CHAPTER 9

テストとトラブルシューティング

この章は、次の内容で構成されています。

システムに関する問題のトラブルシューティングや解決を行うには、いくつかの基本的な方法があります。しかし、IronPort システムには、複雑な問題に対応するテクニカル サポートがあることを覚えておいてください（「IronPort Customer Support」（P.1-7）を参照）。

（注） ここで説明する機能やコマンドの中には、ルーティングの優先順位に影響を与えるものや、逆に影響を受けるものがあります。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録 B、「Assigning Network and IP Addresses」を参照してください。

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 CLI コマンドの trace）では、メッセージをリスナーが受け取ったとしてエミュレートし、システムの現在の設定によって「トリガー」または影響を受ける機能の概要を出力します。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 9-1 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 9-1　[Trace] ページに対する入力

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。	`smtp.example.com`

表 9-1　[Trace] ページに対する入力（続き）

値	説明	例
[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`
[SenderBase Reputation Score (SBRS)]	スプーフされたドメインに与える SBRS を入力するか、システムがソース IP アドレスに対応する SBRS を検索するよう指定します。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。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Implementing Reputation Filtering in a Listener's HAT」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]	テスト メッセージのメッセージ本文を入力します。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」は本文の一部と見なされることに注意してください。	`To: 1@example.com`
		From: ralph
		Subject: Test
		
		`this is 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 9-1 の値が使用されます。

（注）　表 9-2 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 9-2　トレースを実行したときの出力の表示

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 パラメータの設定についての詳細は、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「The Host Access Table (HAT): Sender Groups and Mail Flow Policies」を参照してください。
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「Customizing Listeners」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
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 Routing and Delivery Features」の章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。	
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」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
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「Configuring Routing and Delivery Features」の章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「Configuring the Gateway to Receive Email」の章を参照してください。
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「Configuring Routing and Delivery Features」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
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「Configuring Routing and Delivery Features」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（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「Configuring Routing and Delivery Features」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（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 Routing and Delivery Features」の章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」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（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」の章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フッター スタンプ機能が表示されます。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 9-2　トレースを実行したときの出力の表示（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」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（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」の章を参照してください。

表 9-2　トレースを実行したときの出力の表示（続き）

trace コマンド セクション	出力
Content Filters Processing	システムでイネーブルになっているすべてのコンテンツ 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。このセクションには、順番に処理されたコンテンツ フィルタの結果が出力されます。 『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Email Security Manager」の章を参照してください。
VOF 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のある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」の章を参照してください。
Footer Stamping	このセクションには、メッセージにフッター 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「Text Resources」の章にある「Message Footer Stamping」を参照してください。

表 9-2　トレースを実行したときの出力の表示（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「Configuring Routing and Delivery Features」の章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`** と入力して、結果のメッセージを表示します。	

