CHAPTER 12

Detector モジュールの診断ツールの使用

この章では、Cisco Traffic Anomaly Detector モジュール（Detector モジュール）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。

（注） 1 Gbps 動作の Detector モジュールと 2 Gbps 動作の Detector モジュールの間には、動作および設定上の違いがあります。この章では、1 Gbps 動作と 2 Gbps 動作の違いについて説明します。特に記載がない限り、この章の情報は、両方の動作モードに適用されます。詳細については、P.1-9 の「1 Gbps および 2 Gbps 帯域幅オプションについて」を参照してください。

この章は、次の項で構成されています。

インストールされているソフトウェア バージョン番号とライセンス契約の表示

ソフトウェア ライセンス契約と、Detector モジュールにロードされているソフトウェア イメージのバージョン番号を表示できます。バージョン番号を表示することにより、Detector モジュールが次のどちらの帯域幅オプションを使用しているか確認できます。

- 1 Gbps 動作 : Detector モジュールとスーパーバイザ エンジン間のトラフィックの最大帯域幅は 1 Gbps で、すべてのデータ トラフィックが、1 つのインターフェイス ポートだけを介して移動します。
- 2 Gbps 動作 : Detector モジュールとスーパーバイザ エンジン間のトラフィックの最大帯域幅は 2 Gbps で、すべてのデータ トラフィックが、2 つのインターフェイス ポートを介して移動します。インストールされているソフトウェア イメージが 2 Gbps 動作を許可している場合には、バージョン番号に XG 指定子が含まれます（Cisco Anomaly Detector モジュール Image version 6.0（0.39）-XG など）。

（注）　2 Gbps 動作の場合に Detector モジュールを動作させるには、関連付けられているソフトウェア ライセンス キーをインストールする必要があります（P.12-2 の「ソフトウェア ライセンス キー情報の表示」を参照）。

ソフトウェア バージョン番号とライセンス契約情報を表示するには、次のコマンドを使用します。

show version

ソフトウェア ライセンス キー情報の表示

Detector モジュールが 2 Gbps 動作のためにソフトウェア イメージの XG バージョンを使用している場合には、XG ソフトウェア イメージをアクティブにするために必要なライセンス キーの関連情報を表示できます。ライセンス キー情報を表示して、次の情報を確認します。

- ライセンス キーがロードされていること。
- ライセンス キーの期限が切れていないこと。ライセンス キーがデモ バージョンの場合には、デモ ライセンス キーの失効日が表示されます。インストールされているライセンス キーが永続的である場合には、失効日として permanent の文字が表示されます。

（注）　1 Gbps 動作のソフトウェア イメージについては、ライセンス キーは不要です。Detector モジュールに現在ロードされているソフトウェア イメージを確認するには、**show version** コマンドを使用します（P.12-2 の「インストールされているソフトウェア バージョン番号とライセンス契約の表示」を参照）。

ソフトウェア バージョン番号とライセンス契約情報を表示するには、次のコマンドを使用します。

show license-key

Detector モジュールの設定の表示

Detector 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、Detector モジュールの設定に関する情報が含まれています。

Detector 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** | **detector** | **interfaces** [*interface-name*] | **zones**]

表 12-1 に、**show running-config** コマンドの引数とキーワードを示します。

表 12-1　show running-config コマンドの引数とキーワード

パラメータ	説明
all	（オプション）Detector モジュールのすべての機能（Detector モジュール、ゾーン、およびインターフェイス）の設定ファイルを表示します。
detector	（オプション）Detector モジュールの設定ファイルを表示します。
interfaces	Detector モジュールのインターフェイスの設定ファイルを指定します。
interface-name	（オプション）特定のインターフェイスの名前。 1 Gbps 動作の場合に有効な名前は次のとおりです。 • mng • giga 2 2 Gbps 動作の場合に有効な名前は次のとおりです。 • mng • giga 1 • giga 2
zones	（オプション）すべてのゾーンの設定ファイルを表示します。

