CHAPTER 10

Detector モジュール診断ツールの使用

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）に関する統計情報および診断を表示する方法について説明します。この章には、次の項があります。

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することができます。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、設定されているゾーンなど、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、次のコマンドを入力します。

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

表 10-1 に、**show running-config** コマンドのキーワードを示します。

表 10-1　show running-config コマンドのキーワード

パラメータ	説明
all	Detector モジュールのすべてのモジュール（Detector 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。
Detector module	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表示します。インターフェイス名を入力します。
zones	すべてのゾーンの設定ファイルを表示します。

次の例を参考にしてください。

```
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実行され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.10-3 の「Detector モジュールのゾーンの表示」を参照してください。

Detector モジュールのゾーンの表示

Detector で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。ゾーンのリストを表示するには、グローバル モードで **show** コマンドを使用します。表 10-2 で、さまざまなゾーン ステータスについて説明します。

表 10-2　ゾーンのステータス

ステータス	説明
Auto detect mode	ゾーンは自動検出モードです。ユーザの介入なしに動的フィルタがアクティブになります。 ゾーンが自動検出モードであるときに、Detector モジュールがポリシーのしきい値を調整する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、Detector モジュールはゾーン名の隣に (+learning) を表示します。
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されます。
Threshold Tuning phase	ゾーンはしきい値調整フェーズです。Detector は、ゾーンのトラフィックを分析して、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。

例

```
user@DETECTOR# show
```

ゾーンのカウンタの表示

ゾーン カウンタの表示およびゾーン トラフィックの分析には、次のコマンドを使用できます。

- **show rates :** Received カウンタの平均トラフィック レートを表示します。
- **show rates details :** Received カウンタの平均トラフィック レートを表示します。
- **show rates history :** Received カウンタの平均トラフィック レートを過去 24 時間にわたり 1 分ごとに表示します。
- **show counters** : Received カウンタを表示します。
- **show counters details** : Received カウンタを表示します。
- **show counters history** : 過去の Received カウンタの値を 1 分ごとに表示します。

レート単位は、bps および pps です。

（注）　ゾーンのレートは、ゾーン検出をイネーブルにした場合、またはラーニング プロセスをアクティブにした場合にのみ使用可能です。

Guard は、トラフィックの合計を測定し、平均のトラフィック レートを計算します。値が **cleared** のレートは、ゾーン検出がイネーブルでなかった時間を示します。

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 10-3 に、Detector モジュールのカウンタを示します。

表 10-3　Detector モジュールのカウンタ

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。

次の例を参考にしてください。

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

ゾーンのステータスの表示

特定のゾーンの概要を表示して、そのゾーンの全般的な状況と現在のステータスを知ることができます。ゾーンの概要を表示するには、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**：動作モード（自動またはインタラクティブ）、しきい値とタイマー、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.5-9 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　フィルタの設定も含めて、アクティブな動的フィルタおよびユーザ フィルタの設定数を示します。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.6-6 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。
- **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.10-4 の「ゾーンのカウンタの表示」を参照してください。

次の例を参考にしてください。

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

Detector モジュールのログの表示

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 10-4 に、イベント ログのレベルを示します。

表 10-4　イベント ログのレベル

イベントのレベル	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	危険な状態
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、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。

- イベントのリアルタイム ロギング：P.10-7 の「オンライン イベント ログの表示」を参照してください。
- ログ ファイル：P.10-9 の「ログ ファイルの表示」を参照してください。

オンライン イベント ログの表示

Detector モジュールのモニタリング メカニズムをアクティブにして、リアルタイムのイベント ログを表示できます。この設定により、Detector モジュールのイベントのオンライン ロギングを表示できます。次のコマンドを入力します。

event monitor

次の例を参考にしてください。

```
user@DETECTOR# event monitor
```

画面はイベントで常にアップデートされます。

（注）　モニタリング メカニズム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

ログ ファイルに記録されている Detector モジュールの動作を表示するために、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できます。Detector モジュールのイベントは Detector モジュールのログ ファイルにオンラインで記録されるため、リモート ホストからそのイベントを表示できます。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。複数の syslog サーバに Detector モジュールのログ ファイルをエクスポートできます。1 つのサーバがオフラインになったときに別のサーバでメッセージを受信できるように、追加のサーバを指定できます。

Detector モジュールのオンライン ログのエクスポート機能は、リモート syslog サーバにだけ適用できます。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.
```

syslog メッセージの構文は次のとおりです。

event-date event-time Guard-IP-address protection-module 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）ロギング パラメータを設定します。次のコマンドを入力します。

