IPインターフェイスおよびアプライアンスへのアクセス

この章は、次の項で構成されています。

IP インターフェイスおよびアプライアンスへのアクセス

Cisco コンテンツ セキュリティ アプライアンスで作成する任意の IP インターフェイスには、さまざまなサービスを通してアクセスできます。

デフォルトでは、各インターフェイスに対して次のサービスがイネーブルまたはディセーブルに設定されています。

表 *1 : IP* インターフェイスに対してデフォルトでイネーブルになるサービス

		デフォルトでイネーブルかどうか	
サービス	デフォルトポート	管理インターフェイス	新規作成された IP インターフェイス
FTP	21	[いいえ（No）]	[いいえ（No）]
Telnet	23	[はい（Yes）]	[いいえ（No）]
SSH	22	[はい（Yes）]	[いいえ（No）]
HTTP	80	[はい（Yes）]	[いいえ（No）]
HTTPS	443	[はい（Yes）]	[いいえ（No）]

IP インターフェイス

IPインターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1 つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IPインターフェイス経由でのスパム隔離へのアクセスも設定できます。電子メール配信および仮想ゲートウェイの場合、各 IP インターフェイスは特定の IP アドレスおよびホスト名を持つ1つの仮想ゲートウェイアドレスとして機能します。インターフェイスを独立したグループに（CLI を使用して）「参加」させることもできます。システムは、電子メールの配信時にこれらのグループを順番に使用します。仮想ゲートウェイへの参加またはグループ化は、複数のインターフェイス間で大規模な電子メールキャンペーンをロードバランシングするのに役立ちます。VLAN を作成し、他のインターフェイスと同様に（CLI を使用して）設定することもできます。詳細については、お使いの E メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプの「Advanced Networking」の章を参照してください。

IP インターフェイスの設定

[管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページ（および interface config コマンド）では、IP インターフェイスを追加、編集、または削除できます。

（注） セキュリティ管理アプライアンス上の管理インターフェイスに関連付けられた名前またはイーサネットポートを変更することはできません。さらに、セキュリティ管理アプライアンスは後述のすべての機能をサポートしているわけではありません（たとえば、Virtual Gateway）。

IP インターフェイスを設定する場合は、次の情報が必要です。

表 *2: IP* インターフェイス コンポーネント

[名前（Name）]	**インターフェイスのニックネーム。**
IP アドレス	同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。
ネットマスク（サブネットマスク）	ネットマスクを標準のドット付きオクテット形式（たとえば、255.255.255.0）または 16 進形式（たとえば、0xffffff00）で入力できます。デフォルトのネットマスクは 255.255.255.0、一般的なクラス C 値です。
ブロードキャスト アドレス	AsyncOS はデフォルトのブロードキャストアドレスを IP アドレスおよびネットマスクから自動的に計算します。

[名前（Name）]	インターフェイスのニックネーム。
ホストネーム	インターフェイスに関連するホスト名。ホスト名は、SMTP カンバセーション中のサーバの特定に使用されます。各 IP アドレスに関連付けられた有効なホスト名を入力する必要があります。ソフトウェアは、DNS によってホスト名が一致する IP アドレスに正しく変換されたり、または逆引き DNS によって所定のホスト名が変換されることをチェックしません。
許可されるサービス	FTP、SSH、Telnet、スパム隔離、HTTP、および HTTPS はインターフェイス上で有効または無効にできます。サービスごとにポートを設定できます。スパム隔離の HTTP/HTTPS、ポート、および URL も設定できます。

（注） セットアップ、インストール、および基本設定の説明に従ってシステムセットアップウィザードを完了し、変更を保存している場合は、アプライアンス上に管理インターフェイスがすでに設定されているはずです。

GUI を使用した IP インターフェイスの作成

ステップ 1 [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] を選択します。

ステップ 2 [IPインターフェイスの追加（Add IP Interface）] をクリックします。

ステップ 3 インターフェイスの名前を入力します。

ステップ 4 イーサネット ポートを選択し、IP アドレスを入力します。

ステップ 5 IP アドレスに対応するネットマスクを入力します。

ステップ 6 インターフェイスのホスト名を入力します。

ステップ 7 この IP インターフェイス上でイネーブルにする各サービスの横にあるチェックボックスをオンにします。必要に応じて、対応するポートを変更します。

ステップ 8 アプライアンス管理用にインターフェイスで HTTP から HTTPS へのリダイレクトをイネーブルにするかどうかを選択します。

ステップ 9 スパム隔離を使用している場合は、HTTP、HTTPS、またはその両方を選択し、それぞれにポート番号を指定できます。HTTP 要求を HTTPS にリダイレクトするかどうかも選択できます。最後に、IP インターフェイスをスパム隔離のデフォルトインターフェイスにするかどうか、ホスト名を URL として使用するかどうか、およびカスタム URL を指定するかどうかを指定できます。

ステップ 10 変更を送信し、保存します。

FTP 経由でのアプライアンスへのアクセス

⚠

注意 [管理アプライアンス（Management Appliance）]>[ネットワーク（Network）]>[IPインターフェイス（IP Interfaces）]ページまたはinterfaceconfigコマンドからサービスをディセーブルにすることにより、アプライアンスへの接続方法に応じて、GUIまたはCLIから切断できます。別のプロトコル、シリアルインターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。

ステップ 1 [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] ページ（または `interfaceconfig` コマンド）を選択して、インターフェイスに対して FTP アクセスを有効にします。