次の例は、Detector 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@DETECTOR# show running-config detector
```

設定ファイルは、Detector 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。Detector 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 Detector モジュールにその Detector 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.12-4 の「Detector モジュール ゾーンの動作ステータスの表示」を参照してください。

Detector モジュール ゾーンの動作ステータスの表示

グローバル モードで次の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。

show

表 12-2 に、ゾーンの可能な動作状態を示します。

表 12-2　ゾーンのステータス

ステータス	説明
Auto detect mode	ゾーン異常検出がイネーブルで、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。 Detector モジュールで、ゾーン異常検出がイネーブルで、Detector 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 detect mode	ゾーンはインタラクティブ検出モードです。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。Detector モジュールは、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、Detector 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@DETECTOR# show
```

カウンタを使用したトラフィックの分析

Detector モジュールおよびゾーン カウンタを表示することで、Detector 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 :** 受信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**：受信カウンタの平均トラフィック レートを表示します。**zone** キーワードを使用しないでグローバル モードまたは設定モードからこのコマンドを実行すると、無効なゾーンの平均トラフィック レートも表示されます。
- **show** [**zone** *zone-name*] **rates history**：過去 24 時間における 1 分ごとの受信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**：受信カウンタを表示します。
- **show** [**zone** *zone-name*] **counters details**：受信カウンタを表示します。**zone** キーワードを使用しないでグローバル モードまたは設定モードからこのコマンドを実行すると、無効なゾーンの受信トラフィック レートも表示されます。
- **show** [**zone** *zone-name*] **counters history**：過去 1 時間の受信カウンタの値を 1 分ごとに表示します。

Detector 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：このコマンドは、現在のゾーン設定モードに関連する情報だけを表示するため、**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、ゾーン異常検出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、ゾーン検出をアクティブにしたときにゼロにリセットされます。

表 12-3 に、Detector モジュールのカウンタを示します。

表 12-3　Detector モジュール カウンタ

カウンタ	説明
Received	Detector モジュールが処理した、そのゾーンを宛先としたパケットの合計。
Invalid zone	異常検出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、Detector 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、Detector 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。

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

Detector 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、Detector モジュールまたはゾーン カウンタをクリアできます。Detector 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。

Detector 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、Detector 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@DETECTOR-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**：ゾーン設定モードでこのコマンドを使用します。
- **clear zone** *zone-name* **counters**：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。*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@DETECTOR-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次のコマンドを使用します。

show

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：検出モード（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.5-8 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 フィルタ：フレックスコンテンツ 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示します。ゾーンがインタラクティブ検出モードの場合、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.6-3 の「フレックスコンテンツ フィルタの設定」および P.6-15 の「動的フィルタの設定」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.12-5 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@DETECTOR-conf-zone-scannet# show
```

Detector モジュールのログ管理

Detector 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。Detector モジュールのログを表示して、Detector 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 12-4 に、イベント ログのレベルを示します。

表 12-4　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。Detector 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。

- ロギング パラメータの設定
- オンライン イベント ログの管理
- ログ ファイルの管理

ロギング パラメータの設定

Detector モジュールのログ ファイルの動作を制御するには、ロギング パラメータを設定します。

ロギング パラメータを設定するには、設定モードで次のコマンドを使用します。

logging {**device-log size** *logging-size-init* | **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**} | **host** *remote-syslog-server-ip* | **trap** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} | **zone-log size** *logging-size-init*}

表 12-5 に、**logging** コマンドの引数とキーワードを示します。

表 12-5　logging コマンドの引数とキーワード

パラメータ	説明
device-log size *logging-size-init*	Detector モジュールのすべてのログ ファイル用に割り当てるスペースを指定します。スペースの最大容量は 50 MB で、これがデフォルトの設定です。
facility	エクスポート syslog ファシリティを指定します。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、Detector 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使用できます。 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。
host *remote-syslog-server-ip*	ログ ファイルのエクスポート時に使用するリモート syslog サーバの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します（たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0）。詳細については、「ログ ファイルのネットワーク サーバへのコピー」を参照してください。
trap	リモート syslog に送信する syslog トラップの重大度を指定します。低い重大度を指定した場合、それ以上の重大度がイベント ログに含まれます。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、重大度が高い方から順に次のようになります。 • **emergencies** • **alerts** • **critical** • **errors** • **warnings** • **notification** • **informational** • **debugging** デフォルトは **notification** です。詳細については、表 12-4 を参照してください。 **（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** に設定してください。
zone-log size *logging-size-init*	ゾーンのすべてのログ ファイル用に割り当てるスペースを指定します。スペースの最大容量は 10 MB で、これがデフォルトの設定です。

ロギング パラメータの現在の設定を表示するには、グローバル モードまたは設定モードで、次のいずれかのコマンドを使用します。

- **show logging**
- **show running-config**

次の例は、ゾーンのログ用に 6 MB のスペースを割り当てる方法を示しています。