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

表 10-5 で、**logging** コマンドのキーワードについて説明します。

表 10-5　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ことにより、リモート ユーザは Detector モジュールのイベントをあるファイルで受信し、他のネットワーク サービスのイベント用に別のファイルを使用できます。 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。
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、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　リモート syslog サーバの IP アドレスを設定します。次のコマンドを入力します。

```
logging host remote-syslog-server-ip
```

または

```
export log 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、このコマンドを複数回入力してください。

次の例は、*local3* ファシリティを使用して、*notification* 以上の重大度レベルのトラップが IP アドレス *10.0.0.191* の syslog サーバに送信されるように、Detector モジュールを設定する方法を示しています。

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

オンライン イベント ログのエクスポート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、次のコマンドを入力します。

show log

次の例を参考にしてください。

```
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 ファイルのエクスポート

監視または診断のために、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できます。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*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log sftp** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 10-6 で、**copy log ftp** コマンドの引数とキーワードについて説明します。

表 10-6　copy log ftp コマンドの引数

パラメータ	説明
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、Detector モジュールのログ ファイルがエクスポートされます。
ftp	ログを FTP サーバにエクスポートします。
sftp	ログを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの完全な名前。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。

表 10-6　copy log ftp コマンドの引数（続き）

パラメータ	説明
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。パスワードを挿入しない場合、Detector モジュールによってパスワードを要求されます。

次の例を参考にしてください。

```
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、あるいは、テストを行う予定があり、そのテスト セッションからの情報だけをログ ファイルに反映する場合は、ログ ファイルをクリアできます。

すべてのエントリの Detector モジュールまたはゾーンのログ ファイルをクリアするには、設定モードまたはゾーン設定モードで次のコマンドを入力します。

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、Detector 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発行する場合、**zone** *zone-name* キーワードと引数は使用できません。ゾーン設定モードで **clear log** コマンドを使用すると、現在のゾーン ログの全エントリが消去されます。

次の例を参考にしてください。

```
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

ネットワークのトラフィック パターンを記録および観察できます。ネットワークの動作を阻害しないタップでトラフィックがネットワークから直接記録されるように Detector モジュールを設定し、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にクエリーを発行することにより、トラフィックが通常状態のときに、過去のイベントの分析、攻撃シグニチャの生成、または現在のネットワーク トラフィック パターンと Detector モジュールが記録したトラフィック パターンとの比較を行うことができます。

Detector モジュールが特定の基準を満たすトラフィックだけを記録するように、フィルタを設定できます。または、すべてのトラフィック データを記録し、Detector モジュールが表示するトラフィックをフィルタリングすることもできます。

Detector モジュールは、トラフィックを gzip 圧縮された Packet Capture（PCAP）形式で保存します。これには、記録されたデータについて記述する Extensible Markup Language（XML）形式のファイルが付属します。

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。Detector モジュールには、記録されたトラフィックを分析し、シグニチャを抽出する機能があります。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 モジュールは、次の 2 つの方法でトラフィックを記録できます。

- **自動** : Detector モジュールは、トラフィック データをパケットダンプ キャプチャ ファイルに常に記録します。

  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、FTP サーバまたは SFTP 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**：Detector モジュールは、記録するためにアクティブにされたときに、トラフィックをパケットダンプ キャプチャ ファイルに記録します。

  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。記録されたトラフィックを保存するには、Detector モジュールをアクティブにして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 FTP サーバまたは SFTP サーバにエクスポートする必要があります。

  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。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。

この項では、次のトピックについて取り上げます。

Detector モジュールの自動トラフィック記録の設定

Detector モジュールをアクティブにして、ネットワーク トラフィックを自動的に記録することができます。このようにして、ネットワークの問題や攻撃が発生したときに分析または比較に使用可能な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 フィルタを使用すると、指定した基準を満たすトラフィックだけを記録するように 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 モジュールは、トラフィックをキャプチャ バッファに記録します。キャプチャ バッファのサイズが 50 MB に達するか、10 分が経過すると、Detector モジュールはバッファをローカル ファイルに圧縮形式で保存します。バッファは消去され、トラフィックの記録が続行されます。