（注） 次のステップに移る前に、変更を保存することを忘れないでください。

ステップ 2 FTP経由でインターフェイスにアクセスします。インターフェイスに対して正しいIPアドレスを使用していることを確認します。

例：`ftp 192.168.42.42`

ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。

例：`ftp://192.10.10.10`

ステップ 3 実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照し、ファイルをコピーおよび追加（「`GET`」および「`PUT`」）できます。次の表を参照してください。

IP インターフェイスおよびアプライアンスへのアクセス

表 *3:* アクセスできるディレクトリ

ディレクトリ名	説明
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] ページまたは、logconfig および rollovernow コマンドを使用したロギング用に、自動的に作成されます。各ログの詳しい説明については、お使いの E メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプの「Logging」の章を参照してください。 各ログ ファイル タイプの違いについては、「Logging」の章の「Log File Type Comparison」を参照してください。
/configuration	次のページおよびコマンドからのデータのエクスポート先ディレクトリ、またはインポート元（保存）ディレクトリ。 • Virtual Gateway マッピング（altsrchost） • XML 形式の設定データ（saveconfig、loadconfig） • [ホストアクセステーブル（HAT）（Host Access Table (HAT)）] ページ（hostaccess） • [受信者アクセステーブル（RAT）（Recipient Access Table (RAT)）] ページ（rcptaccess） • [SMTPルート（SMTP Routes）] ページ（smtproutes） • エイリアス テーブル（aliasconfig） • マスカレード テーブル（masquerade） • メッセージ フィルタ（filters） • グローバル配信停止データ（unsubscribe） • trace コマンドのテスト メッセージ
/MFM	メール フロー モニタリング データベース ディレクトリには、GUI から使用できるメール フロー モニタ機能のデータが含まれます。各サブディレクトリには、各ファイルのレコード形式を文書化した README ファイルが含まれます。 記録を残すためにこれらのファイルを異なるマシンにコピーしたり、ファイルをデータベースにロードして独自の分析アプリケーションを作成したりできます。レコード形式は、すべてのディレクトリ内にあるすべてのファイルで同じです。この形式は今後のリリースで変更される場合があります。
/periodic_reports	システムで設定されているすべてのアーカイブ済みレポートが保管されます。

ステップ 4 ご使用の FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

セキュア コピー（scp）アクセス

クライアント オペレーティング システムでセキュア コピー（scp）コマンドがサポートされている場合は、表「アクセスできるディレクトリ」に示すディレクトリ間でファイルをコピーできます。たとえば、次の例ではファイル /tmp/test.txt はクライアント マシンからホスト名「mail3.example.com」のアプライアンスの設定ディレクトリにコピーされます。

（注） このコマンドでは、ユーザ（admin）のパスワードを求めるプロンプトが表示されます。この例は参考用です。オペレーティング システムの secure copy の実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************|  1007       00:00
%
```

この例では、同じファイルがアプライアンスからクライアント マシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's password: (type the password)
test.txt             100% |***************************|  1007       00:00
```

コンテンツ セキュリティ アプライアンスに対するファイルの転送および取得には、セキュア コピー（scp）を FTP に代わる方法として使用できます。

（注） operators グループおよび administrators グループのユーザのみが、アプライアンスへのアクセスにセキュア コピー（scp）を使用できます。詳細については、AsyncOS の以前のバージョンへの復元についてを参照してください。

シリアル接続によるアクセス

シリアル接続を介してアプライアンスに接続する場合は、コンソール ポートに関する次の情報を使用します。

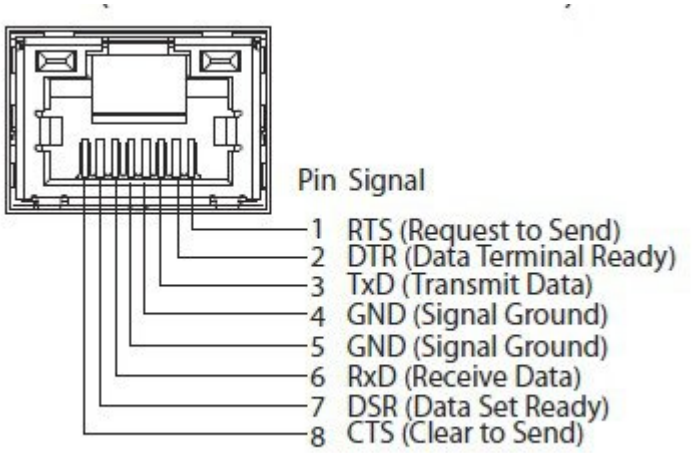
このポートの詳細については、アプライアンスのハードウェア インストール ガイドを参照してください。

関連項目

- 資料

80 および 90 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細

図 *1 : 80* および *90* シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細



70 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細

次の図はシリアル ポート コネクタのピン番号を示しています。またシリアル ポートのピン割り当ての表では、シリアル ポート コネクタのピン割り当てとインターフェイス信号を定義しています。

図 *2 :* シリアル ポートのピン番号

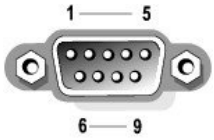


表 *4 :* シリアル ポートのピン割り当て

ピン	信号（Signal）	I/O	定義（Definition）
1	DCD		データ キャリア検出
2	SIN		シリアル入力
3	SOUT		シリアル出力
4	DTR		データ ターミナル レディ

IP インターフェイスおよびアプライアンスへのアクセス

ピン	信号（Signal）	I/O	定義（Definition）
5	GND	適用対象外	信号アース
[6]	DSR		データ セット レディ
7	RTS		送信要求
8	CTS		送信可
9	RI		リング インジケータ
シェル	適用対象外	適用対象外	シャーシ アース