クイック スタート ガイド

Cisco S170 Web セキュリティ アプライアンス

改訂日：2013 年 3 月 13 日
Part Number：78-19643-04-JA

1 ウェルカム

Cisco S170 Web セキュリティ アプライアンス（Cisco S170）をお選びいただき、ありがとうございます。Cisco S170 は、企業の Web トラフィックの保護および管理を支援します。

このマニュアルでは、Cisco S170 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。また、アプライアンスの設定方法については、『*Cisco IronPort AsyncOS for Web User Guide*』の章「Deployment」を参照してください。

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 S170 Web セキュリティ アプライアンスには、以下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

以下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」セクション（3 ページ）に関するネットワークおよび管理者情報、ならびに「稼働時」の設定

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以下の情報を書き出してください。

展開オプション	
• Web プロキシ（Web Proxy） – L4 と透過 – WCCP ルータとの透過スイッチ – 明示的なフォワードプロキシ	• L4 トラフィック モニタ（L4 Traffic Monitor） – シンプレックス タップ/スパン ポート – デュプレックス タップ/SPAN ポート
ネットワーク コンテキスト	
ネットワーク上の別のプロキシの有無:	○
他のプロキシ IP アドレス:	
他のプロキシ ポート:	
ネットワーク設定（Network Settings）	
デフォルトのシステムホスト名:（Default System Hostname:）	
DNS サーバ:	インターネット ルート DNS サーバを使用する。 以下の DNS サーバ（最大 3 つ）を使用する。 1. 2. 3.
Network Time Protocol（NTP）サーバ:	
タイム ゾーンの領域:	
タイム ゾーンの国:	
タイム ゾーンの GMT オフセット:	

インターフェイスの設定	
管理ポート（Management Port）	
IP アドレス（IP Address）：	
ネットワークマスク：（Network Mask:）	
Hostname:	
データ ポート（オプション、「注」を参照）	
IP アドレス（IP Address）：	
ネットワークマスク：（Network Mask:）	
ホスト名（Hostname）：	

（注） Web プロキシは、管理インターフェイスを共有できます。データ インターフェイスの IP アドレスと管理インターフェイスの IP アドレスを別々に設定した場合は、同じサブネットを共有できません。

ルート	
管理用の内部ルート	
デフォルト ゲートウェイ：	
静的ルート名：	
静的ルートの宛先ネットワーク：	
静的ルートのゲートウェイ：	
データ用の内部ルート	
デフォルト ゲートウェイ：	
静的ルート名：	
静的ルートの宛先ネットワーク：	
静的ルートのゲートウェイ：	

透過 ルーティング デバイス	
デバイス タイプ	• Layer 4 Switch または No Device • WCCP ルータ – 標準のサービス ID を有効にする (web-cache)。 – ルータ アドレス: _____ – ルータ セキュリティを有効にする。パスワード (Password) : _____

(注) アプライアンスを WCCP ルータに接続する際は、システム セットアップ ウィザードの実行後に WCCP サービスが作成されるよう、Web セキュリティ アプライアンスの設定が必要になる場合があります。

管理設定 (Administrative Settings)	
管理者パスワード:	
システムアラート メールの送信先:	
SMTP リレー ホスト:	(オプション)
オートサポート: (AutoSupport:)	有効 (Enable)
SenderBase ネットワークに参加: (SenderBase Network Participation:)	有効 (Enable) • 限定的 (Limited) • 標準 (Standard)

セキュリティ サービス	
L4 トラフィック モニタ:	• モニタのみ(Monitor only) • ブロック(Block)
許容できる使用の制御:	有効(Enable) • IronPort URL フィルタ • Cisco IronPort Web 使用コントロール
Web レピュテーション フィルタ:	有効(Enable)
マルウェアおよびスパイウェアのスキャン:	• Webroot を有効にする(Enable Webroot) • McAfee を有効にする(Enable McAfee) • Sophos を有効にする(Enable Sophos)
検出されたマルウェアに対する措置:	• モニタのみ(Monitor only) • ブロック(Block)
IronPort データ セキュリティ フィルタリング:	有効(Enable)