[Trace] ページの GUI の例

図 9-1　[Trace] ページの入力

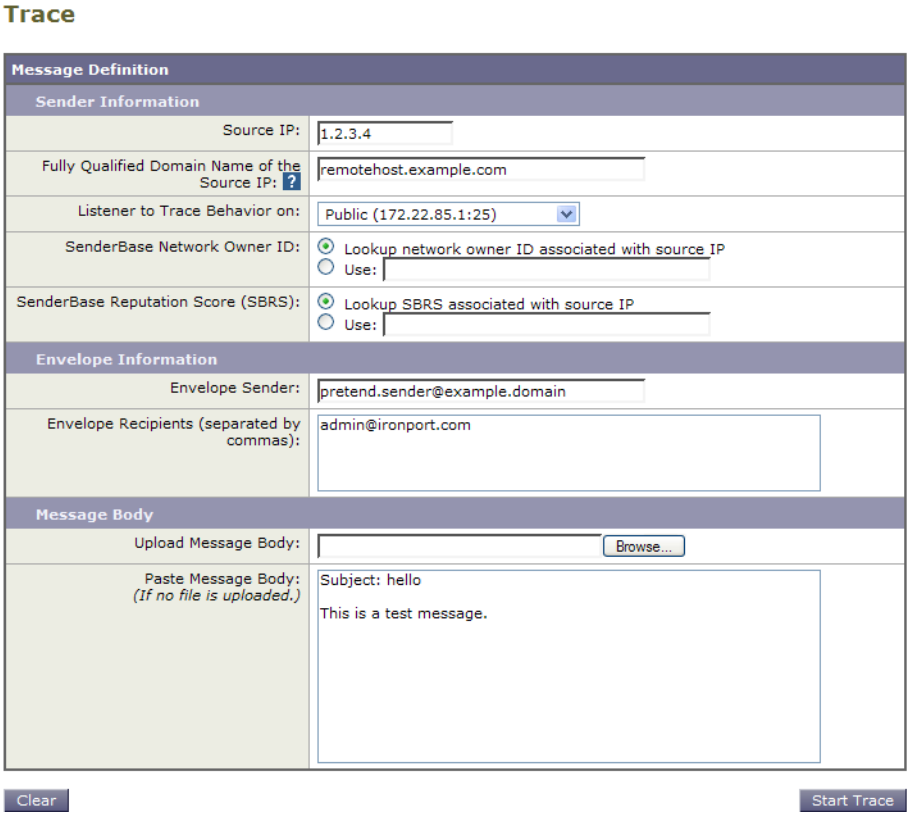


図 9-2　[Trace] ページの出力（1/2）

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 9-3　[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

[Trace] ページの CLI の例

```
mail3.example.com> trace


Enter the source IP

[]> 192.168.1.1


Enter the fully qualified domain name of the source IP

[]> example.com


Select the listener to trace behavior on:

1. InboundMail

2. OutboundMail

[1]> 1


Fetching default SenderBase values...

Enter the SenderBase Org ID of the source IP.  The actual ID is N/A.

[N/A]>


Enter the SenderBase Reputation Score of the source IP.  The actual score
is N/A.

[N/A]>
```

```
Enter the Envelope Sender address:

[]> pretend.sender@example.net


Enter the Envelope Recipient addresses.  Separate multiple addresses by
commas.

[]> admin@example.com


Load message from disk?  [Y]> n


Enter or paste the message body here.  Enter '.' on a blank line to end.

This is a test message.

.


HAT matched on unnamed sender group, host ALL

 - Applying $ACCEPTED policy (ACCEPT behavior).

 - Maximum Message Size:  100M (Default)

 - Maximum Number Of Connections From A Single IP:  1000 (Default)

 - Maximum Number Of Messages Per Connection:  1,000 (Default)

 - Maximum Number Of Recipients Per Message:  1,000 (Default)

 - Maximum Recipients Per Hour:  100 (Default)

 - Use SenderBase For Flow Control:  Yes (Default)

 - Spam Detection Enabled:  Yes (Default)
```

```
 - Virus Detection Enabled:  Yes (Default)

 - Allow TLS Connections:  No (Default)


Processing MAIL FROM:

 - Default Domain Processing:  No Change


Processing Recipient List:

Processing admin@ironport.com

 - Default Domain Processing:  No Change

 - Domain Map:  No Change

 - RAT matched on admin@ironport.com, behavior = ACCEPT

 - Alias expansion:  No Change


Message Processing:

 - No Virtual Gateway(tm) Assigned

 - No Bounce Profile Assigned


Domain Masquerading/LDAP Processing:

 - No Changes.


Processing filter 'always_deliver':

Evaluating Rule:   rcpt-to == "@mail.qa"
```

```
    Result = False

Evaluating Rule:   rcpt-to == "ironport.com"

    Result = True

Evaluating Rule:   OR

    Result = True

Executing Action:  deliver()


Footer Stamping:

 - Not Performed


Inbound Recipient Policy Processing: (matched on Management Upgrade
policy)

Message going to:  admin@ironport.com


AntiSpam Evaluation:

 - Not Spam


AntiVirus Evaluation:

 - Message Clean.

 - Elapsed Time = '0.000 sec'


VOF Evaluation:
```

```
 - No threat detected


Message Enqueued for Delivery


Would you like to see the resulting message? [Y]> y




Final text for messages matched on policy Management Upgrade

Final Envelope Sender:  pretend.sender@example.doma

Final Recipients:

 - admin@ironport.com


Final Message Content:


Received: from remotehost.example.com (HELO TEST) (1.2.3.4)

  by stacy.qa with TEST; 19 Oct 2004 00:54:48 -0700

Message-Id: <3i93q9$@Management>

X-IronPort-AV: i="3.86,81,1096873200";

   d="scan'208"; a="0:sNHT0"

Subject: hello
```

```
This is a test message.


Run through another debug session? [N]>
```

