APPENDIX A

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 インターフェイスでデフォルトでイネーブルに設定されているサービス

		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**	**作成する新しい IP インターフェイス**
FTP	21	いいえ	いいえ
Telnet	23	はい	いいえ
SSH	22	はい	いいえ
HTTP	80	はい	いいえ
HTTPS	443	はい	いいえ

ここに示す「管理インターフェイス」は、IronPort C150/160 アプライアンスのデータ 1 インターフェイスのデフォルト設定でもあります。

- Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）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。
- コンフィギュレーション 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 または Telnet をイネーブルにする必要があります。「FTP アクセ

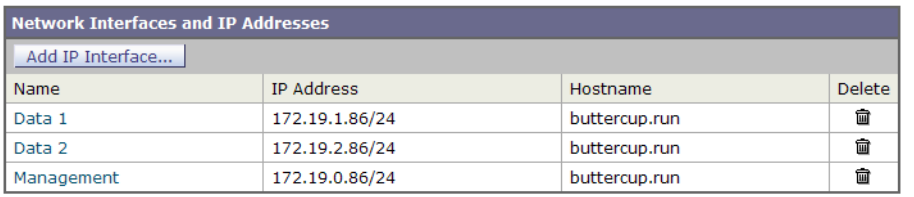
ス」（P.A-578）を参照してください。

- 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

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 IronPort スパム検疫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間を循環します。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 キャンペーンを負荷分散するのに役立ちます。VLAN を作成し、他のインターフェイスを設定するのと同様に（CLI を使用して）VLAN を設定することもできます。詳細については、『*Cisco IronPort AsyncOS for Email 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

[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） M-Series アプライアンス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 ポートは変更できません。さらに、IronPort M-Series アプライアンスは、以降に説明する機能（仮想ゲートウェイなど）をすべてサポートするわけではありません。

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 インターフェイスのコンポーネント

名称	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（またはサブネットマスク）	ネットマスクを標準のドット付きオクテット形式（255.255.255.0 など）または 16 進形式（0xffffff00 など）で入力できます。デフォルトのネットマスクは、一般的なクラス C の値である、255.255.255.0 です。
ブロードキャスト アドレス	IronPort AsyncOS は、IP アドレスおよびネットマスクからデフォルトのブロードキャスト アドレスを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。SMTP カンバセーション時に、このホスト名を使用してサーバを識別します。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 でホスト名が一致する IP アドレスに正しく解決されるか、または逆引き DNS で指定されたホスト名に解決されることをチェックしません。
使用可能なサービス	FTP、SSH、Telnet、IronPort スパム検疫、HTTP、および HTTPS は、インターフェイスでイネーブルまたはディセーブルに設定できます。サービスごとにポートを設定できます。また、IronPort スパム検疫用に HTTP/HTTPS、ポート、および URL も指定できます。

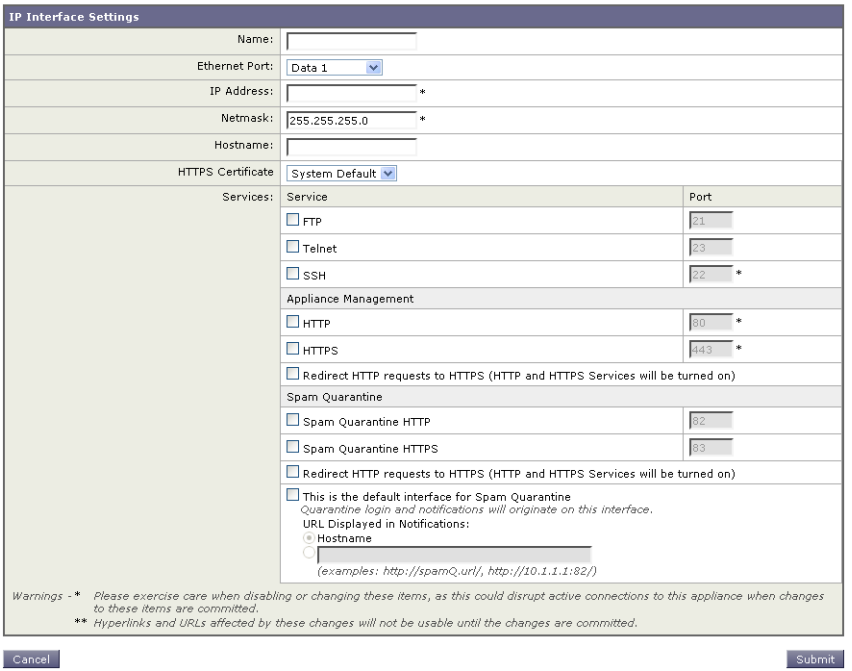
（注） 第 3 章「セットアップおよび設置」で説明されている GUI の System Setup Wizard（またはコマンド ライン インターフェイスの `systemsetup` コマンド）を完了し、変更を確定している場合は、すでにアプライアンスにインターフェイスが 1 つまたは 2 つ設定されているはずです（「Assign and Configure Logical IP Interface(s)」セクションで入力した設定を参照してください）。また、管理インターフェイスも IronPort アプライアンスに設定されています。

