



Cisco IronPort AsyncOS 7.5 for Email コン フィギュレーション ガイド

2011 年 10 月 27 日

【注意】 シスコ製品をご使用になる前に、安全上の注意 (www.cisco.com/jp/go/safety_warning/) をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco IronPort AsyncOS 7.5 for Email コンフィギュレーションガイド

© 2011 Cisco Systems, Inc.

All rights reserved.

Copyright © 2011–2012, シスコシステムズ合同会社.

All rights reserved.



CONTENTS

CHAPTER 1

Cisco IronPort 電子メール セキュリティ アプライアンスをご使用の前に 1-1

今回のリリースでの変更点 1-1

電子メール セキュリティ アプライアンスのアップデート 1-2

新機能：クラウド ユーザ ロール 1-2

クラウド ユーザ アカウント パスワード設定の変更 1-3

新機能：感染フィルタ 1-3

新機能：委任管理 1-4

新機能：限定的なユーザ アカウントおよびパスワードの設定 1-4

新機能：技術者ユーザ ロール 1-5

拡張機能：Administrator ロール 1-5

拡張機能：大量メッセージのスキャン 1-5

新機能：SMTP call-ahead 1-6

拡張機能：DLP ヘッダー スキャン 1-6

新機能：設定履歴ログ 1-6

新機能：スケジュール済みログ ロールオーバー 1-7

新機能：HTTP/HTTPS を使用して手動でダウンロードされたログ 1-7

拡張機能：サービス アップデート拡張機能 1-7

拡張機能：プロキシを介した IP ベースのアクセス 1-8

拡張機能：HTML 免責事項 1-8

拡張機能：Web UI セッション タイムアウト 1-8

拡張機能：メッセージ トラッキングを使用した添付ファイル検索 1-9

拡張機能：レポート作成拡張機能 1-9

拡張機能 : PDF レポートの国際化	1-9
新しい CLI コマンドおよび更新された CLI コマンド	1-9
電子メール セキュリティ アプライアンスのマニュアル セット	1-10
このガイドの使い方	1-12
はじめる前に	1-12
本書の構成	1-13
『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』で説明されているトピック	1-15
『Cisco IronPort AsyncOS for Email Daily Management Guide』では、次のトピックが説明されています。	1-16
印刷時の表記法	1-18
その他の情報の入手先	1-18
シスコのテクニカル サポート	1-20
サードパーティ コントリビュータ	1-21
Cisco IronPort 電子メール セキュリティ アプライアンスの概要	1-22
メール フローおよび Cisco IronPort M-Series アプライアンス	1-24

CHAPTER 2

概要	2-1
Web ベースのグラフィカル ユーザ インターフェイス (GUI)	2-1
アクティブなセッションの表示	2-7
コマンドライン インターフェイス (CLI)	2-8
コマンドライン インターフェイスの表記法	2-8
汎用 CLI コマンド	2-13

CHAPTER 3

セットアップおよび設置	3-1
設置計画	3-2
はじめる前に	3-2
インストール シナリオ	3-4
サポート言語	3-7

物理寸法	3-8
Cisco IronPort アプライアンスのネットワークへの物理接続	3-9
設定シナリオ	3-9
セットアップの準備	3-12
アプライアンスへの接続方式の決定	3-13
ネットワーク アドレスと IP アドレスの割り当ての決定	3-15
セットアップ情報の収集	3-16
System Setup Wizard の使用方法	3-19
Web ベースのグラフィカル ユーザ インターフェイス (GUI) の利用	3-20
Web ベースの System Setup Wizard の実行	3-21
Active Directory の設定	3-35
次の手順	3-37
コマンドライン インターフェイス (CLI) へのアクセス	3-38
コマンドライン インターフェイス (CLI) System Setup Wizard の実行	3-39
次の手順 : 電子メール パイプラインの理解	3-58

CHAPTER 4
電子メール パイプラインの理解 4-1

概要 : 電子メール パイプライン 4-1

着信および受信 4-5

 ホスト アクセス テーブル (HAT)、送信者グループ、およびメール
 フロー ポリシー 4-5

Received: ヘッダー 4-6

デフォルト ドメイン 4-6

バウンス検証 4-7

ドメイン マップ 4-7

受信者アクセス テーブル (RAT) 4-7

エイリアス テーブル 4-7

LDAP 受信者の受け入れ 4-8

SMTP Call-Ahead 受信者検証	4-8
ワーク キューとルーティング	4-8
電子メール パイプラインとセキュリティ サービス	4-9
LDAP 受信者の受け入れ	4-10
マスカレードまたは LDAP マスカレード	4-10
LDAP ルーティング	4-10
メッセージ フィルタ	4-11
電子メール セキュリティ マネージャ (受信者単位のスキャン)	4-11
検疫	4-13
配信	4-14
仮想ゲートウェイ	4-14
配信制限	4-14
ドメインベースの制限値	4-15
ドメインベースのルーティング	4-15
グローバル配信停止	4-15
バウンス制限	4-16

CHAPTER 5

電子メールを受信するためのゲートウェイの設定	5-1
リスナーによる電子メールの受信	5-2
エンタープライズ ゲートウェイ構成	5-3
ホスト アクセス テーブル (HAT) :	
送信者グループとメール フロー ポリシー	5-9
メール フロー ポリシー : アクセス ルールとパラメータ	5-11
送信者グループ	5-25
GUI による送信者グループとメール フロー ポリシーの管理	5-43
GUI によるリスナーの HAT の変更	5-53
HAT の操作	5-55
送信者検証	5-56
送信者検証 : ホスト	5-57

送信者検証：エンベロープ送信者	5-58
送信者検証の実装 — 設定例	5-61
送信者検証設定のテスト	5-69
送信者検証とロギング	5-71
CLI でのホスト DNS 検証のイネーブル化	5-72
パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ	5-72
受信者アクセス テーブル（RAT）	5-73
GUI によるリスナーの RAT の変更	5-77
新しい RAT エントリの追加	5-78
RAT エントリの削除	5-79
RAT エントリの変更	5-79
RAT エントリの順序の変更	5-79
RAT エントリのエクスポート	5-80
RAT エントリのインポート	5-80
CHAPTER 6	電子メール セキュリティ マネージャ 6-1
ユーザベース ポリシーの概要	6-2
着信および 発信メッセージ	6-3
ポリシー マッチング	6-4
メッセージ分裂	6-6
ポリシーの内容	6-9
コンテンツ フィルタの概要	6-10
実際の例（GUI）	6-31
電子メール セキュリティ マネージャへのアクセス	6-32
デフォルト ポリシーの編集：アンチスパム設定	6-34
新しいポリシーの作成	6-36
カスタム ポリシーの作成	6-40
電子メール セキュリティ マネージャのポリシーのユーザの検索	6-46

新しいコンテンツ フィルタの作成	6-48
個々のポリシーへのコンテンツ フィルタのイネーブル化および適用	6-53
GUI でのコンテンツ フィルタの設定に関する注意事項	6-57

CHAPTER 7

評価フィルタリング 7-1

評価フィルタリング	7-2
評価フィルタリング : Cisco IronPort SenderBase 評価サービス	7-3
SenderBase 評価スコア (SBRs)	7-4
SenderBase 評価フィルタの実装	7-6
評価フィルタリングの設定	7-7
リスナーの HAT での評価フィルタリング実装	7-9
SBRs を使用した評価フィルタリングのテスト	7-11
SenderBase 評価サービスのステータスのモニタリング	7-14

CHAPTER 8

アンチスパム 8-1

アンチスパムの概要	8-2
アンチスパム スキャンのイネーブル化	8-2
アンチスパム スキャン エンジンの設定値	8-5
アンチスパム スキャンと Cisco IronPort アプライアンスによって生成されるメッセージ	8-5
IronPort Anti-Spam フィルタリング	8-6
IronPort Anti-Spam および CASE の概要	8-6
IronPort Anti-Spam のイネーブル化とグローバル設定値の設定	8-9
IronPort Intelligent Multi-Scan フィルタリング	8-14
IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定	8-15
アンチスパム ルールのアップデートの設定	8-18

アンチスパムの受信者別ポリシーの設定	8-19
陽性および陽性と疑わしいスパムのしきい値	8-24
陽性と判定されたスパムと陽性と疑わしいスパム	8-26
不要なマーケティング メッセージの検出	8-26
IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー	8-27
誤って分類されたメッセージの Cisco IronPort Systems への報告	8-28
IronPort Anti-Spam のテスト	8-28
着信リレー	8-31
着信リレー機能 : 概要	8-33
メッセージ ヘッダーと着信リレー	8-35
着信リレー機能の設定 (GUI)	8-40
着信リレーとロギング	8-43

CHAPTER 9

アンチウイルス	9-1
アンチウイルス スキャン	9-2
評価キー	9-2
マルチレイヤ アンチウイルス スキャン	9-2
Sophos Anti-Virus フィルタリング	9-3
ウイルス検出エンジン	9-3
ウイルス スキャン	9-4
検出方法	9-4
ウイルスの記述	9-6
Sophos アラート	9-6
ウイルスが発見された場合	9-6
McAfee Anti-Virus フィルタリング	9-7
ウイルス シグニチャとのパターン照合	9-7
暗号化されたポリモーフィック型ウイルスの検出	9-7
発見的分析	9-8

ウイルスが発見された場合	9-8
ウイルス スキャンのイネーブル化およびグローバル設定の構成	9-9
概要	9-9
ウイルス スキャンのイネーブル化およびグローバル設定の構成	9-10
HTTP を使用した Anti-Virus アップデートの取得	9-11
モニタリングおよび手動でのアップデート チェック	9-11
ユーザのウイルス スキャン アクションの設定	9-12
メッセージ スキャン設定	9-13
メッセージ処理設定	9-14
メッセージ処理アクションの設定の構成	9-15
メール ポリシーのアンチウイルス設定の編集	9-21
アンチウイルス設定に関する注意事項	9-25
アンチウイルス アクションのフロー ダイアグラム	9-27
ウイルス スキャンのテスト	9-28

CHAPTER 10

感染フィルタ 10-1

感染フィルタの概要	10-2
脅威カテゴリ	10-3
感染フィルタ：マルチレイヤの対象保護	10-5
Cisco Security Intelligence Operations	10-5
Context Adaptive Scanning Engine	10-6
メッセージの遅延	10-7
URL のリダイレクト	10-8
メッセージの変更	10-9
ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール	10-10
アウトブレイク	10-11
脅威レベル	10-12
感染フィルタの機能概要	10-13

動的検疫	10-15
感染フィルタの管理 (GUI)	10-18
感染フィルタのグローバル設定の構成	10-19
感染フィルタ ルール	10-21
感染フィルタ 機能とメール ポリシー	10-22
感染フィルタ 機能と Outbreak 検疫	10-28
感染フィルタのモニタリング	10-31
感染フィルタ レポート	10-31
感染フィルタの概要とルール リスト	10-31
Outbreak 検疫	10-32
アラート、SNMP トラップ、および感染フィルタ	10-32
感染フィルタ 機能のトラブルシューティング	10-33

CHAPTER 11
データ 消失防止 11-1

Email DLP の動作を理解する	11-2
ハードウェア要件	11-4
RSA Email DLP グローバル設定	11-4
RSA Email DLP のイネーブル化とグローバル設定の設定	11-5
DLP ポリシー	11-6
ポリシーのコンテンツ	11-7
DLP Policy Manager	11-8
事前定義されたテンプレートをもとにした Email DLP ポリシーの作成	11-11
DLP ポリシーに対する分類子のカスタマイズ	11-12
DLP ポリシーのメッセージのフィルタリング	11-14
重大度レベルの設定	11-15
Email DLP ポリシーの順序の設定	11-16
Email DLP ポリシーの編集	11-16
Email DLP ポリシーの削除	11-17
Email DLP ポリシーの複製	11-17

DLP Assessment Wizard の使用	11-17
DLP Assessment Wizard の実行	11-18
コンテンツ照合分類子	11-23
分類子検出ルール	11-24
分類子の例	11-25
コンテンツ照合分類子用の正規表現	11-29
DLP 用の正規表現の例	11-30
高度な DLP ポリシーのカスタマイズ	11-31
Custom Policy テンプレートを使用した DLP ポリシーの作成	11-31
コンテンツ照合分類子の作成	11-33
RSA Email DLP の受信者ごとのポリシーの設定	11-34
メール ポリシーの DLP 設定の編集	11-34

CHAPTER 12

Cisco IronPort 電子メール暗号化	12-1
Cisco IronPort 電子メール暗号化：概要	12-1
暗号化ワークフロー	12-2
電子メール暗号化プロファイルの設定	12-4
電子メール暗号化グローバル設定の編集	12-4
暗号化プロファイルの追加	12-5
PXE エンジンの更新	12-10
暗号化コンテンツ フィルタの設定	12-11
TLS 接続を暗号化の代わりに使用	12-11
Encrypt and Deliver Now コンテンツ フィルタの作成	12-12
Encrypt on Delivery コンテンツ フィルタの作成	12-14
メッセージへの暗号化ヘッダーの追加	12-16
暗号化ヘッダー	12-18
暗号化ヘッダーの例	12-20

CHAPTER 13**SenderBase Network Participation 13-1**

共有のイネーブル化 13-1

よくあるご質問 13-3

CHAPTER 14**テキスト リソース 14-1**

概要 14-1

コンテンツ ディクショナリ 14-3

ディクショナリの内容 14-3

テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 14-4

コンテンツ ディクショナリの管理 (GUI) 14-6

ディクショナリの追加 14-6

ディクショナリの編集 14-9

ディクショナリの削除 14-9

ディクショナリのインポート 14-9

ディクショナリのエクスポート 14-10

コンテンツ ディクショナリを使用する方法およびテスト方法 14-11

ディクショナリの照合フィルタ ルール 14-11

DLP ディクショナリ 14-13

カスタム ディクショナリの追加 14-14

カスタム DLP ディクショナリの編集 14-15

カスタム DLP ディクショナリの削除 14-16

DLP ディクショナリのインポートおよびエクスポート 14-16

テキスト リソースについて 14-18

テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする 14-19

テキスト リソースの管理 (GUI) 14-20

テキスト リソースの追加 14-21

テキスト リソースの編集 14-21

テキスト リソースの削除	14-22
テキスト リソースのインポート	14-22
テキスト リソースのエクスポート	14-23
HTML ベースのテキスト リソースの使用	14-24
テキスト リソースの使用	14-27
免責事項テンプレート	14-27
免責事項スタンプと複数エンコード方式	14-34
通知テンプレート	14-37
アンチウイルス通知テンプレート	14-38
バウンス通知および暗号化失敗通知テンプレート	14-42
DLP 通知テンプレート	14-44
暗号化通知テンプレート	14-47

CHAPTER 15

システム管理 15-1

AsyncOS のアップグレード	15-2
アップグレードする前に	15-2
GUI からの AsyncOS のアップグレード	15-3
CLI からの AsyncOS のアップグレード	15-4
AsyncOS アップグレード設定値の設定	15-5
ストリーミング アップグレードの概要	15-6
リモート アップグレードの概要	15-7
GUI からのアップグレード設定値の設定	15-10
CLI からのアップグレード設定値の設定	15-11
AsyncOS の復元	15-12
利用可能なバージョン	15-12
復元の影響に関する重要な注意事項	15-12
AsyncOS 復元の実行	15-13
サービスのアップデート	15-16
[Service Updates] ページ	15-16
アップデート設定値の編集	15-17

生成されるさまざまなメッセージに対する返信アドレスの設定	15-23
アラート	15-24
アラートの概要	15-25
IronPort AutoSupport	15-27
アラート メッセージ	15-27
アラート受信者の管理	15-29
アラート設定値の設定	15-32
アラート リスト	15-33
ネットワーク設定値の変更	15-60
システム ホスト名の変更	15-60
ドメイン ネーム システム (DNS) 設定値の設定	15-61
TCP/IP トラフィック ルートの設定	15-67
デフォルト ゲートウェイの設定	15-69
admin ユーザのパスワード変更	15-69
電子メール セキュリティ アプライアンスの設定	15-69
ログイン バナーの追加	15-75
システム時刻	15-75
時間帯の選択	15-76
時刻設定の編集 (GUI)	15-77

CHAPTER 16
C350D アプライアンスのイネーブル化 16-1

概要 : C350D アプライアンス	16-1
C350D の追加機能	16-2
C350D でディセーブルにされる機能	16-2
C350D に適用される AsyncOS 機能	16-4
C350D アプライアンスの設定	16-5
リソースを節約するバウンス設定の指定	16-6
IronPort Mail Merge (IPMM)	16-7
概要	16-7

利点	16-7
Mail Merge の使用	16-8
コマンドの説明	16-12
変数定義に関する注意事項	16-13
IPMM カンバセーションの例	16-14

CHAPTER 17

Cisco IronPort M-Series セキュリティ管理アプライアンス 17-1

概要	17-1
ネットワーク プランニング	17-2
メール フローおよび Cisco IronPort M-Series アプライアンス	17-4
モニタリング サービスの設定	17-5
中央集中型レポートングを使用するための電子メール セキュリティ アプライアンスの設定	17-5
中央集中型トラッキングを使用するための電子メールセキュリティ アプライアンスの設定	17-7
外部 IronPort スпам検疫を使用するための電子メール セキュリティ アプライアンスの設定	17-8

APPENDIX A

アプライアンスへのアクセス A-1

IP インターフェイス	A-2
IP インターフェイスの設定	A-3
FTP アクセス	A-6
secure copy (scp) アクセス	A-10
シリアル接続によるアクセス	A-11

APPENDIX B

ネットワーク アドレスと IP アドレスの割り当て B-1

イーサネット インターフェイス	B-1
IP アドレスとネットマスクの選択	B-2
インターフェイスの設定例	B-3

IP アドレス、インターフェイス、およびルーティング まとめ	B-4 B-5
Cisco IronPort アプライアンスの接続時の戦略	B-5

APPENDIX C	ファイアウォール情報	C-1
-------------------	-------------------	------------

APPENDIX D	IronPort エンドユーザ ライセンス契約書	D-1
	Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書	D-1

GLOSSARY

INDEX



CHAPTER 1

Cisco IronPort 電子メール セキュリティ アプライアンスをご使用前に

この章は、次の内容で構成されています。

- 「今回のリリースでの変更点」(P.1-1)
- 「このガイドの使い方」(P.1-12)
- 「Cisco IronPort 電子メール セキュリティ アプライアンスの概要」(P.1-22)

今回のリリースでの変更点

ここでは、AsyncOS for Email Security 7.5 の新機能および拡張機能について説明します。このリリースの詳細については、製品リリース ノートを参照してください。リリース ノートは、次の URL の Cisco IronPort カスタマー サポート ページから入手できます。

<http://www.cisco.com/web/ironport/index.html>

以前のリリースのリリース ノートを見直して、これまでに追加された機能や拡張を確認すると役立つこともあります。サポート ポータルでこれらのリリース ノートを表示するには、該当するアプライアンスのマニュアル ページの [Earlier Releases] リンクをクリックします。

電子メール セキュリティ アプライアンスのアップデート

3.0.0 リリース以降、Cisco IronPort では、Cisco IronPort Cloud Email Security を実現する基本テクノロジーに対して新しいフォーム ファクタが導入されています。つまり、Cloud Email Security を、シスコが管理するデータセンターの仮想アプライアンスやハードウェア アプライアンスによって実現できるようになりました。この変更は、Cisco IronPort Hybrid Email Security 製品のクラウド層にも適用されます。したがって、このマニュアルで記述された「アプライアンス」、「電子メールセキュリティアプライアンス (ESA)」、または「セキュリティ管理アプライアンス (SMA)」は、すべて物理アプライアンスまたは仮想アプライアンスを意味します。これらのフォーム ファクタで利用可能な機能には違いがなく、このサービスのコンシューマに対してユーザ エクスペリエンスがシームレスになります。

新機能：クラウド ユーザ ロール

このリリースでは、Cloud Email Security のユーザに対して次の新しいユーザ ロールが導入されました。

- **Cloud Administrator.** Cloud Administrator ロールは Cloud Email Security に対して作成された特別な管理者ロールであり、クラウド管理者のロールに固有な管理タスクへのアクセスを許可するよう設計されています。
- **Cloud Operator.** 管理権限が制限されたクラウド オペレータ用ユーザ アカウント。
- **Cloud DLP Admin.** DLP ポリシーを管理する役割のクラウド ユーザ用ユーザ アカウント。
- **Cloud Help Desk.** クラウド ヘルプ デスク ユーザ用ユーザ アカウント。このユーザは、メッセージ トラッキングと、スパム検疫およびシステム検疫に対する完全なアクセス権を持ちます。
- **Cloud Guest.** レポートを実行したり、IronPort スпам検疫およびシステム検疫にアクセスしたりするクラウド ゲスト用のユーザ アカウント。
- **カスタム ユーザ ロール.** クラウド管理者は、DLP ポリシー、電子メール ポリシー、レポート、検疫、ローカル メッセージ トラッキング、暗号化プロファイル、およびトレース デバッグ ツールの任意の組み合わせであるカスタム ユーザ ロールを作成することもできます。

詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」の章にある「Managing Cisco IronPort Cloud Email Security」を参照してください。

クラウド ユーザ アカウント パスワード設定の変更

クラウド ユーザ アカウントでは、Cloud Administrator が変更できないパスワード設定が事前に準備されるようになりました。クラウド ユーザには、次のパスワード設定が準備されます。

- ユーザは、最初のログイン時にパスワードを変更する必要があります。
- ユーザは、6 か月ごとにパスワードを変更する必要があります。

パスワードには最小 8 文字を含める必要があります。また、パスワードには 1 つの大文字 (A ~ Z)、1 つの小文字 (a ~ z)、1 つの数字 (1 ~ 9)、および 1 つの特殊文字 (@#\$\$ など) を含める必要があります。

新機能：感染フィルタ

AsyncOS 7.5 では、ウイルス感染フィルタ機能（現在は「感染フィルタ」）が更新され、ウイルス感染以外に、増加している少量かつ対象を絞った電子メール攻撃からユーザを保護します。これらの感染以外の脅威（フィッシング メッセージ、詐欺、マルウェアの配布など）に使用されるメッセージは複雑であり、進化し続けているため、広範なウイルス感染やスパム キャンペーンよりも検出が難しくなることがあります。感染フィルタ機能の拡張により、ユーザはこれらの攻撃から保護され、マルウェアのダウンロードや機密情報の配布が回避されます。

これらの拡張機能の 1 つは、ユーザが、疑わしいメッセージのいずれかのリンクをクリックしたときにそのメッセージの URL を書き換えてユーザをセキュリティ警告にリダイレクトする 電子メール セキュリティ アプライアンスの新機能です。

このアップデートの一部として、ウイルス感染フィルタの以前の CLI コマンドの名前は次のように変更されました。

- vofconfig から outbreakconfig へ
- vofflush から outbreakflush へ
- vofstatus から outbreakstatus へ
- vofupdate から outbreakupdate へ

感染フィルタ機能には、更新された感染フィルタ レポートと免責事項テンプレート用の新しい感染脅威関連の変数も含まれます。

感染フィルタの詳細については、「[感染フィルタ](#)」(P.10-1) を参照してください。

新機能：委任管理

AsyncOS 7.5 では、アプライアンスの電子メール セキュリティ機能に対するユーザのアクセスを、事前定義された管理者ロール、オペレータ ロール、およびヘルプ デスク ユーザ ロールよりも柔軟に制御できるカスタム ユーザ ロールが追加されました。これらのカスタム ユーザ ロールを使用して組織内のそれぞれのロールを持つユーザに特定の責任を委任できます。この結果、これらの**委任管理者**は、自分のジョブに関連しないシステム設定機能ではなく責任がある電子メール セキュリティ機能にのみアクセスできます。



(注)

カスタム ロールに割り当てられたユーザは、コマンドライン インターフェイス (CLI) にアクセスできません。

詳細については『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。

新機能：限定的なユーザ アカウントおよびパスワードの設定

AsyncOS 7.5 では、ユーザ アカウントおよびパスワードの制限を定義して、組織のパスワード ポリシーをローカルの電子メール セキュリティ アプライアンス ユーザに適用できます。これらの制限は次のとおりです。

- **パスワード ルール。** ユーザが選択できるパスワードの種類（省略可能な文字や必須の文字など）を定義できます。
- **ユーザ アカウント ロック。** ユーザをアカウントからロックするログイン失敗試行回数を定義できます。
- **パスワード存続期間ルール。** パスワードの存続期間を定義できます。この期間が終了する前に、ユーザはログイン後にパスワードを変更する必要があります。

詳細については『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。

新機能：技術者ユーザ ロール

AsyncOS 7.5 では、Cisco IronPort 電子メール セキュリティ アプライアンスをアップグレードするユーザ向けに新しい技術者ロールが追加されました。技術者ロールに割り当てられたユーザはシステム アップグレードの実行、アプライアンスのレポート、機能キーの管理、およびアプライアンスをアップグレードするのに必要な他のアクションの実行を行えます。ユーザ アカウントの詳細については『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。

拡張機能：Administrator ロール

AsyncOS 7.5 以降、管理者はシステム アップグレードを実行し、クラスタを作成し、既存のクラスタにアプライアンスを参加させることができるようになりました。

拡張機能：大量メッセージのスキャン

AsyncOS 7.5 では、スパム送信者によって送信される大量のメッセージをスキャンする一方で電子メール セキュリティ アプライアンスのスループットを最適化するために、アンチスパム スキャンが大量のメッセージを処理する方法が改善されました。*always scan* メッセージ サイズ（定義されたサイズよりも小さいメッセージは Cisco IronPort アンチスパム エンジンによって完全にスキャンされ、Cisco IronPort の業界トップ レベルの性能が引き出されます）と *never scan* メッセージ サイズ（定義されたサイズよりも大きいメッセージはスキャンされません）を定義できます。*always scan* サイズよりも大きく、*never scan* サイズよりも小さいメッセージの場合は、アンチスパム エンジンが限定された高速のスキャンを実行します。

詳細については、「[IronPort Anti-Spam のイネーブル化とグローバル設定値の設定](#)」(P.8-9) を参照してください。

新機能 : SMTP call-ahead

AsyncOS 7.5 には、SMTP call-ahead 受信者検証が含まれます。これにより、受信者への着信メールを受け取る前に外部の SMTP サーバに問い合わせ、電子メールセキュリティ アプライアンスが受信者検証を実行することが可能になります。SMTP call-ahead 受信者検証は、ユーザを検証したいが、受信者検証のために LDAP 承認または受信者アクセス テーブル (RAT) を使用できない場合に役に立ちます。

詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「SMTP Call Ahead」の章を参照してください。

拡張機能 : DLP ヘッダー スキャン

AsyncOS 7.5 以降、RSA Email DLP は DLP ポリシー違反を見つけるために送信元、送信先、CC、および件名ヘッダーをスキャンします。DLP ポリシーが DLP 違反がある発信メッセージを暗号化する場合、これらのヘッダーは暗号化されません。電子メールセキュリティ アプライアンスは、メッセージ本文だけを暗号化します。

新機能 : 設定履歴ログ

AsyncOS 7.5 には、ユーザの名前をリストする追加のセクションがある設定ファイル、ユーザが変更した設定箇所の説明、および変更のコミット時にユーザが入力したコメントから構成される設定履歴ログが含まれます。ユーザが変更をコミットするたびに、変更後の設定ファイルを含む新しいログが作成されます。

詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Logging」の章を参照してください。

新機能 : スケジュール済みログ ロールオーバー

アプライアンス上のログ ファイルが大きくなりすぎないように、AsyncOS 7.5 は、ログ ファイルがユーザ指定の最大ファイル サイズまたは時間間隔に到達したときに「ロールオーバー」を実行し、ログ ファイルをアーカイブし、着信ログ データのために新しいファイルを作成します。ログ サブスクリプションに定義された取得方法に基づき、古いログ ファイルは取得のためにアプライアンスに保存されるか、外部のコンピュータに配信されます。

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」の章を参照してください。

新機能 : HTTP/HTTPS を使用して手動でダウンロードされたログ

AsyncOS 7.5 では、[Log Subscriptions] ページでログ ディレクトリへのリンクをクリックし、次に、アクセスするログ ファイルをクリックすることにより、ログ ファイルにいつでもアクセスできるようになりました。使用しているブラウザに応じて、ブラウザ ウィンドウでファイルを参照したり、ファイルをテキスト ファイルとして開いたり、保存したりできます。この方法は、HTTP (S) プロトコルを使用し、デフォルトの取得方法になります。

拡張機能 : サービス アップデート拡張機能

電子メール セキュリティ アプライアンスは、次のサービスを自動的に更新するようになりました。

- Sophos アンチウイルス定義
- IronPort Anti-Spam および Intelligent Multi-Scan ルール
- タイムゾーン

アップデート設定は [Service Updates] ページを使用して管理できます。詳細については、「[\[Service Updates\] ページ](#)」(P.15-16) を参照してください。

拡張機能：プロキシを介した IP ベースのアクセス

組織のネットワークがリモート ユーザのマシンと電子メール セキュリティ アプライアンス間で逆プロキシ サーバを使用する場合、AsyncOS 7.5 では、ユーザが、アプライアンスに接続できるプロキシの IP アドレスを使用してアクセス リストを作成できます。

詳細については、「[電子メール セキュリティ アプライアンスの設定](#)」(P.15-69) を参照してください。

拡張機能：HTML 免責事項

AsyncOS 7.5 では、HTML ベースおよびプレーン テキストのメッセージを使用していくつかのテキスト リソースを作成できます。テキスト リソースが電子メール メッセージに適用された場合、HTML ベースのテキスト リソース メッセージは電子メール メッセージのテキストまたは HTML 部分に適用され、プレーンテキスト リソース メッセージは電子メール メッセージのテキストまたはプレーン部分に適用されます。

詳細については、「[HTML ベースのテキスト リソースの使用](#)」(P.14-24) を参照してください。

拡張機能：Web UI セッション タイムアウト

AsyncOS 7.5 では、ユーザが電子メール セキュリティ アプライアンスの Web UI にログインし続けることができる時間を指定できます。この時間が経過すると、活動がないため、ユーザは AsyncOS によってログアウトされます。この Web UI セッション タイムアウトは、admin を含むユーザ全員に適用されます。また、HTTP セッションと HTTPS セッションのいずれにも使用されます。



(注)

Web UI セッション タイムアウトは、IronPort スпам検疫セッションに適用されません。

詳細については、「[Web UI セッション タイムアウトの設定](#)」(P.15-74) を参照してください。

拡張機能：メッセージ トラッキングを使用した添付ファイル検索

AsyncOS 7.5 では、メッセージ トラッキングで添付ファイル名を使用してメッセージを検索できるようになりました。

拡張機能：レポート作成拡張機能

AsyncOS 7.5 には、表形式のレポートに表示する列の選択、カスタム データ範囲の選択、および PDF 内のリンクをサポートする拡張レポートが含まれます。

拡張機能：PDF レポートの国際化

AsyncOS 7.5 では、電子メールセキュリティ アプライアンスにおいて、ローカライズされた PDF レポートを生成し、PDF レポートで ASCII 以外の記号または国際的な記号をすべて適切にレンダリングできるようになりました。

新しい CLI コマンドおよび更新された CLI コマンド

AsyncOS 7.5 では、新しい CLI コマンドが追加され、既存のいくつかの CLI コマンドが更新されました。これらのコマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

表 1-1 新しいコマンドおよび更新されたコマンド

コマンド名	説明
<code>outbreakconfig</code>	感染フィルタを設定します（以前は <code>vofconfig</code> ）。
<code>outbreakflush</code>	キャッシュされた感染ルールを消去します（以前は <code>vofflush</code> ）。
<code>outbreakstatus</code>	現在の感染ルールを表示します（以前は <code>vofstatus</code> ）。
<code>outbreakupdate</code>	感染フィルタ ルールを更新します（以前は <code>vofupdate</code> ）。
<code>redirectrecipients</code>	すべてのメッセージを別のリレー ホストにリダイレクトします。詳細については、『 <i>Cisco IronPort AsyncOS for Email Daily Management Guide</i> 』の「Managing and Monitoring via the CLI」の章を参照してください。
<code>showrecipients</code>	キューからメッセージを表示します。詳細については、『 <i>Cisco IronPort AsyncOS for Email Daily Management Guide</i> 』の「Managing and Monitoring via the CLI」の章を参照してください。
<code>sievechar</code>	Sieve 電子メール フィルタリングに対して文字を設定します。
<code>tzupdate</code>	タイムゾーン ルールを更新します。
<code>updatenow</code>	すべてのコンポーネントを更新します。

電子メール セキュリティ アプライアンスのマニュアルセット

電子メール セキュリティ アプライアンスには、次のマニュアルがあります。

- 『*Cisco IronPort AsyncOS for Email Daily Management Guide*』。このマニュアルでは、Cisco IronPort アプライアンスの管理およびモニタリングを行うためにシステム管理者が使用する、一般的な日常業務（電子メール セキュリティ モニタを使用した電子メール トラフィックの参照、電子メール メッセージのトラッキング、システム検疫の管理、アプライアンスのトラブルシューティングなど）を実行する方法について説明します。また、電子メー

ルセキュリティ モニタ ページ、AsyncOS ログ、CLI サポート コマンド、検疫など、システム管理者が定期的に介入する機能についての参考情報も記載します。

- 『*Cisco IronPort AsyncOS for Email Configuration Guide*』。このマニュアルは、新しい Cisco IronPort アプライアンスを設定し、この電子メール配信機能について学習するシステム管理者に推奨されます。既存のネットワーク インフラストラクチャへのアプライアンスの導入や電子メール ゲートウェイ アプライアンスとしてのセットアップについて説明します。また、電子メール パイプライン、感染フィルタ、コンテンツ フィルタ、RSA Email DLP、電子メール 暗号化、アンチウイルス スキャン、アンチスパム スキャンなど、電子メール 配信機能の参考情報および設定手順についても説明します。
- 『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』。このマニュアルでは、Cisco IronPort アプライアンスの高度な機能を設定する方法について説明します。LDAP を使用するためのアプライアンスの設定、電子メール ポリシーを施行するためのメッセージ フィルタの作成、複数のアプライアンスのクラスタ化、アプライアンスでのリスナーのカスタマイズなどの項目が含まれています。このガイドでは設定の他に、メッセージ フィルタルールとアクション、コンテンツ ディクショナリとメッセージ フィルタルールで使用される正規表現、LDAP クエリーの構文と属性など、高度な機能の参考資料を提供します。
- 『*Cisco IronPort AsyncOS CLI Reference Guide*』。このガイドでは、AsyncOS コマンドライン インターフェイス (CLI) のコマンドの詳細なリストおよびコマンドの使用例を提供します。システム管理者は、Cisco IronPort アプライアンスで CLI を使用する際の参考資料としてこのマニュアルを使用できます。

トピックの追加情報を得るために、このガイドから他のガイドを参照する場合があります。これらのマニュアルは、Cisco IronPort アプライアンスに同梱の Documentation CD および Cisco IronPort Customer Support Portal で入手できます。詳細については、「[Cisco IronPort サポート コミュニティ](#)」(P.1-20) を参照してください。

このガイドの使い方

このガイドを情報源として使用し、Cisco IronPort アプライアンスの機能について学習します。トピックは論理的な順序で編成されています。本書内のすべての章を読む必要はありません。目次および「[本書の構成](#)」(P.1-13) の項を確認し、ご使用のシステムに関連する章を特定します。

また、このガイドを参考書として使用することもできます。ネットワークおよびファイアウォールの構成設定など、アプライアンスの使用期間を通して参照する可能性のある重要な情報が含まれています。

このガイドは、印刷版の他に、PDF ファイルおよび HTML ファイルで電子データとして配布されています。このマニュアルの電子版は、Cisco IronPort Customer Support Portal で入手できます。また、アプライアンスの GUI の右上隅にある [Help and Support] リンクをクリックすると、本書の HTML オンラインヘルプバージョンにもアクセスできます。

はじめる前に

このガイドを読む前に、『*Cisco IronPort Quickstart Guide*』およびご使用のアプライアンスの最新の製品リリース ノートを確認します。このガイドでは、アプライアンスを梱包箱から取り出し、物理的にラックに取り付けて電源を投入済みであることを前提としています。



(注)

すでにアプライアンスをネットワークに配線済みの場合は、Cisco IronPort アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。(Cisco IronPort X1000/1000T/1050/1060/1070、C60/600/650/660/670、および C30/300/300D/350/350D/360/370 アプライアンス上の) Management ポートまたは (Cisco IronPort C10/100/150/160 アプライアンス上の) Data 1 ポートで事前に設定された IP アドレスは 192.168.42.42 です。

本書の構成

第 1 章「Cisco IronPort 電子メール セキュリティ アプライアンスをご使用の前に」では、Cisco IronPort アプライアンスの概要について説明し、企業ネットワークにおけるその主な機能および役割を定義します。最新リリースの新機能について説明します。

第 2 章「概要」では、Cisco IronPort AsyncOS for Email と、Cisco IronPort アプライアンスの GUI および CLI を使用した管理について説明します。CLI を使用するための表記法について説明します。この章では、汎用的な CLI コマンドの概要についても説明します。

第 3 章「セットアップおよび設置」では、Cisco IronPort アプライアンスへの接続オプションについて、ネットワーク計画、アプライアンスの初期システムセットアップと設定を含めて説明します。

第 4 章「電子メール パイプラインの理解」では、電子メール パイプラインの概要（Cisco IronPort アプライアンスで電子メールが処理されるときのフロー）を説明し、パイプラインを構成する機能について簡単に説明します。この説明には、各機能について詳細に説明しているセクションへの相互参照があります。

第 5 章「電子メールを受信するためのゲートウェイの設定」では、アプライアンスを電子メール ゲートウェイとして設定するプロセスについて説明します。この章では、着信電子メール トラフィックおよびメール フロー モニタをサポートする、インターフェイス、リスナー、およびホスト アクセス テーブル (HAT) の概念について説明します。

第 6 章「電子メール セキュリティ マネージャ」では、Cisco IronPort アプライアンス上のすべての電子メール セキュリティ サービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである電子メール セキュリティ マネージャについて説明します。電子メール セキュリティ マネージャを使用すると、感染フィルタ機能、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを、個別のインバウンドおよびアウトバウンド ポリシーを介して、受信者または送信者単位で管理できます。

第 7 章「評価フィルタリング」では、SenderBase 評価サービスのスコアを使用し、メッセージの送信者の評価に基づいて着信メールを制御する方法の概要を説明します。

第 8 章「アンチスパム」では、Cisco IronPort アプライアンスに統合された SenderBase 評価フィルタ、IronPort Anti-Spam、および IronPort Intelligent Multi-Scan の機能を使用して、スパムに対抗する独自のアプローチについて説明します。

第 9 章「アンチウイルス」では、Cisco IronPort アプライアンスに統合された Sophos および McAfee のアンチウイルス スキャン機能について説明します。

第 10 章「感染フィルタ」では、感染フィルタが新しいウイルス、スパム、およびフィッシングの拡散に対して重要な最初の防御レイヤを積極的に提供する方法を説明します。リアルタイムに新たな拡散を検出し、疑わしいトラフィックがネットワークに侵入するのを阻止するために動的に対処することにより、新しいシングニチャ アップデートがデプロイされるまでの間、感染フィルタによる保護が提供されます。

第 11 章「データ消失防止」では、RSA Security 社のデータ消失防止機能を使用して、組織の情報および知的財産を保護する方法、およびユーザが気付かずに機密データを電子メールで送信することを防ぐことによって、規制上および組織的なコンプライアンスを順守させる方法について説明します。

第 12 章「Cisco IronPort 電子メール暗号化」では、Cisco IronPort 暗号化アプライアンスまたはホステッド キー サービスを使用して、電子メールの暗号化に使用するプロセスについて説明します。

第 13 章「SenderBase Network Participation」では、SenderBase ネットワークを使用してアプライアンスからのデータを共有する方法について説明します。

第 14 章「テキスト リソース」では、AsyncOS のさまざまなコンポーネントで使用するコンテンツ ディクショナリ、通知テンプレート、免責事項などのテキスト リソースの作成について説明します。

第 15 章「システム管理」では、機能キーによる操作、AsyncOS のアップグレード、AsyncOS の復帰、日常のシステム メンテナンスの実行など、Cisco IronPort アプライアンスを管理およびモニタするための代表的な管理コマンドについて説明します。メンテナンス タスクには、システム時刻の設定、管理者パスワードの変更、およびシステムのオフライン化があります。この章では、DNS、インターフェイス、ルーティング、ホスト名の設定など、Cisco IronPort アプライアンスのネットワーク動作の設定方法についても説明します。

第 16 章「C350D アプライアンスのイネーブル化」では、Cisco IronPort C300D、C350D、および C360D のアプライアンスについて説明します。

第 17 章「Cisco IronPort M-Series セキュリティ管理アプライアンス」では、Cisco IronPort M-Series アプライアンスについて説明します。このアプライアンスは、重要なポリシーおよびランタイム データを集中管理および統合するために設計されており、管理者やエンド ユーザにレポート作成の管理および情報の監査のための単一のインターフェイスを提供します。

付録 A 「アプライアンスへのアクセス」では、ファイルをアップロードおよびダウンロードするために Cisco IronPort アプライアンスにアクセスする方法について説明します。

付録 B 「ネットワーク アドレスと IP アドレスの割り当て」では、ネットワークおよび IP アドレスの割り当てに関する全般的なルールについて説明し、企業ネットワーク インフラストラクチャ内で Cisco IronPort アプライアンスに接続する手段を示します。

付録 C 「ファイアウォール情報」では、セキュリティ ファイアウォールの背後にある Cisco IronPort アプライアンスを適切に動作させるために、開く必要性が生じることがあるポートについて説明します。

付録 D 「Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書」には、Cisco IronPort 電子メール セキュリティ アプライアンスのソフトウェア使用許諾契約が含まれています。

『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』で説明されているトピック

『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』では、次のトピックについて説明しています。

第 1 章 「Customizing Listeners」では、企業の電子メール ゲートウェイの設定を調整するためのプロセスについて説明します。この章では、ゲートウェイを通して受信する電子メールを処理するために、インターフェイスおよびリスナーを設定する際に使用できる高度な機能を詳細に説明します。

第 2 章 「Configuring Routing and Delivery Features」では、電子メールのルーティングおよび Cisco IronPort アプライアンスを通過する電子メールの配信に作用する機能について説明します。

第 3 章 「LDAP Queries」では、Cisco IronPort アプライアンスが社内の Lightweight Directory Access Protocol (LDAP) サーバに接続し、承認する受信者の確認（グループ メンバーシップなど）を目的としたクエリーの実行方法、メールのルーティングとアドレスの書き換え、ヘッダーのマスカレード、および SMTP 認証のサポートについて説明します。

第 4 章 「Email Authentication」では、Cisco IronPort アプライアンスで電子メール認証を設定およびイネーブルにするプロセスについて説明します。Cisco IronPort AsyncOS は、着信メールの Sender Policy Framework (SPF) 検証、

Sender ID Framework (SIDF) 検証、DomainKeys Identified Mail (DKIM) 検証、および発信メールの DomainKeys 署名と DKIM 署名などの複数のタイプの電子メール認証をサポートします。

第 5 章「Using Message Filters to Enforce Email Policies」では、メッセージフィルタを使用して、電子メールを処理するためのルールを定義する方法について説明します。また、添付ファイル フィルタリング、イメージ分析、およびコンテンツ ディクショナリの機能を使用してメッセージの内容を修正する機能についても説明します。

第 7 章「Advanced Network Configuration」には、NIC ペアリング、仮想 LAN などの情報が含まれています。

第 8 章「Centralized Management」では、複数のアプライアンスの管理および設定が可能な集中管理機能について説明します。集中管理機能により、ネットワーク内における信頼性、柔軟性、およびスケーラビリティが向上し、ローカル ポリシーに準拠しながら、グローバルに管理できるようになります。

付録 A「AsyncOS Quick Reference Guide」では、CLI のほとんどのコマンドのクイック リファレンスを提供します。

付録 B「Accessing the Appliance」では、Cisco IronPort アプライアンスからファイルを送信および取得するために Cisco IronPort アプライアンスにアクセスする方法について説明します。

『Cisco IronPort AsyncOS for Email Daily Management Guide』では、次のトピックが説明されています。

第 1 章「Managing the Cisco IronPort Email Appliance」では、Cisco IronPort アプライアンスの概要について説明し、企業ネットワークにおけるその主な機能および役割を定義します。

第 2 章「Using Email Security Monitor」では、企業のすべてのインバウンド電子メール トラフィックを全体的に確認できる高性能な Web ベースのコンソールであるメール フロー モニタ機能について説明します。

第 3 章「Tracking Email Messages」では、ローカル メッセージ トラッキングについて説明します。メッセージ トラッキングを使用して、特定のメッセージについて、配信、ウイルスの検出、またはスパム検疫が行われたかどうかを識別できます。

第 4 章「Quarantines」では、メッセージの保留および処理に使用される特別なキューまたはリポジトリについて説明します。検疫されたメッセージは、検疫の設定方法に基づいて配信したり削除したりできます。これには、Cisco IronPort スпам検疫が含まれます。

第 5 章「Logging」では、Cisco IronPort アプライアンスのロギングおよびログサブスクリプション機能について説明します。

第 6 章「Managing and Monitoring via the CLI」では、ゲートウェイを通過するメールフローのモニタ時に使用できる CLI のコマンドについて説明します。

第 7 章「Other Tasks in the GUI」では、GUI を使用して Cisco IronPort アプライアンスを管理およびモニタするための代表的な管理タスクについて説明します。

第 8 章「Common Administrative Tasks」では、ユーザの追加、コンフィギュレーションファイルの管理、SSH キーの管理など、Cisco IronPort アプライアンスの管理およびモニタのための代表的な管理コマンドについて説明します。この章では、テクニカルサポートの依頼方法、アプライアンスへのリモートアクセスを Cisco IronPort カスタマーサポートに許可する方法、および機能キーの使用方法についても説明します。

第 9 章「Testing and Troubleshooting」では、システムパフォーマンスのテストおよび設定上の問題のトラブルシューティング用のいわゆるブラックホールリスナーを作成するプロセスについて説明します。

付録 A「Accessing the Appliance」では、ファイルをアップロードおよびダウンロードするために Cisco IronPort アプライアンスにアクセスする方法について説明します。

印刷時の表記法

書体	意味	例
AaBbCc123	コマンド、ファイル、およびディレクトリの名前。画面上のコンピュータ出力。	Please choose an IP interface for this Listener. sethostname コマンドは、Cisco IronPort アプライアンスの名前を設定します。
AaBbCc123	ユーザ入力。画面上のコンピュータ出力と対比。	mail3.example.com> commit Please enter some comments describing your changes: []> Changed the system hostname
<i>AaBbCc123</i>	マニュアルタイトル、新規用語、強調語句、およびコマンドラインの変数。コマンドラインの変数の場合、斜体のテキストが実際の名前や値のプレースホルダです。	『Cisco IronPort Quickstart Guide』をお読みください。 Cisco IronPort アプライアンスは、発信パケットを送信するインターフェイスを一意的に選択する必要があります。 Before you begin, please reset your password to a new value. Old password: ironport New password: <i>your_new_password</i> Retype new password: your_new_password

その他の情報の入手先

シスコは、Cisco IronPort 電子メール セキュリティ アプライアンスについての理解を深めて頂くために次の資料を提供しています。

Cisco IronPort 技術トレーニング

Cisco IronPort システム技術トレーニング サービスは、Cisco IronPort セキュリティ製品およびソリューションの評価、統合、デプロイ、保守、およびサポートを正しく行うために必要な知識と技術の習得を支援します。

次のいずれかの方法で、Cisco IronPort 技術トレーニング サービスまでお問い合わせください。

トレーニング。登録およびトレーニング全般に関するご質問の場合：

- <http://training.ironport.com>
- training@ironport.com

認定。認定および認定試験に関するご質問の場合：

- <http://training.ironport.com/certification.html>
- certification@ironport.com

ナレッジベース

Customer Support Portal の Cisco IronPort Knowledge Base には、次の URL からアクセスできます。

<http://www.cisco.com/web/ironport/knowledgebase.html>



(注)

サイトにアクセスするには Cisco.com のユーザ ID が必要です。Cisco.com のユーザ ID をお持ちでない場合は、

<https://tools.cisco.com/RPF/register/register.do> で登録できます。

Knowledge Base には、Cisco IronPort 製品に関する豊富な情報が用意されています。

記事は通常、次のいずれかのカテゴリに分類されます。

- **手順。**手順の項目では、Cisco IronPort 製品を使用して何かを実行する方法について説明します。手順の記事では、たとえば、アプライアンスのデータベースのバックアップや復元の手順などを説明します。

- **問題とソリューション。**問題と解決策の記事では、Cisco IronPort 製品の使用時に発生する可能性がある特別なエラーや問題に対する解決策を示します。問題とソリューションの記事では、たとえば、製品の新しいバージョンへのアップグレード時に特定のエラー メッセージが表示された場合に行うことなどを説明します。
- **参考情報。**参考情報の記事では通常、特定のハードウェアに関連するエラーコードなどの情報のリストを提供します。
- **トラブルシューティング。**トラブルシューティングの記事では、Cisco IronPort 製品に関する一般的な問題の分析方法および解決方法について説明します。トラブルシューティングの記事では、たとえば、DNS の問題が発生した場合に従う手順などを提供します。

ナレッジ ベースの各記事は、固有の回答 ID 番号が付いています。

Cisco IronPort サポート コミュニティ

Cisco IronPort サポート コミュニティは、Cisco IronPort のカスタマー、パートナー、および従業員のためのオンライン フォーラムです。電子メールおよび Web のセキュリティに関する一般的な問題および特定の Cisco IronPort 製品に関する技術情報について議論する場を提供します。このフォーラムにトピックを投稿して質問したり、他の Cisco IronPort ユーザと情報を共有したりできます。

Customer Support Portal の Cisco IronPort サポート コミュニティには、次の URL からアクセスします。

<https://supportforums.cisco.com>

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

<http://www.cisco.com/en/US/support/index.html>

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける

- ツールおよびリソースへアクセスする
 - Product Alert の受信登録
 - Field Notice の受信登録
 - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト (<http://www.cisco.com/techsupport>) の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サードパーティ コントリビュータ

Cisco IronPort AsyncOS 内に含まれる一部のソフトウェアは、FreeBSD Inc.、Stichting Mathematisch Centrum、Corporation for National Research Initiatives Inc.、および他のサードパーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、および条件に基づいて配布されています。これらすべての契約条件は、Cisco IronPort ライセンス契約に含まれています。

これらの契約内容の全文は次の URL を参照してください。

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html

Cisco IronPort AsyncOS 内の一部のソフトウェアは、Tobi Oetiker の書面による同意を得て、RRDtool を基にしています。

このマニュアルには、Dell Computer Corporation の許可を得て複製された内容が一部含まれています。このマニュアルには、McAfee の許可を得て複製された内容が一部含まれています。このマニュアルには、Sophos の許可を得て複製された内容が一部含まれています。

Cisco IronPort 電子メール セキュリティ アプライアンスの概要

Cisco IronPort 電子メール セキュリティ アプライアンスは、要求水準が最も高い企業ネットワークの電子メール インフラストラクチャのニーズを満たすために設計された高性能機器です。電子メール セキュリティ アプライアンスは、スパムおよびウイルスを排除し、社内ポリシーを順守させます。また、ネットワーク境界をセキュアに保ち、企業の電子メール インフラストラクチャの Total Cost of Ownership (TCO; 総所有コスト) を削減します。

Cisco IronPort システムは、ハードウェア、セキュリティの強化されたオペレーティング システム、アプリケーション、およびサポート サービスを組み合わせ、目的に合わせて構築された、企業メッセージング専用のラックマウント サーバ アプライアンスを提供します。

Cisco IronPort AsyncOS™ オペレーティング システムは、複数のインテリジェントな機能を Cisco IronPort アプライアンスに統合します。

- **SenderBase** 評価フィルタと **Cisco IronPort Anti-Spam** を統合した独自のマルチレイヤ アプローチによるゲートウェイでの**アンチスパム**。
- **Sophos** および **McAfee** のアンチウイルス スキャン エンジンによるゲートウェイでの**アンチウイルス**。
- 新しいアップデートが適用されるまで危険なメッセージを検疫し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対する **Cisco IronPort** の独自保護機能である**感染フィルタ**。
- 検疫されたスパムおよび陽性と疑わしいスパムへのエンドユーザ アクセスを提供する、オンボックスまたはオフボックスの**スパム検疫**。
- **電子メール認証**。Cisco IronPort AsyncOS は、発信メールに対する **DomainKeys** および **DomainKeys Identified Mail (DKIM)** の署名の他に、着信メールに対する **Sender Policy Framework (SPF)**、**Sender ID Framework (SIDF)**、**DKIM** の検証など、さまざまな形式の電子メール認証をサポートします。
- **Cisco IronPort 電子メール暗号化**。HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、電子メール セキュリティ アプライアンスで暗号化ポリシーを設定し、ローカルキー サーバまたはホステッドキー サービスを使用してメッセージを暗号化します。

- アプライアンス上のすべての電子メール セキュリティ サービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである**電子メール セキュリティ マネージャ**。電子メール セキュリティ マネージャは、ユーザグループに基づいて電子メール セキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、Cisco IronPort 評価フィルタ、感染フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。
- 電子メール ポリシーに違反したメッセージを保持する**オンボックス検査エリア**。検査と感染フィルタ機能は、シームレスに連携します。
- **オンボックスのメッセージ トラッキング**。AsyncOS for Email には、電子メール セキュリティ アプライアンスが処理するメッセージのステータスの検索が容易にできる、オンボックスのメッセージ トラッキング機能があります。
- 企業のすべての電子メール トラフィックを全体的に確認できる、すべてのインバウンドおよびアウトバウンドの電子メール に対する**メール フロー モニタ機能**。
- 送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者の**アクセス コントロール**。
- 広範な**メッセージ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージをドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。
- **セキュアな SMTP over Transport Layer Security 経由のメッセージの暗号化**により、企業のインフラストラクチャとその他の信頼できるホストとの間でやりとりされるメッセージが暗号化されるようになります。
- **Virtual Gateway™**テクノロジーにより、Cisco IronPort アプライアンスは、単一サーバ内で複数の電子メール ゲートウェイとして機能できるため、さまざまな送信元またはキャンペーンの電子メールを、それぞれ独立した IP アドレスを通して送信するように分配できます。これにより、1 つの IP アドレスに影響する配信可能量の問題が、他の IP アドレスに及ばないようにします。

AsyncOS for Email は、インターネット メッセージングのタスク用に高度に最適化された専用のオペレーティング システムです。AsyncOS は、「セキュリティの強化された」オペレーティング システムです。不要なすべてのサービスは取り除かれ、セキュリティの向上とシステム パフォーマンスの最適化が図れています。Cisco IronPort のスタックレスなスレッディング テクノロジーにより、各タスクに対する専用メモリ スタックの割り当ては行われず、MTA の同時並行性と安定性が向上します。従来のオペレーティング システムでの CPU の割り込み型タイム スライシングと比べ、カスタム I/O 駆動型スケジューラは、電子メール ゲートウェイで要求される大量の並列 I/O イベントに対して最適化されています。AsyncOS の基礎となるファイル システムの AsyncFS は、何百万もの小さいファイルを扱うために最適化され、システム障害が発生した場合のデータの復元性を確保します。

AsyncOS for Email は、メッセージを受け入れて配信するために、RFC 2821 準拠の Simple Mail Transfer Protocol (SMTP; シンプル メール転送プロトコル) をサポートします。Cisco IronPort アプライアンスは、設定と管理を簡易化するように設計されています。レポート作成コマンド、モニタリング コマンド、およびコンフィギュレーション コマンドのほとんどは、HTTP 経由でも HTTPS 経由でも Web ベースの GUI から使用できます。さらに、セキュア シェル (SSH)、Telnet、または直接シリアル接続でアクセスするインタラクティブなコマンドライン インターフェイス (CLI) がシステムに用意されています。Cisco IronPort アプライアンスには、確実なロギング機能もあり、システム全体の機能にわたるログ サブスクリプションを設定して、必要な情報を見つけるために費やす時間を削減します。

メール フローおよび Cisco IronPort M-Series アプライアンス

M-Series アプライアンスが構成に含まれている場合は、他の Cisco IronPort (C-Series および X-Series) アプライアンスから Cisco IronPort M-Series アプライアンスにメールが送信されます。Cisco IronPort M-Series アプライアンスにメールを送信するように設定された Cisco IronPort アプライアンスは、その M-Series アプライアンスからリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。メッセージは、HAT などのポリシーやスキャン設定をバイパスして配信されます。これを機能させるために、Cisco IronPort M-Series アプライアンスの IP アドレスが変わらないようにしてください。Cisco IronPort M-Series アプライアンスの IP アドレスが変わると、受信側の C-Series または X-Series のアプライアンス

は、メッセージを他の着信メッセージであるものとして処理します。Cisco IronPort M-Series アプライアンスの受信と配信では、常に同じ IP アドレスを使用する必要があります。

Cisco IronPort M-Series アプライアンスでは、Cisco IronPort スпам検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。Cisco IronPort M-Series アプライアンスでローカル検疫を設定するには、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。Cisco IronPort M-Series アプライアンスのローカル検疫は、M-Series アプライアンスにメールを送信する他の Cisco IronPort アプライアンスからは、外部の検疫と見なされることに注意してください。

Cisco IronPort M-Series アプライアンスによって解放されたメールは、スパム検疫設定の定義に従って、プライマリ ホストおよびセカンダリ ホスト (Cisco IronPort アプライアンスまたは他のグループウェア ホスト) に配信されます (『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照)。したがって、Cisco IronPort M-Series アプライアンスにメールを配信する Cisco IronPort アプライアンスの数に関係なく、解放されるすべてのメール、通知、およびアラートが単一のホスト (グループウェアまたは Cisco IronPort アプライアンス) に送信されます。Cisco IronPort M-Series アプライアンスからの配信によってプライマリ ホストが過負荷にならないように注意してください。



CHAPTER 2

概要

この章では、Cisco IronPort AsyncOS オペレーティング システム、および Web ベースのグラフィカル ユーザ インターフェイス (GUI) とコマンドライン インターフェイス (CLI) の両方を使用した Cisco IronPort アプライアンスの管理について説明します。各インターフェイスを使用する場合の表記法について説明します。この章では、汎用的な CLI コマンドについても説明します。この章は、次の内容で構成されています。

- 「Web ベースのグラフィカル ユーザ インターフェイス (GUI)」 (P.2-1)
- 「コマンドライン インターフェイス (CLI)」 (P.2-8)

Web ベースのグラフィカル ユーザ インターフェイス (GUI)

グラフィカル ユーザ インターフェイス (GUI) は、システムのモニタリングおよび設定のためのコマンドライン インターフェイス (CLI) に代わる Web ベースの方法です。GUI により、Cisco IronPort AsyncOS のコマンド構文を憶える必要がなく、簡単な Web ベースの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。

GUI には、システムの設定およびモニタに必要なほとんどの機能が備わっています。ただし、すべての CLI コマンドを GUI で使用できるわけではなく、一部の機能は CLI でのみ使用できません。このマニュアルを通して示されるタスクの多くは、GUI から先に (可能な場合) タスクの実行方法が例示され、同じタスクを実行する CLI コマンドはその後に続けて示します。

以降の章で、GUI を使用して次の処理を実行する方法について学習します。

- System Setup Wizard にアクセスして、Cisco IronPort アプライアンスの初期インストールおよび設定を実行します。
- 電子メール セキュリティ マネージャにアクセスして、ユーザ グループに基づいて電子メール セキュリティを実施します。インバウンドとアウトバウンドの独立したポリシーを使用して、Cisco IronPort 評価フィルタ、感染フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツフィルタリング ポリシーを管理できます。
- リスナーのホスト アクセス テーブル (HAT) を編集し、SenderBase Reputation Score (SBRs; SenderBase 評価スコア) などの送信者の評価を照合することにより、独自の送信者グループのカスタマイズ (ホワイトリスト、ブラックリスト、およびグレーリストの更新) し、メール フロー ポリシーを調整します。
- ディクショナリ、免責事項などのテキスト リソースを作成および管理します。
- Cisco IronPort 電子メール暗号化を使用してアウトバウンドの電子メールを暗号化するように、暗号化プロファイルを設定します。
- IronPort Anti-Spam、Sophos Anti-Virus、感染フィルタ、および SenderBase Network Participation のグローバル設定を行います。
- XML ページを使用してステータスを表示するか、プログラムで XML ステータス情報にアクセスします。

ブラウザ要件

Web ベースの UI にアクセスするには、ブラウザが JavaScript およびクッキーをサポートし、受け入れが有効になっている必要があります。さらに、Cascading Style Sheet (CSS) を含む HTML ページをレンダリングできる必要があります。



(注)

AsyncOS 5.5 からは、Web ベースの UI は、Yahoo! User Interface (YUI) ライブラリからライブラリを組み込んでいます。これは、リッチでインタラクティブな Web アプリケーションを構築するための、JavaScript で記述されたユーティリティおよびコントロールのセットです。この変更の目的は、Web ベース UI のユーザ操作性を改善することです。

YUI ライブラリは、一般的に使用されているほとんどのブラウザをサポートしています。また、YUI ライブラリは、ブラウザ サポートに対する包括的で公開されたアプローチを取り、「A グレード」ブラウザとして指定されたすべてのブラウザでコンポーネントが問題なく動作することを表明しています。格付けされたブラウザのサポートについては、次の URL を参照してください。

<http://developer.yahoo.com/yui/articles/gbs/>

Cisco IronPort は、Web ベース UI へのアクセスに次のリストの A グレードブラウザを使用してシスコの Web アプリケーションをテストしているため、これらのブラウザを推奨します。

- Firefox 3.0 および 3.5
- Windows XP および Vista : Internet Explorer 7 および 8
- Mac OS X : Safari 4.0

GUI へのアクセス時には、複数のブラウザ ウィンドウまたはタブを同時に使用して、Cisco IronPort アプライアンスに変更を行わないように注意してください。GUI セッションおよび CLI セッションも同時に使用しないでください。同時に使用すると、予期しない動作が生じ、サポートの対象外になります。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUI を使用するには、ブラウザのポップアップ ブロックの設定が必要な場合があります。

GUI へのアクセス

デフォルトで、システムは管理インターフェイス (Cisco IronPort C60/600/650/660/670、C30/300/350/360/370、および X1000/1050/1060/1070 アプライアンスの場合) またはデータ 1 (Cisco IronPort C10/100/150/160) インターフェイスで HTTP がイネーブルに設定された状態で出荷されます。詳細については、「[Enabling the GUI on an Interface](#)」(P.442) を参照してください。

新規システムの GUI にアクセスするには、次の URL にアクセスします。

<http://192.168.42.42>

ログイン ページが表示されたら、デフォルトのユーザ名とパスワードを使用してシステムにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名 : `admin`
- パスワード : `ironport`

次の例を参考にしてください。



新規（以前のリリースの AsyncOS からのアップグレードではなく）システムの場合は、System Setup Wizard へ自動的にリダイレクトされます。

初期システムセットアップ時に、インターフェイスの IP アドレスと、このインターフェイスの HTTP サービス、HTTPS サービス、またはその両方を実行するかどうかを選択します。インターフェイスの HTTP サービス、HTTPS サービス、またはその両方がイネーブルに設定されている場合は、サポートしている任意のブラウザを使用し、ブラウザのロケーションフィールド（「アドレス バー」）に URL として IP インターフェイスの IP アドレスまたはホスト名を入力して GUI を表示できます。次の例を参考にしてください。

`http://192.168.1.1` または
`https://192.168.1.1` または
`http://mail3.example.com` または
`https://mail3.example.com`



(注) インターフェイスの HTTPS がイネーブルに設定されている（かつ HTTP 要求がセキュア サービスにリダイレクトされていない）場合は、「`https://`」のプレフィックスを使用して GUI にアクセスすることに留意してください。

ログイン

GUI にアクセスするすべてのユーザは、ログインが必要です。ユーザ名とパスワードを入力してから [Login] をクリックして GUI にアクセスします。サポートされる Web ブラウザを使用する必要があります（「[ブラウザ要件](#)」(P.2-2) を参照）。admin アカウントまたは作成済みの特定のユーザ アカウントを使用してログインできます（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」章の「Adding Users」を参照してください）。

ログインしたら、[Monitor] > [Incoming Mail Overview] ページが表示されます。

GUI セクションおよび基本ナビゲーション

GUI は、Cisco IronPort アプライアンスの機能に対応する、[Monitor]、[Mail Policies]、[Security Services]、[Network]、および [System Administration] のメニューで構成されています。以降の章では、各セクション内のページで実行するタスクなど、各セクションについて説明します。



(注)

GUI のオンライン ヘルプは、GUI 内のどのページからも使用できます。オンライン ヘルプにアクセスするには、ページの右上にある [Help] > [Online Help] リンクをクリックします。

各メイン セクション（[Monitor]、[Mail Policies]、[Security Services]、[Network]、および [System Administration]）のメニュー見出しをクリックして、インターフェイスのセクション内をナビゲートします。各メニュー内にあるのが、情報やアクティビティをさらにグループ化するサブセクションです。たとえば、[Security Services] セクションには、[Anti-Spam] ページを表示する [Anti-Spam] セクションがあります。GUI の特定のページを参照する場合、マニュアルではそれに沿ってメニュー名に続けて矢印とページ名を表記して使用します。たとえば、[Security Services] > [SenderBase] です。

[Monitor] メニュー

[Monitor] セクションには、メール フロー モニタ機能（概要、着信メール、発信先、発信者、配信ステータス、内部ユーザ、コンテンツ フィルタ、ウイルス拡散、ウイルス タイプ、システム容量、システム ステータス）、ローカル検疫と外部検疫、およびスケジュール済みレポートの各機能のページがあります。このメニューからメッセージ トラッキングにもアクセスできます。

[Mail Policies] メニュー

[Mail Policies] セクションには、電子メール セキュリティ マネージャ機能 (メール ポリシーおよびコンテンツ フィルタを含む)、ホスト アクセス テーブル (HAT) と受信者アクセス テーブル (RAT) 設定、宛先制御、バウンス検証、DomainKeys、テキスト リソース、およびディクショナリのページがあります。

[Security Services] メニュー

[Security Services] セクションには、アンチスパム、アンチウイルス、Cisco IronPort 電子メール暗号化、感染フィルタ、および SenderBase Network Participation の各機能のグローバル設定を行うためのページがあります。このメニューからは、レポート作成、メッセージトラッキング、外部スパム検疫の機能もイネーブルにします。

[Network] メニュー

[Network] セクションには、IP インターフェイス、リスナー、SMTP ルート、DNS、ルーティング、バウンス プロファイル、SMTP 認証、および着信リレーを作成および管理するページがあります。

[System Administration] メニュー

[System Administration] セクションには、トレース、アラート、ユーザ管理、LDAP、ログ サブスクリプション、リターンアドレス、システム時刻、コンフィギュレーション ファイル管理、機能キー設定、機能キー、シャットダウン/リポート、アップグレード、および System Setup Wizard の各機能のページがあります。

集中管理

集中管理機能を使用し、クラスタをイネーブルにしている場合は、クラスタ内のマシンを参照し、クラスタ、グループ、マシン間での設定の作成、削除、コピー、および移動 (つまり、clustermode コマンドおよび clusterset コマンドと同等の内容) を GUI 内から実行できます。

詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Administering a Cluster from the GUI」を参照してください。

[Commit Changes] ボタン

GUI の確定モデルは、CLI で使用されている「明示的な確定」モデルと同じです（詳細については、「[設定変更の確定](#)」(P.2-13) を参照してください)。GUI で設定の変更を行う場合は、[Commit Changes] ボタンをクリックして、その変更の明示的な確定が必要になりました。このボタンは、保存する必要のある未確定の変更がある場合に表示されます。

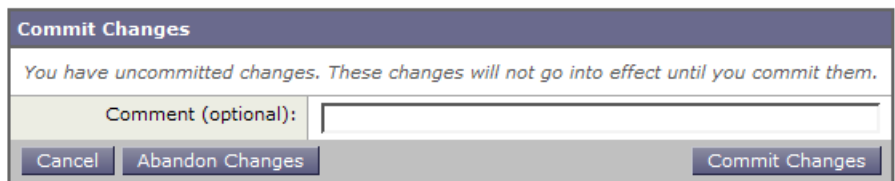
図 2-2 [Commit Changes] ボタン



[Commit Changes] ボタンをクリックして表示されたページでは、コメントを追加し変更を確定したり、最新の確定（CLI の `clear` コマンドと同等。「[設定変更のクリア](#)」(P.2-14) を参照）の後に行われた変更をすべて中止したり、キャンセルすることができます。

図 2-3 確定された変更の確認

Uncommitted Changes



アクティブなセッションの表示

GUI から、現在電子メールセキュリティ アプライアンスにログインしているすべてのユーザとセッションの情報を表示できます。

これらのアクティブなセッションを表示するには、ページの右上にある [Options] > [Active Sessions] をクリックします。

[Active Sessions] ページで、ユーザ名、ユーザ ロール、ログイン時間、アイドル時間、コマンドラインからのログインか、GUI からのログインかを表示できます。

図 2-4 アクティブなセッション
Active Sessions

Username	Role	Login Time	Idle Time	Remote Host	Interface
susan1	DLP Administrator*	17 Mar 2011 22:00 (GMT)	1 min 55 secs	173.37.1.34	GUI
admin	Administrator	17 Mar 2011 22:00 (GMT)	1 min 47 secs	173.37.1.34	GUI

* Custom User Role for delegated administration of web policies.

コマンドライン インターフェイス (CLI)

Cisco IronPort AsyncOS のコマンドライン インターフェイスは、Cisco IronPort アプライアンスを設定およびモニタするために設計されたインタラクティブなインターフェイスです。引数を指定しても指定しなくても、コマンド名を入力すると、コマンドが起動されます。引数を指定せずにコマンドを入力した場合は、必要な情報を要求するプロンプトが表示されます。

コマンドライン インターフェイスには、SSH または Telnet のサービスがイネーブルに設定されている IP インターフェイスで SSH または Telnet 経由、またはシリアル ポートで端末エミュレーション ソフトウェアを使用してアクセスできます。工場出荷時のデフォルトでは、管理ポートに SSH および Telnet が設定されています。これらのサービスをディセーブルにするには、「[電子メールを受信するためのゲートウェイの設定](#)」(P.5-1) に説明されている `interfaceconfig` コマンドを使用します。

特定の CLI コマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

コマンドライン インターフェイスの表記法

ここでは、AsyncOS CLI のルールおよび表記法について説明します。

コマンド プロンプト

最上位のコマンド プロンプトは、完全修飾ホスト名に続いて大なり (>) 記号とスペース 1 つで構成されます。次の例を参考にしてください。

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


アプライアンスが集中管理機能を使用したクラスタの一部として設定されている場合、CLIのプロンプトが変わって現在のモードを示します。次の例を参考にしてください。

```
(Cluster Americas) >
```

または

```
(Machine losangeles.example.com) >
```

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Centralized Management」を参照してください。

コマンドを実行すると、CLIによりユーザの入力が要求されます。CLIがユーザの入力を待機している場合は、コマンドプロンプトとして、角カッコ ([]) で囲まれたデフォルト入力値の後に大なり (>) 記号が表示されます。デフォルトの入力値がない場合、コマンドプロンプトのカッコ内は空です。

次の例を参考にしてください。

```
Please create a fully-qualified hostname for this Gateway
```

```
(Ex: "mail3.example.com"):  
[> mail3.example.com
```

デフォルト設定がある場合は、コマンドプロンプトのカッコ内にその設定が表示されます。次の例を参考にしてください。

```
Ethernet interface:
```

```
1. Data 1  
2. Data 2  
3. Management  
[1]> 1
```

デフォルト設定が表示される場合に **Return** を入力すると、デフォルト値を入力したことになります。

```
Ethernet interface:  
1. Data 1  
2. Data 2  
3. Management  
[1]> (type Return)
```

コマンド構文

インタラクティブ モードで動作中の場合、CLI コマンド構文は、空白スペースを含めず、引数やパラメータも指定しない単一コマンドで構成されます。次の例を参考にしてください。

```
mail3.example.com> systemsetup
```

選択リスト

入力できる複数の選択肢がある場合、コマンドによっては番号付きリストを使用します。プロンプトで選択する番号を入力します。

次の例を参考にしてください。

```
Log level:  
1. Error  
2. Warning  
3. Information  
4. Debug  
5. Trace  
[3]> 3
```

Yes/No クエリー

yes または **no** のオプションがある場合、質問はデフォルト値（カッコ内表示）を付けて表示されます。**Y**、**N**、**Yes**、または **No** で返答できます。大文字小文字の区別はありません。

次の例を参考にしてください。

```
Do you want to enable FTP on this interface? [Y]> n
```

サブコマンド

コマンドによっては、サブコマンドを使用する場合があります。サブコマンドには、NEW、EDIT、および DELETE などの命令があります。EDIT および DELETE の機能の場合、これらのコマンドは、システムですでに設定されているレコードのリストを提供します。

次の例を参考にしてください。

```
mail3.example.com> interfaceconfig
```

```
Currently configured interfaces:
```

```
1. Management (192.168.42.42/24: 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.

```
[1]>
```

サブコマンド内からメイン コマンドに戻るには、空のプロンプトで Enter または Return を入力します。

エスケープ

サブコマンド内でいつでも **Ctrl+C** キーボードショートカットを使用して、すぐに最上位の CLI に戻ることができます。

履歴

CLI は、セッション中に入力するすべてのコマンドの履歴を保持します。最近使用したコマンドの実行リストをスクロールするには、キーボードの↑および↓の矢印キーを使用するか、**Ctrl+P** キーと **Ctrl+N** キーを組み合わせで使用します。

```
mail3.example.com> (type the Up arrow key)
```

```
mail3.example.com> interfaceconfig (type the Up arrow key)
```

```
mail3.example.com> topin (type the Down arrow key)
```

コマンドの補完

Cisco IronPort AsyncOS CLI は、コマンドの補完をサポートします。あるコマンドの先頭数文字を入力して **Tab** キーを入力すると、CLI によって一意のコマンドのストリングが補完されます。入力した文字がコマンドの中で一意ではない場合、CLI はそのセットを「絞り込み」ます。次の例を参考にしてください。

```
mail3.example.com> set (type the Tab key)
setgateway, sethostname, settime, settz
mail3.example.com> seth (typing the Tab again completes the entry
with sethostname)
```

CLI の履歴およびファイルの補完機能では、**Enter** または **Return** を入力してコマンドを起動する必要があります。

設定変更

電子メール操作を通常どおり継続しながら、Cisco IronPort AsyncOS に対する設定変更を行えます。

設定変更は、次の処理を行うまでは有効になりません。

1. コマンドプロンプトで `commit` コマンドを発行します。
2. `commit` コマンドに必要な入力値を指定します。
3. CLI で `commit` 処理の確認を受け取ります。

確定されていない設定に対する変更は記録されますが、`commit` コマンドが実行されるまでは有効になりません。



(注)

AsyncOS のすべてのコマンドが、`commit` コマンドの実行を必要とするわけでは
ありません。変更を有効にする前に確定を行う必要があるコマンドの概要につい
ては、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の付
録 A 「AsyncOS Quick Reference Guide」を参照するか、『Cisco IronPort
AsyncOS CLI Reference Guide』を確認してください。

CLI セッションの終了、システムのシャットダウン、再起動、障害、または
`clear` コマンドの発行により、確定されていない変更はクリアされます。

汎用 CLI コマンド

このセクションでは、変更の確定またはクリア、ヘルプへのアクセス、およびコ
マンドライン インターフェイスの終了に使用するコマンドについて説明します。

設定変更の確定

Cisco IronPort アプライアンスに対する設定変更の保存には、`commit` コマンドが
重要です。設定変更の多くは、`commit` コマンドを入力するまで有効になりませ
ん。(変更内容を有効にするために `commit` コマンドを使用する必要がないコマ
ンドも少数あります。詳細については、『Cisco IronPort AsyncOS for Email
Advanced Configuration Guide』の付録 A 「AsyncOS Quick Reference Guide」
を参照してください。`commit` コマンドは、`commit` コマンドまたは `clear` コマ
ンドが最後に発行されてから、Cisco IronPort AsyncOS に対して行われた設定変
更に適用されます。コメントとして最大 255 文字を使用できます。変更内容は、
タイムスタンプとともに確認を受け取るまでは、確定されたものとして認められ
ません。

`commit` コマンドの後のコメントの入力は任意です。

```
mail3.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Changed "psinet" IP Interface to a different IP address
```

```
Changes committed: Wed Jan 01 12:00:01 2003
```



(注)

変更を正常に確定するには、最上位のコマンドプロンプトになっている必要があります。コマンドライン階層の 1 つ上のレベルに移動するには、空のプロンプトで **Return** を入力します。

設定変更のクリア

`clear` コマンドは、`commit` コマンドまたは `clear` コマンドが最後に発行されてから、Cisco IronPort AsyncOS の設定に対して行われた変更内容があればクリアします。

```
mail3.example.com> clear
```

```
Are you sure you want to clear all changes since the last commit?
```

```
[Y]> y
```

```
Changes cleared: Mon Jan 01 12:00:01 2003
```

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

コマンドライン インターフェイス セッションの終了

`quit` コマンドを実行すると、CLI アプリケーションからログアウトします。確定されていない設定変更はクリアされます。`quit` コマンドは電子メール操作には影響しません。ログアウトはログ ファイルに記録されます (`exit` の入力、`quit` の入力と同じです)。

```
mail3.example.com> quit
```

```
Configuration changes entered but not committed. Exiting will lose changes.
```

```
Type 'commit' at the command prompt to commit changes.
```

```
Are you sure you wish to exit? [N]> Y
```

コマンドライン インターフェイスでのヘルプの検索

`help` コマンドを実行すると、使用可能なすべての CLI コマンドが表示され、各コマンドの簡単な説明を参照できます。`help` コマンドは、コマンド プロンプトで `help` と入力するか、疑問符 (?) を 1 つ入力して実行できます。

```
mail3.example.com> help
```




CHAPTER 3

セットアップおよび設置

この章では、System Setup Wizard を使用して、電子メール配信用に Cisco IronPort C-Series または X-Series アプライアンスを設定するプロセスについて説明します。Cisco IronPort M-Series アプライアンスを設定する場合は、[第 17 章「Cisco IronPort M-Series セキュリティ管理アプライアンス」](#)を参照してください。この章を終了すると、Cisco IronPort アプライアンスによって、インターネット越しまたはネットワーク内で SMTP 電子メールを送信できるようになっています。

エンタープライズ ゲートウェイ（インターネットからの電子メールの受け入れ）としてシステムを設定する場合は、まずこの章を完了してから、詳細について [第 5 章「電子メールを受信するためのゲートウェイの設定」](#)を参照してください。

この章は、次の内容で構成されています。

- 「設置計画」(P.3-2)
- 「Cisco IronPort アプライアンスのネットワークへの物理接続」(P.3-9)
- 「セットアップの準備」(P.3-12)
- 「System Setup Wizard の使用方法」(P.3-19)
- 「次の手順：電子メールパイプラインの理解」(P.3-58)

設置計画

はじめる前に

Cisco IronPort アプライアンスを既存のネットワーク インフラストラクチャに設置する方法は複数あります。ここでは、設置を計画するときに採用可能な複数のオプションについて説明します。

ネットワーク境界に Cisco IronPort アプライアンスを配置する

Cisco IronPort アプライアンスは、メール エクスチェンジャつまり「MX」とも呼ばれる、SMTP ゲートウェイとして機能することを目的としていることに注意してください。インターネット メッセージング専用機能強化されたオペレーティング システムに加え、AsyncOS オペレーティング システムの最新機能の多くは、電子メールの送受信のためにインターネット（つまり外部 IP アドレス）に直接アクセスできる IP アドレスを持つ、最初のマシンとしてアプライアンスを設置した場合に、最適な性能を発揮します。次の例を参考にしてください。

- 受信者ごとの評価フィルタリング、アンチスパム、アンチウイルス、およびウイルス感染フィルタの機能（「[評価フィルタリング](#)」(P.7-2)、「[IronPort Anti-Spam フィルタリング](#)」(P.8-6)、「[Sophos Anti-Virus フィルタリング](#)」(P.9-3)、および「[感染フィルタ](#)」(P.10-1)を参照）は、インターネットからおよび内部ネットワークからのメッセージの直接のフローを扱うことを目的としています。企業が送受信するすべての電子メールトラフィックに対するポリシー施行（「[ホストアクセス テーブル \(HAT\)：送信者グループとメールフローポリシー](#)」(P.5-9)）のために Cisco IronPort アプライアンスを設定できます。

Cisco IronPort アプライアンスは、パブリックインターネットを介してアクセス可能なことと、電子メール インフラストラクチャの「第 1 ホップ」であることの両方を必ず満たす必要があります。別の MTA をネットワーク境界に配置してすべての外部接続を処理させると、Cisco IronPort アプライアンスで送信者の IP アドレスを判別できなくなります。送信者の IP アドレスは、メールフロー モニタで送信元を識別および区別したり、SenderBase 評価サービスに送信者の SenderBase 評価スコア (SBRS) を問い合わせたり、IronPort Anti-Spam 機能および感染フィルタ機能の有効性を高めたりするために必要です。



(注)

インターネットから電子メールを受信する最初のマシンとして IronPort アプライアンスを設定できない場合でも、IronPort アプライアンスで使用可能なセキュリティ サービスの一部は利用できます。詳細は「着信リレー」(P.8-31) を参照してください。

Cisco IronPort アプライアンスを SMTP ゲートウェイとして使用することにより、次の機能が実現されます。

- メールフロー モニタ機能 (『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Using Email Security Monitor」を参照) により、内部および外部の両方の送信者から企業に着信するすべての電子メール トラフィックに対する徹底的な可視性が提供されます。
- ルーティング、エイリアシング、およびマスカレードを対象とする LDAP クエリー (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」) では、ディレクトリ インフラストラクチャを統合でき、更新の単純化につながります。
- エイリアス テーブル (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Creating Alias Tables」)、ドメイン ベースのルーティング (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「The Domain Map Feature」)、およびマスカレード (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Masquerading」) などの一般的なツールによって、オープンソースの MTA からの移行が簡単になります。

DNS への Cisco IronPort アプライアンスの登録

不正な電子メール送信者は、次の攻撃対象を探してパブリック DNS レコードを積極的に検索します。IronPort Anti-Spam、感染フィルタ、McAfee Antivirus、および Sophos Anti-Virus の機能を十分活用するには、Cisco IronPort アプライアンスを必ず DNS に登録する必要があります。Cisco IronPort アプライアンスを DNS に登録するには、アプライアンスのホスト名を IP アドレスにマッピングする A レコードおよびパブリック ドメインをアプライアンスのホスト名にマッピングする MX レコードを作成します。ドメインのプライマリ MTA またはバックアップ MTA のいずれかとして Cisco IronPort アプライアンスをアドバタイズするように MX レコードのプライオリティを指定する必要があります。

次の例では、MX レコードに大きいプライオリティ値（20）が指定されているため、Cisco IronPort アプライアンス（IronPort.example.com）は、ドメイン example.com のバックアップ MTA です。言い換えると、数値が大きいほど、MTA のプライオリティは低くなります。

```
$ host -t mx example.com

example.com mail is handled (pri=10) by mail.example.com

example.com mail is handled (pri=20) by ironport.example.com
```

Cisco IronPort アプライアンスを DNS に登録するということは、MX レコードのプライオリティに設定する値に関係なく、スパム攻撃にさらされることを意味します。ただし、ウイルス攻撃でバックアップ MTA がターゲットになることはまれです。したがって、アンチウイルス エンジンの性能を徹底的に評価するには、Cisco IronPort アプライアンスの MX レコードのプライオリティに、他の MTA のプライオリティ以上の値を設定します。

インストール シナリオ

アプライアンスを設置する前に、すべての機能を検討しなければならない場合があります。第 4 章「電子メール パイプラインの理解」では、インフラストラクチャへの Cisco IronPort アプライアンスの配置に影響する可能性のある、アプライアンスの全機能の概要を提供しています。

大部分のお客様のネットワーク コンフィギュレーションは、以降のシナリオで表現されています。ネットワーク コンフィギュレーションが多少異なっており、設置計画の支援を必要とする場合は、Cisco IronPort カスタマー サポートにお問い合わせください（「Cisco IronPort サポート コミュニティ」（P.1-20）を参照）。

設定の概要



いくつかのシナリオでは、Cisco IronPort アプライアンスはネットワークの DMZ 内に配置されます。その場合は、Cisco IronPort アプライアンスとグループウェア サーバの間にさらにファイアウォールを設置しています。

次のネットワーク シナリオを説明します。

- ファイアウォール内 (図 3-2 (P.3-11) を参照)

実際のインフラストラクチャと最も一致する設定を選択してください。その後、「[セットアップの準備](#)」(P.3-12) に進んでください。

着信

- 指定したローカル ドメイン宛での着信メールは受け入れられます (参照)。
- その他のドメインはすべて拒否されます。
- 外部システムは、ローカル ドメイン宛で電子メールを転送するために Cisco IronPort アプライアンスに直接接続し、Cisco IronPort アプライアンスは、SMTP ルートを介して、そのメールを適切なグループウェア サーバ (Exchange™ Groupwise™ Domino™ など) にリレーします (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Routing Email for Local Domains」を参照)。

発信

- 内部ユーザが送信した発信メールは、グループウェア サーバによって Cisco IronPort アプライアンスにルーティングされます。
- Cisco IronPort アプライアンスでは、プライベート リスナーのホスト アクセス テーブルの設定値に基づいてアウトバウンド電子メールを受け入れます (詳細は、「[リスナーによる電子メールの受信](#)」(P.5-2) を参照してください)。

イーサネット インターフェイス

- これらの設定では、Cisco IronPort アプライアンスにある使用可能なイーサネット インターフェイスのうち 1 つだけを必要とします。ただし、イーサネット インターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。

使用可能なインターフェイスに対する複数 IP アドレスの割り当ての詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」および付録 B 「ネットワークアドレスと IP アドレスの割り当て」を参照してください。



(注)

Cisco IronPort X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 電子メール セキュリティ アプライアンスには、デフォルトで、使用可能なイーサネット インターフェイスが 3 つあります。Cisco IronPort C10/100/150/160 電子メール セキュリティ アプライアンスには、使用可能なイーサネット インターフェイスが 2 つあります。

拡張設定

図 3-2 および図 3-3 に示すこの設定に加え、次の設定も可能です。

- 中央集中管理機能を使用する複数 Cisco IronPort アプライアンス
- Cisco IronPort アプライアンスの 2 つのイーサネット インターフェイスを NIC ペアリング機能によって「チーム化」することによるネットワーク インターフェイス カード レベルでの冗長性

これらの機能については、いずれも『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』を参照してください。

ファイアウォール設定値 (NAT、ポート)

ネットワーク コンフィギュレーションによっては、次のポートへのアクセスを許可するように、ファイアウォールを設定する必要がある場合があります。

SMTP サービスおよび DNS サービスでは、インターネットにアクセスできる必要があります。他のシステム機能では、次のサービスが必要な場合があります。

表 3-1 **ファイアウォール ポート**

• SMTP : ポート 25	• LDAP : ポート 389 または 3268
• DNS : ポート 53	• NTP : ポート 123
• HTTP : ポート 80	• LDAP over SSL : ポート 636
• HTTPS : ポート 443	• グローバル カタログ クエリー用の SSL を使用した LDAP : ポート 3269
• SSH : ポート 22	• FTP : ポート 21、データ ポート TCP 1024 以上
• Telnet : ポート 23	• IronPort スпам検疫 : ポート 6025

Cisco IronPort アプライアンスを適切に運用するために開けなければならない可能性のあるポートに関するすべての情報については、[付録 C「ファイアウォール情報」](#)を参照してください。たとえば、次の接続のためにファイアウォールでポートを開けなければならない場合があります。

- 外部クライアント (MTA) からの Cisco IronPort アプライアンスに対する接続
- グループウェア サーバとの間の接続
- インターネット ルート DNS サーバまたは内部 DNS サーバへの接続
- Cisco IronPort ダウンロード サーバへの接続 (McAfee および Sophos Anti-Virus のアップデート、感染フィルタ ルール、および AsyncOS のアップデートのため)
- NTP サーバへの接続
- LDAP サーバへの接続

サポート言語

AsyncOS は次のいずれかの言語で GUI と CLI を表示できます。

- 英語
- フランス語
- スペイン語

- ドイツ語
- イタリア語
- 韓国語
- 日本語
- ポルトガル語（ブラジル）
- 中国語（中国と台湾）
- ロシア語

物理寸法

Cisco IronPort X1000/1050/1060、C600/650/660、および C300/350/360 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.656 cm (3.40 インチ)
- 幅：レールを取り付けて 48.26 cm (19.0 インチ)（レールを取り付けない場合は 17.5 インチ）
- 奥行：75.68 cm (29.79 インチ)
- 重量：最大 26.76 kg (59 ポンド)

Cisco IronPort X1070、C670 および C370 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.64 cm (3.40 インチ)
- 幅：レールの取り付け有無によらず 48.24 cm (18.99 インチ)
- 奥行：72.06 cm (28.40 インチ)
- 重量：最大 23.59 kg (52 ポンド)

Cisco IronPort C60 および C30 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：8.56 cm (3.375 インチ)
- 幅：レールを取り付けて 48.26 cm (19.0 インチ)（レールを取り付けない場合は 17.5 インチ）
- 奥行：69.85 cm (27.5 インチ)

- 重量：最大 25 kg (55 ポンド)

Cisco IronPort C150 および C160 電子メール セキュリティ アプライアンスには、次の物理寸法が適用されます。

- 高さ：4.2 cm (1.68 インチ)
- 幅：レールを取り付けて 48.26 cm (19.0 インチ) (レールを取り付けない場合は 17.5 インチ)
- 奥行：57.6 cm (22.7 インチ)
- 重量：最大 11.8 kg (26 ポンド)

Cisco IronPort アプライアンスのネットワークへの物理接続

設定シナリオ

Cisco IronPort アプライアンスの一般的な設定シナリオは次のとおりです。

- **インターフェイス**：大部分のネットワーク環境では、Cisco IronPort アプライアンスにある使用可能な 3 つのイーサネット インターフェイスのうち 1 つだけを必要とします。ただし、イーサネット インターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。
- **パブリック リスナー (着信電子メール)**：パブリック リスナーでは、多数の外部ホストからの接続を受け入れ、一定の数の内部グループウェア サーバにメッセージを振り向けます。
 - HAT の設定値に基づいて外部メール ホストからの接続を受け入れます。HAT は、デフォルトでは、すべての外部メール ホストからの接続を受け入れるように設定されています。
 - RAT で指定されているローカル ドメイン宛ての着信メールに限って受け入れます。その他のドメインはすべて拒否されます。
 - SMTP ルートの定義に従って、適切な内部グループウェア サーバにメールをリレーします。

- **プライベート リスナー (発信電子メール)** : プライベート リスナーは、一定の数の内部グループウェア サーバからの接続を受け入れ、多数の外部メール ホストにメッセージを振り向けます。
 - 内部グループウェア サーバは、Cisco IronPort C-Series または X-Series アプライアンスに発信メールをルーティングするように設定されます。
 - Cisco IronPort アプライアンスは、HAT の設定値に基づいて、内部グループウェア サーバからの接続を受け入れます。HAT は、デフォルトでは、すべての内部メール ホストからの接続を受け入れるように設定されています。

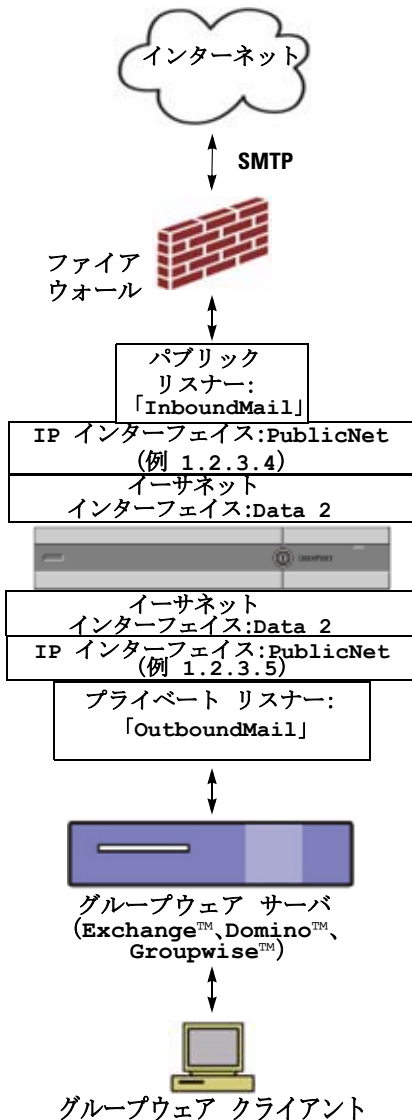
着信メールと発信メールの分離

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。ただし、アプライアンスの System Setup Wizard では、次の設定を持つ初期設定をサポートしています。

- *個別の物理インターフェイスに設定された 2 個の論理 IP アドレス上の 2 つの個別リスナー*
: 着信と発信のトラフィックの分離
- *1 つの物理インターフェイスに設定された 1 つの論理 IP アドレス上の 1 つのリスナー*
: 着信と発信の両トラフィックの組み合わせ

リスナー 1 つと 2 つの両方の設定に対するコンフィギュレーション ワークシートが以下にあります (「[セットアップ情報の収集](#)」(P.3-16) を参照)。大部分の設定シナリオは、次の 3 つの図のいずれかで表現されます。

図 3-2 ファイアウォール越しのシナリオ：リスナー 2 個、IP アドレス 2 個の設定



注：

- リスナー x 2
- IP アドレス x 2
- イーサネット インターフェイス x 1 または 2 (表示されるインターフェイスは 1 個のみ)
- 設定済みの SMTP ルート

インバウンド リスナー：「InboundMail」(パブリック)

- IP アドレス：1.2.3.4
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT (すべてを受け入れ)
- RAT (ローカルドメイン宛てメールを受け入れ、その他すべてを拒否)

アウトバウンド リスナー：「OutboundMail」(プライベート)

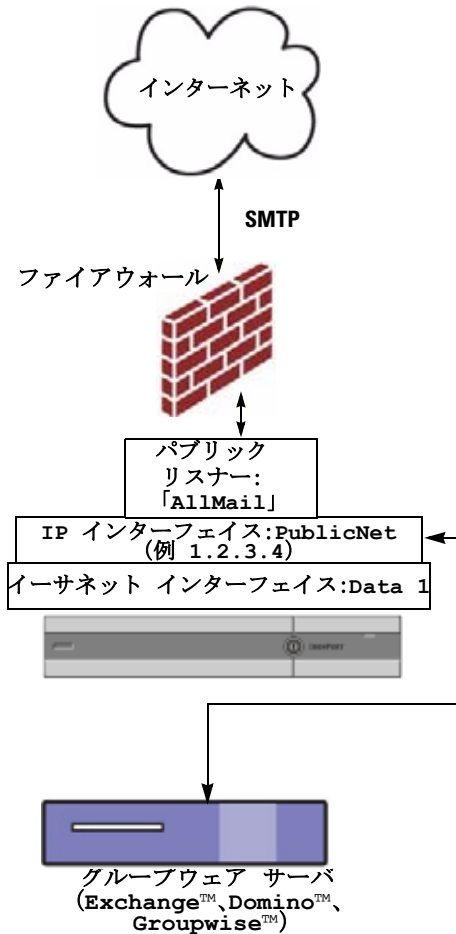
- IP アドレス：1.2.3.5
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT (ローカルドメイン宛てをリレー、その他すべてを拒否)

インターネット ルート サーバまたは内部 DNS サーバを使用するように DNS を設定可能

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと Cisco IronPort アプライアンスの双方の通信用にファイアウォール ポートをオープン

図 3-3 リスナー x 1、IP アドレス x 1 の設定



注:

- リスナー x 1
- IP アドレス x 1
- イーサネット インターフェイス x 1
- 設定済みの SMTP ルート

インバウンド リスナー: 「InboundMail」 (パブリック)

- IP アドレス: 1.2.3.4
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT (すべてを受け入れ) では、RELAYLIST にあるグループウェア サーバ用のエントリが組み込まれます。
- RAT (ローカルドメイン宛てメールを受け入れ、その他すべてを拒否)

インターネット ルート サーバまたは内部 DNS サーバを使用するように DNS を設定可能

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと Cisco IronPort アプライアンスの双方向の通信用にファイアウォール ポートをオープン

セットアップの準備

Cisco IronPort アプライアンスのセットアップ処理は、5 つの手順にわかれています。

- ステップ 1 アプライアンスへの接続方法を決定します。
- ステップ 2 ネットワーク アドレスと IP アドレスの割り当て (IP アドレスは 1 個か 2 個か) を決定します。
- ステップ 3 システム セットアップに関する情報を収集します。
- ステップ 4 Web ブラウザを起動し、アプライアンスの IP アドレスを入力します (または、「[コマンドライン インターフェイス \(CLI\) System Setup Wizard の実行](#)」(P.3-39) で説明されているコマンドライン インターフェイス (CLI) を使用することもできます)。
- ステップ 5 System Setup Wizard を実行してシステムを設定します。

アプライアンスへの接続方式の決定

Cisco IronPort アプライアンスを環境に正常にセットアップするには、Cisco IronPort アプライアンスをネットワークに接続する方法に関する重要なネットワーク情報をネットワーク管理者から収集する必要があります。

アプライアンスへの接続

初期セットアップ時に、次の 2 つのいずれかの方式で、アプライアンスに接続できます。

表 3-2 **アプライアンスに接続するオプション**

イーサネット	PC とネットワークの間およびネットワークと Cisco IronPort 管理ポートの間のイーサネット接続です。工場出荷時に Management ポートに割り当てられている IP アドレスは 192.168.42.42 です。ご使用のネットワーク コンフィギュレーションで使用可能であれば、この方法による接続が手軽です。
シリアル	シリアル通信によって PC と Cisco IronPort シリアル コンソール ポートが接続されます。イーサネット方式を使用できない場合は、コンピュータとアプライアンスをシリアル同士でストレート接続すると、代替ネットワーク設定値を Management ポートに適用できるまでの代用になります。ピン割り当については、「 シリアル接続によるアクセス 」(P.A-11) を参照してください。シリアル ポートの通信設定値は次のとおりです。 Bits per second : 9600 データ ビット : 8 パリティ : なし ストップビット : 1 フロー制御 : ハードウェア



(注)

初期接続方式は、最終的な方式でないことに留意してください。このプロセスは、初期設定だけに適用されます。ネットワーク設定値を後で変更して、別の接続方式を使用できます（詳細については、[付録 A 「アプライアンスへのアクセス」](#)を参照してください）。アプライアンスを利用するための管理者権限が異なる、複数のユーザ アカウントを作成することもできます（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Adding Users」を参照してください）。

ネットワーク アドレスと IP アドレスの割り当ての決定

電子メールを受信および配信するネットワーク接続の選択

大部分のユーザは、Cisco IronPort アプライアンスから 2 つのネットワークに接続することによって、アプライアンス上の 2 つの Data イーサネット ポートを利用します。

- プライベート ネットワークでは、内部システム宛てのメッセージを受け入れて配信します。
- パブリック ネットワークでは、インターネット宛てのメッセージを受け入れて配信します。

1 つの Data ポートだけを両方の機能に使用するユーザもいます。Management イーサネット ポートでは任意の機能をサポートできますが、グラフィカル ユーザ インターフェイスとコマンドライン インターフェイスを利用するために事前設定されています。

物理イーサネット ポートへの論理 IP アドレスのバインド

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。ただし、アプライアンスの System Setup Wizard では、次の設定を持つ初期設定をサポートしています。

- *個別の物理インターフェイスに設定された 2 個の論理 IP アドレス上の 2 つの個別リスナー*
: 着信と発信のトラフィックの分離
- *1 つの物理インターフェイスに設定された 1 つの論理 IP アドレス上の 1 つのリスナー*
: 着信と発信の両トラフィックの組み合わせ

接続用ネットワーク設定値の選択

使用することを選択した各イーサネット ポートに関する次のネットワーク情報が必要になります。

- IP アドレス
- ネットマスク

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワークのデフォルト ルータ（ゲートウェイ）の IP アドレス
- DNS サーバの IP アドレスおよびホスト名（インターネット ルート サーバを使用する場合は不要）
- NTP サーバのホスト名または IP アドレス（Cisco IronPort のタイム サーバを使用する場合は不要）

詳細については、[付録 B「ネットワーク アドレスと IP アドレスの割り当て」](#)を参照してください。



(注)

インターネットと Cisco IronPort アプライアンスの間でファイアウォールを稼動しているネットワークの場合は、Cisco IronPort アプライアンスを正常に機能させるために、特定のポートを開ける必要がある場合があります。詳細については、[付録 C「ファイアウォール情報」](#)を参照してください。

セットアップ情報の収集

これで、System Setup Wizard で必要な内容を選択するための要件および戦略が判明したため、この項を参照しながら次の表を使用して、システムのセットアップに関する情報を収集してください。

ネットワークおよび IP アドレスの詳細については、[付録 B「ネットワーク アドレスと IP アドレスの割り当て」](#)を参照してください。Cisco IronPort M-Series アプライアンスを設定する場合は、[第 17 章「Cisco IronPort M-Series セキュリティ管理アプライアンス」](#)を参照してください。

表 3-3 システム セットアップ ワークシート：2 個の IP アドレスによる電子メール トラフィックの分離

System Settings	
Default System Hostname:	
Email System Alerts To:	
Deliver Scheduled Reports To:	
Time Zone Information:	
NTP Server:	
Admin Password:	
SenderBase Network Participation:	イネーブル/ディセーブル

表 3-3 システム セットアップ ワークシート : 2 個の IP アドレスによる電子メールトラフィックの分離 (続き)

AutoSupport:	イネーブル/ディセーブル	
Network Integration		
Gateway:		
DNS: (インターネットまたは独自指定)		
Interfaces		
Data 1 Port		
IP Address:		
Network Mask:		
Fully Qualified Hostname:		
Accept Incoming Mail:	Domain	Destination
Relay Outgoing Mail:	System	
Data 2 Port		
IP Address:		
Network Mask:		
Fully Qualified Hostname:		
Accept Incoming Mail:	Domain	Destination
Relay Outgoing Mail:	System	
Management Port		
IP Address:		
Network Mask:		
Fully Qualified Hostname:		
Accept Incoming Mail:	Domain	Destination
Relay Outgoing Mail:	System	
Message Security		
SenderBase Reputation Filtering:	イネーブル/ディセーブル	
Anti-Spam Scanning Engine	なし/IronPort	
McAfee Anti-Virus Scanning Engine	イネーブル/ディセーブル	

表 3-3 システム セットアップ ワークシート : 2 個の IP アドレスによる電子メールトラフィックの分離 (続き)

Sophos Anti-Virus Scanning Engine	イネーブル/ディセーブル
Outbreak Filters	イネーブル/ディセーブル

表 3-4 システム セットアップ ワークシート : 1 個の IP アドレスをすべての電子メールトラフィックに使用

System Settings		
Default System Hostname:		
Email System Alerts To:		
Deliver Scheduled Reports To:		
Time Zone:		
NTP Server:		
Admin Password:		
SenderBase Network Participation:	イネーブル/ディセーブル	
AutoSupport:	イネーブル/ディセーブル	
Network Integration		
Gateway:		
DNS: (インターネットまたは独自指定)		
Interfaces		
Data2 Port		
IP Address:		
Network Mask:		
Fully Qualified Hostname:		
Accept Incoming Mail:	Domain	Destination
Relay Outgoing Mail:	System	

表 3-4 システム セットアップ ワークシート：1 個の IP アドレスをすべての電子メール トラフィックに使用（続き）

Data1 Port	
IP Address:	
Network Mask:	
Fully Qualified Hostname:	
Message Security	
SenderBase Reputation Filtering:	イネーブル/ディセーブル
Anti-Spam Scanning Engine	なし /IronPort
McAfee Anti-Virus Scanning Engine	イネーブル/ディセーブル
Sophos Anti-Virus Scanning Engine	イネーブル/ディセーブル
Outbreak Filters	イネーブル/ディセーブル

System Setup Wizard の使用方法

Cisco IronPort AsyncOS オペレーティング システムには、システム コンフィギュレーションの 5 つの手順を実行するための、ブラウザベースの System Setup Wizard が用意されています。コマンドライン インターフェイス (CLI) バージョンの System Setup Wizard も含まれています。詳細については、「[コマンドライン インターフェイス \(CLI\) System Setup Wizard の実行](#)」(P.3-39) を参照してください。System Setup Wizard では使用できないカスタム コンフィギュレーション オプションを利用するユーザもいます。ただし、初期セットアップでは System Setup Wizard を使用して、設定に漏れがないようにする必要があります。「[セットアップの準備](#)」(P.3-12) で必要な情報を収集済みであれば、コンフィギュレーション プロセスを完了するための時間はわずかです。



警告

System Setup Wizard では、システムを完全に再設定します。System Setup Wizard は、アプライアンスをまったく初めて設置する場合か、既存の設定を上書きする場合に限り使用してください。



警告

C60/600/650/660/670、C30/300/350/360/370、および X1000/1050/1060/1070 システムの Management ポートおよび C10/100/150/160 システムの Data 1 ポートの出荷時設定による Cisco IronPort アプライアンスのデフォルト IP アドレスは、192.168.42.42 です。Cisco IronPort アプライアンスをネットワークに接続する前に、他の装置の IP アドレスが、この工場出荷時のデフォルト設定と競合していないことを確認してください。Cisco IronPort M-Series アプライアンスを設定する場合は、「Cisco IronPort M-Series セキュリティ管理アプライアンス」(P.17-1) を参照してください。

工場出荷時の設定を持つ Cisco IronPort アプライアンスをネットワークに複数接続する場合は、各 Cisco IronPort アプライアンスのデフォルト IP アドレスを順に再設定しながら、1 台ずつ追加してください。

Web ベースのグラフィカル ユーザ インターフェイス (GUI) の利用

Web ベースの Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) を利用するには、Web ブラウザを開き、192.168.42.42 を表示します。

Address http://192.168.42.42

ログイン画面が表示されます。

図 3-4 アプライアンスへのログイン
Welcome

下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名 : `admin`
- パスワード : `ironport`



(注)

セッションがタイムアウトした場合は、ユーザ名とパスワードの再入力が必要です。System Setup Wizard の実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。

Web ベースの System Setup Wizard の実行

System Setup Wizard を起動するには、「[Web ベースのグラフィカル ユーザ インターフェイス \(GUI\) の利用](#)」(P.3-20) の説明に従って、グラフィカル ユーザ インターフェイスにログインします。[System Administration] タブで、左方のリンク リストから [System Setup Wizard] をクリックします。新規のシステム (先行リリースの AsyncOS からのアップグレードなし) の場合は、ブラウザが System Setup Wizard に自動的にリダイレクトされます。

System Setup Wizard では、5 つのカテゴリに分割された、次のコンフィギュレーション タスクが順に示されます。

ステップ 1 Start

- ライセンス契約書の参照と受諾

ステップ 2 System

- アプライアンスのホスト名の設定
- アラート設定値、レポート配信設定値、および AutoSupport の設定
- システム時刻設定値および NTP サーバの設定
- admin パスワードのリセット
- SenderBase Network Participation のイネーブル化

ステップ 3 Network

- デフォルト ルータおよび DNS 設定値の定義

- 次のようなネットワーク インターフェイスのイネーブル化および設定
着信メールの設定（インバウンドリスナー）
SMTP ルートの定義（任意）
発信メール（アウトバウンドリスナー）の設定およびアプライアンスを
介してメールをリレーできるシステムの定義（任意）

ステップ 4 Security

- SenderBase 評価フィルタリングのイネーブル化
- アンチスパム サービスのイネーブル化
- IronPort スпам検疫のイネーブル化
- Anti-Virus サービスのイネーブル化
- 感染フィルタサービスのイネーブル化

ステップ 5 Review

- セットアップのレビューおよび設定のインストール

各手順を完了して [Next] をクリックしながら、System Setup Wizard を進めてください。[Previous] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようプロンプトが表示されます。確定するまで、変更は有効になりません。[Next] をクリックしたときに必須フィールドを空白にした場合（または正しくない情報を入力した場合）は、そのフィールドの外枠が赤で表示されます。修正し、もう一度 [Next] をクリックしてください。

手順 1 : Start

ライセンス契約書の参照から開始します。ライセンス契約書を参照し、同意する場合は、同意することを示すボックスをオンにし、[Begin Setup] をクリックして続行します。

図 3-5 System Setup Wizard : 手順 1 : Start



契約書の文面は次の場所でも参照できます。

<https://support.ironport.com/license/eula.html>

手順 2 : System

ホスト名の設定

Cisco IronPort アプライアンスの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

システム アラートの設定

ユーザの介入を必要とするシステム エラーが発生した場合、Cisco IronPort AsyncOS では、電子メールでアラート メッセージを送信します。このアラートの送信先として使用する電子メール アドレス（複数可）を入力します。

システム アラートを受信する電子メール アドレスを 1 つ以上追加する必要があります。単一の電子メール アドレスか、カンマで区切った複数アドレスを入力します。当初、この電子メール受信者は、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。後で、アラート コンフィギュレーションをさらに詳細化できます。詳細については、「アラート」(P.15-24) を参照してください。

レポート配信の設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値を空白にしても、スケジュール済みレポートは引き続き実行されます。スケジュール済みレポートは配信されませんが、アプライアンス上にアーカイブされます。

時間の設定

Cisco IronPort アプライアンス上の時間帯を設定して、メッセージヘッダーおよびログファイルのタイムスタンプが正確になるようにします。ドロップダウンメニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します（詳細については、「GMT オフセットの選択」(P.15-76) を参照してください）。

システムクロック時刻は、後で手動によって設定するか、Network Time Protocol (NTP; ネットワークタイムプロトコル) を使用してネットワーク上またはインターネット上の他のサーバと時刻を同期することもできます。デフォルトでは、Cisco IronPort Systems のタイムサーバ (time.IronPort.com) と時刻を同期するエントリ 1 つが、Cisco IronPort アプライアンスにすでに設定されています。

パスワードの設定

admin アカウントのパスワードを設定します。この手順は必須です。Cisco IronPort AsyncOS の admin アカウントのパスワードを変更する場合、新しいパスワードは、6 文字以上でなければなりません。パスワードは、必ず安全な場所に保管してください。

SenderBase ネットワークへの参加

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールの評価サービスです。

SenderBase ネットワークへの参加に同意した場合、シスコは、組織の電子メールトラフィックを集約した統計情報を収集します。これには、メッセージ属性の要約データおよび Cisco IronPort アプライアンスがどのように各種メッセージを処理したかに関する情報のみが含まれています。たとえば、シスコは、メッセージの本文もメッセージの件名も収集しません。個人を特定できる情報や、組織を特定する情報は、機密情報として扱われます。収集されるデータの例など、

SenderBase の詳細については、[Click here for more information about what data is being shared] リンクをクリックしてください（「よくあるご質問」(P.13-3) を参照）。

SenderBase ネットワークに参加する場合は、[Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats] の横のボックスをオンにし、[Accept] をクリックします。

詳細については、第 13 章「SenderBase Network Participation」を参照してください。

AutoSupport のイネーブル化

IronPort AutoSupport 機能（デフォルトでイネーブル）では、ご使用の Cisco IronPort アプライアンスに関する問題を Cisco IronPort カスタマー サポート チームが認識しておくことで、適切なサポートを提供できるようにします（詳細は、「IronPort AutoSupport」(P.15-27) を参照してください）。

図 3-6 System Setup Wizard : 手順 2 : System Configuration

Before you enter your System and Network settings:

- Choose a configuration that best matches your network infrastructure
- Determine network and IP address assignments
- Gather information about your system setup

System Settings	
Default System Hostname:	<input type="text" value="felroy.run"/> <small>example: ironport-C60.example.com</small>
Email System Alerts To:	<input type="text" value="example: admin@company.com"/>
Deliver Scheduled Reports To:	<input type="text" value="example: admin@company.com. Leave blank to only archive reports on-box."/>
Time Zone:	Region: <input type="text" value="GMT Offset"/> <input type="button" value="v"/> Country: <input type="text" value="GMT"/> <input type="button" value="v"/> Time Zone / GMT Offset: <input type="text" value="GMT"/> <input type="button" value="v"/>
NTP Server:	<input type="text" value="time.ironport.com"/>
Administrator Password:	Password: <input type="text"/> <small>Must be 6 or more characters.</small> Confirm Password: <input type="text"/>
SenderBase Network Participation:	<input checked="" type="checkbox"/> Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats. Learn what information is shared...
AutoSupport:	<input checked="" type="checkbox"/> Send system alerts and weekly status reports to IronPort Customer Support

[Next] をクリックして続行します。

手順 3 : Network

手順 3 では、デフォルト ルータ（ゲートウェイ）を定義し、DNS 設定値を設定してから、Data 1 インターフェイス、Data 2 インターフェイス、および Management インターフェイスを設定することにより、電子メールの受信やリレーを行うようにアプライアンスをセットアップします。

DNS とデフォルト ゲートウェイの設定

ネットワーク上のデフォルト ルータ（ゲートウェイ）の IP アドレスを入力します。

次に、Domain Name Service（DNS）設定値を設定します。Cisco IronPort AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。System Setup Wizard から入力できる DNS サーバは 4 台までです。入力した DNS サーバの初期プライオリティは 0 になっていることに注意してください。詳細については、「ドメイン ネーム システム（DNS）設定値の設定」(P.15-61) を参照してください。



(注)

アプライアンスでは、着信接続のための DNS ルックアップを実行するために、稼動中の DNS サーバを利用できる必要があります。アプライアンスをセットアップするときにアプライアンスからアクセス可能な稼動中の DNS サーバを指定できない場合は、[Use Internet Root DNS Server] を選択するか、Management インターフェイスの IP アドレスを一時的に指定することを回避策として、System Setup Wizard を完了できます。

ネットワーク インターフェイスの設定

Cisco IronPort アプライアンスには、マシンの物理ポートに関連付けられたネットワーク インターフェイスがあります。たとえば、C60/600/650/660/670、C30/300/350/360/370、および X1000/1050/1060/1070 アプライアンスでは、3 個の物理イーサネット インターフェイスが使用可能です。C10/100/150/160 アプライアンスでは、2 個の物理イーサネット インターフェイスが使用可能です。

インターフェイスを使用するには、[Enable] チェックボックスをオンにし、IP アドレス、ネットワーク マスク、および完全修飾ホスト名を指定します。入力する IP アドレスは、DNS レコードに反映されている、インバウンド メール用のアドレスである必要があります。通常、このアドレスには、DNS で MX レコードと関連付けられています。

各インターフェイスは、メールを受け入れる（着信）、電子メールをリレーする（発信）、またはアプライアンスを管理するように設定できます。セットアップ時は、このいずれかに制限されます。通常は、インターフェイスの 1 つを着信用、1 つを発信用、および 1 つをアプライアンス管理用に使用します。C150 アプライアンスおよび C160 アプライアンスでは、1 つのインターフェイスを着信と発信の両方のメール用に使用し、もう 1 つのインターフェイスを管理用に使用することが一般的です。

インターフェイスの 1 つは、電子メールの受信用に設定する必要があります。

アプライアンスのいずれかの物理イーサネット インターフェイスに論理 IP アドレスを割り当てて、設定します。Data 1 イーサネット ポートと Data 2 イーサネット ポートの両方を使用する場合は、両方の接続に対してこの情報が必要です。

C650/660/670、C350/360/370、および X1050/1060/1070 をご利用のお客様：パブリック リスナーを介してインバウンド電子メールを受信するためにインターネットに直接接続するように物理イーサネット ポートの 1 つを使用し、プライベート リスナーを介してアウトバウンド電子メールをリレーするために内部ネットワークに直接接続するようにもう 1 つの物理イーサネット ポートを使用することを推奨しています。

C150/160 をご利用のお客様：通常は、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方のために、リスナー 1 つの物理イーサネット ポート 1 つだけが、System Setup Wizard によって設定されます。

「物理イーサネット ポートへの論理 IP アドレスのバインド」(P.3-15) を参照してください。

次の情報が必要です。

- ネットワーク管理者によって割り当てられた **IP アドレス**。
- インターフェイスの**ネットマスク**。
ネットマスクは、標準のドット付き 10 進形式にするか、16 進形式にすることができます。
- (任意) IP アドレスの完全修飾ホスト名。



(注) 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。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、付録 B 「ネットワーク アドレスと IP アドレスの割り当て」を参照してください。

メールの受け入れ

メールを受け入れるようにインターフェイスを設定する場合は、次の内容を定義します。

- 受け入れるメールの宛先のドメイン
- 各ドメインの宛先 (SMTP ルート) (任意)

[Accept Incoming Mail] のチェックボックスをオンにし、メールを受け入れるインターフェイスを設定します。受け入れるメールのドメインの名前を入力します。

[Destination] を入力します。これは、SMTP ルートまたは指定したドメイン宛での電子メールをルーティングするマシンの名前です。

これは、最初の SMTP ルート エントリです。SMTP ルート テーブルを使用すると、入力する各ドメイン宛でのすべての電子メール (受信者アクセス テーブル (RAT) エントリとも呼ぶ) を特定の Mail Exchange (MX) ホストにリダイレクトできます。標準インストールの場合、SMTP ルート テーブルでは、特定のグループウェア サーバ (たとえば、Microsoft Exchange) やインフラストラクチャの電子メール配信における次のホップを定義します。

たとえば、ドメイン example.com かそのすべてのサブドメイン .example.com のいずれか宛てメールを受け入れた場合に、グループウェア サーバ exchange.example.com にルーティングするよう指定するルートを定義できません。

ドメインおよび宛先は、複数入力できます。ドメインをさらに追加するには、[Add Row] をクリックします。行を削除するには、ゴミ箱アイコンをクリックします。



(注) この手順での SMTP ルートの設定は任意です。SMTP ルートを定義していない場合は、リスナーが受信した着信メールの配信ホストの検索と決定に、DNS が使用されます（詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Routing Email for Local Domains」を参照してください）。

ドメインを受信者アクセス テーブルに少なくとも 1 つ追加する必要があります。ドメイン、たとえば、example.com を入力します。example.net のいずれのサブドメイン宛でのメールとも必ず一致させるために、ドメイン名の他に .example.net も受信者アクセス テーブルに入力します。詳細については、「[受信者の定義](#)」(P.5-74) を参照してください。

メール リレー（任意）

メールをリレーするようにインターフェイスを設定するときは、アプライアンスを介して電子メールのリレーを許可するよう、システムを定義します。

リスナーのホスト アクセス テーブルにある RELAYLIST 内のエントリを使用します。詳細については、「[送信者グループの構文](#)」(P.5-27) を参照してください。

[Relay Outgoing Mail] のチェックボックスをオンにし、メールをリレーするインターフェイスを設定します。アプライアンスを介してメールをリレーできるホストを入力します。

アウトバウンドメールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH が System Setup Wizard によってオンにされます。

次の例では、2 つのインターフェイスが作成されます。

- 192.168.42.42 は、引き続き Management インターフェイスに設定されます。
- 192.168.1.1 は、Data 1 イーサネット インターフェイスでイネーブルになります。example.com で終わるドメイン宛でのメールを受け入れるように設定されており、exchange.example.com 宛での SMTP ルートが定義されています。
- 192.168.2.1 は、Data 2 イーサネット インターフェイスでイネーブルになります。exchange.example.com からのメールをリレーするように設定されません。



(注)

次の例は、X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 アプライアンスに該当します。C10/100/150/160 アプライアンスの場合は、着信と発信の両方のメール用に Data 2 インターフェイスを設定し、アプライアンス管理用に Data 1 インターフェイスを設定することが一般的です（「C10/100 の設置」(P.3-30) を参照）。

図 3-7 ネットワーク インターフェイス : Management および追加の IP アドレス x 2 (トラフィックの分離)

Enable Data 1 Interface	
This interface is typically configured to accept mail.	
IP Address:	192.168.1.1
Network Mask:	255.255.255.0
Fully Qualified Hostname:	mail3.example.com <small>Fully qualified hostname for this appliance</small>
Accept Incoming Mail:	<input checked="" type="checkbox"/> Accept mail on this interface
Domain:	example.com
Destination:	exchange.example.com <small>i.e. An Exchange or Notes server</small>
Relay Outgoing Mail:	<input type="checkbox"/> Relay mail on this interface
Enable Data 2 Interface	
This interface is typically configured to relay mail.	
IP Address:	192.168.2.1
Network Mask:	255.255.255.0
Fully Qualified Hostname:	mail.example.com <small>Fully qualified hostname for this appliance</small>
Accept Incoming Mail:	<input type="checkbox"/> Accept mail on this interface
Relay Outgoing Mail:	<input checked="" type="checkbox"/> Relay mail on this interface
System:	exchange.example.com
	example.com
Enable Management Interface	
This interface is typically configured for system administration. (You are currently connected to this interface.)	
IP Address:	192.168.42.42
Network Mask:	255.255.255.0
Fully Qualified Hostname:	mail.example.com <small>Fully qualified hostname for this appliance</small>
Accept Incoming Mail:	<input type="checkbox"/> Accept mail on this interface
Relay Outgoing Mail:	<input type="checkbox"/> Relay mail on this interface

図 3-2 (P.3-11) のようなネットワークを構築する場合に、この設定を使用します。

C10/100 の設置

すべての電子メールトラフィック用に単一の IP アドレスを設定する場合（トラフィックの分離なし）、System Setup Wizard の手順 3 は次のようになります。

図 3-8 ネットワーク インターフェイス : 着信と発信の (分離されない) トラフィック用に 1 つの IP アドレス

The screenshot shows the 'Interfaces' configuration page. At the top, there is a warning: 'You must set up at least 1 interface and 1 interface must be configured to accept mail from the Internet.' Below this is a diagram of a network card with two ports labeled 'Data 2' and 'Data 1'. The 'Enable Data 2 Interface' section is active and shows the following configuration:

- IP Address: 192.168.1.1
- Network Mask: 255.255.255.0
- Fully Qualified Hostname: mail3.example.com
- Accept Incoming Mail: Accept mail on this interface

Domain	Destination
example.com	exchange.example.com
example: company.com	i.e. An Exchange or Notes server
- Relay Outgoing Mail: Relay mail on this interface

System
exchange.example.com
example: company.com

The 'Enable Data 1 Interface' section is also active and shows the following configuration:

- IP Address: 192.168.42.42
- Network Mask: 255.255.255.0
- Fully Qualified Hostname: mail.example.com
- Accept Incoming Mail: Accept mail on this interface
- Relay Outgoing Mail: Relay mail on this interface

図 3-3 (P.3-12) のようなネットワークを構築する場合に、この設定を使用します。

[Next] をクリックして続行します。

手順 4 : Security

手順 4 では、アンチスパム設定値およびアンチウイルス設定値を設定します。アンチスパム オプションには、SenderBase 評価フィルタリングとアンチスパム スキャン エンジンが含まれます。アンチウイルスについては、感染フィルタおよび Sophos または McAfee のアンチウイルス スキャンをイネーブルにできます。

SenderBase 評価フィルタリングのイネーブル化

SenderBase 評価サービスは、スタンドアロンのアンチスパム ソリューションとしても使用できますが、IronPort Anti-Spam など、コンテンツ ベースのアンチスパム システムの有効性を高めることを主な目的としています。

SenderBase 評価サービス (<http://www.SenderBase.org>) には、リモート ホストの接続 IP アドレスに基づいて、陽性と疑わしいスパムをユーザが拒否したり、制限したりするための正確で柔軟な方法が備わっています。SenderBase 評価サービスは、特定の送信元からのメッセージがスパムである確率に基づく評点を返します。SenderBase 評価サービスは、電子メール メッセージの量をグローバルに表示して、電子メールの送信元の識別とグループ化を容易にする方法でデータを編成している点で独特です。SenderBase 評価フィルタリングをイネーブルにすることを強く推奨しています。

イネーブルにした SenderBase 評価フィルタリングは、着信（受け入れ）リスターで適用されます。

アンチスパム スキャンのイネーブル化

Cisco IronPort アプライアンスには、IronPort Anti-Spam ソフトウェアの 30 日間評価キーが付属している場合があります。System Setup Wizard のこの部分では、アプライアンスで IronPort Anti-Spam をグローバルでイネーブルにすることを選択できます。アンチスパム サービスをイネーブルにしないことも選択できます。

アンチスパム サービスをイネーブルにする場合は、スパムおよび陽性と疑わしいスパム メッセージをローカル IronPort スпам検査エリアに送信するように、AsyncOS を設定できます。IronPort スпам検査は、アプライアンスのエンドユーザ検査として機能します。エンドユーザのアクセス権を設定していない場合は、管理者だけが検査を利用できます。

アプライアンスで使用可能なすべての IronPort Anti-Spam 設定オプションについては、第 8 章「アンチスパム」を参照してください。IronPort スпам検査については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」を参照してください。

アンチウイルス スキャンのイネーブル化

Cisco IronPort アプライアンスには、Sophos Anti-Virus または McAfee Anti-Virus スキャン エンジンの 30 日間評価キーが付属している場合があります。System Setup Wizard のこの部分では、アプライアンスでアンチウイルス スキャン エンジンをグローバルでイネーブルにすることを選択できます。

アンチウイルス スキャン エンジン をイネーブルにすると、デフォルトの着信メール ポリシー および デフォルトの発信メール ポリシー の両方についてイネーブルになります。Cisco IronPort アプライアンスでは、メールをスキャンしてウイルスを検出しますが、感染した添付ファイルの修復は行いません。アプライアンスでは、感染したメッセージをドロップします。

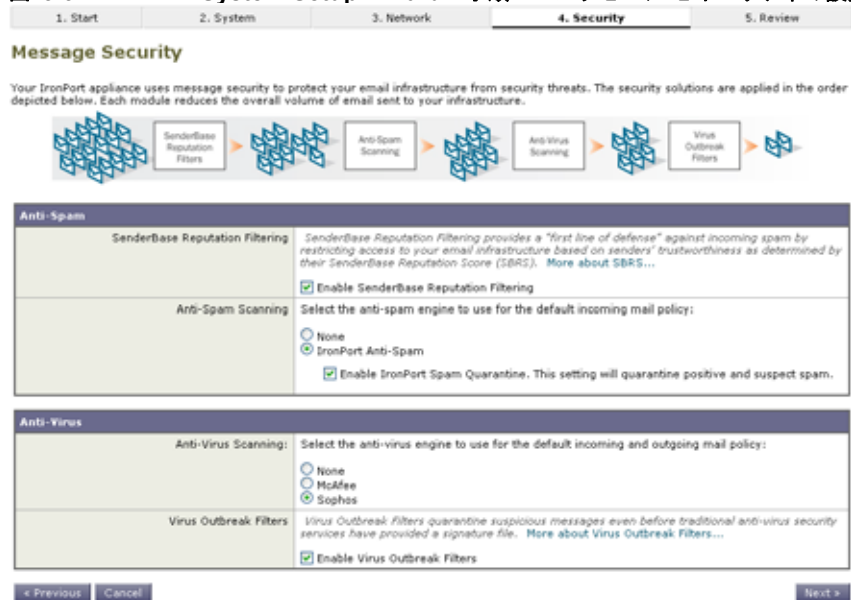
アプライアンスで使用可能なすべてのアンチウイルス コンフィギュレーション オプションについては、第9章「アンチウイルス」を参照してください。

感染フィルタのイネーブル化

Cisco IronPort アプライアンスには、感染フィルタの30日間評価キーが付属している場合があります。感染フィルタは、従来のアンチウイルス セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを検疫することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。

詳細については、第10章「感染フィルタ」を参照してください。

図 3-9 System Setup Wizard : 手順 4 : メッセージ セキュリティ の設定



[Next] をクリックして続行します。

手順 5 : Review

設定情報のサマリーが表示されます。[System Settings]、[Network Integration]、および [Message Security] の情報は、[Previous] ボタンをクリックするか、各セクションの右上にある対応する [Edit] リンクをクリックすることによって編集できます。変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。

図 3-10 System Setup Wizard : 手順 5 : Review

1. Start	2. System	3. Network	4. Security	5. Review
----------	-----------	------------	-------------	-----------

Review Your Configuration

Please review your configuration. If you need to make changes, click the Edit button to return to the page you'd like to edit. [Printable Page](#)

System Settings		Edit
Default System Hostname:	example.com	
Email System Alerts To:	admin@example.com	
Time Zone:	America/Los_Angeles	
NTP Server:	time.ironport.com	
Admin Password:	(hidden)	
SenderBase Network Participation:	Enabled	
AutoSupport:	Enabled	

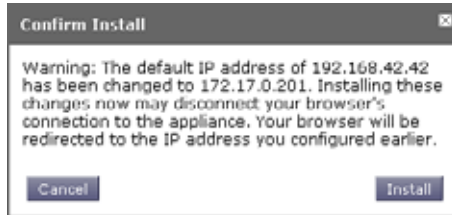
Network Integration		Edit				
Gateway:	192.168.0.1					
DNS:	Use the Internet's Root DNS servers					
Interfaces						
Data 1 Port						
IP Address:	192.168.1.1					
Network Mask:	255.255.255.0					
Fully Qualified Hostname:	mail3.example.com					
Accept Incoming Mail:	<table border="1"> <thead> <tr> <th>Domain</th> <th>Destination</th> </tr> </thead> <tbody> <tr> <td>.example.com</td> <td>exchange.example.com</td> </tr> </tbody> </table>	Domain	Destination	.example.com	exchange.example.com	
Domain	Destination					
.example.com	exchange.example.com					
Data 2 Port						
IP Address:	192.168.2.1					
Network Mask:	255.255.255.0					
Fully Qualified Hostname:	mail.example.com					
Relay Outgoing Mail:	<table border="1"> <thead> <tr> <th>System</th> </tr> </thead> <tbody> <tr> <td>exchange.example.com</td> </tr> </tbody> </table>	System	exchange.example.com			
System						
exchange.example.com						
Management Port						
IP Address:	192.168.42.42					
Network Mask:	255.255.255.0					
Fully Qualified Hostname:	mail.example.com					

Message Security		Edit
SenderBase Reputation Filtering:	Enabled	
Default Incoming Mail Anti-Spam Engine:	IronPort Anti-Spam	
Sophos Anti-Virus:	Enabled	
Virus Outbreak Filters:	Enabled	

[Previous](#) [Cancel](#)
[Install This Configuration](#)

表示されている情報が要件を満たしていれば、[Install This Configuration] をクリックします。確認のダイアログが表示されます。[Install] をクリックして、新しい設定をインストールします。

図 3-11 System Setup Wizard : [Confirm Install]



これで、Cisco IronPort アプライアンスは、電子メールを送信できる状態になりました。



(注)

アプライアンスへの接続に使用するインターフェイス (X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 システムの Management インターフェイスまたは C10/100/150/160 システムの Data 1 インターフェイス) の IP アドレスをデフォルトから変更した場合は、[Install] をクリックすると、現在の URL (<http://192.168.42.42>) への接続が失われます。ただし、ブラウザは、新しい IP アドレスにリダイレクトされます。

システム セットアップが完了すると、複数のアラート メッセージが送信されます。詳細については、「即時アラート」(P.3-57) を参照してください。

Active Directory の設定

System Setup Wizard によって電子メールセキュリティ アプライアンスに設定が正しくインストールされると、Active Directory Wizard が表示されます。ネットワークで Active Directory サーバを稼動している場合は、Active Directory Wizard を使用して、Active Directory サーバ用の LDAP サーバ プロファイルの設定と、受信者検証用リスナーの割り当てを行う必要があります。Active Directory を使用していないか、後で設定する場合は、[Skip this Step] をクリックします。Active Directory Wizard は、[System Administration] > [Active Directory Wizard] ページで実行できます。Active Directory およびその他の LDAP プロファイルは、[System Administration] > [LDAP] ページでも設定できます。

Active Directory Wizard では、認証方式、ポート、ベース DN、および SSL をサポートするかどうかなど、LDAP サーバ プロファイルの作成に必要なシステム情報を取得します。Active Directory Wizard では、LDAP サーバ プロファイル用の LDAP の受け入れクエリーおよびグループ クエリーも作成します。

Active Directory Wizard によって LDAP サーバ プロファイルが作成されてから、[System Administration] > [LDAP] ページを使用して新規プロファイルを表示し、さらに変更を加えます。



クラウド電子メールセキュリティ アプライアンスの LDAP 設定は変更しないことを推奨します。

Active Directory Wizard を使用する手順は、次のとおりです。

- ステップ 1** [Active Directory Wizard] ページで [Run Active Directory Wizard] をクリックします。

図 3-12 Active Directory Wizard : 手順 1 : Start

- ステップ 2** Active Directory サーバのホスト名を入力します。
- ステップ 3** 認証要求のためのユーザ名およびパスワードを入力します。
- ステップ 4** [Next] をクリックして続行します。

Active Directory サーバへの接続が Active Directory Wizard によってテストされます。成功すると、[Test Directory Settings] ページが表示されます。

図 3-13 Active Directory Wizard : 手順 2 : [Directory Lookup Test]
Test Directory Settings

- ステップ 5** Active Directory に存在すると判明している電子メール アドレスを入力し、[Test] をクリックすることによって、ディレクトリ設定値をテストします。接続ステータス フィールドに結果が表示されます。
- ステップ 6** [Done] をクリックします。

次の手順

Active Directory Wizard と連携するようにアプライアンスを正常に設定するか、処理をスキップすると、[System Setup Next Steps] ページが表示されます。

図 3-14 システム セットアップの完了
System Setup Next Steps

The IronPort appliance should now be configured to work within your network infrastructure. See below for additional tasks and information.

<p>Data Loss Prevention</p> <p>Find out what sensitive information is leaving your network. The Data Loss Prevention (DLP) Assessment Wizard allows you to easily apply popular DLP policies to your outgoing mail so you can determine your risk exposure.</p> <p>Start Wizard...</p>	<p>Enter Feature Keys</p> <p>You enabled several features during System Setup. To continue using these features beyond the initial trial period, you must enter valid feature keys.</p> <p>Enter Feature Keys</p>
<p>Reports</p> <p>The IronPort appliance can generate, deliver, and archive periodic reports on email security for your organization.</p> <p>Manage Reports</p>	<p>Send Configuration File</p> <p>There are no recipients configured. Configuration file cannot be sent via email.</p>

[System Setup Next Steps] ページのリンクをクリックして、Cisco IronPort アプライアンスの設定を続行します。

コマンドライン インターフェイス (CLI) へのアクセス

CLI へのアクセスは、「[アプライアンスへの接続](#)」(P.3-14) で選択した管理接続方式によって異なります。工場出荷時のデフォルト ユーザ名およびパスワードを次に示します。当初は、**admin** ユーザ アカウントだけが CLI にアクセスできます。**admin** アカウントを介してコマンドライン インターフェイスに初回アクセスしたうえで、さまざまな許可レベルの他のユーザを追加できます (ユーザの追加については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」を参照してください)。**System Setup Wizard** で、**admin** アカウントのパスワードを変更するよう要求されます。**admin** アカウントのパスワードは、**password** コマンドを使用して、任意の時点で直接再設定することもできます。

イーサネットを介して接続する場合は、工場出荷時のデフォルト IP アドレスの 192.168.42.42 を使用して **SSH** セッションまたは **Telnet** セッションを開始します。**SSH** は、ポート 22 を使用するように設定されています。**Telnet** は、ポート 23 を使用するように設定されています。下記のユーザ名とパスワードを入力します。

シリアル接続を介して接続する場合は、パーソナル コンピュータのシリアル ケーブルが接続されている通信ポートを使用して端末セッションを開始します。「[アプライアンスへの接続](#)」(P.3-14) に示されているシリアル ポートの設定値を使用してください。下記のユーザ名とパスワードを入力します。

下記のユーザ名およびパスワードを入力してアプライアンスにログインします。

工場出荷時のデフォルト ユーザ名とパスワード

- ユーザ名 : **admin**
- パスワード : **ironport**

次の例を参考にしてください。