```
user@DETECTOR-conf# logging zone-log size 6
```

オンライン イベント ログの管理

この項では、Detector 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

Detector 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、Detector 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@DETECTOR# 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

Detector 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 Detector モジュールの動作を表示できます。また、Detector モジュールのログ ファイルに登録されている Detector 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。Detector 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。Detector 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。

Detector 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、Detector 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 ログ メッセージの構文は、次のとおりです。

event-date event-time Detector-IP-address detection-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}
```

詳細については、「ロギング パラメータの設定」の項を参照してください。

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*

詳細については、「ロギング パラメータの設定」の項を参照してください。

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 Detector モジュールを設定する方法を示しています。Detector 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@DETECTOR-conf# logging facility local3
user@DETECTOR-conf# logging trap notifications
user@DETECTOR-conf# logging host 10.0.0.191
```

Detector 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、Detector 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 ファイルのネットワーク サーバへのコピー
- 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 Detector モジュールのログを表示できます。Detector 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。

Detector 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、Detector モジュールのログを表示する方法を示しています。

```
user@DETECTOR# 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、ゾーン設定モードで **show log** コマンドを使用します。

ログ ファイルのネットワーク サーバへのコピー

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、Detector 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*

表 12-6 に、**copy log ftp** コマンドの引数とキーワードを示します。

表 12-6　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）ゾーン名を指定します。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、Detector 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。
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
server	ネットワーク サーバの IP アドレス、パス、およびファイル名。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）。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。*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。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

（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 Detector モジュールを設定できます。詳細については、P.12-10 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。

Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）および Secure Copy Protocol（SCP）はセキュアな通信を Secure Shell（SSH; セキュア シェル）に依存しているので、**sftp** 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、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector 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.4-27 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。

次の例は、Detector 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@DETECTOR# copy log ftp 10.0.0.191 log.txt <user> <password>
```

ログ ファイルのクリア

Detector 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。

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、ゾーン設定モードで次のコマンドを使用します。

clear log

Detector 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、設定モードで次のコマンドを使用します。

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

省略可能な **zone** *zone-name* のキーワードおよび引数でゾーン名を指定します。デフォルトでは、Detector モジュールのログ ファイルがクリアされます。

次の例は、Detector モジュール ログをクリアする方法を示しています。

```
user@DETECTOR-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 Detector 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 Detector 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 Detector 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、Detector 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。

Detector モジュールは、トラフィックを gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式で記録し、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。

Detector モジュールは記録されたトラフィックを分析して、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します。Detector モジュールは、記録されたトラフィックからシグニチャを抽出できます。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。

Detector モジュールでは、次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。

  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。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、それらをネットワーク サーバにエクスポートする必要があります。
- 手動：ユーザが Detector モジュールをアクティブにしてトラフィックを記録している場合、トラフィックはパケットダンプ 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、Detector 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。手動の場合、Detector モジュールは最大 4 つのゾーンのトラフィックを同時に記録できます。

