CHAPTER 11

# 攻撃レポートの使用方法

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）が生成する攻撃レポートについて説明します。この章は、次の項で構成されています。

- レポートのレイアウトについて
- レポートのパラメータについて
- 攻撃レポートの表示
- 攻撃レポートのエクスポート
- 攻撃レポートの削除

# レポートのレイアウトについて

Detector モジュールは、攻撃の包括的な概要を把握するために役立つ、各ゾーンの攻撃レポートを提供します。攻撃の開始は Detector モジュールによって最初に動的フィルタが生成されたときで、攻撃の終了は動的フィルタが使用されなくなり新しい動的フィルタが追加されなくなったときです。レポートには、攻撃の詳細がセクションに分かれて記載されます。各セクションには、攻撃中のトラフィック フローの異なる特性が記載されます。以前の攻撃と進行中の攻撃のレポートを表示できます。また、FTP、Secure FTP（SFTP）、または Secure Copy（SCP）ネットワーク サーバなどのネットワーク サーバにレポートをエクスポートできます。

この項では、次のトピックについて取り上げます。

- General Details
- Attack Statistics
- Detected Anomalies

## General Details

攻撃レポートの General Details セクションには、攻撃に関する一般的な情報が記載されます。

表 11-1 に、レポートのこのセクションのフィールドを示します。

**表 11-1　攻撃レポートの General Details セクションのフィールド説明**

| フィールド | 説明 |
|---|---|
| Report ID | レポートの識別番号。**current** という値は、進行中の攻撃があることを示します。 |
| Attack Start | 攻撃が開始された日時。 |
| Attack End | 攻撃が終了した日時。**Attack in progress** という値は、進行中の攻撃があることを示します。 |
| Attack Duration | 攻撃の期間。 |

## Attack Statistics

Attack Statistics セクションには、受信したトラフィック フローの一般的な分析が記載されます。

## Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Detector モジュールがゾーンのトラフィックで検出したトラフィック異常の詳細が記載されます。動的フィルタの生成を要求するフローは、異常であると分類されます。このような異常はあまり発生しないか、または体系的な Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃となる可能性があります。Detector モジュールは、同じタイプおよび同じフロー パラメータ（送信元 IP アドレスや宛先ポートなど）の異常を 1 つの異常タイプにまとめます。

表 11-2 に、検出された異常の各タイプを示します。

**表 11-2　検出された異常のタイプ**

| タイプ | 説明 |
|---|---|
| dns (tcp) | 攻撃している DNS-TCP プロトコル フロー。 |
| dns (udp) | 攻撃している DNS-UDP プロトコル フロー。 |
| fragments | 断片化されたトラフィックが異常な量であることが検出されたフロー。 |
| http | 異常な HTTP トラフィック フロー。 |
| ip_scan | 多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。 |
| other_protocols | 攻撃している TCP/UDP 以外のプロトコル フロー。 |
| port_scan | 多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。 |
| tcp_connections | 異常な数の TCP 同時接続が検出されたフロー（データの有無は問わない）。 |
| tcp_incoming | TCP サービスを攻撃していることが検出されたフロー。 |

表 11-2　検出された異常のタイプ（続き）

| タイプ | 説明 |
|---|---|
| tcp_outgoing | ゾーンがクライアントである場合に、ゾーンによって開始された接続に対する SYN-ACK フラッドまたは他のパケット攻撃で構成されていることが検出されたフロー。 |
| tcp_ratio | SYN パケット対 FIN/RST パケットの高い比率など、異なるタイプの TCP パケット間の比率が異常であることが検出されたフロー。 |
| udp | 攻撃している UDP プロトコル フロー。 |
| unauthenticated_tcp | ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなど、Detector のスプーフィング防止機能が認証に成功しなかった検出済みのフロー。 |
| user | ユーザ定義によって検出された異常なフロー。 |
| worm_tcp | TCP/IP プロトコルを介したワームの攻撃。 |

# レポートのパラメータについて

レポートの各セクションには、さまざまなトラフィック フローが記載されています。

表 11-3 で、Attack Statistics のフィールドについて説明します。

**表 11-3　Attack Statistics のフィールド説明**

| フィールド | 説明 |
|---|---|
| Total Packets | 攻撃パケットの合計数。 |
| Average pps | 平均トラフィック レート（pps）。 |
| Average bps | 平均トラフィック レート（bps）。 |
| Max. pps | 最大トラフィック レート（pps）。 |
| Max. bps | 最大トラフィック レート（bps）。 |