```
login: admin
password: ironport
```

コマンドライン インターフェイス (CLI) System Setup Wizard の実行

CLI バージョンの System Setup Wizard の手順は、基本的に GUI バージョン同様ですが、次のわずかな例外があります。

- CLI バージョンには、Web インターフェイスをイネーブルにするプロンプトが含まれています。
- CLI バージョンでは、作成する各リスナーのデフォルト メール フロー ポリシーを編集できます。
- CLI バージョンには、グローバルなアンチウイルス セキュリティ設定値および感染フィルタ セキュリティ設定値を設定するためのプロンプトが含まれています。
- CLI バージョンでは、システム セットアップの完了後に LDAP プロファイルを作成することを指示されません。ldapconfig コマンドを使用して LDAP プロファイルを作成してください。

System Setup Wizard を実行するには、コマンド プロンプトで `systemsetup` と入力します。

```
IronPort> systemsetup
```

システムを再設定するよう System Setup Wizard から警告が出されます。アプリケーションをまったく初めて設置する場合か、既存の設定を完全に上書きする場合は、この質問に [Yes] と回答します。

```
WARNING: The system setup wizard will completely delete any existing  
  
'listeners' and all associated settings including the 'Host Access  
Table' - mail operations may be interrupted.
```

```
Are you sure you wish to continue? [Y]> Y
```



(注) 以降のシステム セットアップ手順については、次で説明します。CLI バージョンの System Setup Wizard 対話の例には、「[Web ベースの System Setup Wizard の実行](#) (P.3-21) で説明した GUI バージョンの System Setup Wizard から逸脱する部分だけを含めてあります。

admin パスワードの変更

まず、AsyncOS の admin アカウントのパスワードを変更します。続行するには、現在のパスワードを入力する必要があります。新しいパスワードは 6 文字以上の長さである必要があります。パスワードは、必ず安全な場所に保管してください。パスワードの変更は、システム セットアップ プロセスを終了した時点で有効になります。

ライセンス契約書の受諾

表示されるソフトウェア使用許諾契約を参照して受諾します。

ホスト名の設定

次に、Cisco IronPort アプライアンスの完全修飾ホスト名を定義します。この前には、ネットワーク管理者が割り当てる必要があります。

論理 IP インターフェイスの割り当てと設定

次の手順では、Management (X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 アプライアンス) または Data 1 (C10/100/150/160 アプライアンス) 物理イーサネット インターフェイス上に論理 IP インターフェイスの割り当てと設定を行います。続いて、アプライアンス上で使用可能な他の任意の物理イーサネット インターフェイス上に論理 IP インターフェイスを設定するよう指示されます。

各イーサネット インターフェイスに複数の IP インターフェイスを割り当てることができます。IP インターフェイスは、IP アドレスおよびホスト名を物理イーサネット インターフェイスと関連付ける論理構成概念です。Data 1 と Data 2 の両方のイーサネット ポートを使用する場合は、両方の接続用に IP アドレスとホスト名が必要です。

X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 をご利用のお客様：パブリック リスナーを介してインバウンド電子メールを受信するためにインターネットに直接接続するように物理イーサネットポートの1つを使用し、プライベート リスナーを介してアウトバウンド電子メールをリレーするために内部ネットワークに直接接続するようにもう1つの物理イーサネットポートを使用することを推奨しています。

C10/100/150/160 をご利用のお客様：デフォルトでは、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方のために、リスナー1つの物理イーサネットポート1つだけが、`systemsetup` コマンドによって設定されます。



(注)

アウトバウンドメールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH がシステムによってオンにされます。

次の情報が必要です。

- 後でその IP インターフェイスを参照するために作成した**名前**（ニックネーム）。たとえば、イーサネットポートの1つをプライベート ネットワーク用に使用し、もう1つをパブリック ネットワーク用にしている場合は、それぞれ **PrivateNet** および **PublicNet** などの名前を付けます。



(注)

インターフェイス用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、2つの同じインターフェイス名を作成することはできません。たとえば、**Privatenet** および **PrivateNet** という名前は、異なる（一意の）2つの名前であると見なされます。

- ネットワーク管理者によって割り当てられた **IP アドレス**。
- インターフェイスの**ネットマスク**。ネットマスクは、標準のドット付き 10 進形式にするか、16 進形式にすることができます。



(注)

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。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、[付録 B 「ネットワーク アドレスと IP アドレスの割り当て」](#) を参照してください。



(注) C10/100 をご利用のお客様は、Data 2 インターフェイスを先に設定します。

デフォルト ゲートウェイの指定

`systemsetup` コマンドの次の部分では、ネットワークのデフォルト ルータ (ゲートウェイ) の IP アドレスを入力します。

Web インターフェイスのイネーブル化

`systemsetup` コマンドの次の部分では、アプライアンス (Management イーサネット インターフェイス) の Web インターフェイスをイネーブルにします。Secure HTTP (`https`) を介して Web インターフェイスを実行することもできます。HTTPS を使用する場合は、独自の証明書をアップロードするまで、デモ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「Enabling a Certificate for HTTPS」を参照してください。

DNS 設定値の設定

次に、Domain Name Service (DNS) 設定値を設定します。Cisco IronPort AsyncOS には、インターネットのルート サーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、独自の DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。必要な数の DNS サーバを入力できます (各サーバのプライオリティは 0 になります)。デフォルトでは、独自の DNS サーバのアドレスを入力するよう、`systemsetup` から示されます。

リスナーの作成

特定の IP インターフェイスに対して設定される、インバウンド電子メール処理サービスをリスナーによって管理します。リスナーは、内部システムまたはインターネットのいずれかから Cisco IronPort アプライアンスに着信する電子メールだけに適用されます。Cisco IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要

のある基準を指定します。リスナーは、上記で指定した IP アドレス用には実行されている電子メール リスナーであることを見なすことができます（「SMTP デーモン」と見なすことさえ可能）。

X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 をご利用のお客様：デフォルトでは、パブリックとプライベートのリスナー 1 つずつの合計 2 つのリスナーが `systemsetup` コマンドによって設定されます（使用可能なリスナー タイプの詳細については、「[電子メールを受信するためのゲートウェイの設定](#)」(P.5-1) を参照してください）。

C10/100/150/160 をご利用のお客様：デフォルトでは、インターネットからのメールの受信と内部ネットワークからの電子メールのリレーの両方に対応するパブリック リスナー 1 つが `systemsetup` コマンドによって設定されます。「[C10/100/150/160 のリスナーの例](#)」(P.3-49) を参照してください。

リスナーを定義するときは、次の属性を指定します。

- 後でそのリスナーを参照するために作成した**名前**（ニックネーム）。たとえば、インターネットに配信される、内部システムからの電子メールを受け入れるリスナーには、**OutboundMail** などの名前を付けます。
- 電子メールの受信に使用する、`systemsetup` コマンドで先に作成したいいずれかの IP インターフェイス。
- 電子メールのルーティング先にするマシンの名前（パブリック リスナーのみ）。これは、最初の `smtproutes` エントリです。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「[Routing Email for Local Domains](#)」を参照してください。
- パブリック リスナーで **SenderBase Reputation Score (SBRS; SenderBase 評価スコア)** に基づくフィルタリングをイネーブルにするかどうか。イネーブルにする場合は、**[Conservative]**、**[Moderate]**、または **[Aggressive]** から設定値を選択することも指示されます。
- ホストごとのレート制限：1 時間あたりにリモート ホストから受信する受信者の最大数（パブリック リスナーのみ）。
- 受け入れる電子メールの宛先にされている受信者ドメインまたは特定のアドレス（パブリック リスナーの場合）、またはアプライアンスを介した電子メールのリレーを許可するシステム（プライベート リスナーの場合）。これらは、リスナーの受信者アクセス テーブルおよびホスト アクセス テーブルの最初のエントリです。詳細については、「[送信者グループの構文](#)」(P.5-27) および「[パブリック リスナー \(RAT\) 上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ](#)」(P.5-72) を参照してください。

パブリック リスナー



(注) パブリック リスナーおよびプライベート リスナーを作成する次の例は、X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 をご利用のお客様だけに適用されます。Cisco IronPort C10/100/150/160 をご利用のお客様は、次の「[C10/100/150/160 のリスナーの例](#)」(P.3-49) にスキップしてください。

systemsetup コマンドのこの例の部分では、PublicNet IP インターフェイスで実行されるように InboundMail というパブリック リスナーを設定します。続いて、ドメイン example.com 宛てのすべての電子メールを受け入れるように設定します。Mail Exchange exchange.example.com への初期 SMTP ルートを設定します。レート制限をイネーブルにし、パブリック リスナーに対して単一のホストから受信する 1 時間あたりの受信者の最大値に 4500 を指定します。



(注) 1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」(未承諾の大量電子メールの送信者) である可能性があります。10,000 人規模の会社に対するすべての電子メールを処理する Cisco IronPort アプライアンスを設定する場合は、単一のリモート ホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業へのインバウンド電子メールのレート制限をイネーブルにする(量を絞る)場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、「[送信者グループの構文](#)」(P.5-27) を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

```
You are now going to configure how the IronPort C60 accepts mail by
creating a "Listener".
```

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

```
[ ]> InboundMail
```

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]> **3**

Enter the domains or specific addresses you want to accept mail for.

Hostnames such as "example.com" are allowed.

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

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.

Separate multiple addresses with commas.

[]> **example.com**

Would you like to configure SMTP routes for example.com? [Y]> **y**

Enter the destination mail server which you want mail for example.com to be delivered. Separate multiple entries with commas.

[]> **exchange.example.com**

```
Do you want to enable rate limiting for this listener? (Rate limiting
defines the maximum number of recipients per hour you are willing to
receive from a remote domain.) [Y]> y
```

```
Enter the maximum number of recipients per hour to accept from a
remote domain.
```

```
[ ]> 4500
```

```
Default Policy Parameters
```

```
=====
```

```
Maximum Message Size: 100M
```

```
Maximum Number Of Connections From A Single IP: 1,000
```

```
Maximum Number Of Messages Per Connection: 1,000
```

```
Maximum Number Of Recipients Per Message: 1,000
```

```
Maximum Number Of Recipients Per Hour: 4,500
```

```
Maximum Recipients Per Hour SMTP Response:
```

```
    452 Too many recipients received this hour
```

```
Use SenderBase for Flow Control: Yes
```

```
Virus Detection Enabled: Yes
```

```
Allow TLS Connections: No
```

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

```
Listener InboundMail created.
```

```
Defaults have been set for a Public listener.
```

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

```
*****
```

プライベート リスナー

systemsetup コマンドのこの例の部分では、PrivateNet IP インターフェイスで実行されるように **OutboundMail** というプライベート リスナーを設定します。次に、ドメイン example.com に含まれる任意のホスト宛てのすべての電子メールをリレーするように設定します（エントリ .example.com の先頭のドットに注意してください）。

続いて、レート制限（イネーブルでない）のデフォルト値およびこのリスナーのデフォルト ホスト アクセス ポリシーが受け入れられます。

プライベート リスナーのデフォルト値は、先に作成したパブリック リスナーのデフォルト値と異なることに注意してください。詳細については、「[パブリックリスナーとプライベートリスナー](#)」(P.5-5) を参照してください。

```
Do you want to configure the C60 to relay mail for internal hosts?  
[Y]> y
```

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

```
[ ]> OutboundMail
```

```
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]> 2
```

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 addresses are allowed.

Separate multiple entries with commas.

```
[ ]> .example.com
```

Do you want to enable rate limiting for this listener? (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

Virus Detection Enabled: Yes

Allow TLS Connections: No


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

```
Listener OutboundMail created.
```

```
Defaults have been set for a Private listener.
```

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

```
*****
```

C10/100/150/160 のリスナーの例



(注)

リスナーを作成する次の例は、C10/100/150/160 をご利用のお客様だけに適用されます。

systemsetup コマンドのこの例の部分では、MailNet IP インターフェイスで実行されるように MailInterface というリスナーを設定します。続いて、ドメイン example.com 宛てのすべての電子メールを受け入れるように設定します。Mail Exchange exchange.example.com への初期 SMTP ルートを設定します。次に、ドメイン example.com に含まれる任意のホスト宛てのすべての電子メールをリレーするように同じリスナーを設定します（エントリ .example.com の先頭のドットに注意してください）。

レート制限をイネーブルにし、パブリック リスナーに対して単一のホストから受信する 1 時間あたりの受信者の最大値に 450 を指定します。



(注)

1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性があります。10,000 人規模の会社に対するすべての電子メールを処理する Cisco IronPort アプライアンスを設定する場合は、単一のリモート ホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリックリスナーで、企業へのインバウンド電子メールのレート制限をイネーブルにする

(量を絞る) 場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、「送信者グループの構文」(P.5-27) を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

You are now going to configure how the IronPort C10 accepts mail by creating a "Listener".

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

```
[> MailInterface
```

Please choose an IP interface for this Listener.

1. MailNet (10.1.1.1/24: mail3.example.com)
2. Management (192.168.42.42/24: mail3.example.com)

```
[1]> 1
```

Enter the domain names or specific email addresses you want to accept mail for.

Hostnames such as "example.com" are allowed.

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

Username such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.

Separate multiple addresses with commas.

```
[> example.com
```

Would you like to configure SMTP routes for example.com? [Y]> **y**

Enter the destination mail server where you want mail for example.com to be delivered. Separate multiple entries with commas.

[]> **exchange.example.com**

Please specify the systems allowed to relay email through the IronPort C10.

Hostnames such as "example.com" are allowed.

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

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

Separate multiple entries with commas.

[]> **.example.com**

Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum number of recipients per hour you are willing to receive from a remote domain.) [Y]> **y**

Enter the maximum number of recipients per hour to accept from a remote domain.

[]> **450**

Default Policy Parameters

```
=====
Maximum Message Size: 10M

Maximum Number Of Connections From A Single IP: 50

Maximum Number Of Messages Per Connection: 100

Maximum Number Of Recipients Per Message: 100

Maximum Number Of Recipients Per Hour: 450

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control: Yes

Spam Detection Enabled: Yes

Virus Detection Enabled: Yes

Allow TLS Connections: No

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

Listener MailInterface created.

Defaults have been set for a Public listener.

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

*****
```



(注) この systemsetup コマンドでは、C10/100 を利用しているお客様向けに、インバウンドとアウトバウンドの両方のメールに対してリスナー 1 つだけを設定するため、すべての発信メールがメールフロー モニタ機能（通常はインバウンド

メッセージに使用) で評価されます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using the Email Security Monitor」を参照してください。

IronPort Anti-Spam のイネーブル化

Cisco IronPort アプライアンスには、IronPort Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。systemsetup コマンドのこの部分では、ライセンス契約書を受諾し、アプライアンスでグローバルに IronPort Anti-Spam をイネーブルにすることができます。

次に着信メール ポリシーに対する IronPort Anti-Spam スキャンをイネーブルにします。



(注)

ライセンス契約に合意しない場合、IronPort Anti-Spam はアプライアンスでイネーブルになりません。

アプライアンスで使用可能なすべての IronPort Anti-Spam 設定オプションについては、第 8 章「アンチスパム」を参照してください。

デフォルト アンチスパム スキャン エンジンの選択

複数のアンチスパム スキャン エンジンをイネーブルにした場合は、デフォルト着信メール ポリシーに対してイネーブルにするエンジンを選択するように示されます。

IronPort スпам検査のイネーブル化

アンチスパム サービスをイネーブルにする場合は、スパム メッセージおよび陽性と疑わしいスパム メッセージをローカル IronPort スпам検査エリアに送信するように、着信メール ポリシーをイネーブルできます。IronPort スпам検査をイネーブルにすると、アプライアンスでエンドユーザ検査もイネーブルになります。エンドユーザのアクセス権を設定していないうちは、管理者だけがエンドユーザ検査を利用できます。

IronPort スпам検査については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」を参照してください。

アンチウイルス スキャンのイネーブル化

Cisco IronPort アプライアンスには、ウイルス スキャン エンジンの 30 日間評価キーが付属しています。systemsetup コマンドのこの部分では、1 つまたは複数のライセンス契約書を受諾し、アプライアンスでアンチウイルス スキャンをイネーブルにできます。アプライアンスでイネーブルにするアンチウイルス スキャン エンジンごとにライセンス契約を受諾する必要があります。

契約書を受諾すると、選択したアンチウイルス スキャン エンジンが着信メールポリシーでイネーブルにされます。Cisco IronPort アプライアンスでは、着信メールをスキャンしてウイルスを検出しますが、感染した添付ファイルの修復は行いません。アプライアンスでは、感染したメッセージをドロップします。

アプライアンスで使用可能なアンチウイルス コンフィギュレーション オプションについては、[第 9 章「アンチウイルス」](#)を参照してください。

感染フィルタおよび SenderBase 電子メール トラフィック モニタリング ネットワークのイネーブル化

続くこの手順では、SenderBase への参加と感染フィルタの両方をイネーブルにするよう指示されます。Cisco IronPort アプライアンスには、感染フィルタの 30 日間評価キーが付属しています。

感染フィルタ

感染フィルタは、従来のアンチウイルス セキュリティ サービスが新しいウイルス シングニチャ ファイルで更新されるまで、疑わしいメッセージを検疫することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。感染フィルタをイネーブルにした場合は、デフォルト着信メール ポリシーでイネーブルになります。

感染フィルタをイネーブルにする場合は、しきい値および感染フィルタ アラートを受信するかどうかを入力します。感染フィルタおよびしきい値の詳細については、「[感染フィルタ](#)」(P.10-1)を参照してください。

SenderBase への参加

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールの評価サービスです。

SenderBase 電子メール トラフィック モニタリング ネットワークへの参加に同意した場合は、組織宛に送信された電子メールに関する集約された統計がシスコによって収集されます。メッセージ属性に関する要約データと、さまざまなタイプのメッセージを Cisco IronPort アプライアンスで処理した方法に関する情報が含まれます。

詳細については、[第 13 章「SenderBase Network Participation」](#)を参照してください。

アラート設定値および AutoSupport の設定

ユーザの介入を必要とするシステム エラーが発生した場合、Cisco IronPort AsyncOS では、電子メールでアラート メッセージをユーザに送信します。システム アラートを受信する電子メール アドレスを 1 つ以上追加してください。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メール アドレスでは、当初、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。CLI で `alertconfig` コマンドを使用するか、GUI で [System Administration] > [Alerts] ページを使用することにより、後でアラート コンフィギュレーションを詳細化できます。詳細については、「[アラート](#)」(P.15-24) を参照してください。

IronPort AutoSupport 機能では、ご使用の Cisco IronPort アプライアンスに関する問題を Cisco IronPort カスタマー サポート チームが認識しておくことで、業界トップ水準のサポートを提供できます。IronPort サポート アラートおよび週ごとのステータスの更新をシスコに送信するには、[Yes] と回答します（詳細は、「[IronPort AutoSupport](#)」(P.15-27) を参照してください）。

スケジュール済みレポートの設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値はブランクにすることができ、その場合、レポートは、電子メールで送信される代わりに、アプライアンス上にアーカイブされます。

時刻設定値の設定

Cisco IronPort AsyncOS では、ネットワーク タイム プロトコル (NTP) を使用して、ネットワーク上またはインターネット上の他のサーバと時刻を同期するか、システム クロックを手動で設定することができます。Cisco IronPort アプライアンス上の時間帯を設定して、メッセージ ヘッダーおよびログ ファイルのタ

タイムスタンプを正確にする必要もあります。Cisco IronPort Systems タイム サーバを使用して Cisco IronPort アプライアンス上の時刻を同期することもできます。

[Continent]、[Country]、および [Timezone] を選択し、NTP を使用するかどうかと、使用する NTP サーバの名前を選択します。

変更の確定

最後に、手順全体で行った設定変更を確定するかどうかの確認が、System Setup Wizard から示されます。変更を確定する場合は、[Yes] と回答します。

System Setup Wizard を正常に完了すると、次のメッセージが表示されて、コマンドプロンプトが出されます。

```
Congratulations! System setup is complete. For advanced
configuration, please refer to the User Guide.
```

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

これで、Cisco IronPort アプライアンスは、電子メールを送信できる状態になりました。

設定のテスト

Cisco IronPort AsyncOS の設定をテストするために、`mailconfig` コマンドをすぐに使用して、`systemsetup` コマンドで作成したばかりのシステム コンフィギュレーション データを含むテスト電子メールを送信できます。

```
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
```



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

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

利用可能なメールボックスに設定を送信して、システムでネットワーク上に電子メールを送信できることを確認します。

即時アラート

Cisco IronPort アプライアンスでは、機能キーを使用して機能をイネーブルにします。systemsetup コマンドでリスナーを最初に作成した場合、IronPort Anti-Spam をイネーブルにした場合、Sophos または McAfee Anti-Virus をイネーブルにした場合、または感染フィルタをイネーブルにした場合は、アラートが生成されて、「手順 2 : System」(P.3-23) で指定したアドレスに送信されません。

キーの残り時間を定期的に通知するアラートです。次の例を参考にしてください。

```
Your "Receiving" key will expire in under 30 day(s). Please contact  
IronPort Customer Support.
```

```
Your "Sophos" key will expire in under 30 day(s). Please contact  
IronPort Customer Support.
```

```
Your "Outbreak Filters" key will expire in under 30 day(s). Please  
contact IronPort Customer Support.
```

30 日間の評価期間を超えて機能をイネーブルにする場合は、Cisco IronPort 営業担当者にお問い合わせください。キーの残り時間は、[System Administration] > [Feature Keys] ページからか、featurekey コマンドを発行することによって確認できます（詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください）。

次の手順：電子メールパイプラインの理解

systemsetup が完了したため、Cisco IronPort アプライアンスによって電子メールが送信および受信されます。アンチウイルス、アンチスパム、およびウイルス感染フィルタ セキュリティ機能をイネーブにした場合は、着信メールおよび発信メールでスパムおよびウイルスのスキャンも行われます。

次の手順では、アプライアンスの設定をカスタマイズする方法を理解します。第 4 章「[電子メールパイプラインの理解](#)」では、システムでの電子メールのルーティング方法の詳細な概要を説明しています。各機能は、順次（上から下に）処理されます。各機能については、本書の残りの章で説明します。



CHAPTER 4

電子メールパイプラインの理解

電子メールパイプラインは、Cisco IronPort アプライアンスによる処理に伴う、電子メールのプロセスまたはフローです。Cisco IronPort アプライアンスの性能を最大限まで引き出すには、電子メールパイプラインの理解が不可欠です。

この章では、着信メールの電子メールパイプラインの概要を示し、各機能について簡単に説明します。この簡単な説明には、その機能の詳細説明を含む章または資料へのリンクも含まれています。

この章は、次の内容で構成されています。

- 「概要：電子メールパイプライン」(P.4-1)
- 「着信および受信」(P.4-5)
- 「ワークキューとルーティング」(P.4-8)
- 「配信」(P.4-14)

概要：電子メールパイプライン

表 4-1 および表 4-2 に、システムによる受信からルーティングおよび配信までの、電子メールの処理の概要を示します。各機能は順序どおり（上から下）に処理されます。各機能を以下で簡単に説明します。各機能の詳細説明については、後続の章を参照してください。一部の機能については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』および『*Cisco IronPort AsyncOS for Email Daily Management Guide*』で説明されています。

表 4-2 の網掛け部分は、ワーク キュー（「ワーク キューとルーティング」(P.4-8) を参照）で実行される処理を表します。このパイプラインに含まれる機能の設定の大部分は、trace コマンドを使用してテストできます。詳細については、「Debugging Mail Flow Using Test Messages: Trace」(P.446) を参照してください。

表 4-1 Cisco IronPort アプライアンスの電子メールパイプライン：電子メール受信機能

機能	説明
ホスト アクセス テーブル (HAT) ホスト DNS 送信者検証 送信者グループ エンベロープ送信者検証 送信者検証例外テーブル メール フロー ポリシー	接続の ACCEPT、REJECT、RELAY、または TCPREFUSE。 最大アウトバウンド接続数。 IP アドレスあたりの最大同時インバウンド接続数。 接続あたりの最大メッセージサイズおよびメッセージ数。 メッセージあたりおよび時間あたりの最大受信者数。 TCP リッスン キュー サイズ。 TLS : no/preferred/required。 SMTP AUTH : no/preferred/required。 不正な形式の FROM ヘッダーを持つ電子メールのドロップ。 送信者検証例外テーブル内のエントリからのメールを常に受け入れるか拒否します。 SenderBase オン/オフ (IP プロファイリング/フロー制御)。
Received ヘッダー	受け入れた電子メールに対する Received ヘッダーの追加：オン/オフ。
デフォルト ドメイン	「素」ユーザ アドレスにデフォルト ドメインを追加します。
バウンス検証	着信バウンス メッセージを正規メッセージとして検証します。
ドメイン マップ	ドメイン マップ テーブル内のドメインと一致するメッセージに含まれている各受信者のエンベロープ受信者の書き換え。
受信者アクセス テーブル (RAT)	(パブリック リスナーのみ) RCPT TO およびカスタム SMTP 応答内の受信者の ACCEPT または REJECT 特別な受信者にスロットリングのバイパスを許可します。

表 4-1 Cisco IronPort アプライアンスの電子メール パイプライン：電子メール受信機能（続き）

エイリアス テーブル	エンベロープ受信者を書き換えます。（システム全体を対象に設定されます <code>aliasconfig</code> は、 <code>listenerconfig</code> のサブコマンドではありません）。
LDAP 受信者の受け入れ	受信者受け入れの LDAP 検証は、SMTP カンバセーションで行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりにワーク キュー内で LDAP 検証を行うように設定することもできます。
SMTP Call-Ahead 検証	SMTP Call-Ahead 受信者検証は、SMTP カンバセーションで行われます。電子メールセキュリティ アプライアンスによる外部 SMTP サーバへの事前呼び出し中は、SMTP カンバセーションが中断します。SMTP サーバの応答に応じて、メッセージがドロップまたはバウンスされるか、メールアクションが許可されます。

表 4-2 Cisco IronPort アプライアンスの電子メールパイプライン：ルーティングおよび配信機能

ワークキュー	LDAP 受信者の受け入れ	受信者受け入れの LDAP 検証はワーク キュー内で行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりに SMTP キャンパセーション LDAP 検証を行うよう設定することもできます。
	マスカレード または LDAP マスカレード	マスカレードは、ワーク キューで行われます。マスカレードでは、スタティック テーブルを使用するか LDAP クエリーを使用して、エンベロープ送信者、To:、From:、CC: ヘッダーを書き換えます。
	LDAP ルーティング	LDAP クエリーは、メッセージルーティングまたはアドレス書き換えのために実行されます。グループ LDAP クエリーは、メッセージフィルタ ルール mail-from-group および rcpt-to-group と連携して動作します。
	メッセージフィルタ *	メッセージフィルタは、メッセージが「分裂」される前に適用されます。* メッセージを検疫エリアに送信できます。
	セーフリスト/ブロックリスト スキャン	AsyncOS では、送信者アドレスをエンドユーザ セーフリスト/ブロックリスト データベースと照合します。送信者アドレスがセーフリストにあれば、アンチスパムのスキャンはスキップされます。受信者が複数の場合は、メッセージを分裂できます。* 送信者が Blocklist にある場合は、メッセージを検疫エリアに送信できます。
	アンチスパム **	アンチスパム スキャン エンジンでは、メッセージを検査して、さらに処理するために判定を返します。
	アンチウイルス *	アンチウイルス スキャンでは、ウイルスを検出するためにメッセージを検査します。メッセージはスキャンされ、可能であれば、任意で修復されます。* メッセージを検疫エリアに送信できます。
	コンテンツ フィルタ *	コンテンツ フィルタが適用されます。該当するコンテンツ フィルタ条件が定義されている場合は、DKIM、SPF、および SDF 検証が実行されます。* メッセージを検疫エリアに送信できます。
	感染フィルタ *	感染フィルタ機能を使用すると、ウイルス感染だけではなく、新種の詐欺、フィッシング、悪意のある攻撃から保護できます。* メッセージを検疫エリアに送信できます。
	データ消失防止（発信メッセージのみ）	RSA Email Data Loss Prevention は機密データの発信メッセージを調べます。RSA Email DLP は、発信メッセージ専用です。* メッセージを検疫エリアに送信できます。
仮想ゲートウェイ	特定の IP インターフェイスまたは IP インターフェイスのグループを介してメールを送信します。	

電子メールセキュリティマネージャスキャン (受信者単位)

表 4-2 Cisco IronPort アライアンスの電子メールパイプライン：ルーティングおよび配信機能（続き）

配信制限	1. デフォルト配信インターフェイスを設定します。 2. アウトバウンド接続の合計最大数を設定します。
ドメインベースの制限値	ドメイン単位で、各仮想ゲートウェイおよびシステム全体の最大アウトバウンド接続数、使用するバウンス プロファイル、配信用の TLS プレファレンス： no/preferred/required を定義します。
ドメインベースのルーティング	エンベロープ受信者を書き換えず、ドメインに基づいてメールをルーティングします。
グローバル配信停止	特定のリストに従って受信者をドロップします（システム全体を対象に設定）。
バウンス プロファイル	配信不能メッセージの処理です。リスナー単位、宛先制御エントリ単位、およびメッセージ フィルタ経由で設定可能です。

* これらの機能では、Quarantines という特別なキューにメッセージを送信できます。

** IronPort スпам検疫にメッセージを送信できます。

着信および受信

電子メールパイプラインの受信フェーズでは、送信者のホストからの初期接続が行われます。各メッセージのドメインを設定でき、受信者が検査されて、メッセージはワーク キューに渡されます。

ホスト アクセス テーブル (HAT)、送信者グループ、およびメール フロー ポリシー

HAT では、リスナーへの接続を許可するホスト（つまり、電子メールの送信を許可するホスト）を指定できます。

送信者グループは、1 つまたは複数の送信者をグループに関連付けるために使用されるもので、メッセージ フィルタおよびその他のメール フロー ポリシーを送信者グループに対して適用できます。メール フロー ポリシーは、一連の HAT パラメータ（アクセス ルール、レート制限パラメータ、およびカスタム SMTP コードと応答）を表現する 1 つの方法です。

送信者グループおよびメール フロー ポリシーは合わせて、リスナーの HAT で定義されます。

送信者グループのホスト DNS 検証設定では、SMTP カンバセーションの前に未検証の送信者を分類し、さまざまな種類の未検証の送信者をさまざまな送信者グループに含めることができます。

SMTP カンバセーションに先立って、接続元のホストが送信者グループでホスト DNS 検証の対象になった一方で、エンベロープ送信者のドメイン部分はメール フロー ポリシーで DNS 検証されます。この検証は、SMTP カンバセーションの間に行われます。不正な形式のエンベロープ送信者を含むメッセージを無視できます。送信者検証例外テーブルにエントリを追加できます。このテーブルはメールの受け入れや拒否の基盤となるドメインと電子メール アドレスのリストで、エンベロープ送信者 DNS 検証設定値の影響は受けません。

評価フィルタリングでは、電子メール送信者を分類でき、Cisco IronPort SenderBase 評価サービスによって決定された送信者の信頼性に基づいて電子メール インフラストラクチャの利用を制限できます。

詳細については、「[ホスト アクセス テーブル \(HAT\) : 送信者グループとメール フロー ポリシー](#)」(P.5-9) を参照してください。

Received: ヘッダー

listenerconfig コマンドを使用すると、リスナーで受信したすべてのメッセージに対して、デフォルトでは Received: ヘッダーを組み込まないようにリスナーを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Advanced Configuration Options」を参照してください。

デフォルト ドメイン

完全修飾ドメイン名を含んでいない送信者アドレスにデフォルト ドメインを自動的に追加するようリスナーを設定できます。これらのアドレスを「素」アドレスとも呼びます（「joe」と「joe@example.com」など）。

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。

バウンス検証

発信メールには特別なキーがタグ付けされます。これにより、そのメールがバウンスとして送り返された場合は、そのタグを認識したうえでメールが配信されません。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「IronPort Bounce Verification」を参照してください。

ドメインマップ

設定するリスナーごとにドメインマップテーブルを作成できます。ドメインマップテーブルに含まれているドメインと一致するメッセージでは、各受信者のエンベロップ受信者が書き換えられます。たとえば、joe@old.com -> joe@new.com です。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「The Domain Map Feature」を参照してください。

受信者アクセス テーブル (RAT)

インバウンド電子メールに限っては、Cisco IronPort アプライアンスでメールを受け入れるすべてのローカルドメインのリストを、RATによって指定できます。

詳細については、「[パブリックリスナー \(RAT\) 上でのローカルドメインまたは特定のユーザの電子メールの受け入れ](#)」(P.5-72)を参照してください。

エイリアス テーブル

エイリアステーブルには、1人または複数の受信者にメッセージをリダイレクトするメカニズムが備わっています。エイリアスはマッピングテーブルに格納されます。電子メールのエンベロップ受信者 (Envelope To または RCPT TO と呼ぶ) とエイリアステーブルに定義されているエイリアスが一致すると、電子メールのエンベロップ受信者アドレスが書き換えられます。

エイリアステーブルの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Creating Alias Tables」を参照してください。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メールアドレス（パブリック リスナー上）を SMTP カンバセーションまたはワーク キュー内で処理する方法を定義できます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Accept Queries」を参照してください。これにより、Cisco IronPort アプライアンスでは、独特な方法で Directory Harvest Attacks（DHAP; ディレクトリ獲得攻撃）に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワーク キューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリで見つからない場合は、遅延型バウンスを実行するか、メッセージ全体をドロップするようにシステムを設定できます。

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。

SMTP Call-Ahead 受信者検証

SMTP Call-Ahead 受信者検証用に電子メールセキュリティ アプライアンスを設定した場合、受信者検証時の SMTP サーバへの「事前呼び出し」中、電子メールセキュリティ アプライアンスは送信 MTA を使用して SMTP カンバセーションを一時停止します。Cisco IronPort アプライアンスが SMTP サーバに問い合わせると、SMTP サーバの応答が電子メールセキュリティ アプライアンスに返されます。電子メールセキュリティ アプライアンスは SMTP カンバセーションを再開し、送信 MTA に応答を送信します。カンバセーションは SMTP サーバの応答（および SMTP Call-Ahead プロファイルに指定した設定）に基づいて接続を続行するか、切断します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Validating Recipients Using an SMTP Server」の章を参照してください。

ワーク キューとルーティング

ワーク キューでは、配信フェーズに移動される前の受信メッセージを処理します。処理には、マスカレード、ルーティング、フィルタリング、セーフリスト/ブロックリスト スキャン、アンチスパムおよびアンチウイルス スキャン、感染フィルタ、および検疫が含まれます。



- (注) Data Loss Prevention (DLP) スキャンは、発信メッセージだけで使用可能です。DLP メッセージ スキャンが実行されるワーク キュー内の位置については、「[メッセージ分裂](#)」(P.6-6) を参照してください。

電子メールパイプラインとセキュリティ サービス



クラウド電子メールセキュリティ アプライアンスのセキュリティ サービスは、イネーブルにして変更しないことを推奨します。

原則として、セキュリティ サービス (アンチスパム スキャン、アンチウイルス スキャン、および感染フィルタ) に対する変更は、すでにワーク キューにあるメッセージには影響しません。次に例を示します。

初めてパイプラインに入るメッセージについて、次のいずれかの理由により、アンチウイルス スキャンがバイパスされると仮定します。

- アプライアンスでグローバルにアンチウイルス スキャンがイネーブルにされていなかった。または、
- アンチウイルス スキャンをスキップするように HAT ポリシーで指定されていた。または、
- そのメッセージに対するアンチウイルス スキャンをバイパスさせるメッセージ フィルタが存在していた。

この場合、アンチウイルス スキャンが再イネーブル化されているかどうかを問わず、検疫エリアから解放される時にそのメッセージのアンチウイルス スキャンは行われません。ただし、メール ポリシーに基づいてアンチウイルス スキャンがバイパスされるメッセージの場合は、検疫エリアからの解放時にアンチウイルス スキャンが行われる可能性があります。メッセージが検疫エリアにある間に、メール ポリシーの設定値が変更される可能性があるためです。たとえば、メール ポリシーによってメッセージがアンチウイルス スキャンをバイパスし、検疫されている場合に、検疫エリアからの解放以前にメール ポリシーが更新されて、アンチウイルス スキャンが組み込まれた場合、そのメッセージは、検疫エリアからの解放時にアンチウイルス スキャンが行われます。

同様に、誤ってアンチスパム スキャンをグローバルに (または HAT で) デイセーブルにし、メールがワーク キューに入った後で気付いたとします。その時点でアンチスパムをイネーブルにしても、ワーク キューにあるメッセージについてはアンチスパム スキャンは行われません。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メールアドレス（パブリック リスナー上）を SMTP キャンパセーションまたはワーク キュー内で処理する方法を定義できます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Accept Queries」を参照してください。これにより、Cisco IronPort アプライアンスでは、独特な方法で Directory Harvest Attacks（DHAP; ディレクトリ獲得攻撃）に対処できます。システムでは、メッセージを受け入れて、SMTP キャンパセーションまたはワーク キューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリで見つからない場合は、遅延型バウンスを実行するか、メッセージ全体をドロップするようにシステムを設定できます。

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。

マスカレードまたは LDAP マスカレード

マスカレードは、管理者が作成するテーブルに従って、プライベート リスナーで処理される電子メールのエンベロップ送信者（Sender または MAIL FROM とも呼ぶ）と To:、From:、CC: のヘッダーを書き換える機能です。スタティック マッピング テーブルと LDAP クエリーの 2 通りのうちいずれかによって、作成したリスナーごとに異なるマスカレード パラメータを指定できます。

スタティック マッピング テーブルによるマスカレードの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Configuring Masquerading」を参照してください。

クエリーによるマスカレードの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

LDAP ルーティング

ネットワーク上の LDAP ディレクトリで使用可能な情報に基づいて、適切なアドレスやメール ホストにメッセージをルーティングするように Cisco IronPort アプライアンスを設定できます。

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。

メッセージフィルタ

メッセージフィルタでは、受信直後のメッセージおよび添付ファイルの処理方法を記述した特別なルールを作成できます。フィルタルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージエンベロープ、メッセージヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタアクションでは、メッセージのドロップ、バウンス、アーカイブ、検疫、ブラインドカーボンコピー、または変更を行うことができます。

詳細については、『*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。

複数受信者メッセージは、このフェーズの後に、電子メールセキュリティマネージャに先立って「分裂」されます。メッセージの分裂とは、電子メールセキュリティマネージャによる処理のために、単一の受信者を設定した電子メールの分裂版コピーを作成することを指します。

電子メールセキュリティマネージャ（受信者単位のスキャン）

セーフリスト/ブロックリストスキャン

エンドユーザセーフリストおよびブロックリストは、エンドユーザによって作成されて、アンチスパムスキャンに先行して検査されるデータベースに格納されます。各エンドユーザは、常にスパムとして扱うか、決してスパムとして扱わないドメイン、サブドメイン、または電子メールアドレスを指定できます。送信者アドレスがエンドユーザセーフリストに含まれている場合、アンチスパムスキャンはスキップされます。送信者アドレスがブロックリストに含まれている場合、メッセージは、管理者設定値に応じて検疫するかドロップすることができます。セーフリストおよびブロックリストの設定の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

アンチスパム

アンチスパム機能には、IronPort Anti-Spam スキャンが含まれます。アンチスパム スキャンは、インターネット全体にわたるサーバ側のアンチスパム保護を提供します。アンチスパム スキャンでは、スパム攻撃によってユーザに不便が生じ、ネットワークが蹂躪されたり損傷したりする前に、スパム攻撃を活発に識別し、危険を除去します。その結果、ユーザのプライバシーを侵害することなく、ユーザの受信箱に届く前に、不要なメールを削除できます。

アンチスパム スキャンは、IronPort スпам検疫（オンボックスまたはオフボックス）にメールを配信するように設定できます。IronPort スпам検疫から解放されたメッセージは、電子メールパイプラインの以降のすべてのワーク キュー処理をスキップして、宛先キューに直接移動されます。

詳細については、[第 8 章「アンチスパム」](#)を参照してください。

アンチウイルス

Cisco IronPort アプライアンスには、統合されたウイルス スキャン エンジンが含まれています。「メール ポリシー」ごとを基本に、メッセージおよび添付ファイルをスキャンしてウイルスを検出するように、アプライアンスを設定できます。ウイルスが検出された場合に次の処置を行うようにアプライアンスを設定できます。

- 添付ファイルの修復の試行
- 添付ファイルのドロップ
- 件名ヘッダーの変更
- 追加の X-Header の追加
- 異なるアドレスまたはメールホストへのメッセージの送信
- メッセージのアーカイブ
- メッセージの削除

メッセージが検疫エリア（[「検疫」\(P.4-13\)](#)を参照）から解放されると、ウイルスがスキャンされます。アンチウイルス スキャンの詳細については、[第 9 章「アンチウイルス」](#)を参照してください。

コンテンツ フィルタ

受信者ごとまたは送信者ごとを基準に、メッセージに適用するコンテンツ フィルタを作成できます。コンテンツ フィルタは、電子メールパイプラインで後ほど適用される点、つまり、1つのメッセージが、各電子メールセキュリティ マネージャ ポリシーに対応する個々の複数のメッセージに「分裂」された後で適用される点を除いては、メッセージ フィルタとほぼ同じです。コンテンツ フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。

コンテンツ フィルタの詳細については、「[コンテンツ フィルタの概要](#)」(P.6-10)を参照してください。

感染フィルタ

Cisco IronPort の感染フィルタ機能には、新たな拡散に対抗するための重要な第 1 層となるように活発に動作する特別なフィルタが含まれています。Cisco IronPort の発行するアウトブレイク ルールに基づいて、特定のファイル タイプの添付ファイルを持つメッセージを **Outbreak** という名前の検疫エリアに送信できます。

Outbreak 検疫エリア内のメッセージは、他のすべての検疫エリア内のメッセージと同じように処理されます。検疫エリアおよびワーク キューの詳細については、「[検疫](#)」(P.4-13)を参照してください。

詳細については、[第 10 章「感染フィルタ」](#)を参照してください。

検疫

Cisco IronPort AsyncOS では、着信メッセージまたは発信メッセージをフィルタして、検疫エリアに入れることができます。検疫エリアは、メッセージの保持と処理に使用される特別なキュー、言い換えるとリポジトリです。検疫エリア内のメッセージは、検疫の設定方法に基づいて配信するか削除できます。

次のワーク キュー機能では、メッセージを検疫エリアに送信できます。

- メッセージ フィルタ
- アンチウイルス
- 感染フィルタ
- コンテンツ フィルタ

メッセージが検疫エリアから解放されると、ウイルスが再度スキャンされます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

配信

電子メールパイプラインの配信フェーズでは、接続の制限、バウンス、および受信者など、電子メール処理の最終フェーズを主とします。

仮想ゲートウェイ

Cisco IronPort Virtual Gateway テクノロジーを使用すると、Cisco IronPort アプライアンスを複数の Virtual Gateway アドレスに分割し、そのアドレスを使用して電子メールを送受信できます。各仮想ゲートウェイアドレスには、個別の IP アドレス、ホスト名、およびドメインと電子メール配信キューが割り当てられます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Using Virtual Gateway Technology」を参照してください。

配信制限

配信時に使用する IP インターフェイスに基づく配信の制限およびアプライアンスでアウトバウンドメッセージ配信に適用する最大同時接続数を設定するには、`deliveryconfig` コマンドを使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Set Email Delivery Parameters」を参照してください。

ドメインベースの制限値

各ドメインに対して、一定期間でシステムが超えることができない、接続および受信者の最大数を割り当てることができます。この「グッドネイバー」テーブルは、[Mail Policies] > [Destination Controls] ページ（または `destconfig` コマンド）から定義します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Controlling Email Delivery」を参照してください。

ドメインベースのルーティング

エンベロープ受信者を書き換えることなく、特定のドメイン宛てのすべての電子メールを特定の Mail Exchange (MX) ホストにリダイレクトするには、[Network] > [SMTP Routes] ページ（または `smtproutes` コマンド）を使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Routing Email for Local Domains」を参照してください。

グローバル配信停止

特定の受信者、受信者ドメイン、または IP アドレスに対する Cisco IronPort アプライアンスからのメッセージの配信を確実に停止するには、グローバル配信停止を使用します。グローバル配信停止をイネーブルにすると、すべての受信者アドレスが、グローバル配信停止対象のユーザ、ドメイン、電子メール アドレス、および IP アドレスのリストと照合されます。一致する電子メールは送信されません。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Using Global Unsubscribe」を参照してください。

バウンス制限

作成する各リスナーのキャンパセーションのハードバウンスおよびソフトバウンスを Cisco IronPort AsyncOS で処理する方法を設定するには、[Network] > [Bounce Profiles] ページ（または `bounceconfig` コマンド）を使用します。バウンスプロファイルを作成し、各リスナーにプロファイルを適用するには、[Network] > [Listeners] ページ（または `listenerconfig` コマンド）を使用します。メッセージフィルタを使用して、特定のメッセージにバウンスプロファイルを割り当てることもできます。

バウンスプロファイルの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Directing Bounced Email」を参照してください。



CHAPTER 5

電子メールを受信するためのゲートウェイの設定



Cloud Email Security アプライアンスでリスナーの追加、変更、および削除を回避することが推奨されます。

この時点で、GUI の System Setup Wizard（または CLI の `systemsetup` コマンド）を使用して Cisco IronPort アプライアンスの基本的な設定を行うことにより、Cisco IronPort 電子メール セキュリティ アプライアンスで電子メールを受信するために設定の調整を開始できます。ここでは、受信電子メールを処理するためにアプライアンス上でリスナーの設定を開始するときに使用できるすべての機能について詳しく説明します。

ホスト アクセス テーブル（HAT）の概念について紹介しています。パブリックリスナーのホスト アクセス テーブル（HAT）と、その固有の送信者グループおよびメール フロー ポリシーは、メール フロー モニタ機能を可能にするための基礎となるフレームワークです（メール フロー モニタ機能の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」を参照してください）。

この章は、次の内容で構成されています。

- 「リスナーによる電子メールの受信」 (P.5-2)
- 「ホスト アクセス テーブル（HAT）：送信者グループとメール フロー ポリシー」 (P.5-9)
 - 「メール フロー ポリシー：アクセス ルールとパラメータ」 (P.5-11)
 - 「送信者グループ」 (P.5-25)
- 「GUI によるリスナーの HAT の変更」 (P.5-53)
- 「送信者検証」 (P.5-56)

- 「パブリック リスナー (RAT) 上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ」 (P.5-72)
- 「GUI によるリスナーの RAT の変更」 (P.5-77)

リスナーによる電子メールの受信

Cisco IronPort AsyncOS オペレーティング システムを使用すると、Cisco IronPort アプライアンスは企業のインバウンド電子メールのゲートウェイとして機能することが可能になり、インターネットからの SMTP 接続の処理、メッセージの許可、および適切なシステムへのメッセージの中継を行うことができます。

この構成では、これらの接続を使用可能にするためにリスナーをイネーブルにします。リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、ネットワーク内にある内部システムまたはインターネットから Cisco IronPort アプライアンスに入る電子メールだけに適用されます。Cisco IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要がある基準を指定します。リスナーは、指定した各 IP アドレス (systemsetup コマンドで設定した初期アドレスを含みます) 用に特定のポート上で動作する「電子メールインジェクタ」または「SMTP デーモン」と考えることができます。

メールが単一の IP アドレス上の複数のポートに配信されるようなメール配信ポリシーの設定はできません (たとえば、通常配信用にポート 25 を設定し、IronPort のスパム検疫用にポート 6025 を設定するなど)。各配信オプションを個別の IP アドレスまたはホスト上で実行することが推奨されます。さらに、通常の電子メール配信用と検疫配信用には同じホスト名を使用できません。

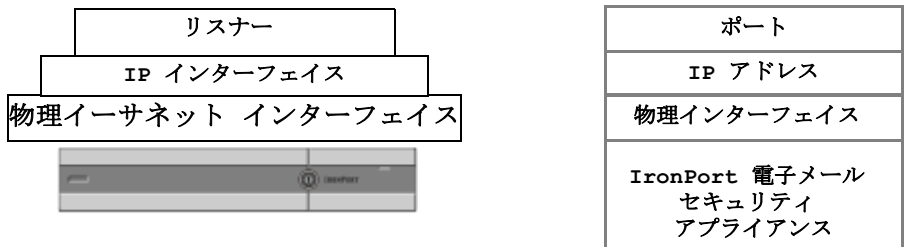
System Setup Wizard または systemsetup コマンド (CLI) は、最初に Cisco IronPort アプライアンス上の使用可能なイーサネット インターフェイスで動作する IP インターフェイスを設定します。Cisco IronPort C150 アプライアンスと C160 アプライアンスでは、これらのイーサネット インターフェイスに Data1 および Data2 というラベルが付与されています。その他すべての Cisco IronPort アプライアンスでは、Data1、Data2、および Management というラベルが付与されています。これらのインターフェイスは後で [Network] メニューの [IP Interfaces] ページか interfaceconfig コマンドを使用して編集できます。GUI の System Setup Wizard (または systemsetup コマンド) を完了し、変更内容を確定した場合、すでに少なくとも 1 つのリスナーがアプライアンス上で構成されています (「手順 3 : Network」 (P.3-26) で入力した設定を参照)。メールを受信するためのアドレスは、その時点と、最初の SMTP ルート ([Network] > [SMTP Routes] または smtpoutes) の入力時に入力します。



(注) System Setup Wizard を使用して新しいリスナーを作成するとき、AsyncOS はデフォルト値でリスナーを作成します。しかし、手動でリスナーを作成する場合、AsyncOS はこれらのデフォルトの SBRs 値を使用しません。

Cisco IronPort アプライアンスの使用可能な IP インターフェイス上で動作するリスナーを設定するには、[Listeners] ページ ([Network] > [Listeners]) または `listenerconfig` コマンドを使用します。リスナーの作成と設定の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」の章を参照してください。『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Virtual Gateway™ Technology」では、Cisco IronPort Virtual Gateway テクノロジーについて説明しています。このテクノロジーを使用すると、1 つ以上の IP アドレス (IP アドレス グループ) に対して IP インターフェイスをさらに定義してグループ化できます。

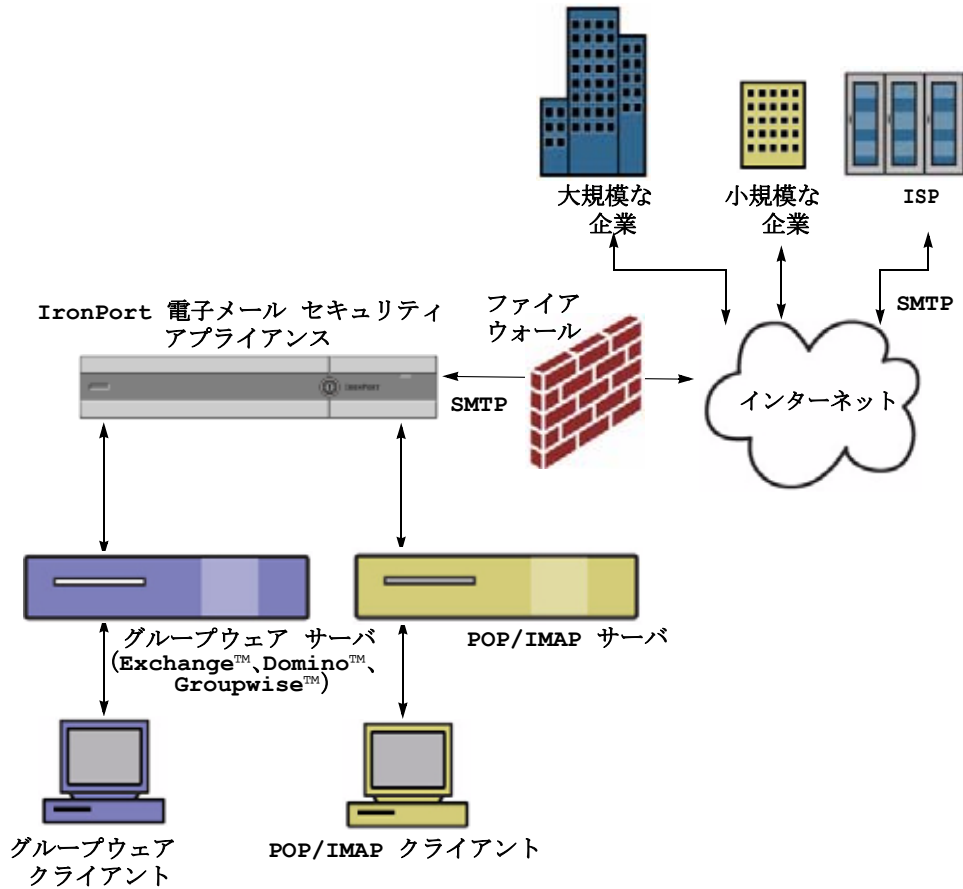
図 5-1 リスナー、IP インターフェイス、物理イーサネット インターフェイスの関係



エンタープライズ ゲートウェイ構成

この構成では、エンタープライズ ゲートウェイ構成はインターネットからの電子メールを許可し、ゲートウェイ サーバ、POP/IMAP サーバ、またはその他の MTA に電子メールを中継します。エンタープライズ ゲートウェイは、それと同時に、グループウェア サーバおよびその他の電子メール サーバからの SMTP メッセージを受け付け、インターネット上の受信者に中継します。

図 5-2 エンタープライズ ゲートウェイとしての Cisco IronPort アプライアンスの使用



この構成では、少なくとも次の 2 つのリスナーが必要です。

- インターネットからのメールを受け付けるために専用設定されたリスナー
- 内部のグループウェアおよび電子メールサーバ (POP/IMAP) からのメールを受け付けるために専用設定されたリスナー

パブリック リスナーとプライベート リスナー

最初のリスナーを「パブリック リスナー」、2 番目のリスナーを「プライベート リスナー」と考えます。Cisco IronPort AsyncOS は、デフォルトでインターネットから電子メールを受信する特性を持つパブリック リスナーと、内部（グループウェア、POP/IMAP などのメッセージ生成）システムからだけの電子メールの受け入れを目的としたプライベート リスナーを区別します。パブリック リスナーとプライベート リスナーは、デフォルトでは、利用できる機能やデフォルト設定が異なります。異なるパブリック ネットワークとプライベート ネットワーク用に個別のパブリック リスナーとプライベート リスナーを作成することで、セキュリティ、ポリシー強制、レポートニング、管理用に電子メールを区別できます。たとえば、パブリック リスナーで受信した電子メールは、デフォルトでは設定されたアンチスパム エンジンとアンチウイルス スキャン エンジンでスキャンされますが、プライベート リスナーで受信した電子メールはスキャンされません。リスナーがある同じ図を [図 5-3](#) に示します。

図 5-3 エンタープライズ ゲートウェイ用のパブリックおよびプライベート リスナー

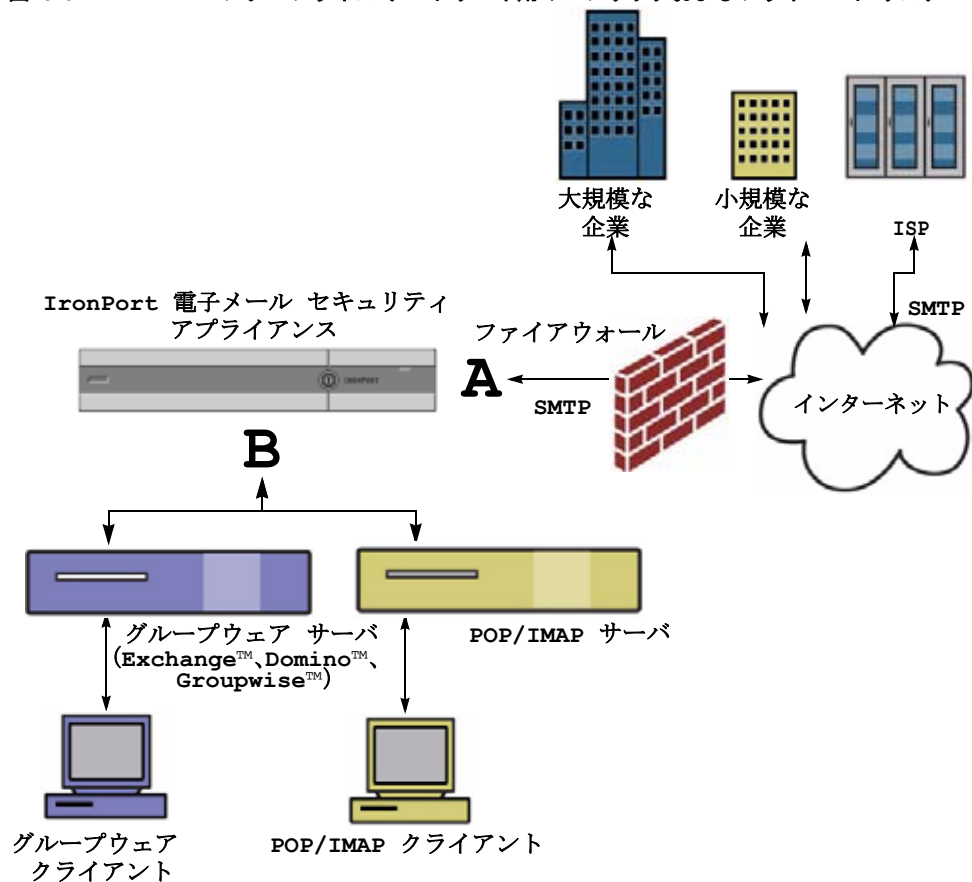


図 5-3 で、1つのパブリック リスナー (A) と 1つのプライベート リスナー (B) が、このエンタープライズ ゲートウェイ構成のアプライアンス上で構成されています。

さらに図 5-4 は、パブリック リスナーとプライベート リスナーのデフォルト設定の違いを示しています。パブリック リスナーは、インターネットからの電子メールを受信することを意図しています。パブリック リスナーは多数のホストからの接続を受信し、限られた数の受信者にメッセージを渡します。これとは逆に、プライベート リスナーは、内部ネットワークからの電子メールを受信することを意図しています。プライベート リスナーは限られた (既知の) 数のホストからの接続を受信し、メッセージを多数の受信者に渡します。

C10/100 カスタマー：System Setup Wizard では、デフォルトで、インターネットからの電子メールの受信と内部ネットワークからの電子メールの中継の両方を行うための、1 つのパブリック リスナーを順を追って設定します。つまり、1 つのリスナーが両方の機能を実行できます。

それぞれの種類のリスナーの、ホスト アクセス テーブルと受信者アクセス テーブルでの違いについては後述します。

図 5-4 パブリック リスナーとプライベート リスナー

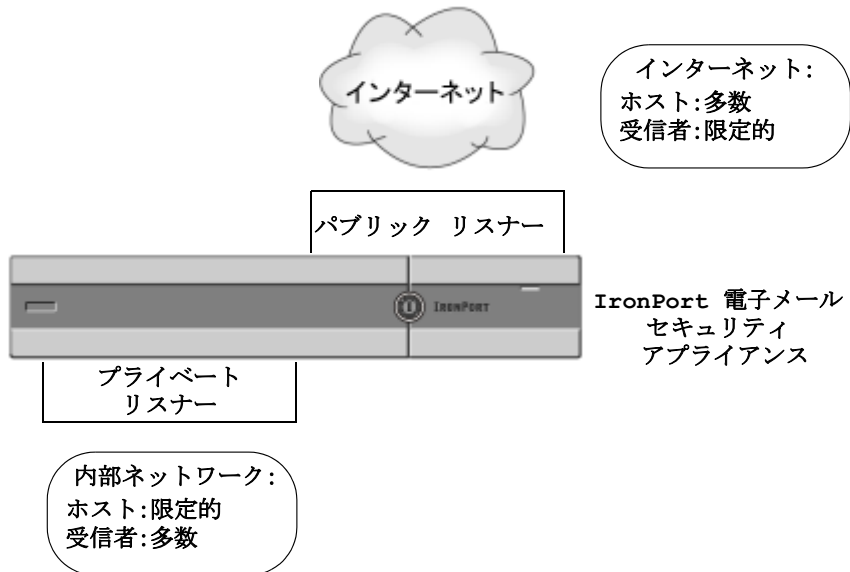
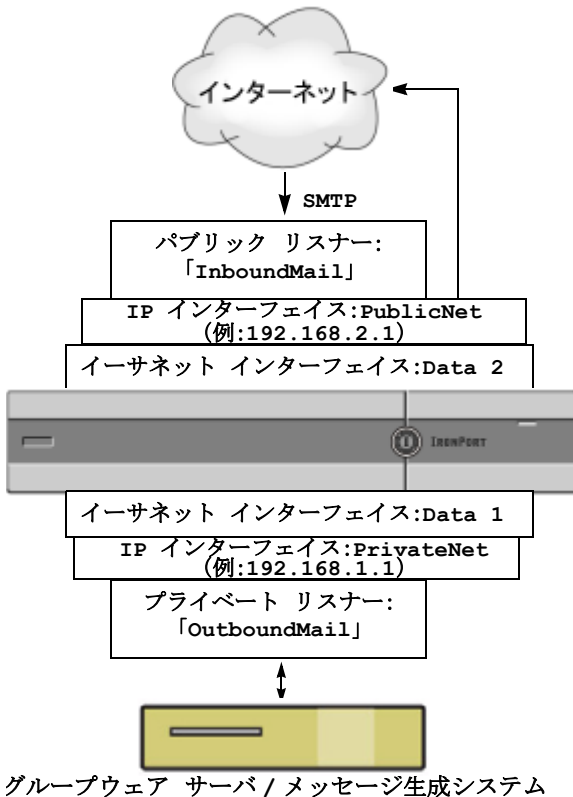


図 5-5 に、Cisco IronPort X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 アプライアンス上で System Setup Wizard (または CLI の `systemsetup` コマンド)によって作成される一般的な電子メールゲートウェイ構成を示します。2 つのリスナーが作成されます。あるインターフェイス上でインバウンド接続を使用可能にするためのパブリック リスナーと、別の IP インターフェイス上でアウトバウンド接続を使用可能にするためのプライベート リスナーです。

図 5-6 に、Cisco IronPort C150/160 アプライアンス上で System Setup Wizard (または CLI の `systemsetup` コマンド)によって作成される一般的な電子メールゲートウェイ構成を示します。1 つの IP インターフェイス上の 1 つのパブリック リスナーが、インバウンド接続とアウトバウンド接続の両方を使用可能にするために作成されます。

図 5-5 X1000/1050/1060/1070、C60/600/650/660/670、C30/300/350/360/370 アプライアンス上のパブリック リスナーとプライベート リスナー



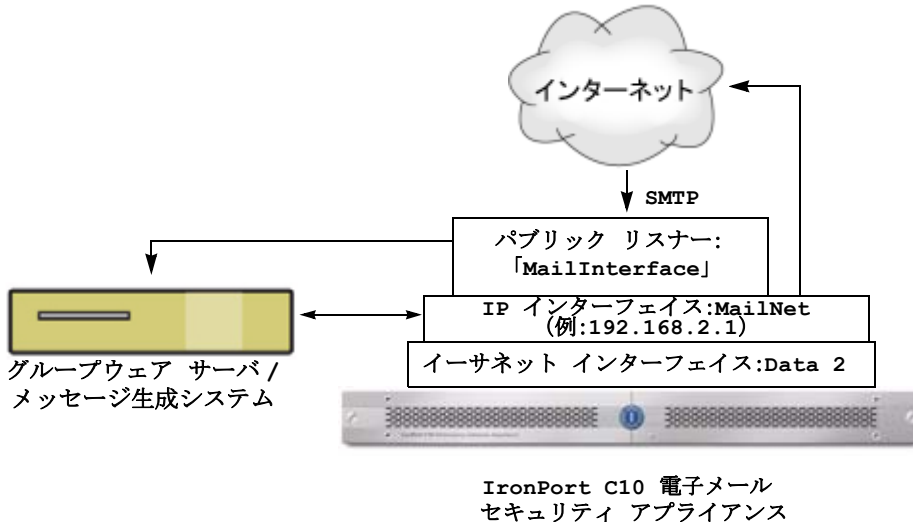
(注) このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信します。IP インターフェイス PublicNet は、インターネット上の宛先ホストにメッセージを送信します。

IronPort 電子メールセキュリティ アプライアンス

IP インターフェイス PrivateNet は、内部のメール ホストにメッセージを送信します。

(注) このプライベート リスナーは、Data1 イーサネット インターフェイス上の PrivateNet IP インターフェイスのポート 25 上で SMTP プロトコルを使用し、.example.com ドメイン内の内部システムからメッセージを受信します。

図 5-6 C10 アプライアンス上のパブリック リスナー



- (注) このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信し、.example.com ドメイン内の内部システムからのメッセージを中継します。IP インターフェイス MailNet は、インターネット上の宛先ホストと内部のメール ホストにメッセージを送信します。

ホスト アクセス テーブル (HAT) : 送信者グループとメール フロー ポリシー

アプライアンス上で設定されている各リスナーには、それが受信するメッセージの動作を変更するために設定可能なプロパティがあります。「概要：電子メールパイプライン」(P.4-1) で説明したように、リスナーの動作に影響を与える最初の構成可能な機能の 1 つがホスト アクセス テーブル (HAT) です。

HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。作成するすべてのリスナーに独自の HAT があります。HAT は、パブリック リスナーとプライベート リスナーの両方に対して定義されます。

HAT 内のエントリーは次の基本的な構文によって定義されます。

表 5-1 HAT の基本的な構文

リモート ホスト定義	ルール
------------	-----

*リモート ホスト定義*は、リスナーに定義しようとするリモート ホストを（たとえば単一の IP アドレスで）定義する方法です。

ルールは、指定したリモート ホストがリスナーに接続できるかどうかを指定します。

AsyncOS の HAT では、基本構文を拡張し、複数のリモート ホスト定義に名前を付けたものを作成できます。これを *送信者グループ*と呼びます。複数のアクセス ルールとパラメータ セットを組み合わせて名前を付けたものを、*メール フロー ポリシー*と呼びます。この拡張された構文を [表 5-2](#) に示します。

表 5-2 HAT の高度な構文

送信者グループ：	メール フロー ポリシー：
リモート ホスト	アクセス ルール + パラメータ
リモート ホスト	
リモート ホスト	
...	

ルールが HAT に現れる順序は重要です。リスナーに接続しようとする各ホストについて、HAT が上から下に向かって読み込まれます。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。

HAT に格納する定義済みエントリーとカスタム エントリーは、最後のホスト エントリーである「ALL」の上に入力します。

デフォルト HAT エントリー

作成するすべてのパブリック リスナーについて、デフォルトでは、すべてのホストからの電子メールを許可するように HAT が設定されます。作成するすべてのプライベート リスナーについて、デフォルトでは、指定したホストからの電子メールを中継し、その他すべてのホストを拒否するように HAT が設定されます。



(注) 指定したホスト以外のすべてのホストを拒否することで、`listenerconfig` コマンドと `systemsetup` コマンドでは、意図せずシステムを「オープンリレー」として設定することが防止されます。オープンリレー（「セキュアでないリレー」または「サードパーティ」リレーとも呼びます）は、第三者による電子メールメッセージのリレーを許す SMTP 電子メール サーバです。オープンリレーがあると、ローカル ユーザ向けでもローカル ユーザからでもない電子メールを処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパムを送信することが可能になります。

メール フロー ポリシー：アクセス ルールとパラメータ

HAT のメール フロー ポリシーを使用すると、リスナーがリモート ホストからメールを受信する速度を制御または制限できます。また、SMTP カンバセーションの間でやりとりされる SMTP コードと応答も変更できます。

HAT には、リモート ホストからの接続に作用する次の 4 つの基本的なアクセス ルールがあります。

ステップ 1 ACCEPT

接続が許可された後、電子メールの許可がさらに受信者アクセス テーブル（パブリック リスナーの場合）などのリスナーの設定によって制限されません。

ステップ 2 REJECT

接続は最初に許可されますが、接続しようとしているクライアントに 4XX または 5XX のグリーティングが送信されます。電子メールは許可されません。



(注) SMTP カンバセーションの開始時ではなく、メッセージ受信レベル (RCPT TO) でこの拒否を実行するように AsyncOS を設定することもできます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。この設定は、CLI の `listenerconfig --> setup` コマンドで設定します。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照してください。

ステップ 3 TCPREFUSE

接続は TCP レベルで拒否されます。

ステップ 4 RELAY

接続は受け付けられます。すべての受信者について受信が許可され、受信者アクセス テーブルで制約されません。

- CONTINUE

HAT 内のマッピングが無視され、HAT の処理が継続されます。着信接続が、CONTINUE でない後続のエントリに一致する場合、代わりにそのエントリが使用されます。CONTINUE ルールは、**Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス)** で HAT を容易に編集できるようにするために使用します。詳細については、「[新しい送信者グループの追加](#)」(P.5-43) を参照してください。

これらの基本的なアクセス コントロール パラメータに加え、作成するリスナーで次のパラメータを使用できます。アクセス ルール (ACCEPT または REJECT) と組み合わされたパラメータは、**メール フロー ポリシー**と呼ばれます。メール フロー ポリシーは、HAT パラメータのグループ (アクセス ルールの後に、接続パラメータ、レート制限パラメータ、カスタム SMTP コードと応答、およびアンチスパム、アンチウイルス、暗号化、認証パラメータを続けたもの) を表現するための 1 つの方法です。

その後メール フロー ポリシーは、リスナーの HAT 内のエントリとして送信者グループにマップされます。

表 5-3 HAT メール フロー ポリシー パラメータ

パラメータ	説明
Connections	
Maximum message size	このリスナーで許可されるメッセージの最大サイズ。最大メッセージ サイズの最小値は 1 KB です。
Maximum concurrent connections from a single IP	単一の IP アドレスからこのリスナーに接続することが許可される最大同時接続数。
Maximum messages per connection	リモート ホストからの接続に対して、このリスナーを通じて送信できる最大メッセージ数。
Maximum recipients per message	このホストからのメッセージに対して許可される最大受信者数。
SMTP Banner	

表 5-3 HAT メール フロー ポリシー パラメータ (続き)

パラメータ	説明
Custom SMTP Banner Code	このリスナーとの接続が確立されたときに返される SMTP コード。
Custom SMTP Banner Text	このリスナーとの接続が確立されたときに返される SMTP バナー テキスト。
Custom SMTP Reject Banner Code	このリスナーにより接続が拒否されたときに返される SMTP コード。
Custom SMTP Reject Banner Text	このリスナーにより接続が拒否されたときに返される SMTP バナー テキスト。
Override SMTP Banner Host Name	デフォルトでは、SMTP バナーをリモート ホストに表示するときに、リスナーのインターフェイスに関連付けられているホスト名が含まれます (たとえば、220- <i>hostname</i> ESMTP)。ここに異なるホスト名を入力することで、このバナーを変更できます。また、ホスト名フィールドを空白のままにすることで、ホスト名をバナーに表示しないこともできます。
Rate Limiting	
Rate Limiting: Maximum Recipients per Hour	このリスナーが 1 台のリモート ホストから受信する、時間あたりの最大受信者数。送信者 IP アドレスあたりの受信者の数は、グローバルに追跡されます。リスナーごとに独自のレート制限しきい値が追跡されますが、すべてのリスナーが 1 個のカウンタに対して検証を行うため、同じ IP アドレス (送信者) が複数のリスナーに接続している場合、レート制限を超える可能性が高くなります。
Rate Limiting: Max.recipient per Hour Exceeded Error Code	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP コード。
Rate Limiting: Max.Recipients Per Hour Exceeded Error Text	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP バナー テキスト。
Flow Control	

表 5-3 HAT メールフローポリシーパラメータ (続き)

パラメータ	説明
Use SenderBase for Flow Control	このリスナーの Cisco IronPort SenderBase 評価サービスへの「ルックアップ」をイネーブルにします。
Group by Similarity of IP Addresses: (有効ビット範囲 0 ~ 32)	リスナーのホストアクセステーブル (HAT) 内のエントリーを大規模な CIDR ブロックで管理しつつ、IP アドレスごとに着信メールを追跡およびレート制限するために使用します。レート制限のために類似の IP アドレスをグループ化するための有効ビットの範囲 (0 ~ 32) を定義しつつ、その範囲内の IP アドレスごとに個別のカウンタを保持します。「Use SenderBase」をディセーブルにする必要があります。HAT の有効ビットの詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Delivery Features」の章の「HAT Significant Bits Feature」を参照してください。
Directory Harvest Attack Prevention (DHAP)	
Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour	このリスナーが 1 台のリモートホストから受信する、時間あたりの最大の無効な受信者数。このしきい値は、RAT 拒否および SMTP call-ahead サーバ拒否の総数と、SMTP キャンペーンでドロップされたか、ワークキューでバウンスされた無効な LDAP 受信者へのメッセージの総数を合計したものを表します (関連付けられているリスナーの LDAP 許可設定で設定します)。LDAP 許可クエリーの DHAP の設定の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」を参照してください。
Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation	Cisco IronPort アプライアンスは、無効な受信者のしきい値に達するとホストへの接続をドロップします。
Max.Invalid Recipients Per Hour Code:	接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。

表 5-3 HAT メール フロー ポリシー パラメータ (続き)

パラメータ	説明
Max.Invalid Recipients Per Hour Text:	ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。
Drop Connection if DHAP threshold is reached within an SMTP Conversation	SMTP カンバセーション中に DHAP しきい値に達した場合の接続のドロップをイネーブルにします。
Max.Invalid Recipients Per Hour Code	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
Max.Invalid Recipients Per Hour Text:	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するテキストを指定します。
Spam Detection	
Anti-spam scanning	このリスナー上でアンチスパム スキャンをイネーブルにします。
Virus Detection	
Anti-virus scanning	このリスナー上でアンチウイルス スキャンをイネーブルにします。
Encryption and Authentication	
Allow TLS Connections	このリスナーの SMTP カンバセーションで、Transport Layer Security (TLS) を拒否、優先、または義務付けします。
SMTP Authentication	リスナーに接続するリモートホストからの SMTP 認証を許可、禁止、義務付けます。SMTP 認証については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「LDAP Queries」の章を参照してください。
If Both TLS and SMTP Authentication are enabled:	TLS に SMTP 認証を提供するよう義務付けます。
Domain Key Signing	

表 5-3 HAT メール フロー ポリシー パラメータ (続き)

パラメータ	説明
Domain Key/ DKIM Signing	このリスナーで DomainKeys または DKIM 署名をイネーブルにします (ACCEPT および RELAY のみ)。
DKIM Verification	DKIM 検証をイネーブルにします。
SPF/SIDF Verification	
Enable SPF/SIDF Verification	このリスナーで SPF/SIDF 署名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「Email Authentication」の章を参照してください。
Conformance Level	SPF/SIDF 準拠レベルを設定します。[SPF]、[SIDF]、[SIDF Compatible] のいずれかを選択します。詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Email Authentication」の章を参照してください。
Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:	準拠レベルとして [SIDF Compatible] を選択した場合、メッセージ中に Resent-Sender: ヘッダーまたは Resent-From: ヘッダーが存在する場合に、PRA Identity 検証の結果 Pass を None にダウングレードするかどうかを設定します。このオプションはセキュリティ目的で選択します。
HELO Test	HELO ID に対してテストを実行するかどうかを設定します ([SPF] および [SIDF Compatible] 準拠レベルで使用します)。
Untagged Bounces	
Consider Untagged Bounces to be Valid	バウンス検証タギング (『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Delivery Features」の章を参照) がイネーブルの場合にのみ適用されます。デフォルトでは、アプライアンスはタグのないバウンスを無効と見なし、バウンス検証の設定に応じて、バウンスを拒否するか、カスタム ヘッダーを追加します。タグ付きでないバウンスを有効と見なす場合、アプライアンスはバウンス メッセージを受け付けます。
Envelope Sender DNS Verification	
	「送信者検証」(P.5-56) を参照してください。

表 5-3 HAT メールフロー ポリシー パラメータ (続き)

パラメータ	説明
Exception Table	
Use Exception Table	送信者検証ドメイン例外テーブルを使用します。例外テーブルは 1 つしか使用できませんが、メールフローポリシーごとにイネーブルにできます。詳細については、「 送信者検証例外テーブル 」(P.5-60) を参照してください。

デフォルトでは、これらのパラメータは、アプライアンス上の各リスナーについて、[表 5-5](#) および [表 5-6](#) に示すデフォルト値に設定されます。



(注)

アンチスパムまたはアンチウイルス スキャンが HAT でグローバルにイネーブルになっている場合は、メッセージが Cisco IronPort アプライアンスによって許可されるときに、アンチスパムまたはアンチウイルス スキャン用にフラグ設定されます。メッセージを許可した後にアンチスパムまたはアンチウイルス スキャンがディセーブルにされた場合、メッセージは、ワーク キューを出るときに引き続きスキャン対象になります。

HAT 変数の構文

表 5-4 では、メール フロー ポリシーに対して定義されるカスタム SMTP およびレート制限バナーと組み合わせることでも使用できる変数のセットを定義します。変数名の大文字と小文字は区別されません（つまり、\$group と \$Group は同じです）。

表 5-4 HAT 変数の構文

変数	定義
\$Group	HAT 内の一致した送信者グループの名前で置き換えられます。送信者グループに名前がない場合、「None」が表示されます。
\$Hostname	Cisco IronPort アプライアンスによって検証された場合にのみ、リモート ホスト名で置き換えられます。IP アドレスの逆引き DNS ルックアップが成功したもののホスト名が返されない場合、「None」が表示されます。逆引き DNS ルックアップが失敗した場合（DNS サーバに到達できない場合や、DNS サーバが設定されていない場合）、「Unknown」が表示されます。
\$OrgID	SenderBase 組織 ID（整数値）で置き換えられます。 Cisco IronPort アプライアンスが SenderBase 組織 ID を取得できないか、SenderBase 評価サービスが値を返さなかった場合、「None」が表示されます。
\$RemoteIP	リモート クライアントの IP アドレスで置き換えられます。
\$HATEntry	リモート クライアントが一致した HAT のエントリで置き換えられます。

HAT 変数の使用



(注)

これらの変数は、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」の章の表 1-3 に示されている高度な HAT パラメータ smtp_banner_text および max_rcpts_per_hour_text とともに使用できます。

これらの変数を使用し、\$TRUSTED ポリシー内で許可された接続のカスタム SMTP バナー応答テキストを GUI で編集できます。

図 5-7 HAT 変数の使用

Rate Limiting:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text"/>
	Max. Recipients Per Hour Code:	<input type="text" value="452"/>
	Max. Recipients Per Hour Text:	<input type="text" value="Too many recipients received this hour from Host: \$hostname"/>

または、CLI で次のように入力します。

```
Would you like to specify a custom SMTP response? [Y]> y
```

```
Enter the SMTP code to use in the response. 220 is the standard code.
```

```
[220]> 200
```

```
Enter your custom SMTP response. Press Enter on a blank line to finish.
```

```
You've connected from the hostname: $Hostname, IP address of: $RemoteIP,
matched the group: $Group, $HATEntry and the SenderBase Organization:
$OrgID.
```

HAT 変数のテスト

これらの変数をテストするには、既知の信頼できるマシンの IP アドレスを、Cisco IronPort アプライアンス上のリスナーの \$WHITELIST 送信者グループに追加します。その後、そのマシンから telnet で接続します。SMTP 応答中で変数の置き換えを確認できます。次の例を参考にしてください。

```
# telnet IP_address_of_IronPort_Appliance
```

```
220 hostname ESMTP
```

```
200 You've connected from the hostname: hostname, IP address of:
IP-address_of_connecting_machine, matched the group: WHITELIST, 10.1.1.1
the SenderBase Organization: OrgID.
```

デフォルト メール フロー ポリシーの参照

図 5-8 に、パブリック リスナーのデフォルト ポリシー パラメータを示します。リスナーのデフォルト ポリシー パラメータを表示するには、次の手順を実行します。

ステップ 1 GUI にアクセスします（「[GUI へのアクセス](#)」(P.2-3) を参照）。

ステップ 2 [Mail Policies] > [Mail Flow Policies] の順にクリックします。

[Mail Flow Policies] ページが表示されます。リスナーが設定されている場合、アルファベット順で最初のリスナーに対して定義されているメール フロー ポリシーが表示されます。

図 5-8 [Mail Flow Policies] ページ
Mail Flow Policies

Policy Name	Behavior	Delete
THROTTLED	Accept	🗑️
ACCEPTED	Accept	🗑️
TRUSTED	Accept	🗑️
BLOCKED	Reject	🗑️
Default Policy Parameters		

ステップ 3 [Default Policy Parameters] リンクをクリックします。

[Default Policy Parameters] ページが表示されます。図 5-9 を参照してください。

図 5-9 パブリック リスナーのデフォルトポリシー パラメータ (1/2)

Default settings		
Connections:	Max. Messages Per Connection:	<input type="text" value="10"/>
	Max. Recipients Per Message:	<input type="text" value="50"/>
	Max. Message Size:	<input type="text" value="20971520"/> <small>(add a trailing K for kilobytes; M for megabytes)</small>
	Max. Concurrent Connections From a Single IP:	<input type="text" value="10"/>
SMTP:	Custom SMTP Banner Code:	<input type="text" value="220"/>
	Custom SMTP Banner Text:	<input type="text"/>
	Custom SMTP Reject Banner Code:	<input type="text" value="554"/>
	Custom SMTP Reject Banner Text:	<input type="text"/>
	Override SMTP Banner Hostname:	<input checked="" type="radio"/> Use Hostname from Interface <input type="radio"/> <input type="text"/>
Mail Flow Limits		
Rate Limiting:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Unlimited <input type="text"/>
	Max. Recipients Per Hour Code:	<input type="text" value="452"/>
	Max. Recipients Per Hour Text:	<input type="text" value="Too many recipients received this hour"/>
Flow Control:	Use SenderBase for Flow Control:	<input checked="" type="radio"/> On <input type="radio"/> Off
	Group by Similarity of IP Addresses:	<i>This feature can only be used if Senderbase Flow Control is off.</i> <input checked="" type="radio"/> Off <input type="radio"/> <input type="text"/> <small>(significant bits 0-32)</small>
Directory Harvest Attack Prevention (DHAP):	Max. Invalid Recipients Per Hour:	<input checked="" type="radio"/> Unlimited <input type="text"/>
	Drop Connection if DHAP threshold is Reached within an SMTP Conversation:	<input checked="" type="radio"/> On <input type="radio"/> Off
	Max. Invalid Recipients Per Hour Code:	<input type="text" value="550"/>
	Max. Invalid Recipients Per Hour Text:	<input type="text" value="Too many invalid recip"/>

図 5-10 パブリック リスナーのデフォルトポリシー パラメータ (2/2)

Security Features	
Spam Detection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Virus Protection:	<input checked="" type="radio"/> On <input type="radio"/> Off
Encryption and Authentication:	TLS: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	SMTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication
Domain Key/DKIM Signing:	<input type="radio"/> On <input checked="" type="radio"/> Off
DKIM Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
SPF/SIDF Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
	Conformance Level: <input type="text" value="SIDF Compatible: on"/>
	Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used: <input type="radio"/> No <input type="radio"/> Yes
	HELO Test: <input type="radio"/> Off <input checked="" type="radio"/> On
Evaluate Untagged Bounces:	<input type="radio"/> Yes <input checked="" type="radio"/> No <small>(Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.)</small>
Sender Verification	
Envelope Sender DNS Verification:	<input type="radio"/> On <input checked="" type="radio"/> Off
Malformed Envelope Senders:	SMTP Code: <input type="text" value="553"/> SMTP Text: <input type="text" value="553.4 Domain required for sender address"/>
Envelope Senders whose domain does not resolve:	SMTP Code: <input type="text" value="451"/> SMTP Text: <input type="text" value="451.8 Domain of sender address <\${Envel}"/>
Envelope Senders whose domain does not exist:	SMTP Code: <input type="text" value="553"/> SMTP Text: <input type="text" value="553.8 Domain of sender address <\${Envel}"/>
Use Sender Verification Exception Table:	<input type="radio"/> On <input checked="" type="radio"/> Off

リスナーのデフォルト ポリシー パラメータ

次の表に、パブリック リスナーのデフォルト パラメータの一覧を示します。

表 5-5 パブリック リスナーの HAT デフォルトポリシー パラメータ

パラメータ	デフォルト値
Maximum message size:	20 MB
Max.concurrent connections allowed to this listener:	10 接続
Maximum messages per connection:	10 メッセージ
Maximum recipients per message:	50 受信者
SMTP Banner Code:	220
SMTP Banner Text:	「hostname_ESMTP」
SMTP Reject Banner Code:	554

表 5-5 パブリック リスナーの HAT デフォルト ポリシー パラメータ (続き)

パラメータ	デフォルト値
SMTP Reject Banner Text:	「Access Denied」
Override SMTP Banner Hostname	インターフェイスからのホスト名を使用
Rate Limiting: Maximum Recipients per Hour:	デフォルトなし。 ユーザ定義。
Rate Limiting: Limit Exceeded Error Code:	452
Rate Limiting: Limit Exceeded Error Text:	「Too many recipients received this hour」
Directory Harvest Attack Prevention	OFF
Use SenderBase:	ON
Group by Similarity of IP address:	OFF
Use anti-spam scanning:	ON (アンチスパムがイネーブルな場合)
Use anti-virus scanning:	ON (アンチウイルスがイネーブルな場合)
Allow TLS Connections:	NO
Override Hostname	NO
SMTP Auth	OFF
Domainkey/DKIM Signing	OFF
DKIM Verification	OFF
SPF/SIDF Verification	OFF
Envelope Sender DNS Verification	OFF
Use Exception Table	OFF

次の表に、プライベート リスナーのデフォルト パラメータの一覧を示します。

表 5-6 プライベート リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
Maximum messages per connection:	10,000 メッセージ
Maximum recipients per message:	100,000 受信者
Maximum message size:	100 MB (104857600 バイト)
Max.concurrent connections from a single IP	50 接続
SMTP Banner Code:	220
SMTP Banner Text:	「 <i>hostname</i> ESMTP」
SMTP Reject Banner Code:	554
SMTP Reject Banner Text:	「Access Denied」
Override SMTP Banner Hostname	インターフェイスからのホスト名を使用
Rate Limiting: Maximum Recipients per Hour:	Unlimited
Rate Limiting: Limit Exceeded Error Code:	N/A
Rate Limiting: Limit Exceeded Error Text:	N/A
Use SenderBase:	OFF
Group by Similarity of IP address:	OFF
Directory Harvest Attack Prevention	OFF
Use anti-spam scanning:	OFF (アンチスパムがイネーブルな場合)
Use anti-virus scanning:	ON (アンチウイルスがイネーブルな場合)
Allow TLS Connections:	NO
Override Hostname	NO
SMTP Auth	OFF

表 5-6 プライベート リスナーの HAT デフォルト ポリシー パラメータ (続き)

パラメータ	デフォルト値
Domainkeys/DKIM Signing	OFF
DKIM Verification	OFF
SPF/SIDF Verification	OFF
Accept Untagged Bounces	NO
Envelope Sender DNS Verification	OFF
Use Exception Table	OFF

送信者グループ

HAT パラメータをアクセスルールと組み合わせることで、メールフローポリシーが作成されます (図 5-6 「メールフローポリシー: アクセスルールとパラメータ」 (P.5-11) を参照)。異なる HAT パラメータをグループ化して名前を割り当てると、送信者のグループに適用できるメールフローポリシーが定義されます。

送信者グループは、単に、複数の送信者からの電子メールを同じ方法で扱う (つまり、送信者のグループにメールフローポリシーを適用する) ために集められた送信者のリストです。送信者グループは、次のもので識別される送信者のリストです。

- IP アドレス
- IP 範囲
- 具体的なホスト名またはドメイン名
- SenderBase 評価サービスの「組織」分類
- SenderBase Reputation Score (SBRIS; SenderBase 評価スコア) の範囲 (またはスコアの欠如)
- DNS リストクエリー応答

送信者グループを構成するリモートホスト (送信者エントリ) を定義するための構文については、表 5-7 を参照してください。これらの送信者エントリは、リスナーの HAT 内でカンマで区切られます。メールフローポリシーと同様に、送信者グループに名前を割り当てます。

送信者グループおよびメール フロー ポリシーは合わせて、リスナーの HAT で定義されます。Cisco IronPort アプライアンスでは、デフォルトで、「パブリックリスナー向けの定義済みのメール フロー ポリシー」(P.5-33) に示すメール フロー ポリシーと送信者グループがあらかじめ定義されています。

第 6 章「電子メール セキュリティ マネージャ」では、定義済みの送信者グループとメール フロー ポリシーを使用して、ゲートウェイを通過するメールをすばやく高性能に分類し、リスナーの HAT に対するリアルタイムな変更を行うことができます。



(注)

二重 DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS (A) ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しない場合、または A レコードが存在しない場合は、システムは IP アドレスのみを使用して HAT 内のエントリと照合します。

送信者グループの構文

表 5-7 HAT 内でのリモートホストの定義：送信者グループの構文

構文	意味
n.n.n.n	フル（完全な）IP アドレス
n.n.n. n.n.n n.n. n.n n. n	部分的な IP アドレス
n.n.n.n-n n.n.n-n. n.n.n-n n.n-n. n.n-n n-n. n-n	IP アドレスの範囲
yourhost.example.com	完全修飾ドメイン名
.partialhost	部分ホスト ドメイン内のすべてのもの
n/c n.n/c n.n.n/c n.n.n.n/c	CIDR アドレス ブロック
SBRs [n:n] SBRs [none]	SenderBase 評価スコア。詳細については、「 SenderBase 評価スコアによって定義された送信者グループ 」（P.5-31）を参照してください。
SBO:n	SenderBase ネットワーク オーナー識別番号。詳細については、「 SenderBase 評価スコアによって定義された送信者グループ 」（P.5-31）を参照してください。

表 5-7 HAT 内でのリモートホストの定義：送信者グループの構文（続き）

構文	意味
dnslist[dnsserver.domain]	DNS リスト クエリー。詳細については、「HAT 内の DNS リストにクエリーを実行することで定義された送信者グループ」（P.5-32）を参照してください。
ALL	すべてのアドレスに一致する特殊なキーワード。これは、すべての送信者グループのみに適用され、常に含まれます（ただしリストされません）。

ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ

SMTP プロトコルには電子メールの送信者を認証するための方法が組み込まれていないため、大量の迷惑メールの送信者は、その身元を隠すためのいくつかの戦略を採用することに成功してきました。たとえば、メッセージのエンベロープ送信者アドレスのスプーフィング、偽造した HELO アドレスの使用、単なる異なるドメイン名のローテーションなどがあります。これにより、多数のメール管理者は、「この大量の電子メールは誰が送信しているのか」という基本的な質問を自問することになります。この質問に答えるために、SenderBase 評価サービスは、接続元ホストの IP アドレスに基づいて身元ベースの情報を集約するための固有の階層を開発してきました。IP アドレスは、メッセージ中で偽造することがほとんど不可能な情報の 1 つです。

IP Address は、送信元メールホストの IP アドレスとして定義します。

Domain は、指定した第 2 レベルドメイン名（たとえば yahoo.com）を持つホスト名を使用するエンティティとして定義され、IP アドレスに対する逆引き（PTR）ルックアップによって決定されます。

Network Owner は、IP アドレスのブロックを管理するエンティティ（通常は会社）として定義され、American Registry for Internet Numbers（ARIN）などのグローバルレジストリやその他のソースからの IP アドレス空間の割り当てに基づいて決定されます。

Organization は、ネットワークオーナーの IP ブロック内のメールゲートウェイの特定のグループを最も詳細に管理するエンティティとして定義され、SenderBase によって決定されます。Organization は Network Owner、Network Owner 内の部門、その Network Owner の顧客のいずれかになります。

HAT に基づくポリシーの設定

表 5-8 に、ネットワーク オーナーと組織の例をいくつか示します。

表 5-8 ネットワーク オーナーと組織の例

例の種類	ネットワーク オーナー	組織
ネットワーク サービス プロバイダー	Level 3 Communications	Macromedia Inc. AllOutDeals.com GreatOffers.com
電子メール サービス プロバイダー	GE	GE Appliances GE Capital GE Mortgage
商用送信者	The Motley Fool	The Motley Fool

ネットワーク オーナーの規模にはかなりの幅があるため、メール フロー ポリシーの基にする適切なエンティティは組織です。SenderBase 評価サービスは、電子メールの送信元について組織レベルまで独自に理解しており、Cisco IronPort アプライアンスはそれを利用して、組織に基づいてポリシーを自動的に適用します。上の例で、ユーザがホスト アクセス テーブル (HAT) で「Level 3 Communications」を送信者グループとして指定した場合、SenderBase はそのネットワーク オーナーによって管理される個別の組織に基づいてポリシーを適用します。

たとえば、上記の表 5-8 で、ユーザが Level 3 に対して時間あたりの受信者数の制限を 10 と入力した場合、Cisco IronPort アプライアンスは、Macromedia Inc.、Alloutdeals.com、およびGreatoffers.com に対して最大 10 個の受信者を許可します (Level 3 ネットワーク オーナーに対しては時間あたり合計 30 個の受信者になります)。このアプローチの利点は、これらの組織のいずれかがスパムを送信し始めても、Level 3 によって管理されているその他の組織には影響がないことです。これを、ネットワーク オーナー「The Motley Fool」の例と対比します。ユーザがレート制限を時間あたり 10 個の受信者に設定した場合、ネットワーク オーナー Motley Fool の合計の制限は、時間あたり 10 個の受信者になります。

Cisco IronPort メール フロー モニタ機能は、送信者を定義する方法の 1 つであり、送信者に関するメール フロー ポリシーの決定を作成するためのモニタリング ツールとなります。特定の送信者に関するメール フロー ポリシーの決定を作成するには、次のことを質問します。

ステップ 1 この送信者によって、どの IP アドレスが制御されているか。

インバウンド電子メールの処理を制御するためのメールフロー モニタ機能が使用する最初の情報が、この質問に対する答えになります。この答えは、SenderBase 評価サービスにクエリーを実行することで得られます。SenderBase 評価サービスは、送信者の相対的な規模に関する情報を提供します (SenderBase ネットワーク オーナーまたは SenderBase 組織)。この質問に答えるにあたり、次のことが仮定されます。

- 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。

ステップ 2 その規模に応じて、この送信者に接続数を全体でいくつ割り当てるべきか。

- 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。そのため、アプライアンスへの接続をより多く割り当てる必要があります。
- 多くの場合、大量の電子メールの送信元は、ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業、迷惑メールの送信元です。ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業は、多数の IP アドレスを管理する組織の例であり、アプライアンスへの接続をより多く割り当てる必要があります。通常、迷惑メールの送信者は、多数の IP アドレスを管理せず、少数の IP アドレスを通じて大量のメールを送信します。このような送信者には、アプライアンスへの接続をより少なく割り当てる必要があります。

メールフロー モニタ機能は、SenderBase ネットワーク オーナーと SenderBase 組織の差別化を使用して、SenderBase 内のロジックに基づき、送信者あたりに接続を割り当てる方法を決定します。メールフロー モニタ機能の使用の詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Using Email Security Monitor」の章を参照してください。

SenderBase 評価スコアによって定義された送信者グループ

Cisco IronPort アプライアンスは、Cisco IronPort SenderBase 評価サービスに対してクエリーを実行して、送信者の評価スコア (SBRS) を決定できます。

SBRS は、SenderBase 評価サービスからの情報に基づき、IP アドレス、ドメイン、または組織に割り当てられた数値です。スコアの範囲は、表 5-9 に示すよう

表 5-9 SenderBase 評価スコアの定義

スコア	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い
なし	この送信者のデータがない (一般にスパムの送信元)

に、-10.0 ~ +10.0 です。

SBRS を使用して、信頼性に基づいてメール フロー ポリシーを送信者に適用するように Cisco IronPort アプライアンスを設定します。たとえば、スコアが -7.5 未満のすべての送信者を拒否することが考えられます。これは、GUI を使用して実現するのが最も簡単です。「[SenderBase 評価スコアを使用した送信者グループの作成](#)」(P.5-49) を参照してください。エクスポートした HAT をテキストファイルで編集する場合、SenderBase 評価スコアを含めるための構文については表 5-10 を参照してください。『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Customizing Listeners」を参照してください。

表 5-10 HAT 内の SenderBase 評価スコアの構文

SBRS [n:n]	SenderBase 評価スコア。送信者は、SenderBase 評価サービスにクエリーを実行することで識別され、スコアは範囲内で定義されます。
SBRS[none]	SBRS がないことを指定します (非常に新しいドメインには、まだ SenderBase 評価スコアがない場合があります)。



(注)

GUI を通じて HAT に追加されるネットワーク オーナーは、SBO:n という構文を使用します。ここで n は、SenderBase 評価サービス内のネットワーク オーナーの一意的識別番号です。

SenderBase 評価サービスにクエリーを実行するようにリスナーを設定するには、[Network] > [Listeners] ページを使用するか、CLI で `listenerconfig -> setup` コマンドを使用します。また、アプライアンスが SenderBase 評価サービスにクエリーを実行するときに待つタイムアウト値を定義することもできます。その後、GUI の [Mail Policies] ページの値を使用するか、CLI の `listenerconfig -> edit -> hostaccess` コマンドを使用して、SenderBase 評価サービスに対するルックアップを使用するさまざまなポリシーを設定できます。



(注) また、SenderBase 評価スコアの「しきい値」を指定するメッセージフィルタを作成し、システムによって処理されたメッセージをさらに操作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「SenderBase Reputation Rule」、「Bypass Anti-Spam System Action」、および「Bypass Anti-Virus System Action」を参照してください。

HAT 内の DNS リストにクエリーを実行することで定義された送信者グループ

リスナーの HAT では、特定の DNS リスト サーバに対するクエリーに一致するものとして送信者グループを定義することもできます。クエリーは、リモートクライアントの接続時に DNS を通じて実行されます。リモート リストにクエリーを実行する機能は、現在メッセージフィルタ ルールとしても存在しますが (『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「DNS List Rule」を参照)、メッセージの内容全体が受信されるのは一度だけです。

このメカニズムにより、グループ内で、DNS リストにクエリーを実行する送信者を設定し、それに応じてメール フロー ポリシーを調整できます。たとえば、接続を拒否したり、接続元ドメインの振る舞いを制限したりできます。



(注) いくつかの DNS リストは、可変の応答 (たとえば「127.0.0.1」、「127.0.0.2」、「127.0.0.3」) を使用して、クエリー対象の IP アドレスに関するさまざまな事実を示すことができます。メッセージフィルタ DNS リスト ルール (『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「DNS List Rule」を参照) を使用すると、クエリーの結果をさまざまな値と比較できます。しかし、HAT 内で DNS リスト サーバにクエリーを実行する指定では、簡潔にするためにブール演算のみがサポートされています (つまり、IP アドレスがリストに現れるかどうか)。



(注)

CLI のクエリーでは必ず角カッコを含めます。GUI で DNS リストクエリーを指定する場合には角カッコは不要です。クエリーのテスト、DNS クエリーの一般的な設定、または現在の DNS リスト キャッシュのフラッシュを行うには、CLI で `dnslistconfig` コマンドを使用します。

このメカニズムは、「異常な」接続に加えて、「正常な」接続を識別するためにも使用できます。たとえば、query.bondedsender.org に対してクエリーを実行すると、その電子メール キャンペーンの健全性を保証するために Cisco IronPort Systems の Bonded Sender™ プログラムに供託金を積んだ接続元ホストが照合されます。デフォルトの WHITELIST の送信者グループを修正して Bonded Sender プログラムの DNS サーバにクエリーを実行し（積極的に供託金を拠出したこれら正規の電子メール送信者が一覧表示されます）、それに応じてメールフロー ポリシーを調整することもできます。

パブリック リスナー向けの定義済みのメール フロー ポリシー

アクセス ルール (ACCEPT または REJECT) と組み合わせる場合、[表 5-3 \(P.5-12\)](#) に示すパラメータが、作成する各パブリック リスナーの次の 4 つのメール フロー ポリシーとして事前に定義されています。

- \$ACCEPTED
- \$BLOCKED
- \$THROTTLED
- \$TRUSTED

リスナーの定義済みのメール フロー ポリシーにアクセスするには、次の手順を実行します。

ステップ 1 GUI にアクセスします（「[GUI へのアクセス](#)」(P.2-3) を参照）。

ステップ 2 [Mail Policies] > [HAT Overview] の順にクリックします。

[Overview] ページが表示されます。リスナーが設定されている場合、アルファベット順で最初のリスナーに対して定義されている [Host Access Table overview] ページが表示されます。[Listener] リストから目的のリスナーを選択します。

図 5-11 パブリック リスナー向けの定義済みのメール フロー ポリシー

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	WHITELIST	10	TRUSTED	🗑️
2	BLACKLIST	-10	BLOCKED	🗑️
3	SUSPECTLIST	-5	THROTTLED	🗑️
4	UNKNOWNLIST	0	ACCEPTED	🗑️
	ALL		ACCEPTED	

ステップ 3 メール フロー ポリシーの名前をクリックして、そのポリシーの接続動作とパラメータを表示します。



(注) デフォルトでは、C10/100 のユーザは、systemsetup コマンドの実行中に 1 つのパブリック リスナーのみを作成するように求められます。Cisco IronPortC10/100 アプライアンスで作成されたパブリック リスナーにも、内部システム用にメールを中継するために使用される \$RELAYED メール フロー ポリシーが含まれています (図 5-12 を参照)。詳細については、「RELAYLIST」(P.5-42) を参照してください。\$RELAYLIST ポリシーは、Cisco IronPort X1000/1050/1060/1070、C60/600/650/660/670、および C30/300/350/360/370 アプライアンス上のプライベート リスナーでのみ表示されます。

図 5-12 単一リスナー向けの定義済みのメール フロー ポリシー

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	🗑️
2	WHITELIST		TRUSTED	🗑️
3	BLACKLIST		BLOCKED	🗑️
4	SUSPECTLIST		THROTTLED	🗑️
5	UNKNOWNLIST		ACCEPTED	🗑️
	ALL		ACCEPTED	

この表で、「デフォルト」は、リスナーで定義されているデフォルト値が使用されることを意味します。

表 5-11 パブリック リスナー向けの定義済みのメール フロー ポリシー

ポリシー名	主要な動作 (アクセスルール)	パラメータ	値
\$ACCEPTED (All で使用)	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Default Default Default Default Default Default Default Default Default No default Default Default ON

注：\$ACCEPTED ポリシーのすべてのパラメータは、CLI の systemsetup および listenerconfig コマンドでユーザが定義します。次の質問が表示されたら「y」を選択します。

Would you like to change the default host access policy?
これによりこれらの値を変更します。GUI を使用してこれらの値を変更するには、図 5-7 「デフォルト メール フロー ポリシーの参照」 (P.5-20) の手順に従います。

表 5-11 パブリック リスナー向けの定義済みのメール フロー ポリシー (続き)

ポリシー名	主要な動作 (アクセス ルール)	パラメータ	値
\$BLOCKED	REJECT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	N/A N/A N/A N/A Default Default Default N/A N/A N/A N/A N/A N/A

表 5-11 パブリック リスナー向けの定義済みのメール フロー ポリシー (続き)

ポリシー名	主要な動作 (アクセスルール)	パラメータ	値
\$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase: Envelope Sender DNS Ver:	1 25 10MB 1 Default Default Default Default Default* 20 Default Default ON ON
\$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	5,000 5,000 100 MB 600 Default Default Default Default OFF* -1(Disable) N/A N/A OFF

* イネーブルな場合

\$ACCEPTED は名前付きポリシーであり、パブリック リスナーのデフォルトの HAT 設定と同じです。\$ACCEPTED ポリシーは作成するどの送信者グループにも割り当てることができます (「新しい送信者グループの追加」(P.5-43) および「Connections」(P.5-12) を参照してください。また、「HAT の操作」(P.5-55) も参照してください)。

パブリック リスナー用の HAT 内の最後の ALL エントリも、主な動作として \$ACCEPTED ポリシーを使用します。

各パブリック リスナーには、表 5-12 に示す送信者グループと対応するメール フロー ポリシーがデフォルトで定義されています。

表 5-12 **パブリック リスナー用の定義済みの送信者グループとメール フロー ポリシー**

送信者グループ	使用するメール フロー ポリシー
WHITELIST	\$TRUSTED
BLACKLIST	\$BLOCKED
SUSPECTLIST	\$THROTTLED
UNKNOWNLIST	\$ACCEPTED

これら 4 つの基本的な送信者グループとメール フロー ポリシーを使用することで、パブリック リスナー上でゲートウェイに流れ込む電子メールの分類を開始するためのフレームワークが得られます。『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Using Email Security Monitor」では、ゲートウェイに流れ込む電子メールのリアルタイム フローを確認し、リスナーの HAT をリアルタイムで変更できます (IP アドレス、ドメイン、または組織の既存の送信者グループへの追加、既存のポリシーまたは定義済みのポリシーの編集、新しいメール フロー ポリシーの作成) を行うことができます。

WHITELIST

信頼する送信者を WHITELIST の送信者グループに追加します。メール フロー ポリシー \$TRUSTED は、信頼できる送信者からの電子メールのレート制限をイネーブルにせず、それらの送信者からの内容をアンチスパムまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。

BLACKLIST

BLACKLIST 送信者グループ内の送信者は拒否されます (メール フロー ポリシー \$BLOCKED で設定されたパラメータにより)。このグループに送信者を追加すると、SMTP HELO コマンドで 5XX SMTP 応答が返され、それらのホストからの接続が拒否されます。

SUSPECTLIST

送信者グループ SUSPECTLIST には、着信メールの速度をスロットリングする（低下させる）メールフローポリシーが含まれています。送信者が疑わしい場合、送信者グループ SUSPECTLIST に追加することで、メールフローポリシーにより次のことが指示されます。

- レート制限により、セッションあたりの最大メッセージ数、メッセージあたりの最大受信者数、最大メッセージサイズ、リモートホストから受け付ける最大同時接続数が制限されます。
- リモートホストからの時間あたりの最大受信者数は 20 に設定されます。この設定は、使用可能な最大のスロットリングであることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。
- メッセージの内容はアンチスパムスキャンエンジンとアンチウイルススキャンエンジンによってスキャンされます（これらの機能がシステムでイネーブルになっている場合）。
- 送信者に関する詳細情報を得るために、Cisco IronPort SenderBase 評価サービスに対してクエリーが実行されます。

UNKNOWNLIST

送信者グループ UNKNOWNLIST は、特定の送信者に対して使用するメールフローポリシーが決まっていない場合に便利です。このグループのメールフローポリシーでは、このグループの送信者についてメールが許可されますが、IronPort Anti-Spam ソフトウェア（システムでイネーブルになっている場合）、アンチウイルススキャンエンジン、および Cisco IronPort SenderBase 評価サービスをすべて使用して、送信者とメッセージの内容に関する詳細情報を取得することが指示されます。このグループに属する送信者に対するレート制限もデフォルト値を使用してイネーブルになります。ウイルススキャンエンジンの詳細については、「[アンチウイルススキャン](#)」(P.9-2) を参照してください。SenderBase 評価サービスの詳細については、「[評価フィルタリング](#)」(P.7-2) を参照してください。

プライベート リスナー用の定義済みのメール フロー ポリシー

表 5-3 に定義されているパラメータを、アクセスルール (RELAY または REJECT) と組み合わせた場合、作成する各プライベートリスナーの次の 2 つのメール フロー ポリシーとして事前に定義されます。

- \$RELAYED
- \$BLOCKED

これらのポリシーの要約を表 5-12 に示します。

図 5-13 プライベート リスナー用の定義済みのメール フロー ポリシー

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	
	ALL		BLOCKED	

表 5-13 プライベート リスナー用の定義済みのメール フロー ポリシー

ポリシー名	主要な動作 (アクセス ルール)	パラメータ	値
\$RELAYED	RELAY	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use Sophos virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Default Default Default Default Default Default Default Default Off (if enabled) -1 (Disabled) Not applicable Not applicable Default
\$BLOCKED (All で使用)	REJECT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use Sophos virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Not applicable Not applicable Not applicable Not applicable Default Default Default Not applicable Not applicable Not applicable Not applicable Not applicable Not applicable

\$BLOCKED は名前付きポリシーであり、プライベートリスナーのデフォルトの HAT 設定と同じです。プライベートリスナー用の HAT 内の最後の ALL エントリも、デフォルトの動作として \$BLOCKED ポリシーを使用します。

各プライベート リスナーには、表 5-14 に示す送信者グループと対応するメール フロー ポリシーがデフォルトで定義されています。

表 5-14 **プライベート リスナー用の定義済みの送信者グループとメール フロー ポリシー**

送信者グループ	使用するメール フロー ポリシー
RELAYLIST	\$RELAYED
ALL	\$BLOCKED

この基本的な送信者グループとメール フロー ポリシーを使用することで、プライベート リスナー上でゲートウェイから出て行く電子メールの分類を開始するためのフレームワークが得られます。

RELAYLIST

中継を許可する必要があることがわかっている送信者を RELAYLIST 送信者グループに追加します。メール フロー ポリシー \$RELAYED は、中継を許可する送信者からの電子メールのレート制限を行わず、それらの送信者からの内容をアンチスパム スキャン エンジンまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。



(注) GUI の System Setup Wizard (または CLI の `systemsetup` コマンド) でアウトバウンド (プライベート) リスナーを作成するときに、Cisco IronPort アプライアンスを通じた電子メールの中継を許可したシステムは、送信者グループ RELAYLIST に自動的に追加されます。「手順 3 : Network」(P.3-26) を参照してください。



(注) デフォルトでは、C10/100 のユーザは、`systemsetup` コマンドの実行中に 1 つのパブリック リスナーのみを作成するように求められます。Cisco IronPort C10/100 アプライアンス上で作成されたパブリック リスナーにも、内部システム用にメールを中継するために使用される \$RELAYED メール フロー ポリシーが含まれます。

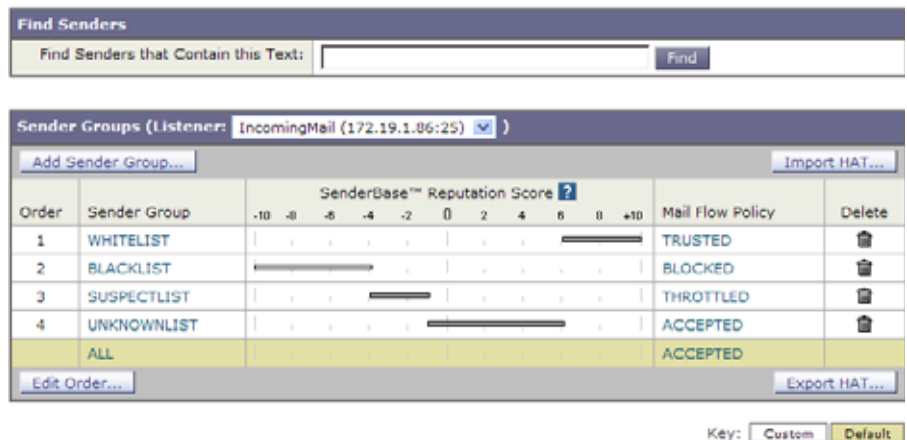
GUI による送信者グループとメール フロー ポリシーの管理

[Mail Policies] > [HAT Overview] ページと [Mail Flow Policy] ページでは、リスナーの HAT 設定を行うことができます。これらのページでは、次のことが可能です。

- 送信者グループからメール フロー ポリシーへのマッピングの参照
- 送信者グループの作成、編集、削除
- メール フロー ポリシーの作成、編集、削除
- リスナーの HAT エントリの順序変更

[Mail Policies] > [HAT Overview] リンクをクリックします。図 5-14 を参照してください。[Listener:] ドロップダウン リストから設定するリスナーを選択します。

図 5-14 [Host Access Table Overview] ページ
HAT Overview



[HAT Overview] ページでは、送信者グループの追加やリスナーのメール フロー ポリシーの編集を行うことができます。

新しい送信者グループの追加

新規送信者グループを追加するには、次の手順を実行します。

ステップ 1 [HAT Overview] ページで、[Add Sender Group] をクリックします。

図 5-15 [Add Sender Group] ページ
Add Sender Group

Sender Group Settings	
Name:	<input type="text"/>
Order:	5 <input type="button" value="v"/>
Comment:	<input type="text"/>
Policy:	select a policy... <input type="button" value="v"/>
SBRS (Optional):	<input type="checkbox"/> to <input type="text"/> <input type="checkbox"/> Include SBRS Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional): ?	<input type="text"/>
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in the DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)

- ステップ 2** 各フィールドに、送信者グループの名前を入力し、送信者グループのリストに配置する順序を選択し、コメントを入力します (任意)。
- ステップ 3** このグループに適用すべきメールフローポリシーがわからない場合 (またはまだメールフローポリシーが存在しない場合) は、デフォルトの「CONTINUE (no policy)」メールフローポリシーを使用します。そうでない場合は、ドロップダウンリストからメールフローポリシーを選択します。
- ステップ 4** SBRS の範囲と DNS リストを選択します (任意)。また、SBRS に情報が無い送信者を含めるためのチェックボックスをオンにすることもできます。これは「none」と呼ばれ、一般に疑いがあることを意味します。
- ステップ 5** ホストの DNS 検証の設定を行います (「[送信者検証の実装 — 設定例](#)」(P.5-61) を参照)。
- ステップ 6** [Submit] をクリックして送信者グループを保存し [Host Access Table] ページに戻るか、[Submit and Add Senders] をクリックしてグループを作成し、送信者のグループへの追加を開始します。
- ステップ 7** 変更を確定します。



(注) 1つの送信者グループに重複するエントリ（同じドメインまたは IP アドレス）を入力すると、重複は廃棄されます。

送信者グループの編集

送信者グループを編集するには、次の手順を実行します。

ステップ 1 [HAT Overview] ページで、既存の送信者グループの名前をクリックします。選択した送信者グループが表示されます。

図 5-16 [Sender Group Detail] ページ
Sender Group: WHITELIST

Sender Group Settings	
Name:	WHITELIST
Order:	1
Comment:	My trusted senders have no Brightmail or rate limiting
Policy:	TRUSTED
SBRs (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included
<< Back to HAT Overview Edit Settings...	

Find Senders	
Find Senders that Contain this Text:	<input type="text"/> Find

Sender List: Display All Items in List	
Add Sender...	
There are no senders.	

ステップ 2 [Edit Settings] をクリックします。[Edit Sender Group] ページが表示されます。

図 5-17 [Edit Sender Group] ページ
Edit Sender Group Settings: WHITELIST

Sender Group Settings	
Name:	WHITELIST
Order:	1
Comment:	My trusted senders have no Brightmail or rate limiting
Policy:	TRUSTED
SBRs (Optional):	6.0 to 10.0 <input type="checkbox"/> Include SBRs Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional):	
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in the DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)

Cancel Submit

ステップ 3 送信者グループを変更し、[Submit] をクリックします。

ステップ 4 変更を確定します。

送信者グループの削除

送信者グループを削除するには、次の手順を実行します。

- ステップ 1** [HAT Overview] ページで、削除する送信者グループの [Delete] 列にあるゴミ箱のアイコンをクリックします。削除を確認するよう求められます。
- ステップ 2** [Yes] をクリックして送信者グループを削除するか、[No] をクリックしてキャンセルします。
- ステップ 3** 変更を確定します。

新しいメール フロー ポリシーの追加

新しいメール フロー ポリシーを追加するには、次の手順を実行します。

- ステップ 1** [Mail Policies] > [Mail Flow Policies] リンクをクリックします。[Mail Flow Policies] ページが表示されます。

- ステップ 2** [Add Policy] をクリックします。[Mail Flow Policies Add Policy] ページが表示されます。
- ステップ 3** メールフローポリシーの情報を入力します。
- ステップ 4** エンベロープ送信者の DNS 検証を設定します（「[送信者検証の実装 — 設定例](#)」(P.5-61) を参照）。
- ステップ 5** 変更を送信して確定します。



(注) [Use Default] オプション ボタンがオンの場合、ポリシーのデフォルト値はグレー表示されます。デフォルト値を上書きするには、[On] オプション ボタンを選択して機能または設定をイネーブルにし、新たにアクセス可能になった値を変更します。



(注) [Custom SMTP Banner Text] および [Max. Recipients Per Hour] テキスト文字列フィールドは、「[HAT 変数の構文](#)」(P.5-18) で説明した HAT 変数をサポートします。



(注) 一部のパラメータは特定の事前設定値に依存します（たとえば、ディレクトリ獲得攻撃の設定を行うには、LDAP 許可クエリーを設定しておく必要があります）。

メールフローポリシーの編集

メールフローポリシーを編集するには、次の手順を実行します。

- ステップ 1** [Mail Flow Policy overview] ページで、ポリシーの名前をクリックします。[Mail Flow Policy Edit Policy] ページが表示されます。
- ステップ 2** ポリシーを変更します。
- ステップ 3** 変更を送信して確定します。

メールフローポリシーの削除

メールフローポリシーを削除するには、次の手順を実行します。

- ステップ 1** 削除するメールフローポリシーの [Delete] 列にあるゴミ箱のアイコンをクリックします。削除を確認するよう求められます。
- ステップ 2** [Yes] をクリックしてメールフローポリシーを削除するか、[No] をクリックしてキャンセルします。
- ステップ 3** 変更を確定します。

送信者グループへの送信者の追加

既存の送信者グループに送信者を追加するには、次の手順を実行します。

- ステップ 1** ドメイン、IP、またはネットワーク オーナー プロファイル ページで、[Add to Sender Group] リンクをクリックします。

図 5-18 [Profile] ページの [Add to Sender Group] リンク

Current Information for rr.com		
Current Information from SenderBase	Sender Group Information	Network Information
Daily Magnitude: 8.0 Monthly Magnitude: 7.7 Days Since First Message from this Domain: 2630.8 days	Last Sender Group: UNKNOWNLIST	Network Owner: Road Runner
More from SenderBase	Add to Sender Group...	

[Add to Sender Group] ページが表示されます。図 5-19 を参照してください。

図 5-19 [Add to Sender Group] ページ

Sender	
Sender:	.fxp0.run, fxp0.run
Sender Group:	OutgoingMail (10.10.2.10:25) <input type="button" value="Select a Sender Group..."/>
	IncomingMail (10.10.1.10:25) <input type="button" value="Select a Sender Group..."/>
Comment:	<input type="text"/>
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

Select a Sender Group...
 WHITELIST
 BLACKLIST
 SUSPECTLIST
 UNKNOWNLIST
 ALL

- ステップ 2** 各リスナーに対して定義されているリストから送信者グループを選択します。
- ステップ 3** [Submit] をクリックして選択した送信者グループにドメインを追加するか、[Cancel] をクリックします。
- ステップ 4** 変更を確定します。



(注) ドメインを送信者グループに追加すると、実際には 2 つのドメインが GUI に表示されます。たとえば、ドメイン `example.net` を追加した場合、[Add to Sender Group] ページには、`example.net` と `.example.net` が追加されます。2 つめのエントリがあることで、`example.net` のサブドメイン内のすべてのホストが送信者グループに追加されます。詳細については、「[送信者グループの構文](#)」(P.5-27) を参照してください。



(注) 送信者グループに追加しようとしている送信者の 1 つ以上がその送信者グループにすでに存在する送信者と重複する場合、重複する送信者は追加されず、確認メッセージが表示されます。

Success — Added sender(s) to sender group(s). Some duplicates existed and were not added.

ステップ 5 [Save] をクリックして送信者を追加し、[Incoming Mail Overview] ページに戻ります。

新しい送信者グループへの送信者の追加

新しい送信者グループに送信者を追加するには、次の手順を実行します。

- ステップ 1** 新しい送信者グループを作成する場合、[Submit and Add Senders] をクリックします。[Add Sender] ページが表示されます。
- ステップ 2** 送信者を入力します。
- ステップ 3** オプションで送信者のコメントを入力します。
- ステップ 4** [Submit] をクリックして送信者グループにドメインを追加するか、[Cancel] をクリックします。
- ステップ 5** 変更を確定します。

SenderBase 評価スコアを使用した送信者グループの作成

SenderBase 評価スコアに基づいて送信者グループを作成するには、次の手順を実行します。

- ステップ 1** [HAT Overview] ページで [Add Sender Group] をクリックします。

- ステップ 2** [Add Sender Group] ページで、送信者グループの名前とオプションのコメントを入力します。
- ステップ 3** リストからメール フロー ポリシーを選択します。
- ステップ 4** [Senders] セクションで、ドロップダウン リストから [SBRS] を選択し、[Add Sender] をクリックします。
- ページがリフレッシュされます。
- ステップ 5** SBRS の [from:] フィールドと [to:] フィールドに範囲を入力し、オプションのコメントを入力します。
- 図 5-20 で、SenderBase 評価スコアが -7.5 未満の送信者は、BLOCKED メール フロー ポリシーを使用してブロックされます。

図 5-20 SenderBase 評価スコアを使用した送信者グループの作成 (1)
Add Sender Group

Sender Group Settings	
Name:	Bad_Reputation
Order:	1
Comment:	Block senders with a bad SenderBase Reputation Score
Policy:	BLOCKED
SBRS (Optional):	-7.5 to -10 <input type="checkbox"/> Include SBRS Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional):	?
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in the DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)

Cancel Submit Submit and Add Senders >>

図 5-21 で、SenderBase 評価スコアが 8.0 を超えている送信者はリスナーのアンチスパム スキャンをバイパスします。

図 5-21 SenderBase 評価スコアを使用した送信者グループの作成 (2)
Add Sender Group

Sender Group Settings	
Name:	Good_Reputation
Order:	1
Comment:	Trust senders with a good SenderBase Reputation Score
Policy:	TRUSTED
SBR5 (Optional):	8.0 to 10 <input type="checkbox"/> Include SBR5 Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional): ?	
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in the DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)

Cancel Submit Submit and Add Senders >>



(注) これらの同じパラメータを使用し、SenderBase 評価スコアに基づいて送信者を含めるように、TRUSTED および BLOCKED のデフォルトポリシーを変更することもできます。詳細については、「[SenderBase 評価フィルタの実装](#)」(P.7-6)を参照してください。

- ステップ 6** [Submit] をクリックし、SenderBase 評価スコアに基づいて送信者グループを作成します。
- ステップ 7** 変更を確定します。

図 5-22 SenderBase 評価スコアを使用したホスト アクセス テーブル
HAT Overview

The screenshot shows the 'HAT Overview' interface. At the top, there is a search bar labeled 'Find Senders that Contain this Text:' with a 'Find' button. Below that, a dropdown menu shows 'Sender Groups (Listener: IncomingMail (172.19.1.86:25))'. There are buttons for 'Add Sender Group...' and 'Import HAT...'. The main part of the interface is a table with the following columns: Order, Sender Group, SenderBase™ Reputation Score (with a scale from -10 to +10), Mail Flow Policy, and Delete. The table contains six rows of data.

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	WHITELIST	8	TRUSTED	🗑️
2	BLACKLIST	-10	BLOCKED	🗑️
3	SUSPECTLIST	-4	THROTTLED	🗑️
4	UNKNOWNLIST	2	ACCEPTED	🗑️
5	Bad_Reputation	-10	BLOCKED	🗑️
6	Good_Reputation	8	TRUSTED	🗑️
	ALL		ACCEPTED	

At the bottom of the table, there are buttons for 'Edit Order...' and 'Export HAT...'.

HAT の順序変更

HAT 内のエントリの順序は重要です。リスナーに接続しようとする各ホストについて、HAT が上から下に向かって読み込まれることを思い出してください。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。

たとえば、CIDR ブロックを送信者グループ A で指定し（ポリシー 1 を使用）、その CIDR ブロック内の IP アドレスに対して送信者グループ B を作成すると、送信者グループ B のポリシーは適用されません。

HAT 内のエントリの順序を編集するには、次の手順を実行します。

- ステップ 1** [HAT Overview] ページで、[Edit Order] をクリックします。[Edit Sender Group Order] ページが表示されます。
- ステップ 2** HAT の既存の行の新しい順序を入力します。
- ステップ 3** 変更を送信して確定します。

[HAT Overview] ページがリフレッシュされ、新しい順序で表示されます。

図 5-23 に示す次の例では、信頼できる送信者が最初に処理され、ブロックされる送信者が次に処理され、不明または疑いのある送信者が最後に処理されるように順序を変更しています。

図 5-23 HAT 内のエントリの順序の変更
Edit Sender Group Order

Order	Sender Group	SenderBase™ Reputation Score ?	Mail Flow Policy
1	WHITELIST	8	TRUSTED
3	BLACKLIST	-8	BLOCKED
5	SUSPECTLIST	-4	THROTTLED
6	UNKNOWNLIST	2	ACCEPTED
4	Bad_Reputation	-8	BLOCKED
2	Good_Reputation	8	TRUSTED
	ALL		ACCEPTED

送信者の検索

[HAT Overview] ページの上部にある [Find Senders] フィールドにテキストを入力することで送信者を検索できます。検索するテキストを入力し [Find] をクリックします。

GUI によるリスナーの HAT の変更

Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) にログインし、[Mail Policies] タブをクリックします (GUI にアクセスする方法については、「[GUI へのアクセス](#)」(P.2-3) を参照してください)。左側のメニューにある [HAT Overview] リンクをクリックします。[Host Access Table Overview] ページが表示されます。

図 5-24 [Host Access Table Overview] ページ
HAT Overview

Find Senders		SenderBase™ Reputation Score ?										Mail Flow Policy	Delete	
Find Senders that Contain this Text:														
Order	Sender Group	-10	-8	-6	-4	-2	0	2	4	6	8	+10		
1	WHITELIST												TRUSTED	🗑️
2	BLACKLIST												BLOCKED	🗑️
3	SUSPECTLIST												THROTTLED	🗑️
4	UNKNOWNLIST												ACCEPTED	🗑️
	ALL												ACCEPTED	

[Host Access Table Overview] ページには、HAT 内の送信者グループが、順序、SenderBase 評価スコア範囲、関連付けられているメールフローポリシーとともに一覧表示されます。

[Host Access Table Overview] ページでは、次のことを行うことができます。

- 送信者グループの HAT への追加
- 送信者グループの HAT からの削除
- 既存の送信者グループの変更
- エントリの順序の変更
- ファイルからの HAT のインポート（既存のエントリの上書き）（HAT のインポートとエクスポートについては、「[HAT の操作](#)」(P.5-55) を参照してください)。
- HAT のファイルへのエクスポート
- 送信者の検索

送信者グループを編集すると、次のことが可能です。

- 送信者グループへの送信者の追加と削除
- 送信者グループの設定の編集

送信者グループの使用方法の詳細については、「[GUI による送信者グループとメールフローポリシーの管理](#)」(P.5-43) を参照してください。

HAT の操作

HAT のエクスポート

HAT をエクスポートするには、次の手順を実行します。

- ステップ 1** [Export HAT] をクリックします。[Export Host Access Table] ページが表示されます。

図 5-25 HAT のエクスポート
Export HAT



- ステップ 2** エクスポートする HAT のファイル名を入力します。これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。
- ステップ 3** 変更を送信して確定します。

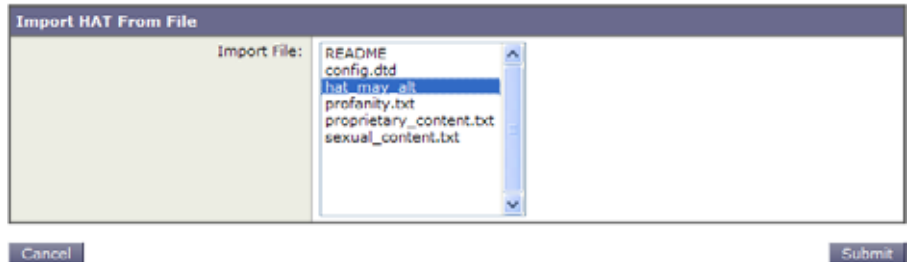
HAT のインポート

HAT をインポートすると、既存のすべての HAT エントリが現在の HAT から削除されます。

HAT をファイルからインポートするには、次の手順を実行します。

- ステップ 1** [Import HAT] をクリックします。[Import Host Access Table] ページが表示されます。

図 5-26 HAT のエクスポート
Import HAT



ステップ 2 リストからファイルを選択します。



(注) インポートするファイルは、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存在する必要があります。

ステップ 3 [Submit] をクリックします。既存のすべての HAT エントリを削除することを確認する警告メッセージが表示されます。

ステップ 4 [Import] をクリックします。

ステップ 5 変更を確認します。

ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次の例を参考にしてください。

