# 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

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 [1] | 新規作成されたインターフェイス |
| FTP | 21 | [いいえ（No）] | [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）] |

[1] ここに示す「管理インターフェイス」の設定は、Cisco C170 および アプライアンスの 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）を使用してアプライアンス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アプライアンス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では、各 IP インターフェイスが特定の 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 アドレスとして動作します。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、次を参照してください。 高度なネットワーク構成

# AsynOS によるデフォルト IP インターフェイスの選択方法

AsyncOS 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`

AsyncOS 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。

# E メール セキュリティ アプライアンスへの FTP アクセスの設定

**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、アプライアンスにどのように接続しているかによって異なります。管理ポートで別のプロトコル、シリアル インターフェイス、または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 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 | 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。<br>• Virtual Gateway マッピング（`altsrchost`）<br>• XML 形式の設定データ（`saveconfig`、`loadconfig`）<br>• ホスト アクセス テーブル（HAT）（`hostaccess`）<br>• 受信者アクセス テーブル（RAT）（`rcptaccess`）<br>• SMTP ルート エントリ（`smtproutes`）<br>• エイリアス テーブル（`aliasconfig`）<br>• マスカレード テーブル（`masquerade`）<br>• メッセージ フィルタ（`filters`）<br>• グローバル配信停止データ（`unsubscribe`）<br>• `trace` コマンドのテスト メッセージ<br>• セーフリスト/ブロックリスト バックアップ ファイル（*slbl*<タイムスタンプ><シリアル番号>*.csv* 形式で保存） |
| /antivirus | 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（`scan.dat`）の成功した最終ダウンロードを手動で確認できます。 |

| ディレクトリ名 | 説明 |
|---|---|
| /configuration<br>/system_logs<br>/cli_logs<br>/status<br>/reportd_logs<br>reportqueryd_logs<br>/ftpd_logs<br>/mail_logs<br>/asarchive<br>/bounces<br>/error_logs<br>/avarchive<br>/gui_logs<br>/sntpd_logs<br>/RAID.output<br>/euq_logs<br>/scanning<br>/antispam<br>/antivirus<br>/euqgui_logs<br>/ipmitool.output | `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。<br>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。 |

**ステップ 5** 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` のアプライアンスの 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）のパスフレーズ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 passphrase: (type the passphrase)
test.txt 100% |***************************| 1007 00:00
%
```

Cisco 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、secure copy（scp）を FTP に代わる方法として使用できます。

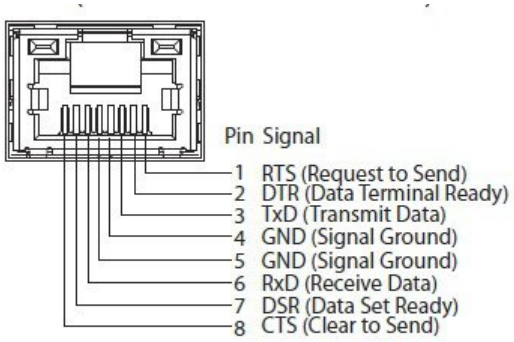
（注） operators グループおよび administrators グループのユーザだけが、アプライアンスへのアクセスに secure copy（scp）を使用できます。詳細については、ユーザの追加を参照してください。

# シリアル接続経由での E メール セキュリティ アプライアンスへのアクセス

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。

# 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**

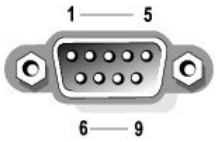



**表 *2*：シリアル ポートのピン割り当て**

| 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 | 信号アース |
| [6] | DSR | | データ セット レディ |

| ピン | 信号（Signal） | I/O | 定義（Definition） |
|---|---|---|---|
| 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 |