CHAPTER 10

# 攻撃レポート

この章では、Cisco Anomaly Guard Module（Guard 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。この章には、次の項があります。

- 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

# レポートのレイアウトについて

Guard は、攻撃を明確に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 Guard 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 フローの異なる面が記載されます。過去の攻撃および進行中の攻撃のレポートを表示できます。また、レポートを FTP サーバまたは セキュア FTP（SFTP）サーバにエクスポートすることもできます。

レポートには、次のセクションがあります。

- General Details
- Attack Statistics
- Dropped/ Replied Packets
- Detected Anomalies
- Mitigated Attacks
- Zombies：このセクションは、**show reports details** コマンドおよび **show zombies** コマンドを発行した場合にだけ表示されます。

## 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 10-1 で、レポートのこのセクションのフィールドについて説明します。

**表 10-1　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。 |
| Attack Start | 攻撃が開始された日時を表示します。 |
| Attack End | 攻撃が終了した日時を表示します。*Attack in progress* は、進行中の攻撃があることを示します。 |
| Attack Duration | 攻撃の期間を表示します。 |

## Attack Statistics

Attack Statistics セクションには、さまざまなパケットのゾーン トラフィック フローの一般的な分析が記載されます。表 10-2 で、パケット タイプについて説明します。

**表 10-2　パケット タイプ**

| タイプ | 説明 |
|---|---|
| Received | 宛先変更されたトラフィックの合計量を示します。 |
| Forwarded | Guard モジュールがゾーンに転送した正当なトラフィックを示します。 |
| Replied | 検証の試行で Guard モジュールのスプーフィング防止メカニズムおよびゾンビ防止メカニズムが送信元に返送したトラフィックを示します。 |
| Dropped | Guard モジュールがドロップしたトラフィックを示します。 |

## Dropped/ Replied Packets

攻撃レポートの Dropped/Replied Packets セクションでは、検証の試行で Guard モジュールによってドロップされたパケットおよび送信元に返送されたパケットが分析されます。レポートでは、パケットがタイプ（スプーフィングまたは不正な形式）および処理メカニズム（フィルタ タイプまたはレート リミット保護モジュール）によって分類されます。表 10-3 で、ドロップされたパケットおよび返送されたパケットのさまざまなタイプについて説明します。

**表 10-3　ドロップされたパケットおよび返送されたパケットのタイプ**

| タイプ | 説明 |
|---|---|
| Rate Limiter | ゾーンのレート リミット保護モジュールによってドロップされたパケットを示します。これらのパケットは、ユーザ フィルタのレート リミット パラメータ、およびゾーンの **rate-limit** コマンドによって定義されます。 |
| Flex-Content Filters | フレックスコンテンツ フィルタによってドロップされたパケットを示します。 |
| User Filters | ユーザ フィルタによってドロップされたパケットを示します。 |
| Dynamic Filters | 動的フィルタによってドロップされたパケットを示します。 |
| Spoofed | Guard モジュールによって、スプーフィングされたパケットまたはゾンビが発信したパケットであると識別されたため、ゾーンに転送されなかったパケットを示します。スプーフィング パケットは、応答された（返送された）パケットのうち、応答を受信しなかったパケットです。 |
| Malformed | 不正な形式の構造であるため、または Guard モジュールのスプーフィング防止メカニズムが原因で、不正な形式であると分析されたパケットを示します。 |

## Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Guard 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。動的フィルタの作成を必要とするフローは、トラフィック異常として分類されます。これらの異常は頻繁に発生するものではなく、組織的な DDoS 攻撃に変化する可能性があります。Guard 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 10-4 で、検出された異常のさまざまなタイプについて説明します。

**表 10-4　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 | データを保持している（または保持していない）、異常な数の TCP 同時接続が検出されたフロー。 |
| tcp_incoming | ゾーンがサーバである場合に、TCP サービスを攻撃していることが検出されたフロー。 |
| 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 | 異なるタイプの TCP パケット間（たとえば、SYN パケット対 FIN/RST パケット）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。 |

**表 10-4　検出された異常のタイプ（続き）**

| タイプ | 説明 |
|---|---|
| unauthenticated_tcp | Guard のスプーフィング防止メカニズムが認証に成功しなかったことが検出されたフロー。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。 |
| user | ユーザ定義によって検出された異常なフロー。 |

