CHAPTER 7

GUI でのその他の作業

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）は、システムのモニタリングおよび設定用の一部の Command Line Interface（CLI; コマンドライン インターフェイス）コマンドに代わる Web ベースのインターフェイスです。GUI を使用することにより、IronPort AsyncOS コマンド構文を知らなくても、単純な Web ベース インターフェイスを使用してシステムをモニタできます。

この章は、次の内容で構成されています。

- 「Cisco IronPort グラフィカル ユーザ インターフェイス（GUI）」（P.7-289）
- 「テスト メッセージを使用したメール フローのデバッグ：トレース」（P.7-296）
- 「GUI からの XML ステータスの収集」（P.7-312）

Cisco IronPort グラフィカル ユーザ インターフェイス（GUI）

インターフェイスに対して HTTP、HTTPS、またはその両方のサービスをイネーブルにすると、GUI にアクセスし、ログインできるようになります。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Overview」の章を参照してください。

インターフェイスでの GUI のイネーブル化

システムはデフォルトで、管理インターフェイス（IronPort C150/160 アプライアンスの Data 1）に対して HTTP がイネーブルになった状態で出荷されます。

GUI をイネーブルにするには、コマンドライン インターフェイスで `interfaceconfig` コマンドを実行し、接続するインターフェイスを編集してから、HTTP サービスまたはセキュア HTTP サービス、あるいはその両方をイネーブルにします。

（注） また、いずれかのインターフェイスで GUI をイネーブルにした後は、[Network] > [IP Interfaces] ページを使用して、別のインターフェイスに対して GUI をイネーブルまたはディセーブルにすることもできます。詳細については、IP Interfaces, page -294 を参照してください。

（注） インターフェイスでセキュア HTTP をイネーブルにするには、証明書をインストールする必要があります。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Enabling a Certificate for HTTPS」を参照してください。

いずれかのサービスに対し、そのサービスをイネーブルにするポートを指定します。デフォルトでは、HTTP はポート 80、HTTPS はポート 443 でイネーブルになります。1 つのインターフェイスで両方のサービスをイネーブルにすると、HTTP 要求をセキュア サービスに自動的にリダイレクトできます。

さらに、このインターフェイスの GUI に（`HTTP` または `HTTPS` 経由で）アクセスしようとするすべてのユーザ（「ユーザの追加」（P.8-333）を参照）は、ユーザ名とパスワードを入力する標準のログイン ページで認証を受ける必要があります。

（注） GUI にアクセスするには、まず、`commit` コマンドを使用して変更を保存する必要があります。

次に、Data 1 インターフェイスに対して GUI をイネーブルにする例を示します。`interfaceconfig` コマンドを使用して、ポート 80 で HTTP、およびポート 443 で HTTPS をイネーブルにします（`certconfig` コマンドが実行可能になるまで、HTTP に対して一時的にデモ用の証明書が使用されます。詳細については、

『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Installing Certificates on the Cisco IronPort Appliance」を参照してください）。Data1 インターフェイスについては、ポート 80 への HTTP 要求がポート 443 に自動的にリダイレクトされるように設定されます。

例

```
mail3.example.com> interfaceconfig

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Data 1]>

IP Address (Ex: 192.168.1.2):
```

```
[192.168.1.1]>


Ethernet interface:

1. Data 1

2. Data 2

3. Management

[1]>


Netmask (Ex: "255.255.255.0" or "0xffffff00"):

[255.255.255.0]>


Hostname:

[mail3.example.com]>


Do you want to enable FTP on this interface?  [N]>


Do you want to enable Telnet on this interface?  [N]>


Do you want to enable SSH on this interface?  [N]>


Do you want to enable HTTP on this interface?  [N]> y
```

```
Which port do you want to use for HTTP?

[80]> 80


Do you want to enable HTTPS on this interface?  [N]> y


Which port do you want to use for HTTPS?

[443]> 443


You have not entered a certificate. To assure privacy, run

'certconfig' first.  You may use the demo certificate

to test HTTPS, but this will not be secure.

Do you really wish to use a demo certificate?  [N]> y


Both HTTP and HTTPS are enabled for this interface, should HTTP
requests

redirect to the secure service?  [Y]> y


Currently configured interfaces:

1. Data 1 (192.168.1.1/24 on Data 1: mail3.example.com)

2. Data 2 (192.168.2.1/24 on Data 2: mail3.example.com)

3. Management (192.168.42.42/24 on Management: mail3.example.com)
```

```
Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>

mail3.example.com> commit


Please enter some comments describing your changes:

[]> enabled HTTP, HTTPS for Data 1


Changes committed: Mon Jul  7 13:21:23 2003

mail3.example.com>
```

