



製品の概要

この章では、Cisco Guard (Guard) Web-Based Manager (WBM) の概要を説明します。WBM は Guard のリモート操作と監視に使用できます。WBM は、HTML ページを Guard コマンドに変換することによって Guard と通信するグラフィカル ユーザー インターフェイスです。

この章は、次の項で構成されています。

- [ユーザー インターフェイス要件](#)
- [WBM の動作のための Guard の要件](#)
- [Cisco Guard 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](#)
- [Java 2 Runtime Environment のインストール](#)

最小要件

Guard 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 (SE) バージョン 5.0 以降：JRE は、リアルタイム カウンタの表示に必要です（「[Java 2 Runtime Environment のインストール](#)」の項を参照）。
- モニタの解像度：1024 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、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 SE ページに移動して、**Java Runtime Environment (JRE) 5.0 Update 11** 以降を選択します。
 - ステップ 3** ライセンス契約に同意し、Java Runtime Environment (JRE) 5.0 Update 11 以降をダウンロードします。
 - ステップ 4** 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。
-

WBM の動作のための Guard の要件

WBM を使用する前に、『*Guard Configuration Guide*』の説明に従って Guard を正しくインストールしてください。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、Guard 上で次の機能が設定されていることを確認します。

- ネットワーク インターフェイスの設定：Guard 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 Guard のインターフェイスを設定するまでは、Guard に接続できません。
- トラフィックの宛先変更設定：ゾーン保護をアクティブにしたときに、Guard がゾーン トラフィックを自身に宛先変更し、正当なトラフィックをネットワークに再注入できるように、トラフィックの宛先変更を設定します。
- WBM サービスのイネーブル化とアクセスの許可：Guard 上の WBM サービスをイネーブルにし、WBM クライアントから Guard へのアクセスを許可します。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（「[WBM のネットワーク アクセスの設定](#)」の項を参照）。

Cisco Guard について

Guard は、Distributed Denial of Service (DDoS; 分散型サービス拒絶) 攻撃を軽減する装置です。不審なトラフィックを正常なネットワーク パスから自身に宛先変更してクリーンにします。トラフィックのクリーニング処理時、Guard は攻撃パケットを識別してドロップし、正当なパケットを目的のネットワークの宛先に転送します。

通常、Guard は、分散型アップストリーム構成にバックボーン レベルで配置します。

管理者がネットワーク要素（ゾーン）を定義し、Guard がそのネットワーク要素を DDoS 攻撃から保護します。ゾーンが攻撃を受けると、Guard はターゲットとされたゾーンを宛先とするネットワーク トラフィックのみを宛先変更して、特定の攻撃パケットを識別してドロップし、正当なトラフィック パケットをゾーンに転送します。Guard は常にゾーンのトラフィックをフィルタリングし、新たに発生する攻撃パターンに応じて攻撃軽減プロセスを変更します。ゾーンへの攻撃が終了したと判断すると、Guard はゾーン トラフィックの自身への宛先変更を停止します。必要なときだけネットワーク トラフィックを宛先変更することにより、Guard は攻撃発生時には保護の役割を果たし、それ以外のときにはネットワークのバックグラウンドに控えた状態を保つことができます。

Guard は次のタスクを実行します。

- トラフィックのラーニング：アルゴリズムに基づいたプロセスを使用して、正常なゾーン トラフィックの特性（サービスとトラフィック レート）をラーニングします。ラーニング プロセス時、Guard は、デフォルトのゾーン トラフィック ポリシーとポリシーのしきい値を正常なゾーン トラフィックの特性に合わせて変更します。トラフィックのポリシーとしきい値は、ゾーンのトラフィックが正常か異常（ゾーンへの攻撃を示す）かを判断するときに Guard によって使用される参照ポイントを定義します。
- トラフィックの保護：正当なトラフィックと悪意のあるトラフィックを区別し、正当なトラフィックだけがゾーンへの転送を許可されるように悪意のあるトラフィックをフィルタリングします。
- トラフィックの宛先変更：ゾーンのトラフィックを正常なネットワーク パスから Guard のラーニング プロセスおよび保護プロセスに宛先変更し、正当なゾーン トラフィックをネットワークに戻します。

DDoS について

DDoS 攻撃は、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します。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。

この項は、次の内容で構成されています。

- [スプーフィングを利用した攻撃について](#)
- [スプーフィング以外の攻撃について](#)

スプーフィングを利用した攻撃について

スプーフィングを利用した攻撃は DDoS 攻撃の一種です。この攻撃では、パケットのヘッダーに実際の送信元デバイスの IP アドレスではない IP アドレスが含まれています。スプーフィング パケットの送信元 IP アドレスは、ランダムな場合も特定のアドレスに集中している場合もあります。スプーフィングを利用した攻撃により、ターゲット サイトのリンクとそのサイトのサーバリソースが飽和します。コンピュータ ハッカーは、スプーフィングを利用した大量の攻撃を単一のデバイスからでも容易に生成できます。

