CHAPTER 13

Guard モジュールの診断ツールの使用

この章では、Cisco Anomaly Guard Module（Guard module）に関する統計情報や診断を表示する方法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。

- Guard モジュールの設定の表示
- Guard モジュールのゾーンの表示
- カウンタを使用したトラフィックの分析
- ゾーンのステータスの表示
- Guard モジュールのログ管理
- ネットワーク トラフィックの監視と攻撃シグニチャの抽出
- 一般的な診断データの表示
- フラッシュ メモリの使用率の表示
- メモリ消費量の表示
- CPU 使用率の表示
- システム リソースの監視
- ARP キャッシュの管理
- ネットワーク統計情報の表示
- traceroute の使用
- 接続の確認
- デバッグ情報の取得
- Guard モジュールの自己保護設定の表示

Guard モジュールの設定の表示

Guard モジュールの設定ファイルを表示できます。このファイルには、インターフェイスの IP アドレス、デフォルト ゲートウェイ アドレス、および設定されたゾーンなど、Guard モジュールの設定に関する情報が含まれています。

Guard モジュールの設定ファイルを表示するには、次のコマンドを使用します。

show running-config [**all** | **Guard module** | **interfaces** *interface-name* | self-protection | zones]

表 13-1 に、**show running-config** コマンドの引数とキーワードを示します。

表 13-1　show running-config コマンドの引数とキーワード

パラメータ	説明
all	Guard モジュールのすべての機能（Guard モジュール、ゾーン、インターフェイス、および自己保護）の設定ファイルを表示します。
Guard module	Guard モジュールの設定ファイルを表示します。
interfaces *interface-name*	Guard モジュールのインターフェイスの設定ファイルを表示します。インターフェイス名を入力します。
self-protection	Guard モジュールの自己保護の設定を表示します。
zones	すべてのゾーンの設定ファイルを表示します。

次の例は、Guard モジュールの設定ファイルを表示する方法を示しています。

```
user@GUARD# show running-config guard
```

設定ファイルは、Guard モジュールを現在の設定値で設定するために入力するコマンドで構成されています。Guard モジュールの設定ファイルをリモート FTP サーバにエクスポートして、バックアップ用にしたり、別の Guard モジュールにその Guard モジュールの設定パラメータを実装できるようにすることができます。詳細については、P.13-3 の「Guard モジュールのゾーンの表示」を参照してください。

Guard モジュールのゾーンの表示

グローバル モードで **show** コマンドを入力することにより、ゾーンの概要を表示して、アクティブなゾーンやゾーンの現在のステータスを確認できます。

表 13-2 に、各種のゾーン ステータスを示します。

表 13-2　ゾーンのステータス

ステータス	説明
Auto protect mode	ゾーン保護がイネーブルで、動的フィルタはユーザの操作なしでアクティブになります。 Guard モジュールで、ゾーン保護がイネーブルで、Guard モジュールがポリシーのしきい値調整のためにゾーンのトラフィック特性をラーニングしている場合、ゾーン名の隣には (+learning) と表示されます。
Interactive protect mode	ゾーンはインタラクティブ保護モードです。動的フィルタは手動でアクティブになります。
Threshold Tuning phase	ゾーンはしきい値調整フェーズです。Guard は、ゾーンのトラフィックを分析して、ラーニング プロセスのポリシー構築フェーズ中に構築されたポリシーのしきい値を定義します。
Policy Construction phase	ゾーンはポリシー構築フェーズです。ゾーンのポリシーが作成されます。
Standby	ゾーンはアクティブではありません。

次の例は、Guard モジュールのゾーンの概要を表示する方法を示しています。

```
user@GUARD# show
```

カウンタを使用したトラフィックの分析

Guard モジュールおよびゾーン カウンタを表示することで、Guard モジュールが処理している現在のトラフィック上の情報を表示したり、ゾーン トラフィックを分析したり、監視タスクを実行することができます。

この項では、次のトピックについて取り上げます。

カウンタおよびトラフィック レートの平均の表示

ゾーン カウンタを表示するには、次のコマンドのいずれかを入力します。

- **show** [**zone** *zone-name*] **rates** : 正当なカウンタと悪意のあるカウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **rates details** : すべての Guard モジュール カウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **rates history** : 過去 24 時間における 1 分ごとの悪意のあるカウンタと正当なカウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **counters** : Guard モジュールの悪意のあるカウンタと正当なカウンタを表示します。
- **show** [**zone** *zone-name*] **counters details** : すべての Guard モジュール カウンタを表示します。
- **show** [**zone** *zone-name*] **counters history** : 過去 1 時間の悪意のあるカウンタおよび正当なカウンタの値を 1 分ごとに表示します。

Guard モジュール カウンタを表示するには、グローバル モードまたは設定モードでこのコマンドを使用します。

ゾーン カウンタを表示するには、次のコマンド モードのいずれかでコマンドを使用します。

- ゾーン設定モード : **zone** *zone-name* キーワードおよび引数を使用しないでください。
- グローバル モードまたは設定モード : **zone** キーワードおよび *zone-name* 引数を入力してゾーン名を指定します。

レート単位は、ビット / 秒（bps）およびパケット / 秒（pps）で表されます。

（注）　ゾーンのレートは、ゾーン保護をイネーブルにしている場合、またはラーニング プロセスをアクティブにしている場合にだけ使用できます。

カウンタの単位はパケットおよびキロビットです。カウンタは、ゾーン保護をアクティブにしたときにゼロにリセットされます。

表 13-3 に、Guard モジュールのカウンタを示します。

表 13-3　Guard モジュール カウンタ

カウンタ	説明
Malicious	ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたカウンタとスプーフィングされたカウンタ（ゾンビ パケットも含む）の合計です。
Legitimate	Guard モジュールによってゾーンに転送された正当なトラフィック。
Received	Guard モジュールが受信し、処理したパケット。受信カウンタは、正当なカウンタと悪意のあるカウンタの合計です。
Forwarded	Guard モジュールによってゾーンに転送された正当なトラフィック。
Dropped	Guard モジュールの保護機能（動的フィルタ、フレックス コンテンツ フィルタ、およびレート リミッタ）によって攻撃の一部と判断され、ドロップされたパケット。
Replied	スプーフィング防止およびゾンビ防止機能の一部として、信頼できるトラフィックと悪意のあるトラフィックのどちらに属するかを確認するために開始クライアントに対して応答が送信されたパケット。

表 13-3　Guard モジュール カウンタ（続き）

カウンタ	説明
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と判断され、ゾーンに転送されなかったパケット。スプーフィングされたパケットは、応答が送信されたパケット（詳細については上の「Replied カウンタ」を参照）のうち、それに対する応答が受信されなかったものです。ゾンビ パケットは、スプーフィング パケット カウンタにも含まれています。
Invalid zone	保護がイネーブルになっているいずれのゾーンにも宛先変更されなかったトラフィック。この情報は、Guard モジュールのカウンタに限り使用可能です（**zone** キーワードを使用せずにグローバル モードまたは設定モードでコマンドを入力した場合）。

次の例は、Guard モジュールの平均トラフィック レートを表示する方法を示しています。

```
admin@GUARD-conf-zone-scannet# show rates
```

Guard モジュールおよびゾーンのカウンタのクリア

テストを行う予定で、カウンタにテスト セッションからの情報だけを含める場合は、Guard モジュールまたはゾーン カウンタをクリアできます。Guard モジュールはカウンタおよび平均トラフィック レートをクリアします。

Guard モジュールのカウンタをクリアするには、グローバル モードまたは設定モードでこのコマンドを使用します。

clear counters

次の例は、Guard モジュールのカウンタをクリアする方法を示しています。

```
user@GUARD-conf# clear counters
```

ゾーン カウンタをクリアするには、次のコマンドのいずれかを入力します。

- **clear counters**：ゾーン設定モード。
- **clear zone** *zone-name* **counters**：グローバル モードまたは設定モード。*zone-name* 引数には、ゾーンの名前を指定します。

次の例は、ゾーン カウンタをクリアする方法を示しています。

```
user@GUARD-conf-zone-scannet# clear counters
```

ゾーンのステータスの表示

ゾーンの概要とそのステータスを表示するには、ゾーン設定モードで **show** コマンドを使用します。概要には、次の情報が含まれます。

- ゾーンのステータス：動作状態を示します。動作状態は、保護モード、保護およびラーニングのモード、しきい値調整モード、ポリシー構築モード、または非アクティブのいずれかです。
- ゾーンの基本設定：保護モード（自動またはインタラクティブ）、しきい値、タイマー、および IP アドレスなど、ゾーンの基本的な設定を示します。

