
# 概要

ここでは、Cisco Traffic Anomaly Detector Web-based Manager（WBM）のインターフェイスの概要を説明します。この章は、次の項で構成されています。

- ユーザ インターフェイス要件
- WBM が動作するための Detector の要件
- Cisco Traffic Anomaly Detector について
- DDoS について
- ゾーンについて
- WBM インターフェイスについて

# ユーザ インターフェイス要件

ここでは、WBM クライアントの最小要件について説明します。この項は、次の内容で構成されています。



## 最小要件

Detector 上で WBM にアクセスして WBM を使用するための最小要件は、次のとおりです。

- Microsoft Internet Exploler 5.5 以降：HTML、テーブル、Cookie、JavaScript、およびフレームをサポートしている必要があります。
- Sun Microsystems Java 2 Runtime Environment（JRE）Standard Edition バージョン 1.4.2_04：JRE は、リアルタイム カウンタの表示だけに必要です（「Java 2 Runtime Environment のインストール」の項を参照）。
- モニタの解像度：1,024 x 768 ピクセル以上にすることをお勧めします。

## Java 2 Runtime Environment のインストール

リアルタイム カウンタを表示するには、Java 2 Runtime Environment（JRE）をインストールする必要があります。JRE を Sun Microsystems の Web サイトからダウンロードしてインストールするには、次の手順を実行します。

**ステップ 1**　Web ブラウザで URL www.sun.com を開きます。

Sun Microsystems のホーム ページが表示されます。

**ステップ 2**　**Downloads** > **Java 2 Standard Edition** を選択して、ダウンロード ページに移動します。

**ステップ 3**　バージョン番号を選択して、使用するバージョンのダウンロード サイトを開きます。

**ステップ 4**　J2SE JRE をダウンロードします。

J2SE v < *バージョン番号* > JRE カテゴリまで下方向にスクロールして、**Download J2SE JRE** を選択します。

**（注）**　J2SE SDK は選択しないでください。

**ステップ 5**　ダウンロードしたファイルを実行して、Sun Microsystems によるオンライン インストールの手順に従います。

**ステップ 6**　次の操作を実行して、使用しているブラウザを JRE がサポートしていることを確認します。

**a.** 使用しているマシン上で **Start** > **Settings** > **Control Panel** を選択して、Windows のコントロール パネルを開きます。コントロール パネルが表示されます。

**b.** Java Plug-in アイコンをダブルクリックします。Java(TM) Plug-in コントロール パネルが表示されます。

**c.** **Advanced** タブをクリックします。

**d.** **<APPLET> tag support** セクションを開いて、使用しているブラウザの隣にあるチェックボックスをオンにします。

**（注）**　JRE の以前のバージョンがインストールされていた場合、サポートされているブラウザは別のタブに表示されます。**Browser** タブをクリックし、**Settings** の下で、使用しているブラウザの隣にあるチェックボックスをオンにします。

**e.** **Apply** をクリックして、設定を保存します。

**f.** ブラウザを再起動します。

# WBM が動作するための Detector の要件

WBM を使用する前に、Detector が『*Cisco Traffic Anomaly Detector Configuration Guide*』の説明に従って適切にインストールされていることを確認します。初期設定プロセスは、CLI を使用して実行する必要があります。WBM を正しく動作させるために、Detector 上で次のタスクが設定されていることを確認します。

- ネットワークの設定 : Detector のネットワーク インターフェイスを設定します。使用しているネットワーク環境で動作するように Detector のインターフェイスを設定するまでは、Detector に接続できません。
- WBM サービスのイネーブル化とアクセスの許可：WBM から Detector へのアクセスをイネーブルにし、許可します。この動作を設定するための CLI の手順については、このマニュアルにも記載されています（第 2 章「WBM の起動とカスタマイズ」の WBM のネットワーク アクセスの設定の項を参照）。
- Remote Guard リスト : Detector がゾーン トラフィックで異常を検出したときに、Detector がアクティブにできるリモート Guard リストを設定します。
- SSL 接続または SSH 接続：Detector と Cisco Guard の間に通信チャネルを設定します。Detector がゾーン トラフィックで異常を検出した場合、Detector は通信チャネルを使用して Cisco Guard をアクティブ化できます。
- ポート ミラーリングまたはスプリット信号：光スプリッタまたはポート ミラーリング機能（SPAN など）を使用して、Detector をネットワーク スイッチに接続すると、Detector は分析するネットワーク トラフィックを受信できます。

