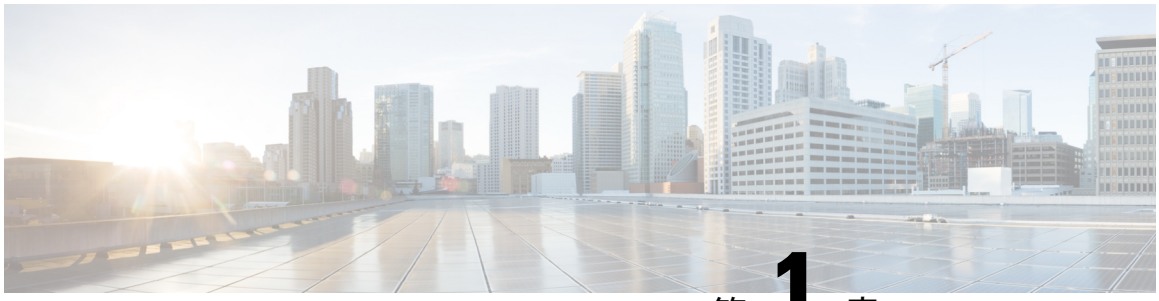
Cisco Secure Web Appliance S196、S396、S696、および S696F スタートアップガイド

初版：2023 年 12 月 15 日

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/

目 次



第 1 章

Secure Web Appliance の概要

Secure Web Appliance について

Cisco Secure Web Appliance S196、S396、S696、および S696F は、組織が Web トラフィックを保護および制御するのに役立ちます。このガイドでは、アプライアンスのセットアップとシステム セットアップ ウィザードを使用したアプライアンスの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、『AsyncOS for Cisco Secure Web Appliances User Guide』の「Deployment」の章を参照してください。

ネットワーク設定の記録

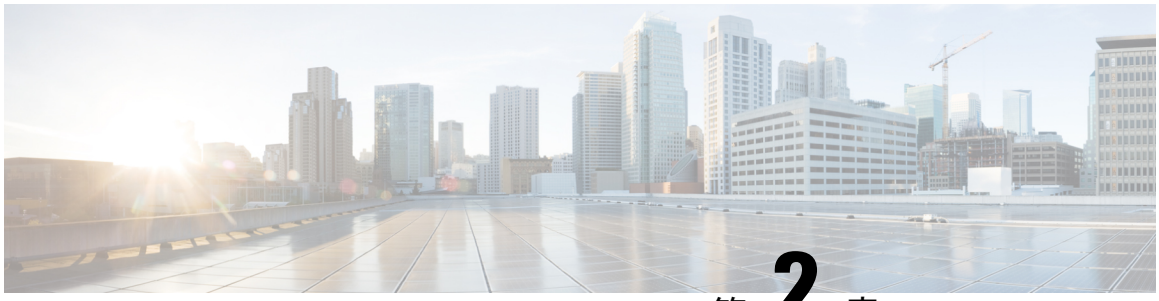
作業に取り掛かる前に、ネットワークおよび管理者の設定について以下の情報を書き出してください。

展開オプション	
Web プロキシ： • 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 モニター： • シンプレックス タップ/SPAN 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	
デフォルトのシステムホスト名:（Default System Hostname:）	
DNS サーバー：	インターネットのルート DNS サーバーを使用。 DNS サーバーを使用（最大 3 台）： 1. 2. 3.
Network Time Protocol（NTP）サーバー：	
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:）	
ホスト名（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（Routes）	

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。 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、Cisco 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 モニター：	• モニターのみ（Monitor only） • ブロック（Block）
許容できる使用の制御：	有効（Enable） • 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：	• モニターのみ（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）



第 2 章

設置の計画

設置の計画

ネットワーク内にどのようにCisco 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。

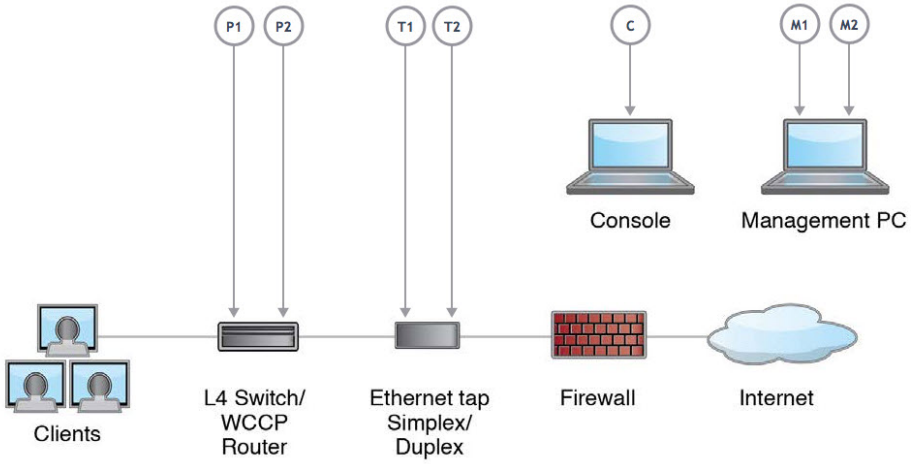
Cisco Web セキュリティアプライアンスは、クライアントとインターネットの間のネットワークに追加のレイヤとして設置するのが通常です。クライアントトラフィックをアプライアンスに送信するためのレイヤ4（L4）スイッチまたはWCCPルータが必要かどうかは、アプライアンスをどのように展開するかによります。

