



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)
- 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 (2 ページ)
- セキュアコピ (scp) アクセス (4 ページ)
- 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 (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 | 非対応 | 非対応 |
| SSH | 22 | 対応 | 非対応 |
| HTTP | 80 | 対応 | 非対応 |
| HTTPS | 443 | 対応 | 非対応 |

¹ ここに示す「管理インターフェイス」の設定は、Cisco C170 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。

■ AsynOS によるデフォルト IP インターフェイスの選択方法

- ・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

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

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、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。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。 <ul style="list-style-type: none"> • Virtual Gateway マッピング (<code>altsrchost</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>slbl<タイムスタンプ><シリアル番号>.csv</code> 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 (<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。 |

セキュア コピー (scp) アクセス

| 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 | |
| /snntp_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 のアプリアンスの 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  
%
```

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)

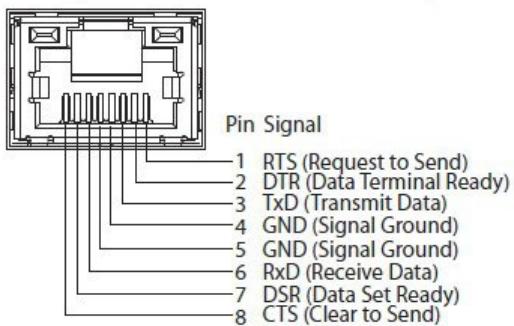
operators グループおよびadministrators グループのユーザのみが、アプライアンスへのアクセスにセキュアコピー (scp) を使用できます。詳細については、[ユーザの追加](#)を参照してください。

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

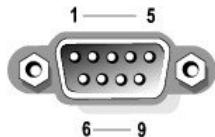


表 2: シリアルポートのピン割り当て

| 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 |

■ FTP、SSH、およびSCPアクセス