```
# File exported by the GUI at 20060530T215438

$BLOCKED

    REJECT {}

[ ... ]
```

送信者検証

スパムや無用なメールは、多くの場合、DNS で解決できないドメインまたは IP アドレスを持つ送信者によって送信されます。DNS 検証とは、送信者に関する信頼できる情報を取得し、それに従ってメールを処理することを意味します。SMTP カンバセーションの前に送信者検証（送信者の IP アドレスの DNS ルッ

クアップに基づく接続のフィルタリング)を行うことは、Cisco IronPort アプライアンス上のメールパイプラインを介して処理されるジャンクメールの量を減らすことにも役立ちます。

未検証の送信者からのメールは自動的に廃棄されます。代わりに、AsyncOS には、未検証の送信者からのメールを処理する方法を決定する送信者検証設定があります。たとえば、SMTP カンパセーションの前に未検証の送信者からのすべてのメールを自動的にブロックしたり、未検証の送信者をスロットリングしたりするように Cisco IronPort アプライアンスを設定できます。

送信者検証機能は、SMTP カンパセーションの前に実行される接続元ホストの検証と、SMTP カンパセーションの最中に実行されるエンベロップ送信者のドメイン部分の検証の 2 つで構成されます。

送信者検証：ホスト

送信者が未検証となる理由にはさまざまなものがあります。たとえば、DNS サーバが「ダウン」または応答しないか、ドメインが存在しないことが考えられます。送信者グループのホスト DNS 検証設定では、SMTP カンパセーションの前に未検証の送信者を分類し、さまざまな種類の未検証の送信者をさまざまな送信者グループに含めることができます。

Cisco IronPort アプライアンスは、着信メールについて、DNS を通じて接続元ホストの送信元ドメインを検証しようとします。この検証は、SMTP カンパセーションの前に実行されます。システムは、二重の DNS ルックアップを実行することで、リモートホストの IP アドレス（つまりドメイン）の有効性を取得および検証します。二重の DNS ルックアップは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、その後の PTR ルックアップの結果に対する正引き DNS (A) ルックアップからなります。その後、アプライアンスは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。PTR ルックアップまたは A ルックアップが失敗するか、結果が一致しない場合、システムは IP アドレスのみを使用して HAT 内のエントリを照合し、送信者は未検証と見なされます。

未検証の送信者は次の 3 つのカテゴリに分類されます。

- 接続元ホストの PTR レコードが DNS に存在しない。
- DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。
- 接続元ホストの逆引き DNS ルックアップ (PTR) が正引き DNS ルックアップ (A) に一致しない。

送信者グループの [Connecting Host DNS Verification] 設定を使用して、未検証の送信者に対する動作を指定できます（「送信者グループ SUSPECTLIST に対するホスト送信者検証の実装」（P.5-62）を参照）。

すべての送信者グループの送信者グループ設定でホスト DNS 検証をイネーブルにできますが、ホスト DNS 検証設定を送信者グループに追加するということは、そのグループに未検証の送信者を含まれることになるという点に注意してください。つまり、スパムやその他の無用なメールが含まれることになります。そのため、これらの設定は、送信者を拒否またはスロットリングする送信者グループに対してのみイネーブルにすることを推奨します。たとえば、送信者グループ WHITELIST に対して DNS 検証をイネーブルにすると、未検証の送信者からのメールが、WHITELIST 内の信頼できる送信者からのメールと同じように扱われることを意味します（メール フロー ポリシーの設定内容に応じて、アンチスパムまたはアンチウイルス チェック、レート制限などのバイパスを含みます）。

送信者検証：エンベロープ送信者

エンベロープ送信者検証を使用すると、エンベロープ送信者のドメイン部分が DNS で検証されます（エンベロープ送信者のドメインが解決されるか。エンベロープ送信者のドメインの A レコードまたは MX レコードが DNS に存在するか）。タイムアウトや DNS サーバの障害など、DNS でのルックアップで一時的なエラー条件が発生した場合、ドメインは解決されません。これに対し、ドメインをルックアップしようとしたときに明確な「domain does not exist」ステータスが返された場合、ドメインは存在しません。この検証が SMTP カンバセーションの中で実行されるのに対し、ホスト DNS 検証はカンバセーションが開始される前に実行され、接続元 SMTP サーバの IP アドレスに適用されます。

詳細：AsyncOS は、送信者のアドレスのドメインに対して MX レコードクエリーを実行します。次に AsyncOS は、MX レコードのルックアップの結果に基づいて、A レコードのルックアップを行います。DNS サーバが「NXDOMAIN」（このドメインのレコードがない）を返した場合、AsyncOS はそのドメインが存在しないものとして扱います。これは「Envelope Senders whose domain does not exist」のカテゴリに分類されます。NXDOMAIN は、ルート ネーム サーバがこのドメインの権威ネームサーバを提供していないことを意味する場合があります。

しかし、DNS サーバが「SERVFAIL」を返した場合、「Envelope Senders whose domain does not resolve」として分類されます。SERVFAIL は、ドメインが存在するものの、DNS にレコードのルックアップで一時的な問題があることを意味します。

スパマーなどの不法なメール送信者が使用する一般的な手法は、MAIL FROM 情報（エンベロープ送信者内）を偽造し、受け付けられた未検証の送信者からのメールが処理されるようにすることです。これにより、MAIL FROM アドレスに送信されたバウンス メッセージが配信不能になるため、問題が生じる可能性があります。エンベロープ送信者検証を使用すると、不正な形式の（ただし空白ではない）MAIL FROM を拒否するように Cisco IronPort アプライアンスを設定できます。

各メール フロー ポリシーで、次のことが可能です。

- エンベロープ送信者の DNS 検証をイネーブルにする。
- 不正な形式のエンベロープ送信者に対し、カスタム SMTP コードと応答を渡す。エンベロープ送信者の DNS 検証をイネーブルにした場合、不正な形式のエンベロープ送信者はブロックされます。
- 解決されないエンベロープ送信者ドメインに対しカスタム応答を渡す。
- DNS に存在しないエンベロープ送信者ドメインに対しカスタム応答を渡す。

送信者検証例外テーブルを使用して、ドメインまたはアドレスのリストを格納し、そこからのメールを自動的に許可または拒否することができます（「[送信者検証例外テーブル](#)」(P.5-60) を参照)。送信者検証例外テーブルは、エンベロープ送信者検証とは独立してイネーブルにできます。そのため、たとえば、例外テーブルで指定した特別なアドレスやドメインを、エンベロープ送信者検証をイネーブルにすることなく拒否できます。また、内部ドメインまたはテストドメインからのメールを、他の方法で検証されない場合でも常に許可することもできます。

ほとんどのスパムは未検証の送信者から受信されますが、未検証の送信者からのメールを受け付けることが必要な理由があります。たとえば、すべての正規の電子メールを DNS ルックアップで検証できるわけではありません。一時的な DNS サーバの問題により送信者を検証できないことがあります。

未検証の送信者からのメール送信が試みられた場合、送信者検証例外テーブルとメール フロー ポリシーのエンベロープ送信者 DNS 検証設定を使用して、SMTP カンパセーション中にエンベロープ送信者が分類されます。たとえば、DNS に存在しないために検証されない送信元ドメインからのメールを受け付けてスロットリングすることができます。いったんそのメールを受け付けた後、MAIL FROM の形式が不正なメッセージは、カスタマイズ可能な SMTP コードと応答で拒否されます。これは SMTP カンパセーションの中で実行されます。

任意のメール フロー ポリシーに対し、メール フロー ポリシー設定中で、エンベロープ送信者の DNS 検証（ドメイン例外テーブルを含む）をイネーブルにできます。これには、GUI または CLI (`listenerconfig -> edit -> hostaccess -> <policy>`) を使用します。

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

エンベロープ送信者検証をイネーブルにするか、リスナーの SMTP アドレス解析オプションで部分ドメインの許可をディセーブルにすると（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「SMTP Address Parsing Options」の項を参照）、そのリスナーのデフォルト ドメイン設定は使用されなくなります。

これらの機能は互いに排他的です。

カスタム SMTP コードと応答

エンベロープ送信者の形式が不正なメッセージ、DNS に存在しないエンベロープ送信者、DNS クエリーで解決できない（DNS サーバがダウンしているなど）エンベロープ送信者に対し、SMTP コードと応答メッセージを指定できます。

SMTP 応答には変数 `$EnvelopeSender` を含めることができます。これは、カスタム応答を送信するときにエンベロープ送信者の値に展開されます。

一般には「Domain does not exist」結果は永続的ですが、これを一時的な状態にすることができます。そのようなケースを扱うために、「保守的な」ユーザは、エラー コードをデフォルトの 5XX から 4XX に変更できます。

送信者検証例外テーブル

送信者検証例外テーブルは、SMTP カンバセーション中に自動的に許可または拒否されるドメインまたは電子メール アドレスのリストです。また、拒否されるドメインについて、オプションの SMTP コードと拒否応答を指定することもできます。Cisco IronPort アプライアンスあたりの送信者検証例外テーブルは 1 つのみであり、メール フロー ポリシーごとにイネーブルにされます。

送信者検証例外テーブルは、明らかに偽物であるものの、形式が正しいドメインまたは電子メール アドレスをリストし、そこからのメールを拒否するために使用できます。たとえば、形式が正しい MAIL FROM `pres@whitehouse.gov` を送信者検証例外テーブルに格納し、自動的に拒否するように設定できます。また、

内部ドメインやテストドメインなど、自動的に許可するドメインをリストすることもできます。これは、受信者アクセステーブル (RAT) で行われるエンベロープ受信者 (SMTP RCPT TO コマンド) 処理に似ています。

送信者検証例外テーブルは、GUI の [Mail Policies] > [Exception Table] ページ (または CLI の `exceptionconfig` コマンド) で定義された後、GUI (「メールフローポリシー ACCEPTED に対する送信者検証の実装」(P.5-66) を参照) または CLI (『Cisco IronPort AsyncOS CLI Reference Guide』を参照) でポリシーごとにイネーブルにされます。

送信者検証例外テーブルのエントリの構文は次のとおりです。

図 5-27 例外テーブルのリスト
Exception Table

Order	Exception	Behavior	SMTP Response	Delete
1	pres@whitehouse.gov	Allow	N/A	🗑️

例外テーブルの変更については「GUI での送信者検証例外テーブルの作成」(P.5-67) を参照してください。

送信者検証の実装 — 設定例

ここでは、ホストとエンベロープ送信者検証の典型的で保守的な実装の例を示します。

この例では、ホスト送信者検証を実装するときに、既存の送信者グループ SUSPECTLIST とメールフローポリシー THROTTLED により、逆引き DNS ルックアップが一致しない接続元ホストからのメールがスロットリングされます。

新しい送信者グループ (UNVERIFIED) と新しいメールフローポリシー (THROTTLEMORE) が作成されます。検証されない接続元ホストからのメールは、SMTP カンバセーションの前にスロットリングされます (送信者グループ UNVERIFIED とより積極的なメールフローポリシー THROTTLEMORE が使用されます)。

メールフローポリシー ACCEPTED に対してエンベロープ送信者検証がイネーブルにされます。

表 5-15 に、送信者検証を実装するための推奨される設定を示します。

表 5-15 送信者検証：推奨される設定

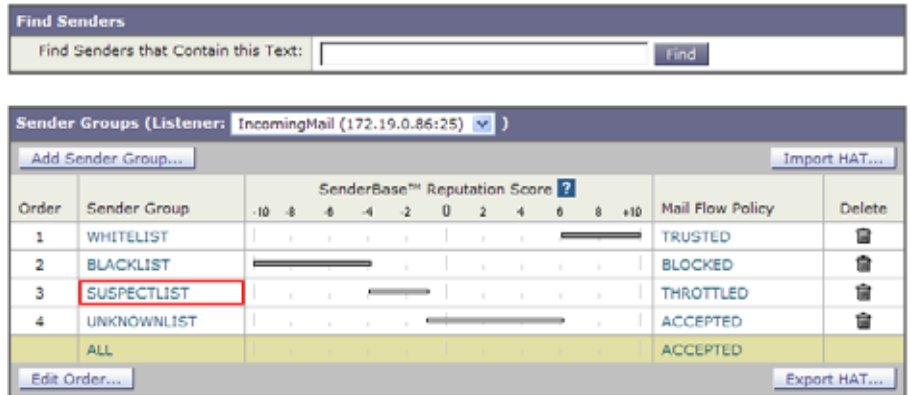
送信者グループ	ポリシー	内容
UNVERIFIED	THROTTLEMORE	SMTP カンバセーションの前。 接続元ホストの PTR レコードが DNS に存在しない。
SUSPECTLIST	THROTTLED	接続元ホストの逆引き DNS ルックアップ (PTR) が正引き DNS ルックアップ (A) に一致しない。
	ACCEPTED	SMTP カンバセーション中のエンベロープ送信者検証。 - 形式が不正な MAIL FROM:。 - エンベロープ送信者が DNS に存在しない。 - エンベロープ送信者が DNS で解決されない。

送信者グループ SUSPECTLIST に対するホスト送信者検証の実装

GUI で、[Mail Policies] タブの [HAT Overview] をクリックします。既存の送信者グループの一覧が表示されます。送信者グループ SUSPECTLIST に対するホスト DNS 検証をイネーブルにして設定するには、次の手順を実行します。

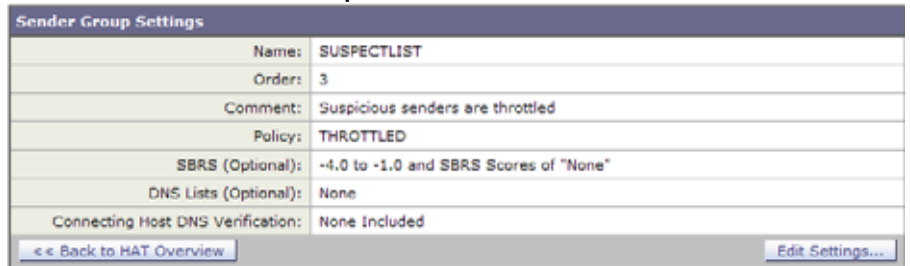
- ステップ 1** [HAT Overview] ページで、送信者グループのリスト中の [SUSPECTLIST] をクリックします。

図 5-28 [HAT Overview] ページ
HAT Overview



ステップ 2 [Sender Group: SUSPECTLIST] ページが表示されます。

図 5-29 Sender Group: SUSPECTLIST



ステップ 3 [Edit Settings] をクリックします。[Edit Settings] ダイアログが表示されます。

図 5-30 Sender Group: SUSPECTLIST: Edit Settings

Sender Group Settings	
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRs (Optional):	-4.0 to -1.0 <input checked="" type="checkbox"/> Include SBRs Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional): ?	
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input checked="" type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

Cancel Submit

- ステップ 4** リストから [THROTTLED] ポリシーを選択します。
- ステップ 5** [Connecting Host DNS Verification] の中の [Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)] チェックボックスをオンにします。
- ステップ 6** 変更を送信して確定します。
- 逆引き DNS ルックアップが失敗した送信者は送信者グループ SUSPECTLIST に一致し、メールフローポリシー THROTTLED のデフォルトアクションが実行されます。



(注) また、CLI でホスト DNS 検証を設定することもできます。詳細については、「[CLI でのホスト DNS 検証のイネーブル化](#)」(P.5-72) を参照してください。

送信者検証の実装

まず、新しいメールフローポリシーを作成し（この例では THROTTLEMORE という名前を付けます）、より厳格なスロットリング設定を行います。

- ステップ 1** [Mail Flow Policies] ページで [Add Policy] をクリックします。
- ステップ 2** メールフローポリシーの名前を入力し、[Connection Behavior] として [Accept] を選択します。
- ステップ 3** メールをスロットリングするようにポリシーを設定します。
- ステップ 4** 変更を送信して確定します。

次に、新しい送信者グループを作成し（この例では、UNVERIFIED という名前を付けます）、THROTTLEMORE ポリシーを使用するように設定します。

ステップ 1 [HAT Overview] ページで [Add Sender Group] をクリックします。

図 5-31 Add Sender Group: THROTTLEMORE
Add Sender Group to IncomingMail (192.168.0.1:25)

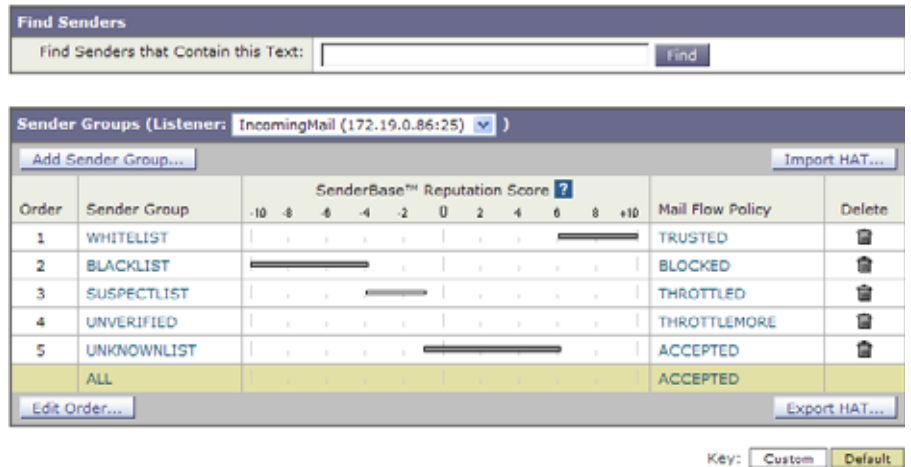
Sender Group Settings	
Name:	UNVERIFIED
Order:	5
Comment:	Throttle when host record is not in DNS
Policy:	THROTTLEMORE
SBR5 (Optional):	<input type="checkbox"/> to <input type="text"/> <input type="checkbox"/> Include SBR5 Scores of "None" <i>Recommended for suspected senders only.</i>
DNS Lists (Optional):	<input type="text"/>
Connecting Host DNS Verification:	<input checked="" type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

ステップ 2 リストから [THROTTLEMORE] ポリシーを選択します。

ステップ 3 [Connecting Host DNS Verification] 中の [Connecting host PTR record does not exist in DNS] チェックボックスをオンにします。

ステップ 4 変更を送信して確定します。これで [HAT Overview] ページは次のようになります。

図 5-32 HAT Overview
HAT Overview



次の手順では、未検証の送信者を扱うようにメールフローポリシー ACCEPTED を設定します。

メールフローポリシー ACCEPTED に対する送信者検証の実装

GUI で、[Mail Policies] タブの [Mail Flow Policies] をクリックします。既存のメールフローポリシーの一覧が表示されます。メールフローポリシー ACCEPTED に対してエンベロープ送信者の DNS 検証をイネーブлにするには、次の手順を実行します。

- ステップ 1** [Mail Flow Policies] ページで、メールフローポリシー [ACCEPTED] をクリックします。
- ステップ 2** メールフローポリシーの最後にスクロールします。

図 5-33 メール フロー ポリシー ACCEPTED のエンベロープ送信者の DNS 検証の設定

Envelope Sender DNS Verification:	<input type="radio"/> Use Default (Off) <input checked="" type="radio"/> On <input type="radio"/> Off
Malformed Envelope Senders:	
SMTP Code:	553
SMTP Text:	#5.5.4 Domain required for sender address
Envelope Senders whose domain does not resolve:	
SMTP Code:	451
SMTP Text:	#4.1.3 Domain of sender address <\$Envelo
Envelope Senders whose domain does not exist:	
SMTP Code:	553
SMTP Text:	#5.1.0 Domain of sender address <\$Envelo
Use Exception Table:	<input type="radio"/> Use Default (Off) <input checked="" type="radio"/> On <input type="radio"/> Off

- ステップ 3** [On] を選択し、このメール フロー ポリシーに対するエンベロープ送信者の DNS 検証をイネーブルにします。
- ステップ 4** カスタム SMTP コードと応答を定義することもできます。
- ステップ 5** [Use Exception Table] で [On] を選択することで、ドメイン例外テーブルをイネーブルにします。
- ステップ 6** 変更を送信して確定します。

最後の手順として、送信者検証例外テーブルを作成し、送信者検証設定に対する例外を列挙します。

GUI での送信者検証例外テーブルの作成

[Mail Policies] > [Exception Table] ページを使用して、送信者検証例外テーブルを設定します。例外テーブルは、[Use Exception Table] がオンになっているすべてのメール フロー ポリシーにグローバルに適用されることに注意してください。

- ステップ 1** [Mail Policies] > [Exception Table] ページで [Add Domain Exception] をクリックします。[Add Domain Exception] ページが表示されます。

図 5-34 例外テーブルへのアドレスの追加
Add Domain Exception

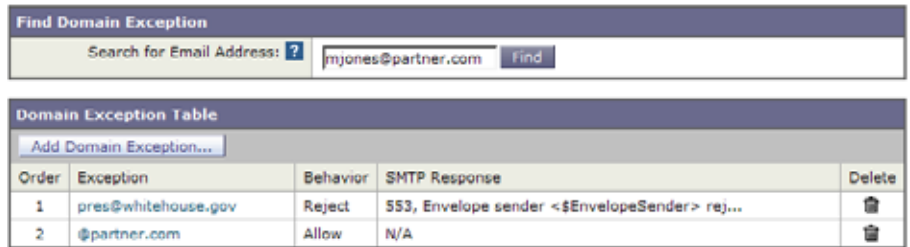
- ステップ 2** 電子メール アドレスを入力します。具体的なアドレス (pres@whitehouse.gov)、名前 (user@)、ドメイン (@example.com または @.example.com)、または IP アドレスを角カッコで囲んだアドレス (user@[192.168.23.1]) を入力できます。
- ステップ 3** そのアドレスからのメッセージを許可するか拒否するかを指定します。メールを拒否する場合、SMTP コードとカスタム応答を指定することもできます。
- ステップ 4** 変更を送信して確定します。

送信者検証例外テーブル内でのアドレスの検索

特定のアドレスが例外テーブルのいずれかのエントリに一致するかどうかを判定するには、次の手順を実行します。

- ステップ 1** [Exception Table] ページの [Find Domain Exception] セクションに電子メールアドレスを入力し、[Find] をクリックします。

図 5-35 例外テーブル中の一致エントリの検索
Exception Table



ステップ 2 テーブル中のいずれかのエントリにアドレスが一致した場合、最初に一致したエントリが表示されます。

図 5-36 例外テーブル中の一致エントリの一覧表示
Exception Table



送信者検証設定のテスト

これで送信者検証設定を完了したため、Cisco IronPort アプライアンスの動作を確認できます。

DNS 関連の設定のテストは、本書の範囲を超えていることに注意してください。

エンベロープ送信者検証の設定のテスト

THROTTLED ポリシーのさまざまな DNS 関連の設定をテストすることは難しい場合がありますが、形式が不正な MAIL FROM 設定をテストできます。

ステップ 1 Cisco IronPort アプライアンスへの Telnet セッションを開きます。

- ステップ 2** SMTP コマンドを使用して、形式が不正な MAIL FROM（ドメインなしの「admin」など）を使用したテスト メッセージを送信します。



(注) デフォルト ドメインを使用するか、メールを送受信するときに部分ドメインを明示的に許可するように Cisco IronPort アプライアンスを設定した場合や、アドレス解析をイネーブルにした場合は、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照)、ドメインがないかドメインの形式が正しくない電子メールを作成、送信、受信できない場合があります。

- ステップ 3** メッセージが拒否されることを確認します。

```
# telnet IP_address_of_IronPort_Appliance_port

220 hostname ESMTF

helo example.com

250 hostname

mail from: admin

553 #5.5.4 Domain required for sender address
```

SMTP コードと応答が、メール フロー ポリシー THROTTLED のエンベロープ送信者検証設定で設定したものになっていることを確認します。

送信者検証例外テーブルのテスト

送信者検証例外テーブルに列挙されている電子メール アドレスからのメールに対し、エンベロープ送信者検証が実行されないことを確認するには、次の手順を実行します。

- ステップ 1** アドレス `admin@zzzaazz.com` を、例外テーブルに動作「Allow」で追加します。
- ステップ 2** 変更を確定します。
- ステップ 3** Cisco IronPort アプライアンスへの Telnet セッションを開きます。

ステップ 4 SMTP コマンドを使用して、送信者検証例外テーブルに入力した電子メール アドレス (admin@zzzaazz.com) からテスト メッセージを送信します。

ステップ 5 メッセージが許可されることを確認します。

```
# telnet IP_address_of_IronPort_Appliance_port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin@zzzaazz.com
250 sender <admin@zzzaazz.com> ok
```

その電子メール アドレスを送信者検証例外テーブルから削除すると、エンベロープ送信者のドメイン部分が DNS で検証されないため、その送信者からのメールが拒否されます。

送信者検証とロギング

次のログ エントリは、送信者検証の判断例を示します。

エンベロープ送信者検証

形式が不正なエンベロープ送信者

```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected,
envelope sender domain missing
```

ドメインが存在しない (NXDOMAIN)

```
Wed Aug 9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com>
sender rejected, envelope sender domain does not exist
```

ドメインが解決されない (SERVFAIL)

```
Wed Aug 9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com>
sender rejected, envelope sender domain could not be resolved
```

CLI でのホスト DNS 検証のイネーブル化

CLI でホスト DNS 検証をイネーブルにするには、`listenerconfig->edit->hostaccess` コマンドを使用します (詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください)。

表 5-16 に、未検証の送信者の種類と対応する CLI 設定を示します。

表 5-16 送信者グループ設定と対応する CLI 値

接続元ホストの DNS 検証	同等の CLI 設定
接続元ホストの PTR レコードが DNS に存在しない。	<code>nx.domain</code>
DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。	<code>serv.fail</code>
接続元ホストの逆引き DNS ルックアップ (PTR) が正引き DNS ルックアップ (A) に一致しない。	<code>not.double.verified</code>

パブリック リスナー (RAT) 上でのローカルドメインまたは特定のユーザの電子メールの受け入れ

パブリック リスナーを作成するとき、受信者アクセス テーブル (RAT) を使用して、アプライアンスがメッセージを受け付けるすべてのローカルドメインを定義します。多くのエンタープライズゲートウェイは、複数のローカルドメインのメッセージを受け付けるように設定されます。たとえば、会社名が変更されたとします。その場合、`currentcompanyname.com` および `oldcompanyname.com` 宛の電子メールメッセージを受信する必要があります。この場合、両方のローカルドメインをパブリックリスナーの RAT に含めることになります (注: ドメインマップ機能はあるドメインから別のドメインにメッセージをマップできま

す。『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Domain Features」の章とドメイン マップ機能の項を参照してください。



(注)

System Setup Wizard または `systemsetup` コマンドを完了し、`commit` コマンドを実行済みの場合、1 つのパブリック リスナーがアプライアンス上ですでに設定されています（「手順 3 : Network」(P.3-26) で入力した設定を参照してください）。そのときに入力した、メールを許可するデフォルト ローカル ドメインまたは具体的なアドレスは、そのパブリック リスナーの RAT の最初のエン트리として設定されます。

受信者アクセス テーブル (RAT)

受信者アクセス テーブルは、パブリック リスナーが許可する受信者を定義します。このテーブルでは、アドレス（部分アドレス、ユーザ名、ドメイン、またはホスト名）と、それを許可するか拒否するかを指定します。オプションで、その受信者の RCPT TO コマンドに対する SMTP 応答を含めたり、特定のエントリでスロットリング制御をバイパスしたりできます。

RAT エントリは次の基本的な構文によって定義されます。

表 5-17 RAT の基本的な構文

受信者定義	ルール	(任意) カスタム SMTP 応答
-------	-----	-------------------

ルール

RAT には、SMTP カンパセーションの中でやりとりするときに受信者に対して実行する、次の 2 つの基本的な動作があります。

ACCEPT	受信者は許可されます。
REJECT	受信者は拒否されます。

受信者の定義

RAT では、受信者または受信者のグループを定義できます。受信者は、完全な電子メールアドレス、ドメイン、部分ドメイン、またはユーザ名で定義できます。

division.example.com	完全修飾ドメイン名。
.partialhost	「partialhost」ドメイン内のすべて。
user@domain	完全な電子メールアドレス。
user@	指定したユーザ名を含むすべてのアドレス。
user@[IP_address]	特定の IP アドレスのユーザ名。IP アドレスは文字「[]」で囲む必要があることに注意してください。 「user@[IP_address]」（角カッコ文字なし）は有効なアドレスではないことに注意してください。有効なアドレスを作成するために、メッセージを受信したときに角カッコが追加され、受信者が RAT で一致するかどうかに影響が出ることがあります。



(注)

GUI の System Setup Wizard の手順 4 でドメインを受信者アクセステーブルに追加する場合（「手順 3 : Network」(P.3-26) を参照）、サブドメインを指定するための別のエントリを追加することを検討してください。たとえば、ドメイン example.net を入力する場合、.example.net も入力したほうがよい場合があります。第 2 のエントリにより、example.net のすべてのサブドメイン宛のメールが受信者アクセステーブルに一致するようになります。RAT で .example.com のみを指定した場合、.example.com のすべてのサブドメイン宛のメールを許可しますが、サブドメインがない完全な電子メールアドレス受信者（たとえば joe@example.com）宛のメールは許可されません。

特別な受信者でのスロットリングのバイパス

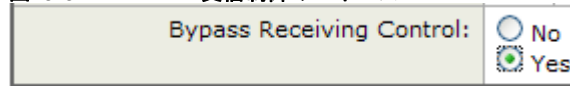
受信者エントリで、リスナーでイネーブルになっているスロットリング制御メカニズムを受信者がバイパスすることを指定できます。

この機能は、特定の受信者のメッセージを制限しない場合に便利です。たとえば、多くのユーザは、メールフローポリシーで定義されている受信制御に基づいて送信元ドメインがスロットリングされている場合でも、リスナー上でアドレ

ス「postmaster@domain」の電子メールを受信します。リスナーの RAT 中で受信制御をバイパスするようにこの受信者を指定することで、同じドメイン中の他の受信者用のメール フロー ポリシーを保持しつつ、リスナーは受信者「postmaster@domain」の無制限のメッセージを受信できます。受信者は、送信元ドメインが制限されている場合に、システムが保持している時間あたりの受信者のカウンタでカウントされません。

GUI で特定の受信者が受信制御をバイパスするように指定するには、RAT エントリを追加または編集するときに、[Bypass Receiving Control] で [Yes] を選択します。

図 5-37 受信制御のバイパス



CLI で特定の受信者が受信制御をバイパスするように指定するには、`listenerconfig -> edit -> rcptaccess` コマンドを使用して受信者を入力するときに、次の質問に「yes」と答えます。

```
Would you like to bypass receiving control for this entry? [N]> y
```

特別な受信者での LDAP 許可のバイパス

LDAP 許可クエリーを設定する場合、特定の受信者について許可クエリーをバイパスすることが必要な場合があります。この機能は、`customercare@example.com` のように、ある受信者宛に受信した電子メールについて、LDAP クエリーの中で遅延させたりキューに格納したりしないことが望ましい場合に便利です。

LDAP 許可クエリーの前にワーク キュー内で受信者アドレスを書き換えるように設定した場合（エイリアシングまたはドメイン マップの使用など）、書き換えられたアドレスは LDAP 許可クエリーをバイパスしません、たとえば、エイリアステーブルを使用して `customercare@example.com` を `bob@example.com` および `sue@example.com` にマップします。`customercare@example.com` について LDAP 許可のバイパスを設定した場合、エイリアシングが実行された後に、`bob@example.com` および `sue@example.com` に対して LDAP 許可クエリーが実行されます。

GUI で LDAP 許可をバイパスするように設定するには、RAT エントリを追加または編集するときに [Bypass LDAP Accept Queries for this Recipient] を選択します。

CLI で LDAP 許可クエリーをバイパスするように設定するには、
`listenerconfig -> edit -> rcptaccess` コマンドを使用して受信者を入力する
 ときに、次の質問に「yes」と答えます。

Would you like to bypass LDAP ACCEPT for this entry? [Y]> **y**

LDAP 許可をバイパスするように RAT エントリを設定する場合、RAT エントリ
 の順序が、受信者アドレスの一致のしかたに影響を与えることに注意してくださ
 さい。条件を満たす最初の RAT エントリを使用して受信者アドレスが一致します。
 たとえば、RAT エントリ `postmaster@ironport.com` と `ironport.com` があるとしま
 します。`postmaster@ironport.com` のエントリについては LDAP 許可クエリーをバイ
 パスするように設定し、`ironport.com` のエントリを ACCEPT に設定します。
`postmaster@ironport.com` 宛のメールを受信した場合、LDAP 許可がバイパスさ
 れるのは、`postmaster@ironport.com` のエントリが `ironport.com` のエントリより
 も前にある場合のみです。`ironport.com` のエントリが `postmaster@ironport.com`
 のエントリの前にある場合、RAT はこのエントリを介して受信者アドレスと一
 致し、ACCEPT アクションが適用されます。

デフォルト RAT エントリ

作成するすべてのパブリック リスナーについて、デフォルトでは、すべての受
 信者からの電子メールを拒否するように RAT が設定されます。

ALL	REJECT
-----	--------

[Recipient Access Table Overview] リストでは、デフォルト エントリの名前は
 [All Other Recipients] になります。



(注)

デフォルトでは、RAT はすべての受信者を拒否し、誤ってインターネット上に
 オープン リレーが作成されないようにします。オープンリレー（「セキュアでな
 いリレー」または「サードパーティ リレー」とも呼びます）は、第三者による
 電子メール メッセージのリレーを許す SMTP 電子メール サーバです。オープン
 リレーがあると、ローカル ユーザ向けでもローカル ユーザからでもないメール
 を処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパム
 を送信することが可能になります。作成するパブリック リスナーの受信者アク
 セス テーブルのデフォルト値を変更するときには注意してください。

デフォルトの「ALL」エントリを RAT から削除してはなりません。

テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする方法

アプライアンスのコンフィギュレーション ディレクトリにアクセスする必要があります。インポートするテキスト ファイルは、アプライアンス上のコンフィギュレーション ディレクトリに存在する必要があります。エクスポートされたテキスト ファイルは、コンフィギュレーション ディレクトリに配置されます。

コンフィギュレーション ディレクトリへのアクセスの詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください。

GUI によるリスナーの RAT の変更

GUI から RAT を変更するには、[Mail Policies] > [Recipient Access Table (RAT)] をクリックします。[Recipient Access Table Overview] ページが表示されます。

図 5-38 [Recipient Access Table Overview] ページ

Order	Recipient Address	Default Action	All Delete
1	.run, ironport.com	Accept	<input type="checkbox"/>
2	redfish.com	Accept (Bypass LDAP)	<input type="checkbox"/>
All Other Recipients		Reject	

[Recipient Access Table Overview] ページには、RAT 内のエントリの一覧が、その順序、デフォルトのアクション、エントリが LDAP 許可クエリーをバイパスするように設定されているかどうかとともに表示されます。

[Recipient Access Table Overview] では、次のことを行うことができます。

- RAT へのエントリの追加
- RAT からのエントリの削除
- 既存の RAT エントリの変更
- エントリの順序の変更
- ファイルからの RAT エントリのインポート (既存のエントリの上書き)
- RAT エントリのファイルへのエクスポート

RAT は、コマンドライン インターフェイス (CLI) を使って直接編集できます。定義したリスナーの RAT をカスタマイズするには、`listenerconfig` コマンドの `edit -> rcptaccess -> new` サブコマンドを使用して、設定する各パブリックリスナーについて、許可されるローカルドメインを RAT に追加します。詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

新しい RAT エントリの追加

RAT にエントリを追加するには、次の手順を実行します。

- ステップ 1** [Add Recipient] をクリックします。[Add to Recipient Access Table] ページが表示されます。

図 5-39 RAT エントリの追加

- ステップ 2** エントリの順序を選択します。
- ステップ 3** 受信者アドレスを入力します (有効なエントリの詳細については、「[受信者の定義](#)」(P.5-74) を参照してください)。
- ステップ 4** 受信者を許可するか拒否するかを選択します。
- ステップ 5** オプションで、受信者に対する LDAP 許可クエリーをバイパスすることを選択できます (「[特別な受信者での LDAP 許可のバイパス](#)」(P.5-75) を参照)。
- ステップ 6** このエントリに対してカスタム SMTP 応答を使用する場合は、[Custom SMTP Response] で [Yes] を選択します。応答コードとテキストを入力します。

- ステップ 7** オプションで、スロットリングをバイパスすることを設定できます（「[特別な受信者でのスロットリングのバイパス](#)」(P.5-74) を参照)。そのためには、[Bypass Receiving Control] で [Yes] を選択します。
- ステップ 8** 変更を送信して確定します。

RAT エントリの削除

RAT エントリを削除するには、次の手順を実行します。

-
- ステップ 1** 削除する各エントリの [Delete] 列のチェックボックスをオンにします。
- ステップ 2** [Delete] をクリックします。
- ステップ 3** チェックボックスをオンにしたエントリが RAT から削除されます。
- ステップ 4** 変更を確定します。

RAT エントリの変更

RAT エントリを変更するには、次の手順を実行します。

-
- ステップ 1** [Recipient Access Table Overview] で RAT エントリをクリックします。[Edit Recipient Access Table] ページが表示されます。
- ステップ 2** エントリを変更します。
- ステップ 3** 変更を確定します。

RAT エントリの順序の変更

RAT 内のエントリの順序を変更するには、次の手順を実行します。

-
- ステップ 1** [Edit Order] をクリックします。[Edit Recipient Access Table Order] ページが表示されます。

図 5-40 RAT エントリの順序の変更
Edit Recipient Access Table Order

Overview for Listener: IncomingMail (172.19.1.86:25)		Items per page 20
Order	Recipient Address	Default Action
1	.run, ironport.com	Accept
2	redfish.com	Accept (Bypass LDAP)
	All Other Recipients	Reject

Cancel Submit

ステップ 2 [Order] 列の値を調整して順序を変更します。

ステップ 3 変更を確定します。

RAT エントリのエクスポート

RAT エントリをエクスポートするには、次の手順を実行します。

ステップ 1 [Export RAT] をクリックします。[Export Recipient Access Table] ページが表示されます。

図 5-41 RAT エントリのエクスポート
Export Recipient Access Table

Export Recipient Access Table To File	
Export to file:	<input type="text"/>

Cancel Submit

ステップ 2 エクスポートするエントリのファイル名を入力します。これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。

ステップ 3 変更を送信して確定します。

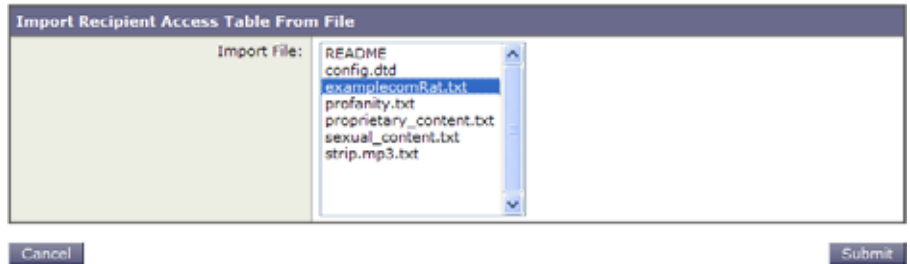
RAT エントリのインポート

RAT をインポートすると、既存のすべての RAT エントリが RAT から削除されます。

一連の RAT エントリをインポートするには、次の手順を実行します。

ステップ 1 [Import RAT] をクリックします。[Import Recipient Access Table] ページが表示されます。

図 5-42 RAT エントリのエクスポート
Import Recipient Access Table



ステップ 2 リストからファイルを選択します。



(注) インポートするファイルは、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存在する必要があります。

ステップ 3 [Submit] をクリックします。既存の RAT エントリをすべて削除することを確認する警告メッセージが表示されます。

ステップ 4 [Import] をクリックします。

ステップ 5 変更を確定します。

ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次の例を参考にしてください。

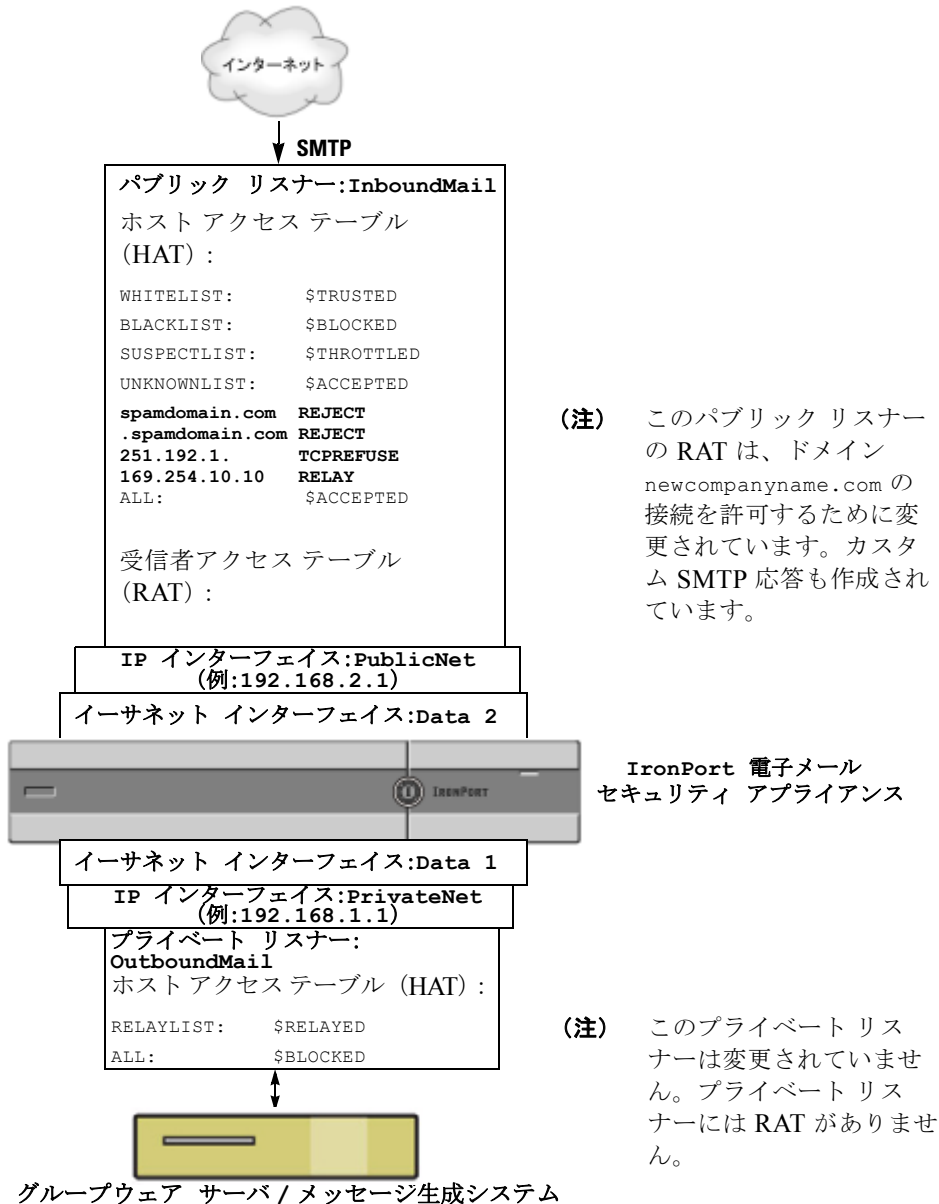
```
# File exported by the GUI at 20060530T220526

.example.com  ACCEPT

ALL  REJECT
```

この時点で、電子メールゲートウェイの設定は次のようになります。

図 5-43 パブリック リスナーの RAT の編集

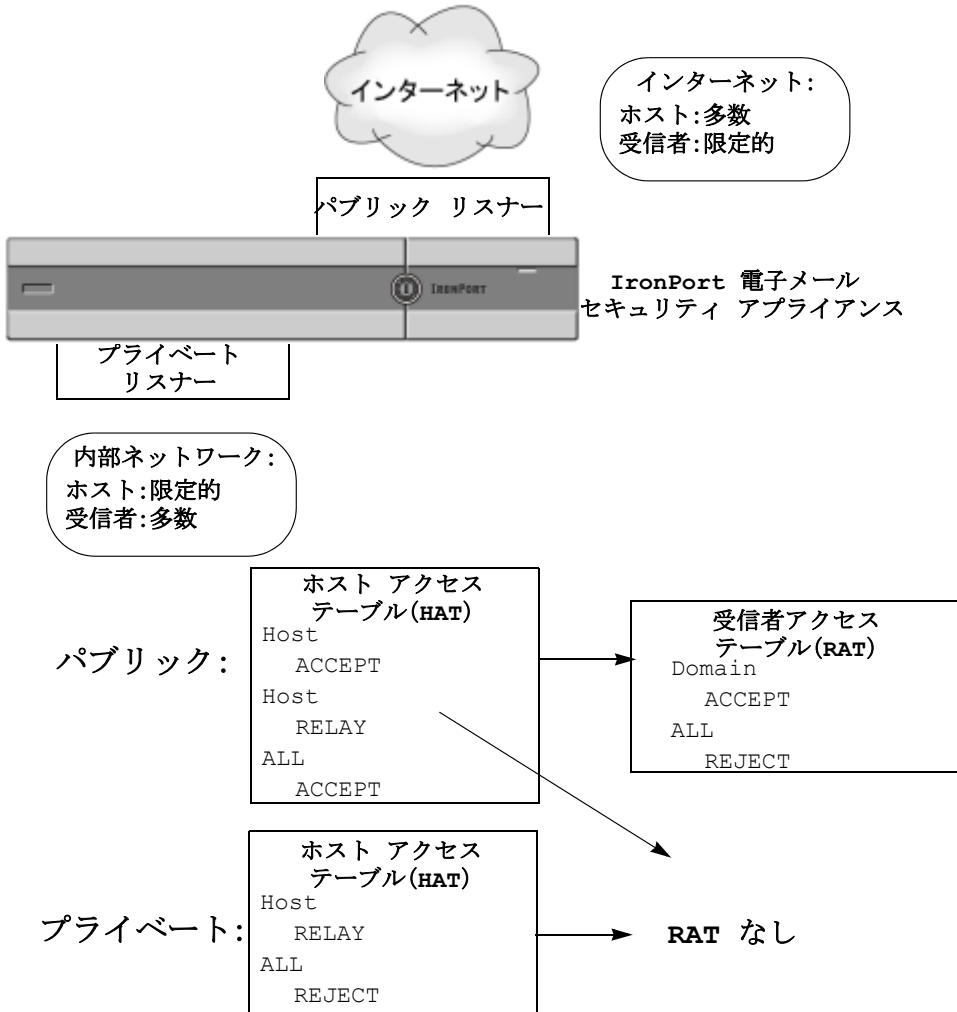


(注) このパブリック リスナーの RAT は、ドメイン newcompanyname.com の接続を許可するために変更されています。カスタム SMTP 応答も作成されています。

(注) このプライベート リスナーは変更されていません。プライベート リスナーには RAT がありません。

図 5-44 は、図 5-4 に示した図を展開したものであり、リスナーの HAT（該当する場合）と RAT の処理シーケンスと、それぞれのデフォルト値が含まれています。

図 5-44 パブリック リスナーとプライベート リスナー





CHAPTER 6

電子メール セキュリティ マネージャ

電子メール セキュリティ マネージャは、Cisco IronPort アプライアンスのすべての電子メール セキュリティ サービスおよびアプリケーションを管理するための1つの包括的なダッシュボードです。本リリースよりも前のリリースでは、アンチスパムおよびアンチウイルス設定は、リスナー単位で行われていました。つまり、ポリシーは、メッセージの受信者または送信者に基づいてではなく、IP アドレスの受信リスナーに基づいて適用されていました。第5章「電子メールを受信するためのゲートウェイの設定」では、リスナーの作成および設定方法について説明します。

電子メール セキュリティ マネージャを使用すると、感染フィルタ機能、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを、個別のインバウンドおよびアウトバウンド ポリシーを介して、受信者または送信者単位で管理できます。

GUI の [Mail Policies] メニュー (CLI の `policyconfig` コマンド) を使用して、着信または発信メール ポリシーを作成および管理します。メール ポリシーは、次の機能の特定の設定にマッピングされるユーザの特定のセットとして定義されます (エンベロップ受信者、エンベロップ送信者、From: ヘッダーまたは Reply-To: ヘッダー)。

- アンチスパム スキャン
- アンチウイルス スキャン
- 感染フィルタ
- コンテンツ フィルタ
- RSA Email Data Loss Prevention ポリシー (アウトバウンド メールのみ)

ユーザは、電子メール アドレス、電子メール ドメインまたは LDAP グループ クエリーにより定義できます。

この章は、次の内容で構成されています。

- 「ユーザベース ポリシーの概要」 (P.6-2)
- 「コンテンツ フィルタの概要」 (P.6-10)
- 「実際の例 (GUI)」 (P.6-31)

ユーザベース ポリシーの概要

電子メール セキュリティ マネージャのユーザベース ポリシーを使用すると、組織内のすべてのユーザのさまざまな、また個別のセキュリティ ニーズを満たすポリシーを作成できます。

たとえば、この機能を使用すると、次の条件を適用するポリシーをすぐに作成できます。

- **IronPort Anti-Spam** スキャンを、販売部へのすべての電子メールではディセーブルにし、エンジニアリング部では、陽性と疑わしいスパム メッセージと問題のないマーケティング メッセージの件名にタグを付け、陽性と判定されたスパムをドロップする中程度のポリシーを適用してイネーブルにします。また、人事部では、陽性と疑わしいスパム メッセージと問題のないマーケティング メッセージを検疫して、陽性と判定されたスパムをドロップする、積極的なポリシーを適用してアンチスパム スキャンをイネーブルにします。
- システム管理者グループ以外のすべてのユーザで、危険な実行可能プログラムの添付ファイルをドロップします。
- エンジニアリング部宛てのメッセージのウイルスをスキャンおよび修復しますが、アドレス `jobs@example.com` に送信されるすべてのメッセージの感染添付ファイルをドロップします。
- **RSA Email Data Loss Prevention (DLP)** を使用してすべての発信メッセージをスキャンし、機密情報として扱う必要がある情報が含まれているかどうか確認します。条件と一致するメッセージは、検疫され、法務部にブラインド カーボン コピーで送信されます。

- 着信メッセージに MP3 添付ファイルが含まれている場合、そのメッセージを検疫して、宛先となっている受信者に、メッセージを受信するにはネットワーク オペレーション センターに問い合わせる必要があることを示すメッセージを送信します。このようなメッセージは 10 日後に有効期限が切れません。
- エグゼクティブ スタッフからのすべての発信メールへの免責事項を企業の最新のタグ ラインに含め、広報部からのすべての発信メールに異なる「将来の見込みに関する」免責事項を含めます。
- すべての着信メッセージの感染フィルタ機能をイネーブルにして、**example.com** へのリンクを含むメッセージまたはファイル拡張子が .dwg の添付ファイルを含むメッセージのスキャンをバイパスします。



(注)

コンテンツ フィルタから、コンテンツ デictionary、免責事項および通知に関するテンプレートを参照するには、これらを事前に作成しておく必要があります。詳細については、「[テキスト リソース](#)」(P.14-1) を参照してください。

着信および 発信メッセージ

電子メール セキュリティ マネージャでは、2 つのポリシー テーブルが定義されます。1 つは、HAT ポリシーにより「Accept」動作として規定される送信ホストからのメッセージ用のテーブルで、もう 1 つのテーブルは、HAT「Relay」動作と見なされる送信ホスト用のテーブルです。前者のテーブルは、**着信**ポリシー テーブルで、後者は、**発信**ポリシー テーブルです。

- **着信**メッセージは、任意のリスナーの ACCEPT HAT ポリシーに一致する接続から受信されるメッセージです。
- **発信**メッセージは、任意のリスナーの RELAY HAT ポリシーに一致する接続からのメッセージです。この接続には、SMTP AUTH で認証された任意の接続が含まれます。



(注)

特定のインストールでは、Cisco IronPort アプライアンスを経由する「内部」メールは、すべての受信者が内部アドレスにアドレス指定されている場合でも、**発信**と見なされます。たとえば、Cisco IronPort C10/100 カスタマーの場合はデフォルトで、System Setup Wizard がインバウンド電子メールの受信およびアウトバウンド電子メールのリレー用として、1 リスナーに物理イーサネット ポートを 1 つだけ設定します。

多くの設定では、いずれもシングル リスナーにより使用される場合でも、着信テーブルはパブリック、発信テーブルはプライベートと見なされます。特定のメッセージで使用されるポリシー テーブルは、メッセージの方向、つまり、送信者アドレスか受信者アドレスかどうか、またはインターネットへの発信かイントラネットへの着信かどうかに依存しません。

これらのテーブルを管理するには、GUI の [Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ、あるいは CLI の `policyconfig` コマンドを使用します。メール システムの管理などを担当する委任管理者に個々のメール ポリシーを割り当てることができます。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」の章を参照してください。



(注) RSA Email DLP スキャンは、発信メッセージだけで実行できます。

ポリシー マッチング

着信メッセージがシステムのリスナーにより受信されると、システムで設定されているリスナーの数に関係なく、各メッセージ受信者は、いずれか 1 つのテーブルのポリシーとマッチングされます。マッチングは、受信者のアドレスまたは送信者のアドレスのいずれかに基づいて行われます。

- 受信者アドレスは、エンベロープ受信者アドレスとマッチングされます。

受信者アドレスのマッチングでは、入力される受信者アドレスは、電子メール パイプラインの先行部による処理後の最後のアドレスです。たとえば、イネーブルにされている場合、デフォルト ドメイン、LDAP ルーティングまたはマスカレード、エイリアス テーブル、ドメイン マップおよびメッセージ フィルタ機能は、エンベロープ受信者アドレスを再作成できます。これにより、電子メール セキュリティ マネージャ（アンチスパム、アンチウイルス、コンテンツ フィルタおよび感染フィルタ）のポリシーとのメッセージのマッチングに影響を与えることがあります。
- 送信者アドレスは、次のアドレスとマッチングされます。
 - エンベロープ送信者 (RFC821 MAIL FROM アドレス)
 - RFC822 From: ヘッダーのアドレス
 - RFC822 Reply-To: ヘッダーのアドレス

アドレス マッチングは、完全な電子メール アドレス、ユーザ、ドメインまたは部分的なドメインのいずれか、あるいは LDAP グループ メンバーシップで行われます。

First Match Wins

各受信者は、該当するテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。

メッセージの各受信者に対して、最初に一致したポリシーが適用されます。受信者がいずれのポリシーにも一致しない場合、その受信者には、自動的に、テーブルのデフォルト ポリシーが適用されます。

マッチングが送信者アドレス（またはアップグレードにより作成される特殊な「リスナー」ルール（以下を参照））に基づいて行われる場合、メッセージの残りの受信者全員に、そのポリシーが適用されます（これは、メッセージごとに存在する送信者またはリスナーが 1 人だけのためです）。

ポリシー マッチングの例

次の例では、ポリシー テーブルがどのように上から順にマッチングされるかを説明します。

次の表 6-1 に示す着信メールの電子メール セキュリティ ポリシーの表では、着信メッセージはさまざまなポリシーとマッチングされます。

表 6-1 **ポリシー マッチングの例**

順序	ポリシー名	ユーザ
1	special_people	受信者: joe@example.com 受信者: ann@example.com
2	from_lawyers	送信者: @lawfirm.com
3	acquired_domains	受信者: @newdomain.com 受信者: @anotherexample.com
4	engineering	受信者: PublicLDAP.ldapgroup: engineers
5	sales_team	受信者: jim@ 受信者: john@ 受信者: larry@
	Default Policy	(全ユーザ)

例 1

送信者 `bill@lawfirm.com` から受信者 `jim@example.com` に送信されるメッセージには、ポリシー 2 が適用されます。これは、表内で、送信者 (`@lawfirm.com`) と一致するユーザ説明が、受信者 (`jim@`) と一致するユーザ説明よりも前に示されているためです。

例 2

送信者 `joe@yahoo.com` は、3 人の受信者、`john@example.com`、`jane@newdomain.com` および `bill@example.com` の着信メッセージを送信します。受信者 `jane@newdomain.com` のメッセージには、ポリシー 3 で定義されているアンチスパム、アンチウイルス、感染フィルタおよびコンテンツ フィルタが適用されますが、受信者 `john@example.com` のメッセージには、ポリシー 5 で定義されている設定が適用されます。受信者 `bill@example.com` は、エンジニアリング LDAP クエリーと一致しないため、このメッセージには、デフォルトポリシーで定義されている設定が適用されます。次の例では、受信者が複数あるメッセージでメッセージ分裂がどのように発生するかについて示します。詳細については、「[メッセージ分裂](#)」(P.6-6) を参照してください。

例 3

送信者 `bill@lawfirm.com` は、受信者 `ann@example.com` および `larry@example.com` にメッセージを送信します。受信者 `ann@example.com` には、ポリシー 1 で定義されているアンチスパム、アンチウイルス、感染フィルタおよびコンテンツ フィルタが適用され、受信者 `larry@example.com` には、ポリシー 2 で定義されているアンチスパム、アンチウイルス、感染フィルタおよびコンテンツ フィルタが定義されます。これは、表内で、送信者 (`@lawfirm.com`) が、受信者 (`jim@`) と一致するユーザ説明よりも前に示されているためです。

メッセージ分裂

インテリジェントなメッセージ分裂 (マッチング ポリシーによる) は、受信者が複数あるメッセージに、受信者に基づいた異なるポリシーを個別に適用できるメカニズムです。

各受信者は、該当する電子メール セキュリティ マネージャ テーブル (着信または発信) の各ポリシーに対して上から順に評価されます。

メッセージに一致する各ポリシーは、これらの受信者に新しいメッセージを作成します。このプロセスが、「メッセージ分裂」と定義されます。

- 一部の受信者が異なるポリシーと一致する場合、受信者は一致したポリシーに基づいてグループ化され、メッセージは一致したポリシー数と同数のメッセージに分裂されます。これらの受信者は、それぞれ適切な「分裂先」に設定されます。
- すべての受信者が同じポリシーと一致する場合、メッセージは分裂されません。反対に、最も多くの分裂が行われるのは、単一のメッセージがメッセージ受信者 1 人 1 人に分裂される場合です。
- 各メッセージ分裂は、アンチスパム、アンチウイルス、DLP スキャン（発信メッセージのみ）、感染フィルタおよびコンテンツ フィルタにより、電子メールパイプラインで個別に処理されます。





表 6-2 に、電子メールパイプラインでメッセージが分裂されるポイントを示します。



(注)

Email DLP スキャンは、発信メッセージだけで使用できます。

表 6-2 電子メール パイプラインでのメッセージ分裂

ワークキュー	メッセージ フィルタ (filters)	電子メールセキュリティ マネージャ スキャン (受信者単位)	↓  すべての受信者のメッセージ
	アンチスパム (antispamconfig, antispamupdate)		メッセージは、メッセージ フィルタ処理の直後からアンチスパム処理の前に分裂されます。
	アンチウイルス (antivirusconfig, antivirusupdate)		
	コンテンツ フィルタ (policyconfig -> filters)		
	感染フィルタ (outbreakconfig, outbreakflush, outbreakstatus, outbreakupdate)		
データ消失防止 (policyconfig)	 すべての受信者のメッセージ ポリシー 1 と一致  すべての受信者のメッセージ ポリシー 2 と一致  その他のすべての受信者のメッセージ (デフォルト ポリシーと一致) (注) RSA Email DLP スキャンは、発信メッセージだけで実行されます。		



(注) 新しい MID (メッセージ ID) が、各メッセージ分裂用に作成されます (たとえば、MID 1 は、MID 2 および MID 3 になります)。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」の章を参照してください。また、トレース機能は、メッセージを分裂したポリシーを示します。

電子メールセキュリティ マネージャ ポリシーのポリシー マッチングおよびメッセージ分裂は、アプライアンスで使用できるメッセージ処理の管理に影響を与えます。

管理例外

分裂メッセージごとの反復処理はパフォーマンスに影響を与えるため、電子メールセキュリティ マネージャの着信および発信メール ポリシー テーブルを使用して、*管理例外*単位でポリシーを設定することを推奨します。つまり、組織のニーズを評価し、大多数のメッセージがデフォルト ポリシーで処理され、少数のメッセージが、追加の「例外」ポリシーで処理されるように機能を設定します。

このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

ポリシーの内容

電子メール セキュリティ マネージャ テーブルは、ユーザの特定のグループ（エンベロープ受信者、エンベロープ送信者、From: ヘッダーまたは Reply-To: ヘッダー）に対して着信または発信メッセージをマッチングし、これらを次の機能の特定の設定にマッピングします。

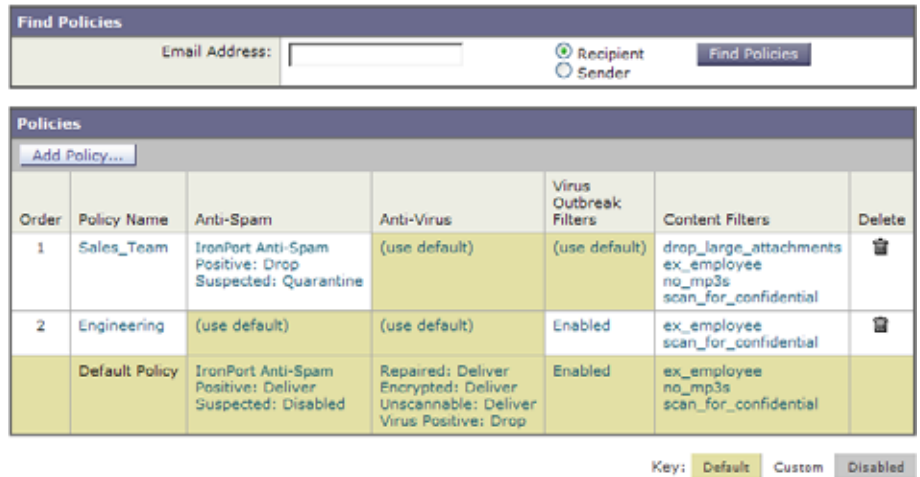
- Anti-Spam スキャン：詳細については、「アンチスパム」(P.8-1) を参照してください。
- Anti-Virus スキャン：詳細については、「アンチウイルス」(P.9-1) を参照してください。
- コンテンツ フィルタ：詳細については、「コンテンツ フィルタの概要」(P.6-10) を参照してください。
- 感染フィルタ

Cisco IronPort の感染フィルタ機能は、従来のアンチウイルスおよびアンチスパム セキュリティ サービスが更新されて検出できるまで、疑わしいメッセージを検疫することで、新種ウイルス、フィッシング、詐欺の発生に対する「第一の防衛ライン」を提供する予測セキュリティ サービスです。感染フィルタは特定の受信者に対してイネーブルまたはディセーブルにできません。また、電子メール セキュリティ マネージャの感染フィルタ機能をバイパスするファイル タイプを定義することもできます。詳細については、[第 10 章「感染フィルタ」](#)を参照してください。

- データ消失防止：詳細については、[第 11 章「データ消失防止」](#)を参照してください。

図 6-1 に、ポリシーで定義されたユーザを特定のアンチスパム、アンチウイルス、感染フィルタ、DLP およびコンテンツ フィルタ設定にマッピングする GUI の電子メール セキュリティ マネージャを示します。

図 6-1 GUI の電子メール セキュリティ マネージャ ポリシーの概要
Incoming Mail Policies



Order	Policy Name	Anti-Spam	Anti-Virus	Virus Outbreak Filters	Content Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	(use default)	(use default)	drop_large_attachments ex_employee no_mp3s scan_for_confidential	
2	Engineering	(use default)	(use default)	Enabled	ex_employee scan_for_confidential	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Disabled	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Enabled	ex_employee no_mp3s scan_for_confidential	

Key: Default Custom Disabled

コンテンツ フィルタの概要

電子メール セキュリティ マネージャ ポリシーでは、受信者または送信者単位でメッセージに適用されるコンテンツ フィルタを作成できます。コンテンツ フィルタは、電子メール パイプラインで後ほど適用される点、つまり、1 つのメッセージが、各電子メール セキュリティ マネージャ ポリシーに対応する個々の複数のメッセージに「分裂」された後で適用される点を除いては、メッセージ フィルタとほぼ同じです。コンテンツ フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。

通常メッセージ フィルタと同様に、各コンテンツ フィルタに名前を定義します。この名前は、使用される着信または発信メール ポリシー テーブルで一意でなければなりません。各着信および発信メール ポリシー テーブルには、コンテンツ フィルタ独自の単一「マスター リスト」があります。順序は、テーブル単位（着信または発信）で定義されます。ただし、各個別のポリシーは、実行される特定のフィルタを決定します。

通常メッセージ フィルタ（アンチスパムおよびアンチウイルス スキャンの前に適用される）とは異なり、コンテンツ フィルタは、CLI および GUI の両方で設定できます。GUI には、「ルール ビルダ」ページがあります。このページでは、コンテンツ

フィルタを構成する条件およびアクションを簡単に作成できます。電子メールセキュリティ マネージャの着信または発信メール ポリシー テーブルは、特定のポリシーに適用される順序で、イネーブルにされるコンテンツ フィルタを管理します。表 6-3 に、コンテンツ フィルタの作成に使用できる条件を示します。表 6-4 に、コンテンツ フィルタの定義に使用できる非最終および最終アクションを示します。コンテンツ フィルタは、条件およびアクションにより構成されます。表 6-5 に、コンテンツ フィルタの作成に使用できるアクション変数を示します。

メール ポリシーでコンテンツ フィルタを編集してイネーブルにすることが可能な委任管理ユーザ ロールを指定できます。委任管理者のコンテンツ フィルタに関するアクセス権限の詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」の章を参照してください。

コンテンツ フィルタの条件

コンテンツ フィルタでの条件の指定はオプションです。

コンテンツ フィルタの条件では、メッセージ本文または添付ファイルでパターンを検索するフィルタ ルールを追加する場合、パターンが検出される回数の最小しきい値を指定できます。AsyncOS は、メッセージをスキャンする場合、メッセージおよび添付ファイルで検出する一致数の「スコア」を合計します。最小しきい値が満たされていない場合、正規表現は true に評価されません。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。

また、「スマート ID」を使用して、データのパターンを識別することもできます。スマート ID は、次のパターンを検出できます。

- クレジット カード番号
- 米国 社会保障番号
- Committee on Uniform Security Identification Procedures (CUSIP) 番号
- American Banking Association (ABA; 米国銀行協会) ルーティング番号

パターンが検出される回数の最小しきい値の指定、およびスマート ID の詳細については、『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。

各フィルタには、複数の条件を定義できます。複数の条件が定義されている場合、条件を論理 OR（「次の任意の条件...」）または論理 AND（「次のすべての条件」）のいずれかで結合するかを選択できます。

表 6-3 コンテンツ フィルタの条件

条件	説明
(条件なし)	コンテンツ フィルタでの条件の指定はオプションです。条件が指定されていない場合、true ルールが適用されます。true ルールはすべてのメッセージに一致し、必ずアクションが実行されます。
Message Body or Attachments	<p>[Contains text] : メッセージ本文に、特定のパターンと一致するテキストまたは添付ファイルが含まれているかどうかを判別します。</p> <p>[Contains smart identifier] : メッセージ本文または添付ファイルのコンテンツが、スマート ID と一致するかどうかを判別します。</p> <p>[Contains term in content dictionary] : メッセージ本文に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.14-3) を参照してください。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。</p> <p>これには、配信ステータス部および関連付けられている添付ファイルが含まれます。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
Message Body	<p>[Contains text] : メッセージ本文に、特定のパターンと一致するテキストが含まれているかどうかを判別します。</p> <p>[Contains smart identifier] : メッセージ本文のコンテンツが、スマート ID と一致するかどうかを判別します。</p> <p>[Contains term in content dictionary] : メッセージ本文に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.14-3) を参照してください。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。このしきい値は、テキストまたはスマート ID に指定できます。</p> <p>このルールは、メッセージの本文だけに適用されます。添付ファイルまたはヘッダーは含まれません。</p>
Message Size	<p>本文サイズが、指定範囲内にあるかどうかを判別します。本文サイズは、ヘッダーと添付ファイルの両方を含む、メッセージのサイズを示します。本文サイズ ルールは、本文サイズが指定数と比較されるメッセージを選択します。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
Attachment Content	<p>[Contains text] : メッセージに、特定のパターンと一致するテキストまたは別の添付ファイルが含まれている添付ファイルが関連付けられているかどうかを判別します。このルールは、body-contains () ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。</p> <p>[Contains a smart identifier] : メッセージ添付ファイルの内容が、指定されたスマート ID と一致するかどうかを判別します。</p> <p>[Contains terms in content dictionary] : 添付ファイルに、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.14-3) を参照してください。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
Attachment File Info	<p>[Filename] : メッセージに、ファイル名が特定のパターンと一致する添付ファイルが含まれているかどうかを判別します。</p> <p>[File type] : メッセージに、フィンガープリントに基づいて特定のパターンと一致するファイルタイプの添付ファイルが含まれているかどうかを判別します (UNIX file コマンドと似ています)。</p> <p>[MIME type] : メッセージに、特定の MIME タイプの添付ファイルが含まれているかどうかを判別します。このルールは、attachment-type ルールと似ていますが、このルールでは、MIME 添付ファイルにより指定される MIME タイプだけが評価されます (アプライアンスは、タイプが明示的に指定されていない場合、拡張子からファイルのタイプを「予測」することはありません)。</p> <p>[Image Analysis] : メッセージに、指定されているイメージ判定と一致するイメージ添付ファイルが含まれているかどうかを判別します。有効なイメージ分析判定には、[Suspect]、[Inappropriate]、[Suspect or Inappropriate]、[Unscannable] または [Clean] があります。</p>
Attachment Protection	<p>[Contains an attachment that is password-protected or encrypted] :</p> <p>(この条件は、たとえば、スキャンできない可能性がある添付ファイルを特定する場合に使用します)</p> <p>[Contains an attachment that is NOT password-protected or encrypted] :</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
Subject Header	<p>[Subject Header] : 件名ヘッダーに、特定のパターンが含まれているかどうかを判別します。</p> <p>[Contains terms in content dictionary] : 件名ヘッダーに、<dictionary name> という名前のコンテンツ デictionary のいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>Dictionary用語を検索するには、Dictionaryがすでに作成されている必要があります。「コンテンツ Dictionary」 (P.14-3) を参照してください。</p>
Other Header	<p>[Header name] : メッセージに、特定のヘッダーが含まれているかどうかを判別します。</p> <p>[Header value] : ヘッダーの値が、特定のパターンと一致するかどうかを判別します。</p> <p>[Header value contains terms in the content dictionary] : 指定されたヘッダーに、<dictionary name> という名前のコンテンツ Dictionary のいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>Dictionary用語を検索するには、Dictionaryがすでに作成されている必要があります。「コンテンツ Dictionary」 (P.14-3) を参照してください。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
Envelope Sender	<p>[Envelope Sender] : エンベロープ送信者 (つまり、Envelope From、<MAIL FROM>) が、特定のパターンと一致するかどうかを判別します。</p> <p>[Matches LDAP group] : エンベロープ送信者 (つまり、Envelope From、<MAIL FROM>) が、特定の LDAP グループに含まれるかどうかを判別します。</p> <p>[Contains term in content dictionary] : エンベロープ送信者に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.14-3) を参照してください。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

条件	説明
Envelope Recipient	<p>[Envelope Recipient] : エンベロープ受信者 (つまり、Envelope To、<RCPT TO>) が、特定のパターンと一致するかどうかを判別します。</p> <p>[Matches LDAP group] : エンベロープ受信者 (つまり、Envelope To、<RCPT TO>) が、特定の LDAP グループに含まれるかどうかを判別します。</p> <p>[Contains term in content dictionary] : エンベロープ受信者に、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。「コンテンツ ディクショナリ」(P.14-3) を参照してください。</p> <p>注 : [Envelope Recipient] ルールは、メッセージ単位です。メッセージに複数の受信者がある場合、グループの受信者が 1 人だけ検出されれば、指定されたアクションがメッセージのすべての受信者に適用されます。</p> <p>エンベロープ送信者 (つまり、Envelope From、<MAIL FROM>) が、特定の LDAP グループに含まれるかどうかを判別します。</p>
Receiving Listener	<p>メッセージが、指定されたリスナーを介して着信したかどうかを判別します。リスナー名は、システムで現在設定されているリスナーの名前でなければなりません。</p>

表 6-3 コンテンツ フィルタの条件 (続き)

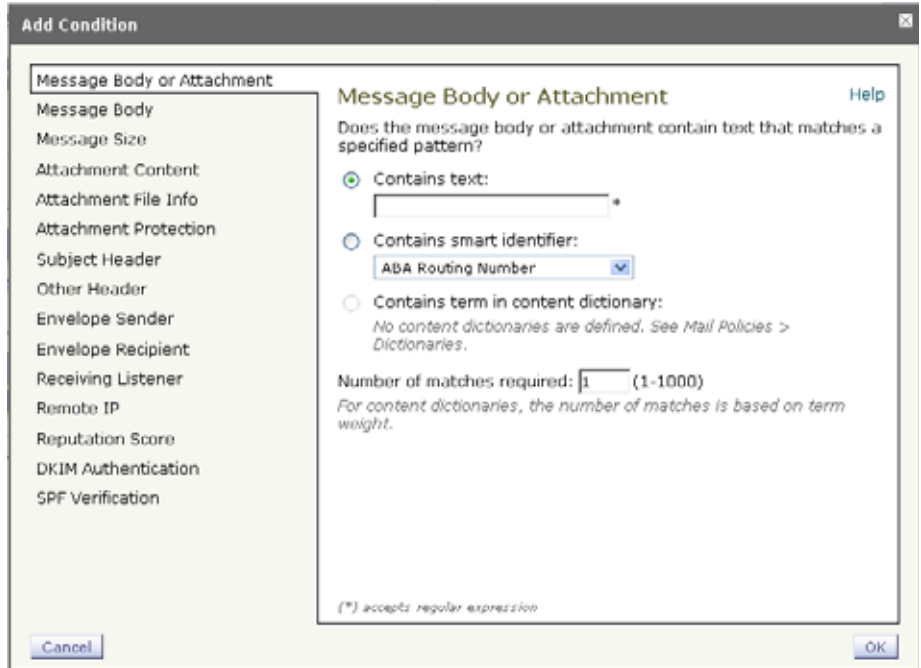
条件	説明
Remote IP	メッセージが、特定の IP アドレスまたは IP ブロックと一致するリモート ホストから送信されたかどうかを判別します。[Remote IP] ルールは、メッセージを送信したホストの IP アドレスが特定のパターンと一致するかどうかをテストします。IP アドレス パターンは、「送信者グループの構文」(P.5-27) で説明されている、許可されたホスト表記を使用して指定されます。ただし、SBO、SBRs、dnstlist 表記および特殊キーワード ALL を除きます。
Reputation Score	送信者の SenderBase 評価スコアを検証します。[Reputation Score] は、別の値に対する SenderBase 評価スコアをチェックします。
DKIM Authentication	DKIM 認証に合格したか、部分的に検証されたか、一時的に検証不可能として返されたか、失敗したか、DKIM 結果が返されていないかどうかを判別します。
SPF Verification	SPF 検証ステータスを判別します。このフィルタでは、さまざまな SPF 検証結果をクエリーできます。SPF 検証の詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Email Authentication」を参照してください。



(注)

ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、「コンテンツ ディクショナリ」(P.14-3) を参照してください。

図 6-2 コンテンツ フィルタの条件



コンテンツ フィルタのアクション

各コンテンツ フィルタには、少なくとも 1 つのアクションを定義する必要があります。

アクションは、順序に従いメッセージで実行されるため、コンテンツ フィルタの複数のアクションを定義する場合、アクションの順序を考慮します。

[Attachment Content] 条件、[Message Body or Attachment] 条件、[Message Body] 条件または [Attachment Content] 条件に一致するメッセージの検疫アクションを設定する場合は、検疫されたメッセージの一致した内容を表示できます。メッセージの本文を表示する場合、一致した内容は、黄色で強調表示されません。また、`$MatchedContent` アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』を参照してください。

フィルタごとに定義できる最終アクションは 1 つだけです。最終アクションは、リストの最後のアクションです。バウンス、配信、およびドロップは、最終アクションです。コンテンツ フィルタのアクションを入力する場合、GUI および CLI により、最終アクションが強制的に最後に配置されます。

表 6-4 コンテンツ フィルタのアクション

アクション	説明
Quarantine	<p>[Quarantine] : いずれかのシステム検疫エリアに保持されるメッセージにフラグを付けます。</p> <p>[Duplicate message] : メッセージのコピーを指定された検疫エリアに送信して、オリジナル メッセージの処理を続行します。任意の追加アクションが、オリジナル メッセージに適用されます。</p>
Encrypt on Delivery	<p>メッセージは、次の処理段階に進みます。すべての処理が完了すると、メッセージが暗号化され、配信されます。</p> <p>[Encryption rule] : メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、「TLS 接続を暗号化の代わりに使用」(P.12-11) を参照してください。</p> <p>[Encryption Profile] : 処理が完了したら、指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco IronPort 暗号化アプライアンスまたはホステッドキー サービスで使用されます。</p> <p>[Subject] : 暗号化されたメッセージの件名です。デフォルトでは、この値は、\$Subject です。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
Strip Attachment by Content	<p>[Attachment contains] : 正規表現を含むメッセージのすべての添付ファイルをドロップします。アーカイブ ファイル (zip、tar) は、それらに含まれる任意のファイルが、正規表現パターンと一致した場合にドロップされます。</p> <p>[Contains smart identifier] : 指定されたスマート ID を含むメッセージのすべての添付ファイルをドロップします。</p> <p>[Attachment contains terms in the content dictionary] : 添付ファイルに、<dictionary name> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。</p> <p>[Number of matches required] : ルールが true と評価されるために必要な一致回数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。</p> <p>[Replacement message] : オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。メッセージに、添付ファイル フッターが追加されます。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
Strip Attachment by File Info	<p>[File name] : 指定された正規表現とファイル名が一致するメッセージのすべての添付ファイルをドロップします。アーカイブ ファイルの添付ファイル (zip、tar) は、それらに含まれるファイルが一致した場合にドロップされません。</p> <p>[File size] : ロー エンコード形式で、指定サイズ (バイト単位) 以上のメッセージのすべての添付ファイルをドロップします。アーカイブ ファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の添付ファイルのサイズを検証するため注意してください。</p> <p>[File type] : ファイルの指定「フィンガープリント」と一致するメッセージのすべての添付ファイルをドロップします。アーカイブ ファイルの添付ファイル (zip、tar) は、それらに含まれるファイルが一致した場合にドロップされます。</p> <p>[MIME type] : タイプが指定 MIME タイプであるメッセージのすべての添付ファイルをドロップします。</p> <p>[Image Analysis Verdict] : 指定されたイメージ判定と一致するイメージ添付ファイルをドロップします。有効なイメージ分析判定には、[Suspect]、[Inappropriate]、[Suspect or Inappropriate]、[Unscannable] または [Clean] があります。</p> <p>[Replacement message] : オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。メッセージに、添付ファイル フッターが追加されます。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
Add Disclaimer Text	<p>[Above] : メッセージ上部に免責事項を追加します (ヘッダー)。</p> <p>[Below] : メッセージ下部に免責事項を追加します (フッター)。</p> <p>注 : このコンテンツ フィルタ アクションを使用するには、免責事項テキストをすでに作成している必要があります。</p> <p>詳細については、「免責事項テンプレート」(P.14-27) を参照してください。</p>
Bypass Outbreak Filter Scanning	このメッセージの感染フィルタ スキャンをバイパスします。
Send Copy (Bcc:)	<p>[Email addresses] : 指定受信者にメッセージを匿名でコピーします。</p> <p>[Subject] : コピーされたメッセージの件名を追加します。</p> <p>[Return path (optional)] : リターン パスを指定します。</p> <p>[Alternate mail host (optional)] : 代替メール ホストを指定します。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
Notify	<p>[Notify] : 指定された受信者にこのメッセージを報告します。オプションで送信者および受信者に通知できます。</p> <p>[Subject] : コピーされたメッセージの件名を追加します。</p> <p>[Return path (optional)] : リターン パスを指定します。</p> <p>[Use template] : 作成したテンプレートからテンプレートを選択します。</p> <p>[Include original message as an attachment] : オリジナルメッセージを添付ファイルとして追加します。</p>
Change Recipient to	<p>[Email address] : メッセージの受信者を指定電子メールアドレスに変更します。</p>
Send to Alternate Destination Host	<p>[Mail host] : メッセージの宛先メール ホストを指定メールホストに変更します。</p> <p>(注) このアクションは、アンチスパム スキャン エンジンによりスパムとして分類されたメッセージが検疫されないようにします。このアクションは、検疫を無効にして、指定メール ホストに送信します。</p>
Deliver from IP Interface	<p>[Send from IP interface] : 指定 IP インターフェイスから送信します。[Deliver from IP Interface] アクションは、メッセージのソース ホストを指定ソースに変更します。ソースホストは、メッセージが配信される IP インターフェイスで構成されます。</p>
Strip Header	<p>[Header name] : 指定ヘッダーを配信前にメッセージから削除します。</p>

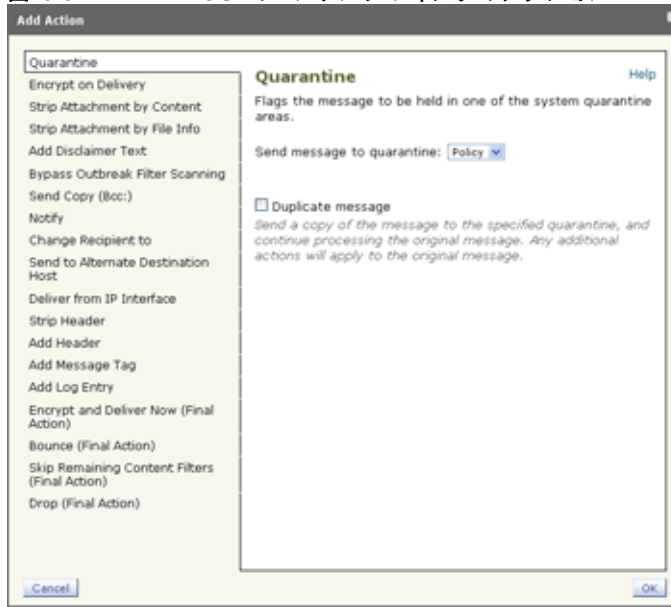
表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
Add Header	<p>[Header name] : ヘッダーを配信前にメッセージに挿入します。</p> <p>[Header value] : ヘッダーの値を配信前にメッセージに挿入します。</p>
Add Message Tag	<p>RSA Email DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに挿入します。RSA Email DLP ポリシーを設定して、スキャンをメッセージ タグの付いたメッセージに制限できます。メッセージ タグは、受信者に表示されません。DLP ポリシーでのメッセージ タグの使用については、「DLP ポリシー」(P.11-6) を参照してください。</p>
Add Log Entry	<p>カスタマイズされたテキストを INFO レベルで IronPort Text Mail ログに挿入します。テキストには、アクション変数を含めることができます。ログ エントリは、メッセージ トラッキングにも表示されます。</p>
Encrypt and Deliver Now (Final Action)	<p>メッセージを暗号化および配信し、その後の任意の処理をスキップします。</p> <p>[Encryption rule] : メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、「TLS 接続を暗号化の代わりに使用」(P.12-11) を参照してください。</p> <p>[Encryption Profile] : 指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco IronPort 暗号化アプライアンスまたはホステッド キー サービスで使用されます。</p> <p>[Subject] : 暗号化されたメッセージの件名です。デフォルトでは、この値は、\$Subject です。</p>
Bounce (Final Action)	<p>メッセージを送信者に戻します。</p>

表 6-4 コンテンツ フィルタのアクション (続き)

アクション	説明
Skip Remaining Content Filters (Final Action)	メッセージを次の処理段階に配信し、その後の任意のコンテンツ フィルタをスキップします。設定に応じて、メッセージが受信者に配信されるか、検疫が実行されるか、感染フィルタによるスキャンが開始されます。
Drop (Final Action)	メッセージをドロップして廃棄します。

図 6-3 GUI のコンテンツ フィルタのアクション



アクション変数

コンテンツ フィルタにより処理されるメッセージに追加されるヘッダーには、アクション実行時にオリジナル メッセージの情報に自動的に置換される変数を含めることができます。これらの特殊変数は、アクション変数と呼ばれます。Cisco IronPort アプライアンスでは、次のアクション変数のセットをサポートしています。

表 6-5 アクション変数

変数	構文	説明
All Headers	<code>\$AllHeaders</code>	メッセージ ヘッダーに置き換えられます。
Body Size	<code>\$BodySize</code>	メッセージのサイズ (バイト単位) に置き換えられます。
Date	<code>\$Date</code>	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
Dropped File Name	<code>\$dropped_filename</code>	直近にドロップされたファイル名のみを返します。

表 6-5 アクション変数 (続き)

変数	構文	説明
Dropped File Names	\$dropped_filenames	\$filenames と同様に、ドロップされたファイルのリストを表示します。
Dropped File Types	\$dropped_filetypes	\$filetypes と同様に、ドロップされたファイル タイプのリストを表示します。
Envelope Sender	\$envelopefrom or \$envelopesender	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
Envelope Recipients	\$EnvelopeRecipients	メッセージのエンベロープ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
File Names	\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
File Sizes	\$filesizes	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。
File Types	\$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
Filter Name	\$FilterName	処理されるフィルタの名前に置き換えられます。
GMTTimeStamp	\$GMTTimeStamp	現在の時刻および日付 (GMT) に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
HAT Group Name	\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。

表 6-5 アクション変数 (続き)

変数	構文	説明
Mail Flow Policy	<code>\$Policy</code>	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
Matched Content	<code>\$MatchedContent</code>	コンテンツ スキャン フィルタをトリガーした 1 つ以上の値に置き換えられます。Matched Content は、コンテンツ ディクショナリ マッチング、スマート ID または正規表現マッチングにすることができます。
Header	<code>\$Header['string']</code>	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
Hostname	<code>\$Hostname</code>	Cisco IronPort アプライアンスのホスト名に置き換えられます。
Internal Message ID	<code>\$MID</code>	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822 「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
Receiving Listener	<code>\$RecvListener</code>	メッセージを受信したリスナーのニックネームに置き換えられます。
Receiving Interface	<code>\$RecvInt</code>	メッセージを受信したインターフェイスのニックネームに置き換えられます。

表 6-5 アクション変数 (続き)

変数	構文	説明
Remote IP Address	<code>\$RemoteIP</code>	メッセージを Cisco IronPort アプリアンスに送信したシステム IP アドレスに置き換えられます。
Remote Host Address	<code>\$remotehost</code>	メッセージを Cisco IronPort アプリアンスに送信したシステムのホスト名に置き換えられます。
SenderBase Reputation Score	<code>\$Reputation</code>	送信者の SenderBase 評価スコアに置き換えられます。評価スコアがない場合は「None」に置き換えられます。
Subject	<code>\$Subject</code>	メッセージの件名に置き換えられます。
Time	<code>\$Time</code>	現在の時刻 (ローカル時間帯) に置き換えられます。
Timestamp	<code>\$Timestamp</code>	現在の時刻および日付 (ローカル時間帯) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

実際の例 (GUI)

この例では、次のタスクを示し、電子メール セキュリティ マネージャの機能について説明します。

- ステップ 1** デフォルトの着信メール ポリシーのアンチスパム、アンチウイルス、感染フィルタおよびコンテンツ フィルタを編集します。
- ステップ 2** 販売部とエンジニアリング部の異なるユーザのセットに 2 つの新しいポリシーを追加して、それぞれに異なる電子メール セキュリティ設定を指定します。
- ステップ 3** [Incoming Mail Overview policy] テーブルで使用する 3 つの新しいコンテンツ フィルタを作成します。
- ステップ 4** ポリシーをもう一度編集して、コンテンツ フィルタをグループによってイネーブルまたはディセーブルにします。

この例では、受信者によって異なる電子メールセキュリティマネージャのアンチスパム、アンチウイルス、感染フィルタおよびコンテンツフィルタの設定を管理できる、機能と柔軟性を示しています。また、これらの機能は、メールポリシーとコンテンツフィルタのアクセス権限を持つ「Policy Administrator」というカスタムユーザロールに割り当てられています。アンチスパム、アンチウイルスおよび感染フィルタ、委任管理の機能の詳細については、次の章を参照してください。

- 「アンチスパム」(P.8-1)
- 「アンチウイルス」(P.9-1)
- 「感染フィルタ」(P.10-1)
- 『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」

電子メール セキュリティ マネージャへのアクセス

新しくインストールされた、またはアップグレードされたシステムでは、[Mail Policies] タブをクリックして、電子メールセキュリティマネージャにアクセスします。デフォルトでは、[Incoming Mail Policies] テーブルが表示されます。

新規システムでは、System Setup Wizard のすべての手順を完了して、IronPort Anti-Spam、Sophos または McAfee Anti-Virus および感染フィルタをイネーブルにするように選択した場合、[図 6-4](#) のような [Incoming Mail Policies] ページが表示されます。

デフォルトでは、これらの設定は、デフォルトの着信メールポリシーでイネーブルにされます。

- アンチスパム (IronPort スпам検査がイネーブルの場合) : イネーブル
 - 陽性と判定されたスパム : 検査、メッセージの件名が追加
 - 陽性と疑わしいスパム : 検査、メッセージの件名が追加
 - マーケティング電子メール : スキャンはイネーブルにされない
- アンチスパム (IronPort スпам検査がイネーブルではない場合) : イネーブル
 - 陽性と判定されたスパム : 配信、メッセージの件名が追加
 - 陽性と疑わしいスパム : 配信、メッセージの件名が追加
 - マーケティング電子メール : スキャンはイネーブルにされない

- アンチウイルス：イネーブル、ウイルスのスキャンおよび修復、アンチウイルス スキャン結果が X-Header に追加
 - 修復されたメッセージ：配信、メッセージの件名が追加
 - 暗号化されたメッセージ：配信、メッセージの件名が追加
 - スキャンできないメッセージ：配信、メッセージの件名が追加
 - ウイルスに感染したメッセージ：ドロップ
- 感染フィルタ：イネーブル
 - ファイル拡張子は予測されない
 - ウイルス感染が疑われる添付ファイルの付いたメッセージの保持期間は 1 日
 - メッセージの変更はイネーブルにされない
- コンテンツ フィルタ：ディセーブル

図 6-4 [Incoming Mail Policies] ページ：新規アプライアンスのデフォルト Incoming Mail Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Uncancellable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

Key: Default Custom Ready



(注)

この例では、着信メール ポリシーは、IronPort スпам検疫がイネーブルにされている場合のデフォルトのアンチスパム設定を使用します。

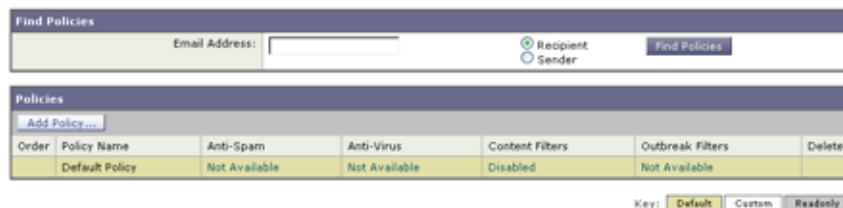
[Enabled]、[Disabled]、[Not Available]

[Email Security Manager] テーブル（着信または発信のいずれか）の列は、各ポリシー名のセキュリティ サービスの状態のリンクを表示します。サービスがイネーブルの場合、単語 [Enabled] またはコンフィギュレーションの要約が表示されます。同様に、サービスがディセーブルの場合、単語 [Disabled] が表示されます。

サービスのライセンス契約書に同意していない場合、またはサービスの有効期限が切れている場合、リンクとして [Not Available] が表示されます。この場合、[Not Available] リンクをクリックすると、[Security Services] タブ内に、サービスのポリシー単位の設定を指定できるページではなく、グローバル ページが表示されます。ページが別のタブに変わったことを示す警告が表示されます。

図 6-5 を参照してください。

図 6-5 使用できないセキュリティ サービス
Incoming Mail Policies



デフォルト ポリシーの編集：アンチスパム設定

電子メール セキュリティ マネージャの各行は、異なるポリシーを表します。各列は、異なるセキュリティ サービスを表します。

- デフォルト ポリシーを編集するには、電子メール セキュリティ マネージャの着信または発信メール ポリシー テーブルの下部の行にあるセキュリティ サービスの任意のリンクをクリックします。

この例では、着信メールのデフォルト ポリシーのアンチスパム設定をより積極的に変更します。デフォルト値では、陽性と判定されたスパム メッセージおよび陽性と疑わしいスパム メッセージが検疫され、マーケティング電子メールのスキャンがディセーブルになります。次に、陽性と判定されたスパムがドロップされるように設定を変更する例を示します。陽性と疑わしいスパムは引き続き検疫されます。マーケティング電子メールのスキャンは、イネーブルにされ、マーケティング メッセージは目的の受信者に配信されます。マーケティング メッセージの件名には、テキスト [MARKETING] が前に追加されます。

- ステップ 1** アンチスパム セキュリティ サービスのリンクをクリックします。図 6-6 に示す [Anti-Spam Settings] ページが表示されます。



(注) デフォルトのセキュリティ サービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。**[Disable]** をクリックして、サービスをディセーブルにできます。

ステップ 2 **[Positively Identified Spam Settings]** セクションでは、**[Action to apply to this message]** を **[Drop]** に変更します。

ステップ 3 **[Marketing Email Settings]** セクションでは、**[Yes]** をクリックして、マーケティング電子メールのスキャンをイネーブルにします。

イネーブルにされている場合、デフォルト アクションでは、テキスト **[MARKETING]** が件名の前に追加され、問題のないマーケティングメッセージが配信されます。

[Add text to message] フィールドでは、US-ASCII 文字だけを使用できます。

ステップ 4 **[Submit]** をクリックします。**[Incoming Mail Policies table]** ページが再表示されます。アンチスパム セキュリティ サービスの要約リンクが変更され、新しい値が反映されているため注意してください。

前述の手順と同様、デフォルト ポリシーのデフォルト アンチウイルスおよびウイルス感染フィルタ設定を変更できます。

図 6-6 [Anti-Spam Settings] ページ
Mail Policies: Anti-Spam

新しいポリシーの作成

この例では、販売部（メンバーは LDAP 受け入れクエリーにより定義されます）用とエンジニアリング部用の 2 つの新しいポリシーを作成します。両方のポリシーが Policy Administrator カスタム ユーザ ロールに割り当てられ、このロールに属する委任管理者にこれらのポリシーを管理する責任が付与されます。次に、それぞれに異なる電子メールセキュリティ設定を設定します。

- ステップ 1** [Add Policy] ボタンをクリックして、新しいポリシーの作成を開始します。
[Add Users] ページが表示されます。
- ステップ 2** 一意な名前を定義して、(必要な場合) ポリシーの順序を調整します。
ポリシーの名前は、定義されるメール ポリシー テーブル（着信または発信のいずれか）で一意でなければなりません。

各受信者は、適切なテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。詳細については、「[First Match Wins](#)」(P.6-5) を参照してください。

ステップ 3 [Editable by (Roles)] リンクをクリックし、メール ポリシーの管理を担当する委任管理者のカスタム ユーザ ロールを選択します。

リンクをクリックすると、メール ポリシーの編集権限を持つ委任管理者のカスタム ロールが表示されます。委任管理者は、ポリシーのアンチスパム、アンチウイルス、および感染フィルタ設定を編集できるとともに、ポリシーのコンテンツ フィルタをイネーブルまたはディセーブルにできます。オペレータと管理者だけがメール ポリシーの名前、またはその送信者、受信者、グループを変更できます。メール ポリシーにはメール ポリシーに対する完全なアクセス権を持つカスタム ユーザ ロールが自動的に割り当てられます。

委任管理の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」の章を参照してください。

ステップ 4 ポリシーのユーザを定義します。

ユーザが、送信者または受信者のいずれであるかを定義します（詳細については、「[ポリシー マッチング](#)」(P.6-4) を参照してください）。[図 6-7](#) では、着信メール ポリシーの受信者および発信メール ポリシーの送信者というデフォルト形式を示しています。

ポリシーのユーザは、次の方法で定義できます。

- 完全な電子メール アドレス : user@example.com
- 電子メール アドレスの一部 : user@
- ドメインのすべてのユーザ : @example.com
- 部分ドメインのすべてのユーザ : @.example.com
- LDAP クエリーとのマッチング



(注) ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 Joe@ を入力した場合、joe@example.com に送信されるメッセージが一致します。

ユーザ情報を、たとえば Microsoft Active Directory、SunONE Directory Server（以前の「iPlanet Directory Server」）または Open LDAP ディレクトリなど、ネットワーク インフラストラクチャの LDAP ディレクトリ内に保存する場合、Cisco IronPort アプライアンスを設定して、LDAP サーバをク

エリーし、受信者アドレスの受け取り、代替アドレスまたはメール ホスト、あるいはその両方へのメッセージのリルーティング、ヘッダーのマスカレード、メッセージに特定のグループの受信者または送信者があるかどうかの判別を行うことができます。

アプライアンスをこのように設定した場合、設定したクエリーを使用して、電子メール セキュリティ マネージャのメール ポリシーのユーザを定義できます。

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。

図 6-7 ポリシーのユーザの定義
Add Incoming Mail Policy

ステップ 5 [Add] ボタンをクリックして、[Current Users] リストにユーザを追加します。

ポリシーには、送信者、受信者および LDAP クエリーを組み合わせる含めることができます。

[Remove] ボタンを使用すると、定義されているユーザを現在のユーザのリストから削除できます。

ステップ 6 ユーザの追加が完了したら、[Submit] をクリックします。

新しいポリシーが追加された状態で [Mail Policies] ページが表示されます。ポリシーを最初に追加する場合、すべてのセキュリティ サービス設定では、デフォルト値が使用されるため注意してください。

図 6-8 新しく追加されたポリシー：販売グループ

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

ステップ 7 [Add Policy] ボタンをもう一度クリックして、別の新しいポリシーを追加します。

このポリシーでは、エンジニアリング チームのメンバーの各電子メール アドレスが定義されます。

図 6-9 エンジニアリング チームのポリシーの作成
Add Incoming Mail Policy

Add Policy

Policy Name: (e.g. my IT policy)

Editable by (Roles):

Insert Before Policy:

Add Users

Sender

Recipient ?

Email Address(es)

bob@example.com
 mary@example.com
 fred@example.com

(e.g. user@example.com, user@, @example.com, @example.com)

LDAP Group Query

Query:

Group:

Current Users

Recipient: bob@example.com
 Recipient: mary@example.com
 Recipient: fred@example.com

Cancel
Submit

ステップ 8 エンジニアリング ポリシーのユーザの追加が完了したら、[Submit] をクリックします。

新しいポリシーが追加された状態で [Mail Policies] ページが表示されます。
 図 6-10 を参照してください。

ステップ 9 変更を確定します。

図 6-10 新しく追加されたポリシー：エンジニアリング チーム

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	(use default)	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	



(注)

この時点では、新しく作成された両方のポリシーに、デフォルト ポリシーで使用される同じ設定が適用されています。いずれかのポリシーのユーザへのメッセージが一致しますが、メール処理設定は、デフォルト ポリシーと同じです。そのため、「Sales_Group」または「Engineering」ポリシーのユーザと一致するメッセージは、デフォルト ポリシーと同様に処理されます。

[Default]、[Custom]、[Disabled]

テーブル下部のキーは、特定のポリシーのセルのカラー コーディングが、デフォルト行に定義されているポリシーとどのように関係するかを示しています。

Key: Default Custom Disabled

- イエローのシェーディングは、ポリシーがデフォルト ポリシーと同じ設定を使用していることを示します。
- シェーディングなし（ホワイト）は、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。
- グレーのシェーディングは、セキュリティ サービスがポリシーでディセーブルにされていることを示します。

カスタム ポリシーの作成

この例では、前述の項で作成した 2 つのポリシーを編集します。

- 販売グループでは、アンチスパム設定をデフォルト ポリシーよりも積極的になるように変更します（「[デフォルト ポリシーの編集：アンチスパム設定](#)」(P.6-34) を参照)。陽性と識別されたスパム メッセージをドロップするデフォルト ポリシーが使用されます。ただし、この例では、IronPort スпам 検疫エリアに送信されるように、マーケティング メッセージの設定を変更します。

この積極的なポリシーでは、販売チームの受信トレイに送信される不要なメッセージが最小限に押さえられます。

アンチスパム設定の詳細については、「[アンチスパム](#)」(P.8-1) を参照してください。

- エンジニアリング チームでは、example.com のリンクを除く、疑わしいメッセージに含まれる URL を変更するように、感染フィルタ機能の設定をカスタマイズします。拡張子「dwg」の付いた添付ファイルを感染フィルタのスキップでバイパスします。

感染フィルタの設定の詳細については、「[感染フィルタ](#)」(P.10-1) を参照してください。

販売チーム ポリシーのアンチスパム設定を編集するには、次の手順を実行します。

- ステップ 1** 販売ポリシー行のアンチスパム セキュリティ サービス ([Anti-Spam]) 列のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は [(use default)] です。

図 6-11 販売チーム ポリシーのアンチスパム設定の編集

Order	Policy Name	Anti-Spam
1	Sales_Team	(use default)
2	Engineering	(use default)
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver

アンチスパムの設定ページが表示されます。

- ステップ 2** アンチスパム セキュリティ サービス ページで、[Enable Anti-Spam Scanning for this Policy] の値を [Use Default Settings] から [Use IronPort Anti-Spam service] に変更します。

[Use IronPort Anti-Spam service] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

- ステップ 3** [Positively-Identified Spam Settings] セクションで、[Apply This Action to Message] を [Drop] に変更します。
- ステップ 4** [Suspected Spam Settings] セクションで、[Yes] をクリックして、陽性と疑わしいスパムのスキャンをイネーブルにします。
- ステップ 5** [Suspected Spam Settings] セクションで、[Apply This Action to Message] を [Spam Quarantine] に変更します。



(注) [IronPort Spam Quarantine] を選択すると、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章で定義されている設定に従って、メールが転送されます。

- ステップ 6** [Add text to subject] フィールドで、[None] をクリックします。
- IronPort スпам検査エリアに配信されるメッセージには、件名タグが追加されません。
- ステップ 7** [Marketing Email Settings] セクションで、[Yes] をクリックして、問題のない送信元からのマーケティングメールのスキャンをイネーブルにします。
- ステップ 8** [Apply This Action to Message] セクションで、[Spam Quarantine] を選択します。
- ステップ 9** 変更を送信して確定します。

販売ポリシーの変更が反映された状態で、[Incoming Mail Policies] ページが表示されます。図 6-12 を参照してください。このシェーディングは、ポリシーがデフォルトポリシーとは異なる設定を使用していることを示します。

図 6-12 変更された販売グループのポリシーのアンチスパム設定

Policies		
Order	Policy Name	Anti-Spam
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine
2	Engineering	(use default)
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver

この時点では、スパムの疑いがあり、その受信者が販売チーム ポリシーで定義されている LDAP クエリーと一致するメッセージは、IronPort スпам検疫エリアに配信されます。

エンジニアリング チーム ポリシーの感染フィルタ設定を編集するには、次の手順を実行します。

ステップ 1 エンジニアリング ポリシー行の感染フィルタ機能セキュリティ サービス ([Outbreak Filters] 列) のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は [(use default)] です。

図 6-13 エンジニアリング チーム ポリシーの感染フィルタ機能設定の編集

Policies						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

ステップ 2 感染フィルタ機能セキュリティ サービス ページで、ポリシーのスキャン設定を [Enable Outbreak Filtering (Customize settings)] に変更します。

ここで [(Customize settings)] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

また、別の設定を選択できるようにページの残りの部分のコンテンツがイネーブルになります。

ステップ 3 ページの [Bypass Attachment Scanning] セクションで、ファイル拡張子フィールドに `dwg` と入力します。

ファイル拡張子「.dwg」は、Cisco IronPort アプライアンスが添付ファイルのスキャン時にフィンガープリントにより認識できる既知のファイル タイプのリストにはありません。



(注) 3 文字のファイル拡張子の前にピリオド (.) を入力する必要はありません。

ステップ 4 [Add Extension] をクリックして、.dwg ファイルを感染フィルタ機能スキャンをバイパスするファイル拡張子のリストに追加します。

ステップ 5 [Enable Message Modification] をクリックします。

メッセージの変更をイネーブルにすると、アプライアンスは、フィッシングや詐欺などの対象とする脅威や、疑わしいか悪意のある Web サイトへのリンクがないかをスキャンします。その Web サイトにアクセスしようとする、アプライアンスはメッセージのリンクを書き換えて、シスコのセキュリティ プロキシを経由するようにリダイレクトします。



(注) 感染フィルタが対象とする非ウイルス性の脅威をスキャンするには、メール ポリシーでアンチスパム スキャンをイネーブルにする必要があります。

ステップ 6 [Enable for Unsigned Messages] を選択します。

これによりアプライアンスは署名されたメッセージの URL の書き換えが可能になります。他のメッセージ変更の設定および非ウイルス性の脅威として検出されたメッセージが解放されるまで検疫に保持される期間を指定できるように、URL の書き換えをイネーブルにする必要があります。この例ではデフォルトの保持期間の 4 時間を使用します。

ステップ 7 [Bypass Domain Scanning] フィールドに example.com と入力します。

example.com へのリンクは変更されません。

ステップ 8 [Threat Disclaimer] として [System Generated] を選択します。

メッセージ本文の上にメッセージの内容について警告する免責事項を挿入できます。この例では、システムが生成する脅威の免責事項を使用します。

図 6-14 感染フィルタ設定
Mail Policies: Outbreak Filters

The screenshot shows the configuration interface for Outbreak Filters. It is divided into three main sections:

- Outbreak Filtering for Policy: Sales_Team**: Includes a dropdown menu to 'Enable Outbreak Filtering (Customize settings)'.
- Outbreak Filter Settings**:
 - Quarantine Threat Level: 3
 - Maximum Quarantine Retention:
 - Viral Attachments: 1 Days
 - Other Threats: 4 Hours
 - Bypass Attachment Scanning:
 - Select File Extension: (empty)
 - File Extensions to Bypass: None defined
 - Add Extension button
- Message Modification**:
 - Enable Message Modification:
 - Message Modification Threat Level: 3
 - Message Subject: Prepend [MODIFIED FOR PROTECTION]
 - URL Rewriting:
 - Cisco Security proxy scans and rewrites suspicious or malicious URLs.
 - Enable only for unsigned messages (recommended)
 - Enable for all messages
 - Disable
 - Bypass Domain Scanning:
 - example.com
 - (examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24)
 - Threat Disclaimer: System Generated

Buttons for 'Cancel' and 'Submit' are located at the bottom of the form.

ステップ 9 変更を送信して確定します。

エンジニアリング ポリシーの変更が反映された状態で、[Incoming Mail Policies] ページが表示されます。図 6-15 を参照してください。このシェーディングは、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。

図 6-15 変更されたエンジニアリング ポリシーのウイルス フィルタ設定

Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	🗑️
2	Engineering	(use default)	(use default)	(use default)	Retention Time: Virus: 1 day Other: 4 hours	🗑️
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

この時点では、ファイル拡張子が `dwg` である添付ファイルを含む任意のメッセージ、および受信者がエンジニアリング チーム ポリシーで定義されている受信者とマッチングする任意のメッセージは、感染フィルタ スキャンをバイパスし、処理を続行します。`example.com` ドメインへのリンクを含むメッセージは、疑わしいとはみなされず、シスコのセキュリティ プロキシを経由してリダイレクトするリンクの変更は行われません。

電子メール セキュリティ マネージャのポリシーのユーザの検索

[Find Policies] ボタンを使用して、[Email Security Manager Incoming] または [Outgoing Mail Policies] ページで定義されているポリシーですでに定義されているユーザを検索します。

たとえば、`joe@example.com` と入力して、[Find Policies] ボタンをクリックすると、ポリシーとマッチングする特定の定義済みユーザを含むポリシーを示す結果が表示されます。

図 6-16 ポリシーでのユーザの検索

The screenshot shows the 'Find Policies' interface. At the top, there is a search bar with 'Email Address: bob@example.com' and a 'Find Policies' button. Below the search bar, the results are displayed: 'Email Address: "Recipient: bob@example.com" is defined in the following policies: Engineering, Default Policy (all users)'. Below the results, there is a table titled 'Policies matching "bob@example.com"'. The table has columns for Order, Policy Name, Anti-Spam, Anti-Virus, Content Filters, Outbreak Filters, and Delete. The table contains two rows: one for 'Engineering' and one for 'Default Policy'.

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
2	Engineering	(use default)	(use default)	(use default)	Retention Time: Virus: 1 day Other: 4 hours	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

ポリシーの名前をクリックして、[Edit Policy] ページに移動してそのポリシーのユーザを編集します。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

電子メール セキュリティ マネージャ : 管理例外

前述の 2 つの例で示されている手順を使用して、*管理例外*に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルト ポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザ グループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。表 6-6 (P.6-48) に、ポリシーの例をいくつか示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達す

るスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、false positive を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 6-6 積極的および保守的な電子メール セキュリティ マネージャ設定

	積極的な設定	保守的な設定
アンチスパム	陽性と判定されたスパム：ドロップ 陽性と疑わしいスパム：検疫 マーケティング メール：メッセージの件名の前に「[Marketing]」が追加されて配信	陽性と判定されたスパム：検疫 陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信 マーケティング メール：ディセーブル
アンチウイルス	修復されたメッセージ：配信 暗号化されたメッセージ：ドロップ スキャンできないメッセージ：ドロップ 感染メッセージ：ドロップ	修復されたメッセージ：配信 暗号化されたメッセージ：検疫 スキャンできないメッセージ：検疫 感染メッセージ：ドロップ
ウイルスフィルタ	イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし すべてのメッセージのメッセージ変更をイネーブルにする	イネーブル、特定のファイル名拡張子またはドメインがバイパス可能 未署名メッセージのメッセージ変更をイネーブルにする

新しいコンテンツ フィルタの作成

この例では、[Incoming Mail Policy] テーブルで使用される新しいコンテンツ フィルタを 3 つ作成します。これらすべてのコンテンツ フィルタは、Policy Administration カスタム ユーザ ロールに属する委任管理者が編集できます。次のフィルタを作成します。

ステップ 1 「scan_for_confidential」

このフィルタは、文字列「**confidential**」が含まれているかメッセージをスキャンします。文字列が見つかり、メッセージのコピーが電子メールエイリアス hr@example.com に送信され、メッセージが **Policy** 検疫エリアに送信されます。

ステップ 2 「no_mp3s」

このフィルタは、MP3 添付ファイルを削除し、MP3 ファイルが削除されたことを受信者に通知します。

ステップ 3 「ex_employee」

このコンテンツ フィルタは、特定のエンベロープ受信者アドレス（元受信者）に送信されるメッセージをスキャンします。メッセージが一致した場合、特定の通知メッセージがメッセージ送信者に送信され、メッセージがバウンスされます。

コンテンツ フィルタを作成したら、各ポリシー（デフォルト ポリシーを含む）を設定して、異なる組み合わせで特定のコンテンツ フィルタをイネーブルにします。

Confidential のスキャン

最初の例のコンテンツ フィルタには、1 つの条件と 2 つのアクションが含まれます。コンテンツ フィルタを作成するには、次の手順を実行します。

ステップ 1 [Mail Policies] タブをクリックします。

ステップ 2 [Incoming Content Filters] をクリックします。

[Incoming Content Filters] ページが表示されます。新しくインストールされたシステムまたはアップグレードされたシステムの場合、デフォルトで、コンテンツ フィルタは定義されていません。

図 6-17 [Incoming Content Filters] ページ
Incoming Content Filters



ステップ 3 [Add Filter] ボタンをクリックします。

[Add Content Filter] ページが表示されます。

- ステップ 4** [Name] フィールドに、新しいフィルタの名前として `scan_for_confidential` と入力します。

フィルタ名には、ASCII 文字、数字、下線またはダッシュを含めることができます。コンテンツ フィルタ名の最初の文字は、文字または下線でなければなりません。

- ステップ 5** [Editable By (Roles)] リンクをクリックし、[Policy Administrator] を選択し、[OK] をクリックします。

Policy Administrator ユーザ ロールに属する委任管理者がメール ポリシーでこのコンテンツ フィルタを編集して使用できます。

- ステップ 6** [Description] フィールドに、説明を入力します。たとえば、`scan all incoming mail for the string 'confidential'` と入力します。

- ステップ 7** [Add Condition] をクリックします。

- ステップ 8** [Message Body] を選択します。

- ステップ 9** [Contains text:] フィールドに `confidential` と入力して、[OK] をクリックします。

[Add Content Filter] ページに、追加される条件が表示されます。

- ステップ 10** [Add Action] をクリックします。

- ステップ 11** [Send Copy To (Bcc:)] を選択します。

- ステップ 12** [Email Addresses] フィールドに、`hr@example.com` と入力します。

- ステップ 13** [Subject] フィールドに、`[message matched confidential filter]` と入力します。

- ステップ 14** [OK] をクリックします。

[Add Content Filter] ページに、追加されるアクションが表示されます。

- ステップ 15** [Add Action] をクリックします。

- ステップ 16** [Quarantine] を選択します。

- ステップ 17** ドロップダウンメニューで、[Policy quarantine area] を選択します。

- ステップ 18** [OK] をクリックします。

[Add Content Filter] ページに、追加される 2 番目のアクションが表示されます。

- ステップ 19** 変更を送信して確定します。

この時点では、コンテンツ フィルタは、いずれの着信メール ポリシーでもイネーブルになっていません。この例では、新しいコンテンツ フィルタをマスター リストに追加しただけの状態です。このコンテンツ フィルタは、いずれのポリシーにも適用されていないため、電子メール セキュリティ マネージャによる電子メール処理は、このフィルタの影響を受けません。

MP3 添付ファイルなし

2 番めの例のコンテンツ フィルタには、条件はなく、アクションは 1 つ含まれます。2 番めのコンテンツ フィルタを作成するには、次の手順を実行します。

- ステップ 1** [Add Filter] ボタンをクリックします。
[Add Content Filter] ページが表示されます。
- ステップ 2** [Name] フィールドに、新しいフィルタの名前として `no_mp3s` と入力します。
- ステップ 3** [Editable By (Roles)] リンクをクリックし、[Policy Administrator] を選択し、[OK] をクリックします。
- ステップ 4** [Description] フィールドに、説明を入力します。たとえば、`strip all MP3 attachments` と入力します。
- ステップ 5** [Add Action] をクリックします。
- ステップ 6** [Strip Attachment by File Info] を選択します。
- ステップ 7** [File type is] を選択します。
- ステップ 8** ドロップダウン フィールドで、`[-- mp3]` を選択します。
- ステップ 9** 必要な場合、置換メッセージを入力します。
- ステップ 10** [OK] をクリックします。
[Add Content] ページに、追加されるアクションが表示されます。
- ステップ 11** 変更を送信して確定します。



(注)

コンテンツ フィルタを作成するときに条件を指定する必要はありません。条件が定義されていない場合、定義されるアクションは常にルールに適用されます (条件を指定しないことは、`true()` メッセージ フィルタ ルールを使用することと同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます)。

元従業員

3 番目のコンテンツ フィルタを作成するには、次の手順を実行します。

-
- ステップ 1** [Add Filter] ボタンをクリックします。
[Add Content Filter] ページが表示されます。
 - ステップ 2** [Name:] フィールドに、新しいフィルタの名前として `ex_employee` と入力します。
 - ステップ 3** [Editable By (Roles)] リンクをクリックし、[Policy Administrator] を選択し、[OK] をクリックします。
 - ステップ 4** [Description:] フィールドに、説明を入力します。たとえば、`bounce messages intended for Doug` と入力します。
 - ステップ 5** [Add Condition] をクリックします。
 - ステップ 6** [Envelope Recipient] を選択します。
 - ステップ 7** エンベロープ受信者に対して、[Begins with] を選択して、`doug@` と入力します。
 - ステップ 8** [OK] をクリックします。
[Content Filters] ページがリフレッシュされ、追加された条件が表示されず。元従業員の電子メール アドレスを含む LDAP ディレクトリを作成できます。元従業員がそのディレクトリに追加されると、このコンテンツ フィルタは、動的に更新されます。
 - ステップ 9** [Add Action] をクリックします。
 - ステップ 10** [Notify] を選択します。
 - ステップ 11** [Sender] チェックボックスを選択して、[Subject] フィールドに、`message bounced for ex-employee of example.com` と入力します。
 - ステップ 12** [Use template] セクションで、通知テンプレートを選択します。



(注) リソースが事前に定義されていないため、コンテンツ フィルタ ルールビルダのいくつかのセクションは、ユーザ インターフェイスに表示されません。たとえば、コンテンツ ディクショナリ、通知テンプレートおよびメッセージ免責事項は、[Mail Policies] > [Dictionaries] ページ（または CLI の dictionaryconfig コマンド）から事前に設定されていない場合、オプションとして表示されません。ディクショナリの作成の詳細については、「[コンテンツ ディクショナリ](#)」(P.14-3) を参照してください。

ステップ 13 [OK] をクリックします。

[Add Content Filters] ページに、追加されるアクションが表示されます。

ステップ 14 [Add Action] をクリックします。

ステップ 15 [Bounce (Final Action)] を選択して、[OK] をクリックします。

コンテンツ フィルタに指定できる最終アクションは 1 つだけです。複数の最終アクションを追加しようとする、GUI にエラーが表示されます。

このアクションを追加すると、この元従業員へのメッセージの送信者が、通知テンプレートとバウンス通知テンプレートの 2 つのメッセージを受け取る可能性があります。

ステップ 16 変更を送信して確定します。

[Incoming Content Filters] ページが表示され、新しく追加されたコンテンツ フィルタが表示されます。

個々のポリシーへのコンテンツ フィルタのイネーブル化および適用

前述の例では、[Incoming Content Filters] ページを使用して、3 つのコンテンツ フィルタを作成しました。[Incoming Content Filters] および [Outgoing Content filters] ページには、ポリシーに適用できるすべてのコンテンツ フィルタの「マスター リスト」が含まれます。

図 6-18 [Incoming Content Filters] : 作成された 3 つのフィルタ
Incoming Content Filters

Filters					
Add Filter...					
Order	Filter Name	Description Rules Policies	Duplicate	Delete	
1	scan_for_confidential	scan all incoming mail for the string 'confidential'			
2	no_mp3s	strip all MP3 attachments			
3	ex_employee	bounce messages intended for Doug			

この例では、[Incoming Mail Policy] テーブルで使用される新しいコンテンツフィルタを 3 つ適用します。

- デフォルト ポリシーには、3 つすべてのコンテンツ フィルタが適用されます。
- エンジニアリング グループには、no_mp3s フィルタは適用されません。
- 販売グループには、デフォルト着信メール ポリシーとしてコンテンツ フィルタが適用されます。

リンクをクリックして、個々のポリシーに対してコンテンツ フィルタをイネーブルにして選択します。デフォルト着信メール ポリシーを編集するには、次の手順を実行します。

ステップ 1 [Incoming Mail Policies] をクリックして、[Incoming Mail Policy] テーブルに戻ります。

ページがリフレッシュされ、デフォルト ポリシーおよび「新しいポリシーの作成」(P.6-36) で追加した 2 つのポリシーが表示されます。コンテンツ フィルタリングは、デフォルトでは、すべてのポリシーでディセーブルにされているため注意してください。

ステップ 2 デフォルト ポリシー行のコンテンツ フィルタ セキュリティ サービス ([Content Filters] 列) のリンクをクリックします。図 6-19 を参照してください。

図 6-19 デフォルト着信メール ポリシーのコンテンツ フィルタ設定の編集

Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	(use default)	Retention Time: Virus: 1 day Other: 4 hours	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

ステップ 3 コンテンツ フィルタ セキュリティ サービス ページで、[Content Filtering for Default Policy] の値を [Disable Content Filters] から [Enable Content Filters (Customize settings)] に変更します。

図 6-20 ポリシーでのコンテンツ フィルタのイネーブル化および特定のコンテンツ フィルタの選択

Mail Policies: Content Filters

Content Filtering for: Default Policy

Enable Content Filters (Customize settings) ▼

Enable Content Filters (Customize settings)

Disable Content Filters

Order	Filter Name	Description	Enable
1	scan_for_confidential	scan all incoming mail for the string 'confidential'	<input type="checkbox"/>
2	no_mp3s	strip all MP3 attachments	<input type="checkbox"/>
3	ex_employee	bounce messages intended for Doug	<input type="checkbox"/>

Cancel Submit

マスター リストで定義されているコンテンツ フィルタ ([Incoming Content Filters] ページを使用して「コンテンツ フィルタの概要」(P.6-10) で作成されたフィルタ) が、このページに表示されます。値を [Enable Content Filters (Customize settings)] に変更すると、各フィルタのチェックボックスがディセーブル (グレー表示) からイネーブルに変わります。

ステップ 4 各コンテンツ フィルタの [Enable] チェックボックスをオンにします。

ステップ 5 [Submit] をクリックします。

[Incoming Mail Policies] ページが表示され、テーブルが更新され、デフォルト ポリシーでイネーブルにされているフィルタの名前が示されます。

図 6-21 デフォルト着信メール ポリシーでイネーブルにされた 3 つのコンテンツ フィルタ

Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	scan_for_confidential no_mp3s ex_employee
----------------	---	--	---

「エンジニアリング」ポリシーの「no_mp3s」コンテンツ フィルタをディセーブルにするには、次の手順を実行します。

- ステップ 1** エンジニアリング チーム ポリシー行の [Content Filters security service] ([Content Filters] 列) のリンクをクリックします。
- ステップ 2** コンテンツ フィルタ セキュリティ サービス ページで、[Content Filtering for Policy: Engineering] の値を [Enable Content Filtering (Inherit default policy settings)] から [Enable Content Filters (Customize settings)] に変更します。
- このポリシーはデフォルト値を使用していたため、値を [Use Default Settings] から [Yes] に変更すると、各フィルタのチェックボックスがディセーブル (グレー表示) からイネーブルに変わります。
- ステップ 3** 「no_mp3s」 フィルタのチェックボックスの選択を解除します。

図 6-22 コンテンツ フィルタの選択解除
Mail Policies: Content Filters



- ステップ 4** [Submit] をクリックします。

[Incoming Mail Policies] ページが表示され、テーブルが更新され、エンジニアリング ポリシーでイネーブルにされているフィルタの名前が示されます。

図 6-23 コンテンツ フィルタが更新された [Incoming Mail Policies]

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	scan_for_confidential ex_employee	Retention Time: Virus: 1 day Other: 4 hours	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	scan_for_confidential no_mp3s ex_employee	Retention Time: Virus: 1 day	

- ステップ 5** 変更を確定します。

この時点では、エンジニアリング ポリシーのユーザリストと一致する着信メッセージで MP3 添付ファイルは削除されません。ただし、他のすべての着信メッセージでは、MP3 添付ファイルが削除されます。

GUI でのコンテンツ フィルタの設定に関する注意事項

- コンテンツ フィルタを作成するときに条件を指定する必要はありません。アクションが定義されていない場合、定義されるアクションは常にルールに適用されます（アクションを指定しないことは、true() メッセージ フィルタ ルールを使用することと同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージが一致します）。
- カスタム ユーザ ロールをコンテンツ フィルタに割り当てていない場合、パブリックのコンテンツ フィルタになり、メール ポリシーの任意の委任管理者が使用できます。委任管理者とコンテンツ フィルタの詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」の章を参照してください。
- 管理者とオペレータは、コンテンツ フィルタがカスタム ユーザ ロールに割り当てられていない場合でも、アプライアンスのすべてのコンテンツ フィルタを表示および編集できます。
- フィルタ ルールおよびアクションのテキストを入力する場合、正規表現照合において、次のメタ文字に特殊な意味があります。^ \$ * + ?{ [] \ | ()

正規表現を使用しない場合、「\」（バックスラッシュ）を使用して、これらの任意の文字をエスケープする必要があります。たとえば、「*Warning*」と入力します。
- コンテンツ フィルタに複数の条件を定義する場合、コンテンツ フィルタが一致したと見なされるために、定義されるアクションのすべて（論理 AND）、または定義されたいずれかのアクション（論理 OR）の適用が必要かどうかを定義できます。

図 6-24 任意またはすべての条件の選択

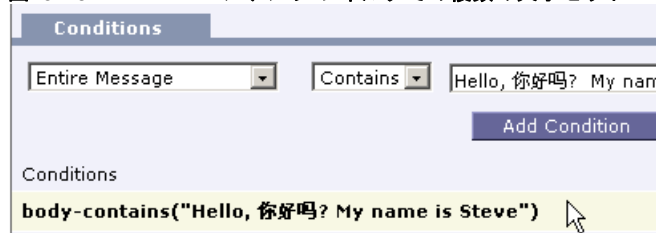
Add Filter	
Name:	<input type="text"/>
Currently used by policies:	
Description:	<input type="text"/>
Order:	5 ▼
Apply filter:	<input checked="" type="radio"/> If one or more conditions match <input type="radio"/> Only if ALL conditions match

- 「benign」コンテンツ フィルタを作成して、メッセージ分裂およびコンテンツ フィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツ フィルタを作成できます。このコンテンツ フィルタは、メール処理に影響を与えませんが、このフィルタを使用して、電子メールセキュリティ マネージャ ポリシー処理が、システムの他の要素（たとえば、メール ログ）に影響を与えているかテストできます。
- 逆に、着信または発信コンテンツ フィルタの「マスター リスト」の概念を使用して、アプライアンスにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツ フィルタを作成できます。このコンテンツ フィルタは次のように作成できます。
 - [Incoming Content Filters] または [Outgoing Content Filters] ページを使用して、順序が 1 の新しいコンテンツ フィルタを作成します。
 - [Incoming Mail Policies] または [Outgoing Mail Policies] ページを使用して、デフォルト ポリシーの新しいコンテンツ フィルタをイネーブルにします。
 - 残りすべてのポリシーでこのコンテンツ フィルタをイネーブルにします。
- コンテンツ フィルタで使用できる [Bcc:] および [Quarantine] アクションは、作成する検疫エリアの保持設定に役に立ちます（詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章を参照してください）。メッセージがすぐにはシステムからリリースされないようにするため（つまり、検疫エリアの割り当てディスク領域がすぐにいっぱいにならないようにするため）、システム検疫とのメールフローをシミュレートするフィルタを作成できます。
- scanconfig コマンドと同じ設定が使用されるため、「Entire Message」条件は、メッセージのヘッダーをスキャンしません。「Entire Message」を選択すると、メッセージ本文および添付ファイルだけがスキャンされます。特定のヘッダー情報を検索するには、「Subject」または「Header」条件を使用します。

- LDAP クエリーによるユーザの設定は、アプライアンスで LDAP サーバが設定されている場合（つまり、`ldapconfig` コマンドを使用して特定の文字列を含む特定の LDAP サーバをクエリーするようにアプライアンスが設定されている場合）だけ GUI に表示されます。
- リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、GUI に表示されません。たとえば、通知 テンプレートおよびメッセージ免責事項は、[Text Resources] ページまたは CLI の `textconfig` コマンドを使用して事前に設定されていない場合、オプションとして表示されません。
- コンテンツ フィルタ機能は、次の文字エンコーディングのテキストを認識し、これらを追加およびスキャンできます。
 - Unicode (UTF-8)
 - Unicode (UTF-16)
 - Western European/Latin-1 (ISO 8859-1)
 - Western European/Latin-1 (Windows CP1252)
 - 中国語 (繁体字) (Big 5)
 - 中国語 (簡体字) (GB 2312)
 - 中国語 (簡体字) (HZ GB 2312)
 - 韓国語 (ISO 2022-KR)
 - 韓国語 (KS-C-5601/EUC-KR)
 - 日本語 (Shift-JIS (X0123))
 - 日本語 (ISO-2022-JP)
 - 日本語 (EUC)

複数の文字セットを 1 つのコンテンツ フィルタ内で組み合わせてマッチングできます。複数の文字エンコーディングでのテキストの表示および入力については、Web ブラウザのマニュアルを参照してください。ほとんどのブラウザでは、複数の文字セットを同時にレンダリングできます。

図 6-25 コンテンツ フィルタでの複数の文字セット



- 着信または発信コンテンツ フィルタの要約ページで、[Description]、[Rules] および [Policies] のリンクを使用して、コンテンツ フィルタに提供されているビューを変更します。
 - [Description] ビューには、各コンテンツ フィルタの説明フィールドに入力したテキストが表示されます（これはデフォルト ビューです）。
 - [Rules] ビューには、ルール ビルダ ページにより構築されたルールおよび正規表現が表示されます。
 - [Policies] ビューには、イネーブルにされている各コンテンツ フィルタのポリシーが表示されます。

図 6-26 コンテンツ フィルタの [Description]、[Rules] および [Policy] を切り替えるリンクの使用
Incoming Content Filters

Filters					
Add Filter...					
Order	Filter Name	Description Rules Policies	Duplicate	Delete	
1	scan_for_confidential	scan_for_confidential: if (body-contains("confidential")) { quarantine ("Policy"); bcc ("hr@example.com", "[message matched confidential filter]"); }			
2	no_mp3s	no_mp3s: if (true) { drop-attachments-by-filetype("mp3", "mp3 deleted"); }			
3	ex_employee	ex_employee: if (rcpt-to == "^doug@") { notify-copy ("%EnvelopeSender", "message bounced for ex-employee of example.com"); bounce(); }			
4	drop_large_attachments	drop_large_attachments: if (true) { drop-attachments-by-size(5242880, "This attachment was too big!"); }			



CHAPTER 7

評価フィルタリング

Cisco IronPort アプライアンスは、独自の階層化された方法により、電子メールゲートウェイでスパムを阻止します。スパム制御の最初の階層である評価フィルタリングを使用すると、Cisco IronPort SenderBase™評価サービスにより決定される送信者の信頼性に基づいて、電子メールの送信者を分類し、ご使用の電子メール インフラストラクチャへのアクセスを制限できます。2 番目の防衛階層であるスキャン（次の章で説明します）では、IronPort Anti-Spam™テクノロジーが使用されています。評価フィルタリングとアンチスパム スキャンを組み合わせることにより、現在使用可能なものの中では最高水準の効率と性能を持つアンチスパム ソリューションが実現されています。

Cisco IronPort アプライアンスを使用すると、既知または信頼性の高い送信者、つまりお客様やパートナーなどからのメッセージに対して、アンチスパム スキャンを一切実施しないでエンドユーザに直接配信するポリシーを非常に簡単に作成できます。未知または信頼性の低い送信者からのメッセージは、アンチスパム スキャンの対象にできます。また、各送信者から受け入れるメッセージの数をスロットリングすることもできます。信頼性の最も低い電子メール送信者に対しては、設定に基づいて接続を拒否したり、その送信者からのメッセージを送り返したりできます。

Cisco IronPort アプライアンスの提供する独自の二層スパム対策により、高性能で今までにない柔軟性を備えた、企業の電子メール ゲートウェイ管理および保護が可能になります。

この章は、次の内容で構成されています。

- 「[評価フィルタリング](#)」 (P.7-2)
- 「[評価フィルタリングの設定](#)」 (P.7-7)

次章「アンチスパム」では、アンチスパム スキャン エンジンの詳細について説明します。

評価フィルタリング

SenderBase 評価サービスを使用すると、ユーザはリモートホストの接続 IP アドレスに基づいて、正確かつ柔軟に陽性と疑わしいスパムを拒否またはスロットリングすることができます。SenderBase 評価サービスは、特定の送信元からのメッセージがスパムである可能性に基づいてスコアを返し、メールフローモニタ機能で客観的データを示すことで、電子メール管理者が電子メールの送信元をより詳しく知ることができるようにします（『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Using Email Security Monitor」を参照）。

SenderBase 評価サービスは、スタンドアロンのアンチスパムソリューションとしても使用できます。IronPort Anti-Spam などの、コンテンツに基づいたアンチスパムシステムの有効性を向上することを主な目的として設計されています。

SenderBase 評価サービスを使用することで、次のことが実行できます。

- スパムの低減

SenderBase 評価サービスを使用することで、企業は接続 IP アドレスに基づいて既知のスパムを特定し、スパムがゲートウェイに到達した時点で、組織がそのスパムをブロックできるようにします。これにより、使用されているアンチスパムスキャンエンジンまたはその他すべてのコンテンツに基づいたフィルタの有効性が高まります。

- スパムフラッドに対する保護

SoBig などのウイルスまたは「当て逃げ」スパム攻撃により、メッセージ量が予期せず急激に増加する場合があります。特定の送信者が大量の送信を開始した場合、SenderBase 評価サービスはグローバルなアフィリエイトネットワークを介してこれを検出し、陰性スコアを割り当てることができます。Cisco IronPort アプライアンスは、このスコアを使用して、送信者に対して許可する 1 時間あたりの受信者数をただちに制限できます（「感染フィルタ」(P.10-1) も参照してください）。

- スループットの向上

Cisco IronPort アプライアンスは、ただちに既知のスパムを拒否し、既知の良好なメッセージをコンテンツフィルタを通過するようにルーティングすることで、システム負荷を低減し、メッセージのスループットを増加できます。

評価フィルタリング : Cisco IronPort SenderBase 評価サービス

Cisco IronPort SenderBase 評価サービス (<http://www.senderbase.org> から入手できます) は、送信者の身元に関する客観的なデータを提供することで、電子メール管理者による質の高い着信電子メール ストリーム管理の実現に役立つように設計されたサービスです。SenderBase 評価サービスは、電子メールの信用レポートに類似しています。企業は、SenderBase 評価サービスの提供するデータを使用して、正規の送信者とスパムの送信元を区別します。SenderBase 評価サービスは、Cisco IronPort アプライアンスの GUI に直接組み込まれており、ここで提供される客観的データを使用して、Unsolicited Commercial Email (UCE) を送信している IP アドレスの信頼性を識別したり、その IP アドレスをブロックしたり、またはビジネス パートナー、顧客、またはその他すべての重要な送信元からの正規着信電子メールの信頼性を確認したりできます。SenderBase 評価サービスは、電子メール メッセージの量をグローバルに表示して、電子メールの送信元の識別とグループ化を容易にする方法でデータを編成している点で独特です。



(注)

Cisco IronPort アプライアンスが、ローカル MX/MTA から電子メールを受信するように設定されている場合は、送信者の IP アドレスをマスクする可能性のあるアップストリーム ホストを識別する必要があります。詳細については、「[着信リレー](#)」(P.8-31) を参照してください。

SenderBase 評価サービスには、次のような主要な要素があります。

- スプーフが不可能

電子メール送信者の信頼性は、電子メールの送信者の IP アドレスに基づいています。SMTP は、TCP/IP を使用した双方向のカンパセーションであるため、IP アドレスを「スプーフ」することはほぼ不可能です。提示される IP アドレスは、メッセージを送信しているサーバにより、実際に制御されているものである必要があります。

- 包括的

SenderBase 評価サービスは、慎重に選択された公開ブラックリストや、オープンプロキシ リストからのデータだけでなく、クレーム率およびメッセージ量の統計情報などの SenderBase Affiliate ネットワークからのグローバル データも使用して、特定の送信元からのメッセージがスパムである可能性を決定します。

- 設定可能

SenderBase 評価サービスは、単純にスパムであるかないか決定を返すブラックリストまたはホワイトリストなどの、その他の「身元に基づいた」アンチスパム手法とは異なり、送信元からのメッセージがスパムである可能性に基づいて、段階的な応答を返します。これにより、スパムをブロックするしきい値を独自に設定したり、SenderBase 評価スコアに基づいて送信者を自動的にさまざまなグループに割り当てたりできます。

SenderBase 評価スコア (SBRs)

SenderBase Reputation Score (SBRs; SenderBase 評価スコア) は、SenderBase 評価サービスからの情報に基づいて、IP アドレスに割り当てられる数値です。SenderBase 評価サービスは、25 個を超える公開ブラックリストおよびオープンプロキシリストのデータを集約し、さらにこのデータを SenderBase のグローバル データと組み合わせて、次のように -10.0 ~ +10.0 のスコアを割り当てます。

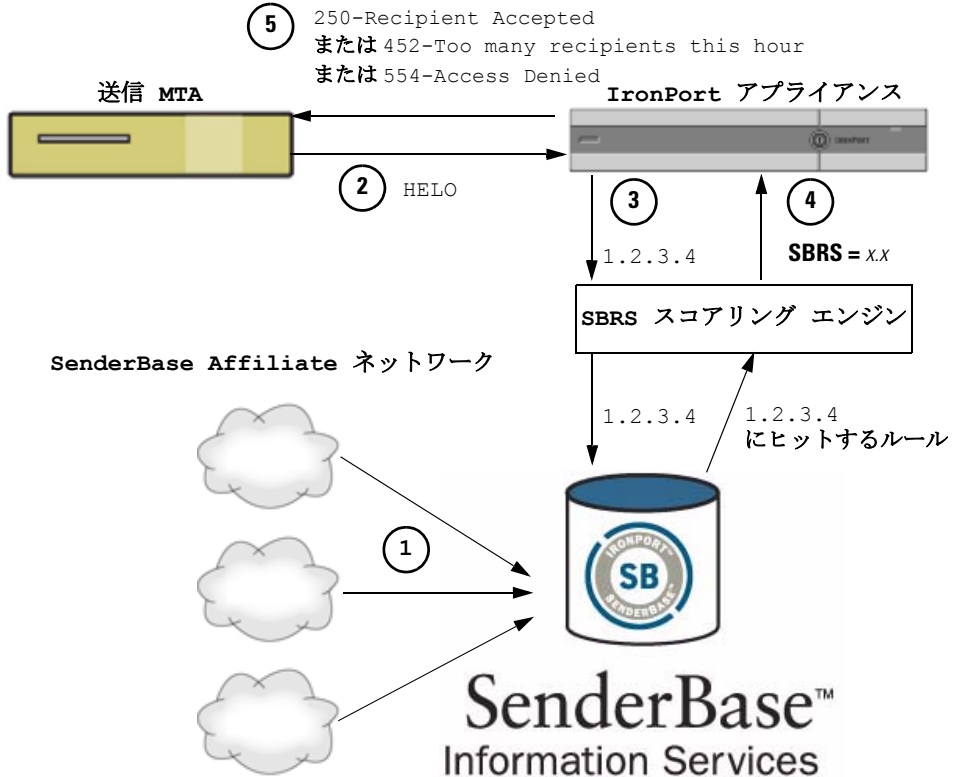
スコア	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い

スコアが低いほど、メッセージがスパムである可能性は高くなります。スコアが -10.0 であれば、そのメッセージはスパムであると「保証」されていることを意味し、スコアが 10.0 であれば、そのメッセージは正規であると「保証」されていることを意味します。

SBRs を使用して、信頼性に基づいてメール フロー ポリシーを送信者に適用するように Cisco IronPort アプライアンスを設定します (メッセージフィルタを作成して SenderBase 評価スコアに「しきい値」を指定し、システムで処理されるメッセージにさらにアクションを実行できます。詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章の「SenderBase Reputation Rule」および「Bypass Anti-Spam System Action」を参照してください)。

図 7-1

SenderBase 評価サービス



- グローバルなクレーム データ
- グローバルな容量データ

- ステップ 1** SenderBase Affiliates から、リアルタイムのグローバル データを送信します。
- ステップ 2** 送信 MTA により、Cisco IronPort アプライアンスとの接続が開始されます。
- ステップ 3** Cisco IronPort アプライアンスにより、接続 IP アドレスのグローバル データがチェックされます。
- ステップ 4** SenderBase 評価サービスにより、このメッセージがスパムである可能性が計算され、SenderBase 評価スコアが割り当てられます。
- ステップ 5** Cisco IronPort により、SenderBase 評価スコアに基づいて応答が返されます。

SenderBase 評価フィルタの実装

Cisco IronPort 評価フィルタ テクノロジーは、Cisco IronPort アプライアンスで
使用可能なその他のセキュリティ サービスの処理から、できる限り多くのメール
を切り離すことを目的としています（「[電子メール パイプラインの理解](#)」
(P.4-1) を参照）。

評価フィルタリングをイネーブルにすると、既知の悪質な送信者は、単純に拒否
されます。世界で 2000 社から送信された既知の良好なメールは、false positive
の可能性を低減するために、自動的にフィルタを避けてルーティングされます。
未知、または「灰色」の電子メールは、アンチスパム スキャン エンジンにルー
ティングされます。評価フィルタは、この方法を使用して、コンテンツ フィル
タにかかる負荷を最大 50 % 低減できます。

図 7-2 評価フィルタリングの例



表 7-2 に、SenderBase 評価フィルタリングを実装する場合に推奨されるポリ
シー セットのリストを示します。企業の目的に応じて、Conservative、
Moderate、Aggressive のいずれかの方法を選択できます。



(注)

シスコではスロットリングが推奨ですが、SenderBase 評価サービスを実装する
もう 1 つの方法として、スパムの疑いのあるメッセージの件名行を変更する方
法があります。このようにするには、表 7-1 に示す次のメッセージ フィルタを
使用します。このフィルタは、reputation フィルタ ルールおよび strip-header
および insert-header フィルタ アクションを使用して、SenderBase 評価スコア
が -2.0 未満のメッセージの件名行を、{Spam SBRs} のように表現される実際
の SenderBase 評価スコアを含む件名行に置き換えます。この例の listener_name

を、ご使用のパブリック リスナーの名前に置き換えます（このテキストを切り取って `filters` コマンドのコマンドライン インターフェイスに直接貼り付けできるように、この行自体にピリオドが含まれています）。

詳細については、『*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。

表 7-1 件名ヘッダーを SBRS に変更するメッセージ フィルタ : 例 1