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 モニター：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。

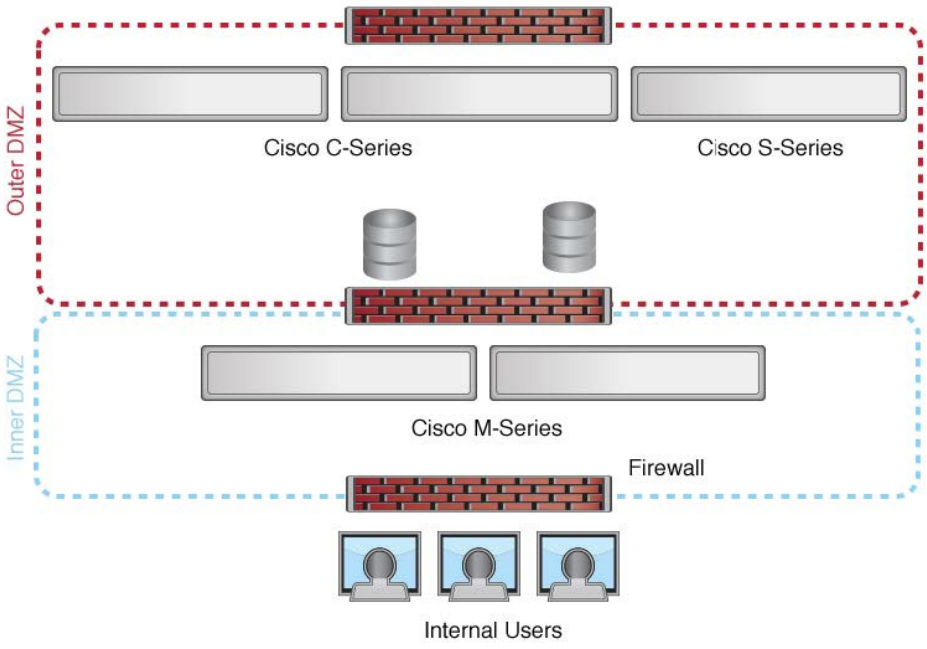
（注） アプライアンスの個々のポートの詳細については、「アプライアンスへの接続」を参照してください。

設置の計画



（注） 真のクライアント IP アドレスをモニターするため、L4 トラフィック モニターは必ず、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。

複数の Cisco Web セキュリティ アプライアンス（S シリーズ）または Cisco E メール セキュリティ アプライアンス（C シリーズ）を設置する場合は、以下のネットワーク図に示すように、それらを管理するためのシスコのコンテンツセキュリティ管理アプライアンス（M シリーズ）も使用することができます。



リモート アクセスのための IP アドレスの一時的な変更

ネットワーク接続を使用してアプライアンスをリモート操作で設定するには、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。

または、IP アドレスを変更せずにシリアル コンソールを使用してアプライアンスを設定できます。シリアルコンソールを使用する場合は、「アプライアンスへの接続」を参照してください。

Windows の IP アドレスの一時的な変更

（注） 正確な手順は、ご使用のオペレーティング システムのバージョンによって異なります。

ステップ 1 システムボックスに同梱されているクロスオーバーまたはイーサネットケーブルを使用して、ラップトップをプライマリ管理ポート（M1）に接続します。Cisco Web セキュリティ アプライアンスでは、M1 管理ポートのみを使用します。「設置の計画」を参照してください。

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 [次の IP アドレスを使用する（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 IP アドレスの一時的な変更

（注） 正確な手順は、ご使用のオペレーティング システムのバージョンによって異なります。

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 錠のアイコンをクリックして変更を許可します。

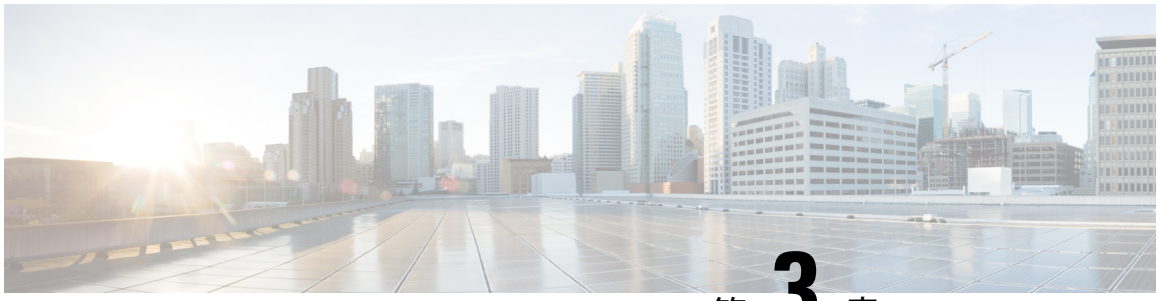
ステップ 4 緑色のアイコンがあるイーサネット ネットワーク構成を選択します。これが、アクティブな接続です。次に、[詳細（Advanced）] をクリックします。

