CISCO SYSTEMS

Cisco Traffic Anomaly Detector Module コンフィギュレーション ガイド

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用

Software Release 6.0 および 6.0-XG
January 2007

Text Part Number: OL-11857-01-J

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

このドキュメントで使用しているインターネット プロトコル（IP）アドレスは、実在のアドレスではありません。ドキュメント中で示される例、コマンドの画面出力、および図は、いずれも視覚的な説明のみを目的としています。実在する IP アドレスが例示されていた場合、それらは意図して使用したものではありません。

Cisco Traffic Anomaly Detector Module コンフィギュレーション ガイド
Copyright © 2006 Cisco Systems, Inc.
All rights reserved.

CONTENTS

このマニュアルについて xvii

対象読者 xviii

このガイドの使用方法 xix

記号および表記法 xxi

技術情報の入手方法 xxiii

Cisco.com xxiii

Product Documentation DVD（英語版） xxiii

マニュアルの発注方法（英語版） xxiv

シスコシステムズマニュアルセンター xxiv

シスコ製品のセキュリティの概要 xxv

シスコ製品のセキュリティ問題の報告 xxv

Product Alerts および Field Notices xxvii

テクニカル サポート xxviii

Cisco Support Web サイト xxviii

Japan TAC Web サイト xxix

サービス リクエストの発行 xxx

サービス リクエストのシビラティの定義 xxx

その他の資料および情報の入手方法 xxxi

CHAPTER 1 製品概要 1-1

Cisco Traffic Anomaly Detector Module について 1-2

DDos について 1-3

ゾーンについて 1-4
Detector モジュールの動作のしくみについて 1-5
ラーニング プロセスについて 1-6
ゾーン ポリシーについて 1-6
Detector モジュールによるゾーン異常検出のしくみについて 1-7
検出およびラーニング機能について 1-7
攻撃レポートについて 1-7
異常検出プロセスについて 1-8
1 Gbps および 2 Gbps 帯域幅オプションについて 1-9

CHAPTER 2 スーパーバイザ エンジンでの Detector モジュールの設定 2-1
Detector モジュールの設置確認 2-3
Detector モジュール管理の設定 2-5
トラフィックをキャプチャするためのトラフィックの送信元の設定 2-6
VACL の設定 2-7
SPAN の設定 2-12
Detector モジュールとのセッションの確立 2-16
Detector モジュールのリブート 2-17
Detector モジュールの設定の確認 2-20

CHAPTER 3 Detector モジュールの初期化 3-1
コマンドライン インターフェイスの使用 3-2
ユーザの特権レベルについて 3-2
コマンド モードについて 3-3
CLI コマンドの入力 3-5
コマンドの no 形式の使用 3-7

show コマンド構文 3-7
CLI のエラー メッセージ 3-7
CLI 使用のヒント 3-8
ヘルプの使用 3-8
タブ補完の使用 3-8
操作の方向の規定について 3-9
コマンドの省略 3-9
ワイルドカード文字の使用 3-9
Detector モジュールのインターフェイスの設定 3-10
物理インターフェイスの設定 3-11
物理インターフェイスのカウンタのクリア 3-13
デフォルト ゲートウェイの設定 3-14
ルーティング テーブルへのスタティック ルートの追加 3-15
Detector モジュールの管理 3-17
Web-Based Manager を使用した Detector モジュールの管理 3-17
MultiDevice Manager を使用した Detector モジュールの管理 3-19
SSH を使用した Detector モジュールへのアクセス 3-20

CHAPTER 4 **Detector の設定** 4-1
Detector のサービスのアクティブ化 4-2
AAA を使用したアクセス コントロールの設定 4-5
認証の設定 4-6
認証方式の設定 4-7
ローカル認証の設定 4-8
認可の設定 4-12
ローカル認可の設定 4-14

認可方式の設定 4-16
ゾーン名のタブ補完のディセーブル化 4-19
アカウンティングの設定 4-20
TACACS+ サーバ アトリビュートの設定 4-22
TACACS+ サーバの IP アドレスの設定 4-23
TACACS+ サーバの暗号鍵の設定 4-24
TACACS+ 検索方式の設定 4-25
TACACS+ サーバの接続タイムアウトの設定 4-26
TACACS+ サーバの統計情報の表示 4-27
Guard との通信の確立 4-28
SSL 通信チャネルの設定 4-29
SSL 通信チャネルのイネーブル化 4-29
SSL 証明書の再生成 4-31
SSH 通信チャネルの設定 4-32
SSH2 通信チャネルのイネーブル化 4-33
SSH2 通信チャネル鍵の再生成 4-33
通信チャネルの確立 4-34
SSH 鍵の管理 4-38
SSH 鍵の追加 4-38
SSH 鍵の削除 4-39
SFTP 接続および SCP 接続用の鍵の設定 4-40
ホスト名の変更 4-42
SNMP トラップのイネーブル化 4-43
SNMP コミュニティ ストリングの設定 4-50
ログイン バナーの設定 4-51
CLI からのログイン バナーの設定 4-51
ログイン バナーのインポート 4-52

ログイン バナーの削除 4-53
Web-Based Manager ロゴの設定 4-54
WBM ロゴのインポート 4-54
WBM ロゴの削除 4-55
セッション タイムアウトの設定 4-56

CHAPTER 5 ゾーンの設定 5-1
ゾーンについて 5-2
ゾーン テンプレートの使用 5-3
新しいゾーンの作成 5-6
ゾーン テンプレートからの新しいゾーンの作成 5-7
既存のゾーンの複製による新しいゾーンの作成 5-9
ゾーンのアトリビュートの設定 5-11
ゾーンの IP アドレス範囲の設定 5-13
Detector モジュールの Guard とのゾーン設定の同期 5-15
設定のガイドライン 5-16
同期用のゾーンの設定 5-17
ゾーンの自動的な同期とエクスポート パラメータの設定 5-19
ゾーン設定の自動的な同期 5-20
Guard から Detector モジュールへのゾーン設定の同期 5-21
Detector モジュールから Guard へのゾーン設定の同期 5-23
ゾーン設定のオフラインでの同期 5-24
ゾーン設定の自動エクスポート 5-26
ゾーン設定の手動エクスポート 5-28
サンプル シナリオ 5-31

CHAPTER 6 **ゾーンのフィルタの設定** 6-1
ゾーン フィルタについて 6-2
フレックスコンテンツ フィルタの設定 6-4
フレックスコンテンツ フィルタの追加 6-5
tcpdump 式の構文の設定 6-9
パターン式構文の設定 6-13
フレックスコンテンツ フィルタの表示 6-14
フレックスコンテンツ フィルタの削除 6-15
フレックスコンテンツ フィルタの状態の変更 6-16
バイパス フィルタの設定 6-18
バイパス フィルタの追加 6-18
バイパス フィルタの表示 6-20
バイパス フィルタの削除 6-21
動的フィルタの設定 6-22
動的フィルタの表示 6-22
動的フィルタの追加 6-25
動的フィルタの削除 6-27
動的フィルタの作成防止 6-28

CHAPTER 7 **ポリシー テンプレートとポリシーの設定** 7-1
ゾーン ポリシーについて 7-2
ポリシー パスの使用 7-2
ポリシーの作成 7-4
ポリシー テンプレートについて 7-5
各種ポリシー テンプレートのタイプについて 7-5
ポリシー テンプレート パラメータの設定 7-8
サービスの最大数の設定 7-10

最小しきい値の設定 7-11
ポリシー テンプレートの状態の設定 7-12
すべてのポリシー テンプレート パラメータの同時設定 7-12
ポリシー パスのセクションについて 7-14
ポリシー テンプレート 7-14
サービス 7-14
サービスの追加 7-15
サービスの削除 7-16
検出レベル 7-18
パケット タイプ 7-18
トラフィック特性 7-19
ポリシー パラメータの設定 7-21
ポリシーの状態の変更 7-22
ポリシーのしきい値の設定 7-24
ポリシーのしきい値の設定 7-25
固定値としてのしきい値の設定 7-25
しきい値の乗数の設定 7-26
係数によるしきい値の乗算 7-28
特定の IP しきい値の設定 7-29
ポリシーのタイムアウトの設定 7-30
ポリシーのアクションの設定 7-31
ポリシーのインタラクティブ ステータスの設定 7-32
ワーム ポリシーについて 7-34
ワーム ポリシーの設定 7-35
ワーム攻撃の識別 7-37
ポリシーの監視 7-39

ポリシーの表示 7-39
ポリシーの統計情報の表示 7-41
ポリシー設定のバックアップ 7-44

CHAPTER 8 ゾーン トラフィックの特性のラーニング 8-1
ラーニング プロセスについて 8-2
ラーニング プロセスのフェーズについて 8-3
ラーニング プロセスの結果の確認 8-4
検出およびラーニング機能について 8-4
ゾーンのラーニング プロセスの結果と Cisco Anomaly Guard Module の同期 8-5
ポリシーの構築 8-6
ポリシーしきい値の調整 8-10
ラーニング パラメータの設定 8-15
定期的なアクションの設定 8-15
しきい値選択方式の設定 8-17
ポリシーに対する調整済みのマーク付け 8-18
ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行 8-20
スナップショットを使用したラーニング プロセスの結果の確認 8-22
スナップショットの作成 8-23
ラーニングの結果の比較 8-24
スナップショットの比較 8-25
ゾーンの比較 8-26
スナップショットの表示 8-26
スナップショットの削除 8-28
ゾーン設定へのポリシーのコピー 8-28

ゾーン ポリシーのバックアップ 8-30

CHAPTER 9 ゾーンのトラフィックの異常の検出 9-1

ゾーン異常検出について 9-2

Detector モジュールがゾーン異常検出を行う方法の設定 9-4

Guard 保護のアクティベーション方式の設定 9-5

ゾーン異常検出のアクティブ化 9-7

ゾーン異常検出の非アクティブ化 9-7

ゾーンを保護するためのリモート Guard のアクティブ化 9-8

リモート Guard リストを使用したリモート Guard のアクティブ化 9-8

リモート Guard のアクティブ化およびゾーン設定の同期 9-10

デフォルトのリモート Guard リストの設定 9-12

ゾーンのリモート Guard リストの設定 9-13

リモート Guard のオフラインでのアクティブ化 9-13

手動でのリモート Guard のアクティブ化 9-14

CHAPTER 10 インタラクティブ検出モードの使用方法 10-1

インタラクティブ検出モードについて 10-2

インタラクティブ検出モードのアクティブ化 10-4

インタラクティブ検出モードのゾーンの設定 10-6

推奨事項の表示 10-7

推奨事項の管理 10-10

インタラクティブ検出モードの非アクティブ化 10-13

CHAPTER 11 攻撃レポートの使用方法 11-1

レポートのレイアウトについて 11-2

General Details 11-2
Attack Statistics 11-3
Detected Anomalies 11-3
レポートのパラメータについて 11-5
攻撃レポートの表示 11-7
攻撃レポートのエクスポート 11-11
攻撃レポートの自動エクスポート 11-11
すべてのゾーンの攻撃レポートのエクスポート 11-12
ゾーン レポートのエクスポート 11-13
攻撃レポートの削除 11-16

CHAPTER 12 Detector モジュールの診断ツールの使用 12-1
インストールされているソフトウェア バージョン番号とライセンス契約の表示 12-3
ソフトウェア ライセンス キー情報の表示 12-4
Detector モジュールの設定の表示 12-5
Detector モジュールのゾーンの表示 12-7
カウンタを使用したトラフィックの分析 12-8
カウンタおよびトラフィック レートの平均の表示 12-8
Detector モジュールおよびゾーンのカウンタのクリア 12-10
ゾーンのステータスの表示 12-11
Detector モジュールのログ管理 12-12
オンライン イベント ログの管理 12-13
オンライン イベント ログの表示 12-13
オンライン イベント ログのエクスポート 12-13
ログ ファイルの管理 12-15
ログ ファイルの表示 12-16

ログ ファイルのエクスポート 12-16
ログ ファイルのクリア 12-18
ネットワーク トラフィックの監視と攻撃シグニチャの抽出 12-19
Detector モジュールの自動トラフィック記録の設定 12-20
Detector モジュールの手動トラフィック記録のアクティブ化 12-23
Detector モジュールの手動トラフィック記録の停止 12-25
手動パケットダンプ設定の表示 12-26
パケットダンプ キャプチャ ファイルの自動エクスポート 12-26
パケットダンプ キャプチャ ファイルの手動エクスポート 12-27
パケットダンプ キャプチャ ファイルのインポート 12-29
パケットダンプ キャプチャ ファイルの表示 12-32
パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成 12-33
パケットダンプ キャプチャ ファイルのコピー 12-36
パケットダンプ キャプチャ ファイルの削除 12-38
一般的な診断データの表示 12-39
フラッシュ メモリの使用率の表示 12-40
メモリ消費量の表示 12-41
CPU 使用率の表示 12-42
システム リソースの監視 12-43
ARP キャッシュの管理 12-46
ネットワーク統計情報の表示 12-47
traceroute の使用 12-51
接続の確認 12-53

デバッグ情報の取得 12-55

CHAPTER 13 メンテナンス タスクの実行 13-1

ファイル サーバの設定 13-2

設定のエクスポート 13-4

設定のインポートとアップデート 13-7

ファイルを自動的にエクスポートする方法 13-10

Detector モジュールのリロード 13-13

Detector モジュールのリブートおよびゾーンの非アクティブ化 13-13

Detector モジュール ソフトウェアのアップグレード 13-14

Supervisor Engine 2 または Supervisor Engine 720 の Cisco IOS ソフトウェア 13-14

Detector モジュール ソフトウェア 13-14

アップグレード操作に関する注釈 13-16

AP イメージのアップグレード 13-17

MP イメージのアップグレード 13-21

AP および MP イメージのインライン アップグレード 13-24

Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け 13-28

1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード 13-30

2 Gbps 動作用 XG ソフトウェア イメージの取得とインストール 13-31

XG ソフトウェア イメージ ライセンス キーの取得とインストール 13-31

2 Gbps 動作用追加データ ポートのアクティブ化 13-33

2 Gbps 動作用 SSL 証明書の再生成 13-33

MP 関連のコマンドの使用 13-34
忘失パスワードの復旧 13-36
工場出荷時のデフォルト設定へのリセット 13-37

INDEX 索引

このマニュアルについて

このマニュアルでは、Cisco Traffic Anomaly Detector Module（Detector モジュール）とその機能、および管理作業の実行方法について説明します。

ここでは、このマニュアルの対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

この章は、次の項で構成されてます。

- 対象読者
- このガイドの使用方法
- 記号および表記法
- 技術情報の入手方法
- シスコ製品のセキュリティの概要
- Product Alerts および Field Notices
- テクニカル サポート
- その他の資料および情報の入手方法

対象読者

『*Cisco Traffic Anomaly Detector Module コンフィギュレーション ガイド*』は、次の読者を主対象としています。

- ネットワーク管理者
- エンジニア
- オペレータ
- ネットワーク セキュリティの専門家

このマニュアルでは、ネットワーキングおよびネットワーク セキュリティに関する幅広い知識を前提としています。

このガイドの使用方法

このマニュアルは、次の章で構成されています。

章番号	説明
第 1 章「製品概要」	Cisco Traffic Anomaly Detector Module（Detector モジュール）の概要を説明し、Detector モジュールの動作状態およびコンポーネントについて概説します。
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」	Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータに Detector モジュールを設定する方法について説明します。
第 3 章「Detector モジュールの初期化」	Detector モジュールを接続し、設定するために必要な最初の手順について説明します。また、Detector モジュールの CLI 環境および認証方法を概説します。
第 4 章「Detector の設定」	Detector モジュールのサービスとアクセス コントロールを設定する方法について説明します。
第 5 章「ゾーンの設定」	ゾーンの作成方法および管理方法について説明します。
第 6 章「ゾーンのフィルタの設定」	ゾーン フィルタおよびフィルタを設定する方法について説明します。
第 7 章「ポリシー テンプレートとポリシーの設定」	ゾーンのポリシー、ポリシー テンプレートおよびこれらを設定する方法について説明します。
第 8 章「ゾーン トラフィックの特性のラーニング」	ラーニング プロセス、およびラーニング プロセスを使用して Detector モジュールがゾーン異常検出に使用するポリシーを構築および微調整する方法について説明します。
第 9 章「ゾーンのトラフィックの異常の検出」	ゾーン トラフィックの異常を検出し、Cisco Anomaly Guard Module をアクティブにして、ゾーンを保護する Detector モジュールの設定とアクティブにする方法について説明します。

章番号	説明
第 10 章「インタラクティブ検出モードの使用方法」	インタラクティブ検出モードおよび推奨事項、ユーザの決定に関するオプション、ポリシーのインタラクティブ ステータスについて説明します。
第 11 章「攻撃レポートの使用方法」	攻撃レポート、レポートの構成、およびオプションの表示について説明します。
第 12 章「Detector モジュールの診断ツールの使用」	Detector モジュールの診断ツールについて説明します。
第 13 章「メンテナンス タスクの実行」	Detector モジュールのメンテナンスに必要な作業を実施する方法について説明します。

記号および表記法

このマニュアルは、次の表記法を使用しています。

スタイルまたは記号	説明
太字	記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
`Screen` フォント	プロンプトなどの画面の表示、および Detector が画面に表示する情報は、`Screen` フォントで示しています。screen フォントの内容をコマンドの一部として入力しないでください。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで示しています。
[**x** | y]	どれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{**x** | y}	必ずどれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。必ずしもどれか 1 つを選択する必要はありません。選択する場合は、指定された選択肢の中から選びます。

このマニュアルでは、例としてゾーン名に *scannet*、プロンプトに *user@DETECTOR-conf-zone-scannet#* を使用しています。

このマニュアルでは、さまざまな種類の情報を区別するために次の記号と表記法を使用しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント *ここに記載されている情報が、問題の解決に役立つことを意味します。*ヒントの情報はトラブルシューティングや対策にはなりませんが、情報として役立てることができます。

ワンポイント・アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。ここでは、シスコが提供する製品マニュアル リソースについて説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

各国のシスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納したライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関するマニュアルにアクセスすることができます。また、この DVD を使用すると、次の URL のシスコの Web サイトに掲載されている HTML マニュアルおよび PDF ファイルにアクセスすることができます。

http://www.cisco.com/univercd/home/home.htm

Product Documentation DVD は、定期的に作成およびリリースされています。DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store から Product Documentation DVD（Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

マニュアルの発注方法（英語版）

Cisco Marketplace にアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザの場合、Product Documentation Store からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ関連の注意事項および回答の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 9.*x* を使用して暗号化された情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に PSIRT に問い合せ、他のデータ暗号化方法を確認してください。

Product Alerts および Field Notices

シスコ製品に対する変更やアップデートは、Cisco Product Alerts および Cisco Field Notices で通知されます。Cisco.com のプロダクト アラート ツールを使用すると、これらの通知を受け取ることができます。このツールを使用すれば、プロファイルを作成して、情報を受け取る製品を選択できます。

プロダクト アラート ツールにアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザは、次の URL でこのツールを使用できます。

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Cisco.com にユーザ登録するには、次の URL にアクセスします。

http://tools.cisco.com/RPF/register/register.do

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Support Web サイト

Cisco Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/en/US/support/index.html

Cisco Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） オンラインまたは電話でサービス リクエストを発行する前に、**Cisco Product Identification Tool** を使用して製品のシリアル番号を確認してください。Cisco Support Web サイトでこのツールを使用するには、**Get Tools & Resources** リンクをクリックし、**All Tools (A-Z)** タブをクリックした後、アルファベット順のリストから **Cisco Product Identification Tool** を選択します。このツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

ヒント **Cisco.com での表示および検索**

ブラウザが Web ページをリフレッシュしていないと思われる場合は、Ctrl キーを押したまま **F5** を押すことで強制的にブラウザに Web ページを更新させます。

技術情報を検索する場合は、Cisco.com の Web サイト全体ではなく、技術マニュアルに検索対象を絞り込みます。Cisco.com のホームページで Search ボックスを使用した後、表示されたページで Search ボックスの隣の **Advanced Search** リンクをクリックし、**Technical Support & Documentation** オプション ボタンをオンにします。

Cisco.com の Web サイトまたは特定の技術マニュアルに関するフィードバックを送るには、Cisco.com のすべての Web ページの下部にある **Contacts & Feedback** をクリックします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Online Subscription Center は、シスコのさまざまな E メール ニュースレターやその他の通信に登録できる Web サイトです。プロファイルを作成し、受信を希望する情報を選択してください。Cisco Online Subscription Center には、次の URL からアクセスできます。

  http://www.cisco.com/offer/subscribe

- 『*Cisco Product Quick Reference Guide*』は手軽でコンパクトな参照ツールです。チャネル パートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコの最新チャネル製品情報が収録されます。『*Cisco Product Quick Reference Guide*』の注文方法および詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコが提供するネットワーキング製品、および各種のカスタマー　サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- 「What's New in Cisco Documentation」は、シスコ製品の最新のマニュアル リリースに関する情報を提供するオンライン出版物です。このオンライン出版物は毎月更新され、製品カテゴリ別に編成されているため、製品のマニュアルを簡単に検索できます。次の URL で「What's New in Cisco Documentation」の最新リリースを見ることができます。

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

製品概要

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）の概要、コンポーネント、および動作のしくみ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。

- Cisco Traffic Anomaly Detector Module について
- DDos について
- ゾーンについて
- Detector モジュールの動作のしくみについて
- 異常検出プロセスについて
- 1 Gbps および 2 Gbps 帯域幅オプションについて

Cisco Traffic Anomaly Detector Module について

Detector モジュールは、Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃の兆候がないかを継続的に調べる受動的な監視デバイスで、監視の対象となるのは、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対象の宛先（ゾーンとして参照される）です。Detector モジュールは、Cisco Anomaly Guard モジュールまたはアプライアンス（Guard）との併用に最も適していますが、単独でも DDoS 検出および警告コンポーネントとして運用できます。

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

ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡す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、保護対象ゾーン（複数も可）を宛先とするすべての着信トラフィックのコピーを分析して、現在のトラフィックと動作のしきい値のセット（ゾーン ポリシー）とを比較し、異常なトラフィックの動作を検出します。Detector モジュールが潜在的な攻撃と見なされる異常な動作を見つけると、Detector モジュールは、Detector モジュールをアクティブにしてこれらの攻撃を軽減することができます。

Detector モジュールでは、次の機能を使用してトラフィックを監視します。

- ゾーンのトラフィックをラーニングし、その特性に合せて自身をチューニングし、Detector モジュールにしきい値とポリシーに基づいた参照とインストラクションを提供する、アルゴリズム ベースのシステム。
- Detector モジュールをリモートでアクティブにしてゾーン（複数も可）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ことにより、Detector モジュールは、バックグラウンドに控えた状態で検出の役割を果たすことができます。

DDos について

DDoS 攻撃は、正当なユーザが特定のコンピュータまたはネットワーク リソースにアクセスできないようにします。このような攻撃は、個人が悪意のある要求をターゲットに送信してネットワーク サービスの質を低下させ、サーバやネットワーク デバイスのネットワーク サービスを妨害し、不要なトラフィックでネットワーク リンクを飽和状態にすることで発生します。

DDoS 攻撃は、悪意のあるユーザがインターネット上で数百、数千台ものホスト（ゾンビ）を操作し、トロイの木馬を仕掛けることにより発生します。トロイの木馬とは、無害なアプリケーションを装った複製しないプログラムで、ユーザが予想もしない有害なアクションを起こすものです。トロイの木馬は、攻撃者により、いつ、どのように組織的攻撃を開始するかの指示をマスター サーバ コントローラから受けます。ゾンビは、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によって使用不能にする自動化スクリプトを実行します。このような攻撃には、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低下させようとしたりするものなどがあります。多くの場合、ゾンビは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。このような分散攻撃は、一般的なゾーンで使用される低い帯域幅では処理できない大量のトラフィックを発生させます。ゾーンの詳細については、P.1-4 の「ゾーンについて」を参照してください。

ゾーンについて

ゾーンは、次のいずれかの要素です。

- ネットワーク サーバ、クライアント、またはルータ
- 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）
- 上記の要素の任意の組み合せ

Detector モジュールは、DDoS 攻撃を発見すると、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、手動で Guard をアクティブにするようにユーザに通知することができます。

Detector モジュールでは、ゾーンのネットワーク アドレス範囲が互いに重複していない場合に複数のゾーンのトラフィックを同時に分析できます。

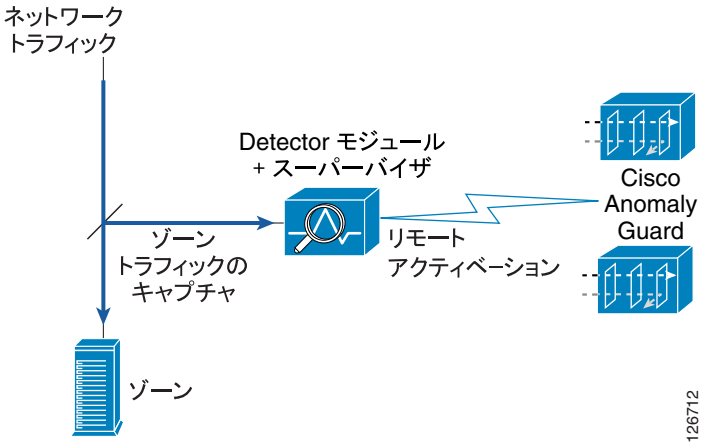
ゾーンを定義するときに、Detector モジュールがゾーンの異常検出に使用するネットワーク アドレスとポリシーを設定します。ゾーンに名前を割り当てて、この名前を使用してゾーンを参照します。

Detector モジュールの動作のしくみについて

Detector モジュールは、近づく DDoS 攻撃の新たな兆候がないか、トラフィックを分析します。トラフィックの異常を検出すると、Detector モジュールはそのイベントを自身の syslog に記録するか、自身と関連付けられた Guard をアクティブにします。Guard は、新たに発生する DDoS 攻撃を軽減してゾーンを保護します。図 1-1 に、検出の動作を示します。

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

図 1-1　Cisco Traffic Anomaly Detector Module の動作



Detector モジュールは、ゾーン トラフィックの特性をラーニングしてゾーン トラフィックの比較基準とし、悪意のある攻撃になりうるあらゆる異常をトレースします。

この項では、次のトピックについて取り上げます。

- ラーニング プロセスについて
- ゾーン ポリシーについて
- Detector モジュールによるゾーン異常検出のしくみについて
- 検出およびラーニング機能について
- 攻撃レポートについて

ラーニング プロセスについて

ラーニング プロセスを使用すると、Detector モジュールが、通常のゾーン トラフィック パターンを解析して、ゾーンでのトラフィックの異常や攻撃を検出するためのポリシーを作成できるようになります。

ラーニング プロセスは、次の 2 つのフェーズで構成されています。

- ポリシー構築フェーズ：Detector モジュールがゾーン ポリシーを作成します。ポリシー テンプレートは、Detector モジュールがゾーン ポリシーの構築に使用する規則を提供します。トラフィックが透過的に Detector モジュールを通過することにより、ゾーンが使用する主なサービスを検出できます。
- しきい値調整フェーズ：Detector モジュールがゾーン サービスのトラフィック レートに合せてゾーン ポリシーを調整します。トラフィックが透過的に Detector モジュールを通過することにより、Detector モジュールはポリシー構築フェーズ中に検出されたサービスのしきい値を調整できます。

ゾーン ポリシーについて

ゾーン ポリシーは Detector モジュールの構成要素で、悪意のあるものになりうる異常をトレースするために、Detector モジュールがゾーン トラフィックを比較する基準になります。トラフィック フローがポリシーしきい値を超えると、Detector モジュールはこれを異常または悪意のあるトラフィックとして認識し、フィルタ セット（動的フィルタ）を動的に設定し、攻撃の重大度に応じて適切な検出レベルをこのトラフィック フローに適用します。

トラフィックのラーニングの詳細については、第 5 章「ゾーンの設定」を参照してください。ゾーン ポリシーの詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

Detector モジュールによるゾーン異常検出のしくみについて

Detector モジュールの保護は、次の方法でアクティブにできます。

- 自動保護モード：Detector モジュールが、作成した動的フィルタを自動的にアクティブにします。
- インタラクティブ保護モード：Detector モジュールが、作成した動的フィルタのキューを作成し、それらのフィルタを推奨されるアクションとしてグループ化します。ユーザは、これらの推奨事項を確認して、推奨事項を受け入れるか、無視するか、自動アクティベーションに切り替えるかを決定します。

詳細については、第 10 章「インタラクティブ検出モードの使用方法」を参照してください。

検出およびラーニング機能について

しきい値調整フェーズとゾーン検出を同時にアクティブにして（検出およびラーニング機能）、Detector モジュールがゾーン ポリシーのしきい値をラーニングすると同時に、ゾーン ポリシーのしきい値でトラフィックの異常がないかを監視するようにできます。Detector モジュールは、攻撃を検出するとラーニング プロセスを停止しますが、ゾーン検出は継続します。このプロセスにより、Detector モジュールでは悪意のあるトラフィックのしきい値がラーニングされなくなります。攻撃が終了すると、Detector モジュールはラーニング プロセスを再開します。詳細については、P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

攻撃レポートについて

Detector モジュールはゾーンごとの攻撃レポートを提供し、ゾーン ステータスが表示できるようになっています。攻撃レポートでは、最初の動的フィルタの生成から保護の終了まで、攻撃の詳細な情報が提供されます。詳細については、第 11 章「攻撃レポートの使用方法」を参照してください。

異常検出プロセスについて

Detector モジュールは、ゾーンのトラフィックを必要な検出レベルに誘導するために、3 種類のフィルタを使用します。これらのフィルタを設定して、Detector モジュールがトラフィックの異常検出で使用する、トラフィックの方向や機能をカスタマイズすることができます。

Detector モジュールでは、次のタイプのフィルタが使用されます。

- バイパス フィルタ：Detector モジュールが特定のトラフィック フローを処理しないようにします。
- フレックスコンテンツ フィルタ：指定されたパケット フローをカウントします。フレックスコンテンツ フィルタには、IP ヘッダーと TCP ヘッダー内のフィールドに応じたフィルタリングや、コンテンツ バイト数に応じたフィルタリングなど、非常に柔軟なフィルタリング機能があります。
- 動的フィルタ：分析検出レベルをトラフィック フローに適用します。Detector モジュールは、トラフィック フローの分析結果として動的フィルタを作成します。動的フィルタは、Detector モジュールの syslog にイベントを記録するか、ゾーンを保護するために Guard をアクティブにします。動的フィルタは有効期間が限定されており、攻撃が終了すると削除されます。

Detector モジュールは、トラフィックの統計分析を行って、ポリシー（これによって異常がないかゾーン トラフィックを監視する）とフィルタ システムとの間の調整を行います。

1 Gbps および 2 Gbps 帯域幅オプションについて

Detector モジュールは、1 ギガビット / 秒（Gbps）と 2 Gbps という 2 つの帯域幅パフォーマンス レベルで動作できます。Detector モジュールにロードされるソフトウェア イメージが、モジュールとスーパーバイザ エンジンの間にある 3 つの物理インターフェイスを Detector モジュールが使用する方法を制御して、動作帯域幅を決めます。インストールされたソフトウェア イメージは、次の方法でインターフェイスを制御します。

- 6.0 ソフトウェア イメージ：このソフトウェア イメージのスループットは 1 Gbps で、1 つのインターフェイス ポートを介して、データ トラフィックをスーパーバイザ エンジンと Detector モジュール間で移動できます。2 番目のインターフェイス ポートは、アウトオブバンド管理トラフィックを転送し、関連付けられている Guard デバイスをアクティブにする場合に使用します。3 番目のインターフェイス ポートは使用されません。
- 6.0-XG ソフトウェア イメージ：このソフトウェア イメージのスループットは 2 Gbps で、データ トラフィックを転送するためのインターフェイス ポートのうち、2 つをイネーブルにします。3 番目のインターフェイスは、アウトオブバンド管理トラフィックの転送と Guard デバイスのアクティブ化のための専用インターフェイスです。XG ソフトウェア イメージを使用するには、Detector モジュールにソフトウェア ライセンスが必要です。

（注） ソフトウェア イメージがインストールされている Detector モジュールを注文することも、6.0 ソフトウェア イメージ（1 Gbps 動作）を 6.0-XG ソフトウェア イメージ（2 Gbps 動作）にアップグレードすることもできます。6.0-XG ソフトウェア イメージが事前にインストールされている Detector モジュールを注文する場合には、Detector モジュールをセットアップするときにライセンスをインストールする必要があります（P.13-30 の「1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード」を参照）。

表 1-1 に、Detector モジュールの物理インターフェイスとスーパーバイザ ポート間の相関を示します。この表では、2 Gbps 動作用のソフトウェア イメージをインストールした後にデータ トラフィック変更用の CLI インターフェイス指定子がどのように変更されるかも示します。

表 1-1　スーパーバイザ エンジン ポートと相関する Detector モジュール インターフェイス

スーパーバイザ エンジン ポート	Detector モジュール 1 Gbps 動作		Detector モジュール 2 Gbps 動作	
	インターフェイス	トラフィック タイプ	インターフェイス	トラフィック タイプ
ポート 1	giga2	データ	giga1	データ
ポート 2	不使用	-	giga2	データ
ポート 3	mng	管理および Guard のアクティベーション	mng	管理および Guard のアクティベーション

1 Gbps 動作と 2 Gbps 動作の間では、スーパーバイザ エンジンでのソース データ トラフィック VLAN の定義方法が次のように異なります。

- 1 Gbps 動作：ポート 1 でのみデータ トラフィック VLAN を定義します。
- 2 Gbps 動作：ポート 1 と 2 でデータ トラフィック VLAN を定義します。各ポートで異なる VLAN を定義します。

CHAPTER 2

スーパーバイザ エンジンでの Detector モジュールの設定

この章では、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのスーパーバイザ エンジンで Cisco Traffic Anomaly Detector Module（Detector モジュール）を設定する方法について説明します。Detector モジュールとのセッションを確立してこれを設定する前に、スーパーバイザ エンジンで Detector モジュールを設定しておく必要があります。

スーパーバイザ エンジンで Detector モジュールを設定するには、EXEC 特権を持っており、設定モードである必要があります。

フラッシュ メモリへの設定変更をすべて保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

(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。

- Detector モジュールの設置確認

- Detector モジュール管理の設定
- トラフィックをキャプチャするためのトラフィックの送信元の設定
- Detector モジュールとのセッションの確立
- Detector モジュールのリブート
- Detector モジュールの設定の確認

Detector モジュールの設置確認

スーパーバイザ エンジンが新しい Detector モジュールを認識してオンラインにしたことを確認します。

（注） Catalyst 6500 シリーズ スイッチに Detector モジュールを設置する方法については、『*Cisco Anomaly Guard Module and Traffic Anomaly Detector Module Installation Note*』を参照してください。

設置を確認するには、次の手順を実行します。

ステップ 1　スーパーバイザ エンジン コンソールにログインします。

ステップ 2　Detector モジュールがオンラインであることを確認します。次のコマンドを入力します。

```
show module
```

次の例は、**show module** コマンドの出力を示しています。

```
Sup# show module
Mod  Ports CardTypeModelSerial No.
--   ---- --------------------------------------------------
1    2   Catalyst 6000 supervisor 2(Active)WS-X6K-SUP2-2GESAL081230TJ
... ...
6    3   Anomaly Detector module ModuleWS-SVC-adm-1-K9SAD081000GG
...
Mod MAC addressesHwFwSwStatus
--- ------------------------------------ ------- ----------- -------
...
6   000e.847f.fe04 to 000e.847f.fe0b1.07.2(1)6.0(0.10)Ok
...
Sup
#
```

（注） Detector モジュールが初めてインストールされたときは、通常、ステータスは「other」です。Detector モジュールが診断ルーチンを完了してオンラインになると、ステータスは「OK」になります。Detector モジュールがオンラインになるまでは少なくとも 5 分間はかかります。

Detector モジュール管理の設定

Detector モジュールとのリモート管理セッションを確立するには、Detector モジュールの管理ポートを設定します。

管理のために VLAN を選択するには、次のコマンドを使用します。

anomaly-detector module *module_number* **management-port access-vlan** *vlan_number*

表 2-1 で、**anomaly-detector module** コマンドの引数とキーワードについて説明します。

表 2-1　anomaly-detector module コマンドの引数とキーワード

パラメータ	説明
module_number	モジュールをシャーシに挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
management-port	スーパーバイザ エンジンと Detector モジュール間で管理トラフィックを転送するポートを指定します。
access-vlan *vlan_number*	管理に使用する VLAN ID を指定します。デフォルトは VLAN 1 です。

現在の管理ポート設定を参照するには、**show anomaly-detector module** コマンドを使用します（P.2-20 の「Detector モジュールの設定の確認」を参照）。

次の例は、シャーシの番号 *4* のスロットに挿入されたモジュールについて、管理のために VLAN *5* を選択する方法を示しています。

```
Sup(config)# anomaly-detector module 4 management-port access-vlan 5
```

Detector モジュールとのリモート管理セッションを確立するには、Detector モジュールで、次のような設定も必要になります。

- Detector モジュールの管理ポート インターフェイスを設定する。P.3-11 の「物理インターフェイスの設定」を参照してください。
- 関連するサービスをイネーブルにする。P.3-17 の「Detector モジュールの管理」を参照してください。

トラフィックをキャプチャするためのトラフィックの送信元の設定

ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡す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、自身を通過するネットワーク トラフィックを分析し、そのトラフィックを監視して、進化し続ける攻撃パターンがないか調べます。

次のいずれかの方法を使用して、ネットワーク トラフィックを Detector モジュールに渡すことができます。

- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）：1 つまたは複数の送信元ポートで受信、送信、または送受信されたトラフィックを分析のために宛先ポートにキャプチャします。Detector モジュールは、SPAN セッション用に 1 つの宛先ポートを提供します。詳細については、P.2-12 の「SPAN の設定」を参照してください。
- VLAN access list（VACL; VLAN アクセスリスト）：WAN インターフェイスまたは VLAN から Detector モジュールのデータ ポートにトラフィックを転送します。この方法は、同じ目的での SPAN の使用に代わるものです。1 つの VLAN または複数の VLAN からのトラフィックをキャプチャするように VACL を設定できます。詳細については、P.2-7 の「VACL の設定」を参照してください。

SPAN の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』または『*Cisco 7600 Series Router Software Configuration Guide*』の「Configuring SPAN and RSPAN」を参照してください。

VACL の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』または『*Cisco 7600 Series Router Software Configuration Guide*』の「Configuring VLAN ACLs」を参照してください。

Detector モジュールで監視するために、1 つの VLAN または複数の VLAN からのトラフィックをキャプチャできます。特定の VLAN からのトラフィックだけを監視する場合は、監視しない VLAN をキャプチャ機能から消去する必要があります。

この項では、次のトピックについて取り上げます。

- VACL の設定
- SPAN の設定

VACL の設定

1 つの VLAN または複数の VLAN からの Detector モジュール用トラフィックをキャプチャするように VACL を設定できます。

（注） この項の手順は、VLAN 上の Detector モジュール用トラフィックをキャプチャするように VACL を設定するための基本情報です。詳細については、該当する Catalyst 6500 シリーズ スイッチまたは 7600 シリーズ ルータの設定ガイドを参照してください。

VLAN 上の Detector モジュール用トラフィックをキャプチャするように VACL を設定するには、次の手順を実行します。

ステップ 1　access control list（ACL; アクセス コントロール リスト）を定義し、次のコマンドを入力して、permit 文および deny 文（あるいはそのいずれか）によって access-control entry（ACE; アクセスコントロール エントリ）を追加します。

```
ip access-list {standard | extended} acl-name
```

表 2-2 で、**ip access-list** コマンドの引数とキーワードについて説明します。

表 2-2　ip access-list コマンドの引数とキーワード

パラメータ	説明
standard	標準の IP アクセスリストを指定します。
extended	拡張 IP アクセスリストを指定します。
acl-name	ACL の名前。名前には、スペースも疑問符も使用できません。また、番号付きアクセスリストと明確に区別するために、名前はアルファベット文字で始める必要があります。

（注） 代わりに、**access-list** コマンドを使用することもできます。

ステップ 2　次のコマンドを入力して、VLAN アクセス マップを定義します。

```
vlan access-map map_name [0-65535]
```

map_name 引数には、アクセス マップの名前タグを指定します。シーケンス番号を指定できます。シーケンス番号を指定しない場合は、番号が自動的に割り当てられます。このコマンドを実行すると、VLAN アクセス マップ設定モードに入ります。

マップ シーケンスごとに 1 つの match 句と 1 つの action 句を入力できます。

ステップ 3　次のコマンドを入力して、VLAN アクセス マップ シーケンスに match 句を設定します。

```
match ip address {acl_number | acl_name}
```

表 2-3 で、**match ip address** コマンドの引数とキーワードについて説明します。

表 2-3　match ip address コマンドの引数

パラメータ	説明
acl_number	VLAN アクセス マップ シーケンス用の 1 つまたは複数の IP ACL。有効な値は、1 ～ 199 および 1300 ～ 2699 です。
acl_name	IP ACL 名。

ステップ 4　次のコマンドを入力して、ネットワーク トラフィックを転送するように、VLAN アクセス マップ シーケンスに action 句を設定します。

```
action forward capture
```

ステップ 5　次のコマンドを入力して、VLAN アクセス マップを VLAN インターフェイスに適用します。

```
vlan filter map_name vlan-list vlan_list
```

表 2-4 に、**vlan filter** コマンドの引数とキーワードを示します。

表 2-4　vlan filter コマンドの引数とキーワード

パラメータ	説明
map_name	VLAN アクセス マップ タグ。
vlan-list *vlan_list*	VLAN リストを指定します。有効な値は、1 ～ 4094 です。

ステップ 6　（オプション）次のコマンドを入力して、キャプチャフラグの付いたトラフィックをキャプチャするように Detector モジュールのデータ ポートを設定します。

次のコマンドを入力します。

anomaly-detector module *slot_number* **data-port** *port_number* **capture allowed-vlan** *vlan_range*

（注）　データ ポートを指定しない場合、Detector はすべての VLAN からのトラフィックのキャプチャをイネーブルにします。

表 2-5 で、**anomaly-detector module capture** コマンドの引数とキーワードについて説明します。

表 2-5　anomaly-detector module capture コマンドの引数とキーワード

パラメータ	説明
slot_number	モジュールをシャーシに挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。

表 2-5　anomaly-detector module capture コマンドの引数とキーワード（続き）

パラメータ	説明
data-port *port_number*	データ用に使用するポートの番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1。 • 2 Gbps 動作：ポート 1 と 2。
allowed-vlan *vlan_range*	VLAN の範囲、またはカンマ区切りリストで指定するいくつかの VLAN を指定します（スペース文字を入力することはできません）。

ステップ 7　次のコマンドを入力して、Detector モジュールでキャプチャ機能をイネーブルにします。

```
anomaly-detector module module_number data-port port_number capture
```

表 2-6 で、**anomaly-detector module capture** コマンドの引数とキーワードについて説明します。

表 2-6　anomaly-detector module capture コマンドの引数とキーワード

パラメータ	説明
module_number	モジュールを挿入するためのシャーシ スロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
data-port *port_number*	データ用に使用するポートの番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1。 • 2 Gbps 動作：ポート 1 と 2。コマンドを 2 回（各ポート番号に 1 回）入力して、両方のデータ ポートでキャプチャ機能をイネーブルにする必要があります。

（注） 1 Gbps 動作の場合は、一方のデータ ポートを SPAN 宛先ポートまたはキャプチャ ポートとして設定する必要があります。2 Gbps 動作の場合は、次の方法で 2 つのデータ ポートを設定できます。

- 両方のデータ ポートを SPAN 宛先ポートとして設定
- 両方のデータ ポートをキャプチャ ポートとして設定
- 一方のデータ ポートを SPAN 宛先ポート、もう一方をキャプチャ ポートとして設定

次の 2-Gpbs 動作の例は、VLAN の Detector モジュール トラフィックをキャプチャするための VACL の設定方法を示しています。

```
Sup (config)# ip access-list extended Permit_Any
Sup (config-ext-nacl)# permit ip any any
Sup (config-ext-nacl)# exit
Sup (config)# vlan access-map Detector 10
Sup (config-access-map)# match ip address Permit_Any
Sup (config-access-map)# action forward capture
Sup (config-access-map)# exit
Sup (config)# vlan filter Detector vlan-list 921,931
Sup (config)# anomaly-detector module 6 data-port 1 capture
Sup (config)# anomaly-detector module 6 data-port 1 capture
allowed-vlan 921
Sup (config)# anomaly-detector module 6 data-port 2 capture
Sup (config)# anomaly-detector module 6 data-port 2 capture
allowed-vlan 931
```

SPAN の設定

SPAN セッションを作成し、送信元（監視される）ポートと宛先（監視する）ポートを指定します。Detector モジュールのポートを SPAN の送信元ポートとして使用することはできません。

（注） この項の手順は、SPAN セッションを作成するための基本情報です。詳細については、該当する Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの設定ガイドを参照してください。

スーパーバイザ エンジン コンソールで特権 EXEC モードから次の手順を実行し、SPAN セッションを作成して、送信元ポートと宛先ポートを指定します。

ステップ 1　次のコマンドを入力して、SPAN　セッションおよび送信元ポート（監視されるポート）を指定します。

```
monitor session session_number source interface interface-id [, | -]
[rx | tx]
```

表 2-7 で、**monitor session** コマンドの引数とキーワードについて説明します。

表 2-7　monitor session コマンドの引数とキーワード

パラメータ	説明
session_number	セッションの識別番号。
source interface *interface-id*	監視対象の送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（port-channel port-channel-number または VLAN）が含まれます。

表 2-7　monitor session コマンドの引数とキーワード（続き）

パラメータ	説明
, | -	（オプション）一連のインターフェイスまたはインターフェイス範囲。カンマの前後およびハイフンの前後にはスペースを入力します。
rx | tx	（オプション）監視対象のトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信トラフィックと受信トラフィックの両方を送信します。 **注意**　Detector モジュールは、指定されたすべての方向のトラフィックのキャプチャを受信します。rx と tx の両方を指定しないでください。パケットの 2 つのコピーが Detector モジュールのポートに転送され、Detector モジュールのパフォーマンスが低下します。 • **rx**：受信トラフィックを監視するように指定します。 • **tx**：送信トラフィックを監視するように指定します。

ステップ 2　次のコマンドを入力して、SPAN セッションおよび宛先ポート（監視するポート）を指定します。

```
monitor session SPAN_session_number destination
anomaly-detector-module module_number [data-port port]
```

表 2-8 で、**monitor session destination** コマンドの引数とキーワードについて説明します。

表 2-8　monitor session destination コマンドの引数とキーワード

パラメータ	説明
SPAN_session_number	インターフェイスの識別番号。1 と指定します。
anomaly-detector-module *module-number*	モジュールをシャーシに挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）を指定します。
data-port *port*	データのキャプチャに使用するポートの番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1。 • 2 Gbps 動作：ポート 1 と 2。コマンドを 2 回（各ポート番号に 1 回）入力して、両方のデータ ポートを宛先ポートとして指定する必要があります。

ステップ 3　次のコマンドを入力して、特権 EXEC モードに戻ります。

```
end
```

ステップ 4　次のコマンドを入力して、エントリを確認します。

```
show monitor [session session_number]
```

session_number 引数には、セッション識別番号を指定します。

次の 1 Gbps 動作の例は、SPAN セッションとしてセッション 1 を設定し、送信元ポートから宛先ポートへのトラフィックを監視する方法を示しています。受信トラフィックが送信元ポート 1 から Detector モジュールにミラーリングされます。

```
Sup(config)# monitor session 1 source interface GigabitEthernet 1/2 rx
Sup(config)# monitor session 1 destination anomaly-detector-module 4
data-port 1
```

次の 2 Gbps 動作の例は、SPAN セッションとしてセッション 1 と 2 を設定し、送信元ポートから 2 つの宛先ポートへのトラフィックを監視する方法を示しています。受信トラフィックが送信元ポート 1 と 2 から Detector モジュールのポート 1 と 2 にミラーリングされます。

```
Sup(config)# monitor session 1 source interface GigabitEthernet 1/2 rx
Sup(config)# monitor session 1 destination anomaly-detector-module 4
data-port 1
Sup(config)# monitor session 2 source interface GigabitEthernet 2/2 rx
Sup(config)# monitor session 2 destination anomaly-detector-module 4
data-port 2
```

Detector モジュールとのセッションの確立

Detector モジュールにログインするには、次の手順を実行します。

ステップ 1　Telnet セッションまたはコンソールのログ セッションを確立してスイッチにログインします。

ステップ 2　スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

```
session slot slot_number processor processor_number
```

表 2-9 で、**session slot** コマンドの引数とキーワードについて説明します。

表 2-9　session slot コマンドの引数とキーワード

パラメータ	説明
slot-number	モジュールをシャーシに挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
processor *processor_number*	Detector モジュールのプロセッサの番号を指定します。Detector モジュールは、プロセッサ 1 を介した管理だけをサポートします。

ステップ 3　次のように、Detector モジュールのログイン プロンプトでログインします。

```
login: admin
```

ステップ 4　パスワードを入力します。

Detector モジュールとのセッションを初めて確立している場合は、admin ユーザ アカウントおよび riverhead ユーザ アカウントのパスワードを選択する必要があります。パスワードは、スペースを含まず、6 ～ 24 文字の英数字にする必要があります。パスワードは、いつでも変更できます。詳細については、P.4-10 の「自分のパスワードの変更」を参照してください。

ログインに成功すると、コマンドライン プロンプトが user@DETECTOR# と表示されます。**hostname** コマンドを入力することにより、このプロンプトを変更できます。

Detector モジュールのリブート

Detector モジュールを制御するために、Cisco IOS には **boot**、**shutdown**、**power enable** および **reset** というコマンドが用意されています。

注意　スーパーバイザ エンジン プロンプトで **reload** コマンドを入力すると、シャーシ全体でリロードが発生し、そのシャーシ内のすべてのモジュールが影響を受けます。Detector モジュールをリロードする方法については、P.13-13 の「Detector モジュールのリロード」を参照してください。

- **shutdown**：オペレーティング システムを正常に停止させ、データが失われないことを保証します。Detector モジュールの破損を防ぐため、Detector モジュールを正常にシャットダウンすることが重要です。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  hw-module module *slot_number* **shutdown**

  slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

  その後、**hw-module module** *module_number* **reset** コマンドを入力して、Detector モジュールを再起動する必要があります。

  次の例は、Detector モジュールをシャットダウンする方法を示しています。

  ```
  Sup# hw-module module 8 shutdown
  ```

(注)　スイッチをリブートすると、Detector モジュールがリブートします。

- **reset**：モジュールをリセットします。このコマンドを使用して、シャットダウンからの復旧や、次の Detector モジュール動作イメージの切り替えを行います。
  - アプリケーション パーティション（AP）：Detector モジュール アプリケーション ソフトウェア イメージ（P.13-14 の「Detector モジュール ソフトウェアのアップグレード」を参照）。
  - メンテナンス パーティション（MP）：基本モジュールの初期化およびドーター カードの制御の機能のために必要なソフトウェア イメージ（P.13-14 の「Detector モジュール ソフトウェアのアップグレード」を参照）。

  hw-module reset コマンドは、モジュールの電源をいったん切った後で入れ、モジュールをリセットします。リセット プロセスには数分かかります。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  hw-module module *slot_number* reset [*string*]

  slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。*string* 引数は PC ブート シーケンス用のオプションの文字列です。MP にリセットするには **cf:1** を、AP にリセットするには **cf:4** を入力します。詳細については、P.13-14 の「Detector モジュール ソフトウェアのアップグレード」を参照してください。

  次の例は、Detector モジュールをリセットする方法を示しています。

  ```
  Sup# hw-module module 8 reset
  ```

- **no power enable**：モジュールをシャットダウンし、シャーシから安全に取り外すことができるようにします。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  no power enable module *slot_number*

  slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

  モジュールをもう一度オンにするには、次のコマンドを使用します。

  power enable module *slot_number*

  次の例は、Detector モジュールをシャットダウンする方法を示しています。

  ```
  Sup (config)# no power enable module 8
  ```

- **boot**：次回電源投入時に Detector モジュールを強制的に MP にブートさせます。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  boot device module *slot_number* cf:1

  slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

  Detector モジュールが次のブート サイクルでデフォルト パーティション（AP）にブートできるようにするには、スーパーバイザ エンジン プロンプトで次のコマンドを使用します。

  no boot device module *slot_number* cf:1

  次の例は、次のブート サイクルで Detector モジュールが AP にブートするための設定方法を示しています。

  ```
  Sup# boot device module 8 cf:1
  ```

注意　ゾーンのラーニング　フェーズは、リブート後に再起動されます。リブート後のゾーンのデフォルト動作の詳細については、P.13-13 の「Detector モジュールのリブートおよびゾーンの非アクティブ化」を参照してください。

Detector モジュールの設定の確認

スーパーバイザ エンジンで Detector モジュールの設定を確認するには、スーパーバイザ エンジン プロンプトで次のコマンドを使用します。

show anomaly-detector module *slot_number* {management-port | data-port *port_number*} [**state** | **traffic**]

表 2-10 で、**show module** コマンドの引数とキーワードについて説明します。

表 2-10　show module コマンドの引数とキーワード

パラメータ	説明
slot-number	モジュールをシャーシに挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
management-port	管理ポートの情報を指定します。
data-port *port_number*	ポート番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1 • 2 Gbps 動作：ポート 1 と 2
state	（オプション）指定のポートの設定を指定します。
traffic	（オプション）指定のポートのトラフィック統計情報を指定します。

次の例は、スーパーバイザ エンジンでの Detector モジュールの設定を表示する方法を示しています。

```
Sup# show anomaly-detector module 7 data-port 1 state
```

CHAPTER 3

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。

(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、現在ど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す。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	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。 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。 `user@DETECTOR#`
設定	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。 設定モードに入るには、グローバル モードで **configure** 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。 `user@DETECTOR-conf#`
インターフェイス設定	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。 インターフェイス設定モードに入るには、設定モードで **interface** 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。 `user@DETECTOR-conf-if-<interface-name>#`

表 3-2　Detector モジュール コマンド設定モード（続き）

モード	説明
ルータ設定	Detector モジュールのルーティング設定を設定できます。 ルータ設定モードに入るには、設定モードで **router** 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。 `router>`
ゾーン設定	ゾーンのアトリビュートを設定できます。 ゾーン設定モードに入るには、設定モードで **zone** コマンドを使用するか、グローバル モードで **configure** 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。 `user@DETECTOR-conf-zone-<zone-name>#`
ポリシー テンプレート設定	ゾーン ポリシーのテンプレートを設定できます。 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 **policy-template** 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。 `user@DETECTOR-conf-zone-<zone-name>-policy_template-<policy-template-name>#`
ポリシー設定	ゾーン ポリシーを設定できます。 ポリシー設定モードに入るには、ゾーン設定モードで **policy** 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。 `user@DETECTOR-conf-zone-<zone-name>-policy-<policy-path>#`
Guard の設定	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。 guard 設定モードに入るには、ゾーン設定モードで **guard-conf** 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。 `user@DETECTOR-conf-zone-<zone-name>(guard)#`

CLI コマンドの入力

この項では、CLI コマンドの入力規則について説明します。

- 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	**Shift** キーを押して **?**（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、**Tab** 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、**Tab** キーを 2 回押す。
more コマンドを使用してスクロールする	**more** *number-of-lines* コマンドを入力する。 **more** コマンドでは、Space 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。 *number-of-lines* 引数は、Space 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）	**Space** 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** キーを押す。
スクロール動作を中止する	**q** キーを押す。

表 3-3　CLI の規則（続き）

操作	キーボード シーケンス
文字列を前方に検索する	/（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	**?**（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 **no** 形を使用する。
現在の操作に関連する情報を表示する	**show** 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	**exit** 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	**end** 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	|（縦線）を押し、**begin** *string* 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	|（縦線）を押し、**include** *string* 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	|（縦線）を押し、**exclude** *string* 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、特定の機能をデイ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。コマンドの初め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セーブルにできます。詳細については、P.4-19 の「ゾーン名のタブ補完のディセーブル化」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、**learning policy-construction *** コマンドを入力すると、Detector モジュールで設定されているすべてのゾーンでポリシー構築フェーズがアクティブになります。

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 MTU 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　手順 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
ip-addr	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）。
ip-mask	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）。
nexthop-ip	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。

表 3-6　ip route コマンドの引数（続き）

パラメータ	説明
if-name	（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 ルーティング テーブルは、ネクストホップ IP アドレスに使用されるインターフェイスを決定します。

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.3-10 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
- MultiDevice Manager を使用した 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 を使用すると、Web ブラウザを使用して Web から Detector モジュールを管理できます。

WBM を使用して 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] | *}
```

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
ip-addr	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）。
ip-mask	（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）。
*	アスタリスク。リモート マネージャによるアクセスを許可します。

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。

Terminal Access Controller Access-Control System Plus（TACACS+）認証が設定されている場合は、ローカル データベースの代わりに TACACS+ ユーザ データベースがユーザ認証に使用されます。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。

MultiDevice Manager を使用した Detector モジュールの管理

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し、MDM による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] | *}
```

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
ip-addr	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）。
ip-mask	（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）。
*	アスタリスク。リモート ネットワークによるアクセスを許可します。

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。

TACACS+ 認証が設定されている場合は、ローカル データベースの代わりに TACACS+ ユーザ データベースがユーザ認証に使用されます。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.4-6 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.4-38 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
```

CHAPTER 4

Detector の設定

この章では、Cisco Traffic Anomaly Detector（Detector モジュール）のサービスの設定方法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。

- Detector のサービスのアクティブ化
- AAA を使用したアクセス コントロールの設定
- Guard との通信の確立
- SSH 鍵の管理
- SFTP 接続および SCP 接続用の鍵の設定
- ホスト名の変更
- SNMP トラップのイネーブル化
- SNMP コミュニティ ストリングの設定
- ログイン バナーの設定
- Web-Based Manager ロゴの設定
- セッション タイムアウトの設定

Detector のサービスのアクティブ化

Detector モジュールでアクティブにするサービスを定義することができます。正しい機能をイネーブルにするためには、サービスをイネーブルにして、そのサービスへのアクセスを許可する必要があります。Detector モジュールのサービスのアクティベーションを制御し、特定の IP アドレスに対してアクセス権を付与または拒否することにより、Detector モジュールにアクセスして制御する IP アドレスを制限することができます。

Detector モジュールは、次のサービスを提供します。

- ノード間通信サービス：Detector モジュールは、Cisco Guard との通信チャネルを確立するときにこのサービスを使用します。詳細については、P.4-28 の「Guard との通信の確立」を参照してください。
- 簡易ネットワーク管理プロトコル（SNMP）サーバ サービス：SNMP を使用して Detector モジュールにアクセスすることにより、Riverhead の専用 MIB、MIB2、および UCDavis MIB で定義された情報を取得することができます。MIB 定義の詳細については、このソフトウェア バージョンでリリースされた MIB ファイルを参照してください。

（注）　Riverhead MIB には、64 ビットのカウンタが含まれています。MIB を読み取るには、SNMP バージョン 2 をサポートするブラウザを使用する必要があります。

- SNMP トラップ サービス：snmp-trap サービスをアクティブにすると、Detector モジュールは SNMP トラップを生成します。詳細については、P.4-43 の「SNMP トラップのイネーブル化」を参照してください。
- セキュア シェル（SSH）サービス：SSH サービスは常にアクティブです。詳細については、P.3-20 の「SSH を使用した Detector モジュールへのアクセス」および P.4-38 の「SSH 鍵の管理」を参照してください。
- Web-Based Manager（WBM）サービス：Web ブラウザを使用して Web から Detector モジュールを制御できます。詳細については、P.3-17 の「Web-Based Manager を使用した Detector モジュールの管理」を参照してください。
- MultiDevice Manager（MDM）サービス：Web ブラウザを使用して、Detector モジュールなどの Guard および Detector デバイスを MDM から監視および制御できます。詳細については、P.3-19 の「MultiDevice Manager を使用した Detector モジュールの管理」を参照してください。

Detector モジュールのサービスをアクティブにするには、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、Detector モジュールのサービスをイネーブルにします。

```
service {internode-comm | mdm | snmp-server | snmp-trap | wbm}
```

表 4-1 に、**service** コマンドの引数を示します。

表 4-1　Detector サービス

サービス	説明
internode-comm	ノード間通信サービスを指定します。
mdm	MDM サービスを指定します。
snmp-server	SNMP サーバ サービスを指定します。
snmp-trap	SNMP トラップ サービスを指定します。
wbm	WBM サービスを指定します。

ステップ 2　イネーブルにするサービスに応じて、次のコマンドのいずれかを入力します。

- MDM サービスの場合は、設定モードで次のコマンドを入力して、MDM から Detector モジュールのサービス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。
- その他のサービスの場合はすべて、設定モードで次のコマンドを入力して、Detector モジュールのサービスへのアクセスを許可し、接続をイネーブルにします。

