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
discovered_users(8-1 ページ)	システムにより検出されたユーザに関する情報。	5.0+
user_discovery_event(8-3 ページ)	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+
user_ioc_state(8-5 ページ)	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
dept	ユーザの所属部門。
email	ユーザの電子メール アドレス。
first_name	ユーザの名前。
ip_address	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 null が返されます。
ipaddr	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。
last_name	ユーザの姓。
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。
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。
name	ユーザの名前。
phone	ユーザの電話番号。
rna_service	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。
user_id	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
user_id	user_discovery_event.user_id user_ipaddr_history.user_id user_ioc_state.user_id

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
application_protocol_id	検出されたアプリケーション プロトコルの内部 ID。
application_protocol_name	次のいずれかになります。 • 接続で使用されたアプリケーションの名前（LDAP、POP3 など） • pending（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） • 空白（接続にアプリケーション情報がない場合）
description	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。
domain_name	ユーザが検出されたのドメインの名前。
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。
event_id	検出イベントの内部識別番号。
event_time_sec	検出イベントの日時を示す UNIX タイムスタンプ。
event_type	検出イベントのタイプ。New User Identity や User Login など。
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。
ipaddr	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。
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。
reported_by	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。
security_group	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 *ipv4_address*,*ipv6_address* 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(sensor_name が null の場合は 0)。
user_dept	ホストの最終ログイン ユーザが所属する部門。
user_email	ホストの最終ログイン ユーザの電子メール アドレス。
user_first_name	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	rna_host_ip_map.ipaddr user_ipaddr_history.ipaddr
user_id	discovered_users.user_id user_ipaddr_history.user_id user_ioc_state.user_id

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
first_seen	侵害が最初に検出された時点を示す UNIX タイムスタンプ。
first_seen_sensor_address	侵害を最初に検出した管理対象デバイスの IP アドレス。形式は *ipv4_address*,*ipv6_address* です。
first_seen_sensor_name	侵害を最初に検出した管理対象デバイス。
user_id	ユーザの ID 番号。
ioc_category	侵害のカテゴリ。有効な値は次のとおりです。 • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
ioc_description	侵害の説明

表 8-6　user_ioc_state フィールド(続き)

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

表 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 *ipv4_address*,*ipv6_address* です。
last_seen_sensor_name	侵害を最後に検出した管理対象デバイス。

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	discovered_users.user_id user_ipaddr_history.user_id user_discovery_event.user_id

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;
```