4 設置の計画

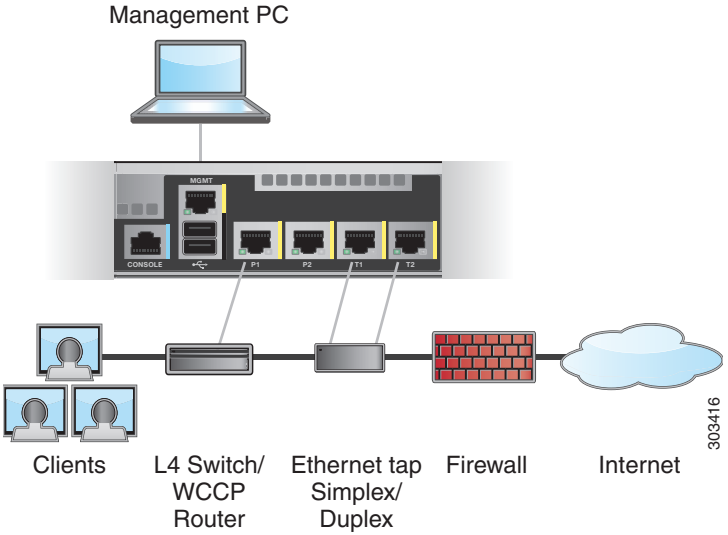
ネットワーク内にどのように Cisco S170 Web セキュリティ アプライアンスを設定するかを決めます。

Cisco S170 アプライアンスは、クライアントとインターネットの間のネットワークに追加のレイヤとして設置するのが通常です。クライアント トラフィックをアプライアンスに送信するためのレイヤ 4(L4)スイッチまたは WCCP ルータが必要かどうかは、アプライアンスをどのように展開するかによります。

以下の展開オプションがあります。

- 透過プロキシ:L4 スイッチを使用した Web プロキシ
- 透過プロキシ:WCCP ルータを使用した Web プロキシ
- 明示的なフォワードプロキシ:ネットワーク スイッチへの接続

- L4 トラフィック モニタ:イーサネット タップ(シンプレックスまたはデュプレックス)
  - シンプレックス モード:ポート T1 はすべての発信トラフィックを受信し、ポート T2 はすべての着信トラフィックを受信します。
  - デュプレックス モード:ポート T1 は、すべての着信および発信トラフィックを受信します。



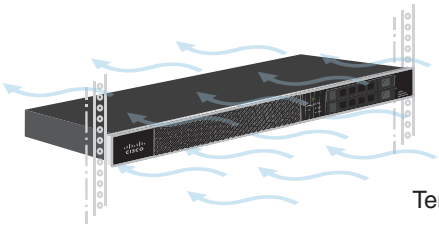
(注) 真のクライアント IP アドレスをモニタするため、L4 トラフィック モニタは必ず、ファイアウォールの内側で、NAT(ネットワーク アドレス変換)の前に設定します。

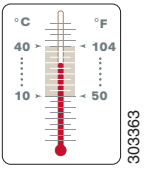
5 ラックへのアプライアンスの取り付け

スライド レールまたは固定ラック マウント ブラケットを使用して Cisco S170 Web セキュリティ アプライアンスを取り付けます。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。

ラックへの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 40 °C(104 °F)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。

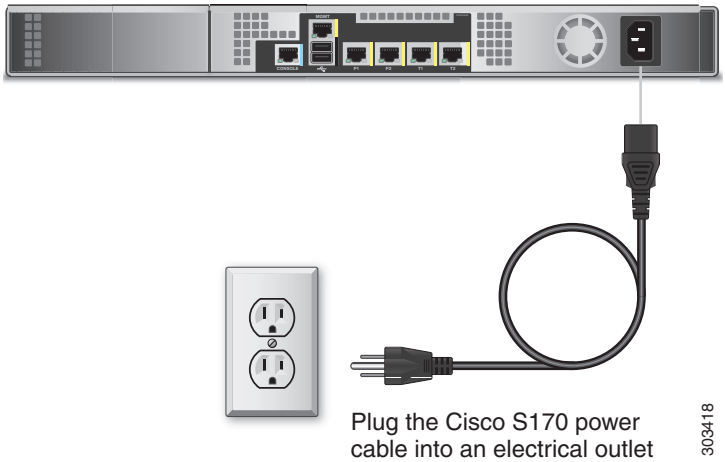




Temperature Limits

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。



Plug the Cisco S170 power cable into an electrical outlet

303418

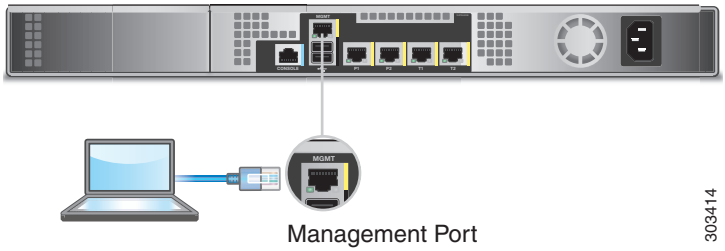
7 IP アドレスの一時的な変更

Cisco S170 アプライアンスに接続するには、一時的にコンピュータの IP アドレスを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 システム ボックスに同梱されているイーサネット ケーブルを使用して、ラップトップを MGMT 管理ポートに接続します。Cisco S170 アプライアンスは、MGMT 管理ポートだけを使用します。