  ```
  permit {internode-comm | snmp-server | ssh | wbm}
  ip-address-general [ip-mask]
  ```

表 4-2 に、**permit** コマンドの引数を示します。

表 4-2　permit コマンドの引数

パラメータ	説明
internode-comm	ノード間通信サービスを指定します。
snmp-server	SNMP サーバ サービスを指定します。
ssh	SSH サービスを指定します。
wbm	WBM サービスを指定します。
ip-address-general	アクセスを許可する 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 192.168.10.2）。すべての IP アドレスからのアクセスを許可するには、アスタリスク（*）を使用します。
ip-mask	（オプション）IP 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）。デフォルトのサブネット マスクは、255.255.255.255 です。

注意　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する（* と入力する）ことはお勧めしません。

次の例は、WBM サービスをアクティブにする方法を示しています。

```
user@DETECTOR-conf# service wbm
user@DETECTOR-conf# permit wbm 192.168.10.35
```

AAA を使用したアクセス コントロールの設定

認証、認可、アカウンティング（AAA）とは、誰に対して Detector モジュールへのアクセスを許可するか、またアクセス後にどのサービスを許可するかを制御する方式のことです。AAA には次の機能があります。

- 認証：ユーザに対しシステムおよびシステム　サービスへのアクセスを許可する前に、そのユーザを識別します。
- 認可：ユーザがシステムへのアクセス権を取得した後で、実行が許可される内容を決定します。このプロセスは、ユーザ認証後に発生します。
- アカウンティング：ユーザが実行中または実行済みの内容を記録します。アカウンティングにより、ユーザがアクセスしているサービスを追跡することができます。

Detector モジュールには、次のシステム ユーザ アカウントがあらかじめ設定されています。

- admin：admin ユーザ アカウントには、Detector モジュールの CLI およびすべての機能にアクセスできる管理アクセス権が設定されています。Detector モジュールの CLI に初めて接続すると、このアカウントに対するパスワードを設定するように要求されます。新しいユーザ アカウントを設定するには admin ユーザ アカウントを使用します。
- riverhead：riverhead ユーザ アカウントには、ダイナミック（dynamic）のアクセス権が設定されています。Detector モジュールはこのユーザ アカウントを使用して、Guard との最初の通信チャネルを確立します。Detector モジュール CLI に初めて接続すると、このアカウントに対するパスワードを設定するように要求されます。

システム ユーザ アカウントは削除できません。

Detector モジュールのユーザ コミュニティをドメインに分割し、安全な管理アクセスのためにパスワードを割り当てることができます。初期設定が完了した後は、ユーザのアクションを監視できるように新しいアカウントを作成し、システム ユーザ アカウントは使用しないことをお勧めします。

次の各項では、アクセス コントロールの設定方法について説明します。

- 認証の設定
- 認可の設定
- アカウンティングの設定
- TACACS+ サーバ アトリビュートの設定

認証の設定

ユーザが Detector モジュールにログインしようとしたとき、または（**enable** コマンドを使用して）上位の特権レベルを要求したときに、Detector モジュールで使用する認証方式を設定することができます。Detector モジュールは、次の認証オプションを提供します。

- ローカル認証：ローカルに設定されたログイン名およびイネーブル　パスワードが認証に使用されます。この認証方式がデフォルトです。詳細については、P.4-8 の「ローカル認証の設定」を参照してください。
- Terminal Access Controller Access-Control System Plus（TACACS+）認証：1 つ以上の TACACS+ サーバを使用したリモート ユーザ認証。

（注） ユーザ認可を設定するには、まず TACACS+ サーバでユーザの認証を設定しておく必要があります。設定していない場合は、Detector モジュールにアクセスできない可能性があります（P.4-12 の「認可の設定」を参照）。

一方または両方のユーザ認証方式を使用するように Detector モジュールを設定できます。TACACS+ 認証を使用するときに、複数の TACACS+ サーバを定義できます。複数の認証方式を定義することにより、通信エラーのために最初の方式が失敗した場合に備えたバックアップが用意されます。

Detector モジュールは、定義された各方式を、Detector モジュールで定義した順序で使用してユーザを認証します。定義された認証方式のリストを表示するには、**show running config** コマンドを入力します。Detector モジュールは、リストの最初に表示されている方式を使用してユーザの認証を試みます。最初の認証方式が応答しない場合、Detector モジュールは、応答のある認証方式が見つかるまで、リストにある次の認証方式を順に選択していきます。

tacacs-server first-hit コマンドを使用して、Detector モジュールが最初の TACACS+ サーバから応答を受信したときに実行するアクションを設定できます。first-hit オプション（デフォルト設定）をディセーブルにしていて、最初のサーバが認証を拒否した場合、Detector モジュールは、他の TACACS+ サーバを順にスキャンして、その認証を受け入れるサーバを検索します。定義されていない TACACS+ サーバが認証を受け入れた場合や、Guard がどのサーバとも通信できない場合は、ユーザ認証が失敗します。first-hit オプションをイネーブルにし

ている場合、Detector モジュールは、最初の TACACS+ サーバの認証応答（拒否または受け入れ）を最終決定として受け入れます。デフォルトでは、first-hit オプションはディセーブルになっています。

（注） Detector モジュールが TACACS+ サーバと通信できない場合に、ローカル データベースをユーザ認証のフォールバックとして使用するように Detector モジュールを設定できます。（「認証方式の設定」の項を参照）。

この項では、次のトピックについて取り上げます。

- 認証方式の設定
- ローカル認証の設定

認証方式の設定

Detector モジュールで使用する認証方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認証が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.4-22 の「TACACS+ サーバ アトリビュートの設定」を参照してください。

ステップ 2　設定モードで次のコマンドを入力し、認証方式を定義します。

```
aaa authentication {enable | login} {local | tacacs+} [tacacs+ | local]
```

表 4-3 に、**aaa authentication** コマンドのキーワードを示します。

表 4-3　aaa authentication コマンドのキーワード

パラメータ	説明
enable	ユーザが上位の特権レベルに入るときに Detector モジュールが認証できるようにします。
login	ユーザがログインするときに Detector モジュールが認証できるようにします。
local	Detector モジュールがユーザを認証するために使用するローカル データベースを指定します。
tacacs+	TACACS+ サーバがユーザを認証できるようにします。
tacacs+ | local	（オプション）設定された認証方式が失敗した場合の代替の認証方式を指定します。

認証方式を変更するには、このコマンドを再入力します。

次の例は、上位の特権レベルに入る際に認証を行うように設定する方法を示しています。最初の認証方式は TACACS+ に設定され、2 番目の認証方式はローカル ユーザ データベースに設定されています。

```
user@DETECTOR-conf# aaa authentication enable tacacs+ local
```

ローカル認証の設定

Detector モジュールには、管理者特権を持つユーザ名（ユーザ定義と呼ばれる）があらかじめ設定されています。このユーザ名を使用して新しいユーザを作成できます。ユーザ定義を使用すると、Detector モジュールのユーザ コミュニティをドメインに分割し、安全な管理アクセスのためにパスワードを割り当てることができます。

TACACS+ サーバを使用した CLI ユーザの認証をイネーブルにするには、P.4-6 の「認証の設定」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。

- ユーザの追加

- 自分のパスワードの変更
- 他のユーザのパスワードの変更
- ローカル ユーザ データベースからのユーザの削除

ユーザの追加

Detector モジュールのローカル データベースにユーザを追加するには、設定モードで次のコマンドを使用します。

username *username* {**admin** | **config** | **dynamic** | **show**} [*password*]

表 4-4 に、**username** コマンドの引数とキーワードを示します。

表 4-4　username コマンドの引数とキーワード

パラメータ	説明
username	ユーザの名前。1 ～ 63 文字の英数字の文字列を入力します。大文字と小文字が区別され、先頭は英字である必要があります。この文字列にはスペースを含めることはできませんが、アンダースコアを含めることはできます。
admin	すべての操作にアクセスできます。
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。
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す。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。
show	監視操作と診断操作にアクセスできます。
password	（オプション）ユーザ パスワード。6 ～ 24 文字の英数字の文字列を入力します。スペースは使用できず、大文字と小文字が区別されます。パスワードを入力しない場合、入力するよう要求されます。

次の例は、新しいユーザを設定し、パスワードを設定する方法を示しています。

```
user@DETECTOR-conf# username Robbin config 123456
```

ユーザはクリア テキストでパスワードを入力しますが、Detector モジュールの設定ファイルでは、パスワードが暗号化されて表示されます。次の例は、Detector モジュールの設定ファイル（running-config）を表示します。

```
username Richard config encrypted 840xdMk3
```

上の例の **encrypted** キーワードは、パスワードが暗号化されていることを示しています。

Detector モジュール上に設定されているユーザのリストを表示するには、**show running-config** コマンドまたは **show detector** コマンドを使用します。

現在 CLI にログインしているユーザのリストを表示するには、**show users** コマンドを使用します。

自分のパスワードの変更

ユーザは、自分自身のパスワードを変更することができます。管理者は、自分自身のパスワードと、他のユーザのパスワードを変更できます（P.4-11 の「他のユーザのパスワードの変更」を参照）。

自分自身のパスワードを変更するには、次の手順を実行します。

ステップ 1　グローバル モードで次のコマンドを入力します。

```
password
```

ステップ 2　現在のパスワードを入力します。新しいパスワードの入力を求めるプロンプトが表示されます。

ステップ 3　新しいパスワードを入力します。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

次の例は、自分のパスワードを変更する方法を示しています。

```
user@DETECTOR# password
Old Password: <old-password>
New Password: <new-password>
Retype New Password: <new-password>
```

他のユーザのパスワードの変更

他のユーザのパスワードを変更するには、管理ユーザ特権を持っている必要があります。

他のユーザのパスワードを変更するには、次の手順を実行します。

ステップ 1　グローバル モードで次のコマンドを入力します。

password *username-password*

username-password 引数は、変更対象のパスワードを持つユーザです。

ステップ 2　新しいパスワードを入力します。

パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

次の例では、管理者がユーザ Jose のパスワードを変更しています。

```
user@DETECTOR# password Jose
New Password: <new-password>
Retype New Password: <new-password>
```

ローカル ユーザ データベースからのユーザの削除

ローカル ユーザ データベースからユーザを削除すると、そのローカル ユーザ データベースのみを使用して認証を行っている場合、関連付けられているユーザが Detector モジュールにアクセスできなくなります。

Detector モジュールのローカル ユーザ データベースからユーザを削除するには、**no username** *username* コマンドを使用します。

次の例は、ローカル ユーザ データベースからユーザを削除する方法を示しています。

```
user@DETECTOR-conf# no username Robbin
```

認可の設定

システム管理者は、ユーザが使用できるサービスを制限することができます。認可をイネーブルにすると、Detector モジュールはユーザ プロファイルを確認します。ユーザ プロファイルは、ローカル ユーザ データベース内または TACACS+ セキュリティ サーバ上にあります。ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセスを許可されます。

ユーザがコマンドを実行しようとするときに Detector モジュールで使用する認可方式を設定することができます。Detector モジュールでは、次の認可オプションが提供されています。

- TACACS+ 認可：1 つ以上の TACACS+ サーバを使用するリモート ユーザ認可方式。

  次の 2 種類の TACACS+ 認可がサポートされています。

  - EXEC 認可：ユーザが Detector モジュールにログインして認証されたときに、そのユーザの特権レベルを決定します。
  - コマンド認可：ユーザがコマンドを入力すると、そのコマンドの許可を取得するために、TACACS+ サーバを調べます。

  TACACS+ 認可では、コマンドごとにアクセス権を指定できます。

注意　認可は **copy running-config** コマンドに制限することをお勧めします。これは、**copy running-config** コマンドを使用することにより、設定ファイル内でユーザに対してすべてのコマンドが認可されているかどうかに関係なく、すべての設定コマンドの実行が許可されるためです。

- ローカル認可：コマンド グループのアクセス コントロールにローカルで設定されたユーザ プロファイルが使用されます。認可は、指定された特権レベルのすべてのコマンドに対して定義されます。この認可方式がデフォルトです。

Detector モジュールのローカル認可は、TACACS+ サーバへの通信に失敗した場合に実行することができます。

ユーザ認可方式を定義する順次認可リストを設定できます。順次認可リストには認可に使用する方式を 1 つ以上指定でき、最初の認可方式への通信が失敗した場合は、バックアップが提供されます。

Detector モジュールは、最初に一覧表示した方式を使用してユーザを認可します。その方式が応答しない場合、Detector モジュールは 2 番目の認可方式を選択します。認可方式が両方とも成功しなかった場合にのみ、認可は失敗します。

Detector　モジュールが認証拒否を最終的なものと見なし、それ以上他の TACACS+ サーバやローカル ユーザ データベースを検索しないように設定するために、TACACS+ サーバ アトリビュートを設定できます。詳細については、P.4-22 の「TACACS+ サーバ アトリビュートの設定」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。

- ローカル認可の設定
- 認可方式の設定
- ゾーン名のタブ補完のディセーブル化

ローカル認可の設定

Detector のサービスにアクセスできるかどうかは、ユーザの特権レベルによって決まります。システム管理者は、ユーザが使用できるサービスを制限することができます。Detector モジュールは、ユーザのプロファイルをチェックして、ユーザのアクセス権を確認します。認可されると、ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。ユーザの特権レベルの詳細については、表 3-1 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。

- パスワードを使用した特権レベルの割り当て
- ユーザ特権レベル間の移動

パスワードを使用した特権レベルの割り当て

管理者は、ユーザの特権レベルへのアクセスを制限するパスワードを設定できます。特権レベルおよびパスワードを指定したら、この特権レベルにアクセスする必要のあるユーザにそのパスワードを付与することができます。ユーザが、ユーザ特権レベルのパスワードを設定する前に、他のユーザ特権レベルに移動することはできません。

ローカル パスワードを設定して特権レベルへのアクセスを制御するには、設定モードで次のコマンドを使用します。

enable password [**level** *level*] [*password*]

表 4-5 に、**enable password** コマンドの引数を示します。

表 4-5　enable password コマンドの引数

パラメータ	説明
level *level*	（オプション）ユーザの特権レベル。レベルは次のいずれかになります。 • **admin**：すべての操作にアクセスできます。 • **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。 • **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す。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。 • **show**：監視操作と診断操作にアクセスできます。 デフォルトのレベルは **admin** です。
password	（オプション）特権レベルのパスワード。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。パスワードを入力しない場合、入力するよう要求されます。

次の例は、ユーザの特権レベル **admin** にパスワードを割り当てる方法を示しています。

```
user@DETECTOR-conf# enable password level admin <password>
```

ユーザ特権レベル間の移動

認可されたユーザは、ユーザ特権レベル間を移動することができます。

ユーザ特権レベル間を移動するには、次の手順を実行します。

ステップ 1　グローバル モードで次のコマンドを入力します。

```
enable [level]
```

level 引数には、ユーザの特権レベルを指定します。このレベルは、次のいずれかです。

- **admin**：すべての操作にアクセスできます。
- **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。
- **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す。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。
- **show**：監視操作と診断操作にアクセスできます。

デフォルトのレベルは **admin** です。

ステップ 2　特権レベルのパスワードを入力します。

次の例は、ユーザの特権レベル **admin** に切り替える方法を示しています。

```
user@DETECTOR> enable admin
Enter enable admin Password: <password>
```

下位の特権レベル（show）に戻る場合は、**disable** コマンドを使用します。

認可方式の設定

認可方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認可が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.4-22 の「TACACS+ サーバ アトリビュートの設定」を参照してください。

ステップ 2　設定モードで次のいずれかのコマンドを入力して、認可方式を定義します。

- **aaa authorization exec tacacs+**
- **aaa authorization commands** *level* {**local** | **tacacs+**} [**local**]

認可方式のシーケンシャルなリストを設定できます。各方式について、**aaa authorization** コマンドを入力します。認可方式を削除するには、このコマンドの **no** 形式を使用します。

表 4-6 に、**aaa authorization** コマンドの引数とキーワードを示します。

表 4-6　aaa authorization コマンドの引数とキーワード

パラメータ	説明
exec	ユーザが EXEC シェルの実行を許可されているかどうかを判別するために認可が実行されます。Detector モジュールは、TACACS+ サーバに確認して、認証されたユーザの特権レベルを判別します。 **注意**　認可を設定する前に、TACACS+ サーバにそのユーザを設定しておく必要があります。設定しておかないと、Detector モジュールにアクセスできない可能性があります。
commands	指定された特権レベルのすべてのコマンドに対して認可が実行されます。複数の特権レベルの認可を設定するには、認可が必要な特権レベルごとにこのコマンドを使用します。
level	次のいずれかの特権レベルに対する認可です。 • **admin**：すべての操作にアクセスできます。 • **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。 • **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す。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。
local	Detector モジュールのローカル データベースでユーザのアクセス権を確認します。
tacacs+	TACACS+ サーバでユーザのアクセス権を確認します。
local	（オプション）設定された認可方式が失敗した場合の代替の認可方式を設定します。

パフォーマンスに影響する可能性があるため、**show** 特権レベルコマンドに対する認可は設定しないことをお勧めします。

（注） コンソール セッションから入力したコマンドには、TACACS+ 認可は実行されません。

次の例は、config 特権レベルを必要とするコマンドの認可を設定する方法を示しています。最初の認可方式は TACACS+ に設定され、2 番目の認可方式はローカル ユーザ データベースに設定されています。

```
user@DETECTOR-conf# aaa authorization commands config tacacs+ local
```

注意 設定コマンド モードにアクセスできるようにするには、dynamic ユーザ特権レベルに対するアクセス権を付与するか、**configure** コマンドへのアクセス権を指定する必要があります。

TACACS+ サーバの設定例

TACACS+ サーバのデータベースで、各コマンドの認可を指定することができます。

次の例は、ユーザ Zoe に対して、TACACS+ サーバ上で認可を設定する方法を示しています。

```
user=Zoe {
    cmd = detect {
        permit .*
    }
    cmd = "no detect" {
        permit .*
    }
    cmd = learning {
        deny policy*
    }
    cmd = "no learning" {
        deny .*
    }
    cmd = dynamic-filter {
        permit .*
    }
    cmd = "no dynamic-filter" {
        permit .*
    }
}
```

ゾーン名のタブ補完のディセーブル化

ゾーン名のタブ補完をディセーブルにして、ゾーン設定へのアクセスを認可されたユーザのみに制限できます。この設定は、ゾーン名を指定するすべてのコマンドに適用されます。

グローバル モードまたは設定モードで **zone** コマンド、**no zone** コマンド、**show zone** コマンド、および **deactivate** コマンドなどのコマンドを入力しても、Detector モジュールはゾーン名の表示や補完を行わなくなります。ゾーンを設定する、ゾーン操作モードを変更する、またはゾーン統計情報を表示するには、ゾーン名を完全に入力する必要があります。

ゾーン名のタブ補完をディセーブルにすると、Detector モジュールは **tab-complete zone-list** コマンドを TACACS+ サーバに送信します。認可されたユーザに対してゾーン名のタブ補完をイネーブルにするには、**tab-complete zone-list** コマンドに対する認可を TACACS+ サーバ上で設定します。

次の例は、すべての **zone** コマンドでゾーン名のタブ補完をディセーブルにする方法を示しています。

```
user@DETECTOR-conf# aaa authorization commands zone-completion tacacs+
```

ゾーン名のタブ補完をイネーブルにするには、このコマンドの **no** 形式を使用します。

アカウンティングの設定

アカウンティング管理により、ユーザがアクセスしているサービスを追跡し、TACACS+ サーバにアカウンティング情報を保存することができます。課金、レポート、またはセキュリティ目的で、要求されたサービスのアカウンティングをイネーブルにできます。デフォルトでは、Detector モジュールでアカウンティング管理はディセーブルに設定されています。

アカウンティングを設定するには、次の手順を実行します。

ステップ 1　TACACS+ サーバ接続を設定します。詳細については、P.4-22 の「TACACS+ サーバ アトリビュートの設定」を参照してください。

ステップ 2　設定モードで次のコマンドを入力して、アカウンティングを設定します。

```
aaa accounting commands {show | dynamic | config | admin} stop-only
{local | tacacs+}
```

表 4-7 に、**aaa accounting** コマンドのキーワードを示します。

表 4-7　aaa accounting コマンドのキーワード

パラメータ	説明
show | dynamic | config | admin	指定された特権レベルのアカウンティングを定義します（ユーザの特権レベルについては、表 3-1 を参照）。
stop-only	コマンドの実行が終了したときにアクションを記録します。
local	アカウンティング情報を保存しません。
tacacs+	アカウンティング情報の記録に TACACS+ サーバのデータベースを使用します。

複数の特権レベルのアカウンティングを設定するには、必要に応じて、特権レベルごとに **aaa accounting** コマンドを入力します。

パフォーマンスに影響する可能性があるため、アカウンティング管理は config ユーザ特権レベルにのみイネーブルにすることをお勧めします。

特権レベルのアカウンティング管理を削除するには、このコマンドの **no** 形式を使用します。

次の例は、TACACS+ サーバ上で config 特権レベルを必要とするコマンドのアカウンティングを設定する方法を示しています。

```
user@DETECTOR-conf# aaa accounting commands config stop-only tacacs+
```

TACACS+ サーバ アトリビュートの設定

TACACS+ サーバで認証、認可、またはアカウンティングをイネーブルにするには、TACACS+ サーバ アトリビュートを設定する必要があります。

注意　TACACS+ 認証方式を適用する前に、TACACS+ サーバ アトリビュートを設定しておく必要があります。設定していない場合は、Detector モジュールにアクセスできないことがあります。

TACACS+ サーバのアトリビュートを設定するには、次の手順を実行します。

ステップ 1　**tacacs-server host** *ip-address* **port** *port_number* コマンドを入力して、TACACS+ サーバの IP アドレスを設定します。

詳細については、P.4-23 の「TACACS+ サーバの IP アドレスの設定」を参照してください。

ステップ 2　**tacacs-server key** *tacacs-key* コマンドを入力して、Detector モジュールが TACACS+ サーバへのアクセスに使用する暗号鍵を設定します。

詳細については、P.4-24 の「TACACS+ サーバの暗号鍵の設定」を参照してください。

ステップ 3　（オプション）**tacacs-server first-hit** コマンドを入力して、Detector モジュールが認証に使用する検索方式を設定します。

詳細については、P.4-25 の「TACACS+ 検索方式の設定」を参照してください。

ステップ 4　（オプション）**tacacs-server timeout** *timeout* コマンドを入力して、TACACS+ サーバ接続のタイムアウトを設定します。

詳細については、P.4-26 の「TACACS+ サーバの接続タイムアウトの設定」を参照してください。

ステップ 5　**show tacacs statistics** コマンドを入力して、TACACS+ サーバ接続の統計情報を表示します。

詳細については、P.4-27 の「TACACS+ サーバの統計情報の表示」を参照してください。

Detector モジュールのユーザ特権レベルは、TACACS+ の特権番号に次のように対応しています。

- **admin** = 15
- **config** = 10
- **dynamic** = 5
- **show** = 0

この項では、次のトピックについて取り上げます。

- TACACS+ サーバの IP アドレスの設定
- TACACS+ サーバの暗号鍵の設定
- TACACS+ 検索方式の設定
- TACACS+ サーバの接続タイムアウトの設定
- TACACS+ サーバの統計情報の表示

TACACS+ サーバの IP アドレスの設定

Detector モジュールが TACACS+ サーバの一連のリストを認証、認可、およびアカウンティングに使用するように設定できます。Detector モジュールは、リストされた TACACS+ サーバを使用してユーザを認証または認可するか、あるいはアカウンティング イベントを送信します。そのサーバが応答しない場合、Detector モジュールは 2 番目のサーバを選択します。リスト上のすべてのサーバが応答しなかった場合にのみ、認証または認可は失敗します。

または、Detector モジュールがリストの最初の TACACS+ サーバのみを使用してユーザを認証するように設定することもできます（詳細については、P.4-25 の「TACACS+ 検索方式の設定」を参照）。

リストには、各 TACACS+ サーバの IP アドレスを定義する必要があります。最大 9 つの TACACS+ サーバを定義できます。

リストに TACACS+ サーバを追加し、IP 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使用します。

tacacs-server host *ip-address* [**port** *port_number*]

ip-address 引数には、TACACS+ サーバの 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）。オプションの **port** キーワードと *port_number* 引数には、使用するポート番号を指定します。ポート番号を入力しない場合、Detector モジュールはデフォルトで 49 を使用します。

TACACS+ サーバは、入力した順序でリストに追加されます。リストには、最大 9 つのサーバを追加できます。

次の例は、TACACS+ サーバ リストにサーバを追加する方法を示しています。

```
user@DETECTOR-conf# tacacs-server host 192.168.33.45 port 60
```

TACACS+ サーバの暗号鍵の設定

TACACS+ サーバにアクセスするには、暗号鍵を設定する必要があります。暗号鍵は、TACACS+ サーバ上の暗号鍵と一致する必要があります。暗号鍵にスペースを含めることはできません。

サーバの暗号アクセス鍵を設定するには、設定モードで次のコマンドを使用します。

tacacs-server key *tacacs-key*

引数 *tacacs-key* は、英数字の文字列です。

（注） 定義できる暗号鍵は 1 つだけです。複数の TACACS+ サーバを使用する場合、Detector モジュールは、同じ鍵を使用して、すべての TACACS+ サーバとの通信を暗号化します。

暗号化機能をディセーブルにするには、次のコマンドを使用します。

no tacacs-server key

次の例は、TACACS+ サーバの暗号鍵を MyKey に設定する方法を示しています。

```
user@DETECTOR-conf# tacacs-server key MyKey
```

TACACS+ 検索方式の設定

設定モードで **tacacs-server first-hit** コマンドを使用することにより、Detector モジュールが認証拒否を最終的なものと見なし、それ以上他の TACACS+ サーバを検索しないように設定できます。Detector モジュールは、サーバ リストの、最初に応答する TACACS+ サーバだけを使用してユーザ認証を実行します。最初の TACACS+ サーバが応答しない場合、Detector モジュールはリストにある次のサーバを選択します。Detector モジュールは、ユーザ認証に対して最初に受け取る承認または拒否を最終決定と見なし、他の TACACS+ サーバを使用したそのユーザ認証の試行を停止します。

ユーザ認証を受け入れるサーバを検索するために、定義済みの TACACS+ サーバのシーケンシャル検索を続行するように Detector モジュールを設定するには、設定モードで **no tacacs-server first-hit** コマンドを使用します。この方式が、first-hit 操作のデフォルト設定です。すべての定義済み TACACS+ サーバがユーザ認証を拒否した場合や、Detector モジュールがどのサーバとも通信できない場合は、ユーザ認証が失敗します。

次の例は、Detector モジュールがリスト内の最初の TACACS+ サーバのみを使用してユーザ認証をするように、TACACS+ 検索方式を設定する方法を示しています。

```
user@DETECTOR-conf# tacacs-server first-hit
```

TACACS+ サーバの接続タイムアウトの設定

Detector モジュールが TACACS+ サーバからの応答を待つ時間を設定できます。タイムアウトが終了すると、Detector モジュールは次の TACACS+ サーバ（そのようなサーバが設定されている場合）との接続を確立しようとするか、ローカルの AAA にフォールバックします（フォールバックが設定されている場合）。フォールバックの方式が設定されていない場合、認証と認可は失敗します。

（注） すべての TACACS+ サーバとの通信に同じサーバ タイムアウトが使用されます。

TACACS+ サーバの接続タイムアウトを設定するには、設定モードで次のコマンドを使用します。

tacacs-server timeout *timeout*

timeout 引数には、Detector モジュールが TACACS+ サーバの応答を待つ時間を秒単位で指定します。デフォルトのタイムアウトは 0 です。

次の例は、TACACS+ サーバの接続タイムアウトを 600 秒に設定する方法を示しています。

```
user@DETECTOR-conf# tacacs-server timeout 600
```

ヒント ネットワークに問題がある場合や、TACACS+ サーバの応答が遅いためにタイムアウトが繰り返し発生する場合は、タイムアウトの値を大きくすることができます。

TACACS+ サーバの統計情報の表示

TACACS+ サーバの統計情報を表示できます。Detector モジュールは、サーバごとに統計データを提供します。

TACACS+ 関連の統計情報を表示するには、設定モードで **show tacacs statistics** コマンドを使用します。

TACACS+ の統計情報をクリアするには、設定モードで **clear tacacs statistics** コマンドを使用します。

表 4-8 に、**show tacacs statistics** コマンド出力のフィールドを示します。

表 4-8　show tacacs statistics コマンド出力のフィールドの説明

フィールド	説明
PASS	Detector モジュールが TACACS+ サーバに正常にアクセスし、アクセス権を付与された回数。
FAIL	Detector モジュールが TACACS+ サーバに正常にアクセスし、アクセス権を拒否された回数。
ERROR	Detector モジュールが TACACS+ サーバにアクセスできなかった回数。

Guard との通信の確立

Detector モジュールと Guard との間に安全な通信チャネルを確立して、次のタスクをイネーブルにすることができます。

- Remote activation of zone protection：Detector モジュールはゾーン トラフィックの異常を検出すると、通信チャネルを使用して、Guard によるゾーン保護をアクティブにします。
- Synchronization of zone configuration information：Detector モジュールと Guard は、通信チャネルを介してゾーン設定情報を交換します。

Detector モジュールは Guard との接続を確立し、通信チャネルの確保に必要な暗号鍵と証明書を交換します。その後 Detector モジュールは接続を閉じ、Guard をアクティブにする、Guard とゾーン設定を同期させる、または Guard にポーリングする必要がある場合に、通信チャネルを確立します。

Detector モジュールは、次の 2 つのタイプの通信チャネルをサポートしています。

- Secure Sockets Layer（SSL）：Remote activation of zone protection および Synchronization of zone configuration information をイネーブルにします。
- セキュア シェル 2（SSH2）：Remote activation of zone protection のみをイネーブルにします。

Detector モジュールは Guard のリスト（リモート Guard リストと呼ばれる）を保持し、ゾーン保護をアクティブにしたり、これらの Guard のゾーン情報を同期させたりします。Detector モジュールは、リモート Guard リストに設定されている各 Guard と通信チャネルを確立します。Guard との通信チャネルを確立する前に、リモート Guard リストに Guard を追加しておく必要があります。詳細については、P.9-8 の「ゾーンを保護するためのリモート Guard のアクティブ化」を参照してください。

Detector モジュールは、SSL 通信チャネルを確立する前に各 Guard と SSH2 通信チャネルを確立します。SSL リモート Guard リストおよび SSH リモート Guard リストを設定する場合は、SSH2 通信チャネルを確立する必要はありません。

この項では、次のトピックについて取り上げます。

- SSL 通信チャネルの設定
- SSH 通信チャネルの設定
- 通信チャネルの確立

SSL 通信チャネルの設定

Guard と Detector は、通信チャネルに SSL 接続を使用します。SSL とは、認証とデータの暗号化を組み合せることにより安全な接続を提供するもので、デジタル証明書、秘密と公開の鍵交換ペア、および Diffie-Hellman 鍵合意パラメータによって高度なセキュリティを実現します。SSL は、指定された受信者のみがデータを解読できるようにデータを暗号化します。

各 Guard および各 Detector は、通信チャネル経由で通信を試みるデバイスに対し、デジタル証明書やそのデバイス固有の情報（デバイスの IP アドレスなど）を使用して認証を行います。

安全な接続を確保するために、Detector は秘密および公開鍵ペアを生成し、公開鍵をリモート Guard リスト内の Guard に配布します。

Guard で通信チャネル サービスをイネーブルにした後で、Detector から通信チャネルを確立します。Detector はまず、Guard 上のユーザ *riverhead* と SSH2 通信チャネルを確立します。次に Detector は、安全な SSH2 通信チャネルを使用して SSL 接続鍵を交換します。詳細については、P.4-34 の「通信チャネルの確立」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。

- SSL 通信チャネルのイネーブル化
- SSL 証明書の再生成

SSL 通信チャネルのイネーブル化

SSL 通信チャネルをイネーブルにするには、Detector モジュールおよび Guard の両方で次の手順を実行します。

注意　Guard が TACACS+ 認証を使用してユーザを認証している場合、Detector が SSH2 接続チャネルを確立できるようにするには、TACACS+ サーバに riverhead ユーザを定義する必要があります。

ステップ 1　設定モードで **permit ssh** *ip-address-general* [*ip-mask*] と入力して、Guard の IP アドレスから Detector モジュール上の SSH サービスへのアクセスを許可します。

引数 *ip-address-general* および *ip-mask* で、Detector モジュールへのアクセスを許可する Guard の IP アドレスを定義します。

（注）　SSH サービスは、Detector モジュールと Guard で常にイネーブルになっているので、ここでイネーブルにする必要はありません。

ステップ 2　設定モードで **service internode-comm** コマンドを入力して、通信チャネル サービスをイネーブルにします。

ステップ 3　設定モードで **permit internode-comm** *ip-address-general* [*ip-mask*] コマンドを入力して、Guard の IP アドレスから通信チャネル サービスへのアクセスを許可します。

引数 *ip-address-general* および *ip-mask* で、Detector モジュールへのアクセスを許可する Guard の IP アドレスを定義します。

（注）　SSL 通信チャネルを確立する方法の詳細については、P.4-34 の「通信チャネルの確立」を参照してください。

（注）　SSL 証明書にある Guard と Detector モジュールの ID は、IP アドレスに関連付けられます。通信チャネルの片側で Guard または Detector モジュールの IP アドレスを変更する場合は、SSL 証明書を再生成する必要があります。詳細については、P.4-31 の「SSL 証明書の再生成」を参照してください。

SSL 証明書の再生成

SSL 証明書で Guard と Detector モジュールを識別する鍵は、IP アドレスに関連付けられます。

次のタスクを実行するとき、通信チャネルの両側で Guard と Detector モジュールの新しい SSL 証明書を再生成する必要があります。

- いずれか一方のデバイスの IP アドレスを変更する。
- いずれか一方のデバイスを交換する。

新しい SSL 証明書を生成する前に、まず、現在使用している証明書を両方のデバイスで削除する必要があります。

現在使用している SSL 証明書を表示するには、**show internode-comm certs** コマンドを使用します。

現在使用している SSL 証明書を再生成するには、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使用して、Guard の SSL 証明書を Detector モジュールから削除します。

cert remove *cert-host-ip*

cert-host-ip 引数には、Guard の IP アドレスを指定します。すべての Guard の SSL 証明書を削除するには、アスタリスク（*）を入力します。

次の例は、SSL 証明書を削除する方法を示しています。

```
user@DETECTOR-conf# cert remove 10.56.36.4
```

ステップ 2　設定モードで次のコマンドを使用して、Detector モジュールの SSL 証明書を Guard から削除します。

cert remove *cert-host-ip*

cert-host-ip 引数には、Detector モジュールの IP アドレスを指定します。Guard との通信チャネルを確立しているすべての Detector モジュールの SSL 証明書を削除するには、アスタリスク（*）を入力します。

ステップ 3　Guard を交換する場合は、Detector モジュールから SSH ホスト鍵も削除する必要があります。

設定モードで次のコマンドを使用して、Guard の SSH ホスト鍵を Detector モジュールから削除します。

no host-keys *ip-address-general*

ip-address 引数には、リモート デバイスの IP アドレスを指定します。

次の例は、ホスト鍵を削除する方法を示しています。

```
user@DETECTOR-conf# no host-keys 10.56.36.4
```

ステップ 4　新しい SSL 証明書を再生成するには、Guard と Detector モジュールとの間に新しい SSL 通信チャネルを確立する必要があります。この処理は Detector モジュールから実行する必要があります。詳細については、P.4-34 の「通信チャネルの確立」を参照してください。

SSH 通信チャネルの設定

トラフィックの異常を検出すると、Detector モジュールはそのイベントをログに記録するか、SSH 通信チャネルを使用して Guard によるゾーン保護をアクティブにします。SSH 通信チャネルを使用している場合、Detector モジュールは次のタスクを実行できません。

- ゾーン設定を同期化する。
- Guard を監視して、ゾーンに対する攻撃が終了したことを確認する。異常検出およびラーニング プロセスをイネーブルにした場合、Detector モジュールはゾーンに対する攻撃が終了したことを確認できず、リモート Guard をアクティブにした後は、ゾーン トラフィックのラーニングを続行しません。
- Guard との通信を監視し、リモート処理（Guard によるゾーン保護のアクティブ化など）が失敗した場合に通知する。

安全な SSH2 通信チャネルを確保するために、Detector モジュールは秘密および公開 SSH 鍵ペアを生成し、公開 SSH 鍵をリモート Guard リストにある Guard に配布します。

SSH 通信チャネルをイネーブルにしたら、Detector モジュールから SSH 通信チャネルを確立する必要があります。詳細については、P.4-34 の「通信チャネルの確立」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。

- SSH2 通信チャネルのイネーブル化
- SSH2 通信チャネル鍵の再生成

SSH2 通信チャネルのイネーブル化

Guard と Detector モジュールの間の SSH2 通信チャネルをイネーブルにするには、**permit ssh** コマンドを入力して、Detector モジュールの IP アドレスから Guard 上の SSH サービスへのアクセスを許可します。

SSH 通信チャネルをイネーブルにしたら、Detector モジュールから SSH 通信チャネルを確立する必要があります。詳細については、P.4-34 の「通信チャネルの確立」を参照してください。

Guard デバイスを交換（スワップアウト）する場合は、SSH2 通信チャネルを再生成する必要があります。P.4-33 の「SSH2 通信チャネル鍵の再生成」を参照してください。

SSH2 通信チャネル鍵の再生成

Guard デバイスを交換した場合は、次の手順を実行して通信チャネルを再生成します。

ステップ 1　Detector モジュール上で **no host-keys** *ip-address-general* 設定モード コマンドを入力して、SSH ホスト鍵を Detector モジュールから削除します。

ip-address 引数には、リモート デバイスの IP アドレスを指定します。

Detector モジュールにリストされているホスト鍵を表示するには、**show host-keys** コマンドを使用します。

ステップ 2　次のいずれかの処理を実行して、リモート Guard で SSH 鍵を設定します。

- 新しい SSH2 通信チャネルを Detector モジュールから確立します。

  P.4-34 の「通信チャネルの確立」を参照してください。
- Detector モジュールの公開鍵をリモート Guard に手動で追加します。Detector モジュールの公開 SSH 鍵をコピーし、Guard が保持している SSH 鍵のリストにペーストすることができます。

  Detector モジュールの公開 SSH 鍵を表示するには、Detector 上で **show public-key** コマンドを使用します。

  Detector モジュールの公開 SSH 鍵を、Guard が保持している SSH 鍵のリストに追加するには、Guard 上で **key add** コマンドを使用します。

通信チャネルの確立

Detector モジュールから Guard に SSH または SSL 通信チャネルを確立して Detector モジュールが Guard をアクティブにできるようにし、ゾーン設定を Guard と同期化させ、さらに Guard にポーリングします。Detector モジュールと Guard の両方で通信チャネルをイネーブルにしてから、通信チャネルを確立する必要があります。詳細については、P.4-29 の「SSL 通信チャネルのイネーブル化」および P.4-33 の「SSH2 通信チャネルのイネーブル化」を参照してください。

Detector モジュールは Guard との接続を確立し、通信チャネルの確保に必要な暗号鍵と証明書を交換します。その後 Detector モジュールは接続を閉じ、Guard をアクティブにする、Guard とゾーン設定を同期させる、または Guard にポーリングする必要がある場合に、通信チャネルを確立します。

注意　Guard で TACACS+ 認証を使用してユーザを認証している場合、**key publish** コマンドを機能させるためには、TACACS+ サーバにユーザ riverhead を定義する必要があります。

Detector モジュールから Guard への通信チャネルを確立するには、Detector モジュール上で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、SSH2 秘密および公開鍵ペアを生成します。

```
key generate
```

ステップ 2　SSH2 の鍵ペアがすでに存在している場合は、次のメッセージが表示されます。

```
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

次のオプションのいずれかを入力して必要なオプションを指定します。

- **y**：Detector モジュールは新しい SSH2 鍵ペアを生成します。
- **n**：Detector モジュールは新しい SSH2 鍵ペアを生成しません。

ステップ 3　SSH2 の公開鍵をパブリッシュします。SSL 通信チャネルを確立している場合、Guard は SSL 認証の生成も実行し、リモート Guard と交換します。

SSH2 公開鍵をパブリッシュして、SSL 認証を生成および交換するには、設定モードで次のいずれかのコマンドを使用します。

- **key publish** *remote-guard-address* {**ssh** | **ssl**}
- **key publish ***

表 4-9 に、**key publish** コマンドの引数とキーワードを示します。

表 4-9　key publish コマンドの引数とキーワード

パラメータ	説明
remote-guard-address	リモート Guard の IP アドレス。
ssh	SSH2 公開鍵を *remote-guard-address* 引数で定義されているリモート Guard にパブリッシュします。

表 4-9　key publish コマンドの引数とキーワード（続き）

パラメータ	説明
ssl	SSH2 公開鍵をパブリッシュし、SSL 認証を生成して *remote-guard-address* 引数で定義されているリモート Guard と交換します。
*	SSH2 鍵をパブリッシュして SSL 認証を生成し、リモート Guard リストに設定されているすべての Guard と SSL 認証を交換します。 Detector モジュールは、リモート Guard リスト内の各 Guard と SSH 通信チャネルを確立します。各リモート Guard について、ステップ 4とステップ 5を繰り返します。

ステップ 4　man-in-the-middle 攻撃を防ぐために、SSH2 ではホスト鍵を使用してリモート ホストの確実性が確認されます。リモート ホストに対して初めて SSH2 通信チャネルを確立したときは、リモート ホストはそのホストの公開鍵を Detector モジュールに送信します。これが Detector から Guard に対して開始される最初の接続である場合は、次のメッセージが表示されます。

```
The authenticity of host '<remote-hostname> (<remote-host IP
address>)' can't be established.
RSA key fingerprint is <RSA key fingerprint>
Are you sure you want to continue connecting (yes/no)?
```

yes と入力します。

次のプロンプト行が表示されます。

```
riverhead@remote-Guard-IP-address's password:
```

ステップ 5　Guard でユーザ riverhead 用に設定されたパスワードを入力します。

次の例で、SSH2 秘密および公開鍵ペアを生成する方法と、Detector モジュールと IP アドレスが 192.168.100.33 のリモート Guard との間で SSH2 通信チャネルを確立する方法について説明します。

```
user@DETECTOR-conf# key generate
user@DETECTOR-conf# key publish 192.168.100.33 ssh
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
The authenticity of host '192.168.100.33 (192.168.100.33)' can't be
established.
RSA key fingerprint is
de:cb:ac:36:9a:fe:33:f9:6a:d8:7b:98:a9:51:75:54.
Are you sure you want to continue connecting (yes/no)? yes
riverhead@192.168.100.33's password: <password>
user@DETECTOR-conf#
```

次の例では、リモート Guard リストに記載されている Guard との通信チャネルを確立する方法について説明します。

```
user@DETECTOR-conf# key publish *
```

Detector モジュール SSH2 公開鍵を表示するには、**show public-key** コマンドを使用します。

Detector モジュールにリストされているホスト鍵を表示するには、**show host-keys** コマンドを使用します。

SSH 鍵の管理

Detector モジュールは、安全なリモート ログインのために SSH をサポートしています。SSH 鍵のリストを追加すると、ログインとパスワードを入力しなくても、リモート デバイスから Detector モジュールに安全な通信ができます。

次の各項では、Detector モジュールの SSH 鍵リストの管理方法について説明します。

- SSH 鍵の追加
- SSH 鍵の削除

SSH 鍵の追加

ログイン名とパスワードを入力しない SSH 接続をイネーブルにするには、Detector モジュールの SSH 鍵リストにリモート接続の SSH 公開鍵を追加します。

設定モードで次のコマンドを入力します。

key add [*user-name*] {**ssh-dsa** | **ssh-rsa**} *key-string comment*

表 4-10 に、**key add** コマンドの引数とキーワードを示します。

表 4-10　key add コマンドの引数とキーワード

パラメータ	説明
user-name	（オプション）SSL 鍵の追加先ユーザの名前。他のユーザの SSH 鍵を追加できるのは管理者だけです。 デフォルトは、現行ユーザの SSH 鍵の追加です。
ssh-dsa	SSH2-DSA 鍵のタイプを指定します。
ssh-rsa	SSH2-RSA 鍵のタイプを指定します。
key-string	Guard またはリモート端末で作成された公開 SSH 鍵。鍵ストリングは、8,192 ビットまでに制限されています。 鍵タイプの識別（ssh-rsa または ssh-dsa）を除いた完全な鍵をコピーする必要があります。

表 4-10　key add コマンドの引数とキーワード（続き）

パラメータ	説明
comment	デバイスの説明。コメントの形式は、通常、鍵の生成に使用されるユーザとマシンを表す user@hostname になります。たとえば、Guard で生成される SSH 公開鍵に使用されるデフォルトのコメントは、root@GUARD です。

次の例は、SSH RSA 鍵を追加する方法を示しています。

```
user@DETECTOR-conf# key add ssh-rsa 14513797528175730. .
.user@Detector module.com
```

SSH 鍵の削除

リストから SSH 鍵を削除できます。SSH 鍵を削除すると、次に Detector モジュールと SSH セッションを確立するときには認証を受ける必要があります。

Detector モジュールから SSH 鍵を削除するには、設定モードで次のコマンドを使用します。

key remove [*user-name*] *key-string*

表 4-11 に、**key remove** コマンドの引数を示します。

表 4-11　key remove コマンドの引数

パラメータ	説明
user-name	（オプション）SSH 鍵の削除元ユーザの名前。 他のユーザの SSH 鍵を削除できるのは管理者だけです。デフォルトは、現行ユーザの SSH 鍵の削除です。
key-string	削除する公開 SSH 鍵。 プロンプトに SSH 公開鍵をペーストします。識別フィールド（ssh-rsa または ssh-dsa）は除き、鍵だけをペーストしてください。

次の例は、**key remove** コマンドにカット アンド ペーストを行えるように、ユーザ鍵を表示する方法を示しています。

```
user@DETECTOR-conf# show keys Lilac
ssh-rsa 2352345234523456... user@Detector module.com
user@DETECTOR-conf# key remove Lilac 2352345234523456...
```

SFTP 接続および SCP 接続用の鍵の設定

SSH2 の最上層にあるセキュア FTP（SFTP）、および SSH に依存する Secure Copy（SCP）は、ファイルのコピー方式を提供します。このコピー方式は、安全で信頼できます。SFTP および SCP では、公開鍵による認証と強力なデータ暗号化を使用しています。この認証と暗号化により、ログイン、データ、およびセッションの情報が送信中に傍受されたり変更されたりすることを防止できます。

SFTP 接続および SCP 接続用の鍵を設定するには、次の手順を実行します。

ステップ 1　設定モードで **show public-key** コマンドを入力して、Detector モジュール上で Detector モジュールの公開鍵を表示します。

鍵が存在する場合は、ステップ 2 を省略してステップ 3 に進みます。

鍵が存在しない場合は、ステップ 2 に進みます。

ステップ 2　設定モードで **key generate** コマンドを入力して、Detector モジュール上で秘密および公開鍵ペアを生成します。

注意　秘密および公開鍵ペアがすでに存在する場合は、再生成しないことをお勧めします。不必要に鍵ペアを再生成すると、現在オンラインになっていないリモート Guard と後で通信するときに問題が発生する可能性があります。秘密および公開鍵ペアを再生成する場合は、**key publish** コマンドを使用して、Detector のデフォルトのリモート Guard リストとゾーンのリモート Guard リストに設定されているすべてのリモート Guard にこの新しい公開鍵をパブリッシュする必要があります。

SSH2 の鍵ペアがすでに存在している場合は、次のメッセージが表示されます。

```
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

y を入力して鍵を生成します。

Detector モジュールが公開および秘密鍵ペアを作成します。Detector モジュールの公開鍵を表示するには、設定モードで **show public-key** コマンドを使用します。

ステップ 3　公開鍵を Detector モジュールからコピーし、ネットワーク サーバ上の鍵ファイル内にペーストします。

たとえば、Linux オペレーティング システムにインストールされている ネットワーク サーバに username というユーザ アカウントで接続している場合は、Detector モジュールの公開鍵を /home/username/.ssh/authorized_keys2 ファイルに追加します。

鍵は 1 行に収まるようにコピーしてください。鍵が 2 行としてコピーされた場合は、1 行目の末尾にある改行文字を削除します。

（注）　公開鍵をコピーしてネットワーク　サーバ上の鍵ファイルにペーストしないと、自動エクスポート機能（**export reports** コマンドなど）が使用できず、手動でネットワーク サーバに接続するたびに、パスワードを入力する必要があります。

ホスト名の変更

Detector モジュールのホスト名を変更できます。この変更はすぐに反映され、新しいホスト名は自動的に CLI プロンプト ストリングに組み込まれます。

Detector モジュールのホスト名を変更するには、設定モードで次のコマンドを使用します。

hostname *name*

name 引数には、新しいホスト名を指定します。

次の例は、Detector モジュールのホスト名を変更する方法を示しています。

```
user@DETECTOR-conf# hostname CiscoDetector
admin@CiscoDetector-conf#
```

SNMP トラップのイネーブル化

Detector モジュールが SNMP トラップを送信し、Detector モジュールで発生する重大なイベントを管理者に通知するように設定することができます。また、Detector モジュールの SNMP トラップ ジェネレータのパラメータを設定し、Detector モジュールが報告する SNMP トラップ情報の範囲を定義することもできます。

トラップのログは、Detector モジュールのイベント ログに記録され、トラップ条件が発生すると、SNMP エージェントがトラップを送信するかどうかに関係なく、イベント モニタに表示されます。

Detector モジュールが SNMP トラップを送信するように設定するには、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て、SNMP トラップ ジェネレータ サービスをイネーブルにします。

```
service snmp-trap
```

ステップ 2　次のコマンドを入力して、SNMP トラップ ジェネレータのパラメータ（トラップの宛先 IP アドレスとトラップ情報の範囲）を設定します。

snmp trap-dest *ip-address* [*community-string* [*min-severity*]]

表 4-12 に、**snmp trap-dest** コマンドの引数を示します。

表 4-12　snmp trap-dest コマンドの引数

パラメータ	説明
ip-address	宛先ホストの IP アドレス。
community-string	（オプション）トラップとともに送信されるコミュニティ ストリング。このストリングは、宛先ホスト用に定義されたコミュニティ ストリングと一致する必要があります。デフォルトのコミュニティ ストリングは、*public* です。1 ～ 15 文字の英数字文字列を入力します。この文字列にスペースを含めることはできません。
min-severity	（オプション）トラップ情報のスコープ。重大度レベルの範囲の下限を指定してスコープを定義します。この定義により、トラップは指定された重大度レベル以上のすべてのイベントを表示します。たとえば、Warnings を指定すると、トラップは Warnings から Emergencies までのすべての重大度レベルのイベントを表示します。重大度レベルのオプションを次に示します。 • Emergencies：システムは使用不能（重大度 = 0）。 • Alerts：即座に処置が必要（重大度 = 1）。 • Critical：深刻な状態（重大度 = 2）。 • Errors：エラー状態（重大度 = 3）。 • Warnings：警告状態（重大度 = 4）。 • Notifications：正常ではあるが、重要な状態（重大度 = 5）。 • Informational：情報メッセージ（重大度 = 6）。 • Debugging：デバッグ メッセージ（重大度 = 7）。 デフォルトでは、レポートにはすべての重大度レベルのイベントが表示されます。

SNMP トラップ ジェネレータ パラメータを削除するには、**no snmp trap-dest** コマンドを使用します。すべての SNMP トラップ宛先パラメータを削除するには、アスタリスク（*****）を入力します。

次の例は、errors 以上の重大度レベルのトラップが、SNMP コミュニティ ストリング tempo とともに宛先 IP アドレス 192.168.100.52 に送信される例を示しています。

```
user@DETECTOR-conf# snmp trap-dest 192.168.100.52 tempo errors
```

表 4-13 に、Detector モジュールが生成する SNMP トラップを示します。

表 4-13　SNMP トラップ

SNMP トラップ	重大度	説明
rhExcessiveUtilizationTrap	EMERGENCY	すべての Detector モジュール ゾーン上で 150,000 個以上の動的フィルタが同時にアクティブになっているため、Detector モジュールは新しい動的フィルタを追加できない。
rhExcessiveUtilizationTrap	EMERGENCY	異常検出エンジン メモリが制限値に達した（90 % を超えた）。
rhGeneralTrap	EMERGENCY	ソフトウェア ライセンスがインストールされていないか、正しくない。このデバイスは動作しません。
rhGeneralTrap	EMERGENCY	インストールされているソフトウェア ライセンスを確認できない。このデバイスは動作しません。
rhGeneralTrap	EMERGENCY	インストールされているソフトウェア ライセンスの期限が明日（<dd-mmm-yyyy>）で切れる。

表 4-13　SNMP トラップ（続き）

SNMP トラップ	重大度	説明
rhGeneralTrap	EMERGENCY	インストールされているソフトウェア ライセンスの期限が今日で切れる。このデバイスは動作しなくなります。
rhGeneralTrap	EMERGENCY	インストールされているソフトウェア ライセンスが無効：< 失敗メッセージ >。
rhGeneralTrap	ALERT	ディスク スペースが 80% である。
rhGeneralTrap	ALERT	インストールされているソフトウェア ライセンスの期限が 3 週間または 2 週間後の <dd-mmm-yyyy> に切れる。
rhGeneralTrap	ALERT	インストールされているソフトウェア ライセンスの期限が 1 週間後の <dd-mmm-yyyy> に切れる。
rhGeneralTrap	ALERT	インストールされているソフトウェア ライセンスの期限が 30、6、5、4、3、または 2 日後の <dd-mmm-yyyy> に切れる。
rhExcessiveUtilizationTrap	CRITICAL	ギガビット インターフェイス リンクの使用率（bps[1] 単位）が 85% を超えている。
rhExcessiveUtilizationTrap	CRITICAL	メモリ使用率が 85% を超えている。
rhExcessiveUtilizationTrap	CRITICAL	アクセラレータ カード CPU 使用率が 85% を超えている。
rhDynamicFilterTrap	ERROR	保留中の動的フィルタ数が 1000 のため、新しい保留動的フィルタは廃棄される。

表 4-13　SNMP トラップ（続き）

SNMP トラップ	重大度	説明
rhProtectionTrap	ERROR	Detector モジュールは SSL 通信チャネルを使用してゾーンを保護するためのリモート Guard のアクティブ化に失敗した。
rhZoneGenericTrap	ERROR	Detector モジュールはゾーン設定の同期化に失敗した。
rhGeneralTrap	ERROR	Detector モジュールが次のようなゾーン異常検出のアクティブ化に失敗した。 • 検出またはラーニングから検出とラーニングまで • 検出とラーニングから検出またはラーニングへ Detector モジュールはゾーン異常検出とラーニング プロセスを非アクティブ化した。
rhDynamicFilterTrap	WARNING	Detector モジュールは動的フィルタの追加に失敗した。 このエラーは次のいずれかの場合に発生する可能性があります。 • アクティブな動的フィルタが多すぎる。 • 動的フィルタのアクションはリモートのアクティブ化であり、Detector モジュールはリモート Guard リストに記載されているリモート Guard と接続できなかった。

表 4-13　SNMP トラップ（続き）

SNMP トラップ	重大度	説明
rhExcessiveUtilizationTrap	WARNING	Detector モジュールに、すべてのゾーン上で同時にアクティブになっている動的フィルタが 135,000 個以上ある。アクティブな動的フィルタの数が 15,000 に到達すると、Detector モジュールは新しい動的フィルタを追加できなくなります。
rhGeneralTrap	WARNING	ディスク スペースが 75% である。
rhPolicyConstructionTrap	WARNING	ラーニング プロセスのポリシー構築フェーズが失敗した。
rhDetectionTrap	WARNING	Detector モジュールはゾーン異常検出の開始に失敗した。
rhReloadTrap	WARNING	Detector モジュールは再起動した。トラップには、MIB2 ウォーム スタート トラップまたはコールド スタート トラップと、Detector モジュールが再始動した原因に関する情報が含まれています。
rhReloadTrap	WARNING	Detector モジュールがシャットダウンした。トラップには、MIB2 ウォーム スタート トラップまたはコールド スタート トラップと、Detector モジュールがシャットダウンした原因に関する情報が含まれています。
rhThresholdTuningTrap	WARNING	ラーニング プロセスのしきい値調整フェーズが失敗した。
rhAttackTrap	NOTIFICATIONS	攻撃が開始した。
rhAttackTrap	NOTIFICATIONS	攻撃が終了した。

表 4-13　SNMP トラップ（続き）

SNMP トラップ	重大度	説明
rhPolicyConstructionTrap	NOTIFICATIONS	ラーニング プロセスのポリシー構築フェーズが開始された。
rhPolicyConstructionTrap	NOTIFICATIONS	ラーニング プロセスのポリシー構築フェーズが受け入れられた。
rhPolicyConstructionTrap	NOTIFICATIONS	ラーニング プロセスのポリシー構築フェーズが停止された。
rhDetectionTrap	NOTIFICATIONS	ゾーン異常検出が開始した。
rhDetectionTrap	NOTIFICATIONS	ゾーン異常検出が終了した。
rhProtectionTrap	NOTIFICATIONS	Detector モジュールは SSL 通信チャネルを使用してゾーンを保護するためのリモート Guard のアクティブ化に失敗している。
rhThresholdTuningTrap	NOTIFICATIONS	ラーニング プロセスのしきい値調整フェーズが開始された。
rhThresholdTuningTrap	NOTIFICATIONS	ラーニング プロセスのしきい値調整フェーズが受け入れられた。
rhThresholdTuningTrap	NOTIFICATIONS	ラーニング プロセスのしきい値調整フェーズが停止された。
rhZoneGenericTrap	NOTIFICATIONS	Detector モジュールはゾーン設定の同期化を開始した。
rhZoneTrap	NOTIFICATIONS	新しいゾーンが作成された。
rhZoneTrap	NOTIFICATIONS	ゾーンが削除された。
rhDynamicFilterControlTrap	INFO	Detector モジュールが特定のポリシーに送信しなかった攻撃検出イベントの数。
rhDynamicFilterControlTrap	INFO	Detector モジュールは、アクティブな動的フィルタが 1000 個以上あるため、削除する動的フィルタのトラップを送信しない。

表 4-13　SNMP トラップ（続き）

SNMP トラップ	重大度	説明
rhDynamicFilterTrap	INFO	動的フィルタが追加された。
rhDynamicFilterTrap	INFO	動的フィルタが削除された。
rhDynamicFilterTrap	INFO	保留動的フィルタが追加された。

1. bps = bits per second（ビット / 秒）

SNMP コミュニティ ストリングの設定

Detector モジュールの SNMP サーバにアクセスすることにより、管理情報ベース 2（MIB2）および Cisco Riverhead 専用 MIB で定義された情報を取得することができます。コミュニティ ストリングはパスワードのように機能し、Detector モジュールの SNMP エージェントからの読み取りアクセスを許可します。Detector モジュールの SNMP コミュニティ ストリングを設定して、異なる組織のクライアントがそれぞれ異なるコミュニティ ストリングを使用して SNMP エージェントにアクセスできるようにすることができます。

SNMP コミュニティ ストリングを追加するには、設定モードで次のコマンドを使用します。

snmp community *community-string*

community-string 引数には、目的の Detector モジュールのコミュニティ ストリングを指定します。1 ～ 15 文字の英数字文字列を入力します。この文字列にスペースを含めることはできません。Detector モジュールのデフォルトのコミュニティ ストリングは riverhead です。コミュニティ名はいくつでも指定できます。コミュニティ ストリングを削除するには、**no community string** コマンドを使用します。すべての SNMP コミュニティ ストリングを削除するには、アスタリスク（*****）を入力します。

次の例は、SNMP コミュニティ ストリングを設定する方法を示しています。

```
user@DETECTOR-conf# snmp community tempo
```

ログイン バナーの設定

ログイン バナーとは、SSH セッション、コンソール ポート接続、または Detector モジュールへの WBM セッションを開いたときに、ユーザ認証の前の画面に表示されるテキストのことです。

認可されていないアクセスに対してユーザに警告したり、適切と見なされるシステムの使用法を説明したり、不適切な使用法や不正な活動を検出するためにシステムが監視されていることをユーザに警告したりするように、ログイン バナーを設定できます。

Detector モジュールは、次の場所にログイン バナーを表示します。

- CLI：パスワード ログイン プロンプトの前、またはポップアップ ウィンドウとして（使用している SSH クライアントによって異なる）。
- WBM：Detector モジュールのログイン ウィンドウの右側。

この項では、次のトピックについて取り上げます。

- CLI からのログイン バナーの設定
- ログイン バナーのインポート
- ログイン バナーの削除

CLI からのログイン バナーの設定

login-banner コマンドを使用すると、単一または複数のメッセージ バナーを作成できます。複数のログイン バナーを入力した場合、新しいログイン バナーは、既存のログイン バナーの最後に新しい行として追加されます。

ログイン バナーを設定するには、設定モードで次のコマンドを使用します。

login-banner *banner-str*

banner-str 引数には、バナーのテキストを指定します。文字列の長さは最大 999 文字です。式にスペースを使用する場合は、式を引用符（" "）で囲みます。

ログイン バナーを表示するには、**show login-banner** コマンドを使用します。

次の例は、ログイン バナーを設定して表示する方法を示しています。