```
sbrs_filter:

if ((recv-inj == "listener_name" AND subject != "\\{Spam -?[0-9.]+\\}"))

{

    insert-header("X-SBRS", "$REPUTATION");

    if (reputation <= -2.0)

    {

        strip-header("Subject");

        insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

    }

}

.
```

評価フィルタリングの設定

評価フィルタリングは、[Mail Policies] > [HAT Overview] ページで設定します。詳細については、「[SenderBase 評価フィルタの実装](#)」(P.7-6) を参照してください。

Conservative

Conservative 方式では、SenderBase 評価スコアが -4.0 未満のメッセージをブロックし、-4.0 ~ -2.0 のメッセージをスロットリングし、-2.0 ~ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率をほぼ 0 に抑えながら、良好なシステム パフォーマンスを実現できます。

Moderate

Moderate では、SenderBase 評価スコアが -3.0 未満のメッセージをブロックし、-3.0 ~ 0 のメッセージをスロットリングし、0 ~ +6.0 のメッセージにデフォルト ポリシーを適用し、+6.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率を非常に低く抑えながら、良好なシステム パフォーマンスを実現できます（より多くのメールがアンチスパム処理から切り離されるため）。

Aggressive

Aggressive では、SenderBase 評価スコアが -2.0 未満のメッセージをブロックし、-2.0 ~ 0.5 のメッセージをスロットリングし、0 ~ +4.0 のメッセージにデフォルト ポリシーを適用し、+4.0 を超えるスコアのメッセージに信頼されたポリシーを適用します。この方式を使用すると、false positive 率がいくらか発生する可能性はありますが、ほとんどのメールをアンチスパム処理から切り離すことにより、システム パフォーマンスが最大化されます。



(注) また、ユーザは SenderBase 評価スコアが 6.0 より大きいすべてのメッセージを、\$TRUSTED ポリシーに割り当てることを推奨します。

表 7-2 SBRS を使用した評価フィルタリング実装の推奨段階的手法

ポリシー	ブラックリスト	スロットリング	デフォルト	ホワイトリスト
Conservative	-10 ~ -4	-4 ~ -2	-2 ~ 7	7 ~ 10
Moderate	-10 ~ -3	-3 ~ -1	-1 ~ 6	6 ~ 10
Aggressive	-10 ~ -2	-2 ~ -0.5	-0.5 ~ 4	4 ~ 10

ポリシー :	特性 :	適用するメール フロー ポリシー
Conservative :	false positive はほぼ 0。良好なパフォーマンス。	\$BLOCKED
Moderate :	false positive は非常に少ない。高パフォーマンス。	\$THROTTLED
Aggressive :	false positive はいくらか発生。パフォーマンスは最大。	\$DEFAULT

次の手順では、評価フィルタリングを実装する段階的手法の概要を示します。

リスナーの HAT での評価フィルタリング実装

パブリック リスナーのデフォルト HAT エントリを編集して、SBRS を含めるには、次の手順を実行します。

- ステップ 1** [Mail Policies] タブで、[Host Access Table] > [HAT Overview] を選択します。
[Sender Groups (Listener)] メニューからパブリック リスナーを選択します。
[HAT Overview] ページに、各送信者グループの SenderBase 評価スコア設定が表示されます。

図 7-3 送信者グループの SenderBase 評価スコア範囲リスト
HAT Overview

The screenshot shows the 'HAT Overview' interface. At the top, there is a search bar for 'Find Senders that Contain this Text:' with a 'Find' button. Below that, the 'Sender Groups (Listener: IncomingMail (10.19.1.10:25))' section is visible. It includes buttons for 'Add Sender Group...', 'Import HAT...', 'Edit Order...', and 'Export HAT...'. The main table lists sender groups with their reputation score ranges and mail flow policies.

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	WHITELIST	0 to +10	TRUSTED	🗑️
2	BLACKLIST	-10 to -8	BLOCKED	🗑️
3	SUSPECTLIST	-4 to 0	THROTTLED	🗑️
4	UNKNOWNLIST	0 to +10	ACCEPTED	🗑️
	ALL		ACCEPTED	

[HAT Overview] には、各送信者グループ（水平バー）に割り当てられた SenderBase 評価スコアの範囲および関連付けられたメールフローポリシーが表示されます。

ステップ 2 送信者グループのリンクをクリックします。

たとえば、「SUSPECTLIST」のリンクをクリックします。[Edit Sender Group] ページが表示されます。

図 7-4 送信者グループの SBRS 範囲
Edit Sender Group Settings: SUSPECTLIST

The screenshot shows the 'Edit Sender Group Settings' form for the 'SUSPECTLIST' group. The form includes fields for Name, Order, Comment, Policy, SBRS (Optional), DNS Lists (Optional), and Connecting Host DNS Verification. The SBRS (Optional) field is highlighted with a red box and shows a range from -4.0 to 0.0.

Name:	SUSPECTLIST
Order:	3
Comment:	Suspicious senders are throttled
Policy:	THROTTLED
SBRS (Optional):	-4.0 to 0.0
DNS Lists (Optional):	
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in the DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)

ステップ 3 SenderBase 評価スコアの範囲を入力して、送信者グループを定義します。任意でコメントを定義することもできます。

たとえば、「SUSPECTLIST」に -4.0 ~ 0 の範囲を入力します。構文については、「[SenderBase 評価スコアによって定義された送信者グループ \(P.5-31\)](#)」を参照してください。

ステップ 4 [Submit] をクリックします。

リスナーの HAT で、各グループについてステップ 2 ~ 5 を繰り返します。たとえば、*conservative* 方式の値を定義します。表 7-2 に示した Moderate または Aggressive 方式の値も定義できます。

送信者グループ	SBRS 範囲	メール フロー ポリシー
WHITELIST	6 ~ 10	TRUSTED
BLACKLIST	-10 ~ -7	BLOCKED
SUSPECTLIST	-7 ~ -2	THROTTLED
UNKNOWNLIST	-2 ~ 6	ACCEPTED



(注) リスナーの HAT で送信者グループを定義するときは、順序に注意してください（リスナーへの接続を試行する各ホストで、HAT は上から下へ順に読み込まれます。接続ホストにルールが一致すると、その接続に対してただちにアクションが実行されます）。シスコでは、リスナーの HAT であらかじめ定義されている送信者グループをデフォルトの順序で維持すること（つまり、RELAYLIST（C10/100 カスタマーのみ）、WHITELIST、BLACKLIST、SUSPECTLIST、UNKNOWNLIST の順）を推奨します。

ステップ 5 [Commit Changes] ボタンをクリックし、必要に応じて任意のコメントを追加してから [Commit Changes] をクリックして、リスナーの HAT での評価フィルタリングの実装を終了します。

SBRS を使用した評価フィルタリングのテスト

常時大量のスパムを受信しているか、または組織に対するスパムを受信するために「ダミー」のアカウントを特に設定していない限り、実装した SBRS ポリシーをただちにテストすることは困難です。ただし、表 7-3 に示すように、リス

ナーの HAT に SenderBase 評価スコアによる評価フィルタリングのエントリを追加した場合は、インバウンドメールのうち「未分類」になるパーセンテージが低くなります。

作成したポリシーは、任意の SBRS で trace コマンドを使用してテストします。「[Debugging Mail Flow Using Test Messages: Trace](#)」(P.446)を参照してください。trace コマンドは、GUI だけでなく CLI でも使用できます。

表 7-3 SBRS 実装の推奨メール フロー ポリシー

ポリシー名	主要な動作 (アクセスルール)	パラメータ	値
\$BLOCKED	REJECT	None	
\$THROTTLED	ACCEPT	Maximum messages / session:	10
		Maximum recipients / message:	20
		Maximum message size:	1 MB
		Maximum concurrent connections:	10
		Use Spam Detection:	ON
		Use TLS:	OFF
		Maximum recipients / hour:	20 (推奨)
		Use SenderBase:	ON

表 7-3 SBRS 実装の推奨メール フロー ポリシー (続き)

ポリシー名	主要な動作 (アクセス ルール)	パラメータ	値
\$ACCEPTED (パブリック リスナー)	ACCEPT	Maximum messages / session:	1,000
		Maximum recipients / message:	1,000
		Maximum message size:	100 MB
		Maximum concurrent connections:	1,000
		Use Spam Detection:	ON
		Use TLS:	OFF
		Use SenderBase:	ON
\$TRUSTED	ACCEPT	Maximum messages / session:	1,000
		Maximum recipients / message:	1,000
		Maximum message size:	100 MB
		Maximum concurrent connections:	1,000
		Use Spam Detection:	OFF
		Use TLS:	OFF
		Maximum recipients / hour:	-1 (ディセーブ ル)
Use SenderBase:	OFF		



(注)

\$THROTTLED ポリシーでは、リモート ホストから受信する 1 時間あたりの最大受信者数は、デフォルトで 1 時間あたり 20 人に設定されています。この設定により、使用可能な最大スロットリングが制御されることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。デフォルトのホスト アクセス ポリシーの詳細については、「[パブリックリスナー向けの定義済みのメール フロー ポリシー](#)」(P.5-33) を参照してください。

SenderBase 評価サービスのステータスのモニタリング

[Security Services] メニューの [SenderBase] ページには、Cisco IronPort アプライアンスから SenderBase Network Status Server および SenderBase 評価スコアサービスに対して最後に実行したクエリーの接続ステータスおよびタイムスタンプが表示されます。SenderBase 評価スコア サービスは、アプライアンスに SRBS スコアを送信します。SenderBase Network Server は、アプライアンスにメール送信元の IP アドレス、ドメイン、および組織などの情報を送信します。AsyncOS は、このデータをレポート作成および電子メール モニタリング機能に使用します。

図 7-5 [SenderBase] ページの [SenderBase Network Status]

SenderBase Network Status		
Type	Status	Last Status Check
SenderBase Network Server	up	Wed Sep 10 13:44:52 2008 PDT
SenderBase Reputation Score Service	up	Wed Sep 10 13:44:52 2008 PDT

CLI の `sbstatus` コマンドでも、同じ情報を表示できます。



CHAPTER 8

アンチスパム

Cisco IronPort アプライアンスは、独自の階層化された方法により、電子メールゲートウェイでスパムを阻止します。スパム制御の最初の階層である評価フィルタリング（第7章「評価フィルタリング」で前述）を使用すると、送信者の信頼性（Cisco IronPort SenderBase™評価サービスにより決定）に基づいて電子メールの送信者を分類し、ご使用の電子メール インフラストラクチャへのアクセスを制限できます。2 番目の防衛階層であるスキャンでは、IronPort Anti-Spam テクノロジーと IronPort Intelligent Multi-Scan テクノロジーが使用されています。評価フィルタリングとアンチスパム スキャンを組み合わせることにより、現在使用可能なものの中では最高水準の効率と性能を持つアンチスパム ソリューションが実現されています。

Cisco IronPort アプライアンスを使用すると、既知または信頼性の高い送信者、つまりお客様やパートナーなどからのメッセージに対して、アンチスパム スキャンを一切実施しないでエンドユーザに直接配信するポリシーを非常に簡単に作成できます。未知または信頼性の低い送信者からのメッセージは、アンチスパム スキャンの対象にできます。また、各送信者から受け入れるメッセージの数をスロットリングすることもできます。信頼性の最も低い電子メール送信者に対しては、設定に基づいて接続を拒否したり、その送信者からのメッセージをドロップしたりできます。

Cisco IronPort アプライアンスの提供する独自の二層スパム対策により、高性能で今までにない柔軟性を備えた、企業の電子メール ゲートウェイ管理および保護が可能になります。

この章は、次の内容で構成されています。

- 「アンチスパムの概要」 (P.8-2)
- 「IronPort Anti-Spam フィルタリング」 (P.8-6)
- 「IronPort Intelligent Multi-Scan フィルタリング」 (P.8-14)

- 「アンチスパム ルールのアップデートの設定」 (P.8-18)
- 「アンチスパムの受信者別ポリシーの設定」 (P.8-19)
- 「着信リレー」 (P.8-31)

アンチスパムの概要

Cisco IronPort アプライアンスでは、IronPort Anti-Spam エンジンと IronPort Intelligent Multi-Scan の 2 つのアンチスパム ソリューションを提供しています。Cisco IronPort アプライアンスでこれらのソリューションのライセンスを許諾し、イネーブルにすることはできますが、同じポリシーに対して両方をイネーブルにはできません。電子メール セキュリティ マネージャを使用すると、異なるユーザのグループに対して異なるアンチスパム ソリューションをすばやく簡単に指定できます。

アンチスパム スキャンのイネーブル化

System Setup Wizard (または CLI の `systemsetup` コマンド) を使用すると、IronPort Intelligent Multi-Scan と IronPort Anti-Spam エンジンのいずれかをイネーブルにするオプションが示されます。システム セットアップの間に両方をイネーブルにはできませんが、システム セットアップの完了後に [Security Services] メニューを使用して、選択しなかったアンチスパム ソリューションをイネーブルにすることはできます。システム セットアップでは、陽性および陽性と疑わしいスパムに対処する IronPort スпам検疫を必要に応じてイネーブルにすることができます。

IronPort スпам検疫エンジンを初めてイネーブルにするときは (システム セットアップ時または後刻)、ライセンス契約書を読んで承諾してください。

図 8-1 アンチスパム エンジン : システム セットアップ時に選択





(注)

アンチスパム スキャンの適用方法および適用条件については、「[電子メール プライベートとセキュリティ サービス](#)」(P.4-9) を参照してください。

システムのセットアップが終了すれば、[Mail Policies] > [Incoming Mail Policies] ページから着信メール ポリシー用のアンチスパム スキャン ソリューションを設定できます (発信メール ポリシーでは、通常は、アンチスパム スキャンをディセーブルにします)。単一のポリシーについてアンチスパム スキャンをディセーブルにすることもできます。

この例では、デフォルト メール ポリシーおよび「Partners」ポリシーで IronPort Anti-Spam スキャン エンジンを使用して、陽性および陽性と疑わしいスパムを検査しています。

図 8-2 メール ポリシー : 受信者ごとのアンチスパム エンジン

Incoming Mail Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Partners	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Enabled	

Key: Default Custom Disabled

IronPort Intelligent Multi-Scan を使用して不要なマーケティング メッセージをスキャンするように Partners ポリシーを変更するには、[Partners] 行に対応する [Anti-Spam] 列のエントリ (「use default」) をクリックします。

スキャン エンジンとして IronPort Intelligent Multi-Scan を選択し、[Yes] を選択して不要なマーケティング メッセージの検出をイネーブルにします。不要なマーケティング メッセージの検出には、デフォルト設定値を使用します。

図 8-3 に、IronPort Intelligent Multi-Scan と不要なマーケティング メッセージの検出がイネーブルにされたポリシーを示します。

図 8-3 メール ポリシー : IronPort Intelligent Multi-Scan のイネーブル化

Anti-Spam Settings

Policy: Test

Enable Anti-Spam Scanning for This Policy:

- Use Settings from Default Policy (IronPort Anti-Spam)
- Use IronPort Anti-Spam service
- Use IronPort Intelligent Multi-Scan
Spam scanning built on IronPort Anti-Spam.
- Disabled

Positively-Identified Spam Settings

Apply This Action to Message: Deliver

Send to Alternate Host (optional):

Add Text to Subject: Prepend [SPAM]

Advanced: Optional settings for custom header and message delivery.

Suspected Spam Settings

Enable Suspected Spam Scanning: No Yes

Apply This Action to Message: Deliver

Send to Alternate Host (optional):

Add Text to Subject: Prepend [SUSPECTED SPAM]

Advanced: Optional settings for custom header and message delivery.

Marketing Email Settings

Enable Marketing Email Scanning: No Yes

Apply This Action to Message: Deliver

Send to Alternate Host (optional):

Add Text to Subject: Prepend [MARKETING]

Advanced: Optional settings for custom header and message delivery.

変更の送信と確定後のメール ポリシーは次のようになります。

図 8-4 メール ポリシー : Intelligent Multi-Scan がイネーブルにされたポリシー

Incoming Mail Policies

Find Policies

Email Address:

Recipient Sender

Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Partners	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver Marketing Messages: Deliver	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Not Available	Disabled	Not Available	

Key:

アンチスパム スキャン エンジンの設定値

各アンチスパム ソリューションには、一連の設定値が関連付けられています。これらの設定値は、対応するエンジンだけに適用される設定で、[Security Services] メニューの [IronPort Anti-Spam] ページと [IronPort Intelligent Multi-Scan] ページおよび着信と発信のメール ポリシーのアンチスパム設定値 ページで使用可能です。スキャン ソリューション固有の設定値については、対応する項で説明します。[IronPort Anti-Spam] ページおよび [IronPort Intelligent Multi-Scan] ページには、最新のアップデート日時を持つアンチスパム ルールのリストも表示されます。

グローバル アンチスパム設定値を設定するときの詳細については、次の資料を参照してください。

- 「[IronPort Anti-Spam のイネーブル化とグローバル設定値の設定](#)」 (P.8-9) および
- 「[IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定](#)」 (P.8-15)

受信者ごとの設定を原則とするアンチスパム スキャン設定の詳細については、「[アンチスパムの受信者別ポリシーの設定](#)」 (P.8-19) を参照してください。

アンチスパム スキャンと Cisco IronPort アプライアンスによって生成されるメッセージ

Cisco IronPort アプライアンスから電子メール アラート、スケジュール済みレポート、およびその他の自動化されたメッセージを受信する受信者の場合は、アンチスパム スキャンをバイパスする着信メール ポリシーに入れるよう推奨しています。これらのメッセージは、企業のメール ストリームでは通常見つかることのない、スパム発信元と関連性のある URL やその他の情報を含むため、これらのメッセージには、スパムとマークされることがあります。または、Cisco IronPort アプライアンスのためにメールの送信元の IP アドレスをホスト アクセス テーブルの「WHITELIST」ポリシーに追加することもできます（「[送信者グループへの送信者の追加](#)」 (P.5-48) を参照）。詳細については、認可された Cisco IronPort アプライアンス サポート センターにお問い合わせください。

IronPort Anti-Spam フィルタリング

IronPort Anti-Spam は従来の技術と革新的な状況依存型検出テクノロジーを使用し、既知のものから新たに出現したものまで多様な電子メール脅威を排除します。

評価キー

Cisco IronPort アプライアンスには、IronPort Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。このキーは、System Setup Wizard または [Security Services] > [IronPort Anti-Spam] ページ (GUI) か、systemsetup コマンドまたは antispamconfig コマンド (CLI) で、ライセンス契約書を受諾して初めてイネーブルになります。デフォルトでは、ライセンス契約書に同意すると、デフォルト着信メールポリシーに対して IronPort Anti-Spam がイネーブルになります。設定した管理者アドレス（「手順 2 : System」(P.3-23) を参照）に対して、IronPort Anti-Spam のライセンスの期限が 30 日後に切れることを通知するアラートの送信も行われます。アラートは、期限切れの 30、15、5、および 0 日前に送信されます。30 日間の評価期間後もこの機能をイネーブルにする場合の詳細については、Cisco IronPort の営業担当者にお問い合わせください。残りの評価期間は、[System Administration] > [Feature Keys] ページを表示するか、または featurekey コマンドを発行することによって確認できます（詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」にある機能キーの使用に関する項を参照してください）。

IronPort Anti-Spam および CASE の概要

IronPort Anti-Spam フィルタリングは、Context Adaptive Scanning Engine (CASE) ™に基づいており、次の目的のために電子メールと Web 評価情報を組み合わせる、1 層目のアンチスパム スキャンエンジンです。

- 最大限多様な電子メール脅威の排除：スパム、フィッシング、ゾンビベースの攻撃、および他の「混合された」脅威を検出します。
- 最大限の精度の実現：SenderBase 評価サービスからの電子メールと Web 評価に基づくアンチスパム ルール。
- 扱いやすさ：ハードウェア コストおよび管理コストの低減を背景とします。

- 業界トップクラスの性能の実現：CASE では、ダイナミックな初期終了基準およびオフボックス ネットワーク見積もりを使用して、きわめて優れた性能を実現できます。
- インターナショナル ユーザのニーズに対応：IronPort Anti-Spam は、世界的に業界トップクラスの性能を発揮するように調整されています。

最大限多様な脅威防止

CASE では、コンテンツ分析、電子メール評価、および Web 評価を組み合わせ、最大限多様な脅威防止要因を収集します。

IronPort Anti-Spam は、できるだけ多様な電子メール脅威を徹底的に検出するように設計されています。IronPort Anti-Spam では、スパム、フィッシング、ゾンビ攻撃などの既知のあらゆる脅威に対応するだけでなく、「419」詐欺など検出が難しく、少量で、短期間の電子メール脅威にも対応します。さらに、IronPort Anti-Spam では、ダウンロード URL または実行ファイルを介して不正なコンテンツを配布するスパム攻撃など、新しい脅威や混合された脅威を識別します。

IronPort Anti-Spam では、これらの脅威を識別するために、業界随一の網羅性を持つ脅威検出方式を使用し、メッセージのコンテキスト全体、つまりメッセージの内容、メッセージの構築方式、送信者の評価、メッセージでアドバタイズされている Web サイトの評価などを調べます。IronPort Anti-Spam だけが、電子メールと Web の評価データを組み合わせ、世界有数の規模を誇る電子メールおよび Web トラフィックのモニタリング ネットワークである SenderBase の検出力を最大限活用して、新しい攻撃が開始され次第その攻撃を検出します。



(注)

ローカル MX/MTA からのメールを受信するよう Cisco IronPort アプライアンスを設定している場合は、送信者の IP アドレスをマスクする可能性のあるアップストリーム ホストを指定する必要があります。詳細については、「[着信リレー](#)」(P.8-31) を参照してください。

最小限の false positive 率

IronPort Anti-Spam および IronPort Outbreak Filter では、Cisco IronPort の特許出願中の Context Adaptive Scanning Engine (CASE) TMを利用してしています。CASE では、4 つの次元にまたがる 100,000 個以上のメッセージ属性を分析することにより、めざましい精度と性能の向上を実現しています。

- ステップ 1 電子メール評価：このメッセージの送信者は誰か。
- ステップ 2 メッセージの内容：このメッセージに含まれている内容は何か。
- ステップ 3 メッセージ構造：このメッセージはどのように構築されているか。
- ステップ 4 Web 評価：遷移先はどこか。

CASE では、多次元的な関係を分析することにより、優れた精度を維持しながら、多様な脅威を検出できます。たとえば、正規金融機関から送信されたと断言する内容を持ちながら、消費者向けのブロードバンド ネットワークに属している IP アドレスから送信されたメッセージや、ゾンビ PC によってホストされている URL を含むメッセージは、疑わしいメッセージであると見なされます。これとは対照的に、肯定的な評価が与えられている製薬会社からのメッセージは、スパムとの関連性が強い単語を含んでいたとしても、スパムであるとタグ付けされません。

業界トップ水準の性能

CASE では、次の機能を組み合わせることにより、正確な判定が迅速に実行されます。

- 単一パスによる複数脅威のスキャン
- 動的な「初期終了」システム

システム性能は、Cisco IronPort 固有の「初期終了」システムを使用して最適化されます。Cisco IronPort では、ルールの精度と計算コストに基づいてルールの適用順序を決定する、独自のアルゴリズムを開発しました。コストが低い一方で正確性の高いルールから実行していき、判定が出た時点でそれ以降のルールは不要になります。この方式によってシステムのスループットが向上されるため、大企業のニーズを満たす製品が実現されます。反対に、高効率なエンジンは低コスト ハードウェアへの実装を可能にしているため、Cisco IronPort のセキュリティ サービスはローエンドのお客様にとって魅力的です。

- オフボックス ネットワーク見積もり

インターナショナル ユーザ

IronPort Anti-Spam は、業界トップ クラスの性能をワールドワイドで発揮するように調整されています。ロケール固有でありコンテンツに依存する脅威検出技術に加え、リージョナル ルール プロファイルを使用することによって、特定の

リージョン向けにアンチスパム スキャンを最適化できます。アンチスパム エンジンには、リージョナルルール プロファイルが含まれています。リージョナルルール プロファイルでは、リージョナル ベースでスパムをターゲットにします。たとえば、中国および台湾で受信するスパムでは、繁体字および簡体字の割合が高くなります。中国語のリージョナルルールは、このタイプのスパムに合わせて最適化されています。主に中国本土、台湾、および香港向けのメールを受信するのであれば、中国語のリージョナルルール プロファイルを使用することを、強く推奨します。リージョナルルール プロファイルは、[Security Services] > [IronPort Anti-Spam] からイネーブルにできます。



(注) リージョナルルール プロファイルでは特定のリージョンに合わせてアンチスパム エンジンが最適化されるため、他のタイプのスパムについては検出率の低下を招くおそれがあります。したがって、指定したリージョンから大量の電子メールを受信する場合に限り、この機能をイネーブルにすることを推奨します。

IronPort Anti-Spam では、南北アメリカ大陸、ヨーロッパ、およびアジアに散在している、125,000 を超える ISP、大学、および企業から提供された、地球規模において代表的な電子メールと Web のコンテンツ不可知データを活用しています。サンパウロ、北京、およびロンドンに中枢機能を置く Threat Operations Center が世界的活動のために設置されています。さらに、中国語、日本語、韓国語、ポルトガル語、およびスペイン語を含む 32 の言語からの専門家たちが加わっています。

IronPort Anti-Spam のイネーブル化とグローバル設定値の設定

概要

IronPort Anti-Spam のイネーブル化とグローバル設定値の変更には、[Security Services] > [IronPort Anti-Spam] ページと [Security Services] > [Service Updates] ページ (GUI) または `antisppamconfig` コマンドと `updateconfig` コマンド (CLI) を使用します。次のグローバル設定値が設定されます。

- アプライアンスの IronPort Anti-Spam をグローバルでイネーブルにします。
- IronPort Anti-Spam によるメッセージ スキャンのしきい値を設定します。

スパム送信者から続々と送信される大量メッセージをスキャンする能力を備えながらも、アプライアンスのスループット最適化を図るため、定義サイズより小さいメッセージがすべて CASE でスキャンされる *always scan* メッセージサイズを定義でき、Cisco IronPort の業界トップレベルの性能を発揮しています。また、定義サイズより大きいメッセージが CASE でスキャンされない *never scan* メッセージサイズを定義できます。*always scan* サイズより大きく、*never scan* サイズより小さいメッセージについては、CASE は限定的な高速スキャンを実行します。



(注) 感染フィルタの最大メッセージサイズが IronPort Anti-Spam の *always scan* メッセージより大きい場合、CASE は感染フィルタの最大サイズより小さいメッセージをすべてスキャンします。

- メッセージをスキャンするときにタイムアウトを待機する時間の長さを入力します。
- IronPort Anti-Spam ルールのアップデートを取得するためのプロキシサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。ルールのアップデートを取得するためのプロキシサーバを定義する場合は、必要に応じて、プロキシサーバに接続するための認証済みユーザ名、パスワード、および特定のポートを設定できます。
- IronPort Anti-Spam ルールのアップデートを受信するダウンロードサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。
- IronPort Anti-Spam ルールの自動アップデートの受信をイネーブルまたはディセーブルにし、アップデート間隔も指定します。



(注) プロキシサーバのセットアップは、[Security Services] > [Service Updates] ページから行うことができます。プロキシサーバの指定方法の詳細については、「[Service Updates] ページ」(P.15-16) を参照してください。これで、プロキシサーバがグローバルになったため、プロキシサーバを使用するように設定されているすべてのサービスで同じプロキシサーバが使用されます。



(注) GUI の System Setup Wizard (または CLI の `systemsetup` コマンド) で IronPort Anti-Spam をイネーブルにすることを選択した場合は、グローバル設定値のデフォルト値を使用し、デフォルト着信メール ポリシーに対してイネーブルになります。

図 8-5 に、[Security Services] > [IronPort Anti-Spam] ページで設定するグローバル設定値を示します。

図 8-5 IronPort Anti-Spam のグローバル設定値：編集
Edit IronPort Anti-Spam Global Settings

IronPort Anti-Spam をイネーブルにするには、次の手順を実行します。

ステップ 1 System Setup Wizard で IronPort Anti-Spam をイネーブルにしなかった場合は、[Security Services] > [IronPort Anti-Spam] を選択します。

ステップ 2 [Enable] をクリックします。

ライセンス契約書ページが表示されます。



(注) ライセンス契約に合意しない場合、IronPort Anti-Spam はアプライアンスでイネーブルになりません。

ステップ 3 ページの下部までスクロールし、[Accept] をクリックしてライセンス契約に合意します。

図 8-6 とほぼ同じページが表示されます。

ステップ 4 [Edit Global Settings] をクリックします。

ステップ 5 [Enable IronPort Anti-Spam scanning] の横のボックスをオンにします。

このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。ただし、メール ポリシーの受信者ごとの設定値をイネーブルにする必要は、引き続きあります。詳細については、「[アンチスパムの受信者別ポリシーの設定](#)」(P.8-19) を参照してください。

ステップ 6 IronPort Anti-Spam の *always scan* メッセージ サイズの値を入力します。

推奨値は 512 Kb 以下です。「初期終了」の場合を除き、*always scan* サイズより小さいメッセージは **CASE** ですべてスキャンします。このサイズより大きいメッセージは、[ステップ 7](#) で入力する *never scan* サイズより小さい場合、**CASE** で部分的にスキャンされます。「初期終了」システムの詳細については、「[業界トップ水準の性能](#)」(P.8-8) を参照してください。



(注) *always scan* メッセージ サイズは 3 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。

ステップ 7 *never scan* メッセージ サイズの値を入力します。

推奨値は 1024 Kb 以下です。このサイズより大きいメッセージは、IronPort Anti-Spam によってスキャンされず、X-IronPort-Anti-Spam-Filtered: true というヘッダーはメッセージに追加されません。



(注) *never scan* メッセージ サイズは 10 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。

ステップ 8 メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。

秒数を指定する場合は、1 ~ 120 の整数を入力します。デフォルト値は 60 秒です。

ステップ 9 リージョナル スキャンをイネーブルまたはディセーブルにします。リージョナル スキャンでは、特定のリージョン用に IronPort Anti-Spam スキャンが最適化されます。この機能では特定のリージョンに合わせてアンチスパム エンジンが最適化されるため、他のタイプのスパムについては検出率の低下を招くおそれがあります。したがって、指定したリージョンから大量の電子メールを受信する場合に限り、この機能をイネーブルにすることを推奨します。リージョナル スキャンの詳細については、「[インターナショナル ユーザ](#)」(P.8-8) を参照してください。

ステップ 10 変更を送信して確定します。

[Security Services] > [IronPort Anti-Spam] ページがリフレッシュされて、前の手順で選択した値が表示されます。

図 8-6 IronPort Anti-Spam のグローバル設定値

IronPort Anti-Spam Overview	
IronPort Anti-Spam Scanning:	Enabled
Message Scanning Thresholds:	Always scan 512K or less. Never scan 10M or more.
Timeout for Scanning Single Message:	60 seconds
Regional Scanning:	Off
Edit Global Settings...	

Rule Updates			
Rule Type	Last Update	Current Version	New Update
CASE Core Files	Never Updated	3.1.0-010	Connecting to update server
CASE Utilities	Never Updated	3.1.0-010	Connecting to update server
Structural Rules	Never Updated	3.0.0-031-20110112_132005	Connecting to update server
Web Reputation DB	Never Updated	20110112_193542	Connecting to update server
Web Reputation Rules	Never Updated	20110112_193542-20110112_193542	Connecting to update server
Content Rules	Never Updated	unavailable	Connecting to update server
Content Rules Update	Never Updated	unavailable	Connecting to update server
No updates in progress. Update Now			

その他の手順

IronPort Anti-Spam をイネーブルにすると、SenderBase 評価スコアに基づいて接続を拒否していない場合であっても、SenderBase 評価サービスのスコアリングがイネーブルになります。SBRs のイネーブル化の詳細については、「[SenderBase 評価フィルタの実装](#)」(P.7-6) を参照してください。

IronPort Intelligent Multi-Scan フィルタリング

IronPort Intelligent Multi-Scan では、IronPort Anti-Spam などの複数のアンチスパム スキャン エンジンを組み込むことにより、インテリジェントな多層アンチスパム ソリューションを実現しています。この方式により、false positive 率を上昇させることなく、判定の精度が向上されて、検出されるスパムの量が増加します。

IronPort Intelligent Multi-Scan によってメッセージを処理する場合は、まず、サードパーティ製アンチスパム エンジンを使用してスキャンされます。次に、メッセージおよびサードパーティ製エンジンによる判定が IronPort Anti-Spam に渡されて、最終判定が下されます。IronPort Anti-Spam 自体によるスキャンの実行後に統合されたマルチスキャン評点が AsyncOS に返されます。サードパーティ製スキャン エンジンと IronPort Anti-Spam の長所を組み合わせることによって、IronPort Anti-Spam の持つ低い false positive 率を維持しながら、検出するスパムの数が増えます。

IronPort Intelligent Multi-Scan で使用されるスキャン エンジンの順序は設定できません。IronPort Anti-Spam は、常に最後にメッセージをスキャンするエンジンであり、サードパーティ製エンジンによってスパムであると判定されたメッセージを IronPort Intelligent Multi-Scan がスキップすることはありません。

IronPort Intelligent Multi-Scan を使用すると、システムのスループットが低下する場合があります。詳細については、IronPort サポート担当者にお問い合わせください。

この機能は、C100 アプライアンス以外のすべての C-Series アプライアンスおよび X-Series アプライアンスでサポートされています。



(注)

Intelligent Multi-Scan 機能キーによって、アプライアンスで IronPort Anti-Spam もイネーブルになります。その結果、メール ポリシーで IronPort Intelligent MultiScan または IronPort Anti-Spam のいずれかをイネーブルにできるようになります。

IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の設定

概要

IronPort Intelligent Multi-Scan のイネーブル化とグローバル設定値の変更には、[Security Services] > [IronPort Intelligent Multi-Scan] ページと [Security Services] > [Service Updates] ページ (GUI) または `antisпамconfig` コマンドと `updateconfig` コマンド (CLI) を使用します。次のグローバル設定値が設定されます。

- アプライアンスでグローバルに IronPort Intelligent Multi-Scan をイネーブルにします。
- IronPort Intelligent Multi-Scan でスキャンするメッセージの最大サイズを設定します。
- メッセージをスキャンするときにタイムアウトを待機する時間の長さを入力します。

大部分のユーザでは、スキャンする最大メッセージサイズもタイムアウト値も変更する必要がありません。ただし、最大メッセージサイズ設定を小さくすると、アプライアンスのスループットを最適化できます。

- IronPort Intelligent Multi-Scan ルールのアップデートを取得するためのプロキシサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。ルールのアップデートを取得するためのプロキシサーバを定義する場合は、必要に応じて、プロキシサーバに接続するための認証済みユーザ名、パスワード、および特定のポートを設定できます。
- IronPort Intelligent Multi-Scan ルールのアップデートを受信するダウンロードサーバを定義し、必要に応じてイネーブルにします ([Security Services] > [Service Updates])。
- IronPort Intelligent Multi-Scan ルールの自動アップデートの受信をイネーブルまたはディセーブルにし、アップデート間隔も指定します。



(注) プロキシ サーバのセットアップは、[Security Services] > [Service Updates] ページから行うことができます。プロキシ サーバの指定方法の詳細については、「[Service Updates] ページ」(P.15-16) を参照してください。これで、プロキシ サーバがグローバルになったため、プロキシ サーバを使用するように設定されているすべてのサービスで同じプロキシ サーバが使用されます。



(注) GUI の System Setup Wizard (または CLI の `systemsetup` コマンド) で IronPort Intelligent Multi-Scan をイネーブルにすることを選択した場合は、グローバル設定値のデフォルト値を使用し、デフォルト着信メール ポリシーに対してイネーブルになります。

図 8-7 に、[Security Services] > [IronPort Intelligent Multi-Scan] ページで設定するグローバル設定値を示します。

図 8-7 IronPort Intelligent Multi-Scan のグローバル設定値 : 編集

IronPort Intelligent Multi-Scan Overview	
IronPort Intelligent Multi-Scan:	Enabled
Maximum Message Size to Scan:	131072 bytes
Timeout for Scanning Single Message:	60 seconds
Edit Global Settings...	

IronPort Intelligent Multi-Scan をイネーブルにするには、次の手順を実行します。

ステップ 1 System Setup Wizard で IronPort Intelligent Multi-Scan をイネーブルにしなかった場合は、[Security Services] > [IronPort Intelligent Multi-Scan] を選択します。

ステップ 2 [Enable] をクリックします。
ライセンス契約書ページが表示されます。



(注) ライセンス契約書を受諾しなければ、IronPort Intelligent Multi-Scan はアプライアンスでイネーブルにされません。

ステップ 3 ページの下部までスクロールし、[Accept] をクリックしてライセンス契約に合意します。

図 8-8 とほぼ同じページが表示されます。

- ステップ 4** [Edit Global Settings] をクリックします。
- ステップ 5** [Enable IronPort Intelligent Multi-Scan] の横のボックスをオンにします。
このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。ただし、メール ポリシーの受信者ごとの設定値をイネーブルにする必要は、引き続きあります。詳細については、「[アンチスパムの受信者別ポリシーの設定](#)」(P.8-19) を参照してください。
- ステップ 6** IronPort Intelligent Multi-Scan でスキャンする最大メッセージサイズの値を選択します。
デフォルト値は 128 Kb です。このサイズより大きいメッセージは、IronPort Intelligent Multi-Scan によってスキャンされません。
- ステップ 7** メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。
秒数を指定する場合は、1 ～ 120 の整数を入力します。デフォルト値は 60 秒です。
- ステップ 8** 変更を送信して確定します。
[Security Services] > [IronPort Intelligent Multi-Scan] ページがリフレッシュされて、前の手順で選択した値が表示されます。

図 8-8 IronPort Intelligent Multi-Scan のグローバル設定値

IronPort Intelligent Multi-Scan

IronPort Intelligent Multi-Scan Overview	
IronPort Intelligent Multi-Scan:	Enabled
Maximum Message Size to Scan:	131072 bytes
Timeout for Scanning Single Message:	60 seconds
Edit Global Settings...	

Rule Updates (Last download attempt made on: Never)		
Rule Type	Last Update	Current Version
CASE Core Files	Base Version	2.7.1-005
Structural Rules	Base Version	2.7.1-005-20090511_160603
CASE Utilities	Base Version	2.7.1-005
Web Reputation DB	Never Updated	20050725_000000
Web Reputation Rules	Never Updated	20050725_000000-20050725_000000
Update Now		

その他の手順

IronPort Intelligent Multi-Scan をイネーブルにすると、SenderBase 評価スコアに基づいて接続を拒否していない場合であっても、SenderBase 評価サービスのスコアリングがイネーブルになります。SBRs のイネーブル化の詳細については、「[SenderBase 評価フィルタの実装](#)」(P.7-6) を参照してください。

アンチスパム ルールのアップデートの設定

IronPort Anti-Spam および IronPort Intelligent Multi-Scan のルールは、デフォルトでは、IronPort のアップデート サーバから取得されます。アップデート用のローカル サーバ、アップデートの取得に使用するプロキシサーバ、ルールのアップデートを確認するかどうかおよび確認する頻度を指定できます。アンチスパム ソリューションのアップデートを設定するには、[Security Services] > [Service Updates] ページの [Edit Update Settings] をクリックします。

詳細については、「サービスのアップデート」(P.15-16) を参照してください。

IronPort Anti-Spam ルールのアップデートを取得するプロキシサーバのイネーブル化

Cisco IronPort アプライアンスは、Cisco IronPort のアップデート サーバに直接接続して、アンチスパム ルールのアップデートを受け取るように設定されます。この接続は、ポート 80 の HTTP によって確立され、コンテンツは暗号化されます。ファイアウォールでこのポートを開くことを避ける場合は、アップデートされたルールをアプライアンスで受け取ることができる、プロキシサーバおよび具体的なポートを定義できます。

プロキシサーバを使用する場合は、任意で認証およびポートを指定できます。

プロキシサーバが定義されている場合、IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、そのプロキシサーバを自動的に使用します。他のすべてのサービス アップデート (感染フィルタ、Sophos Anti-Virus など) についてプロキシサーバをディセーブルにしないで、アンチスパム ソリューションについてプロキシサーバをオフにする方法はありません。



(注)

プロキシサーバを定義すると、プロキシサーバを使用するように設定されているすべてのサービス アップデートで、そのプロキシサーバが自動的に使用されます。

プロキシサーバの定義の詳細については、「HTTP プロキシサーバの指定 (任意)」(P.15-23) を参照してください。

モニタリング ルールのアップデート

ライセンス契約を受諾すると、最新の IronPort Anti-Spam ルールおよび IronPort Intelligent Multi-Scan ルールのアップデートが [Security Services] メニュー (GUI) および `antisпамstatus` コマンド (CLI) の対応するページにリストされます。



(注)

アップデートが実行されていないか、サーバが設定されていない場合は、「Never Updated」という文字列が表示されます。

図 8-9 [Security Services] > [IronPort Anti-Spam] ページの [Rules Updates] セクション : GUI

Rule Updates		
Rule Type	Last Update	Current Version
CASE Core Files	Never Updated	3.0.0-031
CASE Utilities	Never Updated	3.0.0-031
Structural Rules	Never Updated	3.0.0-031-20100217_04203
Web Reputation DB	Never Updated	20100217_001708
Web Reputation Rules	Never Updated	20100217_001708-20100217_001708
Content Rules	Never Updated	unavailable
Content Rules Update	Never Updated	unavailable

アンチスパムの受信者別ポリシーの設定

IronPort Anti-Spam ソリューションおよび IronPort Intelligent Multi-Scan ソリューションでは、電子メールセキュリティ マネージャ機能を使用して設定するポリシー (コンフィギュレーション オプション) に基づいて、着信 (および発信) メール用の電子メールを処理します。IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、フィルタリング モジュールによってメッセージをスキャンすることにより分類します。この分類、言い換えれば判定が、後続の配信アクションのために返されます。判定結果として得られる可能性があるのは、スパムでない、不要なマーケティング電子メール、陽性と判定されたスパム、または陽性と疑わしいスパムの 4 つです。スパム陽性と判定されたメッセージ、スパム陽性と疑わしいメッセージ、または不要なマーケティング メッセージであると識別されたメッセージに対するアクションには、次のアクションが含まれません。

- 陽性または陽性と疑わしいスパムのしきい値の指定。

- 不要なマーケティング メッセージ、陽性と判定されたスパム、または陽性と疑わしいスパム メッセージに対する全般的なアクションの選択：配信、ドロップ、バウンス、または検疫。
- mbox 形式のログ ファイルへのメッセージのアーカイブ。スパムであると識別されたメッセージのアーカイブをイネーブルにするには、ログを作成する必要があります。「識別されたメッセージのアーカイブ」(P.8-22) を参照してください。
- スパムまたはマーケティングであると識別されたメッセージの件名ヘッダーの変更。
- 代替宛先メールホストへのメッセージの送信。
- メッセージに対するカスタム X-Header の追加。
- 代替エンベロープ受信者アドレスへのメッセージの送信（たとえば、スパムであると識別されたメッセージを後で調査するために、管理者のメールボックスにルーティングできます）。複数受信者メッセージの場合は、単一のコピーだけが代替受信者に送信されます。



(注)

これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。同じポリシーで、陽性と判定されたスパムと陽性と疑わしいスパムを別々に扱うことができます。たとえば、陽性と判定されたスパムであるメッセージをドロップする一方で、陽性と疑わしいスパム メッセージを検疫する必要がある場合があります。

IronPort Anti-Spam または IronPort Intelligent Multi-Scan のアクションは、電子メール セキュリティ マネージャ機能を使用して、[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ (GUI) または `policyconfig -> antis spam` コマンド (CLI) から、受信者単位を基本にイネーブルにします。アンチスパム ソリューションがグローバルでイネーブルになってから、作成したメール ポリシーごとに、これらのアクションを個別に設定します。異なるメール ポリシーに対して異なるアクションを設定できます。ポリシーごとにイネーブルにできるアンチスパム ソリューションは 1 つだけです。同じポリシーでは両方をイネーブルにできません。



(注) 発信メールのアンチスパム スキャンをイネーブルにするには、関連するホストアクセス テーブルのアンチスパム設定値、特にプライベート リスナーも確認する必要があります。詳細については、「[メール フロー ポリシー : アクセスルールとパラメータ](#)」(P.5-11) を参照してください。

電子メール セキュリティ マネージャの各行は、異なるポリシーを表します。各列は、異なるセキュリティ サービスを表します。

図 8-10 メール ポリシー : アンチスパム エンジン

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default) IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Deliver	(use default) Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	(use default) Disabled	Enabled Enabled	

Key: Default Custom Enabled

メール ポリシーのアンチスパム設定値の編集

メール ポリシーのアンチスパム設定値をユーザごとに編集する処理は、ポリシーが着信メール用であっても、発信メール用であっても、基本的に同じです。

個々のポリシー（デフォルト以外）には、[Use Default] 設定値という追加のフィールドがあります。このフィールドを選択すると、デフォルト メール ポリシーのすべてのアンチスパム設定値がポリシーに導入されます。

詳細については、「[デフォルト ポリシーの編集 : アンチスパム設定](#)」(P.6-34) も参照してください。

デフォルト ポリシーなどのメール ポリシーのアンチスパム設定値を編集する手順は、次のとおりです。

- ステップ 1** 電子メール セキュリティ マネージャの着信または発信メール ポリシー テーブルの任意の行にある、アンチスパム セキュリティ サービスのリンクをクリックします。

☒ 8-11 に示すようなアンチスパム設定値ページが表示されます。

デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。図 8-11 は、具体的なポリシー（デフォルト以外）の設定値を示します。この画面と図 6-6 (P.6-36) を比較してください。[Use Default] オプションが個々のポリシーに付加されている状態に注意してください。

ステップ 2 ポリシーで使用するアンチスパム ソリューションを選択します。

[Disabled] をクリックすると、メール ポリシーのアンチスパム スキャン全体をディセーブルにできます。

ステップ 3 陽性と判定されたスパム、陽性と疑わしいスパム、および不要なマーケティングメッセージの設定値を設定します。

図 8-11 に、編集直前のデフォルト メール ポリシーの IronPort Anti-Spam 設定値を示します。「陽性と判定されたスパムと陽性と疑わしいスパム」(P.8-26) および「識別されたメッセージの設定値を設定する際の注意事項」(P.8-22) を参照してください。

ステップ 4 変更を送信して確定します。

[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページがリフレッシュされて、これまでの手順で選択した値が反映されます。

識別されたメッセージの設定値を設定する際の注意事項

陽性および陽性と疑わしいスパムのしきい値

陽性と判定されたスパムおよび陽性と疑わしいスパムのしきい値に対する値を入力します。スパムしきい値の詳細については、「陽性および陽性と疑わしいスパムのしきい値」(P.8-24) を参照してください。

適用するアクション

陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティングメッセージに対する全般的なアクションを配信、ドロップ、バウンス、または検疫から選択します。

識別されたメッセージのアーカイブ

識別されたメッセージを「アンチスパム アーカイブ」ログにアーカイブできます。この形式は、mbox 形式のログ ファイルです。詳細については、下の例および『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Logging」の章を参照してください。

件名ヘッダーの変更

特定のテキスト文字列を前または後に追加して、識別されたメッセージ上の件名ヘッダーのテキストを変更することにより、スパムおよび不要なマーケティングメッセージをユーザが識別およびソートしやすくなります。



(注)

[Modify message subject] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、前に追加する場合は、末尾に空白をいくつか付けて [SPAM] というテキストを追加します。



(注)

[Add text to message] フィールドでは、US-ASCII 文字だけを使用できます。

識別されたメッセージの代替宛先ホストへの送信

識別されたメッセージを代替宛先メールホストに送信できます。

カスタム X-Header の追加

識別されたメッセージにカスタム X-Header を追加できます。

[Yes] をクリックし、ヘッダー名およびテキストを定義します。

エンベロープ受信者アドレスの変更

識別されたメッセージを代替エンベロープ受信者アドレスに送信できます。

[Yes] をクリックし、代替アドレスを定義します。

たとえば、スパムであると識別されたメッセージを後で調査するために、管理者のメールボックスにルーティングできます。複数受信者メッセージの場合は、単一のコピーだけが代替受信者に送信されます。

図 8-11 メールポリシー用 IronPort Anti-Spam 設定値

Mail Policies: Anti-Spam

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input type="radio"/> Disabled
Positively-Identified Spam Settings	
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [SPAM]
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [SUSPECTED SPAM]
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
Marketing Email Settings	
Enable Marketing Email Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [MARKETING]
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
Spam Thresholds	
Spam is scored on a 2-100 scale. The higher the score, the more likely a message is a spam.	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings:
Positively Identified Spam:	Score > <input type="text" value="90"/> (50 - 100)
Suspected Spam:	Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

陽性および陽性と疑わしいスパムのしきい値

メッセージがスパムであるかどうかを評価するときに、IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、メッセージの総合スパム評点に達するために何千ものルールを適用します。精度の高さを維持するために、この両方のアンチスパムソリューションでは、デフォルトで高いしきい値に設定されています。90 ~ 100 の評点が返されるメッセージは、陽性と判定されたスパムであると見なされます。陽性と判定されたスパムのしきい値は、75（最も積極的）~ 99（最も保守的）で変更できます。アンチスパムソリューションの設定に組織のスパム許容度を反映できます。IronPort Anti-Spam および IronPort Intelligent Multi-Scan の両方に、メールポリシー単位で適用できる、設定可能な陽性スパムおよび陽性と疑わしいスパムのしきい値が用意されています。これ

を利用して、スパムとの類似が見られる一方で、正規のメッセージと共通する特徴も持つグレイゾーンメッセージを示す、「陽性と疑わしいスパム」という任意のカテゴリを作成できます。

この新しいカテゴリのしきい値設定を変更して異なる積極度に変更することにより、陽性と疑わしいスパム範囲に設定した評点未満のすべてのメッセージを、正規のメッセージであると見なし、陽性と疑わしいしきい値を超えており、陽性しきい値未満のすべてのメッセージを、陽性と疑わしいスパムと見なして、適宜処理するように設定できます。陽性と疑わしいスパムに対して実行する個別のアクションを定義することもできます。たとえば、「陽性と判定された」スパムをドロップする一方で、「陽性と疑わしい」スパムを検疫することができます。

入力する数値が大きいほど、メッセージを陽性と疑わしいスパムであると判定するために使用される **IronPort Anti-Spam** ルールのしきい値が高くなります。低いしきい値をイネーブルにして、その結果「スパムの可能性あり」とマークされるメッセージの数を増やすには（**false positive** 率が高くなる可能性あり）、小さい値を入力します。反対に、確実にスパムメッセージだけをフィルタリング対象にするには、大きい数値を入力します（一部のスパムを見逃す可能性あり）。デフォルト値は **50** です。この 2 つのカテゴリを使用する一般的な設定については、「**陽性と判定されたスパムと陽性と疑わしいスパム**」(P.8-26) を参照してください。

陽性と疑わしいスパムのしきい値は、**IronPort Anti-Spam** のメール ポリシーごとに設定されます。

陽性と判定されたスパムと陽性と疑わしいスパム

IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、陽性と判定されたスパムと陽性と疑わしいスパムが区別されるため（「[陽性および陽性と疑わしいスパムのしきい値](#)」(P.8-24)）、次のいずれかの方法でシステムを設定することが一般的です。

表 8-1 陽性と判定されたスパムおよび陽性と疑わしいスパムの一般的な設定の例

スパム	方式 1 のアクション (Aggressive)	方式 2 のアクション (Conservative)
陽性判定	ドロップ	メッセージの件名に「[Positive Spam]」を追加して配信
陽性と疑わしい	メッセージの件名に「[Suspected Spam]」を追加して配信	メッセージの件名に「[Suspected Spam]」を追加して配信

1 番目の設定方式では、陽性と疑わしいスパム メッセージだけにタグを付け、陽性と判定されたメッセージはドロップされます。管理者およびエンドユーザは、着信メッセージの件名行を調べて、**false positive** でないかどうかを確認でき、管理者は必要に応じて、陽性と疑わしいスパムのしきい値を調整できます。

2 番目の設定方式では、陽性と判定されたスパムおよび陽性と疑わしいスパムは、件名を変更して配信されます。ユーザは、陽性と疑わしいスパムおよび陽性と判定されたスパムを削除できます。この方式は、1 番目の方式よりも保守的です。

電子メール セキュリティ マネージャ機能を使用する、受信者ごとを基本とした積極的なポリシーと保守的なポリシーの混合の詳細については、[表 6-6 \(P.6-48\)](#) を参照してください。

不要なマーケティング メッセージの検出

IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、スパムと正規送信元からの不要なマーケティング メッセージを区別できます。マーケティング メッセージはスパムと見なされませんが、組織やエンドユーザによっては、マーケティング メッセージを受信しないことを希望する場合があります。スパム同様、不要なマーケティング メッセージを配信、ドロップ、検疫、またはバ

ウンスすることを選択できます。メッセージの件名にテキストを追加することによって、不要なマーケティングメッセージにタグを付け、マーケティングであることを識別することもできます。

IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー

メールポリシーで IronPort Anti-Spam スキャンまたは Intelligent Multi-Scan がイネーブルにされている場合、そのポリシーを通過する各メッセージでは、次のヘッダーがメッセージに追加されます。

```
X-IronPort-Anti-Spam-Filtered: true
```

IronPort Anti-Spam または Intelligent Multi-Scan によってフィルタリングされた各メッセージについては、別のヘッダーも挿入されます。このヘッダーには、メッセージのスキャンに使用された CASE ルールとエンジンのバージョンを Cisco IronPort Support で識別できる情報が含まれています。

```
X-IronPort-Anti-Spam: result
```

IronPort Intelligent Multi-Scan では、サードパーティ製アンチスパム スキャンエンジンからのヘッダーも追加します。

また、電子メールセキュリティ マネージャ機能を使用すると、特定のポリシーに従って陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティング メールであると識別されたメッセージであるすべてのメッセージに対して、さらに追加するカスタム ヘッダーを定義することもできます（[「カスタム X-Header の追加」\(P.8-23\)](#) を参照）。

skip-spamcheck アクションを使用して、特定のメッセージの IronPort Anti-Spam スキャンをスキップさせるメッセージ フィルタも作成できます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」にある「Bypass Anti-Spam System Action」を参照してください。

誤って分類されたメッセージの Cisco IronPort Systems への報告

分類が誤っていると思われるメッセージを、分析用に Cisco IronPort に報告できます。各メッセージは、専門家チームによってレビューされ、製品の精度と有効性を向上させるために使用されます。各メッセージは、RFC 822 添付ファイルとして、次のアドレスに転送してください。

- spam@access.ironport.com : 見逃されたスパムの報告用
- ham@access.ironport.com : false positive の報告用

誤って分類されたメッセージの報告の詳細については、Cisco IronPort ナレッジベースを参照するか、Cisco IronPort サポート プロバイダーにお問い合わせください。

IronPort Anti-Spam のテスト

アプライアンスの IronPort Anti-Spam 設定をすばやくテストする手順は、次のとおりです。

ステップ 1 メール ポリシーに対して IronPort Anti-Spam をイネーブルにします (上記)。

ステップ 2 X-Advertisement: spam というヘッダーを含むテスト電子メールをそのメールポリシーに含まれているユーザに送信します。

テストを目的として、IronPort Anti-Spam では、X-Advertisement: spam という形式の X-Header を含むすべてのメッセージをスパムであると見なします。このヘッダーを付けて送信したテストメッセージには、IronPort Anti-Spam によってフラグが設定され、メールポリシーに対して設定したアクション（「[アンチスパムの受信者別ポリシーの設定](#)」(P.8-19)）が実行されることを確認できます。trace コマンドを使用してこのヘッダーを組み込むか、Telnet プログラムを使用して SMTP コマンドをアプライアンスに送信することができます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「[Testing and Troubleshooting](#)」の章および付録 A 「[アプライアンスへのアクセス](#)」を参照してください。



(注) アプライアンスの IronPort Anti-Spam の設定をテストする別の方法として、メッセージのヘッダーを調べて IronPort Anti-Spam によって追加された特定のヘッダーを確認する方法もあります。「[IronPort Anti-Spam および Intelligent Multi-Scan によって追加されるヘッダー](#)」(P.8-27) を参照してください。

アンチスパムの性能の評価

インターネットと直接接続した本物のメール ストリームを使用して製品を評価することを強く推奨しています。これは、IronPort Anti-Spam と IronPort Intelligent Multi-Scan のルールは、活発なスパム攻撃を防ぐためにすぐに追加され、攻撃が終結するとすぐに期限切れになるためです。したがって、古いメッセージを使用してテストすると、テスト結果が不正確になります。

「本物」を使用する場合は、スパムとみなされるメッセージが正しく処理されるシステム設定になっているのであれば、X-Advertisement: spam ヘッダーを使用するテスト方法が最適です。trace コマンドを使用するか（「[Debugging Mail Flow Using Test Messages: Trace](#)」(P.446) を参照）、次の例を参照してください。

評価時に陥りがちな落とし穴には、次のようなものがあります。

- 再送信されたか、転送されたメールまたはカット アンド ペーストされたスパム メッセージによる評価

適切なヘッダー、接続 IP、シグニチャなどを持たないメールを使用すると、評点が不正確になります。

- 「難易度の高いスパム」だけをテスト
SBRS、ブラックリスト、メッセージ フィルタなどを使用して「難易度の低いスパム」を取り除くと、全体の検出率が低くなります。
- 別のアンチスパム ベンダーによって検出されたスパムの再送信
- 以前のメッセージのテスト

CASE では、現行の脅威に基づいて、ルールがすぐに追加および削除されます。以前のメッセージのコレクションを使用してテストすると、結果は大幅に不正確になります。

例 :

SMTP コマンドを使用して、X-advertisement: spam ヘッダーを含むテストメッセージを、アクセス権のあるアドレスに送信します。テストアドレス宛でのメッセージを受信するようにメール ポリシーが設定されていること（「[パブリック リスナー \(RAT\) 上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ](#)」(P.5-72) を参照) および HAT で受け入れられるテスト接続であることを確認してください。

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam
port

220 hostname ESMTTP

helo example.com

250 hostname

mail from: <test@example.com>

250 sender <test@example.com> ok

rcpt to: <test@address>

250 recipient <test@address> ok

data

354 go ahead

Subject: Spam Message Test

X-Advertisement: spam

spam test

.

250 Message MID accepted
```

```
221 hostname
```

```
quit
```

次に、テストアカウントのメールボックスを調べて、メールポリシーに設定したアクションに基づいてテストメッセージが正しく配信されたことを確認します。

次の例を参考にしてください。

- 件名行が変更されている。
- 追加のカスタムヘッダーが追加されている。
- メッセージが代替アドレスに配信された。
- メッセージがドロップされた。

着信リレー

着信リレー機能は、ネットワークのエッジにある 1 つまたは複数の Mail Exchange/Transfer エージェント (MX または MTA)、フィルタリングサーバなどを介して Cisco IronPort アプライアンスにメールを送信している外部マシンの IP アドレスを、Cisco IronPort アプライアンスで取得するために有用です。このタイプの設定では、Cisco IronPort アプライアンスで外部マシンの IP アドレスを自動的に認識しません。代わりに、外部マシンではなくローカル MX/MTA (着信リレー) から発信されたメールであると認識されます。IronPort Anti-Spam および IronPort Intelligent Multi-Scan では、外部送信者の正確な IP アドレスを必要としているため、Cisco IronPort アプライアンスにとってこの情報の取得は不可欠です。

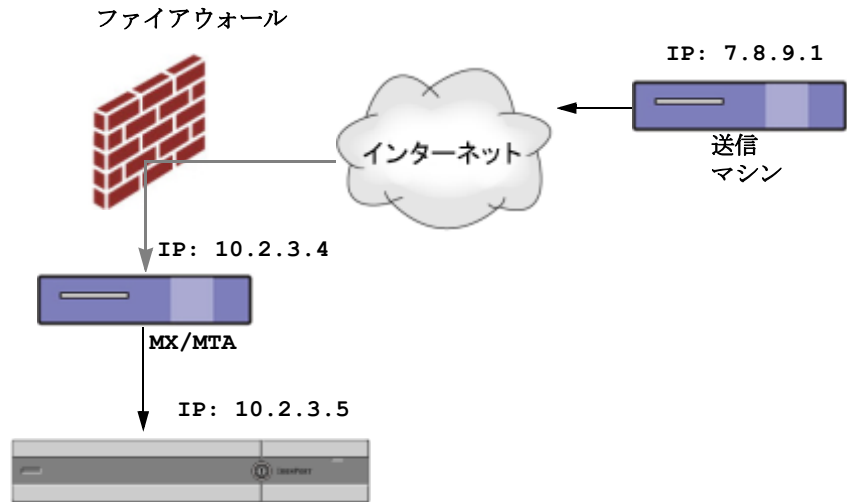


(注)

この機能は、Cisco IronPort アプライアンスにメールをリレーするローカル MX/MTA がある場合に限りイネーブルにしてください。

図 8-12 に、きわめて基本的な着信リレーの例を示します。ローカル MX/MTA によってメールが Cisco IronPort アプライアンスにリレーされているため、IP アドレス 7.8.9.1 からのメールは IP アドレス 10.2.3.4 からのように見えます。

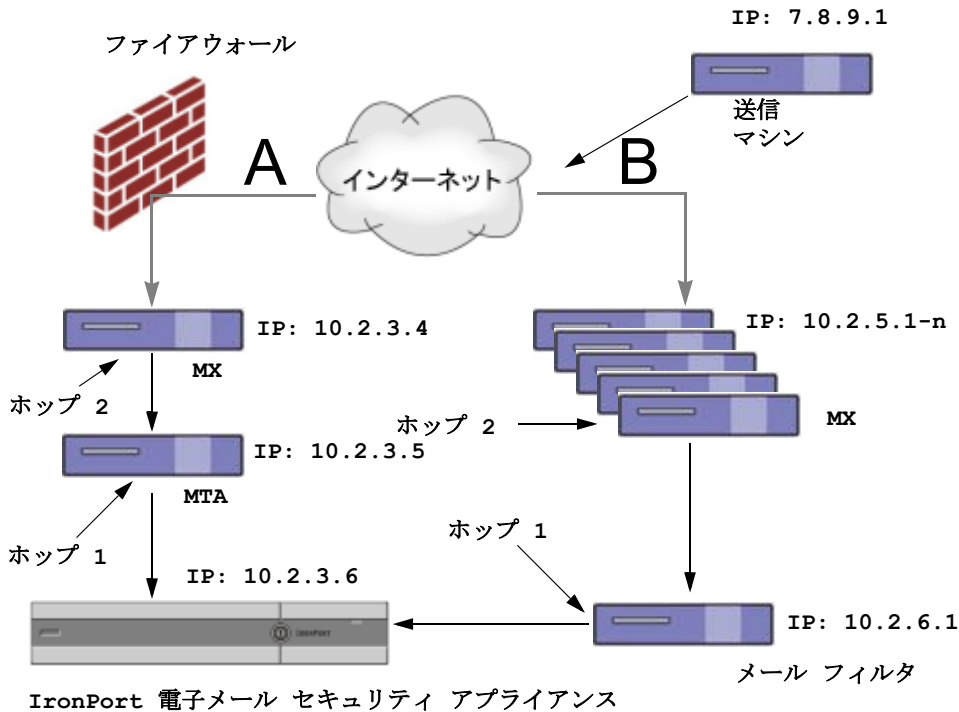
図 8-12 MX/MTA によるメール リレー：簡易



IronPort 電子メール セキュリティ アプライアンス

図 8-13 に別の 2 つの例を示します。この例は、少し複雑であり、ネットワーク内でのメールのリレー方法と、Cisco IronPort アプライアンスへの受け渡し前に実施できる、ネットワーク内の複数サーバにおけるメールの処理方法を示します。例 A では、7.8.9.1 からのメールがファイアウォールを通過し、MX および MTA で処理されてから、Cisco IronPort アプライアンスに配信されます。例 B では、7.8.9.1 からのメールがロード バランサまたは他のタイプのトラフィックシェーピング アプライアンスに送信され、一連の MX のいずれかに送信されてから、Cisco IronPort アプライアンスに配信されます。

図 8-13 MX/MTA によるメール リレー：拡張



着信リレー機能：概要

管理者は、インターネットからメールを直接受信する代わりに、ネットワークのエッジにある Mail Exchange (MX) または Mail Transfer Agent (MTA) の背後で Cisco IronPort アプライアンスを実行しなければならない場合があります。この設定を使用する場合、Cisco IronPort アプライアンスでは、残念ながらインターネットからメールを直接受信しないため、外部ネットワークからの直前の接続 IP アドレスがわかりません。受信メールは、代わりに、ローカル MX/MTA から受信されたと示されます。接続 IP アドレスが既知であり、IronPort Intelligent Multi-Scan および IronPort Anti-Spam のスキャンで SenderBase 評価サービスを使用できることは、Cisco IronPort アプライアンスの正常な動作にとって不可欠です。

これは、着信リレーを設定することによって解決されます。着信リレーを設定するときは、Cisco IronPort アプライアンスに接続するすべての内部 MX/MTA の名前と IP アドレスおよび送信元 IP アドレスの格納に使用するヘッダーを指定します。ヘッダーを指定する方法は、カスタム ヘッダーと既存の Received ヘッダーの 2 通りあります。

着信リレーと電子メール セキュリティ モニタ

着信リレー機能を使用する場合、電子メール セキュリティ モニタによって準備されるデータには、外部 IP と MX/MTA の両方のデータが含まれています。たとえば、外部マシン (IP 7.8.9.1) から内部 MX/MTA (IP 10.2.3.4) を介して 5 通の電子メールが送信された場合、[Mail Flow Summary] には、IP 7.8.9.1 からの 5 個のメッセージに加えて、内部リレー MX/MTA (IP 10.2.3.5) からの 5 個のメッセージが表示されます。

着信リレーとフィルタ

着信リレー機能では、SenderBase 評価サービスに関連するさまざまなフィルタールール (reputation、no-reputation) に正しい SenderBase 評価スコアを提供します。

着信リレー、HAT、SBRS および送信者グループ

HAT ポリシー グループでは、着信リレーからの情報を現時点では使用していません。ご注意ください。ただし、着信リレー機能では SenderBase 評価スコアを提供するため、メッセージフィルタおよび \$reputation 変数によって HAT ポリシー グループ機能をシミュレートできます。

着信リレーとレポート

着信リレーを使用している場合、電子メール セキュリティ モニタ レポートに示される SenderBase 評価スコアは正しくありません。送信者グループが正しく解決されない場合もあります。

IP アドレス

Cisco IronPort アプライアンスに接続するマシンの IP アドレス（着信リレー）を指定するときは、原則としてできるだけ個別に指定してください。つまり、IP アドレスは、標準 CIDR 形式または IP アドレスの範囲でも入力できます。たとえば、電子メールを受信する複数の MTA をネットワークのエッジに配置している場合に、すべての MTA を含む IP アドレスの範囲、たとえば 10.2.3.1/8 や 10.2.3.1-10 を入力する場合があります。

メッセージ ヘッダーと着信リレー

カスタム ヘッダー

カスタム ヘッダーを指定する場合に、この方法を使用します。これは推奨される方法です。元の送信者に接続するマシンでは、このカスタム ヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予期されます。次の例を参考にしてください。

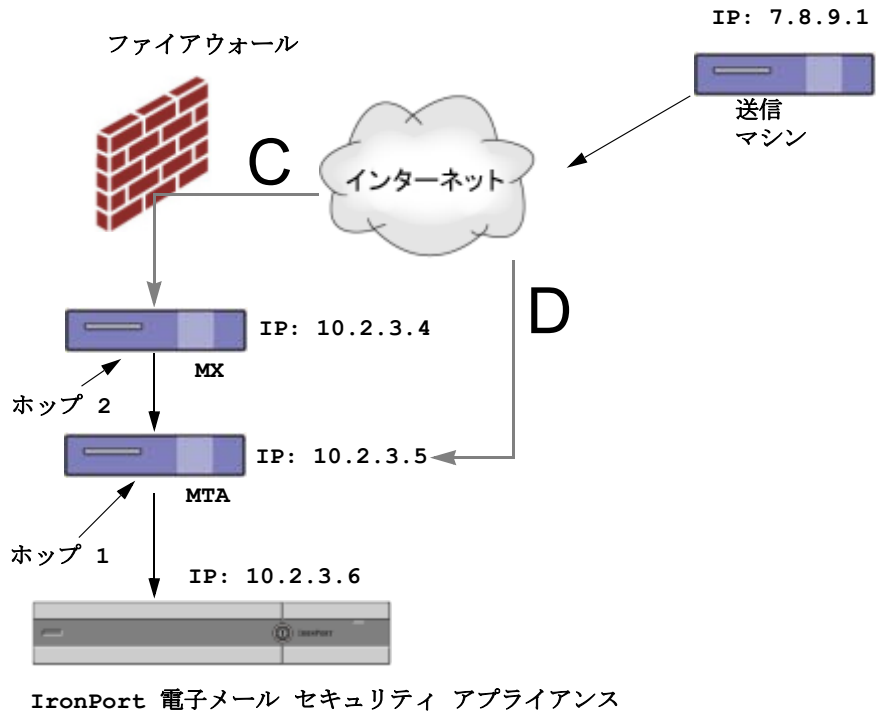
```
SenderIP: 7.8.9.1
```

```
X-CustomHeader: 7.8.9.1
```

ヘッダーを入力する場合に、末尾のコロンを入力する必要はありません。

ローカル MX/MTA で不定ホップ数のメールを受信する場合は、カスタム ヘッダーを挿入することが、着信リレー機能をイネーブルにする唯一の方法です。たとえば、[図 8-14](#) では、パス C とパス D の両方が IP アドレス 10.2.3.5 まで至る一方で、パス C は 2 ホップ、パス D は 1 ホップです。この状況では、ホップ数が異なる場合があるため、カスタム ヘッダーを使用して、着信リレーが正しく設定されるようにする必要があります。

図 8-14 MX/MTA によるメール リレー：不定ホップ数



Received ヘッダー

MX/MTA を設定する場合、送信 IP アドレスを含むカスタム ヘッダーの組み込みは選択肢になりません。着信リレー機能は、メッセージの「Received:」ヘッダーを調査することによって送信 IP アドレスの判別を試行するように設定できます。「Received:」ヘッダーを使用する方法は、ネットワーク ホップ数が常に一定である IP アドレスの場合に限り機能します。つまり、最初のホップにあるマシン (図 8-13 の 10.2.3.5) は、ネットワークのエッジからのホップ数が常に等しい必要があります。Cisco IronPort アプライアンスに接続しているマシンまでの着信メールのパスが異なる可能性がある場合 (したがって、図 8-14 で示したように、ホップ数が異なる場合) は、カスタム ヘッダーを使用する必要があります (「カスタム ヘッダー」(P.8-35) を参照)。

解析対象文字または文字列および逆行して検索するネットワーク ホップ数（または Received: ヘッダー数）を指定します。ホップは、基本的に、メッセージがマシン間で転送されることを指します（Cisco IronPort アプライアンスによる受信はホップとしてカウントされません。詳細については、「[使用されるヘッダーの特定](#)」(P.8-39)を参照してください)。AsyncOS は、指定されたホップ数に対応する Received: ヘッダー内の解析対象文字または文字列の最初のオカレンスに続く最初の IP アドレスを参照します。たとえば、2 ホップを指定した場合は、Cisco IronPort アプライアンスから逆行して 2 つめの Received: ヘッダーが解析されます。解析対象の文字が見つからないか、有効な IP アドレスが見つからない場合、Cisco IronPort アプライアンスでは、接続元マシンの実際の IP アドレスを使用します。

次のメールヘッダーの例で左角カッコ ([]) と 2 ホップを指定した場合、外部マシンの IP アドレスは 7.8.9.1 です。ただし、右カッコ (()) および解析対象文字を指定した場合は、有効な IP アドレスが見つかりません。この場合、着信リレー機能はディセーブルであると見なされ、接続元マシンの IP (10.2.3.5) が使用されます。

図 8-13 の例における着信リレーは次のとおりです。

- パス A : 10.2.3.5 (Received ヘッダーを使用して 2 ホップ) および
- パス B : 10.2.6.1 (Received ヘッダーを使用して 2 ホップ)

表 8-2 に、図 8-13 同様、Cisco IronPort アプライアンスまで複数の移動ホップ数を持つメッセージの電子メールヘッダーの例を示します。この例は、受信者の受信箱に到着したメッセージで表示される、外部からのヘッダー (Cisco IronPort アプライアンスでは無視) を示します。指定するホップ数は 2 になります。表 8-3 に、外部ヘッダーを除いて、同じ電子メールメッセージのヘッダーを示します。

表 8-2 一連の Received: ヘッダー (パス A 例 1)

1	<pre>Microsoft Mail Internet Headers Version 2.0 Received: from smemail.rand.org ([10.2.2.7]) by smmail5.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713); Received: from ironport.customerdomain.org ([10.2.3.6]) by smemail.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713);</pre>
2	<pre>Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTTP; 21 Sep 2005 13:46:07 -0700</pre>

表 8-2 一連の Received: ヘッダー (パス A 例 1) (続き)

3	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4] by mta.customerdomain.org (8.12.11/8.12.11) with ESMTTP id j8LkKwU1008155 for <joefoo@customerdomain.org>
4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTTP id 4F3DA15AC22 for <joefoo@customerdomain.org>
5	Received: from linux1.thespammer.com (HELO linux1.thespammer.com) ([10.1.1.89]) by sending-machine.spamham.com with ESMTTP; Received: from exchangel.thespammer.com ([10.1.1.111]) by linux1.thespammer.com with Microsoft SMTPSVC(6.0.3790.1830); Subject: Would like a bigger paycheck? Date: Wed, 21 Sep 2005 13:46:07 -0700 From: "A.Sender" <asend@otherdomain.com> To: <joefoo@customerdomain.org>

表 8-2 についての注意事項は、次のとおりです。

- ステップ 1** Cisco IronPort アプライアンスでは、これらのヘッダーを無視します。
- ステップ 2** Cisco IronPort アプライアンスがメッセージを受信します (ホップとしてカウントされない)。
- ステップ 3** 最初のホップ (着信リレー)。
- ステップ 4** 第 2 ホップ。これは、送信 MTA です。仮想 IP アドレスは 7.8.9.1 です。
- ステップ 5** Cisco IronPort アプライアンスでは、これらの Microsoft Exchange ヘッダーを無視します。

表 8-3 一連の Received: ヘッダー (パス A 例 2)

1	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTTP; 21 Sep 2005 13:46:07 -0700
---	---

表 8-3 一連の Received: ヘッダー (パス A 例 2) (続き)

2	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4] by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LkKwU1008155 for <joefoo@customerdomain.org>;
3	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;

図 8-15 に、GUI の [Add Relay] ページで設定されたパス A の着信リレーを示します。

図 8-15 設定された着信リレー

The screenshot shows the 'Incoming Relay' configuration interface. It includes the following fields and options:

- Name:** IncomingRelayOne
- IP Address:** 10.2.3.5
- Header:**
 - Specify a custom header
 - Parse the "Received" header
- Begin parsing after:** [Empty field]
- Hop:** 2

使用されるヘッダーの特定

Cisco IronPort アプライアンスでは、メッセージが受信された時点で存在していたヘッダーだけを検査します。したがって、ローカルで追加される追加のヘッダー (Microsoft Exchange のヘッダーなど) や、Cisco IronPort アプライアンスがメッセージを受信するときに追加する追加のヘッダーは、処理されません。使用されるヘッダーを特定する方法の 1 つは、logconfig CLI コマンドの logheaders サブコマンドを使用して、Received ヘッダーを AsyncOS ロギングに含めるよう設定することです。

```
mail3.example.com> logconfig
```

```
Currently configured logs:
```

```
[ ... list of configured logs ... ]
```

Choose the operation you want to perform:

- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
- CLUSTERSET - Set how logs are configured in a cluster.
- CLUSTERSHOW - Display how logs are configured in a cluster.

```
[ ]> logheaders
```

Please enter the list of headers you wish to record in the log files.

