Detector モジュールの初期化

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）をネットワーク内で初期化するために必要な基本的作業とその管理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。

コマンドライン インターフェイスの使用

コマンドライン インターフェイス（CLI）を使用して、Detector モジュールの機能を制御できます。Detector モジュールのユーザ インターフェイスはさまざまなコマンド モードに分かれていて、CLI へのアクセス権はユーザの特権レベルに対応しています。ユーザが使用可能なコマンドは、現在どのモードにいるかによって異なります。

この項では、次のトピックについて取り上げます。

- ユーザの特権レベルについて
- コマンド モードについて
- CLI コマンドの入力
- CLI 使用のヒント

ユーザの特権レベルについて

CLI へのアクセス権は、ユーザの特権レベルに対応しています。各特権レベルには、独自のコマンドのグループがあります。

表 3-1 に、ユーザの特権レベルを示します。

表 3-1　ユーザの特権レベル

ユーザの特権レベル	説明
管理者（admin）	すべての操作にアクセスできます。
設定（config）	ユーザの定義、削除、および修正に関連する操作を除いて、すべての操作にアクセスできます。
ダイナミック（dynamic）	監視と診断、検出、およびラーニングに関する操作にアクセスできます。dynamic 特権を持つユーザは、フレックスコンテンツ フィルタおよび動的フィルタを設定することもできます。
表示（show）	監視操作と診断操作にアクセスできます。

（注）　フィルタの設定はすべて、管理者の特権レベルまたは設定の特権レベルを持つユーザが実行することをお勧めします。これより下位の特権レベルしか持たないユーザも、動的フィルタを追加および削除できます。

コマンド モードについて

この項では、Detector モジュール CLI で使用するコマンドおよび設定モードの概要を説明します。各コマンド モードで使用可能なコマンドのリストを入手するには、システム プロンプトで **?** を入力します。

表 3-2 に、Detector モジュールのコマンド モードを示します。

表 3-2　Detector モジュール コマンド設定モード

モード	説明
グローバル	リモート デバイスに接続してシステム情報を一覧表示できます。 グローバル プロンプトは、Detector モジュールにログインしたときのデフォルトのプロンプトです。コマンド プロンプトは次のようになっています。 `user@DETECTOR#`
設定	Detector モジュール全体に影響する機能を設定できます。また、ユーザのアクセス権が制限されています。 設定モードに入るには、グローバル モードで **configure** コマンドを使用します。コマンド プロンプトは次のようになっています。 `user@DETECTOR-conf#`
インターフェイス設定	Detector モジュール ネットワーキング インターフェイスを設定できます。 インターフェイス設定モードに入るには、設定モードで **interface** コマンドを使用します。コマンド プロンプトは次のようになっています。 `user@DETECTOR-conf-if-<interface-name>#`

表 3-2　Detector モジュール コマンド設定モード（続き）

モード	説明
ルータ設定	Detector モジュールのルーティング設定を設定できます。 ルータ設定モードに入るには、設定モードで router コマンドを使用します。コマンド プロンプトは次のようになっています。 `router>`
ゾーン設定	ゾーンのアトリビュートを設定できます。 ゾーン設定モードに入るには、設定モードで **zone** コマンドを使用するか、グローバル モードで **configure** コマンドを使用します。コマンド プロンプトは次のようになっています。 `user@DETECTOR-conf-zone-<zone-name>#`
ポリシー テンプレート設定	ゾーン ポリシーのテンプレートを設定できます。 ポリシー テンプレート設定モードに入るには、ゾーン設定モードで **policy-template** コマンドを使用します。コマンド プロンプトは次のようになっています。 `user@DETECTOR-conf-zone-<zone-name>-policy_template-<policy-template-name>#`
ポリシー設定	ゾーン ポリシーを設定できます。 ポリシー設定モードに入るには、ゾーン設定モードで **policy** コマンドを使用します。コマンド プロンプトは次のようになっています。 `user@DETECTOR-conf-zone-<zone-name>-policy-<policy-path>#`
Guard の設定	ユーザ フィルタなど、Cisco Anomaly Guard Module に固有のゾーン定義を設定できます。 guard 設定モードに入るには、ゾーン設定モードで **guard-conf** コマンドを使用します。コマンド プロンプトは次のようになっています。 `user@DETECTOR-conf-zone-<zone-name>(guard)#`