ステップ 5 [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 6 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 7 [OK] をクリックします。



第 3 章

アプライアンスへの接続

アプライアンスをラックに取り付けたら、次の手順に従ってケーブルを接続し、電源を投入して、接続を確認します。

（注） 各トピックの接続図には、プライベートネットワークに接続された管理コンピュータを使用したデフォルト設定が示されています。実際の展開は、基本論理ネットワーク接続、ポート、アドレッシング、および設定要件によって異なります。

Cisco S196 Secure Web Appliance

ステップ 1 アプライアンスの背面パネルにある電源に、ストレート電源ケーブルの一方の端を差し込みます。

（注） 必要に応じて、冗長性を確保するために別途電源ケーブルを注文し、アプライアンスの背面パネルの 2 番目の電源に接続します。

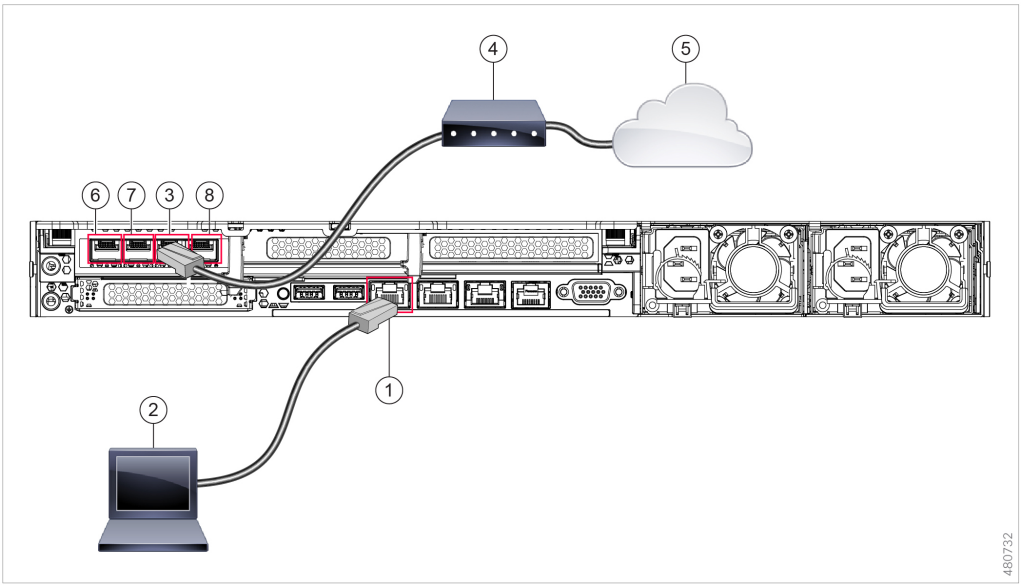
ステップ 2 もう一方の端を電源コンセントに差し込みます。

ステップ 3 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。

- プロキシポートは、P1 と P2 です。
  - 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ーポートは、T1 と T2 です。

- 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着信するすべてのパケットに対応します（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び発信トラフィックに対応します。

ステップ 4 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、ラップトップを管理ポート（M1）に接続します。



1	管理ポート（M1）-（192.168.42.42）	2	管理コンピュータ（192.68.42.43）
3	トラフィック モニタ ポート 1（T1）	4	WAN モデム
5	インターネット	6	プロキシポート 1（P1）
7	プロキシポート 2（P2）	8	トラフィックモニタポート 2（T2）

ステップ 5 アプライアンスの前面パネルにある電源スイッチを押して、アプライアンスに電源を投入します。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 10 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、前面パネルの緑色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。

注意 初期化の完了前に電源をオフにしてしまうと、その後アプライアンスが動作状態になることはなく、そのアプライアンスはシスコに返却する必要が生じます。

（注） アプライアンスに電源を接続した直後に電源を投入すると、アプライアンスの電源がオンになり、ファンが回転し LED がオンになります。30 ～ 60 秒以内にファンが停止し、すべての LED がオフになります。31 秒後にアプライアンスの電源がオンになります。この動作は、システム ファームウェアとコントローラが同期できるようにするための設計によるものです。