デフォルトでは、Detector 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。Detector モジュールは、すべてのゾーンで最大 80 MB のディスク スペースまで、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。

- 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

Detector モジュールによるトラフィックの自動記録の設定

Detector モジュールが自動的にネットワーク トラフィックを記録する機能をアクティブにして、ネットワーク問題のトラブルシューティングや攻撃トラフィックの分析を行うことができます。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 Detector 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。

Detector 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 20 MB に到達するか、または 10 分が経過すると、Detector モジュールはバッファされた情報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。

Detector モジュールでは、パケットダンプ キャプチャ ファイル中に IP サマライズが出力されます。IP サマライズとは、（トラフィックの量に応じて）最も頻繁に検出される送信元 IP アドレスのサマリーです。

Detector モジュールでは自動パケットダンプ キャプチャ ファイルに命名規則が適用され、Detector モジュールでトラフィックが記録された日時やトラフィックの処理方法に関する情報が与えられます。表 12-7 に、自動パケットダンプ キャプチャ ファイル名のセクションを示します。

表 12-7　自動パケットダンプ キャプチャ ファイル名のセクション

セクション	説明
機能およびゾーン名	パケットダンプ キャプチャの際に Detector モジュールで実行されていたゾーン機能とそのゾーン名。ゾーン機能は次のとおりです。 • **detect**：Detector モジュールはゾーン異常検出中にトラフィックを記録。 • **learn**：Detector モジュールはゾーンのラーニング プロセス中または検出およびラーニング プロセス中にトラフィックを記録。
キャプチャ開始時刻	Detector 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）Detector モジュールでトラフィックの記録が終了した時刻。現在 Detector モジュールがファイルにトラフィックを記録している場合、終了時刻は表示されません。
処理	Detector モジュールがトラフィックの処理に使用する方式。Detector モジュールは受信したすべてのトラフィックをドロップするため、サポートするのは **dropped** メソッドだけです。

Detector モジュールは、ラーニング プロセスから取得した 1 つのパケットダンプ キャプチャ ファイル、およびゾーン保護がイネーブルの場合は、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。

- 直前の 10 分間のトラフィック
- 現在のトラフィック

ゾーン検出をアクティブにするか、Detector 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、検出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。

ネットワーク トラフィックを自動的に記録するように Detector 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 Detector 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.12-18 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 Detector モジュールを設定する方法を示しています。

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

Detector モジュールでゾーンのトラフィック 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。

Detector モジュールによるトラフィックの手動記録のアクティブ化

トラフィックの記録を開始するように Detector 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、Detector 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。

指定した数のパケットが記録された時点、またはラーニング プロセスかゾーン検出のどちらかが終了した時点で、Detector モジュールは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。

Detector モジュールでは、パケットダンプ キャプチャ ファイル中に IP サマライズが出力されます。IP サマライズとは、（トラフィックの量に応じて）最も頻繁に検出される送信元 IP アドレスのサマリーです。

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。Detector モジュールは、最大 10 個のゾーンの手動パケットダンプ キャプチャを同時に記録できます。

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* [*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。キャプチャの進行中に作業を続行するには、Detector モジュールとのセッションを追加で確立してください。

表 12-8 に、**packet-dump** コマンドの引数とキーワードを示します。

表 12-8　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）Detector 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（パケット / 秒）。1 ～ 10000 の値を入力します。 （注）　Detector 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。
pdump-count	記録対象のパケットの数。Detector 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。
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。Detector 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.6-6 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@DETECTOR-conf-zone-scannet# packet-dump capture view 10 1000
```

Detector モジュールによるトラフィックの手動記録の停止

Detector 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。ただし、指定した数のパケットが記録される前でも、次のいずれかの操作を実行すると、手動パケットダンプ キャプチャを停止できます。

- 開いている 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、希望の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。

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

手動パケットダンプ設定の表示

Detector モジュールが手動パケットダンプ キャプチャ ファイル用に割り当てたディスク 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。Detector 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、Detector 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@DETECTOR-conf# show packet-dump
```