```
user@DETECTOR-conf# login-banner "Welcome to the Cisco Traffic Anomaly
Detector"
user@DETECTOR-conf# login-banner "Unauthorized access is prohibited."
user@DETECTOR-conf# login-banner "Contact sysadmin@corp.com for
access."
user@DETECTOR-conf# show login banner
Welcome to the Cisco Traffic Anomaly Detector
Unauthorized access is prohibited.
Contact sysadmin@corp.com for access.
```

ログイン バナーのインポート

グローバル モードまたは設定モードで次のいずれかのコマンドを入力して、ネットワーク サーバからテキスト ファイルをインポートし、既存のログイン バナーを差し替えることができます。

- **copy ftp login-banner** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **login-banner** *server full-file-name login*

インポートするファイル内の各行の最大長は、999 文字です。

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 4-14 に、**copy login-banner** コマンドの引数とキーワードを示します。

表 4-14　copy login-banner コマンドの引数とキーワード

パラメータ	説明
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。

表 4-14　copy login-banner コマンドの引数とキーワード（続き）

パラメータ	説明
server	ネットワーク サーバの 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 192.168.10.2）。
full-file-name	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリからファイルをコピーします。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

次の例は、FTP サーバからログイン バナーをインポートする方法を示しています。

```
user@DETECTOR-conf# copy ftp login-banner 10.0.0.191
/root/login-banner <user> <password>
```

ログイン バナーの削除

ユーザ認証の前にメッセージを表示する必要がなくなった場合、ログイン バナーを削除できます。

ログイン バナーを削除するには、設定モードで **no login-banner** コマンドを使用します。

次の例は、ログイン バナーを削除する方法を示しています。

```
user@DETECTOR-conf# no login-banner
```

Web-Based Manager ロゴの設定

エンドユーザ インターフェイスをカスタマイズするために、企業のロゴ（またはカスタマイズされたロゴ）を Web-Based Manager（WBM）Web ページに追加することができます。

新しいロゴは、次の場所に表示されます。

- Detector モジュールのログイン ページで、Cisco Systems ロゴの下。
- すべての WBM ページ（Detector モジュールのログイン ページは除く）で、Cisco Systems ロゴの右側。

新しいロゴは GIF 形式である必要があります。新しいロゴのサイズは、幅 = 87 ピクセル、高さ = 41 ピクセルにすることをお勧めします。

この項では、次のトピックについて取り上げます。

- WBM ロゴのインポート
- WBM ロゴの削除

WBM ロゴのインポート

WBM で使用する新しいロゴをネットワーク サーバからインポートするには、グローバル モードまたは設定モードで次のコマンドを入力します。

- **copy ftp wbm-logo** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **wbm-logo** *server full-file-name login*

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 4-15 に、**copy wbm-logo** コマンドの引数とキーワードを示します。

表 4-15　copy wbm-logo コマンドの引数とキーワード

パラメータ	説明
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
server	ネットワーク サーバの 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 192.168.10.2）。
full-file-name	GIF ファイル拡張子を含む、完全なファイル名。パスを指定しない場合、サーバはユーザのホーム ディレクトリからファイルをコピーします。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

次の例は、FTP サーバから WBM ロゴ ファイルをインポートする方法を示しています。

```
user@DETECTOR-conf# copy ftp wbm-logo 10.0.0.191 /root/WBMlogo.gif
<user> <password>
```

WBM ロゴの削除

WBM ロゴを削除するには、設定モードで **no wbm-logo** コマンドを使用します。

次の例は、WBM ロゴを削除する方法を示しています。

```
user@DETECTOR-conf# no wbm-logo
```

セッション タイムアウトの設定

セッション タイムアウトとは、アクティビティが何もない状態でセッションがアクティブでいられる時間のことです。設定された時間内に何もアクティビティがなかった場合、タイムアウトが発生し、再びログインする必要があります。セッション タイムアウトは、デフォルトではディセーブルになっています。

セッション タイムアウトは CLI にのみ適用され、WBM には適用されません。

設定モードで次のコマンドを入力して、Detector モジュールがアイドル セッションを自動的に切断するまでの分数を設定できます。

session-timeout *timeout-val*

timeout-val 引数には、Detector モジュールが自動的にアイドル セッションを切断するまでの分数を指定します。有効な値は、1 ～ 1,440 分（1 日）です。

次の例は、Detector モジュールが 10 分後にアイドル セッションを切断するように設定する方法を示しています。

```
user@DETECTOR-conf# session-timeout 10
```

Detector モジュールが自動的にアイドル セッションを切断しないようにするには、**no session-timeout** コマンドを使用します。

セッション タイムアウトの値を表示するには、**show session-timeout** コマンドを使用します。

CHAPTER 5

ゾーンの設定

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）でゾーンを作成し、管理する方法について説明します。これらの手順は、ゾーン検出をイネーブルにするために必要です。

この章は、次の項で構成されています。

- ゾーンについて
- ゾーン テンプレートの使用
- 新しいゾーンの作成
- ゾーンのアトリビュートの設定
- ゾーンの IP アドレス範囲の設定
- Detector モジュールの Guard とのゾーン設定の同期

ゾーンについて

ゾーンとは、Detector モジュールが Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を監視するために使用するネットワーク要素のことです。ゾーンは、次の要素を任意に組み合せたものです。

- ネットワークサーバ、クライアント、またはルータ
- 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）

Detector モジュールは、DDoS 攻撃を発見すると、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、手動で Guard をアクティブにするようにユーザに通知することができます。Detector モジュールでは、ゾーンのネットワーク アドレス範囲が互いに重複していない場合に限り、複数のゾーンのトラフィックを同時に分析できます。

ゾーンに名前を割り当て、この名前を使用してゾーンを参照します。

ゾーンの設定処理には、次のタスクがあります。

- ゾーンの作成：ゾーンを作成し、ゾーン名とゾーンの説明を設定できる。詳細については、P.5-6 の「新しいゾーンの作成」を参照してください。
- ゾーン ネットワーク定義の設定：ネットワークの IP アドレスやサブネット マスクなどを含む、ゾーン ネットワーク定義を設定できる。詳細については、P.5-11 の「ゾーンのアトリビュートの設定」を参照してください。
- ゾーン フィルタの設定：ゾーン フィルタを設定できる。ゾーン フィルタは、ゾーンのトラフィックに必要な検出レベルを適用し、Detector モジュールで特定のトラフィック フローを処理する方法を定義します。詳細については、第 6 章「ゾーンのフィルタの設定」を参照してください。
- ゾーン　トラフィック特性のラーニング：ゾーンの検出ポリシーを作成できる。このポリシーは、Detector モジュールで特定のトラフィック フローを分析して、トラフィック フローがポリシーのしきい値を超過した場合にアクションを実行できるようにします。Detector モジュールは、ポリシー構築フェーズおよびしきい値調整フェーズの 2 つのフェーズで構成されるラーニング プロセスの中でポリシーを構築します。詳細については、第 8 章「ゾーン トラフィックの特性のラーニング」を参照してください。

ゾーン テンプレートの使用

ゾーン テンプレートとは、ゾーンのデフォルト設定を定義したものです。

Detector モジュールには、次のプレフィックスを持つ 2 つのゾーン テンプレート セットが含まれています。

- DETECTOR_：Detector モジュール専用に設計されたゾーン テンプレート。ゾーン設定を Guard と共有しない場合は、DETECTOR_ バージョンのゾーン テンプレートを選択します。
- GUARD_：Detector モジュールと Guard 用に設計されたゾーン テンプレート。これらのテンプレートから作成されたゾーンに Detector モジュールと Guard の両方のアトリビュートを設定して、ゾーン設定を Guard にコピーできます。ゾーン設定を Guard と同期させる場合は、GUARD_ バージョンのゾーン テンプレートを選択します。

  これらのテンプレートから作成されたゾーンを設定する方法の詳細については、P.5-17 の「同期用のゾーンの設定」を参照してください。

表 5-1 に、ゾーン テンプレートを示します。

表 5-1　ゾーン テンプレート

テンプレート	説明
DETECTOR_DEFAULT	デフォルトのゾーン テンプレート。このゾーン テンプレートを使用して VoIP[1] サーバを保護することができます。 このゾーン テンプレートを使用してゾーンを作成した場合、ゾーンに対する TCP ワーム攻撃は検出できません。
DETECTOR_WORM	ゾーンに対する TCP ワーム攻撃を Detector モジュールが検出できるようにするゾーン テンプレート。DETECTOR_WORM ゾーン テンプレートから作成されたゾーンには、worm_tcp ポリシー テンプレートから作成されたポリシーが含まれています（詳細については、P.7-34 の「ワーム ポリシーについて」を参照）。

表 5-1　ゾーン テンプレート（続き）

テンプレート	説明
DETECTOR_LINK テンプレート	帯域幅のわかっているゾーンに応じてセグメント化された大規模なサブネットの検出用に設計されたゾーン テンプレート。これらのゾーン テンプレートによって定義されたゾーンに対しては、ラーニング プロセスを行わずにゾーン検出をアクティブにすることができます。Detector モジュールが、攻撃されている IP アドレスまたはサブネットのみに対する Guard 上のゾーン保護をアクティブにするようにするには、**protect-ip-state dst-ip-by-name** コマンドを使用します。**protect-ip-state** コマンドの詳細については、P.9-5 の「Guard 保護のアクティベーション方式の設定」を参照してください。 帯域幅限定リンク ゾーン テンプレートは、128 Kb、1 Mb、4 Mb、および 512 Kb のリンクをそれぞれ対象とした次のものが用意されています。 DETECTOR_LINK_128K DETECTOR_LINK_1M DETECTOR_LINK_4M DETECTOR_LINK_512K これらのテンプレートから作成されたゾーンに対しては、ラーニング プロセスのポリシー構築フェーズを実行することはできません。
GUARD_DEFAULT	デフォルトのゾーン テンプレート。

表 5-1　ゾーン テンプレート（続き）

テンプレート	説明
GUARD_LINK テンプレート	帯域幅のわかっているゾーン用に設計されたゾーン テンプレート。128 Kb、1 Mb、4 Mb、および 512 Kb のリンクを対象とした次のテンプレートが用意されています。 GUARD_LINK_128K GUARD_LINK_1M GUARD_LINK_4M GUARD_LINK_512K これらのテンプレートから作成されたゾーンに対してポリシー構築を実行することはできません。GUARD_LINK ゾーン テンプレートから作成されたゾーンに対しては、しきい値調整フェーズを実行せずにゾーン検出をアクティブにすることができます。 このようなゾーンを定義する際は、**protect-ip-state** コマンドを使用した **dst-ip-by-name** による Guard 保護アクティベーション方式（特定の IP アドレス宛てのゾーン トラフィック異常が検出されると Detector モジュールが Guard をアクティブにしてその IP アドレスを保護する）を使用することをお勧めします。詳細については、P.9-5 の「Guard 保護のアクティベーション方式の設定」を参照してください。
GUARD_TCP_NO_PROXY	TCP プロキシを使用しないゾーン用に設計されたゾーン テンプレート。ゾーンが IP アドレスに基づいて制御されている場合（IRC[2] サーバタイプのゾーンなど）、またはゾーンで実行されているサービスのタイプが不明な場合に、このゾーン テンプレートを使用できます。

1. VoIP = Voice over IP
2. IRC = Internet Relay Chat（インターネット リレー チャット）

新しいゾーンの作成

ゾーンを作成し、ゾーン名、説明、ネットワーク アドレス、動作定義、ネットワーク定義を設定することができます。

新しいゾーンを作成するときには、既存のゾーンをテンプレートとして使用するか、またはシステム定義のゾーン テンプレートからゾーンを作成することができます。ゾーン テンプレートには、ゾーンの初期ポリシーおよびフィルタ設定が定義されています。

新しいゾーンは、次の 2 つの方法で作成できます。

- 新しいゾーンの作成：システム定義のゾーン　テンプレートから新しいゾーンを作成できます。この方式は、デフォルトのポリシーおよびフィルタを使用して新しいゾーンを作成する場合に使用します。

  新しいゾーンを作成したら、ゾーン アトリビュートを設定する必要があります。
- ゾーンの複製：既存のゾーンからゾーンを作成できます。この方式は、新しいゾーンに既存のゾーンと同様のトラフィック パターンを割り当てる場合に使用します。

ゾーン設定の設定値を変更する方法については、P.5-11 の「ゾーンのアトリビュートの設定」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。

- ゾーン テンプレートからの新しいゾーンの作成
- 既存のゾーンの複製による新しいゾーンの作成

ゾーン テンプレートからの新しいゾーンの作成

システム定義のゾーン テンプレートから新しいゾーンを作成するには、次のコマンドのいずれかを使用します。

- **zone** *new-zone-name* [*template-name*] [**interactive**]：新しいゾーンを作成します。*template-name* 引数を入力しなかった場合、新しいゾーンは DETECTOR_DEFAULT ゾーン テンプレートから作成されます。
- **zone** *zone-name* [*template-name*] [**interactive**]：既存のゾーンを削除して、同じ名前で新しいゾーンを作成します。

システム定義のゾーン テンプレートを使用すると、Detector モジュールは、すべてのゾーン アトリビュートにデフォルト設定を適用します。

コマンドが正常に実行されると、Detector モジュールは新しいゾーンの設定モードに入ります。

ゾーン テンプレートを指定せずに既存のゾーンの名前を入力すると、Detector モジュールは、指定したゾーンの設定モードに入ります。

表 5-2 に、**zone** コマンドの引数とキーワードを示します。

表 5-2　zone コマンドの引数とキーワード

パラメータ	説明
new-zone-name	新しいゾーンの名前。名前は、1 ～ 63 文字の英数字の文字列です。この文字列は英字で始まる必要があり、アンダースコアを含むことができますが、スペースを含むことはできません。
zone-name	既存のゾーンの名前。

表 5-2　zone コマンドの引数とキーワード（続き）

パラメータ	説明
template-name	（オプション）ゾーンの設定を定義するゾーン テンプレート。デフォルトでは、DETECTOR_DEFAULT ゾーン テンプレートを使用してゾーンが作成されます。 ゾーン テンプレートは次のいずれかになります。 • GUARD_DEFAULT • GUARD_LINK_128K • GUARD_LINK_1M • GUARD_LINK_4M • GUARD_LINK_512K • GUARD_TCP_NO_PROXY • DETECTOR_DEFAULT • DETECTOR_LINK_128K • DETECTOR_LINK_1M • DETECTOR_LINK_4M • DETECTOR_LINK_512K • DETECTOR_WORM ゾーン テンプレートの詳細については、P.5-3 の「ゾーン テンプレートの使用」を参照してください。
interactive	（オプション）Detector モジュールがゾーン異常検出をインタラクティブ方式で実行するように設定します。ポリシーが作成する動的フィルタは、推奨事項として表示されます。各動的フィルタをアクティブにするかどうかを決定する必要があります。詳細については、第 10 章「インタラクティブ検出モードの使用方法」を参照してください。

次の例は、新しいゾーンを作成し、インタラクティブ検出モードに設定する方法を示しています。

```
user@DETECTOR-conf# zone scannet interactive
user@DETECTOR-conf-zone-scannet#
```

ゾーンを削除するには、**no zone** コマンドを使用します。ゾーンを削除するときは、ゾーン名の末尾に、ワイルドカード文字としてアスタリスク（*）を使用できます。ワイルドカードを使用すると、同じプレフィックスを持つ複数のゾーンを 1 つのコマンドで削除できます。

ゾーン テンプレートを表示するには、グローバル モードまたは設定モードで **show templates** コマンドを使用します。ゾーン テンプレートのデフォルト ポリシーを表示するには、グローバル モードまたは設定モードで **show templates** *template-name* **policies** コマンドを使用します。

既存のゾーンの複製による新しいゾーンの作成

既存のゾーンに基づいて、新しいゾーンを作成することができます。既存のゾーンを新しいゾーンのテンプレートとして使用すると、既存のゾーンのプロパティすべてが、新しく定義したゾーンにコピーされます。スナップショットを指定すると、ゾーン ポリシーはスナップショットからコピーされます。

ゾーンを複製するには、次のコマンドのいずれかを使用します。

- **zone** *new-zone-name* **copy-from-this** [*snapshot-id*]：このコマンドは、現在のゾーン設定を使用して新しいゾーンを作成するときに、ゾーン設定モードで使用します。
- **zone** *new-zone-name* **copy-from** *zone-name* [*snapshot-id*]：このコマンドは、指定されたゾーン設定を使用して新しいゾーンを作成するときに、設定モードで使用します。

表 5-3 に、**zone** コマンドの引数とキーワードを示します。

表 5-3　zone コマンドの引数とキーワード

パラメータ	説明
new-zone-name	新しいゾーンの名前。名前は、1 ～ 63 文字の英数字の文字列です。この文字列は英字で始める必要があります。アンダースコアを含むことができますが、スペースを含むことはできません。
copy-from-this	現在のゾーンの設定をコピーして、新しいゾーンを作成します。

表 5-3　zone コマンドの引数とキーワード（続き）

パラメータ	説明
copy-from	指定されたゾーンの設定をコピーして、新しいゾーンを作成します。
zone-name	既存のゾーンの名前。
snapshot-id	（オプション）既存のスナップショットの ID。詳細については、P.8-26 の「スナップショットの表示」を参照してください。

次の例は、現在のゾーンから新しいゾーンを作成する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# zone mailserver copy-from-this
user@DETECTOR-conf-zone-mailserver#
```

コマンドが正常に実行されると、Detector モジュールは新しいゾーンの設定モードに入ります。

新しいゾーンのポリシーには、未調整のマークが付けられます。ラーニング プロセスのしきい値調整フェーズを実行して、ポリシーのしきい値をゾーンのトラフィックに合せて調整する方法をお勧めします。新しいゾーンのトラフィック特性が、元になるゾーンのトラフィック特性と同じか、よく似ていれば、ポリシーのしきい値に調整済みのマークを付けることができます。詳細については、P.8-18 の「ポリシーに対する調整済みのマーク付け」を参照してください。

ゾーンのアトリビュートの設定

ゾーンを作成したら、ゾーンのアトリビュートを設定できます。

ゾーンのアトリビュートを設定するには、次の手順を実行します。

ステップ 1　ゾーン設定モードに入ります。すでにゾーン設定モードになっている場合、このステップは省略してください。

ゾーン設定モードに入るには、次のコマンドのいずれかを使用します。

- **conf** *zone-name*（グローバル モードから）
- **zone** *zone-name*（設定モードまたはゾーン設定モードから）

zone-name 引数には、既存のゾーンの名前を指定します。

（注）　**aaa authorization commands zone-completion tacacs+** コマンドを使用すると、**zone** コマンドにおけるゾーン名のタブ補完をディセーブルにすることができます。詳細については、P.4-19 の「ゾーン名のタブ補完のディセーブル化」を参照してください。

ステップ 2　**ip address** コマンドを使用して、ゾーンの IP アドレス を定義します。Detector モジュールがゾーン トラフィックをラーニングしてゾーンを検出できるようにするには、除外されない IP アドレスを少なくとも 1 つ定義する必要があります。

詳細については、P.5-13 の「ゾーンの IP アドレス範囲の設定」を参照してください。

ステップ 3　（オプション）ゾーン設定モードで次のコマンドを入力して、識別用の説明をゾーンに追加します。

description *string*

文字列の長さは最大 80 文字の英数字です。式にスペースを使用する場合は、式を引用符（" "）で囲みます。

ゾーンの説明を変更するには、ゾーンの説明を再入力します。前の説明は新しい説明で上書きされます。

ステップ 4　ゾーン設定モードで **show running-config** コマンドを入力して、新しく設定したゾーンの設定を表示します。

設定情報は、Detector モジュールを現在の設定値で設定するために実行される CLI コマンドで構成されています。詳細については、特定のコマンド エントリを参照してください。

次の例は、新しいゾーンを作成し、ゾーン アトリビュートを設定する方法を示しています。ゾーンの IP アドレス範囲は 192.168.100.32/27 に設定されていますが、IP アドレス 192.168.100.50 はこのゾーンの IP アドレス範囲から除外されています。

```
user@DETECTOR-conf# zone scannet
user@DETECTOR-conf-zone-scannet# ip address 192.168.100.32
255.255.255.224
user@DETECTOR-conf-zone-scannet# ip address exclude 192.168.100.50
user@DETECTOR-conf-zone-scannet# description Demonstration zone
user@DETECTOR-conf-zone-scannet# show running-config
```

ゾーンの IP アドレス範囲の設定

ゾーン異常検出をアクティブにする前に、除外されない IP アドレスを少なくとも 1 つ定義する必要がありますが、IP アドレスの IP アドレス範囲への追加や、IP アドレス範囲からの削除はいつでもできます。大規模なサブネットを設定し、特定の IP アドレスがゾーンの IP アドレス範囲に含まれないようにそのサブネットから除外することができます。

ゾーンの IP アドレスを設定するには、ゾーン設定モードで次のコマンドを使用します。

ip address [**exclude**] *ip-addr* [*ip-mask*]

表 5-4 に、**ip address** コマンドの引数とキーワードを示します。

表 5-4　ip address コマンドの引数とキーワード

パラメータ	説明
exclude	IP アドレスをゾーンの IP アドレス範囲から除外します。
ip-addr	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）。 デフォルトで、IP アドレスをゾーンの IP アドレス範囲に含めます。 この IP アドレスはサブネット マスクに一致している必要があります。クラス A、クラス B、またはクラス C のサブネット マスクを入力した場合、IP アドレスのホスト ビットは 0 である必要があります。
ip-mask	（オプション）IP 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）。デフォルトのサブネット マスクは、255.255.255.255 です。

次の例は、ゾーンの IP アドレス範囲を 192.168.100.32/27 に設定し、IP アドレス 192.168.100.50 をゾーンの IP アドレス範囲から除外する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# ip address 192.168.100.32
255.255.255.224
user@DETECTOR-conf-zone-scannet# ip address exclude 192.168.100.50
```

ゾーンの IP アドレス範囲を変更する場合は、次のタスクのいずれかを実行します。

- 新しい IP アドレスまたはサブネットが新しいサービスで構成され、そのサービスがゾーンのネットワークで定義されていない場合は、ゾーン検出をアクティブにする前にポリシー構築フェーズをアクティブにするか、サービスを手動で追加します。詳細については、P.8-6 の「ポリシーの構築」および P.7-15 の「サービスの追加」を参照してください。
- 検出およびラーニング機能をイネーブルにしている場合、**no learning-params threshold-tuned** コマンドを使用して、ゾーン ポリシーに未調整マークを付けます。ゾーン上で攻撃が行われている場合は、ゾーン ポリシーの状態を未調整に変更しないでください。ゾーン ポリシーの状態を変更すると、Detector モジュールは攻撃を検出できなくなり、Detector モジュールが悪意のあるトラフィックのしきい値をラーニングする原因になります。詳細については、P.8-18 の「ポリシーに対する調整済みのマーク付け」を参照してください。
- 検出およびラーニング機能を使用していない場合は、ゾーン異常検出をアクティブにする前に、しきい値調整フェーズをアクティブにする必要があります。P.8-10 の「ポリシーしきい値の調整」を参照してください。

ゾーンの IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

除外された IP アドレスを削除するには、**no ip address exclude** コマンドを使用します。

ゾーンの IP アドレスをすべて削除して IP アドレスを除外するには、**no ip address *** コマンドを使用します。

Detector モジュールの Guard とのゾーン設定の同期

ゾーンの設定およびポリシーを Guard のゾーンと同期させることができます。Detector モジュールは、ゾーン設定全体を Guard にコピーします。このプロセスにより、ゾーンを一度設定するだけで、Detector モジュールと Guard の両方で同じ設定とポリシーを維持できます。

Detector モジュールと Guard との通信には、認証と暗号化を提供する Secure Socket Layer（SSL）プロトコルが必要です。ゾーンを同期させる前に、SSL 通信接続チャネルを設定する必要があります。詳細については、P.4-28 の「Guard との通信の確立」を参照してください。

Detector モジュールが常にゾーン トラフィック特性をラーニングし、ゾーン ポリシーを最新状態に保ち、ゾーン トラフィックが絶え間なく Guard に宛先変更されるのを避けるように設定できます。

この項では、次のトピックについて取り上げます。

- 設定のガイドライン
- 同期用のゾーンの設定
- ゾーンの自動的な同期とエクスポート パラメータの設定
- ゾーン設定の自動的な同期
- Guard から Detector モジュールへのゾーン設定の同期
- Detector モジュールから Guard へのゾーン設定の同期
- ゾーン設定のオフラインでの同期
- ゾーン設定の自動エクスポート
- ゾーン設定の手動エクスポート
- サンプル シナリオ

設定のガイドライン

Guard と Detector モジュールとの間でゾーンを同期させるには、次のガイドラインに従います。

- 両方のデバイス タイプの設定パラメータを含む Guard ゾーン テンプレートのいずれかを使用して、Detector に新しいゾーンを作成します。詳細については、表 5-1 を参照してください。
- ゾーン ポリシーを正しく同期させるには、Guard と Detector モジュールの両方に向かって同じタイプのトラフィック（同じトラフィック レートやプロトコルなど）が流れるようにする必要があります。このように設定しない場合、ゾーンのグローバル ポリシーが高すぎるか、または低すぎるため、スプーフィングを利用した DDoS 攻撃から正しく保護されません。
- Detector モジュールを、Detector モジュール、および Detector モジュールと関連付ける Guard の中央設定ポイントとして使用します。Detector モジュールには、Detector モジュールと Guard デバイスに適用できるゾーン設定を作成するための Guard ゾーン テンプレートがあります。Detector モジュールでゾーン設定を作成し、その設定を、Detector モジュールと関連付けるすべての Guard にコピーします。
- デバイスを交換する場合や、Detector モジュールと Guard が通信に使用するインターフェイスの IP アドレスを変更する場合は、Detector モジュールと Guard が安全な通信に使用する SSL 証明書を再生成する必要があります。
- Guard 上のゾーン設定を確認します。アクティベーション範囲が **ip-address-only** で、アクティベーション方式が **zone-name-only** でない場合は、Detector モジュールがゾーンに対する攻撃が終了したことを確認するために使用するタイマーを、**protection-end-timer** コマンドで設定することをお勧めします。**protection-end-timer** の値を **forever** に設定すると、攻撃が終了しても Detector モジュールはゾーン保護を終了せず、特定の IP アドレスを保護するために作成したサブゾーンも削除しません。

同期用のゾーンの設定

Guard と Detector モジュールの間でゾーンを同期できますが、Guard ゾーン テンプレートを使用して新しいゾーンを Detector モジュールに作成する必要があります。これは、Guard ゾーン テンプレートで作成された新しいゾーンに、Guard 用と Detector モジュール用の 2 つの定義セットがあるためです。ゾーン テンプレートの詳細については、表 5-1 を参照してください。

ゾーンは、次の設定モードで設定できます。

- ゾーン設定モード：リモート Guard など、Detector に固有の定義を設定します。ゾーン設定モードに入るには、設定モードで **zone** 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。

  ```
  user@DETECTOR-conf-zone-scannet#
  ```

- Guard 設定モード：ユーザ フィルタなど、Guard に固有の定義を設定します。guard 設定モードに入るには、ゾーン設定モードで **guard-conf** 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。

  ```
  user@DETECTOR-conf-zone-scannet(guard)#
  ```

- ゾーン設定モードまたは guard 設定モード：IP アドレスなど、Guard と Detector の両方に共通の定義を設定します。

  Guard と Detector の両方に共通の設定を変更する場合、その変更は両方の定義セットに適用されます。たとえば、ゾーン設定モードでゾーンの IP アドレスを変更する場合、Guard のゾーン定義でも新しい IP アドレスに変更されます。guard 設定モードで Guard の新しいゾーン定義を表示できます。guard 設定モードでポリシーの動作状態を変更する場合、Detector のゾーン定義でもその動作状態が変更されます。

ゾーンを作成し、その同期について設定するには、次の手順を実行します。

ステップ 1　Guard ゾーン テンプレートのいずれかを使用して、Detector に新しいゾーンを作成します。

Detector は、ゾーン設定モードでの **show** コマンドの出力において、ゾーン ID フィールドの隣に（Guard/Detector）を表示します。

P.5-7 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。

ステップ 2　ゾーンの特性を設定します。

P.5-11 の「ゾーンのアトリビュートの設定」を参照してください。

ステップ 3　次のいずれかのコマンドを入力して guard 設定モードに入り、Guard に固有の特性を設定します。

- **guard-conf**：（ゾーン設定モードから入力）
- **configure** *zone-name* **guard-conf**：（グローバル モードから入力）
- **zone** *zone-name* **guard-conf**：（設定モードから入力）

zone-name 引数には既存のゾーンの名前を指定します。

Detector モジュールが guard 設定モードに入ります。CLI プロンプトでは、モードを示すため、カッコで囲まれた guard という単語（guard）がプロンプトに追加されます。

次の例は、guard 設定モードに入る方法を示しています。

```
user@DETECTOR-conf-zone-scannet# guard-conf
user@DETECTOR-conf-zone-scannet(guard)#
```

guard 設定モードでは、ユーザ フィルタ、フィルタ終了、ポリシー アクションまたはフィルタ アクションの drop など、Guard に固有のすべてのゾーン アトリビュートを設定できます。詳細については、『*Cisco Guard Configuration Guide*』を参照してください。

ゾーンの自動的な同期とエクスポート パラメータの設定

ゾーン設定をリモート Guard と自動的に同期させるように、またはゾーン設定を自動的にネットワーク サーバにエクスポートするように Detector モジュールを設定できます。

Detector モジュールは、次のアクションを実行します。

- Detector モジュールは、ゾーンの設定を、ゾーンのリモート Guard リストに定義されているすべてのリモート Guard と同期させます。ゾーンのリモート Guard リストが空の場合、Detector モジュールはゾーンの設定を、Detector のデフォルトのリモート Guard リストに定義されているリモート Guard と同期させます。1 つのリモート Guard との同期に失敗すると、Detector モジュールはリスト内の次のリモート Guard から続行します。

  ゾーンのリモート Guard リストと Detector のデフォルトのリモート Guard リストが両方とも空の場合、Detector はゾーンの設定を同期化しません。

  Guard 上に同じ名前のゾーンが存在する場合、既存の設定は新しい設定によって上書きされます。
- しきい値調整フェーズの結果が受け入れられる場合、Detector モジュールは、ゾーンのリモート サーバ リストに記載されているすべてのネットワーク サーバにゾーン設定をエクスポートします。リストが空の場合、Detector モジュールはデフォルトのリモート リストを検索します。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。

  ゾーンのリモート サーバ リストと Detector モジュールのデフォルトのリモート サーバ リストが両方とも空の場合、Detector モジュールはゾーンの設定をエクスポートしません。

ゾーンの設定の自動的な同期とエクスポートをイネーブルにするには、ゾーン設定モードで次のコマンドを使用します。

learning-params sync {**accept** | **remote-activate**}

表 5-5 で、**learning-params sync** コマンドのキーワードについて説明します。

表 5-5　learning-params sync コマンドのキーワード

パラメータ	説明
accept	ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定を同期化およびエクスポートします。
remote-activate	ゾーンの設定を同期させてから、リモート Guard をアクティブにします。リモート Guard 上の設定が最新でない場合にだけ、Detector モジュールはゾーン設定を同期させます。 Detector モジュールは、ゾーン設定をネットワーク サーバにエクスポートしません。

次の例は、ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定を自動的に同期化およびエクスポートする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params sync accept
```

自動的な同期とエクスポートをディセーブルにするには、**no learning-params sync** コマンドを使用します。

ゾーン設定の自動的な同期

ゾーン設定をリモート Guard と自動的に同期させるように Detector モジュールを設定できます。Detector モジュールは、ゾーン設定を Guard にコピーします。Guard 上に同じ名前のゾーンが存在する場合、既存の設定は新しい設定によって上書きされます。

Detector モジュールは、ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させます。ゾーンのリモート Guard リストが空の場合、Detector モジュールはゾーンの設定を、Detector モジュールのデフォルトのリモート Guard リストに定義されているリモート Guard と同期させます。1 つのリモート Guard との同期に失敗すると、Detector モジュールはリスト内の次のリモート Guard から続行します。

ゾーンのリモート Guard リストと Detector モジュールのデフォルトのリモート Guard リストが両方とも空の場合、Detector モジュールはゾーンの設定を同期化しません。

Detector モジュールがいつゾーン設定を同期させるかを定義するには、**learning-params sync** コマンドを使用します。詳細については、P.5-19 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

Guard から Detector モジュールへのゾーン設定の同期

Guard から Detector モジュールにゾーン設定をコピーすることにより、Guard 上のゾーン設定と Detector モジュール上のゾーン設定を同期させることができます。ゾーン ポリシーを攻撃の特性に合せて調整するために Guard のゾーン ポリシーを手動で変更し、その変更で Detector モジュールをアップデートしている場合は、Guard のゾーン設定を Detector モジュールに同期させる必要が生じる場合があります。次の 2 点が保証されるように、特定のポリシーのしきい値を固定値として設定したり、ポリシーのしきい値の固定乗数を設定することができます。

- Detector モジュールが正しいポリシーしきい値を持ち、将来の DDoS 攻撃を適切に検出できる。
- Detector モジュールから将来ゾーン設定を同期化したときに正しいゾーン設定が Guard で維持される。これは、Detector モジュールが継続してゾーン トラフィックの特性をラーニングする場合に必要になることがあります。

詳細については、P.7-25 の「固定値としてのしきい値の設定」および P.7-26 の「しきい値の乗数の設定」を参照してください。

Detector モジュールは、Guard からゾーンの設定をコピーします。既存の設定が新しい設定で上書きされます。

Guard からゾーン設定およびポリシーを Detector モジュールに同期させるには、次の手順を実行します。

ステップ 1　ゾーンが現在アクティブになっている場合は、ゾーン設定モードで **deactivate** コマンドを使用して、ゾーンを非アクティブにします。

ステップ 2　次のいずれかのコマンドを入力して、Detector モジュールのゾーン設定を Guard に同期させます。

- **sync zone** *zone-name remote-guard-address* **local**（グローバル モードで入力）
- **sync** *remote-guard-address* **local**（ゾーン設定モードで入力）

表 5-6 で、**sync** コマンドの引数について説明します。

表 5-6　sync コマンドの引数とキーワード

パラメータ	説明
zone	指定のゾーンの設定を同期させます。
zone-name	既存のゾーンの名前。
remote-guard-address	リモート Guard 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）。
local	Detector のゾーン設定を Guard に同期させます。

ステップ 3　同期プロセスを開始する前にゾーンがアクティブになっていた場合は、ゾーン設定モードで **detect** コマンドまたは **learning** コマンドを使用してゾーンを再度アクティブにします。

詳細については、第 9 章「ゾーンのトラフィックの異常の検出」および P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」を参照してください。

次の例は、ゾーン scannet を非アクティブにし、Guard のゾーン設定を IP アドレス 192.168.55.10 の Detector に同期させる方法を示しています。次に、ゾーンを再度アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# deactivate
user@DETECTOR-conf-zone-scannet# sync 192.168.55.10 local
user@DETECTOR-conf-zone-scannet# detect learning
```

Detector モジュールから Guard へのゾーン設定の同期

Guard がゾーン保護をアクティブにしたときに Guard のゾーン設定とポリシーが必ずアップデートされるように、ゾーン設定とポリシーを Guard のゾーンと同期させることができます。このプロセスによって、Detector でゾーンを一度設定し、継続的にゾーン トラフィックの特性をラーニングしたり、さらに、Guard で同一のゾーン設定とポリシーを保持することでゾーン トラフィックを常に Guard に宛先変更することを回避できます。

Detector は、ゾーンの設定を Guard にコピーします。Guard 上に同じ名前のゾーンが存在する場合、既存の設定は新しい設定によって上書きされます。

（注） ゾーンの同期プロセスを開始する前に、Guard が現在ゾーンを保護していないことを確認します。ゾーン保護を非アクティブにしてからゾーンの設定を同期させます。

次のいずれかのコマンドを入力して、Detector モジュールからゾーンの設定およびポリシーを同期させます。

- **sync zone** *zone-name* **local** {**remote-guards** | *remote-guard-address-to*}
（グローバル モードで入力）
- **sync local** {**remote-guards** | *remote-guard-address-to*}
（ゾーン設定モードで入力）

表 5-7 に、**sync** コマンドの引数とキーワードを示します。

表 5-7　sync コマンドの引数とキーワード

パラメータ	説明
zone	指定のゾーンの設定を同期させます。
zone-name	既存のゾーンの名前。
local	Detector モジュールのゾーンの設定とポリシーを Guard に同期させます。

表 5-7　sync コマンドの引数とキーワード（続き）

パラメータ	説明
remote-guards	ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させます。ゾーンのリモート Guard リストが空の場合は、ゾーンの設定を、Detector モジュールのデフォルトのリモート Guard リストに定義されているリモート Guard と同期させます。
remote-guard-address-to	リモート Guard の IP アドレス。Detector モジュールは、ゾーンの設定を指定されたリモート Guard と同期させます。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）。

次の例は、ゾーンの設定を、ゾーンのリモート Guard リストにあるすべてのリモート Guard と同期させる方法を示しています。

```
user@DETECTOR# sync zone scannet local remote-guards
```

次の例は、ゾーンの設定を IP アドレスが 192.168.100.5 のリモート Guard と同期させる方法を示しています。

```
user@DETECTOR-conf-zone-scannet# sync local 192.168.100.5
```

ゾーン設定のオフラインでの同期

Detector モジュールのゾーン設定と Guard のゾーン設定は、同期させることができます。これは、Detector モジュールと Guard の間で安全な通信チャネルを確立できない場合でも可能です。次のいずれかの場合は、ゾーン設定をオフラインで同期させることが必要になる場合があります。

- Guard が Detector モジュールにアクセスできない場合。
- Detector モジュールが Guard にアクセスできない場合。
- Detector モジュールが、Network Address Translation（NAT; ネットワーク アドレス変換）デバイス経由で Guard と通信する場合。

Detector モジュールのゾーン設定を Guard のゾーン設定とオフラインで同期させるには、FTP、SFTP、または SCP を使用して、まずゾーン設定を Detector モジュールからネットワーク サーバにエクスポートし、次にそのゾーン設定を手動で Guard にインポートします。Guard と Detector モジュールの間に安全な通信チャネルがないため、Detector モジュールがゾーン トラフィックの異常を検出したときは、Guard を手動でアクティブにしてゾーンを保護する必要があります。

Detector モジュールがゾーン設定を同期できるようにするには、次のタスクを実行する必要があります。

- Guard ゾーン テンプレートのいずれかを使用して、Detector モジュールにゾーンを作成する（P.5-7 の「ゾーン テンプレートからの新しいゾーンの作成」を参照）。
- Detector モジュールが SFTP 通信に使用する SSH 鍵を設定して、設定を SFTP または SCP を使用してネットワーク サーバにエクスポートする（P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照）。

Detector モジュールのゾーンと Guard のゾーン設定をオフラインで同期させるには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ソース デバイス（Guard または Detector モジュール）のゾーン設定をエクスポートします。

- 自動：特定の状態が発生すると必ずゾーン設定をエクスポートするように Detector モジュールを設定します。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。
- 手動：次のいずれかのコマンドをグローバル　モードで入力してゾーン設定をエクスポートします。
  - **copy zone** *zone-name* **guard-running-config ftp** *server remote-path* [*login password*]
  - **copy zone** *zone-name* **guard-running-config** {**sftp** | **scp**} *server remote-path login*

  詳細については、P.5-28 の「ゾーン設定の手動エクスポート」を参照してください。

ステップ 2　グローバル　モードで次のコマンドを入力して、ネットワーク　サーバからターゲット デバイスにゾーン設定をインポートします。

(注)　ゾーン設定をインポートする前に、ゾーンを非アクティブにします。

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **running-config** *server full-file-name login*
- **copy** *file-server-name* **running-config** *source-file-name*

詳細については、P.13-7 の「設定のインポートとアップデート」を参照してください。

ゾーン設定の自動エクスポート

Detector がゾーン設定をネットワーク サーバへ自動的にエクスポートするように設定できます。Detector は、ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定をエクスポートします（ラーニング プロセスのしきい値調整フェーズの結果がいつ受け入れられるかの詳細については、P.8-15 の「定期的なアクションの設定」を参照してください）。

ゾーン設定を自動的にエクスポートするには、ネットワーク サーバを設定する必要があります。ネットワーク サーバには、FTP、SFTP、または SCP が設定できます。ネットワーク サーバは、次のリストに設定できます。

- ゾーンのリモート サーバ リスト：Detector がゾーン設定をエクスポートする先のネットワーク サーバのリスト。
- Detector のデフォルトのリモート サーバ リスト：ネットワーク サーバのデフォルト リスト。ゾーンのリモート サーバ リストが空の場合、Detector は、このリスト上のサーバにゾーンの設定をエクスポートします。

ゾーン設定をネットワーク サーバに自動的にエクスポートするように Detector を設定するには、次の手順を実行します。

ステップ 1　**file-server** コマンドを入力してネットワーク サーバを定義します。

SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。

詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。

（注）　Detector が特定のネットワーク サーバにゾーン設定を自動的にエクスポートできるようにするには、Detector のデフォルトのリモート サーバ リストまたはゾーンのリモート サーバ リストにそのサーバを設定する必要があります。

ステップ 2　（オプション）ゾーン設定モードで次のコマンドを入力して、ネットワーク サーバをゾーンのリモート サーバ リストに追加します。

```
export sync-config file-server-name
```

file-server-name 引数には、ネットワーク サーバの名前を指定します。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。

リモート サーバ リストからネットワーク サーバを削除するには、コマンドの **no** 形を使用します。

ステップ 3　（オプション）ゾーン設定モードで次のコマンドを入力して、ネットワーク サーバを Detector のデフォルトのリモート サーバ リストに追加します。

```
export sync-config file-server-name
```

file-server-name 引数には、ネットワーク サーバの名前を指定します。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。

リモート サーバ リストからネットワーク サーバを削除するには、コマンドの **no** 形を使用します。

ステップ 4　**learning-params sync accept** コマンドを入力して、ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーン設定をネットワーク サーバに自動的にエクスポートするように Detector を設定します。

詳細については、P.5-19 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

次の例は、ゾーンのリモート サーバ リストにネットワーク サーバを追加する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# export sync-config Corp-FTP-Server
```

Detector モジュールがゾーン設定をエクスポートするために使用するネットワーク サーバのデフォルトのリストを表示するには、設定モードで **show sync-config file-servers** コマンドを使用します。

リモート サーバ リストを表示するには、ゾーン設定モードで **show sync-config file-servers** コマンドを使用します。

ゾーン設定の手動エクスポート

ゾーン設定をネットワーク サーバにエクスポートすることができます。Detector モジュールは、ゾーンの設定のうち、Guard にゾーンを設定するために必要な部分をエクスポートします。

グローバル モードで次のいずれかのコマンドを入力して、ゾーンの設定をネットワーク サーバにエクスポートします。

- **copy zone** *zone-name* **guard-running-config ftp** *server full-file-name* [*login password*]（ゾーンの設定を FTP サーバにエクスポートします）
- **copy zone** *zone-name* **guard-running-config** {**sftp** | **scp**} *server full-file-name login*（SFTP または SCP を使用してゾーンの設定をネットワーク サーバにエクスポートします）
- **copy zone** *zone-name* **guard-running-config** *file-server-name dest-file-name*（ゾーンの設定をネットワーク サーバにエクスポートします）

- **copy zone** *zone-name* **guard-running-config** *（ゾーン ファイル サーバ リストおよびデフォルトのファイル サーバ リストに定義されているネットワーク サーバにゾーンの設定をエクスポートします）

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 5-8 で、**copy guard-running-config** コマンドの引数について説明します。

表 5-8　copy guard-running-config コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	既存のゾーンの名前を指定します。Detector モジュールは、Guard に適用される、指定されたゾーン設定の一部をエクスポートします。
guard-running-config	ゾーンの設定のうち、Guard にゾーンを設定するために必要な部分だけをエクスポートします。
ftp	FTP を使用しているネットワーク サーバにゾーンの設定をエクスポートします。
sftp	SFTP を使用しているネットワーク サーバにゾーンの設定をエクスポートします。
scp	SCP を使用しているネットワーク サーバにゾーンの設定をエクスポートします。
server	ネットワーク サーバの 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 192.168.10.2）。
full-file-name	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。

表 5-8　copy guard-running-config コマンドの引数とキーワード（続き）

パラメータ	説明
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。
file-server-name	設定ファイルをエクスポートするネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。詳細については、P.13-2 の「ファイル サーバの設定」を参照してください。
destination-file-name	リモート サーバ上の設定ファイルの名前。Detector モジュールは、**file-server** コマンドを入力してネットワーク サーバに対して定義したディレクトリの宛先ファイル名を使用してネットワーク サーバ上に設定ファイルを保存します。
*	ゾーン設定のうち、ゾーンのリモート サーバ リストおよびデフォルトのリモート サーバ リストに定義されている、すべてのネットワーク サーバに Guard のゾーンを設定するために必要な部分のみをエクスポートします。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。

次の例は、ゾーンの設定を FTP サーバにエクスポートする方法を示しています。

```
user@DETECTOR-conf# copy zone scannet guard-running-config ftp
10.0.0.191 /root/ConfigFiles/scannet.txt <user> <password>
```

サンプル シナリオ

次のサンプル シナリオは、Detector モジュールのゾーン設定を Guard のゾーン設定と同期させて、Detector モジュールがゾーン トラフィック特性をラーニングする一方でゾーンを保護する方法を示しています。

1. Guard ゾーン テンプレートのいずれかを使用して、Detector モジュール上に新しいゾーンを作成および設定します。

   Detector は、ゾーン設定モードでの **show** コマンドの出力において、ゾーン ID フィールドの隣に（Guard/Detector）を表示します。

   詳細については、P.5-7 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。

2. Detector で、ゾーンの SSL リモート Guard リストまたはデフォルトの SSL リモート Guard リストに Guard を追加します。

   詳細については、P.9-12 の「デフォルトのリモート Guard リストの設定」および P.9-13 の「ゾーンのリモート Guard リストの設定」を参照してください。

3. **learning policy-construction** コマンドを入力して、Detector がゾーン ポリシーを構築するように設定します。

4. **detect learning** コマンドを入力して、Detector がトラフィックの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ポリシーしきい値を調整するように設定します。

   詳細については、第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

5. **learning-params periodic-action auto-accept** コマンドを使用して、Detector が 24 時間ごとにポリシーしきい値を受け入れ、次々に変化するトラフィック パターンに合せてゾーン ポリシーを最新のものにするように設定します。

   詳細については、P.8-15 の「定期的なアクションの設定」を参照してください。

6. Detector が、新しくラーニングしたポリシーのしきい値を受け入れるたびに、ゾーン設定を Guard と同期させるように設定し、Detector が新しいゾーン ポリシーのしきい値をラーニングした場合に、Guard のゾーン ポリシーも必ず更新されるようにします。

   learning-params sync コマンドを使用して、ゾーン設定を Detector と同期させるように Guard を設定します。詳細については、P.5-19 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

7. Guard によるゾーン保護をアクティブにする前に、Detector のゾーン設定を Guard のゾーン設定と同期させるように設定し、Guard がゾーン保護をアクティブにした場合に、Guard 上のゾーン設定とポリシーが必ず更新されるようにします。

   learning-params sync コマンドを使用します。

   詳細については、P.5-19 の「ゾーンの自動的な同期とエクスポート パラメータの設定」を参照してください。

8. Detector は、ゾーンに対する攻撃を検出すると、次の処理を実行します。

   - Guard のゾーン設定が更新されていることを確認する。Guard のゾーン設定が Detector のゾーン設定と同じものでない場合、Detector はゾーン設定を Guard と同期させます。
   - Guard をアクティブにしてゾーンを保護する（Guard がゾーン保護をアクティブにする）。
   - ゾーンのラーニング プロセスを停止するが、ゾーン トラフィックの異常の検出は続行し、Detector が悪意のあるトラフィックのしきい値をラーニングしないようにする。

   攻撃が進行中でも、Guard 上でゾーン ポリシーを変更できます。

   Detector は、Guard を常にポーリングします。Detector が、Guard がゾーン保護を非アクティブにしたことを確認し（攻撃が終了すると、Guard はゾーン保護を非アクティブにする）、トラフィックの異常がなくなったことを確認すると、Detector はゾーンの異常検出とラーニング プロセスを非アクティブにします。

9. ゾーン ポリシーを攻撃の特性に合せて調整するために Guard のゾーン ポリシーを手動で変更した場合、その新しいポリシーを Detector に同期させることができます。特定のポリシーしきい値を固定値として設定することや、ポリシーしきい値の固定乗数を設定することがゾーン トラフィックに必要になった場合に、この処理が重要になります。ゾーン設定を Detector と同期させることにより、Detector が正しいポリシーしきい値を持ち、将来のしきい値調整フェーズでしきい値を正しく計算し、正しいしきい値を持つ Guard ポリシーが更新されます。

   詳細については、P.7-25 の「固定値としてのしきい値の設定」および P.7-26 の「しきい値の乗数の設定」を参照してください。

   ゾーンの設定およびポリシーを Guard に同期させるには、次のアクションを実行します。

   - **deactivate** コマンドを入力して、ゾーンを非アクティブにする。
   - **sync** コマンドを入力して、Guard のゾーン設定を Detector に同期させる。

- **detect** コマンドを入力して、ゾーン検出を再度アクティブにする。

詳細については、P.5-21 の「Guard から Detector モジュールへのゾーン設定の同期」および第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

CHAPTER 6

ゾーンのフィルタの設定

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）のフィルタの設定方法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。

- ゾーン フィルタについて
- フレックスコンテンツ フィルタの設定
- バイパス フィルタの設定
- 動的フィルタの設定

ゾーン フィルタについて

ゾーン フィルタは、Detector モジュールが特定のトラフィック フローを処理する方法を定義します。これらのフィルタを設定して、Detector モジュールがトラフィックの異常検出で使用する、トラフィックの機能をカスタマイズすることができます。

ゾーン フィルタを使用すると、Detector モジュールは次の機能を実行できます。

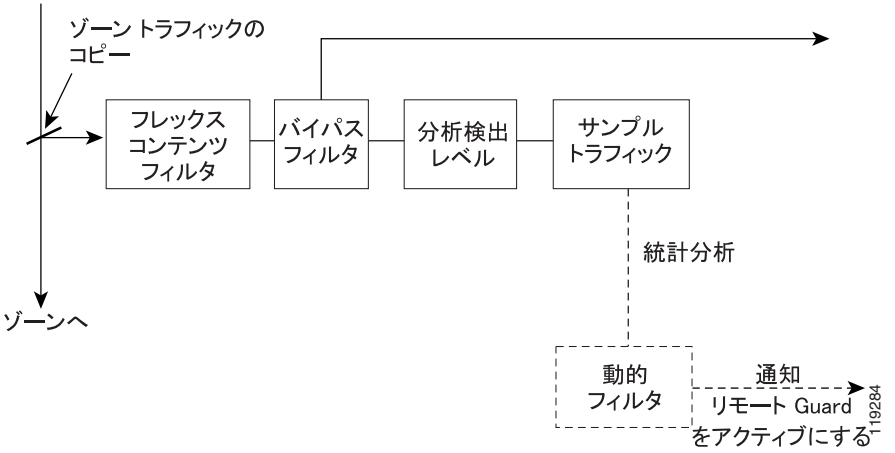
- 異常がないかゾーン トラフィックを分析する。
- トラフィックを直接ゾーンに転送し、Detector モジュールの異常検出機能をバイパスする。

Detector モジュールには、次のタイプのフィルタがあります。

- バイパス フィルタ：Detector モジュールが特定のトラフィック フローを処理しないようにします。信頼されたトラフィックが Detector モジュールの異常検出機能を通らないように誘導し、Detector モジュールによって分析されないようにすることができます。詳細については、P.6-18 の「バイパス フィルタの設定」を参照してください。
- フレックスコンテンツ フィルタ：特定のトラフィック フローをカウントします。IP ヘッダーや TCP ヘッダー内のフィールドに基づいたフィルタリング、ペイロード コンテンツに基づいたフィルタリング、複雑なブール式に基づいたフィルタリングなどの非常に柔軟なフィルタリング機能があります。詳細については、P.6-4 の「フレックスコンテンツ フィルタの設定」を参照してください。
- 動的フィルタ：必要な保護レベルを指定されたトラフィック　フローに適用します。Detector モジュールは、トラフィック フロー分析に基づいて動的フィルタを作成し、ゾーン トラフィックや Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃のタイプに合せて常に動的フィルタ セットを修正しています。動的フィルタは有効期間が限定されており、攻撃が終了すると削除されます。詳細については、P.6-22 の「動的フィルタの設定」を参照してください。

図 6-1 に、Detector モジュールのフィルタ システムを示します。

図 6-1　Detector のフィルタ システム



Detector モジュールは、この分析検出レベルをトラフィック フローに適用して、ゾーン トラフィックを分析します。バイパス フィルタを設定すると、Detector モジュールの検出機能をバイパスするように特定のフローを誘導できます。

トラフィック フローの統計分析を行うために、Detector モジュールには特定のタイプのトラフィックを処理する定義があります。この定義を、ゾーン ポリシーといいます。ゾーン ポリシーは、常にトラフィック フローを測定し、特定のトラフィック フローが悪意のあるものまたは異常である（トラフィック フローがポリシーのしきい値を超えた）と判断すると、そのフローに対してアクションを実行します。Detector モジュールがゾーンのトラフィックに異常を発見すると、イベントを自身の syslog に記録するか、新しいフィルタ（動的フィルタ）を作成します。動的フィルタが作成されると、リモート Guard リストに定義されている、ゾーンを保護する Guard をアクティブにできます。

フレックスコンテンツ フィルタの設定

フレックスコンテンツ フィルタは、パケット ヘッダー内のフィールドまたはパケット ペイロードのパターンに基づいて、ゾーン トラフィックをフィルタリングします。着信トラフィックに現れているパターンに基づいて攻撃を識別できます。これらのパターンでは、既知のワームまたは一定のパターンを持つフラッド攻撃が識別可能です。

(注) フレックスコンテンツ フィルタは大量の CPU リソースを消費します。フレックスコンテンツ フィルタは Detector モジュールのパフォーマンスに影響を及ぼす可能性があるため、使用を制限することをお勧めします。指定のポートに送信される TCP トラフィックなど、動的フィルタによって識別できる特定の攻撃からの検出にフレックスコンテンツ フィルタを使用する場合は、動的フィルタを使用してトラフィックをフィルタリングすることをお勧めします。

フレックスコンテンツ フィルタは、目的のパケット フローをカウントし、トラフィックの特定の悪意ある送信元を明らかにするために使用します。

フレックスコンテンツ フィルタは、次の順序でフィルタリング基準を適用します。

1. プロトコルとポートのパラメータ値に基づいてパケットをフィルタリングする。
2. tcpdump 式の値に基づいてパケットをフィルタリングする。
3. 残りのパケットに対して pattern-expression の値を使用してパターン マッチングを実行する。

この項では、次のトピックについて取り上げます。

- フレックスコンテンツ フィルタの追加
- フレックスコンテンツ フィルタの表示
- フレックスコンテンツ フィルタの削除
- フレックスコンテンツ フィルタの状態の変更

フレックスコンテンツ フィルタの追加

フレックスコンテンツ フィルタは、行番号の昇順でアクティブになります。新しいフレックスコンテンツ フィルタを追加する場合は、リストの適切な位置に配置してください。

フレックスコンテンツ フィルタを設定するには、次の手順を実行します。

ステップ 1　フレックスコンテンツ　フィルタのリストを表示して、リスト内で新しいフィルタを追加する位置を確認します。

詳細については、P.6-14 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　現在の行番号が連番の場合は、新しいフレックスコンテンツ　フィルタを挿入するために、フレックスコンテンツ フィルタ番号が増分するよう番号を割り当て直します。ゾーン設定モードで次のコマンドを入力します。

```
flex-content-filter renumber [start [step]]
```

表 6-1 に、**flex-content-filter renumber** コマンドの引数を示します。

表 6-1　flex-content-filter renumber コマンドの引数

パラメータ	説明
start	（オプション）フレックスコンテンツ フィルタ リストの新しい開始番号を示す 1 ～ 9,999 の整数。デフォルトは 10 です。
step	（オプション）フレックスコンテンツ フィルタの各行番号の増分を指定する 1 ～ 999 の整数。デフォルトは 10 です。

ステップ 3　（オプション）進行中の攻撃や、以前に記録された攻撃のパターン式をフィルタリングします。**show packet-dump signatures** コマンドを使用して、Detector モジュールをアクティブにして攻撃のシグニチャを生成します。

詳細については、P.12-33 の「パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成」を参照してください。

ステップ 4　次のコマンドを入力して、新しいフレックスコンテンツ フィルタを追加します。

```
flex-content-filter row-num {disabled | enabled} {drop | count}
protocol port [start start-offset [end end-offset]] [ignore-case]
expression tcpdump-expression pattern pattern-expression
```

表 6-2 に、**flex-content-filter** コマンドの引数とキーワードを示します。

表 6-2　flex-content-filter コマンドの引数とキーワード

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号。フィルタを識別し、複数のフレックスコンテンツ フィルタにおける優先順位を明確にします。Detector モジュールは、行番号の昇順でフィルタを操作します。
disabled	フィルタの状態をディセーブルに設定します。フィルタはトラフィックを監視しません。
enabled	フィルタの状態をイネーブルに設定します。Detector モジュールはトラフィックを監視し、フィルタに一致するフロー上でアクション（ドロップまたはカウント）を実行します。 これがデフォルトの状態です。
drop	フィルタに一致するフローをドロップします。Guard ゾーン テンプレートからゾーンを作成している場合は、Guard 設定モードにアクションのドロップを設定することができます。ドロップ アクションは Guard にのみ適用されます。
count	フィルタに一致するフローをカウントします。
protocol	特定のプロトコルからのトラフィック。すべてのプロトコルを示すには、アスタリスク（*）を使用します。0 ～ 255 の整数を入力します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers

表 6-2　flex-content-filter コマンドの引数とキーワード（続き）

パラメータ	説明
port	特定の宛先ポート宛てのトラフィック。0 ～ 65535 の整数を入力します。特定のポート番号を定義するには、特定のプロトコル番号を定義する必要があります。 すべての宛先ポートを示すには、アスタリスク（*）を使用します。プロトコル番号を 6（TCP）または 17（UDP）に設定する場合に、アスタリスクを使用できます。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
start-offset	パケット ペイロードの先頭から、*pattern-expression* 引数のパターン マッチングを開始する位置までのオフセット（バイト単位）。デフォルトは 0（ペイロードの先頭）です。0 ～ 1800 の整数を入力します。 **show packet-dump signatures** コマンド出力からパターンをコピーする場合は、コマンド出力の Start Offset フィールドからこの引数をコピーします。
end-offset	パケット ペイロードの先頭から、*pattern-expression* 引数のパターン マッチングを終了する位置までのオフセット（バイト単位）。デフォルトは、パケット長（ペイロードの末尾）です。0 ～ 1800 の整数を入力します。 **show packet-dump signatures** コマンド出力からパターンをコピーする場合は、コマンド出力の End Offset フィールドからこの引数をコピーします。
ignore-case	*pattern-expression* 引数で大文字と小文字が区別されないようにします。 デフォルトでは、*pattern-expression* 引数では大文字と小文字が区別されます。

表 6-2　flex-content-filter コマンドの引数とキーワード（続き）

パラメータ	説明
tcpdump-expression	パケットと照合する式。式はバークリー パケット フィルタの形式です。詳細および設定例については、P.6-9 の「tcpdump 式の構文の設定」を参照してください。 式にスペースを使用する場合は、式を引用符（" "）で囲みます。 空の式を入力するには、二重引用符（" "）を使用します。 式で引用符を使用するには、引用符の前にバックスラッシュをエスケープ文字として使用します（\"）。 **（注）** tcpdump 式の構文については、ヘルプを使用できません。
pattern-expression	パケット ペイロードと照合する正規表現のデータ パターン。詳細については、P.6-13 の「パターン式構文の設定」を参照してください。 Detector　モジュールをアクティブにし、**show　packet-dump signatures**　コマンドを使用してシグニチャを生成できます。P.12-33 の「パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成」を参照してください。 式にスペースを使用する場合は、式を引用符（" "）で囲みます。 空の式を入力するには、二重引用符（" "）を使用します。 式で引用符を使用するには、引用符の前にバックスラッシュをエスケープ文字として使用します（\"）。 **（注）** パターン式の構文については、ヘルプを使用できません。

