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
app_ids_stats_current_timeframe（5-4 ページ）	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+
app_stats_current_timeframe（5-6 ページ）	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+
compliance_events_stats_current_timeframe（5-8 ページ）	コンプライアンスおよびホワイトリスト イベント	6.0+
dns_query_stats_current_timeframe（5-9 ページ）	DNS クエリ	6.0+
geolocation_stats_current_timeframe（5-11 ページ）	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+
ids_impact_stats_current_timeframe（5-13 ページ）	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+
interface_stats_current_timeframe（5-14 ページ）	インターフェイスの統計情報。	6.1 以降
ip_reputation_stats_current_timeframe（5-16 ページ）	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+
qos_rule_stats_current_timeframe（5-17 ページ）	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
session_stats_current_timeframe（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+
ssl_stats_current_timeframe（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+
storage_stats_by_disposition_current_timeframe（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+
storage_stats_by_file_type_current_timeframe（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+
transmission_stats_by_file_type_current_timeframe（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+
tunnel_session_stats_current_timeframe	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
url_category_stats_current_timeframe（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+
url_reputation_stats_current_timeframe（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+
user_ids_stats_current_timeframe（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+
user_stats_current_timeframe（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トを受信するたびに、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くなります。**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くなります（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: **app_ids_stats_current**_*timeframe* および **user_ids_stats_current**_*timeframe*	過去 24 時間のすべての間隔に、現在の間隔を加算した期間
	次のテーブルでは 5 分: **app_stats_current**_*timeframe*、 **user_stats_current**_*timeframe*、 **url_category_stats_current**_*timeframe*、および **url_reputation_stats_current**_*timeframe*	過去 24 時間のすべての間隔に、現在の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
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。
blocked	侵入ポリシーの違反が原因でブロックされた接続の数。
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	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。
impact_level_1	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。
impact_level_2	影響レベル 2（脆弱な可能性あり）の侵入イベントの数。
impact_level_3	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
impact_level_4	影響レベル 4（ターゲットが不明）の侵入イベントの数。
impact_level_5	影響レベル 5（不明な脆弱性）の侵入イベントの数。
is_client_application	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 true/false フラグ。
is_server_application	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 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。
netmap_num	統計情報が収集されたドメインの Netmap ID。
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	推定リスクの説明（very low、low、medium、high、critical）。
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_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、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）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。

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	application_info.application_id application_host_map.application_id application_tag_map.application_id rna_host_service_info.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

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

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
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）。
bypass	遅延が原因でのバイパスが可能なパケットの数。
bytes_in	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。
bytes_out	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。
connections_allowed	許可された接続の数。
connections_denied	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。
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。
is_client_application	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 true/false フラグ。
is_server_application	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 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。
netmap_num	統計情報が収集されたドメインの Netmap ID。
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。
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	推定リスクの説明（very low、low、medium、high、critical）。
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 *ipv4_address*,*ipv6_address* です。
sensor_id	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。
sensor_name	トラフィックを検出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、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）を参照してください。
would_bypass	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 application_host_map.application_id application_tag_map.application_id rna_host_service.application_protocol_id rna_host_client_app_payload.web_application_id rna_host_client_app_payload.client_application_id rna_host_client_app.client_application_id rna_host_client_app.application_protocol_id rna_host_service_payload.web_application_id

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

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
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。
netmap_num	統計情報が収集されたドメインの Netmap ID。
priority_0_events	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。
priority_1_events	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。
priority_2_events	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。
priority_3_events	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。
priority_4_events	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。
priority_5_events	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。
rule	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。
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、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）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

次の表に、**dns_quaery_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
bytes_in	指定された期間中の着信トラフィックのバイト数。
bytes_out	指定された期間中の発信トラフィックのバイト数。
connections_allowed	指定された DNS クエリで許可された接続の数。
connections_denied	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。
dns_record_type	DNS クエリで使用される DNS ルックアップのタイプ。
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。
sensor_addres	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 *ipv4_address*,*ipv6_address* です。
sensor_id	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。
sensor_name	トラフィックを検出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、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）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
bytes_from	セッション レスポンダが送信した合計バイト数。
bytes_to	セッション イニシエータが送信した合計バイト数。
destination_continent	宛先ホストが位置する地域の名前 **:不明 na:北米 as:アジア af:アフリカ eu:欧州 sa:南米 au:オーストラリア an:南極
destination_country	宛先ホストの国のコード。
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。
flows_allowed	許可されたフローの数。
flows_denied	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。
netmap_num	統計情報が収集されたドメインの Netmap 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 *ipv4_address*,*ipv6_address* 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 **:不明 na:北米 as:アジア af:アフリカ eu:欧州 sa:南米 au:オーストラリア an:南極
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、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)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。 **:不明 na:北米 as:アジア af:アフリカ eu:欧州 sa:南米 au:オーストラリア an:南極
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
blocked	侵入ポリシーの違反が原因でブロックされた接続の数。
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。
impact_level_1	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。
impact_level_2	影響レベル 2（脆弱な可能性あり）の侵入イベントの数。
impact_level_3	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
impact_level_4	影響レベル 4（ターゲットが不明）の侵入イベントの数。
impact_level_5	影響レベル 5（不明な脆弱性）の侵入イベントの数。
netmap_num	統計情報が収集されたドメインの Netmap 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 *ipv4_address*,*ipv6_address* 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、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）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
connections_allowed	許可された接続の数。
connections_denied	侵入ポリシーの違反が原因でブロックされた接続の数。
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。
egress_bytes	出力バイト数。
ingress_bytes	入力バイト数。
interface_name	インターフェイスの名前。
interface_uuid	インターフェイスの UUID。
netmap_num	統計情報が収集されたドメインの Netmap ID。
qos_dropped_egress_bytes	QoS によりドロップされた出力バイト数。
qos_dropped_ingress_bytes	QoS によりドロップされた入力バイト数。
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 *ipv4_address*,*ipv6_address* です。
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、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）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
bytes_in	指定された期間中の着信トラフィックのバイト数。
bytes_out	指定された期間中の発信トラフィックのバイト数。
connections_allowed	指定された IP で許可された接続の数。
connections_denied	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。
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。
name	セキュリティ インテリジェンスの名前（例：「URL Malware」）。
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_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、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）を参照してください。
type	エントリの情報のタイプ。有効な値は次のとおりです。 0：ネットワーク インテリジェンス統計情報。 1：DNS セキュリティ インテリジェンス統計情報。 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
deploy_revision	QoS ポリシーのリビジョン UUID。
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。
netmap_num	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 *ipv4_address*,*ipv6_address* 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(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、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)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