表 12-9 に、**show packet-dump** コマンド出力のフィールドを示します。

表 12-9　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（MB）。
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 ファイルによって使用されたパーセンテージ。

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、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 Detector 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、Detector 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。Detector モジュールは、gzip（GNU zip）プログラムで圧縮および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 スキーマは、http://www.cisco.com/public/sw-center/ のソフトウェア センターからダウンロードできる Capture.xsd ファイルに記述されています。

Detector 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、Detector 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.13-7 の「ファイルのネットワーク サーバへの自動エクスポート」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@DETECTOR-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 ファイルを手動でエクスポートできます。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。Detector モジュールは、gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートし、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。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。

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*

表 12-10 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 12-10　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-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、Detector モジュールはゾーンのすべてのパケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.12-21 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。
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
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	Detector 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	（オプション）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。パスワードを入力しない場合、Detector 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、Detector 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.13-7 の「ファイルのネットワーク サーバへの自動エクスポート」を参照してください。

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** 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、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector 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.4-27 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。

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@DETECTOR# 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@DETECTOR# 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 Detector 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 Detector 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。Detector モジュールは、パケットダンプ キャプチャ ファイルを XML 形式と PCAP 形式の両方でインポートします。

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*

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

表 12-11　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	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
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を指定します。
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	（オプション）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）FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

表 12-11　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、Detector 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.13-7 の「ファイルのネットワーク サーバへの自動エクスポート」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。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。

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** 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、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector 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.4-27 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。

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@DETECTOR# 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@DETECTOR# 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、Detector 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 12-12 に、**show packet-dump captures** コマンドの引数を示します。

表 12-12　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、Detector 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 12-13 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た場合、Detector モジュールはそのファイルを TCPDump 形式で表示します。
tcpdump-expression	（オプション）Detector 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。Detector モジュールは、パケットダンプ キャプチャ ファイルのうち、フィルタの基準に一致する部分だけを表示します。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（P.6-6 の「tcpdump 式の構文の設定」を参照）。

