Cisco Secure Email Gateway 向け AsyncOS 14.0.3 ユーザーガイド（メンテナンス導入）

初版：2022 年 9 月 1 日

最終更新：2021 年 8 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章

Cisco Secure Email Gateway スタートアップガイド 1

AsyncOS 14.0.3 の新機能 2

Web インターフェイスの比較、新しい Web インターフェイスとレガシー Web インターフェイス 2

詳細情報の入手先 6

資料 7

トレーニング 7

Cisco 通知サービス 8

ナレッジ ベース 8

シスコサポートコミュニティ 8

シスコカスタマーサポート 9

サード パーティ コントリビュータ 9

マニュアルに関するフィードバック 9

シスコ アカウントの登録 9

Cisco Secure Email Gateway の概要 10

サポートされる言語 11

第 2 章

電子メールゲートウェイへのアクセス 13

Web ベースのグラフィカル ユーザー インターフェイス（GUI） 13

ブラウザ要件 13

GUI へのアクセス 14

工場出荷時のデフォルト ユーザ名とパスフレーズ 14

中央集中型の管理 15

How-To ウィジェットを使用したユーザ エクスペリエンスの強化 15

電子メールゲートウェイで How-To ウィジェットを無効化 15
構成時の設定の変更 16
設定の変更 16
変更の確定またはキャンセル 16
コマンドライン インターフェイス（CLI） 16

第 3 章 セットアップおよび設置 19
インストール計画 19
計画決定に影響を与える情報の確認 19
ネットワーク境界に電子メールゲートウェイを配置する 19
DNS への E メール セキュリティ アプライアンスの登録 20
インストールのシナリオ 21
設定の概要 21
着信 22
発信 22
イーサネット インターフェイス 22
ハードウェアのポート 22
拡張設定 23
ファイアウォール設定値（NAT、ポート） 23
電子メールゲートウェイのネットワークへの物理接続 23
設定シナリオ 23
着信メールと発信メールの分離 24
システム セットアップの準備 27
電子メールゲートウェイへの接続方式の決定 28
電子メールゲートウェイへの接続 28
ネットワーク アドレスと IP アドレスの割り当ての決定 29
管理およびデータ ポート用のデフォルト IP アドレス 29
電子メールを受信および配信するネットワーク接続の選択 30
物理イーサネット ポートへの論理 IP アドレスのバインド 30
接続用ネットワーク設定値の選択 30
セットアップ情報の収集 31

システム セットアップ ウィザードの使用 35
Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス 37
工場出荷時のデフォルト ユーザ名とパスフレーズ 38
レガシー Web インターフェイスへのアクセス 38
新しい Web インターフェイスの暗色モードでの利用 39
Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義 39
手順 1：開始 40
手順 2：システム 40
手順 3：ネットワーク 42
手順 4：セキュリティ 46
手順 5：レビュー 48
Active Directory への接続の設定 48
次の手順 49
コマンドライン インターフェイス（CLI）へのアクセス 49
工場出荷時のデフォルト ユーザ名とパスフレーズ 50
コマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行 51
admin パスフレーズの変更 52
ライセンス契約書の受諾 52
ホスト名の設定 52
論理 IP インターフェイスの割り当てと設定 52
デフォルト ゲートウェイの指定 54
Web インターフェイスのイネーブル化 54
DNS の設定 54
リスナーの作成 54
アンチスパムのイネーブル化 63
デフォルト アンチスパム スキャン エンジンの選択 63
スパム隔離のイネーブル化 63
アンチウイルス スキャンのイネーブル化 63
アウトブレイクフィルタの有効化 64
アラート設定値および AutoSupport の設定 64
スケジュール済みレポートの設定 64

時刻設定値の設定 64
変更の確定 65
設定のテスト 65
即時アラート 65
エンタープライズ ゲートウェイとしてシステムを設定 66
設定と次の手順の確認 66

第 4 章 電子メール パイプラインについて 67
電子メール パイプラインの概要 67
電子メール パイプラインのフロー 67
着信および受信 70
ホスト アクセス テーブル（HAT）、送信者グループ、およびメール フロー ポリシー 70
Received: ヘッダー 71
デフォルト ドメイン 71
バウンス検証 71
ドメイン マップ 72
受信者アクセス テーブル（RAT） 72
エイリアス テーブル 72
LDAP 受信者の受け入れ 72
SMTP コールアヘッド受信者検証 72
ワーク キューとルーティング 73
電子メール パイプラインとセキュリティ サービス 73
LDAP 受信者の受け入れ 74
マスカレードまたは LDAP マスカレード 74
LDAP ルーティング 74
メッセージ フィルタ 75
電子メール セキュリティ マネージャ（受信者単位のスキャン） 75
セーフリスト/ブロックリスト スキャン 75
スパム対策 75
アンチウイルス 76
グレイメールの検出と安全な購読解約 76

ファイル レピュテーション スキャンおよびファイル分析 76
コンテンツ フィルタ 76
アウトブレイク フィルタ 77
隔離 77
配信 77
仮想ゲートウェイ 78
配信制限 78
ドメインベースの制限値 78
ドメインベースのルーティング 78
グローバル登録解除 79
バウンス制限 79

第 5 章 電子メールを受信するためのゲートウェイの設定 81
電子メールを受信するためのゲートウェイ設定の概要 81
リスナーの使用 82
リスナーのグローバル設定 85
複数のエンコーディングが含まれるメッセージの設定 87
Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング 88
部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM 95
CLI を使用してリスナーを作成することによる接続要求のリスニング 95
HAT の詳細パラメータ 96
エンタープライズ ゲートウェイ構成 97

第 6 章 IP レピュテーション フィルタリング 99
送信者 IP レピュテーション フィルタリングの概要 99
IP レピュテーションサービス 99
IP レピュテーションスコア 100
送信者 IP レピュテーションフィルタの仕組み 101
さまざまな送信者 IP レピュテーション フィルタリング手法の推奨設定 102
リスナーの IP レピュテーション フィルタリング スコアのしきい値の編集 102
IP レピュテーションスコアを使用したIP レピュテーション フィルタリングのテスト 103

メッセージサブジェクトへの低 IP レピュテーションスコアの入力 105

第 7 章 ホスト アクセス テーブルを使用した接続を許可するホストの定義 107

接続を許可するホストの定義の概要 107

デフォルト HAT エントリ 108

送信者グループへのリモート ホストの定義 109

送信者グループの構文 110

ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ 111

HAT に基づくポリシーの設定 112

IP レピュテーションスコアを使用した送信者グループの定義 113

DNS リストにクエリーを実行することで定義された送信者グループ 114

メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 115

HAT 変数の構文 116

HAT 変数の使用 117

HAT 変数のテスト 118

定義済みの送信者グループとメール フロー ポリシーの理解 118

送信者グループからのメッセージの同様の処理 121

メッセージ処理の送信者グループの作成 122

既存の送信者グループへの送信者の追加 123

着信接続のために実行するルールの順序の並べ替え 123

送信者の検索 124

メール フロー ポリシーを使用した着信メッセージのルールの定義 124

メール フロー ポリシーのデフォルト値の定義 132

ホスト アクセス テーブルの設定の使用 132

外部ファイルへの ホスト アクセス テーブル設定のエクスポート 133

外部ファイルからのホスト アクセス テーブル設定のインポート 133

着信接続ルールへの送信者アドレス リストの使用 134

SenderBase 設定とメール フロー ポリシー 135

HAT Significant Bits 機能 136

HAT 設定 136

Significant Bits HAT ポリシー オプション 136

インジェクション制御期間 137
送信者の検証 137
送信者検証：ホスト 138
送信者検証：エンベロープ送信者 139
部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM 140
カスタム SMTP コードと応答 140
送信者検証例外テーブル 141
送信者検証の実装 — 設定例 141
送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング 142
未検証の送信者へのより厳格なスロットリング設定の実行 143
メール フロー ポリシー ACCEPTED を使用した未検証送信者への送信メッセージの定義 143
送信者の電子メール アドレスに基づいた送信者検証ルールからの未検証送信者の除外 144
送信者検証例外テーブル内でのアドレスの検索 144
未検証送信者からのメッセージの設定テスト 145
形式が不正な MAIL FROM 送信者アドレスのテスト メッセージの送信 145
送信者検証ルールから除外するアドレスからのメッセージの送信 145
送信者検証とロギング 146
エンベロープ送信者検証 146

第 8 章 ドメイン名または受信者アドレスに基づく接続の許可または拒否 147
受信者のアドレスに基づく接続の許可または拒否の概要 147
受信者アクセス テーブル（RAT）の概要 148
GUI を使用した RAT へのアクセス 148
CLI を使用した RAT へのアクセス 148
デフォルトの RAT エントリの編集 148
ドメインおよびユーザ 149
メッセージを受け入れるドメインおよびユーザの追加 150
受信者アドレスの定義 150
特別な受信者での LDAP 許可のバイパス 151

特別な受信者でのスロットリングのバイパス 152
受信者アクセス テーブルでのドメインおよびユーザの順序の入れ替え 152
受信者アクセス テーブルの外部ファイルへのエクスポート 153
受信者アクセス テーブルの外部ファイルからのインポート 153

第 9 章 メッセージ フィルタを使用した電子メール ポリシーの適用 155
概要 155
メッセージ フィルタのコンポーネント 157
メッセージ フィルタ ルール 157
メッセージ フィルタ アクション 157
メッセージ フィルタの構文例 158
メッセージ フィルタの処理 159
メッセージ フィルタの順番 160
メッセージ ヘッダー ルールおよび評価 160
メッセージ本文とメッセージ添付ファイル 160
コンテンツ スキャンの一致のしきい値 161
しきい値の構文 162
メッセージ本文と添付ファイルのしきい値スコア 162
しきい値スコアリング マルチパート/代替 MIME 部分 163
コンテンツ ディクショナリを使用したしきい値のスコアリング 164
メッセージ フィルタ内の AND テストと OR テスト 164
メッセージ フィルタ ルール 165
フィルタ ルールの概要の表 165
ルールで使用する正規表現 181
メッセージのフィルタリングでの正規表現の使用 183
正規表現の使用に関するガイドライン 184
正規表現と非 ASCII 文字セット 184
n テスト 184
大文字と小文字の区別 184
効率的なフィルタの作成 185
PDF と正規表現 185

スマート ID 186
スマート ID の構文 186
メッセージ フィルタ ルールの説明と例 188
true ルール 190
有効なルール 190
subject ルール 190
エンベロープ受信者ルール 191
グループ内エンベロープ受信者ルール 191
エンベロープ送信者ルール 192
グループ内エンベロープ送信者ルール 192
送信者グループ ルール 193
本文サイズ ルール 193
リモート IP ルール 194
受信リスナー ルール 194
受信 IP インターフェイス ルール 195
日付ルール 195
ヘッダー ルール 195
乱数ルール 196
受信者数ルール 197
アドレス数ルール 197
本文スキャン ルール 197
本文スキャン 198
暗号化検出ルール 198
添付ファイル タイプ ルール 199
添付ファイル名ルール 200
DNS リスト ルール 201
IP レピュテーションルール 202
ディクショナリ ルール 202
SPF-Status ルール 204
SPF-Passed ルール 206
S/MIME ゲートウェイ メッセージ ルール 206

S/MIME ゲートウェイ検証済みルール 206
workqueue-count ルール 206
SMTP 認証済みユーザー一致ルール 207
署名付きルール 209
署名付き証明書ルール 209
ヘッダー繰り返し回数ルール 212
URL レピュテーション ルール 214
URL カテゴリ ルール 215
破損した添付ファイル ルール 215
メッセージ言語ルール 216
マクロ検出ルール 217
偽造メールの検出ルール 218
重複境界検証ルール 219
不正な形式の MIME ヘッダー検出ルール 219
地理位置情報ルール 219
ETF のドメイン レピュテーション ルール 220
SDR のドメイン レピュテーション ルール 220
メッセージ フィルタ アクション 223
フィルタ アクション一覧表 223
添付ファイル グループ 233
アクション変数 235
非 ASCII 文字セットとメッセージ フィルタ アクション変数 237
一致した内容の表示 238
メッセージ フィルタ アクションの説明と例 239
「残りのメッセージ フィルタをスキップ」アクション 239
ドロップ アクション 240
バウンス アクション 240
暗号化アクション 241
配信時の S/MIME 署名/暗号化アクション 241
S/MIME 署名または暗号化アクション 241
通知およびコピー通知アクション 241

ブラインド カーボン コピー アクション 244
隔離および複製アクション 246
受信者変更アクション 247
配信ホスト変更アクション 247
送信元ホスト（Virtual Gateway アドレス）変更アクション 248
アーカイブ アクション 249
ヘッダー削除アクション 250
ヘッダー挿入アクション 250
ヘッダー テキスト編集アクション 251
本文編集アクション 251
HTML 変換アクション 252
バウンス プロファイル アクション 253
アンチスパム システムのバイパス アクション 253
グレイメール アクションのバイパス 254
アンチウイルス システムのバイパス アクション 254
ファイル レピュテーション フィルタリングおよびファイル分析システムのバイパス アクション 255
ウイルス アウトブレイク フィルタのスキャニング処理バイパス アクション 255
メッセージ タグ追加アクション 256
ログ エントリ追加アクション 256
URL レピュテーション アクション 256
URL カテゴリ アクション 259
オペレーションなし 260
偽造メールの検出アクション 260
添付ファイルのスキャン 260
添付ファイルのスキャンで使用するメッセージ フィルタ 262
イメージ分析 264
イメージ分析スキャン エンジンの設定 264
イメージ分析設定の調整 265
イメージ分析結果に基づいたアクション実行のメッセージ フィルタの構成 266
イメージ分析の評価に基づいて添付ファイルを除去するコンテンツ フィルタの作成 267

イメージ分析判定に基づくアクションの設定 268
通知 268
添付ファイルのスキャン メッセージ フィルタの例 269
ヘッダーの挿入 269
ファイル タイプによる添付ファイルのドロップ 270
ディクショナリの一致による添付ファイルのドロップ 271
保護された添付ファイルの隔離 272
保護されていない添付ファイルの検出 272
メッセージ フィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出 272
CLI を使用したメッセージ フィルタの管理 273
新しいメッセージ フィルタの作成 275
メッセージ フィルタの削除 275
メッセージ フィルタの移動 276
メッセージ フィルタのアクティベーションとディアクティベーション 276
メッセージ フィルタのアクティベーションまたはディアクティベーション 279
事前ポリシーフィルタのインポート 279
メッセージ フィルタのエクスポート 280
非 ASCII 文字セットの表示 280
メッセージ フィルタ リストの表示 280
メッセージ フィルタの詳細の表示 280
フィルタ ログ サブスクリプションの構成 281
メッセージのエンコードの変更 282
サンプル メッセージ フィルタ 284
メッセージ フィルタの例 289
オープンリレー防止フィルタ 289
ポリシー適用フィルタ 290
件名に基づき通知するフィルタ 290
競合他社に送信されたメールの BCC およびスキャン 290
特定のユーザをブロックするフィルタ 291
メッセージのアーカイブおよびドロップ フィルタ 291

大きい「To:」ヘッダーのフィルタ 291
空白の「From:」フィルタ 292
IP レピュテーションフィルタ 292
IP レピュテーションフィルタの変更 292
ファイル名の正規表現フィルタ 292
ヘッダー内の IP レピュテーションスコアの表示フィルタ 293
ポリシーのヘッダーへの挿入フィルタ 293
多数の受信者のバウンス フィルタ 293
ルーティングおよびドメイン スプーフィング 293
Virtual Gateway フィルタの使用 294
配信とリスナーのフィルタに対する同じリスナーの使用 294
単一のリスナーのフィルタ 294
スプーフィング ドメインのドロップ フィルタ（単一のリスナー） 295
スプーフィング ドメインのドロップ フィルタ（複数のリスナー） 295
別のスプーフィング ドメインのドロップ フィルタ 295
ルーピングの検出フィルタ 296
ファイル SHA-256 フィルタに一致するメッセージ添付ファイルをドロップする 297
添付ファイルがファイル SHA-256 フィルタと一致する場合にメッセージをドロップする 297
スキャン動作の設定 297
スキャンできないメッセージのメッセージ処理アクションの設定 304
メッセージの配信 305
ポリシー隔離へメッセージの送信 306

第 10 章 メール ポリシー 309
メール ポリシーの概要 309
メール ポリシーをユーザ単位で適用する方法 310
着信メッセージと発信メッセージの異なる処理 311
メール ポリシーへのユーザの一致 312
最初に一致したものが有効 312
ポリシー マッチングの例 313

例 1 313
例 2 314
例 3 314
メッセージ分裂 314
管理例外 316
メール ポリシーの設定 316
着信または発信メッセージのデフォルトのメール ポリシーの設定 316
送信者および受信者のグループのメール ポリシーの作成 317
メール ポリシーの送信者および受信者の定義 318
例 319
送信者または受信者に適用するポリシーの検索 321
管理例外 321
メッセージ ヘッダーの優先順位の設定 322

第 11 章 コンテンツ フィルタ 325
コンテンツ フィルタの概要 325
コンテンツ フィルタの仕組み 325
コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法 326
コンテンツ フィルタの条件 327
コンテンツ フィルタのアクション 338
アクション変数 346
コンテンツに基づくメッセージのフィルタリング方法 349
コンテンツ フィルタの作成 349
デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化 351
特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用 351
GUI でのコンテンツ フィルタの設定に関する注意事項 352

第 12 章 外部脅威フィードを使用する電子メールゲートウェイの設定 355
外部脅威フィードの概要 355
外部脅威フィードを使用する電子メールゲートウェイの設定方法 356
外部脅威フィード機能キーの取得 358

電子メールゲートウェイでの外部脅威フィードエンジンの有効化 359
外部脅威フィード ソースの設定 360
SecureX Threat Response フィードソースの設定 364
脅威が含まれているメッセージの処理 369
脅威が含まれているメッセージの処理に向けた送信者グループの設定 369
脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージ フィルタの設定 370
コンテンツ フィルタを使用した、メッセージの悪意のあるドメインの検出 370
ドメインの例外リストの作成 371
メッセージ フィルタを使用した、メッセージの悪意のあるドメインの検出 372
コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出 372
メッセージ フィルタを使用した、メッセージの悪意のある URL の検出 374
コンテンツ フィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出 376
ファイル ハッシュのリストの作成 377
メッセージ フィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出 377
受信メール ポリシーへのコンテンツ フィルタのアタッチ 378
外部脅威フィードおよびクラスタ 379
外部脅威フィード エンジンの更新のモニタリング 379
アラートの表示 379
メッセージ トラッキングの脅威詳細の表示 380

第 13 章 送信者ドメイン レピュテーション フィルタリング 381
送信者ドメイン レピュテーション フィルタリングの概要 381
SDR 判定 382
送信者ドメイン レピュテーションに基づいてメッセージをフィルタリングする方法 385
電子メールゲートウェイでの送信者ドメイン レピュテーション フィルタリングの有効化 385
送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定 387
メッセージ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング 387

コンテンツ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング 389
ドメインの例外リストの作成 390
受信メール ポリシーへのコンテンツ フィルタのアタッチ 391
送信者ドメイン レピュテーション フィルタリングおよびクラスタ 392
メッセージ トラッキングの送信者ドメイン レピュテーション詳細の表示 392
アラートの表示 393
ログの表示 393
SDR フィルタリングのログ エントリの例 393
送信者ドメイン レピュテーションの認証の失敗 393
送信者ドメイン レピュテーションのリクエストのタイムアウト 394
送信者ドメイン レピュテーションの無効なホスト 394
送信者ドメインのレピュテーションの一般的なエラー 394

第 14 章 **Cisco SecureX Threat Response との統合 397**
電子メールゲートウェイと Cisco SecureX Threat Response の統合 397
電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 398
前提条件 400
電子メールゲートウェイでの Cisco Cloud Services ポータルの有効化 401
Cisco Cloud Services ポータルへの電子メールゲートウェイの登録 402
登録が成功したかどうかの確認 402
電子メールゲートウェイでの Cisco SecureX Threat Response の有効化 403
Cisco Cloud Services ポータルへの電子メールゲートウェイの登録 403
Cisco SecureX Ribbon を使用した攻撃分析の実行 404
Cisco SecureX Ribbon へのアクセス 405
Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 406
Cisco SecureX Threat Response 内のメッセージに対する修復アクションの実行 408
Cisco Success Network を使用した電子メールゲートウェイのユーザエクスペリエンスの向上 409
電子メールゲートウェイでの CSN での有効化 410
電子メールゲートウェイでの CSN の無効化 411

第 15 章 メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定 413

概要 413

メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定方法 414

電子メール ゲートウェイで Safe Print 設定を構成 414

メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタの設定 416

受信メール ポリシーへのコンテンツ フィルタのアタッチ 420

Safe Print の設定とクラスタ 420

Safe Print で出力された添付ファイル付きメッセージのモニタリング 420

ログの表示 421

Safe Print ログエントリの例 421

一時ディレクトリを作成できない 421

Safe Print 対象の PDF 添付ファイルを作成できない 421

破損ファイル 422

暗号化ファイル 422

タイムアウトエラー 422

メッセージトラッキングでの Safe Print 詳細の表示 422

第 16 章 電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合 425

概要 425

電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合方法 426

Cisco Secure Awareness クラウドサービスアカウントの作成 427

Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 428

電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成 429

Cisco Secure Awareness クラウドサービスからの認証トークンの取得 430

電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化 431

リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成 432

Cisco Secure Awareness クラウドサービスとクラスタ 433

ログの表示 433
アラートの表示 435

第 17 章 アンチウイルス 439
アンチウイルス スキャンの概要 439
評価キー 440
複数のアンチウイルス スキャンエンジンによるメッセージのスキャン 440
Sophos アンチウイルス フィルタリング 441
ウイルス検出エンジン 441
ウイルス スキャン 442
検出方法 442
パターン照合 442
発見的手法 442
エミュレーション 443
ウイルスの記述 443
Sophos アラート 443
ウイルスが発見された場合 443
McAfee アンチウイルス フィルタリング 444
ウイルス シグニチャとのパターン照合 444
暗号化されたポリモーフィック型ウイルスの検出 444
発見的分析 445
ウイルスが発見された場合 445
電子メールゲートウェイでのウイルスのスキャンの設定方法 445
ウイルス スキャンのイネーブル化およびグローバル設定の構成 446
ユーザのウイルス スキャン アクションの設定 447
メッセージ スキャン設定 447
メッセージ処理設定 448
メッセージ処理アクションの設定の構成 449
送信者および受信者のグループごとのアンチウイルス ポリシーの設定 454
ウイルス対策設定に関する注意事項 455
アンチウイルス アクションのフロー ダイアグラム 456

アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信 457
ウイルス定義ファイルの更新 459
HTTP を使用したアンチウイルス アップデートの取得について 459
アップデート サーバ設定の構成 460
モニタリングおよび手動での Anti-Virus アップデート チェック 460
手動でのアンチウイルス エンジンの更新 460
電子メールゲートウェイでのアンチウイルスファイルの更新の確認 460

第 18 章 スパムおよびグレイメールの管理 461
スパム対策スキャンの概要 461
スパム対策ソリューション 462
メッセージがスパムかどうかスキャンするための 電子メールゲートウェイの設定方法 462
IronPort スパム対策フィルタリング 464
評価キー 464
Cisco Anti-Spam：概要 465
IronPort Anti-Spam スキャンの設定 465
Intelligent Multi-Scan とグレイメール検出の設定 467
Cisco Intelligent Multi-Scan の設定 468
グレイメールの管理 469
グレイメールの概要 469
電子メールゲートウェイでのグレイメール管理ソリューション 470
グレイメール管理ソリューションの仕組み 471
グレイメールの検出および安全な配信停止の設定 474
グレイメールの検出および安全な配信停止のトラブルシューティング 480
Intelligent Multi-Scan とグレイメール検出のグローバル設定 481
スパム対策ポリシーの定義 481
陽性および陽性と疑わしいスパムのしきい値について 485
設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション 486
正規の送信元からの不要なマーケティング メッセージ 486

カスタムヘッダーを使用して、陽性と疑わしいスパム内のURLをCisco Webセキュリティプロキシにリダイレクトする：設定例 487
異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例 488
スパムフィルタからの 電子メールゲートウェイ生成メッセージの保護 490
スパム対策スキャン中に追加されるヘッダー 490
誤って分類されたメッセージのシスコへの報告 491
誤って分類されたメッセージのシスコへの報告方法 491
誤って分類されたメッセージのシスコへの報告方法 493
Cisco E メール セキュリティ プラグインの使用 494
誤って分類されたメッセージの添付ファイルとしての転送 495
送信を追跡する方法 497
着信リレー構成における送信者の IP アドレスの決定 497
着信リレーを使用した環境例 498
着信リレーを使用する 電子メールゲートウェイの設定 499
着信リレー機能のイネーブル化 499
着信リレーの追加 500
リレーされたメッセージのメッセージ ヘッダー 501
着信リレーが機能にどのように影響するか 505
着信リレーとフィルタ 505
着信リレー、HAT、IP レピュテーションスコア、および送信者グループ 505
着信リレーおよびディレクトリ ハーベスト攻撃防止 505
着信リレーおよびトレース 506
着信リレーと電子メール セキュリティ モニタ（レポート） 506
着信リレーおよびメッセージ トラッキング 506
着信リレーとロギング 506
使用するヘッダーを指定するログの設定 507
モニタリング ルールのアップデート 507
スパム対策のテスト 508
Cisco Anti-Spam をテストするための 電子メールゲートウェイへのメール送信 509
スパム対策設定のテスト：SMTP の使用例 510
スパム対策の有効性をテストできない方法 510

第 19 章 アウトブレイク フィルタ 513
アウトブレイク フィルタの概要 513
アウトブレイク フィルタの動作 514
メッセージの遅延、リダイレクトおよび修正 514
脅威カテゴリ 515
ウイルス アウトブレイク 515
フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威 515
Cisco Security Intelligence Operations 516
コンテキスト適応スキャン エンジン 517
メッセージの遅延 517
URL のリダイレクト 518
メッセージの変更 519
ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール 519
アウトブレイクのルール 519
適応ルール 520
アウトブレイク 520
脅威レベル 521
隔離脅威レベルのしきい値設定ガイドライン 521
コンテナ：特定ルールおよび常時ルール 522
アウトブレイク フィルタの機能概要 522
メッセージ スコアリング 523
動的隔離 524
アウトブレイク ライフサイクルおよびルール発行 525
アウトブレイク フィルタの管理 526
アウトブレイク フィルタのグローバル設定の構成 528
アウトブレイク フィルタ機能の有効化 528
アダプティブ ルールの有効化 529
アウトブレイク フィルタのアラートの有効化 529
URL のロギングと URL のメッセージ トラッキングの詳細の有効化 529
アウトブレイク フィルタ ルール 530

アウトブレイク フィルタ ルールの管理 530
アウトブレイク フィルタ機能とメール ポリシー 531
隔離レベルのしきい値の設定 532
最大隔離保持 532
ファイル拡張子タイプのバイパス 532
メッセージ変更 533
アウトブレイク フィルタ機能とアウトブレイク隔離 536
アウトブレイク隔離のモニタリング 537
[アウトブレイク隔離（Outbreak Quarantine）]および[ルールサマリーによる管理（Manage by Rule Summary）] ビュー 538
アウトブレイク フィルタのモニタリング 539
アウトブレイク フィルタ レポート 539
アウトブレイク フィルタの概要とルール リスト 539
アウトブレイク隔離 540
アラート、SNMP トラップ、およびアウトブレイク フィルタ 540
アウトブレイク フィルタ機能のトラブルシューティング 540
誤って分類されたメッセージのシスコへの報告 540
複数の添付ファイルおよびバイパスされるファイル タイプ 541
メッセージ フィルタ、コンテンツ フィルタ、および電子メール パイプライン 541

第 20 章 **悪意のある URL または望ましくない URL からの保護 543**
URL 関連の保護および制御 543
評価される URL 544
URL フィルタリングの設定 544
URL フィルタリングの要件 545
URL フィルタリングを有効にする 545
Talos インテリジェンスサービスへの接続について 548
URL フィルタリング機能の証明書 548
Web インタラクション トラッキング 549
Web インタラクション トラッキングの設定 549
Cisco Aggregator Server への接続について 549

クラスタ構成での URL フィルタリング 550
URL フィルタリングの許可リストの作成 550
URL リストのインポート 551
サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ 552
メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 553
URL 関連の条件(ルール）およびアクションの使用 554
URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール 554
メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 555
リダイレクト URL：エンドユーザのエクスペリエンス 557
URL フィルタリング用にスキャンできないメッセージの処理 558
コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出 558
メッセージ フィルタを使用した、メッセージの悪意のある URL の検出 560
URL フィルタリング結果のモニタ 562
メッセージ トラッキングの URL 詳細の表示 562
URL フィルタリングのトラブルシューティング 562
ログの表示 563
アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） 563
アラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） 564
Talos インテリジェンスサービスに接続できない 564
アラート：シスコ アグリゲータ サーバに接続できない（Unable to Connect to the Cisco Aggregator Server） 565
アラート：シスコ アグリゲータ サーバから Web インタラクション トラッキング情報を取得できない（Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server） 565
websecurityadvancedconfig コマンドの使用 566
メッセージ トラッキング検索で指定のカテゴリのメッセージが見つからない 566
悪意のある URL とマーケティング メッセージがアンチスパム フィルタまたはアウトブレイク フィルタでキャプチャされない 566
フィルタリングされたカテゴリの URL が正しく処理されない 566

エンドユーザが書き換え後の URL から悪意のあるサイトにアクセスする 567
Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 567
URL カテゴリについて 568
URL カテゴリについて 568
URL のカテゴリの判別 584
未分類の URL と誤って分類された URL の報告 584
将来の URL カテゴリ セットの変更 584