ステップ 2 [スタート(Start)] メニューに移動し、[コントロール パネル(Control Panel)] を選択します。

ステップ 3 [ネットワークと共有センター(Network and Sharing Center)] をダブルクリックします。

ステップ 4 [ローカル エリア接続(Local Area Connection)] をクリックし、次に[プロパティ(Properties)] をクリックします。

ステップ 5 [インターネット プロトコル(TCP/IP) (Internet Protocol (TCP/IP))] を選択して、[プロパティ(Properties)] をクリックします。

ステップ 6 [以下の IP アドレスを使う(Use the Following IP Address)] を選択します。

ステップ 7 以下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 8 [OK] と [閉じる(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、[システム環境設定(System Preferences)] を選択します。

ステップ 2 [ネットワーク(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、[詳細(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 [手動(Manually)] を選択します。

ステップ 5　以下の変更を入力します。

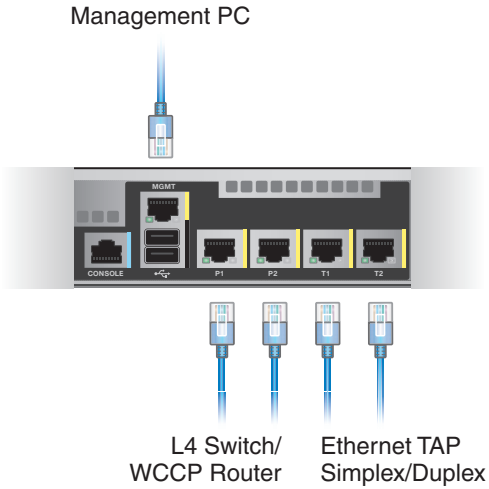
- IP アドレス:**192.168.42.43**
- サブネット マスク:**255.255.255.0**
- ルータ:**192.168.42.1**

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 S170 アプライアンスの背面パネルにある適切なポートに、イーサネット ケーブルを差し込みます。

- プロキシ ポートには、P1 と P2 というラベルが付いています。
  - P1 のみが有効:P1 のみが有効の場合、着信トラフィックと発信トラフィックの両方に対応するネットワークに P1 を接続します。
  - P1 および P2 が有効:P1 と P2 の両方が有効である場合、P1 を内部ネットワーク、P2 をインターネットに接続する必要があります。
- トラフィック モニタ ポートには、T1 と T2 というラベルが付いています。
  - シンプレックス タップ:ポート T1 および T2。1 本のケーブルでインターネットに宛てたすべてのパケットに対応し(T1)、もう 1 本のケーブルでインターネットから入ってくるすべてのパケットに対応(T2)。
  - デュプレックス タップ:ポート T1。1 本のケーブルですべての着信およぶ発信トラフィックに対応。



9 アプライアンスの電源投入

Cisco S170 の前面パネルの電源スイッチを押して、アプライアンスの電源を投入します。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、アプライアンスが作動していることを示します。

Wait five minutes.

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 S170 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

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」セクション（11 ページ）を参照）には、Web ブラウザに次の URL を入力して、Cisco S170 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。

- ユーザ名：**admin**
- パスワード：**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 [ログイン（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 コマンドラインでシリアル ポートを介してアクセスする（「アプライアンスへの接続」セクション（11 ページ）を参照）には、SSH または端末エミュレータ（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**）、およびフロー制御をハードウェアに設定）を使用してコマンドラインにアクセスします。

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

Web ベース インターフェイスを介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 インターフェイスで **systemsetup** コマンドを実行すると）、システム セットアップ ウィザードが自動的に開始され、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」セクション（3 ページ）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 S170 Web セキュリティ 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。

Web セキュリティ アプライアンスは、以下のポートをリッスンできる必要があります。

- FTP：ポート 21、データ ポート TCP 1024 以上
- HTTP：ポート 80
- HTTPS：ポート 443
- 管理アクセス：ポート 8443（HTTPS）および 8080（HTTP）
- SSH：ポート 22

Web セキュリティ アプライアンスは、以下のポートで発信接続できる必要があります。

- DNS：ポート 53
- FTP：ポート 21、データ ポート TCP 1024 以上
- HTTP：ポート 80
- HTTPS：ポート 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
- SMTP：ポート 25