GUI で使用できるその他の作業の概要

- [System Overview] ページでは、次のことができます。
  - 主要システムのステータスとパフォーマンスの一部の情報を示す履歴グラフおよびテーブルを表示する。
  - アプライアンスにインストールされている IronPort AsyncOS オペレーティング システムのバージョンを表示する。
  - 主要統計情報のサブセットを表示する。
- [System Status] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。また、システム統計情報のカウンタをリセットしたり、カウンタが最後にリセットされた時刻を表示したりすることもできます。

- [System Trace] ページでは、テスト メッセージの送信をエミュレートすることによって、システムを介したメッセージ フローをデバッグできます。リスナーに受け入れられているようにメッセージをエミュレートして、現在のシステム設定によって「トリガー」される、または影響を受ける機能の概要を出力できます。

テスト メッセージを使用したメール フローのデバッグ：トレース

[System Administration] > [Trace] ページを使用して（CLI の `trace` コマンドと同等）、テスト メッセージの送信をエミュレートすることにより、システムを介したメッセージ フローをデバッグできます。[Trace] ページ（および `trace` CLI コマンド）では、リスナーに受け入れられているようにメッセージをエミュレートし、現在のシステム設定（*コミットしていない変更を含む*）によって「トリガー」される、または影響を受ける機能の概要を出力できます。テスト メッセージは実際には送信されません。特に、Cisco IronPort アプライアンスで使用できる多数の高度な機能を組み合わせると、[Trace] ページ（および `trace` CLI コマンド）は、強力なトラブルシューティングまたはデバッグ ツールとなります。

[Trace] ページ（および trace CLI コマンド）では、表 7-1 に示されている入力パラメータのプロンプトが表示されます。

表 7-1　[Trace] ページの入力

値	説明	例
[Source IP address]	リモート ドメインの送信元を模倣するため、リモート クライアントの IP アドレスを入力します。 **注：**trace コマンドを実行すると、IP アドレスと完全修飾ドメイン名の入力が求められます。完全修飾ドメイン名が一致するかどうかを確認するための IP アドレスの逆引きは*行われません*。trace コマンドでは、完全修飾ドメイン名フィールドをブランクにすることができないので、DNS で適切に逆引きできない場合にはテストできません。	`203.45.98.109`
[Fully Qualified Domain Name of the Source IP]	模倣する完全修飾リモート ドメイン名を入力します。ヌルのままにすると、送信元 IP アドレスに対してリバース DNS ルックアップが実行されます。	`smtp.example.com`
[Listener to Trace Behavior on]	テスト メッセージの送信をエミュレートするため、システムに設定されているリスナーのリストから選択します。	`InboundMail`
[SenderBase Network Owner Organization ID]	SenderBase ネットワーク オーナーに固有の ID 番号を入力するか、送信元 IP アドレスに関連付けられたネットワーク オーナー ID の検索を指示します。GUI を介して送信者グループにネットワーク オーナーを追加した場合は、この情報を表示できます。	`34`

