Cisco S390 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

- ウェルカム
- はじめる前に
- ネットワーク設定の記録
- 設置の計画
- ラックへのアプライアンスの取り付け
- アプライアンスへの電源接続
- リモート アクセスのための IP アドレスの一時的な変更
- アプライアンスへの接続
- アプライアンスの電源投入
- アプライアンスへのログイン
- システム セットアップ ウィザードの実行
- 利用可能なアップグレードの確認
- ネットワークの設定
- 設定サマリ
- 追加設定
- 関連資料
- Cisco 通知サービス

Cisco Systems, Inc.
www.cisco.com

ウェルカム

Cisco S390 Web セキュリティ アプライアンス(WSA)をお選びいただきありがとうございます。Web セキュリティ アプライアンスは、組織によるWeb トラフィックの保護と制御を支援します。

このマニュアルでは、S390 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アプライアンスの基本設定を行う方法を説明します。また、アプライアンスの設定方法については、『*AsyncOS for Cisco Web Security Appliances User Guide*』の章「Deployment」を参照してください。

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。以下のアイテムが含まれています:
Cisco S390 Web セキュリティ アプライアンス:

- スライド レール キット
- 電源ケーブル(2)
- 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
- コンピュータをコンソール ポートに接続するための RJ45 - DB9 ケーブル
- Cisco コンテンツ セキュリティ ドキュメントのポインタ カード

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)
- 10/100/1000 Base-TX 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)のネットワークおよび管理者の情報

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 との透過** • **WCCP ルータとの透過スイッチ** • **明示的フォワードプロキシ**	L4 トラフィック モニタ: • 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（Network Settings）	
デフォルトのシステムホスト名:（Default System Hostname:）	
DNS サーバ:	インターネットのルート DNS サーバを使用。 DNS サーバを使用（最大 3 台）: 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) • 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)
ロック型前面プレート	
4 桁のコード(S690-LKFP アプライアンスの場合)	

設置の計画

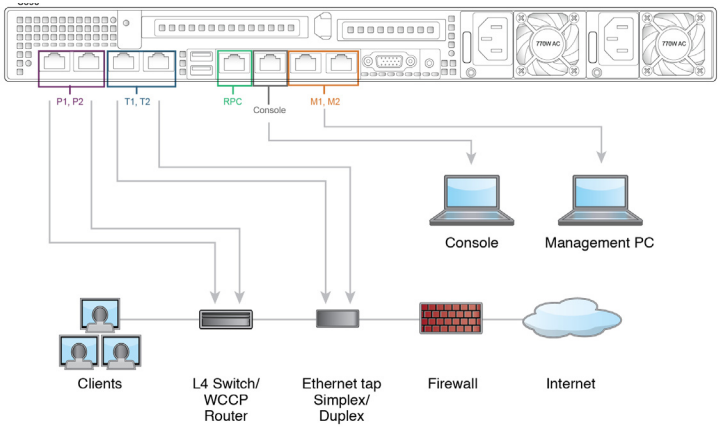
ネットワーク内にどのように Cisco S390 Web セキュリティ アプライアンスを設定するかを決定します。

Cisco S390 は一般的に、クライアントとインターネット間のネットワークに追加のレイヤとして設置されます。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。

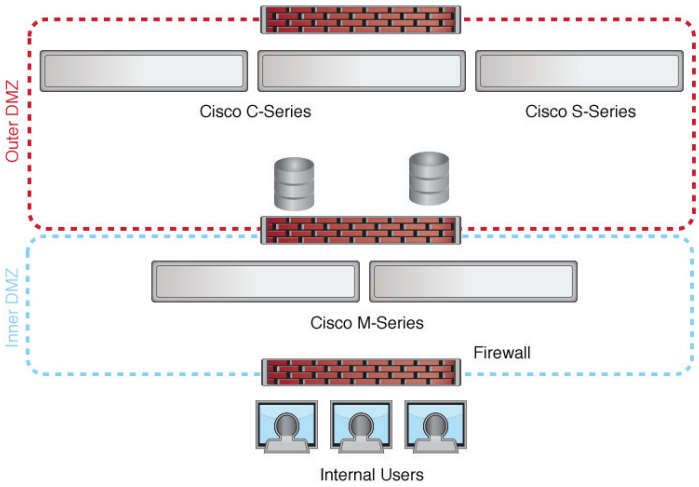
- 透過プロキシ:L4 スイッチを使用する Web プロキシ
- 透過プロキシ:WCCP ルータを使用する Web プロキシ