アプライアンスのテストにリスナーを使用

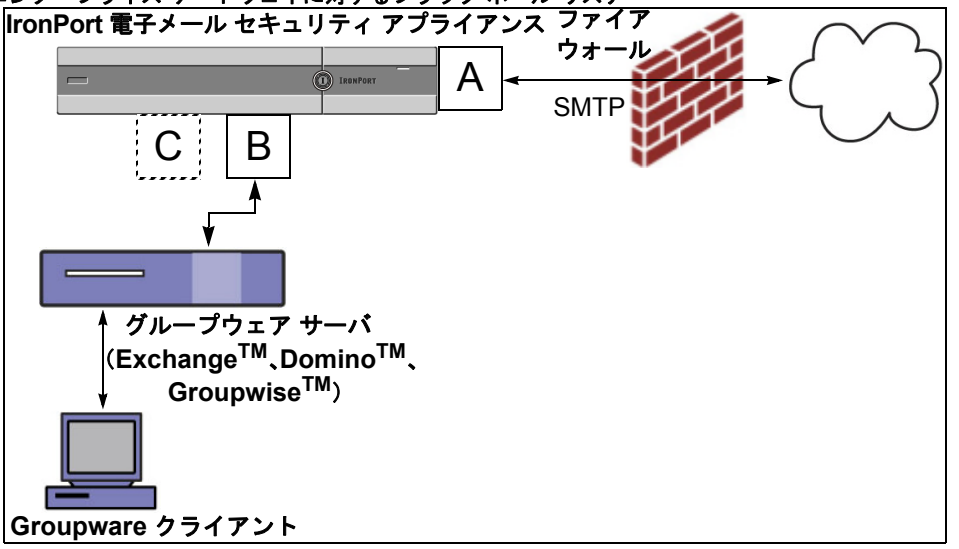
「ブラック ホール」リスナーを使用して、メッセージ生成システムをテストして、受信側のパフォーマンスの大まかな測定を行うことができます。ブラック ホール リスナーには、*キューイング*と*非キューイング*の 2 つのタイプがあります。

キューイング リスナーは、メッセージをキューに保存しますが、その後メッセージをただちに削除します。非キューイング リスナーはメッセージを承認した後、保存しないですぐに削除します。

メッセージ生成システムのインジェクション部分全体のパフォーマンスを測定する場合は、キューイング リスナーを使用します。メッセージ生成システムからアプライアンスまでの接続のトラブルシューティングを行う場合は、非キューイング リスナーを使用します。

たとえば、図 9-4 では、ブラック ホール リスナー「C」を作成して、「B」というプライベート リスナーをミラーリングします。非キューイング版では、グループウェア クライアントからグループウェア サーバを経由してアプライアンスまでのシステムのパフォーマンス パスをテストします。キューイング版では、同じパスと、メッセージをキューイングして SMTP 経由の配信を準備するアプライアンスの能力をテストします。

図 9-4　エンタープライズ ゲートウェイに対するブラック ホール リスナー



次の例では、listenerconfig コマンドを使用して、管理インターフェイスで BlackHole_1 という名前のキューイング タイプのブラック ホール リスナーを作成します。次に、このリスナー用の Host Access Table（HAT）を編集して、次のホストからの接続を受け入れるようにします。

- yoursystem.example.com
- 10.1.2.29
- badmail.tst
- .tst

（注）　最後のエントリである .tst により、.tst ドメイン内にあるすべてのホストから BlackHole_1 という名前のリスナーに電子メールを送信できるようになります。

例

```
mail3.example.com> listenerconfig


Currently configured listeners:
```

```
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new


Please select the type of listener you want to create.

1. Private

2. Public

3. Blackhole

[2]> 3


Do you want messages to be queued onto disk?  [N]> y


Please create a name for this listener (Ex: "OutboundMail"):

[]> BlackHole_1


Please choose an IP interface for this Listener.
```

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

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Choose a protocol.

1. SMTP

2. QMQP

[1]> 1


Please enter the IP port for this listener.

[25]> 25


Please specify the systems allowed to relay email through the IronPort
C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.

[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst


Do you want to enable rate limiting per host? (Rate limiting defines
```

```
the maximum number of recipients per hour you are willing to receive from
a remote domain.) [N]> n


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control:  No

Spam Detection Enabled:  No

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy?  [N]> n


Listener BlackHole_1 created.