表 7-1　[Trace] ページの入力（続き）

値	説明	例
[SenderBase Reputation Score (SBRS)]	スプーフィング ドメインに与える SBRS スコアを入力するか、送信元 IP アドレスに関連付けられた SBRS スコアの検索を指示します。このパラメータは、SBRS スコアを使用するポリシーをテストするときに役立ちます。手動で入力した SBRS スコアは、Context Adaptive Scanning Engine（CASE）に渡されないことに注意してください。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Reputation Filtering」を参照してください。	`-7.5`
[Envelope Sender]	テスト メッセージのエンベロープ送信者を入力します。	`admin@example.net`
[Envelope Recipients]	テスト メッセージの受信者のリストを入力します。複数のエントリを指定する場合は、カンマで区切ります。	`joe` `frank@example.com`

[Message Body]	ヘッダーを含む、テスト メッセージの本文を入力します。メッセージ本文の入力を終了するには、別の行にピリオドを入力します。「ヘッダー」は（空白行で区切られた）メッセージ本文の一部と見なされます。ヘッダーを省略したり、ヘッダーの形式に誤りがあったりすると、予期しないトレース結果を招くことがあります。	`To: 1@example.com`
		From: ralph
		Subject: Test
		
		`A test message`
		.

値を入力したら、[Start Trace] をクリックします。メッセージに影響する、システムに設定されたすべての機能の概要が出力されます。

メッセージ本文は、ローカル ファイル システムからアップロードできます（CLI では、`/configuration` ディレクトリにアップロードしたメッセージ本文を使用してテストできます。Cisco IronPort アプライアンスへのインポート用ファイルの準備に関する詳細については、Appendix A, “Accessing the Appliance” を参照してください）。

概要が出力されると、生成されたメッセージの確認とテスト メッセージの再実行を求められます。別のテスト メッセージを入力する場合、[Trace] ページおよび trace コマンドで、前に入力した表 7-1 の値が使用されます。

（注）　表 7-2 に示す、trace コマンドによってテストされる設定の各セクションは、*順番どおりに*実行されます。この順番は、ある機能の設定が他の機能にどのように影響するかを理解するうえで非常に役立ちます。たとえば、ドメイン マップ機能によって変換される受信者アドレスは、RAT によって評価されるアドレスに影響します。また、RAT の影響を受ける受信者は、エイリアス テーブルによって評価されるアドレスに影響する、というようになります。

表 7-2　トレースを実行した後の出力の表示

trace コマンド セクション	出力
Host Access Table (HAT) and Mail Flow Policy Processing	指定したリスナーに対する Host Access Table の設定が処理されます。システムからは、入力したリモート IP アドレスおよびリモート ドメイン名と一致した HAT 内のエントリが報告されます。デフォルトのメール フロー ポリシーと送信者グループ、およびどちらが所定のエントリに一致したかを確認できます。 Cisco IronPort アプライアンスが（REJECT または TCPREFUSE アクセス ルールを介して）接続を拒否するように設定された場合、処理中の trace コマンドはその時点で終了します。 HAT パラメータの設定の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Envelope Sender Address Processing	
これらのセクションには、指定したエンベロープ送信者に対してアプライアンスの設定がどのように影響するかが要約されます（つまり、MAIL FROM コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。`trace` コマンドは、このセクションの前に「`Processing MAIL FROM:`」を出力します。	
Default Domain	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ送信者に対するすべての変更がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「SMTP Address Parsing Options」を参照してください。
Masquerading	メッセージのエンベロープ送信者を変換するように指定した場合は、ここに変更が表示されます。`listenerconfig -> edit -> masquerade -> config` サブコマンドを使用して、プライベート リスナーに対するエンベロープ送信者のマスカレードをイネーブルにします。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Masquerading」を参照してください。
Envelope Recipient Processing	
これらのセクションでは、指定したエンベロープ受信者に対してアプライアンスがどのように影響するかの要約を示します（つまり、RCPT TO コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。`trace` コマンドは、このセクションの前に「`Processing Recipient List:`」を出力します。	

