



このマニュアルについて

このマニュアルでは、Cisco Anomaly Guard Module (Guard 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](#)
- [このマニュアルの使用方法](#)
- [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 Anomaly Guard 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」	Cisco Anomaly Guard Module (Guard モジュール) の概要を説明し、Guard 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 エンジンへの Guard 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 Guard モジュールを設定する方法について説明します。
第 3 章「Guard モジュールの初期化」	Guard 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、Guard 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「Guard モジュールの設定」	Guard 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「トラフィックの宛先変更の設定」	ゾーンのトラフィックの宛先変更プロセスおよび宛先変更を設定する方法について説明します。
第 6 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 7 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 8 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 9 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 Guard モジュールがゾーン保護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 10 章「ゾーンの保護」	ゾーン保護を設定し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 11 章「インタラクティブ保護モードの使用方法」	インタラクティブ保護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 12 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 13 章「Guard モジュールの診断ツールの使用」	Guard モジュールの診断ツールについて説明します。
第 14 章「メンテナンス タスクの実行」	Guard 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。
第 15 章「Guard モジュールによる軽減の分析」	ゾーンのトラフィック パターンを分析する方法について説明し、設定上の問題を特定します。また、攻撃のタイプを特定する方法と、分析に基づいた推奨アクションを簡単に示します。

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 Guard 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@GUARD-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。

■ 記号および表記法



(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、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わせは、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わせください。

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、緊急でないと思なされます。
- 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 に問い合わせ、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、プロフィールを作成して、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 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、代理店にお問い合わせください。

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 に電話でお問い合わせください (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。

シビルティ 4 (S4) : シスコ製品の機能、インストール、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。プロフィールを作成し、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>