フィルタの状態はいつでも変更できます。詳細については、P.6-16 の「フレックスコンテンツ フィルタの状態の変更」を参照してください。

次の例は、フレックスコンテンツ フィルタを設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * *
expression "ip[6:2] & 0x1fff=0" pattern "/ HTTP/1\.1\ x0D\0AAccept:
.*/.*\x0D\x0AAccept-Language: en*\x0D\x0AAccept-Encoding: gzip,
deflate\x0D\x0AUser-Agent: Mozilla/4\.0"
```

この項では、次のトピックについて取り上げます。

- tcpdump 式の構文の設定
- パターン式構文の設定

tcpdump 式の構文の設定

tcpdump 式はバークリー パケット フィルタ形式で、パケットと照合する式を指定します。

（注） 宛先ポートとプロトコルに基づいてトラフィックをフィルタリングする場合は、tcpdump 式を使用できます。ただし、パフォーマンスへの影響を考慮し、これらの基準でトラフィックをフィルタリングする場合は、フレックスコンテンツ フィルタで *protocol* 引数と *port* 引数を使用することをお勧めします。

式は 1 つ以上の要素からなります。通常、要素は ID（名前または番号）と ID の前に付く 1 つ以上の修飾子からなります。

修飾子には次の 3 つがあります。

- タイプ修飾子：ID（名前または番号）を定義します。指定可能なタイプは、**host**、**net**、および **port** です。**host** タイプ修飾子がデフォルトです。
- 方向修飾子：転送の方向を定義します。指定可能な方向は、**src**、**dst**、**src or dst**、および **src and dst** です。方向修飾子は **src or dst** がデフォルトです。
- プロトコル修飾子：特定のプロトコルへの照合を制限します。指定可能なプロトコルは **ether**、**ip**、**arp**、**rarp**、**tcp**、および **udp** です。プロトコル修飾子を指定しない場合、該当するタイプに適用されるすべてのプロトコルが照合されます。たとえば、ポート 53 とは、TCP または UDP のポート 53 を意味します。

表 6-3 に、tcpdump 式の要素を示します。

表 6-3　tcpdump 式の要素

要素	説明
dst host *host_ip_address*	宛先ホスト IP アドレスへのトラフィック。
src host *host_ip_address*	送信元ホスト IP アドレスからのトラフィック。
host *host_ip_ address*	送信元および宛先の両方のホスト IP アドレスの間のトラフィック。
net *net* mask *mask*	特定のネットワークへのトラフィック。
net *net/len*	特定のサブネットへのトラフィック。
dst port *destination_port_number*	宛先ポート番号への TCP または UDP トラフィック。
src port *source_port_number*	送信元ポート番号からの TCP または UDP トラフィック。
port *port_number*	送信元および宛先の両方のポート番号間の TCP または UDP トラフィック。
less *packet_length*	特定のバイト長以下の長さを持つパケット。
greater *packet_length*	特定のバイト長以上の長さを持つパケット。
ip proto *protocol*	ICMP、UDP、または TCP のプロトコル番号を持つパケット。
ip broadcast	ブロードキャスト IP パケット。
ip multicast	マルチキャスト パケット。
ether proto *protocol*	IP、ARP、または RARP などの特定のプロトコル番号またはプロトコル名を持つイーサネット プロトコル パケット。プロトコル名もキーワードです。プロトコル名を入力する場合は、プロトコル名の前にバックスラッシュ（\）をエスケープ文字として使用する必要があります。
expr relop expr	特定の式に適合するトラフィック。表 6-4 に、tcpdump 式の規則を示します。

表 6-4 に、tcpdump 式の規則を示します。

表 6-4　フレックスコンテンツ フィルタの式の規則

式の規則	説明
relop	>、<、>=、<=、=、!=
expr	整数の定数（標準の C 構文で表現されたもの）、通常のバイナリ演算子（+、-、*、/、&、|）、長さ演算子、および特殊なパケット データ アクセスで構成される算術式。パケット内のデータにアクセスするには、次の構文を使用します。 *proto* [*expr*: *size*]
proto	インデックス操作用のプロトコル層。指定可能な値は ether、ip、tcp、udp、または icmp です。指定されたプロトコル層までの相対的なバイト オフセットは、*expr* 値で指定します。 パケット内のデータにアクセスするには、次の構文を使用します。 *proto* [*expr*: *size*] *size* 引数はオプションで、フィールドのバイト数を指定します。この引数に可能な値は 1、2 または 4 です。デフォルトは 1 です。

次の方法により、式の要素を組み合せることができます。

- 要素と演算子の集まりを丸カッコで囲む：演算子は、通常のバイナリ演算子（+、-、*、/、&、|）と長さ演算子です。

(注) 式でカッコを使用するには、カッコの前にバックスラッシュをエスケープ文字として使用します（\(）。

- 否定：! または **not** を使用します。
- 連結：**&&** または **and** を使用します。
- 代替：|| または **or** を使用します。

否定は、最も高い優先度を持ちます。代替と連結の優先順位は同じで、左から右に関連付けられます。連結には、並置ではなく、明示的な and トークンが必要です。キーワードなしで識別子を指定した場合は、最後に指定されたキーワードが使用されます。

バークリー パケット フィルタの設定オプションの詳細については、次のサイトにアクセスしてください。

http://www.freesoft.org/CIE/Topics/56.htm

次の例は、断片化されていないデータグラムと断片化されたデータグラムのフラグメント 0 のみをカウントする方法を示しています。このフィルタは、TCP と UDP のインデックス操作に暗黙的に適用されます。たとえば、tcp[0] は常に TCP ヘッダーの最初のバイトを意味し、次の例で示すように中間のフラグメントの最初のバイトを意味することはありません。

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * *
expression ip[6:2]&0x1fff=0 pattern ""
```

次の例は、すべての TCP RST パケットをカウントする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# user@DETECTOR-conf-zone-scannet#
flex-content-filter enabled count * * expression tcp[13]&4!=0 pattern
""
```

次の例は、エコー要求およびエコー応答（ping）ではないすべての ICMP パケットをカウントする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * *
expression "icmp [0]!=8 and icmp[0] != 0" pattern ""
```

次の例は、ポート 80 を宛先とし、ポート 1000 を送信元としないすべての TCP パケットをカウントする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled count * *
expression "tcp and dst port 80 and not src port 1000" pattern ""
```

パターン式構文の設定

パターン式の構文とは、一連の文字を含んだ文字列を記述した正規表現です。パターン式は、一連の文字列をその要素を実際にリストせずに表現します。パターン式は、一般文字と特殊文字で構成されます。一般文字には、特殊文字とは見なされない印刷可能な ASCII 文字がすべて含まれます。特殊文字は特殊な意味を持ち、Detector モジュールがパターン式に対して実行するマッチングのタイプを指定します。フレックスコンテンツ フィルタは、パターン式とパケットの内容（パケット ペイロード）を照合します。たとえば、version 3.1、version 4.0、および version 5.2 という 3 つの文字列は、version .*\..* というパターンで表現できます。

表 6-5 に、使用可能な特殊文字を示します。

表 6-5　パターン式で使用する特殊文字

特殊文字	説明
.*	0 個またはそれ以上の文字を含んでいる文字列と照合します。たとえば、goo.*s は、goos、goods、good for ddos などと照合します。
\	特殊文字から特別な意味を取り除きます。リスト中の特殊文字を 1 つの文字パターンとして使用するには、各文字の先頭にバックスラッシュ（\）を入力して特殊な意味を取り除きます。たとえば、2 つのバックスラッシュ（\\）は 1 つのバックスラッシュ（\）と照合し、1 つのバックスラッシュとピリオド（\.）は 1 つのピリオドと照合します。 文字として使用するアスタリスク（*）の前にもバックスラッシュを配置する必要があります。
\xHH	16 進値と照合します。H は 16 進数の数字で、大文字と小文字は区別されません。16 進数の値は 2 桁である必要があります。たとえば、\x41 は 16 進数の値 A と照合します。

デフォルトでは、パターン式では大文字と小文字が区別されます。パターン式で大文字と小文字を区別しないようにするには、**flex-content-filter** コマンドに **ignore-case** キーワードを指定します。詳細については、P.6-5 の「フレックスコンテンツ フィルタの追加」を参照してください。

次の例は、パケット ペイロードに特殊なパターンを持つパケットをドロップする方法を示しています。この例のパターンは、Slammer ワームから抽出されました。*protocol*、*port*、および *tcpdump-expression* パラメータは特定のものでなくてもかまいません。

```
user@DETECTOR-conf-zone-scannet# flex-content-filter enabled drop * *
expression " " pattern
\x89\xE5Qh\.dllhel32hkernQhounthickChGetTf\xB911
Qh32\.dhws2_f\xB9etQhsockf\xB9toQhsend\xBE\x18\x10\xAEB
```

フレックスコンテンツ フィルタの表示

フレックスコンテンツ フィルタを表示するには、ゾーン設定モードで次のコマンドを入力します。

show flex-content-filters

表 6-6 に、**show flex-content-filters** コマンド出力のフィールドを示します。

表 6-6　show flex-content-filters コマンドのフィールドの説明

フィールド	説明
Row	フレックスコンテンツ フィルタの優先順位。
State	フィルタの状態（イネーブルまたはディセーブル）。
Action	フィルタが特定のトラフィック タイプに対して実行するアクション。
Protocol	フィルタが処理するトラフィックのプロトコル番号。
Port	フィルタが処理するトラフィックの宛先ポート。
Start	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット（バイト単位）。このオフセットは、*pattern* フィールドに適用されます。
End	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット（バイト単位）。このオフセットは、*pattern* フィールドに適用されます。

表 6-6　show flex-content-filters コマンドのフィールドの説明（続き）

フィールド	説明
Match-case	フィルタと一致するパターン式で、大文字と小文字が区別されるのか、またはされないのか。 yes の場合は大文字と小文字が区別され、no の場合は区別されません。
TCPDump-expression	パケットと照合する tcpdump 式（バークリー パケット フィルタ形式）。tcpdump 式の構文については、P.6-9 の「tcpdump 式の構文の設定」を参照してください。
Pattern-filter	パケット ペイロードと照合する正規表現のデータ パターン。パターン式の構文については、P.6-13 の「パターン式構文の設定」を参照してください。
RxRate (pps)	このフィルタが測定する現在のトラフィック レート（パケット / 秒）。

フレックスコンテンツ フィルタの削除

フレックスコンテンツ フィルタを削除するか、フレックスコンテンツ フィルタをディセーブルにして Detector モジュールがフィルタ式に基づくパケットのフィルタリングをしないようにすることができます。詳細については、P.6-16 の「フレックスコンテンツ フィルタの状態の変更」を参照してください。

フレックスコンテンツ フィルタを削除するには、次の手順を実行します。

ステップ 1　**show flex-content-filters** コマンドを使用してフレックスコンテンツ フィルタのリストを表示し、削除するフレックスコンテンツ フィルタの行番号を確認します。

次の例は、フレックスコンテンツ フィルタのリストを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show flex-content-filters
```

詳細については、P.6-14 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　**no flex-content-filter** *row-num* コマンドを入力して、フレックスコンテンツ フィルタを削除します。

row-num 引数には、削除するフレックスコンテンツ フィルタの行番号を指定します。すべてのフレックスコンテンツ フィルタを削除するには、*row-num* 引数としてアスタリスク（*）を入力します。

次の例は、フレックスコンテンツ フィルタを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no flex-content-filters 5
```

フレックスコンテンツ フィルタの状態の変更

フレックスコンテンツ フィルタをディセーブルにすると、Detector モジュールはフィルタ式に基づくパケットのフィルタリングと、特定の種類のトラフィックのフィルタリングを実行しなくなります（フィルタはフレックスコンテンツ フィルタのリストに保持されます）。

その後、Detector モジュールが指定されたトラフィックをフィルタリングするように再設定できます（フィルタの再設定は不要）。あるいは、フレックスコンテンツ フィルタを削除することもできます。詳細については、P.6-15 の「フレックスコンテンツ フィルタの削除」を参照してください。

フレックスコンテンツ フィルタの状態を変更するには、次の手順を実行します。

ステップ 1　フレックスコンテンツ　フィルタのリストを表示し、状態を変更するフレックスコンテンツ フィルタの行番号を確認します。

詳細については、P.6-14 の「フレックスコンテンツ フィルタの表示」を参照してください。

ステップ 2　次のコマンドを入力して、フレックスコンテンツ フィルタの状態を変更します。

flex-content-filter *row-num* {**disabled** | **enabled**}

row-num 引数には、フレックスコンテンツ フィルタの行番号を指定します。

次の例は、フレックスコンテンツ フィルタをディセーブルにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# flex-content-filters 5 disabled
```

バイパス フィルタの設定

バイパス フィルタは、特定のトラフィック フローを Detector モジュールが処理しないようにするためのものです。バイパス フィルタを設定して、信頼できるトラフィックを誘導して Detector モジュールの検出機能を通らないようにすることができます。

この項では、次のトピックについて取り上げます。

- バイパス フィルタの追加
- バイパス フィルタの表示
- バイパス フィルタの削除

バイパス フィルタの追加

バイパス フィルタを追加するには、ゾーン設定モードで次のコマンドを入力します。

bypass-filter *row-num src-ip* [*ip-mask*] *protocol dest-port* [*fragments-type*]

表 6-7 に、**bypass-filter** コマンドの引数を示します。

表 6-7　bypass-filter コマンドの引数

パラメータ	説明
row-num	1 ～ 9,999 の固有な番号。行番号はフィルタの ID で、これによって複数のバイパス フィルタの優先順位が定義されます。Detector モジュールは、行番号の昇順でフィルタを操作します。
src-ip	特定の IP アドレスからのトラフィックが処理されます。すべての IP アドレスを示すには、アスタリスク（*）を使用します。
ip-mask	（オプション）特定のサブネットからのトラフィックが処理されます。サブネット マスクには、クラス C の値のみを指定できます。デフォルトのサブネットは、255.255.255.255 です。

表 6-7　bypass-filter コマンドの引数（続き）

パラメータ	説明
protocol	特定のプロトコルからのトラフィックが処理されます。すべてのプロトコルを示すには、アスタリスク（*）を使用します。 指定可能なプロトコル番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/protocol-numbers
dest-port	特定の宛先ポート宛てのトラフィックが処理されます。すべての宛先ポートを示すには、アスタリスク（*）を使用します。 指定可能なポート番号については、次に示す Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の Web サイトを参照してください。 http://www.iana.org/assignments/port-numbers
fragments-type	（オプション）断片化されたトラフィックをフィルタが処理するかどうか。3 つの断片化のタイプは次のとおりです。 • **no-fragments**：断片化されていないトラフィック • **fragments**：断片化されたトラフィック • **any-fragments**：断片化されたトラフィックと断片化されていないトラフィック デフォルトは、**no-fragments** です。

（注） fragments-type と dest-port を両方指定することはできません。fragments-type を設定するには、dest-port にアスタリスク（*）を入力してください。

バイパス フィルタの表示

バイパス フィルタを表示するには、ゾーン設定モードで次のコマンドを入力します。

show bypass-filters

表 6-8 に、**show bypass-filters** コマンド出力のフィールドを示します。

表 6-8　show bypass-filters コマンドのフィールドの説明

フィールド	説明
Row	バイパス フィルタの優先順位。
Source IP	フィルタが処理するトラフィックの送信元 IP アドレス。
Source Mask	フィルタが処理するトラフィックの送信元アドレスのサブネット マスク。
Proto	フィルタが処理するトラフィックのプロトコル番号。
DPort	フィルタが処理するトラフィックの宛先ポート。
Frg	フィルタが処理する断片化の設定。 • **yes**：フィルタは断片化されたトラフィックを処理します。 • **no**：フィルタは断片化されていないトラフィックを処理します。 • **any**：フィルタは、断片化されたトラフィックと断片化されていないトラフィックの両方を処理します。
RxRate (pps)	このフィルタが測定する現在のトラフィック レート（パケット / 秒）。

送信元 IP アドレス、送信元アドレスのマスク、プロトコル番号、および宛先ポートは、特定のものでなくてもかまいません。アスタリスク（*）は、フィルタがすべてのフィールド値に対して動作するか、フィルタに複数の値が一致したことを示します。

バイパス フィルタの削除

バイパス フィルタを削除するには、次の手順を実行します。

ステップ 1　バイパス フィルタのリストを表示し、削除するバイパス フィルタの行番号を確認します。

詳細については、前の項「バイパス フィルタの表示」を参照してください。

ステップ 2　ゾーン設定モードで次のコマンドを入力して、バイパス フィルタを削除します。

no bypass-filter *row-num*

row-num 引数には、削除するバイパス フィルタの行番号を指定します。すべてのバイパス フィルタを削除するには、アスタリスク（*）を入力します。

次の例は、バイパス フィルタを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no bypass-filter 10
```

動的フィルタの設定

動的フィルタは必要な保護レベルをトラフィック フローに適用し、攻撃の処理方法を定義するものです。Detector モジュールは、ゾーン トラフィックに異常があると判断すると（フローがゾーン ポリシーのしきい値を超えたときに発生する）、動的フィルタを作成し、この動的フィルタ セットを常にゾーン トラフィックや DDoS 攻撃のタイプに適合させます。動的フィルタは有効期間が限定されており、攻撃が終了すると Detector モジュールが削除します。Detector モジュールは、すべてのゾーンで同時にアクティブな動的フィルタを最大 150,000 個サポートします。

動的フィルタは、Detector モジュールの syslog に通知レコードを作成するか、リモートの Guard をアクティブにしてゾーンを保護します。

この項では、次のトピックについて取り上げます。

- 動的フィルタの表示
- 動的フィルタの追加
- 動的フィルタの削除
- 動的フィルタの作成防止

動的フィルタの表示

Detector モジュールが作成した動的フィルタを表示することができます。このコマンドには、次のオプションが用意されています。

- **show dynamic-filters** [**details**]：すべての動的フィルタのリストを表示します。
- **show dynamic-filters** *dynamic-filter-id* [**details**]：特定の動的フィルタを 1 つ表示します。
- **show dynamic-filters sort** {**action** | **exp-time** | **id**}：すべての動的フィルタのソートされたリストを表示します。

保留動的フィルタを表示するには、**show recommendations** コマンドを使用します。保留動的フィルタの詳細については、第 10 章「インタラクティブ検出モードの使用方法」を参照してください。

表 6-9 に、**show dynamic-filters** コマンドの引数とキーワードを示します。

表 6-9　show dynamic-filters コマンドの引数とキーワード

パラメータ	説明
dynamic-filter-id	表示する特定の動的フィルタの ID[1]。この整数は Detector モジュールによって割り当てられます。フィルタの ID を確認するには、動的フィルタの完全なリストを表示します。
details	（オプション）動的フィルタを詳細に表示します。詳細情報には、攻撃フローに関する追加情報、トリガーとなるレート、およびそのフィルタを作成したポリシーなどがあります。
action	動的フィルタをアクション別に表示します。
exp-time	動的フィルタを有効期限の昇順で表示します。
id	動的フィルタを ID 番号の昇順で表示します。

1. ID = 識別番号

（注） Detector モジュールは、最大 1000 個の動的フィルタを表示します。1,000 を超える動的フィルタがアクティブになっている場合は、ログ ファイルまたはゾーンのレポートで、動的フィルタに関するすべてのリストを確認してください。

次の例は、動的フィルタを詳細に表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show dynamic-filters 876 details
```

表 6-10 に、**show dynamic-filters** コマンドの出力フィールドを示します。

表 6-10　show dynamic-filters コマンドの出力フィールドの説明

フィールド	説明
ID	フィルタの識別番号。
Action	フィルタがトラフィック フローに対して実行するアクション。

表 6-10　show dynamic-filters コマンドの出力フィールドの説明（続き）

フィールド	説明
Exp Time	フィルタがアクティブになっている時間。この時間が経過すると、フィルタは削除されます。
Source IP	フィルタが処理するトラフィックの送信元 IP アドレス。
Source Mask	フィルタが処理するトラフィックの送信元アドレスのマスク。
Proto	フィルタが処理するトラフィックのプロトコル番号。
DPort	フィルタが処理するトラフィックの宛先ポート。
Frg	フィルタが断片化されたトラフィックを処理するかどうか。 • **yes**：フィルタは断片化されたトラフィックを処理します。 • **no**：フィルタは断片化されていないトラフィックを処理します。 • **any**：フィルタは、断片化されたトラフィックと断片化されていないトラフィックの両方を処理します。
RxRate (pps)	このフィルタが測定する現在のトラフィック レート（パケット / 秒）。
Destination IP	フィルタが処理するトラフィックの宛先 IP アドレス。Detector モジュールは、宛先 IP アドレスおよびゾーンに設定されている **protect-ip-state** の値に基づいて Guard の保護をアクティブにします。

送信元 IP アドレス、送信元アドレスのマスク、プロトコル番号、および宛先ポートは、特定のものでなくてもかまいません。アスタリスク（*）は、フィルタがすべてのフィールド値に対して動作するか、フィルタに複数の値が一致したことを示します。

表 6-11 に、**show dynamic-filters details** コマンド出力の追加フィールドを示します。

表 6-11　show dynamic-filters details コマンドのフィールドの説明

フィールド	説明
Attack flow	攻撃フローの特性。攻撃フローは、Source IP、Source Mask、Proto、Dport、および Frg フィールドで構成されています。これらのフィールドについては、表 6-10 で説明しています。
Triggering Rate	ポリシーのしきい値を超過した攻撃フローのレート。
Threshold	攻撃フローによって超過したポリシーのしきい値。
Policy	動的フィルタを作成したポリシー。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

動的フィルタの追加

ゾーンの攻撃中に、動的フィルタを追加してゾーン異常検出を操作することができます。リモートの Guard リスト（リモート Guard）に定義されている Guard をアクティブにしてゾーンを保護するように動的フィルタを設定することができます。動的フィルタの宛先 IP アドレスが、**protect-ip-state** コマンドとゾーンのアドレス範囲を使用してゾーンに定義した Guard 保護アクティベーション方式と一致しないと、リモート アクティベーションは失敗します。リモート Guard のゾーン保護をアクティブ化するように動的フィルタを設定するには、次のいずれかの方法で実行します。

- ゾーン全体に対してリモート Guard のゾーン保護をアクティブ化する：ゾーン全体でゾーン保護をアクティブ化するには、*dst-ip* 引数を入力しないようにします。ゾーンの Guard 保護アクティベーション方式は、**entire-zone** または **policy-type** に設定する必要があります。
- ゾーン IP アドレス範囲にある特定の IP アドレスに対してのみリモート Guard のゾーン保護をアクティブ化する：特定の IP アドレスのゾーン保護をアクティブ化するには、*dst-ip* 引数を使用して特定の IP アドレスを指定します。ゾーンの Guard 保護アクティベーション方式は、**dst-ip-by-name** に設定する必要があります。

詳細については、P.9-8 の「ゾーンを保護するためのリモート Guard のアクティブ化」および P.9-5 の「Guard 保護のアクティベーション方式の設定」を参照してください。

動的フィルタを追加するには、ゾーン設定モードで次のコマンドを入力します。

dynamic-filter remote-activate {*exp-time* | **forever**} [*dst-ip*]

複数の動的フィルタを追加するには、複数の **dynamic-filter** コマンドを複数使用します。

表 6-12 に、**dynamic-filter** コマンドの引数とキーワードを示します。

表 6-12　dynamic-filter コマンドの引数とキーワード

パラメータ	説明
remote-activate	ゾーンを保護するためのリモート Guard をアクティブ化します。 引数 *dst-ip* を入力しないと、リモート Guard の保護をアクティブにするために Detector モジュールが使用するアクティベーション方式は **entire-zone** になります。
exp-time	フィルタがアクティブである期間（秒単位）を指定する、1 ～ 3,000,000 の整数。
forever	フィルタを無期限でアクティブにします。保護が終了すると、フィルタは削除されます。
dst-ip	（オプション）特定の宛先 IP アドレスまでのトラフィック。Detector モジュールは特定の IP アドレスに基づいてリモート Guard をアクティブにしてゾーンを保護します。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）。 Detector モジュールは、アクティベーション方式 dst-ip-by-name を使用してリモート Guard の保護をアクティブにします。

次の例では、ゾーン全体のリモート Guard の保護をアクティブにする動的フィルタの追加方法を示しています。

```
admin@GUARD-conf-zone-scannet# dynamic-filter remote-activate 600
```

動的フィルタの削除

動的フィルタを削除しても、削除が有効になっている期間は限られています。これは、ゾーン異常検出がイネーブルのときは、Detector モジュールが新しい動的フィルタの設定を続行するためです。Detector モジュールが動的フィルタを作成しないようにする方法の詳細については、P.6-28 の「動的フィルタの作成防止」を参照してください。

動的フィルタを削除するには、次の手順を実行します。

ステップ 1　動的フィルタのリストを表示し、削除する動的フィルタの ID を確認します。

詳細については、前の項「動的フィルタの表示」を参照してください。

ステップ 2　ゾーン設定モードで次のコマンドを入力して、関連する動的フィルタを削除します。

no dynamic-filter *dynamic-filter-id*

dynamic-filter-id 引数には、動的フィルタの ID を指定します。すべての動的フィルタを削除するには、アスタリスク（*****）を使用します。

次の例は、動的フィルタを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no dynamic-filter 876
```

動的フィルタの作成防止

不要な動的フィルタが作成されないようにするには、次のいずれかのアクションを実行します。

- 動的フィルタを作成するポリシーを非アクティブにします（詳細については、P.7-22 の「ポリシーの状態の変更」を参照）。不要な動的フィルタを作成したポリシーを特定するには、P.6-22 の「動的フィルタの表示」を参照してください。
- 目的のトラフィック フローにバイパス フィルタを設定します。詳細については、P.6-18 の「バイパス フィルタの設定」を参照してください。
- 不要な動的フィルタを作成するポリシーのしきい値を増分します。詳細については、P.7-24 の「ポリシーのしきい値の設定」を参照してください。

CHAPTER 7

ポリシー テンプレートとポリシーの設定

この章では、Cisco Traffic Anomaly Detector（Detector モジュール）のゾーン ポリシー、ポリシー構造、およびポリシー テンプレートについて説明します。また、ゾーン ポリシーとポリシー テンプレートのパラメータの設定方法についても説明します。

この章は、次の項で構成されています。

- ゾーン ポリシーについて
- ポリシー テンプレートについて
- ポリシー パスのセクションについて
- ポリシー パラメータの設定
- ワーム ポリシーについて
- ポリシーの監視
- ポリシー設定のバックアップ

ゾーン ポリシーについて

トラフィック フローの統計分析を行うために、Detector モジュールには特定のタイプのトラフィックを処理する定義があります。この定義を、ゾーン ポリシーといいます。ゾーン ポリシーは、トラフィック フローを常に分析し、特定のトラフィック フローがポリシーのしきい値を超え、悪意のあるトラフィックまたは異常なトラフィックであることを示した場合に、そのフローに対してアクションを実行します。フローがポリシーのしきい値を超えると、ポリシーはフィルタ（動的フィルタ）セットを動的に設定して、イベントを自身の syslog に記録するか、リモート Guard リストで定義した Guard をアクティブにします。Guard は、アクティブになると、攻撃を軽減してゾーンを保護します。

ゾーン ポリシーを作成するために、Detector モジュールは 2 つのフェーズのラーニング プロセスでゾーン トラフィックをラーニングします。Detector モジュールは事前定義されたポリシー テンプレートを使用してポリシーを構築し、それからポリシーのしきい値をラーニングします。各ポリシー テンプレートは、Detector モジュールが特定の Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃の脅威を検出するために必要なポリシーの作成に使用します。Detector モジュールがゾーン ポリシーを作成および調整を行ったら、ゾーン ポリシーの追加および削除、またはゾーン ポリシー パラメータの変更が行えます。

この項では、次のトピックについて取り上げます。

- ポリシー パスの使用
- ポリシーの作成

ポリシー パスの使用

ゾーン ポリシーは、Detector モジュールがゾーン トラフィック フローの分析と測定に使用する特性を定義します。ポリシーの名前はセクションで構成されており、各セクションは測定対象であるトラフィック特性を示しています。たとえば、ポリシー http/80/analysis/syns/src_ip は、Detector モジュールの分析検出機能によって認証され、送信元 IP アドレスに応じて集約された、ポート 80 宛ての HTTP SYN パケットのトラフィック フローを測定します。

図 7-1 に、ゾーン ポリシー名の例を示します。

図 7-1　ポリシー名

表 7-1 に、ポリシー名のセクションを示します。

表 7-1　ポリシー名のセクション

セクション	説明
ポリシー テンプレート	ポリシーの構築に使用されたポリシー テンプレート。各ポリシー テンプレートは、特定の DDos 攻撃の脅威の検出のために Detector モジュールが必要とする特性を扱います。詳細については、P.7-5 の「ポリシー テンプレートについて」を参照してください。
サービス	ゾーン ポリシーが監視するトラフィック フローのポート番号またはプロトコル番号。詳細については、P.7-14 の「サービス」を参照してください。
検出レベル	Detector モジュールがトラフィック フローに適用する検出レベル。詳細については、P.7-18 の「検出レベル」を参照してください。
パケット タイプ	Detector モジュールが監視するパケット タイプ。詳細については、P.7-18 の「パケット タイプ」を参照してください。
トラフィック特性	Detector モジュールがポリシーの集約に使用するトラフィック特性。詳細については、P.7-19 の「トラフィック特性」を参照してください。

ポリシー名の最初の 4 つのセクション（ポリシー テンプレート、サービス、検出レベル、および パケット タイプ）は、分析されるトラフィックのタイプを定義します。ポリシー パスの最後のセクション（トラフィック特性）は、フローの分析方法を定義します。

ポリシーには、相互依存性および優先度があります。2 つの異なるポリシーが同じトラフィック フローを定義している場合、Detector モジュールは、より限定的なポリシーを使用してフローを分析します。たとえば、TCP サービスに関連するポリシーでは、HTTP 関連のポリシーによって処理される HTTP サービスが除外されます。

ポリシーの動作面を設定できます。動作面では、ポリシーのトリガーを定義し、ポリシーがアクティブになったときに実行するアクションを定義します。詳細については、P.7-21 の「ポリシー パラメータの設定」を参照してください。

ポリシーの作成

Detector モジュールは、次の 2 つのフェーズで構成されるラーニング プロセスでゾーン ポリシーを作成します。これらのフェーズでは、Detector モジュールはゾーン トラフィックをラーニングし、特定のゾーン トラフィック特性に合せて自己調整します。

1. ポリシー構築フェーズ：Detector モジュールは、ポリシー テンプレートを使用してゾーン ポリシーを構築し、ゾーンが使用する主なサービスを検出します。
2. しきい値調整フェーズ：Detector モジュールは、ポリシー構築フェーズで検出されたサービスのポリシーしきい値を、ゾーン サービスのトラフィック レートに合せて調整します。

ラーニング プロセス中、ゾーン トラフィックは Detector モジュールを透過的に通過します。詳細については、P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」を参照してください。

ポリシー テンプレートについて

ポリシー テンプレートとは、Detector モジュールがポリシー構築フェーズでゾーン ポリシーを作成するときに使用する、ポリシー構築の規則の集まりです。ポリシー テンプレートの名前は、テンプレートから作成されるすべてのポリシーに共通の特性に由来し、プロトコル（DNS など）、アプリケーション（HTTP など）、または目的（ip_scan など）が使用されます。たとえば、ポリシー テンプレート *tcp_connections* は、同時接続数など、接続に関連するポリシーを生成します。新しいゾーンを作成する場合、Detector モジュールのゾーン設定には一連のポリシー テンプレートが用意されています。

この項では、次のトピックについて取り上げます。

- 各種ポリシー テンプレートのタイプについて
- ポリシー テンプレート パラメータの設定

各種ポリシー テンプレートのタイプについて

表 7-2 で、Detector モジュールのポリシー テンプレートについて説明します。DETECTOR_DEFAULT ゾーン テンプレートを使用して新しいゾーンを作成する場合、Detector モジュールには次のポリシー テンプレートが用意されています。

表 7-2　ポリシー テンプレート

ポリシー テンプレート	構築されるポリシーのグループが関連する対象
dns_tcp	DNS-TCP プロトコル トラフィック。
dns_udp	DNS-UDP プロトコル トラフィック。
fragments	断片化されたトラフィック。
http	ポート 80（デフォルト）または他のユーザ設定ポートを経由する HTTP トラフィック。

表 7-2　ポリシー テンプレート（続き）

ポリシー テンプレート	構築されるポリシーのグループが関連する対象
ip_scan	IP スキャニング（1 つのクライアントが特定の送信元 IP アドレスからゾーン内の多数の宛先 IP アドレスにアクセスしようとする状況）。ポリシー テンプレートは、主に IP アドレス定義がサブネットであるゾーン向けに設計されています。 デフォルトでは、このポリシー テンプレートはディセーブルになっています。このポリシー テンプレートのデフォルト アクションは、notify です。 **（注）** このポリシー テンプレートから生成されたポリシーはリソース消費量が多いため、パフォーマンスに影響を及ぼす可能性があります。
other_protocols	TCP 以外のプロトコルと UDP 以外のプロトコル。
port_scan	ポート スキャンニング（1 つのクライアントが特定の送信元 IP アドレスからゾーン内の多数のポートにアクセスしようとする状況）。 デフォルトでは、このポリシー テンプレートはディセーブルになっています。このポリシー テンプレートのデフォルト アクションは、notify です。 **（注）** このポリシー テンプレートから生成されたポリシーはリソース消費量が多いため、パフォーマンスに影響を及ぼす可能性があります。
tcp_connections	TCP 接続の特性。
tcp_not_auth	Detector モジュールのスプーフィング防止機能によって認証されていない TCP 接続。
tcp_outgoing	ゾーンによって開始された TCP 接続。
tcp_ratio	異なるタイプの TCP パケット間の比率。たとえば、FIN/RST パケットに対する SYN パケットの比率など。

表 7-2　ポリシー テンプレート（続き）

ポリシー テンプレート	構築されるポリシーのグループが関連する対象
tcp_services	HTTP 関連のポート（ポート 80 やポート 8080 など）以外のポート上の TCP サービス。
udp_services	UDP サービス。

Detector モジュールには、特定のタイプの攻撃または特定のサービス向けに設定されているゾーン テンプレートから作成されたゾーン用に追加のポリシー テンプレートがあります。表 7-3 に、特定のゾーン テンプレートに基づいて Detector モジュールがゾーン設定に追加する、ポリシー テンプレートを示します。

表 7-3　追加のポリシー テンプレート

ゾーン テンプレート	ポリシー テンプレート
DETECTOR_WORM	worm_tcp：TCP ワームを特定するポリシーのグループを構築します。TCP ポリシーは、ワーム攻撃を管理します。この攻撃では、1 つまたは複数の送信元 IP アドレスから、多数の宛先 IP アドレスに対する多数の未確立の接続が同一ポート上に作成されます。ポリシー テンプレートは、主に IP アドレス定義がサブネットであるゾーン向けに設計されています。 Detector モジュールは、ポリシー構築フェーズではなく、ラーニング プロセスのしきい値調整フェーズで、このポリシー テンプレートから作成されたポリシーにサービスを追加します。ポリシー テンプレート パラメータの max_services と min_threshold は、このポリシー テンプレートには適用されません。詳細については、P.7-34 の「ワーム ポリシーについて」を参照してください。

GUARD_ ゾーン テンプレートからゾーンを作成する場合、Guard に同期させることができる追加のポリシー テンプレートのパラメータを設定できます。Detector モジュールは、表 7-4 に示すポリシー テンプレートを使用して tcp_connections と tcp_outgoing のポリシー テンプレートを http_ns、

tcp_connections_ns および tcp_outgoing_ns policies のポリシー テンプレートに置き換えます。http_ns、tcp_connections_ns、および tcp_outgoing_ns の各ポリシー テンプレートは、Guard に対し、トラフィック フローに強化保護レベルを適用するよう要求するアクションを持つポリシーは作成しません。

表 7-4 に、Detector モジュールの GUARD_TCP_NO_PROXY ポリシー テンプレートの詳細を示します。

表 7-4　GUARD_TCP_NO_PROXY のポリシー テンプレート

ポリシー テンプレート	置き換えるポリシー テンプレート	構築されるポリシーのグループが関連する対象
tcp_connections_ns	tcp_connections	TCP 接続の特性。
tcp_outgoing_ns	tcp_outgoing	ゾーンによって開始された TCP 接続。
http_ns	http	ポート 80（デフォルト）または他のユーザ設定ポートを経由する HTTP トラフィック。

すべてのポリシー テンプレートのリストを表示するには、ゾーン設定モードで **policy-template** コマンドを使用し、**Tab** キーを 2 回押してください。

ポリシー テンプレート パラメータの設定

ラーニング プロセス中、ゾーン トラフィックは Detector モジュールを透過的に通過します。アクティブな各ポリシー テンプレートは、ポリシー定義とゾーン トラフィック特性に基づいてポリシー グループを作成します。Detector モジュールは、トラフィック量のレベルに応じて、ポリシー テンプレートが監視するサービス（プロトコルとポート番号）をランク付けします。次に Detector モジュールは、トラフィック量が最大のサービスと、定義済みの最小しきい値を超えたサービスを選択し、各サービスに対するポリシーを作成します。ポリシー テンプレートの中には、特定のポリシーが追加されなかったすべてのトラフィック フローを処理する、*any* というサービスを備えた追加のポリシーを作成するものもあります。

次のポリシー テンプレート パラメータを設定できます。

- サービスの最大数の設定：Detector モジュールがポリシー テンプレートを選択して特定のポリシーを作成する対象になるサービスの最大数を定義します。
- 最小しきい値の設定：Detector モジュールでサービスをランク付けするために超える必要のある最小しきい値を定義します。
- ポリシー テンプレートの状態の設定：Detector モジュールがポリシー テンプレートからポリシーを作成するかどうかを定義します。

ポリシー テンプレート パラメータである、サービスの最大数と最小しきい値は、worm_tcp ポリシー テンプレートには影響しません。

ポリシー テンプレートのパラメータを設定するには、ゾーン設定モードで次のコマンドを入力して、ポリシー テンプレート設定モードに入ります。

policy-template *policy-template-name*

policy-template-name 引数には、ポリシー テンプレートの名前を指定します。詳細については、表 7-2 を参照してください。

このコマンドを実行すると、Detector モジュールはポリシー テンプレート設定モードに入ります。

次の例は、http ポリシー テンプレート設定モードに入る方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy-template http
user@DETECTOR-conf-zone-scannet-policy_template-http#
```

特定のポリシー テンプレートのパラメータを表示するには、ポリシー テンプレート設定モードで **show** コマンドを使用します。

この項では、次のトピックについて取り上げます。

- サービスの最大数の設定
- 最小しきい値の設定
- ポリシー テンプレートの状態の設定
- すべてのポリシー テンプレート パラメータの同時設定

サービスの最大数の設定

サービスの最大数のパラメータで、ポリシー テンプレートが選択してポリシーを作成する対象となるサービスの最大数（プロトコル番号またはポート番号）を定義します。Detector モジュールは、各サービスのトラフィック量のレベルによってサービスをランク付けします。次に Detector モジュールは、トラフィック量が最大のサービスと、定義済みの最小しきい値（min-threshold パラメータで定義される）を超えたサービスを選択し、各サービスに対するポリシーを作成します。Detector モジュールは **any** というサービスを備えた追加のポリシーを追加し、ポリシー テンプレートの特性を持つその他のすべてのトラフィック フローを処理することができます。

（注） サービスの最大数が大きいほど、ゾーンが必要とする Detector モジュールのメモリも多くなります。

サービスの最大数のパラメータは、サービスを検出するポリシー テンプレート（tcp_services、tcp_services_ns、udp_services、および other protocols など）にのみ定義できます。特定のサービスを監視するポリシー テンプレート（サービス 53 を監視する *dns_tcp* など）や、特定のトラフィック特性に関連するポリシー テンプレート（*fragments* など）には、このパラメータは設定できません。

Detector モジュールは、ポリシーのトラフィック特性に基づいて、サービスのトラフィック レートを測定します。トラフィック特性は、送信元 IP アドレスまたは宛先 IP アドレスになります。**any** サービスを監視するポリシーは、特定のポリシーで処理されないすべてのサービスで送信元 IP アドレスのレートを測定します。したがって、こちらの値は正確ではありません。

サービス数を制限すると、目的のトラフィック フロー要件に合せて Detector モジュールのポリシーを設定できます。

サービスの最大数を設定するには、ポリシー テンプレート設定モードで次のコマンドを使用します。

max-services *max-services*

max-services 引数は、Detector モジュールが選択するサービスの最大数を定義する、1 より大きい整数です。サービスの最大数が 10 を超えないようにすることをお勧めします。

次の例は、Detector モジュールが監視するサービスの最大数を 5 に設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy_template-tcp_services#
max-services 5
```

最小しきい値の設定

最小しきい値のパラメータは、サービスの最小トラフィック量を定義します。このしきい値を超えると、Detector モジュールは、しきい値を超えた特定のトラフィック フローに応じて、サービスのトラフィックに関連するポリシーを構築します。このしきい値を設定すると、ゾーン サービスのトラフィック量に異常検出を合せることができます。

最小しきい値のパラメータは、正しいゾーン異常検出に不可欠で必ずポリシーを構築するポリシー テンプレート（tcp_services、udp_services、other_protocols、http、および fragments）には設定できません。

最小しきい値を設定するには、ポリシー テンプレート設定モードで次のコマンドを使用します。

min-threshold *min-threshold*

min-threshold 引数は、0 以上の実数（小数点以下が 2 桁の浮動小数点型の数字）で、最小しきい値レートをパケット / 秒（pps）単位で定義します。同時接続および SYN/FIN の比率を測定する場合、しきい値は接続の合計数を定義する整数になります。

次の例は、ポリシー テンプレート http の最小しきい値を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy_template-http# min-threshold
12.3
```

ポリシー テンプレートの状態の設定

ポリシー テンプレートの状態のパラメータは、ポリシー テンプレートをイネーブルまたはディセーブルにするかどうかを定義します。Detector モジュールが、ディセーブルになっているポリシー テンプレートをポリシー構築フェーズ中に使用してポリシーを作成することはできません。

注意　ポリシー テンプレートをディセーブルにすると、ゾーン異常検出に重大な支障をきたすおそれがあります。ポリシー テンプレートをディセーブルにすると、Detector モジュールはそのポリシー テンプレートに関連するゾーン トラフィックを検出できません。たとえば、dns_udp ポリシー テンプレートをディセーブルにすると、Detector モジュールは、DNS（UDP）攻撃を管理するゾーン ポリシーを作成しなくなります。

ポリシー テンプレートをディセーブルにするには、**disable** コマンドを使用します。

ポリシー テンプレートをイネーブルにするには、**enable** コマンドを使用します。

すべてのポリシー テンプレート パラメータの同時設定

次のコマンドを入力して、1 つのコマンドで、ポリシー テンプレートのすべての動作パラメータを設定できます。

policy-template *policy-template-name max-services min-threshold* {**disabled** | **enabled**}

表 7-5 に、**policy-template** コマンドの引数とキーワードを示します。

表 7-5　policy-template コマンドの引数とキーワード

パラメータ	説明
policy-template-name	ポリシー テンプレート名。詳細については、表 7-1 を参照してください。
max-services	Detector モジュールが選択して特定のポリシー テンプレートからポリシーを構築する対象となるサービスの最大数。 Detector モジュールで現在の値が変更されないようにするには、-1 という値を入力します。 詳細については、P.7-10 の「サービスの最大数の設定」を参照してください。
min-threshold	Detector モジュールでサービスをランク付けするために超える必要のある最小しきい値。 Detector モジュールで現在の値が変更されないようにするには、-1 という値を入力します。 詳細については、P.7-11 の「最小しきい値の設定」を参照してください。
disabled	ポリシー テンプレートをディセーブルにして、ポリシーが作成されないようにします。詳細については、P.7-12 の「ポリシー テンプレートの状態の設定」を参照してください。
enabled	ポリシー テンプレートをイネーブルにします。詳細については、P.7-12 の「ポリシー テンプレートの状態の設定」を参照してください。

次の例は、ポリシー テンプレート tcp_services のパラメータを設定する方法を示しています。この例では、サービスの最大数は 3 に、ポリシーの状態は **enabled** に設定され、最小しきい値は変更されていません（-1）。

```
user@DETECTOR-conf-zone-scannet# policy-template tcp_services 3 -1
enabled
```

ポリシー パスのセクションについて

ポリシー パスは、次のセクションで構成されます。

- ポリシー テンプレート
- サービス
- 検出レベル
- パケット タイプ
- トラフィック特性

ポリシー テンプレート

ポリシー テンプレートとは、Detector モジュールがポリシー構築フェーズでゾーン ポリシーを作成するときに使用する、ポリシー構築の規則の集まりです。詳細については、P.7-5 の「ポリシー テンプレートについて」を参照してください。

サービス

サービス セクションは、各ポリシーに関連するゾーン アプリケーションのポートまたはプロトコルを定義します。ポリシーには、相互依存性および優先度があります。2 つの異なるポリシーが同じトラフィック フローを定義している場合、Detector モジュールは、より限定的なポリシーを使用してフローを分析します。サービス **any** は、同じポリシー テンプレートから作成された他のサービスと特に一致しないすべてのトラフィックに関連します。

個々のニーズに最適な異常検出にするために、ゾーンのメイン サービスに具体的なポリシーを定義することをお勧めします。

注意　パフォーマンスを低下させるおそれがあるため、複数のポリシーに同じサービス（ポート番号）を追加しないでください。

ゾーン ポリシーへのサービスの追加またはゾーン ポリシーからのサービスの削除を行うと、Detector モジュールはそのゾーン ポリシーに未調整のマークを付けます。ゾーン異常検出とラーニング プロセスをイネーブルにした場合、次のいずれかの操作を実行するまで、Detector モジュールはゾーン トラフィックの異常を検出できません。

- ラーニング　プロセスのしきい値調整フェーズを実行して、その結果を受け入れる（P.8-10 の「ポリシーしきい値の調整」を参照）。
- ゾーンのポリシーを調整済みとしてマークする（P.8-18 の「ポリシーに対する調整済みのマーク付け」を参照）。

この項では、次のトピックについて取り上げます。

- サービスの追加
- サービスの削除

サービスの追加

特定のポリシー テンプレートから作成されたすべてのポリシーに、サービスを追加できます。新しいサービスは、ポリシー構築フェーズ中に検出されたサービスに追加され、デフォルト値で定義されます。しきい値を手動で定義することもできますが、ラーニング プロセスのしきい値調整フェーズを実行して、ポリシーをゾーン トラフィックに合せて調整することをお勧めします。詳細については、P.8-10 の「ポリシーしきい値の調整」を参照してください。

新しいサービスを追加できるのは、次のポリシー テンプレートから作成されたポリシーです。

- tcp_services、udp_services、tcp_services_ns、または worm_tcp

  このサービスは、ポート番号を表します。
- other_protocols

  このサービスは、プロトコル番号を表します。

（注） サービスを追加した後でポリシー構築フェーズをアクティブにすると、新しいサービスによって、手動で追加したサービスが無効にされる場合があります。

次の状況では、ポリシー構築を再度実行しない場合は、サービスを手動で追加する必要があります。

- 新しいアプリケーションまたはサービスがゾーン　ネットワークに追加された。
- ポリシー構築フェーズの実行期間が短かったため、一部のネットワーク サービスが反映されていない（たとえば、週に 1 回のみあるいは夜間のみアクティブになる既知のアプリケーションまたはサービスがある）。

サービスを追加するには、次のコマンドのいずれかを使用します。

- **add-service** *service-num*（ポリシー テンプレート設定モードの場合）
- **policy-template** *policy-template-name* **add-service** *service-num*（ゾーン設定モードの場合）

表 7-6 に、**add-service** コマンドの引数を示します。

表 7-6　add-service コマンドの引数

パラメータ	説明
service-num	プロトコル番号またはポート番号。
policy-template-name	ポリシー テンプレート名。詳細については、表 7-2 を参照してください。

次の例は、ポリシー テンプレート tcp_services から作成されたすべてのポリシーに、サービスを追加する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy_template-tcp_services#
add-service 25
```

サービスの削除

すべてのポリシー テンプレートから作成された特定のサービスを削除できます。Detector モジュールは、特定のポリシー テンプレートから作成されたすべてのポリシーからサービスを削除します。

サービスを削除するには、次のコマンドのいずれかを使用します。

- **remove-service** *service-num*（ポリシー テンプレート設定モードの場合）

- **policy-template** *policy-template-name* **remove-service** *service-num*（ゾーン設定モードの場合）

表 7-7 に、**remove-service** コマンドの引数を示します。

表 7-7　remove-service コマンドの引数

パラメータ	説明
service-num	削除するプロトコル番号またはポート番号。
policy-template-name	ポリシー テンプレート名。詳細については、表 7-2 を参照してください。

注意　サービスを削除すると、Detector モジュールはそのサービスのトラフィックを監視できなくなり、ゾーン異常検出に支障をきたすおそれがあります。

次のポリシー テンプレートからサービスを削除できます。

- tcp_services、udp_services、または tcp_services_ns

  このサービスは、ポート番号です。
- other_protocols

  このサービスは、プロトコル番号です。

次の状況では、ラーニング プロセスのポリシー構築フェーズを実行しない場合は、サービスを手動で削除する必要があります。

- アプリケーションまたはサービスがネットワークから削除された。
- （ネットワーク環境では一般的でないため）イネーブルにしていないアプリケーションまたはサービスが、ポリシー構築フェーズ中に識別された。

（注）　サービスを削除した後でポリシー構築フェーズをアクティブにすると、同じサービスが再度追加される場合があります。

次の例は、ポリシー テンプレート tcp_services から作成されたすべてのポリシーから、サービスを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy_template-tcp_services#
remove-service 25
```

検出レベル

Guard は分析検出レベルをトラフィック フローに適用します。

(注)　検出レベルの設定は静的であり、手動で設定することはできません。

パケット タイプ

Detector モジュールはパケット特性を監視します。パケット特性は、次のいずれかです。

- パケット タイプ（TCP-SYN パケットなど）
- パケット分析（認証済みパケットなど。認証済みパケットとは、パケット接続で TCP ハンドシェイクを実行していることを Detector モジュールが確認済みであるパケットのこと）
- パケット方向（着信接続など）

表 7-8 で、Detector モジュールが監視するパケット タイプについて説明します。

表 7-8　パケット タイプ

パケット タイプ	説明
auth_pkts	TCP ハンドシェイクまたは UDP 認証が実行されたパケット。
auth_tcp_pkts	TCP ハンドシェイクが実行されたパケット。
auth_udp_pkts	UDP 認証が実行されたパケット。
in_nodata_conns	接続上でデータ転送のないゾーン着信接続（データ ペイロードのないパケット）。

表 7-8　パケット タイプ（続き）

パケット タイプ	説明
in_conns	ゾーン着信接続。
in_pkts	ゾーンの着信 DNS クエリー パケット。
in_unauth_pkts	ゾーンの認証されていない着信 DNS クエリー。
non_estb_conns	未確立の接続。失敗したゾーンの着信接続。応答が受信されなかった TCP 接続要求（SYN パケット）です。
out_pkts	ゾーンの着信 DNS 応答パケット。
reqs	データ ペイロードを持つ要求パケット。
syns	同期パケット（TCP SYN フラグの付いたパケット）。
syn_by_fin	SYN および FIN フラグの付いたパケット。Detector モジュールは、SYN フラグの付いたパケット数と FIN フラグの付いたパケット数の比率を確認します。
unauth_pkts	TCP ハンドシェイクが実行されなかったパケット。
pkts	同じ検出レベルの他のどのカテゴリにも入らないすべてのパケット タイプ。

トラフィック特性

トラフィック特性とは、トラフィック フローをどのように分析するか、またポリシーの集約にどのような特性が使用されたかを定義するものです。分析するトラフィックが同じでも、異なる特性に基づいてレートを測定する異なるポリシーがあります。次にその例を示します。

dns_tcp/53/analysis/pkts/dst_ip と dns_tcp/53/analysis/pkts/src_ip。

表 7-9 で、Detector モジュールが監視するトラフィック特性について説明します。

表 7-9　トラフィック特性

トラフィック特性	説明
dst_ip	ゾーンの IP アドレス宛てのトラフィック。
dst_ip_ratio	特定の IP アドレス宛ての、SYN フラグの付いたパケットと FIN フラグの付いたパケットの比率。

表 7-9　トラフィック特性（続き）

トラフィック特性	説明
dst_port	特定のゾーン ポート宛てのトラフィック。
dst_port_ratio	特定のポート宛ての、SYN フラグの付いたパケットと FIN フラグの付いたパケットの比率。
global	他のポリシー セクションによって定義されたすべてのトラフィック フローの合計。
protocol	プロトコルに基づいて集約された、ゾーン宛てのトラフィック。
scanners	特定の宛先ポート上でゾーン宛先 IP アドレスをスキャンする送信元 IP アドレスの数のヒストグラム。詳細については、P.7-34 の「ワーム ポリシーについて」を参照してください。
src_ip	送信元 IP アドレスに応じて集約された、ゾーン宛てのトラフィック。
src_ip_many_dst_ips	多数のゾーン IP アドレスが同じポートにあることを調査する 1 つの IP アドレスからのトラフィック。このキーは IP スキャニングに使用されます。
src_ip_many_ports	1 つのゾーン宛先 IP アドレスに多数のポートがあることを調査する 1 つの IP アドレスからのトラフィック。このキーはポート スキャニングに使用されます。

ポリシー パラメータの設定

ラーニング プロセスが完了したら、特定のポリシー パラメータ（ポリシーの状態、ポリシーのしきい値、ポリシーのタイムアウト、ポリシーのアクション、およびポリシーのインタラクティブ状態）を表示し、そのポリシー パラメータがゾーン トラフィックに適しているかどうかを判断できます。単一のポリシーまたはポリシー グループのポリシー パラメータがゾーン トラフィック要件を満たすように設定できます。

ポリシー パラメータの設定を表示するには、ポリシー設定モードで **show** コマンドを使用します。

ポリシー設定モードに入るには、ゾーン設定モードで次のコマンドを使用します。

policy *policy-path*

policy-path 引数には、ポリシー パス セクションを指定します。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。

(注)　ポリシー パス階層で 1 レベル上に移動するには、ポリシー パス プロンプトで **policy ..** を入力します。

次の例は、dns_tcp/53/analysis/syns/global ポリシー設定モードに入る方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy
dns_tcp/53/analysis/syns/global
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global
#
```

ポリシーの *アクション*、*タイムアウト*、*しきい値*、およびラーニングのパラメータは、ポリシー パスの各セクションで変更できます。ただし、上位レベルのポリシー セクション（ポリシー テンプレート セクションまたはサービス セクションなど）でこれらのパラメータを変更すると、より多くのポリシーが影響を受けます。上位レベルのポリシー パス階層でこれらのパラメータを設定すると、すべてのサブポリシー パスでこれらのパラメータが変更されます。

各ポリシー パス セクションでは、ワイルドカード文字としてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しないと、指定していないセクションが Detector モジュールによってワイルドカード（*）と見なされます。たとえば、ポリシー tcp_services//analysis//global では、サービスとパケット タイプにワイルドカードが使用されています。

この項では、次のトピックについて取り上げます。

- ポリシーの状態の変更
- ポリシーのしきい値の設定
- ポリシーのタイムアウトの設定
- ポリシーのアクションの設定
- ポリシーのインタラクティブ ステータスの設定

ポリシーの状態の変更

ゾーン ポリシーには、次の 3 つの状態があります。

- アクティブ：ポリシーはトラフィックを監視し、しきい値を超えた場合にアクションを実行します。
- 非アクティブ：ポリシーはトラフィックを監視し、しきい値を取得しますが、しきい値を超えてもアクションは実行しません。ポリシーを非アクティブにし、ラーニング プロセスのしきい値調整フェーズが再度実行されないようにすることができます。
- ディセーブル：ポリシーはトラフィック　フローを監視しないため、しきい値を取得しません。

（注） Detector　モジュールが他のポリシーの正確なしきい値を監視するようにするには、ラーニング プロセスのしきい値調整フェーズをアクティブにすることをお勧めします。

注意　あるポリシーをディセーブルにすると、ディセーブルにされたそのポリシーの監視対象だったトラフィックに対して、アクティブなゾーン ポリシーが責任を負うことになります。アクティブなポリシーのしきい値を調整するには、ゾーン異常検出をアクティブにする前に、しきい値調整フェーズをアクティブにすることをお勧めします。

ポリシーの状態を変更するには、ポリシー設定モードで次のコマンドを使用します。

state {**active** | **disabled** | **inactive**}

次の例は、ポリシー状態を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns#
state disabled
```

次の例は、すべてのグローバル ポリシーの状態を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/*/*/*/global# state notify
```

注意　ポリシーを非アクティブまたはディセーブルにすると、ゾーン　ポリシーが機能しなくなるおそれがあり、そのためゾーン異常検出に支障をきたすおそれがあります。

ゾーン ポリシーをディセーブルにした後でポリシー構築フェーズを実行すると、現在のトラフィック フローに応じてすべてのゾーン ポリシーが再設定され、ポリシーが再度アクティブになることがあります。

ポリシーのしきい値の設定

ポリシーのしきい値は、特定のポリシーのしきい値トラフィック レートを定義するもので、しきい値調整フェーズで調整されます。このしきい値を超過すると、ポリシーはポリシー アクションによって定義されたアクションを実行します。

しきい値は、次のポリシー テンプレートで構築されたポリシーを除き、パケット / 秒で測定されます。

- num_soruces：しきい値は IP アドレスまたはポートの数で測定されます。
- tcp_connections：しきい値は接続の数で測定されます。
- tcp_ratio：しきい値は比率値で測定されます。
- worm_tcp：しきい値は、送信元 IP からスキャンできるゾーン宛先 IP アドレスの最大数として測定されます。

ポリシーのしきい値は、次の方法で設定できます。

- しきい値を設定する

  ポリシーのしきい値の値を設定できます。P.7-25 の「ポリシーのしきい値の設定」を参照してください。
- しきい値を乗算する

  Detector モジュールは、現在のポリシーのしきい値に係数を掛けます。新しい値を固定値として設定しない場合、後続のしきい値調整フェーズでこの値が変更されることがあります。P.7-28 の「係数によるしきい値の乗算」を参照してください。
- 特定の IP しきい値を設定する

  Detector モジュールは、ゾーン アドレス範囲内で、特定の IP 送信元アドレスのしきい値を設定します。P.7-29 の「特定の IP しきい値の設定」を参照してください。

ポリシーのしきい値は、しきい値調整フェーズをさらに実行すると変更される場合があります。後続のしきい値調整フェーズでしきい値が変更されるかどうかは、次の方法で指定できます。

- しきい値を固定値として設定する

  Detector モジュールは、以後のしきい値調整フェーズで、ポリシーのしきい値（proxy-threshold および threshold-list）の値を変更しません。P.7-25 の「固定値としてのしきい値の設定」を参照してください。

- ポリシーのしきい値に固定乗数を設定する

  Detector モジュールは、以後のしきい値調整フェーズで、現在のポリシーのしきい値、ラーニングしたしきい値、および固定乗数に基づいてポリシーのしきい値を計算します。P.7-26 の「しきい値の乗数の設定」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。

- ポリシーのしきい値の設定
- 固定値としてのしきい値の設定
- しきい値の乗数の設定
- 係数によるしきい値の乗算
- 特定の IP しきい値の設定

ポリシーのしきい値の設定

ポリシーのしきい値を設定するには、ポリシー設定モードで次のコマンドを使用します。

threshold *threshold*

threshold 引数は、ポリシーのしきい値を指定する正数です。

次の例は、ポリシー policy dns_tcp/53/analysis/syns/global のしきい値を 300 に設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/global
# threshold 300
```

固定値としてのしきい値の設定

ポリシーのしきい値（proxy-threshold および threshold-list）を固定値として設定できます。Detector モジュールは、ラーニング プロセスのしきい値調整フェーズで新しいしきい値を無視し、現在のしきい値を保持します。しきい値を固定値として設定することにより、ポリシーのしきい値を設定しながらも、引き続き他のポリシーのしきい値をラーニングすることが可能になります。