# Cisco Traffic Anomaly Detector について

Detector は、サーバ、ファイアウォール インターフェイス、またはルータ インターフェイスなどの保護された宛先（ゾーンと呼ばれる）に対して Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃の兆候を検出し続けるパッシブ モニタリング デバイスです。Detector が最も効果を発揮するのは Cisco Guard と併用する場合ですが、単独でも DDoS 検出とアラーム送信のためのコンポーネントとして運用できます。

Detector は、スイッチのポート ミラーリング機能（SPAN など）またはスプリットのいずれかを使用して、トラフィックのコピーを受信します。

Detector は保護されたゾーンに送信されるすべてのインバウンド トラフィックのコピーを分析し、現在のトラフィックの行動に関するしきい値（ゾーン ポリシー）のセットと比較して、悪意のあるトラフィックを検出します。Detector が攻撃の可能性があると考えられる悪意のある動作を識別した場合、Detector は Cisco Guard をアクティブ化してこれらの攻撃を軽減します。

Detector では、次の機能を使用してトラフィックを監視します。

- アルゴリズムに基づいたシステムでゾーンのトラフィックをラーニングし、トラフィックの特性に合わせた調整を行い、しきい値とポリシーという形で Detector に参考値と指示を与えます。
- Cisco Guard をリモートでアクティブにしてゾーンを保護状態に置くか、または Detector の syslog にトラフィックの異常を記録するシステム。

これらの機能を使用することで Detector は、ネットワークの動作を阻害せずにバックグラウンドでその検出処理を実行できます。

# DDoS について

DDoS 攻撃の主な目的は、正当なユーザによる特定のコンピュータまたはネットワーク リソースへのアクセスを拒絶することです。この攻撃は、悪意のある要求をターゲットに送信する個人が発信元です。悪意のある要求は、サービスを低下させ、コンピュータ サーバやネットワーク デバイス上のネットワーク サービスを混乱させ、ネットワーク リンクを不要なトラフィックで飽和させます。

DDoS 攻撃は、悪意のあるユーザがインターネット上の数百または数千のホストを改ざん（ゾンビ化）し、システムにトロイの木馬を配置すると発生します。トロイの木馬は、無害なアプリケーションのように見える、複製しないプログラムですが、予期しない有害なアクションを実行します。トロイの木馬は、いつどのように組織的攻撃を開始するかについての攻撃者による指令をマスター サーバ コントローラから受けます。ゾンビは、自動化されたスクリプトを実行します。これは、保護されたサーバのネットワーク リソースを偽のサービス要求で使用できなくします。攻撃には、Web サーバに偽のホーム ページ要求を大量に送信して正当なユーザがアクセスできないようにしたり、Domain Name System（DNS; ドメイン ネーム システム）サーバのアベイラビリティと正確性を損なわせようとするものなどがあります。コンピュータの改ざんは、多くの場合、個人によって開始されますが、実際に攻撃用コードを実行しているコンピュータは、複数の組織によって管理される複数の自律システム上に分散しており、その数は何十万にも及ぶ可能性があります。このような分散型攻撃は、一般的なゾーンで利用可能な低い帯域幅では処理できない量のトラフィックを生成します。詳細については、P.1-7 の「ゾーンについて」を参照してください。

# ゾーンについて

Detector は DDoS 攻撃検出のためにゾーンを監視します。ゾーンは、次の要素のいずれかです。

- ネットワーク サーバ、ネットワーク クライアント、ルータ
- ネットワーク リンクまたはサブネット、またはネットワーク全体
- 個々のインターネット ユーザまたは企業
- インターネット サービス プロバイダー（ISP）
- これらの要素の任意の組み合わせ

DDoS 攻撃を感知すると、Detector は Cisco Guard を自動的にアクティブにしてゾーンを攻撃から保護するか、ユーザに対して Cisco Guard を手動でアクティブにするように通知することができます。

Detector は、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンのトラフィックを同時に分析できます。