## Mitigated Attacks

攻撃レポートの Mitigated Attacks セクションには、Guard モジュールがゾーンを保護する（攻撃を軽減する）ために実行した処置が詳細に記載されます。このレポートには、軽減のタイミングおよび軽減された攻撃のタイプの詳細が記載されます。Guard モジュールは、使用したメカニズムに応じて軽減のタイプを定義します。このメカニズムは、攻撃のタイプとサブタイプを示します。

たとえば、Guard モジュールが syn パケットの攻撃フローに対して基本的なスプーフィング防止メカニズムを使用した場合、軽減された攻撃は **spoofed/tcp_syn_basic** と表示されます。spoofed は攻撃のタイプを示し、tcp_syn_basic はサブタイプを示します。

軽減された攻撃には、次の 5 つのタイプがあります。

- スプーフィング利用
- ゾンビ
- クライアント攻撃
- ユーザ定義
- 不正な形式のパケット

## スプーフィング利用

スプーフィングを利用した攻撃には、スプーフィングされた送信元からの DDoS 攻撃であると識別されるすべてのトラフィック異常が含まれます。表 10-5 で、スプーフィングを利用した攻撃のさまざまなタイプについて説明します。

**表 10-5　スプーフィングを利用した攻撃のタイプ**

| 攻撃のタイプ | 説明 |
|---|---|
| spoofed/tcp_syn (basic) | 基本的なスプーフィング防止メカニズムが認証に成功しなかった SYN パケットのフラッド。 |
| spoofed/tcp_syn (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかった SYN パケットのフラッド。 |
| spoofed/tcp_syn_ack (basic) | 基本的なスプーフィング防止メカニズムが認証に成功しなかった syn_ack パケットのフラッド。 |
| spoofed/tcp_syn_ack (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかった syn_ack パケットのフラッド。 |
| spoofed/tcp_incoming (basic) | 基本的なスプーフィング防止メカニズムが認証に成功しなかったトラフィックのフラッド。 |
| spoofed/tcp_incoming (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかったトラフィックのフラッド。 |
| spoofed/tcp_outgoing (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信トラフィックのフラッド。 |
| spoofed/udp (basic) | 基本的なスプーフィング防止メカニズムが認証に成功しなかった UDP トラフィックのフラッド。 |
| spoofed/udp (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかった UDP トラフィックのフラッド。 |
| spoofed/other_protocols | Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、TCP および UDP トラフィック以外のフラッド。 |
| spoofed/tcp_fragments | Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、断片化された TCP パケットのフラッド。 |

**表 10-5　スプーフィングを利用した攻撃のタイプ（続き）**

| 攻撃のタイプ | 説明 |
|---|---|
| spoofed/udp_fragments | Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、断片化された UDP パケットのフラッド。 |
| spoofed /other_protocols_fragments | Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった、TCP および UDP 以外の断片化されたパケットのフラッド。 |
| spoofed/dns_queries (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかった DNS クエリー パケットのフラッド。 |
| spoofed/dns_replies (basic) | 基本的なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信 DNS パケットのフラッド。 |
| spoofed/dns_replies (strong) | 強力なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信 DNS パケットのフラッド。 |

## ゾンビ

ゾンビ攻撃には、ゾンビによって開始された DDos 攻撃であると識別されるトラフィック異常が含まれます。表 10-6 で、ゾンビ攻撃のタイプについて説明します。

**表 10-6　ゾンビ攻撃のタイプ**

| 攻撃のタイプ | 説明 |
|---|---|
| zombie/http | Guard モジュールのゾンビ防止メカニズムが認証に成功しなかった、スプーフィングされていないと識別された多くの送信元からの HTTP トラフィックのフラッド。 |

## クライアント攻撃

クライアント攻撃には、スプーフィングされていないすべてのトラフィック異常が含まれます。表 10-7 で、さまざまなタイプのクライアント攻撃について説明します。

**表 10-7　クライアント攻撃のタイプ**

| 攻撃のタイプ | 説明 |
|---|---|
| client_attack/tcp_connections | データを保持している（または保持していない）、TCP 同時接続数が異常であるフロー。 |
| client_attack/http | HTTP トラフィック フローのフラッド。 |
| client_attack/tcp_ incoming | ゾーンがサーバである場合に、TCP サービスを攻撃しているフラッド。 |
| client_attack/tcp_outgoing | ゾーンが開始した認証済み IP 接続からの攻撃フラッド。 |
| client_attack /unauthenticated_tcp | TCP ハンドシェイクを経ていない ACK、FIN、または他のパケットのフラッド、あるいは Guard モジュールのスプーフィング防止メカニズムが認証に成功しなかった TCP 接続。 |
| client_attack/dns (udp) | 攻撃している DNS-UDP プロトコル フローのフラッド。 |
| client_attack/dns (tcp) | 攻撃している DNS-TCP プロトコル フローのフラッド。 |
| client_attack/udp | 攻撃している UDP プロトコル フローのフラッド。 |
| client_attack/other_protocols | 攻撃している TCP/UDP 以外のプロトコル フローのフラッド。 |
| client_attack/fragments | 断片化されたトラフィックのフラッド。 |
| client_attack/user | ユーザ定義の攻撃のフラッド。この攻撃は、ユーザによって追加された動的フィルタによって定義されます。 |