ポリシーのしきい値を固定値として設定するには、ポリシー設定モードで次のコマンドを使用します。

learning-params fixed-threshold

次の例は、ポリシー policy dns_tcp/53/analysis/syns/global のしきい値を固定値に設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/syns/
global# learning-params fixed-threshold
```

ゾーン設定モードで次のコマンドを入力すると、1 つのコマンドで複数のポリシーのしきい値を固定値に設定できます。ゾーン設定モードでポリシーのしきい値を固定値として設定するには、次のコマンドを使用します。

policy *policy-path* **learning-params fixed-threshold**

policy-path 引数には、ポリシー パスを指定します。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。

次の例は、ポリシー テンプレート dns_tcp から作成されたすべてのポリシーのしきい値を固定値にする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp learning-params
fixed-threshold
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-params** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-params** コマンドを使用します。

しきい値の乗数の設定

ポリシーのしきい値の乗数を設定できます。Detector モジュールは、以後のしきい値調整フェーズの結果を受け入れる前に、指定された乗数をラーニングしたしきい値に掛けて新しいポリシーのしきい値を計算します。Detector モジュールは、設定されているしきい値選択方式を使用して、しきい値調整フェーズの結果を受け入れます。P.8-17 の「しきい値選択方式の設定」を参照してください。

ポリシーのしきい値の乗数を設定するには、ゾーン設定モードで次のコマンドを使用します。

policy *policy-path* **learning-params threshold-multiplier** *threshold-multiplier*

表 7-10 に、**policy learning-params threshold-multiplier** コマンドの引数とキーワードを示します。

表 7-10　policy learning-params threshold-multiplier コマンドの引数とキーワード

パラメータ	説明
policy-path	しきい値を掛ける対象のポリシー パス。パスは、ポリシー セクションの一部のみを含む部分パスでもかまいません。詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。
learning-params	ラーニング パラメータを設定します。
threshold-multiplier *threshold-multiplier*	ポリシーのしきい値を乗算します。*threshold-multiplier* は、ポリシーのしきい値に掛ける正の実数（小数点以下が 2 桁の浮動小数点型の数字）。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。

ポリシー設定モードでポリシーのしきい値の乗数を設定するには、**learning-params threshold-multiplier** *threshold-multiplier* コマンドを使用します。

次の例は、以後のしきい値調整フェーズで Detector モジュールがポリシー テンプレート dns_tcp から作成されたポリシーのしきい値を半減するように、しきい値乗数を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp learning-params
threshold-multiplier 0.5
```

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-params** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-params** コマンドを使用します。

係数によるしきい値の乗算

ポリシーまたはポリシー グループのしきい値に係数を掛けて、トラフィック量がゾーン トラフィックを表していない場合に、ポリシーまたはポリシー グループのしきい値を増減することができます。Detector モジュールでは、ポリシーのしきい値、プロキシのしきい値、および **policy threshold-list** コマンドで定義されたしきい値の乗算をイネーブルにできます。

ポリシーのしきい値と係数を乗算するには、ゾーン設定モードで次のコマンドを使用します。

policy *policy-path* **thresh-mult** *threshold-multiply-factor*

表 7-11 に、**policy thresh-mult** コマンドの引数とキーワードを示します。

表 7-11　policy thresh-mult コマンドの引数とキーワード

パラメータ	説明
policy-path	ポリシー テンプレート名。詳細については、表 7-2 を参照してください。
thresh-mult *threshold-multiply-factor*	しきい値に掛ける正の実数（小数点以下が 4 桁の浮動小数点型の数字）を指定します。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。

次の例は、ポリシー テンプレート dns_tcp から作成されたポリシーのしきい値を半減する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy */*/*/*/src_ip thresh-mult 0.5
```

（注） Detector モジュールは、後続のしきい値調整フェーズでしきい値を変更する場合があります。Detector モジュールがしきい値を変更しないようにするには、しきい値を固定値として設定します。P.7-25 の「固定値としてのしきい値の設定」を参照してください。

ポリシーのラーニング パラメータを表示するには、ポリシー設定モードで **show learning-params** コマンドを使用するか、ゾーン設定モードで **show policies** *policy-path* **learning-params** コマンドを使用します。

特定の IP しきい値の設定

トラフィックが大量であることがわかっている送信元または宛先 IP アドレスでトラフィックが増加したときに、Detector モジュールが攻撃を誤って検出しないようにするには、その IP アドレスに関連付けられたトラフィック用のしきい値を持つポリシーを設定します。

次の状況のいずれかが発生した場合は、特定の IP しきい値を設定することを考慮する必要があります。

- ある送信元 IP アドレスから大量のトラフィックがあることがわかっている場合は、特定の送信元 IP アドレスからのトラフィックに適用するしきい値を設定できる。
- 非同種ゾーン（複数の IP アドレスで構成されるゾーン）があり、そのゾーンの一部にのみ大量のトラフィックが流れることがわかっている場合は、そのゾーン内の特定の宛先 IP アドレスを対象とするトラフィックに適用するしきい値を設定できる。

宛先 IP（dest_ip）というトラフィック特性を持つポリシーだけに、特定の IP しきい値を設定できます。

特定の IP しきい値を設定するには、次のコマンドのいずれかを使用します。

- **policy** *policy-path* **threshold-list** *ip threshold* [*ip threshold ...*]（ゾーン設定モードの場合）
- **threshold-list** *ip threshold* [*ip threshold ...*]（ポリシー設定モードの場合）

表 7-12 に、**threshold-list** コマンドの引数を示します。

表 7-12　policy threshold-list コマンドの引数

パラメータ	説明
policy-path	ポリシー テンプレート名。詳細については、表 7-2 を参照してください。
ip	具体的な IP アドレス。
threshold	しきい値トラフィック レート（パケット / 秒）。ただし、同時接続および SYN 対 FIN の比率を測定するポリシーの場合、しきい値は接続数になります。

ポリシーごとに特定の IP しきい値を 10 個まで追加できます。特定の IP しきい値をすべて 1 つのコマンドで入力できます。

Detector モジュールは、しきい値選択方式が new-thresholds に設定されている場合、以後のしきい値調整フェーズでポリシーのしきい値を変更する可能性があります。詳細については、P.8-17 の「しきい値選択方式の設定」を参照してください。

次の例は、ポリシー http/80/analysis/syns/src_ip に、IP アドレス 10.10.10.2 および 10.10.15.2 の特定の IP しきい値を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip#
threshold-list 10.10.10.2 500 10.10.15.2 500
```

ポリシーのタイムアウトの設定

タイムアウト パラメータは、ポリシーによって作成される動的フィルタがアクションを適用する最小期間を定義します。

ポリシーのタイムアウトを設定するには、ポリシー設定モードで次のコマンドを使用します。

timeout {**forever** | *timeout*}

表 7-13 に、**timeout** コマンドの引数とキーワードを示します。

表 7-13　timeout コマンドの引数とキーワード

パラメータ	説明
forever	無限の期間を指定します。
timeout	ポリシーによって生成される動的フィルタがアクティブである最小期間を秒単位指定する 1 ～ 3,000,000 の整数。

次の例は、ポリシー http/80/analysis/syns/src_ip のタイムアウトを 100 秒に設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip#
timeout 100
```

ポリシー グループのタイムアウトを同時に変更するには、ゾーン設定モードで **policy set-timeout** コマンドを使用します。

次の例は、HTTP ポリシー テンプレートから作成されたすべてのポリシーのタイムアウトを 100 秒に設定し、送信元 IP アドレスを測定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy http/*/*/*/src_ip set-timeout
100
```

ポリシーのアクションの設定

アクション パラメータは、しきい値を超過したときにポリシーが実行するアクションのタイプを定義します。

ポリシー アクションを設定するには、ポリシー設定モードで次のコマンドを使用します。

action *policy-action*

表 7-14 に、ポリシー アクションを示します。

表 7-14　ポリシーのアクション

ポリシーのアクション	説明
notify	しきい値を超過した場合に通知します。
remote-activate	しきい値超過が発生すると、リモート Guard をアクティブにします。リモート Guard はリモート Guard リストに定義されています。詳細については、P.9-8 の「ゾーンを保護するためのリモート Guard のアクティブ化」を参照してください。

次の例は、ポリシー http/80/analysis/syns/src_ip にアクションを設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/http/80/analysis/syns/src_ip#
action remote-activate
```

ポリシー グループのアクションを同時に変更するには、ゾーン設定モードで **policy set-action** コマンドを使用します。

次の例は、すべての dns_tcp ポリシーにアクションを設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# policy dns_tcp/ set-action
remote-activate
set action of dns_tcp/ to remote-activate:
4 policy actions set.
```

ポリシーのインタラクティブ ステータスの設定

インタラクティブ ステータスのパラメータは、ゾーン ポリシーによって作成される保留動的フィルタのインタラクティブ ステータスを定義します。インタラクティブ ステータスは、ゾーン異常検出がイネーブルになっていて、ゾーンがインタラクティブ検出モードになっている場合にのみ、ゾーンに適用されます。詳細については、第 10 章「インタラクティブ検出モードの使用方法」を参照してください。

ポリシーによって作成された保留動的フィルタのステータスを、推奨事項のインタラクティブ ステータスに設定した後で、**always-accept** または **always-ignore** に変更するには、**interactive-status** コマンドを使用します。

たとえば、推奨事項のステータスを **always-accept** に設定すると、推奨事項と推奨事項の保留動的フィルタが表示されなくなります。推奨事項または推奨事項によって生成される保留動的フィルタを無視するには、ポリシーのインタラクティブ ステータスを **interactive** または **always-accept** に変更します。

ポリシー インタラクティブ ステータスを設定するには、ポリシー設定モードで次のコマンドを使用します。

interactive-status {**always-accept** | **always-ignore** | **interactive**}

表 7-15 に、**interactive-status** コマンドのキーワードを示します。

表 7-15　interactive-status コマンドのキーワード

パラメータ	説明
always-accept	ポリシーによって生成される動的フィルタを自動的に受け入れます。このアクションは、ポリシーによって新しい推奨事項が生成されるたびに、自動的に適用されます。 Detector モジュールはこのような推奨事項を表示しません。
always-ignorealwaysignore	ポリシーによって生成される動的フィルタを自動的に無視します。ポリシーは、しきい値を超過すると推奨事項を生成しません。 Detector モジュールはこのような推奨事項を表示しません。
interactive	ポリシーによって生成される動的フィルタを受け入れるか無視するか、ユーザの決定を待ちます。 Detector モジュールはこのような動的フィルタを推奨事項の一部として表示します。

次の例は、ポリシー dns_tcp/53/analysis/pkts/src_ip のインタラクティブ ステータスを always-accept に設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/pkts/
src_ip# interactive-status always-accept
```

ワーム ポリシーについて

インターネット ワームは、自動化された、自己伝搬する侵入性のエージェントであり、自身のコピーを作成して容易に配布します。ワームは、脆弱なホストを攻撃して感染させた後、そのホストを基点として他の脆弱なターゲットを攻撃します。次に、ネットワーク検査形式（一般的にはスキャン）を使用して他のターゲットを探し、次のターゲットに伝搬します。スキャニング ワームは、脆弱なホストを見つけるために、探索するアドレスのリストを生成し、その後ホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームはすべて、この方法で蔓延する知名度の高いワームの例です。

Detector モジュールは、ゾーン ネットワークがスキャンされていることを示す、異常なトラフィック パターンを通じてワームを識別することで TCP ワーム攻撃を検出することができます。Detector モジュールは、TCP ワーム攻撃が進行中でない場合であっても、ネットワークにはスキャナーが存在する場合があると想定しています。このモジュールは、特定のポート上で、多くのゾーン宛先 IP アドレスに対する未確立の接続（SYN/ACK 応答パケットが識別されなかった着信 SYN パケット）の開始側である送信元 IP アドレスを、スキャナーとして識別します。

ゾーン トラフィックを分析するために、Detector モジュールは周波数データが含まれたテーブルを使用します。このテーブルはネットワーク スキャナーのヒストグラムとして知られています。Detector モジュールは、最初に、攻撃が進行中でないときにゾーンのネットワークをラーニングし、次に同時スキャナーのヒストグラムを作成します。ヒストグラムには、特定の数のゾーン宛先 IP アドレスを同時にスキャンするスキャナーの数が記載されます。Detector モジュールは、特定の数より多くのゾーン宛先 IP アドレスにアクセスするスキャナーの数を測定します。

Detector モジュールは、次の 2 つのタイプのしきい値を使用して、ワームのトラフィック特性を分析します。

- スキャニングしきい値：単一の送信元 IP アドレスからスキャンできるゾーン IP アドレスの最大数を定義します。このしきい値は、ポリシーのしきい値によって定義されます。
- ヒストグラムしきい値：指定された数を超えるゾーン IP アドレスをスキャンできる送信元 IP アドレスの最大数を定義します。

Detector モジュールは、攻撃が進行中でないときにラーニングしたヒストグラムとの偏差がある場合にワーム攻撃と判断します（つまり、その場合は、定義された数を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスの数が超過しています）。詳細については、P.7-37 の「ワーム攻撃の識別」を参照してください。

ワーム ポリシーは、次の点で、他のポリシーと異なっています。

- Detector モジュールは、ポリシー構築フェーズ中ではなく、しきい値調整フェーズ中にワーム ポリシーの新しいサービスをラーニングするため、しきい値調整フェーズ中に、ワーム ポリシーに追加された新しいサービス（ポート）が表示される場合があります。
- **any** サービスは、Detector モジュールに特定のポリシーが存在しないポートに関連付けられます。たとえば、Detector モジュールに、worm_tcp/80 と worm_tcp/50 のポリシーが存在する場合、worm_tcp/any ポリシーは、ポート 50 または 80 を宛先としないトラフィックをすべて監視します。他のポリシーとは異なり、**any** サービスは、指定されていないポートすべてに対するトラフィックを集約しません。Detector モジュールは、ゾーン トラフィックを監視するとき、スキャンされるポートごとに別個の内部ヒストグラムを保持しています。次に、このヒストグラムを **any** サービスのヒストグラムと比較します。

この項では、次のトピックについて取り上げます。

- ワーム ポリシーの設定
- ワーム攻撃の識別

ワーム ポリシーの設定

worm_tcp ポリシー テンプレートは、DETECTOR_WORM ゾーン テンプレートだけで使用できます。

TCP　ワームを管理するポリシーは、worm_tcp　ポリシー　テンプレート、non_estb_conns パケット タイプ、およびスキャナーのトラフィック特性から構築されます。

ポリシー設定モードで次のコマンドを入力すると、ヒストグラムを設定し、スキャニングしきい値を変更することができます。

histogram *num-dst-ips num-src-ips* [*num-dst-ips num-src-ips...*]

表 7-16 に、**histogram** コマンドの引数を示します。

表 7-16　histogram コマンドの引数

パラメータ	説明
num-dst-ips	スキャンされたゾーン宛先 IP アドレスの数。*num-dst-ips* の値は 5、20、および 100 で、システム定義になっています。*num-dst-ips* ごとに定義される *num-src-ips* の値は変更できます。
num-src-ips	ヒストグラムのしきい値。このしきい値を超過すると、ポリシーはポリシー アクション パラメータによって定義されたアクションを実行します。しきい値には、指定された数（*num-dst-ips*）のゾーン宛先 IP アドレスをスキャンできる送信元 IP アドレスの数を指定します。

ヒストグラムしきい値をすべて 1 つのコマンドで入力できます。

次の例は、すべての頻度についてヒストグラムしきい値を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet-
worm_tcp/445/analysis/non_estb_conns/scanners# histogram 5 99 20 80 50
8 100 1
```

現在のヒストグラム設定を表示するには、**show policies** コマンドを使用します。

単一の送信元 IP アドレスからスキャンできるゾーン IP アドレスの最大数を設定できます（スキャニングしきい値）。この数を設定するには、**threshold** コマンドを使用します。詳細については、P.7-24 の「ポリシーのしきい値の設定」を参照してください。

特定のポートのヒストグラムしきい値を指定するには、**add-service** コマンドを使用して、特定のポート番号のサービスを、*worm_tcp* ポリシー テンプレートから作成されたポリシーすべてに追加します。詳細については、P.7-15 の「サービスの追加」を参照してください。

ワーム攻撃の識別

Detector モジュールは、スキャニングしきい値とヒストグラムしきい値の 2 つのタイプのしきい値を使用して、ワームのトラフィック特性を分析します。詳細については、P.7-34 の「ワーム ポリシーについて」を参照してください。

ヒストグラムしきい値を超えると、Detector モジュールは、指定されていない送信元 IP アドレス（*）を持つ動的フィルタを作成します。この動的フィルタは、ワーム攻撃が進行中であることを示します。動的フィルタのポリシーのしきい値は、超過したヒストグラムしきい値を指定します。Detector モジュールは、動的フィルタのポリシーしきい値と等しい新しい内部のスキャニングしきい値を定義します。

ゾーン宛先 IP アドレスをスキャンする送信元 IP アドレスは、ワームに感染したホストの IP アドレスです。ゾーンが攻撃中の場合、ワームに感染した各ホストがスキャンするゾーン宛先 IP アドレスの数が、新しい内部のスキャニングしきい値によって定義された最大数を超えると、動的フィルタが作成されます。Detector モジュールは、動的フィルタのアクションによって定義されたこれらの攻撃フローに対して作用します。

たとえば、ポリシーのしきい値（スキャニングしきい値）が 300 の場合、ポート 445 に関するポリシー スキャナーのヒストグラムは表 7-17 のようになり、Detector モジュールは、350 個のゾーン宛先 IP アドレスをスキャンするスキャナーを識別した場合、マス スキャナーが検出されたことを示す動的フィルタを作成します。ただし、このスキャナーからは、ワーム攻撃が進行中かどうかはまだわかりません。

表 7-17　ヒストグラム例

Number of source IP addresses	10	5	2
Number of Destination IP addresses	5	20	100

Detector モジュールが、ポート 445 で 50 個より多くのゾーン宛先 IP アドレスを同時にスキャンする 6 個の送信元 IP アドレスを識別すると、指定されていない送信元 IP アドレス（*）を持つ動的フィルタを worm_tcp ポリシーから作成します。この動的フィルタは Detector モジュールがポート 445 に対するワーム攻撃を識別したことを示します。動的フィルタのポリシーしきい値である 50 が、新しい内部のスキャニングしきい値に指定されるため、Detector モジュールはスキャナーのしきい値定義を小さくします。この結果、Detector モジュールは新しいスキャニングしきい値（50）を超過してスキャンする送信元 IP アドレスごとに追加の動的フィルタを作成します。

ポリシーの監視

ポリシーを監視して、ポリシーがゾーンのトラフィック量やサービスにどの程度適しているかを確認できます。

この項では、次のトピックについて取り上げます。

- ポリシーの表示
- ポリシーの統計情報の表示

ポリシーの表示

ゾーンのポリシーを表示して、ポリシーがゾーンのトラフィック特性に適しているかどうかを確認できます。ゾーンに構築されたポリシーを表示して、これらのポリシーがゾーンのトラフィックの特性に合せてカスタマイズされていることを確認できます。このリストに表示されるポリシーだけを設定できます。

Detector モジュールは、現在のゾーン ポリシーだけを表示します。ポリシー構築フェーズ中にポリシー テンプレートがディセーブルになっていた場合、Detector モジュールはそのポリシー テンプレートからポリシーを作成しないため、**show policies** コマンドを入力してもポリシーは表示されません。

ゾーン ポリシーを表示するには、ゾーン設定モードで次のコマンドを使用します。

show policies *policy-path*

policy-path 引数には、ポリシー グループを指定します。各ポリシー パス セクションでは、ワイルドカード文字としてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しなかった場合、指定していないセクションは Detector モジュールによってワイルドカード（*）と見なされます。たとえば、tcp_services//analysis//global ポリシーでは、サービスとパケット タイプのセクションにワイルドカードが使用されています。

すべてのポリシーの統計情報を表示するには、ポリシー パスにアスタリスク（*）を入力します。

ポリシー パス セクションの詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。

次の例は、すべてのゾーン ポリシーを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show policies *
```

次の例は、ポート 53 で DNS-over-TCP 同期パケットを監視するすべてのポリシーを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

表 7-18 に、**show policies** コマンド出力のフィールドを示します。

表 7-18　show policies コマンド出力のフィールド説明

フィールド	説明
Policy	ポリシー名。 ポリシー パス セクションの詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。
State	ポリシーの状態。詳細については、P.7-22 の「ポリシーの状態の変更」を参照してください。 act は active、inact は inactive、disab は disabled を指します。
IStatus	ポリシーのインタラクティブ状態。詳細については、P.7-32 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。 a-accept は always-accept、a-ignor は always-ignore、interac は interactive を指します。
Threshold	ポリシーのしきい値。トラフィック レートがこのしきい値を超えると、Detector モジュールが、そのポリシーと関連付けられたアクションを実行します。詳細については、P.7-24 の「ポリシーのしきい値の設定」を参照してください。
List	ポリシーに定義されている特定の IP しきい値の数。詳細については、P.7-29 の「特定の IP しきい値の設定」を参照してください。ワームに関連するポリシーの場合は、ヒストグラムを表す H が表示されます。詳細については、P.7-34 の「ワーム ポリシーについて」を参照してください。

表 7-18　show policies コマンド出力のフィールド説明（続き）

フィールド	説明
Action	トラフィックがそのポリシーのしきい値を超えた場合に Detector モジュールが実行するアクション。詳細については、P.7-31 の「ポリシーのアクションの設定」を参照してください。
Timeout	ポリシーのアクションが有効な最小期間。Detector モジュールは、ポリシーによって作成された動的フィルタを非アクティブにするかどうかを、filter-termination しきい値に従って決定します。詳細については、P.7-30 の「ポリシーのタイムアウトの設定」を参照してください。

ポリシーの統計情報の表示

単一またはグループのゾーン ポリシーを通過するトラフィックのレートを表示し、サービス タイプおよびトラフィック量がゾーンのトラフィックを表すかどうかを判断できます。Detector モジュールは、ゾーンに転送されたトラフィック フローの中で、ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。レートは、トラフィックのサンプルに基づいて計算されます。

ポリシーの統計情報を表示するには、ゾーン設定モードで次のコマンドを使用します。

show policies *policy-path* **statistics** [*num-entries*]

表 7-19 に、**show policies statistics** コマンド出力の引数を示します。

表 7-19　show policies statistics コマンドの引数

パラメータ	説明
policy-path	統計情報を表示するポリシーのグループ。 各ポリシー パス セクションでは、ワイルドカード文字としてアスタリスク（*）を使用できます。ポリシー パス セクションを指定しないと、指定していないセクションが Detector モジュールによってワイルドカード（*）と見なされます。たとえば、tcp_services//analysis//global ポリシーでは、サービスとパケット タイプのセクションにワイルドカードが使用されています。 すべてのポリシーの統計情報を表示するには、ポリシー パスにアスタリスク（*）を入力します。 ポリシー パス セクションの詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。
num-entries	（オプション）表示するエントリの数。1 ～ 100 の数字を入力します。Detector モジュールは、最大の値を持つポリシーを表示します。

次の例は、すべてのゾーン ポリシーの統計情報を表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show policies * statistics
```

次の例は、ポート 53 で DNS-over-TCP 同期パケットを監視するすべてのポリシーの統計情報を表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show policies dns_tcp/53/*/syns/*
```

次の例は、ゾーンのグローバル トラフィックの統計情報を表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show policies */*/*/*/global
statistics
```

Detector モジュールは、4 つのテーブルに情報を表示します。各テーブルの情報は値によってソートされ、テーブルの一番上に最大値が表示されます。

表 7-20 に、**show policies statistics** コマンド出力テーブルのフィールドを示します。

(注) Detector モジュールは、データを含まないテーブルを表示しません。

表 7-20　show policies statistics コマンド出力テーブルのフィールド説明

カラム	説明
すべての出力テーブルのフィールド	
Key	キー（ポリシーの集約に使用されたトラフィック特性）。 たとえば、tcp_services/any/analysis/syns/dst_ip ポリシーの場合、キーは宛先 IP アドレス（dst_ip）です。ポリシーの集約に使用されたトラフィック特性が global である場合、キーには N/A と表示されます。 ワームに関連するポリシー（worm_tcp/any/analysis/non_estb_conns/scanners など）の場合、キーは、ゾーンのネットワーク アドレスをスキャンする送信元 IP アドレス、コロン、およびスキャンされている宛先ポートになります。この例では、192.128.100.3:70 と表示されます。 詳細については、表 7-8 を参照してください。
Policy	ポリシー名。詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。
1 つの出力テーブルのフィールド	
Rate	ポリシーを通過し、パケット / 秒単位で計測されるトラフィックのレート。レートは、トラフィックのサンプルに基づいて計算されます。
Connection	同時接続の数。この情報は、パケット タイプが in_nodata_conns の tcp_connections ポリシーについてのみ表示されます。

表 7-20　show policies statistics コマンド出力テーブルのフィールド説明（続き）

カラム	説明
Ratio	SYN フラグの付いたパケット数と FIN/RST フラグの付いたパケット数の比率。この情報は、syn_by_fin ポリシーでのみ使用できます。
Dst IPs	スキャンされたゾーン宛先 IP アドレスの数。この情報は、worm_tcp ポリシーだけで使用できます。

ポリシー設定のバックアップ

現在のゾーン ポリシーは、**snapshot threshold-selection cur-thresholds** コマンドを使用していつでもバックアップできます。

次の例は、現在のポリシー設定をバックアップするために、スナップショットを作成する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# snapshot threshold-selection
cur-thresholds
```

CHAPTER 8

ゾーン トラフィックの特性のラーニング

この章では、Detector モジュールのラーニング プロセスを使用してゾーン トラフィックの特性を分析し、Detector モジュールがゾーン異常検出に使用するポリシーを作成および調整する方法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。

- ラーニング プロセスについて
- 検出およびラーニング機能について
- ゾーンのラーニング プロセスの結果と Cisco Anomaly Guard Module の同期
- ポリシーの構築
- ポリシーしきい値の調整
- ラーニング パラメータの設定
- ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行
- スナップショットを使用したラーニング プロセスの結果の確認
- ゾーン ポリシーのバックアップ

ラーニング プロセスについて

ラーニング プロセスは、ネットワーク上で現在攻撃が発生していないときに、通常のトラフィック パターンのベースラインを作成します。Detector モジュールは、このベースラインを、ゾーン トラフィック内における異常の存在を検出するための参照ポイントとして使用します。これらの参照ポイントを*ポリシー*といいます。

ポリシーを構築する最初のラーニング プロセスが終了したら、ラーニング プロセスとゾーン異常検出を同時にアクティブにできます。Detector モジュールは、ポリシーのしきい値を調整するとともに、トラフィックに異常がないかどうかについて、ポリシーのしきい値を監視します。このプロセスでは、Detector モジュールがゾーンのトラフィック特性に応じてポリシーのしきい値を常にアップデートしながら、ゾーン トラフィックの異常を検出でき、Detector モジュールで悪意のあるトラフィックのしきい値がラーニングされません。

ラーニング プロセスを実行するには、ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡すようにスイッチを設定する必要があります。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

複数のゾーンに対して同時に **learning** 関連のコマンドを入力できます。これには、グローバル モードで、ワイルドカードにアスタリスク（*）を使用してコマンドを発行します。たとえば、すべてのゾーンについてポリシー構築フェーズを開始する場合は、グローバル モードで **learning policy-construction *** コマンドを入力します。*scan* で始まる名前を持つ Detector モジュールのすべてのゾーン（scannet や scanserver など）のポリシー構築フェーズの結果を受け入れるには、グローバル モードで **no learning** *scan**** **accept** 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。

- ラーニング プロセスのフェーズについて
- ラーニング プロセスの結果の確認

ラーニング プロセスのフェーズについて

ラーニング プロセスは、次の 2 つのフェーズで構成されています。

- ポリシー構築：Detector モジュールはポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックは Detector モジュールを通過し、ゾーンによって使用される主なサービスを検出できます。既存のポリシーが新しいポリシーで上書きされます。

  ポリシー テンプレートは、Detector モジュールのポリシー構築用ツールです。このテンプレートは、Detector モジュールが作成するゾーン ポリシーのタイプを定義します。また、ポリシー テンプレートは、Detector モジュールが厳密に監視するサービスの最大数と、Detector モジュールによる新しいポリシーの作成をトリガーする最小しきい値も定義します。ゾーン ポリシーを構築するための規則を変更するには、ポリシー テンプレート パラメータを変更してから、ポリシー構築フェーズを開始する必要があります。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

  GUARD_LINK ゾーン テンプレートまたは DETECTOR_LINK ゾーン テンプレートを使用して作成されたゾーンに対してポリシー構築フェーズを実行することはできません。

- しきい値調整：Detector モジュールは、ゾーン サービスのトラフィック レートに合せて、ポリシー構築フェーズ中に構築されたポリシーを調整します。トラフィックは Detector モジュールを通過し、ゾーン ポリシーの構築中に検出されたサービスのしきい値を調整できます。既存のしきい値が新しいしきい値で上書きされます。

  しきい値調整フェーズとゾーン異常検出を同時にアクティブにすると（検出およびラーニング機能）、Detector モジュールで悪意のあるトラフィックのしきい値をラーニングすることを防止できます。Detector モジュールが常にゾーン ポリシーを調整するように設定し、Detector モジュールがポリシーのしきい値を更新するときの間隔を定義することができます。

Detector モジュールは、ゾーンのトラフィックの特性をラーニングして、ゾーンのトラフィックを比較するベースラインを作成し、悪意の攻撃となる可能性のある異常をすべてトレースします。Detector モジュールは、ラーニング プロセスの間は、現在のゾーン ポリシーを変更しません。ラーニング フェーズの結果の 1 つを受け入れると決めたときに限り、ポリシーを更新します。ポリシーが作成された後は、ポリシーを追加または削除できます。また、しきい値、サービス、タイムアウト、アクションなどのポリシー パラメータを変更することもできます。

Detector モジュールは、ポリシー構築フェーズ中ではなく、しきい値調整フェーズ中にワーム ポリシーの新しいサービスをラーニングします。そのため、しきい値調整フェーズ中に、ワーム ポリシーに追加された新しいサービス（ポート）が表示される場合があります。

ラーニング プロセスの結果の確認

ラーニング プロセス中のどの段階でも、任意のラーニング フェーズの現在の結果を保存して、後で **snapshot** コマンドを使用して確認できます。ラーニング プロセスのスナップショットを保存することで、スナップショットのポイントまでに Detector モジュールが作成したポリシー情報を表示し、ラーニング プロセスの結果を受け入れるかどうかを判断できます。ラーニング フェーズの結果をスナップショットに保存しても、ゾーン設定には影響はありません。スナップショット内のポリシー情報を使用してゾーン設定をアップデートできます。

検出およびラーニング機能について

ポリシーを構築する最初のラーニング プロセスが終了したら、ラーニング プロセスをアクティブにし、検出およびラーニング機能を使用して、同時にゾーン異常検出をイネーブルにできます。Detector モジュールは、ポリシーのしきい値を調整するとともに、トラフィックに異常がないかどうかについて、ポリシーのしきい値を監視します。検出およびラーニング機能により、ポリシーのしきい値をゾーンのトラフィック特性に基づいて常にアップデートしながら、Detector モジュールでゾーン トラフィックの異常検出を実行できるようになるため、Detector モジュールが悪意のあるトラフィックのしきい値をラーニングすることがなくなります。

保護およびラーニング機能をアクティブにする前に、ラーニング パラメータを設定することで、Detector モジュールがラーニング プロセスの結果をいつ、どのように受け入れるかを設定できます。

詳細については、P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

ゾーンのラーニング プロセスの結果と Cisco Anomaly Guard Module の同期

Detector モジュールは、ゾーン上で攻撃を検出すると、ラーニング プロセスを停止し、関連付けられているすべての Guard をアクティブ化してゾーンを保護します。その後、攻撃が終了すると、ゾーン トラフィックのラーニングを再開します。このプロセスにより、トラフィックに対するゾーンのポリシーのしきい値を継続的に調整できる一方で、ゾーンのトラフィックが常に Guard モジュールに宛先変更されることがなくなります。Detector モジュールがゾーンのトラフィックを常にラーニングして、ゾーンのポリシーで Guard モジュールをアップデートするように設定できます。

ラーニング プロセスの結果を Guard モジュールと同期させるには、次の作業を実施する必要があります。

1. Guard モジュールを Detector モジュール上のリモート Guard リストに追加して、通信方法を Secure Sockets Layer（SSL）として定義します。P.9-8 の「リモート Guard リストを使用したリモート Guard のアクティブ化」を参照してください。
2. Guard モジュールとの SSL 通信チャネルを確立します。P.4-29 の「SSL 通信チャネルの設定」を参照してください。
3. Detector モジュール上で Guard ゾーン テンプレートを使用してゾーンを作成します。P.5-7 の「ゾーン テンプレートからの新しいゾーンの作成」を参照してください。
4. ゾーンの検出およびラーニング機能をアクティブにします。P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

ゾーン設定を Guard モジュールと手動で同期させることも、ゾーン設定を自動的に Guard モジュールと同期させるように Detector モジュールを設定することもできます。詳細については、P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」を参照してください。

ポリシーの構築

ポリシー構築フェーズは、新しいゾーンを作成した後や、ゾーン設定が新しいサービス ポリシーを使用してアップデートを行う必要があるときに使用します。ポリシー構築フェーズを実行した後、しきい値調整フェーズを実行して各ポリシーのしきい値を調整します。

ポリシー構築フェーズでは、Detector モジュールはポリシー テンプレートを使用してゾーン ポリシーを作成します。トラフィックが Detector モジュールを通過し、ゾーンによって使用される主なサービス（ポートとプロトコル）を検出できます。ポリシー構築の規則を設定することもできます。たとえば、Detector モジュールで特定のタイプのポリシーが作成されないようにするには、関連するポリシー テンプレートをディセーブルにします。ゾーン ポリシーを構築するための規則を変更するには、ポリシー テンプレート パラメータを変更してから、ポリシー構築フェーズを開始する必要があります。詳細については、P.7-5 の「ポリシー テンプレートについて」を参照してください。

Detector モジュールは、ポリシー パラメータ（タイムアウト、アクション、およびしきい値）のデフォルト値を設定します。動作パラメータのデフォルト値の設定方法については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

このフェーズで Detector モジュールが作成する新しいポリシーは、既存のポリシーに置き換えられます。

（注） 帯域幅限定リンク ゾーン テンプレート（DETECTOR_LINK_128K、DETECTOR_LINK_1M、DETECTOR_LINK_4M、GUARD_LINK_512K、および GUARD_LINK_128K、GUARD_LINK_1M、GUARD_LINK_4M、GUARD_LINK_512K）に基づくゾーンに対しては、ポリシー構築フェーズを実行できません。

ポリシー構築フェーズをアクティブ化する前に、ゾーン上に攻撃がないことを確認してください。これによって、Detector モジュールが、Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃のトラフィック特性に基づいてポリシーを構築することを回避できます。Detector モジュールが DDoS 攻撃のトラフィック特性をラーニングし、攻撃の結果をベースラインとして保存できるようにすると、攻撃を通常のトラフィックの状態と見なすため、Detector モジュールはその後に発生する攻撃を検出できなくなる場合があります。

ゾーン ポリシーを構築するには、次の手順を実行します。

ステップ 1　ゾーン設定モードで次のコマンドを入力することで、ポリシー構築フェーズを実行できます。

```
learning policy-construction
```

ステップ 2　Detector　モジュールがゾーンのトラフィックのコピーを受信していることを確認してください。

ポリシー構築またはしきい値調整を開始してから少なくとも 10 秒待ってから、**show rates** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、Detector モジュールがゾーンのトラフィックのコピーを受信していないことを示します。トラフィックの送信元が、トラフィックのキャプチャについて設定されていることを確認します。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

ステップ 3　（オプション）Detector モジュールが構築中のポリシーを表示します。

ポリシー構築フェーズの任意の段階で **snapshot** コマンドを使用して、ラーニング パラメータ（サービス、しきい値、およびポリシー関連のその他のデータ）のスナップショットを保存しておいて、後で確認することができます。単一のスナップショットを保存するか、定期的なスナップショットを（指定した間隔で）保存することができます。

詳細については、P.7-44 の「ポリシー設定のバックアップ」を参照してください。

ステップ 4　（オプション）ポリシー構築フェーズを長期間実行する場合、ポリシー構築フェーズを停止しなくても、Detector モジュールによって提案されたポリシーを受け入れることができます。ポリシーを 1 回受け入れるか、提案されたポリシーを Detector モジュールが指定された間隔で自動的に受け入れるように定義できます。これでゾーンが最新のポリシーを持つだけでなく、継続してゾーンのトラフィックをラーニングすることを保証できます。

Detector モジュールによって提案されたポリシーを受け入れ、ポリシー構築フェーズを継続するには、次のコマンドを使用します。

```
learning accept
```

Detector モジュールによって提案されたポリシーを指定した間隔で自動的に受け入れるには、次のコマンドを入力します。

```
learning-params periodic-action auto-accept learn_params_days
learn_params_hours learn_params_minutes
```

詳細については、P.8-15 の「ラーニング パラメータの設定」を参照してください。

定期的なアクションを終了するには、**no learning-params periodic-action** コマンドを使用します。

ステップ 5　十分に時間をおいてからポリシー構築フェーズを終了し、新しく構築されたポリシーの取り扱いを決定します。

（注）　ゾーンが使用する主なサービス（ポートおよびプロトコル）を Detector モジュールが検出するための十分な時間を確保するために、ポリシー構築フェーズを少なくとも 2 時間継続することをお勧めします。

次のアクションのいずれかを行うことができます。

- 提案されたポリシーの受け入れ：Detector モジュールによって提案されたポリシーを受け入れるには、ゾーン設定モードで次のコマンドを入力します。

  ```
  no learning accept
  ```

Detector モジュールは、以前にラーニングしたポリシーとしきい値を消去します。

新しく構築されたポリシーを受け入れた後は、手動でポリシーを追加または削除できます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- 提案されたポリシーの拒否：Detector　モジュールによって提案されたポリシーを拒否するには、ゾーン設定モードで次のコマンドを入力します。

  no learning reject

  Detector モジュールはプロセスを停止し、ラーニングした新しいポリシーを保存しません。ゾーンのポリシーは、Detector モジュールがラーニング プロセスを開始する前か、ポリシー構築フェーズの結果を最後に受け入れる前のポリシーになります。

次の例は、ポリシー構築フェーズを開始し、提案されたポリシーを 12 時間間隔で受け入れる方法を示しています。さらに、ポリシー構築フェーズを停止し、提案されたポリシーを受け入れる方法も示しています。

```
user@DETECTOR-conf-zone-scannet# learning policy-construction
user@DETECTOR-conf-zone-scannet# learning-params periodic-action
auto-accept 0 12 0
user@DETECTOR-conf-zone-scannet# no learning accept
```

ポリシーしきい値の調整

しきい値調整フェーズでは、Detector モジュールがゾーンのトラフィックを分析し、ポリシー構築フェーズで構築されたポリシーのしきい値を定義します。

Detector モジュールが、最後に受け入れられたポリシーしきい値を監視してトラフィックの異常を探しながら、ゾーンのトラフィックをラーニングするように設定できます。Detector モジュールは、ゾーンに対する攻撃を検出した後、しきい値調整フェーズを停止しますが、ゾーン異常検出を継続することで、Detector モジュールが悪意のあるトラフィックのしきい値をラーニングすることがなくなります。

攻撃が終了すると、Detector モジュールはラーニング プロセスを再開します。

ポリシーのしきい値を調整するには、次の手順を実行します。

ステップ 1　ゾーン設定モードで次のコマンドを入力することで、しきい値調整フェーズを実行できます。

```
detect learning
```

（注） 検出およびラーニング機能をイネーブルにすること、つまり、しきい値調整フェーズをアクティブにすると同時に Detector モジュールがゾーンを異常検出するように設定することをお勧めします。

すでにゾーン異常検出またはラーニング プロセスのしきい値調整フェーズをアクティブにしている場合、**learning threshold-tuning** コマンドと **detect** コマンド（順序は問いません）の両方を入力して、検出およびラーニング機能をアクティブにします。

Detector モジュールは、ゾーンに対する攻撃を検出した場合はしきい値調整フェーズを停止しますが、ゾーン検出は継続します。

（注） ゾーン宛てのトラフィックが通常の量のときに、検出およびラーニング機能をアクティブにした場合、Detector モジュールは、ピーク時のトラフィックを攻撃と見なす可能性があります。このような場合は、次のいずれかを行うことができます。

- ゾーン設定モードで **learning-params threshold-tuned** コマンドを入力することで、ゾーン ポリシーしきい値の状態を未調整に設定できます。詳細については、P.8-18 の「ポリシーに対する調整済みのマーク付け」を参照してください。
- ゾーン設定モードで **no detect** コマンドを入力して、ゾーン異常検出を非アクティブにし、ゾーン ポリシーしきい値を継続してラーニングします。

ゾーン異常検出としきい値調整フェーズを同時に非アクティブにするには、ゾーン設定モードで **deactivate** コマンドを使用します。

しきい値調整フェーズだけをアクティブにするには、**learning threshold-tuning** コマンドを使用します。

ステップ 2　Detector　モジュールがゾーンのトラフィックのコピーを受信していることを確認してください。

ポリシー構築フェーズまたはしきい値調整フェーズを開始してから少なくとも 10 秒待ってから、**show rates** コマンドを発行します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、Detector モジュールがゾーンのトラフィックのコピーを受信していないことを示します。トラフィックの送信元が、トラフィックのキャプチャについて設定されていることを確認します。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

ステップ 3　（オプション）Detector モジュールが調整中のゾーン ポリシーを表示します。

しきい値調整フェーズの任意の段階で、**snapshot** コマンドを使用して、ラーニング パラメータ（サービス、しきい値、およびポリシー関連のその他のデータ）のスナップショットを保存できます。後でスナップショットを確認することや、

ラーニング パラメータを別のスナップショットと比較することができます。単一のスナップショットを保存するか、定期的なスナップショットを（指定した間隔で）保存することができます。

詳細については、P.7-44 の「ポリシー設定のバックアップ」を参照してください。

ステップ 4　ポリシーを受け入れます。

Detector モジュールが提案したゾーン ポリシーを受け入れ、しきい値の調整フェーズを継続するか、または Detector モジュールが自動的に提案したポリシーを指定した間隔で受け入れることを定義することで、ゾーンが最新のポリシーを持ち、ゾーンのトラフィックのラーニングを継続することが保証されます。

Detector モジュールによって提案されたポリシーを受け入れ、しきい値調整フェーズを継続するには、次のコマンドを使用します。

```
learning accept [threshold-selection {new-thresholds | max-thresholds
| weighted weight}]
```

threshold-selection の引数とキーワードについては、表 8-2 を参照してください。

Detector モジュールによって提案されたポリシーを指定した間隔で自動的に受け入れるには、次のコマンドを入力します。

```
learning-params periodic-action auto-accept learn_params_days
learn_params_hours learn_params_minutes
```

詳細については、P.8-15 の「ラーニング パラメータの設定」を参照してください。

定期的なアクションを終了するには、**no learning-params periodic-action** コマンドを使用します。

ステップ 5　十分な時間が経過してから、しきい値調整フェーズを終了し、新しく調整されたポリシーの処理方法を決定します。

（注）　しきい値調整フェーズをトラフィックのピーク時（1 日で最も忙しい部分）に、少なくとも 24 時間実行して、Detector モジュールがポリシーしきい値を正しく調整するために十分な時間を確保することをお勧めします。

（注） 検出機能とラーニング機能をイネーブルにし、しきい値調整フェーズを継続することをお勧めします。

次のアクションのいずれかを行うことができます。

- 提案されたポリシーの受け入れ：Detector モジュールによって提案されたポリシーのしきい値を受け入れるには、ゾーン設定モードで次のコマンドを入力します。

  no learning accept [**threshold-selection** {**new-thresholds** | **max-thresholds** | **weighted** *weight*}]

  threshold-selection の引数とキーワードについては、表 8-2 を参照してください。

  Detector モジュールは、以前にラーニングしたしきい値を消去します。

  新しく調整されたポリシーを受け入れた後は、手動でポリシーのパラメータを変更することができます。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

- 提案されたポリシーの拒否：Detector　モジュールによって提案されたポリシーのしきい値を拒否するには、ゾーン設定モードで次のコマンドを入力します。

  no learning reject

  Detector モジュールはしきい値の調整を停止して、前のしきい値の状態に戻します。そのプロセスの結果、新しく構築されたゾーン ポリシーには、以前のトラフィック特性に基づいて取得したしきい値が使用される場合があります。

（注） 後でしきい値調整フェーズをイネーブルにするか、またはそのしきい値を手動で設定することをお勧めします。

次の例は、しきい値調整フェーズを開始し、提案されたポリシーを 1 時間間隔で受け入れる方法を示しています。Detector モジュールは、次に、しきい値調整フェーズを停止し、しきい値が現在の値よりも大きい場合に、提案されたポリシーを受け入れます（max-thresholds 方式）。

```
user@DETECTOR-conf-zone-scannet# learning threshold-tuning
user@DETECTOR-conf-zone-scannet# learning-params periodic-action
auto-accept 0 1 0
user@DETECTOR-conf-zone-scannet# no learning accept
threshold-selection max-thresholds
```

ラーニングの結果を表示するには、**show policies statistics** コマンドを使用します。詳細については、P.7-39 の「ポリシーの表示」を参照してください。

ラーニングしたしきい値を確認した後は、結果の一部を変更できます。この変更がその後のしきい値調整フェーズで上書きされないようにするには、次のタスクのいずれかを実行します。

- ポリシーのしきい値を固定値として設定する：Detector モジュールは新しいしきい値を無視し、現在のしきい値を保持します。詳細については、P.7-25 の「固定値としてのしきい値の設定」を参照してください。
- ポリシーの固定乗数を設定する：Detector モジュールが新しいポリシーのしきい値を計算する場合は、ラーニングしたしきい値に指定の乗数を掛け、その結果にしきい値選択方式を適用します。詳細については、P.7-26 の「しきい値の乗数の設定」を参照してください。

ラーニング パラメータの設定

ラーニング パラメータを使用すると、Detector モジュールで実行できるラーニング関連のアクションを設定し、指定したポリシーを Detector モジュールで処理する方法を定義できます。次のパラメータを定義できます。

- periodic-action：自動的にゾーン　ポリシーを受け入れ、指定した間隔でゾーン ポリシーのスナップショットを保存するように Detector モジュールを設定します。
- threshold-tuned：ゾーンのポリシーに調整済みのマークを付けます。ゾーンのポリシーが調整済みとしてマークされていない場合、Detector モジュールはゾーンに対する攻撃を検出しません。
- threshold-selection：Detector　モジュールがしきい値調整フェーズの結果を受け入れて新しいポリシーのしきい値を生成するときに使用される、デフォルトの方式を設定します。
- fixed-threshold：ポリシーのしきい値を固定値として設定するため、Detector モジュールは後続のしきい値調整フェーズで、ポリシーしきい値の値を変更しません。
- threshold-multiplier：ポリシーのしきい値の固定乗数を設定するので、Detector モジュールは後続のしきい値調製フェーズで新しいポリシーしきい値を計算します。

ラーニング パラメータの設定を表示するには、ゾーン設定モードで **show learning-params** コマンドを使用します。

この項では、次のトピックについて取り上げます。

- 定期的なアクションの設定
- しきい値選択方式の設定
- ポリシーに対する調整済みのマーク付け

定期的なアクションの設定

指定した間隔で次のいずれかのアクションを実行するように Detector モジュールを設定します。

- ゾーン　ポリシーを自動的に受け入れ、ポリシーのスナップショットを保存する
- ゾーン ポリシーのスナップショットだけを保存する

スナップショットの詳細については、P.7-39 の「ポリシーの監視」を参照してください。

Detector モジュールが実行する定期的なアクションを設定するには、ゾーン設定モードで次のコマンドを入力します。

learning-params periodic-action {**auto-accept** | **snapshot-only**}
learn_params_days learn_params_hours learn_params_minutes

表 8-1 に、**learning-params** コマンドの引数とキーワードを示します。

表 8-1　learning-params periodic-action コマンドの引数とキーワード

パラメータ	説明
auto-accept	Detector モジュールによって提案されたポリシーを、指定された間隔で受け入れます。Detector モジュールは新しく提案されたゾーン ポリシーを受け入れた後で、ゾーン ポリシーのスナップショットを保存します。
snapshot-only	指定された間隔でポリシーのスナップショットを保存します。Detector モジュールは新しいポリシーを受け入れず、ポリシーのしきい値を変更しません。
learn_params_days	間隔（日単位）。0 ～ 1000 の整数を入力します。
learn_params_hours	間隔（時間単位）。0 ～ 1000 の整数を入力します。
learn_params_minutes	間隔（分単位）。0 ～ 1000 の整数を入力します。

間隔の値は、*learn_params_days* 値、*learn_params_hours* 値、および *learn_params_minutes* 値の合計となります。

次の例は、Detector モジュールがポリシーを 1 時間間隔で受け入れるように設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params periodic-action
auto-accept 0 1 0
```

しきい値選択方式の設定

しきい値調整フェーズ中に、Detector モジュールが新しいしきい値の生成に使用するデフォルトの方式を設定できます。しきい値調整フェーズの結果を手動で受け入れることも、しきい値調整フェーズの結果を特定の間隔で Detector モジュールが自動的に受け入れるように設定することもできます。

しきい値選択方式を設定するには、ゾーン設定モードで次のコマンドを使用します。

learning-params threshold-selection {**new-thresholds** | **max-thresholds** | **weighted** *weight*}

表 8-2 に、**learning-params threshold-selection** コマンドの引数とキーワードを示します。

表 8-2　learning-params threshold-selection コマンドの引数とキーワード

パラメータ	説明
new-thresholds	ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	現在のポリシーのしきい値をラーニングされたしきい値と比較し、値の大きい方をゾーン設定に保存します。 この方式がデフォルトです。
weighted *weight*	次の数式に基づいて、保存するポリシーのしきい値を計算します。 新しいしきい値 = (ラーニングしたしきい値 * *重み* + 現在のしきい値 * (100 - *重み*)) / 100

次の例は、ラーニングされたしきい値が現在のポリシーのしきい値よりも大きい場合に、提案されたポリシーを Detector モジュールが受け入れるように設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params threshold-selection
max-thresholds
```

ポリシーに対する調整済みのマーク付け

Detector モジュールは、ポリシーしきい値が調整されているかどうかを定義するポリシーしきい値の状態にマークを付け、保護およびラーニング機能をイネーブルにするときにこのステータスに関連付けます。ポリシーのしきい値のステータスは、ポリシーのしきい値を超過したときに、Detector モジュールでゾーンに対する攻撃と見なすかどうかを示します。

新しいゾーンが作成されるとき、またはゾーンに関するポリシー構築フェーズの結果を受け入れた後に、Detector モジュールはゾーンのポリシーのしきい値を未調整としてマークします。ゾーン テンプレートのデフォルトのしきい値は、ゾーンのトラフィックに異常を発見した場合に Detector モジュールがスプーフィング防止機能をすぐにアクティブにするように調整されています。保護およびラーニング機能をイネーブルにしている場合、現在のゾーン トラフィックが現在のポリシーしきい値よりも高いと、ラーニング プロセスは停止します。この状況を防ぐために、ゾーン ポリシーが調整されていなければ、検出およびラーニング機能をイネーブルにした場合、ゾーン ポリシーしきい値が受け入れられるまで Detector モジュールはゾーン トラフィックにおける攻撃を検出しません。

ゾーンのポリシーが未調整である場合、Detector モジュールは、新しいポリシーを受け入れるときに、しきい値選択方式 accept-new をアクティブにして、以前のしきい値を無視します。Detector モジュールがそのゾーンに関するラーニング プロセスのしきい値調整フェーズの結果を受け入れるときに、accept-new 以外のしきい値選択方式を使用すると、ポリシーのしきい値の集合が不適切になる場合があります。しきい値の選択方式の詳細については、P.8-17 の「しきい値選択方式の設定」を参照してください。

Detector モジュールは、次の場合にゾーンのポリシーを未調整としてマークします。

- 新しいゾーンを作成する場合
- ポリシー構築フェーズの結果を受け入れた場合
- ゾーン ポリシーに対してサービスの削除または新しいサービスの追加を行った場合

Detector モジュールは、しきい値調整フェーズの結果を受け入れた後に、ゾーンのポリシーを調整済みとしてマークします。

ユーザは、ゾーン ポリシーの設定を変更できます。ゾーン ポリシーに調整済みのマークを付けるには、ゾーン設定モードで次のコマンドを使用します。

learning-params threshold-tuned

ゾーン ポリシーに未調整のマークを付けるには、このコマンドの **no** 形式を使用します。

次のどちらかの場合は、ゾーン ポリシーのステータスを調整済みに変更することもできます。

- 新しいゾーンが既存のゾーンまたはスナップショットから複製されており、両方のゾーンのトラフィック特性が似ている場合
- ポリシーのしきい値をすべて手動で設定した場合

次のどちらかの場合は、ゾーン ポリシーのステータスを未調整に変更することもできます。

- ゾーンのネットワークに重要な変更を加えた場合
- ゾーンの IP アドレスまたはサブネットを変更した場合
- トラフィックのピーク時の間、検出およびラーニング機能を開始していない場合。ゾーン ポリシーのステータスを未調整に変更し、Detector モジュールがピーク時のトラフィックを攻撃として識別しないようにします。

ゾーン ポリシーが未調整としてマークされている場合、Detector モジュールは現在のポリシーしきい値を監視しません。また、ポリシーしきい値が超過してもゾーンへの攻撃を検出しません。

注意　ゾーンに対する攻撃がある場合は、ゾーン ポリシーのステータスを未調整に変更しないでください。これは、ステータスを変更すると Detector モジュールで攻撃が検出されなくなり、Detector モジュールが悪意のあるトラフィックのしきい値をラーニングするためです。

次の例は、ゾーン ポリシーのステータスに調整済みのマークを付ける方法を示しています。

```
user@DETECTOR-conf-zone-scannet# learning-params threshold-tuned
```

ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行

検出およびラーニング機能を使用することで、ラーニング プロセスのアクティブ化とゾーン異常検出のイネーブル化を同時に実行できます。Detector モジュールは、ポリシーのしきい値を調整し、同時にトラフィックの異常についてポリシーのしきい値を監視します。検出およびラーニング機能により、ポリシーのしきい値をゾーンのトラフィック特性に基づいて常にアップデートしながら、Detector モジュールでゾーン トラフィックの異常を検出できるようになります。検出およびラーニング機能を使用すると、Detector モジュールが悪意のあるトラフィックのしきい値をラーニングすることを回避できます。

（注） 保護およびラーニング機能をアクティブ化する前に、ラーニング プロセスのポリシー構築フェーズをアクティブにして、ゾーン ポリシーを構築する必要があります。

新しいゾーンを作成する場合、ゾーン ポリシーからサービスを追加または削除するか、ポリシー構築フェーズの結果を受け入れることで、Detector モジュールはゾーン ポリシーを未調整としてマークします。Detector モジュールは、ラーニング プロセスのしきい値調整フェーズの結果を受け入れた後にだけ、ゾーンのポリシーを調整済みとしてマークします。しきい値調整フェーズの結果を手動で受け入れることも、**learning-params** コマンドを使用して、Detector モジュールが自動的に受け入れるように設定することもできます。

ラーニング プロセスとゾーン検出が同時にイネーブルになっており、ゾーン ポリシーのステータスが未調整の場合、ゾーン ポリシーのしきい値が受け入れられるまで、Detector モジュールは次のように機能します。

- Detector モジュールはゾーン トラフィックの攻撃を検出しない。
- Detector モジュールは、しきい値選択方式 accept-new をアクティブにする（P.8-17 の「しきい値選択方式の設定」を参照）。

Detector モジュールは、ゾーンに対する攻撃を識別すると、ラーニング プロセスを停止します。Detector モジュールは、Guard をアクティブにしてゾーンを保護した場合、Guard モジュールを定期的にポーリングします。Detector モジュールは、Guard モジュールがゾーンの保護を非アクティブにしたことを識別すると、他のトラフィック異常が存在しないことを確認してから、検出およびラーニング機能を再度アクティブにします。このオプションを使用できるのは、SSL 通信チャネルを設定した場合のみです。

保護およびラーニング機能をアクティブにする前に、Detector モジュールがラーニング プロセスの結果をいつ、どのように受け入れるかを設定できます。詳細については、P.8-15 の「ラーニング パラメータの設定」を参照してください。

ラーニング プロセスとゾーン異常検出を同時にアクティブにするには、**detect learning** コマンドを使用するか、**learning threshold-tuning** コマンドと **detect** コマンドを順番に入力します（順序は問いません）。

詳細については、P.8-10 の「ポリシーしきい値の調整」および第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

スナップショットを使用したラーニング プロセスの結果の確認

ラーニング プロセス中の任意の段階でラーニング パラメータ（サービス、しきい値、その他のポリシー関連データ）のスナップショットを保存して、後で確認できます。2 つのゾーンのラーニング パラメータまたはスナップショットを比較して、ラーニング プロセスの結果を確認し、ポリシー、サービス、およびしきい値の違いをトレースできます。

ラーニング プロセス中、数時間ごとにスナップショットを保存することをお勧めします。ラーニング プロセス中に攻撃が発生した場合は、スナップショット ポリシーをゾーンに使用できます。スナップショットは、手動で撮ることも、指定した間隔で Detector モジュールが自動的に撮るように設定することもできます。Detector モジュール は、スナップショットをゾーンごとに 100 個まで保存します。以前のスナップショットは新しいスナップショットに置き換えられます。

スナップショットからゾーン ポリシーをコピーすることで、必要に応じて、以前のラーニングの結果に基づいてゾーンを設定できます。

この項では、次のトピックについて取り上げます。

- スナップショットの作成
- ラーニングの結果の比較
- スナップショットの表示
- スナップショットの削除
- ゾーン設定へのポリシーのコピー

スナップショットの作成

ゾーンのラーニング パラメータの単一スナップショットを保存することができます。または、指定した間隔で Detector モジュールが自動的にスナップショットを撮るように設定できます。Detector モジュールは、スナップショットが撮られている間も、ラーニング プロセスを続行します。

Detector モジュールが指定した間隔で自動的にスナップショットを撮るように設定する方法の詳細については、P.8-15 の「定期的なアクションの設定」を参照してください。

ゾーンのラーニング パラメータのスナップショットを 1 つ保存するには、ゾーン設定モードで次のコマンドを使用します。

snapshot [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *calc-weight*}]

表 8-3 に、**snapshot** コマンドの引数とキーワードを示します。

表 8-3　snapshot コマンドの引数とキーワード

パラメータ	説明
threshold-selection	（オプション）Detector モジュールがスナップショットのしきい値計算に使用する方式を設定します。デフォルトでは、Detector モジュールは **learning-params threshold-selection** コマンドで定義されたゾーンしきい値選択方式を使用します。ゾーンのデフォルトのしきい値選択方式は、**max-thresholds** です。
new-thresholds	ラーニング プロセスの結果をゾーン設定に保存します。
max-thresholds	現在のポリシーのしきい値をラーニングされたしきい値と比較し、値の大きい方をゾーン設定に保存します。 これがデフォルトの方式です。
cur-thresholds	ラーニング プロセスの新しいしきい値を無視して、現在のポリシーのしきい値をスナップショットに保存します。この方式は、バックアップの目的で使用できます。

表 8-3　snapshot コマンドの引数とキーワード（続き）

パラメータ	説明
weighted *calc-weight*	次の数式に基づいて、保存するポリシーのしきい値を計算します。 しきい値 =（新しいしきい値 * *計算された重み* + 現在のしきい値 *（100 - *計算された重み*））/ 100

snapshot コマンドを使用すると、ゾーンのラーニング プロセスの結果が保存されます。この結果には、ゾーンのポリシー、サービス、およびしきい値が含まれます。スナップショットのパラメータを確認するか、2 つのスナップショットを比較するか、またはスナップショットのパラメータを新しいゾーンにコピーし終わったら、スナップショットを削除できます。

snapshot threshold-selection cur-thresholds コマンドを使用すると、現在のゾーン ポリシーをバックアップできます。

次の例は、ポリシーの現在のしきい値とラーニング プロセスの新しいしきい値のうちで最も大きい値をしきい値として持つスナップショットを作成する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# snapshot threshold-selection
max-thresholds
```

グローバル モードでスナップショットを 1 つ保存するには、**snapshot** *zone-name* [**threshold-selection** {**new-thresholds** | **max-thresholds** | **cur-thresholds** | **weighted** *weight*}] コマンドを使用します。

ラーニングの結果の比較

2 つのスナップショットまたはゾーンのラーニングの結果を比較して、ポリシー、サービス、およびしきい値の違いをトレースできます。

この項では、次のトピックについて取り上げます。

- スナップショットの比較
- ゾーンの比較

スナップショットの比較

2 つのスナップショットを比較するには、ゾーン設定モードで次のコマンドを使用します。

diff snapshots *snapshot-id1 snapshot-id2* [*percent*]

表 8-4 に、**diff** コマンドの引数を示します。

表 8-4　diff コマンドの引数

パラメータ	説明
snapshot-id1	最初に比較するスナップショットの ID。ゾーンのスナップショットのリストを表示するには、**show snapshots** コマンドを使用します。
snapshot-id2	2 番目に比較するスナップショットの ID。ゾーンのスナップショットのリストを表示するには、**show snapshots** コマンドを使用します。
percent	（オプション）違いの割合。Detector モジュールは、2 つのスナップショットを比較して、指定した値よりも大きいポリシーしきい値の違いだけを表示します。デフォルトのパーセンテージは 100% で、Detector モジュールは 2 つのスナップショットにおける相違をすべて表示します。