GUI による 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。

ステップ 1　[Network] > [IP Interfaces] ページで [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



ステップ 2　インターフェイスの名前を入力します。

ステップ 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。

ステップ 4　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 5　インターフェイスのホスト名を入力します。

ステップ 6　HTTPS サービスの TLS 証明書を選択します。

ステップ 7　この IP インターフェイス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にマークを付けます。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　IronPort スパム検疫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 IronPort スパム検疫のデフォルト インターフェイスであるかを指定したり、ホスト名を URL として使用するかを指定するか、またはカスタム URL を指定したりできます。

ステップ 10　[Submit] をクリックします。

ステップ 11　[Commit Changes] ボタンをクリックし、必要に応じて、任意にコメントを追加してから、[Commit Changes] をクリックして IP インターフェイスの作成を完了します。

FTP アクセス

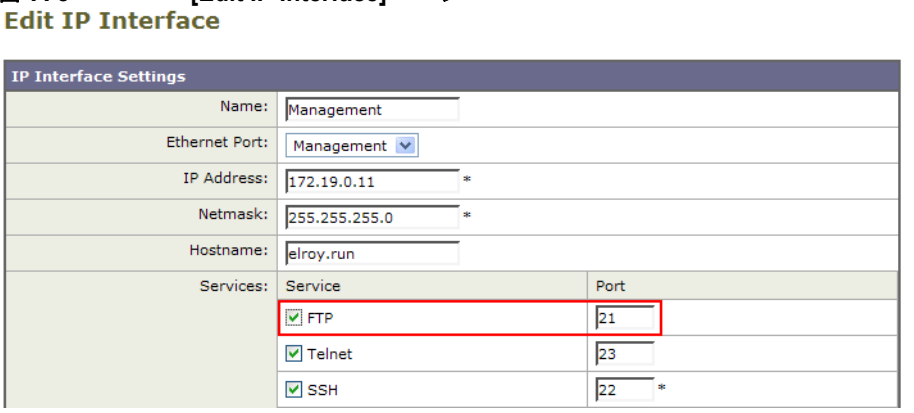
FTP 経由でアプライアンスにアクセスするには、次の手順を実行します。

警告　**アプライアンスに接続している方法によっては、[Network] > [IP Interfaces] ページまたは interfaceconfig コマンドを使用してサービスをディセーブルにすることで、GUI または CLI から独自に切断できます。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する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　[Network] > [IP Interfaces] ページ（または `interfaceconfig` コマンド）を使用して、インターフェイスの 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がポート 21（デフォルト ポート）で 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） 次の手順に進む前に、忘れずに変更を確定してください。

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。次の例を参考にしてください。

```
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。次の例を参考にしてください。

```
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。表 A-2（P.A-580）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
/antivirus	Sophos Anti-Virus エンジンのログ ファイルが保持されるディレクトリ。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。
/avarchive **/bounces** **/cli_logs** **/delivery** **/error_logs** **/ftpd_logs** **/gui_logs** **/mail_logs** **/rptd_logs** **/sntpd.logs** **/status** **/system_logs**	[System Administration] > [Logging] ページまたは `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。各ログの詳しい説明については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」の章を参照してください。 各ログ ファイル タイプ間の違いについては、「Logging」章の「Log File Type Comparison」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（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。 レコード管理のためにこれらのファイルを別のマシンにコピーしたり、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。
/saved_reports	システムで設定されたすべてのアーカイブ済みレポートが保存されるディレクトリ。
/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） • Host Access Table（HAT; ホスト アクセス テーブル）ページ（hostaccess） • Recipient Access Table（RAT; 受信者アクセス テーブル）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

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。

secure copy（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、表 A-2 に示されている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コンフィギュレーション 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 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
```

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、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、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Admistrative Tasks」のユーザの追加に関する情報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（「アプライアンスへの接続」（P.3-45）を参照）、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

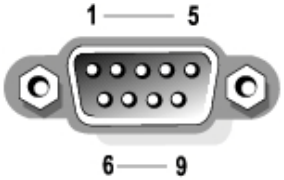


表 A-4　シリアル ポートのピン割り当て

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

表 A-4　シリアル ポートのピン割り当て（続き）

ピン	信号	I/O	定義
9	RI	I	リング インジケータ
シェル	n/a	n/a	シャーシ グラウンド