Defaults have been set for a Black Hole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.
```

```
Currently configured listeners:

1. BlackHole_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole
Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

（commit コマンドを実行して、これらの変更が有効になるようにしてください）

キューイング タイプのブラック ホール リスナーを設定して、HAT でインジェクション システムからの接続を受け入れるよう変更したら、インジェクション システムを使用して、アプライアンスへの電子メールの送信を開始します。status、status detail、および rate コマンドを使用して、システムのパフォーマンスをモニタします。また、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）でシステムをモニタすることもできます。詳細については、次の資料を参照してください。

- 「CLI によるモニタリング」（P.6-239）
- 「GUI でのその他の作業」（P.7-289）

ネットワークのトラブルシューティング

アプライアンスのネットワーク接続に問題があることが疑われる場合は、まずそのアプライアンスが正常に動作していることを確認してください。

アプライアンスのネットワーク接続のテスト方法

アプライアンスがネットワーク上でアクティブであり、電子メールを送信できることを確認するには、次の手順に従ってください。

ステップ 1　システムに接続し、管理者としてログインします。正常にログインできると、次のメッセージが表示されます。

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.


AsyncOS x.x for Cisco IronPort


Welcome to the Cisco IronPort Messaging Gateway Appliance(tm)
```

ステップ 2　`status` コマンドまたは `status detail` コマンドを使用します。

```
mail3.example.com> status
```

または

```
mail3.example.com> status detail
```

`status` コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返される統計情報は、カウンタとゲージの 2 つのカテゴリにグループ化されます。レートなどの電子メールの動作についての全般的なモニタリング情報については、`status detail` コマンドを使用します。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム リブート以降、およびシステムの存続期間に発生したイベントの合計数を表示できます（詳細は、「CLI によるモニタリング」（P.6-239）を参照してください）。

ステップ 3　`mailconfig` コマンドを使用して、機能している既知のアドレスに電子メールを送信します。

mailconfig コマンドによって、アプライアンスで有効な設定のすべてが含まれる、人が読み取ることのできるファイルが作成されます。このファイルをアプライアンスから機能する既知の電子メール アドレスに送信して、アプライアンスがネットワークで電子メールを送信できることを確認します。

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send the

configuration file.

Separate multiple addresses with commas.


[]> user@example.com


Do you want to include passwords? Please be aware that a configuration
without passwords will fail when reloaded with loadconfig.  [N]> y


The configuration file has been sent to user@example.com.

mail3.example.com>
```

トラブルシューティング

アプライアンスがネットワーク上でアクティブであることが確認されたら、次のコマンドを使用して、ネットワークの問題をピンポイントで特定します。

- netstat コマンドを使用すると、次のようなネットワーク接続（着信と発信の両方）、ルーティング テーブル、ネットワーク インターフェイスのさまざまな統計情報が表示されます。
  - アクティブなソケットのリスト
  - ネットワーク インターフェイスの状態
  - ルーティング テーブルの内容

  - リッスン キューのサイズ
  - パケット トラフィック情報

- `diagnostic -> network -> flush` コマンドを使用すると、ネットワークに関連するすべてのキャッシュをフラッシュできます。
- `diagnostic -> network -> arpshow` コマンドを使用すると、システムの ARP キャッシュを表示できます。
- `packetcapture` コマンドを使用すると、コンピュータが接続されているネットワーク上で送受信されている TCP/IP や他のパケットを傍受して表示できます。

  `packetcapture` を使用するには、ネットワーク インターフェイスとフィルタを設定します。このフィルタでは、UNIX の `tcpdump` コマンドと同じ形式を使用します。パケットの捕捉を開始するには `start` を、停止するには `stop` を使用します。捕捉を停止した後、SCP または FTP を使用して `/pub/captures` ディレクトリからファイルをダウンロードする必要があります。詳細については、「パケット キャプチャ」（P.8-325）を参照してください。
- アプライアンスでネットワーク上にアクティブな接続があり、ネットワーク上の特定のセグメントに到達できることを確認するには、動作している既知のホストに対して `ping` コマンドを使用します。

  `ping` コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストできます。

```
mail3.example.com> ping


Which interface do you want to send the pings from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1
```

```
Please enter the host you wish to ping.

[]> anotherhost.example.com


Press Ctrl-C to stop.

PING anotherhost.example.com (x.x.x.x): 56 data bytes

64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms

64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms

^C

--- anotherhost.example.com ping statistics ---

11 packets transmitted, 11 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

（注）　ping コマンドを終了するには、Ctrl+C を使用します。

- traceroute コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

```
mail3.example.com> traceroute


Which interface do you want to trace from?