Separate multiple headers with commas.

```
[ ]> Received
```

着信リレー機能の設定 (GUI)

[Incoming Relays] ページは [Network] タブから使用可能です。

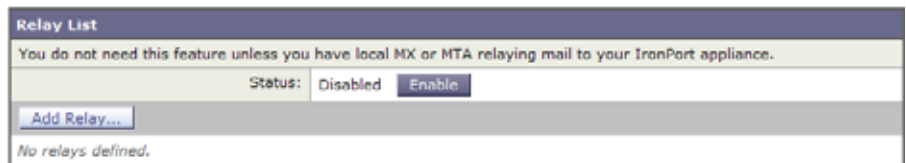
着信リレー機能のイネーブル化

着信リレー機能をイネーブルにした場合は、アプライアンスに対してグローバルでイネーブルになります（リレーはリスナー固有でない）。着信リレー機能をイネーブルにする手順は、次のとおりです。

- ステップ 1** [Network] タブの [Incoming Relays] リンクをクリックします。[Incoming Relays] ページが表示されます。

図 8-16 [Incoming Relays] ページ

Incoming Relays



- ステップ 2** [Enable] をクリックして、着信リレーをイネーブルにします（イネーブルにした着信リレー機能は、[Disable] をクリックすることによって、ディセーブルにできます）。
- ステップ 3** 変更を確定します。

着信リレーとメール ログ

次の例は、着信リレー情報を含む、一般的なログ エントリを示します。

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay):
Header Received found, IP 192.168.230.120 being used
```

リレーの追加

リレーを追加する手順は、次のとおりです。

- ステップ 1** [Incoming Relays] ページの [Add Relay] ボタンをクリックします。[Add Relay] ページが表示されます。

図 8-17 [Add Relay] ページ
Add Relay

- ステップ 2** リレーの名前を入力します。
- ステップ 3** リレーの IP アドレスを入力します。有効な IP アドレス エントリの詳細については、「[IP アドレス](#)」(P.8-35) を参照してください。
- ステップ 4** ヘッダー タイプ ([Custom] または [Received]) を選択します。カスタム ヘッダーの詳細については、「[カスタム ヘッダー](#)」(P.8-35) を参照してください。ヘッダーを入力する場合に、末尾のコロンを入力する必要はありません。
- カスタム ヘッダーの場合は、ヘッダー名を入力します。
 - **Received:** ヘッダーの場合は、IP アドレスの前に配置される文字または文字列を入力します。IP アドレスを調査するホップ数を入力します。詳細については、「[Received ヘッダー](#)」(P.8-36) を参照してください。
- ステップ 5** 変更を確定します。

リレーの編集

リレーを編集する手順は、次のとおりです。

- ステップ 1** [Incoming Relay] ページでリレーの名前をクリックします。[Edit Relay] ページが表示されます。
- ステップ 2** リレーに変更を加えます。
- ステップ 3** 変更を確定します。

リレーの削除

リレーを削除する手順は、次のとおりです。

- ステップ 1** 削除するリレーに対応する行のゴミ箱アイコンをクリックします。削除を確認するよう求められます。
- ステップ 2** [Delete] をクリックします。
- ステップ 3** 変更を確定します。

着信リレーとロギング

次のログの例で、送信者の **SenderBase** 評価スコアは、当初 1 行目に示されます。その後、着信リレーの処理が行われて、正しい **SenderBase** 評価スコアが 5 行目に示されます。

1	Fri Apr 28 17:07:29 2006 Info: ICID 210158 ACCEPT SG UNKNOWNLIST match nx.domain SBRS rfc1918
2	Fri Apr 28 17:07:29 2006 Info: Start MID 201434 ICID 210158
3	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 From: <joe@sender.com>
4	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 RID 0 To: <mary@example.com>
5	Fri Apr 28 17:07:29 2006 Info: MID 201434 IncomingRelay(senderdotcom): Header Received found, IP 192.192.108.1 being used, SBRS 6.8
6	Fri Apr 28 17:07:29 2006 Info: MID 201434 Message-ID '<7.0.1.0.2.20060428170643.0451be40@sender.com>'
7	Fri Apr 28 17:07:29 2006 Info: MID 201434 Subject 'That report...'
8	Fri Apr 28 17:07:29 2006 Info: MID 201434 ready 2367 bytes from <joe@sender.com>
9	Fri Apr 28 17:07:29 2006 Info: MID 201434 matched all recipients for per-recipient policy DEFAULT in the inbound table
10	Fri Apr 28 17:07:34 2006 Info: ICID 210158 close
11	Fri Apr 28 17:07:35 2006 Info: MID 201434 using engine: CASE spam negative
12	Fri Apr 28 17:07:35 2006 Info: MID 201434 antivirus negative
13	Fri Apr 28 17:07:35 2006 Info: MID 201434 queued for delivery



CHAPTER 9

アンチウイルス

Cisco IronPort アプライアンスには、Sophos, Plc 製および McAfee, Inc. 製のウイルス スキャン エンジンが統合されています。Cisco IronPort アプライアンスのライセンス キーを取得して、これらのウイルス スキャン エンジンのいずれかまたは両方を使用し、メッセージのウイルスをスキャンできます。

(一致する着信または発信メール ポリシーに基づいて) メッセージのウイルスをスキャンし、ウイルスが見つかった場合はメッセージに対してさまざまなアクション (たとえば、ウイルスの発見されたメッセージの「修復」、件名ヘッダーの変更、X-Header の追加、代替アドレスまたはメールホストへのメッセージの送信、メッセージのアーカイブ、またはメッセージの削除など) を実行するようにアプライアンスを設定できます。

ウイルス スキャンをイネーブルにした場合は、アンチスパム スキャンの直後に、アプライアンス上の「ワーク キュー」でウイルス スキャンが実行されます (「電子メール パイプラインの理解」(P.4-1) を参照)。

デフォルトでは、ウイルス スキャンはデフォルトの着信および発信メール ポリシーに対してイネーブルになります。

この章の内容は、次のとおりです。

- 「アンチウイルス スキャン」 (P.9-2)
- 「Sophos Anti-Virus フィルタリング」 (P.9-3)
- 「McAfee Anti-Virus フィルタリング」 (P.9-7)
- 「ウイルス スキャンのイネーブル化およびグローバル設定の構成」 (P.9-9)
- 「ユーザのウイルス スキャン アクションの設定」 (P.9-12)
- 「ウイルス スキャンのテスト」 (P.9-28)

アンチウイルス スキャン

Cisco IronPort アプライアンスは、McAfee または Sophos のアンチウイルス スキャン エンジンを使用してウイルスをスキャンするように設定できます。

McAfee および Sophos のエンジンには、特定のポイントでのファイルのスキャン、ファイルで発見されたデータとウイルス定義のパターン照合と処理、エミュレーション環境でのウイルス コードの復号化および実行、新しいウイルスを認識するための発見的手法の適用、および正規ファイルからの感染コードの削除に必要なプログラム ロジックが含まれています。

評価キー

Cisco IronPort アプライアンスには、使用可能な各アンチウイルス スキャン エンジンに対して 30 日間有効な評価キーが同梱されています。評価キーは、System Setup Wizard または [Security Services] > [Sophos] または [McAfee Anti-Virus] ページのライセンス契約書にアクセスするか (GUD)、または `antivirusconfig` または `systemsetup` コマンドを実行して (CLI) イネーブルにします。デフォルトでは、ライセンス契約書に同意すると、アンチウイルス スキャン エンジンはデフォルトの着信および発信メール ポリシーに対してただちにイネーブルになります。30 日間の評価期間後もこの機能をイネーブルにする場合の詳細については、Cisco IronPort の営業担当者にお問い合わせください。残りの評価期間は、[System Administration] > [Feature Keys] ページを表示するか、または `featurekey` コマンドを発行することによって確認できます (詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」にある、機能キーの操作に関する項を参照してください)。

マルチレイヤ アンチウイルス スキャン

AsyncOS は、複数のアンチウイルス スキャン エンジンによるメッセージのスキャン (マルチレイヤ アンチウイルス スキャン) をサポートしています。メール ポリシーごとに、ライセンスを受けたアンチウイルス スキャン エンジンのいずれかまたは両方を使用するように Cisco IronPort アプライアンスを設定できます。たとえば、経営幹部用のメール ポリシーを作成し、そのポリシーでは Sophos および McAfee の両方のエンジンを使用してメールをスキャンするように設定することもできます。

複数のスキャン エンジンでメッセージをスキャンすることにより、Sophos および McAfee のアンチウイルス スキャン エンジン双方の利点を組み合わせた「多重防衛」が実現します。各エンジンともに業界をリードするアンチウイルス捕捉率を誇りますが、各エンジンは別々のテクノロジー基盤（「McAfee Anti-Virus フィルタリング」(P.9-7) および「Sophos Anti-Virus フィルタリング」(P.9-3) を参照）に依存してウイルスを検出しているため、マルチスキャン方式を使用することで、より効果が高まります。複数のスキャン エンジンを使用することで、システム スループットが低下する場合があります。詳細は、Cisco IronPort のサポート担当者にお問い合わせください。

ウイルス スキャンの順序は設定できません。マルチレイヤ アンチウイルス スキャンをイネーブルにした場合、最初に McAfee エンジンによるウイルス スキャンが実行され、次に Sophos エンジンによるウイルス スキャンが実行されます。McAfee エンジンがメッセージはウイルスに感染していないと判断した場合は、Sophos エンジンはさらにメッセージをスキャンして、別の保護層を追加します。McAfee エンジンがメッセージはウイルスを含んでいると判断した場合は、Cisco IronPort アプライアンスは Sophos によるスキャンをスキップし、構成した設定に応じてウイルス メッセージに対してアクションを実行します。

Sophos Anti-Virus フィルタリング

Cisco IronPort アプライアンスには、Sophos の総合的なウイルス スキャン テクノロジーが含まれています。Sophos Anti-Virus は、プラットフォーム間のアンチウイルス保護、検出、および除去を提供します。

Sophos Anti-Virus は、ファイルをスキャンしてウイルス、トロイの木馬、およびワームを検出するウイルス検出エンジンを提供します。これらのプログラムは、「悪意のあるソフトウェア」を意味するマルウェアと総称されます。アンチウイルス スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

ウイルス検出エンジン

Sophos ウイルス検出エンジンは、Sophos Anti-Virus テクノロジーの中心的役割を担います。このエンジンは、Microsoft の Component Object Model (COM; コンポーネント オブジェクト モデル) と同様の、多くのオブジェクトと明確に定義されたインターフェイスで構成された独自のアーキテクチャを使用します。

エンジンで使用されるモジュラ ファイリング システムは、それぞれが異なる「ストレージクラス」（たとえばファイル タイプなど）を処理する、個別の内蔵型動的ライブラリに基づいています。この方法では、タイプに関係なく汎用のデータ ソースにウイルス スキャン操作を適用できます。

エンジンは、データのロードおよび検索に特化したテクノロジーにより、非常に高速なスキャンを実現できます。次の機能が内蔵されています。

- ポリモーフィック型ウイルスを検出するためのフル コード エミュレータ。
- アーカイブ ファイル内をスキャンするためのオンライン解凍プログラム。
- マクロ ウイルスを検出および駆除するための OLE2 エンジン。

Cisco IronPort アプライアンスは、SAV インターフェイスを使用してウイルス エンジンを統合しています。

ウイルス スキャン

大まかにいうと、エンジンのスキャン機能は、検索する場所を特定する分類子と、検索する対象を特定するウイルス データベースという 2 つの重要なコンポーネントの高性能な組み合わせにより管理されています。エンジンは、識別子に依存せずに、タイプでファイルを分類します。

ウイルス エンジンは、システムが受信したメッセージの本文および添付ファイルでウイルスを検索しますが、スキャンの実行方法の決定には、添付ファイルのタイプが役立ちます。たとえば、メッセージの添付ファイルが実行ファイルであれば、エンジンは実行コードの開始場所が記述されているヘッダーを調べて、その場所を検索します。ファイルが Word ドキュメントであれば、エンジンはマクロ ストリームを調べます。MIME ファイル（メール メッセージに使用される形式）であれば、添付ファイルが保存されている場所を調べます。

検出方法

ウイルスの検出方法は、ウイルスのタイプに応じて異なります。スキャン処理中に、エンジンは各ファイルを分析してタイプを特定してから、該当する手法を適用します。すべての方法の根幹には、特定のタイプの命令または特定の命令の順序を検索するという基本概念があります。

パターン照合

パターン照合の手法では、エンジンは特定のコードシーケンスを知っており、そのコードシーケンスと完全一致するコードをウイルスとして特定します。たいていの場合、エンジンは既知のウイルスコードのシーケンスに類似した（必ずしも完全に同一である必要はありません）コードのシーケンスを検索します。スキャン実行中にファイルを比較する対象となる記述を作成する際、Sophosのウイルス研究者達は、エンジンが（次で説明する発見的手法を使用して）オリジナルのウイルスだけでなく、後の派生的なウイルスも発見できるように、識別コードを可能な限り一般的なものに維持することに努めています。

発見的手法

ウイルスエンジンは、基本的なパターン照合手法と発見的手法（特定のルールではなく一般的なルールを使用する手法）を組み合わせることで、Sophosの研究者があるファミリーの1種類のウイルスしか分析していなかったとしても、そのファミリーの複数のウイルスを検出できます。この手法では、記述を1つ作成すれば、ウイルスの複数の派生形を捕らえることができます。Sophosは、発見的手法にその他の手法を加味することで、**false positive**の発生を最低限に抑えています。

エミュレーション

エミュレーションは、ポリモーフィック型ウイルスに対して、ウイルスエンジンによって適用される手法です。ポリモーフィック型ウイルスは、ウイルスを隠す目的のために、ウイルス自体を別の形に変更する暗号化されたウイルスです。明らかな定型的ウイルスコードは存在せず、拡散するたびにウイルス自体が別の形に暗号化されます。このウイルスは、実行されたときに自己復号化します。ウイルス検出エンジンのエミュレータは、DOSまたはWindows実行ファイルに使用されますが、ポリモーフィック型マクロはSophosのウイルス記述言語で記述された検出コードによって発見されます。

この復号化の出力は実際のウイルスコードであり、エミュレータで実行された後にSophosのウイルス検出エンジンによって検出されるのは、この出力です。

スキャン用にエンジンに送信された実行ファイルは、エミュレータ内で実行されます。エミュレータでは、ウイルス本文の復号化がメモリに書き込まれ、これに応じて復号化が追跡されます。通常、ウイルスの侵入ポイントはファイルのフロントエンドにあり、最初に行われる部分です。ほとんどの場合、ウイルスであ

ることを認識するためには、ウイルス本文のほんのわずかな部分を復号化するだけで十分です。クリーンな実行ファイルの多くは、数個の命令をエミュレートするだけでエミュレーションを停止して、負担を軽減します。

エミュレータは制限された領域で実行されるため、コードがウイルスであるとわかっても、アプライアンスに感染することはありません。

ウイルスの記述

Sophos は、他の信用されているアンチウイルス企業と毎月ウイルスを交換しています。さらに、顧客から毎月数千の疑わしいファイルが直接 Sophos に送られ、そのうち約 30 % はウイルスであると判明しています。各サンプルは、非常にセキュアなウイルス ラボで厳しく分析され、ウイルスかどうか判断されます。Sophos は、新しく発見された各ウイルスまたはウイルスのグループに対して、記述を作成します。

Sophos アラート

Sophos Anti-Virus スキャンをイネーブルにしているお客様に対して、Sophos のサイト (<http://www.sophos.com/virusinfo/notifications/>) から Sophos アラートを購読することを推奨しています。

購読して Sophos から直接アラートを受け取ることにより、最新のウイルスの発生および利用可能な解決方法が確実に通知されます。

ウイルスが発見された場合

ウイルスが検出されたら、Sophos Anti-Virus はファイルを修復（駆除）できます。通常、Sophos Anti-Virus は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、**Email Security 機能** ([Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ (GUI) または `policyconfig -> antivirus` コ

マンド (CLI) を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、「[ユーザのウイルス スキャン アクションの設定](#)」(P.9-12) を参照してください。

McAfee Anti-Virus フィルタリング

McAfee® スキャン エンジンは、次の処理を行います。

- ファイルのデータとウイルス シグニチャをパターン照合することにより、ファイルをスキャンします。
- エミュレーション環境でウイルス コードを復号化および実行します。
- 発見的手法を適用して新しいウイルスを認識します。
- ファイルから感染性のコードを削除します。

ウイルス シグニチャとのパターン照合

McAfee は、アンチウイルス定義 (DAT) ファイルをスキャン エンジンで使用して、特定のウイルス、ウイルスのタイプ、またはその他の潜在的に望ましくないソフトウェアを検出します。また、ファイル内の既知の場所を開始点としてウイルス固有の特徴を検索することにより、単純なウイルスを検出できます。多くの場合、ファイルのほんの一部を検索するだけで、ファイルがウイルスに感染していないと判断できます。

暗号化されたポリモーフィック型ウイルスの検出

複雑なウイルスは、次の 2 つの一般的な手法を使用して、シグニチャ スキャンによる検出を回避します。

- **暗号化**。ウイルス内部のデータは、アンチウイルス スキャナがメッセージまたはウイルスのコンピュータ コードを判読できないように、暗号化されます。ウイルスがアクティブになると、ウイルス自体が自発的に実行バージョンに変化し、自己実行します。
- **ポリモーフィック化**。この処理は暗号化に似ていますが、ウイルスが自己複製する際に、その形が変わる点で暗号化とは異なります。

このようなウイルスに対抗するために、エンジンはエミュレーションと呼ばれる手法を使用します。エンジンは、ファイルにこのようなウイルスが含まれていると疑った場合、ウイルスが他に害を及ぼすことなく自己実行して、本来の形が判読できる状態まで自分自身をデコードする人工的な環境を作成します。その後、エンジンは通常どおりウイルスシグニチャをスキャンして、ウイルスを特定します。

発見的分析

新しいウイルスの署名は未知であるため、ウイルスシグニチャを使用するだけでは、新しいウイルスは検出できません。そのため、エンジンは追加で発見的分析という手法を使用します。

ウイルスを運ぶプログラム、ドキュメント、または電子メールメッセージには、多くの場合、特異な特徴があります。これらは、自発的にファイルの変更を試行したり、メールクライアントを起動したり、またはその他の方法を使用して自己複製します。エンジンはプログラムコードを分析して、この種のコンピュータ命令を検出します。また、エンジンは、アクションを実行する前にユーザの入力を求めたりするようなウイルスらしくない正規の動作も検索して、誤ったアラームを発行しないようにしています。

このような手法を使用することで、エンジンは多くの新しいウイルスを検出できます。

ウイルスが発見された場合

ウイルスが検出されたら、McAfee はファイルを修復（駆除）できます。通常、McAfee は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

ファイルの駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、時折、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、Email Security 機能 ([Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ (GUI) または `policyconfig -> antivirus` コマンド (CLI)) を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、「ユーザのウイルス スキャンアクションの設定」(P.9-12) を参照してください。

ウイルス スキャンのイネーブル化およびグローバル設定の構成

ウイルス スキャンを実行するには、最初に Cisco IronPort アプライアンスでウイルス スキャンをイネーブルにする必要があります。ウイルス スキャン エンジン (1 つまたは複数) をイネーブルにした後に、ウイルス スキャン エンジンを着信または発信メール ポリシーに適用できます。

概要

ウイルス スキャン エンジンは、System Setup Wizard を実行したときにイネーブルにできます。または、[Security Services] > [Sophos] または [McAfee Anti-Virus] ページ (GUI) または `antivirusconfig` コマンド (CLI) を使用して、ウイルス スキャン エンジンのグローバル コンフィギュレーション設定をイネーブルにしたり、変更したりできます。次のグローバル設定を構成できます。

- システム全体に対してグローバルに McAfee または Sophos Anti-Virus スキャンをイネーブルにする。
- アンチウイルス スキャンのタイムアウト値を指定する。

グローバル設定ページの 2 つの値に加えて、[Service Updates] ページ ([Security Services] タブから使用できます) で、さらにアンチウイルス設定を構成できます。追加の設定には、次のようなものが含まれます。

- システムのアンチウイルス アップデートの取得方法 (取得先 URL)。ウイルス定義は動的 URL からアップデートされます。厳格なファイアウォールポリシーを適用している場合は、静的 URL からアップデートを取得するように Cisco IronPort アプライアンスを設定する必要がある場合があります。
- システムが新しいウイルス定義をチェックする頻度 (チェックの間隔を何分にするか定義します)。
- 任意で、アンチウイルス アップデートを取得するプロキシ サーバをイネーブルにできます。

追加設定の構成に関する詳細については、「サービスのアップデート」(P.15-16) を参照してください。

ウイルス スキャンのイネーブル化およびグローバル設定の構成

前もって System Setup Wizard でアンチウイルス エンジンを実行している場合（GUI については「[手順 4 : Security](#)」(P.3-31)、CLI については「[アンチウイルス スキャンのイネーブル化](#)」(P.3-54) を参照してください)、アンチウイルス スキャンを実行するには、次の手順を実行してください。

ステップ 1 [Security Services] > [McAfee] を選択します。

または

[Security Services] > [Sophos] を選択します。

ステップ 2 [Enable] をクリックします。ライセンス契約書ページが表示されます。



(注) [Enable] をクリックすると、アプライアンスで機能がグローバルにイネーブルになります。ただし、後で [Mail Policies] で受信者ごとの設定をイネーブルにする必要があります。

ステップ 3 ライセンス契約書を読み、ページの最後までスクロールしてから [Accept] をクリックして契約に同意します。

ステップ 4 [Edit Global Settings] をクリックします。

ステップ 5 ウィルス スキャンの最大タイムアウト値を選択します。

システムがメッセージに対するアンチウイルス スキャンの実行を停止する、タイムアウト値を設定します。デフォルト値は 60 秒です。

ステップ 6 変更を送信して確定します。

ステップ 7 これで、アンチウイルス設定を受信者ごとに構成できるようになりました。「[ユーザのウイルス スキャンアクションの設定](#)」(P.9-12) を参照してください。



(注) アンチウイルス スキャンの適用方法および適用時期の詳細については、「[電子メール パイプラインとセキュリティ サービス](#)」(P.4-9) を参照してください。

HTTP を使用した Anti-Virus アップデートの取得

デフォルトでは、Cisco IronPort アプライアンスは、5 分ごとにアップデートをチェックするように設定されています。Sophos および McAfee のアンチウイルス エンジンの場合は、サーバは動的 Web サイトからアップデートします。

アップデートをアプライアンスにダウンロードしている間は、アップデートのタイムアウトにはなりません。アップデートのダウンロードが長時間中断すると、ダウンロードがタイムアウトします。

システムがタイムアウトせずに、アップデートが完了するまで待機する最大時間は、アンチウイルス アップデート間隔より 1 分短い値に定義された、動的な値です ([Security Services] > [Service Updates] で定義されています)。この設定値は、接続速度の遅いアプライアンスが、完了まで 10 分を超える大きいアップデートをダウンロードする場合に役立ちます。

モニタリングおよび手動でのアップデート チェック

ライセンス契約書に同意し、グローバル設定を構成したら、[Security Services] > [Sophos] または [McAfee Anti-Virus] ページ (GUI) または `antivirusstatus` コマンド (CLI) を使用して、最新のアンチウイルス エンジンおよび識別ファイルがインストールされていることを確認し、いつ最終のアップデートが実行されたか確認できます。

また、手動でアップデートを実行することもできます。[Security Services] > [Sophos] または [McAfee Anti-Virus] ページの [Current McAfee/Sophos Anti-Virus Files] テーブルで、[Update Now] をクリックします。アプライアンスは最新のアップデートを確認してダウンロードします。

図 9-1 Sophos アップデートの手動チェック

Current Sophos Anti-Virus files		
File Type	Version	Updated On
Sophos Anti-Virus Engine	4.13	23 Jan 2007 22:25 (GMT)
Sophos IDE Rules	2007020105	01 Feb 2007 20:24 (GMT)

CLI では、`antivirusstatus` コマンドを使用してウイルス ファイルのステータスをチェックし、`antivirusupdate` コマンドを使用してアップデートを手動でチェックします。

表 9-1 Anti-Virus ステータスの表示

```
example.com> antivirusstatus
Choose the operation you want to perform:
- MCAFEE - Display McAfee Anti-Virus version information
- SOPHOS - Display Sophos Anti-Virus version information
> sophos
SAV Engine Version      3.2.07.286_4.58
  IDE Serial            0
  Last Engine Update    Base Version
  Last IDE Update      Never updated
```

表 9-2 新しい Anti-Virus アップデートのチェック

```
example.com> antivirusupdate
Choose the operation you want to perform:
- MCAFEE - Request updates for McAfee Anti-Virus
- SOPHOS - Request updates for Sophos Anti-Virus
>sophos
Requesting check for new Sophos Anti-Virus updates
example.com>
```

アップデート ログを表示して、アンチウイルス ファイルが、すべて正常にダウンロード、抽出、またはアップデートされたことを確認できます。アップデート ログ サブスクリプションの最終的なエントリを表示して、ウイルス アップデートが取得できていることを確認するには、`tail` コマンドを使用します。

ユーザのウイルス スキャン アクションの設定

Cisco IronPort アプライアンスに統合されているウイルス スキャン エンジンには、いったんグローバルにイネーブルにすると、[Email Security Manager] 機能を使用して設定したポリシー（設定オプション）に基づいて、着信および発信メール メッセージのウイルスを処理します。アンチウイルス アクションは、[Email Security Feature] ([Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ (GUI) または `policyconfig > antivirus` コマンド (CLI)) を使用して受信者ごとにイネーブルにします。

メッセージ スキャン設定

- [Scan for Viruses Only] :
システムにより処理されるメッセージには、ウイルス スキャンが実行されます。感染している添付ファイルがあっても、修復は試行されません。ウイルスが含まれるメッセージまたは修復できなかったメッセージについて、添付ファイルをドロップしてメールを配信するかどうかを選択できます。
- [Scan and Repair Viruses] :
システムにより処理されるメッセージには、ウイルス スキャンが実行されます。添付ファイルにウイルスが発見された場合は、システムは添付ファイルの「修復」を試行します。
- [Dropping Attachments] :
感染した添付ファイルをドロップするように選択できます。
アンチウイルス スキャン エンジンにより、メッセージの添付ファイルがスキャンされ感染したファイルがドロップされると、代わりに「**Removed Attachment**」という名前の新しいファイルが添付されます。この添付ファイルのタイプはテキストまたはプレーンで、次の内容が含まれています。

This attachment contained a virus and was stripped.

Filename: *filename*

Content-Type: application/*filetype*

悪質な添付ファイルによりメッセージが感染していたため、ユーザのメッセージに何らかの修正が加えられた場合は、必ずユーザに通知されます。二次的な通知アクションを設定することもできます（「[通知の送信](#)」(P.9-18)を参照）。感染した添付ファイルをドロップするように選択した場合は、通知アクションにより、ユーザにメッセージが修正されたことを通知する必要はありません。

- [X-IronPort-AV Header] :
アプライアンスのアンチウイルス スキャン エンジンにより処理されたすべてのメッセージには、X-IronPort-AV: というヘッダーが追加されます。このヘッダーは、特に「スキャンできない」と見なされたメッセージについ

て、アンチウイルス設定に関する問題をデバッグする際の追加情報となります。X-IronPort-AV ヘッダーをスキャンされたメッセージに含めるかどうかは、切り替えできます。このヘッダーを含めることを推奨します。

メッセージ処理設定

ウイルス スキャン エンジン は、リスナーにより受信される 4 つの独立したメッセージクラスについて、それぞれ別々のアクションを実行して処理するように設定できます。図 9-2 に、ウイルス スキャン エンジンがイネーブルになっている場合にシステムが実行するアクションをまとめています。GUI 設定については、図 9-3 および図 9-4 を参照してください。

次の各メッセージタイプについて、それぞれ実行するアクションを選択できます。アクションについては後述します（「[メッセージ処理アクションの設定の構成](#)」(P.9-15) を参照）。たとえば、ウイルスに感染したメッセージについて、感染した添付ファイルがドロップされ、電子メールの件名が変更されて、カスタムアラートがメッセージの受信者に送信されるように、アンチウイルスを設定できます。

修復されたメッセージの処理

メッセージが完全にスキャンされ、すべてのウイルスが修復または削除された場合は、そのメッセージは修復されたと見なされます。これらのメッセージはそのまま配信されます。

暗号化されたメッセージの処理

メッセージ内に暗号化または保護されたフィールドがあるために、エンジンがスキャンを完了できなかった場合は、そのメッセージは暗号化されていると見なされます。暗号化されているとマークされたメッセージも、修復可能です。

暗号化検出のメッセージ フィルタ ルール（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「Encryption Detection Rule」を参照）と、「暗号化された」メッセージに対するウイルス スキャン アクションの違いに注意してください。暗号化メッセージ フィルタ ルールは、PGP または S/MIME で暗号化されたすべてのメッセージを「true」と評価します。暗号化ルールで検出できるのは、PGP および S/MIME で暗号化されたデータのみです。パスワードで保護された ZIP ファイル、もしくは暗号化されたコンテンツを含む Microsoft Word または

Excel ドキュメントは検出できません。ウイルス スキャン エンジン は、パスワードで保護されたメッセージまたは添付ファイルはすべて「暗号化されている」と見なします。



(注) AsyncOS バージョン 3.8 以前からアップグレードして、Sophos Anti-Virus スキャンを設定する場合は、アップグレード後に [Encrypted Message Handling] の項を設定する必要があります。

スキャンできないメッセージの処理

スキャン タイムアウト値に到達した場合、または内部エラーによりエンジンが使用不可能になった場合は、メッセージはスキャンできないと見なされます。スキャンできないとマークされたメッセージも、修復可能です。

ウイルスに感染したメッセージの処理

システムが添付ファイルをドロップできない、またはメッセージを完全に修復できない場合があります。このような場合は、依然としてウイルスが含まれるメッセージのシステムでの処理方法を設定できます。

暗号化メッセージ、スキャンできないメッセージ、およびウイルス メッセージの設定オプションは、どれも同じです。

メッセージ処理アクションの設定の構成

適用するアクション

暗号化されたメッセージ、スキャンできないメッセージ、またはウイルス陽性のメッセージの各タイプについて、全般的にどのアクションを実行するか（メッセージをドロップする、新しいメッセージの添付ファイルとしてメッセージを配信する、メッセージをそのまま配信する、またはメッセージをアンチウイルス検疫エリアに送信する（「[検疫およびアンチウイルス スキャン](#)」(P.9-16) を参照)) を選択します。検疫の詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章を参照してください。

感染したメッセージを新しいメッセージの添付ファイルとして配信するようにアプライアンスを設定すると、受信者がオリジナルの感染した添付ファイルをどのように処理するか、選択できるようになります。

メッセージをそのまま配信するか、またはメッセージを新しいメッセージの添付ファイルとして配信することを選択した場合は、追加で次の処理を設定できます。

- メッセージの件名の変更
- オリジナル メッセージのアーカイブ
- 一般的な通知の送信
次のアクションは、GUI の [Advanced] セクションから実行できます。
- メッセージへのカスタム ヘッダーの追加
- メッセージ受信者の変更
- 代替宛先ホストへのメッセージの送信
- カスタムのアラート通知の送信（受信者宛てのみ）



(注)

これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。これらのオプションを使用した、さまざまなスキャン ポリシーの定義に関する詳細については、後述のセクションおよび「[アンチウイルス設定に関する注意事項](#)」(P.9-25) を参照してください。



(注)

修復されたメッセージに対する拡張オプションは、[Add custom header] および [Send custom alert notification] の 2 つのみです。その他すべてのメッセージタイプについては、すべての拡張オプションにアクセスできます。

検疫およびアンチウイルス スキャン

検疫フラグの付けられたメッセージは、電子メール パイプラインの残りの処理を継続します。メッセージがパイプラインの終点に到達したとき、メッセージに 1 つ以上の検疫フラグが付いていれば、そのメッセージはキューに入ります。メッセージがパイプラインの終点に到達しなかった場合は、そのメッセージは検疫されませんので注意してください。

たとえば、コンテンツ フィルタはメッセージをドロップまたは返送する場合がありますが、その場合、メッセージは検疫されません。

メッセージの件名ヘッダーの変更

特定のテキスト文字列を前後に追加することで、識別されたメッセージを変更すると、ユーザがより簡単に識別されたメッセージを判別したり、ソートしたりできるようになります。



(注)

[Modify message subject] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、[WARNING: VIRUS REMOVED] というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

デフォルトのテキストは次のとおりです。

表 9-3 アンチウイルス件名行変更のデフォルト件名行テキスト

判断	件名に追加されるデフォルトのテキスト
暗号化されている	[WARNING: MESSAGE ENCRYPTED]
感染している	[WARNING: VIRUS DETECTED]
修復されている	[WARNING: VIRUS REMOVED]
スキャン不可	[WARNING: A/V UNSCANNABLE]

複数のステートが該当するメッセージについては、アプライアンスがメッセージに対して実行したアクションをユーザに知らせる、複数部分で構成された通知メッセージが作成されます（たとえば、ユーザに対してはメッセージがウイルスを修復されていると通知されていても、メッセージの他の部分は暗号化されている場合があります）。

オリジナル メッセージのアーカイブ

システムにより、ウイルスが含まれている（または含まれている可能性がある）と判断されたメッセージは、「avarchive」ディレクトリにアーカイブできます。この形式は、mbox 形式のログ ファイルです。「Anti-Virus Archive」ログ サブスクリプションを設定して、ウイルスが含まれているメッセージまたは完全にスキャンできなかったメッセージをアーカイブする必要があります。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Logging」を参照してください。



(注)

GUI では、場合により [Advanced] リンクをクリックして [Archive original message] を表示する必要があります。

通知の送信

システムにより、メッセージにウイルスが含まれていると識別されたときに、デフォルトの通知を送信者、受信者、およびその他のユーザまたはそのいずれかに送信できます。その他のユーザを通知対象に指定する場合は、複数のアドレスをコンマで区切ります（CLI および GUI の両方）。デフォルトの通知、メッセージは次のとおりです。

表 9-4 アンチウイルス通知のデフォルト通知

判断	通知
修復されている	The following virus(es) was detected in a mail message: <virus name(s)> Actions taken: Infected attachment dropped. (または Infected attachment repaired.)
暗号化されている	The following message could not be fully scanned by the anti-virus engine due to encryption.
スキャン不可	The following message could not be fully scanned by the anti-virus engine.
感染している	The following unrepairable virus(es) was detected in a mail message: <virus name(s)>.

メッセージへのカスタム ヘッダーの追加

アンチウイルス スキャン エンジンによってスキャンされたすべてのメッセージに追加する、追加のカスタム ヘッダーを定義できます。[Yes] をクリックし、ヘッダー名およびテキストを定義します。

また、skip-viruscheck アクションを使用するフィルタを作成して、特定のメッセージはウイルス スキャンを回避するようにもできます。詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Using Message Filters to Enforce Email Policies」の章の「Bypass Anti-Virus System Action」を参照してください。

メッセージ受信者の変更

メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようになります。[Yes] をクリックして、新しい受信者のアドレスを入力します。

代替宛先ホストへのメッセージの送信

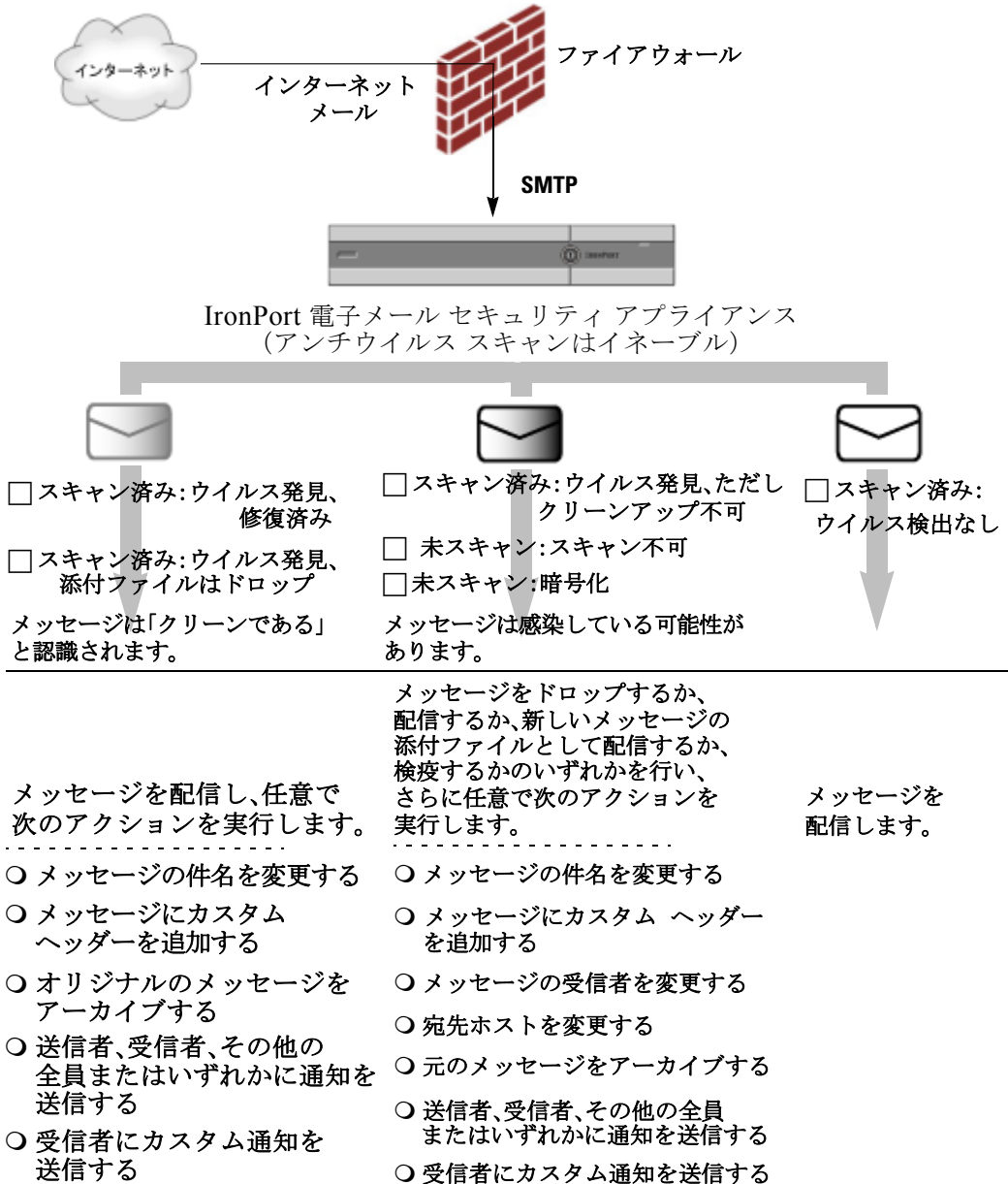
暗号化されたメッセージ、スキャンできないメッセージ、またはウイルスに感染したメッセージについて、異なる受信者または宛先ホストに通知を送信するように選択できます。[Yes] をクリックして代替アドレスまたはホストを入力します。

たとえば、疑わしいメッセージを管理者のメールボックスまたは専用のメールサーバに送信して、後で調査することができます。受信者が複数のメッセージの場合は、代替受信者に送信されるコピーは 1 つのみです。

カスタムのアラート通知の送信（受信者宛てのみ）

受信者にカスタム通知を送信できます。そのためには、この設定を構成する前に、まずカスタム通知を作成する必要があります。詳細については、「[テキストリソースについて](#)」(P.14-18) を参照してください。

図 9-2 ウイルス スキャンを実行したメッセージの処理に関するオプション





(注) デフォルトでは、アンチウイルス スキャンは、WHITELIST 送信者グループが参照するパブリック リスナーの \$TRUSTED メール フロー ポリシーでイネーブルになっています。「メール フロー ポリシー : アクセス ルールとパラメータ」(P.5-11) を参照してください。

メール ポリシーのアンチウイルス設定の編集

メール ポリシーのユーザごとのアンチウイルス設定を編集する処理は、着信メールと発信メールで基本的に同じです。

個々のポリシー（デフォルト以外）には、[Use Default] 設定値という追加のフィールドがあります。この設定は、デフォルトのメール ポリシー設定を継承するように選択します。

アンチウイルス アクションは、[Email Security Feature] ([Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ (GUI) または `policyconfig -> antivirus` コマンド (CLI)) を使用して受信者ごとにイネーブルにします。アンチウイルス設定をグローバルにイネーブルにした後は、作成した各メール ポリシーに対して、これらのアクションを別々に設定します。さまざまなメール ポリシーに対して、異なるアクションを設定できます。

デフォルトのポリシーも含め、メール ポリシーのアンチウイルス設定を編集するには、次の操作を実行します。

ステップ 1 [Email Security Manager] の着信または発信メール ポリシー テーブルの任意の行で、アンチウイルス セキュリティ サービスへのリンクをクリックします。

図 9-3 および図 9-4 に示されている画面のような [Anti-Virus settings] ページが表示されます。

デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。図 9-3 および図 9-4 に、個別のポリシー（デフォルト以外）の設定を示します。

ステップ 2 [Yes] または [Use Default] をクリックして、そのポリシーのアンチウイルス スキャンをイネーブルにします。

このページの最初の設定値は、そのポリシーに対してサービスがイネーブルであるかどうかを定義します。[Disable] をクリックしてすべてのサービスをディセーブルにできます。

デフォルト以外のメール ポリシーでは、[Yes] を選択することで、[Repaired Messages]、[Encrypted Messages]、[Unscannable Messages]、および [Virus Infected Messages] 領域内の各フィールドがイネーブルになります。

- ステップ 3** アンチウイルス スキャン エンジンを選択します。McAfee または Sophos のエンジンを選択できます。
- ステップ 4** [Message Scanning] 設定を構成します。
- 詳細については、「[メッセージ スキャン設定](#)」(P.9-13) を参照してください。
- ステップ 5** [Repaired Messages]、[Encrypted Messages]、[Unscannable Messages]、および [Virus Infected Messages] の設定を構成します。
- [図 9-3](#) および [図 9-4](#) に、「Engineering」という名前のこれから編集するメール ポリシーのアンチウイルス設定を示します。「[メッセージ処理設定](#)」(P.9-14) および「[メッセージ処理アクションの設定の構成](#)」(P.9-15) を参照してください。
- ステップ 6** [Submit] をクリックします。
- [Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページがリフレッシュされて、これまでの手順で選択した値が反映されます。
- ステップ 7** 変更を確定します。

図 9-3 メール ポリシーのアンチウイルス設定 (デフォルト以外) : 1/2

Anti-Virus Settings	
Policy:	Engineering
Enable Anti-Virus Scanning for This Policy:	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> Use Default Settings <input type="radio"/> No
Message Scanning	
	Scan and Repair viruses <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found and it could not be repaired <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="button" value="v"/> Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[WARNING: VIRUS REMOVED]"/>
Send Notification Message:	<input type="checkbox"/> ...to sender <input type="checkbox"/> ...to recipient <input type="checkbox"/> ...to others: <input type="text"/>
Advanced	Optional settings for custom header and message delivery.

図 9-4 メール ポリシーのアンチウイルス設定 (デフォルト以外) : 2/2

Encrypted Messages:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: MESSAGE ENCRYPTED]
Send Notification Message:	<input type="checkbox"/> ...to sender <input type="checkbox"/> ...to recipient <input type="checkbox"/> ...to others: <input type="text"/>
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
Unscannable Messages:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [[WARNING: A/V UNSCANNABLE]]
Send Notification Message:	<input type="checkbox"/> ...to sender <input type="checkbox"/> ...to recipient <input type="checkbox"/> ...to others: <input type="text"/>
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
Virus Infected Messages:	
Action Applied to Message:	Drop Message <input type="button" value="v"/>
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append <input type="text"/>
Send Notification Message:	<input type="checkbox"/> ...to sender <input type="checkbox"/> ...to recipient <input type="checkbox"/> ...to others: <input type="text"/>
<input type="button" value="Advanced"/> Optional settings for custom header and message delivery.	
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

アンチウイルス設定に関する注意事項

添付ファイルのドロップフラグにより、アンチウイルススキャンの動作は大きく異なります。システムが、[Drop infected attachments if a virus is found and it could not be repaired] ように設定されている場合は、ウイルス性またはスキャンできない MIME 部分はすべてメッセージから削除されます。そのため、アンチウイルススキャンの出力は、ほとんど常にクリーンなメッセージになります。GUI ペインに表示された [Unscannable Messages] で定義されるアクションは、実行されることはほとんどありません。

[Scan for Viruses only] 環境では、これらのアクションは悪質なメッセージ部分をドロップすることで、メッセージを「クリーンに」します。RFC822 ヘッダーに限り、RFC822 ヘッダー自体が攻撃された、またはその他の問題に遭遇した場合は、スキャンできなかった場合のアクションが実行されます。ただし、アンチウイルススキャンが [Scan for Viruses only] に設定されているが、[Drop infected attachments if a virus is found and it could not be repaired] が選択されていない場合は、スキャンできなかった場合のアクションが実行される可能性は非常に高くなります。

表 9-5 に、一般的なアンチウイルス設定オプションを示します。

表 9-5 一般的なアンチウイルス設定オプションの表示

状況	アンチウイルス設定
ウイルスが広範囲に発生	添付ファイルのドロップ：しない。
ウイルス性のメッセージは単純にシステムからドロップされ、他の処理が実行されることはほとんどありません。	スキャン：Scan-Only。 クリーンアップされたメッセージ：配信する。 スキャンできないメッセージ：メッセージをドロップする。 暗号化されたメッセージ：管理者に送るか検疫して、後で確認する。 ウイルス性のメッセージ：メッセージをドロップする。

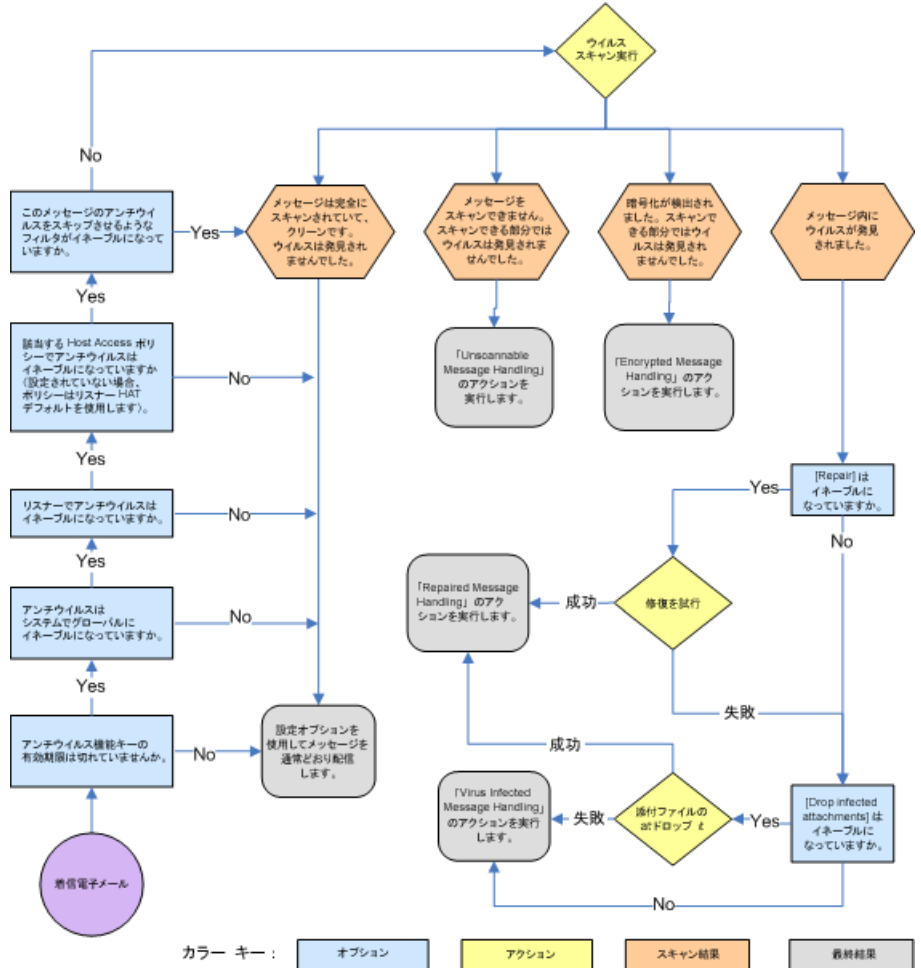
表 9-5 一般的なアンチウイルス設定オプションの表示 (続き)

<p>リベラルなポリシー</p> <p>できる限り多くのドキュメントを送信します。</p>	<p>添付ファイルのドロップ：する。</p> <p>スキャン：Scan and Repair。</p> <p>クリーンアップされたメッセージ：[VIRUS REMOVED] として配信する。</p> <p>スキャンできないメッセージ：添付ファイルとして転送する。</p> <p>暗号化されたメッセージ：マークして転送する。</p> <p>ウイルス性のメッセージ：検疫するか、マークして転送する。</p>
<p>より保守的なポリシー</p>	<p>添付ファイルのドロップ：する。</p> <p>スキャン：Scan and Repair。</p> <p>クリーンアップされたメッセージ：[VIRUS REMOVED] として配信する</p> <p>(より慎重なポリシーでは、クリーンアップしたメッセージをアーカイブします)。</p> <p>スキャンできないメッセージ：通知を送る、検疫する、またはドロップしてアーカイブする。</p> <p>暗号化されたメッセージ：マークして転送する、またはスキャンできないメッセージとして処理する。</p> <p>ウイルス性のメッセージ：アーカイブしてドロップする。</p>
<p>保守的なポリシーでレビューを実施する</p> <p>ウイルスメッセージの可能性 があるものは、後で管理者が 内容を確認できるように、検 疫メールボックスに送信され ます。</p>	<p>添付ファイルのドロップ：しない。</p> <p>スキャン：Scan-Only。</p> <p>クリーンアップされたメッセージ：配信する (通常、このアクションは実行されません)。</p> <p>スキャンできないメッセージ：添付ファイル、alt-src-host、または alt-rcpt-to アクションとして転送する。</p> <p>暗号化されたメッセージ：スキャンできないメッセージとして処理する。</p> <p>ウイルス性のメッセージ：検疫するか管理者に転送する。</p>

アンチウイルス アクションのフロー ダイアグラム

図 9-5 (P.9-27) に、アンチウイルス アクションおよびオプションが、アプライアンスで処理されるメッセージにどのように影響を及ぼすかを示します。

図 9-5 アンチウイルス アクションのフロー ダイアグラム





(注) マルチレイヤ アンチウイルス スキャンを設定した場合は、Cisco IronPort アブライアンスは最初に McAfee エンジンでウイルス スキャンを実行し、次に Sophos エンジンでウイルス スキャンを実行します。アブライアンスは、McAfee エンジンがウイルスを検出しない限りは、両方のエンジンを使用してメッセージをスキャンします。McAfee エンジンがウイルスを検出した場合は、Cisco IronPort アブライアンスは、メール ポリシーで定義されたアンチウイルス アクション（修復、検疫など）を実行します。

ウイルス スキャンのテスト

アブライアンスのウイルス スキャン設定をテストするには、次の操作を実行します。

- ステップ 1** メール ポリシーのウイルス スキャンをイネーブルにします。
- [Security Services] > [Sophos] または [McAfee Anti-Virus] ページ、または antivirusconfig コマンドを使用してグローバル設定を行ってから、[Email Security Manager] ページ (GUI) または policyconfig の antivirus サブコマンドを使用して、特定のメール ポリシーの設定を構成します。
- ステップ 2** 標準のテキスト エディタを開き、次の文字列をスペースまたは改行を使用せず、1 行で入力します。

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```



(注) 上記の行は、テキスト エディタ ウィンドウで 1 行で表示される必要があります。そのため、必ずテキスト エディタのウィンドウは最大にして、改行はすべて削除します。また、テスト メッセージ開始部の「X50...」には、数字の「0」ではなく必ず文字の「O」を入力します。

このマニュアルをコンピュータでお読みの場合は、PDF ファイルまたは HTML ファイルから直接この行をコピーして、テキスト エディタに貼ることができます。この行をコピーする場合は、必ずすべての余分な復帰文字またはスペースを削除します。

ステップ 3 ファイルを **EICAR.COM** という名前で保存します。

ファイルのサイズは 68 ～ 70 バイトになります。



(注) このファイルはウイルスではありません。拡散したり、他のファイルに感染したり、またはコンピュータに害を与えたりするものではありません。ただし、他のユーザにアラームを与えないために、テストを終了したらこのファイルは削除してください。

ステップ 4 ファイル **EICAR.COM** を電子メール メッセージに添付して、ステップ 1 で設定したメール ポリシーに一致するリスナーに送信します。

テストメッセージで指定した受信者が、リスナーで許可されることを確認します（詳細は、「[パブリック リスナー \(RAT\) 上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ](#)」(P.5-72) を参照してください)。

Cisco IronPort 以外のゲートウェイ（たとえば Microsoft Exchange サーバ）で発信メールに対するウイルス スキャン ソフトウェアをインストールしている場合は、ファイルを電子メールで送信することが難しいことがあるため、注意してください。



(注) テスト ファイルは、常に修復不可能としてスキャンされます。

ステップ 5 リスナー上のウイルス スキャンに設定したアクションを評価して、そのアクションがイネーブルであり、予想どおりに動作していることを確認します。

これは、次のいずれかのアクションを実行することで、最も簡単に達成できます。

- ウイルス スキャンを、[Scan and Repair] モードまたは [Scan Only] モードにして、添付ファイルをドロップしないように設定します。

EICAR テスト ファイルを添付ファイルとした電子メールを送信します。

実行されたアクションが、[Virus Infected Messages] の処理で設定した内容（「[ウイルスに感染したメッセージの処理](#)」(P.9-15) の設定）と一致していることを確認します。

- ウイルス スキャンを、[Scan and Repair] モードまたは [Scan Only] モードにして、添付ファイルをドロップするように設定します。

EICAR テスト ファイルを添付ファイルとした電子メールを送信します。

実行されたアクションが、[Repaired Messages] の処理で設定した内容（「修復されたメッセージの処理」(P.9-14) の設定）と一致していることを確認します。

アンチウイルス スキャンのテスト用ウイルス ファイルの取得に関する詳細については、次の URL を参照してください。

http://www.eicar.org/anti_virus_test_file.htm

このページでは、ダウンロード可能な 4 つのファイルを提供しています。クライアント側にウイルス スキャン ソフトウェアをインストールしている場合は、これらのファイルをダウンロードして抽出するのは難しいため、注意してください。



CHAPTER 10

感染フィルタ

添付ファイルを介したウイルスの蔓延が減少する一方で、フィッシングメッセージ、詐欺、およびマルウェア リンクなどの少量のターゲットを定めた電子メール攻撃は増加しています。これらの非ウイルス性の攻撃に使用されるメッセージは、複雑で進化しています。これらのメッセージは本物のように見え、受信者の情報を使用するなど、ソーシャルエンジニアリングのトリックを使用して受信者を騙し、フィッシングおよびマルウェアの Web サイトを指すカスタム URL をクリックさせようとしています。これらの URL は、各受信者または少数の受信者のグループに対して一意にすることができ、これらの Web サイトは、短期間だけオンラインになる、Web セキュリティ サービスにとって未知のサイトです。これらの要因すべてによって、これら小規模の非ウイルス性のアウトブレイクを検出するのは、広範囲のウイルス アウトブレイクやスパム キャンペーンの検出よりもさらに難しくなります。Cisco IronPort の感染フィルタ機能は、新しいウイルスのアウトブレイクだけでなく、この増大傾向のターゲットを定めた攻撃からユーザを保護します。

この章は、次の内容で構成されています。

- 「[感染フィルタの概要](#)」 (P.10-2)
- 「[感染フィルタ：マルチレイヤの対象保護](#)」 (P.10-5)
- 「[感染フィルタの機能概要](#)」 (P.10-13)
- 「[感染フィルタの管理 \(GUI\)](#)」 (P.10-18)
- 「[感染フィルタのモニタリング](#)」 (P.10-31)
- 「[感染フィルタ機能のトラブルシューティング](#)」 (P.10-33)

感染フィルタの概要

ユーザから機密情報を盗んだり、マルウェアをユーザのコンピュータに配信したりするように設計されたメッセージは、進化し続けているため、従来のアンチウイルスおよびアンチスパム スキャン ソフトウェアで見逃される可能性があります。感染フィルタは、積極的にアクションを実行して、これらの新しいアウトブレイクに対する防衛において、非常に重要な第 1 のレイヤとなります。Cisco IronPort の感染フィルタ機能は、リアルタイムで新しいアウトブレイクを検出し、動的に応答して疑いのあるトラフィックのネットワークへの侵入を防ぐことで、新しいアンチウイルスおよびアンチスパムのアップデートが展開されるまでの間の保護を提供します。感染フィルタは、Cisco IronPort のアウトブレイク検出テクノロジーとインテリジェントな検疫システムを使用して、ユーザを保護します。

感染フィルタ機能は、アウトブレイクが発生するとその情報を収集すること、およびこのデータを使用してこれらのアウトブレイクのユーザへの蔓延を防ぐことによって、ユーザとネットワークを保護します。感染フィルタは、着信メッセージを Cisco Security Intelligence Operations (SIO) から発行されたアウトブレイク ルールと比較して、そのメッセージが大規模のウイルス アウトブレイクの一部なのか、より小さい非ウイルス性の攻撃なのかを判断します。AsyncOS は、アウトブレイク ルールと一致するメッセージに、そのメッセージの脅威の重大度を示す脅威レベルを割り当てます。また、その脅威レベルをメール ポリシーに設定した検疫のしきい値およびメッセージ変更のしきい値と比較します。それらのしきい値のいずれかでしきい値以上であるメッセージは、受信者を保護するために検疫されるか変更されます。

アウトブレイク検出およびフィルタリングの処理は、SIO の一部の SenderBase から開始されます。SenderBase は、世界有数の規模を誇る電子メールおよび Web トラフィックのモニタリング システムで、世界の電子メール トラフィックの約 25 % を把握しています。Cisco IronPort は、SenderBase の履歴データを使用して、正常なグローバル トラフィック パターンの統計的なビューを作成します。感染フィルタは、このデータから開発された一連のルールに応じて、着信メッセージの脅威レベルを決定します。

感染フィルタは、機能およびユーザビリティが大幅に拡張されています。大まかには、この拡張には次の内容が含まれます（ただし、これに限定されるものではありません）。

- Cisco Security Intelligence Operations (SIO) によって検出された脅威タイプ、およびウイルス アウトブレイクに加えて、フィッシング詐欺およびマルウェア配布などの非ウイルス性の攻撃を検出するためにアウトブレイク ルールの作成に使用される脅威タイプの強化。

- SIO が提供するアダプティブ ルールとアウトブレイク ルールからコンテンツ分析を組み合わせてアウトブレイクを検出するのに加えて、URL をスキャンして、非ウイルス性の脅威を検出する CASE (Context Adaptive Scanning Engine) スキャン。
- メッセージを定期的に再評価し、アウトブレイク ルールのアップデートに基づいて検疫を自動解除する動的検疫。
- 有害な可能性のある Web サイトへのトラフィックをリダイレクトするための Cisco Web セキュリティ プロキシによる URL の書き換え。アクセスしようとしている Web サイトが不正である可能性があることをユーザに警告するか、その Web サイトを完全にブロックします。

これらの機能拡張は、システムによるアウトブレイクの捕捉率を向上させ、アウトブレイクの可視化を強化し、またユーザのコンピュータや機密情報を保護するように設計されています。

Cisco IronPort アプライアンスには、感染フィルタ機能の 30 日評価ライセンスが同梱されています。

脅威カテゴリー

感染フィルタ機能は、メッセージに基づくアウトブレイクの次の 2 つのカテゴリからの保護を提供します。ウイルス アウトブレイクは、添付ファイルに見たことのないウイルスが含まれるメッセージで、*非ウイルス性の脅威*には、外部 Web サイトへのリンクを経由するフィッシング試行、詐欺、およびマルウェア配布が含まれます。

デフォルトで感染フィルタ機能は、アウトブレイク中の可能性があるウイルスがあるかどうか送受信メッセージをスキャンします。アプライアンスでアンチスパム スキャンをイネーブルにする場合は、ウイルス アウトブレイクに加えて、非ウイルス性の脅威のスキャンをイネーブルにできます。



(注)

感染フィルタが非ウイルス性の脅威についてスキャンするために、アプライアンスには IronPort Anti-Spam または IronPort Intelligent Multi-Scan の機能キーが必要です。

ウイルス アウトブレイク

感染フィルタ機能を使用することで、ウイルス アウトブレイクとの格闘において優位なスタートを切ることができます。アウトブレイクは、見たことのないウイルスまたは既存のウイルスの変異型を含む添付ファイルを持つメッセージがプライベート ネットワークおよびインターネットを経由してすばやく拡散するときに発生します。これらの新しいウイルスまたはウイルスの変異型がインターネットを攻撃した場合、最も危機的な期間はウイルスがリリースされてからアンチウイルス ベンダーがアップデートしたウイルス定義をリリースするまでの期間です。たとえ数時間でも、事前に通知を受けることは、マルウェアまたはウイルスの拡散を抑えるうえで非常に重要です。ウイルス定義がリリースされるまでの間に、新しく発見されたウイルスはグローバルに伝播し、電子メール インフラストラクチャを停止に追い込むことが可能です。

フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威

非ウイルス性の脅威を含んでいるメッセージは、正規の送信元からのメッセージのように設計されていて、多くの場合、少数の受信者に送信されます。これらのメッセージには、信頼できると見せるために次の 1 つまたは複数の特徴がある場合があります。

- 受信者の連絡先情報。
- HTML コンテンツは、ソーシャル ネットワークおよびオンライン販売などの正規の送信元からの電子メールを模倣するように設計されています。
- 新しい IP アドレスを持ち、短期間だけオンラインである Web サイトを指している URL。これは電子メールおよび Web セキュリティ サービスに、その Web サイトが不正かどうか判断するための十分な情報がないことを意味します。
- URL 短縮サービスを指している URL。

これらの特徴すべてによって、これらのメッセージをスパムとして検出するのがさらに難しくなります。感染フィルタ機能によって、これらの非ウイルス性の脅威に対するマルチレイヤの防衛が提供され、ユーザがマルウェアをダウンロードしたり、個人情報新しい不審な Web サイトに提供したりすることを防ぎます。

CASE はメッセージ内に URL を発見すると、そのメッセージを既存のアウトブレイク ルールと比較して、そのメッセージが小規模の非ウイルス性のアウトブレイクの一部かどうか判断し、次に脅威レベルを割り当てます。脅威レベルに応じて、電子メール セキュリティ アプライアンスは、より多くの脅威のデータを集められるまで受信者への配信を遅らせ、Web サイトにアクセスしようとする

と Cisco Web セキュリティ プロキシへ受信者をリダイレクトするようにメッセージ内の URL を書き換えます。プロキシは、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ ページを表示します。

感染フィルタ：マルチレイヤの対象保護

感染フィルタ機能は、ユーザをアウトブレイクから保護するために、次の 3 つの戦略を使用します。

- **遅延。**感染フィルタ機能は、メッセージを検査することによって、ウイルスアウトブレイクまたは非ウイルス性の攻撃の一部の可能性があるメッセージを遅らせます。検査中に、CASE はアップデートされたアウトブレイクルールを受信し、メッセージを再スキャンして攻撃の一部が含まれているかどうかを確認します。CASE は、メッセージの脅威レベルに基づいて再スキャン期間を決定します。詳細については、「[メッセージの遅延](#)」(P.10-7) を参照してください。
- **リダイレクト。**リンクされた Web サイトのいずれかにアクセスしようとすると、感染フィルタは脅威レベルに基づき、Cisco Web セキュリティ プロキシによって受信者をリダイレクトするように非ウイルス性の攻撃のメッセージ内の URL を書き換えます。Web サイトが引き続き使用可能な場合、プロキシは、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ画面を表示します。あるいは、Web サイトがオフラインになった場合は、エラー メッセージを表示します。URL のリダイレクトの詳細については、「[URL のリダイレクト](#)」(P.10-8) を参照してください。
- **変更。**非ウイルス性の脅威のメッセージ内の URL の書き換えに加えて、感染フィルタはメッセージの件名を変更できます。またメッセージ本文上部に免責事項を追加してユーザにメッセージの内容について警告します。詳細については、「[メッセージの変更](#)」(P.10-9) を参照してください。

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations (SIO) は、グローバルな脅威情報、レピュテーションに基づくサービス、および高度な分析を Cisco セキュリティ アプライアンスに結び付け、より強力な保護をより迅速な応答時間で提供するセキュリティ エコシステムです。

SIO は次の 3 種類のコンポーネントからなります。

- **SenderBase**。世界有数の規模を誇る脅威モニタリング ネットワークおよび脆弱性データベース。
- **Threat Operations Center (TOC)**。セキュリティ専門家のグローバル チームおよび **SenderBase** によって収集された実行可能な情報を抽出する自動システム。
- 動的アップデート。アウトブレイク発生時に、**Cisco IronPort** に自動的に配信されるリアルタイム アップデート。

SIO は、グローバル **SenderBase** ネットワークからのリアルタイム データを、共通のトラフィック パターンと比較して、アウトブレイクの確かな前兆である異常を識別します。TOC は、データをレビューしてアウトブレイクの可能性の脅威レベルを発行します。**Cisco IronPort** 電子メールセキュリティ アプライアンスは、アップデートされた脅威レベルとアウトブレイク ルールをダウンロードし、それらを使用してすでに **Outbreak** 検疫エリアにあるメッセージと同様に送信メッセージをスキャンします。

現在のウイルス アウトブレイクに関する情報は、次の **SenderBase** の Web サイトで入手できます。

<http://www.senderbase.org/>

次の **SIO Web** サイトに、スパム、フィッシング、およびマルウェア配布の試行を含む現在の非ウイルス性の脅威のリストが記載されています。

<http://tools.cisco.com/security/center/home.x>

Context Adaptive Scanning Engine

感染フィルタには、**Cisco IronPort** 独自の **Context Adaptive Scanning Engine (CASE)** が使用されています。CASE は、メッセージ脅威に対するリアルタイムの分析に基づいて自動的かつ定期的に調整されている、100,000 を超える適応メッセージ属性を活用しています。

ウイルス アウトブレイクの場合、CASE はメッセージの内容、コンテキスト、および構造を分析してアダプティブ ルールのトリガーである可能性のあるものを、正確に識別します。CASE は、アダプティブ ルールと SIO から発行されるリアルタイムのアウトブレイク ルールを組み合わせ、各メッセージを評価し、独自の脅威レベルを割り当てます。

非ウイルス性の脅威を検出するために、CASE は URL に対してメッセージをスキャンし、1 つまたは複数の URL が発見されると SIO が提供するアウトブレイク ルールを使用してメッセージの脅威レベルを評価します。

メッセージの脅威レベルに基づいて、CASE は、アウトブレイクを防ぐためにメッセージを一定期間検疫することを推奨します。SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージを再評価できるように、CASE は再スキャンの間隔も決定します。脅威レベルが高くなるほど、検疫中のメッセージの再スキャンの頻度が高くなります。

メッセージが検疫解除されるときに、CASE はメッセージの再スキャンも行いません。再スキャン時に、CASE によりメッセージがスパムであるか、ウイルスを含むと判断された場合、メッセージを再度検疫できます。

CASE の詳細については、「[IronPort Anti-Spam および CASE の概要](#)」(P.8-6)を参照してください。

メッセージの遅延

アウトブレイクまたは電子メール攻撃の発生と、ソフトウェア ベンダーによるアップデートしたルールのリリースの間の期間は、ネットワークとユーザが最も脆弱なときです。この期間に、現代のウイルスはグローバルに伝播でき、また不正な Web サイトはマルウェアを配信したり、ユーザの機密情報を収集したりすることができます。限られた期間に疑わしいメッセージを検疫することによって、感染フィルタは、ユーザおよびネットワークを保護し、シスコおよびその他のベンダーに新しいアウトブレイクを調査する時間を与えます。

ウイルス アウトブレイクが発生すると、アップデートされたアウトブレイク ルールおよび新しいアンチウイルス シグニチャにより、その電子メールの添付ファイルがクリーン、またはウイルスであることが証明されるまで添付ファイルを含む疑わしいメッセージは検疫されます。

小規模の非ウイルス性の脅威には、Web セキュリティ サービスによる検出を回避するために短期間オンラインになる可能性のある不正な Web サイトへの URL、または Web セキュリティを回避するため、信頼できる Web サイトを途中に置いて URL 短縮サービスを経由する URL が含まれます。脅威レベルのしきい値を満たす URL を含んでいるメッセージの検疫によって、CASE は SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージの内容を再評価できるだけでなく、リンクされた Web サイトがオフラインになるか、Web セキュリティ ソリューションによってブロックできるほど長く、メッセージを検疫のままにしておくことができます。

疑いのあるメッセージに対する感染フィルタの検疫方法の詳細については、「動的検疫」(P.10-15)を参照してください。

URL のリダイレクト

CASE が感染フィルタの段階でメッセージをスキャンする場合、他の疑わしい内容に加えてメッセージ本文に URL があるかどうかを検索します。CASE は、発行されたアウトブレイク ルールを使用して、そのメッセージが脅威であるかどうかを評価して、次に適切な脅威レベルでメッセージをスコアリングします。脅威レベルに応じて、感染フィルタは、受信者が Cisco Web セキュリティ プロキシにリダイレクトされるように、バイパスされたドメインを指している URL を除くすべての URL を書き換えることによって受信者を保護します。メッセージがより大きなアウトブレイクの一部であると思われる場合は、TOC が Web サイトについてさらに詳しく調べるためにメッセージの配信を遅らせます。信頼ドメインへの URL のバイパスの詳細については、「URL 書き換えおよびドメインのバイパス」(P.10-26)を参照してください。

電子メール セキュリティ アプライアンスがメッセージをリリースおよび配信した後で、受信者による Web サイトへのアクセスの試行があれば、Cisco Web セキュリティ プロキシによってリダイレクトされます。これは、シスコによってホストされている外部プロキシで、Web サイトが引き続き使用可能な場合、その Web サイトが危険である可能性があることをユーザに警告するスプラッシュ画面を表示します。Web サイトがオフラインになった場合は、スプラッシュ画面にエラー メッセージが表示されます。

受信者がメッセージの URL をクリックすることにした場合、Cisco Web セキュリティ プロキシは、ユーザの Web ブラウザにスプラッシュ画面を表示して、メッセージの内容について警告します。図 10-1 に、スプラッシュ画面の警告の例を示します。受信者は、[Ignore this warning] をクリックして Web サイトへ進み続けるか、[Exit] をクリックして退出し、ブラウザ ウィンドウを安全に閉じることができます。

図 10-1 シスコのセキュリティによるスプラッシュ画面の警告



Cisco Web セキュリティ プロキシにアクセスする唯一の方法は、メッセージ内の URL を書き換えることです。Web ブラウザで URL を入力しても、プロキシにはアクセスできません。

メッセージの変更

感染フィルタ機能は、非ウイルス性の脅威であるメッセージのメッセージ本文を変更して、URL を書き換えるだけでなく、メッセージが疑わしい脅威であるというアラートをユーザに出します。感染フィルタ機能は、件名ヘッダーを変更したり、メッセージ本文上部にメッセージの内容について免責事項を追加したりできます。詳細については、「[メッセージ変更](#)」(P.10-25) を参照してください。

脅威の免責事項は、[Mail Policies] > [Text Resources] ページから免責事項テンプレートを使用して作成されます。詳細については、「[テキスト リソースの管理 \(GUI\)](#)」(P.14-20) を参照してください。

ルールのタイプ：アダプティブルールおよびアウトブレイクルール

感染フィルタでは、アダプティブルールおよびアウトブレイクルールの 2 つのタイプのルールを使用して、潜在的なアウトブレイクを検出します。感染フィルタ機能は、これらの 2 つのルールセットを使用して、高い有効性を持ち、綿密的を絞った、一連の脅威検出基準を提供することで、フィルタが確実に特定のアウトブレイクに正確に照準を合わせることができるようにしています。感染フィルタのルールおよびアクションは、水面下に隠されているものではなく、管理者の目に見えるようになっており、検疫されたメッセージにただちにアクセスしたり、検疫された理由を確認したりできるようになっています。

アウトブレイクルール

アウトブレイクルールは、Cisco Security Intelligence Operations の一部である、Cisco IronPort Threat Operations Center (TOC) で作成されるもので、添付ファイルのタイプだけでなく、メッセージ全体に焦点を当てています。アウトブレイクルールは、SenderBase データ（リアルタイムおよび履歴のトラフィックデータ）およびその他のあらゆるメッセージパラメータの組み合わせ（添付ファイルタイプ、ファイル名のキーワード、またはアンチウイルスエンジンのアップデート）を使用して、リアルタイムでアウトブレイクを認識し、防止します。アウトブレイクルールには一意の ID が付けられ、GUI のさまざまな場所（たとえば Outbreak 検疫など）でルールを参照するために使用されます。

グローバル SenderBase ネットワークからのリアルタイムデータは、このベースラインと比較され、アウトブレイクの確かな前兆である異常を識別します。TOC は、データをレビューして脅威のインジケータまたは脅威レベルを発行します。脅威レベルは、メッセージが脅威であり、かつその脅威に対するその他のゲートウェイ防衛が Cisco IronPort の顧客には広く展開されていない可能性を計測して、0（脅威なし）～ 5（きわめて危険）の数値で表すものです（詳細については、「脅威レベル」(P.10-12) を参照してください)。脅威レベルは、TOC によりアウトブレイクルールとして発行されます。

アウトブレイクルール内で組み合わせることができる特性には、たとえば次のようなものがあります。

- ファイルタイプ、ファイルタイプとサイズ、ファイルタイプとファイル名キーワードなど
- ファイル名キーワードとファイルサイズ
- ファイル名キーワード

- メッセージ URL
- ファイル名と Sophos IDE

アダプティブルール

アダプティブルールは、CASE 内の一連のルールであり、メッセージの属性を既知のウイルス アウトブレイク メッセージの属性と正確に比較します。これらのルールは、Cisco IronPort の広範なウイルス コーパスの中で、既知の脅威のメッセージおよび既知の良好なメッセージを研究し、作成されたものです。アダプティブルールは、コーパスの評価に合わせて、頻繁にアップデートされます。アダプティブルールは、既存のアウトブレイクルールを補完して、常にアウトブレイクメッセージを検出します。アウトブレイクルールは、アウトブレイクの可能性がある状態が発生したときに有効になりますが、アダプティブルールは（いったんイネーブルにされると）「常時オン」となり、グローバルな規模で本格的な異常が起きる前にローカルでアウトブレイクメッセージを捕捉します。さらに、アダプティブルールは、電子メールトラフィックおよび構造の小規模および微小な変化にも継続的に対応し、お客様にアップデートした保護を提供します。

アウトブレイク

感染フィルタルールは、基本的に、電子メールのメッセージおよび添付ファイルの一連の特性（ファイルサイズ、ファイルタイプ、ファイル名、メッセージの内容など）に関連付けられた脅威レベル（例：4）です。たとえば、ファイル名に特定のキーワード（たとえば「hello」）が含まれた .exe 形式のファイル（サイズは 143 KB）が添付された、疑わしい電子メールメッセージの発生が増加していることを、Cisco IronPort SIO が通知したと想定します。この基準に一致するメッセージに対する脅威レベルを上げたアウトブレイクルールが発行されます。デフォルトでは、Cisco IronPort アプライアンスは、新しく発行されたアウトブレイクルールおよびアダプティブルールを 5 分ごとにチェックし、ダウンロードします（「[感染フィルタルールのアップデート](#)」（P.10-21）を参照）。アダプティブルールは、アウトブレイクルールほど頻繁にはアップデートされません。Cisco IronPort アプライアンスで、疑わしいメッセージの検疫についてしきい値を設定します。メッセージの脅威レベルが検疫のしきい値以上の場合、メッセージは *Outbreak* 検疫エリアに送信されます。非ウイルス性の脅威のメッセージの変更についてしきい値を設定して、疑わしいメッセージで発見された URL すべてを書き換えたり、メッセージ本文の上部に通知を追加したりできます。

脅威レベル

表 10-1 (P.10-12) に、各レベルの基本的なガイドラインまたは定義のセットを示します。

表 10-1 脅威レベルの定義

レベル	リスク	意味
0	なし	メッセージが脅威であるリスクはありません。
1	低	メッセージが脅威であるリスクは低です。
2	低または中	メッセージが脅威であるリスクは低から中です。これは「疑わしい」脅威です。
3	中	メッセージが確認されているアウトブレイクの一部であるか、メッセージの内容が脅威である中から高のリスクがあります。
4	高	メッセージが大規模アウトブレイクの一部であることが確認されているか、メッセージの内容が非常に危険です。
5	きわめて高	メッセージの内容が、非常に大規模または大規模な、かつ非常に危険なアウトブレイクの一部であることが確認されています。

脅威レベルおよびアウトブレイク ルールの詳細については、「[感染フィルタ ルール](#)」 (P.10-21) を参照してください。

検疫脅威レベルのしきい値設定ガイドライン

検疫脅威レベルのしきい値を使用することで、管理者は疑いのあるメッセージをより積極的または消極的に検疫できるようになります。低い値 (1 または 2) は、より積極的な設定値で、多くのメッセージが検疫されます。反対に、高いスコア (4 または 5) は消極的な設定値で、不正である可能性がきわめて高いメッセージのみが検疫されます。

ウイルス アウトブレイクおよび非ウイルス性の脅威の両方に同じしきい値が適用されますが、ウイルス攻撃およびその他の脅威に対して、異なる検疫の保持期間を指定できます。詳細については、「[動的検疫](#)」 (P.10-15) を参照してください。

シスコは、デフォルト値の 3 を推奨します。

コンテナ：特定ルールおよび常時ルール

コンテナ ファイルとは、他のファイルを含むジップ (.zip) アーカイブなどのファイルです。TOC は、アーカイブ ファイル内の特定のファイル进行处理するルールを発行できます。

たとえば、TOC により、あるウイルス アウトブレイクが、1 つの .exe を含む 1 つの .zip ファイルで構成されていると判別された場合は、.zip ファイル内の .exe ファイル (.zip(exe)) に脅威レベルを設定する特定のアウトブレイク ルールが発行されます。ただし .zip ファイル内に含まれるその他のファイル タイプ (たとえば .txt ファイル) には特定の脅威レベルを設定しません。2 番目のルール (.zip(*)) は、コンテナ ファイル タイプ内のその他すべてのファイル タイプをカバーします。コンテナに対する常時ルールは、コンテナ内にあるファイルのタイプに関係なく、メッセージの脅威レベル計算に常に使用されます。そのようなコンテナ タイプが危険であると判明した場合は、常時ルールが SIO により発行されます。

表 10-2 フォールバック ルールおよび脅威レベル スコア

アウトブレイク ルール	脅威レベル	説明
.zip(exe)	4	このルールは、.zip ファイル内の .exe ファイルの脅威レベルを 4 に設定します。
.zip(doc)	0	このルールは、.zip ファイル内の .doc ファイルの脅威レベルを 0 に設定します。
zip(*)	2	このルールは、含まれているファイルのタイプに関係なく、すべての .zip ファイルの脅威レベルを 2 に設定します。

感染フィルタの機能概要

電子メール メッセージは、Cisco IronPort アプライアンスで処理される際に、「電子メール パイプライン」と呼ばれる一連の手順を通過します (電子メール パイプラインの詳細については、「[電子メール パイプラインの理解](#)」(P.4-1) を参照してください)。対象のメール ポリシーでアンチスパムおよびアンチウイルスがイネーブルになっている場合、メッセージは電子メール パイプラインを通過するときに、アンチスパムおよびアンチウイルス スキャン エンジンにかけられます。これらのスキャンを通過するメッセージのみ、感染フィルタ機能によりスキャンされます (感染フィルタ機能によりスキャンされるメッセージの決定に電子メール パイプラインがどの

ように影響を及ぼすかについての詳細は、「メッセージフィルタ、コンテンツフィルタ、および電子メールパイプライン」(P.10-33)を参照してください。言い換えると、認識されているウイルスが含まれる既知のスパムまたはメッセージは、感染フィルタ機能でスキャンされる前に、アンチスパムおよびアンチウイルス設定に基づいてメールストリームから除去（削除、検疫など）されているため、感染フィルタ機能ではスキャンされません。このため、感染フィルタ機能に到達するメッセージは、スパムおよびウイルスを含まないとマークされています。感染フィルタによって検疫されたメッセージは、CASE によって検疫解除されて、再スキャンされる際、アップデートされたスパムルールおよびウイルス定義に基づいて、スパムまたはウイルスを含んでいるとしてマークされる可能性があることに注意してください。

メッセージスコアリング

新しいウイルス攻撃または非ウイルス性の脅威がコンピュータネットワークに放たれた時点では、脅威を認識できるアンチウイルスやアンチスパムソフトウェアはまだありません。感染フィルタ機能が非常に重要となるのは、このときです。着信メッセージは、発行されているアウトブレイクおよびアダプティブルールを使用して、CASE によりスキャンおよびスコアリングされます（「[ルールのタイプ：アダプティブルールおよびアウトブレイクルール](#)」(P.10-10)を参照）。メッセージスコアはメッセージの脅威レベルに対応しています。メッセージに該当するルールがあった場合は、どのルールに一致したかに従って、CASE は対応する脅威レベルを割り当てます。関連する脅威レベルが存在しない（メッセージに一致するルールが存在しない）場合は、メッセージには脅威レベル 0 が割り当てられます。

その計算が完了すると、電子メールセキュリティアプライアンスは、メッセージの脅威レベルが検疫またはメッセージ変更のしきい値以上であるかどうかをチェックし、メッセージを検疫するかメッセージの URL を書き換えます。脅威レベルがしきい値を下回る場合、パイプラインの後続の処理が継続されます。

さらに、CASE は既存の検疫されているメッセージを最新のルールに照らして再評価し、メッセージの最新の脅威レベルを決定します。これにより、アウトブレイクメッセージに整合する脅威レベルを持つメッセージのみが検疫され続け、脅威と見なされなくなったメッセージは自動再評価の後に検疫エリアから解放されます。

1 つのアウトブレイクメッセージで複数のスコアが存在する場合（1 つのスコアがあるアダプティブルールに基づいたもの（または該当するアダプティブルールが複数ある場合はそのうちの最も高いスコア）で、別のスコアはあるアウトブレイクルールに基づいたもの（または該当するアウトブレイクルールが複数ある場合はそのうちの最も高いスコア）である場合は、インテリジェントアルゴリズムを使用して最終的な脅威レベルが決定されます。



(注) 感染フィルタ機能は、Cisco IronPort アプライアンスでアンチウイルス スキャンをイネーブルにしなくても使用できます。この 2 つのセキュリティ サービスは、お互いを補完するように設計されていますが、別々に動作しています。ただし、Cisco IronPort アプライアンスでアンチウイルス スキャンをイネーブルにしていない場合は、アンチウイルス ベンダーのアップデートをモニタリングして、**Outbreak** 検疫エリアにあるメッセージの一部を手動で検疫解除したり、再評価したりする必要があります。アンチウイルス スキャンをイネーブルにしないで感染フィルタを使用する場合は、次の点に注意してください。

- アダプティブ ルールはディセーブルにする必要があります。
- メッセージはアウトブレイク ルールに従って検疫されます。
- 脅威レベルが引き下げられたり、検疫時間の期限が過ぎたりした場合は、メッセージは検疫解除されます。

ダウストリーム of アンチウイルス ベンダー（デスクトップおよびグループウェア）は、検疫解除されたメッセージを捕捉する場合があります。



(注) 感染フィルタ機能が非ウイルス性の脅威をスキャンするために、アンチスパム スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

動的検疫

感染フィルタ機能の **Outbreak** 検疫エリアは、メッセージが脅威であると確認されるか、ユーザに配信しても安全であることが確認されるまで、一時的にメッセージを保管しておくための保持領域です。（詳細については、「[アウトブレイク ライフサイクルおよびルール発行](#)」(P.10-17) を参照してください)。検疫されたメッセージは、複数の方法で **Outbreak** 検疫エリアから解放できます。新しいルールがダウンロードされると、**Outbreak** 検疫エリアにあるメッセージは、CASE によって計算された推奨再スキャン間隔に基づいて再評価されます。更新されたメッセージの脅威レベルが検疫保持のしきい値よりも低くなった場合、メッセージは自動的に (**Outbreak** 検疫の設定に関係なく) 検疫解除されるため、メッセージが検疫されている時間を最小限に抑えることができます。メッセージの再評価中に新しいルールが発行された場合は、再スキャンが開始されます。

ウイルス攻撃として検疫されるメッセージは、新しいアンチウイルス シグニチャが使用可能な場合は、自動的に **Outbreak** 検疫エリアから解放されることはないため、注意してください。新しいルールは、新しいアンチウイルス シグニ

チャを参照している場合と、参照していない場合があります。ただし、アウトブレイク ルールによりメッセージの脅威レベルが設定されている脅威レベルのしきい値よりも低いスコアに変更されない限り、アンチウイルス エンジンがアップデートされたことによって、メッセージが検疫解除されることはありません。

CASE の推奨保持期間が経過した場合も、メッセージは **Outbreak** 検疫エリアから解放されます。CASE は、メッセージの脅威レベルに基づいて保持期間を計算します。ウイルス アウトブレイクおよび非ウイルス性の脅威に対して別々の最大保持期間を定義できます。CASE の推奨保持期間 がその脅威タイプの最大保持期間を超える場合、電子メール セキュリティ アプライアンスは、最大保持期間が経過した時点でメッセージを解放します。ウイルス性のメッセージのデフォルトの最大検疫期間は 1 日です。非ウイルス性の脅威を検疫するデフォルト期間は 4 時間です。メッセージを、手動で検疫解除できます。

また、検疫エリアがいっぱいであるときに、追加のメッセージが挿入されると電子メール セキュリティ アプライアンスもメッセージを解放します（これはオーバーフローと呼ばれます）。オーバーフローは、**Outbreak** 検疫エリアが容量の 100 % まで使用されているときに、新しいメッセージが検疫エリアに追加された場合のみ発生します。このとき、メッセージが検疫解除される優先順位は次のとおりです。

- アダプティブ ルールにより検疫されたメッセージ（最も早く検疫解除されるようにスケジュール設定されているものから）
- アウトブレイク ルールにより検疫されたメッセージ（最も早く検疫解除されるようにスケジュール設定されているものから）

Outbreak 検疫エリアの使用量が容量の 100 % を下回った時点で、オーバーフローは停止します。検疫エリアのオーバーフローの処理方法に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「**Quarantines**」の章を参照してください。

Outbreak 検疫エリアから解放されたメッセージは、アンチウイルスおよびアンチスパム エンジンがメール ポリシーでイネーブルとなっている場合、アンチウイルスおよびアンチスパム エンジンによって再度スキャンされます。このときに既知のウイルスまたはスパムとしてマークされた場合は、このメッセージはメール ポリシー設定に従って処理されます（**Virus** 検疫エリアまたは **IronPort Spam** 検疫エリアに検疫される場合もあります）。詳細については、「[感染フィルタ機能と Outbreak 検疫](#)」(P.10-28) を参照してください。

このため、メッセージのライフタイムの間に、メッセージは 2 回検疫される場合がある（1 回は感染フィルタ機能により、もう 1 回は **Outbreak** 検疫エリアから解放されたとき）と注意しておくことが重要です。各スキャン（感染フィルタの前および **Outbreak** 検疫エリアから解放されたとき）照合の結果、何らかの判断がな

されたメッセージは、2 回検疫されることはありません。また、感染フィルタ機能により、メッセージに対して最終的なアクションが実行されることはないことにも注意してください。感染フィルタ機能は、(後続の処理のために) メッセージを検疫するか、またはメッセージをパイプラインの次の手順に移動します。

アウトブレイク ライフサイクルおよびルール発行

ウイルスのアウトブレイク ライフサイクルの非常に初期の段階では、メッセージを検疫するために広範なルールが多く使用されます。より詳しい情報が判明していくと、よりの絞ったルールが発行され、検疫する対象の定義が絞り込まれていきます。新しいルールが発行されると、その時点でウイルス メッセージの可能性があると見なされなくなったメッセージは、検疫解除されます (Outbreak 検疫エリアにあるメッセージは、新しいルールが発行されると再スキャンされます)。

表 10-1 にウイルスのアウトブレイク ライフサイクルの例を示します。

表 10-3 アウトブレイク ライフサイクルのルールの例

時間	ルールの種類	ルールの説明	アクション
T=0	アダプティブルール (過去のアウトブレイクに基づく)	10 万を超えるメッセージ属性に基づく、統合されたルールセットで、メッセージの内容、コンテキスト、および構造を分析します。	アダプティブルールに一致したメッセージは、自動的に検疫されます。
T=5 分	アウトブレイクルール	.zip (exe) ファイルが含まれるメッセージを検疫します。	.exe が含まれる .zip 形式の添付ファイルはすべて検疫されます。
T=10 分	アウトブレイクルール	50 KB を超える .zip (exe) ファイルが含まれるメッセージを検疫します。	50 KB 未満の .zip (exe) ファイルが含まれたメッセージはすべて検疫解除されます。
T=20 分	アウトブレイクルール	ファイル名に「Price」が含まれる 50 ~ 55 KB の .zip (exe) ファイルが含まれるメッセージを検疫します。	この基準に一致しないメッセージはすべて検疫解除されます。
T=12 時間	アウトブレイクルール	新しいシグニチャを使用してスキャンします。	残っているすべてのメッセージを、最新のアンチウイルス シグニチャを使用してスキャンします。

感染フィルタの管理 (GUI)

グラフィカル ユーザ インターフェイス (GUI) にログインし、メニューの [Security Services] を選択して、[Outbreak Filters] をクリックします。

図 10-2 [Outbreak Filters] メインページ
Outbreak Filters

The screenshot displays the 'Outbreak Filters Overview' and 'Outbreak Filter Rules' sections. The global settings are as follows:

Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	512K
Receive Emailed Alerts:	No

Below the settings is an 'Edit Global Settings...' button. The 'Outbreak Filter Rules' section includes a table of rule updates:

Rule Type	Last Update	Current Version
CASE Core Files	Never Updated	3.1.0-012
CASE Utilities	Never Updated	3.1.0-012
Virus Outbreak Rules	Never Updated	20050710_000000

A note below the table states: 'Outbreak Filter Rules (higher number indicates greater risk. 1= lowest threat, 5= highest threat)'. The main table of rules is as follows:

Threat Level	Rule ID	Description
3	OUTBREAK_0003427	We are seeing unusual volume for file extension(s) pif. We are raising the Threat Level to 3. We wil...
3	OUTBREAK_0003420	We are seeing unusual volume for file extension(s) exe. We are raising the Threat Level to 3. We wil...
3	OUTBREAK_0003429	We are seeing unusual volume for file extension(s) zip(exe), zip:e(exe). We are raising the Threat L...
3	OUTBREAK_0003430	We are seeing suspicious url(s) propagating through multiple sources. We are raising the Threat Leve...
3	OUTBREAK_0003431	We are seeing suspicious url(s) propagating through multiple sources. We are raising the Threat Leve...

At the bottom, it says 'Rules last updated: Wed May 25 22:36:12 2011' and includes 'Update Rules Now' and 'Clear Current Rules' buttons.

[Outbreak Filters] ページには、[Outbreak Filters Overview] と現在の [Outbreak Filter Rules] (存在する場合) のリストの 2 つのセクションが表示されます。

図 10-2 で、感染フィルタはイネーブル、Adaptive Scanning はイネーブル、また最大メッセージサイズは 512 K に設定されています。これらの設定を変更するには、[Edit Global Settings] をクリックします。グローバル設定の編集に関する詳細については、「感染フィルタのグローバル設定の構成」(P.10-19) を参照してください。

[Outbreak Filter Rules] セクションには、各種コンポーネント（ルール自体だけでなくルール エンジンも含む）の最新アップデートの時刻、日付、およびバージョンのリストと、脅威レベルとともに感染フィルタ ルールのリストが示されます。

アウトブレイク ルールの詳細については、「[感染フィルタ ルール](#)」(P.10-21) を参照してください。

感染フィルタのグローバル設定の構成

感染フィルタのグローバル設定を構成するには、[Edit Global Settings] をクリックします。[Outbreak Filters Global Settings] ページが表示されます。

図 10-3 [Outbreak Filters Global Settings] ページ
Edit Outbreak Filters Settings

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> Enable Outbreak Filters	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	512k Maximum <i>Add a trailing K or M to indicate units.</i>
Emailed Alerts: (?)	<input type="checkbox"/> Receive Emailed Alerts

Cancel Submit

このページを使用して、次のことを行います。

- 感染フィルタをグローバルにイネーブルにします。
- アダプティブ ルールのスキャンをイネーブルにします。
- スキャンするファイルの最大サイズを設定します（サイズをバイトで入力することに注意してください）
- 感染フィルタのアラートをイネーブルにするかどうかを選択します。

アラートおよびアダプティブ ルールはデフォルトではイネーブルになっていないため、注意してください。この機能は、outbreakconfig CLI コマンドからも使用できます（『Cisco IronPort AsyncOS CLI Reference Guide』を参照）。変更を加えたら、送信して確定します。

感染フィルタ機能のイネーブル化

感染フィルタ機能をグローバルにイネーブルにするには、[Outbreak Filters Global Settings] ページの [Enable Outbreak Filters] の横にあるボックスをオンにして、[Submit] をクリックします。事前に感染フィルタのライセンス契約書に同意しておく必要があります。

いったんグローバルにイネーブルにした後は、感染フィルタ機能は、各送受信メールポリシー（デフォルトポリシーも含む）に対して個別にイネーブルまたはディセーブルにできます。詳細については、「[感染フィルタ機能とメールポリシー](#)」(P.10-22) を参照してください。

感染フィルタ機能は、アンチスパム スキャンがイネーブルになっているかどうかに関係なく、Context Adaptive Scanning Engine (CASE) を使用してウイルス性の脅威を検出します。ただし、非ウイルス性の脅威をスキャンするために、アプライアンスで IronPort Anti-Spam または Intelligent Multi-Scan をグローバルにイネーブルにする必要があります。



(注)

システムのセットアップ中にライセンスに同意しなかった場合（「[手順 4 : Security](#)」(P.3-31) を参照）は、[Security Services] > [Outbreak Filters] ページで [Enable] をクリックして、ライセンス契約を読み、同意する必要があります。

アダプティブ ルールのイネーブル化

Adaptive Scanning は、感染フィルタのアダプティブ ルールをイネーブルにします。メッセージの内容に関するウイルス シグニチャまたはスパム基準が使用できない場合は、一連の係数または特性（ファイル サイズなど）が使用されて、メッセージがアウトブレイクの一部である可能性が決定されます。Adaptive Scanning をイネーブルにするには、[Outbreak Filters Global Settings] ページの [Enable Adaptive Rules] の横にあるボックスをオンにして、[Submit] をクリックします。

感染フィルタのアラートのイネーブル化

[Emailed Alerts] というラベルの付いたボックスをオンにして、感染フィルタ機能のアラートをイネーブルにします。感染フィルタの電子メール アラートのイネーブル化は、単にアラート エンジンがイネーブルにして、感染フィルタに関するアラートが送信されるようにするためのものです。送信されるアラートおよび送信先の電子メール アドレスの指定は、[Alerts] ページの [System

Administration] タブで設定します。感染フィルタのアラートの設定に関する詳細については、「アラート、SNMP トラップ、および感染フィルタ」(P.10-32) を参照してください。

感染フィルタ ルール

アウトブレイク ルールは、Cisco IronPort Security Intelligence Operations から発行されます。Cisco IronPort アプライアンスは新しいアウトブレイク ルールを 5 分ごとにチェックおよびダウンロードします。このアップデート間隔を変更できます。詳細については、「アップデート設定値の編集」(P.15-17) を参照してください。

感染フィルタ ルールの管理

感染フィルタ ルールは自動的にダウンロードされるため、ユーザによる管理は一切必要ありません。

ただし、何らかの理由で Cisco IronPort アプライアンスが一定期間 Cisco IronPort のアップデート サーバの新しいルールにアクセスできない場合は、ローカルでキャッシュされているスコアが有効でなくなっている（つまり、既知のウイルス性の添付ファイル タイプが現在ではアンチウイルス ソフトウェアのアップデートに含まれている、またはすでに脅威ではなくなっている、またはその両方の場合）可能性があります。この場合は、これらの特性を持つメッセージを検疫しておく必要はありません。

[Update Rules Now] をクリックすることによって、現在のアウトブレイク ルールを手動でアップデートできます。これは、CLI で `outbreakupdate` コマンドを発行することと同じです（『Cisco IronPort AsyncOS CLI Reference Guide』を参照）。

感染フィルタ ルールのアップデート

デフォルトでは、Cisco IronPort アプライアンスは 5 分ごとに新しい感染フィルタ ルールのダウンロードを試行します。この間隔は、[Security Services] > [Service Updates] ページで変更できます。詳細については、「サービスのアップデート」(P.15-16) を参照してください。

感染フィルタ機能とメール ポリシー

感染フィルタ機能の設定には、メール ポリシーごとに設定できるものがあります。感染フィルタ機能は、アプライアンスでメール ポリシーごとにイネーブルまたはディセーブルにできます。メール ポリシーごとに、特定のファイル拡張子およびドメインを感染フィルタ機能の処理から除外できます。この機能は、`policyconfig CLI` コマンドからも使用できます（『Cisco IronPort AsyncOS CLI Reference Guide』を参照）。



(注) 感染フィルタ機能が非ウイルス性の脅威をスキャンするために、IronPort Anti-Spam または Intelligent Multi-Scan スキャンをアプライアンスでグローバルにイネーブルにする必要があります。

図 10-4 メール ポリシーのリスト
Incoming Mail Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Sales_Team	IronPort Anti-Spam Positive: Drop Suspected: Quarantine Marketing Messages: Quarantine	(use default)	(use default)	(use default)	
2	Engineering	(use default)	(use default)	scan_for_confidential ex_employee	Retention Time: Virus: 1 day Other: 4 hours	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Deliver Marketing Messages: Disabled	Sophos Encrypted: Deliver Uncannable: Deliver Virus Positive: Drop	scan_for_confidential no_mpgs ex_employee	Retention Time: Virus: 1 day	

Key: Default Custom Ready

特定のメール ポリシーに対する感染フィルタ機能の設定を変更するには、変更するポリシーの [Outbreak Filters] 列のリンクをクリックします。[Outbreak Filter Settings] ページが表示されます。

図 10-5 感染フィルタ設定とメール ポリシー
Mail Policies: Outbreak Filters

Outbreak Filtering for Policy: Sales_Team	
Enable Outbreak Filtering (Customize settings) ▼	
Outbreak Filter Settings	
Quarantine Threat Level: ?	3 ▼
Maximum Quarantine Retention:	Viral Attachments: 1 ▼ Days ▼ Other Threats: 4 ▼ Hours ▼
Bypass Attachment Scanning: ▶	None configured
Message Modification	
<input checked="" type="checkbox"/> Enable Message Modification	
Message Modification Threat Level: ?	3 ▼
Message Subject:	Prepend ▼ [MODIFIED FOR PROTECTION]
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input checked="" type="radio"/> Enable only for unsigned messages (recommended) <input type="radio"/> Enable for all messages <input type="radio"/> Disable
Bypass Domain Scanning ?	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24)</small>
Threat Disclaimer:	None ▼ <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources</small>
Cancel Submit	

特定のメール ポリシーに対して感染フィルタ機能をイネーブルにし、カスタマイズするには、[Enable Outbreak Filtering (Customize Settings)] を選択します。メール ポリシーに対して次の感染フィルタ設定を構成できます。

- 検疫脅威レベル。
- 最大検疫保持期間。
- バイパスするファイル拡張子のタイプ。
- メッセージ変更のしきい値。
- メッセージの件名。
- URL 書き換え。
- 脅威の免責事項。

[Enable Outbreak Filtering (Inherit Default mail policy settings)] を選択して、デフォルトのメール ポリシーについて定義されている感染フィルタ設定を使用します。デフォルト メール ポリシーで感染フィルタ機能をイネーブルにしている場合は、その他すべてのメール ポリシーはカスタマイズしない限り同じ感染フィルタ設定を使用します。

設定を変更したら、変更を確定します。

検疫レベルのしきい値の設定

リストからアウトブレイクの脅威に対する [Quarantine Threat Level] のしきい値を選択します。数字が小さいほど検疫されるメッセージは多くなり、数字が大きいほど検疫されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

詳細については、「[検疫脅威レベルのしきい値設定ガイドライン](#)」(P.10-12) を参照してください。

最大検疫保持

メッセージが **Outbreak** 検疫エリアにとどまる最大時間を時間単位または日単位で指定します。ウイルス性の添付ファイルを含む可能性のあるメッセージ、およびフィッシングやマルウェア リンクなどその他の脅威を含む可能性のあるメッセージに対して異なる保持期間を指定できます。ポリシーで [Message Modification] をイネーブルにしない限り、非ウイルス性の脅威を検疫できません。

CASE は、メッセージに脅威レベルを割り当てるときに検疫保持期間を推奨しています。電子メールセキュリティ アプライアンスは、脅威タイプに対する最大検疫保持期間を超えない限り、CASE が推奨する時間の長さの間、検疫されるメッセージを保持します。

ファイル拡張子タイプのバイパス

特定のファイル タイプをバイパスするようにポリシーを変更できます。バイパスされたファイル拡張子は、CASE によるメッセージの脅威レベルの計算から除外されます。ただし、添付ファイルに対する残りの電子メールセキュリティ プライインの処理は行われます。

ファイル拡張子をバイパスするには、[Bypass Attachment Scanning] をクリックし、ファイル拡張子を選択または入力してから、[Add Extension] をクリックします。AsyncOS は、[File Extensions to Bypass] リストに拡張子タイプを表示します。

バイパスされる拡張子のリストから拡張子を削除するには、[File Extensions to Bypass] リストの拡張子の横のゴミ箱アイコンをクリックします。

ファイル拡張子のバイパス：コンテナ ファイルのタイプ

ファイル拡張子をバイパスする場合、コンテナ ファイル内のファイル（たとえば .zip 内の .doc ファイル）もバイパスする拡張子のリストに含まれていれば、バイパスされます。たとえば、バイパスする拡張子のリストに .doc を追加した場合は、コンテナ ファイルに含まれているものも含めて、すべての .doc ファイルがバイパスされます。

メッセージ変更

アプライアンスがフィッシングの試行またはマルウェア Web サイトへのリンクなど非ウイルス性の脅威のメッセージをスキャンする場合は、[Message Modification] をイネーブルにします。

メッセージの脅威レベルに基づいて、AsyncOS はメッセージを変更し、すべての URL を書き換えて、メッセージから Web サイトを開こうとすると Cisco Web セキュリティ プロキシを経由して受信者をリダイレクトすることができます。アプライアンスはメッセージに免責事項を追加して、ユーザにメッセージの内容が疑わしい、または不正であることを警告することもできます。

非ウイルス性の脅威メッセージを検疫するために、メッセージ変更をイネーブルにする必要があります。

メッセージ変更の脅威レベル

リストから [Message Modification Threat Level] のしきい値を選択します。この設定は、CASE によって返される脅威レベルに基づいて、メッセージを変更するかどうかを決定します。数字が小さいほど変更されるメッセージは多くなり、数字が大きいほど変更されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

メッセージの件名

特定のテキスト文字列を前後に追加することで、変更されたリンクを含む非ウイルス性の脅威メッセージで件名ヘッダーのテキストを変更すると、ユーザにメッセージが保護のために変更されたことを通知します。



(注)

[Message Subject] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、[MODIFIED: FOR PROTECTION] というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。



(注)

[Message Subject] フィールドでは、US-ASCII 文字だけを使用できます。

URL 書き換えおよびドメインのバイパス

メッセージの脅威レベルがメッセージ変更のしきい値を超える場合、感染フィルタ機能はメッセージ内のすべての URL を書き換え、これらの URL をクリックするとユーザを Cisco Web セキュリティプロキシのフラッシュ ページにリダイレクトします。（詳細については、「[URL のリダイレクト](#)」(P.10-8) を参照してください)。メッセージの脅威レベルが検疫のしきい値を超える場合、アプライアンスがメッセージの検疫も行います。小規模の非ウイルス性のアウトブレイクが進行中の場合、メッセージの検疫は TOC に、アウトブレイクの可能性があるメッセージからリンクされるすべての疑わしい Web サイトを分析し、その Web サイトが不正であるかどうか判断する時間を与えます。CASE は、SIO が提供するアップデートされたアウトブレイク ルールを使用してメッセージを再スキャンし、メッセージがアウトブレイクの一部であるかを判断します。保持期間が過ぎると、アプライアンスはメッセージを検疫エリアから解放します。

AsyncOS は、バイパスされるドメインを指している URL を除き、メッセージ内のすべての URL を書き換えます。

[URL Rewriting] では次のオプションを使用できます。

- [Enable only for unsigned messages]: このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超える未署名のメッセージ内の URL を書き換えられるようになります。ただし、署名されたメッセージは含まれません。URL 書き換えについて、シスコはこの設定の使用を推奨します。



(注) 電子メール セキュリティ アプライアンス以外のネットワーク上のサーバまたはアプライアンスが DomainKeys/DKIM 署名の検証を担当する場合、電子メール セキュリティ アプライアンスは、DomainKeys/DKIM-signed メッセージ内の URL を書き換えたり、メッセージの署名を無効にしたりすることができます。

- [Enable for all messages]: このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超えるすべてのメッセージ内の URL を書き換えられるようになります。署名されたメッセージも含まれます。AsyncOS が署名されたメッセージを変更すると、署名は無効になります。
- [Disable]: このオプションは感染フィルタに対して URL 書き換えをディセーブルにします。

ポリシーを変更して、特定のドメインへの URL を変更から除外できます。ドメインをバイパスするには、IPv4 アドレス、IPv6 アドレス、CIDR 範囲、ホスト名、部分ホスト名、またはドメインを [Bypass Domain Scanning] フィールドに入力します。複数のエントリを指定する場合は、カンマで区切ります。

脅威の免責事項

電子メール セキュリティ アプライアンスは、疑わしいメッセージのヘッダーの上部に免責事項メッセージを追加して、ユーザにメッセージの内容を警告することができます。この免責事項には、メッセージのタイプに応じて HTML またはプレーン テキストが使用できます。

[Threat Disclaimer] リストから使用する免責事項のテキストを選択するか、[Mail Policies] > [Text Resources] リンクをクリックし、[Disclaimer Template] を使用して新しい免責事項を作成します。[Disclaimer Template] には、アウトブレイク脅威情報に関する変数が含まれます。[Preview Disclaimer] をクリックすると、脅威免責事項のプレビューを表示できます。カスタム免責事項メッセージでは、変数を使用してメッセージの脅威レベル、脅威のタイプ、および脅威の説明を表示できます。免責事項メッセージの作成については、「[テキスト リソースの管理 \(GUI\)](#)」(P.14-20) を参照してください。

感染フィルタ機能と Outbreak 検疫

感染フィルタ機能により検疫されたメッセージは、Outbreak 検疫エリアに送信されます。この検疫エリアは、メッセージを検疫するために使用されるルール（アウトブレイク ルールの場合はアウトブレイク ID、アダプティブルールの場合は一般名称が表示されます）に基づいて、検疫エリアからすべてのメッセージを削除または解放する際に役立つ「サマリー」ビューがあることを除けば、他のあらゆる検疫と同様に機能します（検疫の操作方法の詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章を参照してください）。サマリー ビューの詳細については、[「\[Outbreak Quarantine\] および \[Manage by Rule Summary\] ビュー」](#) (P.10-30) を参照してください。

図 10-6 Outbreak 検疫
Edit Outbreak Quarantine

Settings	
Quarantine Name:	Outbreak
Space Allocation:	2048 MB (Maximum Size 4096 MB)
Default Action:	Release
When Allocated Space is Exceeded Send Messages and:	Modify Subject: Prepend [POSSIBLE VIRUS]
	Add X-Header: Name: <input type="text"/> Value: <input type="text"/>
	Strip Attachments: <input checked="" type="radio"/> No <input type="radio"/> Yes
Local Users:	No users selected
Externally Authenticated Users:	External authentication is disabled. Go to System Administration > Users to enable external authentication.
Custom User Roles:	Quarantine Manager

Cancel Submit

Outbreak 検疫のモニタリング

適切に設定された検疫エリアはほとんどモニタリングを必要としませんが、特にウイルス アウトブレイクの発生中または発生後の、正規のメッセージが遅延する可能性がある間は、Outbreak 検疫エリアに注意を払うことを推奨します。

正規のメッセージが検疫された場合、Outbreak 検疫の設定によっては、次のいずれかが発生します。

- 検疫のデフォルトアクションが [Release] に設定されている場合は、保持期間の期限が切れたとき、または検疫エリアがオーバーフローしたときにメッセージが解放されます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクション

ンがメッセージに対して実行されるように、**Outbreak** 検疫を設定できます。これらのアクションの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「**Quarantines**」の章を参照してください。

- 検疫のデフォルトアクションが **[Delete]** に設定されている場合は、保持期間の期限が切れたとき、または検疫エリアがオーバーフローしたときにメッセージが削除されます。
- オーバーフローは、検疫エリアがいっぱいのときにさらにメッセージが追加された場合に発生します。この場合は、有効期限日に近いメッセージから（必ずしも最も古いメッセージからとは限りません）、新しいメッセージに十分な領域が空くまで、メッセージが解放されていきます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、**X-Header** の追加といったアクションがメッセージに対して実行されるように、**Outbreak** 検疫を設定できます。

検疫されているメッセージは、新しいルールが発行されるたびに再スキャンされるため、**Outbreak** 検疫エリアにあるメッセージは有効期限が切れる前に解放されることがほとんどです。

それでも、デフォルトアクションが **[Delete]** に設定されている場合は、**Outbreak** 検疫をモニタすることが重要です。シスコは、ほとんどのユーザに対して、デフォルトアクションを **[Delete]** に設定しないことを推奨します。**Outbreak** 検疫エリアからのメッセージの解放、または **Outbreak** 検疫のデフォルトアクションの変更に関する詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「**Quarantines**」の章を参照してください。

反対に、新しいルールのアップデートを待つ間、**Outbreak** 検疫エリアに長時間留めておきたいメッセージがある場合は、たとえばそのメッセージの有効期限を遅らせることもできます。メッセージの保持期間を増やすことにより、検疫エリアのサイズが大きくなる場合があるため、注意してください。



(注)

メッセージが **Outbreak** 検疫エリアに留まっている間にアンチウイルス スキャンが（メール ポリシーごとではなく）グローバルにディセーブルにされた場合は、たとえメッセージが解放される前にもう一度アンチウイルス スキャンを再度イネーブルにしたとしても、そのメッセージが解放されたときのアンチウイルス スキャンは実行されません。



(注) 感染フィルタ機能は、Cisco IronPort アプライアンスでアンチウイルス スキャンをイネーブルにしなくても使用できます。ただし、アプライアンスでアンチスパム スキャンがイネーブルでない場合は、感染フィルタは非ウイルス性の脅威をスキャンできません。

[Outbreak Quarantine] および [Manage by Rule Summary] ビュー

GUI の [Monitor] メニューにあるリスト内の検疫名をクリックすることで、Outbreak 検疫エリアの内容を表示できます。Outbreak 検疫には、追加のビューである、Outbreak 検疫の [Manage by Rule Summary] リンクもあります。

図 10-7 Outbreak 検疫の [Manage by Rule Summary] リンク
Quarantines

Quarantines				
Add Quarantine...				
Quarantine	Messages	Default Action	Status	Settings
Spam Quarantine	2565	Retain 14 days then Delete	2% Full	Edit
Outbreak	0	Retention Varies Action: Release	0% Full	Edit
Policy	0	Retain 10 days then Delete	0% Full	Edit
Virus	0	Retain 30 days then Delete	0% Full	Edit

サマリー ビューの使用による Outbreak 検疫エリア内のメッセージに対するルール ID に基づいたメッセージ アクションの実行

[Manage by Rule Summary] リンクをクリックして、ルール ID ごとにグループ化された Outbreak 検疫の内容のリストを表示します。

図 10-8 Outbreak 検疫の [Manage by Rule Summary] ビュー
Outbreak Quarantine Summary

Manage by Rule Summary					
All Select	Rule ID	Number of messages	Average message size	Total size	Capacity
<input type="checkbox"/>	EXE_BAGL	4	16 KB	0.1 MB	0.0%
Totals		4	16 KB		
Select Action...		Submit			

個別にメッセージを選択しなくても、このビューから特定のアウトブレイクまたはアダプティブルールに関するすべてのメッセージに対して、解放、削除、または保持期間延長を実行するように選択できます。また、検索またはリストのソートも実行できます。

この機能は、`quarantineconfig -> outbreakmanage` CLI コマンドからも使用できます。詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

感染フィルタのモニタリング

Cisco IronPort アプライアンスには、感染フィルタ機能のパフォーマンスおよび活動をモニタする複数のツールが含まれています。

感染フィルタ レポート

お使いの Cisco IronPort アプライアンスの感染フィルタの現在のステータスおよび設定に加えて、最近のアウトブレイクや感染フィルタによって検疫されたメッセージに関する情報が表示される感染フィルタ レポートです。この情報は、[Monitor] > [Outbreak Filters] ページで表示します。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Email Security Monitor」の章を参照してください。

感染フィルタの概要とルール リスト

概要およびルール リストは、感染フィルタ機能の現在の状態に関して役立つ情報を提供します。この情報は、[Security Services] > [Outbreak Filters] ページで表示します。

Outbreak 検疫

Outbreak 検疫を使用して、感染フィルタの脅威レベルのしきい値により、フラグ付けされているメッセージの数をモニタします。また、ルールごとの検疫メッセージのリストも使用できます。この情報は、[Monitor] > [Local Quarantines] > [Outbreak] リンクおよび [Monitor] > [Local Quarantines] ページの [Manage Rule by Summary] リンクで表示します。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

アラート、SNMP トラップ、および感染フィルタ

感染フィルタ機能は、定期的な AsyncOS アラートと SNMP トラップという 2 つの異なるタイプの通知をサポートしています。

SNMP トラップは、ルールのアップデートが失敗したときに作成されます。AsyncOS の SNMP トラップの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Managing and Monitoring via the CLI」の章を参照してください。

AsyncOS の感染フィルタ機能には、2 つのタイプのアラート（サイズおよびルール）が用意されています。

AsyncOS アラートは、Outbreak 検疫エリアのサイズが最大サイズの 5、50、75、および 95 を超えるたびに生成されます。95 % のしきい値を超えたときに生成されるアラートの重大度は CRITICAL、その他のアラートしきい値の場合は WARNING です。アラートは、検疫エリアのサイズが大きくなり、しきい値を超えたときに生成されます。検疫エリアのサイズが小さくなり、しきい値を下回ったときは生成されません。アラートの詳細については、「[アラート](#)」(P.15-24) を参照してください。

また、AsyncOS はルールが発行されたとき、しきい値が変更されたとき、またはルールまたは CASE エンジンのアップデート中に問題が発生したときにもアラートを生成します。

感染フィルタ機能のトラブルシューティング

この項では、感染フィルタ機能の基本的なトラブルシューティングに関するヒントをいくつか紹介します。

[Manage Quarantine] ページのチェックボックスを使用すると、Outbreak 検疫がシスコに対して誤分類を通知するようになります。

複数の添付ファイルおよびバイパスされるファイルタイプ

バイパスされるファイルタイプは、メッセージに 1 つだけ添付されているファイルのタイプが指定したタイプであった場合、または、メッセージに複数のファイルが添付されている場合は、その他の添付ファイルに対して既存のルールが存在しない場合のみ、除外されます。これ以外の場合は、メッセージはスキャンされます。

メッセージフィルタ、コンテンツフィルタ、および電子メールパイプライン

メッセージフィルタおよびコンテンツフィルタは、感染フィルタによるスキャンが実行される前にメッセージに適用されます。フィルタを適用することにより、メッセージが感染フィルタ スキャンをスキップしたり、バイパスしたりする場合があります。



CHAPTER 11

データ消失防止

情報化時代では、組織のデータが組織の最も大切な財産の 1 つです。組織では多額の費用をかけ、従業員、顧客、パートナーがデータを利用できるようにしています。データは電子メールと Web を通して絶え間なく行き交っています。このようにデータアクセスが増加したため、機密情報や占有情報の悪意または過失による消失をどのように防止するか答えを見つけ出すことは、情報セキュリティの専門家にとって難問となっています。

Cisco IronPort 電子メールセキュリティ アプライアンスは、統合データ消失防止 (DLP) スキャンエンジンと RSA Security Inc. の DLP ポリシー テンプレートを提供して機密データの識別と保護を行うことにより、データの安全を確保します。RSA Email DLP 機能により、ユーザが過失によって機密データを電子メールで送付しないように防止することで、組織の情報と知的財産を保護し、規制と組織のコンプライアンスを実施します。従業員が電子メールで送付してもよいデータの種類と、機密情報を含むメッセージの検疫やコンプライアンス責任者への通知などアプライアンスが講じるアクションを定義します。

RSA Email DLP スキャンは、イネーブルになっていれば、感染フィルタの段階の直後にアプライアンスの「ワーク キュー」で発信メールに対して実行されません。詳細については、「メッセージ分裂」(P.6-6) を参照してください。

この章は、次の内容で構成されています。

- 「Email DLP の動作を理解する」(P.11-2)
- 「RSA Email DLP グローバル設定」(P.11-4)
- 「DLP ポリシー」(P.11-6)
- 「DLP Assessment Wizard の使用」(P.11-17)
- 「コンテンツ照合分類子」(P.11-23)
- 「コンテンツ照合分類子用の正規表現」(P.11-29)

- 「高度な DLP ポリシーのカスタマイズ」 (P.11-31)
- 「RSA Email DLP の受信者ごとのポリシーの設定」 (P.11-34)

Email DLP の動作を理解する

RSA Email DLP 機能では、3 段階のポリシー構造を使って、組織のデータ損失防止ルールと、メッセージがそのルールに違反したときに Cisco IronPort アプライアンスが講じるアクションを定義します。

- **検出ルール。**最も低いレベルの場合、DLP コンテンツ スキャンは、テキストのブロック内に特定のパターンがないかスキャンする検出ルールで構成されています。これらの検出ルールには、正規表現、単語やフレーズ、ディクショナリ、スマート ID に似たエンティティなどがあります。
- **コンテンツ照合分類子。**次のレベルはコンテンツ照合分類子であり、発信メッセージと、添付ファイルおよびヘッダーにクレジットカードデータや他の個人データなどの機密情報がないかスキャンします。分類子には、さらなる条件を適用するコンテキストルールを伴う検出ルールが多数あります。例として、RSA が開発したクレジットカード番号分類子を検討します。この分類子は、メッセージがクレジットカード番号のパターンに一致するテキスト文字列を含むだけでなく、有効期限、クレジットカード会社 (Visa、AMEX など)、名前および住所などの補足情報も含むように定めています。この追加情報を必須とすることで、メッセージコンテンツの判断がより正確となり、false positive も少なくなります。分類子が、メッセージ内に組織の DLP ルールに違反している機密情報を検出すると、DLP 違反が発生します。
- **DLP ポリシー。**最も高いレベルは、DLP ポリシーで、条件のセットとアクションのセットからなります。条件には、送信者、受信者、添付ファイルのタイプなどの、メッセージのコンテンツに対する分類子とメッセージメタデータのテストが含まれます。アクションでは、メッセージに対する全体的なアクション (配信、ドロップ、または検疫)、およびメッセージの暗号化、コピー、ヘッダーの変更、通知の送信といった二次的なアクションの両方を指定します。

DLP Policy Manager で組織の DLP ポリシーを定義し、発信メール ポリシーでそのポリシーをイネーブルにします。「ワーク キュー」の感染フィルタの段階の後で、アプライアンスは DLP ポリシー違反がないか発信メッセージをスキャン

します。AsyncOS の DLP Assessment Wizard を使うと、最もよく使われる DLP ポリシーを簡単に設定できます。詳細については、「[DLP Assessment Wizard の使用](#)」(P.11-17) を参照してください。

RSA Email DLP スキャン エンジン は、発信メール ポリシーでイネーブルになっている DLP ポリシーの分類子をすべて使って、各メッセージとそのヘッダーおよび添付ファイルをスキャンします。ヘッダーをスキャンするために、Cisco IronPort アプライアンスのコンテンツ スキャン エンジン は、ヘッダーをメッセージ本文またはコンテンツのすべての MIME 部分に付加し、RSA Email DLP スキャン エンジン は、コンテンツ照合分類子スキャンを実行します。添付ファイルをスキャンするために、コンテンツ スキャン エンジン は添付ファイルを抽出し、RSA Email DLP スキャン エンジン はその内容をスキャンします。

スキャンが完了すると、RSA Email DLP エンジン が、イネーブルになっている DLP ポリシーのいずれかに対してメッセージが違反していないか確認します。違反が複数の DLP ポリシーに一致している場合、RSA Email DLP エンジン は、発信メール ポリシーのリストを上から順に調べ、最初に一致する DLP ポリシーを選択します。DLP Policy Manager で DLP ポリシーの順序を定義します。

RSA Email DLP エンジン は、最初に DLP 違反のリスク要因スコアを計算することで、メッセージの取り扱い方を決定します。リスク要因スコアは、DLP 違反の重大度を 0 ～ 100 の範囲で示します。RSA Email DLP エンジン は、リスク要因スコアを DLP ポリシー用に定義されている重大度基準と比較します。重大度基準は、想定される DLP 違反を次の重大度レベルの 1 つに区分します。

- Ignore
- Low
- Medium
- High
- Critical

重大度レベルにより、メッセージに適用されるアクション（設定されていれば）が決まります。

DLP インシデント レポートを使って、発信メールで発生した DLP 違反の情報を見ることができます。また、メッセージ トラッキングを使って、DLP 違反の重大度をもとにしたメッセージの検索もできます。

- DLP 電子メール ポリシーおよびコンテンツ照合分類子の詳細については、「[DLP ポリシー](#)」(P.11-6) を参照してください。
- コンテンツ照合分類子の詳細については、「[コンテンツ照合分類子](#)」(P.11-23) を参照してください。

- DLP インシデント レポートの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。
- メッセージ トラッキングでの、DLP 違反があるメッセージの検索については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Tracking Email Messages」の章を参照してください。



(注)

スキャン エンジンには、メッセージのスキャン時に分類子を 1 回だけ使用します。1 つの発信メール ポリシーに同じ分類子を使う 2 つ以上の DLP ポリシーがある場合、すべてのポリシーは分類子の 1 回のスキャンの結果を使用します。

ハードウェア要件

RSA Email DLP 機能は、すべての C-Series および X-Series アプライアンスでサポートされます。ただし、C10、C30、C60、C100、C300D、C350D、C360D、および C370D アプライアンスは除きます。

RSA Email DLP グローバル設定

機密データがないか発信電子メールをスキャンするには、[Security Services] > [RSA Email DLP] ページを使って、最初にアプライアンス上で RSA Email DLP スキャンをイネーブルにします。DLP Assessment Wizard を起動して、最もよく使われる DLP ポリシーをアプライアンス上でイネーブルにするか、手動で RSA Email DLP 機能をイネーブルにするか選択できます。

DLP Assessment Wizard の起動方法については、「[DLP Assessment Wizard の使用](#)」(P.11-17) を参照してください。RSA Email DLP を手動でイネーブルにする方法については、「[RSA Email DLP のイネーブル化とグローバル設定の設定](#)」(P.11-5) を参照してください。

RSA Email DLP をイネーブルにすると、DLP Policy Manager で DLP ポリシーおよびアクションを設定し、電子メール セキュリティ マネージャを使って発信メール ポリシーでそのポリシーとアクションをイネーブルにすることができます。詳細については、「[DLP ポリシー](#)」(P.11-6) および「[RSA Email DLP の受信者ごとのポリシーの設定](#)」(P.11-34) を参照してください。

RSA Email DLP のイネーブル化とグローバル設定の設定



(注) DLP Assessment Wizard を使って、アプライアンスの DLP ポリシーを設定するには、「[DLP Assessment Wizard の使用](#)」(P.11-17) を参照してください。

RSA Email DLP をアプライアンスでイネーブルにするには、次の手順に従います。

ステップ 1 [Security Services] > [RSA Email DLP] を選択します。

ステップ 2 [Enable] をクリックします。

ステップ 3 ライセンス契約書ページが表示されます。



(注) ライセンス契約に合意しない場合、RSA Email DLP はアプライアンス上でイネーブルになりません。

ステップ 4 ページの下部までスクロールし、[Accept] をクリックしてライセンス契約に合意します。

ステップ 5 [Enable] をクリックします。

RSA Email DLP がアプライアンス上でイネーブルとなります。

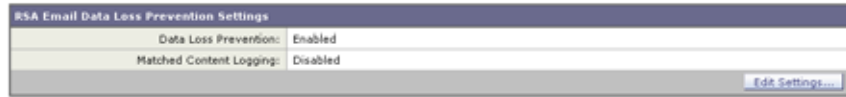
ステップ 6 [Edit Settings] をクリックします。

[Edit RSA Email Data Loss Prevention Global Settings] ページが表示されます。

ステップ 7 メッセージ トラッキングがアプライアンス上ですでにイネーブルになっている場合は、一致したコンテンツのログへの記録をイネーブルにするかしないか選択します。これを選択すると、Cisco IronPort アプライアンスは DLP 違反をログに記録し、AsyncOS は DLP 違反および周辺コンテンツをメッセージ トラッキングに表示します。その中には、クレジットカード番号や社会保障番号などの機密データが含まれます。

ステップ 8 変更を送信して確定します。

図 11-1 RSA Email Data Loss Prevention のイネーブル化
RSA Email Data Loss Prevention Settings



DLP ポリシー

DLP ポリシーは、発信メッセージが機密データとアクションを含んでいるか AsyncOS および RSA Email DLP スキャン エンジンが判断するために使う条件と、メッセージにそのようなデータが含まれている場合 AsyncOS が講じるアクションとを組み合わせたものです。

DLP ポリシーには、RSA が開発したコンテンツ照合分類子が含まれます。分類子は、RSA Email DLP スキャン エンジンによって、メッセージおよび添付ファイル内の機密データ検出のため、使用されます。分類子は、クレジットカード番号や運転免許 ID のようなデータ パターンを探すだけでなく、パターンのコンテキストも検査するため false positive が少なくなります。詳細については、「[コンテンツ照合分類子](#)」(P.11-23) を参照してください。

RSA Email DLP スキャンが行われる前に、Cisco IronPort アプライアンスのコンテンツ スキャン エンジンは送信元、送信先、CC、および件名のヘッダーをメッセージ本文またはコンテンツのタグが付けられたすべての MIME 部分に付加します。これにより、DLP スキャン エンジンは、ポリシーのコンテンツ照合分類子を使用してこれらのヘッダーをスキャンできるようになります。

DLP スキャン エンジンが、メッセージや添付ファイルで DLP 違反を検出すると、DLP スキャン エンジンは、違反のリスク要因を決定し、その結果をマッチング DLP ポリシーに返します。ポリシーは、独自の重大度基準を使ってリスク要因をもとに DLP 違反の重大度を評価し、メッセージに対して適切なアクションを適用します。その基準には、Ignore、Low、Medium、High、Critical の 5 つの重大度レベルがあります。

Ignore 以外のすべてのセキュリティ レベルで講じることができるアクションには次のものがあります。

- 検査中のメッセージに適用する、配信、ドロップ、検疫といった全体的なアクション。
- メッセージの暗号化。このアプライアンスは、メッセージ本文だけを暗号化します。メッセージ ヘッダーは暗号化されません。

- DLP 違反があるメッセージの件名ヘッダーの変更。
- メッセージへの免責事項の追加。
- メッセージの代替送信先メールホストへの送信。
- メッセージのコピー (bcc) の他の受信者への送信 (たとえば、重大な DLP 違反を含むメッセージのコピーを、以降の検査のためにコンプライアンス責任者のメールボックスに送信します)。
- DLP 違反の通知メッセージを、送信者や、マネージャまたは DLP コンプライアンス責任者といった他の連絡先に送信します。



(注)

これらのアクションは相互排他的ではなく、ユーザグループのさまざまな要求を処理するために、異なる DLP ポリシー内でアクションをいくつか組み合わせることができます。同一ポリシー内で重大度レベルに応じて異なる対応になるように設定することも可能です。たとえば、重大な違反を含むメッセージは検疫し、コンプライアンス責任者に通知を送信しますが、重大度レベルが低いメッセージは配信する、といったことです。

ポリシーのコンテンツ

Email DLP ポリシーには次の情報が含まれます。

- ポリシーの名称と説明。
- コンテンツ照合分類子の一覧。ポリシーによっては、識別番号を検索する正規表現の作成が必須場合があります。詳細については、「[コンテンツ照合分類子](#)」(P.11-23) を参照してください。
- メッセージフィルタリング用の特定の送信者および受信者のリスト。詳細については、「[送信者および受信者のフィルタリング](#)」(P.11-14) を参照してください。
- メッセージフィルタリング用の添付ファイルのタイプ一覧。詳細については、「[添付ファイルのフィルタリング](#)」(P.11-15) を参照してください。
- 重大度の設定。設定に適用されるアクションおよび重大度基準の調整を含みます。詳細については、「[重大度レベルの設定](#)」(P.11-15) を参照してください。

DLP Policy Manager

DLP Policy Manager は、Cisco IronPort アプライアンス上で Email DLP ポリシーをすべて管理する単一のダッシュボードです。DLP Policy Manager は [Mail Policies] メニューからアクセスします。DLP Policy Manager から、次のアクションを実行できます。

- 事前定義されたテンプレートをもとにした DLP ポリシーの作成および管理。詳細については、「事前定義されたテンプレートをもとにした Email DLP ポリシーの作成」(P.11-11) を参照してください。
- カスタム テンプレートをもとにした DLP ポリシーの作成および管理。詳細については、「Custom Policy テンプレートを使用した DLP ポリシーの作成」(P.11-31) を参照してください。
- カスタム DLP ディクショナリの作成、インポートおよび管理。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Text Resources」の章を参照してください。
- 米国運転免許証分類子の管理。詳細については、「米国運転免許証分類子」(P.11-10) を参照してください。

図 11-2 アクティブな DLP ポリシーがある DLP Policy Manager
DLP Policy Manager: Active Policies for Outgoing Mail

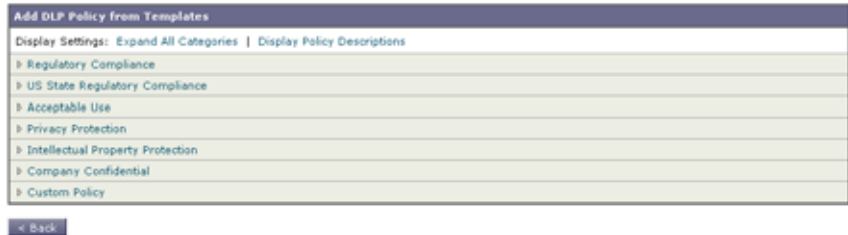
Active DLP Policies for Outgoing Mail			
Add DLP Policy...			
Order	DLP Policy	Duplicate	Delete
1	Payment Card Industry Data Security Standard (PCI-DSS)		
2	Email to Competitor		
3	A&A Routing Numbers		
4	California SB-1386		
Edit Policy Order...			
Advanced Settings			
US Drivers Licenses		All Classifiers Enabled	
Custom DLP Dictionaries (for use in Custom Policies only)		None Available	

RSA Email DLP ポリシー テンプレート

AsyncOS には、組織の知的財産や極秘情報を保護する、RSA の開発による事前定義されたポリシー テンプレートが多数あり、法や業界標準で規定されているルールや規制を強制的に適用します。DLP Policy Manager を使って DLP ポリシーを作成するときには、最初に使用するテンプレートを選択します。

図 11-3 は、使用可能な DLP ポリシー テンプレートのカテゴリを示しています。

図 11-3 テンプレートから DLP ポリシーを追加
DLP Policy Manager: Add DLP Policy



DLP ポリシー テンプレートは次のカテゴリに整理されます。

- [Regulatory Compliance]。個人情報、クレジット情報、他の保護情報や非公開情報を含むメッセージおよび添付ファイルを識別します。
- [Acceptable Use]。競合他社や制限された受信者に送信するメッセージで、組織に関する機密情報を含むものを識別します。
- [Privacy Protection]。金融口座、税金記録、国民 ID の識別番号を含むメッセージおよび添付ファイルを識別します。
- [Intellectual Property Protection]。よく使われるパブリッシングおよびデザインドキュメントファイルタイプで、組織が保護する知的財産を含む可能性があるものを識別します。
- [Company Confidential]。会社の財務情報や近い将来の合併および買収に関する情報を含むドキュメントとメッセージを識別します。
- [Custom Policy]。AsyncOS では、RSA や組織で開発された分類子を使って、独自のポリシーをゼロから作成するオプションもあります。このオプションは高度であり、事前定義されたポリシー テンプレートではユーザーのネットワーク環境の独自の要件を満たせない、まれな場合にのみ使用されることを想定しています。詳細については、「高度な DLP ポリシーのカスタマイズ」(P.11-31) を参照してください。

カスタマイズが必要な DLP ポリシー テンプレートについては、「DLP ポリシーに対する分類子のカスタマイズ」(P.11-12) を参照してください。

図 11-4 に、Family Educational Rights and Privacy Act (FERPA; 家族教育権とプライバシー法) 違反を検出する、事前定義された RSA ポリシー テンプレートを示します。

図 11-4 事前定義された RSA Email DLP ポリシー テンプレート
Mail Policies: DLP: Policy: FERPA (Family Educational Rights and Privacy Act)

Policy: FERPA (Family Educational Rights and Privacy Act)

DLP Policy Name: FERPA (Family Educational Rights and Privacy Act)

Description: Identifies documents and transmissions that contain student information protected by the Family Education Rights and Privacy Act (FERPA) in the United States. FERPA defines regulations that protect personally identifiable information (PII) (student records) held by

Content Matching Classifier: Student Identification Numbers (customization recommended) AND Student Records

Student Identification Numbers as a regular expression:

Combine multiple number patterns with "|" to form a single expression. (Example: 123-C1456789 matches the regular expression [0-9]{3}\-[A-Z]{2}[0-9]{6} See more examples.)

AND match with related words or phrases:

Separate multiple entries with a line break or comma. Sometimes number patterns consistently appear with words or phrases as in "Student Identification Numbers: 123-C1456789." Including the words "Student Identification Numbers:" would improve content matching accuracy.

Filter Senders and Recipients: Restrict this DLP policy by specific recipients and senders.

Filter Attachments: Restrict this DLP policy to detect specific attachment types.

Filter Message Tags: Restrict this DLP policy to detect message tags.

Severity Settings

Critical Severity Settings

Action Applied to Messages: Deliver

Enable Encryption

Encryption is unavailable. This service is disabled. (See Security Services > IronPort Email Encryption)

Advanced: This section contains settings for Message modifications, message delivery and DLP notifications.

High Severity Settings

Inherit Critical Severity settings.

Medium Severity Settings

Inherit High Severity settings.

Low Severity Settings

Inherit Medium Severity settings.

Severity Scale

Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 9	10 - 34	35 - 59	60 - 89	90 - 100

Edit Scale...

Cancel Submit

米国運転免許証分類子

米国運転免許証分類子を使用するポリシーは多数あります。デフォルトでは、この分類子は米国 50 州すべておよびコロンビア特別区の運転免許を検索します。カルフォルニア州の AB-1298 およびモンタナ州の HB-732 など米国の州固有のポリシーでは、51 タイプすべての運転免許を検索します。false positive またはアプライアンスのパフォーマンスが問題となるのであれば、DLP Policy Manager の [Advanced Settings] の下の米国運転免許証用のリンクをクリックし

て、検索を特定の米国の州に限定する、またはどの州も検索しないようにできます。RSA スキャン エンジンが運転免許分類子をどのように使用するかについては、「[米国運転免許証](#)」(P.11-26) 参照してください。

事前定義されたテンプレートをもとにした Email DLP ポリシーの作成

DLP ポリシーは、事前定義されたテンプレートまたはカスタム テンプレートのいずれかを使用して、作成可能です。カスタム テンプレートの使用方法については、「[Custom Policy テンプレートを使用した DLP ポリシーの作成](#)」(P.11-31) を参照してください。

事前定義されたテンプレートをもとにした DLP ポリシーを追加する方法。

ステップ 1 [Mail Policies] > [DLP Policy Manager] を選択します。

ステップ 2 [Add DLP Policy] をクリックします。

ステップ 3 カテゴリ名をクリックし、使用可能な RSA Email DLP ポリシー テンプレートの一覧を表示します。



(注) [Display Policy Descriptions] をクリックして、使用可能なポリシー テンプレートの詳細な説明を表示することができます。

ステップ 4 使用する RSA Email DLP ポリシー テンプレートの [Add] をクリックします。

[図 11-4 \(P.11-10\)](#) とほぼ同じページが開きます。事前定義されたテンプレートすべてに名前と説明がありますが、変更できます。テンプレートのほとんどには 1 つ以上の分類子があり、いくつかのテンプレートには事前定義された添付ファイルのタイプがあります。

ステップ 5 ポリシーが、カスタマイズされた分類子を必要とする場合は、組織の識別番号付けシステムのパターンと、識別番号に関連する単語やフレーズの一覧を定義するための正規表現を入力します。詳細については、「[DLP ポリシーに対する分類子のカスタマイズ](#)」(P.11-12) を参照してください。



(注) 事前定義されたテンプレートをもとにしたポリシーでは、分類子の追加および削除はできません。

- ステップ 6** 任意で、DLP ポリシーの適用を、特定の受信者や送信者、添付ファイルのタイプやメッセージタグを持つメッセージに限定することができます。詳細については、「[DLP ポリシーのメッセージのフィルタリング](#)」(P.11-14) を参照してください。
- ステップ 7** [Critical Settings] セクションで、重大な DLP 違反を含むメッセージをドロップ、配信、または検疫するか選択します。
- ステップ 8** 任意で、メッセージの暗号化、ヘッダーの修正、代替ホストへのメッセージの送信、別の受信者へのコピーの配信 (bcc)、DLP 通知メッセージの送信を選択できます。
- DLP 通知については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。
- ステップ 9** 一致する重大度レベルが High、Medium、Low のメッセージに、別々の設定を定義するときは、適切なセキュリティレベルの [Inherit settings] チェックボックスをオフにします。メッセージへの全体的なアクションや他の設定を編集します。
- ステップ 10** ポリシーに対して DLP 違反の重大度基準を調整する場合は、[Edit Scale] をクリックして設定を調整します。詳細については、「[重大度レベルの設定](#)」(P.11-15) を参照してください。
- ステップ 11** 変更を送信して確定します。

ポリシーが DLP Policy Manager に追加されます。

DLP ポリシーに対する分類子のカスタマイズ

DLP ポリシー テンプレートには、より効果的にするためカスタマイズされた分類子を必要とするものもあります。このような分類子は、発信メッセージ内に患者や学生の識別番号など極秘の識別番号がないか検索しますが、組織の記録番号付けシステムのパターンを定義する正規表現を 1 つ以上必要とします。補足情報の記録識別番号に関連する単語およびフレーズの一覧を追加することもできます。分類子が発信メッセージ内に番号パターンを検出すると、補足情報を検索し、そのパターンが識別番号か、また、ランダムな番号の文字列でないかを確認します。これにより、false positive が少なくなります。

たとえば、Health Insurance Portability and Accountability Act (HIPAA; 医療保険の相互運用性と説明責任に関する法律) テンプレートを使ってポリシーを作成するとします。このテンプレートには、患者識別番号コンテンツ照合分類子という患者識別番号を検出するようにカスタマイズ可能な分類子が含まれます。この分類子に正規表現 `[0-9]{3}\-[A-Z]{2}[0-9]{6}` を入力します。この正規表現

では、123-CL456789 というパターンの番号が検出されます。関連フレーズとして「Patient ID」を入力します。ポリシーの作成を完了し、発信メール ポリシーでイネーブルにします。変更を送信して確定します。これで、ポリシーが発信メッセージ内の番号のパターンを検出し、その近くに「Patient ID」というフレーズがある場合、ポリシーは DLP 違反を返すようになります。

次の DLP ポリシー テンプレートには、カスタマイズ可能なコンテンツ照合分類子があります。

- **Health Insurance Portability and Accountability Act (HIPAA; 医療保険の相互運用性と説明責任に関する法律)**。患者識別番号分類子はカスタマイズ可能ですが、必須ではありません。患者識別番号分類子または患者 ID および HIPAA ディクショナリ分類子に一致すると、DLP 違反を返します。
- **Family Educational Rights and Privacy Act (FERPA; 家族教育権とプライバシー法)**。生徒識別番号分類子のカスタマイズが必要です。生徒識別番号および生徒記録分類子に一致すると、DLP 違反となります。
- **Gramm-Leach Bliley Act (GLBA; グラム リーチ ブライリー法)**。カスタム アカウント番号分類子はカスタマイズ可能ですが、必須ではありません。次の分類子に 1 つ以上一致すると、DLP 違反となります。カスタム アカウント番号、米国運転免許証、クレジット カード番号または米国社会保障番号。
- **California AB-1298**。グループ保険番号、医療記録番号、患者識別番号分類子はカスタマイズ可能ですが、必須ではありません。次の分類子に 1 つ以上一致すると、DLP 違反となります。グループ保険番号、医療記録番号、患者識別番号、米国運転免許証、患者 ID、クレジット カード番号、HIPAA ディクショナリ。
- **Massachusetts CMR-201**。米国銀行口座番号分類子はカスタマイズ可能ですが、必須ではありません。次の分類子に 1 つ以上一致すると、DLP 違反となります。米国銀行口座番号、米国運転免許証、クレジット カード番号、米国社会保障番号、ABA ルーティング番号分類子。このポリシー テンプレートは、AsyncOS 7.1.1 以降で使用可能です。
- **カスタム アカウント番号**。カスタム アカウント番号分類子のカスタマイズが必須です。カスタム アカウント番号分類子に一致すると DLP 違反となります。
- **患者識別番号**。患者識別番号分類子はカスタマイズ可能ですが、必須ではありません。患者識別番号または患者 ID 分類子に一致すると、DLP 違反となります。

- **合併および買収。** 合併および買収コード名分類子のカスタマイズには、単語またはフレーズの一覧を使いますが、必須ではありません。正規表現を使う必要ありません。合併および買収コード名または合併キーワード分類子に一致すると DLP 違反になります。

正規表現の作成方法については、「[コンテンツ照合分類子用の正規表現](#)」(P.11-29) を参照してください。コンテンツ照合分類子がどのようにして DLP 違反を検出するかの詳細については、「[コンテンツ照合分類子](#)」(P.11-23) 参照してください。

DLP ポリシーのメッセージのフィルタリング

AsyncOS が検出した特定の情報に基づいて、DLP ポリシーの適用をメッセージのスキャンのみに限定できます。次の情報に従って、DLP ポリシー スキャンを制限できます。

- 送信者および受信者
- 添付タイプ
- メッセージ タグ

送信者および受信者のフィルタリング

次の方法の 1 つで、DLP ポリシーを特定の受信者または送信者のメッセージだけをスキャンするように限定できます。

- 完全な電子メール アドレス : `user@example.com`
- 電子メール アドレスの一部 : `user@`
- ドメインのすべてのユーザ : `@example.com`
- 部分ドメインのすべてのユーザ : `@.example.com`

改行やカンマで、複数のエントリを分離できます。

発信メッセージに対して、AsyncOS は最初に受信者または送信者が発信メールポリシーと一致するか照合します。受信者または送信者が一致したら、RSA Email DLP は、送信者または受信者がメール ポリシーでイネーブルとなっている DLP ポリシーと一致するか照合します。

添付ファイルのフィルタリング

DLP ポリシーの適用を特定の添付ファイルのタイプを持つメッセージに限定することができます。最初に添付ファイルが AsyncOS のコンテンツ スキャン エンジンにより抽出され、次に添付ファイルの内容が RSA Email DLP スキャン エンジンによってスキャンされます。アプライアンスでは、多数の事前定義されたファイル タイプをスキャンで使用できますが、一覧にないファイル タイプを指定することもできます。事前定義されていないファイル タイプを指定すると、AsyncOS は、添付ファイルの拡張子をもとにファイルタイプを検索します。RSA Email DLP のスキャンを、最小ファイル サイズ (バイト) 以上の添付ファイルに限定することができます。

メッセージ タグによるフィルタリング

DLP ポリシーを特定のフレーズを含むメッセージのスキャンに限定する場合は、メッセージまたはコンテンツ フィルタを使って発信メッセージにそのフレーズがないか検索し、カスタム メッセージ タグを当該メッセージに挿入することができます。DLP ポリシー作成時に、発信メッセージのフィルタリングに使用するメッセージ タグを選択します。詳細については、「[コンテンツ フィルタのアクション](#)」(P.6-20)、および『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Mail Policies」を参照してください。

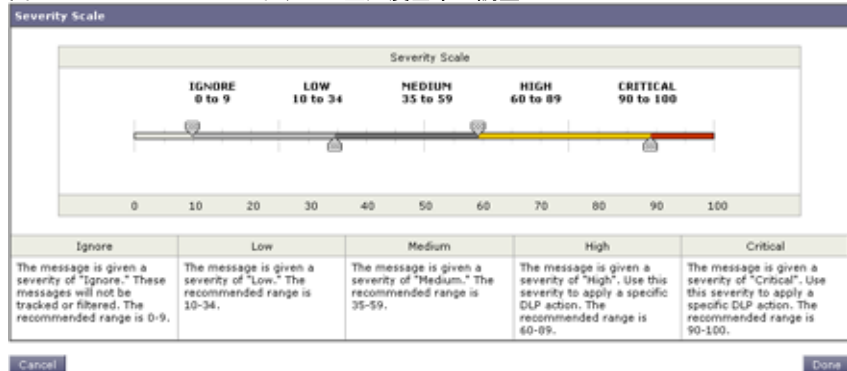
重大度レベルの設定

RSA Email DLP スキャン エンジンが DLP 違反を検出すると、DLP 違反の重大度を示すリスク要因スコア (0 ~ 100 の範囲) を計算します。ポリシーは、リスク要因スコアを重大度基準と比較します。重大度基準には、Ignore、Low、Medium、High、Critical の 5 つの重大度レベルがあります。重大度レベルで、メッセージに適用されるアクションが決まります。デフォルトで、すべての重大度レベル (Ignore を除く) で高位の重大度レベルの設定を継承するようになっています。High の重大度レベルは Critical から設定を継承し、Medium は High から、Low は Medium から継承します。レベルを編集し、異なる重大度に対して別々のアクションを指定することができます。

DLP スキャン エンジンのリスク要因の計算については、「[Email DLP の動作を理解する](#)」(P.11-2) を参照してください。

重大度基準をポリシーに対して調整し、スキャン エンジンが返す DLP 違反の推定重大度を規定できます。図 11-5 は重大度基準を示します。基準の矢印を使って、重大度レベルに対するスコアを調整します。

図 11-5 DLP ポリシー重大度基準の調整



Email DLP ポリシーの順序の設定

DLP Policy Manager でのポリシーの順序は重要です。DLP 違反が発生した場合、RSA Email DLP は、その違反を発信メール ポリシーでイネーブルな DLP ポリシーと照合します。違反が複数の DLP ポリシーに一致する場合、RSA Email DLP は上から順に調べ、最初に一致した DLP ポリシーを選択します。

- ステップ 1 [DLP Policy Manager] ページで、[Edit Policy Order] をクリックします。
- ステップ 2 移動するポリシーの行をクリックし、新しい順序の場所にドラッグします。
- ステップ 3 ポリシーの順序の変更を完了したら、変更を送信して確定します。

Email DLP ポリシーの編集

既存の DLP ポリシーを編集するには、次の手順に従います。

- ステップ 1 [DLP Policy Manager] ページに一覧表示されている RSA Email DLP ポリシーの名前をクリックします。

[Mail Policies: DLP] ページが表示されます。

ステップ 2 DLP ポリシーを変更します。

ステップ 3 変更を送信して確定します。



(注) ポリシーの名前を変更すると、電子メール セキュリティ マネージャで再度イネーブルにする必要があります。

Email DLP ポリシーの削除

DLP ポリシーを削除するには、一覧のポリシーの隣にあるゴミ箱アイコンをクリックします。確認メッセージが表示されます。このメッセージは、DLP ポリシーが 1 つ以上の複数の発信メール ポリシーで使用されているかを示しています。ポリシーの削除により、このようなメール ポリシーからポリシーが削除されます。変更を送信して確定します。

Email DLP ポリシーの複製

既存のポリシーとほぼ同じで設定が異なる DLP ポリシーを作成する場合は、DLP Policy Manager で複製ポリシーを作成することができます。

Email DLP ポリシーを複製するには、次の手順に従ってください。

ステップ 1 [DLP Policy Manager] ページで、一覧の中から複製対象のポリシーの隣にある複製アイコンをクリックします。

ステップ 2 ポリシーの名前を入力します。

ステップ 3 ポリシーの設定を変更します。

ステップ 4 変更を送信して確定します。

DLP Assessment Wizard の使用

AsyncOS のブラウザ ベース DLP Assessment Wizard を使うと、よく使われる DLP ポリシーの設定と、そのポリシーをアプライアンスのデフォルトの発信メール ポリシーでイネーブルにする 3 つの手順のプロセスを簡単に行えます。

DLP Assessment Wizard を使って追加された DLP ポリシーでは、検出された DLP 違反の重大度にかかわらず、メッセージはすべて配信されます。DLP Policy Manager を使って、メッセージに適用される全体的なアクション、受信者または送信者のフィルタリング、添付ファイルのタイプのフィルタリング、および重大度レベルの設定を編集します。DLP ポリシーの編集の詳細については、「[DLP Policy Manager](#)」(P.11-8) 参照してください。

DLP Assessment Wizard により、メッセージトラッキング用に、一致したコンテンツをログに記録できます。電子メールセキュリティアプライアンスは検出した DLP 違反をログに記録し、AsyncOS はメッセージトラッキングにある、クレジットカードや番号や社会保障番号など機密データを含む違反と周辺のコンテンツを表示します。DLP Assessment Wizard は、メッセージトラッキングがイネーブルでなかった場合、アプライアンス上で自動的にイネーブルにします。アプライアンスがこのデータをログに記録しないようにする場合は、[Security Services] > [RSA Email DLP] ページを使って、一致したコンテンツのログへの記録をディセーブルにします。

DLP Assessment Wizard を起動するには、[Security Services] > [RSA Email DLP] ページを開きます。[Enable] をオンにし、[DLP using the DLP Assessment Wizard] チェックボックスを設定します。次に [Enable] をクリックします。

DLP ポリシーがアプライアンスに存在しない場合は、DLP Assessment Wizard のみ使用することができます。

☒ 11-6 は、DLP Assessment Wizard の実行オプションを示しています ([RSA Email Data Loss Prevention Settings] ページより)。

図 11-6 [RSA Email Data Loss Prevention Settings] ページ
RSA Email Data Loss Prevention Settings



DLP Assessment Wizard の実行

DLP Assessment Wizard を使用すると、次の DLP 設定作業が簡単にできます。作業は、3 つの手順に分けることができます。

ステップ 1 ポリシー

- ネットワーク上で保護する情報のタイプに合わせて DLP ポリシーを選択します。
- 機密データを検出するために追加情報を必要とする DLP ポリシーをカスタマイズします。

ステップ 2 レポート

- DLP Incident Summary レポート配信設定を設定します。

ステップ 3 レビュー

- DLP ポリシーをレビューしてイネーブルにします。

各手順を完了させたら、[Next] をクリックして、DLP Assessment Wizard の手順を進めていきます。[Previous] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようプロンプトが表示されます。確定するまで、変更は有効になりません。

手順 1 : ポリシー**DLP ポリシーの選択**

アプライアンスが発信メッセージ内で検出対象とする機密情報のタイプ用の DLP ポリシーを選択します。

次のポリシーを使用できます。

- [Payment Card Industry Data Security Standard (PCI-DSS)]. クレジットカード トラック データおよびクレジットカード。
- [HIPAA (Health Insurance Portability and Accountability Act)] は、HIPAA デクショナリとコードセット、米国社会保障番号、米国国家プロバイダー認証を検出し、患者識別番号を検出するようにカスタマイズできます。
- [FERPA (Family Educational Rights and Privacy Act)] は、生徒記録を検出し、生徒識別番号を検出するようにカスタマイズできます。
- [GLBA (Gramm-Leach Bliley Act)] は、クレジットカード番号、米国社会保障番号、米国運転免許証番号を検出し、カスタム アカウント番号を検出するようにカスタマイズできます。
- [California SB-1386] は、カルフォルニア SB-1386 (民法 1798) で規制されている、米国社会保障番号、クレジットカード番号、米国運転免許証番号などの Personally Identifiable Information (PII; 個人情報) を含むドキュメ

ントと送信を検出します。カルフォルニアでビジネスを営み、カルフォルニア州民のコンピュータ化した PII データを保有またはライセンスしている企業は、物理的な所在地にかかわらず、準拠することが必須となっています。

- [Restricted Files] は、.mdb、.exe、.bat および Oracle 実行ファイル (.fmx、.fm) など制限されているファイルを含む電子メールを検出します。このポリシーは付加的なファイル属性をポリシー違反ルールに追加してカスタマイズできます。

DLP Policy Manager を使って、DLP ポリシーの他のタイプを作成できます。

DLP ポリシーのカスタマイズ

DLP ポリシーには、発信メッセージ内の機密情報を検出するようにカスタマイズできるコンテンツ照合分類子を使うものがあります。HIPAA、FERPA および GLB 用のカスタマイズされた分類子、ポリシーは正規表現を使い、発信メッセージ内に識別番号パターンがないか検索します。Restricted Files ポリシーを選択した場合は、DLP ポリシーで検出する添付ファイルタイプを選択します。Restricted Files ポリシーはデフォルトで .exe および .mdb ファイルを検出しますが、これらのファイルタイプを削除できます。Restricted Files ポリシーを暗号化またはパスワードで保護されたファイルのみに適用するように設定できます。

これらの DLP ポリシー用のコンテンツ照合分類子のカスタマイズの詳細については、「[DLP ポリシーに対する分類子のカスタマイズ](#)」(P.11-12) 参照してください。

[Next] をクリックして続行します。

図 11-7 DLP Assessment Wizard : 手順 1 : ポリシー
DLP Assessment Wizard

How vulnerable is your network to data loss?
Let the DLP Assessment Wizard set up a data loss prevention policy for your network.

What type of information would you like to protect in your network?

- Payment Card Industry Data Security Standard (PCI-DSS)**
This policy will detect credit card track data and credit cards.
- HIPAA (Health Insurance Portability and Accountability Act)**
This policy will detect HIPAA dictionaries and code sets, US Social Security numbers, US National Provider Identifiers and may be customized to detect patient identification numbers.
- FERPA (Family Educational Rights and Privacy Act)**
This policy will detect student records and can be customized to detect student identification numbers.
- GLBA (Gramm-Leach Bliley Act)**
This policy will detect credit card numbers, US Social Security numbers, US Drivers License numbers and may be customized to detect custom account numbers.
- California SB-1386**
Identifies documents and transmissions that contain personally identifiable information (PII) as regulated by California SB-1386 (Civil Code 1798). This policy detects US Social Security numbers, credit card numbers and US drivers license numbers.
- Restricted Files**
Identifies email transmissions that contain restricted files defined by you. By default the policy matches on mds, exe, bat and Oracle executable files (fmx, frm). This policy can be fully customized once the wizard is completed.

Cancel Next >

手順 2 : レポート

スケジュール済み DLP Incident Summary レポート用に電子メールアドレスを入力します。複数のアドレスを区切るには、カンマを使います。この値を空白のままにしておくと、スケジュール済みレポートは作成されません。DLP Incident Summary レポートの詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。

[Next] をクリックして続行します。

図 11-8 DLP Assessment Wizard : 手順 2 : レポート
DLP Reports

手順 3 : レビュー

DLP 設定情報の要約が表示されます。[Previous] ボタンをクリックするか、各セクションの右上にある対応する [Edit] リンクをクリックして、[Policies and Reporting] 情報を編集することができます。変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。

図 11-9 DLP Assessment Wizard : 手順 3 : レビュー
Review DLP Policies

表示されている情報が十分であれば、[Finish] をクリックします。AsyncOS により、[Outgoing Mail Policies] ページに、デフォルトの発信メール ポリシーでイネーブルになっている DLP ポリシーが表示されます。DLP ポリシー設定の要約が、ページの上部に表示されます。変更を確定します。

DLP ポリシーの編集と追加作成については、「[DLP Policy Manager](#)」(P.11-8) を参照してください。DLP ポリシーを他の発信メール ポリシーに対してイネーブルにする方法については、「[RSA Email DLP の受信者ごとのポリシーの設定](#)」(P.11-34) を参照にしてください。

コンテンツ照合分類子

コンテンツ照合分類子は、RSA Email DLP スキャン エンジンの検出コンポーネントです。クレジットカード番号や運転免許識別番号などのデータ パターン、およびそのパターンが出現するコンテキストがないか、メッセージ、メッセージ ヘッダー、および抽出した添付ファイルの内容を検索します。たとえば、クレジットカード番号を検出する分類子は、クレジットカード番号の形式に一致する数値のパターンだけではなく、有効期限やクレジットカード会社名などの補足データもないかスキャンします。データのコンテキストを評価することで、**false positive** が減少します。

RSA のポリシー テンプレートの多くは、分類子の事前定義されたセットを含みます。**Custom Policy** テンプレートをもとにしてポリシーを作成するときは、RSA 分類子を選択するか、独自の分類子を 1 つ追加できます。カスタム DLP ポリシーで使用する独自の分類子の作成については、「[コンテンツ照合分類子の作成](#)」(P.11-33) を参照してください。

多くのポリシー テンプレートでは、機密データ検出のために 1 つ以上の分類子をカスタマイズする必要があります。カスタマイズには、識別番号と、その識別番号とともに決まって出現する可能性がある単語とフレーズの一覧を検索するための正規表現を作成することが含まれます。たとえば、**Family Educational Rights and Privacy Act (FERPA; 家族教育権とプライバシー法)** テンプレートをもとにしたポリシーを追加するには、生徒 ID 番号に一致する正規表現を作成する必要があります。ID 番号が決まって「**Student ID**」というフレーズとともに出現するならば（「**Student ID: 123-45-6789**」など）、そのフレーズをポリシーに追加すればコンテンツ マッチングがより正確になります。DLP ポリシーで必須であるカスタマイズの詳細については、「[DLP ポリシーに対する分類子のカスタマイズ](#)」(P.11-12) 参照してください。



(注)

分類子を持たないポリシーに対しては、メッセージがポリシーに違反した場合、スキャン エンジンは常に「75」のリスク要因値を返します。このようなポリシーには、発生する可能性のある DLP 違反のタイプによって重大度基準を調整します。詳細については、「[重大度レベルの設定](#)」(P.11-15) を参照してください。

分類子検出ルール

分類子では、メッセージやドキュメント内の DLP 違反を検出するルールが必要となります。分類子では、次の検出ルールの 1 つ以上のルールを使用できます。

- **単語またはフレーズ。**分類子が探す単語およびフレーズの一覧。複数のエントリーは、カンマまたは改行で区切ります。
- **正規表現。**メッセージや添付ファイルの検索パターンを定義する正規表現。**false positive** を防止するため、照合から除外するパターンも定義できます。詳細については、「**DLP 用の正規表現の例**」(P.11-30) を参照してください。
- **ディクショナリ。**単語とフレーズに関連するディクショナリ。**RSA Email DLP** には、**RSA** が作成したディクショナリがありますが、独自のディクショナリを作成できます。詳細については、**第 14 章「テキストリソース」** を参照してください。
- **エンティティ。**スマート ID と同様に、エンティティはデータ内のパターン (ABA ルーティング番号、クレジットカード番号、住所、社会保障番号など) を識別します。

分類子は、メッセージ内で検出ルールと一致したものが見つかったと数値を割り当て、メッセージのスコアを計算します。メッセージの DLP 違反の重大度の決定に使われるリスク要因は、分類子の最終的なスコアの範囲を 0 ~ 100 としたものです。分類子は、次の値を使ってパターンを検出し、リスク要因を計算します。

- **近接性。**有効と見なすには、メッセージや添付ファイルの中でルールと一致する箇所がどのくらい近くで発生する必要があるかを定義します。たとえば、社会保障番号に似た数値のパターンが長いメッセージの上部に出現し、末尾の送信者の署名に住所が現れた場合、それらはおそらく関連がなく、分類子は一致と見なしません。
- **最小総合スコア。**分類子が結果を返すのに必要な最小スコア。メッセージの一致のスコアが最小総合スコアに達しなかった場合、そのデータは機密であるとは見なされません。
- **重み。**各ルールで、ルールの重要度を示す「重み」を指定します。分類子は、検出ルールに一致した数にルールの重みを乗算してメッセージのスコアを計算します。重みが 10 のルールで違反が 2 つある場合は、スコアは 20 となります。あるルールが分類子にとって他より重要であれば、より大きい重みをアサインすることになります。
- **最大スコア。**ルールの最大スコアは、重みが低いルールに一致するものが大量に発生しても、スキヤンの最終スコアがゆがめられないようにするものです。

リスク要因を計算するため、分類子は検出ルールに一致する数にルールの重みを乗算します。この値が検出ルールの最大スコアを超過した場合、分類子は最大スコアを使用します。分類子が複数の検出ルールを持つ場合、すべての検出ルールのスコアを合計して 1 つの値にします。分類子は表 11-1 にあるように、検出ルールのスコア（10 ～ 10000）を 10 ～ 100 の対数目盛りにマッピングし、リスク要因を算出します。

表 11-1 リスク要因計算用の対数目盛り

ルールのスコア	リスク要因
10	10
20	20
30	30
50	40
100	50
150	60
300	70
500	80
1000	90
10000	100

分類子の例

次の例は、分類子がメッセージの内容を照合する方法を示します。

クレジットカード番号

DLP ポリシー テンプレートのいくつかは、クレジットカード番号分類子を含みます。クレジットカード番号はそれ自体、数と句読点のパターン、発行者固有のプレフィクス、最後のチェック デジットなどさまざまな制約があります。この分類子で一致するには、別のクレジットカード番号、有効期限、発行者の名前など、追加の補足情報が必要です。これで **false positive** の数が減ります。

例を示します。

- 4999-9999-9999-9996（補足情報がないため一致せず）
- 4999-9999-9999-9996 01/09（一致）

- Visa 4999-9999-9999-9996 (一致)
- 4999-9999-9999-9996 4899 9999 9999 9997 (複数のクレジットカード番号があるため一致)

米国社会保障番号

米国社会保障番号分類子では、正しい形式の番号と誕生日や名前および「SSN」という文字列などの補足データが必要です。

例を示します。

- 321-02-3456 (補足情報がないため一致せず)
- 321-02-3456 July 4 (一致)
- 321-02-3456 7/4/1980 (一致)
- 321-02-3456 7/4 (一致せず)
- 321-02-3456 321-02-7654 (複数の SSN があるため一致)
- SSN: 321-02-3456 (一致)
- Joe Smith 321-02-3456 (一致)
- 321-02-3456 CA 94066 (一致)

ABA ルーティング番号

ABA ルーティング番号分類子は、クレジットカード番号分類子とほぼ同じです。

例を示します。

- 119999992 (補足情報がないため一致せず)
- routing 119999992 account 1234567 (一致)

米国運転免許証

DLP ポリシー テンプレートのいくつかは、米国運転免許証分類子を使用します。この分類子には、米国の各州およびコロンビア特別区用の検出ルールの一式が含まれています。DLP Policy Manager で [Advanced Settings] の下の米国運転免許証用のリンクをクリックすることで、組織のポリシーにとって重要でない州を選択してイネーブルまたはディセーブルにすることができます。



(注) California SB 1386 など特定の州用の事前定義された DLP ポリシー テンプレートは、すべての州向けの検出ルールを使用し、カルフォルニア州以外の運転免許のデータに対して DLP 違反を返します。これは、プライバシー違反と考えられるからです。

各州の分類子はその州のパターンと照合し、対応する州の名前または略称および追加の補足データを定めています。

例を示します。

- CA DL: C3452362 (番号と補足データのパターンが正しいため一致)
- California DL: C3452362 (一致)
- DL: C3452362 (補足データ不足のため一致せず)
- California C3452362 (補足データ不足のため一致せず)
- OR DL: C3452362 (オレゴン州の正しいパターンではないため一致せず)
- OR DL: 3452362 (オレゴン州の正しいパターンのため一致)
- WV DL: D654321 (ウエストバージニア州の正しいパターンのため一致)
- WV DL: G654321 (ウエストバージニア州の正しいパターンでないため一致せず)

HIPAA ディクショナリ

事前定義された HIPAA ポリシー テンプレートは、医療関連のデータを検出するため、HIPAA ディクショナリ分類子を使用します。この分類子は、患者 ID 分類子とともに動作し、個人情報を検出します。HIPAA DLP ポリシーで DLP 違反を返すには、この分類子での一致に加えて、米国社会保障番号や米国国家プロバイダー認証などの個人情報との一致も必要となります。

例を示します。

- angina, cancer (一致)
- angina (複数の用語を必要とするため一致せず)
- headache, fever (一致)
- camphor glycerin (一致)
- fracture paralysis (一致)

- bite cut (一致)

患者 ID

患者 ID 分類子では、HIPAA ポリシー テンプレートの個人情報コンポーネントを使用できます。このコンポーネントは、米国社会保障番号と米国 **National Provider Identifier (NPI; 国家プロバイダー認証)** 番号があるかスキャンします。NPI は、チェック デジットを含む 10 桁の数字です。

例を示します。

- 321-02-4567 7/4/1980 (米国社会保障番号および誕生日と考えられるため一致)
- NPI: 3459872347 (NPI があるため一致)
- 3459872347 (補足情報がないため一致せず)
- NPI: 3459872342 (誤ったチェック デジットのため一致せず)

生徒記録

事前定義された **Family Educational Rights and Privacy Act (FERPA; 家族教育権とプライバシー法)** DLP ポリシー テンプレートは、生徒記録分類子を使用します。より正確に検出するため、この分類子とカスタマイズされた生徒識別番号分類子を組み合わせて、特定の生徒 ID パターンを検出します。

例を示します。

- Joe Smith, Class Rank: 234, Major: Chemistry Transcript (一致)

企業財務情報

事前定義された **Sarbanes-Oxley (SOX)** ポリシー テンプレートは、企業財務情報分類子を使用し、非公開の企業の財務情報を検索します。

例を示します。

2009 Cisco net sales, net income, depreciation (一致)

FORM 10-Q 2009 I.R.S.Employer Identification No. (一致)

コンテンツ照合分類子用の正規表現

多くのポリシー テンプレートで 1 つ以上の分類子をカスタマイズする必要があります。カスタマイズには、カスタム アカウント番号や患者識別番号など極秘情報に結び付く可能性がある識別番号を検索するための正規表現の作成があります。コンテンツ照合分類子に使用される正規表現の形式は、**POSIX 基本正規表現**形式の正規表現です。

次のテーブルを、分類子用の正規表現の作成ガイドとして使用してください。

表 11-2 分類子での正規表現

正規表現 (abc)	<p>正規表現の一連の命令が文字列の一部に一致すると、分類子用の正規表現はその文字列に一致するということになります。</p> <p>たとえば、正規表現 <code>acc</code> は、文字列 <code>ACCOUNT</code> と <code>ACCT</code> に一致します。</p>
[]	<p>大カッコは文字のセットを示すために使用します。文字は個々または範囲で定義できます。</p> <p>たとえば、<code>[a-z]</code> は、<code>a</code> から <code>z</code> までのすべての小文字に一致し、<code>[a-zA-Z]</code> は、<code>A</code> から <code>Z</code> までのすべての大文字と小文字に一致します。<code>[xyz]</code> は、<code>x</code>、<code>y</code> または <code>z</code> の文字のみに一致します。</p>
バックスラッシュ特殊文字 (\)	<p>バックスラッシュは特殊文字をエスケープします。したがって、<code>\.</code> と続けると、ピリオドそのもののみ一致し、<code>\\$</code> はドル記号のみに一致し、<code>\^</code> はキャレット記号のみに一致します。</p> <p>バックスラッシュ文字は、<code>\d</code> などトークンの始まりともなります。</p> <p>重要な注意事項：バックスラッシュは、パーサーに対しても特殊なエスケープ文字となります。結果として、正規表現にバックスラッシュを含める場合には、2 つのバックスラッシュを使います。そうするとパーズングの後、「本物」のバックスラッシュが 1 つだけ残り、正規表現のシステムに渡されます。</p>

表 11-2 分類子での正規表現（続き）

<code>\d</code>	<p>数字（0～9）に一致するトークン。複数の数字に一致させるには、整数を <code>{}</code> に入れ数の長さを規定します。</p> <p>たとえば、<code>\d</code> は、5 などの 1 桁の数字のみに一致しますが、55 には一致しません。<code>\d{2}</code> を使うと、55 などの 2 桁の数に一致しますが、5 には一致しません。</p>
繰り返しの回数 { 最小、最大 }	<p>1 つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。</p> <p>たとえば、<code>\d{8}</code> という表現は、12345678 および 11223344 には一致しますが、8 には一致しません。</p>
論理和 ()	<p>代替、つまり「or」演算子 A と B を正規表現とすると、<code>A B</code> という表現は「A」と「B」のいずれかに一致するすべての文字列に一致します。1 つの正規表現で数パターンを組み合わせるために使用できます。</p> <p>たとえば、<code>foo bar</code> という表現は foo または bar のどちらかに一致しますが、foobar には一致しません。</p>

DLP 用の正規表現の例

コンテンツ照合分類子で正規表現を使用する主なケースは、特定の口座、患者や生徒の識別番号を定義することです。これらは、数や文字のパターンを記述する通常の単純な正規表現です。次の例を参考にしてください。

- 8 桁の数：`\d{8}`
- 数字のセットの間にハイフンがある識別コード：`\d{3}-\d{4}-\d`
- 大文字または小文字の英字 1 つで始まる識別コード：`[a-zA-Z]\d{7}`
- 3 桁の数字で始まり、大文字が 9 つ続く識別コード：`\d{3}[A-Z]{9}`
- | を使い、検索する 2 つの異なる数字パターンを定義：
`\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`



(注)

正規表現では大文字と小文字は区別されるため、[a-zA-Z] のように大文字と小文字を含める必要があります。特定の文字のみ使用する場合は、その文字に合わせて正規表現を定義します。

8 桁の数字など、あまり特殊ではないパターンほど、ランダムな 8 桁の数字を実際の顧客番号と区別するため、追加の単語とフレーズを検索するポリシーが必要になります。

高度な DLP ポリシーのカスタマイズ

使用可能な RSA ポリシー テンプレートでは組織の独自の要件に適合しない場合、ゼロから独自の DLP ポリシーを作成するためのオプションがいくつかあります。オプションには次のものがあります。

- Custom Policy テンプレートを使って独自の DLP ポリシーを作成
- カスタム ポリシーで使用する独自の分類子を作成
- カスタム ポリシーで使用する独自の DLP デictionary を作成しインポート



(注)

これらのオプションは高度であり、事前定義された設定が組織のニーズに適合しない場合にのみ使用されることを想定しています。

Custom Policy テンプレートを使用した DLP ポリシーの作成

Custom Policy テンプレートを使用して、カスタム DLP ポリシーを作成できます。事前定義された RSA 分類子をポリシーで使用することも、カスタム分類子を追加することもできます。分類子の作成の手順については、「[コンテンツ照合分類子の作成](#)」(P.11-33) を参照してください。

ポリシーの定義によって、コンテンツが 1 つの分類子またはすべての分類子に一致した場合に、カスタム ポリシーは DLP 違反を返すことができます。false positive 防止のため、DLP ポリシーには、メッセージの内容と一致する場合、違

反とは見なさなくなる分類子を含めることができます。分類子の [NOT] チェックボックスをオンにすると、その分類子に一致する内容を含むメッセージは、DLP 違反として報告されません。

カスタム ポリシーを追加するには、次の手順に従ってください。

-
- ステップ 1** [Mail Policies] > [DLP Policy Manager] を選択します。
 - ステップ 2** [Add DLP Policy] をクリックします。
 - ステップ 3** Custom Policy カテゴリの名前をクリックします。
 - ステップ 4** Custom Policy テンプレートの [Add] をクリックします。
 - ステップ 5** ポリシーの名前と説明を入力します。
 - ステップ 6** ポリシー用に分類子を選択します。既存の分類子の使用または [Create a Classifier] オプションの選択が可能です。
 - ステップ 7** [Add] をクリックします。

[Create a Classifier] を選択すると、[Add Content Matching Classifier] ページが開きます。それ以外の場合は、事前定義された分類子がポリシーに追加されます。
 - ステップ 8** 複数の分類子をポリシーに追加する場合は、ステップ 6 ~ 7 を繰り返します。
 - ステップ 9** 任意で、特定の受信者または送信者を持つメッセージにのみ DLP ポリシーを適用するよう限定できます。改行やカンマで、複数のエントリを分離できます。詳細については、「[送信者および受信者のフィルタリング](#)」(P.11-14) を参照してください。
 - ステップ 10** 任意で、DLP ポリシーを特定の添付タイプを持つメッセージにのみに適用するよう限定できます。詳細については、「[添付ファイルのフィルタリング](#)」(P.11-15) を参照してください。
 - ステップ 11** [Critical Violations Settings] セクションで、重大な DLP 違反を含むメッセージをドロップ、配信、または検疫するか選択できます。
 - ステップ 12** 任意で、メッセージの暗号化、ヘッダーの修正、代替ホストへのメッセージの送信、別の受信者へのコピーの配信 (bcc)、DLP 通知メッセージの送信を選択できます。

DLP の通知については、「[テキストリソース](#)」(P.14-1) を参照してください。

- ステップ 13** 一致する重大度レベルが High、Medium、Low のメッセージに、別々の設定を定義するときは、適切なセキュリティ レベルの [Inherit settings] チェックボックスをオフにします。メッセージへの全体的なアクションや他の設定を編集します。
- ステップ 14** ポリシーの DLP 違反の重大度基準を調整する場合は、[Edit Scale] をクリックして、設定を調整します。詳細については、「[重大度レベルの設定](#)」(P.11-15) を参照してください。
- ステップ 15** 変更を送信して確定します。
- ポリシーが DLP Policy Manager に追加されます。

コンテンツ照合分類子の作成

カスタム ポリシー作成時は、[Create a Classifier] オプションを選択すると、カスタム分類子を作成できます。分類子の作成に必要なルールと値の詳細については、「[分類子検出ルール](#)」(P.11-24) を参照してください。

分類子を作成して送信すると、カスタム ポリシー作成時に使用可能な分類子の一覧に表示されます。

分類子を作成するには、次の手順に従います。

-
- ステップ 1** 分類子の名前と説明を入力します。
- ステップ 2** 近接性照合としてカウントするために、分類子のルールを検出する文字数を入力します。
- ステップ 3** 分類子の最小総合スコアを入力します。
- ステップ 4** 重みや最大スコアなど分類子のルールを定義します。
- ステップ 5** [Add Rule] をクリックし、ルールを分類子に追加します。複数のルールを追加できます。
- ステップ 6** 分類子を送信し、カスタム ポリシーの作成を続けることができます。

RSA Email DLP の受信者ごとのポリシーの設定

電子メールセキュリティマネージャの機能を使って受信者ごとの RSA Email DLP ポリシーをイネーブルにすることができます。[Mail Policies] > [Outgoing Mail Policies (GUI)] ページまたは、`policyconfig` コマンド (CLI) を使います。異なる発信メールポリシーに対して別々の DLP ポリシーをイネーブルにすることができます。発信メールポリシー内で DLP ポリシーだけを使用することができます。図 11-10 を参照してください。

電子メールの「ワークキュー」の感染フィルタの段階後に、DLP スキャンが行われます。詳細については、『Cisco IronPort AsyncOS for Email Configuration Guide』の「Email Security Manager」の章を参照してください。

図 11-10 イネーブルになっている DLP ポリシーを伴うデフォルトの発信メールポリシー

Outgoing Mail Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	DLP	Delete
	Default Policy	Disabled	Sophos Encrypted: Deliver Uncannable: Deliver Virus Positive: Drop	Disabled	Disabled	Enabled Suspicious Transmiss... Encrypted and Passwo... GLBA (Gramm-Leach Bliley Act) Suspicious Transmiss...	

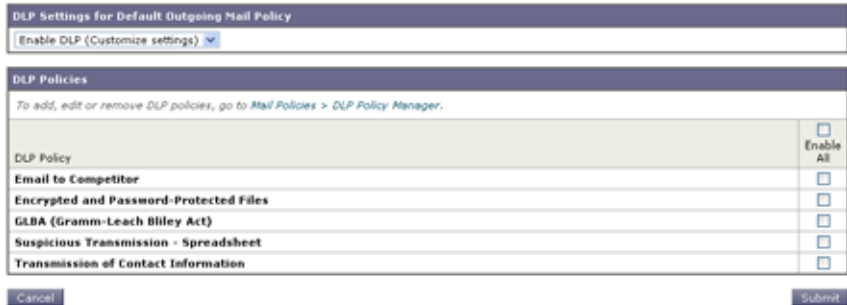
Key: Default Custom Disabled

メールポリシーの DLP 設定の編集

発信メールポリシーに対するユーザごとの DLP 設定を編集するプロセスは、基本的にデフォルトのポリシーと個々のポリシーに対するものと同じです。個々のポリシー（デフォルトでない）には、DLP 設定を [Enable DLP (Inherit default mail policy settings)] にするという追加のオプションがあります。これを選択すると、ポリシーはデフォルトの発信メールポリシーの DLP 設定をすべて採用します。

図 11-11 に、デフォルトの発信メールポリシーでイネーブルな DLP ポリシーの一覧を示します。

図 11-11 デフォルトの発信メール ポリシーで DLP ポリシーをイネーブルにする
Mail Policies: DLP



発信メール ポリシー（デフォルトを含む）に DLP 設定を編集するには、次の手順に従ってください。

- ステップ 1** 電子メール セキュリティ マネージャの発信メール ポリシー テーブルの任意の行にある DLP セキュリティ サービスのリンクをクリックします。
DLP 設定のページが表示されます。
- ステップ 2** デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。
- ステップ 3** メール ポリシーの [Enable DLP (Customize Settings)] を選択します。
DLP Policy Manager で定義されているポリシーの一覧が表示されます。
- ステップ 4** 発信メール ポリシーで使用する RSA Email DLP ポリシーを選択します。
- ステップ 5** 変更を送信して確定します。



CHAPTER 12

Cisco IronPort 電子メール暗号化

Cisco IronPort AsyncOS は、インバウンドおよびアウトバウンド電子メールをセキュアにする暗号化の使用をサポートします。

この章は、次の内容で構成されています。

- 「[Cisco IronPort 電子メール暗号化：概要](#)」 (P.12-1)
- 「[電子メール暗号化プロファイルの設定](#)」 (P.12-4)
- 「[暗号化コンテンツ フィルタの設定](#)」 (P.12-11)
- 「[メッセージへの暗号化ヘッダーの追加](#)」 (P.12-16)

Cisco IronPort 電子メール暗号化：概要

この機能を使用するには、暗号化されたメッセージの特性およびキー（鍵）サーバの接続性の情報を指定する暗号化プロファイルを作成します。キー サーバは、Cisco Registered Envelope Service（マネージド サービス）または Cisco IronPort 暗号化アプライアンス（ローカルのマネージド サーバ）のいずれかになります。次に、メッセージを暗号化するか決めるコンテンツ フィルタまたはメッセージ フィルタ（または両方）を作成します。

フィルタ条件に合致する発信メッセージは、電子メール セキュリティ アプライアンスの暗号化処理のキューに入れられます。メッセージが暗号化されると、暗号化に使われたキーが暗号化プロファイルで指定されたキー サーバに保存され、暗号化されたメッセージが配信のキューに入れられます。キューの中の電子メールの暗号化を妨げるような条件（つまり、一時的な C-Series のビジイー状態や CRES が使用できない状態）が一時的に存在すると、メッセージはキューに入れられ、しばらくしてから再度暗号化が試行されます。



(注) また、メッセージを暗号化する前に、まず TLS 接続経由で送信を試みるようにアプライアンスを設定することもできます。詳細については、「[TLS 接続を暗号化の代わりに使用](#)」(P.12-11) を参照してください。

電子メールセキュリティアプライアンスでアウトバウンド電子メールの暗号化を設定するには、次の手順を実行します。

- ステップ 1** ローカル キー サーバを使用する場合は、**Cisco IronPort 暗号化アプライアンス**を設定します。キー サーバを構成する手順については、『*IronPort Encryption Appliance Local Key Server User Guide*』を参照してください。
- ステップ 2** 暗号化プロファイルを設定します。暗号化プロファイルを設定する手順については、「[電子メール暗号化プロファイルの設定](#)」(P.12-4) を参照してください。
- ステップ 3** ホステッド キー サービスを使用するには、**Cisco Registered Envelope Service** コーポレート アカウントを作成します。暗号化プロファイルを設定した後、**[Provision]** ボタンをクリックしてアカウントを作成します。
- ステップ 4** 発信コンテンツ フィルタを設定します。暗号化しなければならないアウトバウンド電子メールにタグをつけるように、コンテンツ フィルタを設定する必要があります。コンテンツ フィルタの作成手順については、「[暗号化コンテンツ フィルタの設定](#)」(P.12-11) を参照してください。

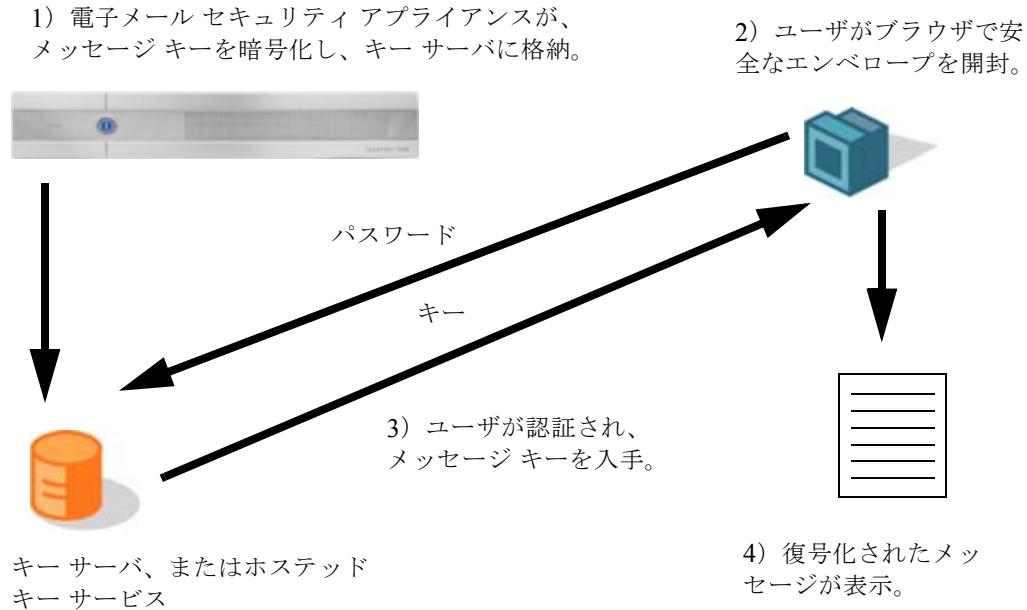
次の Web ブラウザがサポートされます。

- Microsoft® Internet Explorer 7 (Windows XP および Vista)
- Microsoft® Internet Explorer 8 (Windows XP および Vista)
- Firefox 3.0 および 3.5
- Safari 4.0 (Mac OS X)

暗号化ワークフロー

電子メール暗号化を使用する場合、Cisco IronPort 電子メールセキュリティアプライアンスはメッセージを暗号化し、ローカル キー サーバまたはホステッド キー サービスにメッセージ キーを格納します。受信者が暗号化されたメッセージを開封すると、キー サービスによって受信者が認証され、復号化されたメッセージが表示されます。

図 12-1 暗号化ワークフロー



暗号化されたメッセージを開封する基本的なワークフローは次のとおりです。

- ステップ 1** 暗号化プロファイルを設定するときは、メッセージ暗号化のパラメータを指定します。暗号化されたメッセージでは、メッセージ キーが電子メール セキュリティ アプライアンスによりローカル キー サーバ、またはホステッド キー サービス (Cisco Registered Envelope Service) に作成および格納されます。
- ステップ 2** 受信者はブラウザで安全なエンベロープを開封します。
- ステップ 3** ブラウザで暗号化されたメッセージを開封するとき、受信者の本人確認のためパスワードが必要となります。キー サーバはメッセージに関連付けられた暗号化キーを返します。



(注) 暗号化された電子メール メッセージの初回開封時に、受信者は安全なエンベロープを開封するためのキー サービスに登録する必要があります。登録後、暗号化プロファイルの設定によっては、受信者が暗号化されたメッセージを認証なしで開封することも可能です。暗号化プロファイルでは、パスワード不要と指定できますが、特定の機能が使用できなくなります。

ステップ 4 復号化したメッセージが表示されます。

電子メール暗号化プロファイルの設定

電子メールセキュリティアプライアンスによる暗号化を使用するには、暗号化プロファイルを設定する必要があります。encryptionconfig CLI コマンド、または GUI の [Security Services] > [IronPort Email Encryption] で、暗号化プロファイルをイネーブルにして設定することができます。

電子メール暗号化グローバル設定の編集

電子メール暗号化をイネーブルにするには、次の手順を実行します。

-
- ステップ 1** [Security Services] > [IronPort Email Encryption] をクリックします。
 - ステップ 2** [Enable] をクリックします。
 - ステップ 3** 任意で、[Edit Settings] をクリックし、プロキシサーバを設定します。

図 12-2 グローバル設定の構成

暗号化プロファイルの追加

ローカル キー サービスを使う場合、1 つ以上の暗号化プロファイルを作成できます。さまざまな電子メール グループに異なるセキュリティ レベルを使用する場合、それぞれ別の暗号化プロファイルを作成することもできます。たとえば、機密資料を含んだメッセージを高レベルのセキュリティで送信し、他のメッセージを中レベルのセキュリティで送信するという場合です。この場合、特定のキーワード（「confidential」など）を含むメッセージには高レベルのセキュリティ暗号化プロファイルを作成し、他の発信メッセージには別の暗号化プロファイルを作成します。

暗号化プロファイルをカスタム ユーザ ロールに割り当て、そのロールに割り当てられた委任管理者が DLP ポリシーとコンテンツ フィルタで暗号化プロファイルを使用できるようにします。DLP ポリシーとコンテンツ フィルタを設定する場合は、管理者、オペレータ、および委任ユーザだけが暗号化プロファイルを使用できます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。詳細については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」の章を参照してください。



(注)

1 つのホステッド キー サービスに複数の暗号化プロファイルを設定できます。組織に複数のブランドがある場合、PXE エンベロープ用にキー サーバに格納された異なるロゴを参照することができます。

暗号化プロファイルを作成および保存し、次の暗号化の設定を保存します。

- [Key server settings]。キー サーバとそのキー サーバに接続するための情報を指定します。
- [Envelope settings]。セキュリティ レベル、開封確認を返すか、暗号化キューにあるメッセージがタイムアウトするまでの時間、使用する暗号化アルゴリズムのタイプ、および復号化アプレットをブラウザで動作可能にするかなど、メッセージ エンベロープの詳細を指定します。
- [Message settings]。安全なメッセージ転送や安全な「全員に返信」をイネーブルにするかなど、メッセージに関する詳細を指定します。
- [Notification settings]。暗号化失敗通知と同様、テキスト形式および HTML 形式の通知を使う通知テンプレートを指定します。暗号化プロファイル作成時に、テキスト リソース内のテンプレートを作成し、テンプレートを選択します。暗号化失敗通知のメッセージの件名も指定できます。通知の詳細については、「暗号化通知テンプレート」(P.14-47) および「バウンス通知および暗号化失敗通知テンプレート」(P.14-42) を参照してください。

図 12-3 暗号化エンベロープ プロファイルの追加
Add Encryption Envelope Profile

Encryption Profile Settings	
Profile Name:	<input type="text"/>
Used by (Roles):	No roles selected
Key Server Settings	
Key Service Type:	Cisco Registered Envelope Service
Proxy:	A proxy server is not currently configured.
Cisco Registered Envelope Service URL:	https://res.cisco.com
> Advanced	Advanced key server settings
Envelope Settings	
Envelope Message Security:	<input checked="" type="radio"/> High Security <i>Recipient must enter a password to open the encrypted message, even if credentials are cached ("Remember Me" selected).</i> <input type="radio"/> Medium Security <i>No password entry required if recipient credentials are cached ("Remember Me" selected).</i> <input type="radio"/> No Password Required <i>The recipient does not need a password to open the encrypted message.</i>
Logo Link:	<input checked="" type="radio"/> No link <input type="radio"/> Custom link URL: <input type="text"/> <i>By defining a URL, the logo in the upper left corner of the recipient envelope will become a link (e.g. http://www.mycompany.com/).</i>
Read Receipts:	<input checked="" type="checkbox"/> Enable Read Receipts
> Advanced	Encryption Queue Timeout: <input type="text" value="14400"/> seconds Encryption Algorithm: <input checked="" type="radio"/> ARC4 (typical) <input type="radio"/> AES Message Attachment Decryption: <input checked="" type="checkbox"/> Use Decryption Applet <i>Disabling this setting will cause message attachments to be decrypted at the key server. They will take longer to open, but they don't require a Java plug-in.</i>
Message Settings	
End-User Controls:	<input type="checkbox"/> Enable Secure Reply All <input type="checkbox"/> Enable Secure Message Forwarding
Message Settings	
End-User Controls:	<input type="checkbox"/> Enable Secure Reply All <input type="checkbox"/> Enable Secure Message Forwarding
Notification Settings	
Encrypted Message HTML Notification:	System Generated Preview Message <small>(see Mail Policies > Text Resources > Encryption Notification Template - HTML)</small>
Encrypted Message Text Notification:	System Generated Preview Message <small>(see Mail Policies > Text Resources > Encryption Notification Template - Text)</small>
Encryption Failure Notification:	Message Subject: <input type="text" value="[ENCRYPTION FAILURE]"/> Message Body: System Generated Preview Message <small>(see Mail Policies > Text Resources > DSN Bounce and Encryption Failure Notification Template)</small>
File name of the envelope attached to the encryption notification:	<input type="text" value="securedoc_\$(date)T\$(time).html"/>
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

暗号化プロファイルを追加するには次の手順に従ってください。

- ステップ 1** [Email Encryption Profiles] のセクションで [Add Encryption Profile] をクリックします。
- ステップ 2** 暗号化プロファイルの名前を入力します。
- ステップ 3** [Used By (Roles)] リンクをクリックし、暗号化プロファイルへのアクセス権を設定するカスタム ユーザ ロールを選択して、[OK] をクリックします。
- このカスタム ロールに割り当てられた委任管理者は、責任があるすべての DLP ポリシーとコンテンツ フィルタに対して暗号化プロファイルを使用できます。
- ステップ 4** [Key Server Settings] セクションで次のキー サーバから選択します。
- Cisco IronPort Encryption appliance (in network)
 - Cisco Registered Envelope Service (hosted key service)
- ステップ 5** [Cisco Registered Envelope Service] を選択した場合は、ホステッド キー サービスの URL を入力します。キー サービスの URL は、<https://res.cisco.com> です。
- ステップ 6** Cisco IronPort 暗号化アプライアンス（ローカル キー サービス）を選択した場合は、次の設定を入力します。
- [Internal URL]。Cisco IronPort 電子メール セキュリティ アプライアンスは、この URL を使用してネットワーク内の Cisco IronPort 暗号化アプライアンスと通信します。
 - [External URL]。受信者のメッセージは、この URL を使用して Cisco IronPort 暗号化アプライアンスのキーおよび他のサービスにアクセスします。受信者は、この URL でインバウンド HTTPS 要求を行います。
- ステップ 7** [Envelope Settings] のセクションで、メッセージのセキュリティ レベルを選択します。
- [High Security]。受信者は、暗号化されたメッセージを開封するには、パスワードを必ず入力する必要があります。
 - [Medium Security]。受信者の資格情報がキャッシュされていれば、受信者は暗号化されたメッセージを開封するために資格情報を入力する必要はありません。
 - [No Password Required]。暗号化されたメッセージの最も低いセキュリティ レベルです。受信者は、暗号化されたメッセージを開封するためにパスワードを入力する必要はありませんが、開封確認、安全な返信、安全な「全員に返信」、安全なメッセージ転送の機能は使用できず、別の電子メールのユーザが最初の受信者の代理でメッセージを送信することを防止できません。

- ステップ 8** ユーザが組織のロゴをクリックするとその組織の URL が開くようにするよう
に、ロゴのリンクを追加できます。次のオプションから選択します。
- [No link]。実際のリンクは、メッセージ エンベロープに追加されません。
 - [Custom link URL]。URL を入力し、メッセージ エンベロープへの実際のリンクを追加します。
- ステップ 9** 任意で、開封確認をイネーブルにします。このオプションをイネーブルにすると、受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。
- ステップ 10** 任意で、[Advanced] をクリックして次の設定を行います。
- 暗号化キューにあるメッセージがタイムアウトするまでの時間（秒単位）を入力します。メッセージがタイムアウトになると、アプライアンスはメッセージをバウンスし、送信者に通知を送信します。
 - 暗号化アルゴリズムを選択します。
 - [ARC4]。ARC4 は最もよく選択されるアルゴリズムで、メッセージ受信者に対する復号化遅延を最小限にとどめながら強力な暗号化を実現します。
 - [AES]。AES は、より強力な暗号化を実現しますが、復号化により長い時間がかかるため、受信者には遅延が発生します。AES は、通常、政府や銀行業務のアプリケーションで使用されます。
 - 復号化アプレットをイネーブルまたはディセーブルにします。このオプションをイネーブルにすると、メッセージの添付ファイルがブラウザ環境で開かれるようになります。このオプションをディセーブルにすると、メッセージの添付ファイルがキーサーバで復号化されるようになります。ディセーブルの場合、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。
- ステップ 11** [Message Settings] セクションで、[Secure Reply All] をイネーブルまたはディセーブルにします。
- ステップ 12** [Secure Message Forwarding] をイネーブルまたはディセーブルにします。
- ステップ 13** HTML 形式の通知テンプレートを選択します。テキストリソースで設定した HTML 形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。



(注) キーサーバは、受信者の電子メールアプリケーションによって、HTML またはテキスト形式の通知を使います。両方の通知を設定する必要があります。

- ステップ 14** テキスト形式の通知テンプレートを選択します。テキスト リソースで設定したテキスト形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。
- ステップ 15** 暗号化失敗通知用の件名ヘッダーを入力します。暗号化プロセスがタイムアウトした場合、アプライアンスは通知を送信します。
- ステップ 16** メッセージ本文の暗号化失敗通知テンプレートを選択します。テキスト リソースで設定した暗号化失敗通知テンプレートから選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。
- ステップ 17** 変更を送信して確定します。
- ステップ 18** Cisco Registered Envelope Service を使用する場合、アプライアンスをプロビジョニングする手順を追加で実行する必要があります。アプライアンスをプロビジョニングすると、暗号化プロファイルがホステッドキー サービスとともに登録されます。アプライアンスをプロビジョニングするには、登録する暗号化プロファイルの [Provision] ボタンをクリックします。

PXE エンジンの更新

[IronPort Email Encryption Settings] ページでは、PXE エンジンの現行バージョンとアプライアンスが使用するドメイン マッピング ファイルを表示します。AsyncOS の以前のバージョンでは、PXE エンジンを更新するには AsyncOS を更新する必要がありました。この時点で、[Security Services] > [Service Updates] ページ (または CLI の `updateconfig` コマンド) を使って、自動的に PXE エンジンを更新するように Cisco IronPort アプライアンスを設定できます。詳細については、「サービスのアップデート」(P.15-16) を参照してください。

また、[IronPort Email Encryption Settings] ページの [PXE Engine Updates] セクションの [Update Now] ボタン (または CLI の `encryptionupdate` コマンド) を使って、手動でエンジンを更新することもできます。

図 12-4 [IronPort Email Encryption Settings] ページの [PXE Engine Updates]

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	Never updated	6.7.0
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

暗号化コンテンツ フィルタの設定

暗号化プロファイルの作成後、どの電子メール メッセージを暗号化すべきかを定める発信コンテンツ フィルタを作成する必要があります。コンテンツ フィルタは、発信電子メールをスキャンしてメッセージが指定された条件に一致するか判断します。コンテンツ フィルタによりメッセージが条件に一致すると判断されたら、Cisco IronPort 電子メール セキュリティ アプライアンスはメッセージを暗号化し、生成されたキーをキー サーバに送信します。このアプライアンスは、使用するキー サーバを決定するための、暗号化プロファイルで指定された設定と、他の暗号化設定を使用します。

TLS 接続を暗号化の代わりに使用

ドメイン用に指定された宛先制御に基づき、Cisco IronPort アプライアンスは、メッセージを暗号化する代わりに TLS 接続を介してメッセージをセキュアに中継できます (TLS 接続が使用可能な場合)。アプライアンスは、宛先制御 (Required、Preferred、または None) の TLS 設定と暗号化コンテンツ フィルタで定義されたアクションに基づいて、メッセージを暗号化するか TLS 接続で送信するか決定します。

コンテンツ フィルタ作成時に、必ずメッセージを暗号化するか、まず TLS 接続で送信を試みて、TLS 接続が使用不可であればメッセージを暗号化するかを指定できます。表 12-1 では、暗号化制御フィルタが TLS 接続でのメッセージの送信を試みる場合、電子メール セキュリティ アプライアンスが、ドメインの宛先制御の TLS 設定に基づいてどのようにメッセージを送信するかを示しています。

表 12-1 ESA アプライアンスの TLS サポート

宛先制御 TLS 設定	TLS 接続が使用可能である場合のアクション	TLS 接続が使用不可である場合のアクション
None	エンベロープを暗号化して送信します。	エンベロープを暗号化して送信します。
TLS Preferred	TLS を通して送信します。	エンベロープを暗号化して送信します。
TLS Required	TLS を通して送信します。	リトライまたはメッセージのバウンス

宛先制御での TLS のイネーブル化の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

Encrypt and Deliver Now コンテンツ フィルタの作成

メッセージを暗号化して即時に配信し、それ以降のプロセスをスキップするコンテンツ フィルタを作成するには、次の手順に従います。

- ステップ 1 [Mail Policies] > [Outgoing Content Filters] に移動します。
- ステップ 2 [Filters] セクションで、[Add Filter] をクリックします。
- ステップ 3 [Conditions] セクションで、[Add Condition] をクリックします。
- ステップ 4 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。
- ステップ 5 [OK] をクリックします。

条件の作成の詳細については、「[コンテンツ フィルタの概要](#)」(P.6-10) を参照してください。

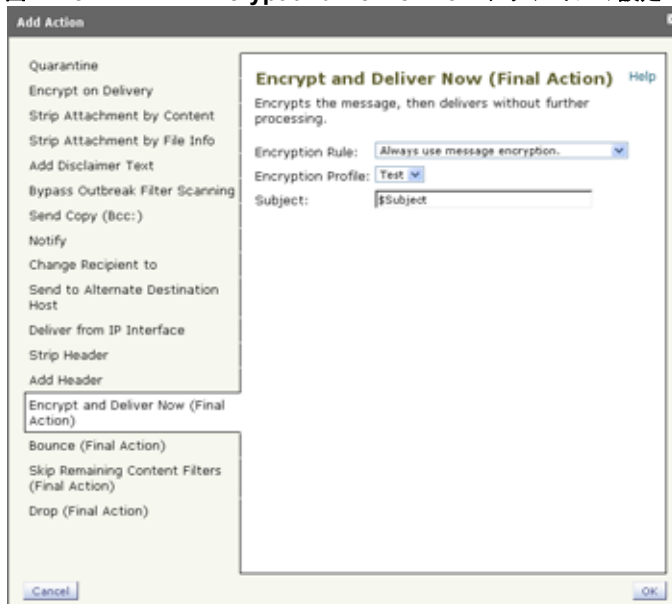
ステップ 6 任意で、[Add Action] をクリックし、[Add Header] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

暗号化ヘッダーの詳細については、「メッセージへの暗号化ヘッダーの追加」(P.12-16) を参照してください。

ステップ 7 [Actions] セクションで、[Add Action] をクリックします。

ステップ 8 [Encrypt and Deliver Now (Final Action)] を選択します。

図 12-5 Encrypt and Deliver Now アクションの設定



ステップ 9 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。

ステップ 10 コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。

暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

ステップ 11 メッセージの件名を入力します。

ステップ 12 [OK] をクリックします。

図 12-6 のコンテンツ フィルタは、メッセージ本文で ABA コンテンツを検索するコンテンツ フィルタを示します。コンテンツ フィルタで定義されているアクションは、電子メールを暗号化して配信すると指定しています。

図 12-6 暗号化コンテンツ フィルタ

Content Filter Settings

Name: sensitive_content

Currently Used by Policies: No policies currently use this rule.

Description: encrypt messages that contain sensitive material

Order: 2 (of 2)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	Message Body	only-body-contains("**aba", 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	Encrypt and Deliver (Final Action)	encrypt ("encrypt_sensitive", "\$Subject")	

Cancel Submit

ステップ 13 暗号化アクションを追加した後、[Submit] をクリックします。

ステップ 14 変更を確定します。

ステップ 15 コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、「[ユーザベース ポリシーの概要](#)」(P.6-2) を参照してください。

Encrypt on Delivery コンテンツ フィルタの作成

配信時にメッセージを暗号化するコンテンツ フィルタを作成するには、次の手順に従ってください。配信時の暗号化とは、メッセージが次の処理の段階に進み、すべての処理が完了した時点で、メッセージが暗号化され、配信されることを意味します。

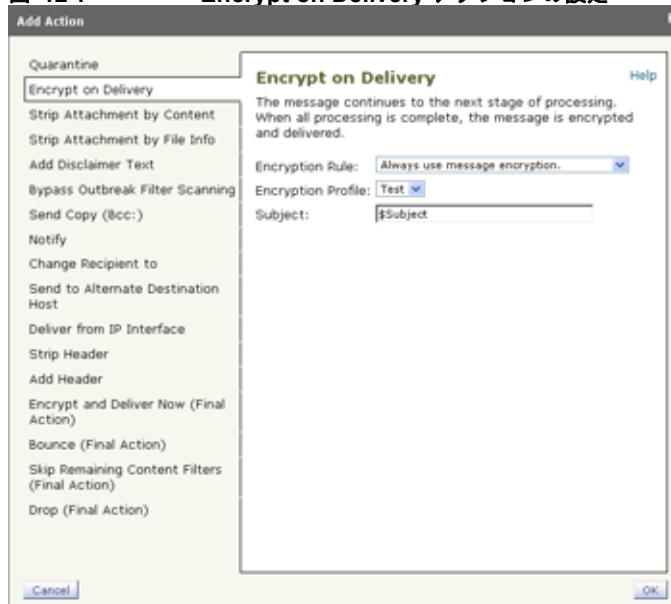
ステップ 1 [Mail Policies] > [Outgoing Content Filters] に移動します。

ステップ 2 [Filters] セクションで、[Add Filter] をクリックします。

ステップ 3 [Conditions] セクションで、[Add Condition] をクリックします。

- ステップ 4** 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。
- ステップ 5** [OK] をクリックします。
- 条件の作成の詳細については、「コンテンツ フィルタの概要」(P.6-10) を参照してください。
- ステップ 6** 任意で、[Add Action] をクリックし、[Add Header] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。
- 暗号化ヘッダーの詳細については、「メッセージへの暗号化ヘッダーの追加」(P.12-16) を参照してください。
- ステップ 7** [Actions] セクションで、[Add Action] をクリックします。
- ステップ 8** [Encrypt on Delivery] を選択します。

図 12-7 Encrypt on Delivery アクションの設定



- ステップ 9** 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。
- ステップ 10** コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。

暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

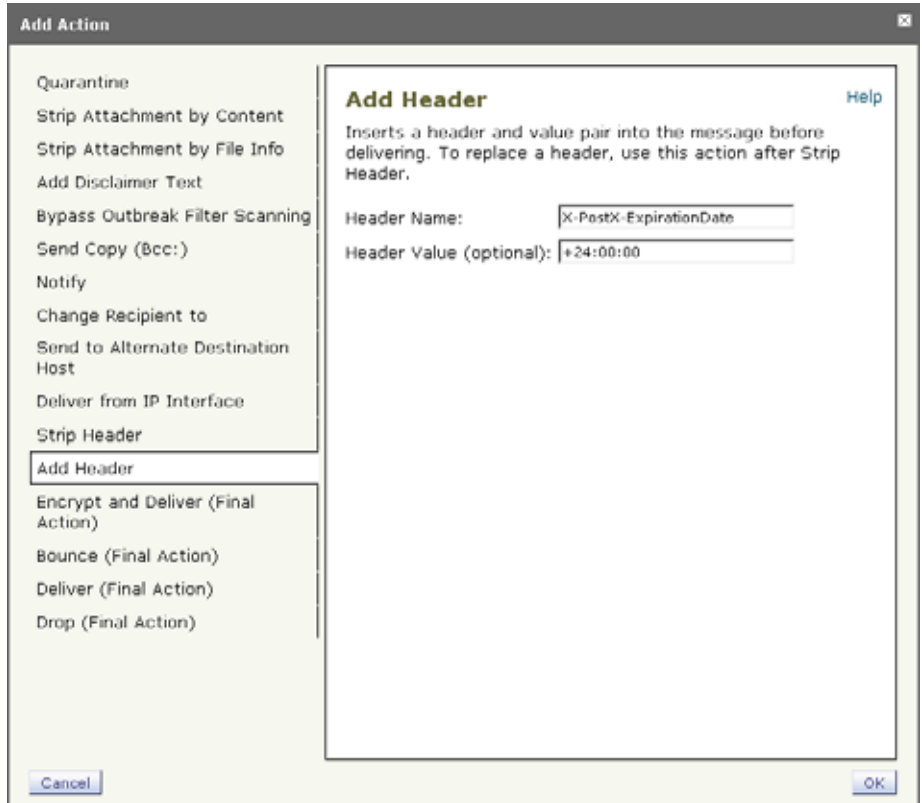
- ステップ 11** メッセージの件名を入力します。
- ステップ 12** [OK] をクリックします。
- ステップ 13** 暗号化アクションを追加した後、[Submit] をクリックします。
- ステップ 14** 変更を確定します。
- ステップ 15** コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、「[ユーザベース ポリシーの概要](#)」(P.6-2) を参照してください。

メッセージへの暗号化ヘッダーの追加

AsyncOS では、コンテンツ フィルタまたはメッセージ フィルタを使って SMTP ヘッダーをメッセージに挿入することで、暗号化設定をメッセージに追加できます。暗号化ヘッダーは、関連付けられた暗号化プロファイルで定義されている暗号化設定を上書きすることが可能で、指定された暗号化機能をメッセージに適用できます。

コンテンツ フィルタを使って暗号化ヘッダーをメッセージに追加するには、**Add Header** フィルタ アクションをコンテンツ フィルタに追加し、暗号化ヘッダーとその値を入力します。たとえば、**Registered Envelope** を送信後 24 時間で期限切れにする場合は、ヘッダー名として X-PostX-ExpirationDate、ヘッダーの値として +24:00:00 を入力します。

図 12-8 Add Header アクションの設定



暗号化コンテンツ フィルタの作成の詳細については、「[Encrypt and Deliver Now コンテンツ フィルタの作成](#)」(P.12-12) を参照してください。メッセージ フィルタを使ったヘッダーの挿入については、『*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。

暗号化ヘッダー

表 12-2 に、メッセージに追加可能な暗号化ヘッダーを示します。

表 12-2 電子メール暗号化ヘッダー

MIME ヘッダー	説明	値
X-PostX-Reply-Enabled	メッセージで安全な返信をイネーブルにするかを示し、メッセージバーに [Reply] ボタンを表示します。このヘッダーは、メッセージに暗号化設定を追加します。	[Reply] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。
X-PostX-Reply-All-Enabled	メッセージで安全な「全員に返信」をイネーブルにするかを示し、メッセージバーに [Reply All] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[Reply All] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。
X-PostX-Forward-Enabled	メッセージの安全な転送をイネーブルにするかを示し、メッセージバーに [Forward] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[Forward] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。
X-PostX-Send-Return-Receipt	開封確認をイネーブルにするかを示します。受信者が安全なエンベロップを開くと、送信者は開封確認を受信します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	開封確認を送信するかを示すブール値。true に設定するとボタンを表示します。デフォルト値は false です。

表 12-2 電子メール暗号化ヘッダー (続き)

MIME ヘッダー	説明	値
X-PostX-ExpirationDate	<p>送信前に Registered Envelope の有効期限の日付けを設定します。有効期限後は、キー サーバにより Registered Envelope へのアクセスが制限されます。Registered Envelope は、メッセージの期限が切れたというメッセージを表示します。このヘッダーは、メッセージに暗号化設定を追加します。</p> <p>Cisco Registered Envelope Service を使用している場合、メッセージ送信後に http://res.cisco.com の Web サイトにログインして、メッセージ管理機能でメッセージの有効期限を設定、調整、削除できます。</p>	<p>相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。</p>
X-PostX-ReadNotificationDate	<p>送信前に Registered Envelope の「開封期限」の日付を設定します。Registered Envelope がこの期限までに読まれなかった場合、ローカル キー サーバは通知を生成します。このヘッダーを持つ Registered Envelope は、Cisco Registered Envelope Service では機能せず、ローカル キー サーバでのみ機能します。このヘッダーは、メッセージに暗号化設定を追加します。</p>	<p>相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。</p>
X-PostX-Suppress-Apple-For-Open	<p>復号化アプレットをディセーブルにするかを示します。復号化アプレットにより、ブラウザ環境でメッセージの添付ファイルが開かれます。アプレットをディセーブルにすると、メッセージの添付ファイルはキー サーバで復号化されます。このオプションをディセーブルにすると、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存なくなります。このヘッダーは、デフォルトのプロファイル設定を上書きします。</p>	<p>復号化アプレットをディセーブルにするかを示すブール値。アプレットをディセーブルにするには true に設定します。デフォルト値は false です。</p>

表 12-2 電子メール暗号化ヘッダー (続き)

MIME ヘッダー	説明	値
X-PostX-Use-Script	JavaScript を含まないエンベロープを送信するかしないかを示します。JavaScript を含まないエンベロープとは、受信者のコンピュータ上でエンベロープをローカルに開封するために使われる JavaScript を含まない Registered Envelope のことです。受信者は、メッセージを見るには Open Online メソッド、または Open by Forwarding メソッドのいずれかを使用する必要があります。受信者のドメインのゲートウェイにより JavaScript が削除され、暗号化されたメッセージを開封できない場合、このヘッダーを使います。このヘッダーはメッセージに暗号化設定を追加します。	JavaScript アプレットを含めるか含めないかのブール値。JavaScript を含まないエンベロープを送信するには、false に設定します。デフォルト値は true です。
X-PostX-Remember-Envelope-Key-Checkbox	オフラインでエンベロープを開封するため、エンベロープ固有のキーのキャッシュを許可するかしないかを示します。エンベロープキーのキャッシングでは、受信者が正しいパスワードを入力し、[Remember the password for this envelope] チェックボックスをオンにした場合、個別のエンベロープの復号化キーが受信者のコンピュータでキャッシュされます。これ以降、受信者はそのコンピュータでエンベロープを再開封するためにパスワードをもう一度入力する必要はありません。このヘッダーは、メッセージに暗号化設定を追加します。	エンベロープ キーのキャッシュをイネーブルにするか、[Remember the password for this envelope] チェックボックスを表示するかしないかのブール値。デフォルト値は false です。

暗号化ヘッダーの例

この項では、暗号化ヘッダーの例を示します。

オフラインでの開封のためエンベロープ キーをイネーブルにする

エンベロープ キーのキャッシュをイネーブルにして Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

[Remember the password for this envelope] チェックボックスが Registered Envelope に表示されます。

JavaScript を含まないエンベロープをイネーブルにする

JavaScript を含めずに Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Use-Script: false
```