- 明示的フォワードプロキシ:ネットワーク スイッチに接続
- 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。

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 電子メール セキュリティ アプライアンス(Cシリーズ)を取り付ける場合は、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 Cisco 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。



ラックへのアプライアンスの取り付け

付属のスライド レールを使用して、Cisco S390 Web セキュリティ アプライアンスを取り付けます。ラックへのアプライアンスの取り付けの詳細については、『*Cisco x90 Series Content Security Appliances Installation and Maintenance 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 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。

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冗長電源に、各ストレート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。

リモート アクセスのための IP アドレスの一時的な変更

ネットワーク設定を使用して Cisco S390 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。あるいは、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 Cisco S390 を設定できます。シリアル コンソールを使用する場合は、以下のセクション 8 に進みます。

(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、ラップトップを管理ポートに接続します。Cisco S390 アプライアンスでは、管理ポートのみを使用します。「設置の計画」セクション(6 ページ)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 [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 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。

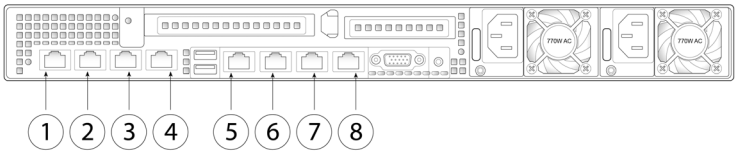
- IP アドレス:**192.168.42.43**
- サブネット マスク:**255.255.255.0**
- ルータ:**192.168.42.1**

ステップ 7 [OK] をクリックします。

アプライアンスへの接続

Cisco S390 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び発信トラフィックに対応。
- 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。



項目	[ポート（Port）]	説明
1	プロキシ ポート 1	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プロキシ ポート P1 を接続します。
2	プロキシ ポート 2	P1 と P2 の両方のプロキシ ポートが有効である場合、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。P1 および P2 は、L4 スイッチ、WCCP ルータ、またはネットワーク スイッチに接続できます。
3	トラフィック モニタ ポート 1	デュプレックス イーサネット タップ用のトラフィック モニタ 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。
4	トラフィック モニタ ポート 2	シンプレックス イーサネット タップ用のトラフィック モニタ ポート: 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します（T2）。
5	リモートからの電源の再投入	このポートはリモートからの電源の再投入（RPC）に使用されます。
6	コンソール	アプライアンスに直接コンピュータを接続するコンソール ポートを示します。
7	管理インターフェイス 1	管理使用のみに限定されるギガビット イーサネット インターフェイスを示します。
8	管理インターフェイス 2	セカンダリ管理ポートこのギガビット イーサネット インターフェイスは使用できません。

アプライアンスの電源投入

Cisco S390 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。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、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。

（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。

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。

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 S390 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」セクション（11 ページ）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。

http://192.168.42.42:8080

ステップ 2　以下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 インターフェイス（CLI）にローカル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」セクション（11 ページ）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。

ステップ 3　プロンプトで、systemsetup コマンドを実行します。

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 ベースの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（EULA とも呼ばれる）が表示されます。

ステップ 1 エンド ユーザ 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」セクション（3 ページ）からの情報を入力します。

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 ラップトップとアプライアンスがネットワークに接続していることを確認します。

ステップ 8 「設置の計画」セクション（6 ページ）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 M390 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、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、この警告は無視できます。

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（またはコマンドライン インターフェイスで通知）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。

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。

設定サマリ

項目	説明
管理	http://192.168.42.42:8080 と入力して、管理ポート（Management Port）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、管理ポート（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。

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、「リモート アクセスのための 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。 **(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。

追加設定

これですべての作業は完了しました。インストールと基本的な設定が完了したため、の使用を開始できます。
Cisco S390 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 S390 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*』の章「Working with Policies」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 S390 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 S390 Web セキュリティ アプライアンス』を参照してください。

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	各国の連絡先
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 S390Web 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/S390_QSG.pdf
『*Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*』には、 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/wsa/hw/Sx90_Series_HW_Install.pdf

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	http://www.cisco.com/en/US/docs/security/content_security/compliance/ContentSecurity_regulatory_compliance_information.fm
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

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。Cisco.com ID をお持ちでない場合は、https://tools.cisco.com/RPF/register/register.do [英語] で登録を行ってください。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks ご確認いただけます。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 年 Cisco Systems, Inc. All rights reserved.