CHAPTER 2

WBM の起動とカスタマイズ

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）の WBM を起動しカスタマイズする方法について説明します。Detector モジュールの WBM にアクセスするには、まず CLI を使用して WBM のネットワーク アクセスを設定する必要があります。

この章は、次の項で構成されています。

WBM のネットワーク アクセスの設定

WBM サービスをイネーブルにし、WBM を介した Detector モジュールへのネットワーク アクセスを許可するには、Detector モジュールの CLI を使用する必要があります。必要な設定変更を行うには、Administration ユーザ特権レベル、または Configuration ユーザ特権レベルの権限を持つユーザとして、ログインする必要があります。Detector モジュールの CLI へのアクセスと使用については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。

WBM のネットワーク アクセスを設定するには、Detector モジュールの CLI を使用して次の手順を実行します。

ステップ 1　コンソールまたは Secure Shell（SSH; セキュア シェル）接続を使用して、Detector モジュールの CLI にログインします。

ステップ 2　次のコマンドをグローバル モードで入力して、設定モードに入ります。

```
admin@DETECTOR# configure
```

ステップ 3　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。

```
admin@DETECTOR-conf# service wbm
```

ステップ 4　次のコマンドを入力して、WBM から Detector モジュールへのアクセスを許可します。

```
admin@DETECTOR-conf# permit wbm ip-addr [ip-mask] [if-service]
```

引数 *ip-addr* および *ip-mask* は、WBM への接続に使用するクライアント デバイスの IP アドレスを定義します。

オプションの *if-service* 引数は、ユーザのアクセス先を管理インターフェイスに制限する管理ポート指定子を指定します。デフォルトはすべてのインターフェイスです。**mng** と入力します。

次の例は、IP アドレス 192.168.30.32 を使用して接続する WBM のネットワーク アクセスを設定する方法を示しています。

```
admin@DETECTOR# configure
admin@DETECTOR-conf# service wbm
admin@DETECTOR-conf# permit wbm 192.168.30.32
```

Detector モジュール上で WBM のネットワーク アクセスを設定した後は、CLI を終了し、Web ブラウザを使用して WBM を起動することができます。

WBM の起動

WBM を起動するには、次の手順を実行します。

ステップ 1　Web ブラウザを開いて、Secure HTTP（HTTPS）を使用して Detector モジュールの IP アドレスを入力します。

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

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

Detector モジュールの WBM ログイン ウィンドウが表示されます。

ステップ 2　ユーザ名とパスワードを入力し、**OK** をクリックします。WBM のホーム ページが表示されます。

（注）　Detector モジュールに Terminal Access Controller Access Control System Plus（TACACS+）認証が設定されている場合、Detector モジュールはユーザ認証にローカル データベースではなく、TACACS+ ユーザ データベースを使用します。TACACS+ サーバ上に詳細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 モジュールは、TACACS+ サーバ上のユーザの設定に基づいて、ユーザに新しいパスワードを要求したり、パスワードの有効期限が近づいたときに通知したりできます。

ユーザ認証方式を設定するには、Detector モジュールの CLI を使用します。Detector モジュールの CLI へのアクセスと使用については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。

Detector モジュールへの接続に失敗した場合は、次に示すトラブルシューティングに関するヒントを確認してください。

- 有効なユーザ名とパスワードを入力したことを確認します。
- 正しい Detector モジュールの管理 IP アドレスを入力したこと、および URL で HTTPS を使用していることを確認します。
- WBM クライアントと Detector モジュールの両方のネットワーク接続を確認します。
- SSH を使用して WBM クライアントから Detector モジュールに接続できることを確認します。

（注）　SSH を使用して接続することにより、WBM と Detector モジュールの間のネットワーク接続が確認されます。

- WBM サービスがイネーブルになっていて、WBM クライアントの IP アドレスから Detector モジュールへのアクセスが許可されていることを確認します（詳細については、「WBM のネットワーク アクセスの設定」の項を参照）。

ログイン バナーの設定

ログイン バナーは、SSH セッション、コンソール ポート接続、または Detector モジュールに対する WBM セッションを開いたときに、ユーザ認証の前に画面に表示されるテキストです。

ログイン バナーは、次の位置に表示されます。

- CLI：パスワード ログイン プロンプトの前
- WBM：Detector モジュール ログイン ウィンドウの右側

ログイン バナーを設定するには、Detector モジュールの CLI にアクセスして設定モードで **login-banner** コマンドを使用する必要があります。必要な設定変更を行うには、Administration ユーザ特権レベル、または Configuration ユーザ特権レベルの権限を持つユーザとして、ログインする必要があります。CLI を使用したログイン バナーの設定とインポートについては、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。

WBM ロゴの設定

WBM Web ページに会社のロゴまたはカスタマイズした任意のロゴを追加することで、WBM インターフェイスをカスタマイズできます。

新しいロゴは、次の位置に表示されます。

- Detector モジュール Login ページでは、Cisco Systems ロゴの下
- すべての WBM ページで、Cisco Systems ロゴの右側

WBM ロゴを設定するには、Detector モジュールの CLI を使用して、グローバル モードまたは設定モードで **copy** {**ftp** | **sftp** | **scp**} **wbm-logo** コマンドを使用する必要があります。必要な設定変更を行うには、Administration ユーザ特権レベル、または Configuration ユーザ特権レベルの権限を持つユーザとして、ログインする必要があります。CLI を使用した WBM ロゴのインポートについては、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。