  詳細については、P.6-10 の「ゾーンのアトリビュートの設定」を参照してください。
- ゾーンのフィルタ：フレックスコンテンツ フィルタの設定、ユーザ フィルタの設定、およびアクティブな動的フィルタの数を含みます。ゾーンがインタラクティブ保護モードの場合、概要には推奨事項の数が表示されます。

  詳細については、P.7-5 の「フレックスコンテンツ フィルタの設定」および P.7-24 の「ユーザ フィルタの設定」を参照してください。
- ゾーンのトラフィック　レート：ゾーンの正当なトラフィックと悪意あるトラフィックのレートを表示します。

  詳細については、P.13-4 の「カウンタを使用したトラフィックの分析」を参照してください。

次の例は、ゾーン ステータスを表示する方法を示しています。

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

Guard モジュールのログ管理

Guard モジュールは、システムのアクティビティおよびイベントを自動的にログに記録します。Guard モジュールのログを表示して、Guard モジュールのアクティビティを確認および追跡できます。

表 13-4 に、イベント ログのレベルを示します。

表 13-4　イベント ログのレベル

イベント レベル	数値コード	説明
Emergencies	0	システムが使用不能
Alerts	1	ただちに対処が必要
Critical	2	深刻な状態
Errors	3	エラー状態
Warnings	4	警告状態
Notifications	5	通常、ただし注意が必要
Informational	6	情報メッセージ
Debugging	7	デバッグ メッセージ

ログ ファイルには、すべてのログ レベル（emergencies、alerts、critical、errors、warnings、notification、informational、および debugging）が表示されます。Guard モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

イベント ログは、ローカルで表示することも、リモート サーバから表示することもできます。この項では、次のトピックについて取り上げます。

- オンライン イベント ログの表示
- ログ ファイルの管理

オンライン イベント ログの管理

この項では、Guard モジュールのイベントのリアルタイム ロギングを管理する方法について説明します。この項では、次のトピックについて取り上げます。

- オンライン イベント ログの表示
- オンライン イベント ログのエクスポート

オンライン イベント ログの表示

Guard モジュールの監視機能をアクティブにして、リアルタイム イベント ログを表示すると、Guard モジュール イベントのオンライン ロギングを表示できます。オンライン イベント ログを表示するには、次のコマンドを使用します。

event monitor

次の例は、モニタリングをアクティブにする方法を示しています。

```
user@GUARD# event monitor
```

画面は新しいイベントを表示するために、定期的にアップデートされます。

（注） モニタリングを非アクティブにするには、**no event monitor** コマンドを使用してください。

オンライン イベント ログのエクスポート

Guard モジュールのオンライン イベント ログをエクスポートして、ログファイルに登録された Guard モジュールの動作を表示できます。また、Guard モジュールのログ ファイルに登録されている Guard モジュールのイベントをリモート ホストから表示できます。Guard モジュールのログ ファイルは、syslog メカニズムを使用してエクスポートされます。Guard モジュールのログ ファイルを複数の syslog サーバにエクスポートし、追加サーバを指定できるため、1 つのサーバがオフラインになっても、他のサーバがメッセージを受信できます。

Guard モジュールのオンライン ログのエクスポートは、リモート syslog サーバだけに適用できます。リモート syslog サーバが使用できない場合は、**copy log** コマンドを使用して、Guard モジュールのログ情報をファイルにエクスポートしてください。

次に、イベント ログの例を示します。

```
Sep 11 16:34:40 10.4.4.4 cm: scannet, 5 threshold-tuning-start: Zone
activation completed successfully.
```

システム log メッセージの構文は、次のとおりです。

event-date event-time Guard-IP-address protection-level zone-name event-severity-level event-type event-description

オンライン イベント ログをエクスポートするには、次の手順を実行します。

ステップ 1　（オプション）設定モードで次のコマンドを入力して、ロギング パラメータを設定します。

```
logging {facility | trap}
```

表 13-5 に、**logging** コマンドのキーワードを示します。

表 13-5　logging コマンドのキーワード

パラメータ	説明
facility	エクスポート syslog ファシリティ。リモート syslog サーバは、ロギング ファシリティを使用してイベントをフィルタリングします。たとえば、ロギング ファシリティを使用すると、リモート ユーザは、Guard モジュール イベントを 1 つのファイルで受信し、他のネットワーク デバイスからのイベントを別のファイルで受信できます。 使用できるファシリティは、local0 ～ local7 です。デフォルトは local4 です。
trap	リモート syslog に送信する syslog トラップの重大度。重大度のトラップ レベルには、それより高い重大度のレベルが含まれます。たとえば、トラップ レベルを **warning** に設定すると、error、critical、alerts、および emergencies も送信されます。指定できるトラップ レベルは、高い方から順に emergencies、alerts、critical、errors、warnings、notification、informational、および debugging です。デフォルトは notification です。

（注） 動的フィルタの追加および削除に関するイベントを受信するには、トラップ レベルを informational に変更してください。

ステップ 2　次のコマンドを入力して、リモート syslog サーバの IP アドレスを設定します。

logging host *remote-syslog-server-ip*

remote-syslog-server-ip　引数には、リモート syslog サーバの IP アドレスを指定します。

ロギング メッセージを受信する syslog サーバのリストを作成するには、**logging host** コマンドを複数回入力してください。

次の例は、重大度レベルが notification より高いトラップを送信するように Guard モジュールを設定する方法を示しています。Guard モジュールは、ファシリティ local3 を使用して、IP アドレス 10.0.0.191 の syslog サーバにトラップを送信します。

```
user@GUARD-conf# logging facility local3
user@GUARD-conf# logging trap notifications
user@GUARD-conf# logging host 10.0.0.191
```

Guard モジュールがオンライン イベント ログのエクスポートに使用する設定を表示するには、**show logging** コマンドまたは **show log export-ip** コマンドを使用します。

ログ ファイルの管理

この項では、Guard モジュールのログ ファイルを管理する方法について説明します。この項では、次のトピックについて取り上げます。

- ログ ファイルの表示
- ログ ファイルのエクスポート
- ログ ファイルのクリア

ログ ファイルの表示

診断または監視のために Guard モジュールのログを表示できます。Guard モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

Guard モジュールのログを表示するには、グローバル モードで次のコマンドを使用します。

show log

次の例は、Guard モジュールのログを表示する方法を示しています。

```
user@GUARD# show log
```

ゾーンのログを表示して、指定したゾーンだけに関連するイベントを確認できます。

ゾーンのログを表示するには、**show log** [*sub-zone-name*] コマンドをゾーン設定モードで使用します。*sub-zone-name* 引数には、ゾーンから作成されたサブゾーンの名前を指定します。詳細については、P.10-11 の「サブゾーンについて」を参照してください。

ログ ファイルのエクスポート

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、監視または診断を行うために、Guard モジュールのログ ファイルをネットワーク サーバにエクスポートできます。

- **copy** [**zone** *zone-name*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log** {**sftp** | **scp**} *server full-file-name login*

（注）　**logging host** コマンドを使用すると、イベント ログを自動的にエクスポートするように Guard モジュールを設定できます。詳細については、P.13-10 の「オンライン イベント ログのエクスポート」を参照してください。

SFTP および SCP は、セキュアな通信では Secure Shell（SSH; セキュア シェル）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 モジュールが使用する鍵が設定されていない場合、Guard モジュールはパスワードの入力を要求します。Guard モジュール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.4-38 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 13-6 に、**copy log ftp** コマンドの引数とキーワードを示します。

表 13-6　copy log ftp コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	（オプション）ゾーン名。ゾーンのログ ファイルをエクスポートします。デフォルトでは、Guard モジュールのログ ファイルがエクスポートされます。
log	ログ ファイルをエクスポートします。

表 13-6　copy log ftp コマンドの引数とキーワード（続き）

パラメータ	説明
ftp	ログを FTP ネットワーク サーバにエクスポートします。
sftp	ログを SFTP ネットワーク サーバにエクスポートします。
scp	ログを SCP 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。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
remote-path	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。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。

次の例は、Guard モジュールのログ ファイルを FTP サーバにエクスポートする方法を示しています。

```
user@GUARD# copy log ftp 10.0.0.191 log.txt <user> <password>
```

ログ ファイルのクリア

Guard モジュールまたはゾーンのログ ファイルが大きい場合、またはテストを行う予定で、ログ ファイルにテスト セッションからの情報だけが含まれるようにする場合は、ログ ファイルをクリアすることができます。

Guard モジュールまたはゾーンのログ ファイルのエントリをすべてクリアするには、設定モードまたはゾーン設定モードで次のコマンドを使用します。

clear [**zone** *zone-name*] **log**

zone-name 引数には、ゾーン名を指定します。デフォルトでは、Guard モジュールのログ ファイルがクリアされます。**clear log** コマンドをゾーン設定モードで入力する場合、**zone** *zone-name* キーワードと引数は使用できません。現在のゾーン ログの全エントリをクリアするには、ゾーン設定モードで **clear log** コマンドを使用します。

