クイック スタート ガイド

Cisco IronPort M170 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。

ようこそ

Cisco IronPort M170 セキュリティ管理アプライアンスをお選びいただき、ありがとうございます。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 IronPort 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。セキュリティ管理アプライアンスは、Cisco IronPort 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、セキュリティ管理アプライアンスを物理的に設置し、システム セットアップ ウィザードを使用してインストールの基本設定を行う方法を説明します。

このマニュアルの構成

このマニュアルの基本項目は次のとおりです。

- 設置前のワークシート / 設置準備
- 設置手順
- システム セットアップ ウィザードの実行
- 設置後の手順
- よくあるご質問
- 補足情報を記した付録

1 はじめに

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。

M170 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
- 製品ドキュメンテーション CD

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
- 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 BaseT TCP/IP ローカル エリア ネットワーク（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）
- Go Live 設定用のネットワーク情報

2 ネットワーキング ワークシート

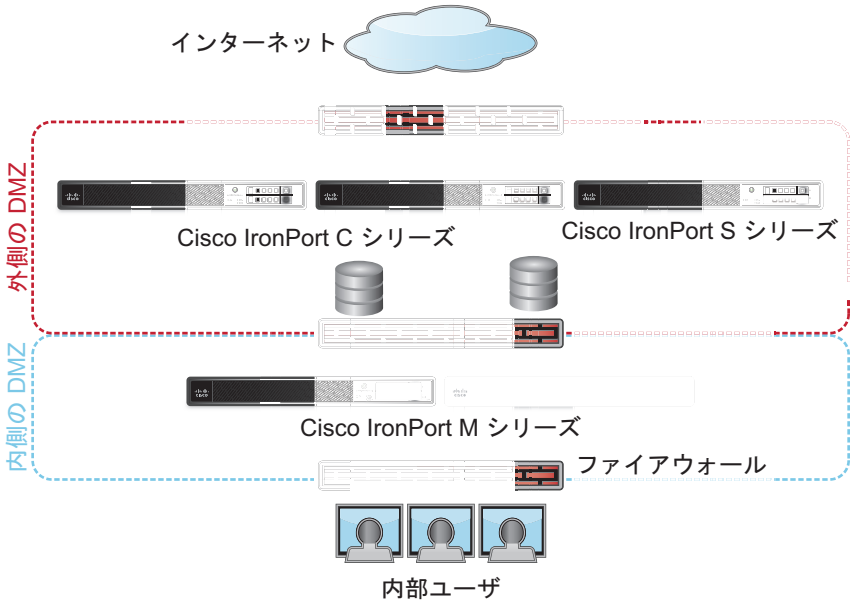
作業に取り掛かる前に、ネットワークおよび管理者の設定について次の情報を書き出してください。ステップ 10 以降、システム セットアップ ウィザードの実行時に次の情報の入力が必要になります。

システム設定	
デフォルト システムのホスト名：	
配信スケジュール済みレポートの送信先：	
タイム ゾーン情報：	
NTP サーバ：	
管理者パスワード：	
AutoSupport	□ イネーブル /□ ディセーブル
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：	
完全修飾ホスト名：	
データ ポート 2	
IP アドレス：	
ネットワーク マスク：	

3 設置の計画

Cisco IronPort 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。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 IronPort C シリーズおよび S シリーズ アプライアンスから検疫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、M170 アプライアンスにアクセスして、検疫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。

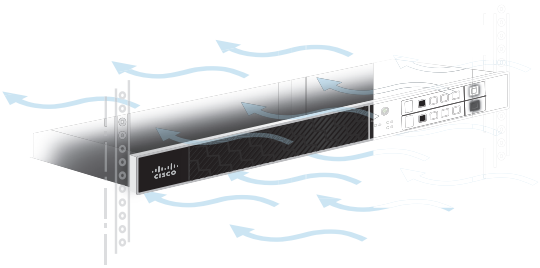


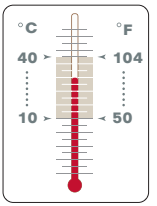
4 ラックへの設置

M170 アプライアンスをラック キャビネットに設置します。システムの周囲温度が指定限度内であることを確認します。装置周辺の**エアーフローが十分**であることを確認します。

配置に関するヒント

- **周囲温度**：M170 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**：M170 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、M170 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。

