



このマニュアルについて

ここでは、このマニュアルの目的、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。

次のトピックについて取り上げます。

- [目的 \(P.xii\)](#)
- [対象読者 \(P.xii\)](#)
- [マニュアルの構成 \(P.xiii\)](#)
- [関連マニュアル \(P.xiv\)](#)
- [表記法 \(P.xiv\)](#)
- [技術情報の入手方法 \(P.xv\)](#)
- [シスコ製品のセキュリティの概要 \(P.xvi\)](#)
- [テクニカルサポート \(P.xviii\)](#)
- [その他の資料および情報の入手方法 \(P.xx\)](#)

目的

『Cisco CallManager セキュリティ ガイド』は、システム管理者および電話機管理者が次の作業を実行する際に役立ちます。

- 認証を設定する。
- 暗号化を設定する。
- ダイジェスト認証を設定する。
- HTTPS に関連付けられているサーバ認証証明書をインストールする。
- セキュリティ プロファイルを設定する。
- サポートされている Cisco IP Phone モデルのローカルで有効な証明書をインストール、アップグレード、または削除できるように Certificate Authority Proxy Function (CAPF) を設定する。
- 電話機のセキュリティを強化する。
- Survivable Remote Site Telephony (SRST) リファレンスについてセキュリティを設定する。
- ゲートウェイおよびトランクについてセキュリティを設定する。
- 問題をトラブルシューティングする。

対象読者

このマニュアルで説明しているリファレンスおよび手順のガイドは、セキュリティ機能の設定を担当するシステム管理者および電話機管理者を対象としています。

マニュアルの構成

表 1 は、このマニュアルの構成を示しています。

表 1 このマニュアルの構成

章番号	説明
セキュリティの基礎	
第 1 章「セキュリティの概要」	セキュリティの用語、システム要件、相互対話と制限、インストール要件、および設定用チェックリストの概要を説明します。また、さまざまなタイプの認証と暗号化についても説明します。
第 2 章「HTTP over SSL (HTTPS) の使用方法」	HTTPS の概要を説明します。また、信頼できるフォルダにサーバ認証証明書をインストールする方法も説明します。
第 3 章「Cisco CTL クライアントの設定」	Cisco CTL クライアントをインストールおよび設定することにより認証を設定する方法を説明します。
電話機およびボイスメール ポートのセキュリティ	
第 4 章「電話機のセキュリティの概要」	Cisco CallManager および電話機でのセキュリティの使用方法について説明し、電話機でセキュリティを設定するために実行するタスクのリストを示します。
第 5 章「電話機セキュリティ プロファイルの設定」	Cisco CallManager Administration でセキュリティ プロファイルを設定し、電話機に適用する方法を説明します。
第 6 章「Certificate Authority Proxy Function の使用方法」	Certificate Authority Proxy Function の概要を説明します。また、サポートされている電話機のローカルで有効な証明書をインストール、アップグレード、削除、またはトラブルシューティングする方法も説明します。
第 7 章「暗号化された電話機設定ファイルの設定」	暗号化された電話機設定ファイルを Cisco CallManager Administration で設定する方法を説明します。
第 8 章「SIP 電話機のダイジェスト認証の設定」	Cisco CallManager Administration を使用してダイジェスト認証を SIP 電話機に設定する方法を説明します。
第 9 章「電話機のセキュリティ強化」	Cisco CallManager Administration を使用して電話機のセキュリティを強化する方法を説明します。
第 10 章「ボイス メッセージング ポートのセキュリティ設定」	Cisco CallManager Administration でボイスメール ポートのセキュリティを設定する方法を説明します。
CTI、JTAPI、および TAPI のセキュリティ	
第 11 章「CTI、JTAPI、および TAPI の認証および暗号化の設定」	Cisco CallManager Administration でアプリケーション ユーザ CAPF プロファイルおよびエンドユーザ CAPF プロファイルを設定する方法を説明します。
SRST リファレンス、ゲートウェイ、およびトランクのセキュリティ	
第 12 章「Survivable Remote Site Telephony (SRST) リファレンスのセキュリティ設定」	Cisco CallManager Administration で SRST リファレンスについてセキュリティを設定する方法を説明します。
第 13 章「ゲートウェイおよびトランクの暗号化の設定」	Cisco CallManager がセキュアなゲートウェイまたはトランクと通信する方法、および IPSec に関する推奨事項と考慮事項について説明します。

表 1 このマニュアルの構成（続き）

章番号	説明
第 14 章「SIP トランク セキュリティ プロファイルの設定」	Cisco CallManager Administration で SIP トランクのセキュリティ プロファイルを設定し、適用する方法を説明します。
第 15 章「SIP トランクのダイジェスト認証の設定」	Cisco CallManager Administration でダイジェスト認証を SIP トランクに設定する方法を説明します。
セキュリティのトラブルシューティング	
第 16 章「トラブルシューティング」	セキュリティ関連の操作および問題について、一般的なガイドラインを示します。

関連マニュアル

Cisco IP テレフォニー関連のアプリケーションと製品の詳細は、次の資料を参照してください。

- *Cisco IP Phone アドミニストレーションガイド for Cisco CallManager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- SRST 対応ゲートウェイをサポートしている Cisco Survivable Remote Site Telephony (SRST) の管理マニュアル
- ご使用の電話機モデルをサポートしているファームウェア リリース ノート

表記法

(注) は、次のように表しています。



(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。

ヒントは、次のように表しています。



ヒント

便利なヒントです。

注意は、次のように表しています。



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。

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/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>

シスコの Web サイトの各国語版には、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>

Product 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 Product Documentation DVD パッケージでご利用いただけます。Product 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。

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、包括的なライブラリです。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複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

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

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

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザーの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

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

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

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品に適用される米国の法律の概要については、

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html> で参照できます。何かご不明な点があれば、export@cisco.com まで電子メールを送信してください。

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。

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 & Documentation 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 Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation 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/techsupport>

Cisco Technical Support & Documentation 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 & Documentation 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、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。

シビラティ 4 (S4) : シスコ製品の機能、インストラクション、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、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書籍を広範囲にわたって出版しています。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 の最新の出版情報やその他の情報を調べるには、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>

デジタル版には、次の URL からアクセスできます。

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- 『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>

- シスコシステムズが提供するネットワーク製品、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、ネットワーク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ク担当者やシスコの専門家や他のネットワーク担当者とは共有できます。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>

- 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>