1. Auto

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

```
3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Please enter the host to which you want to trace the route.

[]> 10.1.1.1


Press Ctrl-C to stop.

traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets

 1  gateway (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms

 2  hostname (10.1.1.1)  0.298 ms  0.302 ms  0.291 ms

mail3.example.com>
```

- diagnostic -> network -> smtpping コマンドを使用すると、リモートの SMTP サーバをテストできます。
- nslookup コマンドを使用すると、DNS の機能をテストできます。

  nslookup コマンドでは、アプライアンスから動作している Domain Name Service（DNS; ドメイン ネーム サービス）サーバを使用してホスト名や IP アドレスを解決して到達できることを確認できます。

```
mail3.example.com> nslookup


Please enter the host or IP to resolve.

[]> example.com
```

```
Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>


A=192.0.34.166 TTL=2d
```

表 9-3　DNS の機能の確認：クエリーのタイプ

クエリーのタイプ	説明
A	ホストのインターネット アドレス
CNAME	エイリアスの正規の名前
MX	メール エクスチェンジャ
NS	指定したゾーンのネーム サーバ
PTR	クエリーがインターネット アドレスの場合はホスト名、そうでない場合は他の情報に対するポインタ
SOA	ドメインの「start-of-authority（権威の開始）」情報
TXT	テキスト情報

- tophosts コマンドを CLI または GUI から使用して、「Active Recipients」の順にソートします。

  tophosts コマンドからは、キューにある上位 20 の受信者のリストが返されます。このコマンドは、ネットワーク接続の問題が、電子メールを送信しようとしている 1 台のホストまたは 1 つのホスト グループに限定されるかどうかを確認するのに役立ちます（詳細については、49 ページの「メール キューの構成の確認」を参照してください）。

```
mail3.example.com> tophosts


Sort results by:

1. Active Recipients

2. Connections Out

3. Delivered Recipients

4. Soft Bounced Events
```

```
5. Hard Bounced Recipients

[1]> 1


Status as of:         Mon Nov 18 22:22:23 2003

    ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1  aol.com36510255218

2  hotmail.com29071982813

3  yahoo.com13461231119

4  excite.com9838494

5  msn.com8427633  29

^C
```

- tophosts コマンドの結果として得られたリストの最上位のドメインに対して hoststatus コマンドを実行し、詳しく調べます。

  hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です（詳細は、「メール ホストのステータスのモニタリング」（P.6-247）を参照してください）。

  最上位のドメインに対して hoststatus コマンドを実行すると、アプライアンスまたはインターネットのいずれかに対する DNS 解決のパフォーマンスの問題を切り分けることができます。たとえば、最上位のアクティブな受信ホストに対して hoststatus コマンドを実行したとき、発信側の多数の接続が保留状態で表示された場合は、特定のホストがダウン状態または到達不能でないかどうか、またアプライアンスがすべてのホストあるいは大半のホストに接続不可能でないかどうかを確認してください。

- ファイアウォールの権限を確認します。

  アプライアンスが正しく機能するためには、ポート 20、21、22、23、25、53、80、123、443、および 628 を開く必要がある場合があります（詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録 C、「Firewall Information」を参照してください）。

- ネットワーク上のアプライアンスから、`dnscheck@ironport.com` に対して電子メールを送信します。

  ネットワーク内から `dnscheck@ironport.com` に対して電子メールを送信して、システム上で基本的な DNS の確認を行います。オートレスポンダによる電子メールによって、次の 4 つのテストについての結果と詳細が返されます。

  DNS PTR レコード：Envelope From の IP アドレスがドメインの PTR レコードと一致するか。

  DNS A レコード：ドメインの PTR レコードが Envelope From の IP アドレスと一致するか。

  HELO マッチ：SMTP HELO コマンドにリストされたドメインが、Envelope From の DNS ホスト名と一致するか。

  遅延バウンス メッセージを受け入れるメール サーバ：SMTP HELO コマンドのリストにあるドメインに、そのドメインの IP アドレスを解決する MX レコードがあるか。