受信者が securedoc.html 添付ファイルを開くと、Registered Envelope が [Open Online] リンクとともに表示され、[Open] ボタンがディセーブルになります。

メッセージ有効期限をイネーブルにする

送信後、24 時間で有効期限が切れるようにメッセージを設定するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-ExpirationDate: +24:00:00
```

送信後 24 時間は、受信者はその暗号化されたメッセージを開封して内容を見ることができます。それ以降、Registered Envelope では、エンベロープの有効期限が切れたことを示すメッセージが表示されます。

復号化アプレットをディセーブルにする

復号化アプレットをディセーブルにし、メッセージの添付ファイルをキー サーバで復号するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Suppress-Applet-For-Open: true
```



(注)

復号化アプレットをディセーブルにしている場合、メッセージの開封には時間がかかりますが、ブラウザ環境には依存しなくなります。



CHAPTER 13

SenderBase Network Participation

SenderBase は、電子メール管理者による送信者の調査、電子メールの正規送信元の識別、およびスパム送信者のブロックに役立つように設計された、電子メールの評価サービスです。

System Setup Wizard (GUI) および `systemsetup` コマンド (CLI) で、SenderBase ネットワークへの参加に同意できます。シスコは、組織の電子メールトラフィックを集約した統計情報を収集します。これには、メッセージ属性の要約データおよび Cisco IronPort アプライアンスがどのように各種メッセージを処理したかに関する情報のみが含まれています。たとえば、シスコは、メッセージの本文もメッセージの件名も収集しません。個人を特定できる情報や、組織を特定する情報は、機密情報として扱われます。

この章は、次の内容で構成されています。

- 「共有のイネーブル化」(P.13-1)
- 「よくあるご質問」(P.13-3)

共有のイネーブル化

ご使用の Cisco IronPort アプライアンスの統計情報を SenderBase ネットワークと共有するには、次の手順を実行します。

ステップ 1 [Security Services] > [SenderBase] ページにアクセスします。

図 13-1 [Security Services] > [SenderBase] ページ
SenderBase



(注) システム セットアップ中にライセンス契約書に同意していない場合（「手順 2 : System」(P.3-23) を参照）は、このページの表示は異なります。グローバル設定を編集できるようにするには、[Security Services] > [SenderBase] ページで [Enable] をクリックして、ライセンス契約を読み、同意する必要があります。

ステップ 2 [Edit Global Settings] をクリックします。

図 13-2 [Security Services] > [SenderBase] ページ : 編集
SenderBase

ステップ 3 ボックスをチェックして、SenderBase Information Service との統計データの共有をイネーブルにします。このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。イネーブルにした場合、(IronPort Anti-Spam スキャンがイネーブルになっているかどうかに関係なく) データの収集およびデータの収集に Context Adaptive Scanning Engine (CASE) が使用されます。

ステップ 4 任意で、SenderBase Information Service との統計データ共有用に、プロキシサーバをイネーブルにできます。ルールのアップデートを取得するようにプロキシサーバを定義する場合は、追加で表示されるフィールドに、プロキシサーバに接続する際に使用する認証済みのユーザ名、パスワード、および特定のポート

も設定できます。これらの設定を編集する方法については、「[システム時刻](#)」(P.15-75)を参照してください。また、CLI の `senderbaseconfig` コマンドを使用して同様の設定を行うこともできます。

よくあるご質問

シスコは、プライバシーが重要であると認識しており、プライバシーを考慮してサービスを設計および操作しています。SenderBase Network Participation に登録した場合は、シスコは組織の電子メールトラフィックに関する集約した統計情報を収集しますが、個人を特定できる情報を収集したり、使用したりすることはありません。シスコが収集した、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます。

なぜ参加する必要があるのですか。

SenderBase Network に参加していただくことで、IronPort がお客様に役立てるようになります。スパム、ウイルス、およびディレクトリ獲得攻撃などの、電子メールをベースとした脅威が組織に影響を及ぼすことを止めるには、IronPort とデータを共有していただくことが重要になります。参加が特に重要になる例として、次のような場合があります。

- お客様の組織を特に標的とした電子メール攻撃では、提供したデータがお客様自身を保護する主要な情報源となります。
- お客様の組織が、最初に新しいグローバルな電子メール攻撃を受けた組織の 1 つであった場合、IronPort と共有したデータにより、新しい脅威に対応するスピードが大幅に向上します。

どのようなデータを共有するのですか。

データは、メッセージ属性の要約情報および Cisco IronPort アプライアンスがどのように各種メッセージを処理したかに関する情報です。メッセージの本文すべてを収集するわけではありません。繰り返しになりますが、シスコに提供された、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます（後述の「[シスコは、共有されたデータがセキュアであることをどのように確認していますか。](#)」(P.13-6)を参照してください）。

表 13-1 および表 13-2 に、「人間にわかりやすい」形式でサンプルのログ エントリを説明します。

表 13-1 Cisco IronPort アプライアンスごとに共有される統計情報

項目	サンプル データ
MGA ID	MGA 10012
タイムスタンプ	2005 年 7 月 1 日午前 8 時～午前 8:05 のデータ
ソフトウェア バージョン番号	MGA バージョン 4.7.0
ルール セットのバージョン番号	アンチスパム ルールセット 102
アンチウイルス アップデート間隔	10 分ごとにアップデート
検疫エリアのサイズ	500 MB
検疫可能メッセージ数	現在 50 件のメッセージを検疫可能
ウイルス スコアしきい値	脅威レベル 3 以上のメッセージを検疫
検疫されたメッセージのウイルス スコアの合計	120
検疫されたメッセージ数	30 (平均スコア 4)
最大検疫時間	12 時間
アンチウイルス結果との関連による検疫理由および検疫解除理由で分類した、Outbreak 検疫メッセージ数の内訳	.exe ルールにより 50 件を検疫 手動で 30 件を検疫解除。このうち 30 件すべてがウイルス陽性
検疫解除の際に実行されたアクションで分類した、Outbreak 検疫メッセージ数の内訳	10 件のメッセージは検疫解除後に添付ファイルを削除
メッセージ検疫時間の合計	20 時間

表 13-2 IP アドレスごとに共有される統計情報

項目	サンプル データ
アプライアンスのさまざまな段階におけるメッセージ数	アンチウイルス エンジンにより発見 : 100 アンチスパム エンジンにより発見 : 80
アンチスパムとアンチウイルスのスコア合計および判断	2,000 (発見されたすべてのメッセージに対するアンチスパム スコアの合計)
さまざまなアンチスパム ルールおよびアンチウイルス ルールの組み合わせにヒットしたメッセージ数	100 件のメッセージがルール A および B にヒット 50 件のメッセージがルール A のみにヒット
接続数	20 SMTP 接続
受信者の総数および無効数	総受信者数 50 無効な受信者数 10
ハッシュされたファイル名 : (a)	<one-way-hash>.zip という名前のアーカイブされた添付ファイル内で、ファイル <one-way-hash>.pif が検出
難読化されたファイル名 : (b)	ファイル aaaaaaa.zip 内で、ファイル aaaaaaa0.aaa.pif が検出
URL ホスト名 (c)	メッセージ内で www.domain.com へのリンクが検出
難読化された URL パス (d)	メッセージ内で aaa000aa/aa00aaa というパスを持つホスト名 www.domain.com へのリンクが検出
スパムおよびウイルス スキャン結果ごとのメッセージ数	スパム陽性 10 件 スパム陰性 10 件 スパムの疑い 5 件 ウイルス陽性 4 件 ウイルス陰性 16 件 ウイルス スキャン不可 5 件
さまざまなアンチスパムおよびアンチウイルス判断によるメッセージ数	スパム 500 件、ハム 300 件

表 13-2 IP アドレスごとに共有される統計情報（続き）

項目	サンプル データ（続き）
サイズ レンジ内のメッセージ数	30 ～ 35 K の範囲に 125 件
さまざまな拡張子タイプごとの数	300 個の「.exe」添付ファイル
添付ファイル タイプ、本当のファイル タイプ、およびコンテナ タイプの相関関係	100 個の添付ファイルの拡張子が「.doc」ですが、実際には「.exe」 50 個の添付ファイルが zip 内に含まれた「.exe」拡張子
拡張子および本当のファイル タイプと添付ファイル サイズの相関関係	30 個の添付ファイルが 50 ～ 55 K の範囲の「.exe」

- (a) ファイル名は一方方向ハッシュ（MD5）でエンコードされます。
- (b) ファイル名は難読化された形式で送信されます。この形式では、すべての小文字の ASCII 文字（[a ～ z]）は「a」、すべての大文字の ASCII 文字（[A ～ Z]）は「A」、すべてのマルチバイト UTF-8 文字は（その他の文字セットにプライバシーを提供するため）「x」に、すべての ASCII 数字（[0 ～ 9]）は「0」に置換され、その他すべてのシングルバイト文字（空白文字、句読点など）はそのまま保持されます。たとえば、ファイル Britney1.txt.pif は Aaaaaaa0.aaa.pif と表示されます。
- (c) IP アドレスと同様に、URL ホスト名はコンテンツを提供する Web サーバを指定します。ユーザ名およびパスワードのような、秘密情報は含まれません、
- (d) ホスト名に続く URL 情報は、ユーザの個人情報が漏えいしないように難読化されています。

シスコは、共有されたデータがセキュアであることをどのように確認していますか。

SenderBase Network への参加に同意すると、次のように処理されます。

Cisco IronPort アプライアンスから送信されたデータは、セキュアなプロトコル HTTPS を使用して Cisco IronPort SenderBase Network サーバに送信されます。

お客様のデータはすべて、シスコで慎重に取り扱われます。このデータは、セキュアな場所に保存され、データへのアクセスは、企業の電子メールセキュリティ製品およびサービスの向上またはカスタマー サポートの提供のためにデータにアクセスする必要があるシスコの従業員および請負業者に限られます。

データに基づいてレポートまたは統計情報が作成された場合、電子メールの受信者またはお客様の企業を特定する情報が、シスコ以外で共有されることはありません。

データを共有することで Cisco IronPort アプライアンスのパフォーマンスに影響はありますか。

シスコは、ほとんどのお客様には若干のパフォーマンス上の影響があると認識しています。IronPort は、電子メール配信プロセスの一環として、既存のデータを記録します。その後、アプライアンス上でお客様のデータが集約され、通常 5 分ごとに SenderBase サーバに一括送信されます。HTTPS を介して転送されるデータの総サイズは、一般的な企業の電子メールトラフィック帯域幅の 1% 未満と予想しています。

イネーブルにした場合、(IronPort Anti-Spam スキャンがイネーブルになっているかどうかに関係なく) データの収集およびデータの収集に Context Adaptive Scanning Engine (CASE) が使用されます。



(注)

C30 および C10/100 アプライアンスでは、SenderBase ネットワークへの参加を選択した場合、メッセージごとに「本文スキャン」が実行されます。これは、メッセージに適用されたフィルタなどのアクションにより本文スキャンが起動されたかどうかに関係なく実行されます。本文スキャンの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Body Scanning Rule」を参照してください。

不明点は、Cisco IronPort カスタマー サポートまでお問い合わせください。
「[Cisco IronPort サポート コミュニティ](#)」(P.1-20) を参照してください。

その他の方法でデータを共有できますか。

シスコがより高品質のセキュリティ サービスを提供できるようにするために、追加のデータの共有をお考えのお客様のために、追加データの提供を可能にするコマンドを用意しています。このより高レベルのデータ共有では、メッセージに含まれる添付ファイルの明確なファイル名、ハッシュされていないテキスト、および URL のホスト名も提供されます。この機能の詳細について関心をお持ちの場合は、システム エンジニアまたは Cisco IronPort カスタマー サポートにお問い合わせください。



CHAPTER 14

テキスト リソース

この章は、次の内容で構成されています。

- 「概要」 (P.14-1)
- 「コンテンツ ディクショナリ」 (P.14-3)
- 「コンテンツ ディクショナリの管理 (GUI)」 (P.14-6)
- 「コンテンツ ディクショナリの使用方法およびテスト方法」 (P.14-11)
- 「DLP ディクショナリ」 (P.14-13)
- 「テキスト リソースについて」 (P.14-18)
- 「テキスト リソースの管理 (GUI)」 (P.14-20)
- 「テキスト リソースの使用」 (P.14-27)

概要

この章では、コンテンツ ディクショナリ、DLP ディクショナリ、免責事項、およびテンプレートなどのさまざまなテキスト リソースの作成および管理について説明します。

コンテンツ ディクショナリ

コンテンツ ディクショナリを使用して、企業のポリシーに沿った適切なアクションを実行できるようにメッセージまたはコンテンツ フィルタに対してメッセージをスキャンできます。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。ディクショナリごとに、大文字と小文字

の区別および単語の区切りの検出方法を決定することもできます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語に対してメッセージをスキャンし、一致する単語を含むメッセージをドロップまたはアーカイブできます。また、単語によってフィルタ アクションをより簡単にトリガーできるように、ディクショナリに「重み」の条件を追加できます。

ディクショナリには、非 ASCII 文字を含めることができます。

DLP ディクショナリ

Data Loss Prevention (DLP; データ消失防止) ディクショナリを使用して、発信メッセージに対して DLP ポリシーに従った機密情報のスキャンができます。コンテンツ ディクショナリと同様に、ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。また、コンテンツ ディクショナリとは異なり、DLP ポリシーの単語には「重み」がありません。AsyncOS には、RSA Security Inc. による事前定義されたディクショナリのセットが存在します。カスタム DLP ディクショナリを作成することもできます。

ディクショナリの単語は大文字と小文字が区別され、非 ASCII 文字を含めることができます。データ消失防止の詳細については、[第 11 章「データ消失防止」](#)を参照してください。

テキスト リソース

テキスト リソースは、免責事項、通知テンプレート、アンチウイルス テンプレートなどのテキスト オブジェクトです。AsyncOS のさまざまなコンポーネントで使用できる新規オブジェクトを作成できます。テキスト リソースをインポートおよびエクスポートできます。

メッセージの免責事項スタンプ

メッセージの免責事項スタンプを使用すると、免責事項のテキスト リソースをメッセージに追加できます。たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

コンテンツ ディクショナリ

AsyncOS では、コンテンツ ディクショナリと DLP ディクショナリの 2 種類のディクショナリを提供しています。DLP ディクショナリの管理については、「[DLP ディクショナリ](#)」(P.14-13) を参照してください。

コンテンツ ディクショナリは、アプライアンスの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツ フィルタおよびメッセージ フィルタの両方に利用できます。定義したディクショナリを使用し、ディクショナリに含まれる単語に対してメッセージ、メッセージ ヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行できます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタルールを使用してリスト内の単語を含むメッセージをスキャンし、メッセージをドロップ、アーカイブ、または検疫できます。

AsyncOS オペレーティング システムには、GUI ([Mail Policies] > [Dictionaries]) または CLI の `dictionaryconfig` コマンドを使用して、合計 100 個のコンテンツ ディクショナリを定義する能力があります。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。

ディクショナリの内容

ディクショナリの単語は 1 行につき 1 つのテキスト文字列で作成し、エントリはプレーン テキストまたは正規表現の形式で記載できます。ディクショナリには、非 ASCII 文字を含めることもできます。正規表現のディクショナリを定義すると、より柔軟に単語を照合させることができます。ただし、このためには適切に単語を区切る方法を理解する必要があります。Python スタイルの正規表現の詳細については、次の URL からアクセスできる「[Python Regular Expression HOWTO](#)」を参考にしてください。

<http://www.python.org/doc/howto/>



(注)

ディクショナリのエントリの最初に特殊文字 # を使用すると、文字クラス [#] をコメントとして扱われることなく使用できます。

単語によってフィルタ条件をより簡単にトリガーできるように、各単語に「重み」を指定できます。AsyncOS では、コンテンツ ディクショナリの単語に対してメッセージをスキャンし、単語インスタンスの数に単語の重みを掛けることで

メッセージのスコアを付けます。2 つの単語インスタンスに 3 の重みが付いている場合、スコアは 6 になります。AsyncOS は、このスコアをコンテンツ フィルタまたはメッセージ フィルタに関連するしきい値と比較し、メッセージがフィルタ アクションをトリガーするかどうかを決定します。

コンテンツ ディクショナリにスマート ID を追加することもできます。スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。これらの ID はポリシーの拡張に便利です。正規表現の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Regular Expressions in Rules」を参照してください。スマート ID の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Smart Identifiers」を参照してください。



(注)

端末の CLI に非 ASCII 文字を含むディクショナリが正しく表示される場合とされない場合があります。非 ASCII 文字を含むディクショナリを表示および変更する最適な方法は、ディクショナリをテキスト ファイルにエクスポートし、テキスト ファイルを編集して、新しいファイルを再びアプライアンスにインポートする方法です。詳細については、「[テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法](#)」(P.14-4) を参照してください。

単語境界と 2 バイト文字セット

一部の言語 (2 バイト文字セット) では、単語または単語の区切りに関する概念や、大文字/小文字がありません。単語を構成する文字 (正規表現構文では「\w」と表される) とそうでない文字のような概念に依存した複雑な正規表現では、ロケールが不明なときや確実なエンコード方式が不明な場合に問題が発生します。この理由から、単語境界の拡張をディセーブルにできます。

テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法

コンテンツ ディクショナリ機能には、デフォルトでアプライアンスのコンフィギュレーション ディレクトリに配置されている次のテキスト ファイルが含まれます。

- config.dtd

- profanity.txt
- proprietary_content.txt
- sexual_content.txt

これらのテキスト ファイルは、コンテンツ ディクショナリ機能と組み合わせて使用することで、新規ディクショナリの作成をサポートすることを目的としています。これらのコンテンツ ディクショナリは重み付けされており、スマート ID を使用することでデータ内のパターンを高い精度で検出し、コンプライアンスの問題となるパターンの場合にはフィルタをトリガーします。



(注)

ディクショナリをインポートおよびエクスポートする場合は、完全に一致する単語の設定と大文字と小文字を区別する設定が保持されません。この設定は、設定ファイルにのみ保持されます。

コンフィギュレーション ディレクトリへのアクセスの詳細については、[付録 A 「アプライアンスへのアクセス」](#) を参照してください。

ユーザ独自のディクショナリ ファイルを作成して、アプライアンスにインポートすることもできます。非 ASCII 文字をディクショナリに追加する最適な方法は、アプライアンス以外の場所でテキスト ファイルのディクショナリに単語を追加し、アプライアンス上にファイルを移動してから新しいディクショナリとしてファイルをインポートする方法です。ディクショナリのインポートの詳細については、「[ディクショナリのインポート](#)」(P.14-9) を参照してください。ディクショナリのエクスポートについては、「[ディクショナリのエクスポート](#)」(P.14-10) を参照してください。

カスタム DLP ディクショナリをインポートおよびエクスポートすることもできます。詳細については、「[DLP ディクショナリのインポートおよびエクスポート](#)」(P.14-16) を参照してください。



警告

これらのテキスト ファイルには、一部の人の間では卑猥、下品または不快に感じられる単語が含まれています。これらのファイルからコンテンツ ディクショナリに単語をインポートした場合、アプライアンスに設定したコンテンツ ディクショナリを後で閲覧する際にこれらの単語が表示されます。

コンテンツ ディクショナリの管理 (GUI)

GUI にログインし、[Mail Policies] タブをクリックします。左側のメニューで [Dictionaries] リンクをクリックします。

図 14-1 [Dictionaries] ページ
Dictionaries

Name	Terms	Ignore case	Match Whole Words Only	Delete
secret_words	codename SecretProjectName	Yes	Yes	🗑️

ディクショナリの追加

新規ディクショナリを作成するには、次の手順を実行します。

- ステップ 1** [Dictionaries] ページで [Add Dictionary] をクリックします。[Add Dictionary] ページが表示されます。

図 14-2 [Dictionaries] ページ
Add Dictionary

- ステップ 2** ディクショナリの名前を入力します。
- ステップ 3** [Match Whole Words Only] の横にあるチェックボックスをオンにすることで、完全に一致する単語のみを検索するかどうかを指定します。詳細については、「完全に一致する単語のみの検索」(P.14-8) を参照してください。
- ステップ 4** 大文字と小文字を区別した検索を実行するかどうかを指定します。詳細については、「大文字と小文字を区別した単語の一致」(P.14-8) を参照してください。



(注) AsyncOS では、完全に一致する単語の設定と大文字と小文字を区別する設定が保持されます（これらの設定が設定ファイルに保存されている場合）。ディクショナリをインポートおよびエクスポートする場合、これらの設定は保持されません。

- ステップ 5** オプションで、ディクショナリにスマート ID を追加します。スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。スマート ID の詳細については、『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。

- ステップ 6** 新規ディクショナリのエントリーを単語のリストに入力します。サポートされているエントリーの種類の詳細については、「[ディクショナリの内容](#)」(P.14-3) を参照してください。
- ステップ 7** 単語に対する重みを指定します。フィルタ アクションを他の単語よりトリガーしやすくなるように、ディクショナリの単語に「重み」を付けられます。この重みがフィルタ アクションの決定に使用される仕組みの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Threshold Scoring for Content Dictionaries」を参照してください。
- ステップ 8** [Add] をクリックします。
- ステップ 9** 変更を送信して確定します。

[Dictionaries] ページには新しいディクショナリが、ディクショナリに含まれている単語およびディクショナリに設定した設定値とともに表示されています。



(注) 正規表現「.*」をエントリーの最初または最後に使用したコンテンツ ディクショナリのエントリーがあると、その「単語」に一致する MIME パートが見つかった場合にシステムがロックされます。コンテンツ ディクショナリのエントリーの最初または最後に、「.*」を使用しないことが推奨されます。

大文字と小文字を区別した単語の一致

このボックスをオンにすると、AsyncOS が照合の際に単語の大文字/小文字を考慮します。たとえば、単語「codename」はディクショナリのエントリー「codename」と一致しますが、単語「CodeName」は一致しません。

完全に一致する単語のみの検索

このボックスをオンにすると、エントリーに完全に一致する単語のみを検索します。たとえば、単語「codename」はディクショナリのエントリー「codename」と一致しますが、単語「code」および「codenam」は一致しません。

単語のソート

カラムの見出しをクリックして、単語の順または重みの順にソートできます。カラムの見出しをもう一度クリックすると、ソート順が逆になります。

ディクショナリの編集

既存のディクショナリを編集するには、次の手順を実行します。

-
- ステップ 1** [Dictionaries] ページで、リストにあるディクショナリの名前をクリックします。[Edit Dictionary page] が表示されます。
 - ステップ 2** ディクショナリのエントリまたは設定値を変更して、[Submit] をクリックします。
 - ステップ 3** 変更を確定します。

ディクショナリの削除

ディクショナリを削除するには、次の手順を実行します。

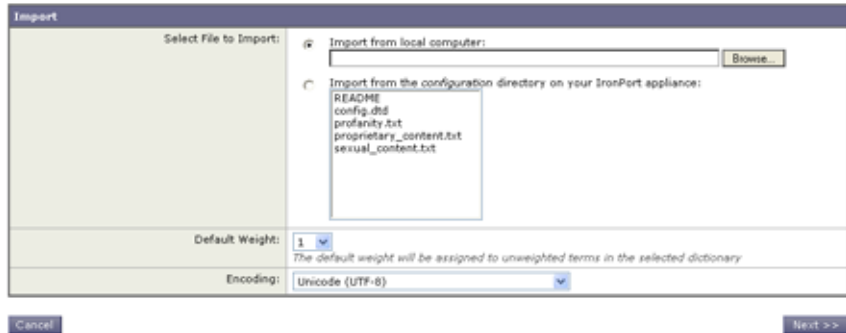
-
- ステップ 1** ディクショナリの横にあるゴミ箱アイコンをクリックして、ディクショナリのリストから削除します。確認メッセージが表示されます。
 - ステップ 2** 確認メッセージには、ディクショナリを現在参照しているフィルタがすべて表示されます。
 - ステップ 3** [Delete] をクリックして、ディクショナリを削除します。
 - ステップ 4** 変更を確定します。
 - ステップ 5** 削除されたディクショナリを参照しているすべてのメッセージ フィルタは、無効としてマークされます。
 - ステップ 6** 削除されたディクショナリを参照しているすべてのコンテンツ フィルタはイネーブルのままになりますが、今後無効と判断されます。

ディクショナリのインポート

ディクショナリを GUI からインポートするには、次の手順を実行します。

-
- ステップ 1** [Dictionaries] ページで [Import Dictionary] をクリックします。[Import Dictionary] ダイアログが表示されます。

図 14-3 [Import Dictionary] ページ
Import Dictionary



ステップ 2 インポート元の場所を選択します。

ステップ 3 インポートするファイルを選択します。



(注) インポートするファイルは、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存在する必要があります。

ステップ 4 ディクショナリの単語に使用するデフォルトの重みを選択します。AsyncOS では、重みが指定されていない単語に対してデフォルトの重みを割り当てます。ファイルのインポート後に重みを編集できます。

ステップ 5 エンコード方式を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 インポートしたディクショナリは、[Add Dictionary] ページに表示されます。

ステップ 8 ディクショナリを追加する前に、ディクショナリの名前の指定およびディクショナリの編集ができます。

ステップ 9 変更を送信して確定します。

ディクショナリのエクスポート

ディクショナリを GUI からエクスポートするには、次の手順を実行します。

ステップ 1 [Dictionaries] ページで [Export Dictionary] をクリックします。[Export Dictionary] ダイアログが表示されます。

図 14-4 [Export Dictionary] ページ

Export Dictionary

- ステップ 2 エクスポートするディクショナリを選択します。
- ステップ 3 ディクショナリのファイル名を入力します。これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。
- ステップ 4 エクスポート先の場所を選択します。
- ステップ 5 テキスト ファイルのエンコード方式を選択します。
- ステップ 6 変更を送信して確定します。

コンテンツ ディクショナリの使用方法およびテスト方法

ディクショナリは、さまざまな `dictionary-match()` メッセージ フィルタ ルールおよびコンテンツ フィルタに使用できます。

ディクショナリの照合フィルタ ルール

メッセージ フィルタ ルール (`dictionary-match(<dictionary_name>)` (および同様のルール) は、メッセージの本文にコンテンツ ディクショナリ (`dictionary_name`) に存在するいずれかの正規表現が含まれる場合に有効と判断されます。該当のディクショナリが存在しない場合は、ルールは無効と判断されます。

`dictionary-match()` ルールは、`body-contains()` 本文スキャン ルールと同様にメッセージ本文と添付ファイルのみをスキャンし、ヘッダーをスキャンしないことに注意してください。

ヘッダーのスキャンには、適切な `*-dictionary-match()` タイプのルールを使用できます (`subject-dictionary-match()` や、より一般的なルールでカスタムヘッダーを含むすべてのヘッダーを指定できる `header-dictionary-match()` など、特定のヘッダーに対するルールが存在します)。ディクショナリの照合の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Dictionary Rules」を参照してください。

表 14-1 コンテンツ ディクショナリのメッセージ フィルタ ルール

ルール	構文	説明
ディクショナリ照合	<code>dictionary-match(<dictionary_name>)</code>	指定したディクショナリに存在するすべての正規表現に一致した単語がメッセージに含まれているか。

次の例では `dictionary-match()` ルールを使用して、Cisco IronPort アプライアンスが（前回の例で作成した）「`secret_words`」という名前のディクショナリ内の単語を含むメッセージをスキャンした際に、管理者にメッセージをブラインドカーボン コピーで送信する新規メッセージ フィルタが作成されます。設定値によっては、大文字/小文字も含めて「`codename`」と完全に一致する単語を含むメッセージのみが、このフィルタで有効と判断されることに注意してください。

`bcc_codenames:`

```
if (dictionary-match ('secret_words'))
{
    bcc('administrator@example.com');
}
```

この例では、Policy 検疫にメッセージを送信します。

`quarantine_codenames:`

```
if (dictionary-match ('secret_words'))
{
```

```
quarantine('Policy');
}
```

ディクショナリ エントリの例

表 14-2 ディクショナリ エントリの例

説明	例 :
ワイルドカード	*
アンカー	最後で使用する場合 : foo\$ 先頭で使用する場合 : ^foo
電子メール アドレス (ピリオドをエスケープしないこと)	foo@example.com, @example.com example.com\$ (最後で使用する場合) @example.*
件名	An email subject (電子メールの件名に ^アンカーを使用する際は、件名の先頭に「RE:」や「FW:」などが多く付いていることを覚えておいてください)

コンテンツ ディクショナリのテスト方法

trace 機能を使用すると、dictionary-match() ルールを使用しているメッセージフィルタに対して迅速なフィードバックが得られます。詳細については、[「Debugging Mail Flow Using Test Messages: Trace」\(P.446\)](#) を参照してください。上記の quarantine_codenames フィルタの例のように、quarantine() アクションを使用してフィルタをテストすることもできます。

DLP ディクショナリ

DLP ディクショナリは、アプライアンスの RSA DLP スキャン機能と連携して動作する単語または語句のグループであり、カスタム DLP ポリシーに利用できます。DLP ディクショナリを使用し、ディクショナリに含まれる単語および語句に対してメッセージおよびメッセージの添付ファイルをスキャンすることで、

企業のポリシーに沿った適切なアクションを実行できます。AsyncOS には、RSA Security Inc. による事前定義されたディクショナリのセットが存在します。カスタム DLP ディクショナリを作成することもできます。

ユーザ独自のディクショナリをテキスト ファイルとしてローカル マシンに作成し、アプライアンスにインポートすることもできます。ディクショナリのテキスト ファイルにおける各単語には、強制改行を使用します。ディクショナリの単語は大文字と小文字が区別され、非 ASCII 文字を含めることができます。

DLP Policy Manager を使用して、DLP ディクショナリを管理します。DLP Policy Manager を開くには、GUI で [Mail Policies] > [DLP Policy Manager] メニューを選択します。DLP Policy Manager の詳細については、[第 11 章「データ消失防止」](#)を参照してください。

カスタム ディクショナリの追加

新規ディクショナリを作成するには、次の手順を実行します。

- ステップ 1** DLP Policy Manager で [Custom DLP Dictionaries] リンクをクリックします。
[DLP Dictionaries] ページが表示されます。
- ステップ 2** [Add Dictionary] をクリックします。
[Add Dictionary] ページが表示されます。

図 14-5 DLP ディクショナリの追加
DLP Policy Manager: Add DLP Dictionaries

- ステップ 3** カスタム ディクショナリの名前を入力します。
- ステップ 4** 新規ディクショナリのエントリを単語のリストに入力します。複数のエントリを一度に入力するには、強制改行を使用します。
- ステップ 5** [Add] をクリックします。
- ステップ 6** 新規ディクショナリを送信し、確定します。

[Dictionaries] ページには新しいディクショナリが、ディクショナリに含まれている単語およびディクショナリに設定した設定値とともに表示されています。

カスタム DLP ディクショナリの編集

カスタム ディクショナリを編集するには、次の手順を実行します。

- ステップ 1** [DLP Dictionaries] ページで、リストにあるディクショナリの名前をクリックします。
- ステップ 2** エントリを変更します。
- ステップ 3** 変更を送信して確定します。

カスタム DLP デクシヨナリの削除

カスタム デクシヨナリを削除するには、次の手順を実行します。

- ステップ 1** デクシヨナリの横にあるゴミ箱アイコンをクリックして、デクシヨナリのリストから削除します。確認メッセージが表示され、デクシヨナリを現在参照しているフィルタがすべて表示されます。
- ステップ 2** [Delete] をクリックして、デクシヨナリを削除します。
- ステップ 3** 変更を確定します。

DLP デクシヨナリのインポートおよびエクスポート

ユーザ独自の DLP デクシヨナリをテキスト ファイルとしてローカル マシンに作成し、AsyncOS にインポートできます。また、同様に既存のカスタム デクシヨナリをテキスト ファイルとしてエクスポートできます。事前定義された DLP デクシヨナリはエクスポートできません。

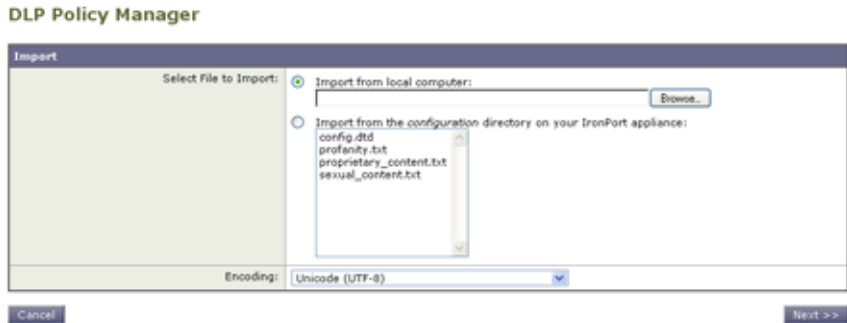
DLP デクシヨナリ ファイルには、デクシヨナリの単語として使用される単語および語句が強制改行で区切られたリストが含まれています。DLP デクシヨナリとして使用するために既存のコンテンツ デクシヨナリをエクスポートする場合は、DLP デクシヨナリとしてテキスト ファイルをインポートする前に重み値を削除し、すべての正規表現を単語または語句に変換する必要があります。

テキスト ファイルとして DLP デクシヨナリをインポートする方法

デクシヨナリをインポートするには、次の手順を実行します。

- ステップ 1** [DLP Dictionaries] ページで [Import Dictionary] をクリックします。
[Import Dictionary] ダイアログが表示されます。

図 14-6 ディクショナリのインポート



- ステップ 2** ファイルをローカル マシンからインポートするか、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からインポートするかを選択します。
- ステップ 3** エンコード方式を選択します。
- ステップ 4** [Next] をクリックします。
- ステップ 5** インポートしたディクショナリは、[Add Dictionary] ページに表示されます。
- ステップ 6** ディクショナリを追加する前に、ディクショナリの名前の指定およびディクショナリの編集ができます。
- ステップ 7** 変更を送信して確定します。

テキスト ファイルとして DLP ディクショナリをエクスポートする方法

ディクショナリをエクスポートするには、次の手順を実行します。

- ステップ 1** [Dictionaries] ページで [Export Dictionary] をクリックします。
[Export Dictionary] ダイアログが表示されます。

図 14-7 ディクショナリのエクスポート

Dictionaries

Export

Dictionary to Export:

File Name:

Export Location:

Export to local computer

Export to the configuration directory on your IronPort appliance

Encoding:

- ステップ 2** エクスポートするディクショナリを選択します。
- ステップ 3** ディクショナリのファイル名を入力します。
- ステップ 4** エクスポートされたディクショナリを保存する場所（ローカル コンピュータまたはアプライアンスのコンフィギュレーション ディレクトリのいずれか）を選択します。
- ステップ 5** ファイルのエンコード方式を選択します。
- ステップ 6** 変更を送信して確定します。

テキスト リソースについて

テキスト リソースは、メッセージへの添付や、メッセージとしての送信が可能なテキスト テンプレートです。テキスト リソースは、次のいずれかの種類になります。

- **メッセージ免責事項**：メッセージに追加されるテキスト。詳細については、「[免責事項テンプレート](#)」(P.14-27) を参照してください。
- **通知テンプレート**：通知として送信されるメッセージ (`notify()` および `notify-bcc()` アクションで使用されます)。詳細については、「[通知テンプレート](#)」(P.14-37) を参照してください。
- **アンチウイルス通知テンプレート**：メッセージにウイルスが見つかったときに、通知として送信されるメッセージ。コンテナ用のテンプレート（元のメッセージに付加）、またはメッセージに付加せず通知として送信されるテンプレートを作成できます。詳細については、「[アンチウイルス通知テンプレート](#)」(P.14-38) を参照してください。

- **バウンスおよび暗号化失敗通知テンプレート**：メッセージがバウンスされたときやメッセージの暗号化に失敗したときに通知として送信されるメッセージ。詳細については、「[バウンス通知および暗号化失敗通知テンプレート](#)」(P.14-42) を参照してください。
- **DLP 通知テンプレート**：電子メール メッセージに、組織のデータ消失防止ポリシーに違反する情報が含まれる場合に送信されるメッセージ。詳細については、「[DLP 通知テンプレート](#)」(P.14-44) を参照してください。
- **暗号化通知テンプレート**：発信電子メールを暗号化するように Cisco IronPort アプライアンスを設定した場合に送信されるメッセージ。このメッセージは、受信者が暗号化されたメッセージを受信したことを受信者に通知し、メッセージを読む手順を示します。詳細については、「[暗号化通知テンプレート](#)」(P.14-47) を参照してください。

CLI (textconfig) または GUI を使用して、テキスト リソースの追加、削除、編集、インポート、およびエクスポートを含むテキスト リソースの管理ができます。GUI を使用したテキスト リソースの管理については、「[テキスト リソースの管理 \(GUI\)](#)」(P.14-20) を参照してください。

テキスト リソースには、非 ASCII 文字を含めることができます。



(注)

非 ASCII 文字を含むテキスト リソースは端末の CLI に正しく表示される場合とされない場合があります。非 ASCII 文字を含むテキスト リソースを表示および変更するには、テキスト リソースをテキスト ファイルにエクスポートし、テキスト ファイルを編集して、新しいファイルを再びアプライアンスにインポートします。詳細については、「[テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする](#)」(P.14-19) を参照してください。

テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする

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対するアクセス権を持っている必要があります。インポートするテキスト ファイルは、アプライアンス上のコンフィギュレーションディレクトリに存在する必要があります。エクスポートされたテキスト ファイルは、コンフィギュレーションディレクトリに配置されます。

コンフィギュレーションディレクトリへのアクセスの詳細については、[付録 A「アプライアンスへのアクセス」](#)を参照してください。

非 ASCII 文字をテキスト リソースに追加するには、アプライアンス以外の場所でテキスト ファイルのテキスト リソースに単語を追加し、アプライアンス上にファイルを移動し、新しいテキスト リソースとしてファイルをインポートします。テキスト リソースのインポートの詳細については、「[テキスト リソースのインポート](#)」(P.14-22) を参照してください。テキスト リソースのエクスポートについては、「[テキスト リソースのエクスポート](#)」(P.14-23) を参照してください。

テキスト リソースの管理 (GUI)

テキスト リソースは、GUI で [Mail Policies] > [Text Resources] ページに移動して管理できます。[Text Resources] ページでは、テキスト リソースを追加、編集、削除、エクスポート、およびインポートできます。

すべてのテキスト リソース タイプに対してプレーンテキスト メッセージを定義できます。また、一部のテキスト リソース タイプに対して HTML ベースのメッセージを定義することもできます。詳細については、「[HTML ベースのテキスト リソースの使用](#)」(P.14-24) を参照してください。

図 14-8 [Text Resources] ページ

Text Resources

Items per page 20

Add Text Resource... Import Text Resource...