次の例は、ゾーンのスナップショットの表示方法と、最新の 2 つのスナップショットを比較する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
3     Feb 10 11:01:50
user@DETECTOR-conf-zone-scannet# diff 2 3
```

グローバル モードでスナップショットを比較するには、**diff** *zone-name* **snapshots** *snapshot-id1 snapshot-id2* [*percent*] コマンドを使用します。

ゾーンの比較

2 つのゾーンのラーニング パラメータを比較するには、グローバル モードまたは設定モードで次のコマンドを使用します。

diff *zone-name1 zone-name2* [*percent*]

表 8-5 に、**diff** コマンドの引数を示します。

表 8-5　diff コマンドの引数

パラメータ	説明
zone-name1	比較対象のラーニング パラメータを持つ最初のゾーンの名前。
zone-name2	比較対象のラーニング パラメータを持つ 2 番目のゾーンの名前。
percent	（オプション）違いの割合。Detector モジュールは、2 つのゾーンを比較して、指定した値よりも大きいポリシーしきい値の違いだけを表示します。デフォルトのパーセンテージは 100% で、Detector モジュールは 2 つのゾーンにおける相違をすべて表示します。

次の例は、2 つのゾーンのラーニング パラメータの比較方法を示しています。

```
user@DETECTOR# diff scannet scannet-mailserver
```

スナップショットの表示

ゾーンのスナップショットまたはスナップショット パラメータのリストを表示し、ゾーンのラーニングの結果を包括的に把握するには、次のコマンドを入力します。

show snapshots [*snapshot-id* [**policies** *policy-path*]]

表 8-6 に、**show snapshots** コマンドのキーワードと引数を示します。

表 8-6　show snapshots コマンドの引数とキーワード

パラメータ	説明
snapshot-id	（オプション）表示するスナップショットの ID。ポリシーを指定しない場合、デフォルトでは、ゾーンのスナップショットすべてのリストが表示されます。スナップショット ID を表示するには、このコマンドを引数なしで使用します。
policies *policy-path*	（オプション）表示対象のポリシーのグループを指定します。詳細については、P.7-2 の「ポリシー パスの使用」を参照してください。

グローバル モードでスナップショットを比較するには、**show zone** *zone-name* **snapshots** [*snapshot-id* [**policies** *policy-path*]] コマンドを使用します。

次の例は、ゾーンのスナップショットのリストを表示する方法と、スナップショット 2 の dns_tcp に関連するポリシーを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID    Time
1     Feb 10 10:32:04
2     Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# show snapshots 2 policies dns_tcp
```

show zone *zone-name* **snapshots** *snapshot-id* **policies** *policy-path* コマンドの出力のフィールドは、**show policies** コマンドの出力のフィールドと同じです。詳細については、P.7-39 の「ポリシーの表示」を参照してください。

表 8-7 に、**show snapshots** コマンド出力のフィールドを示します。

表 8-7　show snapshots コマンド出力のフィールドの説明

フィールド	説明
ID	スナップショット ID。
Time	スナップショットが取得された日付と時刻。

スナップショットの削除

古いスナップショットを削除して、空きディスク スペースを得ることができます。

スナップショットを削除するには、ゾーン設定モードで次のコマンドを使用します。

no snapshot *snapshot-id*

snapshot-id 引数には、既存のスナップショットの ID を指定します。すべてのゾーンのスナップショットを削除するには、アスタリスク（*）を入力します。スナップショットの詳細を表示するには、**show snapshots** コマンドを使用します。

次の例では、すべてのゾーンのスナップショットを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no snapshot *
```

ゾーン設定へのポリシーのコピー

ポリシーの全体の設定または部分的な設定を現在のゾーンにコピーできます。

次の情報をコピーできます。

- サービスのコピー：ソース ゾーンからゾーンにサービスをコピーできます。この操作により、これらのサービスの検出にポリシー構築フェーズを適用することなく、ゾーン ポリシーを設定できます。サービスをゾーンにコピーするには、まず、そのゾーンが同様のトラフィック パターンを持つことを確認します。
- ポリシー パラメータの コピー：ゾーン ポリシー パラメータをゾーンのスナップショットのポリシー パラメータに置き換えることができます。この操作により、以前のラーニングの結果に戻すことができます。Detector モジュールは、既存ポリシーのパラメータだけをコピーします。

ゾーンのポリシーをコピーするには、ゾーン設定モードで次のコマンドを使用します。

copy-policies {*snapshot-id* | *src-zone-name* [*service-path*]}

表 8-8 に、**copy-policies** コマンドの引数とキーワードを示します。

表 8-8　copy-policies コマンドの引数とキーワード

パラメータ	説明
snapshot-id	ポリシーのコピー元のスナップショットの ID。スナップショットの ID を表示するには、**show snapshots** コマンドを使用します。
src-zone-name	サービス ポリシーのコピー元のゾーン名。
service-path	（オプション）コピー元のサービス。サービス パスの形式は、次のいずれかです。 • policy-template：ポリシー テンプレートに関連するすべてのポリシーをコピーします。 • policy-template/service-num：ポリシー テンプレートおよび指定のサービスに関連するすべてのポリシーをコピーします。 デフォルトでは、すべてのポリシーとサービスがコピーされます。

次の例は、ポリシー テンプレート tcp_connections に関連するすべてのサービスを、ゾーン webnet から現在のゾーン scannet にコピーする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# copy-policies webnet tcp_connections/
```

次の例は、ゾーンのスナップショットのリストを表示し、次に ID が 2 のスナップショットからポリシーをコピーする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show snapshots
ID   Time
1    Feb 10 10:32:04
2    Feb 10 10:49:12
user@DETECTOR-conf-zone-scannet# copy-policies 2
```

ゾーン ポリシーのバックアップ

現在のゾーン ポリシーは、**snapshot threshold-selection cur-thresholds** コマンドを使用していつでもバックアップできます。

次の例は、現在のゾーン ポリシーのバックアップ方法を示しています。

```
user@DETECTOR-conf-zone-scannet# snapshot threshold-selection
cur-thresholds
```

CHAPTER 9

ゾーンのトラフィックの異常の検出

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）を設定してトラフィックの異常を検出する方法と、Guard をアクティブにしてゾーンを保護する方法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。

- ゾーン異常検出について
- Detector モジュールがゾーン異常検出を行う方法の設定
- Guard 保護のアクティベーション方式の設定
- ゾーン異常検出のアクティブ化
- ゾーン異常検出の非アクティブ化
- ゾーンを保護するためのリモート Guard のアクティブ化

ゾーン異常検出について

ゾーン異常検出とは、Detector モジュールがゾーンのトラフィックのコピーを積極的に監視し、ゾーンでの Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃の兆候がないかを調べることです。ポリシーしきい値を超える（攻撃を示す）ことによってトラフィック異常がポリシー アクションをトリガーすると、Detector モジュールは、次のいずれかのタスクを実行します。

- Detector モジュールと関連付けている Guard をアクティブにする。Guard が攻撃を軽減します。
- ユーザに通知を送信する。

ゾーン異常検出をアクティブにする前に、Detector モジュールにラーニング プロセスを使用してゾーンのトラフィック パターンを学習させる必要があります。ラーニング プロセスを使用すると、Detector モジュールはゾーンのトラフィック パターンをラーニングして、ゾーン トラフィックの統計分析に従い一連の推奨しきい値を作成できます。

ゾーンが攻撃されていない場合は、**learning policy-construction** コマンドを使用して Detector モジュールにゾーンのポリシーを構築させてから、検出およびラーニング機能をイネーブルにすることをお勧めします。Detector モジュールは、ゾーン トラフィックをラーニングすると同時に、最後に受け入れられたポリシーしきい値を監視してトラフィック異常がないか調べます。Detector モジュールは、ゾーンで攻撃を検出すると、しきい値調整フェーズを停止しますが、悪意あるトラフィックのしきい値のラーニングを回避するためにゾーン トラフィックの異常検出は継続します。詳細については、P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

Guard モジュールをアクティブにしてゾーンを保護する前に、Detector モジュール上のゾーン設定と Guard モジュール上のゾーン設定を同期させることができます。詳細については、P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」および P.9-8 の「ゾーンを保護するためのリモート Guard のアクティブ化」を参照してください。

ゾーン異常検出をアクティブにする前に、ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡すようにスイッチを設定する必要があります。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

ヒント　ポリシー構築フェーズを開始してから少なくとも 10 秒待ってから、**show rates** コマンドを入力して、Detector モジュールがゾーンのトラフィックのコピーを受信していることを確認します。*Received traffic* レートの値がゼロより大きいことを確認します。値がゼロの場合は、Detector モジュールがゾーンのトラフィックのコピーを受信していないことを示します。トラフィックの送信元が、トラフィックのキャプチャについて設定されていることを確認します。詳細については、P.2-6 の「トラフィックをキャプチャするためのトラフィックの送信元の設定」を参照してください。

次の異常検出特性を定義できます。

- 動作モード：Detector モジュールがゾーン異常検出を実行する方法を定義します（Detector モジュールによってゾーン トラフィックの異常を自動的に検出するか、またはインタラクティブ方式で検出するか）。
- Guard 保護アクティベーション方式：Detector モジュールがゾーンを保護するためにリモート Guard をアクティブにする方法を定義します。Detector モジュールは、リモート Guard をアクティブにしてゾーン全体の一部である特定のゾーン（たとえば、保護されたネットワーク環境の一部である特定のサーバ）を保護することも、リモート Guard をアクティブにしてゾーン全体を保護することもできます。

Detector モジュールがゾーン異常検出を行う方法の設定

動作モードによって、ゾーン異常検出がイネーブルな場合に Detector モジュールがどのように動的フィルタをアクティブにするかが決まります。

ゾーン異常検出は、次の 2 つの動作モードにおいてアクティブにできます。

- 自動検出モード：動的フィルタはユーザの操作なしでアクティブになります。この動作モードがデフォルトです。
- インタラクティブ検出モード：動的フィルタは、インタラクティブ モードにおいて手動でアクティブになります。Detector モジュールは、動的フィルタを、ユーザの決定を待つ推奨事項としてグループ化します。ユーザは、推奨事項を確認して、どの推奨事項を受け入れるか、無視するか、自動アクティベーションに切り替えるかを決定できます。

詳細については、第 10 章「インタラクティブ検出モードの使用方法」を参照してください。

Guard 保護のアクティベーション方式の設定

Guard 保護のアクティベーション方式は、リモート Guard として定義されている Guard がゾーン保護をアクティブにする方法を定義します。この方式は、ゾーンの保護要件に焦点を当て、Guard モジュールのリソースを節約することを目的としたものです。

Detector モジュールは、次の Guard 保護のアクティベーション方式をサポートします。

- **entire-zone**：Guard モジュールをアクティブにし、ゾーン トラフィックに異常が検出されるとゾーン全体を保護します。この方式では、Guard モジュールが保護するアクティブなゾーンの数が減るため、Guard モジュールのリソースが節約されます。ゾーンが関連性のあるサブゾーンで構成されている場合にこの方式を使用します。
- **dst-ip-by-name**：Guard モジュールをアクティブにし、特定の IP アドレス宛てのゾーン トラフィックに異常が検出された場合に、その IP アドレスを保護します。Guard モジュールをアクティブにし、攻撃対象の IP アドレスを保護しながら、ゾーン全体のトラフィックが Guard モジュールに宛先変更されるのを回避できます。Detector モジュールは、トラフィック異常を特定の IP アドレスに関連付けることができない場合、Guard モジュールをアクティブにしないため、ゾーンが保護されません。ゾーンが関連性のないサブゾーンで構成されている場合にこの方式を使用します。
- **dst-ip-by-ip**：Guard モジュールをアクティブにし、特定の IP アドレス宛てのゾーン トラフィックに異常が検出された場合に、その IP アドレスを保護します。IP アドレスは、Guard モジュールに定義されているいずれかのゾーンのアドレス範囲内である必要があります。ただし、Detector モジュール上のゾーン名が、Guard モジュール上のゾーン名と一致する必要はありません。**dst-ip-by-ip** Guard 保護アクティベーション方式は、Guard モジュール上で **protect** *ip-address* コマンドを使用した場合と同じ結果になります。Detector モジュール上のゾーン名が Guard モジュール上のゾーン名と一致しない場合、またはゾーン全体が関連性のないサブゾーンで構成されている場合にこの方式を使用します。

（注） 確実に Guard モジュールが攻撃対象の IP アドレスに対してだけゾーン保護をアクティブにし、ゾーン全体のトラフィックがそれ自身に宛先変更されるのを回避するには、アクティベーション範囲が **ip-address-only** になるように Guard モジュール上でゾーンを定義します。

- **policy-type**：Guard モジュールをアクティブにし、Detector モジュールが Guard モジュールをアクティブにする原因となったポリシーに応じて、ゾーン全体を保護するか、またはゾーン内の特定の IP アドレスを保護します。特定の IP アドレス宛てのゾーン トラフィックで異常が検出された場合（たとえば、リモート アクティベーションの原因となったポリシーのトラフィック特性が **dst_ip** である場合）、Detector モジュールは Guard モジュールをアクティブにしてその IP アドレスを保護します。トラフィック異常を特定の IP アドレスと関連付けることができない場合（たとえば、リモート アクティベーションの原因となったポリシーのトラフィック特性が global である場合）、Detector モジュールは Guard モジュールをアクティブにしてゾーン全体を保護します。

  ゾーンが関連するサブゾーンから構成されており、攻撃対象のサブゾーンの状況によってゾーン全体がダメージを受けるのを防止できる場合に、この方式を使用します。

Guard 保護アクティベーション方式をアクティブにするには、ゾーンの設定モードで次のコマンドを入力します。

protect-ip-state {**entire-zone | dst-ip-by-name | dst-ip-by-ip** | **policy-type**}

次の例は、Guard 保護アクティベーション方式を設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# protect-ip-state entire-zone
```

ゾーン異常検出のアクティブ化

ゾーン異常検出をアクティブにするには、ゾーン設定モードで次のコマンドを入力します。

detect [**learning**]

オプションの **learning** キーワードでは、ゾーン トラフィック内の異常を検出すると同時に、ゾーン ポリシーのしきい値を調整するように Detector モジュールが設定されます。詳細については、P.8-20 の「ゾーンのポリシーのしきい値調整とゾーン異常検出のイネーブル化の同時実行」を参照してください。

次の例は、ゾーン scannet の異常検出を非アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# detect
```

ゾーン異常検出の非アクティブ化

ゾーン異常検出を非アクティブにするには、ゾーン設定モードで次のコマンドのいずれかを使用します。

- **no detect**：ゾーン異常検出を終了します。Detector モジュールは、ゾーン トラフィックの異常検出とラーニングの実行中である場合には、ゾーン ポリシーのしきい値のラーニングを継続します。
- **deactivate**：ゾーン異常検出と、ラーニング プロセスのしきい値調整フェーズの両方を終了します。

ゾーンを保護するためのリモート Guard のアクティブ化

Detector モジュールは、ゾーン トラフィックの異常を検出すると、動的フィルタを作成します。このフィルタは、ゾーンを保護するために Guard をアクティブにするか、またはリモート Guard が定義されていない場合はイベントを記録します。

リモート Guard は、次の方法のいずれかでアクティブにできます。

- リモート Guard リストの使用：Secure Sockets Layer（SSL）を使用してリモート アクティベーションとゾーン同期をイネーブルにするか、または SSH を使用してリモート アクティベーションだけをイネーブルにします。
- オフラインでのアクティブ化：ゾーンで攻撃が発生したときに通知を発行するように Detector モジュールを設定します。
- 手動でのアクティブ化：リモート Guard をアクティブにするための動的フィルタを作成します。

Detector モジュールは Guard のダウンストリームに配置されます。進行中の攻撃がない場合、Detector モジュールは、保護されたゾーン宛てのすべてのインバウンド トラフィックを監視します。攻撃を受けている間に、Guard が被害を軽減するために攻撃対象のゾーンからのトラフィックを宛先変更した場合は、Detector モジュールは Guard からそのゾーンに転送された正当なトラフィックを監視します。

この項では、次のトピックについて取り上げます。

- リモート Guard リストを使用したリモート Guard のアクティブ化
- リモート Guard のオフラインでのアクティブ化
- 手動でのリモート Guard のアクティブ化

リモート Guard リストを使用したリモート Guard のアクティブ化

Detector モジュールは、ゾーンを保護するためにアクティブにされる Guard のリスト（リモート Guard リストとも呼ばれる）を保持しています。複数のリモート Guard リストに Guard モジュールを設定できます。Detector モジュールは、次の 2 つのタイプのリモート Guard リストを保持します。

- ゾーン固有のリモート Guard リスト：Detector モジュールは Guard をアクティブにし、ゾーンを保護します。場合によっては、ゾーン設定を Guard と同期します。
- デフォルトのリモート Guard リスト：ゾーンのリモート Guard リストが空であるか、またはどちらの通信方式も含まれていない場合にだけ、Detector モジュールがデフォルト リストを検索します。

（注） リモート Guard リストに Guard を追加する場合は、リモート Guard との通信チャネルを確立する必要があります。詳細については、P.4-28 の「Guard との通信の確立」を参照してください。

各リモート Guard リストは 2 つの通信方式をサポートしています。

- SSL：Detector モジュールは、SSL を使用して Guard と通信します。Detector モジュールは、リモート Guard をアクティブにして、ゾーンを保護し、ゾーン設定とリモート Guard を同期できます。

  Detector モジュールは、Guard をアクティブにしてゾーンを保護する前に、ゾーン設定をリモート Guard リストの Guard と同期できます。詳細については、P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」を参照してください。
- Secure Shell（SSH）：Detector モジュールは、SSH を使用して Guard モジュールと通信します。Detector モジュールは、リモート Guard をアクティブにしてゾーンを保護できますが、ゾーン設定をリモート Guard と同期できません。

Detector モジュールは、同じ通信方式の Guard モジュールがゾーンのリモート Guard リストに定義されていない場合にだけ、デフォルトのリモート Guard リストの Guard モジュールをアクティブにします。

注意 リモート Guard リストを変更する場合は、Detector モジュールがリモート Guard との通信チャネルに使用する SSL 証明書を再生成する必要があります。再生成しないと、通信に失敗します。詳細については、P.4-31 の「SSL 証明書の再生成」を参照してください。

Detector モジュールのリモート Guard リストのいずれか（デフォルトのリモート Guard リスト、またはゾーンのリモート Guard リスト）に少なくとも 1 つは Guard が定義されていることを確認してください。どのリモート Guard リストにもリモート Guard が定義されていない場合、Detector モジュールはログ ファイルにイベントを記録します。

この項では、次のトピックについて取り上げます。

- リモート Guard のアクティブ化およびゾーン設定の同期
- デフォルトのリモート Guard リストの設定
- ゾーンのリモート Guard リストの設定

リモート Guard のアクティブ化およびゾーン設定の同期

リモート Guard をアクティブにしゾーン設定を同期するには、次の手順を実行します。

ステップ 1　Guard ゾーン テンプレートのいずれかを使用して、新しいゾーンを作成および設定します。

P.5-6 の「新しいゾーンの作成」を参照してください。

ステップ 2　リモート Guard IP アドレスを次のいずれかのリストに追加します。

- ゾーンのリモート Guard リスト：そのゾーンの保護用に Detector モジュールによってアクティブにされるリモート Guard のリスト。

  詳細については、P.9-13 の「ゾーンのリモート Guard リストの設定」を参照してください。
- Detector のデフォルト リモート Guard リスト：リモート Guard のデフォルト リスト。ゾーンのリモート Guard リストが空の場合、Detector モジュールはこれらのリモート Guard をアクティブにします。

  詳細については、P.9-12 の「デフォルトのリモート Guard リストの設定」を参照してください。

ステップ 3　リモート Guard との通信チャネルを設定します。

詳細については、P.4-28 の「Guard との通信の確立」を参照してください。

ステップ 4　ゾーン Guard 保護形態（**protect-ip-state**）を設定し、Detector モジュールがリモート Guard をアクティブにするために使用する方式を決定します。

詳細については、P.9-5 の「Guard 保護のアクティベーション方式の設定」を参照してください。

ステップ 5　次のいずれかの方法で、リモート Guard 上に新しいゾーンを作成します。

- SSL を使用して、Detector モジュールのゾーン設定を Guard モジュールに同期させる。

  詳細については、P.5-15 の「Detector モジュールの Guard とのゾーン設定の同期」を参照してください。
- リモート Guard 上に新しいゾーンを作成する。**protect-ip-state dst-ip-by-ip** コマンドを使用して、攻撃対象の IP アドレスのみに基づいて Guard モジュール上の保護をアクティブにするように Detector モジュールを設定していない限り、Guard モジュール上のゾーン名は Detector モジュール上のゾーン名と一致している必要があります。

  protect-ip-state コマンドの詳細については、P.9-5 の「Guard 保護のアクティベーション方式の設定」を参照してください。

ステップ 6　リモート Guard 内で **protection-end-timer** コマンドを使用して、リモート Guard がゾーン保護を終了するために使用するタイマーを設定します。
protection-end-timer の値が **forever** の場合、リモート Guard は攻撃が終了してもゾーン保護を終了しません。

デフォルトのリモート Guard リストの設定

Detector モジュールは、次の両方の条件が当てはまる場合に、デフォルトのリモート Guard リスト内のリモート Guard をアクティブにします。

- ゾーン固有のリモート Guard リストが空であるか、または SSL および SSH の両方の通信方式を持つ Guard モジュールが含まれていない。
- デフォルトのリストのリモート Guard に、ゾーン固有のリモート Guard リストに定義されていない通信方式が設定されている。

Detector モジュールは、同じ通信方式のすべてのリモート Guard をアクティブにします。

デフォルトのリモート Guard リストに Guard 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。

remote-guard [**ssh** | **ssl**] *remote-guard-address* [*description*]

表 9-1 に、**remote-guard** コマンドの引数とキーワードを示します。

表 9-1　remote-guard コマンドの引数とキーワード

パラメータ	説明
ssh	（オプション）リモート Guard の通信方式を SSH に設定します。
ssl	（オプション）リモート Guard の通信方式を SSL に設定します。
remote-guard-address	リモート Guard の IP アドレス。
description	（オプション）リモート Guard の説明。説明は、最大 63 文字です。

次の例は、SSL 通信方式を使用してデフォルトのリモート Guard リストにリモート Guard を追加する方法を示しています。

```
user@DETECTOR-conf# remote-guard ssl 192.168.100.33
```

リモート Guard のデフォルトのリストを表示するには、グローバル モードまたは設定モードで **show remote-guards** コマンドを使用します。

ゾーンのリモート Guard リストの設定

Detector モジュールは、ゾーンのリモート Guard リストに記載されているすべてのリモート Guard をアクティブにします。

ゾーンのリモート Guard リストに Guard を追加するには、ゾーン設定モードで次のコマンドを入力します。

remote-guard [**ssh** | **ssl**] *remote-guard-address* [*description*]

表 9-2 に、**remote-guard** コマンドの引数とキーワードを示します。

表 9-2　remote-guard コマンドの引数

パラメータ	説明
ssh	リモート Guard の通信方式を SSH に設定します。
ssl	リモート Guard の通信方式を SSL に設定します。
remote-guard-address	リモート Guard の IP アドレス。
description	（オプション）リモート Guard の説明。説明は、最大 63 文字の英数字です。

次の例は、SSL 通信方式を使用してゾーンのリモート Guard リストに Guard を追加する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# remote-guard ssl 192.168.100.33
```

ゾーンのリモート Guard リストを表示するには、ゾーン設定モードで **show remote-guards** コマンドを使用します。

リモート Guard のオフラインでのアクティブ化

Detector モジュールは、ゾーン トラフィックに異常を検出すると、イベントをログに記録し、場合によって Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを生成します。その後、手動で Guard をアクティブにし、ゾーンを保護することができます。詳細については、P.4-43 の「SNMP トラップのイネーブル化」を参照してください。

Guard をオフラインでアクティブにするには、次の手順を実行します。

ステップ 1　Detector モジュールと Guard の両方にゾーンを設定するか、またはゾーン設定をオフラインで同期します。

詳細については、P.5-17 の「同期用のゾーンの設定」を参照してください。

ステップ 2　(オプション）リモート Guard 内で **protection-end-timer** コマンドを使用して、リモート Guard がゾーン保護を終了するために使用するタイマーを設定します。protection-end-timer の値を **forever** に設定すると、リモート Guard は攻撃が終了してもゾーン保護を終了しません。

ステップ 3　**protect** コマンドを使用して、Cisco Anomaly Guard Module 上のゾーンをアクティブにします。

手動でのリモート Guard のアクティブ化

Detector モジュールがゾーン トラフィックに異常を検出する前であっても、リモート Guard を手動でアクティブにしてゾーンを保護することができます。

リモート Guard を手動でアクティブにするには、次の手順を実行します。

ステップ 1　ゾーン リモート Guard リストまたはデフォルトのリモート Guard リストにリモート Guard を追加します。

詳細については、P.9-8 の「リモート Guard リストを使用したリモート Guard のアクティブ化」を参照してください。

ステップ 2　**dynamic-filter remote-activate** コマンドを入力して動的フィルタを作成します。

詳細については、P.6-25 の「動的フィルタの追加」を参照してください。

CHAPTER 10

インタラクティブ検出モードの使用方法

ゾーン異常検出をイネーブルにすると、Cisco Traffic Anomaly Detector Module（Detector モジュール）では、ゾーンのトラフィックが分析されて、超過しているポリシーのしきい値が検索されます。ポリシーのしきい値を超過したことを検出すると、トラフィックを分析し、トラフィックを処理するための動的フィルタのセットを作成します。Detector モジュールは、推奨事項を使用して、動的フィルタを自動またはインタラクティブのどちらでもアクティブにできます。この章では、インタラクティブ検出モード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。

- インタラクティブ検出モードについて
- インタラクティブ検出モードのアクティブ化
- インタラクティブ検出モードのゾーンの設定
- 推奨事項の表示
- 推奨事項の管理
- インタラクティブ検出モードの非アクティブ化

インタラクティブ検出モードについて

Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃が開始されると、Detector モジュールのポリシーは動的フィルタを作成します。ゾーンがインタラクティブ検出モードである場合、Detector モジュールはこのような動的フィルタを自動的にアクティブにせず、どのようなアクションを取るかをユーザが決定するのを待ちます。ユーザの決定を待つフィルタは、保留動的フィルタと呼ばれます。Detector モジュールは、保留動的フィルタを推奨事項に従って生成したポリシーに応じて分類します。この推奨事項は、保留フィルタの要約と、保留動的フィルタの作成の元になるポリシーの名前、ポリシーのアクティベーションの原因となったトラフィック異常に関するデータ、保留動的フィルタの数、および推奨アクションについての情報を提供します。ユーザは、どの保留動的フィルタを受け入れるか、無視するか、または自動アクティベーションに向けるかを決定します。インタラクティブ検出モードは、攻撃の進行中に取るアクションを、より詳細に制御できます。

Detector モジュールは、インタラクティブ検出モードになっている限り、保留動的フィルタの生成を続けます。ゾーンの異常検出中は、いつでもインタラクティブ検出モードをアクティブにできますが、Detector モジュールがインタラクティブ検出モードで、ゾーンに対する DDoS 攻撃が進行中である場合に限り、推奨事項およびその保留動的フィルタを表示できます。インタラクティブ検出モードは、ゾーンの定義時、またはゾーン検出の開始前後に設定できます。

1000 個を超える保留動的フィルタがある場合、Detector モジュールは次のように動作します。

- ゾーンを非アクティブにして自動検出モードで再度アクティブにするよう指示するエラー メッセージを表示する。
- ゾーンのログ　ファイルおよびレポートに推奨事項を記録してから、推奨事項を廃棄する。

新しい推奨事項が利用可能になっても、Detector モジュールは通知を表示しません。推奨事項を追跡するには、次のいずれかのタスクを行います。

- ゾーン設定モードで **show** コマンドを使用して、ゾーンのステータスを表示する。
- **event monitor** コマンドを使用して、新しい保留動的フィルタの作成時に通知を受け取る。
- 外部 syslog サーバを使用して、新しい保留動的フィルタの通知を受け取る。

いつでもインタラクティブ検出モードを停止して、自動検出モードに戻ることができます。Detector モジュールは、インタラクティブ検出モード中の決定をすべて無視し、現在のすべての保留動的フィルタを受け入れます。ポリシーは、動的フィルタを自動的に生成してアクティブにするという役割を再開します。詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください。

インタラクティブ検出モードのアクティブ化

インタラクティブ検出モードを使用すると、攻撃の進行中に Detector モジュールが取るアクションを、より詳細に制御できます。インタラクティブ検出モードをアクティブにしない場合、Detector モジュールはゾーン上の攻撃を識別したときに動的フィルタを自動的にアクティブにします。

この項では、インタラクティブ検出モードで Detector モジュールをアクティブにするために必要な手順の概要を説明します。各手順には、タスクを完了するために必要な CLI コマンドが含まれています。

インタラクティブ検出モードをアクティブにするには、次の手順を実行します。

ステップ 1　**zone** *new-zone-name* **interactive** コマンドを使用して、インタラクティブ検出モードに設定された新しいゾーンを作成します。ゾーンがすでに存在する場合、このステップは省略してください。

```
user@DETECTOR-conf# zone scannet interactive
```

新しいゾーンを作成したら、ステップ 2 を省略してステップ 3 に進みます。

詳細については、P.10-6 の「インタラクティブ検出モードのゾーンの設定」を参照してください。

ステップ 2　インタラクティブ検出モードのゾーンの設定インタラクティブ検出モード用に設定されたゾーンがすでに作成されている場合は、このステップを省略します。

既存のゾーンをインタラクティブ検出モード用に設定するには、ゾーン設定モードで **interactive** コマンドを使用します。

```
user@DETECTOR-conf-zone-scannet# interactive
```

詳細については、P.10-6 の「インタラクティブ検出モードのゾーンの設定」を参照してください。

ステップ 3　（オプション）**event monitor** コマンドを使用すると、新しい推奨事項が使用可能になったときに Detector モジュールが通知を表示するように設定できます。

```
user@DETECTOR# event monitor
```

外部の syslog サーバを使用して、新しい保留動的フィルタの通知を受信することや、ゾーン設定モードで **show** コマンドを使用して、ゾーンのステータスを手動で表示することもできます。

ステップ 4　**learning** コマンドを使用して、Detector モジュールをアクティブにし、ゾーン トラフィック パターンをラーニングします。ラーニング プロセスの詳細については、第 8 章「ゾーン トラフィックの特性のラーニング」を参照してください。

ステップ 5　**detect** コマンドを使用して、ゾーン異常検出をアクティブにします。

```
user@DETECTOR-conf-zone-scannet# detect
```

詳細については、第 9 章「ゾーンのトラフィックの異常の検出」を参照してください。

ステップ 6　**show recommendations** コマンドを使用して、新しい推奨事項とその保留動的フィルタを表示します。

```
user@DETECTOR-conf-zone-scannet# show recommendations
user@DETECTOR-conf-zone-scannet# show recommendations 135
pending-filters
```

詳細については、P.10-7 の「推奨事項の表示」を参照してください。

ステップ 7　**recommendation** コマンドを使用して新しい推奨事項を管理する方法を決定します。これらの推奨事項を受け入れるか、無視するか、または自動的にアクティブ化することができます。

```
user@DETECTOR-conf-zone-scannet# recommendation 135 accept
```

詳細については、P.10-10 の「推奨事項の管理」を参照してください。

ステップ 8　**no interactive** コマンドを使用すると、インタラクティブ検出モードをいつでも非アクティブにできます。Detector モジュールは、新しい動的フィルタを自動的にアクティブにできます。

```
user@DETECTOR-conf-zone-scannet# no interactive
```

詳細については、P.10-13 の「インタラクティブ検出モードの非アクティブ化」を参照してください。

インタラクティブ検出モードのゾーンの設定

既存のゾーンのインタラクティブ検出モードをアクティブにするには、ゾーン設定モードで **interactive** コマンドを使用します。

次の例は、既存のゾーンに対してインタラクティブ検出モードをアクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# interactive
```

インタラクティブ検出モードに設定された新しいゾーンを作成するには、設定モードで次のコマンドを使用します。

zone *new-zone-name* **interactive**

new-zone-name 引数には、新しいゾーンの名前を指定します。ゾーン名は英数字の文字列とし、必ず英字で入力を開始してください。スペースは使用できません。また、63 文字以内で入力してください。

次の例は、新しいゾーンを作成し、インタラクティブ検出モードに設定する方法を示しています。

```
user@DETECTOR-conf# zone scannew interactive
```

インタラクティブ検出モードに設定された新しいゾーンが、デフォルト ゾーン テンプレートで作成されます。

推奨事項の表示

ゾーン設定モードで次のコマンドを入力すると、すべての推奨事項のリスト、保留動的フィルタのリスト、およびゾーンに固有の推奨事項を表示できます。

show recommendations [*recommendation-id*] [**pending-filters**]

表 10-1 に、**show recommendations** コマンドのキーワードと引数を示します。

表 10-1　show recommendations コマンドのキーワードと引数

パラメータ	説明
recommendation-id	（オプション）特定の推奨事項の ID。
pending-filters	（オプション）特定の推奨事項の保留フィルタのリストを表示します。

次の例は、すべての推奨事項のリストを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show recommendations
```

表 10-2 に、**show recommendations** コマンド出力のフィールドを示します。

表 10-2　show recommendations コマンド出力のフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

表 10-2　show recommendations コマンド出力のフィールド説明（続き）

フィールド	説明
Min current rate	最小攻撃レート（パケット / 秒）。 複数の保留動的フィルタを持つ推奨事項の場合、保留動的フィルタの最小レートが表示されます。
Max current rate	最大攻撃レート（パケット / 秒）。 複数の保留動的フィルタを持つ推奨事項の場合、保留動的フィルタの最大レートが表示されます。
No. of pending-filters	ポリシーしきい値の超過が発生したために作成された保留動的フィルタの数。
Recommended action	推奨されるアクション。推奨事項を受け入れると、このアクションが実行されます。

特定の推奨事項の保留フィルタを表示する前に、すべての推奨事項とその ID のリストを表示するには、**show recommendations** コマンドを使用します。

表 10-3 に、**show recommendations pending-filters** コマンド出力のフィールドを示します。

表 10-3　show recommendations pending-filters コマンドのフィールド説明

フィールド	説明
ID	推奨事項の識別番号。
Policy	推奨事項を作成したポリシー。
Threshold	超過したポリシーしきい値（パケット / 秒）。
Pending-filter-id	保留動的フィルタの識別番号。
Detection date	推奨事項が作成された日時。
Attack flow	攻撃フローの特性。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

表 10-3　show recommendations pending-filters コマンドのフィールド説明（続き）

フィールド	説明
Triggering rate	保留動的フィルタの作成をトリガーした攻撃レート（パケット / 秒）。
Current rate	現在の攻撃レート（パケット / 秒）。
Recommended action	推奨されるアクション。推奨事項を受け入れると、このアクションが実行されます。
Action flow	保留動的フィルタを受け入れた場合にそのフィルタで処理される、ゾーンへのトラフィック フローの特性。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示しています。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

Detector モジュールは、次の場合に、パラメータの 1 つにワイルドカードとしてアスタリスク（*）を使用できます。

- 値が特定されていない。
- パラメータに対して複数の値が測定された。

（注） Detector モジュールがインタラクティブ検出モードで、ゾーンに対する DDoS 攻撃が進行中である場合にだけ、推奨事項およびその保留動的フィルタを表示できます。

次の例は、推奨事項 135 の保留動的フィルタを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show recommendations 135
pending-filters
```

推奨事項の管理

推奨事項をアクティブにするかどうかを決定できます。すべての推奨事項、特定の推奨事項、または特定の保留動的フィルタに対して決定を行うことができます。その決定によって、ポリシーの保留動的フィルタが動的フィルタになるかどうか、およびその期間が決まります。

特定のポリシーの保留動的フィルタを自動的にアクティブにするよう Detector モジュールに指示できます。また、ポリシーによって推奨事項が生成されないよう Detector モジュールに指示することもできます。Detector モジュールのポリシーは、ゾーンがインタラクティブ検出モードで、DDoS 攻撃が進行中の場合、推奨事項を継続して生成します。ゾーンのステータスを検証して、さらにアクションが必要かどうかを判断するために推奨事項を管理する場合、ゾーンのステータスを表示することをお勧めします。

ゾーン ポリシーは、次のアクションを取ることができます。

- **notify**：ポリシーが Detector の syslog にイベントを記録します。イベントには、しきい値超過が発生したポリシーの詳細が記録されます。
- **remote-activate**：Detector が 1 つまたは複数のリモート Guard をアクティブにし、ゾーンの保護を開始します。

（注） 推奨事項を受け入れると、受け入れた推奨事項と同じまたは受け入れた推奨事項に含まれるフローを持ち、アクションとタイムアウトが同じである、その他の推奨事項も同様に受け入れられます。Detector モジュールは、これらの推奨事項を削除します。

ゾーンの推奨事項を決定するには、ゾーン設定モードで次のコマンドを使用します。

recommendation *recommendation-id* [**pending-filters** *pending-filter-id*] *decision* [*timeout*]

表 10-4 に、**recommendation** コマンドの引数とキーワードを示します。

表 10-4　recommendation コマンドの引数とキーワード

パラメータ	説明
recommendation-id	推奨事項の識別番号。アスタリスク（*）は、すべての推奨事項を示すワイルドカードです。
pending-filters *pending-filter-id*	（オプション）特定の保留動的フィルタの ID を指定します。
decision	推奨事項に対するアクション。指定できる値は、次のとおりです。 • **accept**：特定の推奨事項を受け入れます。保留動的フィルタは、動的フィルタになります。 • **always-accept**：特定の推奨事項を受け入れます。この決定は、推奨ポリシーによって新しい推奨事項が生成されると必ず、自動的に適用されます。保留動的フィルタは、自動的に動的フィルタになります。 このアクションを実行すると、Detector モジュールはこのような推奨事項を表示しなくなります。 • **always-ignore**：特定の推奨事項を無視します。動的フィルタも保留動的フィルタも生成されません。この決定は、ポリシーによって生成される将来のすべての推奨事項に自動的に適用されます。 推奨事項を常に無視するように決定した場合は、Detector モジュールが推奨事項を表示しなくなります。
timeout	（オプション）決定が適用される期間。指定できる値は、次のとおりです。 • **forever**：検出が有効である限り、推奨事項によって生成された動的フィルタをアクティブにします。このタイムアウトがデフォルトです。詳細については、P.6-22 の「動的フィルタの設定」を参照してください。 • *new-timeout*：定義した期間中、ポリシーによって生成された動的フィルタをアクティブにします。この期間は秒で測定されます。詳細については、P.6-22 の「動的フィルタの設定」を参照してください。

次の例は、推奨事項 135 を受け入れる方法を示しています。

```
user@DETECTOR-conf-zone-scannet# recommendation 135 accept
```

特定のポリシーまたはポリシーの任意の部分のインタラクティブ ステータスを設定し、ポリシーのその部分が推奨事項と保留動的フィルタを生成するかどうかを決定できます。ポリシーのインタラクティブ ステータスを設定することで、制御が可能になり、ポリシーをトラフィック フローによりよく適合させることができます。詳細については、P.7-32 の「ポリシーのインタラクティブ ステータスの設定」を参照してください。

Detector モジュールは、**always-accept** および **always-ignore** の推奨事項を表示しません。推奨事項を常に無視するまたは常に受け入れると決定した場合、その決定は、推奨事項を作成したポリシーのインタラクティブ ステータスの一部となります。

ポリシーをディセーブルまたは非アクティブにして、ポリシーが推奨事項と保留動的フィルタを生成しないようにすることができます。ポリシーをディセーブルまたは非アクティブにするには、**state** コマンドを使用します。詳細については、P.7-22 の「ポリシーの状態の変更」を参照してください。

次の例では、dns_tcp/53/analysis のインタラクティブ ステータスを **always-accept** に設定しています。

```
user@DETECTOR-conf-zone-scannet-policy-/dns_tcp/53/analysis/#
interactive-status always-accept
```

インタラクティブ検出モードの非アクティブ化

インタラクティブ検出モードを非アクティブにするには、ゾーン設定モードで **interactive** コマンドを使用します。ユーザがインタラクティブ検出モードを非アクティブにすると、Detector モジュールはすべての新しい動的フィルタを自動的にアクティブにし、ポリシーのインタラクティブ ステータスを **always-accept** に設定します（ゾーン ポリシーの表示方法の詳細については、P.7-39 の「ポリシーの表示」を参照してください）。

次の例は、ゾーン scannet のインタラクティブ検出モードを非アクティブにする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no interactive
```

CHAPTER 11

攻撃レポートの使用方法

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）が生成する攻撃レポート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。

- レポートのレイアウトについて
- レポートのパラメータについて
- 攻撃レポートの表示
- 攻撃レポートのエクスポート
- 攻撃レポートの削除

レポートのレイアウトについて

Detector モジュールは、攻撃の包括的な概要を把握するために役立つ、各ゾーンの攻撃レポートを提供します。攻撃の開始は Detector モジュールによって最初に動的フィルタが生成されたときで、攻撃の終了は動的フィルタが使用されなくなり新しい動的フィルタが追加されなくなったときです。レポートには、攻撃の詳細がセクションに分かれて記載されます。各セクションには、攻撃中のトラフィック フローの異なる特性が記載されます。以前の攻撃と進行中の攻撃のレポートを表示できます。また、FTP、Secure FTP（SFTP）、または Secure Copy（SCP）ネットワーク サーバなどのネットワーク サーバにレポートをエクスポートできます。

この項では、次のトピックについて取り上げます。

- General Details
- Attack Statistics
- Detected Anomalies

General Details

攻撃レポートの General Details セクションには、攻撃に関する一般的な情報が記載されます。

表 11-1 に、レポートのこのセクションのフィールドを示します。

表 11-1　攻撃レポートの General Details セクションのフィールド説明

フィールド	説明
Report ID	レポートの識別番号。**current** という値は、進行中の攻撃があることを示します。
Attack Start	攻撃が開始された日時。
Attack End	攻撃が終了した日時。**Attack in progress** という値は、進行中の攻撃があることを示します。
Attack Duration	攻撃の期間。

Attack Statistics

Attack Statistics セクションには、受信したトラフィック フローの一般的な分析が記載されます。

Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Detector モジュールがゾーンのトラフィックで検出したトラフィック異常の詳細が記載されます。動的フィルタの生成を要求するフローは、異常であると分類されます。このような異常はあまり発生しないか、または体系的な Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃となる可能性があります。Detector モジュールは、同じタイプおよび同じフロー パラメータ（送信元 IP アドレスや宛先ポートなど）の異常を 1 つの異常タイプにまとめます。

表 11-2 に、検出された異常の各タイプを示します。

表 11-2　検出された異常のタイプ

タイプ	説明
dns (tcp)	攻撃している DNS-TCP プロトコル フロー。
dns (udp)	攻撃している DNS-UDP プロトコル フロー。
fragments	断片化されたトラフィックが異常な量であることが検出されたフロー。
http	異常な HTTP トラフィック フロー。
ip_scan	多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。
other_protocols	攻撃している TCP/UDP 以外のプロトコル フロー。
port_scan	多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。
tcp_connections	異常な数の TCP 同時接続が検出されたフロー（データの有無は問わない）。
tcp_incoming	TCP サービスを攻撃していることが検出されたフロー。

表 11-2　検出された異常のタイプ（続き）

タイプ	説明
tcp_outgoing	ゾーンがクライアントである場合に、ゾーンによって開始された接続に対する SYN-ACK フラッドまたは他のパケット攻撃で構成されていることが検出されたフロー。
tcp_ratio	SYN パケット対 FIN/RST パケットの高い比率など、異なるタイプの TCP パケット間の比率が異常であることが検出されたフロー。
udp	攻撃している UDP プロトコル フロー。
unauthenticated_tcp	ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなど、Detector のスプーフィング防止機能が認証に成功しなかった検出済みのフロー。
user	ユーザ定義によって検出された異常なフロー。
worm_tcp	TCP/IP プロトコルを介したワームの攻撃。

レポートのパラメータについて

レポートの各セクションには、さまざまなトラフィック フローが記載されています。

表 11-3 で、Attack Statistics のフィールドについて説明します。

表 11-3　Attack Statistics のフィールド説明

フィールド	説明
Total Packets	攻撃パケットの合計数。
Average pps	平均トラフィック レート（pps）。
Average bps	平均トラフィック レート（bps）。
Max. pps	最大トラフィック レート（pps）。
Max. bps	最大トラフィック レート（bps）。

表 11-4 で、Detected Anomalies のフロー統計情報について説明します。

表 11-4　フロー統計情報のフィールド説明

フィールド	説明
ID	検出された異常の識別番号（ID）。
Start time	異常が検出された日時。
Duration	異常の期間（時間、分、秒）。
Type	異常のタイプ。
Triggering rate	ポリシーのしきい値を超過した異常トラフィック レート。
% Threshold	Triggering rate がポリシーのしきい値を上回っているパーセンテージ。
Flow	異常なフロー。この特性には、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートが含まれています。トラフィックが断片化されているかどうかを示します。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

パラメータの 1 つにワイルドカードとしてアスタリスク（*）を使用できます。アスタリスクは次のいずれかを示します。

- 値が特定されていない。
- 異常のパラメータに対して複数の値が測定された。

数値の前にあるナンバー記号（#）は、そのパラメータに対して測定された値の数を示します。

Detector モジュールは、フローの説明の右側に、notify という値を表示することがあります。notify の値は、その行が説明するトラフィック タイプの通知を Detector モジュールが生成することを示します。Detector モジュールは値が notify の場合、アクションを実行しません。

攻撃レポートの表示

特定のゾーンの攻撃レポートのリスト、または特定の攻撃の詳細なレポートを表示するには、ゾーン設定モードで次のコマンドを使用します。

show reports [**current** | *report-id*] [**details**]

表 11-5 に、**show reports** コマンドの引数とキーワードを示します。

表 11-5　show reports コマンドの引数とキーワード

パラメータ	説明
current	（オプション）進行中の攻撃のレポートを表示します。 進行中の攻撃のビット数およびパケット数は表示されません。進行中の攻撃のレポートでは、パケットとビットのフィールドにゼロ（0）という値が表示されます。
report-id	（オプション）レポートの識別番号。
details	（オプション）フローの詳細を表示します。

次の例は、ゾーン上のすべての攻撃のリストの表示方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show reports
```

表 11-6 に、**show reports** コマンド出力フィールドを示します。

表 11-6　show reports コマンド出力のフィールドの説明

フィールド	説明
Report ID	レポートの識別番号。**current** という値は、進行中の攻撃があることを示します。
Attack Start	攻撃が開始された日時。
Attack End	攻撃が終了した日時。**Attack in progress** という値は、進行中の攻撃があることを示します。
Attack Duration	攻撃の期間。

表 11-6　show reports コマンド出力のフィールドの説明（続き）

フィールド	説明
Attack Type	検出された攻撃のタイプ。指定できる値は、次のとおりです。 • **tcp_connections**：異常な数の TCP 同時接続が検出されたフロー（データの有無は問わない）。 • **http**：異常な HTTP トラフィック フロー。 • **tcp_incoming**：TCP サービスを攻撃していることが検出されたフロー。 • **tcp_outgoing**：ゾーンがクライアントである場合に、ゾーンが開始した接続に対する SYN-ACK 攻撃など、クライアントがゾーンであるように見える検出済み攻撃フロー。 • **unauthenticated_tcp**：Detector モジュールのスプーフィング防止機能が認証できなかった検出済みのフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。 • **dns (udp)**：攻撃している DNS-UDP プロトコル フロー。 • **dns (tcp)**：攻撃している DNS-TCP プロトコル フロー。 • **udp**：攻撃している UDP プロトコル フロー。 • **other_protocols**：攻撃している TCP/UDP 以外のプロトコル フロー。 • **fragments**：異常な量の断片化されたトラフィックが検出されたフロー。 • **hybrid**：特性の異なる複数の攻撃で構成された攻撃。 • **ip_scan**：多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。 • **port_scan**：多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。 • **user_detected**：ユーザ定義によって検出された異常なフロー。 • **worm_tcp**：TCP/IP プロトコルを介したワームの攻撃。

表 11-6　show reports コマンド出力のフィールドの説明（続き）

フィールド	説明
Peak Malicious Traffic	このフィールドは、Guard だけに関連し、Detector モジュールには適用されません。

次の例は、ゾーンにおける現在の攻撃のレポートを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show reports current
```

攻撃レポートには、次のような出力が表示されます。各セクションの詳細については、P.11-2 の「レポートのレイアウトについて」を参照してください。

```
Report ID            :   current
Attack Start         :   Feb 26 2004 09:58:54
Attack End           :   Attack in progress
Attack Duration      :   00:08:34


Attack Statistics:
             Total Packets    Average pps    Average bps     Max pps     Max bps
Received     95878            186.53         110977.74       1455.44     914428.24    N/A


Detected Anomalies:
ID      Start Time          Duration      Type                Triggering Rate    %Threshold
1       Feb 26 09:58:54     00:08:34      HTTP                997.44             897.44
        Flow: 6 *           *             92.168.100.34  80   no fragments
```

異常が検出されたフローに関する詳細なレポートを表示するには、**details** オプションを使用します。

表 11-7 に、詳細なレポートに含まれているフローのフィールドを示します。

表 11-7　詳細なレポートのフローのフィールド説明

フィールド	説明
Detected Flow	動的フィルタが生成される原因となったフロー。検出されたフローが特定の送信元 IP アドレスの特定の送信元ポートを示す場合があります。このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。
Action Flow	動的フィルタによって処理されたフロー。アクション フローが特定の送信元 IP アドレスのすべての送信元ポートを示す場合があります。アクション フローは、検出されたフローよりも広範囲であることがあります。 このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**any** の値は、断片化されたトラフィックと断片化されていないトラフィックの両方があることを示します。

攻撃レポートのエクスポート

監視および診断のために、攻撃レポートをネットワーク サーバにエクスポートできます。テキスト形式または Extensible Markup Language（XML）形式で攻撃レポートをエクスポートできます。

この項では、次のトピックについて取り上げます。

- 攻撃レポートの自動エクスポート
- すべてのゾーンの攻撃レポートのエクスポート
- ゾーン レポートのエクスポート

攻撃レポートの自動エクスポート

攻撃が終了した時点で攻撃レポートが XML 形式で自動的にエクスポートされるよう、Detector モジュールを設定できます。Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。www.cisco.com から、このバージョンに付属の xsd ファイルをダウンロードできます。

Detector モジュールが攻撃レポートを自動的にエクスポートするように設定するには、設定モードで次のコマンドを使用します。

export reports *file-server-name*

file-server-name 引数は、**file-server** コマンドを使用して設定したファイルをエクスポートするネットワーク サーバの名前を指定します。ネットワーク サーバに Secure FTP（SFTP）または Secure Copy（SCP）を設定する場合は、Detector モジュールが SFTP 通信および SCP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。

次の例は、ネットワーク サーバへの攻撃の終了時に、レポートを（XML 形式で）自動的にエクスポートする方法を示しています。

```
user@DETECTOR-conf# export reports Corp-FTP-Server
```

すべてのゾーンの攻撃レポートのエクスポート

グローバル モードで次のいずれかのコマンドを入力することにより、すべてのゾーンの攻撃レポートをテキスト形式または XML 形式でエクスポートできます。

- **copy reports** [**details**] [**xml**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy reports** [**details**] [**xml**] *file-server-name dest-file-name*

表 11-8 に、**copy reports** コマンドの引数とキーワードを示します。

表 11-8　copy reports コマンドの引数とキーワード

パラメータ	説明
details	（オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。
xml	（オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンでリリースされた xsd ファイルを参照してください（www.cisco.com からこのバージョンに付属の xsd ファイルをダウンロードできます）。デフォルトでは、レポートはテキスト形式でエクスポートされます。 XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。
ftp	攻撃レポートを FTP を使用してネットワーク サーバにエクスポートします。
server	ネットワーク サーバの IP アドレス。
full-file-name	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	（オプション）サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

表 11-8　copy reports コマンドの引数とキーワード（続き）

パラメータ	説明
file-server-name	**file-server** コマンドを使用して定義したネットワーク サーバの名前。 ネットワーク サーバは FTP サーバである必要があります。SFTP または SCP を使用して攻撃レポートをネットワーク サーバにエクスポートすることはできません。 詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。
dest-file-name	ファイルの名前。Detector モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。

次の例は、ログイン名 user1 とパスワード password1 を使用して、Detector モジュールによって処理されたすべての攻撃のリストを IP アドレス 10.0.0.191 の FTP サーバに（テキスト形式で）コピーする方法を示しています。

```
user@DETECTOR# copy reports ftp 10.0.0.191 admreports.txt user1
password1
```

次の例は、Detector モジュールによって処理されたすべての攻撃のリストを **file-server** コマンドを使用して定義したネットワーク サーバに（テキスト形式で）コピーする方法を示しています。

```
user@DETECTOR# copy reports Corp-FTP-Server AttackReports.txt
```

ゾーン レポートのエクスポート

特定のゾーンの攻撃レポートを FTP サーバにコピーするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] *file-server-name dest-file-name*

表 11-9 に、**copy zone reports** コマンドの引数とキーワードの説明を示します。

表 11-9　copy zone reports コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	既存のゾーンの名前を指定します。
current	（オプション）進行中の攻撃のレポートをエクスポートします（該当する場合）。 デフォルトでは、すべてのゾーン レポートをエクスポートします。
report-id	（オプション）既存のレポートの ID。指定した ID 番号を持つレポートが Detector モジュールによってエクスポートされます。ゾーン攻撃レポートの詳細を表示するには、**show zone reports** コマンドを使用します。 デフォルトでは、すべてのゾーン レポートをエクスポートします。
xml	（オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンでリリースされた xsd ファイルを参照してください（www.cisco.com からこのバージョンに付属の xsd ファイルをダウンロードできます）。デフォルトでは、レポートをテキスト形式でエクスポートします。 XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。
details	（オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。
ftp	攻撃レポートを FTP を使用してネットワーク サーバにエクスポートします。
server	サーバの IP アドレスと、ファイルの保存先ディレクトリの完全パス。

表 11-9　copy zone reports コマンドの引数とキーワード（続き）

パラメータ	説明
login	（オプション）サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 ネットワーク サーバは FTP サーバである必要があります。SFTP または SCP を使用してレポートをネットワーク サーバにエクスポートすることはできません。 詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。
dest-file-name	ファイルの名前。Detector モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。

次の例は、ログイン名 user1 とパスワード password1 を使用して IP アドレス 10.0.0.191 の FTP サーバにゾーンのすべての攻撃レポートをコピーする方法を示しています。

```
user@DETECTOR# copy zone scannet reports ftp 10.0.0.191
ScannetCurrentReport.txt user1 password1
```

次の例は、現在の攻撃のレポートを **file-server** コマンドを使用して定義したネットワーク サーバに（XML 形式で）コピーする方法を示しています。

```
user@DETECTOR# copy zone scannet reports current xml Corp-FTP-Server
AttackReport-5-10-05.txt
```

攻撃レポートの削除

古い攻撃レポートを削除して、空きディスク スペースを得ることができます。

攻撃レポートを削除するには、ゾーン設定モードで次のコマンドを使用します。

no reports *report-id*

report-id 引数には、既存のレポートの ID を指定します。すべての攻撃レポートを削除するには、アスタリスク（*）を入力します。ゾーン攻撃レポートの詳細を表示するには、**show zone reports** コマンドを使用します。

（注） 進行中の攻撃の攻撃レポートは削除できません。

次の例は、すべてのゾーン攻撃レポートを削除する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# no reports *
```

CHAPTER 12

Detector モジュールの診断ツールの使用

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）に関する統計情報や診断を表示する方法について説明します。

(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。

- インストールされているソフトウェア バージョン番号とライセンス契約の表示
- ソフトウェア ライセンス キー情報の表示
- Detector モジュールの設定の表示
- Detector モジュールのゾーンの表示
- カウンタを使用したトラフィックの分析
- ゾーンのステータスの表示
- Detector モジュールのログ管理

- ネットワーク トラフィックの監視と攻撃シグニチャの抽出
- 一般的な診断データの表示
- フラッシュ メモリの使用率の表示
- メモリ消費量の表示
- CPU 使用率の表示
- システム リソースの監視
- ARP キャッシュの管理
- ネットワーク統計情報の表示
- traceroute の使用
- 接続の確認
- デバッグ情報の取得

インストールされているソフトウェア バージョン番号とライセンス契約の表示

ソフトウェア ライセンス契約と、Detector モジュールにロードされているソフトウェア イメージのバージョン番号を表示できます。バージョン番号を表示することにより、Detector モジュールが次のどちらの帯域幅オプションを使用しているか確認できます。

- 1 Gbps 動作：Detector モジュールとスーパーバイザ エンジン間のトラフィックの最大帯域幅は 1 Gbps で、すべてのデータ トラフィックが、1 つのインターフェイス ポートだけを介して移動します。
- 2 Gbps 動作：Detector モジュールとスーパーバイザ エンジン間のトラフィックの最大帯域幅は 2 Gbps で、すべてのデータ トラフィックが、2 つのインターフェイス ポートを介して移動します。インストールされているソフトウェア イメージが 2 Gbps 動作を許可している場合には、バージョン番号に XG 指定子が含まれます（Cisco Anomaly Detector Module Image version 6.0（0.39）-XG など）。

（注） 2 Gbps 動作の場合に Detector モジュールを動作させるには、関連付けられているソフトウェア ライセンス キーをインストールする必要があります（P.12-4 の「ソフトウェア ライセンス キー情報の表示」を参照）。

ソフトウェア バージョン番号とライセンス契約情報を表示するには、次のコマンドを使用します。

show version

ソフトウェア ライセンス キー情報の表示

Detector モジュールが 2 Gbps 動作のためにソフトウェア イメージの XG バージョンを使用している場合には、XG ソフトウェア イメージをアクティブにするために必要なライセンス キーの関連情報を表示できます。ライセンス キー情報を表示して、次の情報を確認します。

- ライセンス キーがロードされていること。
- ライセンス キーの期限が切れていないこと。ライセンス キーがデモ バージョンの場合には、デモ ライセンス キーの失効日が表示されます。インストールされているライセンス キーが永続的である場合には、失効日として permanent の文字が表示されます。

（注） 1 Gbps 動作のソフトウェア イメージについては、ライセンス キーは不要です。Detector モジュールに現在ロードされているソフトウェア イメージを確認するには、**show version** コマンドを使用します（P.12-3 の「インストールされているソフトウェア バージョン番号とライセンス契約の表示」を参照）。

ソフトウェア ライセンス キー情報を表示するには、次のコマンドを使用します。

show license-key

Detector モジュールの設定の表示

Detector モジュールの設定ファイルを表示できます。このファイルには、インターフェイスの IP アドレス、デフォルト ゲートウェイ アドレス、および設定されたゾーンなど、Detector モジュールの設定に関する情報が含まれています。

Detector モジュールの設定ファイルを表示するには、次のコマンドを使用します。

show running-config [**all | detector | interfaces** [*interface-name*] | **zones**]

表 12-1 に、**show running-config** コマンドの引数とキーワードを示します。

表 12-1　show running-config コマンドの引数とキーワード

パラメータ	説明
all	（オプション）Detector モジュールのすべての機能（Detector モジュール、ゾーン、インターフェイス、および自己保護）の設定ファイルを表示します。
detector	（オプション）Detector モジュールの設定ファイルを表示します。
interfaces	Detector モジュールのインターフェイスの設定ファイルを指定します。
interface-name	（オプション）特定のインターフェイスの名前。 1 Gbps 動作の場合に有効な名前は次のとおりです。 • mng • giga 2 2 Gbps 動作の場合に有効な名前は次のとおりです。 • mng • giga 1 • giga 2
zones	（オプション）すべてのゾーンの設定ファイルを表示します。

次の例は、Detector モジュールの設定ファイルを表示する方法を示しています。

```
user@DETECTOR# show running-config detector
```

設定ファイルは、Detector モジュールを現在の設定値で設定するために入力するコマンドで構成されています。Detector モジュールの設定ファイルをリモート FTP サーバにエクスポートして、バックアップ用にしたり、別の Detector モジュールにその Detector モジュールの設定パラメータを実装できるようにすることができます。詳細については、P.12-7 の「Detector モジュールのゾーンの表示」を参照してください。

Detector モジュールのゾーンの表示

グローバル モードで **show** コマンドを入力することにより、ゾーンの概要を表示して、アクティブなゾーンやゾーンの現在のステータスを確認できます。

表 12-2 に、ゾーンの可能な動作状態を示します。

表 12-2　ゾーンのステータス

ステータス	説明
Auto detect mode	ゾーン異常検出がイネーブルで、動的フィルタはユーザの操作なしでアクティブになります。 Detector モジュールで、ゾーン異常検出がイネーブルで、Detector モジュールがポリシーのしきい値調整のためにゾーンのトラフィック特性をラーニングしている場合、ゾーン名の隣には (+learning) と表示されます。
Interactive detect mode	ゾーンはインタラクティブ検出モードです。動的フィルタは手動でアクティブになります。
Threshold Tuning phase	ゾーンはしきい値調整フェーズです。Detector モジュールは、ゾーンのトラフィックを分析して、ラーニング プロセスのポリシー構築フェーズ中に構築されたポリシーのしきい値を定義します。
Policy Construction phase	ゾーンはポリシー構築フェーズです。ゾーンのポリシーが作成されます。
Standby	ゾーンはアクティブではありません。

次の例は、Detector モジュールのゾーンの概要を表示する方法を示しています。