リスナーのトラブルシューティング

電子メールのインジェクションに問題があると疑われる場合は、次の方法を使用します。

- インジェクションを行っている IP アドレスを確認し、`listenerconfig` コマンドを使用して許可されているホストを確認します。

  作成したリスナーに接続できるよう IP アドレスが許可されていますか。`listenerconfig` コマンドを使用して、リスナーの Host Access Table（HAT）を確認します。次のコマンドを使用して、リスナーの HAT を出力します。

  `listenerconfig` -> `edit` -> *listener_number* -> `hostaccess` -> `print`

HAT は、IP アドレス、IP アドレスのブロック、ホスト名、ドメインなどを使用して、接続を拒否するよう設定できます。詳細については、「接続が許可されているホストの指定」（P.107）を参照してください。

また、limits サブコマンドを使用して、リスナーに許可されている接続の最大数を確認することもできます。

`listenerconfig -> edit -> listener_number -> limits`

- インジェクションを行っているマシンから、Telnet または FTP を使用して、アプライアンスに手動で接続します。次の例を参考にしてください。

```
injection_machine% telnet appliance_name
```

アプライアンス内で telnet コマンドを使用して、リスナーから実際のアプライアンスに接続することもできます。

```
mail3.example.com> telnet


Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3


Enter the remote hostname or IP.

[]> 193.168.1.1


Enter the remote port.
```

```
[25]> 25


Trying 193.168.1.1...

Connected to 193.168.1.1.

Escape character is '^]'.
```

あるインターフェイスから他のインターフェイスに接続できない場合は、アプライアンスの Management、Data1、Data2 インターフェイスからネットワークに接続している方法に問題がある可能性があります。telnet を使用して接続を試みている場合は、ターゲットとするインターフェイスで telnet サービスがイネーブルになっていることを確認してください。詳細については、Appendix A, “Accessing the Appliance” を参照してください。また、リスナーのポート 25 に対して telnet を実行して、SMTP コマンドを手動で入力することもできます（このプロトコルを熟知している場合）。

- IronPort のテキスト メール ログおよびインジェクション デバッグ ログを調べて、受信エラーがあるかどうかを確認します。

  インジェクション デバッグ ログには、アプライアンスとシステムに接続している特定のホストとの間の SMTP カンバセーションが記録されています。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントとアプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、[Sent to]（接続ホストに送信）または [Rcvd from]（接続ホストから受信）に分類されます。

  詳細については、「IronPort テキスト メール ログの使用」（P.5-173）および「IronPort インジェクション デバッグ ログの使用」（P.5-191）を参照してください。

配信のトラブルシューティング

アプライアンスからの電子メールの配信に問題があると疑われる場合は、次の方法を試してください。

- 問題がドメインに限定されたものであるかどうかを判断します。

tophosts コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

「Active Recipients」の順にソートすると、問題のあるドメインが返されますか。

「Connections Out」の順にソートしたとき、リスナーに指定されている最大接続数に達しているドメインがありますか。リスナーに対するデフォルトの最大接続数は 600 です。システム全体でのデフォルトの最大接続数は 10,000 です（deliveryconfig コマンドで設定します）。リスナーに対する最大接続数は、次のコマンドで確認できます。

listenerconfig -> edit -> *injector_number* -> limits

リスナーに対する接続が、destconfig コマンドによってさらに制限されていませんか（システムの最大数または仮想ゲートウェイ アドレスによる）。destconfig による接続の制限を確認するには、次のコマンドを使用します。

destconfig -> list

- hoststatus コマンドを使用します。

  tophosts コマンドの結果として得られたリストの最上位のドメインに対して hoststatus コマンドを実行し、詳しく調べます。

  ホストが使用可能で、接続を受け入れていますか。

  指定したホストに対する特定の MX レコードのメール サーバに問題がありませんか。

  hoststatus コマンドでは、特定のホストに対する 5XX エラー（Permanent Negative Completion Reply）がある場合に、ホストから返された直前の「5XX」のステータス コードと説明が表示されます。このホストに対する直前の発信 TLS 接続が失敗した場合は、hoststatus コマンドで失敗した理由が表示されます。

- ドメインのデバッグ、バウンス、およびテキスト メールの各ログを設定および確認して、受信ホストが使用可能かどうかをチェックします。

  ドメイン デバッグ ログには、アプライアンスと指定した受信ホスト間での SMTP カンバセーションの際のクライアントとサーバの接続が記録されます。このタイプのログ ファイルは、特定の受信ホストに関する問題のデバッグに使用できます。