スプーフィング以外の攻撃について

スプーフィング以外の攻撃（クライアント攻撃）は、ほとんどが実際の TCP 接続を伴う TCP ベースの攻撃で、ネットワーク リンクやオペレーティング システムではなく、サーバのアプリケーション レベルで機能を低下させます。

多数のクライアント（ゾンビ）からのクライアント攻撃では、個別のどのクライアントも異常を発生させることなくサーバ アプリケーションの機能を低下させる場合があります。ゾンビ プログラムは、ターゲット サイトにアクセスする正当なブラウザを模倣しようとします。

ゾーンについて

Guard が保護する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、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

新しいゾーンを作成する場合は、ゾーンに名前を付け、ゾーンにネットワーク アドレスを設定します。Guard は、ゾーンのトラフィックで異常を検出するために、ゾーンにポリシーおよびポリシー しきい値のデフォルト セットを設定します。詳細については、[第 6 章「ポリシー テンプレートの設定」](#)の「[ポリシー テンプレートについて](#)」の項、および[第 8 章「ゾーンのポリシーの管理」](#)の「[ゾーンのポリシーについて](#)」の項を参照してください。

Guard 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、複数のゾーンを同時に保護できます。

WBM インターフェイスについて

WBM は、Guard 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グラフィカルユーザインターフェイス (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、Guard とゾーンの動作の監視を実行できます。Guard の機能の中で、主に Guard 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 の使用方法の詳細については、『*Guard 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 および表 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

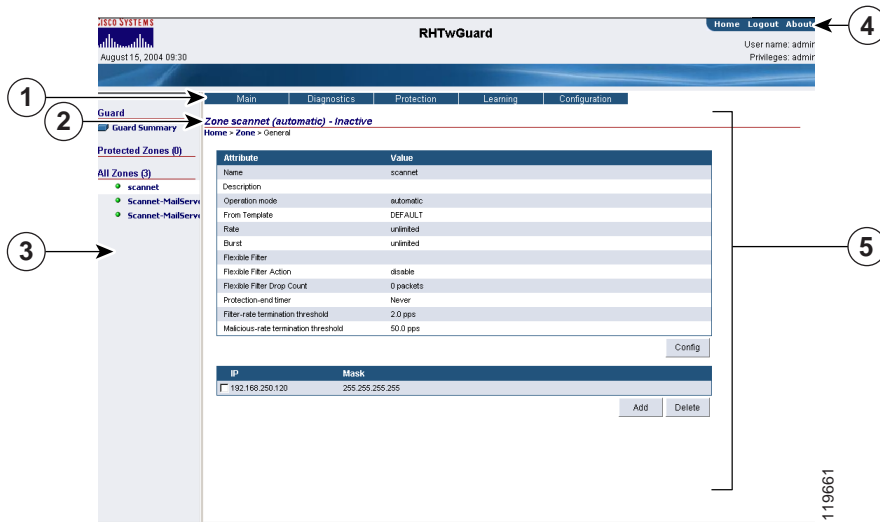






表 1-1 WBM ウィンドウの各セクション

セクション	機能
1	<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"> Guard の要約メニュー：次の Guard 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。 <ul style="list-style-type: none"> Guard のステータス ツールと診断ツール 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>Guard 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) で Guard 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：Guard 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>
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：Guard 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。 Cisco Systems アイコン：cisco.com の Guard のホームページへのリンクです。
5	<p>作業領域：選択した情報を表示します。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、各ステータス アイコンが表す内容の説明を示します。

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
	ゾーンは非アクティブです。Guard は、ゾーンのトラフィックをラーニングしていないか、ゾーンのトラフィックの異常を監視していません。
	ゾーンはアクティブで、ラーニング プロセスのフェーズです。Guard は、ラーニング プロセスのポリシー構築フェーズまたはしきい値調整フェーズを実行しています。
	ゾーンはアクティブです。Guard は、ゾーンのトラフィックの異常を監視しているか、ゾーンのトラフィックの監視とゾーンのトラフィックのラーニングを同時に実行しています。
	ゾーンはアクティブです。Guard はゾーンに対する攻撃を監視中です。ユーザの注意を必要とする新しいゾーン保護推奨事項を使用できます。

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、グレー表示されています。

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。

- Guard の要約メニュー：一般的な Guard の統計ツールと設定ツールにアクセスできます。Guard の要約メニューを表示するには、ナビゲーション領域の **Guard Summary**、または情報領域の **Home** をクリックします。表 1-3 に、Guard の要約メニュー レベルのマップを示します。

表 1-3 Guard の要約メニュー

レベル 1	レベル 2	レベル 3
Main	Summary	
	Protect IP	
Diagnostics	Counters	Device counters Real-time counters
	Event log	
	Device Resources	
Zones	Zone list	
	Create zone	
	Template list	
	Compare zone policies	
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
Protection	Protect	
	Deactivate	
	Dynamic Filters	
	Recommendations	
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