Text Resource Name	Type	Preview	Delete
AVContainer1	Anti-Virus Container Template		
CompanyDisclaimer	Disclaimer Template		
strip.mp3	Notification Template		

Export Text Resource...



(注) テキスト リソースは、textconfig コマンドを使用して CLI から管理できます。

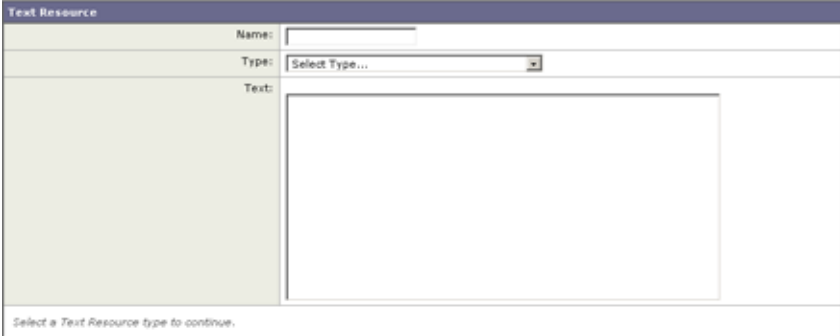
テキスト リソースの追加

新規テキスト リソースを作成するには、次の手順を実行します。

- ステップ 1** [Mail Policies] > [Text Resources] ページに移動し、[Add Text Resource] をクリックします。[Add Text Resource] ページが表示されます。

図 14-9 テキスト リソースの追加

Add Text Resource



Select a Text Resource type to continue.

- ステップ 2** [Name] フィールドにテキスト リソースの名前を入力します。
- ステップ 3** [Type] フィールドからテキスト リソースのタイプを選択します。
- ステップ 4** 適切なフィールドにメッセージ テキストを入力します。テキスト リソースでプレーンテキスト メッセージのみが許可される場合は、[Text] フィールドを使用します。テキスト リソースで HTML およびプレーンテキスト メッセージの両方が許可される場合は、[HTML] フィールドと [Plain Text] フィールドを使用します。詳細については、「[HTML ベースのテキスト リソースの使用](#)」(P.14-24)を参照してください。
- ステップ 5** 変更を送信して確定します。

テキスト リソースの編集

既存のテキスト リソースを編集するには、次の手順を実行します。

-
- ステップ 1** [Mail Policies] > [Text Resources] ページに移動し、編集するテキスト リソースの名前をクリックします。[Edit Text Resource] ページが表示されます。
- ステップ 2** テキスト リソースを変更します。
- ステップ 3** 変更を送信して確定します。

テキスト リソースの削除

テキスト リソースは [Text Resources] ページから削除できます。ただし、次のことに注意してください。

- 削除されたテキスト リソースを参照しているすべてのメッセージ フィルタは、無効としてマークされます。
- 削除されたテキスト リソースを参照しているすべてのコンテンツ フィルタはイネーブルのままになりますが、今後無効と判断されます。

テキスト リソースを削除するには、次の手順を実行します。

-
- ステップ 1** [Mail Policies] > [Text Resources] ページに移動し、削除するテキスト リソースの [Delete] 列にあるゴミ箱アイコンをクリックします。確認メッセージが表示されます。
- ステップ 2** [Delete] をクリックして、テキスト リソースを削除します。
- ステップ 3** 変更を確定します。

テキスト リソースのインポート

テキスト リソースをインポートするには、次の手順を実行します。

-
- ステップ 1** [Mail Policies] > [Text Resources] ページに移動し、[Import Text Resource] をクリックします。[Import Text Resource] ページが表示されます。

図 14-10 テキスト リソースのインポート

Import Text Resource



ステップ 2 インポートするファイルを選択します。



(注) インポートするファイルは、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存在する必要があります。

ステップ 3 エンコード方式を指定します。

ステップ 4 [Next] をクリックします。

インポートされたテキスト リソースは、[Add Text Resource] ページの [Text] フィールドに表示されます。

ステップ 5 名前を選択し、テキスト リソース タイプを編集および選択します。

ステップ 6 変更を送信して確定します。

テキスト リソースのエクスポート

テキスト リソースをエクスポートする場合は、テキスト ファイルが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作成されます。

テキスト リソースをエクスポートするには、次の手順を実行します。

ステップ 1 [Mail Policies] > [Text Resources] ページに移動し、[Export Text Resource] をクリックします。[Export Text Resource] ダイアログが表示されます。

図 14-11 テキスト リソースのエクスポート

Export Text Resource

Export

The file will be exported to the configuration directory on your IronPort MGA.

Text Resource to Export:

File Name:

Encoding:

- ステップ 2** エクスポートするテキスト リソースを選択します。
- ステップ 3** テキスト リソースのファイル名を入力します。
- ステップ 4** テキスト ファイルのエンコード方式を選択します。
- ステップ 5** [Submit] をクリックしてテキスト リソースを含むテキスト ファイルをコンフィギュレーション ディレクトリに作成します。

HTML ベースのテキスト リソースの使用

免責事項などの一部のテキスト リソースは、HTML ベースのメッセージおよびプレーン テキスト メッセージの両方を使用して作成できます。HTML ベースのメッセージとプレーン テキスト メッセージの両方を含むテキスト リソースが電子メール メッセージに適用された場合、HTML ベースのテキスト リソース メッセージは電子メール メッセージのテキストまたは HTML 部分に適用され、プレーン テキスト メッセージは電子メール メッセージのテキストまたはプレーン 部分に適用されます。

HTML ベースのテキスト リソースを追加または編集する場合、GUI には、HTML コードを手動で記述せずにリッチ テキストの入力を可能にするリッチ テキスト編集が含まれます。

図 14-12 に、HTML ベースのテキスト リソース向けのリッチ テキスト エディタを示します。

図 14-12 HTML ベースのテキスト リソースの作成

Add Text Resource

The screenshot shows the 'Add Text Resource' dialog box. It has a title bar 'Text Resource'. Below the title bar, there is a 'Name' field. The 'Type' is set to 'Disclaimer Template'. The 'HTML' section contains a rich text editor with font settings (Arial, Normal) and buttons for Bold, Italic, Underline, and Code View. The 'Plain Text' section has a dropdown set to 'Auto-generate from HTML'. There are 'Preview' and 'Preview Text' buttons at the bottom.

HTML ベースのテキスト リソースを追加および編集する場合は、次のルールとガイドラインに留意してください。

- HTML バージョンに基づいて、メッセージのプレーン テキスト バージョンを自動的に生成するよう選択できます。または、プレーン テキスト バージョンを個別に定義できます。
- [Code View] ボタンをクリックすることにより、リッチ テキスト エディタと HTML コード間を切り替えることができます。
- リッチ テキスト エディタでサポートされない HTML コードを GUI で入力するには、コード ビューに切り替え、HTML コードを手動で入力します。たとえば、これは、`` HTML タグを使用して外部サーバにあるイメージ ファイルへの参照を挿入する場合があります。

HTML ベースのテキスト リソースのインポートおよびエクスポート

HTML ベースのテキスト リソースをテキスト ファイルにエクスポートしたり、テキスト ファイルから HTML ベースのテキスト リソースをインポートしたりできます。HTML ベースのテキスト リソースをファイルにエクスポートする場合、ファイルにはテキスト リソースの各バージョンに対する次のセクションが含まれます。

```
[html_version]
[text_version]
```

これらのセクションの順序は重要ではありません。

たとえば、エクスポートされたファイルには、次のテキストが含まれることがあります。

```
[html_version]
<p>Sample <i>message.</i></p>
[text_version]
Sample message.
```

HTML ベースのテキスト リソースをエクスポートおよびインポートする場合は、次のルールとガイドラインに留意してください。

- プレーンテキストメッセージが HTML バージョンから自動的に生成される HTML ベースのテキスト リソースをエクスポートする場合、エクスポートされたファイルには [text_version] セクションが含まれません。
- テキスト ファイルからインポートするとき、[html_version] セクション下のすべての HTML コードは作成されたテキスト リソースの HTML メッセージに変換されます (テキスト リソース タイプが HTML メッセージをサポートする場合)。同様に、[text_version] セクション下のすべてのテキストは、作成されたテキスト リソースのプレーンテキストメッセージに変換されます。
- HTML ベースのテキスト リソースを作成するために、空の、または存在しない [html_version] セクションを含むファイルからインポートする場合、Cisco IronPort アプライアンスは [text_version] セクションのテキストを使用して HTML およびプレーンテキストメッセージの両方を作成します。

テキスト リソースの使用

すべてのタイプのテキスト リソースは、[Text Resources] ページまたは CLI の `textconfig` コマンドを使用して、同じ方法で作成されます。一度作成されると、各タイプで異なる使われ方をします。免責事項テンプレートおよび通知テンプレートは、フィルタおよびリスナーで使用されます。一方、アンチウイルス通知テンプレートは、メール ポリシーおよびアンチウイルス設定値で使用されます。

免責事項テンプレート

Cisco IronPort アプライアンスは、リスナーが受信した一部またはすべてのメッセージのテキストの上または下（ヘッダーまたはフッター）にデフォルトの免責事項を追加できます。次の方法を使用して、Cisco IronPort アプライアンスでメッセージに免責事項を追加できます。

- リスナーから、GUI または `listenerconfig` コマンドを使用する方法（「[リスナーからの免責事項テキストの追加](#)」(P.14-28) を参照）。
- コンテンツ フィルタ アクション `Add Disclaimer Text` を使用する方法（「[コンテンツ フィルタのアクション](#)」(P.6-20) を参照）。
- メッセージ フィルタ アクション `add-footer()` を使用する方法（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「[Using Message Filters to Enforce Email Policies](#)」の章を参照）。
- データ消失防止プロファイルを使用する方法（「[データ消失防止](#)」(P.11-1) を参照）。
- メッセージの目的がフィッシングまたはマルウェアの配布である可能性があることをユーザに通知するよう感染フィルタに対してメッセージの修正を使用する方法（「[メッセージの変更](#)」(P.10-9) を参照）。このタイプの通知に追加される免責事項は、テキストの上に追加されます。

たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

免責事項テキストを使用する前に、免責事項テンプレートを作成する必要があります。GUI の [Text Resources] ページ（「[テキスト リソースの追加](#)」(P.14-21) を参照）または `textconfig` コマンド（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）を使用して、使用するテキスト文字列のセットを作成および管理します。

リスナーからの免責事項テキストの追加

免責事項テキスト リソースを作成したら、リスナーで受信するメッセージに付加するテキスト文字列を選択します。免責事項テキストをメッセージの上部または下部に追加できます。この機能は、パブリック（インバウンド）リスナーとプライベート（アウトバウンド）リスナーの両方に使用できます。

テキストおよび HTML から構成されるメッセージ（Microsoft Outlook では、このタイプのメッセージを「**multipart alternative**」と呼びます）を送信する場合、Cisco IronPort アプライアンスは、メッセージの両方の部分に免責事項をスタンプします。ただし、メッセージが署名済みのコンテンツである場合、署名が無効になるためコンテンツは変更されません。代わりに、「Content-Disposition inline attachment」という免責条項スタンプを使用して新しい部分が作成されます。マルチパート メッセージの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Message Bodies vs. Message Attachments」を参照してください。

次に、GUI からリスナーのメッセージに適用する免責事項を選択する例を示します。

図 14-13 リスナーに免責事項を含める編集
Add Listener

フィルタからの免責事項の追加

フィルタ アクション `add-footer()` またはコンテンツ フィルタ アクション 「Add Disclaimer Text」を使用して、メッセージの免責事項に特定の事前定義されたテキスト文字列を付加することもできます。たとえば、次のメッセージ フィルタ ルールは、LDAP グループ 「Legal」 のユーザから送信されるすべてのメッセージに、`legal.disclaimer` という名前のテキスト文字列を付加します。

```
Add-Disclaimer-For-Legal-Team:

if (mail-from-group == 'Legal')
{
    add-footer('legal.disclaimer');
}
```

免責事項およびフィルタ アクション変数

メッセージ フィルタ アクション変数を使用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「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照してください）。

免責事項テンプレートには、次の変数を使用できます。

表 14-3 アンチウイルス通知変数

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTimestamp	現在の時刻および日付 (GMT) に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase 評価スコアに置き換えられます。評価スコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイルタイプを示すカンマ区切りリストに置き換えられます。

表 14-3 アンチウイルス通知変数 (続き)

変数	置き換える値
\$filesizes	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。
\$remotehost	メッセージを Cisco IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージ ヘッダーに置き換えられます。
\$EnvelopeFrom	メッセージのエンベロップ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	Cisco IronPort アプライアンスのホスト名に置き換えられます。
\$header['string']	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
\$enveloperecipients	メッセージのエンベロップ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
\$bodysize	メッセージのサイズ (バイト単位) に置き換えられます。
\$FilterName	処理中のフィルタの名前を返します。
\$MatchedContent	スキャン フィルタ ルール (body-contains などのフィルタ ルールやコンテンツ ディクショナリを含む) をトリガーした内容を返します。
\$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
\$DLPSeverity	違反の重大度に置き換えられます。「Low」、 「Medium」、「High」または「Critical」のいずれかです。
\$DLPRiskFactor	メッセージに含まれる機密性の高い情報のリスク係数 (0 ~ 100 のスコア) に置き換えられます。
\$threat_category	フィッシング、ウイルス、詐欺、マルウェアなどの感染フィルタ脅威のタイプに置き換えられます。

表 14-3 アンチウイルス通知変数 (続き)

変数	置き換える値
<code>\$threat_type</code>	感染フィルタ脅威カテゴリのサブカテゴリに置き換えられます。たとえば、チャリティ詐欺、金銭目的のフィッシング、偽の取引などがあります。
<code>\$threat_description</code>	感染フィルタ脅威の説明に置き換えられます。
<code>\$threat_level</code>	メッセージの脅威レベル (スコア 0 ~ 5) に置き換えられます。

メッセージフィルタアクション変数を免責事項で使用するには、(GUI の [Text Resource] ページまたは `textconfig` コマンドから) メッセージの免責事項を作成し、変数を参照します。

```
(running textconfig command)
```

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

```
This message processed at: $Timestamp
```

```
.
```

```
Message disclaimer "legal.disclaimervar" created.
```

```
Current Text Resources:
```

1. legal.disclaimer (Message Disclaimer)
2. legal.disclaimervar (Message Disclaimer)

Choose the operation you want to perform:

- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.

[]>

mail3.example.com>**commit**

次に、新しい免責事項をフィルタに使用します。

Add-Timestamp:

```
if (mail-from-group == 'Legal')  
  
{  
  
    add-footer('legal.disclaimervar');  
  
}
```

`add-footer()` アクションでは、フッターを **inline attachment**、**UTF-8 coded attachment**、**quoted printable attachment** として追加することで、非 ASCII テキストをサポートします。

免責事項スタンプと複数エンコード方式

AsyncOS には、異なる文字エンコード方式を含む免責事項スタンプの動作を変更するために使用される設定値が存在します。デフォルトでは、AsyncOS は電子メール メッセージの本文パート内に添付されるように、免責事項を配置します。localeconfig コマンド内で設定した設定値を使用して、本文パートと免責事項のエンコード方式が異なる場合の動作を設定できます。数個のパートから構成される電子メール メッセージを確認することで、この設定が理解しやすくなります。

To: joe@example.com	ヘッダー
From: mary@example.com	
Subject: Hi!	
<空白行>	
Hello!	本文パート
このメッセージはスキャンされました。	最初の添付パート
Example.zip	2 番目の添付パート

最初の空白行に続くメッセージの本文には、多くの MIME パートが含まれている場合があります。多くの場合、最初のパートは「本文」または「テキスト」と呼ばれ、2 番目以降のパートは「アタッチメント」と呼ばれます。

免責事項は「アタッチメント」（上記の例）または本文の一部として、電子メールに含めることができます。

To: joe@example.com	ヘッダー
From: mary@example.com	
Subject: Hi!	
<空白行>	
Hello!	本文パート
このメッセージはスキャンされました。	本文に含められた免責事項
Example.zip	最初の添付パート

一般的に、メッセージの本文と免責事項の間でエンコード方式の不一致が起こると、免責事項が本文に含まれ（インライン）個別のアタッチメントとして含まれないように、AsyncOS はメッセージ全体をメッセージの本文と同じエンコード方式でエンコードしようとします。つまり、免責事項と本文のエンコード方式が一致する場合、または免責事項のテキストに（本文の）インラインに表示できる文字が含まれている場合は、免責事項はインラインに含められます。たとえば、US-ASCII 文字のみを含む ISO-8859-1 エンコードされた免責事項が生成される可能性があります。結果的に、この免責事項は問題なく「インライン」に表示されます。

ただし、免責事項が本文と組み合わせられない場合、`localeconfig` コマンドを使用し、本文テキストを昇格または変換して免責事項のエンコード方式と一致させるように AsyncOS を設定することで、免責事項をメッセージの本文に含めることができます。

```
example.com> localeconfig
```

```
Behavior when modifying headers: Use encoding of message body
```

```
Behavior for untagged non-ASCII headers: Impose encoding of message body
```

```
Behavior for mismatched footer or heading encoding: Only try encoding from
```

```
message body
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure multi-lingual settings.
```

```
[ ]> setup
```

```
If a header is modified, encode the new header in the same encoding as the message body? (Some MUAs incorrectly handle headers encoded in a different encoding than the body. However, encoding a modified header
```

in the same encoding as the message body may cause certain characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or modified, impose the encoding of the body on the header during processing and final representation of the message?

(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way. Some MUAs handle headers encoded in character sets

that differ from that of the main body in an incorrect way. Imposing the encoding of the body on the header may encode

the header more precisely. This will be used to interpret the content of headers for processing, it will not modify or rewrite the header

unless that is done explicitly as part of the processing.) [Y]>

Footers or headings are added in-line with the message body whenever possible. However, if the footer or heading is encoded differently than the message body, and if imposing a single encoding will cause loss of characters, it will be added as an attachment. The system will always try to use the message body's encoding for the footer or heading. If that fails, and if the message body's encoding is US-ASCII, the system can try to edit the message body to use the footer's or heading's encoding. Should the system try to impose the footer's or headings's encoding on the message body? [N]> **y**

Behavior when modifying headers: Use encoding of message body

Behavior for untagged non-ASCII headers: Impose encoding of message body. Behavior for mismatched footer or heading encoding: Try both body and footer or heading encodings

Choose the operation you want to perform:

- SETUP - Configure multi-lingual settings.

localeconfig コマンドの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。

通知テンプレート

通知テンプレートは、`notify()` および `notify-copy()` フィルタ アクションで使用されます。通知テンプレートには、アンチウイルス通知により使用されるアンチウイルス関連の変数を含む非 ASCII テキストおよびアクション変数を含めることができます（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照）。たとえば、`$Allheaders` アクション変数を使用して、元のメッセージのヘッダーを含めることができます。通知用の **From:** アドレスを設定できます。「[生成されるさまざまなメッセージに対する返信アドレスの設定](#)」(P.15-23) を参照してください。

通知テンプレートを作成したら、コンテンツ フィルタおよびメッセージ フィルタから参照させることができます。図 14-14 は、「`grapewatchers@example.com`」に「`grape_text`」通知が送信されるように `notify-copy()` フィルタ アクションを設定したコンテンツ フィルタを示しています。

図 14-14 コンテンツ フィルタによる通知の例
Edit Content Filter

Edit Filter	
Name:	grapecheck
Currently used by policies:	DEFAULT
Description:	Looking for grapes.
Order:	1
Apply filter:	<input checked="" type="radio"/> If one or more conditions match <input type="radio"/> Only if ALL conditions match
Conditions	
<input type="button" value="Select New Condition..."/> <input type="button" value="Add Condition"/>	
Condition	Delete
body-contains("grape")	
Actions	
<input type="button" value="Select New Action..."/> <input type="button" value="Add Action"/>	
Action	Delete
notify-copy ("grapewatchers@example.com", "Found one!", "", "grape_text")	
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

アンチウイルス通知テンプレート

アンチウイルス通知テンプレートには、次の 2 つのタイプがあります。

- **アンチウイルス通知テンプレート。**アンチウイルス通知テンプレートは、元のメッセージがウイルス通知に添付されていない場合に使用されます。
- **アンチウイルス コンテナ テンプレート。**コンテナ テンプレートは、元のメッセージが添付ファイルとして送信される際に使用されます。

アンチウイルス通知テンプレートは、フィルタの代わりにアンチウイルス エンジンで使用される以外は、基本的に通知テンプレートと同様に使用されます。メール ポリシーの編集集中に送信するカスタム通知を指定できます。アンチウイルス通知用の **From:** アドレスを設定できます。詳細については、「[生成されるさまざまなメッセージに対する返信アドレスの設定](#)」(P.15-23)を参照してください。

カスタム アンチウイルス通知テンプレート

図 14-15 は、カスタム アンチウイルス通知が指定されたメール ポリシーを示しています。

図 14-15 メール ポリシーでのアンチウイルス コンテナ テンプレートの通知例

アンチウイルス通知変数

アンチウイルス通知を作成する際に、表 14-4 に記載されている通知変数を使用できます。

表 14-4 アンチウイルス通知変数

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$AV_VIRUSES	メッセージで発見されたすべてのウイルスのリストに置き換えられます。 "Unix/Apache.Trojan", "W32/Bagel-F"
\$AV_VIRUS_TABLE	パートごとに MIME-Part/Attachment 名とウイルスを示すテーブルに置き換えられます。 "HELLO.SCR": "W32/Bagel-F" <unnamed part of the message>: "Unix/Apache.Trojan"

表 14-4 アンチウイルス通知変数 (続き)

変数	置き換える値
\$AV_VERDICT	アンチウイルスの判定に置き換えられます。
\$AV_DROPPED_TABLE	ドロップされた添付ファイルのテーブルに置き換えられます。各行は、パートまたはファイル名とパートに付随するウイルスのリストにより構成されます。 "HELLO.SCR": "W32/Bagel-f", "W32/Bagel-d" "Love.SCR": "Netsky-c", "W32/Bagel-d"
\$AV_REPAIRED_VIRUSES	発見および修復されたすべてのウイルスのリストに置き換えられます。
\$AV_REPAIRED_TABLE	発見および修復されたすべてのパーツとウイルスのテーブルに置き換えられます。"HELLO.SCR": "W32/Bagel-F"
\$AV_DROPPED_PARTS	ドロップされたファイル名のリストに置き換えられます。 "HELLO.SCR", "CheckThisOut.exe"
\$AV_REPAIRED_PARTS	修復されたファイル名またはパーツのリストに置き換えられます。
\$AV_ENCRYPTED_PARTS	暗号化されたファイル名またはパーツのリストに置き換えられます。
\$AV_INFECTED_PARTS	ウイルスを含むファイルのファイル名のカンマ区切りリストに置き換えられます。
\$AV_UNSCANNABLE_PARTS	スキャンできなかったファイル名またはパーツのリストに置き換えられます。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTimestamp	現在の時刻および日付 (GMT) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

表 14-4 アンチウイルス通知変数 (続き)

変数	置き換える値
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには \$Header を使用します）。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase 評価スコアに置き換えられます。評価スコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。
\$remotehost	メッセージを Cisco IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージ ヘッダーに置き換えられます。
\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	Cisco IronPort アプライアンスのホスト名に置き換えられます。



(注) 変数名は大文字/小文字を区別しません。たとえば、テキストリソースで「\$To」と「\$TO」は同等です。元のメッセージで「AV_」変数が空の場合、文字列 <None> で置き換えられます。

テキストリソースを定義した後、[Mail Policies] > [Incoming/Outgoing Mail Policies] > [Edit Anti-Virus Settings] ページまたは `policyconfig -> edit -> antivirus` コマンドを使用して、修復されたメッセージ、スキャンできなかったメッセージ、暗号化されたメッセージ、またはウイルスが陽性のメッセージに対して、元のメッセージが RFC 822 のアタッチメントとして含まれるように指定します。詳細については、「[カスタムのアラート通知の送信 \(受信者宛のみ\)](#)」(P.9-19) を参照してください。

バウンス通知および暗号化失敗通知テンプレート

バウンス通知および暗号化失敗通知テンプレートは、バウンス通知およびメッセージ暗号化失敗通知で使用される以外は、基本的に通知テンプレートと同様に使用されます。暗号化プロファイルを編集時に、バウンスプロファイルおよびカスタムメッセージ暗号化失敗通知を編集していた場合に送信するカスタムバウンス通知を指定できます。

図 14-16 は、バウンスプロファイルで指定されたバウンス通知テンプレートを示しています。

図 14-16 バウンスプロファイルのバウンス通知の例



(注) カスタムテンプレートを使用する場合は、RFC-1891 の DSN を使用してください。

図 14-17 は、暗号化プロファイルで指定された暗号化失敗テンプレートを示しています。

図 14-17 暗号化プロファイルの暗号化失敗通知の例



バウンス通知および暗号化失敗通知変数

バウンス通知または暗号化失敗通知を作成する際に、表 14-5 に記載されている通知変数を使用できます。

表 14-5 バウンス通知変数

変数	置き換える値
\$Subject	元のメッセージの件名。
\$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
\$Time	現在の時刻（ローカル時間帯）に置き換えられます。
\$GMTTimeStamp	現在の時刻および日付（GMT）に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには \$Header を使用します）。
\$BouncedRecipient	バウンスされた受信者のアドレス。
\$BounceReason	通知理由。
\$remotehost	メッセージを Cisco IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。

DLP 通知テンプレート

DLP 通知テンプレートは、RSA Email DLP 機能を使用するようにアプライアンスを設定した際に使用されます。通知では、発信メッセージが企業のデータ消失防止ポリシーに違反した機密性の高いデータを含んでいる可能性があることを受信者に知らせます。DLP Policy Manager で DLP ポリシーを編集している間に、カスタム DLP 通知を指定できます。

図 14-18 は、DLP ポリシーで使用されている DLP 通知テンプレートの例を示しています。

図 14-18 DLP ポリシーでイネーブルになっている DLP 通知テンプレート

DLP 通知変数

DLP 通知テンプレートでは、次の変数を使用できます。

表 14-6 DLP 通知変数

変数	置き換える値
\$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
\$DLPSeverity	違反の重大度に置き換えられます。「Low」、「Medium」、「High」または「Critical」のいずれかです。
\$DLPRiskFactor	メッセージに含まれる機密性の高い情報のリスク係数 (0 ~ 100 のスコア) に置き換えられます。

表 14-6 DLP 通知変数 (続き)

変数	置き換える値
\$To	メッセージの To: ヘッダーに置き換えられます (エンベロープ受信者には置き換えられません)。
\$From	メッセージの From: ヘッダーに置き換えられます (エンベロープ送信者には置き換えられません)。
\$Subject	元のメッセージの件名に置き換えられます。
\$Date	現在の日付 (MM/DD/YYYY 形式) に置き換えられます。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$GMTimestamp	現在の時刻および日付 (GMT) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
\$MID	メッセージを識別するために内部的に使用されるメッセージ ID または「MID」に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください (「Message-Id」を取得するには \$Header を使用します)。
\$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
\$Reputation	送信者の SenderBase 評価スコアに置き換えられます。評価スコアがない場合は「None」に置き換えられます。
\$filenames	メッセージの添付ファイルのファイル名を示すカンマ区切りリストに置き換えられます。
\$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
\$filesizes	メッセージの添付ファイルのファイル サイズを示すカンマ区切りリストに置き換えられます。
\$remotehost	メッセージを Cisco IronPort アプライアンスに送信したシステムのホスト名に置き換えられます。
\$AllHeaders	メッセージ ヘッダーに置き換えられます。

表 14-6 DLP 通知変数 (続き)

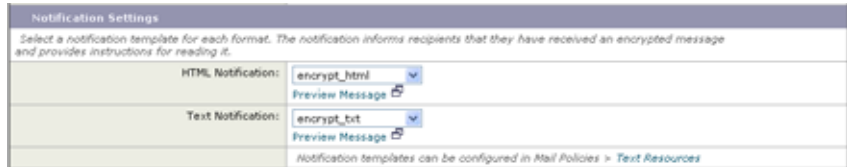
変数	置き換える値
\$EnvelopeFrom	メッセージのエンベロープ送信者 (Envelope From、<MAIL FROM>) に置き換えられます。
\$Hostname	Cisco IronPort アプライアンスのホスト名に置き換えられます。
\$bodysize	メッセージのサイズ (バイト単位) に置き換えられます。
\$header['string']	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
\$remoteip	メッセージを Cisco IronPort アプライアンスに送信したシステム IP アドレスに置き換えられます。
\$recvlistener	メッセージを受信したリスナーのニックネームに置き換えられます。
\$dropped_filenames	\$filenames と同様に、ドロップされたファイルのリストを表示します。
\$dropped_filename	直近にドロップされたファイル名のみを返します。
\$recvint	メッセージを受信したインターフェイスのニックネームに置き換えられます。
\$timestamp	現在の時刻および日付 (ローカル時間帯) に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
\$Time	現在の時刻 (ローカル時間帯) に置き換えられます。
\$orgid	SenderBase 組織 ID (整数値) で置き換えられます。
\$enveloperecipients	メッセージのエンベロープ受信者すべて (Envelope To、<RCPT TO>) に置き換えられます。
\$dropped_filetypes	\$filetypes と同様に、ドロップされたファイルタイプのリストを表示します。
\$dropped_filetype	直近にドロップされたファイルのファイルタイプのみを返します。

暗号化通知テンプレート

暗号化通知テンプレートは、アウトバウンド電子メールを暗号化するように Cisco IronPort 電子メール暗号化を設定した際に使用されます。この通知では、受信者が暗号化されたメッセージを受信したことを通知し、メッセージを読む手順を説明しています。暗号化メッセージと一緒に送信するカスタム暗号化通知を指定できます。暗号化プロファイルを作成する際は、HTML 形式およびテキスト形式の両方の暗号化通知を指定します。このため、カスタム プロファイルを作成する場合は、テキスト形式および HTML 形式の両方の通知を作成する必要があります。

図 14-19 は、暗号化プロファイルで指定された暗号化通知を示しています。

図 14-19 暗号化プロファイルでイネーブルになっている暗号化通知テンプレート





CHAPTER 15

システム管理

一般的なシステム管理は、主に Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) の [System Administration] メニューから実行します。一部のシステム管理機能は、Command Line Interface (CLI; コマンドライン インターフェイス) のみからアクセスできます。

さらに、Cisco IronPort のグラフィカル ユーザ インターフェイス (GUI) から、Cisco IronPort アプライアンスのシステム モニタリング機能にアクセスすることもできます ([「Other Tasks in the GUI」 \(P.441\)](#) を参照)。



(注)

このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、[「IP アドレス、インターフェイス、およびルーティング」 \(P.B-4\)](#) を参照してください。

この章は、次の内容で構成されています。

- [「AsyncOS のアップグレード」 \(P.15-2\)](#)
- [「AsyncOS の復元」 \(P.15-12\)](#)
- [「サービスのアップデート」 \(P.15-16\)](#)
- [「生成されるさまざまなメッセージに対する返信アドレスの設定」 \(P.15-23\)](#)
- [「アラート」 \(P.15-24\)](#)
- [「ネットワーク設定値の変更」 \(P.15-60\)](#)
- [「システム時刻」 \(P.15-75\)](#)

AsyncOS のアップグレード

アップグレードする前に

AsyncOS をアップグレードするには、次の 2 つの手順を実行します。

ステップ 1 アップグレード設定値を設定します。電子メール セキュリティ アプライアンスがアップグレード情報をダウンロードする方法に関する設定値を設定します。たとえば、アップグレード イメージのダウンロード元の選択などが含まれます。詳細については、「[GUI からのアップグレード設定値の設定](#)」(P.15-10) を参照してください。

ステップ 2 AsyncOS をアップグレードします。アップグレード設定値を設定した後は、アプライアンスの AsyncOS のバージョンをアップグレードします。詳細については、「[GUI からの AsyncOS のアップグレード](#)」(P.15-3) および「[CLI からの AsyncOS のアップグレード](#)」(P.15-4) を参照してください。

ベスト プラクティスとして、アップグレードの準備に次の手順を実行することを推奨します。

ステップ 1 XML コンフィグ ファイルのオフボックスを保存します。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合、リストのオフボックスをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。CLI からのアップグレードを実行する場合は、suspendlistener コマンドを使用します。GUI からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。

ステップ 4 キューが空になるまで待ちます。CLI の workqueue コマンドで作業キュー内のメッセージ数を表示するか、rate コマンドでアプライアンスのメッセージ スループットをモニタすることができます。



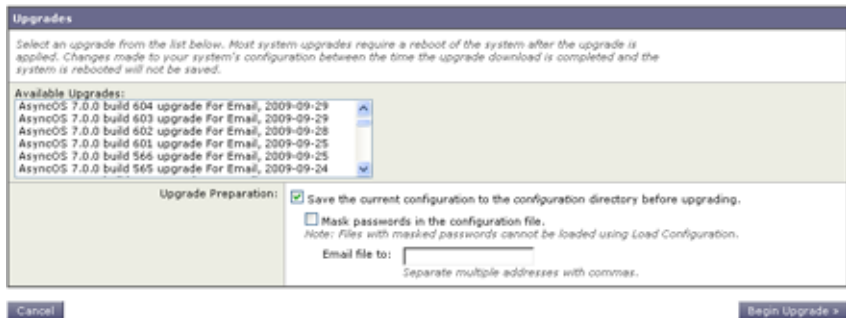
(注) アップグレード後、再びリスナーをイネーブルにします。

GUI からの AsyncOS のアップグレード

アップデート設定値を設定した後に AsyncOS をアップグレードするには、次の手順を実行します。

- ステップ 1** [System Administration] > [System Upgrade] ページで、[Available Upgrades] をクリックします。[Available Upgrades] ページが表示されます。

図 15-1 [Available Upgrades] ページ
Available Upgrades



- ステップ 2** 利用可能なアップグレードのリストから、アップグレードを選択します。
- ステップ 3** 現在の設定を configuration ディレクトリに保存するかどうかを選択します。
- ステップ 4** コンフィギュレーション ファイルでパスワードをマスクするかどうかを選択します。



(注) マスクされたパスワードが記載されたコンフィギュレーション ファイルは、GUI の [Configuration File] ページや CLI の loadconfig コマンドからロードできません。

- ステップ 5** コンフィギュレーション ファイルのコピーを電子メールで送信する場合は、ファイルの送信先の電子メールアドレスを入力します。複数の電子メールアドレスを指定する場合は、カンマで区切ります。
- ステップ 6** [Begin Upgrade] をクリックします。ページの上部の近くに、経過表示バーが表示されます。変更の確定や新しいライセンス契約書への合意などを 1 回以上求められる場合があります。

- ステップ 7** アップグレードが完了すると、アプライアンスをリブートするように求められます。
- ステップ 8** [Reboot Now] をクリックします。

CLI からの AsyncOS のアップグレード

upgrade コマンドを発行して、利用可能なアップグレードのリストを表示します。リストから目的のアップグレードを選択して、インストールします。メッセージの確認やライセンス契約書への合意などを求められる場合があります。現在の設定を configuration ディレクトリに保存するかどうかを選択できます。保存する場合、コンフィギュレーション ファイルでパスワードをマスクするかどうかを選択します。コンフィギュレーション ファイルのコピーを電子メールで送信するかどうかを選択します。



(注) マスクされたパスワードが記載されたコンフィギュレーション ファイルは、loadconfig コマンドからロードできません。

アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。

従来のアップグレード方法との違い

従来の方法と比較して、ローカル サーバから AsyncOS をアップグレードする際は、次の違いがあることに注意してください。

- ステップ 1** ダウンロード中に、アップグレードによるインストールがすぐに実行されます。アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間に Ctrl キーを押した状態で C キーを押して、ダウンロードが開始する前にアップグレードプロセスを終了することもできます。

AsyncOS アップグレード設定値の設定

電子メール セキュリティ アプライアンスが AsyncOS アップグレードをダウンロードする方法を設定します。IronPort では、ストリーミング アップグレードとリモート アップグレードの 2 つの方法（または「ソース」）を用意しています。

ストリーミング アップグレードでは、Cisco IronPort アプライアンスは直接 Cisco IronPort アップデート サーバから AsyncOS アップグレードをダウンロードします。各 Cisco IronPort アプライアンスは、個別にアップグレードをダウンロードします。詳細については、「[ストリーミング アップグレードの概要](#)」(P.15-6) を参照してください。

リモート アップグレードでは、Cisco IronPort アプライアンスはネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。アップグレードイメージを IronPort から一度だけダウンロードし、その後イメージを Cisco IronPort アプライアンスに供給します。詳細については、「[リモート アップグレードの概要](#)」(P.15-7) を参照してください。

[Security Services] > [Service Updates] ページを使用して、2 つのアップグレード方法を切り替えるとともに（デフォルトはストリーミング アップグレード）、アップグレードとプロキシサーバ設定をダウンロードするために使用するインターフェイスを設定します。詳細については、「[GUI からのアップグレード設定値の設定](#)」(P.15-10) を参照してください。オプションで、CLI の `updateconfig` コマンドを使用することもできます。

図 15-2 [Service Updates] ページ
Service Updates

Update Settings for Security Services	
Update Server (images):	Dynamic (IronPort Update Server)
Update Server (list):	Dynamic (IronPort Update Server)
Automatic Updates:	Enabled
Update Interval:	5m
Interface:	Auto Select
HTTP Proxy Server:	Not Enabled
HTTPS Proxy Server:	Not Enabled



(注) 使用するアップグレード方法を問わず、アップグレードが完了した後に `saveconfig` コマンドで設定を保存することも検討してください。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「[Managing the Configuration File](#)」を参照してください。

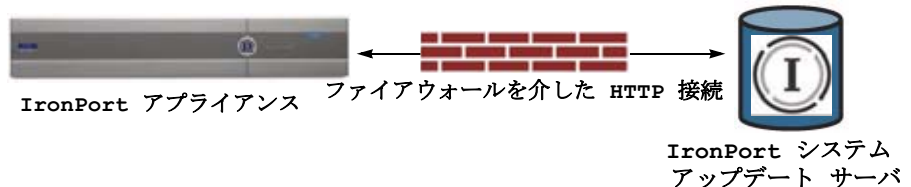
クラスタ化されたシステムのアップグレード

クラスタ化されたマシンをアップグレードする場合は、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Centralized Management」の章の「Upgrading Machines in a Cluster」を参照してください。

ストリーミングアップグレードの概要

ストリーミングアップグレードでは、Cisco IronPort アプライアンスは直接 IronPort アップデート サーバに接続して、アップグレードを検索してダウンロードします。

図 15-3 ストリーミングアップデートの方法



Cisco IronPort Systems では分散アップグレードサーバアーキテクチャを使用して、世界中のお客様が AsyncOS アップグレードをすぐにダウンロードできるようにしています。この分散サーバアーキテクチャにより、Cisco IronPort アップデートサーバはダイナミック IP アドレスを使用します。ファイアウォールポリシーを厳しく設定している場合、AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。詳細については、「[ストリーミングアップグレード用のスタティックアドレスの設定](#)」(P.15-7)を参照してください。

ポート 80 および 443 による Cisco IronPort アップデートサーバからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成する必要があります。ポート 22、25、80、4766 などによる `upgrades.ironport.com` からのレガシーアップグレードのダウンロードを許可するファイアウォールのルールがすでに設定されている場合、そのルールを削除するか、修正したファイアウォールのルールで置き換えるか、もしくはこの両方の必要があります。詳細については、[付録 C 「ファイアウォール情報」](#)を参照してください。

ストリーミング アップグレード用のスタティック アドレスの設定

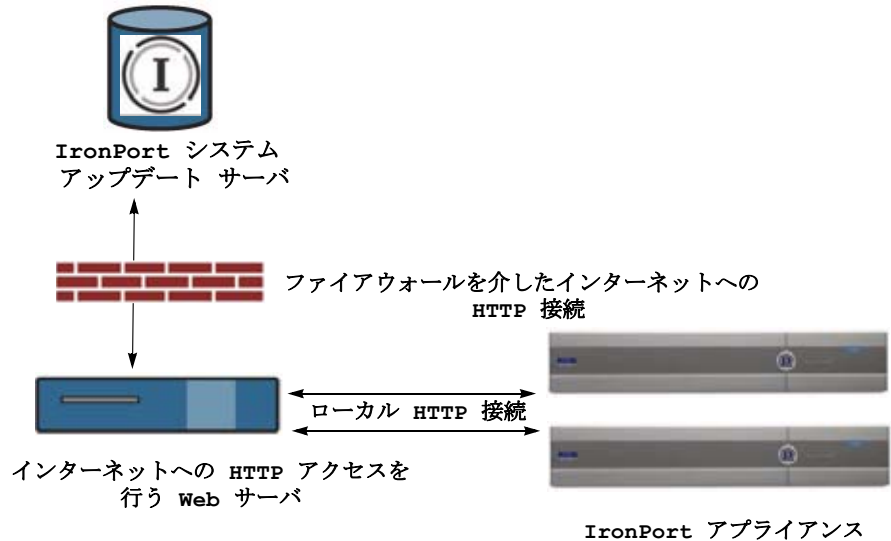
McAfee Anti-Virus および Cisco IronPort AsyncOS アップデート サーバでは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。アップデートに関して、ファイアウォール設定にスタティック IP アドレスが必要だと判断した場合、次の手順を実行します。

- ステップ 1** Cisco IronPort カスタマー サポートに問い合わせ、スタティック URL アドレスを取得します。
- ステップ 2** ポート 80 によるスタティック IP アドレスからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成します。
- ステップ 3** [Security Services] > [Service Updates] ページに移動し、[Edit Update Settings] をクリックします。
- ステップ 4** [Edit Update Settings] ページの [Update Servers (images)] セクションで、[Local Update Servers] を選択し、ステップ 1 で受け取った AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのスタティック URL を [Base URL] フィールドに入力します。
- ステップ 5** IronPort アップデート サーバが [Update Servers (list)] セクションで選択されていることを確認します。
- ステップ 6** 変更を送信して確定します。

リモート アップグレードの概要

直接 Cisco IronPort アップデート サーバからアップグレードを取得するのではなく、AsyncOS アップグレード イメージをローカル サーバにダウンロードし、所有するネットワーク内からアップグレードをホスティングできます。この機能を使用して、インターネットにアクセスできるネットワーク上のすべてのサーバに HTTP でアップグレード イメージをダウンロードします。アップデート イメージのダウンロードを選択した場合、内部 HTTP サーバ（「アップデート マネージャ」）を設定して AsyncOS イメージを Cisco IronPort アプライアンスにホスティングできます。

図 15-4 リモート アップデートの方法



基本プロセスは次のとおりです。

- ステップ 1** アップグレード ファイルを取得および供給するようにローカル サーバを設定します。
- ステップ 2** アップグレード ファイルをダウンロードします。
- ステップ 3** GUI の [Security Services] > [Service Updates] ページまたは CLI の `updateconfig` コマンドのいずれかを使用して、ローカル サーバを使用するようにアプライアンスを設定します。
- ステップ 4** [System Administration] > [System Upgrade] ページまたは CLI の `upgrade` コマンドのいずれかを使用して、アプライアンスをアップグレードします。

リモート アップグレードに関するハードウェアおよびソフトウェア要件

AsyncOS アップグレード ファイルのダウンロードでは、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- Cisco IronPort Systems アップデート サーバへのインターネット アクセス。
- Web ブラウザ ([「ブラウザ要件」\(P.2-2\)](#) を参照)。

**(注)**

今回のリリースでアップデート サーバのアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用する必要があります。

AsyncOS アップデート ファイルのホスティングでは、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- **Web サーバ**：たとえば、Microsoft Internet Information Services (IIS; インターネット インフォメーション サービス) または Apache オープン ソースサーバでは、次の要件を満たしている必要があります。
 - 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
 - ディレクトリの参照ができること
 - 匿名認証（認証不要）または基本（「シンプル」）認証の設定ができること
 - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

リモート アップグレード イメージのホスティング

ローカル サーバの設定が完了したら、

http://updates.ironport.com/fetch_manifest.html にアクセスしてアップグレード イメージの ZIP ファイルをダウンロードします。イメージをダウンロードするには、Cisco IronPort アプライアンスのシリアル番号とバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレードのバージョンをクリックし、ディレクトリ構造を変更せずにローカル サーバのルート ディレクトリにある ZIP ファイルを解凍します。アップグレード イメージを使用するには、[Edit Update Settings] ページで（または CLI の `updateconfig` を使用して）ローカル サーバを使用するようにアプライアンスを設定します。

ローカル サーバは、ネットワーク上の Cisco IronPort アプライアンスで利用可能な AsyncOS アップグレードをダウンロード済みのアップグレード イメージに限定する XML ファイルもホスティングします。このファイルは「マニフェスト」と呼ばれます。マニフェストはアップグレード イメージの ZIP ファイルの `asyncos` ディレクトリに配置されています。ローカル サーバのルート ディレク

トリにある ZIP ファイルを解凍したら、[Edit Update Settings] ページで（または CLI の `updateconfig` を使用して）、XML ファイルの完全な URL（ファイル名を含む）を入力します。

リモート アップグレードの詳細については、Cisco IronPort ナレッジ ベースを参照するか、Cisco IronPort サポート プロバイダーにお問い合わせください。



(注)

ローカル アップデート サーバは AsyncOS アップグレード イメージ専用で使用し、セキュリティ アップデート イメージには使用しないでください。ローカル アップデート サーバを指定した場合、ローカル サーバは IronPort からアップデートされたセキュリティ アップデートを自動的に受信しないため、ネットワーク上のアプライアンスはいずれ古くなります。AsyncOS のアップグレード用にローカル アップデート サーバを使用して、アップデートおよびアップグレード用の設定値を再び Cisco IronPort アップデート サーバを使用するように変更してください。セキュリティ サービスが再び自動的にアップデートされるようになります。

GUI からのアップグレード設定値の設定

アップデート設定には、AsyncOS アップグレードのソース（リモートまたはストリーミング）、アップグレードのダウンロードに使用するインターフェイス、およびプロキシ サーバ設定が含まれています。AsyncOS のアップグレードに加えて、アンチスパム サービス、アンチウイルス サービス、および感染フィルタ サービスなどさまざまな Cisco IronPort サービスの設定値も編集できます。アップデート サービスの詳細については、「[サービスのアップデート](#)」(P.15-16) を参照してください。

AsyncOS アップグレード設定を編集するには、次の手順を実行します。

- ステップ 1** [Security Services] > [Service Updates] ページで、[Edit Update Settings] をクリックします。
[Edit Update Settings] ページが表示されます。
- ステップ 2** AsyncOS アップグレード イメージを Cisco IronPort アップデート サーバからダウンロードするか、またはローカル サーバからダウンロードするかを選択します。

ローカル サーバを選択した場合、AsyncOS アップグレード イメージをホスティングするローカル サーバのベース URL を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。



(注) AsyncOS アップグレードにローカル サーバを指定した場合、ローカル サーバは IronPort からアップデートされた McAfee Anti-Virus 定義ファイルを自動的に受信しないため、ネットワーク上のアプライアンスはいずれ古くなります。アップグレード後に設定値を再び Cisco IronPort アップグレード サーバを使用するように変更してください。McAfee Anti-Virus 定義ファイルが再び自動的にアップデートされるようになります。

- ステップ 3** ローカル サーバからの AsyncOS アップグレード イメージのダウンロードを選択した場合は、利用可能なアップデートのリスト（マニフェスト XML ファイル）のソースとするローカル サーバを選択します。マニフェストの完全な URL（ファイル名と HTTP ポート番号を含む）を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。
- ステップ 4** アップグレードに使用するインターフェイスを選択します。
- ステップ 5** 必要に応じて、HTTP プロキシ サーバまたは HTTPS プロキシ サーバの情報を入力します。
- ステップ 6** 変更を送信して確定します。

CLI からのアップグレード設定値の設定

AsyncOS アップグレードを取得する場所（ローカル サーバまたは Cisco IronPort サーバ）をアプライアンスに設定するには、`updateconfig` コマンドを実行します。アップグレードをインストールするには、`upgrade` コマンドを実行します。

updateconfig コマンド

`updateconfig` コマンドは、AsyncOS アップグレードを含むサービス アップデートを参照する場所を Cisco IronPort アプライアンスに設定するために使用されます。デフォルトでは、`upgrade` コマンドを入力すると、アプライアンスは Cisco IronPort アップグレード サーバに最新のアップデートを問い合わせます。

リモート アップグレードの場合、`updateconfig` コマンドを発行して、アプライアンスがローカル アップデート サーバ（上記で設定したローカル サーバ）を使用するように設定します。



(注) `ping` コマンドを使用して、アプライアンスがローカル サーバに接続できることを確認できます。また、`telnet` コマンドを使用してローカル サーバのポート 80 に Telnet 接続することで、ローカル サーバが該当のポートをリッスンしていることが確認できます。

AsyncOS の復元

AsyncOS には、緊急時に AsyncOS オペレーティング システムを以前の認定済みのビルドに戻す機能があります。



(注) AsyncOS 7.0 にアップグレードした後は、バージョン 6.5 よりも前の AsyncOS には戻せません。

利用可能なバージョン

アップグレードは主要なサブシステムを一方向に変換するため、復元プロセスは複雑で、Cisco IronPort Quality Assurance チームによる認定が必要です。IronPort では、AsyncOS バージョンに対して固有のバージョンの CASE、Sophos、感染フィルタを認証しています。以前のすべてのバージョンの AsyncOS オペレーティング システムが復元に利用できるわけではありません。最初にこの機能がサポートされた AsyncOS バージョンは AsyncOS 5.5.0 です。これより以前のバージョンの AsyncOS はサポートされていません。

復元の影響に関する重要な注意事項

Cisco IronPort アプライアンスにおける `revert` コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての設定ログおよびデータベースを破壊します。管理インターフェイスのネットワーク情報のみが保存されます。他のすべてのネットワーク設定は削除されます。さらに、復元はアプライアンスが再

設定されるまでメール処理を中断します。このコマンドはネットワーク設定を破壊するため、`revert` コマンドを発行する場合は Cisco IronPort アプライアンスへの物理的なローカル アクセスが必要になります。



警告

戻し先のバージョンのコンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルに下位互換性は**ありません**。

AsyncOS 復元の実行

`revert` コマンドを実行するには、次の手順を実行します。

- ステップ 1** 戻し先のバージョンのコンフィギュレーション ファイルがあることを確認してください。コンフィギュレーション ファイルに下位互換性は**ありません**。コンフィギュレーション ファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。簡単な方法は、CLI の `mailconfig` コマンドを実行する方法です。
- ステップ 2** アプライアンスの現在の設定のバックアップ コピーを、(パスワードをマスクしない状態で) 別のマシンに保存します。



(注) このコピーは、バージョンを戻した後にロードするコンフィギュレーション ファイルではありません。

- ステップ 3** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。
- ステップ 4** メール キューが空になるまで待ちます。
- ステップ 5** バージョンを戻すアプライアンスの CLI にログインします。

`revert` コマンドの実行時には、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないでください。

- ステップ 6** CLI から `revert` コマンドを発行します。



(注) 復元プロセスは時間のかかる処理です。復元が完了して、Cisco IronPort アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ~ 20 分かかります。

次に、revert コマンドの例を示します。

```
mail.mydomain.com> revert
```

```
This command will revert the appliance to a previous version of AsyncOS.
```

```
WARNING: Reverting the appliance is extremely destructive.
```

```
The following data will be destroyed in the process:
```

- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all IronPort Spam Quarantine message and end-user safelist/blocklist data

```
Only the network settings will be preserved.
```

```
Before running this command, be sure you have:
```

- saved the configuration file of this appliance (with passwords unmasked)
- exported the IronPort Spam Quarantine safelist/blocklist database to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.

After rebooting, the appliance reinitializes itself and reboots again to the desired version.

Do you want to continue?

Are you *really* sure you want to continue? yes

Available version	Install date
=====	=====
Available version	Install date
1. 5.5.0-236	Tue Aug 28 11:03:44 PDT 2007
2. 5.5.0-330	Tue Aug 28 13:06:05 PDT 2007
3. 5.5.0-418	Wed Sep 5 11:17:08 PDT 2007

Please select an AsyncOS version: 2

You have selected "5.5.0-330".

The system will now reboot to perform the revert operation.

- ステップ 7** アプライアンスは 2 回リブートします。
- ステップ 8** マシンが 2 回リブートしたら、シリアル コンソールで `interfaceconfig` コマンドを使用して、アクセス可能な IP アドレスをインターフェイスに設定します。
- ステップ 9** 設定したインターフェイスの 1 つで FTP または HTTP をイネーブルにします。
- ステップ 10** 作成した XML コンフィギュレーション ファイルを FTP で取得するか、または GUI インターフェイスに貼り付けます。
- ステップ 11** 戻し先のバージョンの XML コンフィギュレーション ファイルをロードします。
- ステップ 12** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースをインポートして復元します。
- ステップ 13** 変更を確定します。
復元が完了した Cisco IronPort アプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

サービスのアップデート

Cisco IronPort アプライアンスがさまざまなサービス（アンチスパム、アンチウイルス、感染フィルタ サービスなど）をアップデートする方法の設定には、多くの設定値が使用されています。これらの設定値には、[Security Services] メニューの [Service Updates] ページ、または CLI の `updateconfig` コマンドからアクセスできます。

[Service Updates] ページ

[Service Updates] ページ（GUI の [Security Services] メニューから利用可能）では、Cisco IronPort アプライアンスのさまざまなサービスのアップデートに関する現在の設定値を表示します。アップデート設定には、アップデート サーバ（イメージ）、アップデート サーバ（リスト）、さまざまなコンポーネントのアップデート URL、自動アップデートのイネーブル化、自動アップデート間隔、HTTP プロキシ サーバおよび HTTPS プロキシ サーバが含まれます。



(注) Cisco IronPort アップデート サーバでは、**ダイナミック IP アドレス**を使用します。ファイアウォール ポリシーを厳しく設定している場合、セキュリティ コンポーネント アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。アップデートおよびアップグレードに関して、ファイアウォール設定にスタティック IP アドレスが必要だと判断した場合、次の指示に従ってアップデート設定値を編集し、Cisco IronPort カスタマーサポートに必要な URL アドレスを問い合わせで取得します。

アップデート設定値の編集

Cisco IronPort アプライアンスのアップデート設定値を編集するには、[Edit Update Settings] ボタンをクリックします。[Update Servers (images)]、[Update Servers (list)]、[Automatic Updates]、[Interface]、および [Proxy Servers] の設定値を設定します。アップデート設定値の詳細については、[表 15-1 \(P.15-20\)](#) を参照してください。

図 15-5 は、アップデート サーバの利用可能な設定値を示しています。

図 15-5 イメージおよびリストに関するアップデート サーバの設定値

<p>Update Servers (images):</p>	<p>The update servers will be used to obtain update images for the following services:</p> <ul style="list-style-type: none"> - Feature Key updates - McAfee Anti-Virus definitions - PXE Engine updates - Sophos Anti-Virus definitions - IronPort Anti-Spam rules - Outbreak Filters rules - Time zone rules - IronPort AsyncOS upgrades <p>IronPort Update Servers</p> <p>Local Update Servers (location of update image files)</p> <p>Base Url (Feature Key updates): <input type="text" value="http://downloads.ironport.com/"/> Port: <input type="text" value="80"/> Ex. http://downloads.example.com</p> <p>Authentication (optional):</p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Retype Password: <input type="password"/></p> <p>Host (McAfee Anti-Virus definitions, PXE Engine updates, Sophos Anti-Virus definitions, IronPort Anti-Spam rules, Outbreak Filters rules, IronPort AsyncOS upgrades): <input type="text" value="downloads.example.com"/> Port: <input type="text" value="80"/> (optional) Ex. downloads.example.com</p>
<p>Update Servers (list):</p>	<p>The URL will be used to obtain the list of available updates for the following services:</p> <ul style="list-style-type: none"> - McAfee Anti-Virus definitions - PXE Engine updates - Sophos Anti-Virus definitions - IronPort Anti-Spam rules - Outbreak Filters rules - Time zone rules - IronPort AsyncOS upgrades <p>IronPort Update Servers</p> <p>Local Update Servers (location of list of available updates file)</p> <p>Full Url <input type="text" value="http://updates.example.com/my_updates.xml"/> Port: <input type="text" value="80"/> Ex. http://updates.example.com/my_updates.xml</p> <p>Authentication (optional):</p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Retype Password: <input type="password"/></p>

図 15-6 は、[Automatic Updates] および [Interface] で利用可能な設定値を示しています。

図 15-6 [Automatic Updates] および [Interfaces] の設定値

<p>Automatic Updates:</p>	<p><input type="checkbox"/> Enable automatic updates for McAfee Anti-Virus definitions, PXE Engine updates, Sophos Anti-Virus definitions, IronPort Anti-Spam rules, Outbreak Filters rules, Time zone rules</p> <p>Update Interval: <input type="text" value="5m"/></p>
<p>Interface:</p>	<p><input type="text" value="Auto Select"/></p> <p>Interface section applies only to McAfee Anti-Virus definitions, PXE Engine updates, Sophos Anti-Virus definitions, IronPort Anti-Spam rules, Outbreak Filters rules, Time zone rules and IronPort AsyncOS upgrades</p>

図 15-7 は、プロキシ サーバの利用可能な設定値を示しています。

図 15-7 プロキシ サーバの設定値

Proxy Servers (optional):	HTTP Proxy Server	
	If an HTTP proxy server is defined it will be used to update the following services:	
	- Feature Key updates	
	- McAfee Anti-Virus definitions	
	- FXE Engine updates	
	- Sophos Anti-Virus definitions	
	- IronPort Anti-Spam rules	
	- Outbreak Filters rules	
	- Time zone rules	
	- IronPort AsyncOS upgrades	
	HTTP Proxy Name:	<input type="text"/> Port: <input type="text" value="80"/>
	Username:	<input type="text"/>
	Password:	<input type="text"/>
	Retype Password:	<input type="text"/>
HTTPS Proxy Server		
If an HTTPS proxy server is defined it will be used to update the following services:		
- McAfee Anti-Virus definitions		
- FXE Engine updates		
- Sophos Anti-Virus definitions		
- IronPort Anti-Spam rules		
- Outbreak Filters rules		
- Time zone rules		
- IronPort AsyncOS upgrades		
- SenderBase Network Participation sharing		
HTTPS Proxy Name:	<input type="text"/> Port: <input type="text" value="443"/>	
Username:	<input type="text"/>	
Password:	<input type="text"/>	
Retype Password:	<input type="text"/>	

表 15-1 に、設定可能なアップデート設定値を示します。

表 15-1 アップデート設定値

設定	説明
Update Servers (images)	<p>サービス アップデート イメージおよび Cisco IronPort AsyncOS アップグレード イメージを IronPort アップデート サーバからダウンロードするか、またはローカル Web サーバからダウンロードするかを選択します。</p> <p>デフォルトは、IronPort アップデート サーバです。これらのサーバは AsyncOS アップグレードのほかにも、Sophos および McAfee Anti-Virus 定義ファイル、IronPort Anti-Spam および IronPort Intelligent Multi-Scan ルール、感染フィルタルール、時間帯ルール、機能キーのアップデート、および PXE Engine のアップデートに関するアップデート イメージの取得に使用されます。</p> <p>次の条件のいずれかが該当する場合は、ローカル Web サーバを選択します。</p> <ul style="list-style-type: none"> • IronPort からアップグレード イメージおよびアップデート イメージをダウンロードする際に、Cisco IronPort カスタマー サポートから提供されるスタティック アドレスを入力する必要がある場合。 • 一時的に、ローカル Web サーバに保存されたアップグレード イメージをダウンロードする場合。イメージをダウンロードした後は、セキュリティ コンポーネントが引き続き自動アップデートできるように、この設定を再び IronPort アップデート サーバ（または使用していたスタティック アドレス）に戻すことを推奨します。 <p>ローカル アップデート サーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。</p> <p>(注) IronPort Intelligent Multi-Scan でサードパーティのアンチスパム ルールのアップデートをダウンロードするには、別のローカル サーバが必要です。</p>

表 15-1 アップデート設定値 (続き)

設定	説明
Update Servers (lists)	<p>利用可能なアップデートのリスト (マニフェスト XML ファイル) を IronPort アップデート サーバからダウンロードするか、またはローカル Web サーバからダウンロードするかを選択します。マニフェスト XML ファイルには、AsyncOS アップグレードのほかに McAfee Anti-Virus や PXE Engine などのさまざまなセキュリティ コンポーネントのアップデートが含まれます。</p> <p>デフォルトは、IronPort アップデート サーバです。一時的に、ローカル Web サーバに保存されたアップグレード イメージをダウンロードする場合は、ローカル Web サーバを選択します。イメージをダウンロードした後は、セキュリティ コンポーネントが引き続き自動アップデートできるように、この設定を再び IronPort アップデート サーバに戻すことを推奨します。</p> <p>ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。</p> <p>詳細については、「リモート アップグレードの概要」(P.15-7) を参照してください。</p>
Automatic Updates	<p>Sophos および McAfee Anti-Virus 定義ファイル、IronPort Anti-Spam ルール、IronPort Intelligent Multi-Scan ルール、PXE Engine アップデート、感染フィルタ ルール、時間帯ルールに対する自動アップデートとアップデート間隔 (アプライアンスがアップデートを確認する頻度) をイネーブルにします。</p>
Interface	<p>表示されているセキュリティ コンポーネントのアップデートおよび Cisco IronPort AsyncOS アップグレードをアップデート サーバに問い合わせる際に使用するネットワーク インターフェイスを選択します。利用可能なプロキシ データ インターフェイスが表示されます。デフォルトでは、アプライアンスは使用するインターフェイスを選択します。</p>
HTTP Proxy Server	<p>GUI に表示されているサービスで使用されるオプションのプロキシ サーバ。</p> <p>プロキシ サーバを指定すると、これらのすべてのサービスで指定したプロキシ サーバが使用されることに注意してください。</p>

表 15-1 アップデート設定値 (続き)

設定	説明
HTTPS Proxy Server	HTTPS を使用したオプションのプロキシ サーバ。HTTPS プロキシ サーバを定義すると、GUI に表示されているサービスのアップデートで使用されます。

アップデート サーバの設定

Cisco IronPort アプライアンスのアップデート サーバを設定するには、次の手順を実行します。

- ステップ 1** IronPort アップデート サーバまたはローカル アップデート サーバのいずれかから、サービスのアップデート イメージを取得するサーバを選択します。



(注) アップグレードのソースとしてローカル サーバを選択した場合、Sophos および McAfee Anti-Virus 定義ファイルなど、複数のセキュリティ コンポーネントの自動アップデートが停止します。これらのセキュリティ コンポーネントのアップデートを継続するには、アップデート イメージまたはアップデートのリストをローカル サーバでホスティングします。

- ステップ 2** アップデート イメージの取得先にローカル アップデート サーバを選択した場合、最初に AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルを除く、すべてのサービス アップデートをホスティングするローカル サーバのベース URL、ポート番号、およびオプションの認証情報を入力します。次に、AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルをホスティングするローカル サーバのベース URL を入力します。
- ステップ 3** IronPort アップデート サーバまたはローカル アップデート サーバのいずれかから、利用可能な Cisco IronPort AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのリストを取得するサーバを選択します。
- ステップ 4** 利用可能なアップグレードのリストの取得先にローカル アップデート サーバを選択した場合、ファイル名、HTTP ポート番号およびオプションの認証情報を含む、リストの XML ファイルへの完全なパスを入力します。

自動アップデートの設定

自動アップデートをイネーブルにし、アップデート間隔を設定するには、次の手順を実行します。

-
- ステップ 1** チェックボックスをオンにして、自動アップデートをイネーブルにします。
 - ステップ 2** アップデート間隔（次のアップデートの確認までに待機する時間）を入力します。数字の後に **m**（分）および **h**（時）を追加します。最大アップデート間隔は 1 時間です。

HTTP プロキシ サーバの指定（任意）

HTTP プロキシ サーバを指定するには、次の手順を実行します。

-
- ステップ 1** サーバの URL とポート番号を入力します。
 - ステップ 2** 必要に応じて、サーバのアカウントのユーザ名とパスワードを入力します。
 - ステップ 3** 変更を送信して確定します。

HTTPS プロキシ サーバの指定（任意）

HTTPS プロキシ サーバを指定するには、次の手順を実行します。

-
- ステップ 1** サーバの URL とポート番号を入力します。
 - ステップ 2** 必要に応じて、サーバのアカウントのユーザ名とパスワードを入力します。
 - ステップ 3** 変更を送信して確定します。

生成されるさまざまなメッセージに対する返信アドレスの設定



Cloud Email Security アプライアンスの返信アドレスは変更しないことを推奨します。

AsyncOS によって、次のタイミングで生成されるメールのエンベロープ送信者を設定できます。

- Anti-Virus 通知
- バウンス
- 通知 (notify() および notify-copy() フィルタの動作)
- 検疫通知 (および検疫管理機能における「コピー送信」)
- レポート

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイドメインの使用を選択することもできます。

GUI で [System Administration] メニューから利用できる [Return Addresses] ページを使用するか、CLI で addressconfig コマンドを使用します。

図 15-8 [Return Addresses] ページ
Return Addresses

Return Addresses for System-Generated Email	
Anti-Virus Messages:	"Mail Delivery System" <MAILER-DAEMON@hostname>
Bounce Messages:	"Mail Delivery System" <MAILER-DAEMON@hostname>
Notifications:	"Mail Delivery System" <MAILER-DAEMON@hostname>
Quarantine Messages:	"Mail Delivery System" <MAILER-DAEMON@hostname>
Reports:	IronPort Reporting <reporting@hostname>

システムで生成された電子メールメッセージの返信アドレスを GUI から変更するには、[Return Addresses] ページで [Edit Settings] をクリックします。1 つ以上のアドレスを変更して、[Submit] をクリックし、最後に変更を確定します。

アラート

アラートとは、Cisco IronPort アプライアンスで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナーからメジャーまでの重要度 (または重大度) レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。アラートは、Cisco IronPort アプライアンスで生成されます。送信するアラートメッセージの種類、重大度、および送信するユーザを非常に詳細なレベルで指定できます。アラートは、GUI の [System Administration] > [Alerts] ページ (または CLI の alertconfig コマンド) で管理します。

アラートの概要

アラート機能は 2 つの主要な部分から構成されます。

- [Alerts] : アラート受信者 (アラートを受信する電子メール アドレス)、および受信者に送信されるアラート通知 (重大度およびアラート タイプ)。
- [Alert Settings] : アラート送信者 ([FROM:] アドレス、次に重複したアラートを送信するまでに待機する秒数、および AutoSupport をイネーブルにするかどうか (およびオプションで毎週 AutoSupport レポートを送信するかどうか) などのアラート機能に関する全般的な動作を指定します。

アラート : アラート受信者、アラート分類、および重要度

アラートとは、アラート受信者に送信される、ハードウェアやアンチウイルスの問題など特定の機能 (またはアラート分類) に関する情報が記載された電子メール メッセージまたは通知のことです。アラート受信者とは、アラート通知が送信される電子メール アドレスのことです。通知に含まれる情報は、アラート分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。アラート エンジンでは、送信するアラートの種類とアラート受信者を詳細に制御できます。たとえば、アラート受信者が **System** (アラートの種類) に関する **Critical** (重大度) の情報が送信されたときのみ通知を受信するように設定することで、アラート受信者に特定のアラートのみを送信するように設定できます。また、一般的な設定値も設定できます ([「アラート設定値の設定」 \(P.15-32\)](#) を参照してください)。

すべてのアラートのリストについては、[「アラート リスト」 \(P.15-33\)](#) を参照してください。

アラート分類

AsyncOS では、次のアラート分類を送信します。

- System
- Hardware
- Updater
- Outbreak Filters
- Anti-Virus
- Anti-Spam

- Directory Harvest Attack Prevention

重大度

アラートは、次の重大度に従って送信されます。

- [Critical] : すぐに対処が必要です。
- [Warning] : 今後モニタリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります。
- [Information] : デバイスのルーティン機能で生成される情報。

アラート設定

アラート設定では、アラートの全般的な動作と設定を制御します。設定には次のような項目があります。

- **RFC 2822 Header From** : アラートを送信するタイミング（アドレスを入力するか、デフォルトの「alert@<hostname>」を使用します）。また、`alertconfig -> from` コマンドを使用して、この値を CLI で設定することもできます。
- 重複したアラートを送信するまでに待機する秒数の初期値。
- 重複したアラートを送信するまでに待機する秒数の最大値。
- **AutoSupport** のステータス（イネーブルまたはディセーブル）。
- **Information** レベルの **System** アラートを受信するように設定されたアラート受信者への、**AutoSupport** の毎週のステータス レポートの送信。

重複したアラートの送信

AsyncOS が重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を **0** に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に大きな秒数になります。[Maximum Number of Seconds to Wait Before Sending a Duplicate Alert] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

SMTP ルートおよびアラート

アプライアンスから [Alert Recipient] で指定されたアドレスに送信されるアラートは、該当の送信先に対して定義された SMTP ルートに従います。

IronPort AutoSupport

十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラートメッセージをシスコに送信するように Cisco IronPort アプライアンスを設定できます。この機能は AutoSupport と呼ばれ、シスコによるお客様のニーズへのプロアクティブな対応に役立ちます。また、AutoSupport はシステムの稼働時間、status コマンドの出力、および使用されている AsyncOS バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラートタイプが System で重大度レベルが Information のアラートを受信するように設定されているアラート受信者は、シスコに送信される各メッセージのコピーを受信します。内部にアラートメッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能をイネーブ爾またはディセーブルにするには、「アラート設定値の設定」(P.15-32) を参照してください。

アラートメッセージ

アラートメッセージは標準的な電子メールメッセージです。Header From: アドレスは設定できますが、メッセージのその他の部分は自動的に生成されます。

アラートの From アドレス

[Edit Settings] ボタンまたは CLI (『Cisco IronPort AsyncOS CLI Reference Guide』を参照) を使用して、Header From: アドレスを設定できます。

アラートの件名

アラートの電子メール メッセージの件名は、次の形式に従っています。

```
Subject: [severity]-[hostname]: ([class]) short message
```

アラートの配信

アラート メッセージは Cisco IronPort アプライアンス内の問題の通知に使用されるため、送信に AsyncOS の標準メール配信システムを使用しません。代わりに、アラート メッセージは AsyncOS で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メール システムで処理されます。

アラート メール システムは、AsyncOS と同一の設定を共有しません。このため、アラート メッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラート メッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
 - 5.X 以前の AsyncOS バージョンでは、アラート メッセージは `smtproutes` を使用しません。
 - アラート メッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- アラート メッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージ フィルタまたはコンテンツ フィルタの処理対象にも含まれません。
- アラート メッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

アラート メッセージの例

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via
http://newproxy.example.com failed
```

The Critical message is:

```
update via http://newproxy.example.com failed
```

```
Version: 4.5.0-419
```

```
Serial Number: XXXXXXXXXXXX-XXXXXXX
```

```
Timestamp: Tue May 10 09:39:24 2005
```

For more information about this error, please see

```
http://support.ironport.com
```

If you desire further information, please contact your support provider.

アラート受信者の管理

Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) にログインして、[System Administration] タブをクリックします (GUI へのアクセス方法については、「[GUI へのアクセス](#)」(P.2-3) を参照してください)。左のメニューにある [Alerts] リンクをクリックします。

図 15-9 [Alerts] ページ
Alerts

Alert Recipients								
Add Recipient...								
Recipient Address	System	Hardware	Updater	Virus Outbreak Filters	Anti-Virus	Anti-Spam	Directory Harvest Attack Prevention	Delete
joe@example.com	All	All	All	All	All	All	All	🗑
mary@example.com	Critical	Critical	Critical	Critical	Critical	Critical	Critical	🗑

Alert Settings	
From Address to Use When Sending Alerts:	Automatically Generated
Initial Number of Seconds to Wait Before Sending a Duplicate Alert:	300
Maximum Number of Seconds to Wait Before Sending a Duplicate Alert:	3600
IronPort AutoSupport:	Enabled
	Send copy of weekly AutoSupport reports to System Information Alert recipients.
Edit Settings...	



(注)

システムのセットアップ時に AutoSupport をイネーブ爾にした場合、指定した電子メール アドレスにすべての重大度およびクラスのアラートを受信します (デフォルト)。この設定はいつでも変更できます。

[Alerts] ページは、既存のアラート受信者およびアラート設定のリストを表示します。

[Alerts] ページからは、次の操作ができます。

- アラート受信者の追加、設定、または削除
- アラート設定値の変更

新規アラート受信者の追加

新規アラート受信者を追加するには、次の手順を実行します。

- ステップ 1** [Alerts] ページで [Add Recipient] をクリックします。[Add Alert Recipients] ページが表示されます。

図 15-10 新規アラート受信者の追加
Add Alert Recipient

Alert Recipient				
Recipient Address: <input type="text"/>				
Separate multiple email addresses with commas				
Alert Severities to Receive				
	All	Critical ⓘ	Warning ⓘ	Info ⓘ
Alert Type	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hardware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Updater	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Virus Outbreak Filters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anti-Virus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anti-Spam	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Directory Harvest Attack Prevention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Submit

- ステップ 2** 受信者の電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力することもできます。
- ステップ 3** 受信するアラートの重大度を選択します。
- ステップ 4** 変更を送信して確定します。

既存のアラート受信者の設定

既存のアラート受信者を編集するには、次の手順を実行します。

- ステップ 1** [Alert Recipients] のリストからアラート受信者をクリックします。[Configure Alert Recipient] ページが表示されます。
- ステップ 2** アラート受信者の設定を変更します。
- ステップ 3** 変更を送信して確定します。

アラート受信者の削除

アラート受信者を削除するには、次の手順を実行します。

- ステップ 1** [Alert Recipient] のリストから、アラート受信者に対応するゴミ箱アイコンをクリックします。
- ステップ 2** 表示される警告ダイアログで [Delete] をクリックして、削除を確定します。
- ステップ 3** 変更を確定します。

アラート設定値の設定

アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

アラート設定値の編集

アラート設定値を編集するには、次の手順を実行します。

- ステップ 1** [Alerts] ページで [Edit Settings] をクリックします。[Edit Alert Settings] ページが表示されます。

図 15-11 アラート設定値の編集
Edit Alert Settings

Alert Settings	
From Address to Use When Sending Alerts:	<input type="radio"/> <input type="text"/> <input checked="" type="radio"/> Automatically generated <small>(example: IronPort C60 Alert <alert@host.example.com>.)</small>
Wait Before Sending a Duplicate Alert:	<input checked="" type="checkbox"/> Enable <input type="text" value="300"/> Initial Number Of Seconds to Wait Before Sending a Duplicate Alert <input type="text" value="3600"/> Maximum Number Of Seconds to Wait Before Sending a Duplicate Alert:
IronPort AutoSupport:	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Send copy of weekly AutoSupport reports to System Information Alert recipients.

- ステップ 2** アラートの送信に使用する Header From: アドレスを入力するか、[Automatically Generated] (「alert@<hostname>」を自動生成) を選択します。

- ステップ 3** 重複したアラートを送信するまでに待機する秒数を指定する場合は、チェックボックスをオンにします。詳細については、「[重複したアラートの送信](#)」(P.15-26) を参照してください。

- 重複したアラートを送信するまでに待機する秒数の初期値を指定します。
- 重複したアラートを送信するまでに待機する秒数の最大値を指定します。

ステップ 4 [IronPort AutoSupport] オプションをオンにすることで、AutoSupport をイネーブルにできます。AutoSupport の詳細については、「[IronPort AutoSupport](#)」(P.15-27) を参照してください。

- AutoSupport がイネーブルの場合、Information レベルの System アラートを受信するように設定されたアラート受信者に、毎週 AutoSupport レポートが送信されます。チェックボックスを外すことでディセーブルにできます。

ステップ 5 変更を送信して確定します。

アラート リスト

次の表に、分類したアラートのリストを示します。表には、アラート名 (IronPort で使用される内部記述子)、アラートの実際のテキスト、説明、重大度 (critical、information、または warning) およびメッセージのテキストに含まれるパラメータ (存在する場合) が含まれています。アラートの実際のテキストでは、パラメータ値は置き換えられます。たとえば、次のアラートメッセージではメッセージのテキストに「\$ip」が記述されています。アラート生成時に「\$ip」は実際の IP アドレスに置き換えられます。

アンチスパム アラート

表 15-2 に、AsyncOS で生成される可能性があるさまざまなアンチスパムに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-2 発生する可能性があるアンチスパム アラートのリスト

アラート名	メッセージと説明	パラメータ
AS.SERVER.ALERT	\$engine anti-spam - \$message \$tb Critical。アンチスパム エンジンに障害が発生した場合に送信されます。	「engine」: アンチスパム エンジンのタイプ。 「message」: ログ メッセージ。 「tb」: イベントのトレースバック。

表 15-2 発生する可能性があるアンチスパム アラートのリスト (続き)

アラート名	メッセージと説明	パラメータ
AS.TOOL.INFO_ALERT	Update - \$engine - \$message	「engine」: アンチスパム エンジン の名前。 「message」: メッセージ。
	Information。アンチスパム エンジンに問題が発生した場合に送信されます。	
AS.TOOL.ALERT	Update - \$engine - \$message	「engine」: アンチスパム エンジン の名前。 「message」: メッセージ。
	Critical。アンチスパム エンジンの管理に使用されるツールの 1 つに問題があり、アップデートが中止される場合に送信されます。	

アンチウイルス アラート

表 15-3 に、AsyncOS で生成される可能性があるさまざまなアンチウイルスに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-3 発生する可能性があるアンチウイルス アラートのリスト

アラート名	メッセージと説明	パラメータ
AV.SERVER.ALERT/ AV.SERVER.CRITICAL	\$engine antivirus - \$message \$tb	「engine」: アンチウイルス エンジン のタイプ。 「message」: ログ メッセージ。 「tb」: イベント のトレースバック。
	Critical。アンチウイルス スキャン エンジンに重大な問題が発生した場合に送信されます。	
AV.SERVER.ALERT.INFO	\$engine antivirus - \$message \$tb	「engine」: アンチウイルス エンジン のタイプ。 「message」: ログ メッセージ。 「tb」: イベント のトレースバック。
	Information。アンチウイルス スキャン エンジンに情報イベントが発生した場合に送信されます。	

表 15-3 発生する可能性があるアンチウイルス アラートのリスト (続き)

アラート名	メッセージと説明	パラメータ
AV.SERVER.ALERT.WARN	Engine antivirus - \$message \$tb	<p>「engine」: アンチウイルス エンジンタイプ。</p> <p>「message」: ログ メッセージ。</p> <p>「tb」: イベントのトレースバック。</p>
	Warning。アンチウイルス スキャン エンジンに問題が発生した場合に送信されます。	
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID \$mid antivirus \$what error \$tag	<p>「mid」: MID</p> <p>「what」: 発生したエラー。</p> <p>「tag」: ウイルス発生名 (設定されている場合)。</p>
	Critical。メッセージのスキャン中に、アンチウイルス スキャンがエラーを生成した場合に送信されます。	
MAIL.SCANNER.PROTOCOL_MAX_RETRY	MID \$mid is malformed and cannot be scanned by \$engine.	<p>「mid」: MID</p> <p>「engine」: 使用されているエンジン。</p>
	Critical。メッセージが不正なため、スキャン エンジン はメッセージのスキャンに失敗しました。再試行の最大回数を超過したため、メッセージはエンジンにスキャンされずに処理されません。	

ディレクトリ獲得攻撃（DHAP）アラート

表 15-4 に、AsyncOS で生成される可能性があるさまざまな DHAP に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-4 発生する可能性があるディレクトリ獲得攻撃アラートのリスト

アラート名	メッセージと説明	パラメータ
LDAP.DHAP_ALERT	LDAP: Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack.	
	Warning。ディレクトリ獲得攻撃の可能性を検出した場合に送信されます。	

ハードウェア アラート

表 15-5 に、AsyncOS で生成される可能性があるさまざまなハードウェア アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-5 発生する可能性があるハードウェア アラートのリスト

アラート名	メッセージと説明	パラメータ
INTERFACE.ERRORS	Port \$port: has detected \$in_err input errors, \$out_err output errors, \$col collisions please check your media settings.	「port」：インターフェイス名。 「in_err」：最後のメッセージからの入力エラー数。 「out_err」：最後のメッセージからの出力エラー数。 「col」：最後のメッセージからのパケット衝突数。
	Warning。インターフェイスエラーを検出した場合に送信されます。	

表 15-5 発生する可能性があるハードウェア アラートのリスト (続き)

アラート名	メッセージと説明	パラメータ
MAIL.MEASUREMENTS_FILESYSTEM	The \$file_system partition is at \$capacity% capacity	「file_system」: ファイルシステムの名前。
	Warning。ディスクパーティションが 75 % の使用率に近づいた場合に送信されます。	「capacity」: ファイルシステムの使用率 (%)。
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	The \$file_system partition is at \$capacity% capacity	「file_system」: ファイルシステムの名前。
	Critical。ディスクパーティションが 90 % の使用率に達した場合 (95 %、96 %、97 % など) に送信されます。	「capacity」: ファイルシステムの使用率 (%)。
SYSTEM.RAID_EVENT_ALERT	A RAID-event has occurred: \$error	「error」: RAID エラーのテキスト。
	Warning。重大な RAID-event が発生した場合に送信されます。	
SYSTEM.RAID_EVENT_ALERT_INFO	A RAID-event has occurred: \$error	「error」: RAID エラーのテキスト。
	Information。RAID-event が発生した場合に送信されます。	

IronPort スпам検疫アラート

表 15-6 に、AsyncOS で生成される可能性があるさまざまな IronPort スпам検疫に関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-6 発生する可能性がある IronPort スпам検疫アラートのリスト

アラート名	メッセージと説明	パラメータ
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at \$host:\$port	「 host 」: オフボックス検疫のアドレス。 「 port 」: オフボックス検疫に接続するポート。
	Information。AsyncOS が (オフボックス) IP アドレスに接続できない場合に送信されます。	
ISQ.CRITICAL	ISQ: \$msg	「 msg 」: 表示されるメッセージ
	Critical。IronPort スпам検疫に重大なエラーが発生した場合に送信されます。	
ISQ.DB_APPROACHING_FULL	ISQ: Database over \$threshold% full	「 threshold 」: アラートを開始する使用率のしきい値
	Warning。IronPort スпам検疫データベースがフルに近い場合に送信されます。	
ISQ.DB_FULL	ISQ: database is full	
	Critical。IronPort スпам検疫データベースがフルになった場合に送信されます。	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID \$mid for \$rcpt: \$reason	「 mid 」: MID 「 rcpt 」: 受信者または「 all 」 (全員) 「 reason 」: メッセージが削除されない理由
	Warning。IronPort スпам検疫からの電子メールの削除に失敗した場合に送信されます。	

表 15-6 発生する可能性がある IronPort スпам検査アラートのリスト (続き)

アラート名	メッセージと説明	パラメータ
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: \$reason	「 reason 」: 通知が送信されない理由
	Warning。通知メッセージの送信に失敗した場合に送信されます。	
ISQ.MSG_QUAR_FAILED		
	Warning。メッセージの検査に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID \$mid to \$rcpt: \$reason	「 mid 」: MID 「 rcpt 」: 受信者または「 all 」(全員) 「 reason 」: メッセージが開放されない理由
	Warning。メッセージの開放に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID \$mid: \$reason	「 mid 」: MID 「 reason 」: メッセージが開放されない理由
	Warning。受信者が不明のため、メッセージの開放に失敗した場合に送信されます。	
ISQ.NO_EU_PROPS	ISQ: Could not retrieve \$user's properties.Setting defaults	「 user 」: エンドユーザ名
	Information。AsyncOS がユーザの情報を取得できない場合に送信されます。	

表 15-6 発生する可能性がある IronPort スпам検疫アラートのリスト (続き)

アラート名	メッセージと説明	パラメータ
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host Information。AsyncOS が外部検疫を参照するように設定されているものの、外部検疫が定義されていない場合に送信されます。	

セーフリスト/ブロックリスト アラート

次の表に、AsyncOS で生成される可能性があるさまざまなセーフリスト/ブロックリストに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-7 発生する可能性があるセーフリスト/ブロックリストアラートのリスト

アラート名	メッセージと説明	パラメータ
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '\$error'. Critical。セーフリスト/ブロックリスト データベースの復旧に失敗しました。	「 error 」: エラーの理由
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: \$current of \$limit. Critical。セーフリスト/ブロックリスト データベースが許容されたディスク領域を超過しました。	「 current 」: データベース使用量 (MB) 「 limit 」: 設定された制限使用量 (MB)

システム アラート

表 15-8 に、AsyncOS で生成される可能性があるさまざまなシステム アラートのリストを示します。この表には、アラートの説明とアラートの重大度が含まれています。

表 15-8 発生する可能性があるシステム アラートのリスト

アラート名	メッセージと説明	パラメータ
COMMON.APP_FAILURE	An application fault occurred: \$error	「 error 」: エラーのテキスト (通常はトレースバック)
	Warning。不明なアプリケーション障害が発生した場合に送信されます。	
COMMON.KEY_EXPIRED_ALERT	Your "\$feature" key has expired.Please contact your authorized Cisco IronPort sales representative.	「 feature 」: 有効期限が切れる機能の名前。
	Warning。機能キーの有効期限が切れた場合に送信されます。	
COMMON.KEY_EXPIRING_ALERT	Your "\$feature" key will expire in under \$days day(s).Please contact your authorized Cisco IronPort sales representative.	「 feature 」: 有効期限が切れる機能の名前。 「 days 」: 有効期限が切れるまでの日数。
	Warning。機能キーの有効期限が切れる場合に送信されます。	
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice.Your "\$feature" key will expire in under \$days day(s).Please contact your authorized Cisco IronPort sales representative.	「 feature 」: 有効期限が切れる機能の名前。 「 days 」: 有効期限が切れるまでの日数。
	Warning。機能キーの有効期限が切れる場合の最後の通知として送信されます。	

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver.Unable to contact root servers.	
	Warning。アプライアンスがルート DNS サーバに問い合わせることができない場合に送信されます。	
INTERFACE.FAILOVER.FAILURE_BACKUP_DETECTED	Standby port \$port on \$pair_name failure	「port」：検出されたポート
	Warning。バックアップ NIC ペアリング インターフェイスが故障した場合に送信されます。	「pair_name」：フェールオーバーのペア名。
INTERFACE.FAILOVER.FAILURE_BACKUP_RECOVERED	Standby port \$port on \$pair_name okay	「port」：故障したポート
	Information。NIC ペアのフェールオーバーが復旧した場合に送信されます。	「pair_name」：フェールオーバーのペア名。
INTERFACE.FAILOVER.FAILURE_DETECTED	Port \$port failure on \$pair_name, switching to \$port_other	「port」：故障したポート。
	Critical。インターフェイス故障により、NIC ペアリングフェールオーバーが検出された場合に送信されます。	「port_other」：新しいポート。 「pair_name」：フェールオーバーのペア名。
INTERFACE.FAILOVER.FAILURE_DETECTED_NO_BACKUP	Port \$port_other on \$pair_name is down, can't switch to \$port_other	「port」：故障したポート。
	Critical。インターフェイス故障により NIC ペアリングフェールオーバーは検出されたけれども、バックアップインターフェイスが利用できない場合に送信されます。	「port_other」：新しいポート。 「pair_name」：フェールオーバーのペア名。

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
INTERFACE.FAILOVER. FAILURE_RECOVERED	Recovered network on \$pair_name using port \$port	「port」：故障したポート
	Information。NIC ペアのフェールオーバーが復旧した場合に送信されます。	「pair_name」：フェールオーバーのペア名。
INTERFACE.FAILOVER. MANUAL	Manual failover to port \$port on \$pair_name	「port」：新しいアクティブポート。
	Information。別の NIC ペアへの手動フェールオーバーが検出された場合に送信されます。	「pair_name」：フェールオーバーのペア名。
COMMON.INVALID_FILTER	Invalid \$class: \$error	「class」：「Filter」、 「SimpleFilter」などのいずれか。
	Warning。無効なフィルタが存在する場合に送信されます。	「error」：フィルタが無効な理由に関する追加の情報。
LDAP.GROUP_QUERY_ FAILED_ALERT	LDAP: Failed group query \$name, comparison in filter will evaluate as false	「name」：クエリーの名前。
	Critical。LDAP グループクエリーに失敗した場合に送信されます。	
LDAP.HARD_ERROR	LDAP: work queue processing error in \$name reason \$why	「name」：クエリーの名前。
	Critical。LDAP クエリーが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。	「why」：エラーが発生した理由。
LOG.ERROR.*	Critical。さまざまなロギングエラー。	

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	<p>LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server.</p> <p>Critical。各受信者のスキャン時に LDAP グループクエリーに失敗した場合に送信されます。</p>	
MAIL.QUEUE.ERROR.*	<p>Critical。メールキューのさまざまなハードエラー。</p>	
MAIL.RES_CON_START_ALERT.MEMORY	<p>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 \$memory_threshold_start%. The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches \$memory_threshold_halt%.</p> <p>Critical。メモリ使用率がシステムリソース節約しきい値を超過した場合に送信されます。</p>	<p>「hostname」：ホストの名前。</p> <p>「memory_threshold_start」：メモリのターゲットを開始するパーセントしきい値。</p> <p>「memory_threshold_halt」：メモリがフルのためにシステムが停止するパーセントしきい値。</p>

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	<p>This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. The queue is overloaded and is unable to maintain the current throughput.</p> <p>Critical。メールキューが過負荷となり、システムリソース節約がイネーブルになった場合に送信されます。</p>	「 hostname 」：ホストの名前。
MAIL.RES_CON_START_ALERT.QUEUE	<p>This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Queue utilization for this system has exceeded the resource conservation threshold of \$queue_threshold_start%. The allowed receiving rate for this system will be gradually decreased as queue utilization approaches \$queue_threshold_halt%.</p> <p>Critical。キュー使用率がシステムリソース節約しきい値を超過した場合に送信されます。</p>	<p>「hostname」：ホストの名前。</p> <p>「queue_threshold_start」：キューのターゲットを開始するパーセントしきい値。</p> <p>「queue_threshold_halt」：キューがフルのためにシステムが停止するパーセントしきい値。</p>

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ALERT.WORKQ	This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Listeners have been suspended because the current work queue size has exceeded the threshold of \$suspend_threshold. Listeners will be resumed once the work queue size has dropped to \$resume_threshold. These thresholds may be altered via use of the 'tarpit' command on the system CLI.	<p>「hostname」: ホストの名前。</p> <p>「suspend_threshold」: リスナーが一時停止されるワークキューの下限サイズ。</p> <p>「resume_threshold」: リスナーが再開されるワークキューの上限サイズ。</p>
	Information。ワークキューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されません。	
MAIL.RES_CON_START_ALERT	This system (hostname: \$hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.	「 hostname 」: ホストの名前。
	Critical。アプライアンスが「リソース節約」モードに入った場合に送信されます。	

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_STOP_ALERT	This system (hostname: \$hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.	「 hostname 」: ホストの名前。
	Information。アプライアンスの「リソース節約」モードが解除された場合に送信されます。	
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, \$num msgs, \$reason	「 num 」: ワークキューに存在するメッセージ数。 「 reason 」: ワークキューが中断された理由。
	Critical。ワークキューが中断された場合に送信されます。	
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, \$num msgs	「 num 」: ワークキューに存在するメッセージ数。
	Critical。ワークキューが再開された場合に送信されます。	
NTP.NOT_ROOT	Not running as root, unable to adjust system time	
	Warning。Sent when the Cisco IronPort appliance is unable to adjust time because NTP is not running as root.	
QUARANTINE.ADD_DB_ERROR	Unable to quarantine MID \$mid - quarantine system unavailable	「 mid 」: MID
	Critical。メッセージを検疫エリアに送ることができない場合に送信されます。	

表 15-8 発生する可能性があるシステムアラートのリスト (続き)

アラート名	メッセージと説明	パラメータ
QUARANTINE.DB_UPDATE_FAILED	Unable to update quarantine database (current version: \$version; target \$target_version)	「 version 」: 検出されたスキーマバージョン。 「 target_version 」: 対象のスキーマバージョン。
	Critical。検疫データベースがアップデートできない場合に送信されます。	
QUARANTINE.DISK_SPACE_LOW	The quarantine system is unavailable due to a lack of space on the \$file_system partition.	「 file_system 」: ファイルシステムの名前。
	Critical。検疫用のディスク領域がフルになった場合に送信されます。	
QUARANTINE.THRESHOLD_ALERT	Quarantine "\$quarantine" is \$full% full	「 quarantine 」: 検疫エリアの名前。
	Warning。検疫エリアの容量使用率が 5 %、50 %、または 75 % に達した場合に送信されます。	「 full 」: 検疫エリアの容量使用率。
QUARANTINE.THRESHOLD_ALERT.SERIOUS	Quarantine "\$quarantine" is \$full% full	「 quarantine 」: 検疫エリアの名前。
	Critical。検疫エリアの容量使用率が 95 % に達した場合に送信されます。	「 full 」: 検疫エリアの容量使用率。

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
REPORTD.DATABASE_OPEN_FAILED_ALERT	The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: \$err_msg	「 err_msg 」：発生したエラーメッセージ
	Critical。レポートエンジンがデータベースを開けない場合に送信されます。	
REPORTD.AGGREGATION_DISABLED_ALERT	<p>Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above \$threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc.). Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically.</p> <p>Warning。システムのディスク領域が不足している場合に送信されます。ログエントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。</p>	「 threshold 」：しきい値

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
REPORTING.CLIENT. UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time (\$duration).	「 duration 」：クライアントがレポート デーモンへの問い合わせを試行する時間。この値は、人間が読み取れる形式の文字列です（「1h 3m 27s」）。
	Warning。レポート エンジンがレポート データを保存できなかった場合に送信されます。	
REPORTING.CLIENT. JOURNAL.FULL	Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	
	Critical。レポート エンジンが新規データを保存できない場合に送信されます。	
REPORTING.CLIENT. JOURNAL.FREE	Reporting Client: The reporting system is now able to handle new data.	
	Information。レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	
PERIODIC_REPORTS. REPORT_TASK.BUILD_ FAILURE	A failure occurred while building periodic report '\$report_title'. This subscription has been removed from the scheduler.	「 report_title 」：レポートのタイトル
	Critical。レポート エンジンがレポートを作成できない場合に送信されます。	

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
PERIODIC_REPORTS. REPORT_TASK.EMAIL_ FAILURE	A failure occurred while emailing periodic report '\$report_title'. This subscription has been removed from the scheduler.	「 report_title 」：レポートのタイトル
	Critical。レポートを電子メールで送信できなかった場合に送信されます。	
PERIODIC_REPORTS. REPORT_TASK.ARCHIVE_FAILUR E	A failure occurred while archiving periodic report '\$report_title'. This subscription has been removed from the scheduler.	「 report_title 」：レポートのタイトル
	Critical。レポートをアーカイブできなかった場合に送信されます。	
SENDERBASE.ERROR	Error processing response to query \$query: response was \$response	「 query 」：クエリーするアドレス。 「 response 」：受信した応答の raw データ。
	Information。SenderBase からの応答を処理中にエラーが発生した場合に送信されます。	
SMTPAUTH.FWD_SERVER_FAIL D_ALERT	SMTP Auth: could not reach forwarding server \$ip with reason: \$why	「 ip 」：リモートサーバの IP。 「 why 」：エラーが発生した理由。
	Warning。SMTP 認証転送サーバが到達不能である場合に送信されます。	
SMTPAUTH.LDAP_QUERY_FAIL D	SMTP Auth: LDAP query failed, see LDAP debug logs for details.	
	Warning。LDAP クエリーが失敗した場合に送信されます。	

表 15-8 発生する可能性があるシステムアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
SYSTEM.HERMES_SHUTDOWN_FAILURE. REBOOT	While preparing to \${what}, failed to stop mail server gracefully: \${error}\$what:=reboot	「 error 」: 発生したエラー。
	Warning。リブート中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	While preparing to \${what}, failed to stop mail server gracefully: \${error}\$what:=shut down	「 error 」: 発生したエラー。
	Warning。システムをシャットダウンしている際に問題が発生した場合に送信されます。	
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Error updating recipient validation data: \$why	「 why 」: エラーメッセージ。
	Critical。受信者検証のアップデートに失敗した場合に送信されます。	
SYSTEM.SERVICE_TUNNEL.DISABLED	Tech support: Service tunnel has been disabled	
	Information。Cisco IronPort サポート サービス用に作成されたトンネルがディセーブルの場合に送信されます。	
SYSTEM.SERVICE_TUNNEL.ENABLED	Tech support: Service tunnel has been enabled, port \$port	「 port 」: サービストンネルに使用されるポート。
	Information。Cisco IronPort サポート サービス用に作成されたトンネルがイネーブルの場合に送信されます。	

アップデータ アラート

表 15-9 に、AsyncOS で生成される可能性があるさまざまなアップデータ アラートのリストを示します。

表 15-9 発生する可能性があるアップデータ アラートのリスト

アラート名	メッセージと説明	パラメータ
UPDATER.APP.UPDATE_ABANDONED	\$app abandoning updates until a new version is published.The \$app application tried and failed \$attempts times to successfully complete an update.This may be due to a network configuration issue or temporary outage	「 app 」: アプリケーションの名前。 「 attempts 」: 試行した回数。
	Warning。アプリケーションはアップデートを中止しています。	
UPDATER.UPDATERD.MANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least \$threshold.	「 threshold 」: 人間が読み取れるしきい値の文字列。
	Warning。サーバのマニフェストの取得に失敗しました。	
UPDATER.UPDATERD.RELEASE_NOTIFICATION	\$mail_text	「 mail_text 」: 通知するテキスト。 「 notification_subject 」: 通知するテキスト。
	Warning。リリースの通知です。	
UPDATER.UPDATERD.UPDATE_FAILED	Unknown error occured: \$traceback	「 traceback 」: トレースバック。
	Critical。アップデートの実行に失敗しました。	

感染フィルタ アラート

表 15-10 に、AsyncOS で生成される可能性があるさまざまな感染フィルタに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。感染フィルタは、検疫（具体的には Outbreak 検疫）で使用されるシステム アラートでも参照される場合があることに注意してください。

表 15-10 発生する可能性がある感染フィルタ アラートのリスト

アラート名	メッセージと説明	パラメータ
VOF.GTL_THRESHOLD_ALERT	Cisco IronPort Outbreak Filters Rule Update Alert:\$text All rules last updated at: \$time on \$date.	「 text 」: アップデートアラートのテキスト。 「 time 」: 最終アップデートの時刻。
	Information。感染フィルタのしきい値が変更された場合に送信されます。	「 date 」: 最終アップデートの日付。
AS.UPDATE_FAILURE	\$engine update unsuccessful.This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com.The specific error on the appliance for this failure is: \$error	「 engine 」: アップデートに失敗したエンジン。 「 error 」: 発生したエラー。
	Warning。アンチスパム エンジンまたは CASE ルールのアップデートに失敗した場合に送信されます。	

クラスタリング アラート

表 15-11 に、AsyncOS で生成される可能性があるさまざまなクラスタリングに関するアラートのリストを示します。この表には、アラートの説明とアラートの重大度が記載されています。

表 15-11 発生する可能性があるクラスタリングアラートのリスト

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.AUTH_ERROR	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Machine does not appear to be in the cluster	「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。 「ip」: リモートホストの IP。 「why」: エラーに関する詳細なテキスト。
	Critical。認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Existing connection dropped	「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。 「ip」: リモートホストの IP。 「why」: エラーに関する詳細なテキスト。
	Warning。クラスタへの接続がドロップされた場合に送信されます。	
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Connection failure	「name」: マシンのホスト名およびシリアル番号 (またはいずれか)。 「ip」: リモートホストの IP。 「why」: エラーに関する詳細なテキスト。
	Warning。クラスタへの接続に失敗した場合に送信されます。	

表 15-11 発生する可能性があるクラスタリングアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.FORWARD_FAILED	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Message forward failed, no upstream connection	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。 「ip」：リモートホストの IP。
	Critical。アプライアンスがクラスタのマシンにデータを転送できなかった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=No route found	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。 「ip」：リモートホストの IP。
	Critical。マシンがクラスタの別のマシンへのルートを取得できなかった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Invalid host key	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。 「ip」：リモートホストの IP。
	Critical。無効な SSH ホストキーがあった場合に送信されます。	「why」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine \$name at IP \$ip - \$error - \$why\$error:=Operation timed out	「name」：マシンのホスト名およびシリアル番号（またはいずれか）。 「ip」：リモートホストの IP。
	Warning。指定された操作がタイムアウトした場合に送信されます。	「why」：エラーに関する詳細なテキスト。

表 15-11 発生する可能性があるクラスタリングアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine \$name - \$Error - \$why	「 name 」：マシンのホスト名およびシリアル番号（またはいずれか）。
	Critical。アプライアンスがクラスタの別のマシンの有効な IP アドレスを取得できなかった場合に送信されます。	「 why 」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	Error connecting to cluster machine \$name - \$Error - \$why\$Error:=Machine does not appear to be in the cluster	「 name 」：マシンのホスト名およびシリアル番号（またはいずれか）。
	Critical。クラスタのマシンに接続する際に認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	「 why 」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.DROPPED	Error connecting to cluster machine \$name - \$Error - \$why\$Error:=Existing connection dropped	「 name 」：マシンのホスト名およびシリアル番号（またはいずれか）。
	Warning。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、クラスタへの接続がドロップした場合に送信されます。	「 why 」：エラーに関する詳細なテキスト。

表 15-11 発生する可能性があるクラスタリングアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Connection failure	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	Warning。不明な接続エラーが発生し、マシンがクラスタの別のマシンの有効な IP アドレスを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Message forward failed, no upstream connection	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、アプライアンスがマシンにデータを転送できなかった場合に送信されます。	
CLUSTER.CC_ERROR_NOIP.NOROUTE	Error connecting to cluster machine \$name - \$Error - \$why\$error:=No route found	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、別のマシンへのルートを取得できなかった場合に送信されます。	

表 15-11 発生する可能性があるクラスタリングアラートのリスト（続き）

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP.SSH_KEY	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Invalid host key	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	Critical。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、有効な SSH ホストキーを取得できなかった場合に送信されます。	
CLUSTER.CC_ERROR_NOIP.TIMEOUT	Error connecting to cluster machine \$name - \$Error - \$why\$error:=Operation timed out	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「why」：エラーに関する詳細なテキスト。</p>
	Warning。マシンがクラスタの別のマシンの有効な IP アドレスを取得できず、指定された操作がタイムアウトした場合に送信されます。	
CLUSTER.SYNC.PUSH_ALERT	Overwriting \$sections on machine \$name	<p>「name」：マシンのホスト名およびシリアル番号（またはいずれか）。</p> <p>「sections」：送信中のクラスタ セクションのリスト。</p>
	Critical。設定データが同期から外れ、リモートホストに送信された場合に送信されます。	

ネットワーク設定値の変更

このセクションでは、Cisco IronPort アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、「[System Setup Wizard の使用方法](#)」(P.3-19) で System Setup Wizard (または `systemsetup` コマンド) を利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- `sethostname`
- DNS 設定 (GUI および `dnsconfig` コマンドを利用)
- ルーティング設定 (GUI、`routeconfig` コマンドおよび `setgateway` コマンドを利用)
- `dnsflush`
- パスワード
- ネットワーク アクセス
- ログイン バナー

システム ホスト名の変更

ホスト名は、CLI プロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。`sethostname` コマンドは、Cisco IronPort アプライアンスの名前を設定します。新規ホスト名は、`commit` コマンドを発行して初めて有効になります。

sethostname コマンド

```
oldname.example.com> sethostname
```

```
[oldname.example.com]> mail3.example.com
```

```
oldname.example.com>
```

ホスト名の変更を有効にするには、commit コマンドを入力する必要があります。ホスト名の変更を確定すると、CLI プロンプトに新しいホスト名が表示されます。

```
oldname.example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Changed System Hostname
```

```
Changes committed: Mon Jan 01 12:00:01 2003
```

プロンプトに新規ホスト名が次のように表示されます。mail3.example.com>

ドメイン ネーム システム (DNS) 設定値の設定

GUI の [Network] メニューの [DNS] ページまたは `dnsconfig` コマンドで、Cisco IronPort アプライアンスの DNS 設定値を設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用する具体的なサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまでに待機する秒数

- DNS キャッシュのクリア

DNS サーバの指定

Cisco IronPort AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、またはインターネットのルート DNS サーバおよび指定した権威 DNS サーバを使用できます。インターネットのルート サーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット」DNS を設定しているときは、`in-addr.arpa` (PTR) エントリも同様に設定する必要があります。このため、たとえば「`.eng`」クエリーをネームサーバ `1.2.3.4` にリダイレクトする際に、すべての `.eng` エントリが `172.16` ネットワークにある場合、スプリット DNS 設定に「`eng,16.172.in-addr.arpa`」を指定する必要があります。

複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリーを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。システムは最初のクエリーの有効期限が切れるか「タイムアウト」するまで短時間待機し、その後次のクエリーに対しては前回よりも少し長い時間待機します。その後も同様です。待機時間は、DNS サーバの正確な合計数と設定されているプライオリティに依存します。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウ

トは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 15-12 DNS サーバ、プライオリティ、およびタイムアウト間隔の例

プライオリティ	サーバ	タイムアウト (秒)
0	1.2.3.4、1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバが 1 つダウンしている場合、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ (1.2.3.6) が使用され、最終的にプライオリティ 2 (1.2.3.7) のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

インターネット ルート サーバの使用

Cisco IronPort AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。



(注)

デフォルト DNS サーバにインターネットルートサーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリーを再帰的に解決できる必要があります。

逆引き DNS ルックアップのタイムアウト

Cisco IronPort アプライアンスは電子メールの送受信の際、リスナーに接続しているすべてのリモート ホストに対して「二重 DNS ルックアップ」の実行を試みます（二重 DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS (A) ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しない場合、または A レコードが存在しない場合は、システムは IP アドレスのみを使用してホスト アクセス テーブル (HAT) 内のエントリと照合します)。この特別なタイムアウト時間は上記ルックアップのみに適用され、「複数エントリとプライオリティ」(P.15-62) で説明している一般的な DNS タイムアウトとは関係ありません。

デフォルト値は、20 秒です。秒数に 0 を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトをディセーブルにできます。

値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。また、受信ホストの証明書にホストの IP ルックアップにマッピングされた一般名 (CN) がある場合、TLS 認証接続を求めるドメインにアプライアンスがメールを送信するのを防止します。

DNS アラート

アプライアンスのリポート時に、メッセージ「Failed to bootstrap the DNS cache」が付与されたアラートが生成される場合がたまにあります。メッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

DNS キャッシュのクリア

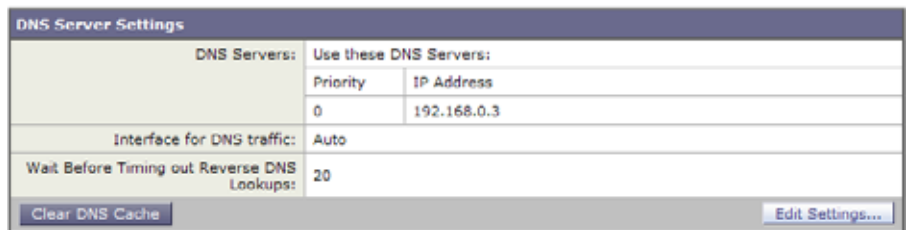
GUI の [Clear Cache] ボタン、または `dnsflush` コマンドを使用して、DNS キャッシュのすべての情報をクリアします (`dnsflush` コマンドの詳細については、『Cisco IronPort AsyncOS CLI Reference Guide』を参照してください)。

ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

グラフィカル ユーザ インターフェイスを使用した DNS 設定値の設定

Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) にログインして、[Network] タブの [DNS] リンクをクリックします。

図 15-12 [DNS] ページ
DNS



DNS Servers:		Use these DNS Servers:	
	Priority	IP Address	
	0	192.168.0.3	

Interface for DNS traffic: Auto

Wait Before Timing out Reverse DNS Lookups: 20

Clear DNS Cache Edit Settings...

DNS 設定値を GUI から編集するには、次の手順を実行します。

ステップ 1 [Edit Settings] をクリックします。[Edit DNS] ページが表示されます。

図 15-13 [Edit DNS] ページ
Edit DNS

Cancel

Submit

- ステップ 2** インターネットのルート DNS サーバまたはユーザ独自の DNS サーバを使用するか、またはインターネットのルート DNS サーバを使用して代替 DNS サーバを指定するかを選択します。
- ステップ 3** ユーザ独自の DNS サーバを使用する場合は、サーバ ID を入力し [Add Row] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、「DNS サーバの指定」(P.15-62) を参照してください。
- ステップ 4** あるドメインに対して代替 DNS サーバを指定する場合は、ドメインと代替 DNS サーバの IP アドレスを入力します。[Add Row] をクリックし、ドメインを追加します。



(注) ドメイン名をカンマで区切ることで、1 つの DNS サーバに対して複数のドメインを入力できます。IP アドレスをカンマで区切ることで、複数の DNS サーバを入力することもできます。

- ステップ 5** DNS トラフィック用のインターフェイスを選択します。

- ステップ 6** 逆引き DNS ルックアップを中止するまでに待機する秒数を入力します。
- ステップ 7** [Clear Cache] をクリックして、DNS キャッシュをクリアすることもできます。
- ステップ 8** 変更を送信して確定します。

TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。GUI の [Network] タブの [Routing] ページ、または CLI の `routeconfig` コマンドから、スタティック ルートを管理できます。

スタティック ルートの管理 (GUI)

[Network] タブの [Routing] ページから、スタティック ルートの作成、編集または削除ができます。このページからデフォルト ゲートウェイの変更もできます。

スタティック ルートの追加

新しいスタティック ルートを作成するには、次の手順を実行します。

- ステップ 1** [Routing] ページのルート リストで [Add Route] をクリックします。[Add Static Route] ページが表示されます。

図 15-14 スタティック ルートの追加
Add Static Route

Static Route Settings	
Route Name:	<input type="text"/>
Destination IP Address:	<input type="text"/>
Gateway IP Address:	<input type="text"/>
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

- ステップ 2** ルートの名前を入力します。
- ステップ 3** 宛先 IP アドレスを入力します。
- ステップ 4** ゲートウェイの IP アドレスを入力します。
- ステップ 5** 変更を送信して確定します。

スタティック ルートの削除

スタティック ルートを削除するには、次の手順を実行します。

- ステップ 1** [Static Routes] のリストから、スタティック ルート名に対応するゴミ箱アイコンをクリックします。
- ステップ 2** 表示される警告ダイアログで [Delete] をクリックして、削除を確定します。
- ステップ 3** 変更を確定します。

スタティック ルートの編集

スタティック ルートを編集するには、次の手順を実行します。

- ステップ 1** [Static Routes] のリストでルートの名前をクリックします。[Edit Static Route] ページが表示されます。
- ステップ 2** ルートの設定を変更します。
- ステップ 3** 変更を確定します。

デフォルト ゲートウェイの変更 (GUI)

デフォルト ゲートウェイを変更するには、次の手順を実行します。

- ステップ 1** [Routing] ページのルート リストで [Default Route] をクリックします。[Edit Static Route] ページが表示されます。

図 15-15 デフォルト ゲートウェイの編集
Edit Static Route

Gateway Settings	
Route Name:	Default Router
Destination IP Address:	All Destinations
Gateway IP Address:	<input type="text" value="172.19.0.1"/>

Cancel Submit

- ステップ 2** ゲートウェイの IP アドレスを変更します。
- ステップ 3** 変更を送信して確定します。

デフォルト ゲートウェイの設定

GUI の [Network] メニューの [Static Routes] ページ ([「デフォルト ゲートウェイの変更 \(GUI\)」 \(P.15-68\)](#)) を参照 または CLI の `setgateway` コマンドから、デフォルト ゲートウェイを設定できます。

admin ユーザのパスワード変更

admin ユーザのパスワードは GUI または CLI から変更できます。

パスワードを GUI から変更するには、[System Administration] タブから利用可能な [Users] ページを使用します。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にあるユーザ管理に関する項を参照してください。

admin ユーザのパスワードを CLI から変更するには、`password` コマンドを使用します。パスワードは 6 文字以上である必要があります。`password` コマンドでは、セキュリティのために古いパスワードの入力が必要です。



(注) パスワードの変更はすぐに有効になり、`commit` コマンドの実行は不要です。

電子メール セキュリティ アプライアンスの設定

AsyncOS では電子メール セキュリティ アプライアンスへのユーザアクセスを管理するために、管理者は Web UI セッションのタイムアウトや、アプライアンスにアクセス可能なユーザ IP アドレスと組織のプロキシサーバ IP アドレスを規定したアクセス リストなどを制御できます。

IP ベースのネットワーク アクセスの設定

アプライアンスに直接接続するユーザおよび逆プロキシで接続するユーザ（リモートユーザに逆プロキシを使用する組織の場合）のアクセス リストを作成して、電子メール セキュリティ アプライアンスにアクセスするユーザの IP アドレスを制御できます。

直接接続

電子メール セキュリティ アプライアンスに接続可能なマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザのアクセスは拒否されます。

プロキシ経由の接続

リモート ユーザのマシンと電子メール セキュリティ アプライアンスの間で逆プロキシ サーバが使用される組織のネットワークの場合、AsyncOS ではアプライアンスに接続可能なプロキシの IP アドレスを含むアクセス リストを作成できません。

逆プロキシを使用する場合にも、AsyncOS はユーザ接続用に許可された IP アドレスのリストとリモート ユーザのマシンの IP アドレスを照合します。リモート ユーザの IP アドレスを電子メール アプライアンスに送信するためには、プロキシはアプライアンスへの接続要求に `x-forwarded-for` HTTP ヘッダーを追加する必要があります。

`x-forwarded-for` ヘッダーは RFC 非準拠の HTTP ヘッダーであり、次の形式になります。