```
user@DETECTOR# show
```

カウンタを使用したトラフィックの分析

Detector モジュールおよびゾーン カウンタを表示することで、Detector モジュールが処理している現在のトラフィック上の情報を表示したり、ゾーン トラフィックを分析したり、監視タスクを実行することができます。

この項では、次のトピックについて取り上げます。

- カウンタおよびトラフィック レートの平均の表示
- Detector モジュールおよびゾーンのカウンタのクリア

カウンタおよびトラフィック レートの平均の表示

ゾーン カウンタを表示するには、次のコマンドのいずれかを入力します。

- **show** [**zone** *zone-name*] **rates**：受信カウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **rates detai**ls：受信カウンタの平均トラフィック レートを表示します。**zone** キーワードを使用しないでグローバル モードまたは設定モードからこのコマンドを実行すると、無効なゾーンの平均トラフィック レートも表示されます。
- **show** [**zone** *zone-name*] **rates** history：過去 24 時間における 1 分ごとの受信カウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **counters**：受信カウンタを表示します。
- **show** [**zone** *zone-name*] **counters details**：受信カウンタを表示します。**zone** キーワードを使用しないでグローバル モードまたは設定モードからこのコマンドを実行すると、無効なゾーンの受信トラフィック レートも表示されます。
- **show** [**zone** *zone-name*] **counters history**：過去 1 時間の受信カウンタの値を 1 分ごとに表示します。

Detector モジュール カウンタを表示するには、グローバル モードまたは設定モードでこのコマンドを使用します。

ゾーン カウンタを表示するには、次のコマンド モードのいずれかでコマンドを使用します。

- ゾーン設定モード：このコマンドは、現在のゾーン設定モードに関連する情報だけを表示するため、**zone** *zone-name* キーワードおよび引数を使用しないでください。

- グローバル モードまたは設定モード：**zone** キーワードおよび *zone-name* 引数を入力してゾーン名を指定します。

レート単位は、ビット / 秒（bps）およびパケット / 秒（pps）で表されます。

（注） ゾーンのレートは、ゾーン異常検出をイネーブルにしている場合、またはラーニング プロセスをアクティブにしている場合にだけ使用できます。

カウンタの単位はパケットおよびキロビットです。カウンタは、ゾーン検出をアクティブにしたときにゼロにリセットされます。

表 12-3 に、Detector モジュールのカウンタを示します。

表 12-3　Detector モジュール カウンタ

カウンタ	説明
Received	Detector モジュールが処理した、そのゾーンを宛先としたパケットの合計。
Invalid zone	異常検出がイネーブルになっているいずれのゾーンにも宛先変更されなかったトラフィック。この情報は、Detector モジュールのカウンタに限り使用可能です（**zone** キーワードを使用せずにグローバル モードまたは設定モードでコマンドを入力した場合）。

次の例は、Detector モジュールの平均トラフィック レートを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show rates
```

Detector モジュールおよびゾーンのカウンタのクリア

テストを行う予定で、カウンタにテスト セッションからの情報だけを含める場合は、Detector モジュールまたはゾーン カウンタをクリアできます。Detector モジュールはカウンタおよび平均トラフィック レートをクリアします。

Detector モジュールのカウンタをクリアするには、グローバル モードまたは設定モードでこのコマンドを使用します。

clear counters

次の例は、Detector モジュール のカウンタをクリアする方法を示しています。

```
user@DETECTOR-conf# clear counters
```

ゾーン カウンタをクリアするには、次のコマンドのいずれかを入力します。

- **clear counters**：ゾーン設定モード。
- **clear zone** *zone-name* **counters**：グローバル モードまたは設定モード。*zone-name* 引数には、ゾーンの名前を指定します。

次の例は、ゾーン カウンタをクリアする方法を示しています。

```
user@DETECTOR-conf-zone-scannet# clear counters
```

ゾーンのステータスの表示

ゾーンの概要とそのステータスを表示するには、ゾーン設定モードで **show** コマンドを使用します。概要には、次の情報が含まれます。

- ゾーンのステータス：動作状態を示します。動作状態は、保護モード、保護およびラーニングのモード、しきい値調整モード、ポリシー構築モード、または非アクティブのいずれかです。
- ゾーンの基本設定：検出モード（自動またはインタラクティブ）、しきい値、タイマー、および IP アドレスなど、ゾーンの基本的な設定を示します。

  詳細については、P.5-11 の「ゾーンのアトリビュートの設定」を参照してください。
- ゾーン フィルタ：フレックスコンテンツ フィルタの設定、およびアクティブな動的フィルタの数を示します。ゾーンがインタラクティブ検出モードの場合、概要には推奨事項の数が表示されます。

  詳細については、P.6-4 の「フレックスコンテンツ フィルタの設定」および P.6-22 の「動的フィルタの設定」を参照してください。
- ゾーンのトラフィック　レート：ゾーンの正当なトラフィックと悪意あるトラフィックのレートを表示します。

  詳細については、P.12-8 の「カウンタを使用したトラフィックの分析」を参照してください。

次の例は、ゾーン ステータスを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show
```

Detector モジュールのログ管理

Detector モジュールは、システムのアクティビティおよびイベントを自動的にログに記録します。Detector モジュールのログを表示して、Detector モジュールのアクティビティを確認および追跡できます。

表 12-4 に、イベント ログのレベルを示します。

表 12-4　イベント ログのレベル

イベント レベル	数値コード	説明
Emergencies	0	システムが使用不能
Alerts	1	ただちに対処が必要
Critical	2	深刻な状態
Errors	3	エラー状態
Warnings	4	警告状態
Notifications	5	通常、ただし注意が必要
Informational	6	情報メッセージ
Debugging	7	デバッグ メッセージ

ログ ファイルには、すべてのログ レベル（emergencies、alerts、critical、errors、warnings、notification、informational、および debugging）が表示されます。Detector モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

イベント ログは、ローカルで表示することも、リモート サーバから表示することもできます。この項では、次のトピックについて取り上げます。

- オンライン イベント ログの管理
- ログ ファイルの管理

オンライン イベント ログの管理

この項では、Detector モジュールのイベントのリアルタイム ロギングを管理する方法について説明します。この項では、次のトピックについて取り上げます。

- オンライン イベント ログの表示
- オンライン イベント ログのエクスポート

オンライン イベント ログの表示

Detector モジュールの監視機能をアクティブにして、リアルタイム イベント ログを表示すると、Detector モジュール イベントのオンライン ロギングを表示できます。オンライン イベント ログを表示するには、次のコマンドを使用します。

event monitor

次の例は、監視をアクティブにする方法を示しています。

```
user@DETECTOR# event monitor
```

画面は新しいイベントを表示するために、定期的にアップデートされます。

(注)　監視を非アクティブにするには、**no event monitor** コマンドを使用してください。

オンライン イベント ログのエクスポート

Detector モジュールのオンライン イベント ログをエクスポートして、ログファイルに登録された Detector モジュールの動作を表示できます。また、Detector モジュールのログ ファイルに登録されている Detector モジュールのイベントをリモート ホストから表示できます。Detector モジュールのログ ファイルは、syslog メカニズムを使用してエクスポートされます。Detector モジュールのログ ファイルを複数の syslog サーバにエクスポートし、追加サーバを指定できるため、1 つのサーバがオフラインになっても、他のサーバがメッセージを受信できます。

Detector モジュールのオンライン ログのエクスポートは、リモート syslog サーバだけに適用できます。リモート syslog サーバが使用できない場合は、**copy log** コマンドを使用して、Detector モジュールのログ情報をファイルにエクスポートしてください。

次に、イベント ログの例を示します。

```
Sep 11 16:34:40 10.4.4.4 cm: scannet, 5 threshold-tuning-start: Zone
activation completed successfully.
```

システム ログ メッセージの構文は、次のとおりです。

event-date event-time Detector-IP-address detection-level zone-name event-severity-level event-type event-description

オンライン イベント ログをエクスポートするには、次の手順を実行します。

ステップ 1　（オプション）設定モードで次のコマンドを入力して、ロギング パラメータを設定します。

logging {**facility** | **trap**}

表 12-5 に、**logging** コマンドのキーワードを示します。

表 12-5　logging コマンドのキーワード

パラメータ	説明
facility	エクスポート syslog ファシリティを指定します。リモート syslog サーバは、ロギング ファシリティを使用してイベントをフィルタリングします。たとえば、ロギング ファシリティを使用すると、リモート ユーザは、Detector モジュール イベントを 1 つのファイルで受信し、他のネットワーク デバイスからのイベントを別のファイルで使用できます。 使用できるファシリティは、local0 ～ local7 です。デフォルトは local4 です。
trap	リモート syslog に送信する syslog トラップの重大度を指定します。低い重大度を指定すると、それよりも高い重大度がイベント ログに記録されます。たとえば、トラップ レベルを **warning** に設定すると、error、critical、alerts、および emergencies も送信されます。指定できるトラップ レベルは、高い方から順に emergencies、alerts、critical、errors、warnings、notification、informational、および debugging です。デフォルトは notification です。

（注） 動的フィルタの追加および削除に関するイベントを受信するには、トラップ レベルを informational に変更してください。

ステップ 2　次のコマンドを入力して、リモート syslog サーバの IP アドレスを設定します。

logging host *remote-syslog-server-ip*

remote-syslog-server-ip　引数には、リモート syslog サーバの IP アドレスを指定します。

ロギング メッセージを受信する syslog サーバのリストを作成するには、**logging host** コマンドを複数回入力してください。

次の例は、重大度レベルが notification より高いトラップを送信するように Detector モジュールを設定する方法を示しています。Detector モジュールは、ファシリティ local3 を使用して、IP アドレス 10.0.0.191 の syslog サーバにトラップを送信します。

```
user@DETECTOR-conf# logging facility local3
user@DETECTOR-conf# logging trap notifications
user@DETECTOR-conf# logging host 10.0.0.191
```

Detector モジュールがオンライン イベント ログのエクスポートに使用する設定を表示するには、**show logging** コマンドまたは **show log export-ip** コマンドを使用します。

ログ ファイルの管理

この項では、Detector モジュールのログ ファイルを管理する方法について説明します。この項では、次のトピックについて取り上げます。

- ログ ファイルの表示
- ログ ファイルのエクスポート
- ログ ファイルのクリア

ログ ファイルの表示

診断または監視のために Detector モジュールのログを表示できます。Detector モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

Detector モジュールのログを表示するには、グローバル モードで次のコマンドを使用します。

show log

次の例は、Detector モジュールのログを表示する方法を示しています。

```
user@DETECTOR# show log
```

ゾーンのログを表示して、指定したゾーンだけに関連するイベントを確認できます。

ゾーンのログを表示するには、ゾーン設定モードで **show log** コマンドを使用します。

ログ ファイルのエクスポート

グローバル モードで次のいずれかのコマンドを入力することにより、監視または診断を行うために、Detector モジュールのログ ファイルをネットワーク サーバにエクスポートできます。

- **copy** [**zone** *zone-name*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log** {**sftp** | **scp**} *server full-file-name login*

（注） **logging host** コマンドを使用すると、イベント ログを自動的にエクスポートするように Detector モジュールを設定できます。詳細については、P.12-13 の「オンライン イベント ログのエクスポート」を参照してください。

Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）および Secure Copy Protocol（SCP）はセキュアな通信を Secure Shell（SSH; セキュア シェル）に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。セキュアな通信のために Detector モジュールで使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 12-6 に、**copy log ftp** コマンドの引数とキーワードを示します。

表 12-6　copy log ftp コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	（オプション）ゾーン名を指定します。ゾーンのログ ファイルをエクスポートします。デフォルトでは、Detector モジュールのログ ファイルがエクスポートされます。
log	ログ ファイルをエクスポートします。
ftp	ログを FTP ネットワーク サーバにエクスポートします。
sftp	ログを SFTP ネットワーク サーバにエクスポートします。
scp	ログを SCP ネットワーク サーバにエクスポートします。
server	ネットワーク サーバの IP アドレス、パス、およびファイル名。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 192.168.10.2）。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

次の例は、Detector モジュールのログ ファイルを FTP サーバにエクスポートする方法を示しています。

```
user@DETECTOR# copy log ftp 10.0.0.191 log.txt <user> <password>
```

ログ ファイルのクリア

Detector モジュールまたはゾーンのログ ファイルが大きい場合、またはテストを行う予定で、ログ ファイルにテスト セッションからの情報だけが含まれるようにする場合は、ログ ファイルをクリアすることができます。

Detector モジュールまたはゾーンのログ ファイルのエントリをすべてクリアするには、設定モードまたはゾーン設定モードで次のコマンドを使用します。

clear [**zone** *zone-name*] **log**

zone-name 引数には、ゾーン名を指定します。デフォルトでは、Detector モジュールのログ ファイルがクリアされます。**clear log** コマンドをゾーン設定モードで入力する場合、**zone** *zone-name* キーワードと引数は使用できません（Detector モジュールは、ゾーン設定モードに関連するゾーンのログのみクリアできます）。現在のゾーン ログの全エントリをクリアするには、ゾーン設定モードで **clear log** コマンドを使用します。

次の例は、Detector モジュール ログをクリアする方法を示しています。

```
user@DETECTOR-conf# clear log
```

ネットワーク トラフィックの監視と攻撃シグニチャの抽出

ネットワークの動作を阻害しないタップを使用して、ネットワークから直接トラフィックを記録するように Detector モジュールを設定できます。記録されたトラフィックからデータベースを作成できます。記録されたトラフィックのデータベースのクエリーによって、過去のイベントの分析、攻撃シグニチャの生成、ネットワークの現在のトラフィック パターンと Detector モジュールで以前に正常のトラフィック状態で記録されたトラフィック パターンとの比較などを行うことができます。

フィルタを設定すると、特定の基準を満たすトラフィックだけを Detector モジュールで記録することや、すべてのトラフィック データを記録して、Detector モジュールに表示するトラフィックをフィルタリングするように指定できます。

Detector モジュールは、トラフィックを gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式で記録し、記録されたデータを説明する Extensible Markup Language（XML）形式のファイルを添付します。

Detector モジュールは、記録されたトラフィックを分析して、記録された攻撃パケットのペイロードに共通のパターンまたはシグニチャが見られるかどうかを判断します。Detector モジュールは、記録されたトラフィックからシグニチャを抽出できます。シグニチャを使用すると、そのシグニチャと一致するパケット ペイロードを含むすべてのトラフィックをブロックするようにフレックスコンテンツ フィルタを設定できます。

Detector モジュールは、次の 2 つの方法でトラフィックを記録できます。

- 自動：トラフィック データは持続的にパケットダンプ キャプチャ ファイルに記録されます。

  以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。以前のパケットダンプ キャプチャ ファイルを保存するには、それらをネットワーク サーバにエクスポートする必要があります。

- 手動：ユーザが Detector モジュールをアクティブにしてトラフィックを記録している場合、トラフィックはパケットダンプ キャプチャ ファイルに記録されます。

  以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。記録されたトラフィックを保存するには、Detector モジュールでトラフィックの記録を再開する前に、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。手動の場合、Detector モジュールは最大 4 つのゾーンのトラフィックを同時に記録できます。

デフォルトでは、Detector モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。Detector モジュールは、すべてのゾーンで最大 80 MB のディスク スペースまで、手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイル用にディスク スペースを開放するため、古いファイルを削除する必要があります。

この項では、次のトピックについて取り上げます。

- Detector モジュールの自動トラフィック記録の設定
- Detector モジュールの手動トラフィック記録のアクティブ化
- Detector モジュールの手動トラフィック記録の停止
- 手動パケットダンプ設定の表示
- パケットダンプ キャプチャ ファイルの自動エクスポート
- パケットダンプ キャプチャ ファイルの手動エクスポート
- パケットダンプ キャプチャ ファイルのインポート
- パケットダンプ キャプチャ ファイルの表示
- パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成
- パケットダンプ キャプチャ ファイルのコピー
- パケットダンプ キャプチャ ファイルの削除

Detector モジュールの自動トラフィック記録の設定

Detector モジュールは、自動的にネットワーク トラフィックを記録するようにアクティブにすることができます。これによって、ネットワークに問題や攻撃が発生したときに、分析または比較に使用できるトラフィックの記録を入手できます。パケットダンプ キャプチャ フィルタを使用して、指定した基準を満たすトラフィックだけが記録されるように Detector モジュールを設定できます。また、すべてのトラフィックを記録し、その記録済みのトラフィックを表示するときにパケットダンプ キャプチャ フィルタを適用することもできます。

Detector モジュールでは、トラフィックがキャプチャ バッファに記録されます。キャプチャ バッファのサイズが 50MB に到達するか、または 10 分が経過すると、Detector モジュールはバッファされた情報を圧縮形式のローカル ファイルに保存し、バッファをクリアしてから、トラフィックの記録を継続します。

Detector モジュールは、複数の自動パケットダンプ キャプチャ ファイルを保存します。Detector モジュールによって記録されたトラフィックは、トラフィックの処理方法に基づいて分割されるため、複数の自動パケットダンプ キャプチャ ファイルを 1 つの時間枠から取得できます。自動パケットダンプ キャプチャ ファイルの名前には、Detector モジュールでトラフィックが記録された日時およびトラフィックの処理方法に関する情報が含まれます。

表 12-7 に、自動パケットダンプ キャプチャ ファイルの名前セクションを示します。

表 12-7　自動パケットダンプ キャプチャ ファイルの名前のセクション

セクション	説明
機能	パケットダンプ キャプチャの際に実行される Detector モジュールの機能のタイプ。 • **protect**：Detector モジュールはゾーン異常検出中にトラフィックを記録。 • **learn**：Detector モジュールはゾーンのラーニング プロセス中または検出およびラーニング プロセス中にトラフィックを記録。
キャプチャ開始時刻	Detector モジュールでトラフィックの記録が開始した時刻。
キャプチャ終了時刻	（オプション）Detector モジュールでトラフィックの記録が終了した時刻。現在 Detector モジュールがファイルにトラフィックを記録している場合、終了時刻は表示されません。

表 12-7　自動パケットダンプ キャプチャ ファイルの名前のセクション（続き）

セクション	説明
処理	Detector モジュールがトラフィックの処理に使用する方式。Detector モジュールでは、次の方式をサポートしています。 **dropped**：Detector モジュールはトラフィックを受信しました。ただし、Detector モジュールはトラフィックを転送しないため、トラフィックはドロップされます。

Detector モジュールは、ラーニング プロセスから取得した 1 つのパケットダンプ キャプチャ ファイル、およびゾーン保護がイネーブルの場合は、次の 2 つのタイプのパケットダンプ キャプチャ ファイルを保存します。

- 直前の 10 分間のトラフィック
- 現在のトラフィック

ゾーン検出をアクティブにした場合、またはネットワーク トラフィックを自動的に記録するために Detector モジュールをアクティブにした場合、Detector モジュールは検出プロセス中に記録した以前のパケットダンプ キャプチャ ファイルをすべて消去し、新しいファイルを作成します。

ネットワーク トラフィックを自動的に記録するように Detector モジュールを設定するには、次の手順を実行します。

ステップ 1　ゾーン トラフィックを自動的に記録するように Detector モジュールを設定します。ゾーン設定モードで次のコマンドを入力します。

```
packet-dump auto-capture
```

ステップ 2　（オプション）パケットダンプ キャプチャ データベースを作成するには、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。パケットダンプ キャプチャ データベースを作成するには、パケットダンプ キャプチャ ファイルをエクスポートする必要があります。

P.12-26 の「パケットダンプ キャプチャ ファイルの自動エクスポート」を参照してください。

次の例は、自動的にゾーン トラフィックを記録するように Detector モジュールを設定する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# packet-dump auto-capture
```

Detector モジュールでゾーンのトラフィック データの自動キャプチャを停止するには、**no packet-dump auto-capture** コマンドを使用します。

現在のパケットダンプ設定を表示するには、**show packet-dump** コマンドを使用します。

Detector モジュールの手動トラフィック記録のアクティブ化

トラフィックの記録を開始するように Detector モジュールをアクティブにできるため、特定の期間のトラフィックを記録したり、Detector モジュールがトラフィックの記録に使用する基準を変更することができます。

指定した数のパケットが記録された時点、またはラーニング プロセスかゾーン検出のどちらかが終了した時点で、Detector モジュールはトラフィックの記録を停止し、手動パケットダンプ キャプチャをファイルに保存します。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Detector モジュールは、最大 10 個のゾーンの手動パケットダンプ キャプチャを同時に記録できます。

手動パケットダンプ キャプチャをアクティブにするには、ゾーン設定モードで次のコマンドを使用します。

packet-dump capture [**view**] *capture-name pdump-rate pdump-count* [*tcpdump-expression*]

（注） トラフィックをキャプチャする間は、CLI セッションが停止します。キャプチャの進行中に作業を続行するには、Detector モジュールとのセッションを追加で確立してください。

表 12-8 に、**packet-dump** コマンドの引数とキーワードを示します。

表 12-8　packet-dump コマンドの引数とキーワード

パラメータ	説明
view	（オプション）Detector モジュールでリアルタイムに記録されているトラフィックを表示します。
capture-name	パケットダンプ キャプチャ ファイルの名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。
pdump-rate	サンプル レート（パケット / 秒）。1 ～ 10000 の値を入力します。 **（注）** Detector モジュールでは、同時に発生するすべての手動キャプチャについて、最大で 10,000 パケット/秒の累積パケットダンプ キャプチャ レートがサポートされます。 高いサンプル レート値を設定したパケットダンプ キャプチャは、多くのリソースを消費します。パフォーマンスに悪影響を与える可能性があるため、高いレート値を設定するときは注意してください。

表 12-8　packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
pdump-count	記録対象のパケットの数。Detector モジュールが指定した数のパケットの記録を終了した時点で、手動パケットダンプ キャプチャ バッファがファイルに保存されます。1 ～ 5000 の整数を入力します。
tcpdump-expression	（オプション）記録対象のトラフィックを指定するために適用するフィルタ。Detector モジュールは、フィルタの式に適合するトラフィックだけをキャプチャします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.6-9 の「tcpdump 式の構文の設定」を参照してください。

次の例は、手動パケットダンプ キャプチャをアクティブにして、10 pps のサンプルレートで 1000 パケットを記録して、キャプチャしたパケットを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# packet-dump capture view 10 1000
```

Detector モジュールの手動トラフィック記録の停止

Detector モジュールでは、キャプチャをアクティブにしたときに指定したパケット数が記録された時点で、手動パケットダンプ キャプチャが停止します。ただし、Detector モジュールが指定された数のパケットを記録する前に、ユーザは手動パケットダンプ キャプチャを停止できます。

Detector モジュールで手動トラフィック記録を停止するには、次のいずれかのアクションを実行します。

- 開かれている CLI セッションで **Ctrl+C** キーを押す。
- 新しい CLI セッションを開き、希望のゾーン設定モードで次のコマンドを入力する。

  no packet-dump capture *capture-name*

capture-name 引数には、停止するキャプチャの名前を指定します。

Detector モジュールがパケットダンプ キャプチャ ファイルを保存します。

手動パケットダンプ設定の表示

Detector モジュールが手動パケットダンプ キャプチャ ファイル用に割り当てたディスク スペースの現在の容量を表示するには、設定モードまたはグローバル モードで **show packet-dump** コマンドを使用します。Detector モジュールでは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に、単一ブロックのディスク スペースが割り当てられます。

次の例は、Detector モジュールがゾーンの手動パケットダンプ キャプチャ ファイルに割り当てるディスク スペースの現在の総計を表示する方法を示しています。

```
user@DETECTOR-conf# show packet-dump
```

表 12-9 に、**show packet-dump** コマンド出力のフィールドを示します。

表 12-9　手動の show packet-dump コマンド出力のフィールドの説明

フィールド	説明
Allocated disk-space	すべてのゾーンの手動パケットダンプ キャプチャ用に割り当てられたディスク スペースの総容量（MB）。
Occupied disk-space	割り当てられたディスク スペースのうち、すべてのゾーンからの手動パケット ダンプ ファイルによって消費されたパーセンテージ。

パケットダンプ キャプチャ ファイルの自動エクスポート

FTP、SFTP、または SCP を使用してファイルを転送するネットワーク サーバにパケットダンプ キャプチャ ファイルを自動的にエクスポートするように Detector モジュールを設定できます。自動エクスポート機能をイネーブルにすると、Detector モジュールでパケットダンプ バッファの内容がローカル ファイルに保存されるたびに、パケットダンプ キャプチャ ファイルがエクスポートされます。Detector モジュールは、「gzip」（GNU zip）プログラムで圧縮、符号化された PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートし、記録されたデータを説明する XML 形式のファイルを添付します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。www.cisco.com から、このバージョンに付属の xsd ファイルをダウンロードできます。

Detector モジュールがパケットダンプ キャプチャ ファイルを自動的にエクスポートするように設定するには、設定モードで次のコマンドを使用します。

export packet-dump *file-server-name*

file-server-name 引数は、**file-server** コマンドを使用して設定したファイルをエクスポートするネットワーク サーバの名前を指定します。SFTP または SCP を使用するようにネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。

次の例は、パケットダンプ キャプチャ ファイルを自動的にエクスポートする方法を示しています。

```
user@DETECTOR-conf# export packet-dump Corp-FTP-Server
```

パケットダンプ キャプチャ ファイルの手動エクスポート

FTP、SFTP、または SCP を使用してファイルを転送するネットワーク サーバにパケットダンプ キャプチャ ファイルを手動でエクスポートするように設定できます。パケットダンプ キャプチャ ファイルを 1 つエクスポートすることも、特定のゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートすることもできます。Detector モジュールは、gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートし、記録されたデータを説明する XML 形式のファイルを添付します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。www.cisco.com から、このバージョンに付属の xsd ファイルをダウンロードできます。

パケットダンプ キャプチャ ファイルをネットワーク サーバに手動でエクスポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **ftp** *server remote-path* [*login* [*password*]]
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] {**sftp** | **scp**} *server remote-path login*
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] *file-server-name*

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 12-10 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 12-10　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	既存のゾーンの名前を指定します。
packet-dump captures	パケットダンプ キャプチャ ファイルをエクスポートします。
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Detector モジュールはゾーンのすべてのパケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.12-32 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。
ftp	パケットダンプ キャプチャ ファイルを FTP ネットワーク サーバからエクスポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP ネットワーク サーバからエクスポートします。
scp	パケットダンプ キャプチャ ファイルを SCP ネットワーク サーバからエクスポートします。
server	ネットワーク サーバの 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 192.168.10.2）。
remote-path	Detector モジュールがパケットダンプ キャプチャ ファイルを保存する場所の完全なパス名。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。

表 12-10　copy zone packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを FTP サーバ 10.0.0.191 に手動でエクスポートする方法を示しています。

```
user@DETECTOR# copy zone scannet packet-dump captures ftp 10.0.0.191
<user> <password>
```

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを、**file-server** コマンドを使用して定義されたネットワーク サーバに手動でエクスポートする方法を示しています。

```
user@DETECTOR# copy zone scannet packet-dump captures cap-5-10-05
Corp-FTP-Server
```

パケットダンプ キャプチャ ファイルのインポート

ネットワーク サーバからパケットダンプ キャプチャ ファイルを Detector モジュールにインポートできるため、過去のイベントを分析することや、現在のネットワーク トラフィック パターンと Detector モジュールが以前に通常のトラフィック状態で記録したトラフィック パターンとを比較することができます。Detector モジュールは、パケットダンプ キャプチャ ファイルを XML 形式と PCAP 形式の両方でインポートします。

パケットダンプ キャプチャ ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy ftp zone** *zone-name* **packet-dump captures** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **zone** *zone-name* **packet-dump captures** *server full-file-name login*
- **copy** *file-server-name* **zone** *zone-name* **packet-dump captures** *capture-name*

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 12-11 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 12-11　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
ftp	パケットダンプ キャプチャ ファイルを FTP ネットワーク サーバからインポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP ネットワーク サーバからインポートします。
scp	パケットダンプ キャプチャ ファイルを SCP ネットワーク サーバからインポートします。
zone *zone-name*	パケットダンプ キャプチャ ファイルをインポートする既存のゾーンの名前を指定します。
packet-dump captures	パケットダンプ キャプチャ ファイルをインポートします。
server	ネットワーク サーバの 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 192.168.10.2）。

表 12-11　copy zone packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
full-file-name	インポート対象のファイルの完全なパスとファイル名。ファイル拡張子は除きます。パスを指定しない場合、サーバはユーザのホーム ディレクトリからファイルをコピーします。 **（注）** ファイル拡張子を指定しないでください。指定すると、インポート プロセスが失敗する場合があります。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.13-10 の「ファイルを自動的にエクスポートする方法」を参照してください。
capture-name	インポートするファイルの名前。Detector モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを FTP サーバ 10.0.0.191 からインポートする方法を示しています。

```
user@DETECTOR# copy ftp zone scannet packet-dump captures 10.0.0.191
/root/scannet/captures/capture-1 <user> <password>
```

次の例は、ネットワーク サーバからパケットダンプ キャプチャ ファイルをインポートする方法を示しています。

```
user@DETECTOR# copy CorpFTP running-config capture-1
```

パケットダンプ キャプチャ ファイルの表示

パケットダンプ キャプチャ ファイルのリスト、または 1 つのパケットダンプ キャプチャ ファイルの内容を表示できます。デフォルトでは、Detector モジュールはすべてのゾーンのパケットダンプ キャプチャ ファイルのリストを表示します。

パケットダンプ キャプチャ ファイルを表示するには、ゾーン設定モードで次のコマンドを使用します。

show packet-dump captures [*capture-name* [*tcpdump-expression*]]

表 12-12 に、**show packet-dump captures** コマンドの引数を示します。

表 12-12　show packet-dump captures コマンドの引数

パラメータ	説明
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Detector モジュールはすべてのゾーンのパケットダンプ キャプチャ ファイルのリストを表示します。コマンド出力のフィールドの説明については、表 12-13 を参照してください。 パケットダンプ キャプチャ ファイルの名前を指定した場合、Detector モジュールはそのファイルを TCPDump 形式で表示します。
tcpdump-expression	（オプション）Detector モジュールでパケットダンプ キャプチャ ファイルを表示する際に使用されるフィルタ。Detector モジュールは、パケットダンプ キャプチャ ファイルのうち、フィルタの基準に一致する部分だけを表示します。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.6-9 の「tcpdump 式の構文の設定」を参照してください。

次の例は、パケットダンプ キャプチャ ファイルのリストを表示する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show packet-dump captures
```

表 12-13 に、**show packet-dump captures** コマンド出力フィールドを示します。

表 12-13　show packet-dump captures コマンド出力のフィールドの説明

フィールド	説明
Capture -name	パケットダンプ キャプチャ ファイルの名前。自動パケットダンプ キャプチャ ファイルの名前の説明については、表 12-7 を参照してください。
Size (MB)	パケットダンプ キャプチャ ファイルのサイズ（MB 単位）。
Filter	Detector モジュールがトラフィックの記録時に使用するユーザ定義のフィルタ。このフィルタは TCPDump 形式です。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.6-9 の「tcpdump 式の構文の設定」を参照してください。

パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成

攻撃シグニチャは、攻撃パケットのペイロードに見られる共通パターンを記述するものです。Detector モジュールをアクティブにして異常なトラフィックのシグニチャを生成し、この情報を使用して同じタイプの将来の攻撃をすばやく識別できます。この機能を使用すると、シグニチャが発行される前であっても（アンチウィルス ソフトウェアのメーカーやメーリング リストなどから）、新しい DDoS 攻撃（分散型サービス拒絶攻撃）やインターネット ワームを検出することができます。

Detector モジュールでは、フレックスコンテンツ フィルタのパターン式の構文を使用して、攻撃シグニチャが生成されます。このシグニチャをフレックスコンテンツ フィルタのパターンで使用して、異常なトラフィックをフィルタリングして排除できます。詳細については、P.6-4 の「フレックスコンテンツ フィルタの設定」を参照してください。

トラフィックが通常状態のときに Detector モジュールが記録したパケットダンプ キャプチャ ファイルを、参照のために追加で指定できます。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Detector モジュールでは、異常なトラフィックのシグニチャが生成され、トラフィックが通常状態のときに記録されたトラフィックの中に、シグニチャが存在している時間の割合が特定されます。正常のトラフィック状態で記録されたトラフィックに攻撃シグニチャが高い確率で出現しても、攻撃のパターンを意味するとは限りません。

攻撃のシグニチャを生成するには、次の手順を実行します。

ステップ 1　**packet-dump capture** コマンドを使用して、Detector モジュールをアクティブにし、攻撃中のトラフィックを記録します。

詳細については、P.12-23 の「Detector モジュールの手動トラフィック記録のアクティブ化」を参照してください。

ステップ 2　攻撃進行中に Detector モジュールが記録したパケットダンプ キャプチャ ファイルを確認します。パケットダンプ キャプチャ ファイルのリストを表示するには、**show packet-dump captures** コマンドを使用します。

詳細については、P.12-32 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。

ステップ 3　Detector　モジュールで攻撃トラフィックのシグニチャの生成をアクティブにします。ゾーン設定モードで次のコマンドを入力します。

```
show packet-dump signatures capture-name [reference-capture-name]
```

表 12-14 に、**show packet-dump signatures** コマンドの引数を示します。

表 12-14　show packet-dump signatures コマンドの引数

パラメータ	説明
capture-name	シグニチャの生成元である既存のパケットダンプ キャプチャ ファイルの名前。
reference-capture-name	（オプション）トラフィックが通常状態のときに Detector モジュールが記録した既存のパケットダンプ キャプチャ ファイルの名前。参照用のパケットダンプ キャプチャ ファイルを指定した場合は、シグニチャが参照用のパケットダンプ キャプチャ ファイルに存在する時間の割合が表示されます。

表 12-15 に、**show packet-dump signatures** コマンド出力フィールドを示します。

表 12-15　show packet-dump signatures コマンド出力のフィールドの説明

フィールド	説明
Start Offset	パケット ペイロードの先頭から、パターンが開始する位置までのオフセット（バイト単位）。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *start-offset* 引数にコピーします。
End Offset	パケット ペイロードの先頭から、パターンが終了する位置までのオフセット（バイト単位）。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *end-offset* 引数にコピーします。

表 12-15　show packet-dump signatures コマンド出力のフィールドの説明（続き）

フィールド	説明
Pattern	Detector モジュールが生成したシグニチャ。Detector モジュールでは、フレックスコンテンツ フィルタのパターン式の構文を使用して、シグニチャが生成されます。詳細については、P.6-13 の「パターン式構文の設定」を参照してください。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーできます。
Percentage	シグニチャが *reference-capture-name* ファイルに存在する時間の割合。

次の例は、手動パケットダンプ キャプチャ ファイルからシグニチャを生成する方法を示しています。

```
user@DETECTOR-conf-zone-scannet# show packet-dump signatures
PDumpCapture
```

パケットダンプ キャプチャ ファイルのコピー

1 つのパケットダンプ キャプチャ ファイル、または 1 つのファイルの一部を、新しい名前でコピーできます。Detector モジュールは、既存の自動パケットダンプ キャプチャ ファイルを新しい自動パケットダンプ キャプチャ ファイルで上書きします。自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルをコピーする場合、Detector モジュールはこれらのファイルを手動ファイルとして保存します。ディスク スペースを解放する必要がある場合は、そのコピーを手動で削除します。詳細については、P.12-38 の「パケットダンプ キャプチャ ファイルの削除」を参照してください。

パケットダンプ キャプチャ ファイルをコピーするには、設定モードで次のコマンドを使用します。

copy zone *zone-name* **packet-dump captures** *capture-name* [*tcpdump-expression*] *new-name*

表 12-16 に、**copy zone packet-dump captures** コマンドの引数とキーワードを示します。

表 12-16　copy zone packet-dump captures コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	既存のゾーンの名前を指定します。
packet-dump	パケットダンプ キャプチャ ファイルをコピーします。
captures *capture-name*	既存のパケットダンプ キャプチャ ファイルの名前を指定します。
tcpdump-expression	（オプション）Detector モジュールでパケットダンプ キャプチャ ファイルのコピーに使用されるフィルタ。Detector モジュールは、パケットダンプ キャプチャ ファイルのうち、フィルタの基準に一致する部分だけをコピーします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.6-9 の「tcpdump 式の構文の設定」を参照してください。
new-name	新しいパケットダンプ キャプチャ ファイルの名前。 名前は、1 ～ 63 文字の英数字の文字列で、スペースを含めることはできませんが、アンダースコアを含めることはできます。

次の例は、パケットダンプ キャプチャ ファイル capture-1 の一部で capture-2 という名前のキャプチャ ファイルに適合する部分をコピーする方法を示しています。

```
user@DETECTOR-conf# copy zone scannet capture-1 “tcp and dst port 80
and not src port 1000” capture-2
```

パケットダンプ キャプチャ ファイルの削除

デフォルトでは、Detector モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

ゾーンごとに保存できる手動パケットダンプ キャプチャ ファイルは 1 つだけです。また、Detector モジュールに保存できるパケットダンプ キャプチャ ファイルは 10 個までです。新しい手動パケットダンプ キャプチャ ファイルのためのスペースを解放するには、古いファイルを削除する必要があります。

自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルを削除するには、次のいずれかのコマンドを使用します。

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*}（設定モードで）
- **clear packet-dump captures** {***** | *name*}（ゾーン設定モードで）

表 12-17 に、**clear packet-dump** コマンドの引数とキーワードを示します。

表 12-17　clear packet-dump コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	既存のゾーンの名前を指定します。
packet-dump captures	パケットダンプ キャプチャ ファイルを削除します。
*****	すべてのパケットダンプ キャプチャ ファイルを消去します。
name	削除対象のパケットダンプ キャプチャ ファイルの名前。

次の例は、すべての手動パケットダンプ キャプチャ ファイルを削除する方法を示しています。

```
user@DETECTOR-conf# clear packet-dump captures *
```

一般的な診断データの表示

一般的な診断データを表示するには、次のコマンドを使用します。

show diagnostic-info [**details**]

診断データには、次の情報があります。

- Line Card Number：Detector モジュールの識別子文字列。
- Number of Pentium-class Processors：Detector モジュールのプロセッサの番号。Detector モジュールはプロセッサ 1 をサポートします。
- BIOS Vendor：Detector モジュール上の BIOS のベンダー。
- BIOS Version：Detector モジュール上の BIOS バージョン。
- Total available memory：Detector モジュール上で使用可能なメモリの合計。
- Size of compact flash：Detector モジュール上のコンパクト フラッシュのサイズ。
- Slot Num：モジュールをシャーシに挿入するためのスロットの番号（1 ～ 9）。
- CFE version：CFE のバージョン番号。

（注） CFE のバージョンを変更するには、新しいフラッシュ バージョンをインストールする必要があります。CFE の新しいバージョンを焼き付けるには、**flash-burn** コマンドを使用します。詳細については、P.13-28 の「Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け」を参照してください。

- Recognition Average Sample Loss：計算済みの平均パケット サンプル損失。
- Forward failures (no resources)：システム リソースが不足しているために転送されなかったパケット数。

（注） Recognition Average Sample Loss または Forward failures の値が大きい場合、Detector モジュールのトラフィックが過負荷の状態に陥っています。負荷分散型の構成で複数の Detector モジュールをインストールすることをお勧めします。

フラッシュ メモリの使用率の表示

Detector モジュールは、アクティビティ ログおよびゾーン攻撃レポートを保持します。ディスクの使用率が 75% を超えている場合、または Detector モジュールに多数のゾーン（500 を超える）が定義されている場合は、ファイル履歴パラメータの値を小さくすることをお勧めします。使用されているディスク スペースがディスクの最大キャパシティの約 80% に達すると、Detector モジュールは syslog に警告メッセージを表示します。

Detector モジュールが警告メッセージを表示する場合は、ゾーン攻撃レポートをネットワーク サーバにエクスポートしてから、古い攻撃レポートを削除できます（P.11-11 の「攻撃レポートのエクスポート」および P.11-16 の「攻撃レポートの削除」を参照）。

Detector モジュールのレコードをネットワーク サーバに定期的に格納してから、ログをクリアすることをお勧めします。

（注） ディスク使用率がディスクの最大キャパシティの 80% に達すると、Detector モジュールは情報を消去して、ディスク使用率を約 75% に減らします。

Detector モジュールにインストールされているフラッシュ メモリの合計に対する使用可能なフラッシュ メモリの割合を表示するには、グローバル モードで次のコマンドを入力します。

show flash-usage

次の例は、フラッシュ メモリの使用率を表示する方法を示しています。

```
user@DETECTOR# show flash-usage
2%
```

メモリ消費量の表示

Detector モジュールは次の情報を表示します。

- メモリ使用量（KB 単位）。
- Detector モジュール統計エンジンが Anomaly Detection Engine Used Memory フィールドとして使用するメモリのパーセンテージ。

異常検出エンジンのメモリ使用量は、アクティブなゾーンの数および各ゾーンが監視するサービスの数に影響されます。

（注） 異常検出エンジンのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

Detector モジュールのメモリ消費量を表示するには、次のコマンドを使用します。

show memory

次の例は、Detector モジュールのメモリ消費量を表示する方法を示しています。

```
user@DETECTOR# show memory
              total    used    free    shared   buffers   cached
 In KBytes:  2065188  146260  1918928    0     2360      69232

 Anomaly detection engine used memory: 0.3%
```

（注） Detector モジュールの空きメモリの合計量は、空きメモリとキャッシュ メモリの合計です。

CPU 使用率の表示

Detector モジュールはユーザ モード、システム モード、ナイス値が負のタスク（負のナイス値を持つタスク、ナイス値はプロセスの優先順位を表す）、およびアイドル状態の CPU 時間のパーセンテージを表示します。ナイス値が負のタスクは、システム時間およびユーザ時間の両方でカウントされるため、CPU 使用率の合計が 100% を超えることがあります。

現在の CPU 使用率を表示するには、次のコマンドを使用します。

show cpu

次の例は、現在の CPU 使用率の表示方法を示しています。

```
user@DETECTOR# show cpu
Host CPU1: 0.0% user, 0.1% system, 0.1% nice, 98.0% idle
```

システム リソースの監視

グローバル モードまたは設定モードで次のコマンドを入力することで、Detector モジュールがシステム ステータスの分析および監視の支援に使用しているリソースの概要を表示できます。

show resources

次の例は、システム リソースを表示する方法を示しています。

```
user@DETECTOR# show resources
```

表 12-18 に、**show resources** コマンド出力フィールドを示します。

表 12-18　show resources コマンド出力のフィールド説明

フィールド	説明
Host CPU1	ユーザ モード、システム モード、ナイス値が負のタスク（負のナイス値を持つタスクで、プロセスの優先順位を表す）、およびアイドル状態における CPU1 の CPU 時間のパーセンテージ。ナイス値が負のタスクは、システム時間およびユーザ時間にもカウントされるため、CPU 使用率の合計が 100% を超えることがあります。
Flash space usage	Detector モジュールが使用している、割り当て済みのフラッシュ スペースのパーセンテージ。 フラッシュ スペースの使用率がフラッシュの最大キャパシティの約 75% に達すると、Detector モジュールは syslog に警告メッセージを表示し、トラップを送信します。 **（注）** フラッシュ使用率がフラッシュの最大キャパシティの 80% に達すると、Detector モジュールは情報を消去して、フラッシュ使用率を約 75% に減らします。 Detector モジュールのレコードをネットワーク サーバに定期的に格納してから、古いレコードを削除することをお勧めします。

表 12-18　show resources コマンド出力のフィールド説明（続き）

フィールド	説明
Flash space usage（*続き*）	フラッシュ スペースの使用率が 80% に達した場合は、ゾーン攻撃レポートをネットワーク サーバにエクスポートしてから、古い攻撃レポートを削除することができます（P.11-11 の「攻撃レポートのエクスポート」および P.11-16 の「攻撃レポートの削除」を参照）。
Accelerator card memory usage	アクセラレータ カードが使用しているポート当たりのメモリのパーセンテージ：1 Gbps 動作の場合は 1 ポート、2 Gbps 動作の場合は 2 ポート。 アクセラレータ カードのメモリ使用率が 85 パーセントを超えると、Detector モジュールは SNMP トラップを生成します。値が大きいときは、Detector モジュールが大量のトラフィックを監視している場合があります。
Accelerator card CPU utilization	アクセラレータ カード CPU 使用量のポート当たりのパーセンテージ：1 Gbps 動作の場合は 1 ポート、2 Gbps 動作の場合は 2 ポート。 アクセラレータ カードの CPU の使用率が 85 パーセントを超えた場合、Detector モジュールは SNMP トラップを生成します。値が大きいときは、Detector モジュールが大量のトラフィックを監視している場合があります。
Anomaly detection engine used memory	Detector モジュール統計エンジンが使用するメモリのパーセンテージを指定。異常検出エンジンのメモリ使用率は、アクティブなゾーンの数、各ゾーンが監視するサービスの数、Detector モジュールが監視しているスプーフィングされていないトラフィックの合計に影響されます。 異常検出エンジンのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

表 12-18　show resources コマンド出力のフィールド説明（続き）

フィールド	説明
Dynamic filters used	すべてのゾーンでアクティブな動的フィルタの総数。Detector モジュールは、アクティブな動的フィルタの数と、Detector モジュールがサポートする動的フィルタの総数（150,000）に対するアクティブな動的フィルタのパーセンテージを表示します。アクティブな動的フィルタの数が 150,000 に到達すると、Detector モジュールは重大度 EMERGENCY の SNMP トラップを生成します。アクティブな動的フィルタの数が 135,000 に到達すると、Detector モジュールは、重大度 WARNING の SNMP トラップを生成します。 値が大きいときは、Detector モジュールが大量の DDoS 攻撃のトラフィックを監視していることを示します。

Detector モジュールが生成するトラップの詳細については、表 4-13 を参照してください。

ARP キャッシュの管理

Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュを表示または操作して、アドレス マッピング エントリを消去または手動で定義できます。ARP キャッシュを管理するには、設定モードで次のコマンドを使用します。

arp {**-a** [*arp_hostname*] | **-d** *arp_hostname* | **-n** [*arp_hostname*] | **-s** *arp_hostname hw_addr*}

表 12-19 に、**arp** コマンドの引数とキーワードを示します。

表 12-19　arp コマンドの引数とキーワード

キーワード	説明
-a [*arp_hostname*]	ホストのエントリを代替（BSD）形式で表示します。オプションのホスト名を入力すると、指定したホストのエントリだけが表示されます。この **arp** コマンド オプションをグローバル コンフィギュレーション モードで実行することもできます。
-d *hostname*	指定したホストのエントリを削除します。
-n [*arp_hostname*]	ホストの数値アドレスを表示します。オプションのホスト名を入力すると、指定したホストの数値アドレスだけが表示されます。この **arp** コマンド オプションをグローバル コンフィギュレーション モードで実行することもできます。
-s *arp_hostname hw_addr*	ハードウェア アドレスを *hw_addr* クラス値に設定して、hostname の ARP アドレス マッピング エントリを作成します。

注意　Detector モジュールの ARP キャッシュを設定するには、Detector モジュール システムとネットワークに精通している必要があります。

ネットワーク統計情報の表示

ホスト ネットワーク接続、ルーティング テーブル、インターフェイス統計情報、およびマルチキャスト メンバシップを表示してネットワークの問題をデバッグするには、次のいずれかのコマンドを入力します。

netstat [*address_family_options*] [**--tcp** | **-t**] [**--udp** | **-u**] [**--raw** | **-w**] [**--listening** | **-l**] [**--all** | **-a**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--symbolic** | **-N**] [**--extend** | **-e** [**--extend** | **-e**]] [**--timers** | **-o**] [**--program** | **-p**] [**--verbose** | **-v**] [**--continuous** | **-c**] [*delay*]

netstat {**--route** | **-r**} [*address_family_options*] [**--extend** | **-e** [**--extend** | **-e**]] [**--verbose** | **-v**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--interfaces** | **-i**} [*iface*] [**--all** | **-a**] [**--extend** | **-e** [**--extend** | **-e**]] [**--verbose** | **-v**] [**--program** | **-p**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--groups** | **-g**} [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--masquerade** | **-M**} [**--extend** | **-e**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-ports**] [**--continuous** | **-c**] [*delay*]

netstat {**--statistics** | **-s**} [**--tcp** | **-t**] [**--udp** | **-u**] [**--raw** | **-w**] [*delay*]

netstat {**--version** | **-V**}

netstat {**--help** | **-h**}

(注) アドレス ファミリを指定しない場合、Detector モジュールは設定されているすべてのアドレス ファミリのアクティブなソケットを表示します。

表 12-20 に、**netstat** コマンドの引数とキーワードを示します。

（注） キーワードを完全に入力することも、キーワードの省略形を入力することもできます。キーワードの省略形には、先頭にダッシュ（-）が付きます。完全なキーワードには先頭にダッシュが 2 つ（--）付きます。

表 12-20　netstat コマンドの引数とキーワード

パラメータ名の省略形	パラメータの完全な名前	説明
address_family_options		（オプション）アドレス ファミリ オプションは、次のいずれかです。 • [--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]] • [--unix|-x] [--inet|--ip] [--ax25] [--ipx] [--netrom] • [--ddp]
-r	**--route**	Detector モジュールのルーティング テーブルを表示します。
-g	**--groups**	IPv4 および IPv6 のマルチキャスト グループ メンバシップ情報を表示します。
-i *iface*	**--interface** *iface*	すべてのネットワーク インターフェイスまたはオプションの *iface* 値のテーブルを表示します。
-M	**--masquerade**	Network Address Translation（NAT; ネットワーク アドレス変換）が使用されたマスカレード接続のリストを表示します。
-s	**--statistics**	各プロトコルのサマリー統計情報を表示します。
-v	**--verbose**	（オプション）出力を詳細に表示します。
-n	**--numeric**	（オプション）数値アドレスを表示します。

表 12-20　netstat コマンドの引数とキーワード（続き）

パラメータ名の省略形	パラメータの完全な名前	説明
	--numeric-hosts	（オプション）数値ホスト アドレスを表示しますが、ポートまたはユーザ名の解決には影響を与えません。
	--numeric-ports	（オプション）数値ポート番号を表示しますが、ホストまたはユーザ名の解決には影響を与えません。
	--numeric-users	（オプション）数値ユーザ ID を表示しますが、ホストまたはポート名の解決には影響を与えません。
-c	**--continuous**	（オプション）選択した情報を 1 秒ごとに継続的に表示します。
-e	**--extend**	（オプション）追加情報を表示します。最も詳しい情報を表示するには、このオプションを 2 回使用します。
-o	**--timers**	（オプション）ネットワーキング タイマーに関連する情報を表示します。
-p	**--program**	（オプション）各ソケットが属するプログラムの PID および名前を表示します。
-l	**--listening**	（オプション）リスニング ソケットだけを表示します。デフォルトでは、これらのソケットは省略されます。
-a	**--all**	（オプション）リスニング ソケットおよび非リスニング ソケットの両方を表示します。
delay		（オプション）*delay* 秒ごとに、netstat が統計情報からの出力を繰り返します。

（注） 1 つのコマンドに最大 13 の引数とキーワードを入力できます。

次の例は、netstat 情報を詳細に表示する方法を示しています。

```
user@DETECTOR# netstat -v
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address         State
tcp        0      0 localhost:1111  localhost:32777    ESTABLISHED
tcp        0      0 localhost:8200  localhost:32772    ESTABLISHED
.
.
.
tcp        0      0 localhost:33464 localhost:8200     TIME_WAIT
tcp        1      0 localhost:1113  localhost:33194    CLOSE_WAIT
.
.
.
Active UNIX domain sockets (w/o servers)
unix  2      [ ]         STREAM     CONNECTED     928
unix  3      [ ]         STREAM     CONNECTED     890  /tmp/.zserv
.
.
.
user@DETECTOR#
```

traceroute の使用

次のコマンドを入力することで、ネットワーク問題をデバッグするために、パケットがネットワーク ホストに到達するまでに取るルートを決定できます。

traceroute *ip-address* [**-F**] [**-f** *first_ttl*] [**-g** *gateway*] [**-i** *iface*] [**-m** *max_ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] [*packetlen*]

（注） **traceroute** コマンドでは IP アドレスだけが表示され、名前は表示されません。

表 12-21 に、**traceroute** コマンドの引数とキーワードを示します。

表 12-21　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	ルートがトレースされる IP アドレス。
-F	（オプション）*don't fragment* ビットを設定します。
-f *first_ttl*	（オプション）最初の発信プローブ パケットで使用される最初の Time-To-Live（TTL; 存続可能時間）を設定します。
-g *gateway*	（オプション）ルース ソース ルート ゲートウェイを指定します。各ゲートウェイに対して **-g** を使用することで、2 つ以上のゲートウェイを指定できます。ゲートウェイの最大数は 8 個です。
-i *iface*	（オプション）発信プローブ パケットの送信元 IP アドレスを取得するネットワーク インターフェイスを指定します。これは通常、マルチホーム ホストで役立ちます。
-m *max_ttl*	（オプション）発信プローブ パケットで使用される最大存続可能時間（最大ホップ数）を設定します。デフォルトは 30 ホップです。
-p *port*	（オプション）プローブで使用されるベース UDP ポート番号を設定します。デフォルトは 33434 です。

表 12-21　traceroute コマンドの引数とキーワード（続き）

パラメータ	説明
-q *nqueries*	（オプション）ttl 値に対して定義されるプローブの数を設定します。デフォルトは 3 です。
-s *src_addr*	（オプション）IP アドレス *src_addr* を発信プローブ パケットで送信元 IP アドレスとして設定します。
-t *tos*	（オプション）プローブ パケットのタイプ オブ サービスを、*tos* の値に設定します。デフォルトはゼロです。
-w *waittime*	（オプション）プローブに対する応答を待つ時間（秒）を設定します。デフォルトは 5 秒です。
packetlen	（オプション）プローブ パケットの長さを設定します。

次の例は、IP アドレス 10.10.10.34 へのルートをトレースする方法を示しています。

```
user@DETECTOR# traceroute 10.10.10.34
traceroute to 10.10.10.34 (10.10.10.34), 30 hops max, 38 byte packets
 1 10.10.10.34 (10.10.10.34) 0.577 ms  0.203 ms  0.149 ms
```

接続の確認

次のコマンドを入力することにより、ネットワーク ホストに ICMP ECHO_REQUEST パケットを送信して、接続を確認できます。

ping *ip-address* [**-c** *count*] [**-i** *interval*] [**-l** *preload*] [**-s** *packetsize*] [**-t** *ttl*] [**-w** *deadline*] [**-F** *flowlabel*] [**-I** *interface*] [**-Q** *tos*] [**-T** *timestamp option*] [**-W** *timeout*]

表 12-22 に、**ping** コマンドの引数とキーワードを示します。

表 12-22　ping コマンドの引数とキーワード

パラメータ	説明
ip-address	宛先 IP アドレス。
-c *count*	（オプション）ECHO_REQUEST パケットを *count* 個送信します。deadline オプションが指定されている場合、このコマンドはタイムアウトになるまで *count* 個の ECHO_REPLY パケットを待ちます。
-i *interval*	（オプション）パケットの送信を待ちます。この間隔は秒で表されます。デフォルトでは、1 秒に設定されます。
-l *preload*	（オプション）応答を待たずに *preload* 個のパケットを送信します。
-s *packetsize*	（オプション）送信するデータ バイト数を指定します。デフォルトは 56 です。
-t ttl	（オプション）IP の TTL を設定します。
-w *deadline*	（オプション）送受信されたパケット数に関係なく ping が終了するまでのタイムアウト（秒）を指定します。
-F *flow label*	（オプション）各エコー要求パケットに 20 ビットのフローラベルを割り当てて設定します。値がゼロの場合は、ランダムなフロー ラベルが使用されます。
-I *interface*	（オプション）送信元 IP アドレスを、指定したインターフェイス アドレスに設定します。

表 12-22　ping コマンドの引数とキーワード（続き）

パラメータ	説明
-Q *tos*	（オプション）インターネット制御メッセージ プロトコル（ICMP）データグラムに Type of Service（ToS; タイプ オブ サービス）関連のビットを設定します。
-T *timestamp option*	（オプション）特別な IP タイムスタンプ オプションを設定します。
-W *timeout*	（オプション）応答を待つ時間（秒）。

1 つのコマンドに最大 10 の引数とキーワードを入力できます。

次の例は、1 つの ICMP ECHO_REQUEST パケットを IP アドレス 10.10.10.30 に送信する方法を示しています。

```
user@DETECTOR# ping 10.10.10.30 -n 1
```

デバッグ情報の取得

Detector モジュールに動作上の問題が発生した場合は、Cisco TAC がお客様に Detector モジュールの内部デバッグ情報のコピーを送信するようお願いすることがあります。Detector モジュールのデバッグ コア ファイルには、Detector モジュールの動作不良をトラブルシューティングするための情報が含まれています。このファイルの出力は暗号化されており、Cisco TAC の担当者のみが使用するよう意図されています。

デバッグ情報を FTP サーバに抽出するには、次の手順を実行します。

ステップ 1　Detector モジュール ログ ファイルを表示します。

詳細については、P.12-16 の「ログ ファイルの表示」を参照してください。

ステップ 2　デバッグ情報を抽出する時期を判断するため、問題を示す最初のログ メッセージを識別します。Detector モジュールは、指定した時間から現在の時間までのデバッグ情報を抽出します。

ステップ 3　グローバル モードで次のコマンドを入力して、FTP サーバにデバッグ情報を抽出します。

```
copy debug-core time ftp server full-file-name [login [password]]
```

表 12-23 に、**copy debug-core** コマンドの引数とキーワードを示します。

表 12-23　copy debug-core コマンドの引数とキーワード

パラメータ	説明
time	デバッグ情報が必要となった原因のイベントの時刻。時刻の文字列では、次のように、*MMDDhhmm*[[*CC*]*YY*][*.ss*] という形式を使用します。 • *MM*：月（数値）。 • *DD*：日。 • *hh*：時（24 時間表記）。 • *mm*：分。 • *CC*：（オプション）年の最初の 2 桁（たとえば **20**05）。 • *YY*：（オプション）年の最後の 2 桁（たとえば 20**05**）。 • *.ss*：（オプション）秒（小数点が必要）。
ftp *server*	FTP サーバの IP アドレスを指定します。
full-file-name	バージョン ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	（オプション）FTP サーバのログイン名。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

次の例は、今年の 11 月 9 日 午前 6:45 のデバッグ情報を FTP サーバ 10.0.0.191 に抽出する方法を示しています。

```
user@DETECTOR# copy debug-core 11090645 ftp 10.0.0.191
/home/debug/debug-file <user> <password>
```

CHAPTER 13

メンテナンス タスクの実行

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）の一般的なケアや保守用の作業を行う方法について説明します。

（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。

- ファイル サーバの設定
- 設定のエクスポート
- 設定のインポートとアップデート
- ファイルを自動的にエクスポートする方法
- Detector モジュールのリロード
- Detector モジュールのリブートおよびゾーンの非アクティブ化
- Detector モジュール ソフトウェアのアップグレード
- 1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード
- MP 関連のコマンドの使用
- 忘失パスワードの復旧
- 工場出荷時のデフォルト設定へのリセット

ファイル サーバの設定

ネットワーク サーバを Detector モジュールで定義すると、そのサーバと Detector モジュールとの間でファイルをインポートおよびエクスポートできます。Detector モジュールでは、IP アドレス、通信方式、ログインの詳細など、ネットワーク サーバのアトリビュートを定義するネットワーク サーバ プロファイルを作成できます。ネットワーク サーバ プロファイルを作成することにより、サーバ名を指定するだけで、ファイルをインポートまたはエクスポートできます。

ネットワーク サーバを設定したら、次に export コマンドまたは import コマンドを設定する必要があります。たとえば、export reports コマンドを使用すると、Detector モジュールが攻撃レポートをネットワーク サーバにエクスポートするように設定できます。

ネットワーク サーバを設定するには、設定モードで次のいずれかのコマンドを使用します。

- **file-server** *file-server-name description* **ftp** *server remote-path login password*
- **file-server** *file-server-name description* [**sftp** | **scp**] *server remote-path login*

Secure FTP（SFTP）および Secure Copy（SCP）は、セキュアな通信を Secure Shell（SSH; セキュア シェル）に依存しているので、SFTP 通信および SCP 通信に Detector モジュールで使用する SSH 鍵を設定する必要があります。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 13-1 に、**file-server** コマンドの引数とキーワードを示します。

