CHAPTER 11

攻撃レポートの使用方法

この章では、Cisco Guard（Guard）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

Guard 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 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。

レポートには、次の情報が含まれています。各セクションの説明を参照してください。

- General Details
- Attack Statistics
- Malicious Packet Statistics
- 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** コマンドを入力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 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、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 11-2 に、パケット タイプを示します。

表 11-2　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。
Forwarded	Guard がゾーンに転送した正当なトラフィック。
Replied	検証の試行で Guard 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。
Dropped	Guard がドロップしたトラフィック。

Malicious Packet Statistics

攻撃レポートの Malicious Packets Statistics セクションでは、Guard がドロップしたパケットおよび検証の試行で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、パケットをタイプ（スプーフィングまたは不正な形式）、およびそれらを処理する Guard の機能（フィルタ タイプまたはレート リミッタ）によって分類します。

表 11-3 に、さまざまなタイプの悪意のあるパケットを示します。

表 11-3　悪意のあるパケットのタイプ

タイプ	説明
Rate Limiter	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への注入を許可されているゾーン **rate-limit** コマンドにより定義されたトラフィックのレートを超過したためドロップされます。
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。
User Filters	ユーザ フィルタによってドロップされたパケット。
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 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、ゾーンに転送されなかったパケット。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 のスプーフィング防止機能が原因で、不正な形式であると分析されたパケット。

Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Guard 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。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 11-4 に、検出された異常の各タイプを示します。

表 11-4　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 パケットの高い比率）の比率が異常であることが検出されたフロー。

表 11-4　検出された異常のタイプ（続き）

タイプ	説明
udp	攻撃している UDP プロトコル フロー。
unauthenticated_tcp	Guard 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。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。
sip_udp	SIP[1] over UDP を使用して VoIP セッションを確立する、検出済みの VoIP[2] の異常なフロー。

1. SIP = Session Initiation Protocol
2. VoIP = Voice over IP

Mitigated Attacks

攻撃レポートの Mitigated Attacks セクションには、Guard 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 は、Guard が攻撃を軽減するために使用した機能に応じて軽減のタイプを定義します。この機能は、攻撃のタイプとサブタイプを示します。

たとえば、Guard が syn パケットの攻撃フローを軽減するために基本的なスプーフィング防止機能を使用した場合、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 は攻撃の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。

- スプーフィングを利用した攻撃
- ゾンビ攻撃
- クライアント攻撃
- ユーザ定義の攻撃
- 不正な形式のパケット

スプーフィングを利用した攻撃

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 11-5 に、スプーフィングを利用した攻撃のさまざまなタイプを示します。

表 11-5　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機能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機能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 のスプーフィング防止機能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 のスプーフィング防止機能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 11-5　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 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 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機能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機能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機能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/sip	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 SIP over UDP パケットのフラッド。

ゾンビ攻撃

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 11-6 に、ゾンビ攻撃のタイプを示します。

表 11-6　ゾンビ攻撃のタイプ

攻撃のタイプ	説明
zombie/http	Guard のゾンビ防止機能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 11-7 に、さまざまなタイプのクライアント攻撃を示します。

表 11-7　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 のスプーフィング防止機能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。

ユーザ定義の攻撃

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、デフォルトまたは手動による設定で機能します。詳細については、第 7 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 11-8 に、ユーザ定義攻撃のタイプを示します。

表 11-8　ユーザ定義攻撃のタイプ

攻撃のタイプ	説明
user_defined/ 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/ 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。 • 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。 • 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。 • 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/ 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 11-9 に、さまざまなタイプの不正形式パケットを示します。

表 11-9　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 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 の DNS スプーフィング防止機能の動作が原因の不正形式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	ヘッダーの宛先ポート、送信元ポート、プロトコル、および送信元 IP アドレス 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。
malformed_packets /sip_bad_header	不正な形式のヘッダーを持つ SIP over UDP 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 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 11-15 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 11-10 に、Attack Statistics および Malicious Packet Statistics のフィールドを示します。

表 11-10　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 11-11 に、Detected Anomalies および Mitigated Attacks のフロー統計情報を示します。

表 11-11　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 11-11　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。

ワイルドカードとして使用できるアスタリスク（*）は、次を示すパラメータの 1 つに使用できます。

- 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。

Guard 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 Guard が生成することを示します。Guard 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 [*sub-zone-name*] [**current** | *report-id*] [**details**]

表 11-12 に、**show reports** コマンドの引数とキーワードを示します。

表 11-12　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.9-12 の「サブゾーンについて」を参照してください。
current	進行中の攻撃のレポートを表示します。 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。