表 11-4 で、Detected Anomalies のフロー統計情報について説明します。

**表 11-4　フロー統計情報のフィールド説明**

| フィールド | 説明 |
|---|---|
| ID | 検出された異常の識別番号（ID）。 |
| Start time | 異常が検出された日時。 |
| Duration | 異常の期間（時間、分、秒）。 |
| Type | 異常のタイプ。 |
| Triggering rate | ポリシーのしきい値を超過した異常トラフィック レート。 |
| % Threshold | Triggering rate がポリシーのしきい値を上回っているパーセンテージ。 |
| Flow | 異常なフロー。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示します。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。 |

パラメータの 1 つにワイルドカードとしてアスタリスク（*）を使用できます。アスタリスクは次のいずれかを示します。

- 値が特定されていない。
- 異常のパラメータに対して複数の値が測定された。

数値の前にあるナンバー記号（#）は、そのパラメータに対して測定された値の数を示します。

Detector モジュールは、フローの説明の右側に、notify という値を表示することがあります。notify の値は、その行が説明するトラフィック タイプの通知を Detector モジュールが生成することを示します。Detector モジュールは値が notify の場合、アクションを実行しません。

# 攻撃レポートの表示

特定のゾーンの攻撃レポートのリスト、または特定の攻撃の詳細なレポートを表示するには、ゾーン設定モードで次のコマンドを使用します。

**show reports** [**current** | *report-id*] [**details**]

表 11-5 に、**show reports** コマンドの引数とキーワードを示します。

**表 11-5　show reports コマンドの引数とキーワード**

| パラメータ | 説明 |
|---|---|
| **current** | （オプション）進行中の攻撃のレポートを表示します。<br><br>進行中の攻撃のビット数およびパケット数は表示されません。進行中の攻撃のレポートでは、パケットとビットのフィールドにゼロ（0）という値が表示されます。 |
| *report-id* | （オプション）レポートの識別番号。 |
| **details** | （オプション）フローの詳細を表示します。 |

次の例は、ゾーン上のすべての攻撃のリストの表示方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show reports
```

表 11-6 に、**show reports** コマンド出力フィールドを示します。

**表 11-6　show reports コマンド出力のフィールドの説明**

| フィールド | 説明 |
|---|---|
| Report ID | レポートの識別番号。**current** という値は、進行中の攻撃があることを示します。 |
| Attack Start | 攻撃が開始された日時。 |
| Attack End | 攻撃が終了した日時。**Attack in progress** という値は、進行中の攻撃があることを示します。 |
| Attack Duration | 攻撃の期間。 |

**表 11-6　show reports コマンド出力のフィールドの説明（続き）**

| フィールド | 説明 |
|---|---|
| Attack Type | 検出された攻撃のタイプ。指定できる値は、次のとおりです。<br>• **tcp_connections**：異常な数の TCP 同時接続が検出されたフロー（データの有無は問わない）。<br>• **http**：異常な HTTP トラフィック フロー。<br>• **tcp_incoming**：TCP サービスを攻撃していることが検出されたフロー。<br>• **tcp_outgoing**：ゾーンがクライアントである場合に、ゾーンが開始した接続に対する SYN-ACK 攻撃など、クライアントがゾーンであるように見える検出済み攻撃フロー。<br>• **unauthenticated_tcp**：Detector モジュールのスプーフィング防止機能が認証できなかった検出済みのフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。<br>• **dns (udp)**：攻撃している DNS-UDP プロトコル フロー。<br>• **dns (tcp)**：攻撃している DNS-TCP プロトコル フロー。<br>• **udp**：攻撃している UDP プロトコル フロー。<br>• **other_protocols**：攻撃している TCP/UDP 以外のプロトコル フロー。<br>• **fragments**：異常な量の断片化されたトラフィックが検出されたフロー。<br>• **hybrid**：特性の異なる複数の攻撃で構成された攻撃。<br>• **ip_scan**：多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。<br>• **port_scan**：多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。<br>• **user_detected**：ユーザ定義によって検出された異常なフロー。<br>• **worm_tcp**：TCP/IP プロトコルを介したワームの攻撃。 |

**表 11-6　show reports コマンド出力のフィールドの説明（続き）**

| フィールド | 説明 |
|---|---|
| Peak Malicious Traffic | このフィールドは、Guard だけに関連し、Detector モジュールには適用されません。 |

次の例は、ゾーンにおける現在の攻撃のレポートを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show reports current
```