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
bytes_in	指定された期間中の着信トラフィックのバイト数。
bytes_out	指定された期間中の発信トラフィックのバイト数。
connections_allowed	指定された URL カテゴリで許可された接続の数。
connections_denied	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。
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。
id	このフィールドは使用されず、常に 0 を返します。
sensor_address	イベントを生成した管理対象デバイスの IP アドレス。形式は *ipv4_address*,*ipv6_address* です。
sensor_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、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）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
block	リセットなしでドロップされた SSL セッションの数。
block_with_reset	リセットありでドロップされた SSL セッションの数。
cached_session	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。
cannot_determine_verdict	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。
cert_expired	証明書が期限切れであった SSL セッションの数。
cert_invalid_issuer	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。
cert_invalid_signature	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。
cert_not_checked	証明書が検査されなかった SSL セッションの数。
cert_not_yet_valid	証明書が有効ではなかった SSL セッションの数。
cert_revoked	証明書が失効していた SSL セッションの数。
cert_self_signed	証明書が自己署名されていた SSL セッションの数。
cert_unknown	証明書ステータスが不明だった SSL セッションの数。
cert_valid	証明書が有効だった SSL セッションの数。
cert_validation_cache_hit	証明書が検証キャッシュ内で見つかった回数。
cert_validation_cache_miss	証明書が検証キャッシュ内で見つからなかった回数。
decrypt_resign_self_signed	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。
decrypt_resign_self_signed_replace_key_only	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。
decrypt_resign_signed_cert	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。
decrypt_with_known_key	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 *ipv4_address*,*ipv6_address* 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（sensor_name 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、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）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_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
bytes_written	ファイルのサイズ(バイト単位)。
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。 • 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。 • UNKNOWN:ファイルにマルウェアが含まれているかどうかが不明である。 • MALWARE:ファイルにマルウェアが含まれている。 • 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。 • 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。
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。
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特性のファイルの数。
number_stored	保存されたこの特性のファイルの数。
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 *ipv4_address*,*ipv6_address* です。
sensor_name	侵入イベントを生成した管理対象デバイスの名前。
sensor_uuid	管理対象デバイスの固有識別子(sensor_name が null の場合は 0)。
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、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)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 *ipv4_address*,*ipv6_address* 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、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）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

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
bytes_sent	送信バイト数。
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。
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_sent	送信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 *ipv4_address,ipv6_address* です。
sensor_name	侵入イベントを生成した管理対象デバイスの名前。
sensor_uuid	管理対象デバイスの固有識別子（sensor_name が null の場合は 0）。
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、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）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
bytes_in	指定された期間中の着信トラフィックのバイト数。
bytes_out	指定された期間中の発信トラフィックのバイト数。
category	URL のカテゴリ。
connections_allowed	指定された URL カテゴリで許可された接続の数。
connections_denied	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。
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。
netmap_num	統計情報が収集されたドメインの Netmap ID。
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 *ipv4_address*,*ipv6_address* です。
sensor_id	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。
sensor_name	トラフィックをモニタする管理対象デバイス。
sensor_uuid	管理対象デバイスの固有識別子（sensor_name が null の場合は 0）。
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、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）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
bytes_in	指定された期間中の着信トラフィックのバイト数。
bytes_out	指定された期間中の発信トラフィックのバイト数。
connections_allowed	許可された接続の数。
connections_denied	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。
domain_name	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。 • High risk • Suspicious site • Benign site with security risks • Benign site • Well known • Risk unknown
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 *ipv4_address*,*ipv6_address* 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（sensor_name 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、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）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
blocked	侵入ポリシーの違反が原因でブロックされた接続の数。
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。
impact_level_1	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。
impact_level_2	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。
impact_level_3	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。
impact_level_4	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。
impact_level_5	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。
netmap_num	統計情報が収集されたドメインの Netmap ID。
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 *ipv4_address*,*ipv6_address* です。
sensor_id	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。
sensor_name	トラフィックを検出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、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）を参照してください。
user_id	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

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
bytes_in	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。
bytes_out	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。
connections_allowed	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。
connections_denied	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。
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。
netmap_num	統計情報が収集されたドメインの Netmap ID。
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。
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 *ipv4_address*,*ipv6_address* です。
sensor_id	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。
sensor_name	トラフィックを検出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、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）を参照してください。
user_id	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。
username	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;
```