クイック スタート ガイド

Cisco M170 コンテンツ セキュリティ管理アプライアンス

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

改訂日：2013 年 3 月 13 日
Part Number：78-19644-04-J

1 ようこそ

Cisco M170 コンテンツ セキュリティ管理アプライアンス（Cisco M170）をお選びいただき、ありがとうございます。

コンテンツ セキュリティ管理アプライアンスは、重要なポリシーとランタイム データを集中化し、統合することで、電子メールと Web セキュリティ システムを管理するための単一のインターフェイスを管理者およびエンドユーザに提供します。また、展開の柔軟性を高めることで、Cisco C シリーズおよび S シリーズ アプライアンスから最上のパフォーマンスを確保し、企業ネットワークの整合性を保護します。

コンテンツ セキュリティ管理アプライアンスは、Cisco 電子メールおよび Web セキュリティ アプライアンスに関するすべてのレポーティング情報と監査情報を管理するための中央プラットフォームを提供します。オプションの管理機能を利用することで、1 つのコンテンツ セキュリティ管理アプライアンスからすべてのセキュリティ操作を調整したり、複数のアプライアンスに負荷を分散させたりすることができます。

このマニュアルでは、Cisco M170 アプライアンスの物理的な設置、およびシステム セットアップ ウィザードを使用した基本設定の方法について説明します。

2 はじめる前に

設置を開始する前に、必要な品目が揃っていることを確認してください。

Cisco M170 コンテンツ セキュリティ管理アプライアンスには、次の品目が含まれています。

- クイック スタート ガイド（本書）
- レールおよびアダプタ キット
- 電源ケーブル
- アプライアンスをネットワークに接続するためのイーサネット ケーブル
- 安全規制および規制への準拠に関する情報

次の品目は各自で用意する必要があります。

- ラック キャビネット棚（アプライアンスをラックマウントする場合）
- レールを組み立てるためのプラス ドライバ
- 10/100 ギガビット Base-T TCP/IP LAN
- デスクトップまたはラップトップ コンピュータ
- Web ブラウザ（または、SSH およびターミナル ソフトウェア）
- 「ネットワーク設定の記録」（P.5）のネットワークおよび管理者の情報

3 ネットワーク設定の記録

作業に取り掛かる前に、ネットワークおよび管理者の設定について次の情報を書き出してください。システム セットアップ ウィザードの実行時には、この情報が必要になります。

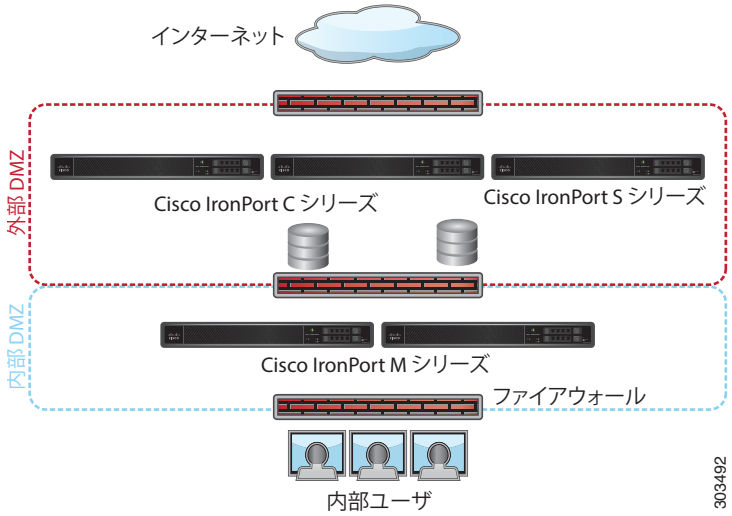
システム設定	
デフォルト システム ホスト名：	
定期レポートの送信先：	
タイム ゾーン情報：	
NTP サーバ：	
管理者パスワード：	
AutoSupport：	有効 / 無効
ネットワーク インテグレーション	
デフォルト ゲートウェイ（ルータ）の IP アドレス：	
DNS（インターネットまたは独自指定）：	
インターフェイス	
データ ポート 1	
IP アドレス：	
ネットワーク マスク：	
正式なホスト名：	
データ ポート 2	
IP アドレス：	
ネットワーク マスク：	

4 設置の計画

Cisco M170 コンテンツ セキュリティ管理アプライアンスは、企業ポリシーの設定および監査情報をモニタするための外部または「オフ ボックス」ロケーションとして機能するように設計されています。このアプライアンスは、ハードウェア、オペレーティング システム（AsyncOS）、およびサポート サービスを組み合わせることで、重要なポリシーとランタイム データを集中化し、統合します。