次の例は、Guard モジュール ログをクリアする方法を示しています。

```
user@GUARD-conf# clear log
```

ネットワーク トラフィックの監視と攻撃シグニチャの抽出

ネットワークの動作を阻害しないタップを使用して、ネットワークから直接トラフィックを記録するように Guard モジュールを設定できます。記録されたトラフィックからデータベースを作成できます。記録されたトラフィックのデータベースのクエリーによって、過去のイベントの分析、攻撃シグニチャの生成、ネットワークの現在のトラフィック パターンと Guard モジュールで以前に正常のトラフィック状態で記録されたトラフィック パターンとの比較などを行うことができます。

フィルタを設定すると、特定の基準を満たすトラフィックだけを Guard モジュールで記録することや、すべてのトラフィック データを記録して、Guard モジュールに表示するトラフィックをフィルタリングするように指定できます。

Guard モジュールは、トラフィックを gzip（GNU zip）プログラムで圧縮された PCAP 形式で保存し、記録されたデータを説明する Extensible Markup Language（XML）形式のファイルを添付します。

記録されたトラフィックの重要な用途は、記録された攻撃パケットのペイロードに共通のパターンまたはシグニチャが見られるかどうかを判断するというものです。Guard モジュールには、記録されたトラフィックを分析して、シグニチャを抽出する機能が備わっています。シグニチャを使用すると、そのシグニチャと一致するパケット ペイロードを含むすべてのトラフィックをブロックするようにフレックスコンテンツ フィルタを設定できます。

Guard モジュールは、次の 2 つの方法でトラフィックを記録できます。

- 自動：トラフィック データは持続的にパケットダンプ キャプチャ ファイルに記録されます。

  新しいパケットダンプ キャプチャ ファイルによって、以前のファイルは置き換えられます。以前のパケットダンプ キャプチャ ファイルを保存するには、ネットワーク サーバにそれらのファイルをエクスポートする必要があります。

- 手動：ユーザがアクティブにしている場合に、トラフィックがパケットダンプ キャプチャ ファイルに記録されます。

  以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。記録されたトラフィックを保存するには、Guard モジュールでトラフィックの記録を再開する前に、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Guard モジュールは、手動で同時に最大 4 つのゾーンについてトラフィックを記録できます。

デフォルトでは、Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイル用にディスク スペースを開放するため、古いファイルを削除する必要があります。

この項では、次のトピックについて取り上げます。

- Guard モジュールの設定によるトラフィックの自動記録
- Guard モジュールのアクティブ化によるトラフィックの手動記録
- Guard モジュールによるトラフィックの手動記録の停止
- 手動パケットダンプ設定の表示
- パケットダンプ キャプチャ ファイルの自動エクスポート
- パケットダンプ キャプチャ ファイルの手動エクスポート
- パケットダンプ キャプチャ ファイルのインポート
- パケットダンプ キャプチャ ファイルの表示
- パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成
- パケットダンプ キャプチャ ファイルのコピー
- パケットダンプ キャプチャ ファイルの削除

Guard モジュールの設定によるトラフィックの自動記録

Guard モジュールは、自動的にネットワーク トラフィックを記録するようにアクティブにすることができます。これにより、ネットワークに問題や攻撃が発生したときに、分析または比較に使用できるトラフィックの記録を入手できます。パケットダンプ キャプチャ フィルタを使用して、指定した基準を満たすトラフィックだけが記録されるように Guard モジュールを設定できます。また、すべてのトラフィックを記録し、その記録済みのトラフィックを表示するときにパケットダンプ キャプチャ フィルタを適用することもできます。

Guard モジュールでは、トラフィックがキャプチャ バッファに記録されます。キャプチャ バッファのサイズが 50MB に到達するか、または 10 分が経過すると、Guard モジュールはバッファを圧縮形式のローカル ファイルに保存し、バッファをクリアしてから、トラフィックの記録を継続します。

Guard モジュールは、複数の自動パケットダンプ キャプチャ ファイルを保存します。Guard モジュールによって記録されたトラフィックは、トラフィックの処理方法に基づいて分割されるため、複数の自動パケットダンプ キャプチャ ファイルを 1 つの時間枠から取得できます。自動パケットダンプ キャプチャ ファイルの名前には、Guard モジュールでトラフィックが記録された日時およびトラフィックの処理方法に関する情報が含まれます。

表 13-7 に、自動パケットダンプ キャプチャ ファイルの名前セクションを示します。

表 13-7　自動パケットダンプ キャプチャ ファイルの名前のセクション

セクション	説明
機能	パケットダンプ キャプチャの際に実行される Guard モジュールの機能のタイプ。 • protect：Guard　モジュールはゾーン保護中にトラフィックを記録。 • learn：Guard モジュールはゾーンのラーニング プロセス中または保護およびラーニング プロセス中にトラフィックを記録。
キャプチャ開始時刻	Guard モジュールでトラフィックの記録が開始した時刻。
キャプチャ終了時刻	（オプション）Guard モジュールでトラフィックの記録が終了した時刻。Guard モジュールが現在トラフィックをファイルに記録している場合、終了時刻は表示されません。

表 13-7　自動パケットダンプ キャプチャ ファイルの名前のセクション（続き）

セクション	説明
処理	Guard モジュールがトラフィックの処理に使用する方式。この方式は次のいずれかになります。 • forwarded : Guard モジュールはトラフィックを正当であると識別して、ゾーンに転送する。 • dropped : Guard モジュールはトラフィックを悪意があるトラフィックであると識別して、削除する。 • replied : Guard モジュールは、スプーフィング防止およびゾンビ防止機能の一部として、信頼できるトラフィックと悪意のあるトラフィックのどちらに属するかを確認するために開始クライアントに対して応答を送信する。

Guard モジュールは、ラーニング プロセスでは、1 つのパケットダンプ キャプチャ ファイルを、ゾーン保護がイネーブルのときには次の 2 つのタイプのパケットダンプ キャプチャ ファイルを保存します。

- 直前 10 分間のトラフィック
- 現在のトラフィック

ゾーン保護をアクティブにするか、Guard モジュールでネットワーク トラフィックが自動的に記録されるように設定すると、保護プロセス中に記録された以前のパケットダンプ キャプチャ ファイルがすべて消去され、新しいファイルが作成されます。

自動的にネットワーク トラフィックを記録するように Guard モジュールを設定するには、次の手順を実行します。

ステップ 1　ゾーン トラフィックを自動的に記録するように Guard モジュールを設定します。ゾーン設定モードで次のコマンドを入力します。

```
packet-dump auto-capture
```

ステップ 2　（オプション）パケットダンプ キャプチャ データベースを作成するには、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。パケットダンプ キャプチャ データベースを作成するには、パケットダンプ キャプチャ ファイルをエクスポートする必要があります。

P.13-24 の「パケットダンプ キャプチャ ファイルの自動エクスポート」を参照してください。

次の例は、自動的にゾーン トラフィックを記録するように Guard モジュールを設定する方法を示しています。

```
user@GUARD-conf-zone-scannet# packet-dump auto-capture
```

Guard モジュールによるゾーン トラフィック データの自動キャプチャを停止するには、**no packet-dump auto-capture** コマンドを使用します。

現在のパケットダンプ設定を表示するには、**show packet-dump** コマンドを使用します。

Guard モジュールのアクティブ化によるトラフィックの手動記録

トラフィックの記録を開始するように Guard モジュールをアクティブにできるため、特定の期間のトラフィックを記録したり、Guard モジュールがトラフィックの記録に使用する基準を変更することができます。

Guard モジュールは指定した数のパケットが記録されるか、またはラーニング プロセスとゾーン保護のいずれかが終了した時点で、トラフィックの記録を停止し、手動パケットダンプ キャプチャをファイルに保存します。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Guard モジュールは、同時に 10 ゾーンまで手動パケットダンプ キャプチャを記録できます。

手動パケットダンプ キャプチャをアクティブにするには、ゾーン設定モードで次のコマンドを使用します。

packet-dump capture [**view**] *capture-name pdump-rate pdump-count* {**all** | **dropped** | **forwarded** | **replied**} [*tcpdump-expression*]

（注） トラフィックをキャプチャする間は、CLI セッションが停止します。キャプチャの実行中に作業を続行するには、Guard モジュールとの追加のセッションを確立してください。