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

表 11-13 に、**show reports** コマンド出力フィールドを示します。

表 11-13　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。**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 Type	軽減された攻撃のタイプ。指定できる値は、次のとおりです。 • **client_attack**：スプーフィング以外のすべてのトラフィック異常。 • **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。 • **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。 • **user_defined**：ユーザ フィルタによって処理されたすべての異常。ユーザ 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。 • **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。 • **hybrid**：特性の異なる複数の攻撃で構成された攻撃。 • **traffic_anomaly**：短期間のみ検出され、軽減を必要としなかった異常。
Peak Malicious Traffic	次のタイプのパケットの個数の合計です。 • Guard が攻撃の一部として識別し、ドロップしたパケット • パケットが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 から開始側のクライアントに応答が送信されたパケット。

次の例は、ゾーン上の現在の攻撃のレポートの表示方法を示しています。

```
user@GUARD-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	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

Malicious Packets Statistics:

	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 11-14 に、詳細なレポートに含まれているフローのフィールドを示します。

表 11-14　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。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、および宛先ポートを含み、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。

表 11-14　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。 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。

表 11-15 に、ゾンビ攻撃に関する詳細なレポートのフィールドを示します。

表 11-15　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 アドレスを示します。
Start Time	ゾンビ接続が初めて識別された日時を示します。
Duration	ゾンビ攻撃の期間を示します。
#Requests	ゾンビによって送信された HTTP get 要求の数を示します。

（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、攻撃レポートをネットワーク サーバにエクスポートします。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

攻撃の終了時に、攻撃レポートが自動的に XML 形式でエクスポートされるように、Guard を設定できます。ゾーンに対する攻撃が終了すると、Guard から任意のゾーンのレポートがエクスポートされます。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。次の URL にある Cisco.com の ソフトウェア センター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。

http://www.cisco.com/public/sw-center/

Guard 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、ゾーン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、Guard が SFTP 通信および SCP 通信に使用する SSH キー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 サーバへの攻撃が終了したら、レポート（XML 形式）を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 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**] {**sftp** | **scp**} *server full-file-name login*
- **copy reports** [**details**] [**xml**] *file-server-name dest-file-name*

SFTP および SCP はセキュアな通信では SSH を使用するため、**sftp** オプションまたは **scp** オプションを使用して **copy** コマンドを入力する前に Guard が使用する鍵を設定していない場合、Guard はパスワードの入力を要求します。

Guard がセキュアな通信のために使用する鍵を設定する方法の詳細については、P.3-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 11-16 に、**copy reports** コマンドの引数とキーワードを示します。

表 11-16　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、このバージョンに付属の xsd ファイルを参照してください（Cisco.com のソフトウェア センター（http://www.cisco.com/public/sw-center/）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。 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	FTP を使用しているネットワーク サーバに攻撃レポートをエクスポートします。
sftp	SFTP 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します。

表 11-16　copy reports コマンドの引数とキーワード（続き）

パラメータ	説明
scp	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	サーバのログイン名。 *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。
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。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Guard が SFTP 通信および SCP 通信で使用する 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。
dest-file-name	ファイルの名前。Guard は、**file-server** コマンドを使用してネットワーク サーバに対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、Guard 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
```

次の例は、Guard 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 **file-server** コマンドを使用して定義したネットワーク サーバにコピーする方法を示しています。

```
user@GUARD# 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ネットワーク 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** | **scp**} *server full-file-name login*
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] *file-server-name dest-file-name*

SFTP および SCP はセキュアな通信では SSH に依存しているため、**sftp** オプションまたは **scp** オプションを使用して **copy** コマンドを入力する前に、Guard が使用する鍵を設定していない場合、Guard はパスワードの入力を要求します。Guard がセキュアな通信のために使用する鍵を設定する方法の詳細については、P.3-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 11-17 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 11-17　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。
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)。 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 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。 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 11-17　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（Cisco.com の ソフトウェア センター（http://www.cisco.com/public/sw-center/）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。 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。
sftp	攻撃レポートを SFTP を使用してネットワーク サーバにエクスポートします。
scp	攻撃レポートを SCP 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。
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。 *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。

表 11-17　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
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。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Guard が SFTP 通信および SCP 通信で使用する 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。
dest-file-name	ファイルの名前。Guard は、**file-server** コマンドを使用して、ネットワーク サーバに対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@GUARD# 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@GUARD# 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@GUARD-conf-zone-scannet# no reports *
```