第 21 章 ファイル レピュテーション フィルタリングとファイル分析 585
ファイル レピュテーション フィルタリングとファイル分析の概要 585
ファイル脅威判定のアップデート 586
ファイル処理の概要 586
ファイル レピュテーションおよび分析サービスでサポートされるファイル 588
アーカイブ ファイルまたは圧縮ファイルの処理 589
クラウドに送信される情報のプライバシー 590
ファイル レピュテーションと分析機能の設定 590
ファイル レピュテーションと分析サービスとの通信の要件 591
オンプレミスのファイル レピュテーション サーバの設定 592
オンプレミスのファイル分析サーバの設定 593
ファイル レピュテーションと分析サービスの有効化と設定 594
AMP for Endpoints コンソールとアプライアンスの統合 602
重要：ファイル分析設定に必要な変更 605
（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定 605
分析グループ内のアプライアンスの確認 607
ファイル レピュテーション スキャンおよびファイル分析のメール ポリシーの設定 607
分析のために送信した添付ファイルがあるメッセージの隔離 610
ファイル分析隔離の使用 612
ファイル分析隔離の設定の編集 612
ファイル分析隔離領域内のメッセージの手動処理 613
中央集中型のファイル分析の隔離 614
ファイル レピュテーションと分析の X ヘッダー 614

ドロップされたメッセージまたは添付ファイルに関する通知のエンドユーザへの送信 614
高度なマルウェア防御とクラスタ 615
Advanced Malware Protection の問題に関するアラートの確実な受信 615
Advanced Malware Protection 機能の集約管理レポートの設定 616
ファイル レピュテーションおよびファイル分析のレポートとトラッキング 616
SHA-256 ハッシュによるファイルの識別 616
ファイル レピュテーションとファイル分析レポートのページ 617
その他のレポートでのファイル レピュテーション フィルタ データの表示 619
メッセージ トラッキング機能と Advanced Malware Protection 機能について 619
ファイルの脅威判定の変更時のアクションの実行 620
ファイル レピュテーションと分析のトラブルシューティング 620
ログ ファイル 620
トレースの使用 621
ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート 621
API キーのエラー（オンプレミスのファイル分析） 622
ファイルが予想どおりにアップロードされない 622
分析のために送信できるファイル タイプに関するアラート 623

第 22 章 データ損失の防止 625
データ消失防止の概要 625
DLP スキャン プロセスの概要 626
データ消失防止の動作 626
データ消失防止のシステム要件 627
データ漏洩防止の設定方法 627
データ消失防止の有効化（DLP） 628
データ損失防止のポリシー 629
DLP ポリシーの説明 629
定義済み DLP ポリシー テンプレート 630
ウィザードを使用した DLP 防止の設定 630
事前定義されたテンプレートを使用した DLP ポリシーの作成 632

カスタム DLP ポリシーの作成（詳細） 633
コンテンツ照合分類子を使用した拒否されたコンテンツの定義について 635
コンテンツ照合分類子の例 635
カスタム DLP ポリシーに対するコンテンツ照合分類子の作成 637
機密情報を特定する分類子検出ルール（カスタム DLP ポリシーのみ） 639
識別番号を識別する正規表現 639
機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用 641
疑わしい違反のリスク要因の判別子 643
エンティティベースのルールで最小スコアを使用する（カスタム DLP ポリシーのみ） 645
カスタム コンテンツ分類子が使用されるポリシーの表示 646
DLP ポリシーのメッセージのフィルタリング 646
違反の重大度の評価について 647
重大度スケールの調整 648
違反との一致に対する Email DLP ポリシーの順序の調整 648
発信メール ポリシーとの DLP ポリシーの関連付け 649
デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け 649
発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て 650
DLP ポリシーの編集または削除に関する重要な情報 650
メッセージ アクション 650
DLP 違反アクション（メッセージ アクション）に対して実行するアクションの定義 651
メッセージ アクションの表示および編集 653
DLP 通知のドラフト 654
DLP 通知テンプレートの変数の定義 655
メッセージ トラッキングでの機密性の高い DLP データの表示 657
DLP エンジンおよびコンテンツ照合分類子の更新について 657
DLP エンジンの現在のバージョンの決定 658
DLP エンジンとコンテンツ照合分類子の手動による更新 658
自動アップデートの有効化（推奨されません） 658
一元化された（クラスタ化された）電子メールゲートウェイの DLP 更新 659
DLP インシデントのメッセージとデータの使用 659

トラブルシューティング データ消失防止 660
DLP が電子メールの添付ファイルの違反を検出しない 660

第 23 章 Cisco 電子メール暗号化 663
Cisco 電子メール暗号化の概要 663
Cisco Secure Email Encryption Service でメッセージを暗号化する方法 664
暗号化ワークフロー 665
電子メールゲートウェイを使用したメッセージの暗号化 665
電子メールゲートウェイでのメッセージの暗号化のイネーブル化 666
キー サービスによる暗号化メッセージの処理方法の設定 667
エンベロープのデフォルト ロケールの設定 670
PXE エンジンの最新バージョンへの更新 671
暗号化するメッセージの決定 672
TLS 接続を暗号化の代わりに使用 672
コンテンツ フィルタを使用したメッセージの暗号化と即時配信 673
コンテンツ フィルタを使用した配信時のメッセージの暗号化 674
メッセージへの暗号化ヘッダーの挿入 675
暗号化ヘッダー 676
暗号化ヘッダーの例 678
オフラインでの開封のためエンベロープ キーをイネーブルにする 679
JavaScript を含まないエンベロープのイネーブル化 679
メッセージ有効期限のイネーブル化 679
復号アプレットの無効化 679

第 24 章 S/MIME セキュリティ サービス 681
S/MIME セキュリティ サービスの概要 681
電子メールゲートウェイでの S/MIME セキュリティサービス 682
S/MIME セキュリティ サービスのしくみについて 682
シナリオ：Business-to-Business（B2B） 683
シナリオ：Business-to-Consumer 684
S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化 685

電子メールゲートウェイでの S/MIME 署名および暗号化ワークフロー 685
S/MIME 署名ワークフロー 686
S/MIME 暗号化ワークフロー 686
S/MIME を使用して発信メッセージの署名、暗号化、または署名と暗号化を行う方法 686
S/MIME 署名用の証明書の設定 688
自己署名 S/MIME 証明書の作成 688
S/MIME 署名証明書のインポート 690
S/MIME 暗号化用の公開キーの設定 691
S/MIME 暗号化用の公開キーの追加 691
S/MIME 収集済み公開キー 692
公開キーの収集 692
S/MIME 送信プロファイルの管理 693
メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成 694
S/MIME 送信プロファイルの編集 695
署名、暗号化、または署名と暗号化を行うメッセージの決定 696
コンテンツ フィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信 696
コンテンツ フィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化 697
S/MIME を使用した着信メッセージの検証、復号、または復号と検証 698
電子メールゲートウェイでの S/MIME 検証および復号ワークフロー 698
S/MIME 検証ワークフロー 698
S/MIME 復号ワークフロー 699
S/MIME を使用して着信メッセージの検証、復号、または復号と検証を行う方法 699
メッセージを復号するための証明書の設定 700
署名されたメッセージを検証するための公開キーの設定 701
S/MIME 検証用の公開キーの追加 701
S/MIME 検証用の公開キーの収集 702
公開キーの収集のイネーブル化 702
S/MIME 検証用の収集された公開キーの追加 703
S/MIME 復号および検証のイネーブル化 703

S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定 704
S/MIME 証明書の要件 704
署名のための証明書の要件 704
暗号化のための証明書の要件 705
公開キーの管理 706
公開キーの追加 707
既存のエクスポート ファイルからの公開キーのインポート 707
公開キーのエクスポート 708

第 25 章 メールボックスでのメッセージの修復 709
概要 709
ワークフロー 710
電子メールゲートウェイによる自動修復アクションの実行の仕組み 712
メールボックス内のメッセージに対する修復アクションの実行 714
Microsoft Exchange Online メールボックス内のメッセージに対する修復アクションの実行 714
Microsoft Exchange Online メールボックスのメッセージに対する修復アクションの設定方法 714
Microsoft Exchange オンプレミスメールボックス内のメッセージに対する修復アクションの実行 717
Microsoft Exchange オンプレミス メールボックスのメッセージに対する修復アクションの設定方法 718
ハイブリッド展開のメールボックス内のメッセージに対する修復アクションの実行 719
ハイブリッド展開のメールボックスのメッセージに対する修復アクションの実行方法 719
電子メールゲートウェイでのメールボックス修復機能の設定 722
前提条件 723
Microsoft Exchange Online メールボックスのメッセージ修復の前提条件 723
オンプレミス アカウントのメッセージ修復の前提条件 724
Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 725
電子メールゲートウェイでのアカウント設定の有効化 727
アカウント プロファイルの作成 728

連結プロファイルの作成 730
アカウント プロファイルへのドメインのマッピング 731
メールボックス内のメッセージに対する自動修復アクションの設定 732
メールボックス内のメッセージの検索と修復 733
AsyncOS 13.0 以降のリリースへのアップグレード 734
メールボックス修復結果のモニタリング 735
メッセージ トラッキングでのメールボックス修復の詳細の表示 735
メールボックス修復のトラブルシューティング 735
接続エラー 736
ログの表示 738
アラート 738
設定された是正措置が実行されない 739

第 26 章 電子メール認証 741
電子メール認証の概要 741
DomainKeys と DKIM 認証 742
DomainKeys と DKIM 認証ワークフロー 742
AsyncOS の DomainKeys および DKIM 署名 742
DomainKeys および DKIM 署名の構成 744
署名キー 744
署名キーのエクスポートとインポート 745
公開キー 745
ドメイン プロファイル 746
ドメイン プロファイルのエクスポートとインポート 747
送信メールの署名のイネーブル化 747
バウンスおよび遅延メッセージの署名のイネーブル化 747
DomainKeys/DKIM 署名の設定（GUI） 748
DomainKeys 署名のドメイン プロファイルの作成 749
DKIM 署名の新しいドメイン プロファイルの作成 750
署名キーの作成または編集 752
署名キーのエクスポート 753

既存の署名キーのインポートまたは入力 753
署名キーの削除 754
DNS テキスト レコードの生成 755
ドメイン プロファイルのテスト 756
ドメイン プロファイルのエクスポート 756
ドメイン プロファイルのインポート 756
ドメイン プロファイルの削除 757
ドメイン プロファイルの検索 757
DKIM グローバル設定の編集 758
ドメイン キーとロギング 758
DKIM を使用した受信メッセージの検証方法 759
AsyncOS による DKIM 検証チェック 759
DKIM 検証プロファイルの管理 760
DKIM 検証プロファイルの作成 761
DKIM 検証プロファイルのエクスポート 762
DKIM 検証プロファイルのインポート 762
DKIM 検証プロファイルの削除 762
DKIM 検証プロファイルの検索 763
メール フロー ポリシーでの DKIM 検証の設定 763
DKIM 検証とロギング 764
DKIM 検証済みメールのアクションの設定 764
SPF および SIDF 検証の概要 765
有効な SPF レコードに関する注意 766
有効な SPF レコード 766
有効な SIDF レコード 766
SPF レコードのテスト 767
SPF/SIDF を使用した受信メッセージの検証方法 767
SPF と SIDF のイネーブル化 768
CLI を使用した SPF および SIDF のイネーブル化 769
Received-SPF ヘッダー 772
SPF/SIDF 検証済みメールに対して実行するアクションの決定 773

検証結果 773
CLI での spf-status フィルタ ルールの使用 774
GUI での spf-status コンテンツ フィルタ ルール 775
spf-passed フィルタ ルールの使用 775
SPF/SIDF 結果のテスト 776
SPF/SIDF 結果の基本の詳細度のテスト 776
SPF/SIDF 結果の高い詳細度のテスト 777
DMARC 検証 777
DMARC 検証のワークフロー 778
DMARC を使用した受信メッセージの検証方法 779
DMARC 検証プロファイルの管理 780
DMARC のグローバル設定 783
メール フロー ポリシーでの DMARC 検証の設定 784
DMARC フィードバック レポートの返信アドレスの設定 785
DMARC 集計レポート 785
偽装メールの検出 787
偽造メールの検出の設定 787
偽装メールの検出結果の監視 788
メッセージ トラッキングでの偽装メールの詳細の表示 789

第 27 章 テキスト リソース 791
テキスト リソースの概要 791
コンテンツ ディクショナリ 791
テキスト リソース 792
メッセージの免責事項スタンプ 793
コンテンツ ディクショナリ 793
ディクショナリの内容 794
単語境界と 2 バイト文字セット 795
テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 795
ディクショナリの追加 796
ディクショナリの削除 797

ディクショナリのインポート 797
ディクショナリのエクスポート 798
コンテンツ ディクショナリ フィルタ ルールの使用方法およびテスト方法 798
ディクショナリの照合フィルタ ルール 799
ディクショナリ エントリの例 800
コンテンツ ディクショナリのテスト方法 800
テキスト リソースについて 800
テキスト ファイルとしてのテキスト リソースのインポートおよびエクスポート 801
テキスト リソース管理の概要 802
テキスト リソースの追加 802
テキスト リソースの削除 803
テキスト リソースのインポート 803
テキスト リソースのエクスポート 804
HTML ベースのテキスト リソースの概要 804
HTML ベースのテキスト リソースのインポートおよびエクスポート 805
テキスト リソースの使用 805
免責事項テンプレート 806
リスナーからの免責事項テキストの追加 806
フィルタからの免責事項の追加 807
免責事項およびフィルタ アクション変数 807
免責事項スタンプと複数エンコード方式 809
通知テンプレート 812
アンチウイルス通知テンプレート 812
カスタム アンチウイルス通知テンプレート 813
バウンス通知および暗号化失敗通知テンプレート 816
バウンス通知および暗号化失敗通知変数 816
暗号化通知テンプレート 817

第 28 章 SMTP サーバを使用した受信者の検証 819
SMTP コールアヘッド受信者検証の概要 819
SMTP コールアヘッド受信者検証のワークフロー 819

外部 SMTP サーバを使用した受信者の検証方法 821
コールアヘッド サーバ プロファイルの設定 821
SMTP コールアヘッド サーバ プロファイルの設定 822
コールアヘッド サーバの応答 825
リスナーでの SMTP サーバ経由の着信メール検証のイネーブル化 826
LDAP ルーティング クエリの構成 826
SMTP コールアヘッド クエリのルーティング 827
特定のユーザまたはグループの SMTP コールアヘッド検証のバイパス 828

第 29 章 **他の MTA との暗号化通信 829**
他の MTA との暗号化通信の概要 829
TLS を使用した SMTP カンバセーションの暗号化方法 830
証明書の使用 830
署名付き証明書の導入 831
自己署名証明書の導入 831
証明書と集中管理 832
中間証明書 832
自己署名証明書の作成 833
認証局への証明書署名要求（CSR）の送信について 834
認証局によって署名された証明書のアップロード 834
証明書のインポート 835
証明書のエクスポート 836
リスナー HAT の TLS の有効化 837
GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て 838
CLIを使用したパブリックまたはプライベートのリスナーへのTLS接続のための証明書の割り当て 838
ログ 838
GUI の例：リスナーの HAT の TLS 設定の変更 839
CLI の例：リスナーの HAT の TLS 設定の変更 839
配信時の TLS および証明書検証の有効化 840

要求された TLS 接続が失敗した場合のアラートの送信 843
TLS 接続アラートの有効化 843
ログ 843
名前付きエンティティの DNS ベースの認証 844
名前付きエンティティの SMTP DNS ベースの認証の概要 844
SMTP DANE ワークフロー 845
TLSA レコードの作成 846
DANE をサポートする配信に向けた TLS の有効化 846
DANE 失敗時のアラートの送信 848
DANE アラートの有効化 848
認証局のリストの管理 848
プレインストールされた認証局リストの参照 849
システム認証局リストの無効化 850
カスタム認証局リストのインポート 850
認証局リストのエクスポート 850
証明書の更新 851
信頼できるルート証明書の管理 851
HTTPS の証明書のイネーブル化 852

第 30 章 ルーティングおよび配信機能の設定 853
ローカル ドメインの電子メールのルーティング 853
SMTP ルートの概要 854
デフォルトの SMTP ルート 855
SMTP ルートの定義 855
SMTP ルートの制限 856
SMTP ルートと DNS 856
SMTP ルートおよびアラート 856
SMTP ルート、メール配信、およびメッセージ分裂 856
SMTP ルートと発信 SMTP 認証 857
GUI を使用した発信電子メール送信の SMTP ルート管理 857
SMTP ルートの追加 857

SMTP ルートのエクスポート 858
SMTP ルートのインポート 858
アドレスの書き換え 859
エイリアス テーブルの作成 860
コマンド ラインによるエイリアス テーブルの設定 861
エイリアス テーブルのエクスポートおよびインポート 862
エイリアス テーブルのエントリの削除 862
エイリアス テーブルの例 862
aliasconfig コマンドの例 864
マスカレードの構成 868
マスカレードと altsrchost 869
スタティック マスカレード テーブルの構成 869
プライベート リスナー用マスカレード テーブルの例 871
マスカレード テーブルのインポート 871
マスカレードの例 871
ドメイン マップ機能 878
ドメイン マップ テーブルのインポートおよびエクスポート 883
バウンスした電子メールの処理 884
配信不可能な電子メールの処理 885
ソフト バウンスおよびハード バウンスに関する注意 886
バウンス プロファイルのパラメータ 886
ハード バウンスと status コマンド 890
カンバセーション バウンスおよび SMTP ルートのメッセージ フィルタ アクション 891
バウンス プロファイルの例 891
配信ステータス通知形式 892
遅延警告メッセージ 892
遅延警告メッセージとハード バウンス 892
新しいバウンス プロファイルの作成 893
デフォルトのバウンス プロファイルの編集 893
minimalist バウンス プロファイルの例 893
リスナーへのバウンス プロファイルの適用 893

宛先制御による電子メール配信の管理 894
レート制限 895
TLS 895
バウンス検証 895
[バウンス プロファイル（Bounce Profile）] 895
メール配信に使用するインターフェイスの決定 896
デフォルトの配信制限 896
送信先コントロールの使用 896
IP アドレス バージョンの管理 897
ドメインに対する接続、メッセージ、受信者の数の管理 897
TLS の管理 899
バウンス検証タギングの管理 899
バウンスの管理 900
新しい送信先コントロール エントリの追加 900
宛先制御設定のインポートおよびエクスポート 900
宛先制御と CLI 904
バウンス検証 904
概要：タギングとバウンス検証 905
着信バウンス メッセージの処理 905
バウンス検証アドレスのタギング キー 906
タグなしのバウンスされたメッセージの合法的受け入れ 906
バウンス検証を使用してバウンス メッセージ ストームを防止 907
バウンス検証アドレスのタグ付けキーの設定 907
バウンス検証設定値の設定 908
CLI を使用したバウンス検証の構成 908
バウンス検証とクラスタ設定 909
電子メール配信パラメータの設定 909
デフォルトの配信 IP インターフェイス 909
配信可能性あり機能 910
デフォルトの最大同時接続数 910
deliveryconfig の例 910

Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメールゲートウェイ 912
概要 913
Virtual Gateway アドレスの設定 913
仮想ゲートウェイで使用する新しい IP インターフェイスの作成 914
メッセージから配信用 IP インターフェイスへのマッピング 916
altsrchost ファイルのインポート 917
altsrchost の制限 918
altsrchost コマンド用に有効なマッピングが記載されたテキスト ファイルの例 918
CLI を使用した altsrchost マッピングの追加 918
Virtual Gateway アドレスのモニタ 921
Virtual Gateway アドレスごとの配信接続の管理 921
グローバル配信停止機能の使用 922
CLI を使用したグローバル配信停止へのアドレスの追加 923
グローバル配信停止ファイルのエクスポートおよびインポート 925
確認：電子メール パイプライン 926

第 31 章 **電子メールゲートウェイと Cisco Advanced Phishing Protection の統合 931**
Cisco Advanced Phishing Protection の概要 931
Cisco Advanced Phishing Protection の利点 932
ワークフロー 932
電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法 933
前提条件 934
Cisco Advanced Phishing Protection クラウドサービスのアカウントの利用 934
Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール 934
Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得 934
電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 935
電子メールゲートウェイでの Advanced Phishing Protection の有効化 936
Cisco Advanced Phishing Protection クラウドサービスからの API アクセスキーの取得 937
メッセージメタデータの転送を有効にするための受信メールポリシーの設定 938

Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング 940
Advanced Phishing Protection およびクラスタ 940
[高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ 940
Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング 941
Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの表示 942

第 32 章 **LDAP クエリ 943**
LDAP クエリの概要 943
LDAP クエリについて 944
LDAP と AsyncOS との連携の仕組み 945
電子メールゲートウェイを LDAP サーバと連携させるための設定 946
LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 947
LDAP サーバのテスト 950
特定のリスナーで実行する LDAP クエリの有効化 950
LDAP クエリのグローバル設定の構成 950
LDAP サーバ プロファイル作成の例 951
パブリック リスナー上の LDAP クエリの有効化 952
プライベート リスナーでの LDAP クエリのイネーブル化 952
Microsoft Exchange 5.5 に対する拡張サポート 953
LDAP クエリに関する作業 955
LDAP クエリのタイプ 955
ベース識別名（DN） 956
LDAP クエリの構文 956
トークン: 956
セキュア LDAP（SSL） 957
ルーティング クエリー 957
LDAP サーバへの匿名のバインドをクライアントに許可する 957
匿名認証のセットアップ 958
Active Directory の匿名バインドのセットアップ 959

Active Directory の実装に関する注意 961
LDAP クエリのテスト 961
LDAP サーバへの接続のトラブルシューティング 963
受信者検証で受け入れクエリを使用する 963
受け入れクエリの例 964
Lotus Notes の場合の受け入れクエリの設定 965
複数ターゲット アドレスへのメール送信にルーティング クエリを使用する 965
ルーティング クエリの例 965
ルーティング：MAILHOST と MAILROUTINGADDRESS 966
エンベロープ送信者を書き換えるためのマスカレード クエリの使用 966
マスカレード クエリの例 967
「フレンドリ名」のマスカレード 967
受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 968
グループ クエリの例 969
グループ クエリの設定 969
例：グループ クエリを使用してスパムとウイルスのチェックをスキップする 971
特定のドメインへルーティングするためのドメイン ベース クエリの使用 972
ドメインベース クエリの作成 973
一連の LDAP クエリを実行するためのチェーン クエリの使用 974
チェーン クエリの作成 975
LDAP によるディレクトリ ハーベスト攻撃防止 976
SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止 976
作業キュー内でのディレクトリ ハーベスト攻撃防止 978
ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定 978
SMTP 認証を行うための AsyncOS の設定 979
SMTP 認証の設定 980
属性としてのパスフレーズの指定 980
SMTP 認証クエリの設定 981
第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth） 982
LDAP を使用する SMTP 認証 983
リスナーでの SMTP 認証の有効化 983

クライアント証明書を使用した SMTP セッションの認証 986
発信 SMTP 認証 987
ロギングと SMTP 認証 987
ユーザの外部 LDAP 認証の設定 988
ユーザー アカウント クエリ 988
グループ メンバーシップ クエリ 989
スパム隔離機能へのエンド ユーザ認証 991
Active Directory エンドユーザ認証の設定例 992
OpenLDAP エンドユーザ認証の設定の例 992
スパム隔離のエイリアス統合クエリ 993
Active Directory エイリアス統合の設定例 993
OpenLDAP エイリアス統合の設定例 994
ユーザ識別名の設定の例 995
AsyncOS を複数の LDAP サーバと連携させるための設定 995
サーバとクエリのテスト 996
フェールオーバー 996
LDAP フェールオーバーのための電子メールゲートウェイの設定 997
ロード バランシング 997
ロードバランシングのための電子メールゲートウェイの設定 998

第 33 章 クライアント証明書を使用した SMTP セッションの認証 999
証明書と SMTP 認証の概要 999
クライアント証明書でのユーザの認証方法 1000
SMTP 認証 LDAP クエリでのユーザの認証方法 1000
クライアント認証が無効な場合の LDAP SMTP 認証クエリでのユーザの認証方法 1001
クライアント証明書の有効性の確認 1001
LDAP ディレクトリを使用したユーザの認証 1002
クライアント証明書を使用した TLS 経由の SMTP 接続の認証 1003
電子メールゲートウェイからの TLS 接続の確立 1003
無効にされた証明書のリストの更新 1004
クライアント証明書を使用したユーザの SMTP セッションの認証 1005

SMTP AUTH コマンドを使用したユーザの SMTP セッションの認証 1006
クライアント証明書または SMTP AUTH を使用したユーザの SMTP セッションの認証 1007

第 34 章 電子メール セキュリティ モニタの使用方法 1009
電子メール セキュリティ モニタの概要 1009
電子メール セキュリティ モニタと集中管理 1010
電子メール セキュリティ モニタ ページ 1011
検索と電子メール セキュリティ モニタ 1013
レポートに含まれるメッセージの詳細の表示 1013
[マイ ダッシュボード（My Dashboard）] ページ 1014
[概要（Overview）] ページ 1015
システム概要 1016
送受信のサマリーとグラフ 1017
電子メールの分類 1018
メッセージの分類方法 1019
[受信メール（Incoming Mail）] ページ 1020
受信メール 1021
[受信メールの詳細（Incoming Mail Details）] リスト 1022
データが読み込まれる報告ページ：送信者プロファイル ページ 1024
送信者グループ レポート 1026
[送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ 1027
送信先 1027
送信者 1028
地理的分散ページ 1028
[送信処理ステータス（Delivery Status）] ページ 1029
配信の再試行 1030
[送信処理ステータス詳細（Delivery Status Details）] ページ 1030
[内部ユーザ（Internal Users）] ページ 1030
内部ユーザの詳細 1031
特定の内部ユーザの検索 1032
[DLP インシデント（DLP Incidents）] ページ 1032

DLP インシデントの詳細（DLP Incidents Details） 1033
[DLP ポリシー詳細（DLP Policy Detail）] ページ 1033
[コンテンツフィルタ（Content Filters）] ページ 1033
コンテンツ フィルタの詳細 1034
[DMARC検証（DMARC Verification）] ページ 1034
[マクロ検出（Macro Detection）] ページ 1034
[外部脅威フィード（External Threat Feeds）] ページ 1035
[アウトブレイク フィルタ（Outbreak Filters）] ページ 1035
[ウイルス タイプ（Virus Types）] ページ 1037
[URL フィルタリング（URL Filtering）] ページ 1038
[Webインタラクショントラッキング（Web Interaction Tracking）] ページ 1039
偽造メールの一致レポート 1040
ファイル レピュテーションおよびファイル分析レポート 1040
[メールボックスの自動修復（Mailbox Auto Remediation）] レポート 1041
[TLS 接続（TLS Connections）] ページ 1041
[受信 SMTP 認証（Inbound SMTP Authentication）] ページ 1042
[レート制限（Rate Limits）] ページ 1043
[システム容量（System Capacity）] ページ 1043
[システム容量（System Capacity）] : [ワークキュー（Workqueue）] 1045
[システム容量（System Capacity）] : [受信メール（Incoming Mail）] 1045
[システム容量（System Capacity）] : [送信メール（Outgoing Mail）] 1046
[システム容量（System Capacity）] : [システムの負荷（System Load）] 1046
メモリ ページ スワッピングに関する注意事項 1047
[システム容量（System Capacity）] : [すべて（All）] 1047
[システムステータス（System Status）] ページ 1047
システム ステータス 1048
ゲージ 1048
レート 1049
カウンタ 1049
[大容量のメール（High Volume Mail）] ページ 1049
[メッセージフィルタ（Message Filters）] ページ 1050

[Safe Print] ページ 1050
CSV データの取得 1050
自動プロセスによる CSV データの取得 1051
新しい Web インターフェイスの電子メール セキュリティ モニタ ページ 1053
検索およびインタラクティブ電子メール レポート ページ 1055
レポートに含まれるメッセージの詳細の表示 1056
レポートの時間範囲 1056
[お気に入りレポート（My Favorite Reports）] ページ 1057
[マイ レポート（My Reports）] ページに追加できないモジュール 1058
[お気に入りレポート（My Favorite Reports）] ページでのレポートの追加 1059
[メール フロー概要（Mail Flow Summary）] ページ 1060
電子メールゲートウェイによる電子メールメッセージの分類方法 1063
送受信のサマリーとグラフ 1063
[メールフロー概要（Mail Flow Summary）] ページでの電子メール メッセージの分類 1064
カウンタを使用しての、トレンド グラフ上のデータのフィルタリング 1066
[システム容量（System Capacity）] ページ 1066
[システム容量（System Capacity）] : [ワークキュー（Workqueue）] 1067
[システム容量（System Capacity）] : [受信メール（Incoming Mail）] 1068
[システム容量（System Capacity）] : [送信メール（Outgoing Mail）] 1068
[システム容量（System Capacity）] : [システムの負荷（System Load）] 1069
メモリ ページ スワッピングに関する注意事項 1070
[システム容量（System Capacity）] : [すべて（All）] 1070
レポート データの有効性 1070
[高度なマルウェア防御（Advanced Malware Protection）] ページ 1070
[高度なマルウェア防御（Advanced Malware Protection）] : [概要（Summary）] 1071
[高度なマルウェア防御（Advanced Malware Protection）] - [AMP レピュテーション（AMP Reputation）] 1072
[高度なマルウェア防御（Advanced Malware Protection）] – [ファイル分析（File Analysis）] 1073
[高度なマルウェア防御（Advanced Malware Protection）] – [ファイル レトロスペクション（File Retrospection）] 1074

