能する識別番号。   |
| sandboxed           | ファイルが動的分析のために送信されているかどうかを示します。値は次のとおりです。 <ul style="list-style-type: none"> <li>• Sent for Analysis</li> <li>• Failed to Send</li> <li>• File Size is Too Small</li> <li>• File Size is Too Large</li> <li>• Sent for Analysis</li> <li>• Analysis Complete</li> <li>• Failure (Network Issue)</li> <li>• Failure (Rate Limit)</li> <li>• Failure (File Too Large)</li> <li>• Failure (File Read Error)</li> <li>• Failure (Internal Library Error)</li> <li>• File Not Sent, Disposition Unavailable</li> <li>• Failure (Cannot Run File)</li> <li>• Failure (Analysis Timeout)</li> <li>• File Not Supported</li> </ul> |
| 得点                  | 動的分析中に観測された、悪意のある可能性がある振る舞いに基づく数値 (0 ~ 100)。  |
| security_context    | トラフィックが通過したセキュリティ コンテキスト(仮想ファイアウォール)の説明。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスの場合だけです。  |
| sensor_address      | イベントを提供したデバイスの IP アドレスのバイナリ表現。  |
| sensor_id           | イベントを提供したデバイスの ID。  |
| sensor_name         | イベントレコードを生成した管理対象デバイスのテキスト名。接続デバイスではなくレポート デバイス自体を参照するイベントの場合、このフィールドは null です。   |
| sensor_uuid         | 管理対象デバイスの固有識別子(sensor_name が null の場合は 0)。  |
| signature_processed | ファイルの署名が処理されたかどうかを示します。   |



表 10-2 file\_event のフィールド(続き)

| フィールド                         | 説明  |
|-------------------------------|---|
| src_continent_name            | 送信元ホストが位置する地域の名前<br>*:不明<br>na:北米<br>as:アジア<br>af:アフリカ<br>eu:欧州<br>sa:南米<br>au:オーストラリア<br>an:南極   |
| src_country_id                | 送信元ホストの国のコード。   |
| src_country_name              | 送信元ホストの国の名前。  |
| src_ip_address_v6             | バージョン 5.2 で廃止されたフィールド。すべてのクエリに対して null を返します。   |
| src_ipaddr                    | トリガー イベントに関連する送信元ホストの IPv4 または IPv6 アドレスのバイナリ表現。  |
| src_port                      | 接続元のポート番号。  |
| ssl_issuer_common_name        | SSL 証明書の発行元の共通名。これは一般に証明書発行元のホストとドメイン名ですが、その他の情報が含まれていることもあります。   |
| ssl_issuer_country            | SSL 証明書の発行元の国。  |
| ssl_issuer_organization       | SSL 証明書の発行元の組織。   |
| ssl_issuer_organization_unit  | SSL 証明書の発行元の組織単位。   |
| ssl_serial_number             | 発行元 CA によって割り当てられた SSL 証明書のシリアル番号。  |
| ssl_subject_common_name       | SSL 証明書の件名共通名。これは一般に証明書の件名のホストとドメイン名ですが、その他の情報が含まれていることもあります。   |
| ssl_subject_country           | SSL 証明書の件名の国。   |
| ssl_subject_organization      | SSL 証明書の件名の組織。  |
| ssl_subject_organization_unit | SSL 証明書の件名の組織単位。  |
| storage                       | ファイルの保存ステータス。値は次のとおりです。 <ul style="list-style-type: none"> <li>File Stored</li> <li>Unable to Store File</li> <li>File Size is Too Large</li> <li>File Size is Too Small</li> <li>Unable to Store File</li> <li>File Not Stored, Disposition Unavailable</li> </ul> |
| threat_name                   | 脅威の名前。  |
| timestamp                     | ファイルタイプを識別するために十分なファイルが送信された時点を示す UNIX タイムスタンプ。   |

表 10-2 file\_event のフィールド(続き)

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

## file\_event の結合

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

表 10-3 file\_event の結合

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

## file\_event のサンプルクエリ

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

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



## 廃止テーブル

この付録では、以前のリリースで使用され、現在は廃止となったテーブルについて説明します。これらのテーブルを照会できますが、フィールドの値が正しくない可能性があります(ほとんどの場合フィールド値は null です)。これらのテーブルでは結合はサポートされていません。

