



概要

ここでは、WBM インターフェイスの概要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。

- [ユーザ インターフェイス要件](#)
- [WBM 動作の Detector モジュールの要件](#)
- [Cisco Traffic Anomaly Detector Module 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](#)

ユーザー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](#)
- [Java 2 Runtime Environment のインストール](#)

最小要件

Detector モジュール上で 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 Explorer 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 動作の Detector モジュールの要件

WBM を使用する前に、『Cisco Traffic Anomaly Detector Module Configuration Guide』に記載されているように、Detector モジュールが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 モジュール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 モジュールのネットワーク 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 モジュールのインターフェイスを設定するまでは、Detector モジュールに接続できません。
- WBM サービスのイネーブル化とアクセスの許可 : WBM から Detector モジュール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）。
- リモート Guard リスト : Detector モジュールがゾーンのトラフィックで異常を検出したときに、Detector モジュール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 または SSH 接続 : Detector モジュールと Cisco Anomaly Guard Module の間の通信チャネルを設定します。Detector モジュールがゾーンのトラフィックで異常を検出したときに、Detector モジュールは通信チャネルを使用して Cisco Anomaly Guard Module をアクティブにできます。
- ゾーン トラフィックのコピー : ゾーン トラフィックのコピーを分析用に Detector モジュールに送信するように、スーパーバイザ エンジンを設定します。

Cisco Traffic Anomaly Detector Module について

Detector モジュールは、サーバ、ファイアウォール インターフェイス、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）を対象に、Distributed Denial of Service (DDoS; 分散型サービス拒絶) 攻撃の兆候を継続的に検出するパッシブ モニタリング デバイスです。Detector モジュールは、Cisco Anomaly Guard Module との併用に最も適していますが、別個の DDoS 検出および警告コンポーネントとしても運用できます。

Detector モジュールは、次のいずれかの製品にインストールすることができます。

- Catalyst 6500 シリーズ スイッチ
- Cisco 7600 シリーズ ルータ

ゾーンに送信されたトラフィックをキャプチャし、そのコピーを Detector モジュールに送信するようにスイッチを設定する必要があります。

Detector モジュールは、1 つまたは複数の保護されたゾーンが宛先となっているすべての着信トラフィックのコピーを分析し、現在のトラフィックを動作のしきい値セット（ゾーン ポリシー）と比較して、異常なトラフィック動作を検出します。Detector モジュールは、攻撃の可能性がある異常な動作を識別すると、こうした攻撃を軽減するために Cisco Anomaly Guard Module をアクティブにします。

Detector モジュールは、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。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せた調整を行い、しきい値とポリシーという形で、参考値と指示を Detector モジュールに提供します。
- Cisco Anomaly Guard Module をリモートでアクティブにして、1 つまたは複数のゾーンを保護状態に置くか、または Detector モジュールの 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と、Detector モジュールはバックグラウンドに控えた状態を保ちながら、検出の役割を果たすことができます。

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。ゾーンの詳細については、「[ゾーンについて](#)」の項を参照してください。

ゾーンについて

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 モジュールでは、Cisco Anomaly Guard Module 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 Anomaly Guard Module 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 モジュールは、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。

ゾーンを定義する際に、Detector モジュール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 モジュールの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 モジュールとゾーンの動作の監視を実行できます。Detector モジュールの機能の中で、主に Detector モジュール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 Module Configuration Guide』を参照してください。

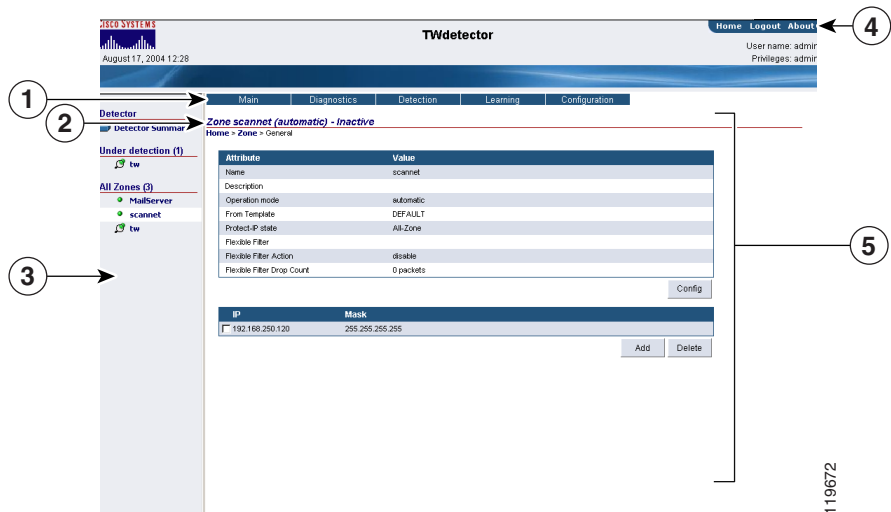
この項は、次の内容で構成されています。

- [WBM ブラウザ ウィンドウについて](#)
- [ゾーンのステータスアイコンについて](#)
- [WBM のナビゲーションマップについて](#)

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 画面の各セクション



119672

表 1-1 WBM ウィンドウの各セクション

セクション	機能
1	<p>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。</p> <ul style="list-style-type: none"> • Detector の要約メニュー：Detector モジュールの次の統計オプションおよび設定オプションへのアクセスを提供します。 <ul style="list-style-type: none"> – Detector モジュールのステータス ツールおよび診断ツール – 定義済みゾーンのリスト – ユーザ プロファイル マネージャ <p>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) にある Detector Summary をクリックします。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>
2	<p>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。</p>
3	<p>ナビゲーション領域：Detector モジュール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。</p> <p>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。</p>

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	<p>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。</p> <ul style="list-style-type: none"> • Home : Detector の要約画面に戻ります。 • Enable : ユーザ特権レベル間を移動します。 • Logout : WBM セッションを閉じます (System Login 画面が表示されます)。 • 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。 • シスコシステムズのアイコン : cisco.com の Detector モジュールのホームページへのリンクです。
5	<p>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。</p>

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 ゾーンの状態アイコン (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を検出しています。または、異常を検出しながらゾーン トラフィックをラーニングしています)。
	ゾーンはアクティブで、インタラクティブ保護モードで動作しています。ゾーンで使用できる新しい保護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 要約メニュー**：一般の Detector モジュールの統計ツールおよび設定ツールへのアクセスを提供します。Detector の要約メニューを表示するには、ナビゲーション領域の **Detector Summary** または情報領域の **Home** をクリックします。表 1-3 に、Detector 要約メニューのレベルのマップを示します。

表 1-3 Detector 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 要約メニュー（続き）

レベル 1	レベル 2	レベル 3
Users	User list	
	Create user	
	Change password	

- 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、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
		Learning Parameters