ステップ 6 設定の詳細については、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。

Cisco S396 Secure Web Appliance

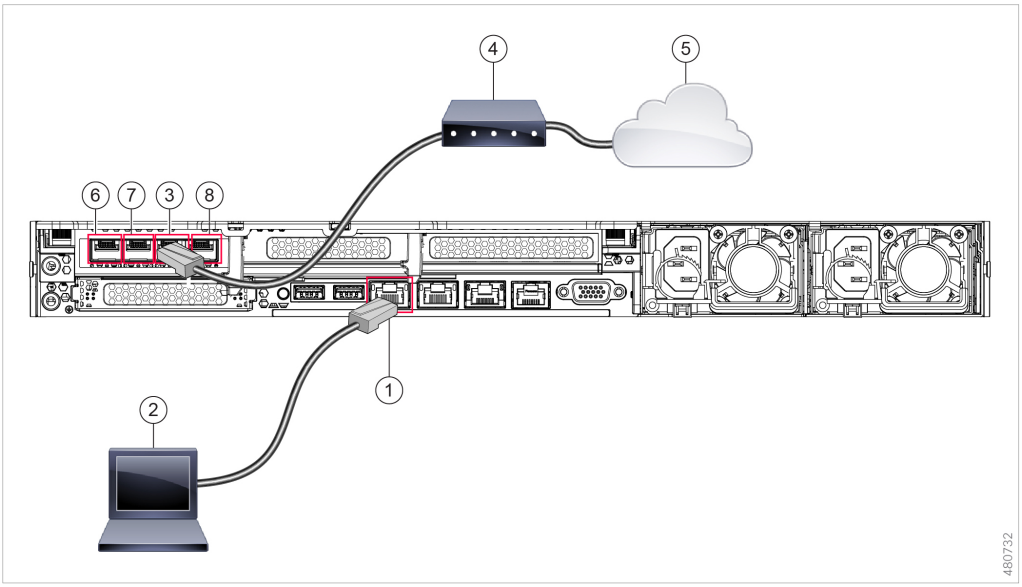
ステップ 1 アプライアンスの背面パネルにある冗長電源に、各ストレート電源ケーブルの一方の端を差し込みます。

ステップ 2 もう一方の端を電源コンセントに差し込みます。

ステップ 3 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。

- プロキシポートは、P1 と P2 です。
  - 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ーポートは、T1 と T2 です。
  - 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着信するすべてのパケットに対応します（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び発信トラフィックに対応します。

ステップ 4 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、ラップトップを管理ポートに接続します。S シリーズ アプライアンスでは、M1 管理ポートのみを使用します。



1	管理ポート（M1）-（192.168.42.42）	2	管理コンピュータ（192.168.42.43）
3	トラフィック モニタ ポート 1（T1）	4	WAN モデム
5	インターネット	6	プロキシポート 1（P1）
7	プロキシポート 2（P2）	8	トラフィックモニタポート 2（T2）

ステップ 5 アプライアンスの前面パネルにある電源スイッチを押して、アプライアンスに電源を投入します。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10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、前面パネルの緑色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。

注意 初期化の完了前に電源をオフにしてしまうと、その後アプライアンスが動作状態になることはなく、そのアプライアンスはシスコに返却する必要が生じます。

（注） アプライアンスに電源を接続した直後に電源を投入すると、アプライアンスの電源がオンになり、ファンが回転しLEDがオンになります。30～60秒以内にファンが停止し、すべてのLEDがオフになります。31秒後にアプライアンスの電源がオンになります。この動作は、システム ファームウェアとコントローラが同期できるようにするための設計によるものです。

ステップ 6 設定の詳細については、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。

Cisco S696 Secure Web Appliance

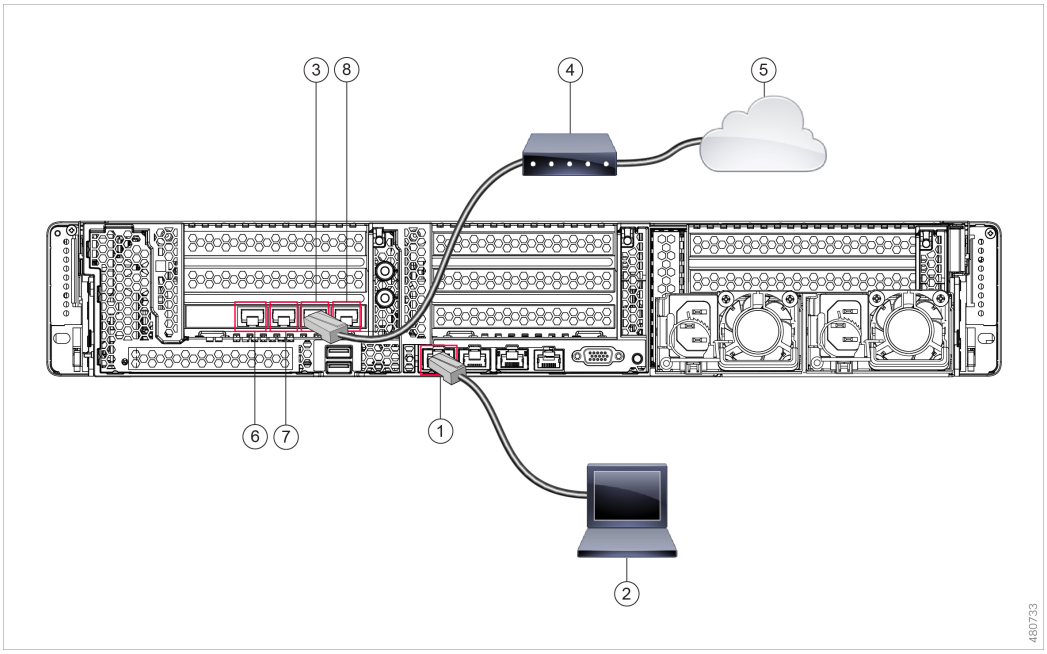
ステップ 1 アプライアンスの背面パネルにある冗長電源に、各ストレート電源ケーブルの一方の端を差し込みます。