[高度なマルウェア防御（Advanced Malware Protection）] - [メールボックスの自動修復（Mailbox Auto Remediation）] 1074
SHA-256 ハッシュによるファイルの識別 1076
その他のレポートでのファイル レピュテーション フィルタ データの表示 1076
[ウイルス フィルタリング（Virus Filtering）] ページ 1076
[マクロ検出（Macro Detection）] ページ 1077
[DMARC検証（DMARC Verification）] ページ 1078
[URL フィルタリング（URL Filtering）] ページ 1078
[アウトブレイク フィルタリング（Outbreak Filtering）] ページ 1079
[偽装メールの検出（Forged Email Detection）] ページ 1081
[送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ 1082
[外部脅威フィード（External Threat Feeds）] ページ 1082
[メール フローの詳細（Mail Flow Details）] ページ 1083
メール フローの詳細ページ内のビュー 1084
[受信メール（Incoming Mails）] テーブル 1086
[送信者プロファイル（Sender Profile）] ページ 1090
[送信者の詳細（Sender Details）] テーブル 1092
送信者グループ レポート 1093
送信先 1093
[TLS暗号化（TLS Encryption）] ページ 1094
[受信 SMTP 認証（Inbound SMTP Authentication）] ページ 1094
[レート制限（Rate Limits）] ページ 1095
[国別の接続（Connections by Country）] ページ 1096
[ユーザー メール サマリー（User Mail Summary）] ページ 1096
[ユーザメールフローの詳細（User Mail Flow Details）] 1098
特定の内部ユーザの検索 1098
[DLP インシデント サマリー（DLP Incident Summary）] ページ 1098
[DLPインシデントの詳細（DLP Incident Details）] 1099
[DLP ポリシー詳細（DLP Policy Detail）] ページ 1099
[Web インタラクション（Web Interaction）] ページ 1100
[修復レポート（Remediation Report）] ページ 1101

[メッセージフィルタ（Message Filters）] ページ 1103
[大容量のメール（High Volume Mail）] ページ 1104
[コンテンツフィルタ（Content Filters）] ページ 1104
コンテンツ フィルタの詳細 1105
[Safe Print] ページ 1105
[高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ 1105
[メールポリシーの詳細（Mail Policy Details）] レポートページ 1106
レポート作成の概要 1106
スケジュール設定されたレポートまたはアーカイブ レポートのタイプ 1107
レポートに関する注意事項 1108
レポート用返信アドレスの設定 1108
レポートの管理 1108
スケジュール設定されたレポート 1108
自動的に生成するレポートのスケジュール 1109
スケジュール設定されたレポートの編集 1110
スケジュール設定されたレポートの削除 1110
アーカイブ レポート 1110
オンデマンド レポートの生成 1111
メール レポートのトラブルシューティング 1112
メッセージ トラッキングへのリンクが予期しない結果になる 1112
クラウド内のファイル分析の詳細が完全でない 1112

第 35 章 メッセージ トラッキング 1113
メッセージ トラッキングの概要 1113
メッセージ トラッキングの有効化 1113
レガシー インターフェイスでのメッセージの検索 1115
新しい Web インターフェイスでの電子メール メッセージの検索 1118
メッセージ トラッキングの検索結果の使用 1121
メッセージ トラッキングの詳細 1122
メッセージ トラッキング データの有効性の検査 1125
メッセージ トラッキングおよびアップグレードについて 1126

メッセージ トラッキングのトラブルシューティング 1126
添付ファイルが検索結果に表示されない 1126
予想されるメッセージが検索結果に表示されない 1126

第 36 章 ポリシー、ウイルス、およびアウトブレイク隔離 1129
ポリシー、ウイルス、およびアウトブレイク隔離の概要 1129
隔離の種類 1131
ポリシー、ウイルス、およびアウトブレイク隔離の管理 1133
ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て 1133
隔離内のメッセージの保持期間 1134
隔離メッセージに自動的に適用されるデフォルト アクション 1135
システム作成の隔離の設定を確認 1135
ポリシー、ウイルス、およびアウトブレイク隔離の設定 1135
ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について 1138
ポリシー隔離を割り当てるフィルタおよびメッセージ アクションの決定 1138
ポリシー隔離の削除について 1138
隔離のステータス、容量、およびアクティビティのモニタリング 1139
ポリシー隔離のパフォーマンス 1141
隔離用のディスク容量の使用率に関するアラート 1141
ポリシー隔離とロギング 1141
メッセージ処理タスクの他のユーザへの割り当てについて 1142
ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定 1142
クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について 1143
ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法 1143
ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作 1143
隔離内のメッセージの表示 1144
隔離されたメッセージおよび国際文字セット 1145
ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの索 1145
隔離内のメッセージの手動処理 1146
メッセージのコピーの送信 1147

ポリシー隔離間のメッセージの移動について 1147
複数の隔離内にあるメッセージ 1147
メッセージの詳細およびメッセージ内容の表示 1148
一致した内容の表示 1149
添付ファイルのダウンロード 1150
ウイルス テスト 1150
隔離されたメッセージの再スキャンについて 1151
アウトブレイク隔離 1151
アウトブレイク隔離のメッセージの再スキャン 1152
[ルール サマリー管理（Manage by Rule Summary）] リンク 1152
シスコへの偽陽性または不審なメッセージの報告 1152

第 37 章 スパム隔離 1153
スパム隔離の概要 1153
ローカルのスパム隔離と外部のスパム隔離 1154
ローカルのスパム隔離の設定 1154
レガシー Web インターフェイスでのスパム隔離の有効化と設定 1155
スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定 1157
スパム隔離への管理ユーザ アクセスの設定 1158
スパムを隔離するためのメール ポリシーの設定 1159
隔離対象のメールの受信者の制限 1159
メッセージ テキストが正しく表示されることの確認 1160
デフォルト エンコーディングの指定 1160
スパム隔離の言語 1161
セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御 1161
セーフリストとブロックリストのメッセージ処理 1161
レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 1162
外部スパム隔離およびセーフリスト/ブロックリスト 1163
セーフリストおよびブロックリストへの送信者とドメインの追加（管理者） 1164
セーフリスト エントリとブロックリスト エントリの構文 1169
すべてのセーフリストおよびブロックリストのクリア 1170

セーフリストおよびブロックリストへのエンドユーザ アクセスについて 1170
セーフリストへのエントリの追加（エンド ユーザー） 1170
ブロックリストへの送信者の追加（エンド ユーザー） 1172
複数の 電子メールゲートウェイ（ Cisco Secure Email and Web Manager を使用しない展開）でのセーフリストまたはブロックリストの同期 1172
セーフリスト/ブロックリストのバックアップと復元 1173
セーフリストとブロックリストのトラブルシューティング 1174
セーフリストに登録されている送信者からのメッセージが配信されない 1174
エンド ユーザのためのスパム管理機能の設定 1174
スパム管理機能にアクセスするエンド ユーザの認証オプション 1175
LDAP 認証プロセス 1176
IMAP/POP 認証プロセス 1177
Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定 1177
スパム隔離へのエンドユーザ アクセスの設定 1178
スパム隔離へのエンドユーザ アクセス用 URL の決定 1179
エンド ユーザに表示されるメッセージ 1180
エンド ユーザへの隔離されたメッセージに関する通知 1180
受信者の電子メールのメーリング リスト エイリアスおよびスパム通知 1183
通知のテスト 1184
スパム通知のトラブルシューティング 1185
スパム隔離内のメッセージの管理 1185
スパム隔離へのアクセス（管理ユーザ） 1186
スパム隔離内でのメッセージの検索 1186
大量メッセージの検索 1187
スパム隔離内のメッセージの表示 1187
スパム隔離内のメッセージの配信 1187
スパム隔離からのメッセージの削除 1188
スパム隔離のディスク領域 1188
外部スパム隔離の無効化について 1188
スパム隔離機能のトラブルシューティング 1189

第 38 章 管理タスクの分散 1191

ユーザー アカウントを使用する作業 1191

ユーザの役割 1192

ユーザの管理 1194

ユーザの追加 1195

ユーザの編集 1196

ユーザにパスフレーズの変更を強制 1196

ユーザの削除 1196

メッセージ トラッキングでの機密情報へのアクセスの制御 1197

委任管理のためのカスタム ユーザー ロールの管理 1198

[アカウント権限（Account Privileges）] ページ 1199

アクセス権限の割り当て 1199

メール ポリシーとコンテンツ フィルタ 1200

DLP ポリシー 1202

電子メール レポーティング 1203

メッセージ トラッキング 1204

トレース 1204

隔離 1204

暗号化プロファイル 1205

ログ サブスクリプション 1205

カスタム ユーザー ロールの定義 1205

ユーザー アカウント追加時のカスタム ユーザー ロールの定義 1205

カスタム ユーザー ロールの責任のアップデート 1206

カスタム ユーザー ロールの編集 1207

カスタム ユーザー ロールの複製 1207

カスタム ユーザー ロールの削除 1207

パスフレーズ 1208

パスフレーズの変更 1208

ユーザー アカウントのロックおよびロック解除 1209

制限的なユーザ アカウントとパスフレーズの設定値の構成 1209

外部認証 1210
LDAP 認証のイネーブル化 1210
RADIUS 認証の有効化 1211
SAML 認証の有効化 1214
二要素認証 1215
二要素認証の有効化 1215
二要素認証の無効化 1216
電子メールゲートウェイへのアクセスの設定 1216
IP ベースのネットワーク アクセスの設定 1217
直接接続 1217
プロキシ経由の接続 1217
ネットワーク アクセスを制限する際の重要な注意事項 1217
アクセス リストの作成 1218
セッション タイムアウトの設定 1219
Web UI セッション タイムアウトの設定 1220
CLI セッション タイムアウトの設定 1220
管理ユーザへのメッセージの表示 1221
ログイン前のメッセージの表示 1221
ログイン後のメッセージの表示 1221
セキュア シェル（SSH）キーの管理 1222
例：新しい公開キーのインストール 1222
例：SSH サーバ設定の編集 1223
リモート SSH コマンド実行 1224
管理ユーザー アクセスのモニタリング 1224

第 39 章 システム管理 1227
電子メールゲートウェイの管理 1228
電子メールゲートウェイのシャットダウンおよび再起動 1228
電子メールの受信と配信の一時停止 1228
一時停止している電子メールの受信と配信の再開 1229
出荷時の初期状態へのリセット 1230

次のステップ 1230
AsyncOS のバージョン情報の表示 1231
電子メールゲートウェイのライセンス 1231
ライセンス キー 1231
ライセンス キーの追加および管理 1231
ライセンス キーのダウンロードとアクティベーションの自動化 1232
期限切れ機能キー 1233
スマート ソフトウェア ライセンシング 1233
概要 1233
スマート ソフトウェア ライセンシングのイネーブル化 1235
Cisco Smart Software Manager での電子メールゲートウェイの登録 1236
ライセンスの要求 1238
Cisco Smart Software Manager からの電子メールゲートウェイの登録解除 1238
Cisco Smart Software Manager での電子メールゲートウェイの再登録 1239
転送設定の変更 1239
認証と証明書の更新 1239
アラート 1240
スマート エージェントの更新 1240
クラスタ モードでのスマート ライセンス 1241
仮想電子メールゲートウェイのライセンス 1242
仮想電子メールゲートウェイのライセンスの有効期限 1242
設定ファイルの管理 1243
XML 設定ファイルを使用した複数の電子メールゲートウェイの管理 1243
コンフィギュレーション ファイルの管理 1244
現在の設定ファイルの保存およびエクスポート 1244
設定ファイルのメール送信 1245
コンフィギュレーション ファイルのロード 1245
現在の設定のリセット 1248
設定ファイルの表示 1248
[設定ファイル（Configuration File）] ページ 1249
ディスク領域の管理 1249

（仮想 E メール ゲートウェイのみ）使用可能なディスク領域の増加 1249
ディスク領域の使用率の表示および割り当て 1250
その他のクォータのディスク領域の管理 1250
ディスク領域に関するアラートの受信の確認 1251
ディスク領域と集中管理 1251
セキュリティ サービスの管理 1251
エンジンの手動アップデート 1252
エンジンの以前のバージョンへのロールバック 1253
ログの表示 1253
サービス アップデート 1253
アップグレードおよびアップデートを取得するための設定 1254
アップグレードおよびアップデートの配信オプション 1254
Cisco サーバからアップグレードおよびアップデートをダウンロードするためのネットワークの設定 1255
厳密なファイアウォール環境でのアップグレードとアップデートのための 電子メールゲートウェイの設定 1255
ローカル サーバからのアップグレードおよびアップデート 1256
ローカル サーバからアップグレードおよびアップデートするためのハードウェアおよびソフトウェア要件 1257
ローカル サーバでのアップグレード イメージのホスト 1258
プロキシ サーバを経由したアップデート 1259
アップグレードおよびアップデートをダウンロードするためのサーバ設定 1259
自動アップデートの設定 1262
アップデータサーバ証明書の有効性を検証するための 電子メールゲートウェイの設定 1262
プロキシサーバとの通信を信頼するためのアプライアンスの設定 1263
AsyncOS のアップグレード 1264
クラスタ化されたシステムのアップグレードについて 1264
アップグレード手順用のバッチ コマンドについて 1264
使用可能なアップグレードの通知 1264
使用可能なアップグレードの通知 1265
AsyncOS のアップグレードの準備 1266
アップグレードのダウンロードとインストール 1266

バックグラウンド ダウンロードのキャンセルまたは削除ステータスの表示 1269
リモート電源再投入の有効化 1269
AsyncOS の以前のバージョンへの復元 1271
復元の影響 1271
仮想電子メールゲートウェイでの AsyncOS の復元がライセンスに影響を及ぼす可能性 1271
AsyncOS の復元 1271
電子メールゲートウェイに生成されるメッセージの返信アドレスの設定 1272
システム状態パラメータのしきい値の設定 1273
電子メールゲートウェイの状況の確認 1274
アラート 1275
アラートの重大度 1275
AutoSupport 1275
アラートの配信 1276
アラート メッセージの例 1277
アラート受信者の追加 1277
アラート設定値の設定 1278
アラート設定 1278
最新アラートの表示 1279
アラートの説明 1279
アンチスパム アラート 1280
アンチウイルス アラート 1280
ディレクトリ獲得攻撃（DHAP）アラート 1281
ハードウェア アラート 1282
スパム隔離アラート 1283
セーフリスト/ブロックリスト アラート 1284
システム アラート 1285
アップデータ アラート 1298
アウトブレイク フィルタ アラート 1299
クラスタリング アラート 1300
ネットワーク設定値の変更 1303

システム ホスト名の変更 1303
ドメイン ネーム システム（DNS）設定値の構成 1303
DNS サーバの指定 1304
複数エントリとプライオリティ 1304
インターネット ルート サーバの使用 1305
逆引き DNS ルックアップのタイムアウト 1305
DNS アラート 1306
DNS キャッシュのクリア 1306
グラフィカル ユーザー インターフェイスを使用した DNS 設定値の設定 1306
TCP/IP トラフィック ルートの設定 1307
デフォルト ゲートウェイの設定 1307
SSL 設定の指定 1307
SAML 2.0 を使用したシングル サインオン（SSO） 1309
シングル サインオン（SSO）と SAML 2.0 について 1309
SAML 2.0 SSO のワークフロー 1309
SAML 2.0 に関する注意事項と制約事項 1310
一般 1310
ログアウト 1311
制限事項 1311
電子メールゲートウェイでの SSO の設定方法 1311
前提条件 1311
電子メールゲートウェイをサービスプロバイダーとして設定する 1312
電子メールゲートウェイと通信するように ID プロバイダーを設定する 1315
電子メールゲートウェイでの ID プロバイダーの設定 1319
AsyncOS API 向けの電子メールゲートウェイでの OpenID Connect 1.0 の設定 1320
概要 1320
ワークフロー 1320
サンプルアクセストークン 1321
前提条件 1321
電子メールゲートウェイでの OpenID Connect の設定 1321
システム タイム 1323

タイム ゾーンの選択 1323
GMT オフセットの選択 1324
時刻設定の編集 1324
（推奨）Network Time Protocol（NTP）を使用した電子メールゲートウェイのシステム時刻の設定 1324
電子メールゲートウェイのシステム時刻の手動設定 1325
ビューのカスタマイズ 1325
お気に入りページの使用 1325
ユーザ設定値の設定 1326
全般設定 1327
Internet Explorer の互換モードの上書き 1327
新しい Web インターフェイスを使用した電子メールゲートウェイの使用状況統計の収集 1328
最大 HTTP ヘッダー サイズの構成 1328
サービス エンジンの再起動とステータスの表示 1328
国際化ドメイン名（IDN）を含むメッセージの受信と配信 1329
前提条件 1329
電子メールゲートウェイで IDN ドメインを使用して設定可能な機能 1330

第 40 章 CLI による管理およびモニタリング 1333
CLI を使用した管理およびモニタリングの概要 1333
使用可能なモニタリング コンポーネントの読み取り 1334
イベント カウンタの読み取り 1334
システム ゲージの読み取り 1336
配信およびバウンスされたメッセージのレートの読み取り 1339
CLI を使用したモニタリング 1340
電子メール ステータスのモニタリング 1340
例 1341
詳細な電子メール ステータスのモニタリング 1341
例 1342
メール ホストのステータスのモニタリング 1343

仮想ゲートウェイ 1344
例 1345
電子メール キューの構成の確認 1346
例 1346
リアルタイム アクティビティの表示 1346
例 1347
例 1348
着信電子メール接続のモニタリング 1348
例 1349
DNS ステータスの確認 1349
例 1350
電子メール モニタリング カウンタのリセット 1350
例 1351
アクティブな TCP/IP サービスの識別 1351
電子メール キューの管理 1351
キュー内の受信者の削除 1351
例 1352
キュー内の受信者のバウンス 1352
例 1353
キュー内のメッセージのリダイレクト 1354
例 1354
キュー内の受信者に基づいたメッセージの表示 1354
例 1354
電子メール配信の一時停止 1355
例 1355
電子メール配信の再開 1355
構文 1356
電子メールの受信の一時停止 1356
構文 1356
電子メールの受信の再開 1356
構文 1356

電子メールの配信と受信の再開 1357
構文 1357
電子メールの即時配信スケジュール 1357
構文 1357
ワーク キューの休止 1358
古いメッセージの検索およびアーカイブ 1359
構文 1359
構文 1359
システム内のメッセージのトラッキング 1360
SNMP を使用したシステムの状態のモニタリング 1361
MIB ファイル 1362
ハードウェア オブジェクト 1362
ハードウェア トラップ 1363
SNMP トラップ 1363
例：snmpconfig コマンド 1364

第 41 章 サービスログを使用したフィッシング検知機能の有効性の向上 1367
概要 1367
電子メールゲートウェイでのサービスログの有効化 1368
電子メールゲートウェイでのサービスログの無効化 1368
FAQ 1368
どのようなデータを共有するのですか。 1368
シスコは、共有されたデータがセキュアであることをどのように確認していますか。 1370
データを共有することで Cisco 電子メールゲートウェイのパフォーマンスに影響はありますか。 1370
その他の方法でデータを共有できますか。 1370

第 42 章 GUI での他のタスク 1371
グラフィカル ユーザー インターフェイス（GUI） 1371
インターフェイスでの GUI のイネーブル化 1371
GUI のシステム情報 1372

GUI からの XML ステータスの収集 1373

第 43 章 高度なネットワーク構成 1375

イーサネット インターフェイスのメディア設定 1375

etherconfig を使ったイーサネット インターフェイスのメディア設定の編集 1375

メディア設定の編集例 1376

ネットワーク インターフェイス カードのペアリングおよびチーミング 1377

NIC ペアリングと VLAN 1377

NIC ペアの名前 1377

NIC ペアリングと既存のリスナー 1378

etherconfig コマンドを使った NIC ペアリングのイネーブル化 1378

仮想ローカル エリア ネットワーク（VLAN） 1379

VLAN の設定について 1380

VLAN の管理 1380

etherconfig コマンドによる新しい VLAN の作成 1380

interfaceconfig コマンドによる VLAN の IP インターフェイスの作成 1382

Web インターフェイスを使用した VLAN の設定 1384

Direct Server Return 1384

Direct Server Return のイネーブル化 1384

etherconfig コマンドによるループバック インターフェイスのイネーブル化 1385

interfaceconfig コマンドによるループバック上の IP インターフェイスの作成 1386

新しい IP インターフェイス上のリスナーの作成 1387

イーサネット インターフェイスの最大伝送単位 1388

マルチキャスト アドレスでの ARP 応答の受け入れまたは拒否 1389

第 44 章 ログ 1391

概要 1391

ログ ファイルおよびログ サブスクリプションについて 1391

ログ タイプ 1391

ログ タイプの特徴 1397

ログ取得方法 1402

ログ ファイル名とディレクトリ構造 1405
ログのロールオーバーおよび転送スケジュール 1405
デフォルトで有効になるログ 1405
ログ タイプ 1405
ログ ファイル内のタイムスタンプ 1406
テキスト メール ログの使用 1407
テキスト メール ログの解釈 1407
テキスト メール ログ エントリの例 1409
送信者の発信国に基づいて受信したメッセージ 1416
メッセージ添付ファイル内の最大 URL 数が URL スキャン制限を超えている 1416
メッセージ本文内の最大 URL 数が URL スキャン制限を超えている 1416
Cisco プロキシ サーバにリダイレクトされる悪意のある短縮 URL 1416
メッセージ内の短縮 URL を展開できない 1416
メッセージ添付ファイルでの悪意のある URL のログ エントリ 1417
抽出エラーが原因でスキャン不可とマークされたメッセージ 1417
RFC 違反が原因でスキャン不可とマークされたメッセージ 1417
生成またはリライトされたメッセージに対するログ エントリ 1418
スパム隔離エリアに送信されたメッセージ 1418
外部脅威フィードのメール ログの例 1419
SDR フィルタリングのログ エントリの例 1419
有効期限が切れた Cisco Advanced Phishing Protection クラウドサービス 1421
Cisco Advanced Phishing Protection クラウドサービスの有効期限に関するリマインダ 1421
API アクセス UID と API アクセス秘密鍵がない 1421
無効な API アカウント UID または API アクセス秘密鍵 1421
配信ログの使用 1421
配信ログ エントリの例 1423
バウンス ログの使用 1424
バウンス ログ エントリの例 1425
ステータス ログの使用 1425
ステータス ログの読み取り 1426
ドメイン デバッグ ログの使用 1429

ドメイン デバッグ ログの例 1429
インジェクション デバッグ ログの使用 1429
インジェクション デバッグ ログの例 1430
システム ログの使用 1431
システム ログの例 1431
CLI 監査ログの使用 1431
CLI 監査ログの例 1432
FTP サーバ ログの使用 1432
FTP サーバ ログの例 1432
HTTP ログの使用 1433
HTTP ログの例 1433
NTP ログの使用 1434
NTP ログの例 1434
スキャン ログの使用 1434
スキャン ログの例 1434
アンチスパム ログの使用 1435
アンチスパム ログの例 1435
グレイメール ログの使用 1435
グレイメール ログの例 1436
アンチウイルス ログの使用 1436
アンチウイルス ログの例 1436
AMP エンジン ログの使用 1436
AMP エンジン ログ エントリの例 1437
スパム隔離ログの使用 1442
スパム隔離ログの例 1442
スパム隔離 GUI ログの使用 1443
スパム隔離 GUI ログの例 1443
LDAP デバッグ ログの使用 1443
LDAP デバッグ ログの例 1444
セーフリスト/ブロックリスト ログの使用 1445
セーフリスト/ブロックリスト ログの例 1446

レポーティング ログの使用 1446
レポーティング ログの例 1446
レポーティング クエリー ログの使用 1447
レポーティング クエリー ログの例 1447
アップデータ ログの使用 1448
アップデータ ログの例 1448
アップデータ ログの例 1449
トラッキング ログについて 1449
認証ログの使用 1450
認証ログの例 1450
正しくないパスコードが原因の二要素認証ログイン失敗の例 1450
タイムアウトが原因の二要素認証ログイン失敗の例 1451
二要素認証のログインの成功例 1451
コンフィギュレーション履歴ログの使用 1451
コンフィギュレーション履歴ログの例 1451
外部脅威フィードのエンジン ログの使用 1452
外部脅威フィードのエンジン ログの例 1452
統合イベント ログの使用 1453
CSN ログの使用 1461
Advanced Phishing Protection ログの使用 1461
監査ログの使用 1462
CSA ログの使用 1464
ログ サブスクリプション 1466
ログ サブスクリプションの設定 1467
ログ レベル 1468
GUI でのログ サブスクリプションの作成 1469
ログ サブスクリプションの編集 1469
ロギングのグローバル設定 1469
メッセージ ヘッダーのロギング 1471
GUI を使用したロギングのグローバル設定の構成 1471
ログ サブスクリプションのロールオーバー 1472

ファイル サイズによるロールオーバー 1472
時刻によりロールオーバー 1473
オンデマンドでのログ サブスクリプションのロールオーバー 1474
GUI での最近のログ エントリの表示 1475
CLI での最近のログ エントリの表示（tail コマンド） 1475
例 1475
ホスト キーの設定 1476

第 45 章 クラスタを使用した中央集中型管理 1481
クラスタを使用した中央集中型管理の概要 1481
クラスタの要件 1482
クラスタの構成 1483
初期設定 1484
クラスタの作成とクラスタへの参加 1484
clusterconfig コマンド 1485
既存のクラスタへの参加 1486
SSH を使った既存クラスタへの参加 1486
CCS を使った既存クラスタへの参加 1488
事前共有キーによる SSH を使った既存クラスタへの参加 1490
グループの追加 1491
クラスタの管理 1492
CLI でのクラスタの管理 1492
設定のコピーと移動 1492
新しい設定の実験 1493
クラスタからの脱退（削除） 1494
クラスタ内のマシンのアップグレード 1494
CLI コマンドのサポート 1495
すべてのコマンドがクラスタに対応 1495
commit および clearchanges コマンド 1495
新たに追加された操作 1496
制限コマンド 1496

GUI でのクラスタの管理 1498
クラスタ通信 1500
DNS とホスト名の解決 1501
クラスタリング、完全修飾ドメイン名、およびアップグレード 1501
クラスタ通信のセキュリティ 1501
クラスタの整合性 1502
切断/再接続 1502
互いに依存する設定 1504
クラスタ化された電子メールゲートウェイの設定のロード 1505
ベスト プラクティスとよく寄せられる質問（FAQ） 1507
ベストプラクティス 1507
コピーと移動の違い 1508
適切な CM の設計方法 1508
クラスタのセットアップでスパム隔離またはポリシー隔離へアクセスするためのベスト プラクティス 1509
手順：サンプル クラスタの設定 1509
GUI でクラスタのデフォルト以外の CM 設定を使用する場合のオプションの要約 1511
セットアップと設定に関する質問 1512
一般的な質問 1512
ネットワークに関する質問 1513
計画と設定 1514

第 46 章 テストとトラブルシューティング 1515
テスト メッセージを使用したメール フローのデバッグ：トレース 1515
電子メールゲートウェイのテストにリスナーを使用 1523
例 1524
ネットワークのトラブルシューティング 1527
電子メールゲートウェイのネットワーク接続テスト 1527
トラブルシューティング 1528
リスナーのトラブルシューティング 1532
アプライアンスからの電子メール配信のトラブルシューティング 1534

パフォーマンスのトラブルシューティング 1536
Web インターフェイスの外観およびレンダリングの問題 1538
アラートへの応答 1538
その他のディスク使用量がクォータに近づいているというアラートのトラブルシューティング 1538
ハードウェア問題のトラブルシューティング 1538
電子メールゲートウェイの電源のリモートリセット 1538
テクニカル サポートの使用 1539
仮想電子メールゲートウェイのテクニカルサポート 1540
電子メールゲートウェイからのサポートケースのオープンおよび更新 1540
シスコのテクニカル サポート担当者のリモート アクセスの有効化 1541
インターネット接続された電子メールゲートウェイへのリモートアクセスの有効化 1541
インターネットに直接接続されていない電子メールゲートウェイへのリモートアクセスの有効化 1542
テクニカル サポートのトンネルの無効化 1543
リモート アクセスの無効化 1543
サポートの接続状態の確認 1543
パケット キャプチャの実行 1543

第 47 章 **D-Mode を使用した発信メール配信電子メールゲートウェイの最適化 1547**
機能の概要：最適化された発信配信の D-Mode 1547
D-Mode 対応電子メールゲートウェイ固有の機能 1547
D-Mode 対応電子メールゲートウェイでディセーブルになっている標準機能 1548
D-Mode 対応電子メールゲートウェイに適用される標準機能 1548
最適化された発信メール配信の電子メールゲートウェイの設定 1549
リソースを節約するバウンス設定の構成 1550
リソースを節約するバウンス設定をイネーブルにする例 1550
IronPort Mail Merge（IPMM）を使用した大量のメールの送信 1551
IronPort Mail Merge の概要 1551
Mail Merge 機能の利点 1551
Mail Merge の使用 1552

SMTP インジェクション 1552
変数置換 1552
予約変数 1552
メッセージの例 1 1553
パーツ アセンブリ 1553
メッセージの例 2（パート 1） 1554
メッセージの例 2（パート 2） 1554
IPMM および DomainKeys 署名 1554
コマンドの説明 1554
XMRG FROM 1554
XDFN 1555
XPRT 1555
変数定義に関する注意事項 1555
IPMM カンバセーションの例 1556
コード例 1558