Cisco M170 アプライアンスは、内側の DMZ 内に設置し、外側の DMZ にある Cisco C シリーズおよび S シリーズ アプライアンスから隔離されたスパムを受信するように設計されています。内部ユーザは、コンテンツ セキュリティ管理アプライアンスにアクセスして、隔離のメッセージを表示し、管理します。

次のようなネットワーク構成を計画してください。

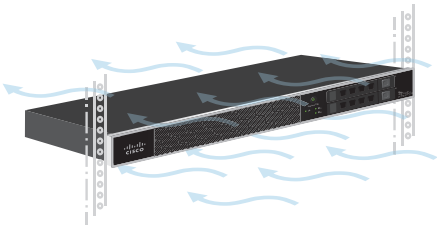


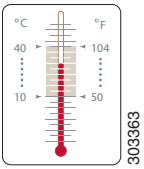
5 ラックへのアプライアンスの取り付け

スライド レールまたは固定ラック マウント ブラケットのいずれかを使用して、Cisco M170 コンテンツ セキュリティ管理アプライアンスを設置します。これらの設置オプションの詳細については、『*Cisco 170 Series Hardware Installation Guide*』を参照してください。

アプライアンスの配置

- 周囲温度：アプライアンスの過熱を防止するため、周囲温度が 104 °F（40 °C）を超える場所では操作しないでください。
- エアーフロー：アプライアンス周辺のエアー フローが十分であることを確認してください。
- 機械的加重：危険な状況を避けるため、アプライアンスが水平で安定していることを確認してください。

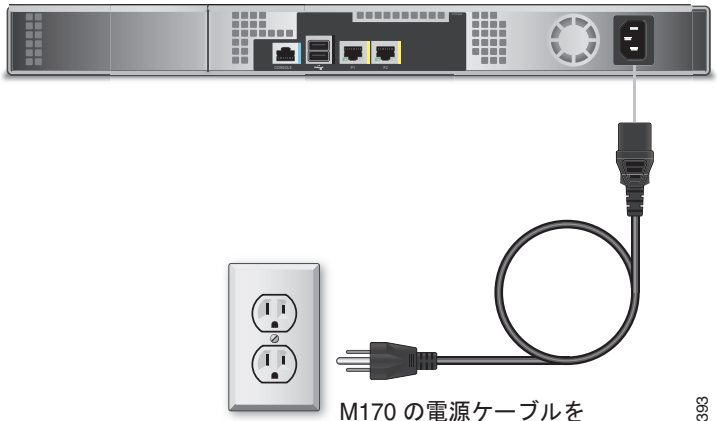




温度制限

6 アプライアンスへの電源接続

アプライアンスの背面パネルにある電源に、電源ケーブルのメス端子を差し込みます。オス端子を電気コンセントに差し込みます。



M170 の電源ケーブルを
電気コンセントに差し込みます。

303393

7 IP アドレスの一時的な変更

Cisco M170 に接続するには、コンピュータの IP アドレスを一時的に変更する必要があります。

（注） 設定が完了したら元に戻す必要があるため、現在の IP 設定を書き留めておきます。

Windows の場合

ステップ 1 [Start] メニューに移動し、[Control Panel] を選択します。

ステップ 2 [Network and Sharing Center] をダブルクリックします。

ステップ 3 [Local Area Connection] をクリックし、[Properties] をクリックします。

ステップ 4 [Internet Protocol (TCP/IP)] を選択して、[Properties] をクリックします。

ステップ 5 [Use the Following IP Address] を選択します。

ステップ 6 次の変更を入力します。

- IP アドレス：**192.168.42.43**
- サブネット マスク：**255.255.255.0**
- デフォルト ゲートウェイ：**192.168.42.1**

ステップ 7 [OK] と [Close] をクリックして、ダイアログ ボックスを閉じます。

Mac の場合

ステップ 1 Apple メニューを起動し、[System Preferences] を選択します。

ステップ 2 [Network] をクリックします。

ステップ 3　緑色のアイコンがあるネットワーク設定を選択します。これが、アクティブな接続です。次に、[Advanced] をクリックします。

ステップ 4　[TCP/IP] タブをクリックし、イーサネット設定のドロップダウン リストから [Manually] を選択します。

ステップ 5　次の変更を入力します。

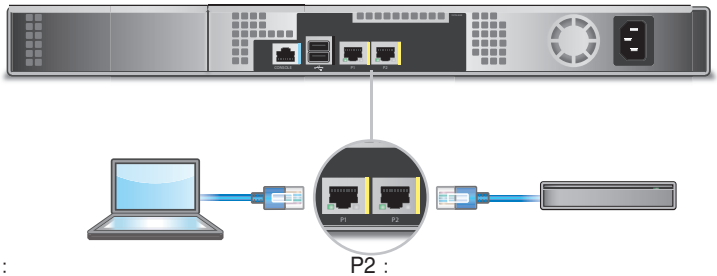
- IP アドレス：**192.168.42.43**
- サブネット マスク：**255.255.255.0**
- ルータ：**192.168.42.1**