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@DETECTOR-conf-zone-scannet# show packet-dump captures
```

表 12-13 に、**show packet-dump captures** コマンド出力のフィールドを示します。

表 12-13　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 12-7 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。単位はメガバイト。
Filter	Detector 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.6-6 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。Detector モジュールをアクティブにして攻撃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、（アンチウィルス ソフトウェアのメーカーやメーリング リストなどで）シグニチャが公開される前であっても、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 ワームを検出できます。

Detector 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、攻撃シグニチャを生成できます。攻撃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、攻撃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.6-3 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。

攻撃シグニチャの生成プロセスを実行する際、クリーンな（正当な）トラフィックが含まれる参照用のパケットダンプ キャプチャ ファイルを指定することによって、生成される攻撃シグニチャの正確性を判定できます。Detector で悪意のあるトラフィックが含まれるパケットダンプ キャプチャ ファイルから攻撃シグニチャが生成されると、Detector により分析が実行され、攻撃シグニチャが参照用のパケットダンプ キャプチャ ファイルのクリーンなトラフィックに現れる頻度が判定され

ます。分析の結果は、参照用のパケットダンプ キャプチャ ファイルにおける、パケット数に対して攻撃シグニチャの出現数が占める割合として表示されます。割合の値が 10% 未満の場合、攻撃シグニチャは正確なので、このシグニチャを悪意のあるトラフィックの検出に使用できます。

割合の値が 10% を超える場合、シグニチャの生成プロセスは失敗したことになります。このシグニチャを悪意のあるトラフィックの検出に使用しないでください。Detector でクリーンなトラフィックが悪意のあるトラフィックとして誤認される結果になります。シグニチャの生成プロセスが失敗する原因として、次のようなことが考えられます。

- 悪意のあるトラフィックが含まれるパケットダンプ キャプチャ ファイルに、有効なトラフィックも含まれている。シグニチャの生成プロセスの間は、悪意のあるトラフィックだけが含まれるパケットダンプ キャプチャ ファイルを使用してください。
- Detector のシグニチャの生成アルゴリズムでは、悪意のあるトラフィックのサンプルから固有のシグニチャを検出できない。

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、Detector 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.12-16 の「Detector モジュールによるトラフィックの手動記録のアクティブ化」を参照してください。

ステップ 2　攻撃進行中に Detector モジュールが記録したパケットダンプ キャプチャ ファイルを確認します。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.12-21 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　Detector　モジュールで攻撃トラフィックのシグニチャの生成をアクティブにします。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 12-14 に、**show packet-dump signatures** コマンドの引数を示します。

表 12-14　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 Detector モジュールが記録した既存のパケットダンプ キャプチャ ファイルの名前。Detector モジュールにより、分析が実行され、攻撃シグニチャが参照用のファイルに現れる頻度が判定されます。

表 12-15 に、**show packet-dump signatures** コマンド出力のフィールドを示します。

表 12-15　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	Detector モジュールが生成したシグニチャ。Detector 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.6-9 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	参照用のパケットダンプ キャプチャ ファイルにおける、パケット数に対して攻撃シグニチャの出現数が占める割合。

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@DETECTOR-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。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、Detector 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。既存の自動パケットダンプ キャプチャ ファイルを保存したい場合は、Detector モジュールによって新しいファイルで上書きされる前に、コピーを作成しておく必要があります。

ディスク スペースを解放する必要がある場合は、パケットダンプ キャプチャ ファイルを手動で削除します。詳細については、P.12-25 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 12-16 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 12-16　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-name	既存のゾーンの名前。
capture-name	既存のパケットダンプ キャプチャ ファイルの名前。

表 12-16　copy zone packet-dump captures コマンドの引数とキーワード（続き）

パラメータ	説明
tcpdump-expression	（オプション）Detector 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。Detector モジュールは、パケットダンプ キャプチャ ファイルのうち、フィルタの基準に一致する部分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.6-6 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@DETECTOR-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、Detector 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、Detector 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 12-17 に、**clear packet-dump** コマンドの引数とキーワードを示します。

表 12-17　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を指定します。
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@DETECTOR-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：Detector モジュールの識別子文字列。
- Number of Pentium-class Processors：Detector モジュールのプロセッサの番号。Detector モジュールはプロセッサ 1 をサポートします。
- BIOS Vendor：Detector モジュール上の BIOS のベンダー。
- BIOS Version：Detector モジュール上の BIOS バージョン。
- Total available memory：Detector モジュール上で使用可能なメモリの合計。
- Size of compact flash：Detector モジュール上のコンパクト フラッシュのサイズ。
- Slot Num：モジュールをシャーシに挿入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.13-18 の「CFE をアップグレードするため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、Detector 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。負荷分散型の構成で複数の Detector モジュールを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

Detector 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 Detector 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、Detector モジュールは syslog に警告メッセージを表示します。

Detector モジュールが警告メッセージを表示する場合は、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てから、古い攻撃レポートを削除できます（P.11-8 の「攻撃レポートのエクスポート」および P.11-11 の「攻撃レポートの削除」を参照）。

Detector 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、Detector モジュールは情報の 5% を自動的に消去して、ディスク使用率を約 75% に減らします。

グローバル モードで次のコマンドを入力すると、Detector モジュールにインストールされているフラッシュ メモリの合計に対する使用可能なフラッシュ メモリの割合を表示できます。

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@DETECTOR# show flash-usage
2%
```

メモリ消費量の表示

Detector 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）。
- Detector 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。

Detector 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、Detector 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@DETECTOR# show memory
              total    used    free    shared   buffers   cached
    In KBytes:  2065188  146260  1918928    0     2360      69232

    Anomaly detection engine used memory: 0.3%
```

（注）　Detector 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

Detector 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@DETECTOR# 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、Detector 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@DETECTOR# show resources
```