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Default Domain	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ受信者に対するすべての変更がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「SMTP Address Parsing Options」を参照してください。
Domain Map Translation	ドメイン マップ機能によって、受信者アドレスが代替アドレスに変換されます。ドメイン マップの変更を指定しており、指定した受信者アドレスが一致した場合は、このセクションに変換が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「The Domain Map Feature」を参照してください。
Recipient Access Table (RAT)	ポリシーとパラメータのほか、このセクションには、RAT 内のエントリに一致する各エンベロープ受信者が出力されます（たとえば、リスナーの RAT の制限をバイパスするように、受信者を指定した場合）。 受け入れる受信者の指定の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Accepting Email for Local Domains or Specific Users on Public listeners (RAT)」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Alias Table	このセクションには、アプライアンスで設定されたエイリアス テーブル内のエントリに一致する各エンベロープ受信者（および 1 つまたは複数の受信者アドレスへの後続の変換）が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Creating Alias Tables」を参照してください。

Pre-Queue Message Operations

ここでは、メッセージのコンテンツを受信してから、メッセージを作業キューに入れるまでに、アプライアンスが各メッセージにどのような影響を及ぼすかを説明します。この処理は、最後の `250 ok` コマンドがリモート MTA に返される前に実行されます。

`trace` コマンドは、このセクションの前に「Message Processing:」を出力します。

Virtual Gateways	`altsrchost` コマンドを実行すると、エンベロープ送信者の完全アドレス、ドメイン、または名前、あるいは IP アドレスの一致に基づいて、特定のインターフェイスにメッセージが割り当てられます。エンベロープ送信者が `altsrchost` コマンドのエントリに一致すると、その情報がこのセクションに出力されます。 ここで割り当てられた仮想ゲートウェイ アドレスは、後述のメッセージ フィルタ処理によって上書きされる場合があります。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Bounce Profiles	バウンス プロファイルは、処理中の 3 つの時点で適用されます。ここが最初のポイントです。リスナーにバウンス プロファイルが割り当てられる場合は、プロセス内のこの時点で割り当てられます。その情報がこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Handling Undeliverable Email」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Work Queue Operations	
次の一連の機能は、作業キュー内のメッセージに対して実行されます。機能が実行されるのは、クライアントからのメッセージが受け入れられた後、そのメッセージが配信用として宛先キューに入れられる前です。`status` コマンドおよび `status detail` コマンドによって「Messages in Work Queue」が報告されます。	
Masquerading	メッセージの [To:]、[From:]、および [CC:] ヘッダーが（リスナーから入力されたスタティック テーブルまたは LDAP クエリーを通じて）マスクされるように指定した場合は、ここに変更が表示されます。`listenerconfig -> edit -> masquerade -> config` サブコマンドを使用して、プライベート リスナーに対してメッセージ ヘッダーのマスカレードをイネーブルにします。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Masquerading」を参照してください。
LDAP Routing	リスナーに対して LDAP クエリーがイネーブルになっている場合は、このセクションに LDAP 許可、再ルーティング、マスカレード、およびグループ クエリーの結果が出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Message Filters Processing	システムでイネーブルになっているすべてのメッセージ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最後の結果が「true」であれば、そのフィルタの各アクションが順次実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。ルールが「false」と評価された場合、アクションのリストが `else` 句に関連付けられていれば、それらのアクションが代わりに評価されます。このセクションには、順番に処理されたメッセージ フィルタの結果が出力されます。 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」を参照してください。
Mail Policy Processing	メール ポリシーの処理セクションには、アンチスパム、アンチウイルス、ウイルス感染フィルタ機能と、指定されたすべての受信者に対する免責事項のスタンプが表示されます。複数の受信者が電子メール セキュリティ マネージャの複数のポリシーに一致する場合は、一致する各ポリシーが次の各セクションに繰り返し表示されます。「Message going to」というストリングは、どの受信者がどのポリシーに一致したかを定義します。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Anti-Spam	このセクションには、アンチスパム スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチスパム スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco IronPort アプライアンスが、その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。 注：システムでアンチスパム スキャンが使用できない場合、この手順は省略されます。アンチスパム スキャンを使用できても、機能キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Spam」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Anti-Virus	このセクションには、アンチウイルス スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチウイルス スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco IronPort アプライアンスが、感染メッセージを「クリーニング」するように設定されている場合は、その情報が表示されます。その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、`trace` コマンドの処理は停止します。 注：システムでアンチウイルス スキャンが使用できない場合、この手順は省略されます。アンチウイルス スキャンを使用できても、機能キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Anti-Virus」を参照してください。
Virus Outbreak Filters Processing	このセクションには、ウイルス感染フィルタ機能をバイパスする添付ファイルを含むメッセージが示されます。メッセージが受信者に対するウイルス感染フィルタ機能によって処理されることになっている場合、メッセージは処理され、その評価が出力されます。アプライアンスが、判定に基づいてメッセージを検疫、バウンス、またはドロップするように設定されている場合、その情報が出力されて、処理が停止します。 詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Virus Outbreak Filters」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Footer Stamping	このセクションには、メッセージに免責事項テキスト リソースが付加されたかどうかが示されます。テキスト リソースの名前が表示されます。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Message Disclaimer Stamping」を参照してください。