表 13-8 に、**packet-dump** コマンドの引数とキーワードを示します。

表 13-8　packet-dump コマンドの引数とキーワード

パラメータ	説明
view	（オプション）Guard モジュールでリアルタイムに記録されているトラフィックを表示します。
capture-name	パケットダンプ キャプチャ ファイルの名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。
pdump-rate	サンプル レート（pps）。1 ～ 10000 の値を入力します。 **（注）** Guard モジュールでは、同時に発生するすべての手動キャプチャについて、最大で 10,000 パケット/秒の累積パケットダンプ キャプチャ レートがサポートされます。 高いサンプル レート値を設定したパケットダンプ キャプチャは、多くのリソースを消費します。パフォーマンスに悪影響を与える可能性があるため、高いレート値を設定するときは注意してください。

表 13-8　packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
pdump-count	記録対象のパケットの数。Guard モジュールが指定した数のパケットの記録を終了した時点で、手動パケットダンプ キャプチャ バッファがファイルに保存されます。1 ～ 5000 の整数を入力します。
all	すべてのトラフィックをキャプチャします。
dropped	Guard モジュールがドロップしたトラフィックだけをキャプチャします。
forwarded	Guard モジュールからゾーンに転送された正当なトラフィックだけをキャプチャします。
replied	検証の試行で Guard モジュールのスプーフィング防止機能およびゾンビ防止機能によって送信元に返送されたトラフィックだけをキャプチャします。
tcpdump-expression	（オプション）記録対象のトラフィックを指定するために適用するフィルタ。Guard モジュールはフィルタの式に適合するトラフィックだけをキャプチャします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-11 の「tcpdump 式の構文の設定」を参照してください。

次の例は、手動パケットダンプ キャプチャをアクティブにして、10 pps のサンプルレートで 1000 パケットを記録して、キャプチャしたパケットを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# packet-dump capture view 10 1000 all
```

Guard モジュールによるトラフィックの手動記録の停止

Guard モジュールでは、キャプチャをアクティブにしたときに指定したパケット数が記録された時点で、手動パケットダンプ キャプチャが停止します。しかし、指定したパケット数が Guard モジュールによって記録される前に、手動パケットダンプ キャプチャを停止することができます。

Guard モジュールによるトラフィックの手動記録を停止するには、次のいずれかのアクションを実行します。

- 開かれている CLI セッションで **Ctrl+C** キーを押す。
- 新しい CLI セッションを開き、関連するゾーン設定モードで次のコマンドを入力する。

  no packet-dump capture *capture-name*

capture-name 引数には、停止するキャプチャの名前を指定します。

Guard モジュールは、パケットダンプ キャプチャ ファイルを保存します。

手動パケットダンプ設定の表示

手動パケットダンプ キャプチャ ファイル用に割り当てられたディスク スペースの現在の容量を表示するには、設定モードまたはグローバル モードで **show packet-dump** コマンドを使用します。Guard モジュールでは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に、単一ブロックのディスク スペースが割り当てられます。

次の例は、Guard モジュールがゾーンの手動パケットダンプ キャプチャ ファイルに割り当てるディスク スペースの現在の総計を表示する方法を示しています。

```
user@GUARD-conf# show packet-dump
```

表 13-9 に、**show packet-dump** コマンド出力のフィールドを示します。

表 13-9　手動の show packet-dump コマンド出力のフィールドの説明

フィールド	説明
Allocated disk-space	すべてのゾーンの手動パケットダンプ キャプチャ用に割り当てられたディスク スペースの総容量を MB 単位で指定します。
Occupied disk-space	割り当てられたディスク スペースのうち、すべてのゾーンからの手動パケット ダンプ ファイルによって消費されたパーセンテージを示します。

パケットダンプ キャプチャ ファイルの自動エクスポート

FTP、Secure FTP（SFTP）、または Secure Copy（SCP）を使用してファイルを転送するネットワーク サーバにパケットダンプ キャプチャ ファイルを自動的にエクスポートするように Guard モジュールを設定できます。自動エクスポート機能をイネーブルにすると、Guard モジュールでパケットダンプ バッファの内容がローカル ファイルに保存されるたびに、パケットダンプ キャプチャ ファイルがエクスポートされます。Guard モジュールは、「gzip」（GNU zip）プログラムで圧縮、符号化したパケットダンプ キャプチャ ファイルを PCAP 形式でエクスポートし、記録されたデータを説明する XML 形式のファイルを添付します。XML スキーマについては、このバージョンに付属の Capture.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 モジュールがパケットダンプ キャプチャ ファイル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 packet-dump *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。SFTP または SCP を使用するようにネットワーク サーバを設定する場合は、Guard モジュールが 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.14-11 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、パケットダンプ キャプチャ ファイル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 packet-dump Corp-FTP-Server
```

パケットダンプ キャプチャ ファイルの手動エクスポート

FTP、SFTP、または SCP を使用してファイルを転送するネットワーク サーバにパケットダンプ キャプチャ ファイルを自動的にエクスポートするように設定できます。パケットダンプ キャプチャ ファイルを 1 つエクスポートすることも、特定のゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートすることもできます。Guard モジュールは、gzip（GNU zip）プログラムで圧縮、符号

化したパケットダンプ キャプチャ ファイルを PCAP 形式でエクスポートし、記録されたデータを説明する XML 形式のファイルを添付します。XML スキーマについては、このバージョンに付属の Capture.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/

パケットダンプ キャプチャ ファイルをネットワーク サーバに手動でエクスポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **ftp** *server remote-path* [*login* [*password*]]
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] {**sftp** | **scp**} *server remote-path login*
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] *file-server-name*

SFTP および SCP は安全な通信の SSH に従うので、Guard モジュールは **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 モジュールが使用する鍵を設定しない場合、パスワードの入力を求めます。Guard モジュール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.4-38 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 13-10 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 13-10　copy zone packet-dump 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。
packet-dump captures	パケットダンプ キャプチャ ファイルのエクスポート。
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートします。詳細については、P.13-29 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。

表 13-10　copy zone packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
ftp	パケットダンプ キャプチャ ファイルを FTP ネットワーク サーバからエクスポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP ネットワーク サーバからエクスポートします。
scp	パケットダンプ キャプチャ ファイルを SCP ネットワーク サーバから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。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
remote-path	Guard モジュールがパケットダンプ キャプチャ ファイルを保存する場所の完全なパス名。
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。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。
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 モジュールが 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.14-11 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、ゾーン scannet のパケットダンプ キャプチャ ファイルを FTP サーバ 10.0.0.191 にエクスポートする方法を示しています。

```
user@GUARD# copy zone scannet packet-dump captures ftp 10.0.0.191
<user> <password>
```

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを **file-server** コマンドを使用して定義されたネットワーク サーバに手動でエクスポートする方法を示しています。

```
user@GUARD# copy zone scannet packet-dump captures cap-5-10-05
Corp-FTP-Server
```

パケットダンプ キャプチャ ファイルのインポート

ネットワーク サーバからパケットダンプ キャプチャ ファイルを Guard モジュールにインポートできるため、過去のイベントを分析することや、現在のネットワーク トラフィック パターンと Guard モジュールが以前に通常のトラフィック状態で記録したトラフィック パターンとを比較することができます。Guard モジュールは、XML 形式と PCAP 形式のパケットダンプ キャプチャ ファイルをどちらもインポートします。

パケットダンプ キャプチャ ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy ftp zone** *zone-name* **packet-dump captures** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **zone** *zone-name* **packet-dump captures** *server full-file-name login*
- **copy** *file-server-name* **zone** *zone-name* **packet-dump captures** *capture-name*

SFTP および SCP は安全な通信の SSH に従うので、Guard モジュールは **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 モジュールが使用する鍵を設定しない場合、パスワードの入力を求めます。Guard モジュール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.4-38 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 13-11 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 13-11　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
ftp	パケットダンプ キャプチャ ファイルを FTP ネットワーク サーバからインポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP ネットワーク サーバからインポートします。
scp	パケットダンプ キャプチャ ファイルを SCP ネットワーク サーバからインポートします。
zone *zone-name*	パケットダンプ キャプチャ ファイルをインポートする既存のゾーンの名前。
packet-dump captures	パケットダンプ キャプチャ ファイルのインポート。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
full-file-name	インポート対象のファイルの完全なパスとファイル名。ファイル拡張子は除きます。パスを指定しない場合、サーバはユーザのホーム ディレクトリからファイルをコピーします。 **（注）** ファイル拡張子を指定しないでください。指定すると、インポート プロセスが失敗する場合があります。
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）FTP サーバのパスワード。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。

表 13-11　copy zone packet-dump 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 モジュールが 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.14-11 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。
capture-name	インポートするファイルの名前。Guard 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、ゾーン scannet のパケットダンプ キャプチャ ファイルを FTP サーバ 10.0.0.191 からインポートする方法を示しています。

```
user@GUARD# copy ftp zone scannet packet-dump captures 10.0.0.191
/root/scannet/captures/capture-1 <user> <password>
```