第 48 章 **Cisco Secure Email and Web Manager（M シリーズ）の集中型サービス 1559**
Cisco Secure Email and Web Manager サービスの概要 1559
ネットワーク プランニング 1560
外部スパム隔離の操作 1560
メールフローおよび外部スパム隔離 1561
ローカルのスパム隔離から外部の隔離への移行 1561
外部スパム隔離と外部セーフリスト/ブロックリストの有効化 1562
ローカルのスパム隔離を無効化して外部隔離をアクティブ化する 1563
外部のスパム隔離のトラブルシューティング 1564
一元化されたポリシー、ウイルス、アウトブレイク隔離について 1564
集約されたポリシー、ウイルス、およびアウトブレイク隔離 1564
一元化されたポリシー、ウイルス、アウトブレイク隔離の制限事項 1565
クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件 1565
ポリシー、ウイルス、アウトブレイク隔離の移行について 1565
ポリシー、ウイルス、およびアウトブレイク隔離の集約 1566

一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について 1568
中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化 1569
一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング 1569
中央集中型レポーティングの設定 1570
高度なマルウェア防御レポートの要件 1570
中央集中型レポーティングに変更後のレポート情報の可用性 1570
中央集中型レポーティングのディセーブル化について 1571
中央集中型メッセージ トラッキングの設定 1571
中央集中型サービスの使用 1572

付録 A： FTP、SSH、および SCP アクセス 1573
IP インターフェイス 1573
AsynOS によるデフォルト IP インターフェイスの選択方法 1574
電子メールゲートウェイへの FTP アクセスの設定 1574
セキュア コピー（scp）アクセス 1576
シリアル接続経由での 電子メールゲートウェイへのアクセス 1577
80 および 90 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細 1578
70 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細 1578

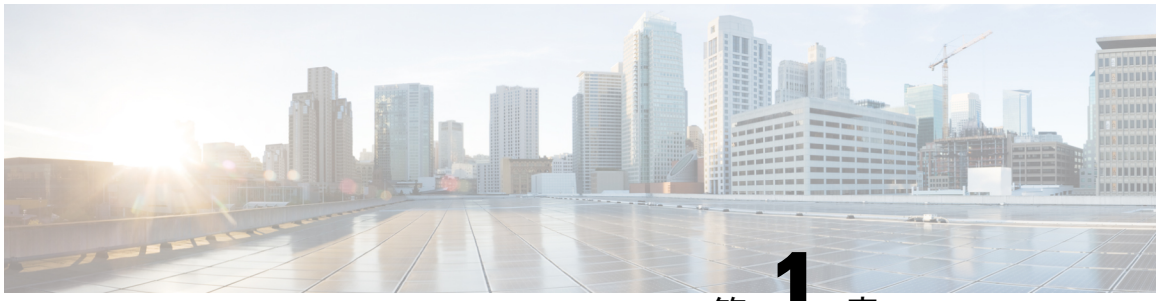
付録 B： ネットワークと IP アドレスの割り当て 1581
イーサネット インターフェイス 1581
IP アドレスとネットマスクの選択 1581
インターフェイス設定のサンプル 1582
IP アドレス、インターフェイス、およびルーティング 1583
要約 1583
電子メールゲートウェイを接続するための戦略 1584

付録 C： メール ポリシーとコンテンツ フィルタの例 1585
受信メール ポリシーの概要 1585
メール ポリシーへのアクセス 1586
[有効（Enabled）]、[無効（Disabled）]、[利用不可（Not Available）] 1587
着信メッセージのデフォルトのアンチスパム ポリシーの設定 1587

送信者および受信者のグループのメール ポリシーの作成 1589
[デフォルト（Default）]、[カスタム（Custom）]、[無効（Disabled）] 1592
送信者および受信者のグループごとのメール ポリシーの作成 1593
送信者および受信者のグループごとのメール ポリシーの作成 1594
メール ポリシーでの送信者または受信者の検索 1596
管理例外 1597
コンテンツに基づくメッセージのフィルタリング 1598
件名に「Confidential」とあるメッセージの隔離 1598
メッセージから MP3 添付ファイルを除去 1599
元従業員に送られたバウンス メッセージ 1600
各受信者のグループごとのコンテンツ フィルタの適用 1601
デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化 1602
エンジニアリングの受信者への MP3 添付ファイルの許可 1602
GUI でのコンテンツ フィルタの設定に関する注意事項 1603

付録 D： ファイアウォール情報 1607
ファイアウォール情報 1607
ネットワーク攻撃からの電子メールゲートウェイの保護 1613

付録 E： エンド ユーザー ライセンス契約書 1615
Cisco Systems エンド ユーザー ライセンス契約書 1615
Cisco コンテンツ セキュリティ ソフトウェア用エンド ユーザー ライセンス契約補則 1622



第 1 章

Cisco Secure Email Gateway スタートアップガイド

この章は、次の項で構成されています。

- AsyncOS 14.0.3 の新機能 （2 ページ）
- Web インターフェイスの比較、新しい Web インターフェイスとレガシー Web インターフェイス （2 ページ）
- 詳細情報の入手先 （6 ページ）
- Cisco Secure Email Gateway の概要 （10 ページ）

AsyncOS 14.0.3 の新機能

表 *1 : AsyncOS 14.0.3* の新機能

機能	説明
パスワードで保護された添付ファイルを開くためのユーザー定義のパスフレーズのみを使用	このリリース以降、メールゲートウェイで作成されたユーザー定義のパスフレーズのみを使用して、受信および送信メッセージでパスワードで保護された添付ファイルを開くことを選択できます。 この機能は、次のいずれかの方法で設定できます。 • Web インターフェイスの [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] > [グローバル設定の編集（Edit Global Settings）] ページで、[ユーザー定義のパスワードのみを適用（Apply User-defined Passwords Only）] チェックボックスを使用します。 • 「ユーザー定義のパスワードのみを適用しますか? y/n」ステートメントは、CLI の `scanconfig` > `protectedattachmentconfig` サブコマンドの下にあります。 詳細については、スキャン動作の設定 （297 ページ） を参照してください。

Web インターフェイスの比較、新しい Web インターフェイスとレガシー Web インターフェイス

次の表は、新しい Web インターフェイスの以前のバージョンとの比較を示しています。

表 *2 :* 新しい *Web* インターフェイスとレガシー *Web* インターフェイスとの比較

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディングページ	電子メールゲートウェイにログインすると、[メールフロー概要（Mail Flow Summary）] ページが表示されます。	電子メールゲートウェイにログインすると、[マイダッシュボード（My Dashboard）] ページが表示されます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
レポートドロップダウン	[レポート（Reports）] ドロップダウンで、電子メールゲートウェイのレポートを表示できます。	[モニタ（Monitor）] メニューで、電子メールゲートウェイのレポートを表示できます。
[マイ レポート（My Reports）] ページ	[レポート（Reports）] ドロップダウンから [マイ レポート（My Reports）] を選択します。	[マイ レポート（My Reports）] ページは、[モニタ（Monitor）] > [マイダッシュボード（My Dashboard）] から表示できます。
[メール フロー概要（Mail Flow Summary）] ページ	[メールフロー概要（Mail Flow Summary）] ページには、着信および送信メッセージに関するトレンド グラフやサマリー テーブルが表示されます。	[受信メール（Incoming Mail）] には、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。
高度なマルウェア防御レポートページ	[レポート（Reports）] メニューの [高度なマルウェア防御（Advanced Malware Protection）] レポートページでは、次のセクションを使用できます。 • [概要（Overview）] • [AMP ファイル レピュテーション（AMP File Reputation）] • [ファイル分析（File Analysis）] • [ファイル レトロスペクション（File Retrospection）] • [メールボックスの自動修復（Mailbox Auto Remediation）]	電子メールゲートウェイの [モニタ（Monitor）] メニューには、次の [高度なマルウェア防御（Advanced Malware Protection）] レポートページがあります。 • [高度なマルウェア防御（Advanced Malware Protection）] • [AMP ファイル分析（AMP File Analysis）] • [AMP判定のアップデート（AMP Verdict Updates）] • [メールボックスの自動修復（Mailbox Auto Remediation）]

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
アウトブレイク フィルタ ページ	新しい Web インターフェイスの[アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページでは、[過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去1年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] は使用できません。	[モニタ（Monitor）] > [アウトブレイクフィルタ（Outbreak Filters）] ページには、[過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および[過去1年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] が表示されます。
スパム隔離（管理ユーザーおよびエンド ユーザー）	新しい Web インターフェイスで **[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）]** をクリックします。 エンドユーザは、次の URL を使用してスパム隔離にアクセスできます。 `https://example.com:<https-api-port>/euq-login` `example.com` はアプライアンス ホスト名で、`<https-api-port>` はファイアウォールで開いている AsyncOS API HTTPS ポートです。	スパム隔離は、[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] から表示できます。
ポリシー、ウイルスおよびアウトブレイク隔離	新しい Web インターフェイスで **[隔離（Quarantine）] > [その他の隔離（Other Quarantine）]** をクリックします。 新しい Web インターフェイスでは、[ポリシー、ウイルス、およびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] のみを表示できます。	電子メールゲートウェイでは、[モニタ（Monitor）] > [ポリシー、ウイルス、およびアウトブレイク隔離（Policy, Virus and Outbreak Quarantines）] を使用して、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
隔離内のメッセージに対するすべてのアクションの選択	複数（またはすべて）のメッセージを選択し、削除、遅延、リリース、移動などのメッセージ アクションを実行できます。	複数のメッセージを選択して、メッセージ アクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-
拒否された接続	拒否された接続を検索するには、 で、[トラッキング（Tracking）] > [検索（Search）]> [拒否された接続（Rejected Connection）] タブをクリックします。	-
クエリ設定	では、メッセージトラッキング機能の [クエリ設定（Query Settings）] フィールドは使用できません。	メッセージ トラッキング機能の [クエリ設定（Query Settings）] フィールドで、クエリのタイムアウトを設定できます。
有効なメッセージ トラッキング データ	[有効なメッセージトラッキングデータ（Message Tracking Data Availability）] ページにアクセスするには、Web インターフェイスのページの右上にある歯車アイコンをクリックします。	電子メールゲートウェイの欠落データインターバルを表示することができます。
メッセージの追加詳細の表示	[判定チャート（Verdict Charts）]、[最後の状態（Last State）]、[送信者グループ（Sender Groups）]、[送信者IP（Sender IP）]、[IPレピュテーションスコア（IP Reputation Score）]、[ポリシー一致（Policy Match）] の詳細など、メッセージの追加詳細を表示できます。	-

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
判定チャートと最後の状態の判定	判定チャートに、電子メールゲートウェイ内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。 メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。
メッセージの詳細におけるメッセージ添付ファイルとホスト名	電子メールゲートウェイでは、メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、IP レピュテーションスコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、IP レピュテーションスコア、およびポリシー一致の詳細は、電子メールゲートウェイの [メッセージの詳細（Message Details）] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、IP レピュテーショスコア、およびポリシー一致は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。
メッセージの方向（受信または送信）	メッセージの方向（受信または送信）は、電子メールゲートウェイのメッセージトラッキング結果ページに表示されます。	メッセージの方向（受信または送信）は、メッセージ トラッキング結果ページには表示されません。

詳細情報の入手先

シスコでは、電子メールゲートウェイに関する理解を深めて頂くために次の資料を提供しています。

- 資料 （7 ページ）
- トレーニング （7 ページ）
- Cisco 通知サービス （8 ページ）
- ナレッジ ベース （8 ページ）

- シスコサポートコミュニティ （8 ページ）
- シスコカスタマーサポート （9 ページ）
- サード パーティ コントリビュータ （9 ページ）
- マニュアルに関するフィードバック （9 ページ）
- シスコ アカウントの登録 （9 ページ）

資料

アプライアンスの GUI で右上の [ヘルプとサポート（Help and Support）] をクリックすることにより、ユーザー ガイドのオンライン ヘルプ バージョンに直接アクセスできます。

Cisco Secure Email Gateway のマニュアルセットには次のマニュアルが含まれます。

- リリース ノート
- ご使用の Cisco Email Security Appliances モデルのクイック スタート ガイド
- ご使用のモデルまたはシリーズのハードウェア インストール ガイドまたはハードウェア インストールおよびメンテナンス ガイド
- 『*Cisco Content Security Virtual Appliance Installation Guide*』
- 『 *Cisco Secure Email Gateway* 向け *AsyncOS* ユーザーガイド』（本書）
- 『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway* 』
- 『AsyncOS API for Cisco Secure Email Gateway - Getting Started Guide』

Cisco Content Security 製品のすべてに関する資料が以下で入手できます。

Cisco コンテンツ セキュリティ製品のマニュアル	**参照先**
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco E メール セキュリティ	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/series.html
Cisco Web セキュリティ	https://www.cisco.com/c/ja_jp/support/security/web-security-appliance/series.html
Cisco コンテンツ セキュリティ管理	https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/series.html
Cisco コンテンツ セキュリティ アプライアンスの CLI リファレンス ガイド	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 暗号化	https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html

トレーニング

シスコでは、技術者、パートナー、学生など、それぞれのニーズに合わせた、さまざまなトレーニングプログラムおよびトレーニングコースを用意しています。

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

Cisco 通知サービス

セキュリティ アドバイザリ、フィールド ノーティス、販売終了とサポート終了の通知、およびソフトウェアアップデートと既知の問題に関する情報などのCiscoコンテンツセキュリティアプライアンスに関連する通知が配信されるように署名して参加します。

受信する情報通知の頻度やタイプなどのオプションを指定できます。使用する製品ごとの通知に個別に参加する必要があります。

参加するには、http://www.cisco.com/cisco/support/notifications.html に移動します。

Cisco.com アカウントが必要です。ない場合は、シスコ アカウントの登録 （9 ページ）を参照してください。

ナレッジ ベース

手順

ステップ 1 製品のメイン ページ（http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html）にアクセスします。

ステップ 2 名前に **TechNotes** が付くリンクを探します。

シスコサポートコミュニティ

シスコ サポート コミュニティは、シスコのお客様、パートナー、および従業員のオンラインフォーラムです。電子メールおよびWebセキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコ ユーザと情報を共有したりできます。

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

- 電子メール セキュリティと関連管理:

  https://supportforums.cisco.com/community/5756/email-security

- Web セキュリティと関連管理：

  https://supportforums.cisco.com/community/5786/web-security

シスコカスタマーサポート

シスコ TAC：http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/c/en/us/services/acquisitions/ironport.html

重大ではない問題の場合は、電子メールゲートウェイからカスタマーサポートにアクセスすることもできます。手順については、ユーザー ガイドまたはオンライン ヘルプを参照してください。

サードパーティ コントリビュータ

次のページにある、ご使用のリリースのオープン ソース ライセンス情報を参照してください。
http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html

Cisco AsyncOS 内に付属の一部のソフトウェアは、FreeBSD、Stichting Mathematisch Centrum、Corporation for National Research Initiatives などのサードパーティ コントリビュータのソフトウェア使用許諾契約の条項、通知、条件の下に配布されています。これらすべての契約条件は、Cisco ライセンス契約に含まれています。

これらの契約内容の全文は次の URL を参照してください。

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

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

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

マニュアルに関するフィードバック

シスコのテクニカル マニュアル チームは、製品ドキュメントの向上に努めています。コメントおよびご提案をお待ちしています。ぜひ以下の電子メールまでお知らせください。

contentsecuritydocs@cisco.com

メッセージの件名には、製品名、リリース番号、このマニュアルの発行日をご記入ください。

シスコ アカウントの登録

Cisco.com の多数のリソースへアクセスするには、シスコのアカウントが必要です。

Cisco.com のユーザ ID をお持ちでない場合は次のリンク先で登録できます。
https://idreg.cloudapps.cisco.com/idreg/register.do

関連項目

- Cisco 通知サービス　（8 ページ）

• ナレッジ ベース （8 ページ）

Cisco Secure Email Gateway の概要

AsyncOS™ オペレーティング システムには、次の機能が組み込まれています。

- SenderBase レピュテーション フィルタと Cisco Anti-Spam を統合した独自のマルチレイヤアプローチによるゲートウェイでの**スパム対策**。
- SophosおよびMcAfeeウイルス対策スキャンエンジンによるゲートウェイでの**ウイルス対策**。
- 新しいアップデートが適用されるまで危険なメッセージを隔離し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対するシスコの独自保護機能である**アウトブレイク フィルタ™**。
- **ポリシー、ウイルス、およびアウトブレイク検疫**は、疑わしいメッセージを保存して管理者が評価するための安全な場所を提供します。
- 隔離されたスパムおよび陽性と疑わしいスパムへのエンドユーザアクセスを提供する、オンボックスまたはオフボックスの**スパム隔離**。
- **電子メール認証**。Cisco AsyncOS は、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- Cisco **電子メール暗号化**。HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、電子メールゲートウェイで暗号化ポリシーを設定し、ローカルキーサーバまたはホステッドキーサービスを使用してメッセージを暗号化します。
- 電子メールゲートウェイ上のすべての電子メールセキュリティサービスおよびアプリケーションを管理する、単一で包括的なダッシュボードである**電子メール セキュリティ マネージャ**。電子メール セキュリティ マネージャは、ユーザー グループに基づいて電子メールセキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、Cisco レピュテーション フィルタ、アウトブレイク フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。
- **オンボックスのメッセージ トラッキング**。AsyncOS for Email には、電子メールゲートウェイが処理するメッセージのステータスの検索が容易にできる、オンボックスのメッセージトラッキング機能があります。
- 企業のすべての電子メール トラフィックを全体的に確認できる、すべてのインバウンドおよびアウトバウンドの電子メールに対する**メール フロー モニタ機能**。
- 送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者の**アクセス制御**。
- 広範な**メッセージおよびコンテンツ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージをド

ロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。

- **セキュアな SMTP over Transport Layer Security 経由のメッセージの暗号化**により、企業のインフラストラクチャとその他の信頼できるホストとの間でやりとりされるメッセージが暗号化されるようなります。
- **Virtual Gateway**™テクノロジーにより、電子メールゲートウェイは、単一サーバ内で複数の電子メールゲートウェイとして機能できるため、さまざまな送信元またはキャンペーンの電子メールを、それぞれ独立した IP アドレスを通して送信するように分配できます。これにより、1 つの IP アドレスに影響する配信可能量の問題が、他の IP アドレスに及ばないようにします。
- 複数のサービスによって提供される、電子メール メッセージ内の**悪意のある添付ファイルやリンクからの保護**。
- **データ損失防止**により、組織から出る情報の制御と監視を行います。

AsyncOS は、メッセージを受け入れて配信するために、RFC 2821 準拠の Simple Mail Transfer Protocol（SMTP）をサポートします。

レポート作成コマンド、モニタリング コマンド、およびコンフィギュレーション コマンドのほとんどは、HTTP 経由でも HTTPS 経由でも Web ベースの GUI から使用できます。さらに、セキュア シェル（SSH）または直接シリアル接続でアクセスするインタラクティブなコマンドライン インターフェイス（CLI）がシステムに用意されています。

また、複数の電子メールゲートウェイのレポート、トラッキング、および隔離管理を統合するように Cisco Secure Email and Web Manager を設定できます。

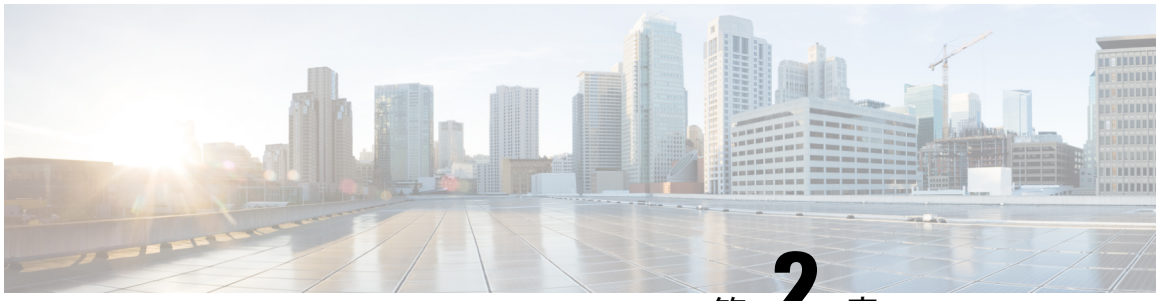
関連項目

- サポートされる言語 （11 ページ）

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- 英語
- フランス語
- スペイン語
- ドイツ語
- イタリア語
- 韓国語
- 日本語
- ポルトガル語（ブラジル）
- 中国語（繁体字および簡体字）
- ロシア語



第 2 章

電子メールゲートウェイへのアクセス

この章は、次の項で構成されています。

- Web ベースのグラフィカル ユーザー インターフェイス（GUI） （13 ページ）
- 構成時の設定の変更 （16 ページ）
- コマンドライン インターフェイス（CLI） （16 ページ）

Web ベースのグラフィカル ユーザー インターフェイス（GUI）

Web ベースのグラフィカルユーザーインターフェイス（GUI）とコマンドラインインターフェイス（CLI）の両方を使用して電子メールゲートウェイを管理できます。GUI には、システムの設定およびモニタに必要な機能のほとんどが含まれています。ただし、すべての CLI コマンドが GUI から使用できるわけではありません。一部の機能は CLI からのみ使用できます。

- ブラウザ要件 （13 ページ）
- GUI へのアクセス （14 ページ）

ブラウザ要件

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

ブラウザ	オペレーティング システム
Internet Explorer 11.0	Microsoft Windows 7、10
Safari 7.0 以降	Mac OS X
Firefox 39.0 以降	Microsoft Windows 7、10、Mac OS X
Chrome 44.0 以降	Microsoft Windows 7、10、Mac OS X

電子メールゲートウェイを変更する場合は、複数のブラウザウィンドウまたはタブを同時に使用しないでください。GUIセッションとCLIセッションを同時に使用しないてください。同時に使用すると、予期しない動作が発生し、サポート対象外になります。

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

GUI へのアクセス

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

http://192.168.42.42/

ログインページが表示されたら、デフォルトのユーザ名とパスフレーズを使用してシステムにログインします。

関連項目

- 工場出荷時のデフォルト ユーザ名とパスフレーズ （14 ページ）
- 中央集中型の管理 （15 ページ）

工場出荷時のデフォルト ユーザ名とパスフレーズ

- ユーザ名：**admin**
- パスフレーズ：**ironport**

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

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

次に例を示します。

`http://192.168.1.1` または

`https://192.168.1.1` または

`http://mail3.example.com` または

`https://mail3.example.com`

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

関連項目

- ユーザの追加 （1195 ページ）

中央集中型の管理

クラスタが作成されている場合は、クラスタ内のマシンを参照して、クラスタ、グループ、マシン間での設定の作成、削除、コピー、および移動（つまり、`clustermode` コマンドおよび `clusterset` コマンドと同等の操作）を GUI 内から実行できます。

詳細については、GUI でのクラスタの管理 （1498 ページ）を参照してください。

How-To ウィジェットを使用したユーザ エクスペリエンスの強化

How-To は、電子メールゲートウェイで複雑なタスクを実行するためにウォークスルー形式でユーザにアプリ内アシスタンスを提供する、コンテキスト型ウィジェットです。このリリースでサポートされているウォークスルーのリストを表示するには、「ウォークスルーのリスト」を参照してください。

ウォークスルーは、電子メールゲートウェイの Web インターフェイスで How-To ウィジェットをクリックすることでアクセスできます。How-To ウィジェットは電子メールゲートウェイでデフォルトで有効化されています。How-To ウィジェットのコンテンツはクラウドで更新できます。

各ウォークスルーには、以下に分類されるように、特定の設定可能な値に対する推奨設定があります。

- 保守的な設定 - 控え目な、過剰な制限を避けた設定
- 中程度の設定 - 平均的な、合理的な制限の設定
- 積極的な設定 - 強硬的な、積極的な制限の設定

（注）

- 現在の一連のウォークスルーを利用できるユーザは、管理者、クラウド管理者、オペレータに限定されています。
- 電子メールゲートウェイの Web インターフェイスにアクセスするために Internet Explorer のバージョン 11 を使用している場合、How-To ウィジェットを表示できない場合があります。How-To ウィジェットを表示するには、Web インターフェイスの [システム管理（System Administration）] > [全般設定（General Settings）] ページに移動し、IE 互換性モードを上書きするオプションを有効化してください。

電子メールゲートウェイで How-To ウィジェットを無効化

電子メールゲートウェイで How-To ウィジェットを無効化するには、CLI で `adminaccessconfig > how-tos` サブコマンドを使用します。

例：電子メールゲートウェイでの How-To ウィジェットの無効化

```
mail.example.com> adminaccessconfig

Choose the operation you want to perform:

- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- XSS - Configure Cross-Site Scripting Attack protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSIZE - Configure maximum HTTP header Field size.
- HOW-TOS - Configure How-Tos feature.

[]> how-tos
How-Tos consists of a list of generic walkthroughs to assist the users in completing
a particular task (for example, "enabling and configuring a service engine on the
appliance").

Would you like to enable How-Tos? [Y]> no
```

構成時の設定の変更

- 設定の変更 （16 ページ）
- 変更の確定またはキャンセル （16 ページ）

設定の変更

電子メールの通常の動作を妨げることなく、設定を変更できます。

変更の確定またはキャンセル

ほとんどの設定変更は明示的に保存する必要があります。

変更の確定が保留になっている場合は、[変更を確定（Commit Changes）] ボタンがオレンジ色に変化します。

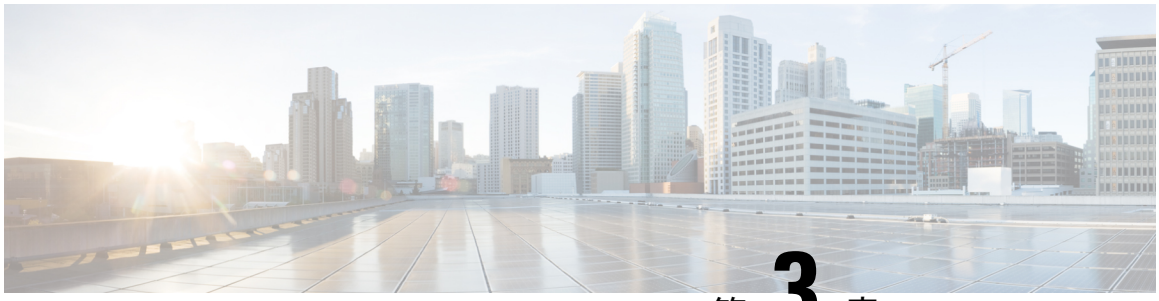
これらの変更をクリアまたは確定するには、[変更を確定（Commit Changes）] をクリックします。

コマンドライン インターフェイス（CLI）

コマンドライン インターフェイスには、SSH サービスがイネーブルに設定されている IP インターフェイスで SSH 経由か、またはシリアル ポートの端末エミュレーション ソフトウェア経由でアクセスできます。工場出荷時のデフォルトでは、SSHは管理ポートに設定されます。これらのサービスをディセーブルにするには、`interfaceconfig` コマンドを使用します。

CLI コマンドと規定の詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

（注） CLI にアクセスするための工場出荷時のデフォルトのユーザ名とパスフレーズは、Web インターフェイスと同じです。工場出荷時のデフォルト ユーザ名とパスフレーズ （14 ページ） を参照してください。



第 3 章

セットアップおよび設置

この章は、次の項で構成されています。

- インストール計画 （19 ページ）
- 電子メールゲートウェイのネットワークへの物理接続 （23 ページ）
- システム セットアップの準備 （27 ページ）
- システム セットアップ ウィザードの使用 （35 ページ）
- 設定と次の手順の確認 （66 ページ）

インストール計画

- 計画決定に影響を与える情報の確認 （19 ページ）
- ネットワーク境界に電子メールゲートウェイを配置する （19 ページ）
- DNS への E メール セキュリティ アプライアンスの登録 （20 ページ）
- インストールのシナリオ （21 ページ）

計画決定に影響を与える情報の確認

- 仮想電子メールゲートウェイを設定する場合は、この章に進む前に『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。
- Cisco Secure Email and Web Manager を設定する場合は、 Cisco Secure Email and Web Manager （M シリーズ）の集中型サービス （1559 ページ）を参照してください。
- インフラストラクチャへの電子メールゲートウェイの配置に影響する可能性のある一部の機能について、設置前に電子メール パイプラインについて （67 ページ）を参照することを推奨します。

ネットワーク境界に電子メールゲートウェイを配置する

お使いの電子メールゲートウェイが、Mail Exchange（MX）とも呼ばれる SMTP ゲートウェイとして機能するように設計されています。最適な結果を得るために、機能によっては、電子メールゲートウェイが電子メールを送受信するためにインターネットに直接アクセスできる IP アドレス（つまり、外部 IP アドレス）を割り当てられた最初のマシンである必要があります。

受信者ごとのレピュテーションフィルタリング、アンチスパム、アンチウィルス、およびウイルス アウトブレイク フィルタの機能（IronPort スパム対策フィルタリング （464 ページ）、Sophos アンチウイルス フィルタリング （441 ページ）、アウトブレイク フィルタ （513 ページ）を参照）は、インターネットおよび内部ネットワークから送られるメッセージの直接フローを処理することを目的としています。企業が送受信するすべての電子メールトラフィックに対するポリシー施行（接続を許可するホストの定義の概要（107ページ））のために電子メールゲートウェイを設定できます。

電子メールゲートウェイは、パブリックインターネットを介してアクセス可能なことと、電子メールインフラストラクチャの「第1ホップ」であることの両方を満たすことを確認します。別の MTA をネットワーク境界に配置してすべての外部接続を処理させると電子メールゲートウェイで送信者の IP アドレスを判別できなくなります。送信者の IP アドレスは、メールフローモニタで送信元を識別および区別したり、IP レピュテーションサービスに送信者の IP レピュテーションスコアを問い合わせたり、スパム対策機能やアウトブレイクフィルタ機能の有効性を高めたりするために必要です。