ステップ 2 もう一方の端を電源コンセントに差し込みます。

ステップ 3 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。

- プロキシポートは、P1 と P2 です。
  - 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ーポートは、T1 と T2 です。
  - 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着信するすべてのパケットに対応します（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び発信トラフィックに対応します。

ステップ 4 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、ラップトップを管理ポートに接続します。



1	管理ポート（M1）-（192.168.42.42）	2	管理コンピュータ（192.168.42.43）
3	トラフィック モニタ ポート（T1）	4	WAN モデム
5	インターネット	6	プロキシポート 1（P1）
7	プロキシポート 2（P2）	8	トラフィックモニタポート 2（T2）

ステップ 5 アプライアンスの前面パネルにある電源スイッチを押して、アプライアンスに電源を投入します。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10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、前面パネルの緑色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。

注意 システムの電源投入が完了し LED が緑色に点灯するまで、少なくとも 10 分間待機してください。初期化の完了前に電源をオフにしてしまうと、その後アプライアンスが動作状態になることはなく、そのアプライアンスはシスコに返却する必要が生じます。

（注） アプライアンスに電源を接続した直後に電源を投入すると、アプライアンスの電源がオンになり、ファンが回転し LED がオンになります。30 ～ 60 秒以内にファンが停止し、すべての LED がオフになります。31 秒後にアプライアンスの電源がオンになります。この動作は、システム ファームウェアとコントローラが同期できるようにするための設計によるものです。

ステップ 6 設定の詳細については、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。

Cisco S696F Secure Web Appliance

次の図に、光ファイバ ポートが搭載された Cisco S696F モデルを示します。これらの光ファイバ ポートは、図に示すイーサネット ポート上にあり、イーサネット ポートは搭載されていません。詳細については、『Cisco x96 Secure Web Appliances Installation and Maintenance Guide』を参照してください。

上部の 2 つの光ファイバ ポートは、以下の表に記載されているイーサネット プロキシ ポートと同じようにプロキシ ポートとして使用されます。中央の 2 つの光ファイバ ポートはトラフィック ポートとして使用されます。下部の 2 つの光ファイバ ポートは管理ポートとして使用されます。

ステップ 1 アプライアンスの背面パネルにある冗長電源に、各ストレート電源ケーブルの一方の端を差し込みます。

ステップ 2 もう一方の端を電源コンセントに差し込みます。

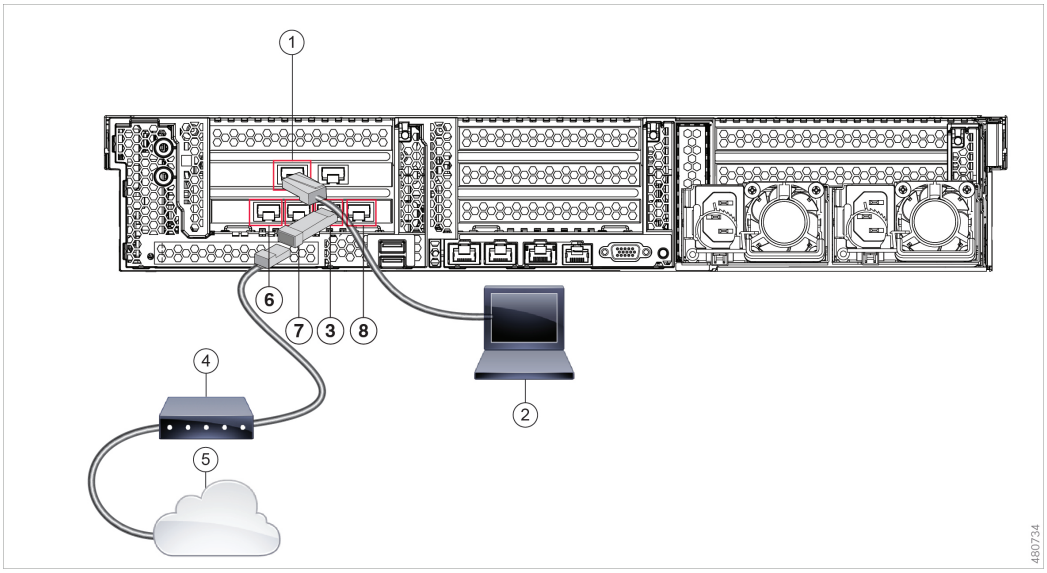
ステップ 3 アプライアンスの背面パネルにある適切なポートに、イーサネット ケーブルを差し込みます。