## ユーザ定義

ユーザ定義攻撃には、ユーザ フィルタによって処理されたすべての異常が含まれます。ユーザ フィルタは、デフォルトで機能するか、またはユーザによって手動で設定されます（詳細については、第 8 章「ポリシー テンプレートとポリシーの設定」を参照してください）。表 10-8 で、ユーザ定義攻撃のさまざまなタイプについて説明します。

**表 10-8　ユーザ定義攻撃のタイプ**

| 攻撃のタイプ | 説明 |
|---|---|
| user_defined/<br>user_filter_rate_limit | ユーザ フィルタ用に定義されたレート リミットを超過したためにドロップされたフラッド。 |
| user_defined/<br>user_drop_filters | ユーザ フィルタによってドロップされたフラッド。 |
| user_defined/rate_limit | 次のいずれかの原因により ドロップされたフラッド。<br>• ユーザ フィルタ用に定義されたレート リミットを超過した。<br>• ゾーンの **rate-limit** コマンドによって定義されたレート リミットを超過した。<br>• 認証されていない TCP RST パケットまたは認証されていない DNS ゾーン転送パケット用に定義された内部レート リミットを超過した。 |
| user_defined/<br>flex_content_filter | フレックスコンテンツ フィルタによってドロップされたフラッド。 |

### 不正な形式のパケット

不正な形式のパケットには、悪意のある不正形式パケットで構成されると識別されたすべてのトラフィック異常が含まれます。表 10-9 で、さまざまなタイプの不正形式パケットについて説明します。

**表 10-9　不正形式パケットのタイプ**

| 攻撃のタイプ | 説明 |
|---|---|
| malformed_packets /packets_to_proxy_ip | Guard モジュールの プロキシ IP アドレスを攻撃しているフラッド。 |
| malformed_packets /dns_anti_spoofing_algo | Guard モジュールの DNS スプーフィング防止メカニズムの動作が原因の不正な形式のパケットのフラッド。 |
| malformed_packets /dns (queries) | 不正な形式の DNS パケットのフラッド。 |
| malformed_packets /dns (short_queries) | 短い DNS クエリーのフラッド。 |
| malformed_packets /dns (replies) | 不正な形式の DNS 応答のフラッド。 |
| malformed_packets /src ip = dst ip | 送信元および宛先としてゾーンの IP アドレスを持つパケットのフラッド。 |
| malformed_packets /zero_header_field | ヘッダーのポート、プロトコル、および IP のフィールドが不正にゼロとなっているパケットのフラッド。 |

## Zombies

ゾンビ攻撃には、ゾンビによって開始された DDoS 攻撃であると識別されたトラフィック異常が含まれます。Guard モジュールの攻撃レポートには、現在ゾーンを攻撃しているゾンビを一覧表示するテーブルが表示されます。現在攻撃しているゾンビのリストを表示するには、**show reports details** コマンドおよび **show zombies** コマンドを使用します。

show zombies コマンド出力のフィールドについては、表 10-15 を参照してください。

# レポートのパラメータについて

レポートの異なるセクションには、トラフィック フローの異なる面が記載されます。

表 10-10 で、Attack Statistics および Dropped/ Replied Packets のフィールドについて説明します。

**表 10-10　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を示します。 |
| Average pps | 平均トラフィック レート（pps）を示します。 |
| Average bps | 平均トラフィック レート（bps）を示します。 |
| Max. pps | 最大トラフィック レート（pps）を示します。 |
| Max. bps | 最大トラフィック レート（bps）を示します。 |
| Percentage | 受信パケットの合計数に対する、転送されたパケット、返送されたパケット、およびドロップされたパケットのパーセンテージを示します。 |

表 10-11 で、Detected Anomalies および Mitigated Attacks のフロー統計情報について説明します。

**表 10-11　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）を示します。 |
| Start time | 異常が検出された日時を示します。 |
| Duration | 異常の期間（時間、分、秒）を示します。 |
| Type | 異常または軽減された攻撃のタイプを示します。 |
| Triggering Rate | ポリシーのしきい値を超過した異常トラフィック レートを示します。 |
| % 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を示します。 |

