このマニュアルについて

このマニュアルでは、Cisco Traffic Anomaly Detector モジュール（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います。

対象読者

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

- 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。

このマニュアルの使用方法

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」	Detector モジュールの概要を示し、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説明します。
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示します。また、Detector モジュールの CLI 環境および認証方法を説明します。
第 4 章「Detector モジュールの設定」	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 トラフィック異常の検出」	ゾーン トラフィックの異常を検出し、Cisco Anomaly Guard モジュール 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。
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。

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、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここには、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html