ゾーンを定義するときに、Detector がゾーンの異常検出のために使用するネットワーク アドレスとポリシーを設定します。ゾーンには名前を付け、ゾーンを指すときはその名前を使用します。

# WBM インターフェイスについて

WBM は、Detector 設定と管理機能へのアクセスを提供するブラウザベースの GUI です。WBM では、CLI 機能のサブセットが提供され、ゾーンの設定の作成と変更、ゾーン保護の管理、Detector とゾーンの動作の監視を実行できます。Detector の機能の中で、主に Detector の初期インストールと設定に関連するものには、CLI によってのみ設定でき、WBM では設定できないものがあります。CLI の使用に関する詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

この項は、次の内容で構成されています。



## WBM ブラウザ ウィンドウについて

図 1-1 に、WBM ウィンドウの各セクションを示します。

**図 1-1　　WBM 画面のセクション**

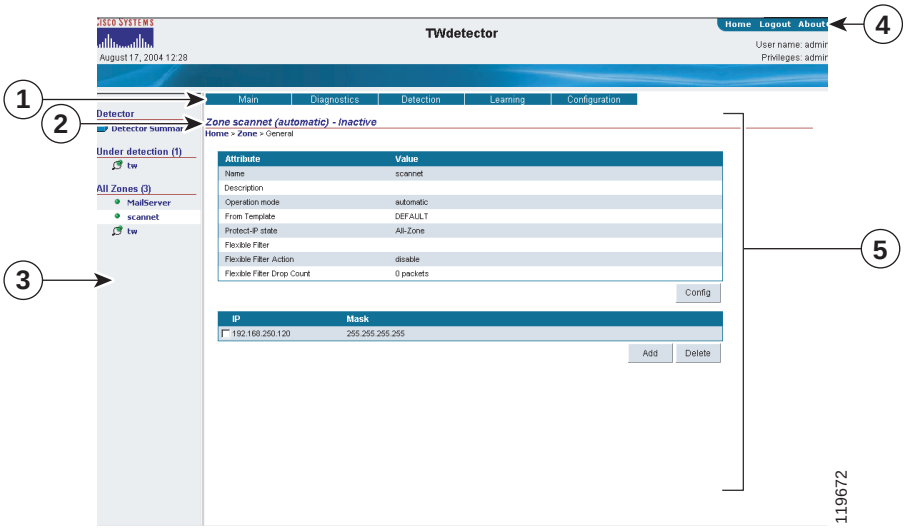

**表 1-1　WBM ウィンドウの各セクション**

| セクション | 機能 |
|---|---|
| 1 | **メイン メニュー バー**：ナビゲーション ペインで選択されたリンクのメイン メニューを表示します。このセクションには、次の 2 つのメニュー バーのいずれかが表示されます。<br>• Detector の要約メニュー : Detector の次の統計オプションと設定オプションにアクセスできます。<br>— Detector のステータスと診断ツール<br>— 定義済みゾーンのリスト<br>— ユーザ プロファイル マネージャ<br>Detector の要約メニューを表示するには、ナビゲーション ペイン（3）の **Detector Summary** をクリックします。<br>• ゾーンのメイン メニュー : ゾーンの詳細情報および設定オプションにアクセスできます。<br>個々のゾーンのメニューを表示するには、ナビゲーション領域（3）に表示されているゾーンをクリックします。 |
| 2 | **ナビゲーション パス**：作業領域（5）に表示された画面へのパスを表示します。パスの特定のセクションに移動するには、パスの目的のセクションをクリックします。 |
| 3 | **ナビゲーション領域**：Detector の要約画面およびゾーンのステータス画面へのリンクのリストを表示します。リストにあるリンクをクリックすると、関連するステータス情報が作業領域（5）に表示されます。ナビゲーション領域で選択したリンクは、白色の枠で強調表示されます。<br>ナビゲーション領域のサイズを変更するには、ナビゲーション領域と表示領域の間にあるフレーム バーをドラッグします。 |