CLI コマンドの入力

この項では、CLI コマンドの入力規則について説明します。

- コマンドの no 形式の使用
- show コマンド構文
- CLI のエラー メッセージ

表 3-3 に、CLI コマンドの入力規則を示します。

表 3-3　CLI の規則

操作	キーボード シーケンス
コマンド履歴をスクロールして変更する	矢印キーを使用する
特定のコマンド モードで使用可能なコマンドを表示する	Shift キーを押して ?（疑問符）を入力する
コマンドの補完を表示する	コマンドの最初の部分を入力し、Tab キーを押す
コマンド構文の補完を表示する	コマンドを入力して、Tab キーを 2 回押す
more コマンドを使用してスクロールする	**more** *number-of-lines* コマンドを入力する。 **more** コマンドでは、Space キーを押したときにウィンドウに表示される追加の行数が設定されます。デフォルトは、その端末で表示可能な行数より 2 行少ない行数です。 *number-of-lines* 引数は、Space キーを押したときに表示される追加の行数を設定します。
一画面分スクロールする（コマンド出力内）	Space キーを押す
一画面分後方にスクロールする（コマンド出力内）	b キーを押す
スクロール動作を中止する	q キーを押す

表 3-3　CLI の規則（続き）

操作	キーボード シーケンス
文字列を前方に検索する	/（スラッシュ記号）を押し、*文字列*を入力する
文字列を後方に検索する	?（疑問符）キーを押し、*文字列*を入力する
アクションをキャンセルするか、パラメータを削除する	そのコマンドの **no** 形を使用する
現在の操作に関連する情報を表示する	**show** コマンドを入力する
現在のコマンド グループ レベルを終了して上位のグループ レベルに移る	**exit** コマンドを入力する
すべてのコマンド グループ レベルを終了してルート レベルに戻る	**end** コマンドを入力する
特定の *文字列*を含む最初の行も含めて、その行からコマンド出力を表示する	|（縦線）を押し、**begin** *string* コマンドを入力する
特定の *文字列*を含むコマンド出力の行を表示する	|（縦線）を押し、**include** *string* コマンドを入力する
特定の *文字列*を含まないコマンド出力の行を表示する	|（縦線）を押し、**exclude** *string* コマンドを入力する

（注） ルート レベルで **exit** コマンドを入力すると、CLI 環境が終了し、オペレーティング システムのログイン画面に戻ります。

コマンドの no 形式の使用

ほとんどすべての設定コマンドに、**no** 形式があります。一般に、コマンドの **no** 形式は、特定の機能をデイセーブルにする場合に使用します。ディセーブルになっている機能をイネーブルにするには、キーワード **no** を取ってそのコマンドを使用します。たとえば、**event monitor** コマンドではイベント モニタが有効になり、**no event monitor** コマンドでは無効になります。

show コマンド構文

ゾーン設定モードから、ゾーン関連の **show** コマンドを実行できます。また、これらのコマンドは、グローバル モードまたは設定モードからも実行できます。

グローバル モードまたは設定モードの **show** コマンドの構文は、次のとおりです。

show zone *zone-name parameters...*

ゾーン設定モードの **show** コマンドの構文は、次のとおりです。

show *parameters...*

（注） このマニュアルでは、明示的な指定がない限り、ゾーン設定モードの **show** コマンド構文を使用します。

CLI のエラー メッセージ

Detector モジュール CLI では、次の場合にエラー メッセージが表示されます。

- コマンドの構文が不完全であるか、間違っている場合。
- コマンドがシステムの設定と一致しない場合。
- システムの障害のために操作を実行できなかった場合。この場合は、システムのログにエントリが作成されます。

