APPENDIX A

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

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。

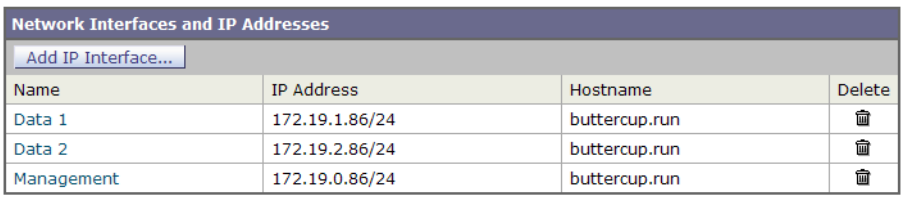
表 A-1　IP インターフェイスに対してデフォルトでイネーブルになるサービス

		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	No	No
Telnet	23	Yes	No
SSH	22	Yes	No
HTTP	80	Yes	No
HTTPS	443	Yes	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の Cisco IronPort 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。また、インターフェイスは個別のグループに（CLI を介して）「参加」させることもできます。その場合、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繰り返して使用します。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 を介して）設定することもできます。詳細については、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』の「Advanced Networking」の章を参照してください。

図 A-1　[IP Interfaces] ページ



IP インターフェイスの設定

[Management Appliance] > [Network] > [IP Interfaces] ページ（および `interfaceconfig` 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、仮想ゲートウェイ）。

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 A-2　IP インターフェイス コンポーネント

名前	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。
ホスト名	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 アドレスに正しく解決されたり、または逆引き DNS によって所定のホスト名が解決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、Cisco IronPort スパム隔離、HTTP、および HTTPS はインターフェイス上でイネーブルまたはディセーブルにできます。サービスごとにポートを設定できます。Cisco IronPort スパム隔離の HTTP/HTTPS、ポート、および URL も設定できます。

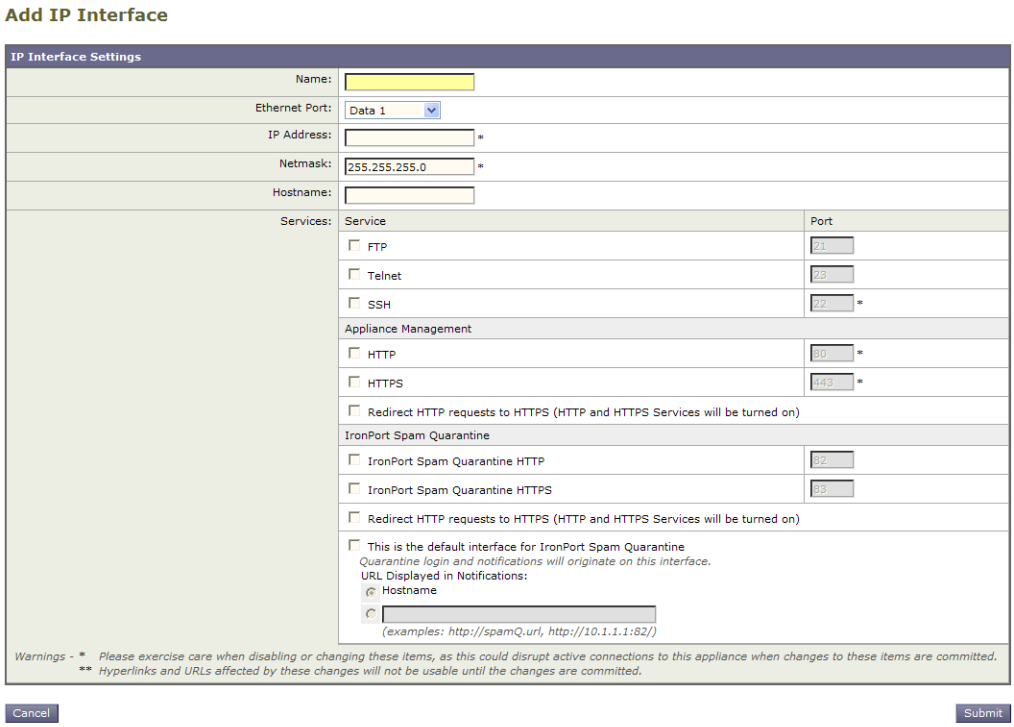
（注）　第 2 章「セットアップ、インストール、および基本設定」の説明に従ってシステム セットアップ ウィザードを完了し、変更を保存している場合は、アプライアンス上に管理インターフェイスがすでに設定されているはずです。