次の例は、ネットワーク サーバからパケットダンプ キャプチャ ファイルをインポートする方法を示しています。

```
user@GUARD# copy CorpFTP running-config capture-1
```

パケットダンプ キャプチャ ファイルの表示

パケットダンプ キャプチャ ファイルのリスト、または 1 つのパケットダンプ キャプチャ ファイルの内容を表示できます。デフォルトでは、Guard モジュールはすべてのゾーンのパケットダンプ キャプチャ ファイルのリストを表示します。

パケットダンプ キャプチャ ファイルを表示するには、ゾーン設定モードで次のコマンドを使用します。

show packet-dump captures [*capture-name* [*tcpdump-expression*]]

表 13-12 に、**show packet-dump captures** コマンドの引数を示します。

表 13-12　show packet-dump captures コマンドの引数

パラメータ	説明
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはすべてのゾーンのパケットダンプ キャプチャ ファイルのリストを表示します。コマンド出力のフィールドの説明については、表 13-13 を参照してください。 パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはファイルを TCPDump 形式で表示します。
tcpdump-expression	（オプション）Guard モジュールでパケットダンプ キャプチャ ファイルを表示する際に使用されるフィルタ。Guard モジュールは、フィルタ基準に一致する一部のパケットダンプ キャプチャ ファイルだけを表示します。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-11 の「tcpdump 式の構文の設定」を参照してください。

次の例は、パケットダンプ キャプチャ ファイルのリストを表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show packet-dump captures
```

表 13-13 に、**show packet-dump captures** コマンド出力のフィールドを示します。

表 13-13　show packet-dump captures コマンド出力のフィールドの説明

フィールド	説明
Capture -name	パケットダンプ キャプチャ ファイルの名前。自動パケットダンプ キャプチャ ファイルの名前の説明については、表 13-7 を参照してください。
Size (MB)	パケットダンプ キャプチャ ファイルのサイズ（MB）。
Filter	Guard モジュールがトラフィックの記録時に使用するユーザ定義のフィルタ。このフィルタは TCPDump 形式です。この式の規則は、フレックスコンテンツ　フィルタの TCPDump 式の規則と同じです。詳細については、P.7-11 の「tcpdump 式の構文の設定」を参照してください。

パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成

攻撃シグニチャは、攻撃パケットのペイロードに見られる共通パターンを記述するものです。Guard モジュールをアクティブにして異常なトラフィックのシグニチャを生成し、この情報を使用して同じタイプの将来の攻撃をすばやく識別できます。この機能を使用すると、シグニチャが発行される前であっても（アンチウィルス ソフトウェアのメーカーやメーリング リストなどから）、新しい DDoS 攻撃（分散型サービス拒絶攻撃）やインターネット ワームを検出することができます。

Guard モジュールでは、フレックスコンテンツ フィルタのパターン式の構文を使用して、攻撃シグニチャが生成されます。このシグニチャをフレックスコンテンツ フィルタのパターンで使用して、異常なトラフィックをフィルタリングして排除できます。詳細については、P.7-5 の「フレックスコンテンツ フィルタの設定」を参照してください。

トラフィックが通常状態のときに Guard モジュールが記録したパケットダンプ キャプチャ ファイルを、参照のために追加で指定できます。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Guard モジュールでは、異常なトラフィックのシグニチャが生成され、トラフィックが通常状態のときに記録されたトラフィックの中に、シグニチャが存在している時間の割合が特定されます。正常のトラフィック状態で記録されたトラフィックに攻撃シグニチャが高い確率で出現しても、攻撃のパターンを意味するとは限りません。

攻撃のシグニチャを生成するには、次の手順を実行します。

ステップ 1　**packet-dump capture** コマンドを使用して、Guard モジュールをアクティブにし、攻撃中のトラフィックを記録します。

詳細については、P.13-20 の「Guard モジュールのアクティブ化によるトラフィックの手動記録」を参照してください。

ステップ 2　攻撃進行中に Guard モジュールが記録したパケットダンプ キャプチャ ファイルを識別します。パケットダンプ キャプチャ ファイルのリストを表示するには、**show packet-dump captures** コマンドを使用します。

詳細については、P.13-29 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。

ステップ 3　Guard モジュールをアクティブにして、攻撃されたトラフィックのシグニチャを生成します。ゾーン設定モードで次のコマンドを入力します。

```
show packet-dump signatures capture-name [reference-capture-name]
```

表 13-14 に、**show packet-dump signatures** コマンドの引数を示します。

表 13-14　show packet-dump signatures コマンドの引数

パラメータ	説明
capture-name	シグニチャの生成元である既存のパケットダンプ キャプチャ ファイルの名前。
reference-capture-name	（オプション）トラフィックが通常状態のときに Guard モジュールによって記録された既存のパケットダンプ キャプチャ ファイルの名前。参照用のパケットダンプ キャプチャ ファイルを指定した場合は、シグニチャが参照用のパケットダンプ キャプチャ ファイルに存在する時間の割合が表示されます。

表 13-15 に、**show packet-dump signatures** コマンド出力のフィールドを示します。

表 13-15　show packet-dump signatures コマンド出力のフィールドの説明

フィールド	説明
Start Offset	パケット ペイロード開始からのオフセット（バイト単位）。ここでパターンが開始します。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *start-offset* 引数にコピーします。
End Offset	パケット ペイロード開始からのオフセット（バイト単位）。ここでパターンが終了します。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *end-offset* 引数にコピーします。
Pattern	Guard モジュールが生成したシグニチャ。Guard モジュールでは、フレックスコンテンツ フィルタのパターン式の構文を使用して、シグニチャが生成されます。詳細については、P.7-15 の「パターン式構文の設定」を参照してください。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーできます。
Percentage	シグニチャが *reference-capture-name* ファイルに存在する時間の割合。

次の例は、手動パケットダンプ キャプチャ ファイルからシグニチャを生成する方法を示しています。

```
user@GUARD-conf-zone-scannet# show packet-dump signatures PDumpCapture
```

パケットダンプ キャプチャ ファイルのコピー

1 つのパケットダンプ キャプチャ ファイル、または 1 つのファイルの一部を、新しい名前でコピーできます。Guard モジュールは、既存の自動パケットダンプ キャプチャ ファイルを新しいファイルで上書きします。自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルをコピーする場合、Guard モジュールはこれらのファイルを手動ファイルとして保存します。ディスク スペースを解放する必要がある場合は、そのコピーを手動で削除します。詳細については、P.13-35 の「パケットダンプ キャプチャ ファイルの削除」を参照してください。

パケットダンプ キャプチャ ファイルをコピーするには、設定モードで次のコマンドを使用します。

copy zone *zone-name* **packet-dump captures** *capture-name* [*tcpdump-expression*] *new-name*

表 13-16 に、**copy zone packet-dump captures** コマンドの引数とキーワードを示します。

表 13-16　copy zone packet-dump captures 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。
packet-dump	パケットダンプ キャプチャ ファイルのコピー。
captures *capture-name*	既存のパケットダンプ キャプチャ ファイルの名前。
tcpdump-expression	（オプション）Guard モジュールでパケットダンプ キャプチャ ファイルのコピーに使用されるフィルタ。Guard モジュールは、フィルタ基準に一致する一部のパケットダンプ キャプチャ ファイルだけをコピーします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-11 の「tcpdump 式の構文の設定」を参照してください。
new-name	新しいパケットダンプ キャプチャ ファイルの名前。 名前は、1 ～ 63 文字の英数字の文字列で、スペースを含めることはできませんが、アンダースコアを含めることはできます。

次の例は、パケットダンプ キャプチャ ファイル capture-1 の一部で capture-2 という名前のキャプチャ ファイルに適合する部分をコピーする方法を示しています。

```
user@GUARD-conf# copy zone scannet capture-1 "tcp and dst port 80 and
not src port 1000" capture-2
```

パケットダンプ キャプチャ ファイルの削除

デフォルトでは、Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

ゾーンごとに保存できる手動パケットダンプ キャプチャ ファイルは 1 つだけです。また、Guard モジュールに保存できるパケットダンプ キャプチャ ファイルは 10 個までです。新しい手動パケットダンプ キャプチャ ファイルのためのスペースを解放するには、古いファイルを削除する必要があります。

自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルを削除するには、次のいずれかのコマンドを使用します。

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*}（設定モードで）
- **clear packet-dump captures** {***** | *name*}（ゾーン設定モードで）

表 13-17 に、**clear packet-dump** コマンドの引数とキーワードを示します。

表 13-17　clear packet-dump 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。
packet-dump captures	パケットダンプ キャプチャ ファイルの削除。
*	すべてのパケットダンプ キャプチャ ファイルを消去します。
name	削除対象のパケットダンプ キャプチャ ファイルの名前。

次の例は、すべての手動パケットダンプ キャプチャ ファイルを削除する方法を示しています。