Detector 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。記録されたトラフィックは、処理方法に基づいて分割されます。したがって、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、Detector モジュールがトラフィックを記録した時刻と処理方法に関する情報が示されています。

表 10-7 で、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について説明します。

表 10-7　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 キャプチャ時に実行された Detector モジュールの機能。機能は次のいずれかになります。 • **protect**：Detector モジュールは、ゾーンの異常検出中にトラフィックを記録しました。 • **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しました。
キャプチャ開始時刻	Detector モジュールがトラフィックの記録を開始した時刻。

表 10-7　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
キャプチャ終了時刻	（オプション）Detector モジュールがトラフィックの記録を終了した時刻。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を処理した方法。アクションは次のとおりです。 • dropped : Detector モジュールが受信したトラフィック。Detector モジュールはトラフィックを転送しません。したがって、トラフィックはドロップされます。

Detector モジュールは、ラーニング プロセスから 1 つのパケットダンプ キャプチャ ファイルを保存します。ゾーンの異常検出中に、Detector モジュールは次のパケットダンプ 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のパケットダンプ キャプチャ ファイル 1 つ
- 現在のトラフィックのパケットダンプ キャプチャ ファイル 1 つ

ゾーン検出をアクティブにした場合、またはネットワーク トラフィックを自動的に記録するために Detector モジュールをアクティブにした場合、Detector モジュールは検出プロセス中に記録した以前のパケットダンプ キャプチャ ファイルをすべて消去し、新しいファイルを作成します。

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ために、パケットダンプ キャプチャ ファイルを FTP サーバまたは SFTP サーバにエクスポートします。P.10-19 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。

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。

次の例を参考にしてください。

```
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 モジュールの手動トラフィック記録のアクティブ化

Detector モジュールをアクティブにして、トラフィックの記録を開始できます。このようにして、特定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したりできます。

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。

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入力します。

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 10-8 で、**packet-dump** コマンドの引数とキーワードについて説明します。

表 10-8　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 モジュールが記録しているトラフィックをリアルタイムで表示します。
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）　Detector モジュールは、すべての同時手動キャプチャに対して、10000 パケット / 秒の最大累積パケットダンプ キャプチャ レートをサポートします。 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ので、高いレート値を設定するときは注意してください。

表 10-8　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。Detector モジュールは、指定された数のパケットの記録を終了した後に、手動パケットダンプ キャプチャ バッファをファイルに保存します。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.6-11 の「TCPDump 式の構文について」を参照してください。

次の例を参考にしてください。

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

Detector モジュールの手動トラフィック記録の停止

Detector モジュールは、キャプチャのアクティブ時に指定された数のパケットを記録すると、手動パケットダンプ キャプチャを停止します。ただし、Detector モジュールが指定された数のパケットを記録する前に、ユーザは手動パケットダンプ キャプチャを停止できます。

Detector モジュールで手動トラフィック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 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。

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 1 ブロックのディスク スペースを割り当てます。

次の例を参考にしてください。

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

表 10-9 で、**show packet-dump** コマンド出力のフィールドについて説明します。

表 10-9　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	Detector モジュールが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ているディスク スペースの合計を MB 単位で示します。
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

パケットダンプ キャプチャ ファイルを自動的に FTP サーバまたは SFTP サーバ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 モジュールはパケットダンプ バッファの内容を保存するたびにパケットダンプ キャプチャ ファイルをローカル ファイルにエクスポートします。パケットダンプ キャプチャ ファイルは gzip 圧縮された PCAP 形式でエクスポートされ、記録されたデータについて記述する XML 形式のファイルが付属します。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。

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には、設定モードで次のいずれかのコマンドを入力します。

- **export packet-dump ftp** *server full-file-name* [*login* [*password*]]
- **export packet-dump sftp** *server full-file-name login*

（注） **copy reports** コマンドを入力する前に、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

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

表 10-10　export packet-dump コマンドの引数

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 サーバに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 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	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	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。パスワードを挿入しない場合、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、IP アドレスが *10.0.0.191* の FTP 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方法を示しています。