表 7-2　トレースを実行した後の出力の表示（続き）

trace コマンド セクション	出力
Delivery Operations	
次の各セクションには、メッセージが配信されるときに発生する動作が示されます。`trace` コマンドは、このセクションの前に「`Message Enqueued for Delivery`」を出力します。	
Global Unsubscribe per Domain and per User	`trace` コマンドの入力として指定した受信者が、グローバル配信停止機能に示されている受信者、受信者ドメイン、または IP アドレスに一致すると、未登録の受信者アドレスがこのセクションに出力されます。 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Global Unsubscribe」を参照してください。
Final Result	
すべての処理が出力されると、最終結果が表示されます。CLI では、「Would you like to see the resulting message?」という問いに対して **y** を入力します。	

[Trace] ページの GUI の例

図 7-1　[Trace] ページの入力

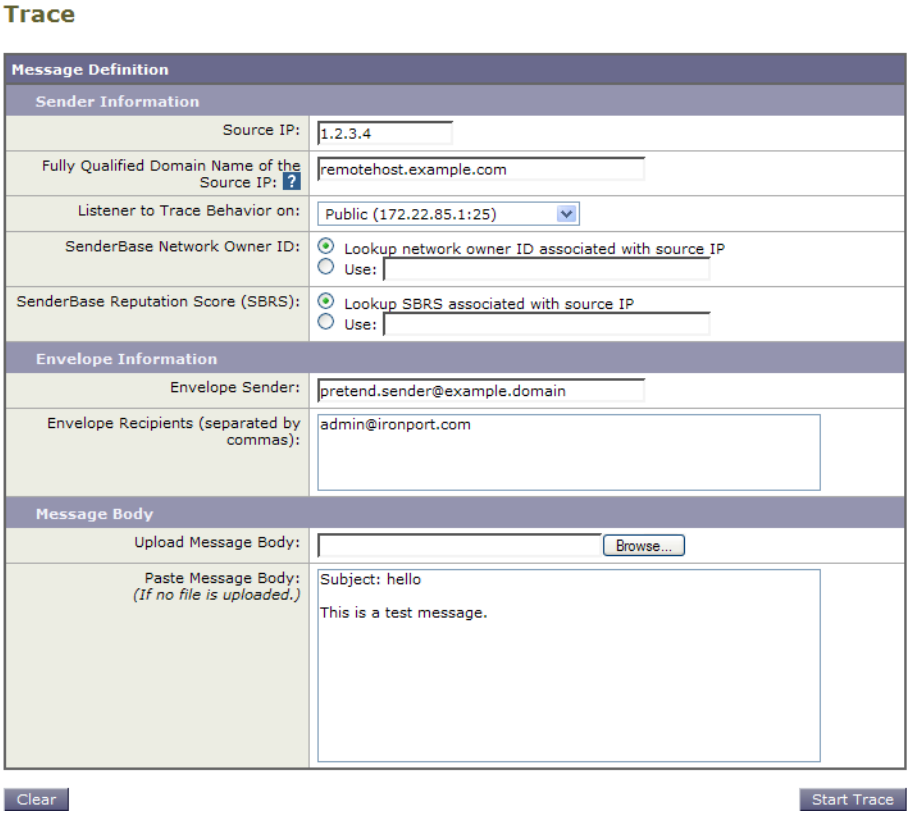

図 7-2　[Trace] ページの出力（1/2）

Trace

Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		

図 7-3　[Trace] ページの出力（2/2）

Domain Masquerading	
	No changes
Filter Processing	
skipper	Skipped (Inactive)
always_deliver	Rule: rcpt-to == "@mail.qa": False Rule: rcpt-to == "ironport.com": True Rule: OR: True Action: deliver()
Mail Policy Processing: Inbound (matched on policy Public Upgrade)	
Message going to:	admin@ironport.com
Anti-Spam Processing	
Evaluation:	Not Spam
Anti-Virus Processing	
Evaluation:	No Viruses Detected Elapsed Time: 0.000 sec
Actions Taken:	Delivered
VOF Processing	
Evaluation:	No threat detected
Footer Stamping	
Appended Text Resource:	footer
DomainKey Signing	
Result of DomainKeys processing:	DomainKeys signing not enabled in this listener's HAT