```
user@GUARD-conf# clear packet-dump captures *
```

一般的な診断データの表示

一般的な診断データを表示するには、次のコマンドを使用します。

show diagnostic-info [**details**]

診断データには、次の情報があります。

- Line Card Number：Guard モジュールの識別子ストリング。
- Number of Pentium-class Processors：Guard モジュールのプロセッサの番号。Guard モジュールはプロセッサ 1 をサポートします。
- BIOS Vendor：Guard モジュールの BIOS のベンダー。
- BIOS Version：Guard モジュールの BIOS バージョン。
- Total available memory：Guard モジュールで使用可能なメモリの合計量。
- Size of compact flash：Guard モジュールのコンパクト フラッシュのサイズ。
- Slot Num：モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
- CFE version：CFE のバージョン番号。

（注）　CFE のバージョンを変更するには、新しいフラッシュ バージョンをインストールする必要があります。CFE の新しいバージョンを焼き付けるには、**flash-burn** コマンドを使用します。詳細については、P.14-27 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

- Recognition Average Sample Loss：計算済みの平均パケット サンプル損失。
- Forward failures (no resources)：システム リソースが不足しているために転送されなかったパケット数。

（注）　Recognition Average Sample Loss または Forward failures の値が大きい場合、Guard モジュールのトラフィックが過負荷の状態に陥っています。複数の Guard モジュールを負荷分散型構成にインストールすることをお勧めします。

フラッシュ メモリの使用率の表示

Guard モジュールは、アクティビティ ログおよびゾーン攻撃レポートを保持します。ディスクの使用率が 75% を超えている場合、または Guard モジュールに多数のゾーン（500 を超える）が定義されている場合は、ファイル履歴パラメータの値を小さくすることをお勧めします。使用されているディスク スペースがディスクの最大キャパシティの約 80% に達すると、Guard モジュールは syslog に警告メッセージを表示します。

Guard モジュールが警告メッセージを表示した場合、ゾーン攻撃レポートをネットワーク サーバにエクスポートし、古い攻撃レポートを削除できます（P.12-19 の「攻撃レポートのエクスポート」および P.12-24 の「攻撃レポートの削除」を参照）。

Guard モジュールのレコードをネットワーク サーバに定期的に格納してから、ログをクリアすることをお勧めします。

（注）　ディスク使用率がディスクの最大キャパシティの 80% に達すると、Guard モジュールは情報を消去して、ディスク使用率を約 75% に減らします。

Guard モジュール上にインストールしたフラッシュの全体量の中で利用できるフラッシュの容量を表示するには、グローバル モードで次のコマンドを使用します。

show flash-usage

次の例は、フラッシュ メモリの使用率を表示する方法を示しています。

```
user@GUARD# show flash-usage
2%
```

メモリ消費量の表示

Guard モジュールは次の情報を表示します。

- メモリ使用量（KB 単位）。
- Guard モジュール統計エンジンが Anomaly Detection Engine Used Memory フィールドとして使用するメモリのパーセンテージ。

異常検出エンジンのメモリ使用量は、アクティブなゾーンの数および各ゾーンが監視するサービスの数に影響されます。

（注） 異常検出エンジンのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

Guard モジュールのメモリ消費量を表示するには、次のコマンドを使用します。

show memory

次の例は、Guard モジュールのメモリ消費量を表示する方法を示しています。

```
user@GUARD# show memory
              total    used    free    shared   buffers   cached
 In KBytes:  2065188  146260  1918928    0     2360      69232

 Anomaly detection engine used memory: 0.3%
```

（注） Guard モジュールの空きメモリの合計量は、空きメモリとキャッシュ メモリの合計です。

CPU 使用率の表示

Guard モジュールはユーザ モード、システム モード、ナイス値が負のタスク（負のナイス値を持つタスク、ナイス値はプロセスの優先順位を表す）、およびアイドル状態の CPU 時間のパーセンテージを表示します。ナイス値が負のタスクは、システム時間およびユーザ時間の両方でカウントされるため、CPU 使用率の合計が 100% を超えることがあります。

現在の CPU 使用率を表示するには、次のコマンドを使用します。

show cpu

次の例は、現在の CPU 使用率の表示方法を示しています。

```
user@GUARD# show cpu
Host CPU1: 0.0% user, 0.1% system, 0.1% nice, 98.0% idle
```

システム リソースの監視

グローバル モードまたは設定モードで次のコマンドを入力することで、Guard モジュールがシステム ステータスの分析および監視の支援に使用しているリソースの概要を表示できます。

show resources

次の例は、システム リソースを表示する方法を示しています。

```
user@GUARD# show resources
```

表 13-18 に、**show resources** コマンド出力のフィールドを示します。

表 13-18　show resources コマンドのフィールド説明

フィールド	説明
Host CPU1	ユーザ モード、システム モード、ナイス値が負のタスク（負のナイス値を持つタスクで、プロセスの優先順位を表す）、およびアイドル状態における CPU1 の CPU 時間のパーセンテージ。ナイス値が負のタスクは、システム時間およびユーザ時間にもカウントされるため、CPU 使用率の合計が 100% を超えることがあります。
Flash space usage	Guard モジュールが使用している、割り当て済みのフラッシュ スペースのパーセンテージ。 フラッシュ スペースの使用率がフラッシュの最大キャパシティの約 75% に達すると、Guard モジュールは syslog に警告メッセージを表示し、トラップを送信します。 **（注）** フラッシュ使用率がフラッシュの最大キャパシティの 80% に達すると、Guard モジュールは情報を消去して、フラッシュ使用率を約 75% に減らします。 Guard モジュールのレコードをネットワーク サーバに定期的に格納してから、古いレポートを削除することをお勧めします。

表 13-18　show resources コマンドのフィールド説明（続き）

フィールド	説明
Flash space usage（*続き*）	フラッシュ スペースの使用率が 80% に達した場合、ゾーン トラフィック レポートをネットワーク サーバにエクスポートし、古い攻撃レポートを削除できます（P.12-19 の「攻撃レポートのエクスポート」および P.12-24 の「攻撃レポートの削除」を参照）。
Accelerator card memory usage	アクセラレータ カードが使用しているメモリのパーセンテージ。 アクセラレータ カードのメモリ使用率が 85 パーセントを超えると、Guard モジュールは SNMP トラップを生成します。値が大きいときは、Guard モジュールが大量のトラフィックを監視している場合があります。
Accelerator card CPU utilization	アクセラレータ カードの CPU 使用率のパーセンテージ。 アクセラレータ カードの CPU の使用率が 85 パーセントを超えた場合、Guard モジュールは SNMP トラップを生成します。値が大きいときは、Guard モジュールが大量のトラフィックを監視している場合があります。
Anomaly detection engine used memory	Guard モジュール統計エンジンが使用するメモリのパーセンテージを指定。異常検出エンジンのメモリ使用率は、アクティブなゾーンの数、各ゾーンが監視するサービスの数、Guard モジュールが監視しているスプーフィングされていないトラフィックの合計に影響されます。 異常検出エンジンのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

表 13-18　show resources コマンドのフィールド説明（続き）

フィールド	説明
Dynamic filters used	すべてのゾーンでアクティブな動的フィルタの総数。Guard モジュールは、アクティブな動的フィルタの数と、Guard モジュールがサポートする動的フィルタの総数（150,000）に対するアクティブな動的フィルタのパーセンテージを表示します。アクティブな動的フィルタの数が 150,000 に到達すると、Guard モジュールは重大度 EMERGENCY の SNMP トラップを生成します。アクティブな動的フィルタの数が 135,000 に到達すると、Guard モジュールは、重大度 WARNING の SNMP トラップを生成します。 値が大きいときは、Guard モジュールが大量の DDoS 攻撃のトラフィックを監視していることを示します。

Guard モジュールが生成するトラップの詳細については、表 4-13 を参照してください。

ARP キャッシュの管理

ARP キャッシュを表示または操作して、アドレス マッピング エントリを消去または手動で定義できます。ARP キャッシュを管理するには、次のコマンドのいずれかを入力します。

arp [**-evn**] [**-H** *type*] [**-i** *if*] **-a** [*hostname*]

arp [**-v**] [**-i** *if*] **-d** *hostname* [**pub**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**netmask** *nm*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if*] **-Ds** *hostname ifa* [**netmask** *nm*] **pub**

arp [**-vnD**] [**-H** *type*] [**-i** *if*] **-f** [*filename*]

（注） キーワードを完全に入力することも、キーワードの省略形を入力することもできます。キーワードの省略形には、先頭にダッシュ（-）が付きます。完全なキーワードには先頭にダッシュが 2 つ（--）付きます。

表 13-19 に、**arp** コマンドの引数とキーワードを示します。

表 13-19　arp コマンドの引数とキーワード

パラメータ名の省略形	パラメータの完全な名前	説明
-H *type*, **-t** *type*	**--hw-type** *type*	（オプション）Guard モジュールがチェックするエントリのクラスを指定します。デフォルトのタイプ値は、ether（IEEE 802.3 10Mbps イーサネットに対応するハードウェア コード 0x01）です。
-i *If*	**--device** *If*	（オプション）インターフェイスを指定します。ARP キャッシュをダンプすると、指定したインターフェイスに一致するエントリだけが出力されます。永続的または一時的な ARP エントリを設定する場合、このインターフェイスがそのエントリに関連付けられます。このオプションを使用しない場合、Guard モジュールはルーティング テーブルに基づいてインターフェイスを決定します。**pub** キーワードを使用する場合、このインターフェイスは Guard モジュールが ARP 要求に応えるインターフェイスで、IP データグラムのルーティング先のインターフェイスとは異なる必要があります。
-s *hostname hw_addr*	**--set** *hostname hw_addr*	ハードウェア アドレスを *hw_addr* クラス値に設定して、hostname の ARP アドレス マッピング エントリを作成します。**temp** フラグを入力しなければ、エントリは ARP キャッシュ内に永続的に保存されます。
-a [*hostname*]	**--display** [*hostname*]	指定したホストのエントリを代替（BSD）形式で表示します。デフォルトでは、すべてのエントリが表示されます。
-v	**--verbose**	（オプション）出力を詳細に表示します。
-n	**--numeric**	数値アドレスを表示します。

表 13-19　arp コマンドの引数とキーワード（続き）

パラメータ名の省略形	パラメータの完全な名前	説明
-d *hostname*	**--delete** *hostname*	指定したホストのエントリを削除します。
-D	**--use-device**	インターフェイス if*a* のハードウェア アドレスを使用します。
-e		エントリをデフォルトの形式で表示します。
-f *filename*	**--file** *filename*	ARP アドレス マッピング エントリを作成します。情報は、*filename* ファイルから取得されます。ファイル形式は、ホスト名とハードウェア アドレスが空白で区切られた ASCII テキスト行です。pub、temp、および netmask フラグを使用することもできます。ホスト名を入力するどの場所にも、ドット区切り 10 進表記で IP アドレスを入力できます。

注意　Guard モジュールの ARP キャッシュを設定するには、Guard モジュールシステムとネットワークに精通している必要があります。

次の例は、デフォルトの形式で ARP エントリを表示する方法を示しています。