- プロキシポートは、P1 と P2 です。
  - 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ーポートは、T1 と T2 です。
  - 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着信するすべてのパケットに対応します（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び発信トラフィックに対応します。

ステップ 4 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、ラップトップを管理ポートに接続します。

注意 10 ギガビットの光ファイバ インターフェイスに付属するトランシーバ モジュールのみを使用します。他のトランシーバ モジュールの使用は、光ファイバ インターフェイス カードを損傷する恐れがあります。



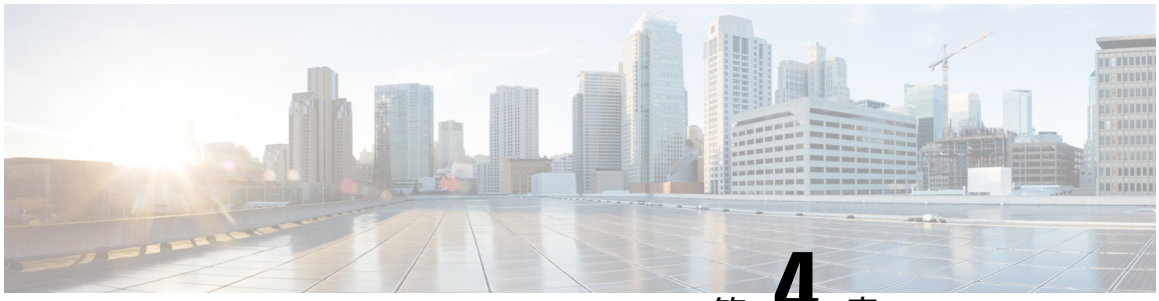
1	管理ポート（M1）-（192.168.42.42）	2	管理コンピュータ（192.168.42.43）
3	トラフィック モニタ ポート（T1）	4	WAN モデム
5	インターネット	6	プロキシポート 1（P1）
7	プロキシポート 2（P2）	8	トラフィックモニタポート 2（T2）

ステップ 5 アプライアンスの前面パネルにある電源スイッチを押して、アプライアンスに電源を投入します。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10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、前面パネルの緑色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。

注意 システムの電源投入が完了し LED が緑色に点灯するまで、少なくとも 10 分間待機してください。初期化の完了前に電源をオフにしてしまうと、その後アプライアンスが動作状態になることはなく、そのアプライアンスはシスコに返却する必要が生じます。

（注） アプライアンスに電源を接続した直後に電源を投入すると、アプライアンスの電源がオンになり、ファンが回転しLEDがオンになります。30～60秒以内にファンが停止し、すべてのLEDがオフになります。31秒後にアプライアンスの電源がオンになります。この動作は、システムファームウェアとコントローラが同期できるようにするための設計によるものです。

ステップ6 設定の詳細については、『*AsyncOS for Cisco Web Security Appliances User Guide*』を参照してください。



第 4 章

アプライアンスへのログイン

2 つのインターフェイス（Web インターフェイスまたは CLI）のいずれかを使用して Cisco Web セキュリティアプライアンスにログインできます。

Web インターフェイスを使用したアプライアンスへのログイン

ステップ 1 イーサネットポートを通じた Web ブラウザアクセスについては（「アプライアンスへの接続」を参照）、Web ブラウザで以下の URL 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。

https://10.10.193.32:8443/

ステップ 2 以下のログイン情報を入力します。

- ユーザー名：**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:8443）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 サーバー データベースに追加する必要があります。

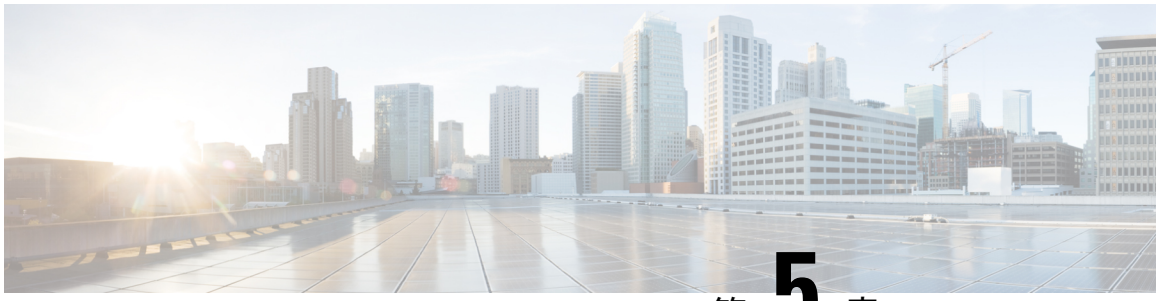
ステップ 3 [ログイン（Login）] をクリックします。

CLI を使用したアプライアンスへのログイン

ステップ 1 CLI にローカルか、またはリモートでアクセスします。

- CLI にローカルでアクセスするには、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**）で端末がシリアル ポートに接続するように設定し、フロー制御を Hardware に設定します。端末を物理的に接続するには、「アプライアンスへの接続」を参照してください。
- CLI にリモートでアクセスするには、IP アドレス **192.168.42.42** との SSH セッションを開始します。