ステップ 6　[OK] をクリックします。

8 アプライアンスへの接続

Cisco M170 アプライアンスには、2 個のギガビット ネットワーク ポート（P1 および P2）があります。

セットアップのため、管理インターフェイスとして P1 に接続し、P2 インターフェイスに着信 Web トラフィックまたは電子メールを設定します。これらの設定は、初期インストール後に変更することができます。



P1：
管理：192.168.42.42

イーサネット ケーブルを使用して、P1 ポートをコンピュータに接続します。

P2：
着信 Web トラフィックまたは電子メール

イーサネット ケーブルを使用して、P2 ポートをネットワークに接続します。

303494

9 アプライアンスの電源投入

Cisco M170 の前面パネルにあるオン / オフ スイッチを押して、アプライアンスの電源をオンにします。システムの電源を投入するたびに、システムが初期化するまで 5 分待機する必要があります。

アプライアンスの電源が投入されると、グリーンのライトが点灯して、アプライアンスが動作可能であることを示します。

303362

5 分間待機します。

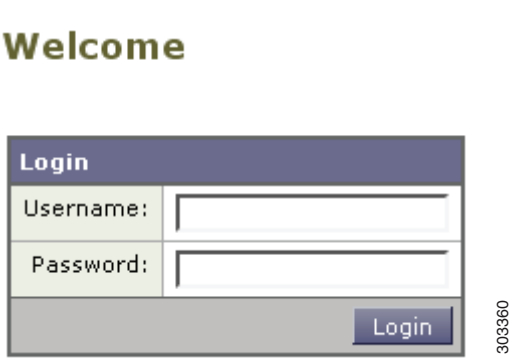
10 アプライアンスへのログイン

Web ベース インターフェイスまたはコマンドライン インターフェイスのいずれかを使用して、Cisco M170 にログインできます。

Web ベースのインターフェイス

ステップ 1　イーサネット ポートを介して Web ブラウザにアクセスする（「アプライアンスへの接続」（P.10）を参照）には、Web ブラウザに次の URL を入力して、Cisco M170 アプライアンスの管理インターフェイスにアクセスします。

http://192.168.42.42



ステップ 2　次のログイン情報を入力します。

- [Username]：**admin**
- [Password]：**ironport**

（注）　システムのセットアップ時に、ホスト名パラメータが割り当てられます。ホスト名（http://hostname:8080）を使用して管理インターフェイスに接続するには、まず、アプライアンスの *ホスト名* と IP アドレスを DNS サーバ データベースに追加する必要があります。

ステップ 3　[Login] をクリックします。

コマンドライン インターフェイス

ステップ 1 シリアル ポートを介してコマンドライン インターフェイスにアクセスする場合（「アプライアンスへの接続」（P.10）を参照）、9600 ビット、8 ビット、パリティなし、1 ストップ ビット（**9600、8、N、1**）、ハードウェアに設定したフロー制御を使用して、コマンドライン インターフェイスのターミナル エミュレータにアクセスします。

ステップ 2 IP アドレス **192.168.42.42** へのセッションを開始します。

ステップ 3 パスワード **ironport** を使用して **admin** としてログインします。

ステップ 4 プロンプトで、**systemsetup** コマンドを実行します。

11 システム セットアップ ウィザードの実行

システム セットアップ ウィザードは、Web ベース インターフェイスを使用してアプライアンスにアクセスすると（または、コマンドライン インターフェイスから **systemsetup** コマンドを実行すると）自動的に起動され、エンド ユーザ ライセンス契約書（EULA とも呼ばれる）が表示されます。

ステップ 1 システム セットアップ ウィザードを起動します。

ステップ 2 エンド ユーザ ライセンス契約書に同意します。

ステップ 3 登録情報を入力します。

ステップ 4 「ネットワーク設定の記録」（P.5）からの情報を入力します。

ステップ 5 Web セキュリティの設定を行います。

ステップ 6 設定サマリー ページを確認します。

ステップ 7 ユーザ名 **admin** と、システム セットアップ ウィザードで新たに設定したパスワードを使用して、アプライアンスにログインしなおします。

Cisco M170 コンテンツ セキュリティ管理アプライアンスでは自己署名証明書が使用されるため、Web ブラウザから警告が出る可能性があります。証明書を受け入れるだけで、この警告は無視できます。