攻撃レポートには、次のような出力が表示されます。各セクションの詳細については、P.11-2 の「レポートのレイアウトについて」を参照してください。

```
Report ID            :   current
Attack Start         :   Feb 26 2004 09:58:54
Attack End           :   Attack in progress
Attack Duration      :   00:08:34


Attack Statistics:
              Total Packets    Average pps    Average bps     Max pps     Max bps
Received      95878            186.53         110977.74       1455.44     914428.24    N/A


Detected Anomalies:
ID      Start Time          Duration      Type                Triggering Rate    %Threshold
1       Feb 26 09:58:54     00:08:34      HTTP                997.44             897.44
        Flow: 6 *           *             92.168.100.34  80   no fragments
```

異常が検出されたフローに関する詳細なレポートを表示するには、**details** オプションを使用します。

表 11-7 に、詳細なレポートに含まれているフローのフィールドを示します。

**表 11-7　詳細なレポートのフローのフィールド説明**

| フィールド | 説明 |
|---|---|
| Detected Flow | 動的フィルタが生成される原因となったフロー。検出されたフローが特定の送信元 IP アドレスの特定の送信元ポートを示す場合があります。このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。 |
| Action Flow | 動的フィルタによって処理されたフロー。アクション フローが特定の送信元 IP アドレスのすべての送信元ポートを示す場合があります。アクション フローは、検出されたフローよりも広範囲であることがあります。<br><br>このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。 |

# 攻撃レポートのエクスポート

監視および診断のために、攻撃レポートをネットワーク サーバにエクスポートできます。テキスト形式または Extensible Markup Language（XML）形式で攻撃レポートをエクスポートできます。

この項では、次のトピックについて取り上げます。



## 攻撃レポートの自動エクスポート

攻撃が終了した時点で攻撃レポートが XML 形式で自動的にエクスポートされるよう、Detector モジュールを設定できます。Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。www.cisco.com から、このバージョンに付属の xsd ファイルをダウンロードできます。

Detector モジュールが攻撃レポートを自動的にエクスポートするように設定するには、設定モードで次のコマンドを使用します。

**export reports** *file-server-name*

*file-server-name* 引数は、**file-server** コマンドを使用して設定したファイルをエクスポートするネットワーク サーバの名前を指定します。ネットワーク サーバに Secure FTP（SFTP）または Secure Copy（SCP）を設定する場合は、Detector モジュールが SFTP 通信および SCP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。

次の例は、ネットワーク サーバへの攻撃の終了時に、レポートを（XML 形式で）自動的にエクスポートする方法を示しています。

```
user@DETECTOR-conf# export reports Corp-FTP-Server
```

# すべてのゾーンの攻撃レポートのエクスポート

グローバル モードで次のいずれかのコマンドを入力することにより、すべてのゾーンの攻撃レポートをテキスト形式または XML 形式でエクスポートできます。

- **copy reports** [**details**] [**xml**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy reports** [**details**] [**xml**] *file-server-name dest-file-name*

表 11-8 に、**copy reports** コマンドの引数とキーワードを示します。

**表 11-8　copy reports コマンドの引数とキーワード**

| パラメータ | 説明 |
|---|---|
| **details** | （オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。 |
| **xml** | （オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンでリリースされた xsd ファイルを参照してください（www.cisco.com からこのバージョンに付属の xsd ファイルをダウンロードできます）。デフォルトでは、レポートはテキスト形式でエクスポートされます。<br><br>XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。 |
| **ftp** | 攻撃レポートを FTP を使用してネットワーク サーバにエクスポートします。 |
| *server* | ネットワーク サーバの IP アドレス。 |
| *full-file-name* | ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。 |
| *login* | （オプション）サーバのログイン名。<br><br>*login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。 |
| *password* | （オプション）リモート FTP サーバのパスワード。 |