```
user@GUARD# arp -e

Address         HWtype  HWaddress           Flags Mask  Iface
10.10.1.254     ether   00:02:B3:C0:61:67   C           eth1
10.10.8.11      ether   00:02:B3:45:B9:F1   C           eth1
10.10.8.253     ether   00:D0:B7:46:72:37   C           eth1
10.10.10.54     ether   00:03:47:A6:44:CA   C           eth1
```

ネットワーク統計情報の表示

ホスト ネットワーク接続、ルーティング テーブル、インターフェイス統計情報、およびマルチキャスト メンバシップを表示してネットワークの問題をデバッグするには、次のいずれかのコマンドを入力します。

netstat [*address_family_options*] [**--tcp** | **-t**] [**--udp** | **-u**] [**--raw** | **-w**] [**--listening** | **-l**] [**--all** | **-a**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--symbolic** | **-N**] [**--extend** | **-e** [**--extend** | **-e**]] [**--timers** | **-o**] [**--program** | **-p**] [**--verbose** | **-v**] [**--continuous** | **-c**] [*delay*]

netstat {**--route** | **-r**} [*address_family_options*] [**--extend** | **-e** [**--extend** | **-e**]] [**--verbose** | **-v**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--interfaces** | **-i**} [*iface*] [**--all** | **-a**] [**--extend** | **-e** [**--extend** | **-e**]] [**--verbose** | **-v**] [**--program** | **-p**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--groups** | **-g**} [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--masquerade** | **-M**} [**--extend** | **-e**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--statistics** | **-s**} [**--tcp** | **-t**] [**--udp** | **-u**] [**--raw** | **-w**] [*delay*]

netstat {**--version** | **-V**}

netstat {**--help** | **-h**}

（注） アドレス ファミリを指定しない場合、Guard モジュールは設定されているすべてのアドレス ファミリのアクティブなソケットを表示します。

表 13-20 に、**netstat** コマンドの引数とキーワードを示します。

（注） キーワードを完全に入力することも、キーワードの省略形を入力することもできます。キーワードの省略形には、先頭にダッシュ（-）が付きます。完全なキーワードには先頭にダッシュが 2 つ（--）付きます。

表 13-20　netstat コマンドの引数とキーワード

パラメータ名の省略形	パラメータの完全な名前	説明
address_family_options		（オプション）アドレス ファミリ オプションは、次のいずれかです。 • [--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]] • [--unix|-x] [--inet|--ip] [--ax25] [--ipx] [--netrom] • [--ddp]
-r	**--route**	Guard モジュールのルーティング テーブルを表示します。
-g	**--groups**	IPv4 および IPv6 のマルチキャスト グループ メンバシップ情報を表示します。
-i *iface*	**--interface** *iface*	すべてのネットワーク インターフェイスまたはオプションの *iface* 値のテーブルを表示します。
-M	**--masquerade**	Network Address Translation（NAT; ネットワーク アドレス変換）が使用されたマスカレード接続のリストを表示します。
-s	**--statistics**	各プロトコルのサマリー統計情報を表示します。
-v	**--verbose**	（オプション）出力を詳細に表示します。
-n	**--numeric**	（オプション）数値アドレスを表示します。
	--numeric-hosts	（オプション）数値ホスト アドレスを表示しますが、ポートまたはユーザ名の解決には影響を与えません。
	--numeric-ports	（オプション）数値ポート番号を表示しますが、ホストまたはユーザ名の解決には影響を与えません。

表 13-20　netstat コマンドの引数とキーワード（続き）

パラメータ名の省略形	パラメータの完全な名前	説明
	--numeric-users	（オプション）数値ユーザ ID を表示しますが、ホストまたはポート名の解決には影響を与えません。
-c	**--continuous**	（オプション）選択した情報を 1 秒ごとに継続的に表示します。
-e	**--extend**	（オプション）追加情報を表示します。最も詳しい情報を表示するには、このオプションを 2 回使用します。
-o	**--timers**	（オプション）ネットワーキング タイマーに関連する情報を表示します。
-p	**--program**	（オプション）各ソケットが属するプログラムの PID および名前を表示します。
-l	**--listening**	（オプション）リスニング ソケットだけを表示します。デフォルトでは、これらのソケットは省略されます。
-a	**--all**	（オプション）リスニング ソケットおよび非リスニング ソケットの両方を表示します。
delay		（オプション）*delay* 秒ごとに、netstat が統計情報からの出力を繰り返します。

（注）　1 つのコマンドに最大 13 の引数とキーワードを入力できます。

次の例は、netstat 情報を詳細に表示する方法を示しています。

```
user@GUARD# netstat -v
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address         State
tcp        0      0 localhost:1111  localhost:32777    ESTABLISHED
tcp        0      0 localhost:8200  localhost:32772    ESTABLISHED
.
.
.
tcp        0      0 localhost:33464 localhost:8200     TIME_WAIT
tcp        1      0 localhost:1113  localhost:33194    CLOSE_WAIT
.
.
.
Active UNIX domain sockets (w/o servers)
unix  2      [ ]         STREAM     CONNECTED     928
unix  3      [ ]         STREAM     CONNECTED     890  /tmp/.zserv
.
.
.
user@GUARD#
```

traceroute の使用

次のコマンドを入力することで、ネットワーク問題をデバッグするために、パケットがネットワーク ホストに到達するまでに取るルートを決定できます。

traceroute *ip-address* [**-F**] [**-f** *first_ttl*] [**-g** *gateway*] [**-i** *iface*] [**-m** *max_ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] [*packetlen*]

（注） **traceroute** コマンドでは IP アドレスだけが表示され、名前は表示されません。

表 13-21 に、**traceroute** コマンドの引数とキーワードを示します。

表 13-21　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	ルートがトレースされる IP アドレス。
-F	（オプション）*don't fragment* ビットを設定します。
-f *first_ttl*	（オプション）最初の発信プローブ パケットで使用される最初の Time-To-Live（TTL; 存続可能時間）を設定します。
-g *gateway*	（オプション）ルース ソース ルート ゲートウェイを指定します（最大 8 個）。各ゲートウェイに対して -g を使用することで、2 つ以上のゲートウェイを指定できます。ゲートウェイの最大数は 8 個です。
-i *iface*	（オプション）発信プローブ パケットの送信元 IP アドレスを取得するネットワーク インターフェイスを指定します。これは通常、マルチホーム ホストで役立ちます。
-m *max_ttl*	（オプション）発信プローブ パケットで使用される最大存続可能時間（最大ホップ数）を設定します。デフォルトは 30 ホップです。
-p *port*	（オプション）プローブで使用されるベース UDP ポート番号を設定します。デフォルトは 33434 です。

表 13-21　traceroute コマンドの引数とキーワード（続き）

パラメータ	説明
-q *nqueries*	（オプション）ttl 値に対して定義されるプローブの数を設定します。デフォルトは 3 です。
-s *src_addr*	（オプション）IP アドレス *src_addr* を発信プローブ パケットで送信元 IP アドレスとして設定します。
-t *tos*	（オプション）プローブ パケットのタイプ オブ サービスを、*tos* の値に設定します。デフォルトはゼロです。
-w *waittime*	（オプション）プローブに対する応答を待つ時間（秒）を設定します。デフォルトは 5 秒です。
packetlen	（オプション）プローブ パケットの長さを設定します。

次の例は、IP アドレス 10.10.10.34 へのルートをトレースする方法を示しています。

