



このマニュアルについて

このマニュアルでは、Cisco Guard (Guard) について説明します。具体的には、管理作業の実行方法、Guard の運用に必要となる一般的な操作の方法、および Guard の使用方法を示します。

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。

この章には、次の項があります。

- [対象読者](#)
- [マニュアルの構成](#)
- [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](#)
- [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 Guard ユーザガイド』は、次の方を対象としています。

- 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。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
第 1 章「概要」	Cisco Guard (Guard) の概要を示し、Guard の動作モードおよびコンポーネントについて概説します。
第 2 章「Guard の初期化」	Guard を接続し、設定するために必要な最初の手順について情報を提供します。また、Guard の CLI 環境および認証方法を概説します。
第 3 章「Guard の設定」	Guard のインターフェイス設定およびデフォルトのリモート Guard リストについて情報を提供します。また、SSH 管理およびアクティベーション設定の手順を示します。
第 4 章「ゾーン トラフィックの宛先変更」	ゾーンのトラフィックの宛先変更プロセスについて情報を提供し、宛先変更を設定する方法を説明します。
第 5 章「ゾーンの設定」	ゾーンを作成し、管理する方法について説明します。

章	説明
第 6 章「ゾーンのフィルタの設定」	Guard のフィルタについて情報を提供し、Guard に対してゾーンの高度な設定作業を実行する方法を説明します。
第 7 章「ポリシー テンプレートとポリシーの設定」	Guard のポリシーおよびポリシー テンプレートについて情報を提供し、これらを設定する方法を説明します。
第 8 章「インタラクティブ推奨モード」	インタラクティブ推奨動作モードについて情報を提供します。また、Guard の推奨事項、ユーザの決定に関するオプション、および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 9 章「攻撃レポート」	Guard の攻撃レポート、レポートの構成、およびオプションの表示について情報を提供します。
第 10 章「Guard の診断とメンテナンス」	Guard の診断およびメンテナンス操作に関連するコマンドについて情報を提供します。
第 11 章「Guard 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情報を提供し、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。
付録 A「宛先変更の設定」	宛先変更の手順に関する追加情報を、サンプル コードを示しながら説明します。
付録 B「宛先変更のトラブルシューティング」	宛先変更のトラブルシューティング手順について、サンプル画面を示しながら説明します。

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	太字のテキストを記載されているとおりに入力します。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変数を示します。
標準スタイルのテキスト	プロンプトなどの画面表示を表します。標準スタイルのテキストをコマンドの一部として入力しないでください。
[x]	角カッコの中のキーワードは、省略可能です。
[x y]	角カッコの中のキーワードが縦棒で区切られている場合は、省略可能なキーワードを複数の値の中から1つ選択することを示します。
{x y z}	必須キーワードの選択肢は、波カッコで囲まれ、縦棒で区切られています。必ず1つ選択する必要があります。
[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 *admin@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

注意は、ユーザによる特定の操作が、データ損失または機器への悪影響につながる可能性があることを意味します。



警告

警告は、人身事故または機器の損傷につながる可能性のある操作を表します。



(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、情報として役立つことができます。



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。また、テクニカル サポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法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/univercd/home/home.htm>

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>

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

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>

Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Documentation DVD パッケージでご利用いただけます。Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。また、この Documentation DVD パッケージのみを発注することもできます。

Cisco.com 登録ユーザ (Cisco Direct Customers) の場合、Ordering Tool または Cisco Marketplace から Cisco Documentation DVD (Product Number DOC-DOCDVD=) を発注できます。

Cisco Ordering Tool :

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace :

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

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering Tool 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/en/US/partner/ordering/>

- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

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および注意事項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>

勧告および注意事項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) フィードにアクセスしてください。

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）
- 緊急でない場合 : psirt@cisco.com（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 8.x と互換性のある暗号化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キーは、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キーは、次の公開キー サーバのリストで作成日が最新のキーです。

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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)

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。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、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 Technical Support Web サイト

Cisco Technical 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 365 日、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/techsupport>

Cisco Technical 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)

Web 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 (CPI) ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI 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。

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、Cisco TAC 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、Cisco TAC 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 Marketplace では、シスコの書籍やリファレンス ガイド、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>

- 『Packet』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

日本語版『Packet』は、米国版『Packet』と日本版のオリジナル記事で構成されています。日本語版『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/japanese/warp/public/3/jp/news/packet/>

- 『iQ Magazine』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、事例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『iQ Magazine』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

- 『*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>