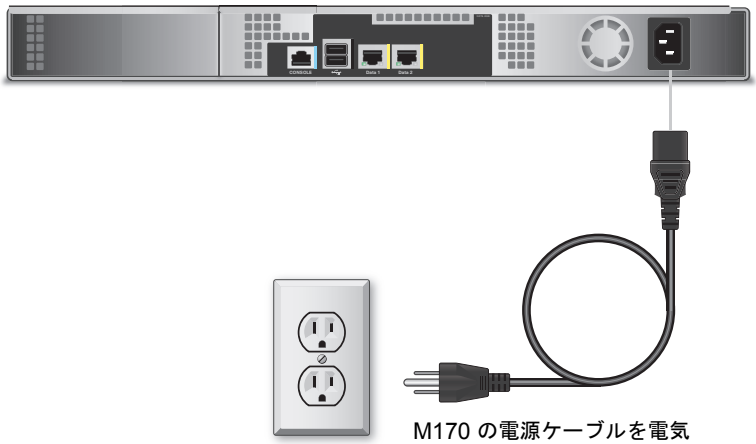




温度制限

5 プラグ イン

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。

6 IP アドレスの変更

M170 セキュリティ管理アプライアンスに接続するには、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。

後で設定を戻す必要があるため、まずは、現在の IP 設定を書き留めておきます。

その後、IP アドレスを次のように変更します。

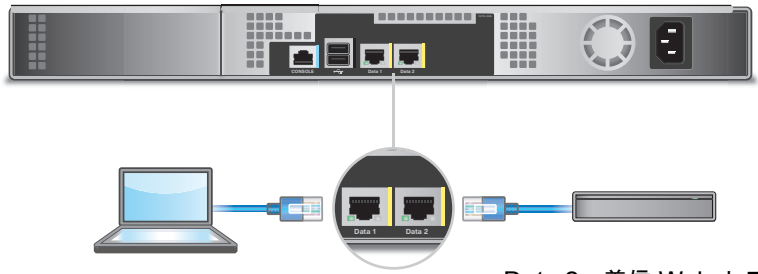
- IP アドレス：192.168.42.xx
- サブネット マスク：255.255.255.0
- ゲートウェイ：192.168.42.1

（注）UNIX ユーザおよび Mac ユーザの場合は、関連する製品マニュアルを参照してください。同梱のイーサネット ケーブルを使用して、ラップトップを管理ネットワーク ポートに接続します。

Windows または Mac 環境での IP アドレスの変更の詳細については、付録 A「ラップトップ IP アドレスの変更」を参照してください。

7 アプライアンスへの接続

M170 アプライアンスには、**Data 1** と **Data 2** の **2 つのギガビット ネットワーク ポート**が搭載されています。



Data 1：管理インターフェイス
192.168.42.42

イーサネット ケーブルを使用して、Data 1 ポートをコンピュータに接続します。

Data 2：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、Data 2 ポートをネットワークに接続します。

セットアップのため、管理インターフェイスとして Data 1 に接続し、Data 2 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。必要に応じて、初期インストール後にこれらの設定を変更できます。

8 電源投入

アプライアンスの前面パネルにある**オン / オフ** スイッチを押して、システム電源をオンにします。最初に電源を投入するときに、システムが初期化されるまで 5 分間待機してからアプライアンスに接続する必要があります。

マシンの電源が投入されると、グリーンのライトが点灯して、マシンが動作可能であることを示します。

5 分間待機します。

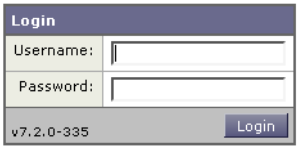
9 アプライアンスへのログイン

Web ベース インターフェイスおよびコマンドライン インターフェイスのいずれかを使用して、M170 アプライアンスにログインできます。

Web ベースのインターフェイス

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場合（ステップ 7 を参照）、Web ブラウザに URL **http://192.168.42.42** を入力してアプライアンスの管理インターフェイスに移動します。

M170 アプライアンスのログイン ページが開きます。



次のログイン情報を入力します。

ユーザ名：**admin**

パスワード：**ironport**

コマンドライン インターフェイス

コマンドライン インターフェイスにアクセスするには、IP アドレス **192.168.42.42** へのセッションを開始します。**パスワード** ironport を使用して **admin** としてログインします。

10 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自動的に開始され、エンド ユーザ ライセンス契約書が表示されます。先に進むには、ライセンス契約書を読み、同意してください。

ステップ 1 システム セットアップ ウィザードを開始します。

ステップ 2 ライセンスに同意します。

ステップ 3 登録情報を入力します。

ステップ 4 **「ネットワーキング ワークシート」（P.4）**からの情報を入力します。

ステップ 5 設定サマリー ページを確認します。

ステップ 6 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。

M170 アプライアンスでは自己署名証明書が使用され、Web ブラウザから警告がトリガーされる可能性があります。証明書を受け入れるだけで、これらの警告は無視して構いません。

新しい管理者パスワードを書き留め、安全な場所に保管することを忘れないでください。

11 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 および DNS サービスは、インターネットにアクセスできる必要があります。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。

