



# 用語集

---

## #

### 5 タプル

(Quintuple)すべての IP ベース ネットワーク パケット内で使用される 5 ピースのデータ (送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、およびプロトコル)。5 タプル内のデータを使用して、インスペクション規則、クエリー、およびレポートを定義できます。

## M

### MIB

MIB (管理情報ベース)

## N

### NAT 前の送信元アドレス

セッション エンドポイント

### NAT 後の送信元アドレス

宛先に表示される送信元

### NAT 後の宛先アドレス

セッション エンドポイント

### NAT 前の宛先アドレス

送信元に表示される宛先

## あ

### アクセス IP アドレス

デバイスに接続して設定情報を取得するために MARS が使用する IP アドレス。MARS が NAT (ネットワーク アドレス変換) 関連セッションの相互関係、攻撃パスの計算、および軽減入力アクセス情報を取得するには、このアドレスが必要です。

### アクティブ化

変更を送信したあとに、MARS にとって既知の変更または編集を行うこと

---

**い**

<b>イベント</b>	MARS STM アプライアンスに報告されたセキュリティ イベント。イベントには、タイプ、送信元、宛先、レポート デバイスなどが含まれます。
<b>イベントタイプ</b>	類似したセキュリティ イベントのグループ。イベントタイプはレポート デバイスから送信される、標準化されたシグニチャです。
<b>インシデント</b>	特定の規則の基準を満たし、この規則を起動したイベントおよびセッションの集合
<b>インシデント インスタンス</b>	インシデントのインスタンス

---

**お**

<b>オフセット</b>	起動イベントのオフセットは、この起動イベントと一致する規則基準の行番号です。
--------------	--

---

**き**

<b>規則</b>	起動した指定の規則からなるインシデントの要因になったイベントのサブセット
<b>起動イベント</b>	規則を起動したイベント

---

**く**

<b>クエリー</b>	データベースの情報を求めるユーザ定義の要求
-------------	-----------------------

---

**け**

<b>軽減</b>	検出された攻撃または異常状態を停止すること。軽減方法はネットワーク構成によって異なります。
<b>検出</b>	ネットワーク内のデバイスを自動または手動で識別する処理

---

**さ**

<b>サービス</b>	プロトコルおよび IP アドレス範囲
-------------	--------------------

---

**せ**

<b>セッション</b>	指定の時間枠内で報告された、共通の送信元および宛先をすべて共有するイベントの集合。たとえば、セッション内のイベントは通常、TCP/IP 接続を開いてから閉じるまでに生成されたイベントに対応します。
<b>セッション化</b>	複数のレポート デバイスから送信されたイベント データを結合して、セッションを再構築します。セッション化には、2 つの形式があります。TCP などのセッション指向プロトコルの再構築では、初期ハンドシェイクおよびセッションが解体されます。UDP などのセッションレス プロトコルの再構築では、初期起動時刻およびセッション終了時刻が、制限時間内に追跡された先頭パケットおよび最終パケットに基づいて詳細に定義されます。つまり、指定期間外のパケットは、別のセッションに属しているとみなされます。

---

**て**

<b>デバイス</b>	システム内にあるホストおよびレポート デバイス
-------------	-------------------------

---

**と**

<b>動的な脆弱性スキャンング</b>	選択されたネットワーク、およびそのコンポーネントの脆弱性に関する MARS STM のプローブ
<b>ツール ポジティブ</b>	有効なセキュリティ脅威
<b>ツール ポジティブ</b>	有効なセキュリティ脅威

---

**ふ**

<b>フォールス ポジティブ</b>	有効なセキュリティ脅威と似ているが、セキュリティ脅威ではないイベント
--------------------	------------------------------------

---

**み**

<b>未レポート デバイス</b>	MARS アプライアンスが受信するイベント (Syslog メッセージ、SNMP 通知、または NetFlow イベントなど) の送信元であるが、アプライアンス内で定義されていないデバイス。MARS は解析で使用するメッセージ フォーマットについて認識しておく必要があるため、デバイスが定義されていない場合、MARS はイベントを正しく関係付けることができません。
-------------------	--

---

**れ**

<b>レポート</b>	自動、またはオンデマンドで実行されるデータベースに対するユーザ定義の要求
<b>レポート デバイス</b>	MARS STM アプライアンスに情報 (通常は、ログ形式) を報告する検出済みデバイス
<b>レポート IP アドレス</b>	MARS に表示される IP アドレス。このアドレスからログ (Syslog、SNMP トラップ、LEA) が取得されます。