表 13-1　file-server コマンドの引数とキーワード

パラメータ	説明
file-server-name	ネットワーク サーバの名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。
description	ネットワーク サーバを説明する文字列。文字列の長さは最大 80 文字の英数字です。式にスペースを使用する場合は、式を引用符（" "）で囲みます。
ftp	ネットワーク サーバで FTP を使用するように定義します。

表 13-1　file-server コマンドの引数とキーワード（続き）

パラメータ	説明
sftp	ネットワーク サーバで SFTP を使用するように定義します。
scp	ネットワーク サーバで SCP を使用するように定義します。
server	ネットワーク サーバの 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 192.168.10.2）。
remote-path	ファイルの保存先ディレクトリまたはファイルのインポート元ディレクトリの完全パス。
login	ネットワーク サーバのログイン名。
password	ネットワーク サーバのパスワード。 このオプションは FTP サーバに対してだけ有効です。Detector モジュールは公開鍵を使用して SFTP および SCP を使用するネットワーク サーバを認証します。

次の例は、IP アドレス 10.0.0.191 を使用して FTP サーバを定義する方法を示しています。

```
user@DETECTOR-conf# file-server CorpFTP-Server “Corp’s primary FTP
server” ftp 10.0.0.191 /root/ConfigFiles <user> <password>
```

ネットワーク サーバを削除するには、設定モードで **no file-server** [*file-server-name* | *] コマンドを使用します。

ネットワーク サーバのリストを表示するには、グローバル モードまたは設定モードで **show file-servers** コマンドを使用します。

設定のエクスポート

Detector モジュールの設定ファイルまたはゾーン設定ファイル（running-config）をネットワーク サーバにエクスポートできます。Detector モジュールまたはゾーンの設定ファイルをリモート サーバにエクスポートすることで、次を実行できます。

- Detector モジュールの設定パラメータを別の Detector モジュールに実装する。
- Detector モジュールの設定をバックアップする。

Detector モジュールの設定ファイルをエクスポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy** [**zone** *zone-name*] **running-config ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **running-config** {**sftp** | **scp**} *server full-file-name login*
- **copy** [**zone** *zone-name*] **running-config** *file-server-name dest-file-name*

Cisco Anomaly Guard Module でゾーンを設定するために必要なゾーン設定の一部をエクスポートするには、**copy guard-running-config** コマンドを使用します。詳細については、P.5-28 の「ゾーン設定の手動エクスポート」を参照してください。

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 13-2 に、**copy running-config ftp** コマンドの引数とキーワードを示します。

表 13-2　copy running-config ftp コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	（オプション）ゾーン名を指定します。ゾーン名を指定すると、Detector モジュールはゾーン設定ファイルをエクスポートします。デフォルトでは、Detector モジュールの設定ファイルがエクスポートされます。
running-config	Detector モジュールのすべての設定、または指定されたゾーンの設定をエクスポートします。
ftp	File Transfer Protocol（FTP; ファイル転送プロトコル）を指定します。
sftp	Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）を指定します。
scp	Secure Copy Protocol（SCP）を指定します。
server	ネットワーク サーバの 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 192.168.10.2）。
full-file-name	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。

表 13-2　copy running-config ftp コマンドの引数とキーワード（続き）

パラメータ	説明
file-server-name	設定ファイルをエクスポートするネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.13-2 の「ファイル サーバの設定」を参照してください。
dest-file-name	リモート サーバ上の設定ファイルの名前。 Detector モジュールは、**file-server** コマンドを使用してネットワーク サーバに対して定義したディレクトリの宛先ファイル名を使用してネットワーク サーバ上に設定ファイルを保存します。

次の例は、Detector モジュールの設定ファイルを FTP サーバにエクスポートする方法を示しています。

```
user@DETECTOR# copy running-config ftp 10.0.0.191 run-conf.txt <user>
<password>
```

次の例は、Detector モジュールの設定ファイルをネットワーク サーバにエクスポートする方法を示しています。

```
user@DETECTOR# copy running-config CorpFTP Configuration-12-11-05
```

設定のインポートとアップデート

Detector モジュールまたはゾーンの設定ファイルを FTP サーバからインポートし、新しく転送されたファイルに応じて Detector モジュールを再設定できます。設定をインポートするには、次のいずれかのタスクを行います。

- Detector モジュールの既存の設定ファイルに基づいて Detector モジュールを設定する。
- Detector モジュールの設定を復元する。

ゾーンの設定は、Detector モジュールの設定の一部です。**copy ftp running-config** コマンドを使用して、両方のタイプの設定ファイルを Detector モジュールにコピーし、それに応じて再設定します。

(注)　既存の設定を新しい設定で置き換えます。新しい設定を有効にするには、Detector モジュールをリロードする必要があります。

すべてのゾーンを非アクティブにしてからインポート プロセスを開始することをお勧めします。Detector モジュールはゾーンを非アクティブにしてからゾーンの設定をインポートします。

Detector モジュールの設定ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **running-config** *server full-file-name login*
- **copy** *file-server-name* **running-config** *source-file-name*

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** または **scp** オプションを使用して **copy** コマンドを入力する前に、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-40 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 13-3 に、**copy ftp running-config** コマンドの引数を示します。

表 13-3　copy ftp running-config コマンドの引数

パラメータ	説明
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
server	ネットワーク サーバの 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 192.168.10.2）。
full-file-name	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリでファイルを検索します。
login	（オプション）サーバのログイン名。*login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Detector モジュールによってパスワードを要求されます。
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Detector モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.13-2 の「ファイル サーバの設定」を参照してください。
source-file-name	インポートするファイルの名前。Detector モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。

次の例は、Detector モジュール設定ファイルを FTP サーバからインポートする方法について示しています。

```
user@DETECTOR# copy ftp running-config 10.0.0.191
/root/backup/conf/scannet-conf <user> <password>
```

次の例は、Detector モジュールの設定ファイルをネットワーク サーバからインポートする方法について示しています。

```
user@DETECTOR# copy CorpFTP running-config scannet-conf
```

ファイルを自動的にエクスポートする方法

Detector モジュールが次のファイルをネットワーク サーバへ自動的にエクスポートするように設定できます。

- パケットダンプ キャプチャ ファイル

  Detector モジュールは、キャプチャ バッファのサイズが 50 MB に到達するか、または 10 分が経過すると、パケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.12-26 の「パケットダンプ キャプチャ ファイルの自動エクスポート」を参照してください。

- 攻撃レポート

  Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点でエクスポートします。詳細については、P.11-11 の「攻撃レポートの自動エクスポート」を参照してください。

- ゾーン設定

  ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、Detector モジュールはゾーンの設定ファイルをエクスポートします。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。

Detector モジュールはパケットダンプ キャプチャ ファイルと攻撃レポートを Extensible Markup Language（XML）形式でエクスポートします。ソフトウェア バージョンには、XML スキーマを記述した xsd ファイルが付属しています。www.cisco.com から xsd ファイルをダウンロードできます。

ファイルをネットワークサーバへ自動的にエクスポートするには、次の手順を実行します。

ステップ 1　ファイルをエクスポートできるネットワーク サーバを定義します。

詳細については、P.13-2 の「ファイル サーバの設定」を参照してください。

ステップ 2　次のコマンドを入力することにより、Detector モジュールがファイルを自動的にエクスポートするように設定します。

```
export {packet-dump | reports | sync-config} file-server-name
```

表 13-4 に、**export** コマンドの引数とキーワードを示します。

表 13-4　export コマンドの引数とキーワード

パラメータ	説明
packet-dump	パケットダンプ バッファの内容がローカル ファイルに保存されるたびに、パケットダンプ キャプチャ ファイルをエクスポートします。Detector モジュールは、gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートし、記録されたデータを説明する XML のファイルを添付します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。パケットダンプ キャプチャ ファイルの詳細については、P.12-19 の「ネットワーク トラフィックの監視と攻撃シグニチャの抽出」を参照してください。
reports	攻撃が終了したら、攻撃レポートを XML 形式でエクスポートします。Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点でエクスポートします。XML スキーマについては、このバージョンに付属の ExportedReports.xsd ファイルを参照してください。詳細については、P.11-11 の「攻撃レポートのエクスポート」を参照してください。
sync-config	ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定をエクスポートします。その後、その設定を Guard モジュールにインポートしてアクティブにし、ゾーンを保護することができます。 Detector モジュールがネットワーク サーバにゾーン設定を自動的にエクスポートできるようにするには、Detector モジュールのデフォルトのリモート サーバ リストまたはゾーンのリモート サーバ リストにそのサーバを設定する必要があります。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。

表 13-4　export コマンドの引数とキーワード（続き）

パラメータ	説明
file-server-name	ファイルを保存できるネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。

次の例は、IP アドレス 10.0.0.191 を使用して FTP サーバを定義し、攻撃の最後でそのサーバへ自動的にレポートを XML 形式でエクスポートするように Detector モジュールを設定する方法を示しています。

```
user@DETECTOR-conf# file-server CorpFTP-Server “Corp’s primary FTP
server” ftp 10.0.0.191 /root/ConfigFiles <user> <password>
user@DETECTOR-conf# export reports CorpFTP-Server
```

ネットワーク サーバへのファイルの自動エクスポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

Detector モジュールがゾーン設定をエクスポートするネットワーク サーバのデフォルト リストを表示するには、設定モードで **show sync-config file-servers** コマンドを使用します。

ゾーンのリモート サーバ リストを表示するには、ゾーン設定モードで **show sync-config file-servers** コマンドを使用します。

Detector モジュールのリロード

reload コマンドを使用すると、マシンをリブートすることなく Detector モジュールの設定をリロードできます。

次の変更内容を反映するには、Detector モジュールをリロードする必要があります。

- **shutdown** コマンドを使用した、物理インターフェイスの非アクティブ化またはアクティブ化
- 新しいフラッシュの組み込み

Detector モジュールのリブートおよびゾーンの非アクティブ化

デフォルトでは、Detector モジュールは、リブート プロセスの前にアクティブになっていたゾーンを再度アクティブにします。

非アクティブ動作状態のすべてのゾーンを Detector モジュールがロードするようにデフォルトの動作を変更するには、設定モードで次のコマンドを入力します。

no boot reactivate-zones

注意　ゾーンのラーニング フェーズは、リブート後に再起動されます。

Detector モジュール ソフトウェアのアップグレード

この項では、Detector モジュールが動作するために必要な次の 2 つのソフトウェア コンポーネントについて取り上げます。

- Supervisor Engine 2 または Supervisor Engine 720 をサポートする Cisco IOS リリース
- Detector モジュール ソフトウェア（メンテナンス パーティション イメージとアプリケーション パーティション イメージ）

Detector モジュール ソフトウェアをアップグレードするには、スーパーバイザ エンジンにログインする必要があります。

この項では、次のトピックについて取り上げます。

- Supervisor Engine 2 または Supervisor Engine 720 の Cisco IOS ソフトウェア
- Detector モジュール ソフトウェア

Supervisor Engine 2 または Supervisor Engine 720 の Cisco IOS ソフトウェア

Cisco IOS ソフトウェア イメージは、Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの Supervisor Engine 2 または Supervisor Engine 720 に存在します。スーパーバイザ エンジンに存在するイメージは、Detector モジュールとそのプロセッサを認識し、初期化します。Detector モジュールをサポートする Cisco IOS ソフトウェア リリースを使用する必要があります。

Detector モジュール ソフトウェア

Detector モジュール ソフトウェアは、プロセッサ制御複合体に組み込まれたコンパクト フラッシュ（CF）カード上に存在します。コンパクト フラッシュには、ソフトウェア イメージのパーティションが 2 つあります。それぞれには独自の Detector モジュール ソフトウェア イメージが用意されています。

- メンテナンス　パーティション（MP）：基本モジュールの初期化およびドーター カードの制御の機能のために必要な Detector モジュールのメンテナンス ソフトウェア イメージを格納しています。スーパーバイザ エンジンは、MP を cf:1 として識別します。

- アプリケーション パーティション（AP）：Detector モジュール アプリケーション ソフトウェア イメージを格納しています。スーパーバイザ エンジンは、AP を cf:4 として識別します。

スーパーバイザ エンジン コンソールで、コンパクト フラッシュ カード上の Detector モジュール ソフトウェアをアップグレードできます。このアップグレード プロセスでは、最新バージョンの AP イメージや MP イメージを Cisco Software Center から FTP サーバまたは Trivial File Transfer Protocol（TFTP）サーバにダウンロードし、コンパクト フラッシュ カードにインストールします。

(注)　Detector モジュール ソフトウェアをアップグレードして帯域幅のパフォーマンスを 1 Gbps から 2 Gbps に向上させる場合は、P.13-30 の「1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード」を参照してください。

Detector モジュールについては、次のアップグレード手順が利用可能です。

- AP のアップグレード手順：スーパーバイザ エンジンの CLI を使用して AP イメージをアップグレードします。P.13-17 の「AP イメージのアップグレード」を参照してください。
- MP のアップグレード手順：スーパーバイザ エンジンの CLI を使用して MP イメージをアップグレードします。MP イメージは、アップグレードの必要がほとんどありません。この手順は、ソフトウェア リリースに付属のリリース ノートで指示されている場合にのみ使用してください。P.13-21 の「MP イメージのアップグレード」を参照してください。
- インライン イメージのアップグレード手順：Detector モジュールの CLI を使用して、AP または MP イメージをアップグレードします。P.13-24 の「AP および MP イメージのインライン アップグレード」を参照してください。
- Common Firmware Environment（CFE）：Detector モジュールで CFE をアップグレードします。新しい AP または MP イメージをインストールする過程で CFE もアップグレードされるため、CFE のアップグレードの必要はほとんどありません。現在の CFE と新しい MP または AP イメージの不適合を表すエラー メッセージを Detector モジュールが表示した場合にのみ、CFE をアップグレードする必要があります。P.13-28 の「Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け」を参照してください。

アップグレード操作に関する注釈

AP および MP ソフトウェア イメージと CFE をアップグレードするときには、次のガイドラインに従います。

- AP および MP のバージョンをアップグレードするには、スーパーバイザ エンジンにログインします。
- CFE をアップグレードするには、Detector モジュールにログインします。
- AP イメージと MP イメージの両方をアップグレードする場合は、MP イメージを先にアップグレードする必要があります。
- MP に切り替えるには、**hw-module module** *slot_number* **reset cf:1** コマンドを使用します。MP モードで操作する主な目的は、AP イメージをアップグレードすることです。
- AP に切り替えるには、**hw-module module** *slot_number* **reset cf:4** コマンドを使用します。AP が通常の動作モードです。
- **show module** コマンドを使用すると、実行しているパーティション イメージのソフトウェア バージョンを表示できます。AP イメージを実行している場合、**show module** コマンドを使用すると AP イメージのバージョンが表示されます。たとえば、AP イメージのバージョン形式は 5.1(0.12) のように表示されます。MP イメージを実行している場合は、MP イメージのバージョンが表示されます。たとえば、MP イメージのバージョン形式は 5.1(0.0)m のように表示されます。
- MP イメージのファイル名の形式は、c6svc-mp.5-0-3.bin です。
- AP イメージのファイル名の形式は、c6svc-adm-k9.5-0-3.bin です。
- MP は、Detector モジュールと同じネットワーク設定を使用します。ネットワーク設定は、Detector モジュールのイメージをアップグレードする前に設定する必要があります。詳細については、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」および第 3 章「Detector モジュールの初期化」を参照してください。
- 1 Gbps の帯域幅動作で AP イメージのバージョン 5.x をバージョン 6.x にアップグレードする場合、インストール プロセスによって管理ポート指定子のインスタンスがすべて eth1 から mng に変更されます。

(注) **logging console** コマンドをスーパーバイザ エンジンに対してグローバルに設定し、アップグレード手順の出力の詳細を表示することをお勧めします。コンソールではなく Telnet セッションから接続している場合、コンソール メッセージを表示するには **terminal monitor** コマンドを使用します。

AP イメージのアップグレード

AP イメージをアップグレードするには、次の手順を実行します。

ステップ 1　アップグレード プロセスを開始する前に、**copy running-config** コマンドを使用して、Detector モジュールの設定をバックアップします。バックアップすることにより既存の設定を保存できるため、必要な場合は、設定を現在の状態に迅速に復元できます。詳細については、P.13-4 の「設定のエクスポート」を参照してください。

ステップ 2　保存するファイルをエクスポートします。次のファイルをエクスポートできます。

- **copy reports** コマンドまたは **copy zone** *zone-name* **reports** コマンドを使用することで、保存する攻撃レポートをエクスポートできます。詳細については、P.11-12 の「すべてのゾーンの攻撃レポートのエクスポート」および P.11-13 の「ゾーン レポートのエクスポート」を参照してください。
- **copy log** コマンドを使用して、保存するログをエクスポートします。詳細については、P.12-16 の「ログ ファイルのエクスポート」を参照してください。
- **copy zone** *zone-name* **packet-dump captures** コマンドを使用して、保存するパケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.12-27 の「パケットダンプ キャプチャ ファイルの手動エクスポート」を参照してください。

ステップ 3　www.cisco.com でイメージを見つけて、アプリケーション イメージを最新の利用可能なソフトウェア リリースにアップグレードします。

FTP または TFTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

ステップ 4　Detector モジュールをリセットし、MP イメージをロードします（この作業には約 3 分かかります）。すでに MP イメージを実行している場合は、このステップを省略します。

スーパーバイザ エンジンで次のコマンドを入力します。

hw-module module *slot_number* reset cf:1

slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 5　MP がブートしたこと、および Detector モジュールのステータスが OK であることを確認します。次のコマンドを入力します。

show module *slot_number*

ステップ 6　AP イメージをコンパクト フラッシュにインストールします。接続の速度によって異なりますが、この処理には、最大で 30 分かかります。次のコマンドを入力します。

copy ftp://*path***/***filename* **pclc#***slot_number***-fs:**

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に *ftp://user@host/absolute-path/filename* という構文を使用します。パスワードを要求されたら入力します。

また、TFTP サーバから目的のバージョンをダウンロードすることもできます。

注意　Detector モジュールのコンソールに「You can now reset the module.」というメッセージが表示されるまで、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードは失敗します。

ステップ 7　次のコマンドを入力して、Detector モジュールを AP にリセットします。

```
hw-module module slot_number reset cf:4
```

ステップ 8　次のコマンドを入力して、コピーした AP イメージが **show module** コマンドの出力に表示されていることを確認します。

```
show module slot_number
```

(注)　新しいバージョンで Common Firmware Environment（CFE）のアップデートが必要になることがあります。詳細については、各ソフトウェア リリースに対応するリリース ノートを参照してください（リリース ノートは www.cisco.com にあります）。CFE が不適合な場合、Detector モジュールは、AP イメージのアップグレード後に Detector モジュールへの最初のセッションを確立したときに、「Bad CFE version (*X*). This version requires version *Y*.」というメッセージを表示します。

詳細については、P.13-28 の「Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け」を参照してください。

次の例は、AP イメージをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified. <<< This message is informational

Proceed with reload of module? [confirm]

% reset issued for module 8
Sup# copy tftp:images/ap/adm-APUpgrade-4.0.0.x.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/adm-APUpgrade-4.0.0.x.bin]?
Destination filename [adm-APUpgrade-4.0.0.x.bin]?
.
.
.
19:50:06: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has
started>
19:50:06: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till
upgrade completes!!>

......<<< Wait

19:59:58: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has
succeeded>
19:59:58: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>

Sup# hw-module module 8 reset cf:4 <<<<< Resets Detector module to AP
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
...
%OIR-SP-6-INSCARD:Card inserted in slot 8, interfaces are now online
```

MP イメージのアップグレード

MP イメージは、アップグレードの必要がほとんどありません。MP ソフトウェアをアップデートするようソフトウェア リリースに付属のリリース ノートで指示されている場合、次の手順を実行します。

ステップ 1　www.cisco.com でソフトウェア イメージを見つけて、最新のソフトウェア リリースにアップグレードします。

FTP または TFTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

Detector モジュールをリセットし、MP イメージをロードするには（この作業には約 3 分かかります）、スーパーバイザ エンジンで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

すでに MP イメージを実行している場合は、このステップを省略します。

slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 2　次のコマンドを入力して、MP がブートされ、Detector モジュールのステータスが OK であることを確認します。

```
show module slot_number
```

ステップ 3　スーパーバイザ エンジンで次のコマンドを入力して、MP イメージをコンパクト フラッシュにコピーします。

```
copy ftp://path/filename pclc#slot_number-fs:
```

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。

FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に ftp://user@host/absolute-path/filename という構文を使用します。パスワードを要求されたら入力します。

アプリケーション イメージのダウンロードの所要時間は、接続の速度によって異なりますが、最大で約 30 分です。

注意　Detector モジュールのコンソールに「You can now reset the module.」というメッセージが表示されるまで、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードは失敗します。

また、TFTP サーバから目的のバージョンをダウンロードすることもできます。

MP コマンドの詳細については、P.13-34 の「MP 関連のコマンドの使用」を参照してください。

ステップ 4　次のコマンドを入力して、コピーした MP イメージが **show module** コマンドの出力に表示されることを確認します。

show module *slot_number*

ステップ 5　次のコマンドを入力して、Detector モジュールを AP にリセットします。

hw-module module *slot_number* **reset cf:4**

次の例は、MP イメージをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified. <<< This message is informational

Proceed with reload of module? [confirm]

% reset issued for module 8
Sup# copy tftp:images/mp/MPUpgrade-4.0.0.0.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/MPUpgrade-4.0.0.0.bin]?
Destination filename [MPUpgrade-4.0.0.0.bin]?
.
.
.
3d19h:%SVCLC-SP-5-STRRECVD:mod 8:<Upgrade of MP was successful.>
3d19h:%SVCLC-SP-5-STRRECVD:mod 8:<You can now reset the module>
Sup# show module 8
.
The Following output shows MP image name because Detector module is
reset to MP (cf:1)
.
Mod MAC addressesHwFwSwStatus
--- ----------------------------------- ------- ----------- -------
8   000f.348d.d7f0 to 000f.348d.d7f70.3017.2(1)4.0(0.0)mOther
...
Sup# hw-module module 8 reset cf:4 <<< Resets Detector module to AP
(normal operation)
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
...
%OIR-SP-6-INSCARD:Card inserted in slot 8, interfaces are now online
```

AP および MP イメージのインライン アップグレード

インライン イメージのアップグレード手順では、AP イメージおよび MP イメージをアップグレードする別の方法を示します。インライン イメージ アップグレードを実行する場合には、スーパーバイザ エンジンではなく、Detector モジュールからアップグレードを実行します。

ソフトウェア イメージをアップグレードするには、次の手順を実行します。

ステップ 1　アップグレード プロセスを開始する前に、**copy running-config** コマンドを使用して、Detector モジュールの設定をバックアップします。バックアップすることにより既存の設定を保存できるため、必要な場合は、設定を現在の状態に迅速に復元できます。詳細については、P.13-4 の「設定のエクスポート」を参照してください。

ステップ 2　保存するファイルをエクスポートします。次のファイルをエクスポートできます。

- **copy reports** コマンドまたは **copy zone** *zone-name* **reports** コマンドを使用することで、保存する攻撃レポートをエクスポートできます。詳細については、P.11-12 の「すべてのゾーンの攻撃レポートのエクスポート」および P.11-13 の「ゾーン レポートのエクスポート」を参照してください。
- **copy log** コマンドを使用して、保存するログをエクスポートします。詳細については、P.12-16 の「ログ ファイルのエクスポート」を参照してください。
- **copy zone** *zone-name* **packet-dump captures** コマンドを使用して、保存するパケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.12-27 の「パケットダンプ キャプチャ ファイルの手動エクスポート」を参照してください。

ステップ 3　www.cisco.com でイメージを見つけて、イメージを使用可能な最新のバージョンにアップグレードします。

FTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

ステップ 4　コンソール ポートまたは Telnet セッションを介してスーパーバイザ エンジンにログインします。

ステップ 5　メンテナンス イメージで Detector モジュールが稼働中の場合は、ステップ 7 に進みます。メンテナンス イメージで Detector モジュールが稼働中でない場合は、スーパーバイザ エンジンで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 6　Detector モジュールがオンラインに戻ったら、Detector モジュールとのコンソール セッションを確立し、ルート アカウントにログインします。このルート アカウントのデフォルトのパスワードは *cisco* です。コンソール セッションを確立するには、スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

```
session slot slot_number processor processor_number
```

slot-number は、Detector モジュールが挿入されているシャーシ内のスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）です。*processor_number* は、Detector モジュールのプロセッサの番号です。Detector モジュールは、プロセッサ 1 を介した管理だけをサポートします。

ステップ 7　次のコマンドを入力して、ソフトウェア イメージをアップグレードします。

```
upgrade ftp://path/filename
```

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。

FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に ftp://user@host/absolute-path/filename という構文を使用します。パスワードを要求されたら入力します。

AP ソフトウェア イメージをアップグレードするには、AP ソフトウェア イメージのファイル名を入力します。MP ソフトウェア イメージをアップグレードするには、MP ソフトウェア イメージのファイル名を入力します。詳細については、P.13-16 の「アップグレード操作に関する注釈」を参照してください。

注意　Detector モジュールのコンソールに、「Application image upgrade complete. You can boot the image now.」というメッセージが表示されるまで、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードは失敗します。

ステップ 8　アップグレードが完了したら、**exit** コマンドを入力して、Detector モジュールからログアウトします。

ステップ 9　次のコマンドを入力して、Detector モジュールを AP ソフトウェア イメージにリセットします。

```
hw-module module slot_number reset cf:4
```

（注）　新しいソフトウェア リリースへアップグレードするために、Common Firmware Environment（CFE）のアップデートが必要となる場合があります。詳細については、各ソフトウェア リリースに対応するリリース ノートを参照してください。CFE が不適合な場合、Detector モジュールは、AP イメージのアップグレード後に Detector モジュールへの最初のセッションを確立したときに、「Bad CFE version (*X*). This version requires version *Y*.」というメッセージを表示します。詳細については、P.13-28 の「Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け」を参照してください。

ステップ 10　Detector モジュールがリブートされたら、**show version** コマンドを入力してソフトウェア バージョンを確認します。

次の例は、Detector モジュール アプリケーション ソフトウェアをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
.
.
.
Proceed with reload of module? [confirm]
% reset issued for module 9
.
.
.
Sup# session slot 8 proc 1
.
.
.
login:root
Password:
.
.
.
root@localhost.cisco.com# upgrade
ftp://psdlab-pc1/pub/images/ap/adm-APUpgrade-4.0.0.x.bin


Downloading the image. This may take several minutes...
.
.
.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:



Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.
.
.
.
Application image upgrade complete. You can boot the image now.
root@hostname.cisco.com# exit
logout
                                                                [  OK  ]
[Connection to 127.0.0.91 closed by foreign host]
Sup# hw-module module 8 reset cf:4
```

Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け

現在の CFE とソフトウェア リリースが適合していない場合にだけ、新しいフラッシュ バージョンを焼き付けることができます。不適合は、Detector モジュール の AP または MP ソフトウェアをアップデートするときに発生する場合があります。

CFE の不適合が検出された場合、ソフトウェア リリースのアップグレード後に Detector モジュールとのセッションを初めて確立するときに、Detector モジュールは次のメッセージを表示します（X は古いフラッシュ バージョンを、Y は新しいフラッシュ バージョンを示します）。
「Bad CFE version (X). This version requires version Y.」

（注） CFE と Detector モジュールのソフトウェア バージョンが適合している場合に新しいフラッシュ バージョンを焼き付けようとすると、操作が失敗します。

注意 新しいフラッシュ バージョンを焼き付けている間は、Detector モジュールに安定して電源が供給されるようにし、かつ Detector モジュールを動作させないようにする必要があります。上記の制限に対応できない場合、アップグレードは正常に終了せず、Detector モジュールにアクセスできなくなる可能性があります。

新しいフラッシュ バージョンを焼き付けるには、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ます。

```
flash-burn
```

ステップ 2　Detector モジュールをリロードするには、次のコマンドを入力します。

```
reload
```

新しいフラッシュ バージョンを焼き付けた後、**reload** コマンドを入力する必要があります。Detector モジュールは、**reload** コマンドを実行した後でないと完全に機能しません。

次の例は、新しいフラッシュ バージョンを焼き付ける方法を示しています。

```
user@DETECTOR-conf# flash-burn
Please note: DON'T PRESS ANY KEY WHILE IN THE PROCESS!
. . .
Burned firmware successfully
SYSTEM IS NOT FULLY OPERATIONAL. Type 'reload' to restart the system
```

1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード

Detector モジュールが現在最大 1 Gbps の帯域幅で動作している場合には、ソフトウェア イメージの XG バージョンと対応するソフトウェア ライセンス キーをインストールすることによって、帯域幅パフォーマンスを 2 Gbps にアップグレードできます。XG ソフトウェア イメージは、Detector モジュールとスーパーバイザ エンジン間のデータ トラフィックに使用する追加インターフェイス ポートをアクティブにします（1 Gbps ソフトウェア イメージは、データ トラフィックに 1 つのインターフェイスだけを使用します）。ソフトウェア ライセンス キーにより、インストールされた XG ソフトウェア イメージがアクティブになります。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。

XG ソフトウェア イメージをインストールしても、対応するソフトウェア ライセンスをインストールし、2 Gbps 動作に必要な設定変更を行うまで、Detector モジュールは動作しません。その設定変更として、次の項目があります。

- インターフェイス設定：スーパーバイザ　エンジンで新しいインターフェイスを設定します。
- SSL 証明書：Detector モジュールおよび関連付けられている Guard で新しい SSL 証明書を生成します。

XG ソフトウェア イメージとライセンスをインストールしても、次の Detector モジュールの項目には影響しません。

- ゾーン設定：既存のゾーン設定情報は変わりません。
- 管理アクセス：1 Gbps 動作の場合に mng で設定した設定パラメータは、2 Gbps 動作でも同じです。

この項では、次のトピックについて取り上げます。

- 2 Gbps 動作用 XG ソフトウェア イメージの取得とインストール
- XG ソフトウェア イメージ ライセンス キーの取得とインストール
- 2 Gbps 動作用追加データ ポートのアクティブ化
- 2 Gbps 動作用 SSL 証明書の再生成

2 Gbps 動作用 XG ソフトウェア イメージの取得とインストール

XG ソフトウェア イメージのコピーを取得し、Detector モジュールにソフトウェアをインストールするには、P.13-17 の「AP イメージのアップグレード」を参照してください。

XG ソフトウェア イメージがロードされたことを確認するには、**show version** コマンドを使用します。XG ソフトウェア イメージがロードされると、ソフトウェア バージョン番号の後に XG と表示されます（version 6.0(.0.39)-XG など）。

XG ソフトウェア イメージ ライセンス キーの取得とインストール

XG ソフトウェア イメージをアクティブにするために必要なライセンス キーは、XG ソフトウェア イメージが格納されている Detector モジュールの Media Access Control（MAC; メディア アクセス制御）アドレスと対応付けられます。この項では、XG ソフトウェア ライセンス キーを注文するプロセスについて説明します。

（注） XG バージョン 6.0 オペレーティング ソフトウェア（またはそれ以降）を Detector モジュールにロードした上で、対応するライセンスを注文およびインストールする必要があります。Detector モジュールに現在ロードされているソフトウェアのバージョンを確認するには、**show version** コマンドを使用します。XG ソフトウェア イメージがロードされると、ソフトウェアのバージョン番号に -XG 接尾辞が付きます（version 6.0(0.39)-XG など）。

2 Gbps ライセンスを取得し、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　Detector モジュールから **show license-key unique-identifier** コマンド（このコマンドを使用するには admin 特権レベルが必要）を入力して、Detector モジュールの MAC アドレスを表示します。

ステップ 2　MAC アドレス情報を記録します。この情報は、2 Gbps 動作ライセンスを注文するときに必要です。

ステップ 3　www.cisco.com で利用可能な Cisco Ordering ツールを使用して、lic-adm-2g-k9 ライセンスを注文します。

ステップ 4　Cisco から Software License Claim Certificate を受け取ったら、次の Cisco.com Web サイトにアクセスする手順に従います。

http://www.cisco.com/go/license

ステップ 5　購入証明として Software License Claim Certificate に記載されている製品認可キー（PAK）番号を入力します。

ステップ 6　要求された情報をすべて入力して、ライセンス キーを生成します。

ライセンス キーが生成されると、ライセンス ファイルが添付され、インストール手順が記載されたライセンス キー電子メールを受信します。ライセンス キー電子メールは、今後必要となる場合に備えて、安全な場所に保存します。

ステップ 7　テキスト エディタを使用してライセンス キー ファイルを開き、その内容をデスクトップ コンピュータのクリップボードにコピーします。

ステップ 8　Detector モジュールから、設定モードで **license-key add** コマンドを入力します。キーの入力を求める CLI プロンプトが表示されます。

ステップ 9　デスクトップ コンピュータのクリップボードの（ライセンス キーを含む）内容を貼り付け、**Enter** キーを押します。

ステップ 10　空行を入力して、**Enter** キーを押します。以前にインストールしたライセンスが Detector モジュールに残っている場合には、新しいライセンスをインストールするかどうかを尋ねる確認メッセージが表示されます。

ステップ 11　**y**（yes）を入力します。これで XG ソフトウェア イメージがアクティブになり、2 Gbps 動作の準備は完了です。

ステップ 12　（オプション）**show license-key** コマンドを入力して、キーが適切にロードされ、有効であることを確認します。

2 Gbps 動作用追加データ ポートのアクティブ化

XG ソフトウェア イメージをインストールし、アクティブ化することにより、スーパーバイザ エンジンと Detector モジュール間のデータ トラフィックが、1 つだけではなく 2 つのインターフェイス ポートを介して移動できるようになります。Detector モジュールで 2 Gbps 動作用の追加データ ポートをアクティブ化するには、インターフェイス設定モードで **no shutdown** コマンドを使用します。

詳細については、P.3-11 の「物理インターフェイスの設定」を参照してください。

2 Gbps 動作用 SSL 証明書の再生成

Detector モジュールは、Secure Sockets Layer（SSL）証明書を使用して、関連付けられている Guard サービスと安全な通信チャネルを確立します。1 Gbps ソフトウェア イメージから 2 Gbps ソフトウェア イメージにアップグレードすると、既存の SSL 証明書が Detector モジュールから削除されます。2 Gbps ソフトウェア イメージとライセンスをインストールした後、Detector モジュールおよび関連付けられている Guard が安全な通信チャネルを確立するために使用する SSL 証明書を再生成する必要があります。関連付けられている Guard については、最初に既存の SSL 証明書を削除した後に、新しい証明書を作成できます。

詳細については、P.4-31 の「SSL 証明書の再生成」を参照してください。

MP 関連のコマンドの使用

Detector モジュールを MP にブートできます。Detector モジュールを管理および診断するためのインターフェイスのセットを MP 上で使用できます。MP の主要な特徴の 1 つは、新しい AP イメージをインストールする機能を提供することです。

MP にブートするには、**hw_module module reset** コマンドを入力し、その後 **session slot** コマンドを入力して MP にログインします。

表 13-5 で、MP 関連のコマンドの要点を説明します。

表 13-5　MP 関連のコマンド

コマンド	説明
clear ap password	Detector モジュールで定義した次の情報を消去します。 • すべてのユーザ パスワード • すべての TACACS+ 定義
clear ap config	Detector モジュールをデフォルト設定に戻します。このコマンドは、すべての Detector モジュール設定、ログ、レポート、およびライセンス キー（インストールされている場合）を削除します。
ip address [*ip address*] [*subnet*]	Detector モジュールが外部ネットワークへのアクセスに使用する IP アドレスを設定します。
ip gateway [*default-gateway*]	ネットワークのデフォルト ゲートウェイを指定します。
passwd	現行ユーザのパスワードを変更します。
passwd-guest	ゲスト アカウントのパスワードを変更します。
ping {*host-name* | *ip address*}	ネットワーク上の特定のホストに ping を実行し、ネットワーク パラメータが正しく設定されていることを確認します。
show images	アプリケーション パーティションに格納されているイメージを表示します。

表 13-5　MP 関連のコマンド（続き）

コマンド	説明
show ip	Detector モジュールのネットワーク パラメータを表示します。
upgrade *ftp-url*	イメージをアップグレードします。ここで、ftp-url は、イメージがある FTP サーバとイメージへのパスを指定する URL です。パスの形式は ftp://user:password@server-name/path です。 FTP サーバの名前または IP アドレスを指定できます。

忘失パスワードの復旧

忘失したパスワードを復旧するには、次の手順を実行します。

ステップ 1　スーパーバイザ エンジンで次のコマンドを入力して、Detector モジュールを MP にリセットします。

```
hw-module module slot_number reset cf:1
```

slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 2　Detector モジュールがオンラインに戻ったら、Detector モジュールとのセッションを確立し、ルート アカウントにログインします。

ステップ 3　次のコマンドを入力して、Detector　モジュールに設定されているすべてのパスワードを削除します。

```
clear ap password
```

ステップ 4　次のコマンドを入力して、Detector モジュールを AP にリセットします。

```
hw-module module slot_number reset cf:4
```

ステップ 5　Detector　モジュール上に設定されているユーザの新しいパスワードを設定します（P.4-10 の「自分のパスワードの変更」を参照してください）。Detector モジュールのユーザのリストを表示するには、**show running-config** コマンドを使用します。

ヒント　**show running-config** コマンド出力の表示を絞り込んで、Detector モジュール ユーザのリストだけが含まれるようにするには、**show running-config | include username** コマンドを使用してください。

工場出荷時のデフォルト設定へのリセット

状況によっては、Detector モジュールの設定を、工場出荷時のデフォルト設定に戻す必要が生じる場合があります。工場出荷時のデフォルト設定へのリセットは、設定が複雑になった場合や、Detector モジュールをあるネットワークから別のネットワークに移動させる場合に、Detector モジュールに存在する不要な設定を削除するときに役立ちます。Detector モジュールを工場出荷時のデフォルト設定にリセットして、新しい Detector モジュールとして設定できます。

工場出荷時のデフォルト設定にリセットする前に、**copy running-config** コマンドを使用して、Detector モジュールの設定をバックアップする必要があります。P.13-4 の「設定のエクスポート」を参照してください。

管理インターフェイス設定（eth1）は、Detector モジュールをリロードするまで使用可能です。

注意　アウトオブバンド コンソール接続を使用して（利用可能な場合）、clear config all コマンドを実行します。Detector モジュールが clear config コマンドを実行すると設定がクリアされ、ユーザがリブート要求を確認するとリブートします。インライン SSH 接続を使用して clear config all コマンドを実行すると、clear config プロセスの途中で接続が解除され、Detector モジュールがリブートしません。スーパーバイザ エンジンに接続し、手動で Detector モジュールをリブートする必要があります。

Detector モジュールを工場出荷時のデフォルト設定にリセットするには、設定モードで次のコマンドを使用します。

clear config all

設定した変更内容は、リセットをした後に有効になります。

次の例は、Detector モジュールを工場出荷時のデフォルト設定にリセットする方法を示しています。

```
user@DETECTOR-conf# clear config all
```

INDEX

Symbols

#（ナンバー記号）　11-6
*（ワイルドカード）　3-9, 5-9, 11-6

Numerics

1 Gbps および 2 Gbps 帯域幅オプション
　2 Gbps へのアップグレード　13-30
　説明　1-9
　ソフトウェア バージョンの表示　12-3
　ソフトウェア ライセンス キーの表示　12-4
2 Gbps 動作のアップグレード
　SSL 証明書の再生成　13-33
　追加データ ポートのアクティブ化　13-33

A

AAA
　アカウンティング　4-20
　設定　4-5
　認可　4-16
　認証　4-7
aaa accounting コマンド　4-20
aaa authentication コマンド　4-7
aaa authorization コマンド　4-16
action コマンド　7-31
add-service コマンド　7-16
admin 特権レベル　3-2, 4-9
always-accept　7-33
always-ignore　7-33
AP
　アップグレード　13-17
　アップグレード、インライン　13-24
　設定の消去　13-34
　パスワードの消去　13-34, 13-36
　～へのブート　2-19
auth パケット タイプ　7-18

B

boot コマンド　2-19

C

CFE　13-19, 13-26, 13-28
clear ap config コマンド　13-34
clear ap password コマンド　13-34, 13-36
clear counters コマンド　3-13, 12-10
clear log コマンド　12-18
CLI
　エラー メッセージ　3-7
　コマンドのショートカット　3-9

コマンドの発行 3-5
使用 3-2
タブ補完 3-8
プロンプトの変更 4-42
ヘルプの取得 3-8
config 特権レベル 3-2, 4-9
copy guard-running-config コマンド 5-25, 5-28
copy login-banner コマンド 4-52
copy wbm-logo コマンド 4-54
copy コマンド
ftp running-config 13-7
packet-dump 12-27
running-config 5-26, 13-4
ゾーンのログ 12-16
レポート 11-12
ログ 12-13, 12-16
copy-from-this 5-9
copy-policies コマンド 8-28
CPU 使用率 12-42

D

DDoS
概要 1-3
deactivate コマンド 8-11, 9-7
default-gateway コマンド 3-14
description コマンド 5-11
detect learning コマンド 8-10
detect コマンド 9-7
DETECTOR_DEFAULT 5-3
DETECTOR_WORM 5-3
diff コマンド 8-25, 8-26
disable コマンド 7-12
Distributed Denial of Service
「DDoS」を参照
DNS
TCP プロトコル フロー 11-8
TCP ポリシー テンプレート 7-5
検出された異常 11-3
dst トラフィック特性 7-19
dst-ip-by-ip アクティベーション形態 9-5, 9-11
dst-ip-by-name アクティベーション形態 9-5
dynamic 特権レベル 3-2, 4-9

E

enable
password コマンド 4-14
コマンド 4-15, 7-12
entire-zone アクティベーション形態 9-5
event monitor コマンド 12-13
export sync-config コマンド 5-27
export コマンド 13-10
packet-dump 12-26, 12-27
reports 11-11

F

file-server
コマンド 5-27, 13-2
設定 13-2
sync-config の表示 5-28, 13-12
削除 13-3
表示 13-3, 13-13

fixed-threshold 7-26
flash-burn コマンド 13-28
fragments 11-8
検出された異常 11-3
ポリシー テンプレート 7-5

G

global トラフィック特性 7-20
Guard
設定のエクスポート 13-10
設定モード 3-4
GUARD 設定、インポート 5-26
GUARD 設定、エクスポート 5-25, 5-28
GUARD_ ゾーン テンプレート
ゾーン テンプレートに含まれるポリシー テンプレート 7-7
Guard 保護のアクティベーション方式 9-5
guard-conf コマンド 5-17
GUARD_DEFAULT 5-4
GUARD_LINK 5-4, 5-5
GUARD_TCP_NO_PROXY 5-5

H

histogram コマンド 7-35
hostname
コマンド 4-42
変更 4-42
HTTP
検出された異常 11-3
ポリシー テンプレート 7-5
hw-module コマンド 2-17, 13-18, 13-19, 13-21, 13-25, 13-36

I

in パケット タイプ 7-18
Interactive
動作モード 10-6
ポリシーのステータス 7-33
interactive-status コマンド 7-33
ip address コマンド
インターフェイス 3-12
削除 5-14
除外 5-13
ゾーン 5-13
ip route コマンド 3-15
IP アドレス
変更、ゾーン 5-14
IP しきい値設定 7-29
IP スキャン 11-8
検出された異常 11-3
ポリシー テンプレート 7-6

K

key publish コマンド 4-34, 4-35
key コマンド
add 4-34, 4-38
generate 4-35, 4-40
remove 4-39

L

learning
  policy-construction コマンド 8-7
  threshold-tuning コマンド 8-10, 8-11
  コマンド 8-8, 8-13
learning accept コマンド 8-8, 8-12
learning-params
  periodic-action コマンド 5-20, 8-8, 8-12, 8-16
  periodic-action コマンドの無効化 8-8
  threshold-multiplier コマンド 7-27
  threshold-selection コマンド 8-12, 8-17
  threshold-tuned コマンド 5-14, 8-19
  定期的なアクションの非アクティブ化 8-12
learning-params fixed-threshold コマンド 7-26
learning-params コマンド 5-19, 5-28
LINK テンプレート 8-6
logging コマンド 12-14
login-banner コマンド 4-51

M

max-services コマンド 7-11
MDM
  アクティブ化 3-19
min-threshold コマンド 7-11
MP
  アップグレード 13-21
  アップグレード、インライン 13-24
  ～へのブート 2-19
mtu コマンド 3-12

N

netstat コマンド 12-47
no learning コマンド 8-8, 8-13
non_estb_conns パケット タイプ 7-19
notify 11-6
notify ポリシー アクション 7-32
ns ポリシー テンプレート 7-8

O

out_pkts パケット タイプ 7-19

P

packet-dump
  auto-capture コマンド 12-22
  エクスポート 12-26, 12-27, 13-10
  シグニチャ 12-34
  自動
    アクティブ化 12-20
    非アクティブ化 12-23
  設定の表示 12-23
packet-dump コマンド 12-23
permit
  コマンド 3-17, 3-20, 4-3
permit ssh コマンド 4-33
ping コマンド 12-53
pkts パケット タイプ 7-19
policy set-timeout コマンド 7-31
policy-template add-service コマンド 7-16
policy-template remove service コマンド 7-17
policy-type アクティベーション形態 9-6

power enable コマンド 2-18
protect コマンド 9-7
protection-end-timer 9-11, 9-14
protect-ip-state コマンド 9-6
protocol トラフィック特性 7-20

R

reactivate-zones 13-13
reload コマンド 13-13
remote-activate ポリシー アクション 7-32
remote-guard コマンド 9-12, 9-13
remove service コマンド 7-16
reqs パケット タイプ 7-19
reset コマンド 2-18
running-config
  copy 5-26, 13-4, 13-7
  show 12-5

S

scanners トラフィック特性 7-20
service
  MDM 3-19
  snmp-trap 4-43
  WBM 3-17
  コマンド 3-17, 3-19, 4-3
session-timeout コマンド 4-56
set-action 7-32
show public-key コマンド 4-41
show コマンド
  cpu 12-42
  diagnostic-info 12-39
  dynamic-filters 6-22
  file-server 13-3, 13-13
  host-keys 4-33, 4-37
  learning-params 7-26
  log export-ip 12-15
  login-banner 4-51
  memory 12-41
  packet-dump 12-23
  packet-dump signatures 12-34
  public-key 4-37, 4-40
  recommendations pending-filters 10-5, 10-9
  remote-guards 9-12, 9-13
  running-config 12-5
  show 12-7
  sync-config 5-28
  sync-config file-servers 5-28, 13-12, 13-13
  カウンタ 12-8
  推奨事項 10-7, 10-8
  ゾーンのポリシー 7-39
  テンプレート 5-9
  動的フィルタのソート 6-22
  フレックスコンテンツ フィルタ 6-14
  ポリシー 7-39
  ポリシーの統計情報 7-41, 8-14
  モジュール 2-3, 13-18, 13-21, 13-22
  ラーニング パラメータ 8-15
  レート 12-8
  レポートの詳細 11-7
  ロギング 12-15
  ログ 12-16
show 特権レベル 3-2, 4-9

shutdown コマンド　3-12
snapshot コマンド　8-22
SNMP
　トラップ ジェネレータの設定　4-43
　トラップの説明　4-45
snmp コマンド
　community　4-50
　trap-dest　4-43
SPAN、設定　2-12
src トラフィック特性　7-20
SSH
　鍵の削除　4-39
　鍵の生成　4-35, 4-40
　公開鍵の表示　4-37
　サービス　3-20
　設定　3-20
　ホスト鍵　4-36
ssh 鍵、パブリッシュ　4-35
state コマンド　7-23
syn_by_fin パケット タイプ　7-19
sync コマンド　5-22, 5-23
syns パケット タイプ　7-19
syslog
　エクスポート パラメータの設定　12-14
　サーバの設定　12-15
　メッセージの形式　12-14

T

TACACS+
　サーバの IP アドレス　4-24
　サーバの暗号鍵　4-24
　サーバの接続タイムアウト　4-26
　サーバの設定　4-22
　統計情報のクリア　4-27
　統計情報の表示　4-27
　認証
　　key generate コマンド　4-29
　　key publish コマンド　4-34
tacacs-server コマンド
　clear statistics　4-27
　first-hit　4-22
　host　4-22, 4-24
　key　4-22, 4-24, 4-25
　show statistics　4-27
　timeout　4-22, 4-26
TCP
　検出された異常　11-3, 11-8
　プロキシが使用されない場合のポリシー テンプレート　7-8
　ポリシー テンプレート　7-6
thresh-mult　7-28
threshold
　コマンド　7-25
threshold-list コマンド　7-29
threshold-selection　8-12
timeout コマンド　7-30
traceroute コマンド　12-51
trap-dest　4-43

U

UDP
　検出された異常　11-4
　ポリシー テンプレート　7-7

unauth_pkts パケット タイプ　7-19
upgrade コマンド　13-35
username コマンド　4-9

V

VACL、設定　2-7

W

WBM
　アクティブ化　3-17
WBM ロゴ
　削除　4-55
　追加　4-54
worm_tcp ポリシー テンプレート　7-9

X

XG ソフトウェア イメージ、2 Gbps 動作
　ソフトウェア イメージの取得　13-31
XG ソフトウェア バージョン、2 Gbps 動作　13-30
XG ソフトウェア ライセンス キー　13-31
XML スキーマ　11-11 - 11-14, 12-26, 13-11

Z

zone
　コマンド　5-7, 5-9
　コマンド補完　4-19, 5-11

あ

アイドル セッション、タイムアウトの設定　4-56
アイドル セッション、タイムアウトの表示　4-56
アカウンティング、設定　4-20
アクション フロー　11-10
アップグレード
　AP　13-17
　MP　13-21
　インライン　13-24
アップグレード ライセンス　13-31
アプリケーション パーティション
　「AP」を参照

い

異常
　検出された　11-3
　フロー　11-5
異常検出エンジンのメモリ使用率　12-41, 12-44
イネーブル化、サービスの　4-3
イベント ログ
　アクティブ化　12-13
　非アクティブ化　12-13
インターフェイス
　IP アドレスの設定　3-12
　アクティブ化　3-11, 3-12
　カウンタのクリア　3-13
　コマンド　3-11
　設定モード　3-3
インタラクティブ検出モード　1-7, 9-4
インタラクティブ保護モード　9-4

インポート
設定 13-7
インポート、GUARD 設定の 5-26
インライン アップグレード 13-24

え

エクスポート
自動でのディセーブル化 13-12
設定ファイル 13-4
レポートを自動的に 11-11
ログ ファイル 12-16
エクスポート、GUARD 設定の 5-25, 5-28

か

カウンタ
クリア 3-13, 12-10
履歴 12-8
カウンタ、表示 12-8
監視
ネットワーク トラフィック 12-26, 12-27
管理
MDM 3-19
SSH 3-20
VLAN 2-5
WBM 3-17
概要 3-17
ポート 2-5

き

キー
生成、ライセンス用 13-31
キャプチャ、パケット 12-23

く

グローバル モード 3-3

け

検出
インタラクティブ モード 1-7, 9-4
自動モード 1-7, 9-4
検出された
異常 11-3
フロー 11-10
検出された攻撃 11-8
検出レベル
分析 7-18

こ

公開鍵
表示 4-40
攻撃のタイプ
検出された攻撃 11-8
攻撃レポート
エクスポート 11-11, 13-10
エクスポート、自動的に 11-11
検出された異常 11-3
コピー 11-12

タイミング 11-2
通知 11-6
統計情報 11-3
表示 11-7
レイアウト 11-2
コマンドのショートカット 3-9
コマンドの無効化
コマンド、無効化 3-7
コマンド補完 4-19
コマンドライン インターフェイス
「CLI」を参照 3-2

さ

サービス
アクセス権 4-3
イネーブル化 4-3
コピー 8-28
削除 7-16
追加 7-15

し

しきい値
IP しきい値の設定 7-29
受け入れ前の乗算 7-27
固定値として設定 7-25
選択 8-23
調整 1-6, 8-3
調整済みのマーク付け 5-14, 8-19
特定の IP の設定 7-29
リストの設定 7-29
ワーム 7-34
しきい値の調整
結果を定期的に保存 8-15
シグニチャ
生成 12-33
システム ログ
メッセージの形式 12-14
自動検出モード 1-7, 9-4
自動保護モード 9-4

す

推奨事項
アクティブ化 10-6, 10-10
受け入れ 10-11
概要 10-2
決定の変更 7-33
コマンド 10-10
通知の受信 10-2
非アクティブ化 10-6, 10-13
表示 10-2, 10-7
保留フィルタの表示 10-5, 10-9
無視 10-11
スーパーバイザ エンジン
シャットダウン 2-17
設定 2-1
設定の確認 2-20
設定の保存 2-1
電源の切断 2-18
ブート 2-19
リセット 2-18

スタティック ルート
追加 3-15
スナップショット
コマンド 8-23
削除 8-28
定期的に保存 8-15
比較 8-25
表示 8-26
保存 8-23, 8-24
ポリシーのバックアップ 7-44, 8-24, 8-30

せ

生成、シグニチャの 12-33
セッション、アイドル タイムアウトの表示 4-56
セッション タイムアウト、ディセーブル化 4-56
セッション、タイムアウトの設定 4-56
設置
確認 2-3
設定
インポート 13-7
スーパーバイザ エンジンの保存 2-1
ファイル
インポート 13-7
エクスポート 13-4
コピー 13-4
表示 12-5
設定、コマンド モードへのアクセス 4-18
設定コマンド 3-10
設定モード 3-3

そ

ゾーン
IP アドレス 5-13
IP アドレスの削除 5-14
IP アドレスの除外 5-13
IP アドレスの定義 5-13
IP アドレスの変更 5-14
LINK テンプレート 8-6
オフラインでの同期 5-24
カウンタのクリア 12-10
検出 9-2
コピー 5-9
コマンド 10-6
再設定 5-11
削除 5-9
作成 5-7
自動的な同期 5-19
ステータスの表示 12-7
設定のエクスポート 5-27
設定の同期 5-15
設定の表示 5-12
設定モード 3-4, 5-11
テンプレート 5-3
動作モード 5-8
比較 8-26
複製 5-9
ポリシーの表示 7-39
ラーニング 8-2
ゾーンのポリシー
調整済みのマーク付け 5-14, 8-19
ソフトウェア バージョン番号、表示 12-3

ソフトウェア ライセンス キー
キー情報の表示 12-4

た

帯域幅オプション
2 Gbps へのアップグレード 13-30
説明 1-9
ソフトウェア バージョンの表示 12-3
ソフトウェア ライセンス キーの表示 12-4
タイムアウト セッション、設定 4-56
タイムアウト セッション、ディセーブル化 4-56

ち

注意
記号の概要 xxi
注釈
記号の概要 xxii
抽出、シグニチャの 12-33

て

定期的なアクション
非アクティブ化 8-8, 8-12
ポリシーの自動受け入れ 8-8, 8-12
ディセーブル化
自動エクスポート 13-12
デフォルト設定、～に戻す 13-34
テンプレート
LINK 8-6
ゾーン 5-3
ポリシーの表示 5-9

と

同期
設定のエクスポート 13-10
動的フィルタ
1000 以上 6-23
イベントの表示 12-15
概要 6-2, 6-22
コマンド 6-26, 6-27, 9-14
削除 6-27
ソート 6-22
定義 1-8
～の作成の防止 6-28
表示 6-22
ワーム 7-37
特定の IP しきい値 7-29
特権レベル 3-2
～の間の移動 4-15
パスワードの割り当て 4-14
トラップ 12-14
トラフィック
監視 12-26, 12-27
トラフィックの送信元
SPAN 2-6
VACL 2-6
キャプチャ 2-6
設定 2-6

に

認可
zone コマンド補完のディセーブル化 4-19, 5-11

認可、設定　4-12, 4-14
認証、設定　4-7
認証されていない TCP の検出された異常　11-4

ね

ネットワーク サーバ
　sync-config の表示　5-28, 13-12
　削除　13-3
　設定　13-2
　表示　13-3, 13-13
ネットワーク サーバ、sync-config の表示　13-13

は

バークリー パケット フィルタ　6-12
バージョン、アップグレード　13-35
バイパス フィルタ
　コマンド　6-18
　削除　6-21
　設定　6-18
　定義　1-8, 6-2
　表示　6-20
ハイブリッド　11-8
パケット、キャプチャ　12-23
パスワード
　暗号化された　4-10
　イネーブル化　4-14
　復旧　13-34, 13-36
　変更　4-10
パスワード、復旧　13-36
バナー
　ログインの設定　4-51
番号の割り当て直し、フレックスコンテンツ フィルタの　6-5

ひ

ヒント
　記号の概要　xxii

ふ

ファイル サーバ
　設定　13-2
ファイル サーバ、sync-config の表示　13-13
ファシリティ　12-14
フィルタ
　動的　1-8, 6-2, 6-22
　バイパス　1-8, 6-18
　フレックスコンテンツ　1-8, 6-4
フラッシュの焼き付け　13-28
フレックスコンテンツ フィルタ
　設定　6-5
　定義　1-8, 6-2
　番号の割り当て直し　6-5
　表示　6-14
　フィルタリング基準　6-4
プロキシ
　プロキシが使用されない場合のポリシー テンプレート　7-8
プロキシが使用されない場合のポリシー テンプレート　7-8
分析検出レベル　7-18

ほ

ポート スキャン　11-8
　検出された異常　11-3
　ポリシー テンプレート　7-6
他のプロトコル
　検出された異常　11-3
　ポリシー テンプレート　7-6
保護
　アクティベーション方式　9-5
　非アクティブ化　9-7
ホスト、ロギング　12-15
ホスト鍵
　削除　4-32, 4-33
ポリシー
　copy-policies　8-28
　learning-params fixed-threshold コマンド　7-26
　threshold　7-25
　threshold-list コマンド　7-29
　アクション　7-21, 7-31, 7-32
　アクティブ化　7-22
　現在の～のバックアップ　7-44, 8-24, 8-30
　構造　7-2
　構築　1-6, 7-4, 8-3, 8-6
　コマンド　7-21
　サービスの削除　7-16
　サービスの追加　7-15
　しきい値　7-4, 7-21
　しきい値の乗算　7-28
　しきい値の調整　1-6, 7-4, 8-3, 8-10
　しきい値を固定　7-26
　状態　7-22
　設定モード　3-4
　タイムアウト　7-21, 7-30
　調整済みのマーク付け　5-14, 8-19
　ディセーブル化　7-22
　統計情報の表示　7-41, 8-14
　トラフィック特性　7-19
　ナビゲーション パス　7-21
　パケット タイプ　7-18
　パラメータのコピー　8-28
　非アクティブ化　7-22
　ワイルドカードの使用　7-22, 7-39, 7-42
ポリシー テンプレート
　max-services　7-11
　min-threshold　7-11
　worm_tcp　7-9
　概要　7-5, 7-14
　コマンド　7-8, 7-9, 7-12
　状態　7-12
　設定コマンド レベル　7-9
　設定モード　3-4
　同期化のための Guard ポリシー テンプレート　7-7
　パラメータ　7-9
　リストの表示　7-8
ポリシーの構築　8-6
ポリシーのしきい値の調整　8-10
保留動的フィルタ　10-2
　表示　10-5, 10-9

め

メモリ消費量　12-41
メモリ使用率、異常検出エンジン　12-41, 12-44

メンテナンス パーティション
「MP」を参照

ゆ

ユーザ
username コマンド 4-9
新しい～の追加 4-9
検出された異常 11-4
削除 4-12
システム ユーザ
Admin 2-16
riverhead 2-16
追加 4-9
特権レベル 3-2, 4-14
特権レベルの割り当て 4-8
ユーザ フィルタ
コマンド 6-5
ユーザ名
暗号化されたパスワード 4-10

ら

ラーニング
概要 8-2
結果の同期 8-5
しきい値の調整 8-10
プロセスの終了 8-8, 8-13
ポリシーの構築 8-6
ラーニング パラメータ、表示 8-15
ライセンス
XG アップグレード ライセンスの注文 13-31
キーの生成 13-31

り

リブート
パラメータ 13-13
リモート Guard
アクティブ化 6-25, 9-8
デフォルト リスト 9-12
保護の終了 9-11, 9-14
リスト 9-13
リストのアクティベーション順序 9-13
リモート Guard リスト
表示 9-12, 9-13

る

ルータ設定モード 3-4
ルーティング テーブル
操作 3-15
表示 3-16

れ

レート
履歴 12-8
レート、表示 12-8
レポート
「攻撃レポート」を参照 11-2
エクスポート 13-10
詳細 11-7

ろ

ロギング、設定の表示　12-15
ログ ファイル
　エクスポート　12-13, 12-16
　クリア　12-18
　表示　12-16
ログイン バナー
　インポート　4-52
　削除　4-53
　設定　4-51
ロゴ、WBM の削除　4-55
ロゴ、WBM の追加　4-54

わ

ワーム
　概要　7-34
　攻撃の識別　7-37
　しきい値　7-34, 7-35
　動的フィルタ　7-37
　ポリシー　7-19, 7-20
　ポリシー テンプレート　7-7, 7-35
ワンポイント アドバイス
　記号の概要　xxii