



## Detector モジュールの初期化

この章では、Cisco Traffic Anomaly Detector (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。

この章には、Detector モジュールの関連製品である Cisco Guard (Guard) についての記述がありません。Guard は、DDoS 攻撃 (分散型サービス拒絶攻撃) を検出して軽減するデバイスです。Guard は、ゾーントラフィックが通過する際に攻撃トラフィックをドロップして正常なトラフィックをネットワークに戻し、ゾーントラフィックをクリーンにします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにできます。また、Detector モジュールは Guard とゾーン設定を同期させることができます。Guard の詳細については、『Cisco Anomaly Guard Module Configuration Guide』または『Cisco Guard Configuration Guide』を参照してください。



(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。

- [コマンドライン インターフェイスの使用](#)
- [Detector モジュールのインターフェイスの設定](#)
- [デフォルト ゲートウェイの設定](#)
- [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 モジュールの管理](#)

## 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せん。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	<p>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。</p> <p>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。</p> <pre>user@DETECTOR#</pre>
設定	<p>Detector モジュールの動作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。</p> <p>設定モードに入るには、グローバル モードで <b>configure</b> 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。</p> <pre>user@DETECTOR-conf#</pre>
インターフェイス設定	<p>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。</p> <p>インターフェイス設定モードに入るには、設定モードで <b>interface</b> 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。</p> <pre>user@DETECTOR-conf-if-&lt;interface-name&gt;#</pre>
ルータ設定	<p>Detector モジュールのルーティング設定を設定できます。</p> <p>ルータ設定モードに入るには、設定モードで <b>router</b> 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。</p> <pre>router&gt;</pre>
ゾーン設定	<p>ゾーンの属性を設定できます。</p> <p>ゾーン設定モードに入るには、設定モードで <b>zone</b> コマンドを使用するか、グローバル モードで <b>configure</b> 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。</p> <pre>user@DETECTOR-conf-zone-&lt;zone-name&gt;#</pre>
ポリシー テンプレート設定	<p>ゾーン ポリシーのテンプレートを設定できます。</p> <p>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 <b>policy-template</b> 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。</p> <pre>user@DETECTOR-conf-zone-&lt;zone-name&gt;-policy_template-&lt;policy-template-name&gt;#</pre>
ポリシー設定	<p>ゾーン ポリシーを設定できます。</p> <p>ポリシー設定モードに入るには、ゾーン設定モードで <b>policy</b> 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。</p> <pre>user@DETECTOR-conf-zone-&lt;zone-name&gt;-policy-&lt;policy-path&gt;#</pre>
Guard の設定	<p>ユーザ フィルタなど、Guard に固有のゾーン定義を設定できます。</p> <p>guard 設定モードに入るには、ゾーン設定モードで <b>guard-conf</b> 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。</p> <pre>user@DETECTOR-conf-zone-&lt;zone-name&gt;(guard) #</pre>

## CLI コマンドの入力

この項では、次のトピックについて取り上げます。

- 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	<b>Shift</b> キーを押して <b>?</b> (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、 <b>Tab</b> 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、 <b>Tab</b> キーを 2 回押す。
<b>more</b> コマンドを使用してスクロールする	<b>more number-of-lines</b> コマンドを入力する。  <b>more</b> コマンドでは、 <b>Space</b> 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。  <b>number-of-lines</b> 引数は、 <b>Space</b> 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)	<b>Space</b> 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>b</b> キーを押す。
スクロール動作を中止する	<b>q</b> キーを押す。
文字列を前方に検索する	<b>/</b> (スラッシュ記号) キーを押し、文字列を入力する。
文字列を後方に検索する	<b>?</b> (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 <b>no</b> 形式を使用する。
現在の操作に関連する情報を表示する	<b>show</b> 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	<b>exit</b> 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	<b>end</b> 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	<b> </b> (縦線) を押し、 <b>begin string</b> 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	<b> </b> (縦線) を押し、 <b>include string</b> 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	<b> </b> (縦線) を押し、 <b>exclude string</b> 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、特定の機能をディ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](#)
- [タブ補完の使用](#)
- [操作の方向の規定について](#)
- [コマンドの省略](#)
- [ワイルドカード文字の使用](#)