```
user@DETECTOR# export packet-dump ftp 10.0.0.191 /root/captures/
<user> <password>
```

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 ファイルを FTP サーバに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 モジュールはパケットダンプ キャプチャ ファイルを gzip 圧縮された PCAP 形式でエクスポートします。これには、記録されたデータについて記述する XML ファイルが付属します。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。

パケットダンプ キャプチャ ファイルを FTP 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入力します。

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

（注）　**copy reports** コマンドを入力する前に、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 10-11 で、**copy zone packet-dump** コマンドの引数とキーワードについて説明します。

表 10-11　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
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.10-24 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 10-11　copy zone packet-dump コマンドの引数とキーワード（続き）

ftp	パケットダンプ キャプチャ ファイルを FTP サーバに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 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	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	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。パスワードを挿入しない場合、Detector モジュールによってパスワードを要求されます。

次の例を参考にしてください。

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

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 ファイルを FTP サーバから Detector モジュールにインポートできます。こうして、過去のイベントを分析したり、現在のネットワーク トラフィック パターンと、トラフィックが通常状態のときに Detector モジュールが以前に記録したトラフィック パターンとを比較したり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入力します。

- **copy ftp zone** *zone-name* **packet-dump captures** *server full-file-name* [*login* [*password*]]
- **copy sftp zone** *zone-name* **packet-dump captures** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 10-12 で、**copy zone packet-dump** コマンドの引数について説明します。

表 10-12　copy zone packet-dump コマンドの引数

パラメータ	説明
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。
ftp	パケットダンプ キャプチャ ファイルを FTP 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 サーバからインポートします。
server	サーバの IP アドレス。
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 プロセスは失敗します。
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。パスワードを挿入しない場合、Detector モジュールによってパスワードを要求されます。

次の例を参考にしてください。

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

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 モジュールはゾーンのすべてのパケットダンプ 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入力します。

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

表 10-13 で、**show packet-dump captures** コマンドの引数について説明します。

表 10-13　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 モジュールはゾーンのすべてのパケットダンプ 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 10-14 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。

表 10-13　show packet-dump captures コマンドの引数（続き）

tcpdump-expression	（オプション）Detector モジュールがパケットダンプ キャプチャ ファイルを表示するときに使用するフィルタ。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。詳細については、P.6-11 の「TCPDump 式の構文について」を参照してください。

次の例を参考にしてください。

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

表 10-14 で、**show packet-dump captures** コマンド出力のフィールドについて説明します。

表 10-14　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 ファイルの名前については、表 10-7 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	Detector モジュールがトラフィックを記録するときに使用したユーザ定義フィルタ。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.6-11 の「TCPDump 式の構文について」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

攻撃シグニチャには、攻撃パケットのペイロードに表示される共通パターンが記載されます。Detector モジュールで異常なトラフィックのシグニチャの生成をアクティブにし、その情報を使用して、将来同じタイプの攻撃をすばやく発見することができます。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 リストなどからシグニチャが発行される前であっても、新しい DDoS 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。

Detector モジュールは、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します。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.6-6 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（平時）に Detector モジュールが記録したパケットダンプ キャプチャ ファイルを参照用として追加で指定することができます。参照パケットダンプ キャプチャ ファイルを指定すると、Detector モジュールは異常なトラフィックからシグニチャを生成し、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にそのシグニチャが存在する時間の割合を示します。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　Detector モジュールで攻撃進行中のトラフィックの記録をアクティブにします。**packet-dump capture** コマンドを使用します（P.10-16 の「Detector モジュールの手動トラフィック記録のアクティブ化」を参照）。

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。**show packet-dump captures** コマンドを使用して、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。詳細については、P.10-24 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 10-15 で、**show packet-dump signatures** コマンドの引数について説明します。

表 10-15　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。参照パケットダンプ キャプチャ ファイルを指定した場合、Detector モジュールは参照パケットダンプ キャプチャ ファイルにそのシグニチャが存在する時間の割合を表示します。

表 10-16 で、**show packet-dump signatures** コマンド出力のフィールドについて説明します。

表 10-16　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 ペイロードの先頭から、パターンが開始する位置までのオフセット（バイト単位）。 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 ペイロードの先頭から、パターンが終了する位置までのオフセット（バイト単位）。 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。

表 10-16　show packet-dump signatures コマンド出力のフィールドの説明（続き）

フィールド	説明
Pattern	Detector モジュールが生成したシグニチャ。Detector モジュールは、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を生成します。詳細については、P.6-14 の「パターン式の構文について」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@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。

Detector モジュールは、既存の自動パケットダンプ キャプチャ ファイルを新しい自動パケットダンプ キャプチャ 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 ファイルをコピーすると、Detector モジュールはそのファイルを手動パケットダンプ キャプチャ ファイルとして保存し、新しい自動パケットダンプ キャプチャ ファイルで上書きしません。したがって、ディスク スペースを解放するには、そのファイルを手動で削除する必要があります。

手動パケットダンプ キャプチャ ファイルをコピーした場合、Detector モジュールは元の手動パケットダンプ キャプチャ ファイルのコピーも保存します。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.10-30 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入力します。

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

表 10-17 で、**copy packet-dump captures** コマンドの引数について説明します。

表 10-17　copy packet-dump captures コマンドの引数

パラメータ	説明
zone-name	コピー対象のパケットダンプ キャプチャ ファイルがある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。
tcpdump-expression	(オプション) Detector モジュールがパケットダンプ キャプチャ ファイルをコピーするために使用するフィルタ。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.6-11 の「TCPDump 式の構文について」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。この名前は 1 ～ 63 文字の英数字の文字列です。アンダースコアを含めることができますが、スペースを含めることはできません。

次の例を参考にしてください。