（注） インターネットから電子メールを受信する最初のマシンとして電子メールゲートウェイを設定できない場合でも、電子メールゲートウェイで使用可能なセキュリティサービスの一部は利用できます。詳細については、着信リレー構成における送信者の IP アドレスの決定 （497 ページ）を参照してください。

電子メールゲートウェイを SMTP ゲートウェイとして使用することにより、次の機能が実現されます。

- メール フローモニタ機能（電子メール セキュリティ モニタの使用方法（1009ページ）を参照）により、内部および外部の両方の送信者から企業に着信するすべての電子メール トラフィックを把握できます。
- ルーティング、エイリアシング、およびマスカレードを対象とする LDAP クエリー（LDAP クエリ （943ページ）を参照）では、ディレクトリ インフラストラクチャを統合でき、更新を単純化できます。
- エイリアステーブル（エイリアステーブルの作成（860ページ）を参照）、ドメインベースのルーティング（ドメイン マップ機能 （878 ページ）を参照）、およびマスカレード（マスカレードの構成（868ページ）を参照）などの一般的なツールによって、オープンソースの MTA からの移行が簡単になります。

DNS への E メール セキュリティ アプライアンスの登録

不正な電子メール送信者は、次の攻撃対象を探してパブリック DNS レコードを積極的に検索します。Anti-Spam、アウトブレイクフィルタ、McAfee Antivirus および Sophos Anti-Virus のすべての機能を利用するために、電子メールゲートウェイが DNS に登録されていることを確認します。

電子メールゲートウェイを DNS に登録するには、電子メールゲートウェイのホスト名を IP アドレスにマッピングする A レコードおよびパブリックドメインを電子メールゲートウェイのホスト名にマッピングする MX レコードを作成します。ドメインのプライマリ MTA またはバッ

クアップ MTA のいずれかとして電子メールゲートウェイをアドバタイズするように MX レコードのプライオリティを指定する必要があります。

次の例では、MX レコードに大きいプライオリティ値（20）が指定されているため、電子メールゲートウェイ（ironport.example.com）は、ドメイン example.com のバックアップ MTA です。言い換えると、数値が大きいほど、MTA のプライオリティは低くなります。

```
$ host -t mx example.com
```

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

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

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

インストールのシナリオ

電子メールゲートウェイを既存のネットワーク インフラストラクチャに設置する方法は複数あります。

大部分のお客様のネットワーク コンフィギュレーションは、以降のシナリオで表現されています。ネットワーク コンフィギュレーションが大幅に異なっており、設置計画の支援を必要とする場合は、シスコ カスタマー サポートにお問い合わせください（シスコカスタマーサポート（9 ページ）を参照）。

- 設定の概要 （21 ページ）
- 着信 （22 ページ）
- 発信 （22 ページ）
- イーサネット インターフェイス （22 ページ）
- 拡張設定 （23 ページ）
- ファイアウォール設定値（NAT、ポート） （23 ページ）

設定の概要

次の図は、エンタープライズネットワーク環境における電子メールゲートウェイの一般的な設置方法を示します。

いくつかのシナリオでは、電子メールゲートウェイはネットワークの「DMZ」内に配置されます。その場合は、電子メールゲートウェイとグループウェアサーバの間にさらにファイアウォールを設置しています。

次のネットワーク シナリオを説明します。

- ファイアウォールの内側：リスナー 2 個の設定（図「ファイアウォールの内側のシナリオ：リスナー 2 個の設定」）

実際のインフラストラクチャと最も一致する設定を選択してください。その後、システムセットアップの準備 （27 ページ）に進んでください。

着信

- 指定したローカル ドメイン宛ての着信メールは受け入れられます
- その他のドメインはすべて拒否されます。
- 外部システムは、ローカルドメイン宛て電子メールを転送するために電子メールゲートウェイに直接接続し、電子メールゲートウェイは、SMTP ルートを介して、そのメールを適切なグループウェアサーバ（Exchange™、Groupwise™、Domino™ など）にリレーします。（ローカル ドメインの電子メールのルーティング （853 ページ） を参照。）

発信

- 内部ユーザが送信した発信メールは、グループウェアサーバによって電子メールゲートウェイにルーティングされます。
- 電子メールゲートウェイでは、プライベートリスナーのホストアクセステーブルの設定値に基づいて発信電子メールを受け入れます。（詳細については、リスナーの使用 （82 ページ）を参照してください。）

イーサネット インターフェイス

これらの設定では、電子メールゲートウェイにある使用可能なイーサネットインターフェイスのうち 1 つだけを必要とします。ただし、イーサネットインターフェイスを 2 つ設定すると、内部ネットワークを外部インターネット ネットワーク接続と分離できます。

使用可能なインターフェイスに対する複数 IP アドレスの割り当ての詳細については、Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （912 ページ）およびネットワークと IP アドレスの割り当て （1581 ページ）を参照してください。

ハードウェアのポート

ハードウェア アプライアンスのポートの数とタイプはモデルによって異なります。

ポート	タイプ	C190	C390	C690	C690F	C195	C395	C695	C695F
管理	イーサネット	0	1	1	1	0	1	1	1

ポート	タイプ	C190	C390	C690	C690F	C195	C395	C695	C695F
データ	イーサネット	2*	5	5	3	2*	5	5	3
コンソール	シリアル	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45
リモート電源管理（RPC）	イーサネット	対応	対応	対応	対応	対応	対応	対応	対応

* 専用管理ポートのないアプライアンスでは、Data1 ポートを管理用に使用します。

ポートの詳細については、お使いのアプライアンス モデルの『Hardware Installation Guide』を参照してください。

関連項目

- ネットワーク インターフェイスの設定 （43 ページ）
- シリアル接続経由での 電子メールゲートウェイへのアクセス （1577 ページ）
- リモート電源再投入の有効化 （1269 ページ）

拡張設定

「ファイアウォールの内側のシナリオ：リスナー 2 個の設定」、および「リスナー 1 個の設定」の図に示す設定に加えて、次も設定できます。

- 中央集中管理機能を使用する複数電子メールゲートウェイ。クラスタを使用した中央集中型管理 （1481 ページ）を参照してください
- 電子メールゲートウェイの 2 つのイーサネット インターフェイスを NIC ペアリング機能によって「チーム化」することによるネットワーク インターフェイス カード レベルでの冗長性。高度なネットワーク構成 （1375 ページ）を参照してください

ファイアウォール設定値（NAT、ポート）

SMTP サービスおよびDNS サービスでは、インターネットにアクセスできる必要があります。他のサービスも場合によってはファイアウォール ポートを開く必要があります。詳細については、ファイアウォール情報 （1607 ページ） を参照してください。

電子メールゲートウェイのネットワークへの物理接続

- 設定シナリオ （23 ページ）

設定シナリオ

電子メールゲートウェイの一般的な設定シナリオは次のとおりです。

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

関連項目

- 着信メールと発信メールの分離 （24 ページ）

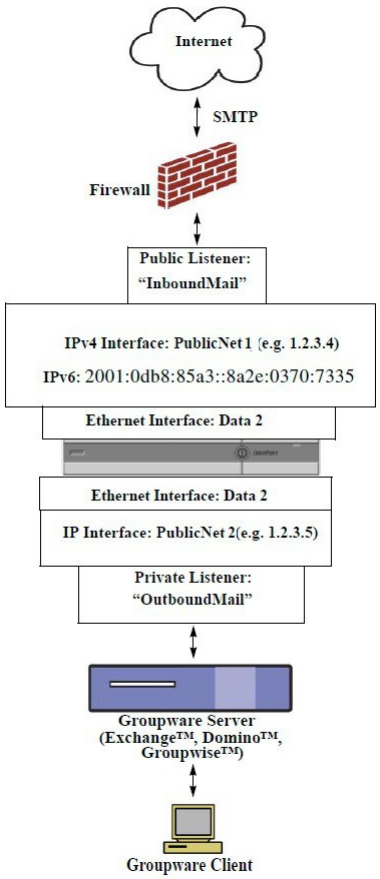
着信メールと発信メールの分離

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスを使用できます。ただし、電子メールゲートウェイのシステムセットアップ ウィザードでは、次の構成を持つ初期設定をサポートしています。

- 個別の物理インターフェイスに設定された 2 個の論理 IPv4 アドレスおよび 2 個の IPv6 アドレス上の 2 つの個別リスナー
  - 着信と発信のトラフィックの分離
  - IPv4 アドレスおよび IPv6 アドレスを各リスナーに割り当てることができます。
- 1 つの物理インターフェイスに設定された 1 つの論理 IPv4 アドレス上の 1 つのリスナー
  - 着信と発信の両トラフィックの組み合わせ
  - IPv4 アドレスおよび IPv6 アドレスの両方ともリスナーに割り当てることができます。

リスナー 1 つと 2 つの両方の設定に対する設定ワークシートが以下にあります（セットアップ情報の収集 （31 ページ）を参照）。大部分の設定シナリオは、次の 3 つの図のいずれかで表現されます。

図 *1*: ファイアウォールの内側のシナリオ：リスナー *2* 個の設定



（注）

- リスナー x 2
- IPv4 アドレス x 2
- IPv6 アドレス x 2
- イーサネット インターフェイス x 1 または 2（表示されるインターフェイスは 1 個のみ）
- 設定済みの SMTP ルート

インバウンド リスナー：「InboundMail」（パブリック）

- IPv4 アドレス：1.2.3.4
- IPv6 アドレス: 2001:0db8:85a3::8a2e:0370:7334
- Data 2 インターフェイスのリスナーでポート 25 をリッスン

- HAT（すべてを受け入れ）
- RAT（ローカル ドメイン宛てメールを受け入れ、その他すべてを拒否）

アウトバウンド リスナー：「OutboundMail」（プライベート）

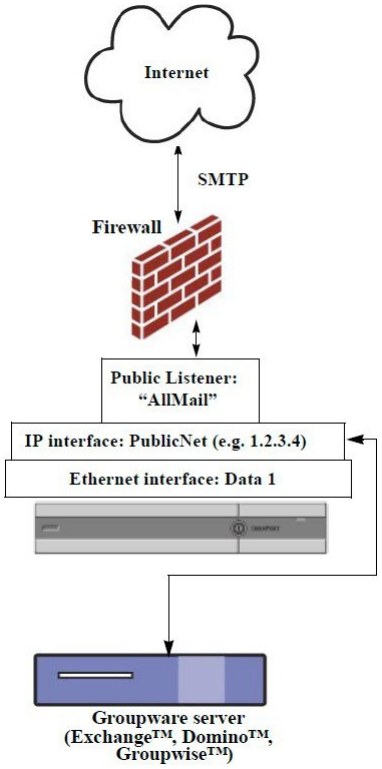
- IP アドレス：1.2.3.5
- IPv6 アドレス: 2001:0db8:85a3::8a2e:0370:7335
- Data 2 インターフェイスのリスナーでポート 25 をリッスン
- HAT（ローカル ドメイン宛てをリレー、その他すべてを拒否）

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

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと電子メールゲートウェイの双方向の通信用にファイアウォールポートをオープン

図 *2:* リスナー *1* 個の設定



注：

- リスナー X 1
- IP アドレス X 1

- イーサネット インターフェイス X 1
- 設定済みの SMTP ルート

インバウンド リスナー：「InboundMail」（パブリック）

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

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

SMTP ルートでは、適切なグループウェア サーバにメールを振り向け

適切なサービスと電子メールゲートウェイの双方向の通信用にファイアウォールポートをオープン。

システム セットアップの準備

- 電子メールゲートウェイへの接続方式の決定 （28 ページ）
- ネットワーク アドレスと IP アドレスの割り当ての決定 （29 ページ）
- セットアップ情報の収集 （31 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	電子メールゲートウェイへの接続方法を決定します。	電子メールゲートウェイへの接続方式の決定 （28 ページ）を参照してください
ステップ 2	ネットワーク アドレスと IP アドレスの割り当てを決定します。 • すでに 電子メールゲートウェイをネットワークに配線済みの場合は、電子メールゲートウェイのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。	参照先： 電子メールゲートウェイへの接続方式の決定 （28 ページ）およびネットワーク アドレスと IP アドレスの割り当ての決定 （29 ページ）
ステップ 3	システム セットアップに関する情報を収集します。	セットアップ情報の収集 （31 ページ）を参照してください。
ステップ 4	電子メールゲートウェイの最新の製品リリースノートを確認します。	資料 （7 ページ）のリンクから、リリース ノートを入手できます。

	コマンドまたはアクション	目的
ステップ 5	電子メールゲートウェイを開梱し、物理的にラックに設置してオンにします。	お使いの 電子メールゲートウェイのクイックスタートガイドを参照してください。このガイドは、資料 （7 ページ）のリンクから入手できます。
ステップ 6	コマンド ライン インターフェイス（CLI）を使用してセットアップ ウィザードを実行すると、CLIにアクセスします。	コマンドライン インターフェイス（CLI）システムセットアップ ウィザードの実行 （51 ページ）を参照してください。
ステップ 7	Web インターフェイスを使用してセットアップ ウィザードを実行する場合、	1. （仮想アプライアンスの場合のみ）コマンド ライン インターフェイスにアクセスし、`interfaceconfig` コマンドを使用して、HTTP および HTTPS を有効にします。 2. Web ブラウザを起動し、 電子メールゲートウェイの IP アドレスを入力します。
ステップ 8	仮想 電子メールゲートウェイをセットアップする場合は、お使いの仮想電子メールゲートウェイのライセンスをロードしてください。	`loadlicense` コマンドを使用します。詳細については、資料 （7 ページ）のリンクから利用できる『*Content Security Virtual Appliance Installation Guide*』を参照してください。
ステップ 9	システムの基本設定を行います。	システム セットアップ ウィザードの使用 （35 ページ）を参照してください

電子メールゲートウェイへの接続方式の決定

電子メールゲートウェイを環境に正常にセットアップするには、電子メールゲートウェイをネットワークに接続する方法に関する重要なネットワーク情報をネットワーク管理者から収集する必要があります。

関連項目

- 電子メールゲートウェイへの接続 （28 ページ）

電子メールゲートウェイへの接続

初期セットアップ時に、次の 2 つのいずれかの方式で 電子メールゲートウェイに接続できます。

表 *3:* 電子メールゲートウェイに接続するためのオプション

イーサネット	PC とネットワークの間およびネットワークと管理ポートの間のイーサネット接続です。工場出荷時に管理ポートに割り当てられている IPv4 アドレスは 192.168.42.42 です。ご使用のネットワーク コンフィギュレーションで使用可能であれば、この方法による接続が手軽です。
シリアル	シリアル通信によって PC とシリアル コンソール ポートが接続されます。イーサネット方式を使用できない場合は、コンピュータと電子メールゲートウェイをシリアル同士でストレート接続すると、代替ネットワーク設定値を管理ポートに適用できるまでの代用になります。ピン割り当ての詳細については、シリアル接続経由での 電子メールゲートウェイへのアクセス （1577 ページ）を参照してください。シリアル ポートの通信設定値は次のとおりです。 **ビット/秒**：9600 **データ ビット**：8 **パリティ**：なし **ストップビット**：1 **フロー制御**：ハードウェア

（注） 初期接続方式は、最終的な方式でないことに留意してください。このプロセスは、初期設定だけに適用されます。ネットワーク設定値を後で変更して、別の接続方式を使用できます（詳細については、FTP、SSH、および SCP アクセス （1573 ページ）を参照してください。） 電子メールゲートウェイを利用するための管理者権限が異なる、複数のユーザアカウントを作成することもできます。（詳細については、ユーザの追加 （1195 ページ）を参照してください。）

ネットワーク アドレスと IP アドレスの割り当ての決定

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

- 管理およびデータ ポート用のデフォルト IP アドレス （29 ページ）
- 電子メールを受信および配信するネットワーク接続の選択 （30 ページ）
- 物理イーサネット ポートへの論理 IP アドレスのバインド （30 ページ）
- 接続用ネットワーク設定値の選択 （30 ページ）

管理およびデータ ポート用のデフォルト IP アドレス

管理ポート（C170 および C190 電子メールゲートウェイの Data 1 ポート）に事前に設定されている IP アドレスは、192.168.42.42 です。

電子メールを受信および配信するネットワーク接続の選択

大部分のユーザは、 電子メールゲートウェイから 2 つのネットワークに接続することによって、電子メールゲートウェイ上の 2 つの Data イーサネットポートを利用します。

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

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

物理イーサネット ポートへの論理 IP アドレスのバインド

着信と発信の電子メール トラフィックを個別のリスナーおよび個別の IP アドレスで分離できます。インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスを使用できます。ただし、電子メールゲートウェイのシステム セットアップ ウィザードでは、次の構成を持つ初期設定をサポートしています。

- 個別の物理インターフェイスに設定された 2 個の論理 IPv4 アドレスおよび 2 個の IPv6 アドレス上の 2 つの個別リスナー
  - 着信と発信のトラフィックの分離
  - IPv4 アドレスおよび IPv6 アドレスを各リスナーに割り当てることができます。
- 1 つの物理インターフェイスに設定された 1 つの論理 IPv4 アドレス上の 1 つのリスナー
  - 着信と発信の両トラフィックの組み合わせ
  - IPv4 アドレスおよび IPv6 アドレスの両方ともリスナーに割り当てることができます。

電子メールゲートウェイは、1 つのリスナーで IPv4 アドレスと IPv6 アドレスの両方をサポートできます。リスナーは両方のアドレスでメールを受け入れます。リスナーの設定はすべて、IPv4 と IPv6 両方のアドレスに適用されます。

接続用ネットワーク設定値の選択

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

- IP アドレス（IPv4 または IPv6、あるいはその両方）
- CIDR 形式の IPv4 アドレスのネットマスク
- CIDR 形式の IPv6 アドレスのプレフィックス

さらに、ネットワーク全体に関する次の情報も必要になります。

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

- NTP サーバのホスト名または IP アドレス（シスコのタイム サーバを使用する場合は不要）

詳細については、ネットワークと IP アドレスの割り当て（1581 ページ）を参照してください。

（注） インターネットと 電子メールゲートウェイの間でファイアウォールを稼働しているネットワークの場合は、 電子メールゲートウェイを正常に機能させるために、特定のポートを開ける必要が生じる場合があります。詳細については、ファイアウォール情報 （1607 ページ）を参照してください。

セットアップ情報の収集

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

ネットワークおよび IP アドレスの詳細については、ネットワークと IP アドレスの割り当て（1581 ページ）を参照してください。 Cisco Secure Email and Web Manager を設定する場合は、Cisco Secure Email and Web Manager（M シリーズ）の集中型サービス （1559 ページ）を参照してください。

表 *4:* システム セットアップ ワークシート：*2*個のリスナーによる電子メール トラフィックの分離

システム設定		
デフォルトのシステム ホスト名（Default System Hostname）：		
システム アラート メールの送信先（Email System Alerts To）：		
定期レポートの送信先:（Deliver Scheduled Reports To:）		
タイムゾーン情報（Time Zone Information）：		
NTP サーバ:（NTP Server:）		
管理者パスフレーズ（Admin Passphrase）：		

システム設定		
SenderBase ネットワークに参加:（SenderBase Network Participation:）	イネーブル/ディセーブル（Enable / Disable）	
オートサポート:（AutoSupport:）	イネーブル/ディセーブル（Enable / Disable）	
ネットワーク インテグレーション（Network Integration）		
ゲートウェイ（Gateway）：		
DNS:（インターネットまたは独自指定）		
インターフェイス		
データ1ポート（Data 1 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
受信メールの受け入れ:（Accept Incoming Mail:）	**ドメイン（Domain）**	**送信先（Destination）**
外部への送信メールを中継:（Relay Outgoing Mail:）	**システム（System）**	
データ2ポート（Data 2 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
受信メールの受け入れ:（Accept Incoming Mail:）	**ドメイン（Domain）**	**送信先（Destination）**

システム設定		
外部への送信メールを中継:（Relay Outgoing Mail:）	**システム（System）**	
管理ポート		
IP アドレス：（IP Address:）		
ネットワークマスク:（Network Mask:）		
IPv6アドレス:（IPv6 Address:）		
プレフィックス:（Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
受信メールの受け入れ:（Accept Incoming Mail:）	**ドメイン（Domain）**	**送信先（Destination）**
外部への送信メールを中継:（Relay Outgoing Mail:）	**システム（System）**	
メッセージセキュリティ（Message Security）		
IP レピュテーション フィルタリング（IP Reputation Filtering）：	イネーブル/ディセーブル（Enable / Disable）	
スパム対策スキャン エンジン（Anti-Spam Scanning Engine）	なし/IronPort	
McAfee ウイルス対策スキャン エンジン（McAfee Anti-Virus Scanning Engine）	イネーブル/ディセーブル（Enable / Disable）	
Sophos ウイルス対策スキャン エンジン（Sophos Anti-Virus Scanning Engine）	イネーブル/ディセーブル（Enable / Disable）	
アウトブレイク フィルタ（Outbreak Filters）	イネーブル/ディセーブル（Enable / Disable）	

表 *5:* システム セットアップ ワークシート：*1*個のリスナーをすべての電子メール トラフィックに使用

システム設定		
デフォルトのシステム ホスト名（Default System Hostname）：		
システム アラート メールの送信先（Email System Alerts To）：		
定期レポートの送信先:（Deliver Scheduled Reports To:）		
タイム ゾーン:（Time Zone:）		
NTP サーバ:（NTP Server:）		
管理者パスフレーズ（Admin Passphrase）：		
SenderBase ネットワークに参加:（SenderBase Network Participation:）	イネーブル/ディセーブル（Enable / Disable）	
オートサポート:（AutoSupport:）	イネーブル/ディセーブル（Enable / Disable）	
ネットワーク インテグレーション（Network Integration）		
ゲートウェイ（Gateway）：		
DNS:（インターネットまたは独自指定）		
インターフェイス		
データ2ポート（Data 2 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		

システム設定		
受信メールの受け入れ:（Accept Incoming Mail:）	**ドメイン（Domain）**	**送信先（Destination）**
外部への送信メールを中継:（Relay Outgoing Mail:）	**システム（System）**	
データ1ポート（Data 1 Port）		
IPv4アドレス/ネットマスク:（IPv4 Address / Netmask:）		
IPv6アドレス/プレフィックス:（IPv6 Address / Prefix:）		
完全なホスト名:（Fully Qualified Hostname:）		
メッセージセキュリティ（Message Security）		
IP レピュテーション フィルタリング（IP Reputation Filtering）：	イネーブル/ディセーブル（Enable / Disable）	
スパム対策スキャン エンジン（Anti-Spam Scanning Engine）	なし/IronPort	
McAfee ウイルス対策スキャン エンジン（McAfee Anti-Virus Scanning Engine）	イネーブル/ディセーブル（Enable / Disable）	
Sophos ウイルス対策スキャン エンジン（Sophos Anti-Virus Scanning Engine）	イネーブル/ディセーブル（Enable / Disable）	
アウトブレイク フィルタ（Outbreak Filters）	イネーブル/ディセーブル（Enable / Disable）	

システム セットアップ ウィザードの使用

- Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス （37 ページ）
- Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義 （39 ページ）
- Active Directory への接続の設定 （48 ページ）

- 次の手順 （49 ページ）
- コマンドライン インターフェイス（CLI）へのアクセス （49 ページ）
- コマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行 （51 ページ）
- エンタープライズ ゲートウェイとしてシステムを設定 （66 ページ）

初期セットアップではシステム セットアップ ウィザードを使用して、設定に漏れがないようにする必要があります。後で、システム セットアップ ウィザードで利用できないカスタム オプションを設定できます。

ブラウザまたはコマンドラインインターフェイス（CLI）を使用して、システム設定ウィザードを実行できます。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス （37 ページ）またはコマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行 （51 ページ）を参照してください。

開始する前に、システム セットアップの準備 （27 ページ）にある前提条件をクリアします。

注意 仮想 電子メールゲートウェイをセットアップする場合は、システム セットアップ ウィザードを実行する前に、仮想 電子メールゲートウェイのライセンスをロードするために loadlicense コマンドを使用する必要があります。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。

注意 システム セットアップ ウィザードでは、システムを完全に再設定します。システム セットアップ ウィザードは、 電子メールゲートウェイをまったく初めて設置する場合か、既存の設定を上書きする場合に限り使用してください。

注意 電子メールゲートウェイは、すべてのハードウェアの管理ポートにデフォルト IP アドレスの 192.168.42.42 を設定した状態で出荷されます（Data 1 ポートを代わりに使用する C170 および C190 電子メールゲートウェイを除く）。電子メールゲートウェイをネットワークに接続する前に、他の装置の IP アドレスが、この工場出荷時のデフォルト設定と競合していないことを確認してください。 Cisco Secure Email and Web Manager を設定する場合は、 Cisco Secure Email and Web Manager（M シリーズ）の集中型サービス （1559 ページ）を参照してください。

工場出荷時の設定を持つ複数のコンテンツ セキュリティ アプライアンスをネットワークに接続する場合は、1 つずつ追加して、各アプライアンスのデフォルト IP アドレスを順に再設定してください。

Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス

電子メールゲートウェイには、標準の Web ベースのグラフィカル ユーザー インターフェイス、電子メールセキュリティ モニタ機能（モニタ、追跡、隔離）を管理するための新しい Web ベースのインターフェイス、およびコマンドライン インターフェイスがあります。

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

（新しい Web インターフェイスのみ）新しい Web インターフェイスには次のいずれかの方法でアクセスできます。

（注） 電子メールゲートウェイの新しい Web インターフェイスは、AsyncOS API HTTP/HTTPS ポート（6080/6443）および trailblazer HTTPS ポート（4431）を使用します。CLI で `trailblazerconfig` コマンドを使用して、trailblazer HTTPS ポートを設定できます。trailblazer HTTPS ポートがファイアウォールで開かれていることを確認します。

- `trailblazerconfig` CLI コマンドが有効になっているときは、URL（`https://example.com:<trailblazer-https-port>/ng-login`）を使用します

  ここで、`example.com` は 電子メールゲートウェイのホスト名、`<trailblazer-https-port>` は電子メールゲートウェイで設定されている trailblazer HTTPS ポートです。

  trailblazerconfig CLI コマンドの詳細については、『Cisco Email Security Command Reference Guide』を参照してください。

- レガシー Web インターフェイスにログインし、**セキュア電子メールゲートウェイの外観が新しくなりました。お試しください!** リンクで新しい Web インターフェイスにアクセスできます。

特記事項

- 電子メールゲートウェイで AsyncOS API が有効になっていることを確認してください。
- AsyncOS HTTPS API ポートが複数のインターフェイスで有効になっていないことを確認します。
- 電子メールゲートウェイのレガシー Web インターフェイスにログインする必要があります。
- `trailblazerconfig` が有効になっている場合は、設定済み HTTPS ポートがファイアウォールで開いている必要があります。デフォルトの HTTPS ポートは 4431 です。

  また、 電子メールゲートウェイにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。

関連項目

- 工場出荷時のデフォルト ユーザ名とパスフレーズ （38 ページ）
- 新しい Web インターフェイスの暗色モードでの利用 （39 ページ）

工場出荷時のデフォルト ユーザ名とパスフレーズ

新しい仮想またはハードウェア電子メールゲートウェイをインストールする場合、完全なアクセス権を取得して電子メールゲートウェイを設定するために、デフォルトのパスフレーズを変更する必要があります。初めて電子メールゲートウェイにログインすると、Webインターフェイスによってデフォルトのパスフレーズを変更するように指示されます。デフォルトのパスフレーズを変更するまで、CLI で以下のコマンドへのアクセスが制限されます。

- Commit
- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense（仮想 電子メールゲートウェイ向け）
- ライセンス キー
- Ping
- Telnet
- netstat

- ユーザ名：**admin**
- パスフレーズ：**ironport**

例：

```
login: admin
passphrase: ironport
```

（注） セッションがタイムアウトした場合は、ユーザ名とパスフレーズの再入力が求められます。システム セットアップ ウィザードの実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。

レガシー Web インターフェイスへのアクセス

新しい Web インターフェイスからレガシー Web インターフェイスにアクセスするには、次の図に示すように、歯車アイコン（⚙）をクリックします。

図 *3:* レガシー *Web* インターフェイスへのアクセス

レガシー Web インターフェイスが新しいブラウザ ウィンドウで開きます。アクセスするには再度ログインする必要があります。

アプライアンスから完全にログアウトする場合は、電子メールゲートウェイの新しい Web インターフェイスとレガシー Web インターフェイスの両方からログアウトする必要があります。

新しい Web インターフェイスの暗色モードでの利用

暗色モードは反転カラースキームであり、暗い色の背景上で明るい色のタイポグラフィ、UI 要素、アイコンが使用されます。

電子メールゲートウェイの新しい Web インターフェイスを暗色モードで利用できるようになりました。

暗色モードに切り替えるには、新しい Web インターフェイスの右上隅にあるユーザアイコンをクリックし、[暗色表示テーマ（Dusk Theme）] を選択します。

Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義

手順

ステップ 1 システム セットアップ ウィザードの起動

- Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス （37 ページ）に記載されている方法で、グラフィカル ユーザー インターフェイスにログインします。
- 新規のシステム（先行リリースの AsyncOS からのアップグレードなし）の場合は、ブラウザがシステム セットアップ ウィザードに自動的にリダイレクトされます。
- それ以外の場合は、[システム管理（System Administration）] タブで、左方のリンク リストから [システムセットアップウィザード（System Setup Wizard）] をクリックします。