ステップ 8 新しい管理者パスワードを書き留め、安全な場所に保管します。

12 ネットワークの設定

ネットワークの設定によっては、次のポートを使用したアクセスを許可するように、ファイアウォールを設定することが必要になる場合があります。SMTP サービスおよび DNS サービスでは、インターネットにアクセスできる必要があります。

- DNS：ポート 53
- SMTP：ポート 6025 および 25

他のシステム機能では、次のサービスが必要な場合があります。

- FTP：ポート 21、データ ポート TCP 1024 以上
- HTTP：ポート 80 または 82
- HTTPS：ポート 83 または 443
- LDAP：ポート 389 または 3268
- LDAP over SSL：ポート 636
- グローバル カタログ クエリー用の SSL を使用した LDAP：ポート 3269
- NTP：ポート 123
- 隔離認証：110（POP）または 143（IMAP）、あるいはその両方
- SSH：ポート 22
- Telnet：ポート 23

（注） ポート 443 を開かないと、機能キーをダウンロードできません。

詳細については、『*Cisco AsyncOS for Content Security Management User Guide*』の付録「Firewall Information」を参照してください。

警告 **キューおよびコンフィギュレーション ファイルの破損を防止するため、[System Administration] > [Shutdown/Reboot] ページからアプライアンスをシャットダウンする必要があります。**

13 設定の概要

次に示す設定の詳細を確認してください。

項目	説明
Management	http://192.168.42.42 を入力するか、システム セットアップ ウィザードを実行したときにアプライアンスに割り当てられるホスト名を入力して、管理ポート（P1）からコンテンツ セキュリティ管理アプライアンスを管理できます。 工場出荷時設定にリセットした場合は（システム セットアップ ウィザードの再実行などにより）、P1 ポートからのみ管理インターフェイスにアクセスできるので（http://192.168.42.42）、P1 ポートに接続できることを確認してください。 また、管理インターフェイスで HTTP 用にファイアウォール ポート 80 または 82、HTTPS 用に 83 および 443 が開かれていることを確認してください。
Computer Address	コンピュータの IP アドレスを、「ネットワーク設定の記録」（P.5）で書き留めた元の設定に戻すことを忘れないでください。 システム設定のサマリーは、[Management Appliance] > [Centralized Services] > [Security Appliances] ページから確認できます。

14 これで終了です

おめでとうございます。いつでも Cisco M170 コンテンツ セキュリティ管理アプライアンスの使用を開始できます。アプライアンスをさらに活用するために、次の手順のいくつかを実行することも検討してください。

セキュリティ アプライアンスの追加

管理する Cisco 電子メール セキュリティ アプライアンスと Cisco Web セキュリティ アプライアンスを追加できます。Cisco M170 に Cisco セキュリティ アプライアンスを追加するには、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

集約メールおよび Web レポートの有効化

Cisco M170 コンテンツ セキュリティ管理アプライアンスは、Web トラッキングだけではなく、電子メール レポーティングと Web レポーティングの両方をサポートしており、複数の電子メール アプライアンスおよび Web セキュリティ アプライアンス間の電子メールおよび Web トラフィックの中央集中型表示を可能にします。

集約メール レポートを有効にするには、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

集約 Web レポートを有効にするには、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

集約管理レポートを有効にすると、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] または [Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting Overview] ページから、Web レポートおよびメール レポートの統計情報やその他の情報を確認できます。

メッセージ トラッキング

メッセージ トラッキング サービスを（GUI で）使用してクエリーを実行することにより、メッセージの送信とブロッキングに関する詳細を表示できます。

電子メール セキュリティ アプライアンスのメッセージ トラッキングにアクセスするには、[Monitor] > [Message Tracking] を選択します。

定期メール レポートおよび定期 Web レポート

Cisco M170 コンテンツ セキュリティ管理アプライアンスでは、電子メール アプライアンスまたは Web セキュリティ アプライアンスから受信するデータを使用して、スケジュールされたレポートを生成できます。レポートは、毎日、毎週、または毎月実行されるようにスケジュールでき、前日、前週、または前月のデータが含まれるように設定できます。

追加情報

その他にも、Cisco M170 アプライアンスに設定できる機能があります。使用可能なその他の機能の詳細については、コンテンツ セキュリティ管理アプライアンスのマニュアルを参照してください。