CLI 使用のヒント

この項では、CLI の使用に関するヒントを提供し、次のトピックについて取り上げます。

ヘルプの使用

CLI では、コマンド階層のすべてのモードで状況依存のヘルプが用意されています。ヘルプの情報では、現在のコマンド モードで使用可能なコマンドが示され、各コマンドの簡単な説明が提供されます。

ヘルプを取得するには、**?** と入力します。

コマンドのヘルプを表示するには、そのコマンドの後ろに **?** を入力します。

モードで使用可能なすべてのコマンドとその簡単な説明を表示するには、コマンド プロンプトで **?** を入力します。

ヘルプには、現在のモードで使用可能なコマンドのみが表示されます。

タブ補完の使用

タブ補完を使用すると、コマンドの入力に必要な文字数を減らすことができます。コマンドの初めの文字をいくつか入力して Tab キーを押すと、コマンドを補完することができます。

複数のオプションで値を指定するコマンドを入力し、Tab キーを 2 回押すと、使用可能な入力パラメータが表示されます。これにはシステム定義のパラメータとユーザ定義のパラメータも含まれます。たとえば、ゾーン設定モードで **policy-template** コマンドを入力し、Tab キーを 2 回押すと、ポリシー テンプレート名のリストが表示されます。設定モードで **zone** コマンドを入力し、Tab キーを 2 回押すと、定義済みのゾーンが表示されます。

タブ補完で複数のコマンドが一致する場合は、何も表示されず、入力した現在の行がもう一度表示されます。

タブ補完機能では、現在のモードで使用可能なコマンドのみが表示されます。

aaa authorization commands zone-completion tacacs+ コマンドを使用すると、グローバル モードと設定モードですべてのコマンド（**zone** コマンドや **show zone** コマンドなど）におけるゾーン名のタブ補完をディセーブルにできます。詳細については、P.4-18 の「ゾーン名のタブ補完のディセーブル化」を参照してください。

操作の方向の規定について

コマンド構文中のキーワードの順序によって、操作の方向が規定されます。コマンドを入力する前にキーワードを入力すると、Detector モジュールは Detector モジュールからサーバにデータをコピーします。キーワードを入力する前にコマンドを入力すると、Detector モジュールはサーバから Detector モジュールにデータをコピーします。たとえば、**copy log ftp** コマンドではログ ファイルが Detector モジュールから FTP サーバにコピーされます。**copy ftp new-version** コマンドでは、新規ソフトウェア バージョン ファイルが FTP サーバから Detector モジュールにコピーされます。

コマンドの省略

コマンドやキーワードは、一意な省略形を保てる文字数まで短縮できます。

たとえば、**show** コマンドは **sh** まで短縮できます。

ワイルドカード文字の使用

ワイルドカードとして、アスタリスク（*）を使用できます。

たとえば、**learning policy-construction *** コマンドを入力すると、Detector モジュールで設定されているすべてのゾーンでポリシー構築フェーズがアクティブになります。

learning policy-construction scan* コマンドを入力すると、scan で始まる名前を持つ Detector モジュールで設定されているすべてのゾーン（scannet や scanserver など）でポリシー構築フェーズがアクティブになります。

no zone * コマンドを入力すると、すべてのゾーンが削除されます。

Detector モジュールのインターフェイスの設定

Detector モジュールは、スーパーバイザ上に 1 つの管理ポートと 2 つのデータ ポートを持っています。1 つのデータ ポートのみ使用されます。

次のコマンドを入力し、設定モードに入って Detector モジュールを設定します。

configure [**terminal**]