ステップ 2 [開始（Start）]。手順 1：開始 （40 ページ）を参照してください。

- ライセンス契約書の参照と受諾

ステップ 3 システム。手順 2：システム （40 ページ）を参照してください。

- 電子メールゲートウェイのホスト名の設定
- アラート、レポート配信、および AutoSupport の設定
- システム時刻と NTP サーバの設定

- admin パスフレーズのリセット
- サービスログの有効化

ステップ 4 [ネットワーク（Network）]。手順 3：ネットワーク （42 ページ）を参照してください。

- デフォルト ルータおよび DNS 設定値の定義
- ネットワーク インターフェイスの有効化および構成：これには受信メール（受信リスナー）の設定、SMTP ルートの定義（オプション）、送信メール（送信リスナー）の設定、および電子メールゲートウェイを介したメールのリレーが許可されるシステムの定義が含まれます。

ステップ 5 [セキュリティ（Security）]。手順 4：セキュリティ （46 ページ）を参照してください。

- IP レピュテーション フィルタリングの有効化
- スパム対策サービスのイネーブル化
- スパム隔離のイネーブル化
- Anti-Virus サービスのイネーブル化
- 高度なマルウェア防御のイネーブル化（ファイル レピュテーションおよび分析サービス）
- アウトブレイク フィルタサービスのイネーブル化

ステップ 6 [レビュー（Review）]。手順 5：レビュー （48 ページ）を参照してください。

- セットアップのレビューおよび設定のインストール
- 手順の最後に表示されるプロンプト

ステップ 7 変更点の確定

確定するまで、変更は有効になりません。

手順 1：開始

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

契約書の文面は次の場所でも参照できます。https://support.ironport.com/license/eula.html

手順 2：システム

- ホスト名の設定 （41 ページ）
- システム アラートの設定 （41 ページ）
- レポート配信の設定 （41 ページ）
- 時間の設定 （41 ページ）
- パスフレーズの設定 （41 ページ）
- サービスログを使用したフィッシング検知機能の有効性の向上 （1367 ページ）
- AutoSupport のイネーブル化 （42 ページ）

ホスト名の設定

電子メールゲートウェイの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

システム アラートの設定

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

システム アラートを受信する電子メール アドレスを 1 つ以上追加する必要があります。単一の電子メールアドレスか、カンマで区切った複数アドレスを入力します。当初、この電子メール受信者は、ディレクトリ獲得攻撃対策アラート以外のすべてのタイプおよびすべてのレベルのアラートを受信します。後で、アラートコンフィギュレーションをさらに詳細化できます。詳細については、アラート （1275 ページ）を参照してください。

レポート配信の設定

デフォルトのスケジュール済みレポートの送信先にするアドレスを入力します。この値をブランクにしても、スケジュール済みレポートは引き続き実行されます。スケジュール済みレポートは配信されませんが、 電子メールゲートウェイ上にアーカイブされます。

時間の設定

電子メールゲートウェイ上にタイムゾーンを設定して、メッセージヘッダーおよびログファイルのタイムスタンプが正確に表示されるようにします。ドロップダウン メニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します（詳細については、GMT オフセットの選択 （1324 ページ）を参照してください）。

システム クロック時刻は、後で手動によって設定するか、ネットワーク タイム プロトコル（NTP）を使用してネットワーク上またはインターネット上の他のサーバと時刻を同期することもできます。デフォルトでは、Cisco Systems のタイムサーバ（**time.ironport.com**）と時刻を同期するエントリ 1 つが 電子メールゲートウェイにすでに設定されています。

パスフレーズの設定

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

ログインパスフレーズを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスフレーズも作成できます。

サービスログの有効化

「サービスログ」は、フィッシング検出精度を向上させるために、Cisco Talos クラウドサービスに送信されます。

サービスログを有効にすると、Cisco E メール セキュリティ ゲートウェイは、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能を

専用分析システムと組み合わせると、検出された脅威アクティビティの収集、トレンド分析、および関連付けが可能になります。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

詳細については、サービスログを使用したフィッシング検知機能の有効性の向上（1367ページ）を参照してください。

AutoSupport のイネーブル化

AutoSupport 機能（デフォルトでイネーブル）では、ご使用の 電子メールゲートウェイに関する問題をシスコ カスタマー サポート チームが認識しておくことで、適切なサポートを提供できるようにします。（詳細については、AutoSupport （1275 ページ）を参照してください。）

[次へ（Next）] をクリックして続行します。

手順 3：ネットワーク

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

- DNS とデフォルト ゲートウェイの設定 （42 ページ）
- ネットワーク インターフェイスの設定 （43 ページ）
- メールの受け入れ （44 ページ）
- メール リレー（任意） （45 ページ）
- C170 および C190 のインストール （46 ページ）

DNS とデフォルト ゲートウェイの設定

ネットワーク上のデフォルト ルータ（ゲートウェイ）の IP アドレスを入力します。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。

次に、Domain Name Service（DNS）を設定します。Cisco AsyncOS には、インターネットのルートサーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスおよびホスト名を指定する必要があります。システム セットアップ ウィザードから入力できる DNS サーバは 4 台までです。入力した DNS サーバの初期プライオリティは 0 になっていることに注意してください。詳細については、ドメイン ネーム システム（DNS）設定値の構成 （1303 ページ）を参照してください。

（注） 電子メールゲートウェイでは、着信接続のための DNS ルックアップを実行するために、稼働中の DNS サーバを利用できる必要があります。 電子メールゲートウェイをセットアップするときに電子メールゲートウェイからアクセス可能な稼働中の DNS サーバを指定できない場合は、[インターネットルートDNSサーバを使用（Use Internet Root DNS Server）] を選択するか、Management インターフェイスの IP アドレスを一時的に指定することを回避策として、システム セットアップ ウィザードを完了できます。

ネットワーク インターフェイスの設定

電子メールゲートウェイには、マシンの物理イーサネットポートに関連付けられたネットワーク インターフェイスがあります。

インターフェイスを使用するには、[有効（Enable）] チェックボックスをオンにし、IP アドレス、ネットワーク マスク、および完全修飾ホスト名を指定します。入力する IP アドレスは、DNS レコードに反映されている、インバウンド メール用のアドレスである必要があります。通常、このアドレスには、DNS で MX レコードと関連付けられています。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。両方使用すると、インターフェイスは両方のタイプの接続を受け入れます。

各インターフェイスは、メールを受け入れる（着信）、電子メールをリレーする（発信）、またはアプライアンスを管理するように設定できます。セットアップ時は、このいずれかに制限されます。ほとんどの 電子メールゲートウェイでは、通常、インターフェイスの 1 つを着信用、1 つを発信用、1 つをアプライアンス管理用に使用します。C170 および C190 電子メールゲートウェイでは、1 つのインターフェイスを着信と発信の両方のメール用に使用し、もう 1 つのインターフェイスを管理用に使用することが一般的です。

インターフェイスの 1 つは、電子メールの受信用に設定する必要があります。

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

C390 および C690 アプライアンスの場合：物理イーサネットポートの 1 つは、インターネットに直接接続して、パブリックリスナー経由でインバウンド電子メールを受信するために使用し、もう 1 つの物理イーサネットポートは、内部ネットワークに直接接続して、プライベートリスナー経由でアウトバウンド電子メールをリレーするために使用することを推奨しています。

C190 アプライアンスの場合：通常、システム セットアップ ウィザードによって、物理イーサネットポートが 1 つのリスナーに 1 つだけ設定され、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方に対応します。

物理イーサネット ポートへの論理 IP アドレスのバインド（30 ページ）を参照してください。

次の情報が必要です。

- ネットワーク管理者によって割り当てられた **IP アドレス**。IPv4 アドレス、IPv6 アドレス、またはその両方を使用できます。

- IPv4 アドレスの場合：インターフェイスの**ネットマスク**。AsyncOS は、CIDR 形式のネットマスクだけを受け入れます。たとえば、`255.255.255.0` サブネットの `/24` など。

  IPv6 アドレスの場合：CIDR 形式の**プレフィックス**。64 ビット プレフィックスの `/64` など。

- （任意）IP アドレスの完全修飾ホスト名。

（注） 同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、ネットワークと IP アドレスの割り当て（1581 ページ）を参照してください。

メールの受け入れ

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

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

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

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

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

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

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

（注） この手順での SMTP ルートの設定は任意です。SMTP ルートを定義していない場合は、リスナーが受信した着信メールの配信ホストの検索と決定に、DNS が使用されます（ローカル ドメインの電子メールのルーティング （853 ページ） を参照。）

ドメインを受信者アクセステーブルに少なくとも 1 つ追加する必要があります。ドメイン、たとえば、`example.com` を入力します。`example.net` のいずれのサブドメイン宛てのメールとも必ず一致させるために、ドメイン名の他に `.example.net` も受信者アクセス テーブルに入力します。詳細については、受信者アドレスの定義 （150 ページ）を参照してください。

メール リレー（任意）

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

リスナーのホスト アクセス テーブルにある RELAYLIST 内のエントリを使用します。詳細については、送信者グループの構文 （110 ページ）を参照してください。

[外部への送信メールを中継（Relay Outgoing Mail）] のチェックボックスをオンにし、メールをリレーするインターフェイスを設定します。 電子メールゲートウェイを介してメールをリレーできるホストを入力します。

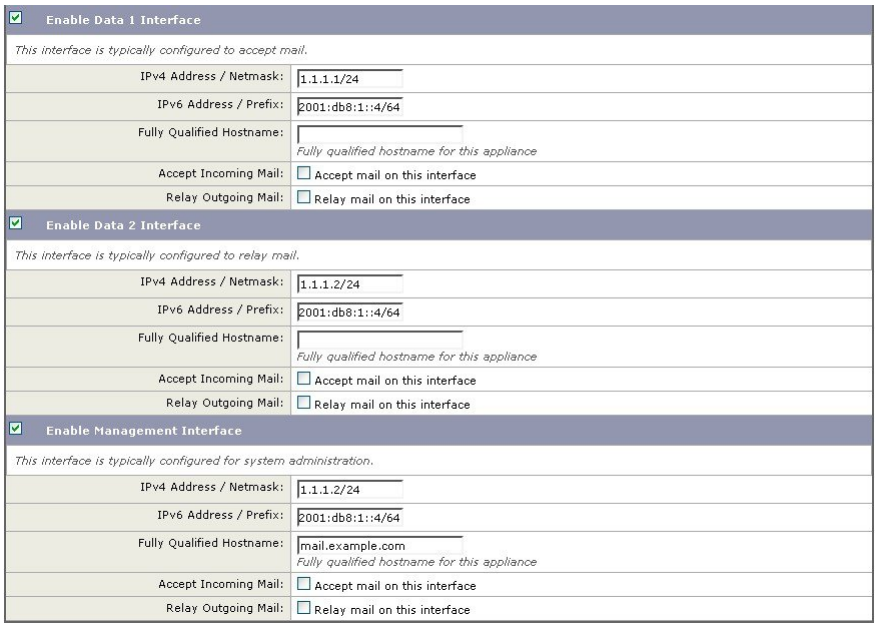
アウトバウンドメールをリレーするようにインターフェイスを設定すると、そのインターフェイスを使用するパブリック リスナーが設定されている場合を除き、そのインターフェイスの SSH がシステム セットアップ ウィザードによってオンにされます。

次の例では、IPv4 アドレスの 2 個のインターフェイスが作成されます。

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

C390 および C690 のインストール

図 *4 :* ネットワーク インターフェイス：*Management* および追加のインターフェイス *x 2*（トラフィックの分離）

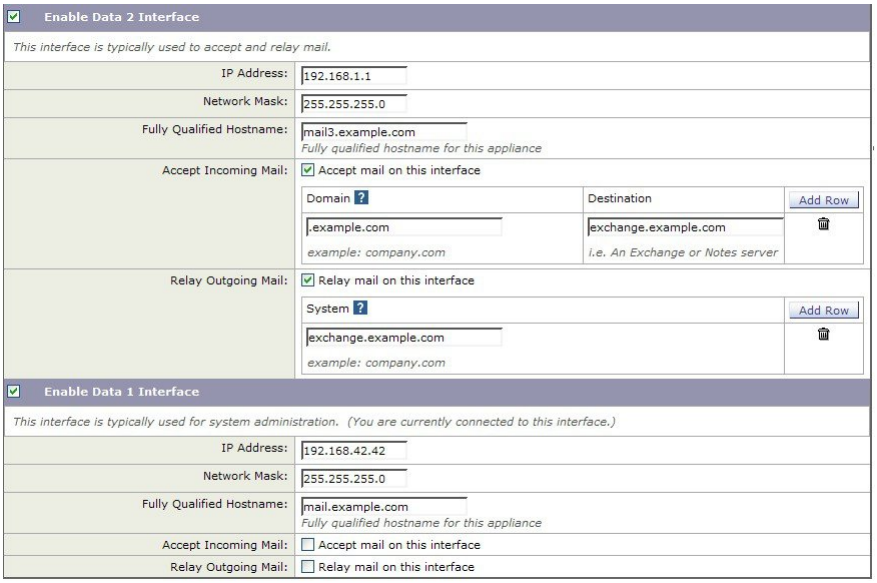


C170 および C190 のインストール

C170 および C190 アプライアンスの場合は、着信と発信の両方のメール用に Data 2 インターフェイスを設定し、アプライアンス管理用に Data 1 インターフェイスを設定することが一般的です。

すべての電子メール トラフィック用に単一の IP アドレスを設定する場合（トラフィックの分離なし）、システム セットアップ ウィザードの手順 3 は次のようになります。

図 *5:* ネットワーク インターフェイス：着信と発信の（分離されない）トラフィック用に *1* つの *IP* アドレス



[次へ（Next）] をクリックして続行します。

手順 4：セキュリティ

手順 4 では、アンチスパム設定値およびアンチウイルス設定値を設定します。アンチスパムオプションには、IP レピュテーション フィルタリングとアンチスパム スキャン エンジンの選択が含まれます。アンチウイルスについては、アウトブレイク フィルタおよび Sophos または McAfee のアンチウイルス スキャンをイネーブルにできます。

- IP レピュテーション フィルタリングの有効化 （46 ページ）
- アンチスパム スキャンのイネーブル化 （47 ページ）
- アンチウイルス スキャンのイネーブル化 （47 ページ）
- 高度なマルウェア防御のイネーブル化（ファイル レピュテーションおよび分析サービス）（47 ページ）
- アウトブレイク フィルタのイネーブル化 （48 ページ）

IP レピュテーション フィルタリングの有効化

IP レピュテーションサービスは、スタンドアロンのスパム対策ソリューションとしても使用できますが、コンテンツベースのスパム対策システム（Anti-Spam など）の有効性を高めることを主な目的としています。

IP レピュテーションサービスを使用すると、ユーザはリモートホストの接続 IP アドレスに基づいて、正確かつ柔軟に、陽性と疑わしいスパムを拒否またはスロットリングできます。IP レピュテーションサービスは、特定の送信元からのメッセージがスパムである確率に基づく評点を返します。IP レピュテーションサービスは、電子メールメッセージの量をグローバルに表示して、電子メールの送信元の識別とグループ化を容易にする方法でデータを編成している点で独特です。シスコでは、IP レピュテーション フィルタリングを有効にすることを強く推奨しています。

有効にしたIP レピュテーション フィルタリングは、着信（受け入れ）リスナーで適用されます。

アンチスパム スキャンのイネーブル化

電子メールゲートウェイには、スパム対策ソフトウェアの 30 日間有効な評価キーが付属している場合があります。システム セットアップ ウィザードのこの部分では、 電子メールゲートウェイで Anti-Spam をグローバルでイネーブルにすることを選択できます。スパム対策サービスをイネーブルにしないことも選択できます。

スパム対策サービスをイネーブルにする場合は、スパムおよび陽性と疑わしいスパム メッセージをローカル スパム隔離に送信するように、AsyncOS を設定できます。スパム隔離は、 電子メールゲートウェイのエンドユーザ隔離として機能します。エンドユーザのアクセス権を設定していないうちは、管理者だけが隔離を利用できます。

電子メールゲートウェイで使用可能なすべての Anti-Spam 設定オプションについては、スパムおよびグレイメールの管理 （461 ページ）を参照してください。ポリシー、ウイルス、およびアウトブレイク隔離 （1129 ページ） を参照してください。

アンチウイルス スキャンのイネーブル化

電子メールゲートウェイには、Sophos Anti-Virus または McAfee Anti-Virus スキャンエンジンの 30 日間評価キーが付属している場合があります。システム セットアップ ウィザードのこの部分では、電子メールゲートウェイでウイルス対策スキャンエンジンをグローバルでイネーブルにすることを選択できます。

ウイルス対策スキャン エンジンを有効にすると、デフォルトの着信メール ポリシーおよびデフォルトの発信メール ポリシーの両方について有効になります。 電子メールゲートウェイでは、メールをスキャンしてウイルスを検出しますが、感染した添付ファイルの修復は行いません。 電子メールゲートウェイでは、感染したメッセージをドロップします。

電子メールゲートウェイで使用可能なすべてのウイルス対策設定オプションについては、アンチウイルス （439 ページ）を参照してください。

高度なマルウェア防御のイネーブル化（ファイル レピュテーションおよび分析サービス）

高度なマルウェア防御では、クラウドベースのサービスから添付ファイルのレピュテーション情報を取得します。

詳細については、「ファイル レピュテーション フィルタリングとファイル分析（585 ページ）」を参照してください。

アウトブレイク フィルタのイネーブル化

電子メールゲートウェイには、アウトブレイクフィルタの 30 日間評価キーが付属している場合があります。アウトブレイク フィルタは、従来のウイルス対策セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを隔離することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。

詳細については、アウトブレイク フィルタ （513 ページ）を参照してください。

[次へ（Next）] をクリックして続行します。

手順 5：レビュー

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

表示されている情報が要件を満たしていれば、[この設定をインストール（Install This Configuration）] をクリックします。

確認のダイアログが表示されます。[インストール（Install）] をクリックして、新しい設定をインストールします。

これで、 電子メールゲートウェイが電子メールを送信できる状態になりました。

（注） 電子メールゲートウェイへの接続に使用するインターフェイスの IP アドレスをデフォルトから変更した場合、[インストール（Install）] をクリックすると、現在の URL（http://192.168.42.42）への接続が失われます。ただし、ブラウザは、新しい IP アドレスにリダイレクトされます。

システム セットアップが完了すると、複数のアラート メッセージが送信されます。詳細については、即時アラート （65 ページ）を参照してください。

Active Directory への接続の設定

システムセットアップ ウィザードによって電子メールゲートウェイに設定が正しくインストールされると、Active Directory Wizard が表示されます。ネットワークで Active Directory サーバを稼働している場合は、Active Directory Wizard を使用して、Active Directory サーバ用の LDAP サーバプロファイルの設定と、受信者検証用リスナーの割り当てを行う必要があります。Active Directory を使用していないか、後で設定する場合は、[このステップをスキップ（Skip this Step）] をクリックします。Active Directory Wizard は、[システム管理（System Administration）] > [Active Directory ウィザード（Active Directory Wizard）] ページで実行できます。Active Directory およびその他の LDAP プロファイルは、[システム管理（System Administration）] > [LDAP] ページでも設定できます。

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

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

手順

ステップ 1 [Active Directoryウィザード（Active Directory Wizard）] ページで [Active Directoryウィザードを実行（Run Active Directory Wizard）] をクリックします。

ステップ 2 Active Directory サーバのホスト名を入力します。

ステップ 3 認証要求のためのユーザ名およびパスフレーズを入力します。

ステップ 4 [次へ（Next）] をクリックして続行します。

Active Directory サーバへの接続が Active Directory Wizard によってテストされます。成功すると、[ディレクトリ設定のテスト（Test Directory Settings）] ページが表示されます。

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

ステップ 6 [完了（Done）] をクリックします。

次の手順

Active Directory Wizard と連携するように 電子メールゲートウェイを正常に設定するか、処理をスキップすると、[システムセットアップの次のステップ（System Setup Next Steps）] ページが表示されます。

[システムセットアップの次のステップ（System Setup Next Steps）] ページのリンクをクリックして、 電子メールゲートウェイの設定を続行します。

コマンドライン インターフェイス（CLI）へのアクセス

CLI へのアクセスは、電子メールゲートウェイへの接続 （28 ページ）で選択した管理接続方式によって異なります。工場出荷時のデフォルト ユーザ名およびパスフレーズを次に示します。当初は、admin ユーザー アカウントだけが CLI にアクセスできます。admin アカウントを介してコマンドラインインターフェイスに初回アクセスしたうえで、さまざまな許可レベルの他のユーザを追加できます（ユーザの追加の詳細については、ユーザの追加 （1195 ページ）を参照してください）。システム セットアップ ウィザードで、admin アカウントのパスフレーズ

を変更するように要求されます。admin アカウントのパスフレーズは、`passphrase` コマンドを使用して、任意の時点で直接再設定することもできます。

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

シリアル接続を介して接続する場合は、パーソナル コンピュータのシリアル ケーブルが接続されている通信ポートを使用して端末セッションを開始します。電子メールゲートウェイへの接続 （28 ページ）に示されているシリアル ポートの設定値を使用してください。下記のユーザ名とパスフレーズを入力します。

ユーザ名およびパスフレーズを入力して 電子メールゲートウェイにログインします。

関連項目

- 工場出荷時のデフォルト ユーザ名とパスフレーズ （38 ページ）

工場出荷時のデフォルト ユーザ名とパスフレーズ

新しい仮想またはハードウェア電子メールゲートウェイをインストールする場合、完全なアクセス権を取得して電子メールゲートウェイを設定するために、デフォルトのパスフレーズを変更する必要があります。初めて電子メールゲートウェイにログインすると、Web インターフェイスによってデフォルトのパスフレーズを変更するように指示されます。デフォルトのパスフレーズを変更するまで、CLI で以下のコマンドへのアクセスが制限されます。

- Commit
- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense（仮想 電子メールゲートウェイ向け）
- ライセンス キー
- Ping
- Telnet
- netstat

- ユーザ名：**admin**
- パスフレーズ：**ironport**

例：

```
login: admin
passphrase: ironport
```

（注） セッションがタイムアウトした場合は、ユーザ名とパスフレーズの再入力が求められます。システム セットアップ ウィザードの実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。

コマンドライン インターフェイス（CLI）システム セットアップ ウィザードの実行

CLI バージョンのシステム セットアップ ウィザードの手順は、基本的に GUI バージョン同様ですが、次のわずかな例外があります。

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

システム セットアップ ウィザードを実行するには、コマンド プロンプトで `systemsetup` と入力します。

```
IronPort> systemsetup
```

システムを再設定するようシステム セットアップ ウィザードから警告が出されます。電子メール ゲートウェイをまったく初めて設置する場合か、既存の設定を完全に上書きする場合は、この質問に [はい（Yes）] と回答します。

```
WARNING: The system setup wizard will completely delete any existing

'listeners' and all associated settings including the 'Host Access Table' -
mail operations may be interrupted.


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

（注） 以降のシステム セットアップ手順については、次で説明します。CLI バージョンのシステム セットアップ ウィザード対話の例には、Web ベースのシステム セットアップ ウィザードを使用した基本設定の定義 （39 ページ）で説明した GUI バージョンのシステム セットアップ ウィザードから逸脱する部分だけを含めてあります。

関連項目

- admin パスフレーズの変更 （52 ページ）
- ライセンス契約書の受諾 （52 ページ）
- ホスト名の設定 （52 ページ）
- 論理 IP インターフェイスの割り当てと設定 （52 ページ）
- デフォルト ゲートウェイの指定 （54 ページ）
- Web インターフェイスのイネーブル化 （54 ページ）
- DNS の設定 （54 ページ）
- リスナーの作成 （54 ページ）
- アンチスパムのイネーブル化 （63 ページ）
- デフォルト アンチスパム スキャン エンジンの選択 （63 ページ）
- スパム隔離のイネーブル化 （63 ページ）
- アンチウイルス スキャンのイネーブル化 （63 ページ）
- アウトブレイクフィルタの有効化 （64 ページ）
- アラート設定値および AutoSupport の設定 （64 ページ）
- スケジュール済みレポートの設定 （64 ページ）
- 時刻設定値の設定 （64 ページ）
- 変更の確定 （65 ページ）
- 設定のテスト （65 ページ）
- 即時アラート （65 ページ）

admin パスフレーズの変更

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

ログインパスフレーズを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスフレーズも作成できます。

ライセンス契約書の受諾

表示されるソフトウェア ライセンス契約書を参照して受諾します。

ホスト名の設定

次に、電子メールゲートウェイの完全修飾ホスト名を定義します。この名前は、ネットワーク管理者が割り当てる必要があります。

論理 IP インターフェイスの割り当てと設定

次の手順では、Management（C390、および C690 アプライアンス）または Data 1（C190 アプライアンス）物理イーサネット インターフェイス上に論理 IP インターフェイスの割り当てと

設定を行います。続いて、電子メールゲートウェイ上で使用可能な他の任意の物理イーサネット インターフェイス上に論理 IP インターフェイスを設定するよう指示されます。

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

C390 および C690 アプライアンスの場合：物理イーサネットポートの 1 つは、インターネットに直接接続して、パブリックリスナー経由でインバウンド電子メールを受信するために使用し、もう 1 つの物理イーサネットポートは、内部ネットワークに直接接続して、プライベートリスナー経由でアウトバウンド電子メールをリレーするために使用することを推奨しています。

C190 アプライアンスの場合：デフォルトでは、`systemsetup` コマンドによって物理イーサネットポートが 1 つのリスナーに 1 つのみ設定され、インバウンド電子メールの受信とアウトバウンド電子メールのリレーの両方に対応します。

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

次の情報が必要です。

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

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

- ネットワーク管理者によって割り当てられた IP **アドレス**。これは、IPv4 アドレスまたは IPv6 アドレスにできます。1 つの IP インターフェイスに両方のタイプの IP アドレスを割り当てることができます。
- インターフェイスの**ネットマスク**。ネットマスクは、CIDR 形式である必要があります。たとえば、`255.255.255.0` サブネットでは `/24` を使用します。

（注） 同じサブネットに含まれる IP アドレスを、別々の物理イーサネットインターフェイスには設定できません。ネットワークおよび IP アドレスのコンフィギュレーションの詳細については、ネットワークと IP アドレスの割り当て （1581 ページ）を参照してください。

C190 アプライアンスの場合、Data 2 インターフェイスを最初に設定します。

デフォルト ゲートウェイの指定

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

Web インターフェイスのイネーブル化

`systemsetup` コマンドの次の部分で、 電子メールゲートウェイ（管理イーサネット インターフェイス）の Web インターフェイスを有効にします。Secure HTTP（https）を介して Web インターフェイスを実行することもできます。HTTPS を使用する場合は、独自の証明書をアップロードするまで、デモ証明書が使用されます。

DNS の設定

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

リスナーの作成

特定の IP インターフェイスに対して設定される、着信電子メール処理サービスを「リスナー」によって管理します。リスナーは、内部システムまたはインターネットのいずれかから電子メールゲートウェイに着信する電子メールだけに適用されます。Cisco AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーは、上記で指定した IP アドレス用に実行されている電子メール リスナーであると見なすことができます（「SMTP デーモン」と見なすことさえ可能）。

C390、および C690 アプライアンスの場合：デフォルトでは、`systemsetup` コマンドによって 2 個のリスナー（プライベート 1 つ、パブリック 1 つ）が設定されます。（使用可能なリスナータイプの詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください）。

C190アプライアンスの場合：デフォルトでは、インターネットからのメールの受信と内部ネットワークからの電子メールのリレーの両方に対応するパブリックリスナー 1 つが `systemsetup` コマンドによって設定されます。C190 アプライアンスのリスナーの例 （60 ページ）を参照してください。

リスナーを定義するときは、次の属性を指定します。

- 後でそのリスナーを参照するために作成した**名前**（ニックネーム）。たとえば、インターネットに配信される、内部システムからの電子メールを受け入れるリスナーには、OutboundMail などの名前を付けます。
- 電子メールの受信に使用する、`systemsetup` コマンドで先に作成したいずれかの IP インターフェイス。
- 電子メールのルーティング先にするマシンの名前（パブリック リスナーのみ）。（これは、最初の `smtproutes` エントリです。ローカル ドメインの電子メールのルーティング （853 ページ） を参照してください。）
- パブリックリスナーで IP レピュテーションスコアに基づくフィルタリングを有効にするかどうか。イネーブルにする場合は、[コンサーバティブ（Conservative）]、[適度（Moderate）]、または [アグレッシブ（Aggressive）] から設定値を選択することも指示されます。
- ホストごとのレート制限：1 時間あたりにリモート ホストから受信する受信者の最大数（パブリック リスナーのみ）。
- 受け入れる電子メールの宛先にされている受信者ドメインまたは特定のアドレス（パブリックリスナーの場合）、あるいは電子メールゲートウェイを介した電子メールのリレーを許可するシステム（プライベートリスナーの場合）。これらは、リスナーの受信者アクセス テーブルおよびホスト アクセス テーブルの最初のエントリです。詳細については、送信者グループの構文 （110 ページ）およびメッセージを受け入れるドメインおよびユーザの追加 （150 ページ）を参照してください。

関連項目

- パブリック リスナー （55 ページ）
- プライベート リスナー （58 ページ）
- C190 アプライアンスのリスナーの例 （60 ページ）

パブリック リスナー

（注） パブリックリスナーおよびプライベートリスナーを作成する次の例は、C390 および C690 アプライアンスのみに適用されます。C190 アプライアンスの場合は、C190 アプライアンスのリスナーの例 （60 ページ）の項までスキップしてください。

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

（注） 1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性がありますが、10,000 人規模の企業に対するすべての電子メールを処理する 電子メールゲートウェイを設定する場合は、単一のリモートホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業への着信電子メールのレート制限をイネーブルにする（量を絞る）場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、送信者グループの構文 （110 ページ）を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

```
You are now going to configure how the appliance accepts mail by

creating a "Listener".

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

[]> InboundMail


Please choose an IP interface for this Listener.

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

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

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

[1]> 3


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


Hostnames such as "example.com" are allowed.