15 よくあるご質問

Q. Cisco M170 コンテンツ セキュリティ管理アプライアンスで古いコンフィギュレーション マスターを削除するには、どうしたらよいですか

A. [Web] > [Utilities] > [Security Services Display] ページに移動し、[Edit Settings] をクリックします。各コンフィギュレーション マスターの上部で、対応するコンフィギュレーション マスターのチェックボックスをオフにできます。[Submit] をクリックします。すると、そのコンフィギュレーション マスターは、GUI の [Configuration] タブとして表示されなくなります。

Q. Cisco M170 コンテンツ セキュリティ管理アプライアンスにアプライアンスを追加するには、どうしたらよいですか

A. Cisco M170 アプライアンスでモニタリング サービスをイネーブルにした後は、管理するアプライアンスの接続情報を追加できます。AsyncOS 6.0 またはそれ以降のリリースを使用して任意の Cisco 電子メール セキュリティ アプライアンスに接続でき、AsyncOS 5.7、6.3、7.1、またはそれ以降のリリースを実行して任意の Cisco Web セキュリティ アプライアンスに接続できます。

a. Cisco M170 コンテンツ セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

b. [Add Email Appliance] をクリックして [Add Email Security Appliance] ページを表示するか、[Add Web Appliance] をクリックして [Add Web Security Appliance] ページを表示します。

c. [Appliance Name and IP Address] テキスト フィールドに、Cisco アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

d. Cisco アプライアンスを管理するときに使用するサービスを選択します。

e. [Establish Connection] をクリックします。

f. [Test Connection] をクリックして、リモート アプライアンスのモニタリング サービスが正しく設定されていて矛盾がないことを確認します。

g. Web セキュリティ アプライアンスを追加する場合は、アプライアンスを割り当てるコンフィギュレーション マスターを選択します。

h. [Submit] をクリックして、ページ上の変更を送信し、[Commit Changes] をクリックして変更を保存します。

Q. Web セキュリティ アプライアンスからコンテンツ セキュリティ管理アプライアンスにアクセス ログを転送する必要はありますか

A. いいえ。これは、集約管理レポートを有効にした後で、Web セキュリティ アプライアンスで内部的に処理されるものです。集約管理レポートを有効にするには、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] に移動します。

Q. Web レポート ツールでのデータの使用可能期間を教えてください

A. データの保持は、全体的な使用量、つまり、存在するレコードの数によって異なります。ただし、各アプライアンスは最低でも 45 日分のレポートを収容するようにサイズ設定されています。

Q. Web レポートでユーザ名を非表示にするには、どうしたらよいですか

a. Cisco M170 コンテンツ セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

b. [Edit Settings] をクリックします。

c. [Anonymize User Names in Reports] チェックボックスをオンにします。

d. [Submit] をクリックします。

Q. レポート データの更新頻度を教えてください

A. Cisco M170 コンテンツ セキュリティ管理アプライアンスは、約 15 分ごとにすべての管理対象アプライアンスからすべてのレポート データを取得し、これらのアプライアンスからのデータを集約します。アプライアンスによっては、個々のメッセージにコンテンツ セキュリティ管理アプライアンス上のレポート データを含める際に多少時間がかかる場合があります。データの詳細については、[System Status] ページを確認してください。

16 関連資料

サポート	
Cisco Email Security Support Community Cisco Web Security Support Community (コンテンツ セキュリティ管理アプライアンスのサポートを含む)	https://supportforums.cisco.com/community/netpro/security/email https://supportforums.cisco.com/community/netpro/security/web
製品に関する資料	
『Content Security Management Appliance Quick Start Guide』(このマニュアル)	http://www.cisco.com/en/US/docs/security/security_management/sma/hw/quick_start/M170_QSG.pdf
『Cisco 170 Series Hardware Installation Guide』 LED、技術仕様、およびラックマウント オプションに関する情報が含まれています。	http://www.cisco.com/en/US/docs/security/esa/hw/170Series_HW_Install.pdf
Cisco コンテンツ セキュリティ管理アプライアンスのマニュアル アプライアンスの機能の設定、CLI コマンド、およびリリース ノートに関するドキュメントが含まれています。	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
安全性および適合規格に関するガイド	http://www.cisco.com/en/US/docs/security/esa/hw/SafetyAndComplianceGuide.pdf

MIB	
AsyncOS MIBs for Cisco Content Security Management Appliance （「Related Tools」の項）	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

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

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/cisco/web/support/index.html）の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート 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/cisco/web/JP/support/index.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』には、シスコの新規および改訂版の技術マニュアルの一覧が示されており、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/