  詳細については、「IronPort ドメイン デバッグ ログの使用」（P.5-190）を参照してください。

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。

詳細については、「IronPort バウンス ログの使用」（P.5-185）を参照してください。

テキスト メール ログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。ステータス情報も、1 分ごとにメール ログに書き込まれます。これらのログは、特定のメッセージの配信を理解し、システム パフォーマンスを分析するうえで有益な情報源となります。

詳細については、「IronPort テキスト メール ログの使用」（P.5-173）を参照してください。

- `telnet` コマンドを使用して、アプライアンスから問題のあるドメインに接続します。

```
mail3.example.com> telnet


Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Enter the remote hostname or IP.

[]> problemdomain.net


Enter the remote port.

[25]> 25
```

- 必要に応じて tlsverify コマンドを使用して発信 TLS 接続を確立し、宛先ドメインに関する TLS 接続の問題をデバッグすることができます。接続を確立するには、検証するドメインと宛先ホストを指定します。AsyncOS では、必要な（検証）TLS 設定に基づいて TLS 接続を確認します。

```
mail3.example.com> tlsverify


Enter the TLS domain to verify against:

[]> example.com


Enter the destination host to connect to.  Append the port
(example.com:26) if you are not connecting on port 25:

[example.com]> mxe.example.com:25


Connecting to 1.1.1.1 on port 25.

Connected to 1.1.1.1 from interface 10.10.10.10.

Checking TLS connection.

TLS connection established: protocol TLSv1, cipher RC4-SHA.

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.
```

```
TLS successfully connected to mxe.example.com.

TLS verification completed.
```

パフォーマンスのトラブルシューティング

アプライアンスのパフォーマンスに関する問題があると疑われる場合は、次の方法を使用してください。

- `rate` コマンドと `hostrate` コマンドを使用して、現在のシステムのアクティビティを確認します。

  `rate` コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。詳細については、「リアルタイム アクティビティの表示」（P.6-255）を参照してください。

  `hostrate` コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。

- `status` コマンドを使用して、これまでのレートを比較して、状態の悪化を確認します。
- `status detail` コマンドを使用して、メモリの使用率を確認します。

  `status detail` コマンドを使用すると、システムのメモリ、CPU、ディスク I/O の使用率を、素早く確認できます。

（注） メモリの使用率は、常に 75 % 未満である必要があります。メモリの使用率が 75 % を超えると、アプライアンスは「リソース節約モード」に入ります。これによって「バックオフ」アルゴリズムが起動され、リソースのオーバーサブスクリプションが防止され、電子メールによる次のアラートが送信されます。

```
This system (hostname: hostname) has entered a 'resource conservation'
mode in order to prevent the rapid depletion of critical system
resources.
```

```
RAM utilization for this system has exceeded the resource conservation
threshold of 75%. The allowed injection rate for this system will be
gradually decreased as RAM utilization approaches 85%.
```

この状況は、配信機能が低下していて、大量のインジェクションが行われているときにのみ発生します。メモリの使用率が 75 % を超えたときには、キュー内のメッセージの数を調べて、特定のドメインがダウン状態または配信不可能になっていないかどうかを確認します（`hoststatus` コマンドまたは `hostrate` コマンドを使用します）。また、システムのステータスも確認して、配信が中断されないようにします。インジェクションが停止しても、依然としてメモリの使用率が高い場合は、IronPort カスタマー サポートにご連絡ください。「IronPort Customer Support」（P.1-7）を参照してください。

- 問題が 1 つのドメインに限定されていますか。

  `tophosts` コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

  キューのサイズを確認します。このサイズを制御したり、問題が生じている特定のドメインの受信者に対処するために、電子メール キューにあるメッセージを削除、バウンス、中断、またはリダイレクトすることができます。詳細については、「電子メール キューの管理」（P.6-263）を参照してください。以下のコマンドを使用します。

  - `deleterecipients`
  - `bouncerecipients`
  - `redirectrecipients`
  - `suspenddel` / `resumedel`
  - `suspendlistener` / `resumelistener`

  `tophosts` コマンドを使用して、ソフト バウンスおよびハード バウンスの数を確認します。[Soft Bounced Events]（オプション 4）または [Hard Bounced Recipients]（オプション 5）でソートします。特定のドメインに対するパフォーマンスに問題があることが疑われる場合は、上記のコマンドを使用して、そのドメインへの配信を制御します。