表 12-18 に、**show resources** コマンド出力のフィールドを示します。

表 12-18　show resources コマンド出力のフィールドの説明

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	Detector 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、Detector 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、Detector モジュールは情報を自動的に消去して、フラッシュ使用率を約 75% に減らします。 Detector 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、古いレコードを削除することをお勧めします。 フラッシュ スペースの使用率が 80% に達した場合は、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てから、古い攻撃レポートを削除することができます（P.11-8 の「攻撃レポートのエクスポート」および P.11-11 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ポート当たりのメモリのパーセンテージ：1 Gbps 動作の場合は 1 ポート、2 Gbps 動作の場合は 2 ポート。 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、Detector 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、Detector 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 CPU 使用量のポート当たりのパーセンテージ：1 Gbps 動作の場合は 1 ポート、2 Gbps 動作の場合は 2 ポート。 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、Detector 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、Detector 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。

表 12-18　show resources コマンド出力のフィールドの説明（続き）

フィールド	説明
Anomaly detection engine used memory	Detector 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、Detector 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。
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。Detector モジュールは、アクティブな動的フィルタの数と、Detector 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、Detector 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、Detector 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、Detector 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。

Detector モジュールが生成するトラップの詳細については、P.4-30 の表 4-14 を参照してください。

ARP キャッシュの管理

Address Resolution Protocol（ARP; アドレス解決プロトコル）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、設定モードで次のコマンドを使用します。

arp {**-a** [*arp_hostname*] | **-d** *arp_hostname* | **-n** [*arp_hostname*] | **-s** *arp_hostname hw_addr*}

表 12-19 に、**arp** コマンドの引数とキーワードを示します。

表 12-19　arp コマンドの引数とキーワード

キーワード	説明
-a *arp_hostname*	ホストのエントリを代替（BSD）形式で表示します。オプションのホスト名を入力すると、指定したホストのエントリだけが表示されます。この **arp** コマンド オプションをグローバル コンフィギュレーション モードで実行することもできます。
-d *hostname*	指定したホストのエントリを削除します。
-n *arp_hostname*	ホストの数値アドレスを表示します。オプションのホスト名を入力すると、指定したホストの数値アドレスだけが表示されます。この **arp** コマンド オプションをグローバル コンフィギュレーション モードで実行することもできます。
-s *arp_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。

注意　Detector モジュールの ARP キャッシュを設定するには、Detector 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。

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-users**] [**--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-users**] [**--continuous** | **-c**] [*delay*]

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

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

netstat {**--masquerade** | **-M**} [**--extend** | **-e**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--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、Detector 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 12-20 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 12-20　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**	Detector 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。

表 12-20　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
-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。
	--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@DETECTOR# 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@DETECTOR#
```

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 12-21 に、**traceroute** コマンドの引数とキーワードを示します。

表 12-21　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。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。
-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@DETECTOR# 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 12-22 に、**ping** コマンドの引数とキーワードを示します。

表 12-22　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。
-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）インターネット制御メッセージ プロトコル（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。
-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@DETECTOR# ping 10.10.10.30 -n 1
```

デバッグ情報の取得

Detector モジュールに動作上の問題が発生した場合は、Cisco TAC がお客様に Detector 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。Detector モジュールのデバッグ コア ファイルには、Detector モジュールの動作不良をトラブルシューティングする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、SCP、または SFTP 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　Detector 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.12-11 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。Detector 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、SCP、または SFTP サーバにデバッグ情報をコピーします。

```
copy debug-core time {ftp | scp | sftp} server full-file-name [login [password]]
```

表 12-23 に、**copy debug-core** コマンドの引数とキーワードを示します。

表 12-23　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、次のように、*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	FTP を指定します。
scp	SCP を指定します。
sftp	SFTP を指定します。
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）。
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）サーバのログイン名。ログイン名を入力しない場合、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）サーバ パスワード。パスワードを入力しない場合、Detector 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@DETECTOR# copy debug-core 11090645 ftp 10.0.0.191 /home/debug/debug-file <user>
<password>
```