**表 10-11　フロー統計情報のフィールド説明（続き）**

| フィールド | 説明 |
|---|---|
| Flow | 異常フローおよび軽減された攻撃のフローを示します。この特性は、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** は、断片化されている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。 |

パラメータの値が ***** となっている場合は、次のいずれかの状態であることを示します。

- 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。

任意のパラメータの # という値（数値の前にある）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。

Guard 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場合があります。レポートの行に *notify* という値が表示された場合、Guard モジュールはその行が示すトラフィック タイプの通知を生成するだけで、アクションを実行しないことを示します。

# 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、**show** コマンドを使用します。次のコマンドを入力します。

**show reports** [*sub-zone-name*] [**current** | *report-id*] [**details**]

表 10-12 で、**show reports** コマンドの引数とキーワードについて説明します。

**表 10-12　show reports コマンドの引数とキーワード**

| パラメータ | 説明 |
|---|---|
| *sub-zone-name* | （オプション）ゾーンから作成されたサブゾーンの名前です。詳細については、P.6-42 の「サブゾーンについて」を参照してください。 |
| current | 進行中の攻撃。<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* | レポートの識別番号。 |
| **details** | （オプション）フローおよび攻撃しているゾンビの詳細を表示します。 |

たとえば、ゾーンに対するすべての攻撃のリストを表示するには、次のコマンドを入力します。

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

表 10-13 で、**show reports** コマンド出力のフィールドについて説明します。

**表 10-13　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。 |
| 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 Type | 軽減された攻撃のタイプ。使用可能な値は、次のいずれかです。<br>• **client_attack**：スプーフィング以外のすべてのトラフィック異常。<br>• **malformed_packets**：悪意のある不正形式パケットと見なされたすべてのトラフィック異常。<br>• **spoofed**：スプーフィングされた送信元からの DDoS 攻撃と見なされたトラフィック異常。<br>• **user_defined**：ユーザ フィルタによって処理されたすべての異常。これらのフィルタは、デフォルト設定で動作することも、ユーザが動作を設定することもできます。<br>• **zombie**：ゾンビが発信元であると見なされたトラフィック異常。<br>• **hybrid**：特性の異なる複数の攻撃で構成された攻撃。<br>• **traffic_anomaly**：短期間のみ検出され、軽減を必要としなかった異常。 |
| Malicious Traffic | Guard モジュールによって攻撃の一部と見なされ、ドロップされたパケット数と、正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、Guard モジュールによって開始側のクライアントに応答が送信されたパケット数の合計。 |

ゾーンに対する現在の攻撃のレポートを表示するには、次のコマンドを入力します。

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

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.10-2 の「レポートのレイアウトについて」を参照してください。

```
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 | Percentage |
|---|---|---|---|---|---|---|
| Received | 95878 | 186.53 | 110977.74 | 1455.44 | 914428.24 | N/A |
| Forwarded | 53827 | 104.72 | 64278.54 | 1430.85 | 899196.24 | 56.14 |
| Replied | 1870 | 3.64 | 2172.89 | 23.03 | 14433.88 | 1.95 |
| Dropped | 40181 | 78.17 | 44526.32 | 96.82 | 55010.13 | 41.91 |

Dropped/Replied Packets:

| | Total Packets | Average pps | Average bps | Max pps | Max bps | Percentage |
|---|---|---|---|---|---|---|
| Rate Limiter | 0 | 0 | 0 | 0 | 0 | 0 |
| Flex-Content Filter | 0 | 0 | 0 | 0 | 0 | 0 |
| User Filters | 0 | 0 | 0 | 0 | 0 | 0 |
| Dynamic Filters 40128 | 78.07 | 44473.53 | 96.82 | 55010.13 | 99.84 | |
| Spoofed | 12 | 0.02 | 11.95 | 0.15 | 75.29 | 0.03 |
| Malformed | 53 | 0.1 | 52.79 | 1.56 | 798.12 | 0.13 |

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


Mitigated Attacks:
ID          Start Time          Duration    Type                    Triggering    %Threshold
                                                                    Rate
1          Feb 26 09:59:40      00:07:59   client_attack/            38            280
                                           tcp_connections
           Flow: 6 (#52)        *          92.168.200.254 80         no fragments
```