表 11-8　copy reports コマンドの引数とキーワード（続き）

| パラメータ | 説明 |
|---|---|
| *file-server-name* | **file-server** コマンドを使用して定義したネットワーク サーバの名前。<br><br>ネットワーク サーバは FTP サーバである必要があります。SFTP または SCP を使用して攻撃レポートをネットワーク サーバにエクスポートすることはできません。<br><br>詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。 |
| *dest-file-name* | ファイルの名前。Detector モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。 |

次の例は、ログイン名 user1 とパスワード password1 を使用して、Detector モジュールによって処理されたすべての攻撃のリストを IP アドレス 10.0.0.191 の FTP サーバに（テキスト形式で）コピーする方法を示しています。

```
user@DETECTOR# copy reports ftp 10.0.0.191 admreports.txt user1
password1
```

次の例は、Detector モジュールによって処理されたすべての攻撃のリストを **file-server** コマンドを使用して定義したネットワーク サーバに（テキスト形式で）コピーする方法を示しています。

```
user@DETECTOR# copy reports Corp-FTP-Server AttackReports.txt
```

## ゾーン レポートのエクスポート

特定のゾーンの攻撃レポートを FTP サーバにコピーするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] *file-server-name dest-file-name*

表 11-9 に、**copy zone reports** コマンドの引数とキーワードの説明を示します。

**表 11-9　copy zone reports コマンドの引数とキーワード**

| パラメータ | 説明 |
|---|---|
| **zone** *zone-name* | 既存のゾーンの名前を指定します。 |
| **current** | （オプション）進行中の攻撃のレポートをエクスポートします（該当する場合）。<br><br>デフォルトでは、すべてのゾーン レポートをエクスポートします。 |
| *report-id* | （オプション）既存のレポートの ID。指定した ID 番号を持つレポートが Detector モジュールによってエクスポートされます。ゾーン攻撃レポートの詳細を表示するには、**show zone reports** コマンドを使用します。<br><br>デフォルトでは、すべてのゾーン レポートをエクスポートします。 |
| **xml** | （オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンでリリースされた xsd ファイルを参照してください（www.cisco.com からこのバージョンに付属の xsd ファイルをダウンロードできます）。デフォルトでは、レポートをテキスト形式でエクスポートします。<br><br>XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。 |
| **details** | （オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。 |
| **ftp** | 攻撃レポートを FTP を使用してネットワーク サーバにエクスポートします。 |
| *server* | サーバの IP アドレスと、ファイルの保存先ディレクトリの完全パス。 |

**表 11-9　copy zone reports コマンドの引数とキーワード（続き）**

| パラメータ | 説明 |
|---|---|
| *login* | （オプション）サーバのログイン名。<br><br>*login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。 |
| *password* | （オプション）リモート FTP サーバのパスワード。 |
| *file-server-name* | ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。<br><br>ネットワーク サーバは FTP サーバである必要があります。SFTP または SCP を使用してレポートをネットワーク サーバにエクスポートすることはできません。<br><br>詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。 |
| *dest-file-name* | ファイルの名前。Detector モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。 |

次の例は、ログイン名 user1 とパスワード password1 を使用して IP アドレス 10.0.0.191 の FTP サーバにゾーンのすべての攻撃レポートをコピーする方法を示しています。

```
user@DETECTOR# copy zone scannet reports ftp 10.0.0.191
ScannetCurrentReport.txt user1 password1
```

次の例は、現在の攻撃のレポートを **file-server** コマンドを使用して定義したネットワーク サーバに（XML 形式で）コピーする方法を示しています。

```
user@DETECTOR# copy zone scannet reports current xml Corp-FTP-Server
AttackReport-5-10-05.txt
```

# 攻撃レポートの削除

古い攻撃レポートを削除して、空きディスク スペースを得ることができます。

攻撃レポートを削除するには、ゾーン設定モードで次のコマンドを使用します。

**no reports** *report-id*

*report-id* 引数には、既存のレポートの ID を指定します。すべての攻撃レポートを削除するには、アスタリスク（*）を入力します。ゾーン攻撃レポートの詳細を表示するには、**show zone reports** コマンドを使用します。

**（注）** 進行中の攻撃の攻撃レポートは削除できません。

次の例は、すべてのゾーン攻撃レポートを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no reports *
```