表 1-1　WBM ウィンドウの各セクション（続き）

| セクション | 機能 |
|---|---|
| 4 | **情報領域**：現在のユーザのユーザ名と特権レベルを表示し、次のリンクを示します。<br>• Home：Detector の要約画面に戻ります。<br>• Enable：ユーザ特権レベル間を移動します。<br>• Logout：WBM セッションを閉じます（System Login 画面が表示されます）。<br>• About：WBM ソフトウェアに関する情報を表示します。ソフトウェアのバージョン番号、システムのシリアル番号、およびソフトウェア ライセンス契約が含まれています。 |
| 5 | **作業領域：**選択した情報が表示されます。作業領域のサイズを変更するには、ナビゲーション領域と作業領域の間にあるフレーム バーをドラッグします。 |

## ゾーンのステータス アイコンについて

WBM では、ゾーンの現在のステータスを示すためにアイコンが使用されています。ステータス アイコンは、ナビゲーション領域とゾーンのステータス バーに表示されます。表 1-2 に、ゾーン ステータスを表すアイコンの説明を示します。

表 1-2　ゾーンのステータス アイコン

| アイコン | ステータス |
|---|---|
|  | ゾーンが非アクティブです（ゾーンのトラフィックをラーニングしていないか、ゾーンを保護していません）。 |
|  | ゾーンはアクティブで、ラーニング プロセス（ポリシー構築フェーズまたはしきい値調整フェーズのいずれか）に入っています。 |

表 1-2　ゾーンのステータス アイコン（続き）

| アイコン | ステータス |
|---|---|
|  | ゾーンはアクティブです（ゾーン トラフィックの異常の検出中またはゾーン トラフィックの異常検出およびラーニングの実行中）。 |
|  | ゾーンはアクティブで、インタラクティブ検出モードで動作しています。ゾーンで使用できる新しい検出推奨事項が参照できます。 |

## WBM のナビゲーション マップについて

メニューまたはナビゲーション パスを使用して、画面階層内を移動できます（表 1-1 のセクション 2 を参照）。メニューの選択項目は、ドロップダウン リストで示されます。現在の表示で使用できない選択項目は、グレーアウトされています。

この項の表では、2 つの WBM メニュー バーから使用できるリンクの一覧と配置を示します。

- Detector の要約メニュー：Detector の統計ツールと設定ツールにアクセスできます。Detector の要約メニューを表示するには、ナビゲーション領域で **Detector Summary** をクリックするか、情報領域で **Home** をクリックします。表 1-3 に、Detector の要約メニューの各レベルのマップを示します。

表 1-3　Detector の要約メニュー

| レベル 1 | レベル 2 | レベル 3 |
|---|---|---|
| Main | Summary | |
| Diagnostics | Counters | Detector counters |
| | | Real time counters |
| | Event log | |
| Zones | Zone list | |
| | Create zone | |
| | Template list | |
| | Compare zone policies | |

**表 1-3　Detector の要約メニュー（続き）**

| レベル 1 | レベル 2 | レベル 3 |
|---|---|---|
| Main | Summary | |
| Users | User list | |
| | Create user | |

- ゾーン　メニュー：個々のゾーンの統計ツールおよび設定ツールにアクセスできます。ゾーン メニューを表示するには、ナビゲーション領域に表示されている目的のゾーンをクリックします。表 1-4 に、様々なゾーン メニュー レベルのマップを示します。

**表 1-4　ゾーン メニュー**

| レベル 1 | レベル 2 | レベル 3 |
|---|---|---|
| Main | Summary | |
| | Create zone | |
| | Save as. . . | |
| Diagnostics | Counters | Zone Counters |
| | | Real time counters |
| | Event log | |
| | Attack reports | Attack Summary |
| | | HTTP Zombies |
| | Statistics | Policy statistics |
| | | Drop Statistics |
| | Packet-Dump | Start Packet-Dump |
| | | Stop Packet-Dump |
| | | Packet-Dump List |
| Detection | Detect | |
| | Deactivate | |
| | Dynamic Filters | |
| | Recommendations | |

表 1-4　ゾーン メニュー（続き）

| レベル 1 | レベル 2 | レベル 3 |
|---|---|---|
| Learning | Construct Policies | |
| | Tune Thresholds | |
| | Deactivate | |
| | Stop Learning | |
| | Accept | |
| | Snapshot | |
| | Snapshot List | |
| Configuration | General | |
| | Filters | User Filters |
| | | Bypass Filters |
| | | Flex-Content Filters |
| | Policy Templates | View |
| | | Add Service |
| | | Remove Service |
| | Policies | View |
| | | Compare Policies |