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

Usernames such as "postmaster@" are allowed.

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

```
Separate multiple addresses with commas.

[]> example.com


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


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

[]> exchange.example.com


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


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

[]> 4500


Default Policy Parameters

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

Maximum Message Size: 100M

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

Maximum Number Of Messages Per Connection: 1,000

Maximum Number Of Recipients Per Message: 1,000

Maximum Number Of Recipients Per Hour: 4,500

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No
```

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


Listener InboundMail created.

Defaults have been set for a Public listener.

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

*****
```

プライベート リスナー

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

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

プライベート リスナーのデフォルト値は、先に作成したパブリック リスナーのデフォルト値と異なることに注意してください。詳細については、リスナーの使用 （82 ページ）を参照してください。

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


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

[]> OutboundMail


Please choose an IP interface for this Listener.

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

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

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

[1]> 2


Please specify the systems allowed to relay email through the appliance.

Hostnames such as "example.com" are allowed.
```

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

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

Separate multiple entries with commas.

[]> .example.com


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


Default Policy Parameters

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

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control:  No

Virus Detection Enabled:  Yes

Allow TLS Connections: No

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


Listener OutboundMAil created.

Defaults have been set for a Private listener.

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

*****
```

C190 アプライアンスのリスナーの例

（注） リスナーを作成する次の例は、C170 および C190 アプライアンスのみに適用されます。

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

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

（注） 1 台のリモート ホストから 1 時間あたりに受信する最大受信者数に入力する値は、完全に自由裁量の値です。通常は、管理対象の電子メールを所有している企業の規模に比例します。たとえば、1 時間に 200 通のメッセージを送信する送信者は、「スパム送信者」（未承諾の大量電子メールの送信者）である可能性がありますが、10,000 人規模の企業に対するすべての電子メールを処理する 電子メールゲートウェイを設定する場合は、単一のリモートホストからの 1 時間あたりのメッセージが 200 通であっても、理にかなった値である可能性があります。対照的に、50 人規模の会社の場合に、1 時間あたり 200 通のメッセージを送信してくる送信者は、おそらく、明らかなスパム送信者です。パブリック リスナーで、企業への着信電子メールのレート制限をイネーブルにする（量を絞る）場合は、適切な値を選択してください。デフォルトのホスト アクセス ポリシーの詳細については、送信者グループの構文 （110 ページ）を参照してください。

次に、リスナーのデフォルトのホスト アクセス ポリシーが受け入れられます。

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

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

[]> MailInterface


Please choose an IP interface for this Listener.

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

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

[1]> 1
```

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

Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
Separate multiple addresses with commas.
[]> example.com

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

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

Please specify the systems allowed to relay email through the appliance.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[]> .example.com

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

Enter the maximum number of recipients per hour to accept from a remote domain.
[]> 450
```

```
Default Policy Parameters

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

Maximum Message Size: 10M

Maximum Number Of Connections From A Single IP: 50

Maximum Number Of Messages Per Connection: 100

Maximum Number Of Recipients Per Message: 100

Maximum Number Of Recipients Per Hour: 450

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Spam Detection Enabled:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No

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


Listener MailInterface created.

Defaults have been set for a Public listener.

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

*****
```

（注） この systemsetup コマンドでは、C170 および C190 アプライアンスの受信メールと送信メール両方に対してリスナーを 1 つだけ設定するため、すべての発信メールがメール フロー モニタ機能（通常はインバウンド メッセージに使用）で評価されます。電子メール セキュリティ モニタの使用方法 （1009 ページ）を参照してください

アンチスパムのイネーブル化

電子メールゲートウェイには、Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。**systemsetup** コマンドのこの部分では、ライセンス契約書を受諾し、電子メールゲートウェイでグローバルに Anti-Spam をイネーブルにすることができます。

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

（注） ライセンス契約書を受諾しない場合、Anti-Spam は電子メールゲートウェイでイネーブルになりません。

電子メールゲートウェイで使用可能なすべての Anti-Spam 設定オプションについては、スパムおよびグレイメールの管理 （461 ページ）を参照してください。

デフォルト アンチスパム スキャン エンジンの選択

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

スパム隔離のイネーブル化

スパム対策サービスをイネーブルにした場合は、着信メール ポリシーをイネーブルにして、スパム メッセージおよび陽性と疑わしいスパム メッセージをローカル スパム隔離に送信できます。スパム隔離をイネーブルにすると、電子メールゲートウェイでエンドユーザ隔離もイネーブルになります。エンドユーザのアクセス権を設定していないうちは、管理者だけがエンドユーザ隔離を利用できます。

ローカルのスパム隔離の設定 （1154 ページ） を参照してください。

アンチウイルス スキャンのイネーブル化

電子メールゲートウェイには、ウイルススキャンエンジンの 30 日間評価キーが付属しています。`systemsetup` コマンドのこの部分では、1 つまたは複数のライセンス契約書を受諾し、 電子メールゲートウェイでウイルス対策スキャンをイネーブルにできます。 電子メールゲートウェイでイネーブルにするウイルス対策スキャンエンジンごとにライセンス契約書を受諾する必要があります。

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

電子メールゲートウェイで使用可能なウイルス対策設定オプションについては、アンチウイルス （439 ページ）を参照してください。

アウトブレイクフィルタの有効化

続くこの手順では、アウトブレイクフィルタを有効化するよう指示されます。電子メールゲートウェイには、アウトブレイクフィルタの 30 日間評価キーが付属しています。

関連項目

- アウトブレイク フィルタ （64 ページ）

アウトブレイク フィルタ

アウトブレイク フィルタは、従来のウイルス対策セキュリティ サービスが新しいウイルス シグニチャ ファイルで更新されるまで、疑わしいメッセージを隔離することで、新種ウイルスの発生に対する「第一の防衛ライン」になります。アウトブレイク フィルタをイネーブルにした場合は、デフォルト着信メール ポリシーでイネーブルになります。

アウトブレイク フィルタをイネーブルにする場合は、しきい値およびアウトブレイク フィルタ アラートを受信するかどうかを入力します。アウトブレイク フィルタおよびしきい値の詳細については、アウトブレイク フィルタ （513 ページ）を参照してください。

アラート設定値および AutoSupport の設定

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

AutoSupport 機能では、ご使用の電子メールゲートウェイに関する問題をシスコ カスタマー サポート チームが認識しておくことで、業界トップ水準のサポートを提供できます。サポート アラートと週ごとのステータス更新をシスコに送信するには、[はい（Yes）] と回答します詳細については、『*Cisco Secure Email Gateway Guide*』で、「*Distributing Administrative Tasks*」章の「*AutoSupport*」項を参照してください。

スケジュール済みレポートの設定

デフォルトの定期レポートの送信先にするアドレスを入力します。この値はブランクのままにしておくことができ、その場合、レポートは、電子メールで送信される代わりに、電子メールゲートウェイ上にアーカイブされます。

時刻設定値の設定

Cisco AsyncOS では、ネットワーク タイム プロトコル（NTP）を使用して、ネットワーク上またはインターネット上の他のサーバと時刻を同期するか、システム クロックを手動で設定することができます。電子メールゲートウェイ上の時間帯を設定して、メッセージヘッダーおよび

ログファイルのタイムスタンプを正確にする必要もあります。また、Cisco Systems タイムサーバを使用して電子メールゲートウェイ上の時刻を同期することもできます。

[大陸（Continent）]、[国（Country）]、および[タイムゾーン（Timezone）] を選択し、NTP を使用するかどうかと、使用する NTP サーバの名前を選択します。

変更の確定

最後に、手順全体で行った設定変更を確定するかどうかの確認が、システムセットアップ ウィザードから示されます。変更を確定する場合は、[はい（Yes）] と回答します。

システム セットアップ ウィザードを正常に完了すると、次のメッセージが表示されて、コマンド プロンプトが出されます。

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

mail3.example.com>
```

これで、 電子メールゲートウェイから電子メールを送信できる状態になりました。

設定のテスト

Cisco AsyncOS の設定をテストする際は、mailconfig コマンドを使用して、`systemsetup` コマンドで作成したばかりのシステム設定データを含むテスト電子メールをただちに送信できます。

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send

the configuration file. Separate multiple addresses with commas.