次の例は、設定モードに入る方法を示しています。

```
user@DETECTOR# configure
user@DETECTOR-conf#
```

Detector モジュールが正しく動作するように、Detector モジュールのインターフェイスを設定する必要があります。インターフェイス特性には、IP アドレスやインターフェイスの MTU などがあります。

多くの機能は、インターフェイス単位でイネーブルになります。**interface** コマンドを入力するときには、インターフェイスのタイプと番号を指定する必要があります。

次のガイドラインは、すべての物理インターフェイスおよび仮想インターフェイスの設定プロセスに適用されます。

- 各インターフェイスには、IP アドレスと IP サブネット マスクを設定する必要があります。
- **no shutdown** コマンドを使用して、各インターフェイスをアクティブにする必要があります。

インターフェイスの設定を表示するには、**show** または show running-config コマンドを入力します。

この項では、次のトピックについて取り上げます。

物理インターフェイスの設定

Detector モジュールをネットワークに接続するには、物理インターフェイスを設定します。

注意　同じサブネット上で 2 つの物理インターフェイスを設定しないでください。Detector モジュールのルーティングが正しく機能しなくなる場合があります。

物理インターフェイスを設定するには、次の手順を実行します。

ステップ 1　設定モードで次のコマンドを入力し、インターフェイス設定モードに入ります。

```
interface if-name
```

if-name 引数には、インターフェイス名を指定します。

Detector モジュールは、次のインターフェイスをサポートしています。

- eth1：管理ポート
- giga2：データ ポート

ステップ 2　次のコマンドを入力して、インターフェイスの IP アドレスを設定します。

```
ip address ip-addr ip-mask
```

ip-addr 引数および *ip-mask* 引数には、インターフェイスの 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）。

ステップ 3　（オプション）次のコマンドを入力して、インターフェイスの MTU を定義します。

```
mtu integer
```

integer 引数は、eth1 インターフェイスの場合は 576 ～ 16,384 バイトの整数で、giga2 インターフェイスの場合は 576 ～ 1,824 の整数です。

デフォルトの MTU の値は 1,500 バイトです。

ステップ 4　（オプション）次のコマンドを入力して、インターフェイスの速度とデュプレックス モードを設定します。

```
speed {auto | half speed | full speed}
```

表 3-4 に、**speed** コマンドの引数とキーワードを示します。

表 3-4　speed コマンドの引数とキーワード

パラメータ	説明
auto	インターフェイスのオートネゴシエーション機能を有効にします。インターフェイスは、ネットワーク設定で使用されているメディア タイプ、およびピア ルータ、ハブ、スイッチの伝送速度などの環境要因に応じて、10 Mbps、100 Mbps、1000 Mbps のいずれか、半二重または全二重で自動的に動作します。 このモードがデフォルトです。
half	半二重動作を指定します。
full	全二重動作を指定します。
speed	インターフェイスの速度。10 Mbps、100 Mbps、および 1000 Mbps にそれぞれ対応する 10、100、または 1000 を入力します。

ステップ 5　次のコマンドを入力して、インターフェイスをアクティブにします。

```
no shutdown
```

設定変更を有効にするには、Detector モジュールをリロードする必要があります。

次の例は、インターフェイス eth1 を設定してアクティブにする方法を示しています。

```
user@DETECTOR-conf# interface eth1
user@DETECTOR-conf-if-eth1# ip address 10.10.10.33 255.255.255.252
user@DETECTOR-conf-if-eth1# no shutdown
```

物理インターフェイスを非アクティブにするには、**shutdown** コマンドを使用します。

物理インターフェイスのカウンタのクリア

テストを行う予定があり、データ（ギガ）に使用される物理インターフェイスのカウンタにテスト セッションの情報だけを反映する場合は、このカウンタをクリアすることができます。

物理インターフェイスのカウンタをクリアするには、インターフェイス設定モードで次のコマンドを入力します。

clear counters

次の例は、インターフェイス giga2 のカウンタをクリアする方法を示しています。

```
user@DETECTOR-conf-if-giga2# clear counters
```