ステップ 2 パスワード **ironport** を使用して **admin** としてログインします。



第 5 章

System Setup ウィザードの実行

System Setup ウィザードの実行

始める前に

- システム セットアップ ウィザードを実行する前に、スマートライセンスを有効にして登録します。詳細については、「Smart Software Licensing」を参照してください。

システム セットアップ ウィザードを実行して、基本的な設定を行い、システム デフォルトを有効にします。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通じ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（EULA）が表示されます。

ステップ 1 エンド ユーザー ライセンス契約書に同意します。

ステップ 2 「ネットワーク設定の記録」から情報を入力します。

この設定に関する追加情報が必要な場合は、[ヘルプとサポート（Help and Support）] > [オンラインヘルプ（Online Help）]を選択してください。

ステップ 3 設定サマリー ページを確認します。

ステップ 4 [この設定をインストール（Install This Configuration）] をクリックします。

ステップ 5 アプライアンスが設定を受け入れていないかまたはインストールが行われていないように見えることがあります。これは、IP アドレスを変更したものの、インストールがまだ途中であるためです。

ステップ 6 前述の説明に従ってコンピュータの IP アドレスを一時的に変更した場合は、IP アドレスを元の設定に戻します。

ステップ 7 コンピュータとアプライアンスがネットワークに接続されていることを確認します。

ステップ 8 「設置の計画」でメモしたホスト名または IP アドレスでアプライアンスに再度ログインします。ユーザー名 **admin** と、ウィザードに入力した新しいパスワードを使用します。

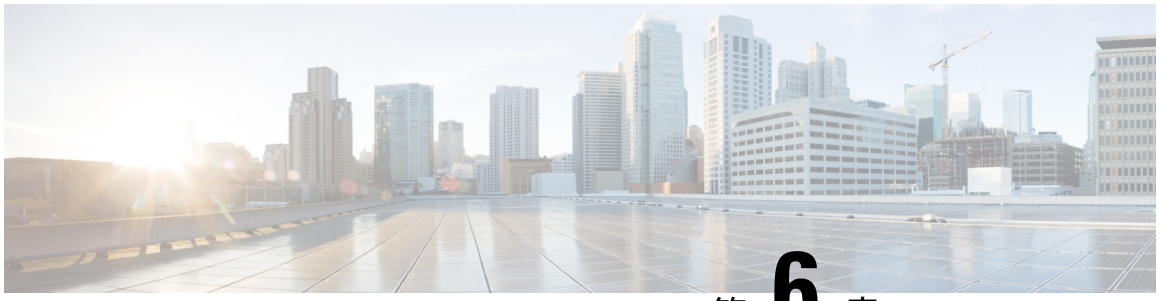
Cisco Web セキュリティアプライアンスでは自己署名証明書が使用され、Web ブラウザから警告がトリガーされる可能性があります。証明書を受け入れ、この警告を無視します。

ステップ 9 管理者パスワードを安全な場所に保管してください。

利用可能なアップグレードの確認

アプライアンスにログインした後で、Web ブラウザ ウィンドウの上部でアップグレード通知（または CLI で通知）があるかどうかを確認してください。アップグレードが適用可能な場合は、アップグレードをインストールする必要があるかどうかを検討します。

各リリースの詳細情報は、AsyncOS バージョンのリリース ノートに記載されています。



第 6 章

ネットワークの設定

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

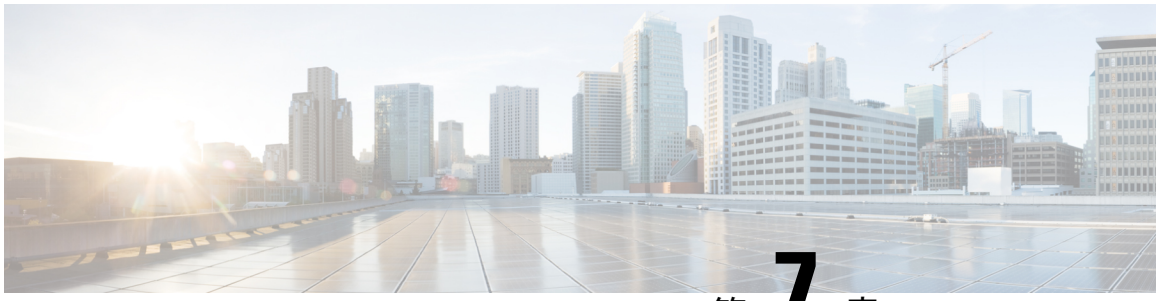
（注） ポート 80 および 443 を開いておかないと、機能キーをダウンロードできません。