```
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。

Detector モジュールでは、1 つのゾーンにつき 1 つの手動パケットダンプ キャプチャ ファイルだけを保存できます。また、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入力します。

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*}—In configuration mode
- **clear packet-dump captures** {***** | *name*}—In zone configuration mode

表 10-18 で、**clear packet-dump** コマンドの引数について説明します。

表 10-18　clear packet-dump コマンドの引数

パラメータ	説明
zone-name	既存のゾーンの名前。
*	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	消去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 ファイルを消去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

Detector モジュールの一般的な診断データを表示できます。

一般的な診断データを表示するには、次のコマンドを入力します。

show diagnostic-info

診断データは、次の情報で構成されます。

- **Line Card Number**：Detector 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 上の BIOS のベンダー。
- **BIOS Version**：Detector 上の BIOS バージョン。
- **Total available memory**：Detector 上で使用可能なメモリの合計。
- **Size of compact flash**：Detector 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** コマンドを使用してください。詳細については、P.11-7 の「Detector モジュールのバージョンのアップグレード」を参照してください。

- **Recognition Average Sample Loss**：認識モジュールの、計算されたパケット 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** の値が大きい場合は、Detector モジュールがトラフィックによって過負荷になっていることを示します。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。

メモリ消費量の表示

Detector モジュールのメモリ消費量を表示できます。Detector モジュールは、メモリ使用量を KB 単位で表示します。さらに、Detector モジュールは、検出モジュールが使用しているメモリのパーセンテージも表示します。認識検出モジュールのメモリ使用率は、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）　認識検出モジュールのメモリ使用率が 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。

次のコマンドを入力します。

show memory

次の例を参考にしてください。

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

  Recognition Used Memory: 0.3%
```

（注）　Detector モジュールの空きメモリの合計量は、**free** メモリと **cached** メモリの合計です。

CPU 使用率の表示

現在の CPU 使用率（パーセンテージ）を表示できます。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、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。

次のコマンドを入力します。

show cpu

次の例を参考にしてください。

```
user@DETECTOR# show cpu
Host CPU:  0.0% user,  0.1% system,  0.0% nice, 99.0% idle
```

ARP キャッシュの操作

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。次のいずれかのコマンドを入力します。

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*]

表 10-19 で、**arp** コマンドの引数とキーワードについて説明します。

表 10-19　arp コマンドの引数とキーワード

パラメータ	説明
-v、**--verbose**	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。
-H *type*、**--hw-type** *type*、**-t** *type*	Detector 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。このパラメータのデフォルト値は、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。
-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。
-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 ifa 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。

表 10-19　arp コマンドの引数とキーワード（続き）

パラメータ	説明
-i *If*、**--device** *If*	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、Detector 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推測します。pub エントリの場合、これは Detector 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*	ハードウェア アドレスを *hw_addr* クラスに設定して、ホスト *hostname* の ARP アドレス マッピング エントリを作成します。ほとんどのクラスでは、通常の表現を使用できます。
-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、ファイル *filename* 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　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の知識が必要です。

次の例を参考にしてください。