表 A-1 廃止テーブル

| テーブル                                    | 置き換わるテーブル   | 最終使用バージョン: |
|---|---|------------|
| application_ip_map                      | <a href="#">application_host_map</a> (6-5 ページ)                  | 5.1.1      |
| rna_ip_host                             | <a href="#">rna_host</a> (6-14 ページ)                             | 5.1.1      |
| rna_ip_host_attribute                   | <a href="#">rna_host_attribute</a> (6-16 ページ)                   | 5.1.1      |
| rna_ip_host_client_app                  | <a href="#">rna_host_client_app</a> (6-17 ページ)                  | 5.1.1      |
| rna_ip_host_client_app_payload          | <a href="#">rna_host_client_app_payload</a> (6-20 ページ)          | 5.1.1      |
| rna_ip_host_os                          | <a href="#">rna_host_os</a> (6-30 ページ)                          | 5.1.1      |
| rna_ip_host_os_vulns                    | <a href="#">rna_host_os_vulns</a> (6-31 ページ)                    | 5.1.1      |
| rna_ip_host_sensor                      | <a href="#">rna_host_sensor</a> (6-34 ページ)                      | 5.1.1      |
| rna_ip_host_service                     | <a href="#">rna_host_service</a> (6-36 ページ)                     | 5.1.1      |
| rna_ip_host_service_banner              | <a href="#">rna_host_service_banner</a> (6-38 ページ)              | 5.1.1      |
| rna_ip_host_service_info                | <a href="#">rna_host_service_info</a> (6-39 ページ)                | 5.1.1      |
| rna_ip_host_service_payload             | <a href="#">rna_host_service_payload</a> (6-43 ページ)             | 5.1.1      |
| rna_ip_host_service_subtype             | <a href="#">rna_host_service_subtype</a> (6-45 ページ)             | 5.1.1      |
| rna_ip_host_service_vulns               | <a href="#">rna_host_service_vulns</a> (6-47 ページ)               | 5.1.1      |
| rna_ip_host_third_party_vuln            | <a href="#">rna_host_third_party_vuln</a> (6-48 ページ)            | 5.1.1      |
| rna_ip_host_third_party_vuln_bugtraq_id | <a href="#">rna_host_third_party_vuln_bugtraq_id</a> (6-50 ページ) | 5.1.1      |
| rna_ip_host_third_party_vuln_cve_id     | <a href="#">rna_host_third_party_vuln_cve_id</a> (6-52 ページ)     | 5.1.1      |
| rna_ip_host_third_party_vuln_rna_id     | <a href="#">rna_host_third_party_vuln_rna_id</a> (6-54 ページ)     | 5.1.1      |
| rna_ip_host_user_history                | <a href="#">user_ipaddr_history</a> (6-62 ページ)                  | 5.1.1      |
| rna_mac_host                            | <a href="#">rna_host_mac_map</a> (6-28 ページ)                     | 5.1.1      |
| rna_mac_host_sensor                     | <a href="#">rna_host_mac_map</a> (6-28 ページ)                     | 5.1.1      |

表 A-1 廃止テーブル

| テーブル               | 置き換わるテーブル   | 最終使用バージョン: |
|--------------------|---|------------|
| rna_mac_ip_map     | <a href="#">rna_host_ip_map (6-27 ページ)</a><br><a href="#">rna_host_mac_map (6-28 ページ)</a> | 5.1.1      |
| rule_documentation | NONE  | 6.2.0      |
| sru_import_log     | NONE  | 6.0        |



---

## A

app\_ids\_stats [5-5](#), [5-11](#), [5-13](#), [5-15](#), [5-16](#), [5-17](#), [5-19](#), [5-20](#), [5-23](#),  
[5-24](#), [5-26](#)  
app\_stats [5-7](#), [5-9](#), [5-10](#)  
application\_info [6-8](#)  
application\_ip\_map [6-6](#)  
application\_tag\_map [6-10](#), [6-12](#)  
audit\_log [3-1](#)

---

## C

compliance\_event [9-2](#)  
connection\_log [7-2](#), [7-19](#)  
connection\_summary [7-16](#)

---

## D

DHCP [2-2](#)  
DHCP を使用したネットワーク設定 [2-2](#)  
discovered\_users [8-2](#)

---

## F

file\_event [10-1](#)  
fireamp\_event [3-2](#)

---

## H

health\_event [3-9](#)

---

## I

intrusion\_event [4-2](#)  
intrusion\_event\_packet [4-8](#)

---

## N

network\_discovery\_event [6-13](#)

---

## R

remediation\_status [9-7](#)  
rna\_host\_protocol [6-33](#)  
rna\_ip\_host\_attribute [6-16](#)  
rna\_ip\_host\_client\_app [6-18](#)  
rna\_ip\_host\_client\_app\_payload [6-21](#)  
rna\_ip\_host\_os [6-30](#)  
rna\_ip\_host\_os\_vulns [6-32](#)  
rna\_ip\_host\_sensor [6-35](#)  
rna\_ip\_host\_service [6-36](#)  
rna\_ip\_host\_service\_banner [6-38](#)  
rna\_ip\_host\_service\_info [6-40](#)  
rna\_ip\_host\_service\_payload [6-43](#)  
rna\_ip\_host\_service\_subtype [6-46](#)  
rna\_ip\_host\_service\_vulns [6-47](#)  
rna\_ip\_host\_third\_party\_vuln [6-49](#), [6-50](#)  
rna\_ip\_host\_third\_party\_vuln\_bugtraq\_id [6-51](#)  
rna\_ip\_host\_third\_party\_vuln\_cve\_id [6-53](#)  
rna\_ip\_host\_third\_party\_vuln\_rna\_id [6-55](#)  
rna\_ip\_host\_user\_history [6-62](#)  
rna\_mac\_ip\_map [6-24](#), [6-27](#), [6-29](#), [8-5](#)  
rna\_vuln [6-57](#), [6-58](#)  
rule\_message [4-9](#)

---

## T

tag\_info [6-59](#)

---

## U

url\_categories [6-60](#)

url\_category\_stats [5-27](#)

url\_reputation\_stats [5-28](#)

url\_reputations [6-61](#)

user\_discovery\_event [8-3](#)

user\_ids\_stats [5-30](#)

user\_stats [5-32](#)

---

## W

white\_list\_event [9-8](#)

white\_list\_violation [9-10](#)