（注） ポート 80 および 443 を開いておかないと、機能キーをダウンロードできません。

13 設定サマリ

項目	説明
管理（Management）	http://192.168.42.42:8080 と入力して、管理ポート（MGMT ポート）から Web セキュリティ アプライアンスを管理することができます。また、システム セットアップ ウィザードを完了した後に、管理インターフェイスに割り当てられた IP アドレスを使用して管理することもできます。 （システム セットアップ ウィザードの再実行などにより）工場出荷時のデフォルト設定にリセットした場合は、MGMT ポート（http://192.168.42.42:8080）からしか管理インターフェイスにアクセスできなくなるため、必ず、MGMT ポートに接続できるようにしてください。 また、管理インターフェイスでファイア ウォール ポート 80 および 443 を開いていることを確認します。

項目	説明
データ	システム セットアップ ウィザードを実行した後、アプライアンスの少なくとも 1 つのポートを、ネットワーク上のクライアントから Web トラフィックを受信するように設定します：M1 のみ。M1 および P1。M1、P1 および P2。P1 のみ。または P1 および P2。  **（注）** Web プロキシを明示的な転送モードに設定した場合は、データ用に設定された IP アドレス、およびM1 または P1 のいずれかを使用して、Web セキュリティ アプライアンスの Web プロキシに明示的に Web トラフィックを転送するよう、クライアント マシンのアプリケーションを設定する必要があります。
トラフィック モニタ	システム セットアップ ウィザードを実行すると、1 つまたは両方の L4 トラフィック モニタ ポート（T1 のみ、または T1 と T2 の両方）が、すべての TCP ポートのトラフィックをリッスンするように設定されます。L4 トラフィック モニタのデフォルト設定は、モニタのみです。セットアップ時、またはセットアップ後に、疑わしいトラフィックに対するモニタおよびブロックの両方を行うよう、L4 トラフィック モニタを設定できます。
コンピュータ アドレス	コンピュータの IP アドレスを、「IP アドレスの一時的な変更」セクション（9 ページ）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。

14 これで完了です

これですべての作業は完了しました。これで Cisco S170 Web セキュリティ アプライアンスを使用して無効にすることができます。アプライアンスをさらに活用するために、以下の手順のいくつかを実行することも検討してください。

ユーザ ポリシー

Web インターフェイスを使用し、必要に応じて、どのユーザがどの Web リソースにアクセスできるかを定義するポリシーを作成します。

- ユーザの識別: インターネットにアクセスできるユーザ グループを定義するには、[Web Security Manager] > [Identities]を選択します。
- アクセス ポリシーの定義: 許可または拒否するオブジェクトおよびアプリケーション、監視または拒否する URL カテゴリ、Web レピュテーションおよびマルウェア対策を設定してユーザのインターネットへのアクセスを制御するには、[Web Security Manager] > [Access Policies] を選択します。

また、その他複数のポリシー タイプを定義して、インターネットへのアクセスを制御することにより、組織の許容可能な使用ポリシーを実施できます。たとえば、HTTPS トランザクションを復号化するためのポリシーや、アップロード要求を制御するその他のポリシーを定義できます。

Cisco S170 アプライアンスでのポリシーの設定については、*Cisco IronPort AsyncOS for Web User Guide* の「Working with Policies」の章を参照してください。

レポート

Web インターフェイスで使用できるレポートを表示することにより、ネットワーク上でブロックおよびモニタされる Web トラフィックの統計情報を表示できます。ブロックされた上位の URL カテゴリ、クライアント アクティビティ、システム ステータスなどに関するレポートを表示できます。

追加情報

その他にも、Cisco S170 アプライアンスに設定できる機能があります。機能キーの設定、エンド ユーザの通知、ロギングに関する詳細と、その他の使用可能な Web セキュリティ アプライアンス機能の詳細については、マニュアル『Cisco S170 Web セキュリティ アプライアンス』を参照してください。

15 関連資料

サポート	
Cisco IronPort Support	http://www.cisco.com/en/US/products/ps11169/serv_group_home.html
米国の無料通話番号	1-800-553-2447 1-408-526-7209
International Contacts	http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html
Online Technical Support and Documentation (login may be required)	www.cisco.com/support
Cisco Web セキュリティ アプライアンス サポート コミュニティ	https://supportforums.cisco.com/community/netpro/security/web
製品に関する資料	
Cisco S170 Web セキュリティ アプライアンス クイック スタート ガイド (本マニュアル)	http://www.cisco.com/en/US/docs/security/wsa/hw/S170_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 Web セキュリティ 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/ps10164/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	
Cisco Web セキュリティ アプライアンス向け AsyncOS MIB（「Related Tools」の項）	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.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 の『*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*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、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をデスクトップに配信することもできます。RSS フィードは無料のサービスです。

この資料の記載内容は 2019 年 3 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。

お問い合わせ先

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

78-19643-04JA 19.3