検出された異常フローと軽減された攻撃フローに関する詳細なレポート、およびゾンビ攻撃のリストを表示するには、**details** オプションを使用します。

表 10-14 に、詳細なレポートに含まれているフローのフィールドの説明を示します。

**表 10-14　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を示します。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** は、断片化されている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。 |

**表 10-14　詳細なレポートのフローのフィールド説明（続き）**

| フィールド | 説明 |
|---|---|
| Action Flow | 動的フィルタによって処理されたフローを示します。アクション フローは、検出されたフローよりも範囲が広い可能性があります。たとえば、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し、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** は、断片化されている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。 |

表 10-15 で、ゾンビ攻撃に関する詳細なレポートのフィールドについて説明します。

**表 10-15　ゾンビ攻撃に関するテーブルのフィールドの説明**

| フィールド | 説明 |
|---|---|
| IP | ゾンビの IP アドレス。 |
| Start Time | ゾンビ接続が初めて識別された日時。 |
| Duration | ゾンビ攻撃の期間。 |
| #Requests | ゾンビによって送信された HTTP get 要求の数。 |

（注）　ゾンビ攻撃がない場合は、レポートの Zombies という見出しの下に **Report doesn’t exist** と表示されます。

# 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 FTP サーバまたは SFTP 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
- すべてのゾーンの攻撃レポートのエクスポート
- ゾーン レポートのエクスポート

## 攻撃レポートの自動エクスポート

攻撃が終了したときに攻撃レポートが XML 形式で自動的にエクスポートされるように Guard モジュールを設定できます。Guard モジュールは、ゾーンに対する攻撃が終了すると、いずれかのゾーンのレポートを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。設定モードで、次のいずれかのコマンドを入力します。

- **export reports ftp** *server remote-path* [*login*] [*password*]
- **export reports sftp** *server remote-path login*

（注）　**copy reports** コマンドを入力する前に、Guard モジュールが SFTP 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.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 10-16 で、**export reports** コマンドの引数について説明します。

**表 10-16　export reports コマンドの引数**

| パラメータ | 説明 |
|---|---|
| **ftp** | 攻撃レポートを FTP サーバにエクスポートします。 |
| **sftp** | 攻撃レポートを SFTP サーバにエクスポートします。 |
| *server* | サーバの IP アドレス。 |
| *remote-path* | ファイルの保存先ディレクトリの完全パス。 |
| *login* | 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い場合、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。 |

次の例は、IP アドレス *10.0.0.191* の FTP サーバへの攻撃が終了した後、ログイン名 *user1* とパスワード *password1* を使用してレポートを 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@GUARD-conf# export reports ftp 10.0.0.191 /root/reports user1
password1
```

## すべてのゾーンの攻撃レポートのエクスポート

すべてのゾーンの攻撃レポートをテキストまたは XML 形式でエクスポートできます。レポートを FTP サーバまたは SFTP サーバに手動でコピーするには、**copy reports** コマンドを使用します。

グローバル モードで次のコマンドを入力します。

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

表 10-17 で、**copy reports** コマンドの引数とキーワードについて説明します。

**表 10-17　copy reports コマンドの引数とキーワード**

| パラメータ | 説明 |
|---|---|
| **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、このバージョンに付属の xsd ファイルを参照してください。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。 |
| **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 サーバにエクスポートします。 |
| *server* | サーバの IP アドレス。 |
| *remote-path* | サーバによるファイルの保存先ディレクトリの完全パス。 |
| *login* | 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い場合、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。 |

次の例は、ログイン名 *user1* とパスワード *password1* を使用して、Guard 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テキスト形式で IP アドレス *10.0.0.191* の FTP サーバにコピーする方法を示しています。

```
user@GUARD# copy reports ftp 10.0.0.191 AGMreports.txt user1 password1
```

# 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**] **sftp** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard モジュールが SFTP 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.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 10-18 で、**copy zone reports** コマンドの引数とキーワードについて説明します。

**表 10-18　copy zone reports コマンドの引数とキーワード**

| パラメータ | 説明 |
|---|---|
| *zone-name* | 既存のゾーンの名前。 |
| **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 Guard 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。 |

**表 10-18　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 |
|---|---|
| **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、このバージョンに付属の xsd ファイルを参照してください。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 サーバにエクスポートします。 |
| **sftp** | 攻撃レポートを SFTP サーバにエクスポートします。 |
| *server* | サーバの IP アドレス。 |
| *remote-path* | ファイルの保存先ディレクトリの完全パス。 |
| *login* | 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い場合、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。 |

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