Message Delivery (matched on policy Public Upgrade)	
Final Envelope Sender:	pretend.sender@example.domain
Final Recipients:	admin@ironport.com
Final Message:	Received: from remotehost.example.com (HELO TEST) ([1.2.3.4]) by mail3.example.com with TEST; 21 Jul 2005 14:40:05 -0700 Message-Id: <48q06k$@Public> X-Brightmail-Tracker: AAAAAA== X-BrightmailFiltered: true X-IronPort-Anti-Spam-Filtered: true X-IronPort-AV: i="3.95,134,1120460400"; d="scan'"; a="0:sNHT0" Subject: hello Content-Transfer-Encoding: base64 Content-Type: text/plain; charset="utf-8" VGhpcyBpcyBhIHRlc3QgbWVzc2FnZS4KPT09PT09PT09PT09CuODleODg+OCv+ODvOOBp+OBmeOA guOCj+OBhOOCj+OBhOOAggpUaGlzIGlzIGEgSmFwYW5lc2UgZm9vdGVyCj09PT09PT09PQo=

Done

GUI からの XML ステータスの収集

- XML ページを通じてステータスを表示するか、XML ステータス情報にプ

ログラムでアクセスします。

XML ステータス機能は、電子メールのモニタリング統計情報にプログラムでアクセスする方法を提供します。最新のブラウザによっては、XML データを直接表示できるものもあります。

次の表に示す GUI の各ページの情報は、対応する URL にアクセスすることにより、動的な XML 出力としても使用できます。

GUI のページ名	対応する XML ステータス URL
[Mail Status]	`http://`*hostname*`/xml/status`
[Host Mail Status for a Specified Host]	`http://`*hostname*`/xml/hoststatus?hostname=`*host*
[DNS Status]	`http://`*hostname*`/xml/dnsstatus`
[Top Incoming Domains]	`http://`*hostname*`/xml/topin`
[Top Outgoing Domains[a]]	`http://`*hostname*`/xml/tophosts`

[a] このページはデフォルトで、アクティブ受信者の番号順にソートされます。この順番を変更するには、URL に「?sort=**order**」を付加します。ここで、**order** は conn_out、deliv_recip、soft_bounced、または hard_bounced です。