詳細については、Cisco Web セキュリティ アプライアンスのご使用の AsyncOS バージョンに関するユーザー ガイドでファイアウォール情報を参照してください。

設定の概要

項目	説明
管理	https://192.168.42.42:8443 と入力するか、システム セットアップ ウィザードを実行した後で管理インターフェイスに割り当てられる IP アドレスを使用して、管理ポートから Web セキュリティアプライアンスを管理できます。 （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、管理ポート（https://192.168.42.42:8443）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、必ず管理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。
データ	システム セットアップ ウィザードを実行した後は、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、アプライアンス上の少なくとも 1 つのポート、つまり M1 のみ、M1 と P1、M1、P1、および P2、P1 のみ、または P1 と P2 が設定されます。 （注） Web プロキシを明示的な転送モードで設定した場合は、データ用に設定された IP アドレス、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。

項目	説明
トラフィック モニター	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 モニター 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 モニターのデフォルト設定は、モニターのみです。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ーおよびブロックの両方を行うよう、L4 トラフィック モニターを設定できます。
コンピュータ アドレス	コンピュータの IP アドレスを、「リモート アクセスのための IP アドレスの一時的な変更」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は、[システム管理（System Administration）] > [設定サマリ（Configuration Summary）]のページから確認できます。



第 7 章

その他の設定

次のトピックでは、アプライアンスで設定できるいくつかの追加機能について説明します。詳細については、ご使用のリリースの AsyncOS のオンライン ヘルプまたはユーザー ガイドを参照してください。

ユーザー ポリシー

Web インターフェイスを使用し、必要に応じて、どのユーザーがどの 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。

- ユーザーの識別：インターネットにアクセスできるユーザー グループを定義するには、[Web セキュリティマネージャ（Web Security Manager）]>[アイデンティティ（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、モニターまたは拒否する 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ーのアクセスを制御するには、[Web セキュリティマネージャ（Web Security Manager）]>[アクセスポリシー（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。

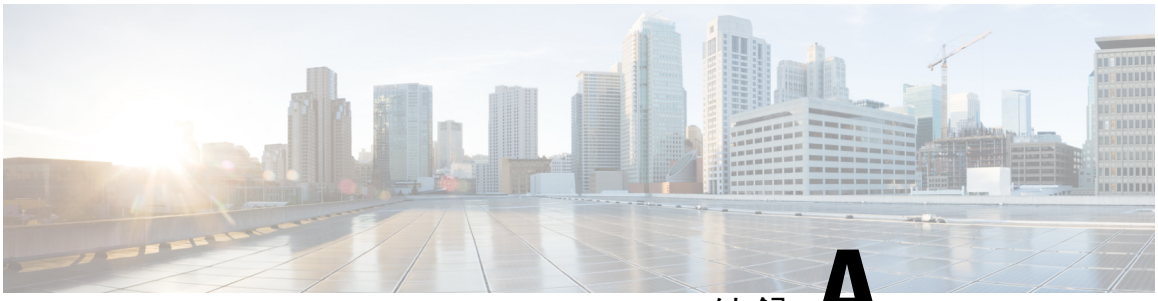
Cisco Web セキュリティアプライアンスの設定ポリシーについては、『*AsyncOS for Cisco Web Security Appliances User Guide*』の「Working with Policies」の章を参照してください。

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ーされる 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。

詳細情報

その他にも、Cisco Web セキュリティ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、エンドユーザーの通知、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 Web Security Appliance S196, S396, S696, and S696F』を参照してください。



付録 A

その他の情報

関連資料

サポート	
Cisco サポート ポータル	http://www.cisco.com/support
米国およびカナダの無料通話番号	800-553-2447
International Contacts	各国の電話番号
電子メール：	tac@cisco.com
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 Secure Web Appliance スタートアップガイド（本マニュアル）	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
Cisco Secure Web Appliances Installation and Maintenance Guide LED、技術仕様、およびマウントオプションに関する情報が含まれています。	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
Cisco Web セキュリティ アプライアンスのマニュアルには、 リリース ノート、CLIリファレンス、および設定用のガイドが含まれています。	http://www.cisco.com/en/US/customer/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	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
MIB	
Cisco Web セキュリティ アプライアンス向け AsyncOS MIB（関連ツールセクション）	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェア アップデートと既知の問題に関する情報などの Cisco コンテンツ セキュリティ アプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、http://www.cisco.com/cisco/support/notifications.html に移動します。

Cisco.com アカウントが必要です。お持ちでない場合は、https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui で登録してください。

翻訳について
このドキュメントは、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。