## 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。コマンドの最初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isableにできます。詳細については、[P.4-13](#) の「[ゾーン名のタブ補完のディisable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、**permit wbm \*** コマンドを入力すると、すべてのリモート マネージャの IP アドレスから Web-Based Manager (WBM) を使用した Detector モジュールにアクセスできるようになります。

**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 モジュールのインターフェイスを設定するには、Detector モジュールと、Detector モジュールをスイッチ ファブリックに接続する 3 つのギガビット イーサネット ポート間のマッピングを理解しておく必要があります。インターフェイスの指定子と機能は、Detector モジュールの帯域幅動作 (1 Gbps または 2 Gbps) によって異なります。表 3-4 に、スーパーバイザ エンジンのポートと Detector モジュールのインターフェイス間の相関を示します。

表 3-4 スーパーバイザ エンジンと Detector モジュールのインターフェイス ポートのマッピング

スーパーバイザのポート	Detector モジュールのインターフェイス	
	1 Gbps 動作	2 Gbps 動作
ポート 1	giga2 : データ トラフィック	giga1 : データ トラフィック
ポート 2	不使用	giga2 : データ トラフィック
管理	mng : 管理トラフィックおよび Guard のアクティベーション	mng : 管理トラフィックおよび Guard のアクティベーション

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

```
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。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。

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ついて、次のガイドラインに従います。

- mng と識別される管理ポートには、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ステータスと設定を表示するには、インターフェイス設定モードで **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](#)
- [物理インターフェイスのカウンタのクリア](#)

### 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、表 3-5 に示されているインターフェイス名を指定します。

**表 3-5 Detector モジュールのインターフェイス**

1 Gbps 動作	2 Gbps 動作
giga1 : 不使用	giga1 : データ トラフィック
giga2 : データ トラフィック	giga2 : データ トラフィック
mng : 管理トラフィック	mng : 管理トラフィック

**ステップ 2** mng 管理ポートの場合のみ、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 Maximum Transmission Unit (MTU; 最大伝送ユニット) を定義します。

```
mtu integer
```

*integer* 引数は、すべてのインターフェイスを対象とする 576 ~ 1800 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** 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
```

**ステップ 5** ステップ 1 ~ 4 を繰り返して、残りの各物理インターフェイスを設定します。

データ ポート インターフェイスをアクティブまたは非アクティブにしたら、Detector モジュールをリロードして設定変更を有効にする必要があります。

次の例は、管理インターフェイス (mng) 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 mng
user@DETECTOR-conf-if-mng# ip address 10.10.10.23 255.255.255.252
user@DETECTOR-conf-if-mng2# no shutdown
```

次の 1 Gbps 動作の例は、インターフェイス `giga2` 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 giga2
user@DETECTOR-conf-if-giga2# no shutdown
```

次の 2 Gbps 動作の例は、インターフェイス `giga1` と `giga2` 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 giga1
user@DETECTOR-conf-if-giga1# no shutdown
user@DETECTOR-conf-if-giga1# interface giga2
user@DETECTOR-conf-if-giga2# 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、データトラフィック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 1 Gbps 動作の例は、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
```

次の 2 Gbps 動作の例は、インターフェイス `giga1` と `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-giga1# clear counters
user@DETECTOR-conf-if-giga1# interface giga2
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 3-6 に、`ip route` コマンドの引数を示します。

表 3-6 ip route コマンドの引数

パラメータ	説明
<code>ip-addr</code>	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）。
<code>ip-mask</code>	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）。
<code>nexthop-ip</code>	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。
<code>if-name</code>	（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 テーブルのネクストホップ IP アドレスが、使用されるインターフェイスを判別します。

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.3-8 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 Detector モジュールへのアクセス。
- Web-Based Manager (WBM) を使用した Detector モジュールへのアクセス。
- MultiDevice Manager (MDM) 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 Detector モジュールへのアクセス。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 を使用した Detector モジュールの管理](#)
- [Cisco DDoS MultiDevice 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 を使用した Detector モジュールの管理

WBM と Web ブラウザを使用して Detector モジュールを管理できます。

WBM をイネーブルにして 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] | *} [if-service]
```