GUI を使用した IP インターフェイスの作成

IP インターフェイスを作成するには、次の手順を実行します。

1. [Management Appliance] > [Network] > [IP Interfaces] ページ上で [Add IP Interface] をクリックします。[Add IP Interface] ページが表示されます。

図 A-2　[Add IP Interface] ページ



2. インターフェイスの名前を入力します。
3. イーサネット ポートを選択し、IP アドレスを入力します。
4. IP アドレスに対応するネットマスクを入力します。
5. インターフェイスのホスト名を入力します。
6. 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。
7. 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。
8. Cisco IronPort 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 インターフェイスが Cisco IronPort スパム隔離のデフォルト インターフェイスであるかどうか、およびホスト名を URL として使用するかまたはカスタム URL を指定するかを指定できます。
9. 変更を送信し、保存します。

FTP アクセス

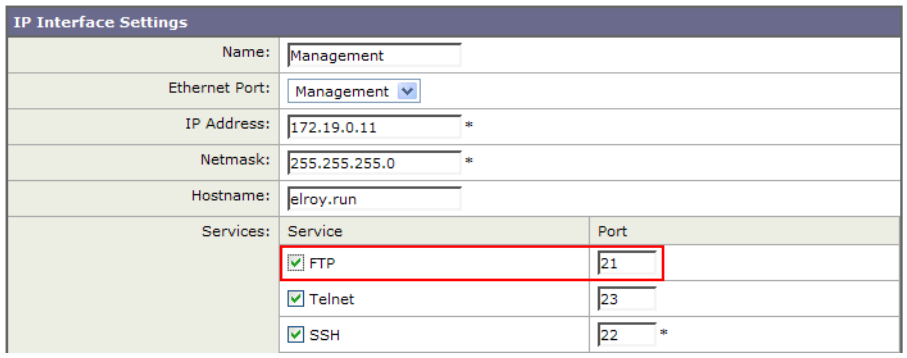
FTP 経由でアプライアンスにアクセスするには、次の手順を実行します。

警告　**[Management Appliance] > [Network] > [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。**

1. [Management Appliance] > [Network] > [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。

   この例では、管理インターフェイスはポート 21（デフォルト ポート）上での FTP アクセスをイネーブルにするように編集されています。

図 A-3　[Edit IP Interface] ページ



（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。

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
   ```

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てファイルをコピーおよび追加（「GET」および「PUT」）できます。表 A-3 を参照してください。

表 A-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**	[Management Appliance] > [System Administration] > [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、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』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」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。 • 仮想ゲートウェイ 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）ページ（hostaccess） • 受信者アクセス テーブル（RAT）ページ（rcptaccess） • SMTP ルート 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

表 A-3　アクセスできるディレクトリ （続き）

ディレクトリ名	説明
/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。

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 A-3（P.A-5）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 を持つアプライアンスの configuration 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。この例を参考用としてだけ示します。オペレーティング システムのセキュア コピー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
```

Cisco IronPort 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 グループのユーザだけが、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」（P.13-27）を参照してください。

シリアル接続によるアクセス

シリアル接続を使用してアプライアンスに接続している場合、図 A-4 にシリアル ポート コネクタのピン番号を示し、表 A-4 にシリアル ポート コネクタのピン割り当ておよびインターフェイス信号を定義します。

図 A-4　　シリアル ポートのピン番号

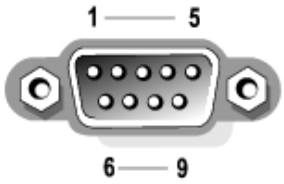


表 A-4　　シリアル ポートのピン割り当て

ピン	信号	I/O	定義
1	DCD	I	データ キャリア検出
2	SIN	I	シリアル入力
3	SOUT	O	シリアル出力
4	DTR	O	データ ターミナル レディ
5	GND	n/a	信号用接地
6	DSR	I	データ セット レディ
7	RTS	I	送信要求
8	CTS	O	送信可
9	RI	I	リング インジケータ
シェル	n/a	n/a	シャーシ アース