```
user@GUARD# traceroute 10.10.10.34
traceroute to 10.10.10.34 (10.10.10.34), 30 hops max, 38 byte packets
 1 10.10.10.34 (10.10.10.34) 0.577 ms  0.203 ms  0.149 ms
```

接続の確認

次のコマンドを入力することにより、ネットワーク ホストに ICMP ECHO_REQUEST パケットを送信して、接続を確認できます。

ping *ip-address* [**-c** *count*] [**-i** *interval*] [**-l** *preload*] [**-s** *packetsize*] [**-t** *ttl*] [**-w** *deadline*] [**-F** *flowlabel*] [**-I** *interface*] [**-Q** *tos*] [**-T** *timestamp option*] [**-W** *timeout*]

表 13-22 に、**ping** コマンドの引数とキーワードを示します。

表 13-22　ping コマンドの引数とキーワード

パラメータ	説明
ip-address	宛先 IP アドレスを指定します。
-c *count*	（オプション）ECHO_REQUEST パケットを *count* 個送信します。deadline オプションが指定されている場合、このコマンドはタイムアウトになるまで *count* 個の ECHO_REPLY パケットを待ちます。
-i *interval*	（オプション）パケットの送信を待ちます。この間隔は秒で表されます。デフォルトでは、1 秒に設定されます。
-l *preload*	（オプション）応答を待たずに *preload* 個のパケットを送信します。
-s *packetsize*	（オプション）送信するデータ バイト数を指定します。デフォルトは 56 です。
-t ttl	（オプション）IP の TTL を設定します。
-w *deadline*	（オプション）送受信されたパケット数に関係なく ping が終了するまでのタイムアウト（秒）を指定します。
-F *flow label*	（オプション）各エコー要求パケットに 20 ビットのフローラベルを割り当てて設定します値がゼロの場合は、ランダムなフロー ラベルが使用されます。
-I *interface*	（オプション）送信元 IP アドレスを、指定したインターフェイス アドレスに設定します。
-Q *tos*	（オプション）ICMP データグラムに Type of Service（ToS; タイプ オブ サービス）関連のビットを設定します。

表 13-22　ping コマンドの引数とキーワード（続き）

パラメータ	説明
-T *timestamp option*	（オプション）特別な IP タイムスタンプ オプションを設定します。
-W *timeout*	（オプション）応答を待つ時間（秒）。

1 つのコマンドに最大 10 の引数とキーワードを入力できます。

次の例は、1 つの ICMP ECHO_REQUEST パケットを IP アドレス 10.10.10.30 に送信する方法を示しています。

```
user@GUARD# ping 10.10.10.30 -n 1
```

デバッグ情報の取得

Guard モジュールに動作上の問題が発生した場合は、シスコのテクニカルサポートがお客様に Guard モジュールの内部デバッグ情報のコピーを送信するようお願いすることがあります。Guard モジュールのデバッグ コア ファイルには、Guard モジュールの誤動作についてトラブルシューティングを行うための情報が含まれています。このファイルの出力は暗号化されており、Cisco TAC の担当者のみが使用するよう意図されています。

デバッグ情報を FTP サーバに抽出するには、次の手順を実行します。

ステップ 1　Guard モジュール ログ ファイルを表示します。

詳細については、P.13-12 の「ログ ファイルの表示」を参照してください。

ステップ 2　デバッグ情報を抽出する時期を判断するため、問題を示す最初のログ　メッセージを識別します。Guard モジュールは、指定した時間から現在の時間までのデバッグ情報を抽出します。

ステップ 3　グローバル モードで次のコマンドを入力して、FTP サーバにデバッグ情報を抽出します。

```
copy debug-core time ftp server full-file-name [login [password]]
```

表 13-23 に、**copy debug-core** コマンドの引数とキーワードを示します。

表 13-23　copy debug-core コマンドの引数とキーワード

パラメータ	説明
time	デバッグ情報が必要となった原因のイベントの時刻。時刻の文字列では、*MMDDhhmm*[[*CC*]*YY*][*.ss*] という形式を使用します。 • *MM*：月（数値）。 • *DD*：日。 • *hh*：時（24 時間表記）。 • *mm*：分。 • *CC*：（オプション）年の最初の 2 桁（たとえば **20**05）。 • *YY*：（オプション）年の最後の 2 桁（たとえば 20**05**）。 • *.ss*：（オプション）秒（小数点が必要）。
ftp *server*	FTP サーバの IP アドレス。
full-file-name	バージョン 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）FTP サーバのログイン名。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）FTP サーバのパスワード。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。

次の例は、今年の 11 月 9 日 午前 6:45 のデバッグ情報を FTP サーバ 10.0.0.191 に抽出する方法を示しています。

```
user@GUARD# copy debug-core 11090645 ftp 10.0.0.191
/home/debug/debug-file <user> <password>
```

Guard モジュールの自己保護設定の表示

独立した IP アドレスを持つネットワーク要素としての Guard モジュールは、潜在的な DDoS 攻撃の危険にさらされています。Guard モジュールのデフォルトの設定では、このような攻撃に対する保護が提供されます。ユーザは、この自己防衛保護設定にアクセスし、変更することができます。

注意　Guard　モジュールの自己防衛保護のデフォルト設定は変更しないことを強くお勧めします。不要な設定を行うと、Guard モジュールの自己保護機能に大きな支障をきたす場合があります。

Guard モジュールの自己防衛保護設定を変更するには、自己保護設定モードに入る必要があります。

自己保護設定モードに入るには、設定モードで次のコマンドを使用します。

self-protection

Guard モジュールの自己防衛保護に使用できるコマンドのセットは、通常のゾーンで使用するコマンドと同じです。ゾーンの設定の詳細については、第 6 章「ゾーンの設定」、第 7 章「ゾーンのフィルタの設定」、第 8 章「ポリシー テンプレートとポリシーの設定」、および 第 11 章「インタラクティブ保護モードの使用方法」を参照してください。

Guard モジュールの自己保護設定ファイルを表示するには、**show running-config** コマンドを使用します。詳細については、P.13-2 の「Guard モジュールの設定の表示」を参照してください。

フレックスコンテンツ フィルタのデフォルト設定

デフォルトで Guard モジュール flex-content filter が設定されていると、明示的に指定されない限り、すべてのトラフィック フローをブロック（ドロップ）します。

表 13-24 に、Guard モジュールが適切に機能するために必要な通信を可能にするためのフレックスコンテンツ フィルタのデフォルト設定を示します。

表 13-24　フレックスコンテンツ フィルタのデフォルト設定

サービス	IP プロトコル	送信元ポート	宛先ポート	同期の許可
ftp-control	6	21	*	no
ftp-data	6	20	*	yes
tacacs	6	49	*	yes
ssh	6	22	*	no
ssh	6	*	22	yes
https	6	*	443	yes
icmp	1	*	*	—
snmp	17	*	161	—
ssl	6	*	3220	no
ssl	6	3220	*	yes

フレックスコンテンツ フィルタのデフォルト設定は、次の内容で構成されます。

- Guard モジュールによって開始される FTP サーバとの FTP 通信をイネーブル化し、送信元ポート 21 で着信 FTP 制御 SYN パケットをブロックする。
- 認証、認可、アカウンティングのために TACACS+ サーバとの TACACS 通信をイネーブルにし、送信元ポート 49 からの着信 SYN パケットをブロックする。
- 着信および発信 SSH 通信をイネーブルにする。
- 着信 HTTPS 通信をイネーブルにする。
- ICMP 通信をイネーブルにする。
- SNMP 通信をイネーブルにする。
- SSL 通信をイネーブルにする。