表 3-7 に、`permit wbm` コマンドの引数を示します。

表 3-7 `permit wbm` コマンドの引数


パラメータ	説明
<code>ip-addr</code>	リモート マネージャの 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 192.168.100.1）。
<code>ip-mask</code>	(オプション) 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）。
*	ワイルドカード文字としてのアスタリスク (*)。アスタリスク (*) を使用すると、すべてのリモート マネージャの IP アドレスからのアクセスが許可されます。
	 <b>注意</b> セキュリティ上の理由から、すべての IP アドレスからのサービスへのアクセスを許可しないことをお勧めします。

表 3-7 permit wbm コマンドの引数 (続き)

パラメータ	説明
<i>if-service</i>	(オプション: 1 Gbps 動作のみ) ユーザ アクセスを管理インターフェイスだけに制限する管理ポート デジグネータ。デフォルトはすべてのインターフェイスです。mng を入力します。  デフォルト設定に戻すには、このコマンドの <b>no</b> バージョンを使用します。

**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。

Detector モジュールが Terminal Access Controller Access-Control System Plus (TACACS+) 認証を使用するように設定されている場合、Detector モジュールはローカル データベースではなく TACACS+ ユーザ データベースをユーザ認証に使用します。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
```

WBM を使用して Detector モジュールを管理する方法については、該当する『*Cisco Web-Based Manager Configuration Guide*』を参照してください。

## Cisco DDoS MultiDevice Manager による Detector モジュールの管理

Cisco DDoS MultiDevice Manager (MDM) は、Web ブラウザを使用して 1 つ以上の Detector モジュールを管理できるサーバベースのアプリケーションです。MDM を使用して Detector モジュールのネットワークを管理するには、次の処理を実行します。

- ネットワーク サーバに MDM ソフトウェアをインストールし、設定します (『*Cisco DDoS MultiDevice Manager Configuration Guide*』を参照)。
- Detector モジュールで MDM サービスをイネーブルにし、MDM によるアクセスを許可します (次の手順の説明を参照)。

Detector モジュールで MDM サービスをイネーブルにするには、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、MDM のサービスをイネーブルにします。

```
service mdm
```

**ステップ 2** 設定モードで次のコマンドを入力して、MDM から Detector モジュールへのアクセスを許可します。

```
mdm server ip-addr
```

*ip-addr* 引数には、MDM サーバの IP アドレスを定義します。IP アドレスをドット区切り 10 進表記で入力します。

次の例は、MDM のサービスをイネーブルにする方法、および MDM からのアクセスを許可する方法を示しています。

```
user@DETECTOR-conf# service mdm
user@DETECTOR-conf# mdm server 192.168.30.32
```

MDM を使用して Detector モジュールを管理する方法については、『Cisco DDoS MultiDevice Manager Configuration Guide』を参照してください。

## SSH を使用した Detector モジュールへのアクセス

SSH 接続を使用して、Detector モジュールにアクセスできます。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] | *} [if-service]
```

表 3-8 に、`permit ssh` コマンドの引数を示します。

表 3-8 `permit ssh` コマンドの引数


パラメータ	説明
<i>ip-addr</i>	リモート ネットワークの 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 192.168.100.1)。
<i>ip-mask</i>	(オプション) 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)。
*	ワイルドカード文字としてのアスタリスク (*)。アスタリスク (*) を使用すると、すべてのリモート ネットワークからのアクセスが許可されます。
	 <p><b>注意</b> セキュリティ上の理由から、すべてのリモート ネットワークへのアクセスを許可しないことをお勧めします。</p>

表 3-8 permit ssh コマンドの引数 (続き)

パラメータ	説明
<i>if-service</i>	(オプション: 1 Gbps 動作のみ) ユーザ アクセスを管理インターフェイスだけに制限する管理ポート デジグネータ。デフォルトはすべてのインターフェイスです。mng を入力します。  デフォルト設定に戻すには、このコマンドの <b>no</b> バージョンを使用します。

**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。

Detector モジュールが TACACS+ 認証を使用するように設定されている場合、Detector モジュールはローカル データベースではなく TACACS+ ユーザ データベースをユーザ認証に使用します。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.4-4](#) 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.4-25](#) 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
```