



FTP、SSH、および SCP アクセス

この付録の構成は、次のとおりです。

- [IP インターフェイス](#) (1 ページ)
- [電子メールゲートウェイへの FTP アクセスの設定](#) (2 ページ)
- [セキュア コピー \(scp\) アクセス](#) (4 ページ)
- [シリアル接続経由での 電子メールゲートウェイへのアクセス](#) (5 ページ)

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 インターフェイスまたは両方にインターネット プロトコルバージョン 4 (IPv4) または IP Version 6 (IPv6) を割り当てることができます。

表 1: 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

		デフォルトで有効かどうか	
サービス	デフォルト ポート	管理インターフェイス ¹	新規作成されたインターフェイス
FTP	21	×	×
SSH	22	対応	×
HTTP	80	対応	×
HTTPS	443	対応	×

¹ ここに示す「管理インターフェイス」の設定は、Cisco C170 電子メールゲートウェイの Data 1 インターフェイスのデフォルト設定でもあります。

- グラフィカル ユーザ インターフェイス (GUI) を使用して電子メールゲートウェイにアクセスする必要がある場合は、インターフェイスで HTTP、HTTPS、またはその両方をイネーブルにする必要があります。

- 設定ファイルのアップロードまたはダウンロードを目的として電子メールゲートウェイにアクセスする必要がある場合は、インターフェイスで FTP をイネーブルにする必要があります。
- Secure Copy (scp) を使用しても、ファイルをアップロードまたはダウンロードできます。

IP インターフェイス経由のスパム隔離への HTTP または HTTPS アクセスを設定できます。

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。

仮想ゲートウェイの参加またはグループ化は、大規模な電子メールキャンペーンを複数のインターフェイス間でロード バランシングする際に役立ちます。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、[高度なネットワーク構成](#)を参照してください。

関連項目

- [AsynOS によるデフォルト IP インターフェイスの選択方法 \(2 ページ\)](#)

AsynOS によるデフォルト IP インターフェイスの選択方法

AsynOS は、[ネットワーク (Network)]>[IP インターフェイス (IP Interfaces)] ページまたは `ifconfig` CLI コマンドで表示された最も小さな番号の IP アドレスに基づいてデフォルト IP インターフェイスを選択します。当該のサブネット上に存在するリストの最初の IP インターフェイスが使用されます。

同一サブネット内で複数の IP アドレスがデフォルトゲートウェイとして設定されている場合、最も小さな番号の IP アドレスが使用されます。たとえば、次の IP アドレスが同一サブネット内で設定されているとします。

- 10.10.10.2/24
- 10.10.10.30/24
- 10.10.10.100/24
- 10.10.10.105/24

AsynOS はデフォルトの IP インターフェイスとして 10.10.10.2/24 を選択します。

電子メールゲートウェイへの FTP アクセスの設定

手順

- ステップ 1** [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` コマンドを使用して、インターフェイスに対して FTP アクセスをイネーブルにします。

危険 サービスを `interfaceconfig` コマンドでディセーブルにすると、CLI との接続が解除されることがあります。これは、電子メールゲートウェイにどのように接続しているかによって異なります。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電子メールゲートウェイ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 2 変更を送信し、保存します。

ステップ 3 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。次に例を示します。

```
§ ftp 192.168.42.42
```

(注) 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。

ステップ 4 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。

ディレクトリ名	説明
/configuration	<p>以下のコマンドからのデータがこのディレクトリにエクスポートされるか、このディレクトリからデータがインポート（保存）されます。</p> <ul style="list-style-type: none"> • Virtual Gateway マッピング (<code>altsrghost</code>) • XML 形式の設定データ (<code>saveconfig</code>、<code>loadconfig</code>) • ホスト アクセス テーブル (HAT) (<code>hostaccess</code>) • 受信者アクセス テーブル (RAT) (<code>rcptaccess</code>) • SMTP ルート エントリ (<code>smtproutes</code>) • エイリアス テーブル (<code>aliasconfig</code>) • マスカレード テーブル (<code>masquerade</code>) • メッセージフィルタ (<code>filters</code>) • グローバル配信停止データ (<code>unsubscribe</code>) • <code>trace</code> コマンドのテスト メッセージ • セーフリスト/ブロックリストバックアップ ファイル (<code>sbl<タイムスタンプ><シリアル番号>.csv</code> 形式で保存)
/antivirus	<p>Anti-Virus エンジンのログ ファイルが保存されるディレクトリです。このディレクトリにあるログ ファイルを検査して、ウイルス定義ファイル (<code>scan.dat</code>) の成功した最終ダウンロードを手動で確認できます。</p>

ディレクトリ名	説明
/configuration	logconfig コマンドと rollovernow コマンドを使用する ロギング 用に自動的に作成されます。各ログの詳細については、 ログ を参照してください。
/system_logs	
/cli_logs	ログ ファイル タイプの違いについては、「 ログ ファイル タイプの比較 」を参照してください。
/status	
/reportd_logs	
reportqueryd_logs	
/ftpd_logs	
/mail_logs	
/asarchive	
/bounces	
/error_logs	
/avarchive	
/gui_logs	
/sntpd_logs	
/RAID.output	
/euq_logs	
/scanning	
/antispam	
/antivirus	
/euqgui_logs	
/ipmitool.output	

ステップ 5 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 **secure copy (scp)** コマンドをサポートしている場合は、前述の表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が `mail3.example.com` の電子メールゲートウェイの `configuration` ディレクトリにコピーされます。

コマンドを実行すると、ユーザ (`admin`) のパスワードを求めるプロンプトが表示されることに注意してください。この例を参考用としてだけ示します。特殊な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 passphrase: (type the passphrase)
```

```
test.txt 100% |*****| 1007 00:00
```

```
%
```

この例では、同じファイルが電子メールゲートウェイ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 passphrase: (type the passphrase)
```

```
test.txt 100% |*****| 1007 00:00
```

```
%
```

電子メールゲートウェイ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。



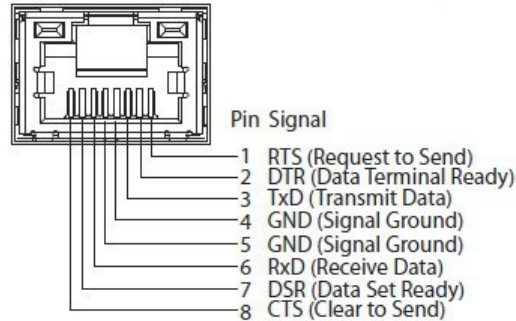
(注) operators グループおよび administrators グループのユーザのみが、電子メールゲートウェイへのアクセスにセキュアコピー (scp) を使用できます。詳細については、[ユーザの追加](#)を参照してください。

シリアル接続経由での電子メールゲートウェイへのアクセス

シリアル接続を介して電子メールゲートウェイに接続する場合は、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。

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

次の図に、シリアルポートコネクタのピン番号を示し、以下の表で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ます。

図 1: シリアルポートのピン番号

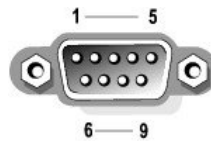


表 2: シリアルポートのピン割り当て

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
5	GND	適用対象外	信号用接地
6	DSR		データ セット レディ
7	RTS		送信要求
8	CTS		送信可

ピン	信号 (Signal)	I/O	定義 (Definition)
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

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。