```
user@DETECTOR# 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
```

netstat の使用

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、マスカレード接続、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できます。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、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 10-20 で、**netstat** コマンドの引数とキーワードについて説明します。

表 10-20　netstat コマンドの引数とキーワード

パラメータ	説明
address_family_options	[--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]][--unix|-x] [--inet|--ip] [--ax25] [--ipx] [--netrom] [--ddp]
--route、-r	Detector モジュールのルーティング テーブルを表示します。
--groups、-g	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。
--interface、-i *iface*	すべてのネットワーク インターフェイスまたはインターフェイス *iface* のテーブルを表示します。
--masquerade、-M	マスカレード接続のリストを表示します。
--statistics、-s	各プロトコルのサマリー統計情報を表示します。
-v、--verbose	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。
--numeric-hosts	数値ホスト アドレスを表示します。これは、ポート名およびユーザ名の解決に影響を及ぼしません。
--numeric-ports	数値ポート番号を表示します。これは、ホスト名およびユーザ名の解決に影響を及ぼしません。
--numeric-users	数値ユーザ ID を表示します。これは、ホスト名およびポート名の解決に影響を及ぼしません。
--protocol、-A *family*	接続を表示するアドレス低レベル プロトコル（ファミリ）を指定するカンマ区切りリスト。アドレス ファミリ inet には、raw、udp、および tcp プロトコル ソケットが含まれます。
-c、--continuous	選択した情報を 1 秒ごとに継続的に表示します。

表 10-20　netstat コマンドの引数とキーワード（続き）

パラメータ	説明
-e、--extend	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	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	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	リスニング ソケットだけを表示します。デフォルトでは、リスニング ソケットは省略されます。
-a、--all	リスニング ソケットと非リスニング ソケットの両方を表示します。
-F	FIB からのルーティング情報を表示します。
-C	ルート キャッシュからのルーティング情報を表示します。
delay	*delay* 秒ごとに、netstat が統計情報からの出力を繰り返します。

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。

次の例を参考にしてください。

```
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

パケットがネットワーク ホストに到達するまでのルートを出力して、ネットワークの問題をデバッグできます。次のコマンドを入力します。

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 10-21 で、**traceroute** コマンドの引数とキーワードについて説明します。

表 10-21　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	どの IP アドレスへのルートをトレースするか。
-f *first_ttl*	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。
-F	*don't fragment* ビットを設定します。
-g *gateway*	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）。
-i *iface*	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*	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*	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。
packetlen	プローブのパケットの長さを設定します。
-s *src_addr*	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。

表 10-21　traceroute コマンドの引数とキーワード（続き）

パラメータ	説明
-t *tos*	プローブ パケットのサービス タイプを、*tos* の値に設定します。デフォルトはゼロです。
-w *waittime*	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。

次の例を参考にしてください。

```
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
```

ping の使用

ネットワーク ホストに ICMP ECHO_REQUEST パケットを送信して、接続性を確認できます。次のコマンドを入力します。

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 10-22 で、**ping** コマンドの引数とキーワードについて説明します。

表 10-22　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*	*count* 個の ECHO_REQUEST パケットを送信します。deadline オプションが指定されている場合、ping はタイムアウトになるまでこの数の ECHO_REPLY パケットを待ちます。
-F *flow label*	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（ping6 のみ）。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 *interval*	パケットの送信間隔を *interval* 秒に設定します。デフォルトでは、1 秒に設定されます。
-I *interface*	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。
-l *preload*	応答を待たずに *preload* 個のパケットを送信します。
-Q *tos*	ICMP データグラムに Quality of Service（QoS）関連のビットを設定します。
-s *packetsize*	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	IP の TTL を設定します。
-T *timestamp option*	特別な IP タイムスタンプ オプションを設定します。

表 10-22　ping コマンドの引数とキーワード（続き）

パラメータ	説明
-w *deadline*	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。
-W *timeout*	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。

次の例を参考にしてください。

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

デバッグ情報の取得

万一 Detector 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 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 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 モジュールのログ ファイルを表示します。詳細については、P.10-9 の「ログ ファイルの表示」を参照してください。

ステップ 2　デバッグ情報を収集する時刻を特定します。問題があることを示している最初のログ メッセージを識別します。

ステップ 3　デバッグ情報を FTP サーバに抽出します。次のコマンドを入力します。

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

表 10-23 で、**copy debug-core** コマンドの引数について説明します。

表 10-23　copy debug-core コマンドの引数

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）。

表 10-23　copy debug-core コマンドの引数（続き）

パラメータ	説明
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。パスワードを挿入しない場合、Detector モジュールによってパスワードを要求されます。

次の例を参考にしてください。

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