デフォルト ゲートウェイの設定

デフォルト ゲートウェイは、ローカル ネットワークで未知の IP アドレスを持つパケットの受信と転送を行います。ほとんどの場合、Detector モジュールのデフォルト ゲートウェイの IP アドレスは、Detector モジュールとインターネットの間に存在する隣接ルータです。デフォルト ゲートウェイ アドレスは、Detector モジュールのネットワーク インターフェイスの IP アドレスのいずれかと同じネットワーク上にある必要があります。

デフォルト ゲートウェイ アドレスを割り当てるには、設定モードで次のコマンドを入力します。

default-gateway *ip-addr*

ip-addr 引数には、デフォルト ゲートウェイの IP アドレスを指定します。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 192.168.100.1）。

デフォルト ゲートウェイ アドレスを変更するには、このコマンドを再入力します。

次の例は、デフォルト ゲートウェイを設定する方法を示しています。

```
user@DETECTOR-conf# default-gateway 192.168.100.1
```

ルーティング テーブルへのスタティック ルートの追加

Detector モジュールのルーティング テーブルにスタティック ルートを追加できます。スタティック ルートは、Detector モジュールの IP インターフェイスに関連付けられたローカル ネットワークの外側にあるサーバやネットワークのルートを指定するために追加します。

スタティック ルートは永続的に追加され、Detector モジュールのリブート後も削除されません。

Detector モジュールのルーティング テーブルにスタティック ルートを追加するには、設定モードで次のコマンドを入力します。

ip route *ip-addr ip-mask nexthop-ip* [*if-name*]

表 3-5 に、**ip route** コマンドの引数を示します。

表 3-5　ip route コマンドの引数

パラメータ	説明
ip-addr	ルートの宛先ネットワーク。宛先には、IP ネットワーク アドレス（ネットワーク アドレスのホスト ビットは 0 に設定）またはホスト ルートの IP アドレスを指定できます。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 192.168.100.1）。
ip-mask	宛先ネットワークに関連付けられたサブネット マスク。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 255.255.255.0）。
nexthop-ip	宛先ネットワークとサブネット マスクによって定義された一連のアドレスへの到達を可能にする転送アドレスまたはネクストホップ IP アドレス。ネクストホップ IP アドレスは、インターフェイスのサブネット内にある必要があります。ローカル サブネット ルートでは、ネクストホップ IP アドレスは、そのサブネットに接続されたインターフェイスに割り当てられている IP アドレスです。1 つ以上のルータをまたいで使用可能なリモート ルートの場合、ネクストホップ IP アドレスは、ネイバールータに割り当てられている直接到達可能な IP アドレスです。

表 3-5　ip route コマンドの引数（続き）

パラメータ	説明
if-name	（オプション）宛先への到達が可能な Detector モジュールのインターフェイス。インターフェイスを指定しなかった場合、Detector モジュールのルーティング テーブルに従って、使用されるインターフェイスはネクストホップ IP アドレスによって判別されます。

次の例は、スタティック ルートを設定する方法を示しています。

```
user@DETECTOR-conf# ip route 172.16.31.5 255.255.255.255
192.168.100.34
```

ルーティング テーブルを表示するには、**show ip route** コマンドを入力します。

Detector モジュールの管理

スーパーバイザ エンジンからセッションを確立し、Detector モジュールのネットワーク機能を設定した後は（第 2 章「スーパーバイザ エンジンでの Detector モジュールの設定」および P.3-11 の「Detector モジュールのインターフェイスの設定」を参照）、次のいずれかの方法を使用して Detector モジュールにアクセスし、管理することができます。

- Secure Shell（SSH; セキュア シェル）のセッションを使用したアクセス。
- Web-Based Manager（WBM）を使用した Detector モジュールへのアクセス。
- DDoS 検知ネットワーク要素からのアクセス。詳細については、該当するマニュアルを参照してください。

