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 モニタ、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
audit_log（3-1 ページ）	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+
fireamp_event（3-2 ページ）	AMP for Endpoints マルウェア検出および検疫イベント。	5.1+
health_event（3-9 ページ）	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
application_id	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。
application_name	転送を実行するアプリケーションの名前。
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）。
cloud_name	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 cloud_name 値には cloud_uuid 値が関連付けられています。
cloud_uuid	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 cloud_uuid 値には cloud_name 値が関連付けられています。
connection_sec	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）。
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。
detection_name	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。
detector_type	マルウェアを検出したディテクタ。各 detector_type 値には detector_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。 • ClamAV：128 • ETHOS：8 • SPERO：32 • SHA：4 • Tetra：64
detector_type_id	マルウェアを検出した検出テクノロジーの内部 ID。各 detector_type_id 値には detector_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。 • 4：SHA • 8：ETHOS • 32：SPERO • 64：Tetra • 128：ClamAV

表 3-3　fireamp_event のフィールド(続き)

フィールド	説明
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を示す値。次のいずれかの値になります。 • ダウンロード • Upload 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)。
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	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 **: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
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	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。 • Create：1 • Execute：2 • Move：22 • Scan：4
event_subtype_id	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。 • 1：作成 • 2：実行 • 4：スキャン • 22：移動
event_type	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。 • Blocked Execution：553648168 • Cloud Recall Quarantine：553648155 • Cloud Recall Quarantine Attempt Failed：2164260893 • Cloud Recall Quarantine Started：553648147 • Cloud Recall Restore from Quarantine：553648154 • Cloud Recall Restore from Quarantine Failed：2164260892 • Cloud Recall Restore from Quarantine Started：553648146 • FireAMP IOC：1107296256 • Quarantine Failure：2164260880 • Quarantined Item Restored：553648149 • Quarantine Restore Failed：2164260884 • Quarantine Restore Started：553648150 • Scan Completed, No Detections：554696715 • Scan Completed With Detections：1091567628 • Scan Failed：2165309453 • Scan Started：554696714 • Threat Detected：1090519054 • Threat Detected in Exclusion：553648145 • Threat Detected in Network File Transfer：1 • Threat Detected in Network File Transfer (Retrospective)：2 • Threat Quarantined：553648143

表 3-3　fireamp_event のフィールド（続き）

フィールド	説明
event_type_id	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。 • 553648143：Threat Quarantined • 553648145：Threat Detected in Exclusion • 553648146：Cloud Recall Restore from Quarantine Started • 553648147：Cloud Recall Quarantine Started • 553648149：Quarantined Item Restored • 553648150：Quarantine Restore Started • 553648154：Cloud Recall Restore from Quarantine • 553648155：Cloud Recall Quarantine • 553648168：Blocked Execution • 554696714：Scan Started • 554696715：Scan Completed, No Detections • 1090519054：Threat Detected • 1091567628：Scan Completed With Detections • 1107296256：FireAMP IOC • 2164260880：Quarantine Failure • 2164260893：Cloud Recall Quarantine Attempt Failed • 2164260884：Quarantine Restore Failed • 2164260892：Cloud Recall Restore from Quarantine Failed • 2165309453：Scan Failed
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(fireamp_event.sensor_name 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 **: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
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 **discovered_users** 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 または src_ipaddr	rna_host_ip_map.ipaddr 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 **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）。
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。 • red：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。 • yellow：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。 • green：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。 • recovered：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。 • disabled：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。 • error：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。

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;
```