- SMTP：ポート 6025 および 25
- DNS：ポート 53
- HTTP：ポート 80 または 82
- HTTPS：ポート 83 または 443
- SSH：ポート 22
- Telnet：ポート 23
- NTP：ポート 123
- 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
- FTP：ポート 21、データ ポート TCP 1024 以上
- 検疫認証：110（POP）または 143（IMAP）、あるいはその両方

重要：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 IronPort AsyncOS for Security Management User Guide』の「Firewall Information」を参照してください。

12 設定の概要

次に示す設定の詳細を確認してください。

管理

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（Data 1）から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）、Data 1 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）、Data 1 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。

コンピュータ アドレス

コンピュータの IP アドレスを、ステップ 2 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。

注：
システム設定のサマリーは、[Management Appliance] > [Centralized Services] > [Security Appliances] から確認できます。

13 これで終了です。

おめでとうございます。いつでも M170 アプライアンスの使用を開始できます。M170 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 Email セキュリティ アプライアンスと Web セキュリティ アプライアンスを追加できます。セキュリティ管理アプライアンスでは、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択して、Cisco IronPort アプライアンスを追加します。

中央集中型電子メールおよび Web レポーティングのイネーブル化

セキュリティ管理アプライアンスは現在、電子メールおよび Web レポーティングと Web トラッキングの両方をサポートしており、複数の電子メールおよび 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。

中央集中型電子メール レポーティングをイネーブルにするには、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] に移動します。

中央集中型 Web レポーティングをイネーブルにするには、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] に移動します。

中央集中型レポーティングをイネーブルにすると、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] または [Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting Overview] ページから、Web および電子メール レポーティングの統計情報やその他の情報を表示できます。

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] に移動します。

スケジュールされた電子メールおよび Web レポーティング

セキュリティ管理アプライアンスでは、電子メールまたは 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、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セキュリティ管理機能の詳細については、セキュリティ管理アプライアンスのドキュメンテーション（アプライアンスに同梱のドキュメンテーション CD に収録）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。

14 よくあるご質問

Q. 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

[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. M170 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

セキュリティ管理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 Email 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 Web セキュリティ アプライアンスに接続できます。

1. セキュリティ管理アプライアンスでは、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。
2. [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。
3. [Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort 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。
4. Cisco IronPort 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。
5. [Establish Connection] をクリックします。
6. [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。
7. 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。
8. [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確定します。

Q. Web セキュリティ アプライアンスから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

いいえ。これは、中央集中型レポーティングをイネーブルにした後で、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。中央集中型レポーティングをイネーブルにするには、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] に移動します。

Q. Web レポーティング ツールでのデータの使用可能期間を教えてください

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 日分のレポーティング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

1. 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。
2. [Edit Settings] をクリックします。
3. [Anonymize User Names in Reports] チェックボックスをオンにします。
4. [Submit] をクリックします。

Q. レポーティング データの更新頻度を教えてください

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のデータをプルし、それらのアプライアンスのデータを集約します。使用するアプライアンスによっては、セキュリティ管理アプライアンスでレポーティング データに特定のメッセージを組み込むのに時間が掛かる場合があります。データの情報については、[System Status] ページを確認してください。

15 関連資料

サポート	
Cisco IronPort サポート コミュニティ	supportforums.cisco.com/community/netpro/security/ironport
製品マニュアル	
Cisco IronPort セキュリティ管理アプライアンス	www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
	『Cisco IronPort AsyncOS for Security Management Appliance User Guide』
	『Cisco IronPort M170 クイック スタート ガイド』

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/techsupport）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/jp/go/tac

A 付録

ラップトップ IP アドレスの変更（ステップ 6 に対応）

Windows の場合：

1. [Start] メニューに移動し、[Control Panel] をクリックします。[Control Panel] が開きます。
2. [Network Connections] をダブルクリックします。[Network Connections] ウィンドウが開きます。
3. LAN または適切なローカル エリア接続を右クリックして、[Properties] をクリックします。
4. [Internet Protocol (TCP/IP)] を選択して、[Properties] をクリックします。
5. [Use the following IP Address] チェックボックスをオンにして、IP アドレス 192.168.42.43 とサブネット マスク 255.255.255.0 を入力します。
6. [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：

1. Apple メニューを起動します。[System Preferences] を選択します。次に、[Network Control Panels]、[TCP/IP] の順にクリックします。
2. TCP/IP から、グリーンのアイコンが点灯してい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、[Configure] をクリックします。
3. [Ethernet] の設定に進み、ドロップダウン メニューから [Manually] を選択します。
4. [IP Address] フィールドに 192.168.42.43 と入力し、[Subnet Mask] フィールドに 255.255.255.0 と入力します。
5. [Apply] をクリックします。

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/

78-19644-02-J

モデル：MRSA