この項では、次のトピックについて取り上げます。

- Web-Based Manager による Detector モジュールの管理
- SSH を使用した Detector モジュールへのアクセス

Web-Based Manager による Detector モジュールの管理

WBM を使用すると、Web ブラウザを使用して Web から Detector モジュールを管理できます。

WBM を使用して Detector モジュールを管理するには、次の手順を実行します。

ステップ 1　設定モードで次のコマンドを入力して、WBM サービスをイネーブルにします。

```
service wbm
```

ステップ 2　設定モードで次のコマンドを入力して、リモート マネージャの IP アドレスから Detector モジュールへのアクセスを許可します。

```
permit wbm ip-addr [ip-mask]
```

ip-addr 引数および *ip-mask* 引数には、リモート マネージャの 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。

ステップ 3　ブラウザを開いて、次のアドレスを入力します。

```
https://Detector module-ip-address/
```

Detector module-ip-address 引数には、Detector モジュールの IP アドレスを指定します。

Detector モジュールの WBM ウィンドウが表示されます。

（注）　Web ベース管理制御をイネーブルにするには、HTTP ではなく HTTPS が使用されます。

ステップ 4　ユーザ名とパスワードを入力し、**OK** をクリックします。

ユーザ名とパスワードを正しく入力すると、Detector モジュールのホームページが表示されます。

TACACS+ 認証が設定されている場合は、ローカル データベースの代わりに TACACS+ ユーザ データベースがユーザ認証に使用されます。TACACS+ サーバ上で高度な認証アトリビュート（パスワードの有効期限など）が設定されている場合、Detector モジュールが TACACS+ サーバ上のユーザ設定に基づいて新しいパスワードの入力を要求したり、パスワードがいつ期限切れになるかを通知したりします。

次の例は、Detector モジュール WBM をイネーブルにする方法を示しています。

```
user@DETECTOR-conf# service wbm
user@DETECTOR-conf# permit wbm 192.168.30.32
```

SSH を使用した Detector モジュールへのアクセス

セキュア シェル（SSH）の接続を使用して、Detector モジュールにアクセスすることができます。

SSH サービスは、デフォルトでイネーブルになっています。

SSH を使用して Detector モジュールにアクセスするには、次の手順を実行します。

ステップ 1　設定モードで次のコマンドを入力して、リモート ネットワークの IP アドレスから Detector モジュールへのアクセスを許可します。

```
permit ssh ip-addr [ip-mask]
```

ip-addr 引数および *ip-mask* 引数には、リモート ネットワークの 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 アドレスとして 192.168.10.2 を、サブネット マスクとして 255.255.255.252 を入力）。

ステップ 2　リモート ネットワーク アドレスから接続を確立し、ログイン ユーザ名とパスワードを入力します。

TACACS+ 認証が設定されている場合は、ローカル データベースの代わりに TACACS+ ユーザ データベースがユーザ認証に使用されます。TACACS+ サーバ上で高度な認証アトリビュート（パスワードの有効期限など）が設定されている場合、Detector モジュールが TACACS+ サーバ上のユーザ設定に基づいて新しいパスワードの入力を要求したり、パスワードがいつ期限切れになるかを通知したりします。

ログイン ユーザ名とパスワードを入力しないで SSH 接続をイネーブルにするには、次の手順を実行します。

- ローカルに設定されたログインとパスワードを認証に使用するように Detector モジュールを設定します。詳細については、P.4-6 の「認証の設定」を参照してください。

- リモート接続 SSH の公開鍵を Detector モジュール SSH 鍵リストに追加します。詳細については、P.4-37 の「SSH 鍵の管理」を参照してください。

次の例は、Detector モジュールへの SSH 接続をイネーブルにする方法を示しています。

```
user@DETECTOR-conf# permit ssh 192.168.30.32
```