```
x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.
```

このヘッダーでは IP アドレスをカンマ区切りにします。左端のアドレスはリモート ユーザのマシンのアドレス、続いて接続要求を転送した一連のプロキシのアドレスが示されます（ヘッダー名を設定可能です）。電子メール セキュリティ アプライアンスは、ヘッダーのリモート ユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセス リストで許可されたユーザ IP アドレスやプロキシ IP アドレスと照合します。



(注) AsyncOS は `x-forwarded-for` ヘッダーでは IPv4 アドレスだけをサポートしません。

アクセス リストの作成

GUI の [Network Access] ページまたは CLI の `adminaccessconfig > ipaccess` コマンドから、ネットワーク アクセス リストを作成できます。図 15-16 は、電子メール セキュリティ アプライアンスへの直接接続が許可されているユーザ IP アドレスのリストが表示された [Network Access] ページを示しています。

図 15-16 ネットワーク アクセス設定
Network Access

Network Access

Web UI Inactivity Timeout: Minutes
Enter a value between 5 - 1440 Minutes (24 hours).

User Access: *Control system access by IP Address, IP Range or CIDR.*

*(Valid entries are an IP address, IP range or CIDR range. Separate multiple entries with commas.
Examples: 10.0.0.1, 10.0.0.1-24, 10.0.0.0/8)*

IP Address of Proxy Server:

(Separate multiple entries with commas.)

Origin IP Header:

AsyncOS はアクセス リストの制御で 4 種類のモードを用意しています。

- [Allow All]。このモードはアプライアンスへの接続をすべて許可します。これが操作のデフォルト モードです。
- [Only Allow Specific Connections]。このモードは、アクセス リストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザの IP アドレスが一致すれば、アプライアンスへの接続を許可します。
- [Only Allow Specific Connections Through Proxy]。このモードは、次の条件を満たせば、逆プロキシ経由でアプライアンスへの接続を許可します。
 - 接続プロキシの IP アドレスがアクセス リストの [IP Address of Proxy Server] フィールドに含まれている。
 - プロキシの接続要求に x-forwarded-header HTTP ヘッダーが記載されている。
 - x-forwarded-header の値が空ではない。

- リモート ユーザの IP アドレスが `x-forwarded-header` に記載され、アクセス リストでユーザに定義された IP アドレス、IP 範囲、CIDR 範囲のいずれかに一致する。
- [Only Allow Specific Connections Directly or Through Proxy]。このモードは、アクセス リストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザの IP アドレスが一致すれば、アプライアンスへの逆プロキシ経由接続または直接接続を許可します。プロキシ経由接続の条件は、[Only Allow Specific Connections Through Proxy] モードと同じです。

次のいずれかの条件が `true` の場合、変更を送信して確定した後、アプライアンスにアクセスできなくなることがありますので注意してください。

- [Only Allow Specific Connections] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [Only Allow Specific Connections Through Proxy] を選択し、現在アプライアンスに接続されているプロキシの IP アドレスがプロキシリストに存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。
- [Only Allow Specific Connections Directly or Through Proxy] を選択し、
 - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合
または
 - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、アプライアンスに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

電子メールセキュリティアプライアンスのアクセスリストを作成するには、次の手順を実行します。

-
- ステップ 1** [System Administration] > [Network Access] ページを使用します。
 - ステップ 2** [Edit Settings] をクリックします。
 - ステップ 3** アクセス リストの制御モードを選択します。
 - ステップ 4** アプライアンスへの接続を許可するユーザの IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを指定する場合は、カンマで区切ります。
 - ステップ 5** プロキシ経由接続が許可されている場合は、次の情報を入力します。
 - アプライアンスへの接続を許可するプロキシの IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。
 - プロキシがアプライアンスに送信した送信元 IP ヘッダーの名前。リモートユーザのマシンおよび要求を転送したプロキシサーバの IP アドレスが記載されています。デフォルトのヘッダー名は `x-forwarded-for` です。
 - ステップ 6** 変更を送信して確定します。
-

Web UI セッション タイムアウトの設定

非アクティブな状態によりログアウトになるまで、電子メールセキュリティアプライアンスの Web UI にログイン可能な期間を指定できます。この Web UI セッション タイムアウトは、**admin** を含むユーザ全員に適用されます。また、HTTP セッションと HTTPS セッションのいずれにも使用されます。

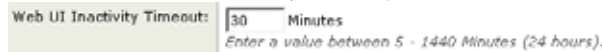
ユーザがログアウトになると、アプライアンスはユーザの Web ブラウザをログイン ページにリダイレクトします。



(注)

[Web UI Session Timeout] は、タイムアウトが 30 分（設定不可）の IronPort スパム検疫セッションには適用されません。

図 15-17 Web UI 非アクティブ タイムアウト



Web UI セッションの非アクティブ タイムアウトを定義するには、次の手順を実行します。

- ステップ 1 [System Administration] > [Network Access] ページを使用します。
- ステップ 2 [Edit Settings] をクリックします。
- ステップ 3 ログアウトになるまでの非アクティブ時間を分単位で入力します。5 ~ 1440 分のタイムアウト期間を定義できます。
- ステップ 4 変更を送信して確定します。

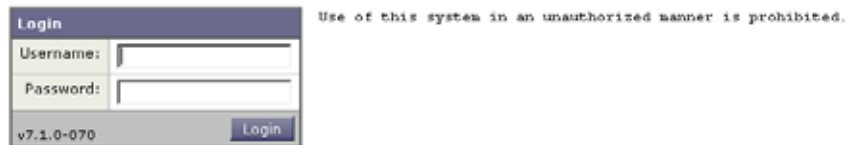
ログイン バナーの追加

ユーザが SSH、Telnet、FTP、または Web UI からログインしようとした際に、「ログイン バナー」と呼ばれるメッセージを表示するように電子メール セキュリティ アプライアンスを設定できます。ログイン バナーは、CLI でログイン プロンプトの上部に表示され、GUI でログイン プロンプトの右側に表示されるカスタマイズ可能なテキストです。ログイン バナーを使用して、内部のセキュリティ情報またはアプライアンスのベスト プラクティスに関する説明を表示できます。たとえば、許可しないアプライアンスの使用を禁止する簡単な注意文言を作成したり、ユーザがアプライアンスに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

CLI の `adminaccessconfig > banner` コマンドを使用して、ログイン バナーを作成します。ログイン バナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログイン バナーは、アプライアンスの `/data/pub/configuration` ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更を確定します。

☒ 15-18 は、Web UI ログイン画面に表示されたログイン バナーを示しています。

図 15-18 バナーが表示された Web UI ログイン画面



システム時刻



Cloud Email Security アプライアンスの時間設定は変更しないことを推奨します。

Cisco IronPort アプライアンスのシステム時刻の設定、使用する時間帯の設定、または NTP サーバとクエリー インターフェイスの選択を行うには、GUI の [System Administration] メニューから [Time Zone] ページまたは [Time Settings] ページを使用するか、CLI の `ntpconfig` コマンド、`settime` コマンドおよび `settz` コマンドを使用します。

AsyncOS で使用される時間帯ファイルは、[System Administration] > [Time Settings] ページ、または tzupdate CLI コマンドで確認することもできます。

時間帯の選択

[Time Zone] ページ (GUI の [System Administration] メニューから利用可能) では、Cisco IronPort アプライアンスの時間帯を表示します。特定の時間帯または GMT オフセットを選択できます。

特定の時間帯を利用して時間帯を定義するには、次の手順を実行します。

- ステップ 1** [System Administration] > [Time Zone] ページで、[Edit Settings] をクリックします。[Edit Time Zone] ページが表示されます。

図 15-19 [Time Zone] ページ

Edit Time Zone

Time Zone Setting	
Time Zones:	Region: America ▼
	Country: United States ▼
	Time Zone: Pacific Time (Los_Angeles) ▼

Cancel Submit

- ステップ 2** 地域、国、および時間帯をプルダウン メニューから選択します。
- ステップ 3** 変更を送信して確定します。

GMT オフセットの選択

GMT オフセットを利用して時間帯を定義するには、次の手順を実行します。

- ステップ 1** [System Administration] > [Time Zone] ページで、[Edit Settings] をクリックします。[Edit Time Zone] ページが表示されます。
- ステップ 2** 地域のリストから [GMT Offset] を選択します。[Time Zone Setting] ページが更新されます。

図 15-20 [Time Zone] ページ

Edit Time Zone

Time Zone Setting		
Time Zone:	Region:	GMT Offset
	Country:	GMT
	Time Zone:	GMT+08 (GMT+8)

Cancel Submit

ステップ 3 [Time Zone] リストでオフセットを選択します。オフセットは、GMT（グリニッジ子午線）に達するために足し引きする必要がある時間を示しています。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の東側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の西側にあたります。

ステップ 4 変更を送信して確定します。

時刻設定の編集（GUI）

Cisco IronPort アプライアンスの時刻設定を編集するには、[System Administration] > [Time Settings] ページの [Edit Settings] ボタンをクリックします。[Edit Time Settings] ページが表示されます。

図 15-21 [Edit Time Settings] ページ

Edit Time Settings

Time Settings	
Time Keeping Method:	<input checked="" type="radio"/> Use Network Time Protocol <input type="radio"/> Set Time Manually
	NTP Server: <input type="text" value="time.ironport.com"/> <input type="button" value="Add Row"/> <input type="button" value="Remove"/> Interface for NTP Server Queries: <input type="text" value="Auto select"/>
	Local Time: MM <input type="text" value="10"/> DD <input type="text" value="20"/> YYYY <input type="text" value="2005"/> HH <input type="text" value="1"/> MM <input type="text" value="19"/> SS <input type="text" value="23"/> <input type="text" value="PM"/>
	<i>Note: manual time set will take place immediately when the Submit button is clicked — it is not necessary to "commit" these changes.</i>

Cancel Submit

ネットワーク タイム プロトコル (NTP) 設定の編集 (Time Keeping Method)

他のコンピュータとのシステム クロックの同期に NTP サーバを使用し、NTP サーバの設定値を編集するには、次の手順を実行します。

- ステップ 1** [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Settings] ページが表示されます。
- ステップ 2** [Time Keeping Method] セクションで、[Use Network Time Protocol] を選択します。
- ステップ 3** NTP サーバのアドレスを入力し、[Add Row] をクリックします。複数の NTP サーバを追加できます。
- ステップ 4** NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。
- ステップ 5** NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。
- ステップ 6** 変更を送信して確定します。

システム時刻の設定 (NTP サーバを使用しない方法)

NTP サーバを使用せずに手動でシステム時刻を設定するには、次の手順を実行します。

- ステップ 1** [System Administration] > [Time Settings] ページで、[Edit Settings] をクリックします。[Edit Time Settings] ページが表示されます。
- ステップ 2** [Time Keeping Method] セクションで、[Set Time Manually] を選択します。
- ステップ 3** 月、日、年、時、分、および秒を入力します。
- ステップ 4** [A.M.] または [P.M.] を選択します。
- ステップ 5** 変更を送信して確定します。



CHAPTER 16

C350D アプライアンスのイネーブル化

C350D/C360D/C370D アプライアンスは、アウトバウンド電子メール配信を専用とした、Cisco IronPort アプライアンスの特殊なモデルです。この章では、C350D アプライアンスに固有な AsyncOS オペレーティング システムのさまざまな機能および変更点について説明します。この章では、C350D、C360D、および C370D アプライアンスは同じアプライアンスを意味します。この章の以降の箇所では、C350D だけが示されていますが、説明されている情報はすべて、C370D および C360D アプライアンスにも適用されます。

この章は、次の内容で構成されています。

- 「[概要 : C350D アプライアンス](#)」 (P.16-1)
- 「[C350D アプライアンスの設定](#)」 (P.16-5)
- 「[IronPort Mail Merge \(IPMM\)](#)」 (P.16-7)

概要 : C350D アプライアンス

C350D アプライアンスは、メールのアウトバウンド配信用に設計および最適化された AsyncOS 変更の機能キーがある、C350/360/370 アプライアンスです。C350D アプライアンスでは、アウトバウンド カスタマー メッセージングの特定のニーズを満たすように、パフォーマンスが劇的に改善されます。

C350D の追加機能

メッセージ配信を最適化するため、C350D アプライアンスには、標準の Cisco IronPort アプライアンスにはない追加機能がいくつかあります。

追加機能

- 256 の仮想ゲートウェイ アドレス : Cisco IronPort Virtual Gateway テクノロジーを使用すると、個別の IP アドレス、ホスト名およびドメインを使用してホストするすべてのドメインのエンタープライズ メール ゲートウェイを設定し、同じ物理アプライアンス内でホストしながら、これらのドメインの個別の企業電子メール ポリシー拡張およびアンチスパム方針を作成できます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照してください。
- IronPort Mail Merge (IPMM) : IronPort Mail Merge (IPMM) を使用すると、個別の個人向けメッセージをカスタマー システムから生成する手間を省くことができます。ユーザは、数千の個別メッセージを生成し、メッセージ生成システムと電子メール ゲートウェイ間で送信する必要がなくなるため、システムにかかる負荷が軽減され、電子メール配信のスループットが向上します。詳細については、「[IronPort Mail Merge \(IPMM\)](#)」(P.16-7) を参照してください。
- リソースを節約するバウンス設定 : C350D アプライアンスでは、ブロックされる可能性がある宛先を検出して、その宛先へのすべてのメッセージをバウンスするように、システムを設定できます。詳細については、「[リソースを節約するバウンス設定の指定](#)」(P.16-6) を参照してください。
- ソフトウェアに基づいたパフォーマンス拡張 : C350D アプライアンスには、アウトバウンド配信パフォーマンスを大幅に拡張するソフトウェア モジュールが含まれています。

C350D でディセーブルにされる機能

C350D アプライアンスでは、AsyncOS オペレーティング システムの一部が変更されています。アウトバウンド電子メール配信やシステム パフォーマンスの改善に適さない、標準 C および X-Series アプライアンスのいくつかの機能は、ディセーブルにされています。次に、これらの変更点と相違点について説明します。

適していない機能

- **IronPort Anti-Spam スキャンおよびオン/オフボックス スпам検査**：アンチスパム スキャンは、通常、着信メールに関係するため、IronPort Anti-Spam スキャン エンジンがディセーブルにされます。そのため、第 9 章は適用されません。
- **感染フィルタ**：Cisco IronPort の感染フィルタ機能は、着信メールの検査に使用されるため、この機能は C350D ではディセーブルにされています。そのため、第 11 章は適用されません。
- **SenderBase Network Participation 機能**：SenderBase Network Participation は、着信メールに関する情報を報告するため、この機能は、C350D アプライアンスではディセーブルにされています。そのため、第 8 章および第 12 章は適用されません。
- **レポート**：レポート機能は限定されます。一部のレポートは使用できません。発生するレポートも、パフォーマンス問題のため、非常に限定的なレベルで実行するように設定されています。
- **RSA Data Loss Prevention**：発信メッセージの RSA DLP スキャンは、C350D アプライアンスでディセーブルにされています。
- これらの機能が C350D アプライアンスでディセーブルにされている場合であっても、350D アプライアンスの電子メールセキュリティ モニタ概要レポートに示される合計には、スパムおよび疑わしいスパムの数が誤って含まれることがあります。

C350D に適用される AsyncOS 機能

C350D アプライアンスには、最新の AsyncOS 機能のほとんどが含まれています。これらの機能の多くは、C350D ユーザにとって魅力的な機能です。表 16-1 に、これらの機能の一部を示します。

表 16-1 C350D アプライアンスに含まれる AsyncOS 機能

機能	追加情報
DomainKeys 署名	DKIM/DomainKeys は、送信者により使用される署名キーに基づいて電子メールの信頼性を確認する方式です。『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Email Authentication」の章を参照してください。
集中管理	『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Centralized Management」の章を参照してください。
配信スロットリング	各ドメインに対して、一定期間でシステムが超えることができない、接続および受信者の最大数を割り当てることができます。「グッドネイバー」テーブルは、destconfig コマンドで定義されます。 詳細については、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Delivery Features」の章の「Controlling Email Delivery」の項を参照してください。
バウンス検証	バウンス メッセージの信頼性を検証します。『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Configuring Routing and Delivery Features」の章にある「Cisco IronPort Bounce Verification」の項を参照してください。
委任管理	ユーザの追加については、『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Common Administrative Tasks」の章を参照してください。
トレース (デバッグ)	「Debugging Mail Flow Using Test Messages: Trace」(P.446) を参照してください。

表 16-1 C350D アプライアンスに含まれる AsyncOS 機能 (続き)

機能	追加情報
VLAN、NIC ペアリング	『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Advanced Network Configuration」の章を参照してください。
オプションのアンチウイルス エンジン	オプションのアンチウイルス スキャンを追加することで、アウトバウンド メッセージの完全性を保障できます。「 アンチウイルス スキャン 」(P.9-2) を参照してください。

C350D アプライアンスの設定

C350D をイネーブルにするには、次の手順を実行します。

- ステップ 1** 提供されている機能キーを適用します。 *System Setup Wizard* を実行する前 (アプライアンスを設定する前) に、このキーを C350D Cisco IronPort 電子メールセキュリティ アプライアンスに適用する必要があります。キーの適用は、[System Administration] > [Feature Key] ページを介して、または CLI の `featurekey` コマンドを入力して行います。



(注) 前述の機能キーには、サンプルの Sophos または McAfee Anti-Virus の 30 日間ライセンスが含まれています。これは、アウトバウンド メールでのアンチウイルス スキャンのテストに使用できます。

- ステップ 2** アプライアンスをリポートします。
- ステップ 3** System Setup Wizard (GUI または CLI) を実行して、アプライアンスを設定します。

Cisco IronPort C350D アプライアンスには、アンチスパム スキャンまたは感染フィルタ機能が含まれていないことに注意してください (コンフィギュレーション ガイドのこれらの章は無視してください)。



(注) クラスタ化された環境では、C350D アプライアンスを、配信パフォーマンス パッケージでは設定されない AsyncOS アプライアンスと組み合わせることはできません。

リソースを節約するバウンス設定の指定

C350D アプライアンスが設定されていると、潜在的な配信問題を検出して、宛先のすべてのメッセージをバウンスするように、システムを設定できます。



(注)

この設定を使用すると、配信不能と見なされる宛先ドメインのキューのすべてのメッセージがバウンスされます。メッセージは、配信問題が解決された後で再送信する必要があります。

リソースを節約するバウンス設定をイネーブルにする例

```
mail3.example.com> bounceconfig
```

```
Choose the operation you want to perform:
```

- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
- SETUP - Configure global bounce settings.

```
[> setup
```

```
Do you want to bounce all enqueued messages bound for a domain if the  
host is down? [N]> y
```

この機能を使用する場合、最新の接続試行が 10 回連続で失敗すると、ホストは「ダウン」と見なされます。AsyncOS は、ダウン ホストを 15 分ごとにスキャンします。そのため、接続は、キューがクリアされる前に 11 回以上試行されます。

IronPort Mail Merge (IPMM)



(注) IronPort Mail Merge は、IronPort C350D アプライアンスだけで使用できます。

概要

IronPort Mail Merge を使用すると、個別の個人向けメッセージをカスタマー システムから生成する手間を省くことができます。ユーザは、数千の個別メッセージを生成し、メッセージ生成システムと電子メール ゲートウェイ間で送信する必要がなくなるため、システムにかかる負荷が軽減され、電子メール配信のスループットが向上します。

IPMM では、個人向けに置換されるメッセージの場所を表す変数を使用して、各メッセージの本文が作成されます。各メッセージ受信者に対して、受信電子メールアドレスおよび変数置換だけを電子メール ゲートウェイに送信する必要があります。また、IPMM を使用して、受信者に応じて、送信するメッセージの本文の特定の「パーツ」を含めたり、除外したりできます（たとえば、2 つの異なる国の受信者に送信するメッセージの最後に異なる著作権宣言文を含めることができます）。

利点

Cisco IronPort C350D アプライアンスの Mail Merge 機能を使用すると、次のような多くの利点があります。

- メール管理者にとって使いやすい。IPMM は、変数置換および一般的な多くの言語の抽象化インターフェイスを提供するため、各受信者の個人向けメッセージを簡単に作成できます。
- メッセージ生成システムの負荷を軽減する。メッセージ本文の 1 つのコピーと必須の置換のテーブルだけが必要であるため、ほとんどのメッセージ生成「作業」をメッセージ生成システムから Cisco IronPort C350D アプライアンスに移行して、負荷を軽減できます。
- 配信スループットが改善される。数千の着信メッセージを受け取り、キューに入れるために必要なリソースを軽減することで、Cisco IronPort アプライアンスは、アウトバウンド配信パフォーマンスを大幅に改善できます。

- キュー ストレージの効率性が向上する。各メッセージ受信に保存する情報を減らすことで、ユーザは、C350D アプライアンスのキュー ストレージの使用効率を大幅に向上できます。

Mail Merge の使用

SMTP インジェクション

IPMM は、SMTP をトランスポート プロトコルとして拡張します。Cisco IronPort C350D アプライアンスで行う特別な設定は必要ありません (デフォルトでは、IPMM は、プライベート リスナーでイネーブルにして、Cisco IronPort C350D 電子メール セキュリティ アプライアンスのパブリック リスナーでディセーブルにできます)。ただし、現在、SMTP をインジェクション プロトコルとして使用していない場合は、Cisco IronPort C350D アプライアンス インターフェイスを介して SMTP を利用する新しいプライベート リスナーを作成する必要があります。

リスナーの設定の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「**Customizing Listeners**」の章を参照してください。listenerconfig の setipmm サブコマンドを使用して、インジェクタで IPMM をイネーブルにします。

IPMM は、MAIL FROM と DATA の 2 つのコマンドを変更し、XDFN を追加することで、SMTP を変更します。MAIL FROM コマンドは XMRG FROM に、DATA コマンドは XPRT に置き換えられています。

Mail Merge メッセージを生成するには、メッセージの生成に使用されるコマンドを特定の順序で発行する必要があります。

-
- ステップ 1** 送信ホストを示す、初期 EHLO ステートメント。
 - ステップ 2** 各メッセージは、送信者アドレスを示す、XMRG FROM: ステートメントで始まります。
 - ステップ 3** 各受信者は、次のように定義されます。
 - 1 つ以上の XDFN 変数割り当てステートメントが含まれます。これには、パーツ定義 (XDFN *PART=1,2,3...) やその他の任意の受信者固有の変数が含まれます。

- 受信者電子メール アドレスは、RCPT TO: ステートメントで定義されま
す。RCPT TO: の前にあり、前述の XMRG FROM または RCPT TO コ
マンドの後にある任意の変数割り当ては、この受信者電子メール アドレ
スにマッピングされます。

ステップ 4 各パーツは、XPRT n コマンドを使用して定義されます。各パーツは、DATA コ
マンドと同様にピリオド (.) 文字で終了します。最後のパーツは、XPRT n
LAST コマンドで定義されます。

変数置換

メッセージ ヘッダーなど、メッセージ本文の任意のパーツに、置換用の変数を
含めることができます。変数は、HTML メッセージにも表示できます。変数は、
ユーザが定義し、アンパサンド (&) 文字で始まり、セミコロン (;) で終了する
必要があります。アスタリスク (*) で始まる変数名は、予約されているため使
用できません。

予約変数

IPMM には、事前に定義されている 5 つの特殊な「予約」変数が含まれます。

表 16-2 IPMM : 予約変数

*FROM	予約変数 *FROM は、「Envelope From」パラメータから派生しま す。「Envelope From」パラメータは、「XMRG FROM:」コマ ンドにより設定されます。
*TO	予約変数 *TO は、「RCPT TO:」コマンドで設定される、エンベ ロープ受信者値から派生します。
*PARTS	予約変数 *PARTS は、パーツのカンマ区切りリストを含みます。 これは、「RCPT TO:」で受信者を定義する前に設定され、特定の ユーザが受信する「XPRT n」メッセージ本文ブロックを決定しま す。
*DATE	予約変数 *DATE は、現在の日付スタンプに置き換えられます。
*DK	予約変数 *DK は、DomainKeys 署名プロファイルの指定に使用さ れます (このプロファイルはすでに AsyncOS に存在している必 要があります)。DomainKeys 署名プロファイルの作成の詳細につ いては、『Cisco IronPort AsyncOS for Email Advanced Configuration Guide』の「Email Authentication」の章を参照し てください。

たとえば、次の例のメッセージ本文（ヘッダーを含む）には、最後のメッセージで置換される、4 つの異なる変数と 5 つの置換用の場所が含まれます。同じ変数がメッセージ本文で複数回使用されることがあるため注意してください。また、予約変数 `&*TO;` が使用されます。これは、受信者の電子メール アドレスに置換されます。この予約変数は、個別の変数として渡す必要はありません。次の例の変数は太字で示されています。

メッセージの例 1

From: Mr.Spacely <spacely@sprockets.com>

To: **&first_name;** &last_name; **&*TO;**

Subject: Thanks for Being a Spacely Sprockets Customer

Dear **&first_name;**,

Thank you for purchasing a **&color;** sprocket.

このメッセージは、Cisco IronPort C350D アプライアンスに一度だけインジェクトする必要があります。各受信者に対して、次の追加情報が必要です。

- 受信者の電子メール アドレス
- 変数置換の名前と値のペア

パーツ アセンブリ

SMTP は、各メッセージ本文に単一の DATA コマンドを使用し、IPMM は、1 つ以上の XPRN コマンドを使用してメッセージを作成します。パーツは、受信者ごとに指定される順序に従ってアセンブルされます。各受信者は、任意またはすべてのメッセージ パーツを受信できます。パーツは、任意の順序でアセンブルできます。

特殊な変数 `*PARTS` は、パーツのカンマ区切りリストを含みます。

たとえば、次の例のメッセージでは、2 つのパーツが含まれます。

最初のパーツには、メッセージ ヘッダーとメッセージ本文の一部が含まれます。2 番目のパーツには、特別なカスタマー向けに含めることができる割引価格が含まれます。

メッセージの例 2 (パーツ 1)

From: Mr. Spacely <spacely@sprockets.com>

To: **&first_name;** **&last_name;** **&*TO;**

Subject: Thanks for Being a Spacely Sprockets Customer

Dear **&first_name;**,

Thank you for purchasing a **&color;** sprocket.

メッセージの例 2 (パーツ 2)

Please accept our offer for 10% off your next sprocket purchase.

メッセージ部分は、Cisco IronPort C350D アプライアンスに一度だけインジェクトする必要があります。この場合、各受信者に、次の追加情報が必要です。

- 最後のメッセージに含まれる、パーツの順序付きリスト
- 受信者の電子メール アドレス
- 変数置換の名前と値のペア

IPMM および DomainKeys 署名

IPMM は、DomainKeys 署名をサポートします。DomainKeys プロファイルを指定するには、*DK 予約変数を使用します。次の例を参考にしてください。

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2
*DK=mass_mailing_1
```

この例では、「mail_mailing_1」は、前に設定した DomainKeys プロファイルの名前です。

コマンドの説明

クライアントは、IPMM メッセージをリスナーにインジェクトするときに、次のキー コマンドで拡張 SMTP を使用します。

XMRG FROM

構文：

```
XMRG FROM: <sender email address>
```

このコマンドは、SMTP MAIL FROM: コマンドの代わりに使用されます。これは、次に IPMM メッセージがあることを示します。IPMM ジョブは、XMRG FROM: コマンドで開始されます。

XDFN

構文：

```
XDFN <KEY=VALUE> [KEY=VALUE]
```

XDFN コマンドは、受信者別のメタデータを設定します。キーと値のペアは、オプションでかぎカッコまたは角カッコで囲むことができます。

*PARTS は、XPRT コマンド（以下を参照）で定義されているように、インデックス番号を示す特殊な予約変数です。*PARTS 変数は、整数のカンマ区切りリストとして分割されます。整数は、XPRT コマンドにより定義されているように送信される本文パーツと一致します。その他の予約変数には、*FROM、*TO および *DATE があります。

XPRT

構文：

```
XPRT index_number LAST
```

Message

.

XPRT コマンドは、SMTP DATA コマンドの代わりに使用されます。このコマンドは、コマンド入力後にメッセージ パーツの送信者を受け取ります。コマンドは、行の末尾に単一のピリオドを付けて完了します（これは、SMTP DATA コマンドを完了する方法と同じです）。

特殊キーワード **LAST** は、Mail Merge ジョブの最後を示します。これは、インジェクトされる最後のパーツを指定するときに使用する必要があります。

LAST キーワードが使用されると、メッセージがキューに入り、配信が始まります。

変数定義に関する注意事項

- XDFN コマンドで変数を定義する場合、実際のコマンドラインは、システムの物理的制限を超えることはできないため注意してください。Cisco IronPort C350D アプライアンスの場合、この制限は、1 行あたり 4 KB です。ホスト システムによっては、しきい値がこれより低くなる場合があります。非常に長いコマンドラインで複数の変数を定義する場合は注意してください。
- 変数キーと値のペアを定義する場合、スラッシュ「/」文字を使用して、特殊文字をエスケープできます。これは、メッセージ本文に、誤って変数定義と置換される可能性がある HTML 文字エンティティが含まれる場合に役に立ちます（たとえば、文字エンティティ `™` は、商標文字の HTML 文字エンティティを定義します）。コマンド `XDFN trade=foo` を作成して、HTML 文字エンティティ「`™`」を含む IPMM メッセージを作成した場合、アセンブルされるメッセージには、商標文字ではなく、変数置換（「`foo`」）が含まれます。これは、GET コマンドを含む URL で使用されることがあるアンパサンド文字「`&`」の場合も同じです。

IPMM カンバセーションの例

次に、メッセージの例 2（前述の例）での IPMM カンバセーションの例を示します。このメッセージは、この例の 2 人の受信者「Jane User」および「Joe User」に送信されます。

この例では、**太字**フォントは、Cisco IronPort C350D アプライアンスとの手動による SMTP カンバセーションで入力する内容です。また、モノスペース タイプのフォントは、SMTP サーバからの応答を表し、イタリック体フォントは、コメントまたは変数を表します。

接続が確立されます。

```
220 ESMTTP
```

```
EHLO foo
```

```
250-ehlo responses from the injector enabled for IPMM
```

カンバセーションが開始されます。

```
XMRG FROM:<user@domain.com> [Note: This replaces the MAIL FROM: SMTP command.]
```

```
250 OK
```

変数およびパーツが各受信者に設定されます。

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2
```

```
[Note: This line defines three variables (first_name, last_name, and color) and then uses the *PARTS reserved variable to define that the next recipient defined will receive message parts numbers 1 and 2.]
```

```
250 OK
```

```
RCPT TO:<jane@example.com>
```

```
250 recipient <jane@example.com> ok
```

```
XDFN first_name="Joe" last_name="User" color="black" *PARTS=1
```

*[Note: This line defines three variables (first_name, last_name, and color) and then uses the *PARTS reserved variable to define that the next recipient defined will receive message parts numbers 1 only.]*

RCPT TO:<joe@example.com>

250 recipient <joe@example.com> ok

次に、パーツ 1 が送信されます。

XPRT 1 *[Note: This replaces the DATA SMTP command.]*

354 OK, send part

From: Mr. Spacely <spacely@sprockets.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being a Spacely Sprockets Customer

&*DATE;

Dear &first_name;;

Thank you for purchasing a &color; sprocket.

.

次に、パーツ 2 が送信されます。LAST キーワードは、パーツ 2 がアセンブルする最後のパーツであることを示すときに使用されます。

XPRT 2 LAST

Please accept our offer for 10% off your next sprocket purchase.

.

250 Ok, mailmerge message enqueued

「250 Ok, mailmerge message queued」は、メッセージが受け取られたことを示します。

この例に基づいて、受信者 **Jane User** は、このメッセージを受信します。

From: Mr. Spacely <spacely@sprockets.com>
To: Jane User <jane@example.com>
Subject: Thanks for Being a Spacely Sprockets Customer

message date

Dear Jane,

Thank you for purchasing a red sprocket.

Please accept our offer for 10% off your next sprocket purchase.

受信者 **Joe User** は、このメッセージを受信します。

From: Mr. Spacely <spacely@sprockets.com>
To: Joe User <joe@example.com>
Subject: Thanks for Being a Spacely Sprockets Customer

```
message date
```

```
Dear Joe,
```

```
Thank you for purchasing a black sprocket.
```

コード例

IronPort は、一般的なプログラミング言語でライブラリを作成して、IPMM メッセージを IPMM 対応の Cisco IronPort アプライアンス リスナーにインジェクトするタスクを抽象化します。IPMM ライブラリの使用例については、Cisco IronPort カスタマー サポートにお問い合わせください。コードは、構文説明のために広範囲にわたってコメント化されています。



CHAPTER 17

Cisco IronPort M-Series セキュリティ管理アプライアンス

Cisco IronPort M-Series アプライアンスは、他の Cisco IronPort アプライアンスと組み合わせて使用する、外部または「オフボックス」のスパム検疫として機能することを特に目的とした、Cisco IronPort アプライアンスの特別なモデルです。この章では、Cisco IronPort M-Series アプライアンスのネットワーク プランニング、システム セットアップ、および一般的な用途を説明します。

この章は、次の内容で構成されています。

- 「概要」(P.17-1)
- 「ネットワーク プランニング」(P.17-2)
- 「モニタリング サービスの設定」(P.17-5)

概要

Cisco IronPort M-Series セキュリティ管理アプライアンスを使用すると、Cisco IronPort 電子メールセキュリティ アプライアンスの機能を補完できます。Cisco IronPort M-Series セキュリティ管理アプライアンスは、企業のポリシー設定値および監査情報をモニタする外部または「オフボックス」の場所として機能することを目的としています。ハードウェア、オペレーティング システム (AsyncOS)、および補助サービスを組み合わせて重要なポリシーと実行時データの集中化と統合を行うことにより、Cisco IronPort C-Series と X-Series の電子メールセキュリティ アプライアンスで使用するレポート情報および監査情報を管理者およびエンド ユーザが管理するための単一インターフェイスになります。Cisco IronPort M-Series アプライアンスを使用すると、Cisco IronPort 電子メールセキュリティ アプライアンスの性能を十分に引き出すことができ、配置の柔

軟性を高めることで企業ネットワークの整合性が保護されます。セキュリティ運用を単一の Cisco IronPort M-Series アプライアンスから行うように調整することも、複数のアプライアンス間で負荷を分散するように調整することもできます。

セキュリティ管理アプライアンスの AsyncOS には次の機能が含まれています。

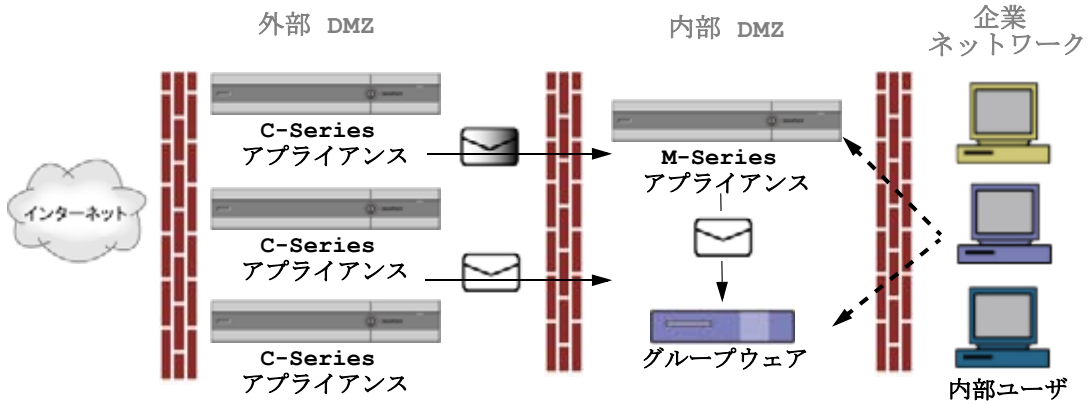
- 外部 IronPort スпам検疫。エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 中央集中型レポート。複数の電子メール セキュリティ アプライアンスから集約されたデータに対してレポートを実行します。
- 中央集中型トラッキング。複数の電子メール セキュリティ アプライアンスを横断して電子メール メッセージを追跡します。

Cisco IronPort セキュリティ管理アプライアンスの設定および使用については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

ネットワーク プランニング

Cisco IronPort M-Series アプライアンスを使用すると、エンド ユーザ インターフェイス（メール アプリケーションなど）を、さまざまな DMZ 内のよりセキュアなゲートウェイ システムから切り離すことができます。2 層ファイアウォールの使用によって、ネットワーク プランニングの柔軟性が高まり、エンドユーザが外部 DMZ に直接接続することを防止できます（[図 17-1](#) を参照）。

図 17-1 Cisco IronPort M-Series アプライアンスを含む一般的なネットワーク設定



大規模な企業データセンターでは、外部 IronPort スпам検疫として機能している 1 台の Cisco IronPort M-Series アプライアンスを、1 台または複数台の Cisco IronPort C-Series または X-Series アプライアンスで共有できます。さらに、ローカル使用のために独自のローカル Cisco IronPort アプライアンス検疫を保守するリモートオフィスをセットアップできます (C-Series または X-Series アプライアンス上でローカル IronPort スпам検疫を使用)。

図 17-1 に、Cisco IronPort M-Series アプライアンスおよび複数の DMZ を含む、通常のネットワーク設定を示します。インターネットからの着信メールは、外部 DMZ の Cisco IronPort アプライアンスによって受信されます。正規のメールは、内部 DMZ の MTA (グループウェア) に従って、最終的に企業ネットワーク内のエンドユーザまで送信されます。

スパムおよび陽性と疑わしいスパム (メールフローポリシー設定値に基づく) は、Cisco IronPort M-Series アプライアンスのスパム検疫エリアに送信されます。次にエンドユーザが検疫エリアにアクセスして、スパムを削除し、自分宛に配信されるメッセージを解放することを選択できます。IronPort スпам検疫エリアに残っているメッセージは、設定可能な期間の経過後に自動的に削除されます (『Cisco IronPort AsyncOS for Email Daily Management Guide』の「Quarantines」の章を参照)。

メール フローおよび Cisco IronPort M-Series アプライアンス

メールは、他の Cisco IronPort (C-Series および X-Series) アプライアンスから Cisco IronPort M-Series アプライアンスに送信されます。Cisco IronPort M-Series アプライアンスにメールを送信するように設定された Cisco IronPort アプライアンスは、その M-Series アプライアンスからリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。メッセージは、HAT などのポリシーやスキャン設定をバイパスして配信されます。これを機能させるために、Cisco IronPort M-Series アプライアンスの IP アドレスが変わらないようにしてください。Cisco IronPort M-Series アプライアンスの IP アドレスが変わると、受信側の C-Series または X-Series のアプライアンスは、メッセージを他の着信メッセージであるものとして処理します。Cisco IronPort M-Series アプライアンスの受信と配信では、常に同じ IP アドレスを使用する必要があります。

Cisco IronPort M-Series アプライアンスでは、IronPort スпам検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。Cisco IronPort M-Series アプライアンスでローカル検疫を設定するには、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。Cisco IronPort M-Series アプライアンスのローカル検疫は、M-Series アプライアンスにメールを送信する他の Cisco IronPort アプライアンスからは、外部の検疫と見なされることに注意してください。

Cisco IronPort M-Series アプライアンスによって解放されたメールは、スパム検疫設定の定義に従って、プライマリ ホストおよびセカンダリ ホスト (Cisco IronPort アプライアンスまたは他のグループウェア ホスト) に配信されます (『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照)。したがって、Cisco IronPort M-Series アプライアンスにメールを配信する Cisco IronPort アプライアンスの数に関係なく、解放されるすべてのメール、通知、およびアラートが単一のホスト (グループウェアまたは Cisco IronPort アプライアンス) に送信されます。Cisco IronPort M-Series アプライアンスからの配信によってプライマリ ホストが過負荷にならないように注意してください。

モニタリング サービスの設定

中央集中型レポーティングまたは中央集中型トラッキングのためや、外部 IronPort スпам検疫としてセキュリティ管理アプライアンスを使用するには、まず、電子メールセキュリティアプライアンス上にモニタリング サービスを設定（構成）する必要があります。

電子メールセキュリティアプライアンス上にモニタリング サービスを設定するときは、セキュリティ管理アプライアンス上でモニタリング サービスをイネーブルにする必要もあります。詳細については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。

モニタリング サービスは、電子メールトラフィックに関するレポートを実行したり、メッセージルーティングを追跡したり、スパムの疑いがあるメッセージおよびスパムメッセージを外部 IronPort スпам検疫エリアに配信したりするために使用します。次の 1 つまたは複数のサービスを設定できます。

- **中央集中型レポーティング**。詳細については、「[中央集中型レポーティングを使用するための電子メールセキュリティアプライアンスの設定](#)」(P.17-5) を参照してください。
- **中央集中型トラッキング**。詳細については、「[中央集中型トラッキングを使用するための電子メールセキュリティアプライアンスの設定](#)」(P.17-7) を参照してください。
- **IronPort スпам検疫**。詳細については、「[外部 IronPort スпам検疫を使用するための電子メールセキュリティアプライアンスの設定](#)」(P.17-8) を参照してください。

中央集中型レポーティングを使用するための電子メールセキュリティアプライアンスの設定

電子メールセキュリティアプライアンスに対する中央集中型レポーティングの設定は随時行うことができます。通常は、セキュリティ管理アプライアンスで監視機能をイネーブルにしてから中央集中型レポーティングを設定します。



(注)

中央集中型レポーティングをイネーブルにする前に、十分なディスク容量が監視サービスに割り当てられていることを確認してください。

電子メールセキュリティアプライアンスで中央集中型レポーティングをイネーブルにする手順は、次のとおりです。

- ステップ 1** [Security Services] > [Reporting] をクリックします。
[Reporting Service Settings] ページが表示されます。

図 17-2 [Reporting Service Settings] ページ
Reporting Service Settings



- ステップ 2** [Reporting Service] セクションで [Centralized Reporting] オプションを選択します。
- ステップ 3** 変更を送信して確定します。



(注)

中央集中型レポーティングを使用するには、電子メールセキュリティアプライアンスおよびセキュリティ管理アプライアンスで監視機能をイネーブルにする必要があります。セキュリティ管理アプライアンス上での中央集中型レポーティングのイネーブル化については、『Cisco IronPort AsyncOS for Security Management User Guide』を参照してください。

中央集中型レポーティング モード

中央集中型レポーティングを使用するように電子メールセキュリティアプライアンスを設定し、管理対象アプライアンスとしてセキュリティ管理アプライアンスに追加すると、電子メールセキュリティアプライアンスは、中央集中型レポーティングモードで動作するようになります。電子メールセキュリティアプライアンスが中央集中型レポーティングモードになっている場合、そのアプライアンスのスケジュール済みレポートは中断され、そのアプライアンスのスケジュール済みレポートの設定ページやアーカイブされたレポートを利用できません。また、そのアプライアンスで保存するデータは 1 週間分だけになります。月次レポートおよび年次レポート用の新規データは、セキュリティ管理アプライアンスに保存されます。電子メールセキュリティアプライアンスにある月次レ

ポート用の既存データは、セキュリティ管理アプライアンスに転送されません。中央集中型レポーティングをディセーブルにすると、電子メールセキュリティアプライアンスで新規月次レポートデータの保存が開始されます。

電子メールセキュリティアプライアンスで中央集中型レポーティングをディセーブルにすると、スケジュール済みレポートが再開されて、アーカイブされたレポートを利用できるようになります。中央集中型レポーティングをディセーブルにした場合に、電子メールセキュリティアプライアンスでは、過去の時間および日ごとのデータだけが表示され、過去の週ごとや月ごとのデータは表示されません。これは、一時的な変更です。十分なデータが蓄積されれば、過去の週および月のレポートが表示されます。電子メールセキュリティアプライアンスを中央集中型レポーティングモードに戻した場合、過去の週のデータはインタラクティブレポートに表示されます。

中央集中型トラッキングを使用するための電子メールセキュリティアプライアンスの設定

電子メールセキュリティアプライアンスは、ローカル（オンボックス）トラッキングまたは中央集中型トラッキングのいずれかを使用するように設定できます。



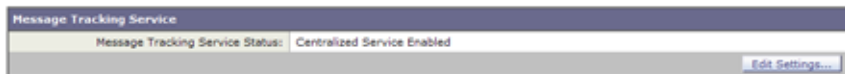
(注)

1 台の電子メールセキュリティアプライアンスで中央集中型とローカルの両方のトラッキングをイネーブルにはできません。

電子メールセキュリティアプライアンスで中央集中型トラッキングをイネーブルにする手順は、次のとおりです。

- ステップ 1** [Security Services] > [Message Tracking] をクリックします。
[Message Tracking Service] ページが表示されます。

図 17-3 [Message Tracking Service] ページ
Message Tracking Service



- ステップ 2** [Message Tracking Service] セクションで [Edit Settings] をクリックします。

図 17-4 [Message Tracking Service Settings] ページ
Message Tracking Service Settings

- ステップ 3** [Enable Message Tracking Service] チェックボックスを選択します。
- ステップ 4** [Centralized Tracking] オプションを選択します。
- ステップ 5** 必要に応じて、拒否された接続の情報を保存するチェックボックスを選択します。



(注) 拒否された接続のトラッキング情報を保存すると、セキュリティ管理アプライアンスのパフォーマンスに悪影響を与えるおそれがあります。

- ステップ 6** 変更を送信して確定します。



(注) 中央集中型トラッキングを使用するには、電子メールセキュリティアプライアンスおよびセキュリティ管理アプライアンスで監視機能をイネーブルにする必要があります。セキュリティ管理アプライアンス上での中央集中型トラッキングのイネーブル化については、『Cisco IronPort AsyncOS for Security Management User Guide』を参照してください。

外部 IronPort スпам検疫を使用するための電子メールセキュリティアプライアンスの設定

セキュリティ管理アプライアンスを IronPort スпам検疫として使用するには、電子メールセキュリティアプライアンスで外部スпам検疫機能をイネーブルにする必要があります。外部スпам検疫エリアに接続するために電子メールセキュリティアプライアンスで使用する、IP アドレスとポート番号を指定する必要があります。

電子メールセキュリティアプライアンスでセキュリティ管理アプライアンスを外部 IronPort スпам検疫として使用できるようにする手順は、次のとおりです。

- ステップ 1** [Security Services] > [External Spam Quarantine] をクリックします。
[External Spam Quarantine] ページが表示されます。
- ステップ 2** [Configure] をクリックします。
[Configure External Spam Quarantine] ページが表示されます。

図 17-5 [Configure External Spam Quarantine] ページ
Configure External Spam Quarantine

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	IronPort_Spam_Quarantine (e.g. spam_quarantine)
IP Address:	111.111.1.11
Port:	9025
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: Quarantine
<input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

- ステップ 3** [External Spam Quarantine] セクションで、[Enable External Spam Quarantine] チェックボックスを選択します。
- ステップ 4** [Name] フィールドにセキュリティ管理アプライアンスの名前を入力します。
- ステップ 5** IP アドレスおよびポート番号を入力します。セキュリティ管理アプライアンスの IP アドレスおよびポート番号は、[IronPort Spam Quarantine] ページで設定します。
- ステップ 6** 必要に応じて、エンドユーザ セーフリスト/ブロックリスト機能をイネーブルにするチェックボックスを選択し、適切なブロックリストアクションを指定します。
- ステップ 7** 変更を送信して確定します。

IronPort スпам検疫およびエンドユーザ セーフリスト/ブロックリスト機能の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。M-Series アプライアンスで IronPort スпам検疫を使用する場合の詳細については、『*Cisco IronPort AsyncOS for Security Management User Guide*』を参照してください。



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

サービス	デフォルトポート	デフォルトでイネーブルかどうか	
		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、Cisco IronPort C10/100 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。

- 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-6) 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пам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 Interfaces

Network Interfaces and IP Addresses			
Add IP Interface...			
Name	IP Address	Hostname	Delete
Data 1	172.19.1.86/24	buttercup.run	🗑
Data 2	172.19.2.86/24	buttercup.run	🗑
Management	172.19.0.86/24	buttercup.run	🗑

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。また、Cisco 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（0xffffffff00 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	Cisco 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。

表 A-2 IP インターフェイスのコンポーネント (続き)

ホスト名	インターフェイスに関連するホスト名。SMTP カンパセーション時に、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пам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пам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 Cisco 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
Add IP Interface

- 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пам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を選択できます。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せん。

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
Edit IP Interface

IP Interface Settings		
Name:	Management	
Ethernet Port:	Management	
IP Address:	172.19.0.11 *	
Netmask:	255.255.255.0 *	
Hostname:	elroy.run	
Services:	Service	Port
	<input checked="" type="checkbox"/> FTP	21
	<input checked="" type="checkbox"/> Telnet	23
	<input checked="" type="checkbox"/> SSH	22 *



(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-8) 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	[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。
/bounces	
/cli_logs	
/delivery	
/error_logs	
/ftpd_logs	
/gui_logs	
/mail_logs	
/rptd_logs	
/sntpd.logs	
/status	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。
/system_logs	

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	<p>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。</p> <p>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。</p>
/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	<p>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。</p> <ul style="list-style-type: none"> • 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

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
```

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、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 Administrative 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.3-14)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

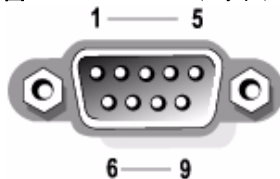


表 A-4 シリアルポートのピン割り当て

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

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
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 グラウンド



APPENDIX **B**

ネットワーク アドレスと IP アドレスの割り当て

この付録では、ネットワーク アドレスと IP アドレスの割り当てに関する一般的なルールについて説明し、ネットワークに Cisco IronPort アプライアンスを接続するための戦略の一部を示します。

この付録の主なトピックは次のとおりです。

- 「イーサネット インターフェイス」(P.B-1)
- 「IP アドレスとネットマスクの選択」(P.B-2)
- 「Cisco IronPort アプライアンスの接続時の戦略」(P.B-5)

イーサネット インターフェイス

Cisco IronPort X1000/1050/1060/1070、C600/650/660/670、および C300/350/360/370 アプライアンスには、システムの背面パネルに構成に応じて 4 つものイーサネット インターフェイスが搭載されています (オプションの光 ネットワーク インターフェイスの有無を問いません)。これらには次のようなラベルが付けられています。

- Management
- Data1
- Data2
- Data3
- Data4

Cisco IronPort C60 および C30 アプライアンスには、システムの背面パネルにイーサネット インターフェイスが 3 つ搭載されています。これらには次のようなラベルが付けられています。

- Management
- Data1
- Data2

Cisco IronPort C10/100/150/160 アプライアンスには、システムの背面パネルにイーサネット インターフェイスが 2 つ搭載されています。これらには次のようなラベルが付けられています。

- Data1
- Data2

IP アドレスとネットマスクの選択

ネットワークを設定する場合、Cisco IronPort アプライアンスが発信パケットを送信するインターフェイスを一意に選択できる必要があります。この要件により、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関する一部の内容が決定されます。単一のネットワークに配置できるインターフェイスは 1 つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、特定のネットワーク上の物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとして任意の IP アドレスを 1 つ使用して、インターフェイスからパケットを送信できます。このプロパティは、**Virtual Gateway** テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホストアドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホストアドレスは IP アドレスの残りのビットです。4 オクテットアドレスの有効ビット数は、**Classless Inter-Domain Routing (CIDR; クラスレス ドメイン間ルーティング)** スタイルで表現されることがあります。すなわち、ビット数（1 ~ 32）の先頭にスラッシュが付きます。

ネットマスクはこうした表現を、単純にバイナリ表記で 1 を数える形で行うことができます。したがって 255.255.255.0 は「/24」となり、255.255.240.0 は「/20」となります。

インターフェイスの設定例

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。Cisco IronPort アプライアンスの場合、これらのインターフェイス名は、3 つの Cisco IronPort インターフェイス (Management、Data1、Data2) のうちのいずれか 2 つを表します。

ネットワーク 1:

インターフェイスはそれぞれ、別々のネットワークに配置する必要があります。

インターフェイス	IP アドレス	ネットマスク	ネットアドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.x にアドレス指定されたデータ (ここで X は自身のアドレスを除く 1 ~ 255 のいずれか。この場合は 10) は、Int1 に進みます。192.168.0.x にアドレス指定されたデータはすべて、Int2 に進みます。このような形式に該当しないその他のアドレス (WAN やインターネット上のアドレスである可能性が高い) が指定されているパケットはデフォルトのゲートウェイに送信されます。このゲートウェイは、これらのネットワークのいずれかに存在している必要があります。次に、デフォルトゲートウェイがパケットを転送します。

ネットワーク 2:

2 つの異なるインターフェイスのネットワーク アドレス (IP アドレスのネットワーク部分) は同じにすることができません。

イーサネット インターフェイス	IP アドレス	ネットマスク	ネットアドレス
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

この場合、2つの異なるイーサネットインターフェイスが同じネットワーク アドレスを持つという矛盾した状態になっています。Cisco IronPort アプライアンスからのパケットを 192.168.1.11 に送信する場合に、どのイーサネット インターフェイスを使用してパケットを送信すべきかを決定する方法がありません。2つのイーサネットインターフェイスが2つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。Cisco IronPort アプライアンスを使用すると、矛盾を含むネットワークを設定できなくなります。

2つのイーサネットインターフェイスを同じ物理ネットワークに接続することはできますが、Cisco IronPort アプライアンスが一意的な配信インターフェイスを選択できるように IP アドレスとネットマスクを設定する必要があります。

IP アドレス、インターフェイス、およびルーティング

GUI または CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルトのゲートウェイ）が選択した内容より優先されます。

たとえば、3つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定された次のような Cisco IronPort アプライアンスがあるとします（すべて /24 と仮定）。

イーサネット	IP
Management	192.19.0.100
data1	192.19.1.100
data2	192.19.2.100

デフォルトのゲートウェイは 192.19.0.1 です。

AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、data1 (192.19.1.100) の IP を選択した場合、ユーザはすべての TCP トラフィックが data1 イーサネット インターフェイスを介して発生すると想定します。しかし、トラフィックはデフォルト ゲートウェイとして設定されているインターフェイス（この場合は Management）から発生し、data1 の IP の送信元アドレスのスタンプが付されます。

まとめ

Cisco IronPort アプライアンスは、配信するパケットが経由する一意のインターフェイスを常に識別できなければなりません。この決定を行うために、Cisco IronPort アプライアンスは、パケットの宛先 IP アドレスと、そのイーサネットインターフェイスのネットワークおよび IP アドレス設定を組み合わせ使用します。次の表に、ここまで説明してきた例をまとめます。

	同じネットワーク	異なるネットワーク
同じ物理インターフェイス	可	可
異なる物理インターフェイス	不可	可

Cisco IronPort アプライアンスの接続時の戦略

Cisco IronPort アプライアンスを接続する際には、次の点に留意してください。

- 管理トラフィック（CLI、Web インターフェイス、ログ配信）は通常、電子メールのトラフィックに比べて小さいサイズになります。
- 2つのイーサネット インターフェイスが、同じネットワーク スイッチに接続されているが別のホスト ダウンストリーム上の単一のインターフェイスとのトークで終了する場合、またはすべてのデータがすべてのポートにエコーされるネットワーク ハブに接続されている場合、2つのインターフェイスを使用しても得られる利点はありません。
- 1000 Base-T で動作するインターフェイスを介した SMTP キャンパセーションは、100 Base-T で動作する同じインターフェイスを介した場合より若干速くなりますが、これは理想的な条件下でのみです。
- 配信ネットワークのその他の部分にボトルネックがある場合、ネットワークへの接続を最適化しても意味がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続する Cisco IronPort アプライアンス インターフェイスの数や、それらのアドレスを指定する方法は、基幹ネットワークの複雑さを考慮した上で決定する必要があります。ご使用のネットワーク トポロジやデータのボリュームから判断して不要であれば、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。



APPENDIX **C**

ファイアウォール情報

次の表は、Cisco IronPort アプライアンスを正常に動作させるために開けなければならないことがあるポートのリストです（デフォルト値を示す）。

表 C-1 ファイアウォール ポート

ポート	プロトコル	入力/出力	ホスト名	説明
20/21	TCP	入力または出力	AsyncOS IP、FTP サーバ	ログ ファイル集約用 FTP。
22	TCP	入力	AsyncOS IP	CLI への SSH アクセス、ログ ファイルの集約。
22	TCP	出力	SSH サーバ	ログ ファイルの SSH 集約。
22	TCP	出力	SCP サーバ	ログ サーバへの SCP 配信。
23	Telnet	入力	AsyncOS IP	CLI への Telnet アクセス、ログ ファイルの集約。
23	Telnet	出力	Telnet サーバ	Telnet アップグレード、ログ ファイルの集約（非推奨）。
25	TCP	出力	Any	電子メールを送信する SMTP。
25	TCP	入力	AsyncOS IP	バウンスされた電子メールを受信する SMTP またはファイアウォール外部からの電子メールのインジェクト。
80	HTTP	入力	AsyncOS IP	システム モニタリングのための GUI への HTTP アクセス。
80	HTTP	出力	downloads.ironport.com	AsyncOS アップグレードおよび McAfee 定義を除くサービス更新。

表 C-1 ファイアウォール ポート (続き)

80	HTTP	出力	updates.ironport.com	AsyncOS アップグレードおよび McAfee Anti-Virus 定義。
82	HTTP	入力	AsyncOS IP	IronPort Anti-Spam の検疫の表示に使用。
83	HTTPS	入力	AsyncOS IP	IronPort Anti-Spam の検疫の表示に使用。
53	UDP/TCP	入力および出力	DNS サーバ	インターネットルートサーバを使用するか、ファイアウォール外の他の DNS サーバを使用するように設定されている場合、DNS。SenderBase クエリーにも使用。
110	TCP	出力	POP サーバ	IronPort スпам検疫のためのエンドユーザの POP 認証。
123	UDP	入力および出力	NTP サーバ	タイム サーバがファイアウォール外部の場合、NTP。
143	TCP	出力	IMAP サーバ	IronPort スпам検疫のためのエンドユーザの IMAP 認証。
161	UDP	入力	AsyncOS IP	SNMP クエリー。
162	UDP	出力	管理ステーション	SNMP トラップ。
389 3268	LDAP	出力	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォール外部の場合、LDAP。 IronPort スпам検疫のための LDAP 認証。
636 3269	LDAPS	出力	LDAPS	LDAPS : Active Directory のグローバルカタログサーバ。
443	TCP	入力	AsyncOS IP	システム モニタリングのための GUI への Secure HTTP (https) アクセス。
443	TCP	出力	res.cisco.com	Cisco Registered Envelope Service。
443	TCP	出力	updates-static.ironport.com	更新サーバの最新ファイルの検証。
443	TCP	出力	phonehome.senderbase.org	感染フィルタの受信/送信。
514	UDP/TCP	出力	Syslog サーバ	Syslog ロギング。

表 C-1 ファイアウォール ポート (続き)

628	TCP	入力	AsyncOS IP	ファイアウォール外部から電子メールをインジェクトする場合、QMQP。
2222	CCS	入力および出力	AsyncOS IP	クラスタ通信サービス (中央集中管理用)。
6025	TCP	出力	AsyncOS IP	IronPort スпам検疫。



APPENDIX **D**

IronPort エンドユーザ ライセンス 契約書

この付録の内容は、次のとおりです。

- 「Cisco IronPort Systems, LLC ソフトウェア使用許諾契約書」(P.D-1)

Cisco IronPort Systems, LLC ソフトウェア使 用許諾契約書

すべてのユーザに対する警告：本ソフトウェア（以下で定義）のライセンスについて、以下の法的な契約書（「契約書」）を注意深くお読みください。同意ボタンをクリックするか、質問に「Y」を入力することで、お客様（個人または単一の実在者のいずれかを指し、総称して「お客様」と呼びます）は、デラウェア州法人である Cisco IronPort Systems, LLC（以下「IronPort」）とお客様（総称して「両当事者」と呼びます）との間の以下の契約に従い、その当事者となることに同意したことになります。同意ボタンをクリックするか、質問に「Y」を入力することで、お客様は（A）お客様がお客様の会社を代表する権限を正式に与えられており、（B）お客様の会社を代表して本契約の条件に同意することを表明し、それによって契約が成立します。お客様またはお客様が代表する会社（総称して「お客様」と呼びます）が本契約の条件に同意しない場合は、キャンセル ボタンをクリックするか、質問に「N」を入力し、即座に（ただし後述のとおり納品日から 30 日以内に）、IronPort または本ソフトウェアの提供元である販売代理店に通知し、本ソフトウェアに対して支払った代金の全額の返金を受けてください。

1. 定義

1.1 「お客様のサービス」とは、お客様の内部的なビジネスを遂行することを目的とし、購入契約、評価契約、ベータまたはプレリリース契約、注文書、見積書、お客様と IronPort またはその販売代理店との間のその他同様の契約（以下「契約」）、ならびにシステム アーキテクチャおよびそのインターフェイスの概要が記載されている該当するユーザ インターフェイスおよび IronPort の標準システム ガイド ドキュメント（総称して「ライセンス文書」と呼びます）で規定されているとおり、お客様の製品を通じて可能となる、エンドユーザに提供される、お客様の電子メールまたはインターネット サービスを意味します。

1.2 「エンドユーザ」とは、お客様のサービスを通じてインターネットへアクセスすること、もしくは電子メール サービスを利用することをお客様が承認した従業員、請負業者、またはその他の代理人を意味します。

1.3 「本サービス」とは、(i) アップデートおよびアップグレードを含む、本ソフトウェアの機能の提供、および (ii) 場合によって IronPort またはその販売代理店によるサポートの提供を意味します。

1.4 「本ソフトウェア」とは、(i) IronPort が所有し、IronPort のハードウェア製品とともに IronPort によってお客様にライセンス付与されるソフトウェア、(ii) IronPort のサードパーティ ライセンサーによって提供され、IronPort のハードウェア製品で使用するためお客様にライセンス付与された任意のソフトウェア、(iii) IronPort のハードウェア製品とともに IronPort によってお客様にライセンス付与されたその他の任意の IronPort ソフトウェア モジュール、および (iv) それらに対するすべてのアップデートおよびアップグレードを意味します。

1.5 「アップデート」とは、本ソフトウェアに大規模な新機能を追加せず、IronPort またはそのサードパーティ ライセンサーによってリリースされる、マイナー アップデート、エラー修正およびバグ修正を意味します。アップデートは、本ソフトウェアのリリース番号における小数点の右側の増加（たとえば、ソフトウェア 1.0 からソフトウェア 1.1 へ）により示されます。「アップデート」という用語は、IronPort またはそのサードパーティ ライセンサーにより個別の製品として販売およびライセンス付与されるアップグレードまたは新しいソフトウェア バージョンを明確に除外します。

1.6 「アップグレード」は、本ソフトウェアに対する改訂を意味し、IronPort またはそのサードパーティ ライセンサーによりその独自の裁量でリリースされた場合に、新しい拡張機能を既存の機能に追加します。アップグレードは、本ソフトウェアのリリース番号における小数点の左側の増加（たとえば、ソフトウェア 1.x からソフトウェア 2.0 へ）により示されます。いかなる場合にも、アップグ

レードには、IronPort またはそのサードパーティ ライセンサーにより個別の製品として販売およびライセンス付与される本ソフトウェアの新しいバージョンは含まれません。

2. ライセンスの付与とデータ収集条件についての同意

2.1 ソフトウェアのライセンス。本ソフトウェアおよびライセンス文書を使用することにより、お客様は本契約の条件に従うことに同意し、お客様が本契約に準拠している限り、IronPort はお客様に、契約期間中、お客様のサービスをエンドユーザに提供することに関連してのみ、IronPort のハードウェア製品上でのみ本ソフトウェアを使用する非独占的、二次ライセンス不能、譲渡不能、世界的なライセンスを付与します。本ライセンスの期間と範囲は、ライセンス文書で別途規定します。本契約で明示する場合を除き、IronPort、IronPort の販売代理店、またはその各ライセンサーは、お客様に対し、いずれの本ソフトウェアにおける権利、権原、権益も付与しません。本ライセンスとすべての本サービスは同時に終了します。

2.2 データの使用についての同意とライセンス。本契約の第 8 項と、お客様への通知をもって IronPort により随時修正される可能性がある IronPort プライバシー声明 (<http://www.IronPort.com/privacy.html>) に従い、お客様は、IronPort により随時修正される可能性があるライセンス文書に規定されているとおり、お客様からデータ（以下「データ」）を収集し使用することに同意し、そのライセンスを IronPort に付与します。データを使用してレポートまたは統計情報を生成する範囲において、データは全体としてのみ開示され、ユーザ名、電話番号、難読化されていないファイル名、電子メール アドレス、物理アドレス、およびファイルの内容など、エンドユーザの識別情報をデータから推測できないようにするものとします。上記にかかわらず、お客様は、事前に書面または電子的な手段で通知することで、IronPort がデータを収集および使用する権利をいつでも終了させることができますが、かかる権利が終了した場合、お客様は本ソフトウェアまたは本ソフトウェアのコンポーネントを利用できなくなります。

3. 機密性。各当事者は、相手方当事者のすべての機密情報を、自身の同様の機密情報を保護するのと同じ程度に（また、いかなる場合にも妥当な程度の注意を払って）秘密に保持し、かかる機密情報を本契約で許された範囲でのみ使用することに同意します。本契約での「機密情報」とは、「機密」と表示された当事者の情報または開示元の当事者が独占的または機密として見なすことが妥当な情報を意味します。ただし、IronPort によって提供される本ソフトウェアの設計レビューおよびあらゆる製造前のリリースで開示されたデータ、本ソフトウェア、情報は、機密と表示されているどうかにかかわらず明らかに機密情報と見なされます。

4. 財産権、所有権。IronPort またはその販売代理店によりお客様に提供された本ソフトウェアおよびその他の資料の権原および所有権、ならびに前記にかかわるすべての知的財産権（以下で定義）は、IronPort および/またはその上位ライセンサーの独占的所有物です。お客様ならびにその従業員および代理人は、IronPort またはその販売代理店によってお客様に提供された本ソフトウェアまたはその他の資料のコピーに現れる商標またはその他の所有権表記、説明文、記号またはラベルを削除または改変しないものとします。お客様は、本ソフトウェアまたは本ソフトウェアによって生成される内部データファイルの変更、変換、営利目的での転売、配布、複製、機能拡張、適合、翻訳、逆コンパイル、リバースエンジニアリング、逆アセンブルを行ったり、本ソフトウェアまたは本ソフトウェアによって生成される内部データファイルのソースコードを特定したり、取得しようとしたり、本ソフトウェアまたはライセンス文書に基づいて二次的著作物を作成したりしないものとし、他者によるそのような行為を許可または承認しないことに同意します。別途書面で合意しない限り、本契約または関連するすべてのコンサルティングまたはプロフェッショナル サービス契約の履行途中に IronPort またはその上位ライセンサーによって作成または開発されたプログラム、発明、概念、文書、仕様、またはその他の文書化された資料または図面による資料および媒体は、すべての著作権、データベース権、特許、企業秘密、商標、著作者人格権、またはかかる作業の遂行に関連するその他すべての知的財産権（「知的財産権」）を含め、IronPort またはその上位ライセンサーに独占的に属するものとし、合衆国法典第 17 編（1976 年著作権法）の意味の範囲内でお客様ののために有償で行われた作業とは見なさないものとします。

5. 制限付き保証と保証の放棄

5.1 制限付き保証。IronPort はお客様に対し、本ソフトウェアが適切にインストールされ正しく使用されている場合に、ライセンス文書に記載された仕様に相当程度に従うことを、納品日から 90 日間か、ライセンス文書に記載されている期間のうちの長いほうの期間（以下「保証期間」）にわたり保証します。本項に記載されている保証のいずれかの違反に対し、お客様の唯一の法的救済および IronPort の全責任は、保証期間内にお客様によって不適合が IronPort および/またはその販売代理店に報告された場合に限り、誤りまたは不適合をすみやかに修正することです。この保証は、お客様に対してのみ行われ、エンドユーザまたは他の第三者への譲渡はできません。本項で定める保証の違反、または本契約の違反に対し、かかる違反が直接的または間接的に次のいずれかから、またはそれに関連して生じた場合、IronPort は一切の責任を負いません。(i) お客様または第三者による、本ソフトウェアの無許可の、不適切な、不完全な、または不適当なメンテナンスまたはキャリブレーション、(ii) 第三者のハードウェア、ソフトウェア、サービスまたはシステム、(iii) 本ソフトウェアまたは本サービスの許可のない変更または改造、(iv) 本ソフトウェアの無許可の、もしくは不適切な

使用もしくは操作、またはお客様が該当する環境仕様に従わなかった場合、(v) IronPort またはその販売代理店から随時提供されるアップデート、アップグレード、修正、改訂をインストールおよび/または使用しなかった場合。

5.2 保証の否認。本契約書の 5.1 項に記載されている明示的な保証は、本ソフトウェアまたは本サービスに関する唯一の保証を構成します。適用法によって許される最大の限度まで、IronPort は本契約上の本ソフトウェアと本サービスのライセンスを「現状のまま」付与します。本契約で明示的に規定しない限り、IronPort およびその上位ライセンサーは、明示、黙示または制定法上の（事実上の、または法律の運用による）いかなる形の表明も保証も行わず、市場性または特定目的適合性の黙示的保証などを含むその他のあらゆる保証を明示的に否認します。IronPort もそのサードパーティライセンサーも、本ソフトウェアまたは本サービスが (1) 不具合、エラー、バグを含まないこと、(2) 本ソフトウェアの動作が中断しないこと、(3) 本ソフトウェアの使用により得られるか得られる可能性がある結果または情報が正確で、完全で、信頼でき、安全であることを保証しません。

6. 責任制限。適用法で許される最大限度まで、いずれの当事者も相手方に対して、利益の損失、代替商品またはサービスの調達コスト、取引上の損失、使用またはデータの損失、事業の中断、またはあらゆる種類の間接的損害、特別損害、偶発的損害、結果的損害について、かかる当事者がかかる損害の可能性を示す事前通知を受け取っていた場合であっても、責任を負わないものとします。いかなる場合でも、本契約のいずれかの条項の下で生じる各当事者の責任は、かかる損害の請求が契約、不法行為、その他の法理論に基づくかどうかにかかわらず、そのような責任を生じさせる事象よりも前の 12 か月間に、本ソフトウェアまたは本サービスに対して支払われた総額を超えないものとします。

7. 契約の期間および終了。本契約の期間（「契約期間」）は、ライセンス文書で規定するものとします。IronPort が本契約またはライセンス文書の重要な条項を履行しなかった場合、お客様は、書面で通知してから 30 日の間に不履行が解決されなかった場合、通知から 30 日後に本契約を終了させることができます。お客様が本契約またはライセンス文書の重要な条項を履行しなかった場合、IronPort は、書面で通知してから 30 日の間に不履行が解決されなかった場合、通知から 30 日後に返金することなく本契約を終了させることができます。本契約は、次の場合に、いずれかの当事者により、いつでもただちに通告なく終了させることができます。(i) 相手方当事者によるまたは相手方当事者に対する債務超過、管財人管理または破産手続き、またはかかる当事者の負債の調停のためのその他の訴訟手続、(ii) 相手方当事者による債権者への一括譲渡、(iii) 相手方当事者の解散。本契約が終了または満了した場合、第 2 項で付与されたライセンスはただちに終了します。お客様は、本契約が終了または満了してから 30 暦日以内に、

本契約の下で IronPort またはその販売代理店によりお客様に提供された本ソフトウェアおよびその他のすべての資料またはドキュメントのすべてのコピーを IronPort またはその販売代理店に返却または破棄するものとします。

8. 米国 政府による権利の制限、輸出管理。本ソフトウェアおよび付随するライセンス文書は、該当する DFAR 227.7202 および FAR 12.212 に従い、それぞれ「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア文書」と見なされます。米国政府による本ソフトウェアおよび付随するライセンス文書の使用、変更、複製、リリース、実行、表示、開示は、本契約の条項のみによって決定され、本契約の条項によって明示的に許される範囲を除き禁止されます。本ソフトウェアおよびライセンス文書は米国の輸出管理規則に従って輸出しなければならないが、米国の法律に反する行為は禁止されることを、お客様は認めます。お客様は、米国輸出管理局もその他の連邦政府関係機関も、お客様が輸出する権利の停止、取り消し、拒否をしていないことを表明します。お客様は、お客様が本ソフトウェアを核兵器、科学兵器または生物兵器、ミサイル技術に関連して使用せず、これらの関連する最終使用のために譲渡しないことを表明します。ただし、米国政府により、規制または特定のライセンスによって許可されている場合を除きます。お客様は、米国およびその他の国におけるあらゆる輸入および輸出規制、その他の適用法に従うのは、最終的にお客様の責任であることを認め、IronPort またはその販売代理店が、元の販売国内でお客様に最初に販売した後はいかなる責任も負わないことを認めます。

9. 雑則。本契約は、法の抵触のルールを排除して、米国およびカリフォルニア州の法律に準拠します。国際物品売買契約に関する国連条約の適用は、明示的に除外されます。本契約に含まれるすべての規定は、両当事者間の代理関係、提携、その他の合同企業を構成するものと解釈されません。いずれの当事者も、下記による義務の不履行または履行遅延を理由とした責任を負わないものとします（金銭の支払いを除きます）。(i) 米国の現在もしくは将来の法令または本契約に適用される法律の条項、(ii) 電力供給の中断、インターネットの障害、ストライキ、品不足、暴動、反乱、火災、洪水、暴風雨、爆発、天災、戦争、テロ、政府の行動、労働条件、地震、またはかかる当事者の合理的な支配の及ばないその他の事由。本契約およびライセンス文書は、本ソフトウェアの使用に対するすべての権利を定め、両当事者間の完全な合意であり、本ソフトウェアおよびライセンス文書にかかわるその他のあらゆる通信に優先します。本契約の条件は、ライセンス文書、注文、当事者によって提出されたその他の書面との相違がある場合でも、相手方当事者によって正式に拒否されたかどうかにかかわらず、優先されます。本契約の変更は、IronPort の正式に認められた代表者が提供する書面での追記による場合を除き、禁止されます。ただし、IronPort は、お客様への通知により、IronPort プライバシー声明をその裁量においていつでも変更でき、その内容は <http://www.IronPort.com/privacy.html> に掲載されます。本契約のいずれの条項も、権利放棄されたものと見なされません。ただし、かかる権利放棄が書面に

より IronPort または IronPort の正式に認められた代表者によって署名されたものである場合を除きます。本契約のいずれかの条項が無効とされた場合であっても、本契約の残りの部分は完全な効力を維持するものとします。両当事者は、本契約書が英語のみで書かれていることは各自が希望したものであることを認めます。

10. IronPort の連絡先情報。お客様が何らかの理由で IronPort に連絡する必要がある場合の連絡先は次のとおりです。住所：IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066、電話：650.989.6500、FAX：650.989.6543。



GLOSSARY

C

CIDR の表記

Classless Inter-Domain Routing。任意のビット数でネットワーク コンテキスト内の IP アドレス範囲を説明するのに便利な省略表現。この表記を使用して、スラッシュ (/) の後に続けて、ネットワーク部分に使用するビット数を追加することで、アドレスのネットワーク プレフィクス部分を記述します。したがって、クラス C ネットワークは、プレフィクス表記で **192.168.0.1/24** と記述できます。CIDR 仕様による **206.13.1.48/25** は、アドレスの先頭 25 ビットが、**206.13.1.48** の先頭 25 ビットと一致する任意のアドレスを含みます。

D

DLP

Data Loss Prevention (データ消失防止)。RSA Security の DLP スキャンエンジンを使用して、ユーザによる機密データの電子メールでの誤送信を防ぐことにより、組織の情報および知的財産を守り、規制および組織的なコンプライアンスを順守させます。

DLP インシデント

データ消失防止インシデントは、DLP ポリシーにより発信メッセージ内に留意すべき 1 つ以上の DLP 違反を検出すると発生します。

DLP ポリシー

データ消失防止ポリシーは、発信メッセージに機密データが含まれているかどうかを判断し、そのようなデータを含むメッセージに対して AsyncOS が実行するアクションの決定に使用される条件のセットです。

DLP リスク要因

発信メッセージで検出される DLP 違反のセキュリティ リスクを表す 0 ~ 100 のスコア。リスク要因に基づいて、DLP ポリシーによってメッセージに対して実行するアクションが決まります。

DLP 違反

一例として、メッセージ内で検出された、組織の DLP ルールに違反するデータ。

- DNS** ドメイン ネーム システム (Domain Name System)。「RFC 1045」および「RFC 1035」を参照してください。ネットワーク上の DNS サーバは IP アドレスをホスト名に、ホスト名を IP アドレスに解決します。
- DoS 攻撃** Denial of Service (サービス拒絶) 攻撃。Distributed Denial of Service (DDoS; 分散型サービス拒絶) 攻撃にもなり得ます。ネットワークまたはコンピュータ上での攻撃。特定のサービスへのアクセスを中断させることを主な目的とします。
- DSN** Delivery Status Notification (配信ステータス通知)。バウンスされるメッセージ。

F

- False Negative** スпам メッセージ、またはウイルスや DLP 違反を含むメッセージであるが、検出されなかったメッセージ。
- False Positive** スпамとして、またはウイルスや DLP 違反を含むメッセージとして誤って分類されたメッセージ。

H

- HAT** Host Access Table (ホスト アクセス テーブル)。HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。いずれのリスナーにも独自の HAT があります。HAT は、パブリックおよびプライベートのリスナー用に定義され、メール フロー ポリシーおよび送信者グループを含みます。

I

- IDE ファイル** ウィルス定義ファイル。IDE ファイルには、ウィルスを検出するアンチウイルス ソフトウェアによって使用されるシグニチャまたは定義が格納されています。

L

LDAP Lightweight Directory Access Protocol。インターネット ディレクトリまたはイントラネット ディレクトリのユーザ（電子メール アドレスを含む）、組織などのリソースに関する情報へのアクセスに使用されるプロトコルです。

M

MAIL FROM 「エンベロープ送信者」を参照してください。

MTA Mail Transfer Agent または Messaging Transfer Agent。電子メール メッセージの受け入れ、ルーティング、配信を担当するプログラム。Mail User Agent または他の MTA からのメッセージの受信時、MTA はメッセージを一時的にローカルに保存し、受信者を分析し、他の MTA にメッセージをルーティングします。メッセージ ヘッダーを編集したり、追加したりする場合があります。Cisco IronPort アプライアンスは、ハードウェア、セキュリティの強化されたオペレーティング システム、アプリケーション、およびサポート サービスを組み合わせて、目的に合わせて構築された、企業のメッセージング専用のラックマウント サーバ アプライアンスを提供する MTA です。

MUA Mail User Agent。ユーザが電子メール メッセージを作成および読むことができるプログラム。MUA は、ユーザと Message Transfer Agent 間のインターフェイスを提供します。発信メールは、最終的に MTA に渡されて配信されます。

MX レコード 特定のドメインのメールの受け入れを担当するインターネット上の MTA を指定します。Mail Exchange レコードは、ドメイン名のメール ルートを作成します。1 つのドメイン名には、複数のメール ルートを作成でき、それぞれにプライオリティ番号が割り当てられます。最も小さい番号のメール ルートは、そのドメインを担当するプライマリ サーバになります。リストされる他のメール サーバは、バックアップとして使用されます。

N

NTP Network Time Protocol（ネットワーク タイム プロトコル）。ntpconfig コマンドでは、Network Time Protocol (NTP; ネットワーク タイム プロトコル) を使用してシステム クロックを他のコンピュータと同期するように、IronPort AsyncOS を設定します。

R

RAT Recipient Access Table (受信者アクセス テーブル)。受信者アクセス テーブルでは、パブリック リスナーが受け入れる受信者を定義します。テーブルは、アドレス (場合により、部分的なアドレスまたはホスト名) およびそのアドレスを受け入れるか拒否するかを指定します。その受信者に対する **RCPT TO** コマンドへの **SMTP** 応答を任意に含めることができます。RAT には通常、ローカルドメインを含めます。

RCPT TO 「エンベロープ受信者」を参照してください。

S

STARTTLS Transport Layer Security (TLS) は、Secure Socket Layer (SSL) テクノロジーの改良版です。これは、インターネット上での **SMTP** カンバセーションの暗号化に広く使用されているメカニズムです。IronPort AsyncOS オペレーティング システムは、RFC 2487 に記述されている、**SMTP** の **STARTTLS** 拡張 (Secure SMTP over TLS) をサポートします。

T

TOC Threat Operations Center。これは、ウイルス拡散の検出と対応にかかわる、すべてのスタッフ、ツール、データ、およびファシリティを指します。

あ

アンチウイルス Sophos および McAfee のアンチウイルス スキャン エンジン、ファイルのスキャンしてウイルス、トロイの木馬、およびワームを見つけるウイルス検出エンジンを使用して、プラットフォーム間のアンチウイルス保護、検出、および除去を提供します。これらのプログラムは、「悪意のあるソフトウェア」を意味するマルウェアと総称されます。アンチウイルス スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

え

- エンベロープ受信者** RCPT TO: SMTP コマンドで定義される電子メール メッセージの受信者。「Recipient To」または「Envelope To」アドレスと呼ばれることもあります。
- エンベロープ送信者** MAIL FROM: SMTP コマンドで定義される電子メール メッセージの送信者。「Mail From」または「Envelope From」アドレスと呼ばれることもあります。

お

- オープン リレー** オープン リレー（「セキュアでないリレー」または「サードパーティ」リレーともいう）は、電子メール メッセージの検査なしのサードパーティ リレーを許可する SMTP 電子メール サーバです。オープン リレーは、ローカル ユーザ以外が送受信する電子メールを処理することで、不明な送信者が大量の電子メール（典型的にはスパム）をご使用のゲートウェイを通過してルーティングできるようにします。listenerconfig コマンドおよび systemsetup コマンドは、ユーザが気付かずにシステムをオープン リレーとして設定することを防止します。

か

- 完全修飾ドメイン名 (FQDN)** ドメイン名でよりレベルの高いドメイン名からトップレベルドメイン名までを含めたドメイン名。たとえば、mail13.example.com は、192.168.42.42 のホストの完全修飾ドメイン名であり、example.com は、example.com ドメインの完全修飾ドメイン名です。完全修飾ドメイン名は、インターネット内で一意である必要があります。
- 感染フィルタ** IronPort の感染フィルタ機能は、ウイルスから保護するための追加の層を提供します。感染フィルタ機能は、疑わしい電子メール メッセージを検疫し、更新されたウイルス IDE が使用可能になるまで、または脅威なしと判断されるまで、そのメッセージを保持します。
- カンパセーション型バウンス** SMTP カンパセーション内で発生するバウンス。カンパセーション型バウンスには、ハードバウンスとソフトバウンスの 2 種類があります。

き

キュー Cisco IronPort アプライアンスでは、電子メール キュー内のメッセージを削除、バウンス、保留、またはリダイレクトできます。宛先ドメインへのメッセージのこの電子メール キューは、**配信キュー**とも呼ばれます。IronPort Anti-Spam またはメッセージフィルタ アクションによる処理を待機しているメッセージのキューは、**ワーク キュー**とも呼ばれます。status detail コマンドを使用して、両方のキューのステータスを表示できます。

キューの最大時間 ハードバウンスされる前に、**配信用**の電子メール キューにソフト バウンスメッセージがとどまる最大時間。

許可ホスト プライベート リスナー経由で Cisco IronPort アプライアンスを使用した電子メールのリレーが許可されたコンピュータ。許可ホストは、そのホスト名または IP アドレスによって定義されます。

こ

コンテンツ フィルタ 電子メール パイプラインのワーク キューの受信者単位のスキャン フェーズ中にメッセージを処理するために使用されるコンテンツ ベースのフィルタ。コンテンツ フィルタはメッセージ フィルタの後に呼び出され、個々の分裂されたメッセージに対して実行されます。

コンテンツ照合分類子 RSA データ消失防止スキャン エンジンの検出コンポーネント。分類子には、裏付けデータを検索するコンテキスト ルールとともに、機密データを検出するためのいくつかのルールが含まれます。たとえば、クレジットカードの分類子には、メッセージにクレジットカード番号と一致するストリングが含まれているだけでなく、期限データ、クレジットカード会社名、住所などの裏付け情報も含まれる必要があります。

さ

最大リトライ回数 ハードバウンスされる前に、ソフト バウンスメッセージの再配信を試行する最大回数。

し

受信 IP インターフェイスで設定された特定のリスナーの電子メールメッセージを受信する動作。Cisco IronPort アプライアンスは、インターネットからのインバウンドまたはイントラネットシステムからのアウトバウンドの電子メールメッセージを受信するようにリスナーを設定します。

す

スパム Unwanted, Unsolicited Commercial Bulk Email (UCE/UBE)。アンチスパム スキャンでは、フィルタリング ルールに従って、スパムの疑いがある電子メールメッセージを識別します。

そ

送信者グループ 送信者グループは、単に、複数の送信者からの電子メールを同じ方法で扱う（つまり、送信者のグループにメール フロー ポリシーを適用する）ために集められた送信者のリストです。送信者グループは、リスナーのホスト アクセス テーブル (HAT) でカンマ区切りの送信者 (IP アドレス、IP 範囲、ホスト/ドメイン、SenderBase 評価サービスの分類、SenderBase 評価スコア範囲、または DNS リスト クエリー応答により識別) のリストです。メール フロー ポリシーと同様に、送信者グループに名前を割り当てます。

ソフト バウンス メッセージ キューに設定された最大リトライ回数または最大時間に基づいて、後から配信が再試行されるメッセージ。

ち

遅延型バウンス SMTP カンバセーション内で発生するバウンス。受信者のホストは、配信用のメッセージを受け入れますが、後でバウンスするだけです。

で

デバウンス タイムアウト システムがユーザに同一のアラートの送信を控える時間（秒単位）。

電子メール セキュリティ マネージャ IronPort アプライアンス上ですべての電子メール セキュリティ サービスおよびアプリケーションを管理するための、単一で包括的なダッシュボード。電子メール セキュリティ マネージャでは、感染フィルタ、アンチスパム、アンチウイルス、および電子メール内容のポリシーを、受信者単位または送信者単位で、インバウンドとアウトバウンドの独立したポリシーを使用して管理できます。「コンテンツ フィルタ」も参照してください。

は

ハード バウンス メッセージ 永続的に配信できないメッセージ。SMTP カンパセーション中またはその後に生じることがあります。

配信

特定の IP インターフェイスから、受信者のドメインまたは Cisco IronPort アプライアンスの内部メール ホストに電子メール メッセージを配信する動作。Cisco IronPort アプライアンスは、Virtual Gateway テクノロジーを使用して、同じ物理マシン内の複数の IP インターフェイスからメッセージを配信できます。各仮想ゲートウェイには、独立した IP アドレス、ホスト名とドメイン、および電子メール キューがあり、それぞれに異なるメール フロー ポリシーおよびスキャンの方法を設定できます。

リモート ホストへの最大同時接続、仮想ゲートウェイ単位のホストへの最大同時接続の制限、およびリモート ホストへのカンパセーションを暗号化するかどうかなど、Cisco IronPort アプライアンスが実行する配信の設定を、調整できます。

ひ

非カンパセーション型バウンス

受信者のホストがメッセージを受け入れて配信した後に、そのメッセージが返されたために発生するバウンス。ソフト (4XX) またはハード (5XX) のバウンスがあります。これらのバウンス応答を分析し、受信者メッセージに対して実行する処理 (ソフト バウンスされた受信者メッセージの再送信、ハード バウンスされた受信者のデータベースからの削除など) を判断します。

評価フィルタ

疑わしい送信者を評価に基づいてフィルタリングする方法。SenderBase 評価サービスは、リモート ホストの接続 IP アドレスに基づいて、陽性と疑わしいスパムを拒否または抑制するための、正確で柔軟な方法を提供します。

ふ

ブラックリスト

既知の不適切な送信者のリスト。デフォルトで、パブリック リスナーのブラックリスト送信者グループに含まれる送信者は、\$BLOCKED メール フロー ポリシーで設定されたパラメータによって拒否されます。

ほ

ホワイトリスト

既知の適切な送信者のリストです。信頼する送信者をホワイトリストの送信者グループに追加します。\$TRUSTED メール フロー ポリシーは、信頼する送信者からの電子メールはレート制限をイネーブルにせず、これらの送信者のコンテンツはアンチスパム スキャンの対象にならないように設定されます。

め

メール フロー ポリシー

メール フロー ポリシーは、リスナーの *Host Access Table* (HAT; ホスト アクセス テーブル) パラメータ (アクセス ルールの後に *rate limiting* パラメータ、カスタム SMTP コード、および応答が続く) のグループを表す方法です。送信者グループおよびメール フロー ポリシーは合わせて、リスナーの HAT で定義されます。ご使用の Cisco IronPort アプライアンスは、リスナーの事前定義済みメール フロー ポリシーおよび送信者グループが設定された状態で出荷されます。

も

文字セット (2 バイト) 2 バイト文字セットは、各文字の表現に 2 バイト以上の情報を必要とする外国語文字セットです。

り

リスナー

リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、ネットワーク内にある内部システムまたはインターネットから Cisco IronPort アプライアンスに入る電子メールだけに適用されません。IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーを「電子メールのインジェクタ」として、または指定する IP アドレスごとに実行される「SMTP デーモン」として考えることもできます。

IronPort AsyncOS は、デフォルトでインターネットから電子メールを受信する特性を持つパブリックリスナーと、内部（グループウェア、POP/IMAP などのメッセージ生成）システムからだけの電子メールの受け入れを目的としたプライベートリスナーを区別します。

れ

レート制限

レート制限では、リモート ホストから受け入れるセッション単位の最大メッセージ数、メッセージ単位の最大受信者数、最大メッセージ サイズ、時間単位の最大受信者数、および最大同時接続数を制限します。

ろ

ログ サブスクリプション

Cisco IronPort アプライアンスのパフォーマンスをモニタするログ ファイルの作成。ログ ファイルは、ローカル ディスクに保存され、リモート システムに転送および保管することもできます。ログ サブスクリプションの典型的な属性には、名前、モニタ対象コンポーネント（電子メール操作、サーバ）、形式、転送方法などがあります。



INDEX

記号

\$ACCEPTED メールフロー ポリシー	5-33
\$BLOCKED メールフロー ポリシー	5-33, 5-40
\$EnvelopeSender 変数	5-60
\$RELAYED メールフロー ポリシー	5-40
\$THROTTLED メールフロー ポリシー	5-33
\$TRUSTED メールフロー ポリシー	5-33, 9-21

数字

16 進数形式	3-27, 3-41
5XX SMTP 応答	5-38

A

Active Directory Wizard	3-35
Adaptive Scanning	10-20
[Add to Sender Group] ページ	5-48
admin パスワード 変更	3-24, 3-40
ALL エントリ	

HAT 内の ALL エントリ	5-28, 5-37, 5-41
-----------------	------------------

RAT 内の ALL エントリ	5-76
-----------------	------

antispam サブコマンド	8-20, 9-21
-----------------	------------

antivirus サブコマンド	9-12
------------------	------

AsyncOS 更新サーバ	15-21
---------------	-------

AsyncOS のアップグレード	15-2
------------------	------

AsyncOS の復元	15-12
-------------	-------

AutoSupport 機能	3-25, 3-55, 15-27
----------------	-------------------

B

BLACKLIST 送信者グループ	5-38
-------------------	------

C

CIDR アドレス ブロック	5-27
----------------	------

Cisco Security Intelligence Operations	10-5
--	------

clear コマンド	2-14
------------	------

CLI

「コマンドライン インターフェイス」を参照

CLI の履歴	2-12
---------	------

Command Line Interface (CLI)	2-8
------------------------------	-----

- 大文字と小文字の区別 [2-10](#)
 - 空白文字 [2-10](#)
 - コマンドの補完 [2-12](#)
 - サブコマンド [2-11](#)
 - 終了 [2-12](#)
 - デフォルト設定 [2-9](#)
 - 表記法 [2-8](#)
 - 履歴 [2-12](#)
 - commit コマンド [2-13](#)
-
- D**
- DHAP
 - メール フロー ポリシー [5-14](#)
 - DLP
 - Assessment Wizard [11-17](#)
 - Policy Manager [11-8](#)
 - 機能概要 [11-2](#)
 - グローバル設定 [11-4](#)
 - コンテンツ照合分類子 [11-23](#)
 - 正規表現 [11-29](#)
 - ディクショナリ [14-13](#)
 - 発信メール ポリシーでのポリシーのイネーブル化 [11-34](#)
 - 分類子のカスタマイズ [11-12](#)
 - ヘッダーのスキャン [11-3](#)
 - ポリシーの内容 [11-7](#)
 - DLP ポリシー
 - DLP Policy Manager [11-8](#)
 - 概要 [11-6](#)
 - 拡張設定 [11-31](#)
 - カスタム ポリシーの作成 [11-31](#)
 - コンテンツ照合分類子 [11-23](#)
 - 削除 [11-17](#)
 - 重大度スケール [11-15](#)
 - 順序の並べ替え [11-16](#)
 - 正規表現 [11-29](#)
 - 送信者および受信者のフィルタリング [11-14](#)
 - 添付ファイルのフィルタリング [11-15](#)
 - テンプレートに基づいたポリシーの作成 [11-11](#)
 - 発信メール ポリシーでのイネーブル化 [11-34](#)
 - 複製 [11-17](#)
 - 編集 [11-16](#)
 - ポリシーの内容 [11-7](#)
- DNS** [C-2](#)
- 逆引き DNS ルックアップのタイムアウト [15-64](#)
 - 逆引き DNS ルックアップのタイムアウトのディセーブル化 [15-64](#)
 - 権威サーバ [15-62](#)
 - サーバ [3-26, 3-42](#)
 - 設定 [3-26, 3-42](#)
 - タイムアウト [15-62](#)
 - ダブル ルックアップ [5-26, 5-57](#)
 - プライオリティ [15-62](#)
 - 分割 [15-62](#)
 - dnsconfig コマンド [15-61](#)
 - dnsflush コマンド [15-64](#)

DNS キャッシュ、フラッシュ **15-64**

DNS サーバ **15-62**

DNS 設定 **15-65**

DomainKeys

メールフローポリシーを介して有効化 **5-16**

Domain Name Service (DNS)

設定 **3-26, 3-42**

E

encryptionconfig CLI コマンド **12-4**

exit コマンド **2-15**

F

featurekey コマンド **3-57, 8-6, 9-2**

FTP **A-2, C-1**

FTP アクセス **A-6**

G

GUI

アクセス **2-3**

イネーブル化 **3-42**

概要 **2-1**

ナビゲーション **2-5**

ブラウザ要件 **2-2**

ログイン **2-5**

GUI session timeout **15-74**

GUI のメニュー **2-5**

GUI へのログイン **2-5**

GUI を使用した DNS 設定の編集 **15-65**

GUI を使用したシステム モニタリング **2-1**

H

HAT **5-53**

HAT 変数の使用 **5-18**

HAT 変数の使用【ESCAPE_-32442】CLI の例 **5-19**

HAT 変数の使用【ESCAPE_-32442】GUI の例 **5-19**

HAT 変数のテスト **5-19**

インポート **5-55**

エクスポート **5-55**

遅延拒否 **5-11**

有効ビット **5-14**

HAT 順序

GUI を使用した編集 **5-52**

HAT 遅延拒否 **5-11**

HAT 内の最終エントリ **5-37, 5-41**

HAT 変数の使用 **5-18**

HAT 変数のテスト **5-19**

help コマンド **2-15**

Host Access Table (HAT)

GUI での順序変更 **5-52**

HAT 内の順序 **5-10**

カンマ区切り記号 **5-25**

- 構文 **5-10**
 - デフォルト ポリシー、パブリック **5-37**
 - デフォルト ポリシー、プライベート **5-41**
 - パラメータ **5-12**
 - ルール **5-9**
 - HTTP **A-1, C-1**
 - イネーブル化 **3-22**
 - HTTPS **A-1**
 - イネーブル化 **3-42**
 - HTTPS プロキシ サーバ **15-22**
 - HTTPS ログイン **2-4**
 - HTTP プロキシ サーバ **15-21**
-
- IronPort Anti-Spam ルール用プロキシ サーバ **8-18**
 - IronPort Intelligent Multi-Scan
 - イネーブル化 **8-15**
 - IronPort スпам検疫
 - 解放されたメッセージと電子メール パイプライン **4-12**
 - IronPort 電子メール暗号化
 - 暗号化プロファイル **12-4**
 - エンベロープ設定 **12-6**
 - キー サーバ設定 **12-6**
 - 設定 **12-1**
 - 通知設定 **12-6**
 - フィルタ アクションとの併用 **12-11**
 - メッセージ設定 **12-6**
-
- implementsv **5-61**
 - IP インターフェイス **5-2**
 - グループ化 **5-3**
 - リスナーの定義 **3-43**
 - 割り当て **3-27, 3-40**
 - IronPort Anti-Spam
 - アーカイブ **8-22**
 - イネーブル化 **8-9**
 - 概要 **7-1, 8-1**
 - テスト **8-28**
 - 評価キー **3-32, 3-53, 8-6**
 - フィルタ **8-27**
 - IronPort Anti-Spam 用評価キー **3-53, 8-6**
-
- LDAP **C-2**
 - メール ポリシー **6-37**
 - LDAPS **C-2**
 - Global Catalog Server **C-2**
 - listenerconfig コマンド **5-3**
 - logconfig コマンド **8-39**
-
- MAIL FROM **6-17, 6-18**
 - 通知用に設定 **15-23**

mbox 形式のログ ファイル [8-22](#), [9-18](#)

McAfee

更新サーバ [15-21](#)

評価キー [3-54](#)

McAfee Anti-Virus エンジン [9-7](#)

McAfee の評価キー [9-2](#)

MTA [3-1](#), [5-2](#), [5-3](#)

N

Network Time Protocol (NTP)

設定 [3-24](#), [3-55](#)

not.double.verified [5-58](#), [5-72](#)

NTP [C-2](#)

NTP サーバ [15-75](#)

削除 [15-78](#)

NXDOMAIN [5-58](#), [5-71](#)

nx.domain [5-72](#)

P

password コマンド [15-69](#)

POP/IMAP サーバ [5-3](#)

Q

QMQP [C-3](#)

quit コマンド [2-15](#)

R

RAT

受信者のバイパス [5-74](#)

受信者のバイパス (CLI) [5-75](#)

受信者のバイパス (GUI) [5-75](#)

RCPT TO [6-18](#)

RCPT TO コマンド [5-73](#)

Received ヘッダー [8-37](#)

Recipient Access Table (RAT)

CLI を使用した編集 [5-78](#)

構文 [5-73](#)

定義 [5-72](#)

デフォルト エントリ [5-76](#)

ルール [5-73](#)

RFC

2821 [1-24](#)

821 [6-4](#)

822 [6-4](#)

S

SBRS

テスト [7-12](#)

なし [5-31](#)

SBRS。「Senderbase 評価サービス スコア」を参照

SBRS のメッセージフィルタ [7-6](#)

scp コマンド [A-10](#)

SenderBase [5-14](#), [5-39](#), [C-2](#)

- 送信者グループの SBO **5-31**
- SenderBase Affiliate ネットワーク **7-3**
- SenderBase Network Owner Identification Number **5-27**
- SenderBase、クエリー **5-32**
- SenderBase 評価サービス **7-2**
- SenderBase 評価サービス スコア **5-31**
- SenderBase 評価スコア **5-31, 5-49, 7-4**
- SenderBase 評価スコア、CLI の構文 **5-31**
- SERVFAIL **5-58, 5-72**
- serv.fail **5-72**
- [Service Updates] ページ **15-16**
- sethostname コマンド **15-60**
- SMTP **C-1**
- HELO コマンド **5-38**
- IronPort Anti-Spam のテスト **8-30**
- 応答 **5-73**
- コード **5-11**
- バナー テキスト **5-11**
- バナー ホスト名 **5-13**
- メッセージ **5-3**
- SMTP デーモン
- 「インジェクタ」を参照
- 「リスナー」を参照
- SMTP 認証
- HAT エントリ **5-15**
- Sophos
- アップデート **9-11**
- 評価キー **3-32, 3-54, 9-2**
- Sophos ウイルス スキャン
- フィルタ **9-19**
- SSH **2-8, C-1**
- SUSPECTLIST 送信者グループ **5-38**
- System Setup Wizard **3-19**
- systemsetup コマンド **3-39**
-
- T**
- TCPREFUSE **5-12**
- Telnet **2-8, A-2, C-1**
- Threat Operations Center (TOC) **10-10**
- [Time Zone] ページ **15-76**
- trace コマンド **7-12**
- Transport Layer Security (TLS) **5-15**
- tzupdate
- CLI コマンド **15-76**
-
- U**
- UNKNOWNLIST 送信者グループ **5-38**
- Unsolicited Commercial Email **7-3**
-
- V**
- Virtual Gateway テクノロジー **5-3**
-
- W**
- Web UI セッション タイムアウト **15-74**

Web インターフェイス

イネーブル化 **3-42**

WHITELIST 送信者グループ **5-38, 9-21**

X

X-advertisement ヘッダー **8-30**

X-IronPort-Anti-Spam-Filtered ヘッダー **8-27**

X-IronPort-Anti-Spam ヘッダー **8-27**

X-IronPort-AV ヘッダー **9-13**

XML **2-2**

あ

アクセス ルール

HAT 内のアクセス ルール **5-11**

事前定義 **5-33**

アクティブなセッション **2-7**

アップグレード

CLI を使用した取得 **15-4, 15-11**

GUI を使用した取得 **15-7**

使用可能 **15-3**

ストリーミング **15-6**

リモート **15-7**

アップグレード サーバ **15-7**

アップデートの強制 **9-11**

アプライアンスの奥行き **3-8**

アプライアンスの重量 **3-8**

アプライアンスの寸法 **3-8**

アプライアンスの高さ **3-8**

アプライアンスの幅 **3-8**

アプライアンスの物理的寸法 **3-8**

アラート

アラート分類 **15-25**

感染フィルタでのイネーブル化 **10-20**

重大度 **15-26**

受信者 **15-25**

設定 **15-25**

アラート設定 **3-23, 3-55, 15-25**

アラート メッセージ **3-23, 3-55**

アラートリスト **15-33**

暗号化

フィルタ アクションとの併用 **12-11**

暗号化プロファイル

設定 **12-4**

暗号化ヘッダー **12-16**

アンチウイルス **14-39**

Dropping Attachments **9-13**

Scan and Repair **9-13**

Scan Only **9-13**

アクション **9-15**

暗号化 **9-14**

ウイルスに感染 **9-15**

オリジナル メッセージのアーカイブ **9-18**

拡張オプション **9-16**

カスタムのアラート通知の送信 **9-19**

カスタム ヘッダーの追加 **9-19**

グローバル オプション **9-9**

グローバルでのイネーブル化 **9-10**
 スキャンできない **9-15**
 代替宛先ホストへの送信 **9-19**
 デフォルト通知の送信 **9-18**
 メールフローポリシー **5-15**
 メッセージ件名の変更 **9-17**
 メッセージ受信者の変更 **9-19**
 リスナーごとのアクション **9-12**

アンチスパム

false positive および陰性のレポート **8-28**
 HAT エントリ **5-15**
 IronPort Anti-Spam **8-6**
 X-IPASFiltered ヘッダー **8-12**
 アーカイブ **8-20, 8-22**
 アプライアンス生成メッセージのスキャン **8-5**
 大きいメッセージのスキャン **8-9**
 テスト **8-28**
 デフォルト スキャン エンジンの選択 **8-2**
 複数のスキャン エンジンの使用 **9-2**
 陽性スパムのしきい値 **8-19**
 陽性と疑わしいスパムのしきい値 **8-19**

い

イーサネット インターフェイス **5-2, B-1, B-2**

インジェクタ

「リスナー」を参照

インストール **3-1**
 復元 **15-12**
 陰性スコア **5-31**
 インターフェイスのサービス **A-1**
 インバウンド電子メール ゲートウェイ **5-2**
 インポート
 HTML テキスト リソース **14-26**
 テキスト リソース **14-22**

う

ウィザード
 Active Directory **3-35**
 システム セットアップ **3-1, 3-19**
 ウイルス定義
 自動アップデート間隔 **15-21**
 疑わしい送信者、スロットリング **5-39**

え

エクスポート
 HTML テキスト リソース **14-26**
 テキスト リソース **14-23**
 エンコード
 免責事項 **14-34**
 エンタープライズ ゲートウェイ **3-1**
 エンタープライズ ゲートウェイ構成 **5-3**
 エンベロープ送信者の DNS 検証 **5-59**

お

- 大きいメッセージのスキャン **8-9**
- オーバーフロー **10-16**
- オープン リレー、定義 **5-76**
- 大文字と小文字の区別
 - CLI **2-10**
 - systemsetup コマンド **3-41**
- 大文字と小文字を区別した照合 **14-8**
- オフセットの指定 **15-77**
- オンライン ヘルプ **2-5, 2-15**

か

- カスタム SMTP 応答
 - 変数 **5-60**
- カスタム ヘッダー **8-35**
- 画像分析 **6-15, 6-23**
- 角カッコ **2-9**
- 完全修飾ドメイン名 **5-27**
- 感染フィルタ
 - Adaptive Scanning **10-20**
 - CASE **10-6**
 - Context Adaptive Scanning Engine **10-6**
 - SNMP トラップ **10-32**
 - アラート **10-32**
 - アラートのイネーブル化 **10-20**
 - アンチウイルス アップデート **10-15**
 - アンチウイルス スキャンとの非併用 **10-15**

- ウイルス感染 **10-4**
- 概要 **10-2**
- 脅威カテゴリ **10-3**
- 検疫レベルのしきい値の設定 **10-24**
- 常時ルール **10-13**
- スキップ **6-24**
- 定義済みアウトブレイク ルール **10-10**
- 定義済みアダプティブ ルール **10-11**
- 非ウイルス性の脅威 **10-4**
- 評価キー **3-33, 3-54**
- ファイル拡張子のバイパス **10-24**
- 複数のスコア **10-14**
- メッセージの再評価 **10-15, 10-17**
- メッセージの遅延 **10-7**
- メッセージの変更 **10-9**
- メッセージ変更レベルのしきい値の設定 **10-25**
- リンクのリダイレクト **10-8**
- ルール **10-11**
- ルールのアップデート **10-21**
- 感染フィルタの評価キー **3-33, 3-54**
- 管理コマンド **15-1**

き

- 逆引き DNS ルックアップ
 - タイムアウト **15-61**
 - ディセーブル化 **15-64**
- 脅威レベル
 - 定義 **10-10**

局所的なスキャン [8-12](#)

く

空白スペース [8-23, 9-17](#)

クエリー インターフェイス [15-75](#)

グラフィカル ユーザ インターフェイス

「GUI」を参照

け

ゲートウェイ設定 [5-1](#)

検疫脅威レベルのしきい値

推奨デフォルト [10-12](#)

設定 [10-12](#)

検疫のオーバーフロー [10-16](#)

検疫レベルのしきい値 [10-24](#)

こ

工場出荷時の設定 [3-20](#)

更新サーバ [15-20](#)

コマンドの補完 [2-12](#)

コメント [5-56](#)

インポートしたファイル内のコメント [5-56](#)

コンテンツ ディクショナリ [14-1](#)

コンテンツ フィルタ

アクション [6-20](#)

条件 [6-11](#)

電子メールパイプライン中の適用 [6-10](#)

非 ASCII 文字セット [6-59](#)

変数 [6-28](#)

命名 [6-10](#)

メッセージフィルタとの比較 [6-10](#)

例 [6-49, 6-51, 6-52](#)

さ

サードパーティ リレー [5-76](#)

再帰的な DNS クエリー [15-63](#)

再設定 [3-19](#)

最大値

1 時間あたりの受信者数、
systemsetup [3-44, 3-49](#)

HAT 内での 1 時間あたりの受信者
数 [5-13, 7-13](#)

HAT 内での 1 メッセージあたりの受信者
数 [5-12](#)

HAT 内での 1 メッセージあたりの接続
数 [5-12](#)

HAT 内での同時接続数 [5-12](#)

HAT 内でのメッセージ サイズ [5-12](#)

サブネット [3-28, 3-41](#)

し

時間帯、設定 [3-24, 3-55](#)

時間帯ファイル

更新 **15-76**

時間の同期 **3-24, 3-55**

しきい値、SenderBase 評価スコアの **5-32**

時刻、システム **3-24, 3-55**

システム管理 **15-1**

システム クロック **3-24, 3-55**

システム時刻

 設定 **3-24, 3-55**

システム セットアップ **3-1**

システム セットアップの次の手順 **3-37**

自動アップデート **15-21**

 間隔 **15-21**

週ごとのステータス アップデート **3-55**

受信者へのアラート **15-25**

受信制御、バイパス **5-75**

使用可能なアップグレード **15-3**

常時ルール **10-13**

証明書

 デモ **3-42**

シリアル接続のピン割り当て **3-14, A-11**

信頼性 **5-31**

す

スタートアップ ガイド **3-1**

ストリーミング アップグレード **15-6**

スパム

 スパムにカスタムの X-Header を含める **8-20, 8-23**

 スパムの件名行の変更 **8-20, 8-23**

代替アドレスへの送信 **8-20, 8-23**

代替メールホストへの送信 **8-20, 8-23**

 テスト **8-28**

スプーフィング IP アドレス **7-3**

スロットリング **5-39, 7-1, 8-1**

スロットリングの推奨段階的手法 **7-8**

せ

セキュア コピー **A-10**

セキュアでないリレー **5-76**

設定

 電子メール セキュリティ アプライアンス **17-5**

設定、テスト **3-56**

セットアップ **3-1**

説明 **5-59**

選択したインターフェイスよりも優先されるルーティング **B-4**

そ

送信者

 GUI を使用した送信者の送信者グループへの追加 **5-48**

送信者グループ **5-12**

 BLACKLIST **5-38**

 GUI を使用した削除 **5-46**

 GUI を使用した追加 **5-43, 5-46**

 GUI を使用した編集 **5-45**

SUSPECTLIST [5-38](#)UNKNOWNLIST [5-38](#)WHITELIST [5-38](#)

送信者検証

不正な形式の MAIL FROM およびデフォルト ドメイン [5-60](#)例外テーブル [5-67](#)送信者検証例外テーブル [5-60](#)送信者の検索 [5-53](#)

た

代替アドレス [9-1](#)タイム サーバ [3-24, 3-56](#)タイムゾーン [15-75, 15-77](#)ダミー アカウント [7-11](#)単語の区切りの照合 [14-8](#)

ち

着信メッセージ、定義 [6-3](#)着信リレー [8-31](#)Received ヘッダー [8-37](#)カスタム ヘッダー [8-35](#)ログ エントリの例 [8-41](#)

つ

通知の選択 [14-39](#)

て

ディクショナリ用語のソート [14-8](#)

データ消失防止

「DLP」を参照

テキスト リソース

HTML リソースのエクスポートおよび HTML リソースへのインポート [14-26](#)インポート [14-22](#)エクスポート [14-23](#)概要 [14-18](#)管理 [14-20](#)コード ビュー [14-24](#)コンテンツ ディクショナリ [14-1](#)非 ASCII 文字 [14-19](#)ポリシーおよび設定での使用 [14-27](#)免責条項 [14-27](#)

テキスト リソースの

HTML ベース [14-24](#)

テスト

IronPort Anti-Spam [8-28](#)Sophos ウイルス エンジン [9-28](#)システム セットアップ [3-56](#)

デフォルト

IP アドレス [3-20](#)ゲートウェイ [3-26, 3-42](#)ドメイン [5-73](#)ホスト名 [3-23, 3-40](#)ルータ [3-26, 3-42](#)デフォルト DNS サーバ [15-63](#)

デフォルト ルータ **3-26**
 デモ証明書 **3-42**
 電子メール インジェクタ
 「リスナー」を参照
 電子メール セキュリティ アプライアンス
 設定 **17-5**
 電子メールの受け付け **5-10**
 電子メールの受信、設定 **5-1**
 電子メールの分類 **5-26, 5-38**
 電子メールのリダイレクト **3-28**
 電子メールのリレー **5-10**

と

ドット付き 10 進数形式 **3-27, 3-41**

ね

ネットワーク アクセス リスト **15-69**
 ネットワーク トポロジ **B-5**
 ネットマスク **3-27, 3-41**
 ネットマスク、選択 **B-2**
 ネットワーキング ワークシート **3-16**

は

バイパス
 スロットリング **5-74**
 パスワード **2-5**

パスワード、変更 **15-69**
 発信メッセージ、定義 **6-3**
 パブリック リスナー **3-44, 5-5**
 デフォルト エントリ **5-10**
 判断
 画像分析 **6-15, 6-23**

ひ

評価キー
 McAfee **3-54**
 Sophos **3-54**
 評価フィルタの推奨段階的手法 **7-6**
 評価フィルタリング **7-1, 8-1**

ふ

ファイアウォール ポート **C-1**
 フィッシング **8-6**
 復元
 インストール **15-12**
 使用可能なバージョン **15-12**
 複数のアプライアンス **3-20**
 複数の受信者 **6-7**
 部分的アドレス
 HAT 内の部分的アドレス **5-27**
 RAT 内の部分的アドレス **5-73**
 プライベート インジェクタ **3-47**
 プライベート リスナー **5-5**

デフォルト エントリ **5-10**
 ブラウザ
 複数のウィンドウまたはタブ **2-3**
 プロキシ サーバ **15-21**

へ

ヘッダー、挿入 **12-16**
 ヘッダーの挿入 **12-16**

ほ

ホスト DNS 検証、説明 **5-57**
 ホスト名 **3-23, 3-40**
 セットアップ中のホスト名の指定 **3-23**
 ホスト名、設定 **15-60**
 ポリシー、事前定義 **5-26**

ま

マルウェア
 定義 **9-3**
 マルチレイヤアンチウイルス スキャン **9-2**

め

メール フロー ポリシー
 \$ACCEPTED **5-33**
 \$BLOCKED **5-33, 5-40**

\$RELAYED **5-40**
 \$THROTTLED **5-33**
 \$TRUSTED **5-33**
 GUI **2-2**
 GUI を使用した削除 **5-47**
 GUI を使用した編集 **5-43, 5-47**
 HAT パラメータ **5-12**
 定義 **5-25**
 パブリック リスナー用 **5-33**
 プライベート リスナー用 **5-40**

メール ポリシー **6-1**
 First Match Wins **6-5**
 LDAP **6-37**
 アンチスパム設定の例 **6-34**
 ユーザの削除 **6-38**
 ユーザの追加 **6-38**
 メッセージのリレー **3-42, 5-2**
 メッセージ フィルタ アクションの変数
 免責事項の使用 **14-32**
 メッセージ分裂
 定義 **6-7**
 メッセージ変更レベルのしきい値 **10-25**
 免責事項
 メッセージへの追加 **14-28**
 免責事項スタンプ **14-28, 14-29**
 複数のエンコード **14-34**
 免責条項
 HTML テキスト リソース **14-24**
 テキスト リソースの使用 **14-27**

も

モニタリング サービス

C-Series での設定 [17-5](#)

ゆ

有効ビット

メール フロー ポリシーにセットされた有効ビット [5-14](#)

よ

陽性スコア [5-31](#)

り

リアルタイム、HAT の変更 [5-38](#)

リスナー

設定 [5-1](#)

定義 [5-2](#)

免責事項の追加 [14-28](#)

リバース DNS ルックアップ [5-18](#)

リモート アップグレード [15-7](#)

る

ルート サーバ (DNS) [3-26, 3-42](#)

ルックアップ

DNS A [5-26, 5-57](#)

DNS PTR [5-26, 5-57](#)

れ

例外テーブル

エントリの追加 [5-67](#)

レート制限 [5-39, 5-42](#)

ろ

ログ サブスクリプション

IronPort Anti-Spam [8-22](#)

Sophos [9-18](#)

論理 IP インターフェイス [3-27, 3-40](#)