[]> user@example.com


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

mail3.example.com>
```

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

即時アラート

電子メールゲートウェイでは、ライセンス キーを使用して機能をイネーブルにします。`systemsetup` コマンドでリスナーを最初に作成した場合、Anti-Spam をイネーブルにした場合、Sophos または McAfee Anti-Virus をイネーブルにした場合、あるいはアウトブレイク フィルタをイネーブルにした場合は、アラートが生成されて、手順 2：システム （40 ページ）で指定したアドレスに送信されます。

キーの残り時間を定期的に通知するアラートです。次に例を示します。

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


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


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

30 日間の評価期間を超えて機能を有効にする場合は、シスコのセールス担当者にお問い合わせください。キーの残り時間は、[システム管理（System Administration）] > [ライセンスキー（Feature Keys）] ページからか、`featurekey` コマンドを発行することによって確認できます（詳細については、ライセンス キー （1231 ページ）を参照してください。）

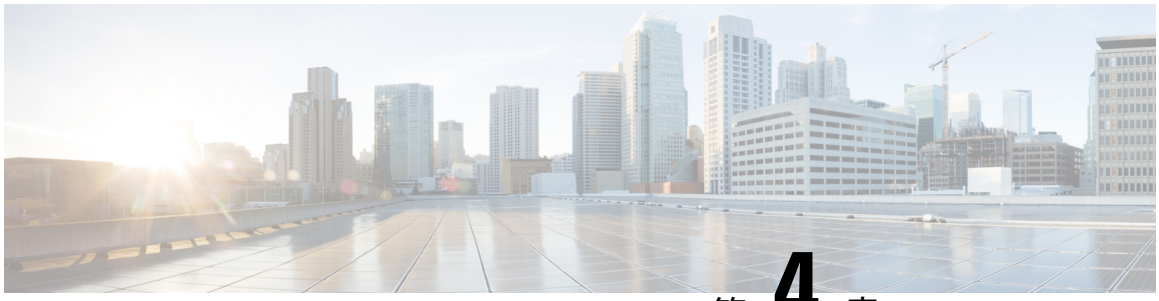
エンタープライズ ゲートウェイとしてシステムを設定

エンタープライズ ゲートウェイ（インターネットからの電子メールの受け入れ）としてシステムを設定する場合は、まずこの章を完了してから、詳細について電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

設定と次の手順の確認

システムセットアップが完了したため、電子メールゲートウェイによって電子メールが送信および受信されます。ウイルス対策、スパム対策、およびウイルス アウトブレイク フィルタ セキュリティ機能をイネーブルにした場合は、着信メールおよび発信メールでスパムおよびウイルスのスキャンも行われます。

次は、電子メールゲートウェイの設定をカスタマイズする方法を理解します。電子メール パイプラインについて （67 ページ） は、電子メールがシステムをルーティングされる方法を詳しく説明しています。各機能は、順次（上から下に）処理されます。各機能については、本書の残りの章で説明します。



第 4 章

電子メール パイプラインについて

この章は、次の項で構成されています。

- 電子メール パイプラインの概要 （67 ページ）
- 電子メール パイプラインのフロー （67 ページ）
- 着信および受信 （70 ページ）
- ワーク キューとルーティング （73 ページ）
- 配信 （77 ページ）

電子メール パイプラインの概要

電子メールパイプラインは電子メールゲートウェイで処理されるため、電子メールフローです。これには 3 フェーズあります。

- 受信：着信電子メールを受信するように電子メールゲートウェイはリモートホストに接続されるため、設定された制限やその他の受信ポリシーに従います。たとえば、ホストがユーザのメールを送信できることを確認し、受信接続とメッセージ制限を適用し、メッセージの受信者を検証します。
- ワークキュー：電子メールゲートウェイは着信および発信メールを処理し、フィルタリング、セーフリスト/ブロックリストスキャン、スパム対策およびウイルス対策スキャン、アウトブレイクフィルタ、隔離などを実行します。
- 配信：発信電子メールを送信するように電子メールゲートウェイは接続されるため、設定された配信制限とポリシーに従います。たとえば、発信接続制限を適用し、指定された配信不能メッセージを処理します。

電子メール パイプラインのフロー

次の図に、受信から配信へのルーティングまで、電子メールがシステムで処理される様子の概要を示します。各機能は順番に処理されます（上から下へ）。このパイプラインに含まれる機能の設定の大部分は、trace コマンドを使用してテストできます。

図 *6:* 電子メール パイプライン：電子メール接続の受信

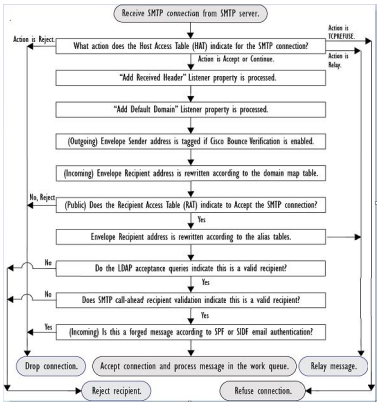


図 7:電子メール パイプライン - 作業キュー

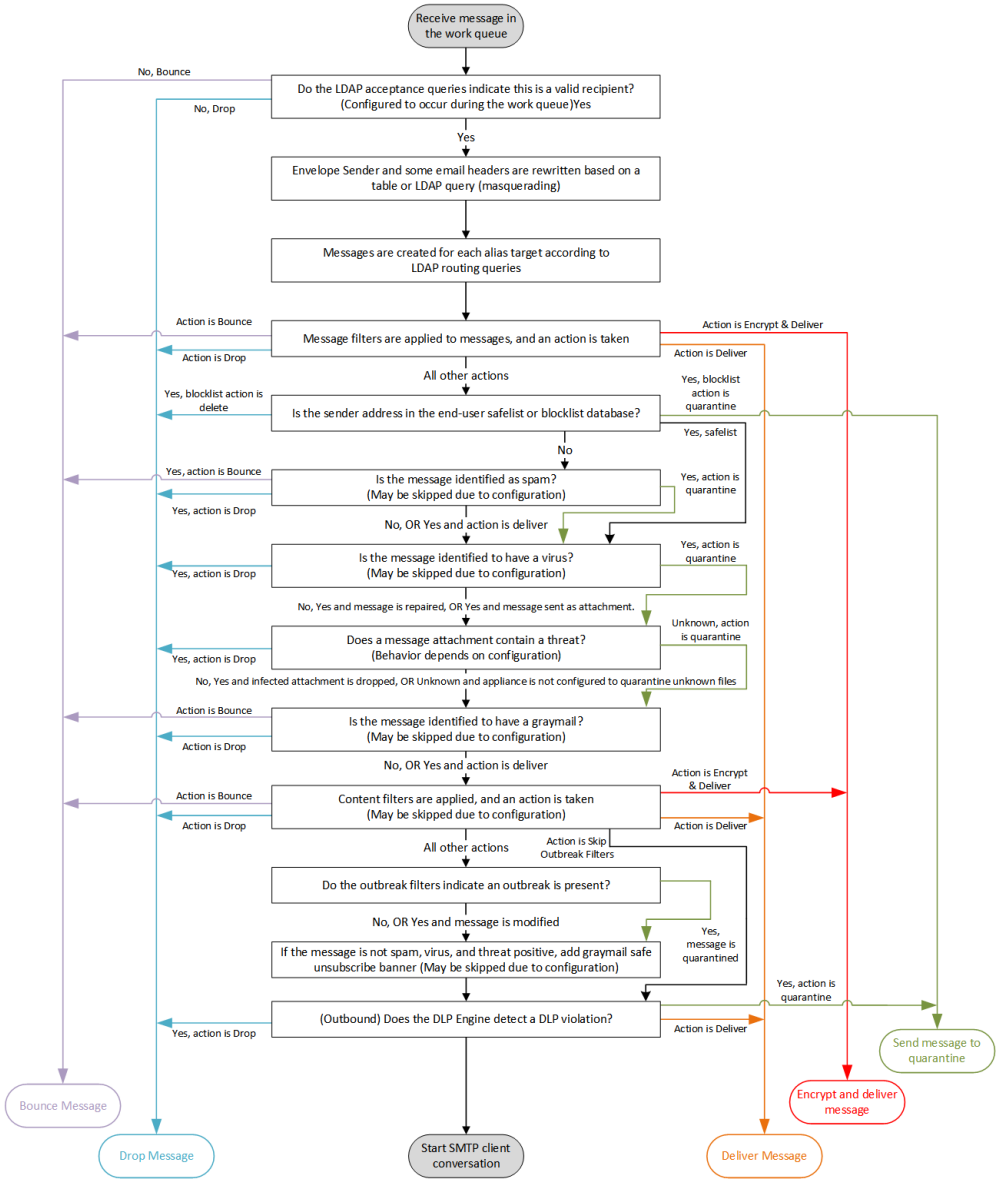
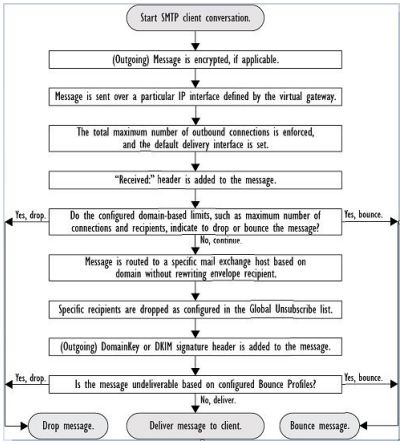


図 *8:* 電子メール パイプライン：電子メールの配信



着信および受信

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

関連項目

- ホスト アクセス テーブル（HAT）、送信者グループ、およびメール フロー ポリシー （70 ページ）
- Received: ヘッダー （71 ページ）
- デフォルト ドメイン （71 ページ）
- バウンス検証 （71 ページ）
- ドメイン マップ （72 ページ）
- 受信者アクセス テーブル（RAT） （72 ページ）
- エイリアス テーブル （72 ページ）
- LDAP 受信者の受け入れ （72 ページ）
- SMTP コールアヘッド受信者検証 （72 ページ）

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

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

送信者グループは、1つまたは複数の送信者をグループに関連付けるために使用されるもので、メッセージ フィルタおよびその他のメール フロー ポリシーを送信者グループに対して適用で

きます。メール フロー ポリシーは、一連の HAT パラメータ（アクセス ルール、レート制限パラメータ、およびカスタム SMTP コードと応答）を表現する 1 つの方法です。

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

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

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

送信者レピュテーション フィルタリングでは、IP レピュテーションサービスによって決定された送信者の信頼性に基づいて、電子メールの送信者を分類し、電子メールインフラストラクチャの利用を制限できます。

詳細については、定義済みの送信者グループとメール フロー ポリシーの理解 （118 ページ）を参照してください。

Received: ヘッダー

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

詳細については、リスナーの使用 （82 ページ）を参照してください。

デフォルト ドメイン

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

詳細については、リスナーの使用 （82 ページ）を参照してください。

バウンス検証

発信メールには特別なキーがタグ付けされます。これにより、そのメールがバウンスとして送り返された場合は、そのタグを認識したうえでメールが配信されます。詳細については、バウンス検証 （895 ページ）を参照してください。

ドメイン マップ

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

詳細については、ドメイン マップ機能 （878 ページ）を参照してください。

受信者アクセス テーブル（RAT）

着信電子メールに限っては、電子メールゲートウェイでメールを受け入れるすべてのローカルドメインのリストを、RAT によって指定できます。

詳細については、受信者のアドレスに基づく接続の許可または拒否の概要 （147 ページ）を参照してください。

エイリアス テーブル

エイリアステーブルを使用すると、1 人または複数の受信者にメッセージをリダイレクトできます。エイリアスはマッピング テーブルに格納されます。電子メールのエンベロープ受信者（Envelope To または RCPT TO とも呼ぶ）とエイリアス テーブルに定義されているエイリアスが一致すると、電子メールのエンベロープ受信者アドレスが書き換えられます。

エイリアステーブルの詳細については、エイリアステーブルの作成 （860 ページ）を参照してください。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メール アドレス（パブリック リスナー上）を SMTP カンバセーションまたはワークキュー内で処理する方法を定義できます。詳細については、リスナーの使用 （82 ページ）を参照してください。これにより、電子メールゲートウェイでは、独特な方法でディレクトリ獲得攻撃（DHAP）に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワークキューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。

詳細については、LDAP クエリに関する作業 （955 ページ）を参照してください。

SMTP コールアヘッド受信者検証

電子メールゲートウェイで SMTP コールアヘッド受信者検証を設定すると、電子メールゲートウェイは、SMTP サーバに「事前に電話して」受信者を検証する間、送信側の MTA との SMTP 通信を中断します。電子メールゲートウェイが SMTP サーバに問い合わせると、SMTP サーバの応答が電子メールゲートウェイに返されます。電子メールゲートウェイは SMTP 通信を再開し、送信側の MTA に応答を送信し、SMTP サーバの応答（および SMTP コールアヘッドプロファイルの設定）に基づいて接続を続行するかドロップします。

詳細については、「SMTP サーバを使用した受信者の検証 （819 ページ）」を参照してください。

ワーク キューとルーティング

ワーク キューでは、配信フェーズに移動される前の受信メッセージを処理します。処理には、マスカレード、ルーティング、フィルタリング、セーフリスト/ブロックリスト スキャン、アンチスパムおよびアンチウイルス スキャン、ファイル レピュテーションのスキャンと分析、アウトブレイク フィルタ、および隔離が含まれます。

（注） データ漏洩防止（DLP）スキャンは、発信メッセージだけで使用可能です。DLP メッセージ スキャンが実行されるワーク キュー内の位置については、メッセージ分裂 （314 ページ）を参照してください。

関連項目

- 電子メール パイプラインとセキュリティ サービス （73 ページ）
- LDAP 受信者の受け入れ （72 ページ）
- マスカレードまたは LDAP マスカレード （74 ページ）
- LDAP ルーティング （74 ページ）
- メッセージ フィルタ （75 ページ）
- 電子メール セキュリティ マネージャ（受信者単位のスキャン） （75 ページ）
- 隔離 （77 ページ）

電子メール パイプラインとセキュリティ サービス

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

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

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

この場合、アンチウイルス スキャンが再イネーブル化されているかどうかを問わず、隔離エリアから解放されるときにそのメッセージのアンチウイルス スキャンは行われません。ただし、メール ポリシーに基づいてアンチウイルス スキャンがバイパスされるメッセージの場合は、

隔離エリアからの解放時にアンチウイルス スキャンが行われる可能性があります。メッセージが隔離エリアにある間に、メール ポリシーの設定値が変更される可能性があるためです。たとえば、メール ポリシーによってメッセージがアンチウイルス スキャンをバイパスし、隔離されている場合に、隔離エリアからの解放以前にメール ポリシーが更新されて、アンチウイルス スキャンが組み込まれた場合、そのメッセージは、隔離エリアからの解放時にアンチウイルス スキャンが行われます。

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

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メール アドレス（パブリック リスナー上）を SMTP カンバセーションまたはワークキュー内で処理する方法を定義できます。詳細については、リスナーの使用 （82 ページ）を参照してください。これにより、電子メールゲートウェイでは、独特な方法でディレクトリ獲得攻撃（DHAP）に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワークキューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。

詳細については、LDAP クエリに関する作業 （955 ページ）を参照してください。

マスカレードまたは LDAP マスカレード

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

スタティック マッピング テーブルによるマスカレードの詳細については、マスカレードの構成 （868 ページ）を参照してください。

LDAP クエリーによるマスカレードの詳細については、LDAP クエリに関する作業 （955 ページ）を参照してください。

LDAP ルーティング

ネットワーク内の LDAP ディレクトリに格納されている情報に基づいてメッセージを適切なアドレスやメールホストへルーティングするように、電子メールゲートウェイを設定できます。

詳細については、LDAP クエリに関する作業 （955 ページ）を参照してください。

メッセージ フィルタ

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

詳細については、メッセージフィルタを使用した電子メール ポリシーの適用（155 ページ）を参照してください。

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

電子メール セキュリティ マネージャ（受信者単位のスキャン）

- セーフリスト/ブロックリスト スキャン （75 ページ）
- スパム対策 （75 ページ）
- アンチウイルス （76 ページ）
- グレイメールの検出と安全な購読解約 （76 ページ）
- ファイル レピュテーション スキャンおよびファイル分析 （76 ページ）
- コンテンツ フィルタ （76 ページ）
- アウトブレイク フィルタ （77 ページ）

セーフリスト/ブロックリスト スキャン

エンドユーザセーフリストおよびブロックリストは、エンドユーザによって作成されて、アンチスパム スキャンに先行して検査されるデータベースに格納されます。各エンドユーザは、常にスパムとして扱うか、決してスパムとして扱わないドメイン、サブドメイン、または電子メール アドレスを指定できます。送信者アドレスがエンドユーザ セーフリストに含まれている場合、アンチスパム スキャンはスキップされます。送信者アドレスがブロックリストに含まれている場合、メッセージは、管理者設定値に応じて隔離するかドロップすることができます。セーフリストおよびブロックリストの設定に関する詳細については、スパム隔離 （1153 ページ）を参照してください。

スパム対策

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

スパム対策スキャンはスパム隔離にメールを配信するように設定できます（オンボックスまたはオフボックス）。スパム隔離からリリースされるメッセージは電子メールパイプラインで処理する以降のワーク キューをとばし、宛先キューに直接進みます。

詳細については、スパムおよびグレイメールの管理 （461 ページ）を参照してください。

アンチウイルス

電子メールゲートウェイには、統合されたウイルススキャンエンジンが含まれています。「メールポリシー」ごとを基本に、メッセージおよび添付ファイルをスキャンしてウイルスを検出するように、電子メールゲートウェイを設定できます。ウイルスが検出された場合に次の処置を行うように電子メールゲートウェイを設定できます。

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

メッセージが隔離エリア（隔離 （77 ページ）を参照）から解放されると、ウイルスがスキャンされます。アンチウィルス スキャンの詳細については、アンチウイルス （439ページ）を参照してください。

グレイメールの検出と安全な購読解約

グレイメールメッセージを検出し、エンドユーザに代わって安全な購読解約を実行するように電子メールゲートウェイを設定できます。実行できるアクションは、アンチウイルス スキャンで実行できるアクションに似ています。

詳細については、スパムおよびグレイメールの管理 （461 ページ）を参照してください。

ファイル レピュテーション スキャンおよびファイル分析

メッセージの添付ファイルをスキャンし、新たな脅威や標的型の脅威が含まれているかどうかを確認するように、電子メールゲートウェイを設定できます。実行できるアクションは、アンチウイルス スキャンで実行できるアクションに似ています。

詳細については、「ファイル レピュテーション フィルタリングとファイル分析 （585ページ）」を参照してください。

コンテンツ フィルタ

受信者ごとまたは送信者ごとを基準に、メッセージに適用するコンテンツ フィルタを作成できます。コンテンツ フィルタは、電子メール パイプラインで後ほど適用される点、つまり、1つのメッセージが、各電子メール セキュリティ マネージャ ポリシーに対応する個々の複数のメッセージに「分裂」された後で適用される点を除いては、メッセージ フィルタとほぼ同じです。

コンテンツ フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。

コンテンツ フィルタの詳細については、コンテンツ フィルタ （325 ページ）を参照してください。

アウトブレイク フィルタ

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

Outbreak 隔離エリア内のメッセージは、他のすべての隔離エリア内のメッセージと同じように処理されます。隔離エリアおよびワーク キューの詳細については、隔離 （77 ページ）を参照してください。

詳細については、アウトブレイク フィルタ （513 ページ）を参照してください。

隔離

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

次のワーク キュー機能では、メッセージを隔離エリアに送信できます。

- スパム フィルタ
- メッセージ フィルタ
- ウイルス対策
- アウトブレイク フィルタ
- コンテンツ フィルタ
- ファイル分析（高度なマルウェア防御）

メッセージが隔離エリアから配信されると、脅威が再度スキャンされます。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離 （1129 ページ）
- スパム隔離 （1153 ページ）

配信

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

関連項目

- 仮想ゲートウェイ （78 ページ）
- 配信制限 （78 ページ）
- ドメインベースの制限値 （78 ページ）
- ドメインベースのルーティング （78 ページ）
- グローバル登録解除 （79 ページ）
- バウンス制限 （79 ページ）

仮想ゲートウェイ

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

詳細については、Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （912 ページ）を参照してください。

配信制限

配信時に使用する IP インターフェイスに基づく配信の制限および電子メールゲートウェイでアウトバウンドメッセージ配信に適用する最大同時接続数を設定するには、`deliveryconfig` コマンドを使用します。

詳細については、電子メール配信パラメータの設定 （909 ページ）を参照してください。

ドメインベースの制限値

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

詳細については、宛先制御による電子メール配信の管理 （894 ページ）を参照してください。

ドメインベースのルーティング

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

詳細については、ローカル ドメインの電子メールのルーティング （853 ページ）を参照してください。

グローバル登録解除

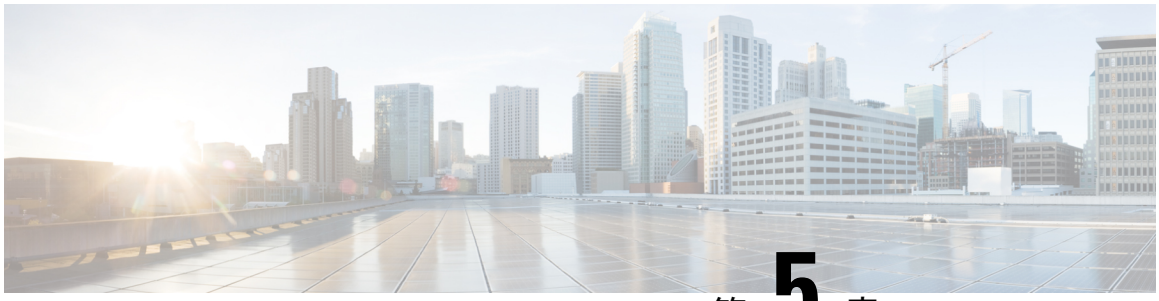
特定の受信者、受信者ドメイン、または IP アドレスに対する電子メールゲートウェイからのメッセージの配信を確実に停止するには、グローバル配信停止を使用します。グローバル配信停止をイネーブルにすると、すべての受信者アドレスが、グローバル配信停止対象のユーザ、ドメイン、電子メール アドレス、および IP アドレスのリストと照合されます。一致する電子メールは送信されません。

詳細については、グローバル配信停止機能の使用 （922 ページ）を参照してください。

バウンス制限

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

バウンス プロファイルの詳細については、バウンスした電子メールの処理 （884 ページ）を参照してください。



第 5 章

電子メールを受信するためのゲートウェイの設定

この章は、次の項で構成されています。

- 電子メールを受信するためのゲートウェイ設定の概要 （81 ページ）
- リスナーの使用 （82 ページ）
- リスナーのグローバル設定 （85 ページ）
- Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング （88 ページ）
- CLI を使用してリスナーを作成することによる接続要求のリスニング （95 ページ）
- エンタープライズ ゲートウェイ構成 （97 ページ）

電子メールを受信するためのゲートウェイ設定の概要

電子メールゲートウェイは、組織のゲートウェイとして機能し、電子メール接続の提供、メッセージの受け入れ、それらの適切なシステムへのリレーを行います。電子メールゲートウェイは、インターネットからユーザのネットワーク内の受信者ホストへ、ユーザのネットワーク内のシステムからインターネットに電子メール接続を提供できます。通常、電子メール接続要求は Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）を使用します。アプライアンスは、SMTP 接続をデフォルトで提供し、SMTP ゲートウェイとして機能し、ネットワークのメール エクスチェンジまたは「MX」とも呼ばれます。

電子メールゲートウェイは、着信 SMTP 接続要求を提供するためにリスナーを使用します。リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、インターネットまたはインターネットに到達しようとするユーザのネットワーク内のシステムから、アプライアンスに入る電子メールだけに適用されます。メッセージおよび接続が、メッセージを受け入れて受信者のホストにリレーするために満たす必要のある基準を、リスナーを使用して指定します。リスナーは、指定された各 IP アドレスを特定のポート上で実行する「SMTP デーモン」として見なすことができます。また、リスナーは電子メールゲートウェイが電子メールゲートウェイにメールを送信しようとするシステムと通信する方法を定義します。

次のタイプのリスナーを作成できます。

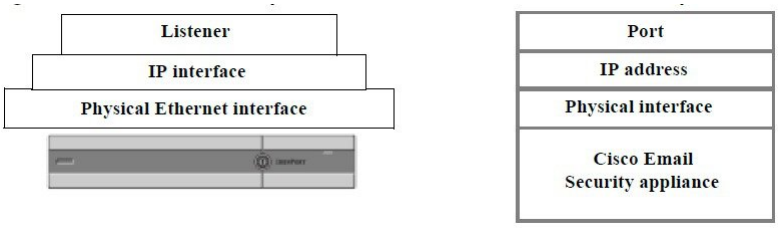
- **[パブリック（Public）]。**インターネットから着信するメール メッセージをリッスンし、受け入れます。パブリック リスナーは多数のホストからの接続を受信し、限られた数の受信者にメッセージを渡します。
- **[プライベート（Private）]。**ユーザのネットワーク内のシステムから（インターネット中でネットワークの外にいる受信者ではなく、通常内部グループウェアおよび電子メール サーバ（POP/IMAP）から）、電子メール メッセージをリッスンし、受け入れます。プライベート リスナーは、限られた（既知の）数のホストからの接続を受信し、多数の受信者にメッセージを渡します。

リスナーを作成するときは、次の情報も指定します。

- **リスナーのプロパティ。**すべてのリスナーに適用するグローバル プロパティおよび各リスナーに固有のプロパティを定義します。たとえば、リスナーに使用する IP インターフェイスおよびポート、そしてこれがパブリックまたはプライベートのリスナーのどちらかを指定することができます。この方法の詳細については、リスナーの使用 （82 ページ）を参照してください。
- **リスナーに接続が許可されているのはどのホストか。**リモート ホストからの着信接続を制御するルールを定義します。たとえば、リモート ホストを定義し、リスナーに接続できるかどうかを定義できます。この方法の詳細については、ホスト アクセス テーブルを使用した接続を許可するホストの定義 （107 ページ）を参照してください。
- **（パブリック リスナーのみ）リスナーがメッセージを受け入れるローカル ドメイン。**どの受信者がパブリック リスナーによって許可されるかを定義します。たとえば、組織で `currentcompany.com` ドメインを使用しているが、以前は `oldcompany.com` ドメインを使用していた場合は、currentcompany.com と `oldcompany.com` の両方のメッセージを受け入れることができます。この方法の詳細については、ドメイン名または受信者アドレスに基づく接続の許可または拒否 （147 ページ）を参照してください。

ホストアクセステーブルおよび受信者アクセステーブルを含むリスナーでの設定は、リスナーがSMTPカンバセーション中にSMTPサーバと通信する方法に影響します。これによって、接続が閉じる前に電子メールゲートウェイがスパムを送信するホストをブロックできます。

図 *9*: リスナー、*IP* インターフェイス、物理イーサネット インターフェイスの関係



リスナーの使用

GUI の [ネットワーク（Network）] > [リスナー（Listeners）] ページまたは CLI の listenerconfig コマンドを使用してリスナーを設定します。

すべてのリスナーに適用されるグローバル設定を定義できます。詳細については、リスナーのグローバル設定 （85 ページ）を参照してください。

電子メールゲートウェイでリスナーを使用および設定する場合は、次のルールとガイドラインに留意してください。

- 設定済みの IP インターフェイスごとに複数のリスナーを定義できますが、各リスナーは異なるポートを使用する必要があります。
- デフォルトでは、リスナーは電子メール接続を提供するためのメール プロトコルとして SMTP を使用します。ただし、Quick Mail Queuing Protocol（QMQP）を使用して電子メール接続を提供するようにアプライアンスを設定することもできます。これを行うには、`listenerconfig` CLI コマンドを使用します。
- リスナーは、インターネットプロトコルバージョン4（IPv4）およびバージョン6（IPv6）アドレスの両方をサポートします。単一のリスナーでどちらかのプロトコルバージョンまたは両方を使用できます。リスナーは、接続ホストとしてメール配信に同じプロトコルバージョンを使用します。たとえば、リスナーが IPv4 と IPv6 の両方に設定され、IPv6 を使用してホストに接続する場合、リスナーはIPv6 を使用します。ただし、リスナーが IPv6 アドレスのみの使用を設定されている場合は、IPv4 アドレスのみを使用するホストに接続できません。
- 少なくとも 1 つのリスナー（デフォルト値）がシステム セットアップ ウィザードの実行後に 電子メールゲートウェイ上に設定されます。ただし、リスナーを手動で作成する場合、AsyncOS ではこれらのデフォルト IP レピュテーションスコア値は使用されません。
- **C170 および C190** アプライアンス：システム セットアップ ウィザードでは、デフォルトで、インターネットからの電子メールの受信と内部ネットワークからの電子メールの中継の両方を行うための、1 つのパブリック リスナーを順を追って設定します。つまり、1 つのリスナーで両方の機能を実行できます。
- 電子メールゲートウェイのテストおよびトラブルシューティングに利用するために、パブリックまたはプライベートリスナーの代わりに、「シンクホール」タイプのリスナーを作成できます。シンクホールリスナーの作成時に、メッセージを削除する前にそのメッセージをディスクに書き込むかどうかを選択します。（詳細については、「テストとトラブルシューティング」の章を参照してください。）メッセージを削除する前にディスクに書き込むと、受信レートおよびキューの速度の測定に役立ちます。メッセージをディスクに書き込まないリスナーは、メッセージ生成システムからの純粋な受信レートの測定に役立ちます。このリスナーのタイプは、CLI の `listenerconfig` コマンドを使用した場合にだけ利用できます。

図：3つ以上のイーサネットインターフェイスを持つ電子メールゲートウェイモデル上のパブリックおよびプライベートリスナーは、3つ以上のイーサネットインターフェイスを持つ電子メールゲートウェイモデル上でシステム セットアップ ウィザードによって作成される、標準的な電子メールゲートウェイ構成を示しています。2 つのリスナーが作成されます。あるインターフェイス上でインバウンド接続を使用可能にするためのパブリック リスナーと、別の IP インターフェイス上でアウトバウンド接続を使用可能にするためのプライベート リスナーです。

図：2 つだけイーサネット インターフェイスを持つ 電子メールゲートウェイモデル上のパブリックリスナーは、イーサネット インターフェイスが 2 つだけの 電子メールゲートウェイモデル上でシステム セットアップ ウィザードによって作成される、標準的な電子メールゲート

ウェイ構成を示しています。インバウンド接続およびアウトバウンド接続の両方を提供するために、単一の IP インターフェイスで 1 つのリスナーが作成されます。

図 *10 : 3* つ以上のイーサネット インターフェイスを持つ電子メールゲートウェイモデル上のパブリックおよびプライベートリスナー

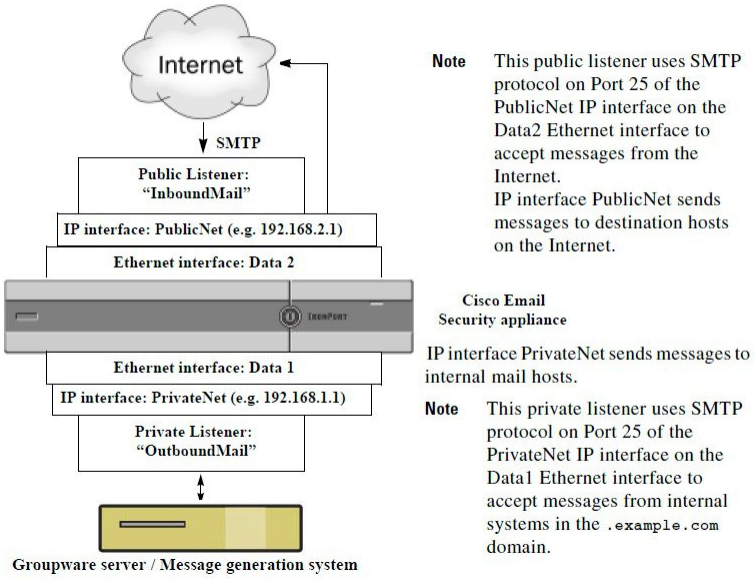
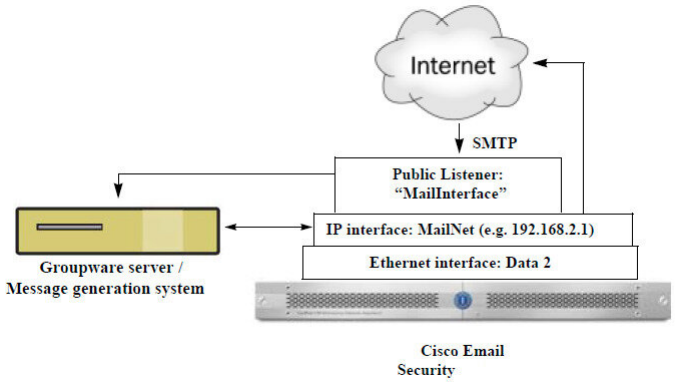


図 *11 : 2* つだけイーサネット インターフェイスを持つ電子メールゲートウェイモデル上のパブリックリスナー



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

リスナーのグローバル設定

リスナーのグローバル設定は、電子メールゲートウェイで設定されたすべてのリスナーに影響します。リスナーが、インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスの両方を持つインターフェイスを使用する場合、リスナーの設定は IPv4 および IPv6 トラフィックの両方に適用されます

手順

ステップ 1 [ネットワーク（Network）] > [リスナー（Listeners）] を選択します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 次の表に定義された設定を変更します。

表 *6*: リスナーのグローバル設定

グローバル設定	説明
最大同時接続数（Maximum Concurrent Connections）	リスナーに同時に接続できる最大数を設定します。C3x0 および C6x0 モデルのデフォルト値は 300 で、C1x0 モデルのデフォルト値は 50 です。リスナーが IPv4 と IPv6 の両方の接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 300 の場合、IPv4 および IPv6 接続の最大同時接続数が合計 300 を超えることはできません。
最大 TLS 同時接続数（Maximum Concurrent TLS Connections）	すべてのリスナーでの同時 TLS 接続の最大数を設定します。デフォルト値は 100 です。リスナーが IPv4 と IPv6 の両方の TLS 接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 100 の場合、IPv4 および IPv6 の TLS 接続の最大同時接続数が合計 100 を超えることはできません。
受信カウンタリセット時間（Injection Counters Reset Period）	インジェクション制御カウンタがリセットされた場合に調整できます。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に（たとえば、60 分間隔ではなく 15 分間隔で）リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。 現在のデフォルト値は 1 時間です。最小 1 分（60 秒）から最大 4 時間（14,400 秒）までの期間を指定できます。 インジェクション制御期間 （137 ページ）を参照してください。

グローバル設定	説明
受信接続のタイムアウトまでの待ち時間（Timeout Period for Unsuccessful Inbound Connections）	AsyncOS が失敗した着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 失敗した接続は SMTP カンバセーションとなり、正常なメッセージ インジェクションが発生することなく、SMTP コマンドまたは ESMTP コマンドが発行され続けます。指定したタイムアウトに達した場合は、次のエラーが送信され、接続が解除されます。 「421 Timed out waiting for successful message injection, disconnecting.」 正常なメッセージ インジェクションが発生するまで、接続に失敗したと見なされます。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 5 分です。
すべてのインバウンド接続の合計時間制限（Total Time Limit for All Inbound Connections）	AsyncOS が着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 この設定は、最大許容接続時間を適用することにより、システム リソースを保持するためのものです。この最大接続時間の約 80% が経過すると、次のメッセージが表示されます。 「421 Exceeded allowable connection time, disconnecting.」 電子メールゲートウェイは、接続が最大接続時間の 80% を超えると、接続がメッセージの途中で切断されることを防ぐために接続を切断しようとします。着信接続を最大接続時間の 80% に到達する期間開いている場合、発生する可能性がある問題です。時間制限を指定する場合、このしきい値に注意してください。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 15 分です。
件名の最大サイズ（Maximum size of subject）	件名のサイズが指定された制限内であるメッセージが承認され、その他のメッセージは拒否されます。この値を 0 に設定すると、制限は適用されません。

グローバル設定	説明
HAT 遅延拒否（HAT delayed rejections）	メッセージ受信者レベルでHAT拒否を実行するかどうかを設定します。デフォルトでは、HATによって拒否された接続はSMTPカンバセーションの開始時にバナー メッセージをともなって終了されます。 HAT「拒否」設定で電子メールが拒否されると、AsyncOS では SMTP カンバセーションの開始時ではなく、メッセージ受信者レベル（RCPT TO）で拒否を実行できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。たとえば、ブロックされたメッセージのアドレスおよび各受信者のアドレスからメールを表示できます。また、HAT 拒否の遅延によって、送信側 MTA が何度も再試行される可能性も小さくなります。 HAT 遅延拒否をイネーブルにすると、次の動作が発生します。 MAIL FROM コマンドが許可されるが、メッセージオブジェクトは作成されない。 電子メールの送信のためのアクセスが拒否されたというメッセージが表示され、すべての RCPT TO コマンドが拒否される。 SMTP AUTH を使用して送信側 MTA が認証される場合、RELAY ポリシーが許可され、メールを通常どおりに送信できる。 CLI の `listenerconfig --> setup` コマンドからのみ設定できます。

ステップ 4 変更を送信し、保存します。

次のタスク

関連項目

- 複数のエンコーディングが含まれるメッセージの設定 （87 ページ）

複数のエンコーディングが含まれるメッセージの設定

次のパラメータのメッセージのエンコード方式を変更する際の、電子メールゲートウェイの動作を定義できます。

- ヘッダー
- タグなしの ASCII 以外のヘッダー
- フッターまたはヘッダーのエンコード方式の不一致

この動作を設定するには、CLI で localeconfig コマンドを使用します。

（注） Web インターフェイスを使用してこの動作を設定することはできません。

CLI トランスクリプトのサンプルについては、免責事項スタンプと複数エンコード方式 （809 ページ）を参照してください。

Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング

手順

ステップ 1 [ネットワーク（Network）] > [リスナー（Listener）] を選択します。

ステップ 2 [リスナーを追加（Add Listener）] をクリックします。

ステップ 3 次の表に定義されている設定を設定します。

表 7: リスナー設定

名前	リスナーには、簡単に参照できるように一意の名前を付けてください。リスナー用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、複数のリスナーに同一の名前を付けることはできません。
リスナーのタイプ（Type of Listener）	次のリスナー タイプのいずれかを選択します。 • **[パブリック（Public）]**。パブリック リスナーには、インターネットから電子メールを受信するためのデフォルト特性が含まれます。 • **[プライベート（Private）]**。プライベート リスナーは、プライベート（内部）ネットワークで使用することを目的としています。
インターフェイス（Interface）	リスナーを作成する設定済み電子メールゲートウェイの IP インターフェイスおよび TCP ポートを選択します。インターフェイスで使用する IP アドレスのバージョンによって、リスナーは IPv4 アドレス、IPv6 アドレス、または両方のバージョンからの接続を受け入れます。デフォルトでは、SMTP ではポート 25 を使用し、QMQP ではポート 628 を使用します。
[バウンス プロファイル（Bounce Profile）]	バウンス プロファイルを選択します（CLI の `bounceconfig` コマンドを使用して作成されたバウンス プロファイルをリストから選択できます。新しいバウンス プロファイルの作成 （893 ページ）を参照）。

上記の免責条項（Disclaimer Above）	電子メールの上または下に添付する免責条項を選択します（[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページまたは CLI の `textconfig` コマンドで作成された文章をリストから選択できます。「テキスト リソース」の章を参照）。
下記の免責条項（Disclaimer Below）	電子メールの上または下に添付する免責条項を選択します（[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページまたは CLI の `textconfig` コマンドで作成された文章をリストから選択できます。「テキスト リソース」の章を参照）。
SMTP 認証プロファイル（SMTP Authentication Profile）	SMTP 認証プロファイルを指定します。
証明書	リスナーへの TLS 接続のための証明書を指定します（[ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の `certconfig` コマンドで追加された証明書をリストから選択できます。他の MTA との暗号化通信の概要 （829 ページ）を参照）。

ステップ 4 （任意）次の表で定義される SMTP「`MAIL FROM`」および「`RCPT TO`」コマンドでの解析の制御の設定を行います。

設定	説明
アドレス パーサー タイプ（Address Parser Type）	次のパーサータイプのいずれかを使用して、 電子メールゲートウェイが RFC2821 規格にどの程度厳密に準拠するかを選択します。 **Strict モード**： • Strict モードは RFC 2821 に準拠します。Strict モードでは、アドレス解析が RFC 2821 の規格に準拠しますが、次の例外および追加機能があります。 • 「MAIL FROM：<joe@example.com>」のように、コロンの後にスペースを挿入できます。 • ドメイン名に下線を使用できます。 • 「MAIL FROM」コマンドおよび「RCPT TO」コマンドでは、大文字と小文字が区別されます。 • ピリオドは特殊な用途に使用できません（たとえば、RFC 2821 では「J.D.」のようなユーザ名を作成できません）。 以下の追加オプションの一部は、イネーブルにできますが、そうすると、RFC 2821 に技術的に違反します。 **Loose モード**： Loose 解析は基本的に AsyncOS の以前のバージョンからの既存の動作です。電子メール アドレスの「検索」を最優先し、次のことを行います。 • コメントの無視。ネストされたコメント（カッコで囲まれている）がサポートされ、それらは無視されます。 • 「RCPT TO」コマンドおよび「MAIL FROM」コマンドで指定された電子メール アドレスの前後には山カッコが不要です。 • 複数のネストされた山カッコを使用できます（最も深いネスト レベルの電子メール アドレスが検索される）。
8 ビットユーザ名を許可（Allow 8-bit User Names）	イネーブルにすると、（エスケープ処理なしで）アドレスのユーザ名部分に 8 ビットの文字を使用できます。
8 ビットドメイン名を許可（Allow 8-bit Domain Names）	イネーブルにすると、アドレスのドメイン部分に 8 ビットの文字を使用できます。

設定	説明
部分ドメインを許可（Allow Partial Domains）	イネーブルにすると、部分ドメインを使用できます。部分ドメインは完全なドメインではなく、ドットなしのドメインです。 次のアドレスは、部分ドメインの例です。 • foo • foo@ • foo@bar デフォルトのドメイン機能を正常に動作させるために、このオプションをイネーブルにする必要があります。 [デフォルトドメインを追加（Add Default Domain）]：完全修飾ドメイン名ではなく、デフォルトのドメインを電子メール アドレスに使用します。[SMTPアドレス解析オプション（SMTP Address Parsing options）] で [部分ドメインを許可（Allow Partial Domains）] がイネーブルになっていない限り、このオプションはディセーブルです。これは「デフォルト送信者ドメイン」を送信者のアドレスおよび完全修飾ドメイン名を含まない受信者のアドレスに追加することによって、リスナーがリレーする電子メールを変更する方法に影響します（言い換えると、リスナーの「そのままの」アドレスの処理方法をカスタマイズできます）。 従来のシステムで、送信者アドレスに企業のドメインを追加（付加）せずに電子メールを送信する場合、これを使用してデフォルトの送信者ドメインを追加できます。たとえば、従来のシステムでは電子メールの送信者として自動的に文字列「joe」のみが入力された電子メールが作成されます。デフォルトの送信者ドメインを変更すると、「@yourdomain.com」が「joe」に付加され、完全修飾送信者名 joe@yourdomain.com が作成されます。
ソース ルーティング（Source Routing）	「MAIL FROM」アドレスおよび「RCPT TO」アドレスで送信元ルーティングが検出された場合の動作を決定します。送信元ルーティングは、複数の「@」文字を使用してルーティングを指定する、電子メール アドレスの特殊な形式です（例：@one.dom@two.dom:joe@three.dom）。「reject」を設定すると、アドレスは拒否されます。「strip」を設定すると、アドレスの送信元ルーティング部分が削除され、メッセージが通常どおり挿入されます。

設定	説明
不明なアドレス文字（Unknown Address Literals）	システムで処理できないアドレス リテラルを受信したときの動作を決定します。現在は、IPv4 以外のすべてです。そのため、たとえばIPv6 アドレス リテラルの場合、プロトコル レベルで拒否するか、受信後すぐにハードバウンスを行うことができます。 リテラルが含まれる受信者アドレスは即時ハード バウンスの原因となります。送信者アドレスは配信される場合があります。メッセージを配信できない場合、ハードバウンスがハードバウンスされます（二重ハードバウンス）。 拒否された場合、送信者と受信者のアドレスがプロトコル レベルですぐに拒否されます。
ユーザ名で次の文字を拒否（Reject These Characters in User Names）	文字（たとえば、% や !）を含むユーザ名を入力すると、拒否されます。

ステップ 5 （任意）次の表に定義されているリスナーの動作をカスタマイズするための高度な設定を設定します。

設定	説明
最大同時接続数（Maximum Concurrent Connections）	許可される最大接続数。
TCPリッスン用キューサイズ（TCP Listen Queue Size）	SMTP サーバが受け入れる前に AsyncOS で管理される接続のバックログ。
CR と LF の取り扱い（CR and LF Handling）	そのままの CR（復帰）文字および LF（改行）文字を含むメッセージの処理方法を選択します。 • **[正常（Clean）]**。メッセージを許可しますが、そのままの CR 文字および LF 文字を CRLF 文字に変換します。 • **[拒否（Reject）]**。メッセージを拒否します。 • **[許可（Allow）]**。メッセージを許可します。

設定	説明
Receivedヘッダーを追加（Add Received Header）	すべての受信メールにReceived:ヘッダーを追加します。また、リスナーは各メッセージにReceived:ヘッダーを追加してリレーする電子メールを変更します。Received:ヘッダーが含まれないようにするには、このオプションを使用してディセーブルにします。 （注） Received:ヘッダーは、ワーク キューの処理ではメッセージに追加されません。このヘッダーは配信のためにメッセージがキューから出たときに追加されます Received:ヘッダーをディセーブルにすると、インフラストラクチャの外部に送信されるすべてのメッセージで内部サーバのIPアドレスまたはホスト名が表示されることによって、ネットワークのトポロジが公開されないようにすることができます。Received:ヘッダーをディセーブルにする際には注意が必要です。
SenderBase IPプロファイルを使用（Use SenderBase IP Profiling）	[SenderBase IPプロファイルを使用（SenderBase IP Profiling）] をイネーブルにするかどうかを選択し、次のように設定を行います。 • **[接続ごとのSenderBaseタイムアウト（SenderBase Timeout per Connection）]**。SMTP接続ごとのSenderBase情報をアプライアンスがどのくらいの期間キャッシュするかを定義します。

ステップ 6 （任意）次の表に定義されているこのリスナーに関連付けられたLDAPクエリーを制御する設定を行います。

リスナーのLDAPクエリーをイネーブルにするには、次の設定を使用します。このオプションを使用する前に、LDAPクエリーを作成しておく必要があります。クエリーの各タイプには、設定するための個別のサブセクションがあります。クエリーのタイプをクリックしてサブセクションを展開します。

LDAP クエリー作成の詳細については、LDAP クエリ （943 ページ）を参照してください。

クエリーのタイプ	説明
アクセプト クエリ	アクセプト クエリの場合は、使用するクエリをリストから選択します。LDAP アクセプトをワーク キューの処理中に実行するか、SMTP カンバセーションで実行するかを指定できます。 ワーク キューの処理中に LDAP アクセプトを実行する場合、一致しない受信者に対する動作として、バウンスまたはドロップに指定します。 SMTP カンバセーションで LDAP アクセプトを実行する場合、LDAP サーバに到達できない場合にメールを処理する方法を指定します。メッセージを許可するか、コードとカスタム応答で接続をドロップするかを選択できます。最後に、SMTP カンバセーションで Directory Harvest Attack Prevention（DHAP;ディレクトリ獲得攻撃防止）のしきい値に達した場合に接続をドロップするかどうかを選択します。 SMTP カンバセーションで受信者の検証を行うと、複数の LDAP クエリー間の遅延を低減できます。したがって、対話形式の LDAP アクセプトをイネーブルにした場合、ディレクトリ サーバの負荷が増大することに注意してください。 詳細については、LDAP クエリの概要（943 ページ）を参照してください。
ルーティング クエリ	ルーティング クエリーの場合は、リストからクエリーを選択します。詳細については、LDAP クエリの概要（943 ページ）を参照してください。
クエリのマスカレード	マスカレード クエリーの場合は、リストからクエリーを選択して、From または CC ヘッダー アドレスといった、マスカレードするアドレスを選択します。 詳細については、LDAP クエリの概要（943 ページ）を参照してください。
グループ クエリ	グループ クエリーの場合は、リストからクエリーを選択します。詳細については、LDAP クエリの概要（943 ページ）を参照してください。

ステップ 7 変更を送信し、保存します。

次のタスク

関連項目

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM（95 ページ）

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

エンベロープ送信者検証をイネーブルにした場合、またはリスナーのSMTPアドレス解析オプションで部分ドメインの許可をディセーブルにした場合、リスナーのデフォルトドメイン設定が使用されなくなります。

これらの機能は互いに排他的です。

CLIを使用してリスナーを作成することによる接続要求のリスニング

次の表に、リスナーの作成および編集に関連するタスクに使用するlistenerconfigサブコマンドの一部を示します。

表 *8*: リスナーを作成するタスク

リスナーを作成するタスク	コマンドおよびサブコマンド
新しいリスナーの作成	`listenerconfig -> new`
リスナーのグローバル設定の編集	`listenerconfig -> setup`
リスナーのバウンス プロファイルの指定	`bounceconfig, listenerconfig-> edit -> bounceconfig`
リスナーへの免責条項の関連付け	`textconfig, listenerconfig -> edit -> setup -> footer`
SMTP 認証の設定	`smtpauthconfig, listenerconfig -> smtpauth`
SMTP アドレス解析の設定	`textconfig, listenerconfig -> edit -> setup -> address`
リスナーのデフォルト ドメインの設定	`listenerconfig -> edit -> setup -> defaultdomain`
Received: ヘッダーの電子メールへの追加	`listenerconfig -> edit -> setup -> received`
そのままの CR および LF 文字の CRLF への変更	`listenerconfig -> edit -> setup -> cleansmtp`
ホスト アクセス テーブルの修正	`listenerconfig -> edit -> hostaccess`
ローカル ドメインまたは特定のユーザ（RAT）への電子メールの受け入れ（パブリック リスナーのみ）	`listenerconfig -> edit -> rcptaccess`

リスナーを作成するタスク	コマンドおよびサブコマンド
リスナーの暗号化カンバセーション（TLS）	`certconfig, listenerconfig -> edit`
証明書の選択（TLS）	`listenerconfig -> edit -> certificate`

listenerconfig コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

電子メールのルーティングおよび配信設定の詳細については、ルーティングおよび配信機能の設定 （853 ページ）を参照してください。

関連項目

HAT の詳細パラメータ （96 ページ）

HAT の詳細パラメータ

次の表では、HAT 詳細パラメータの構文を定義しています。以下の数値については、後ろに **k** を追加してキロバイトを表すか、後ろに **M** を追加してメガバイトを表すことができます。文字のない値はバイトと見なされます。アスタリスクが付いたパラメータは、次の表に示す変数構文をサポートしています。

表 *9 : HAT* 詳細パラメータの構文

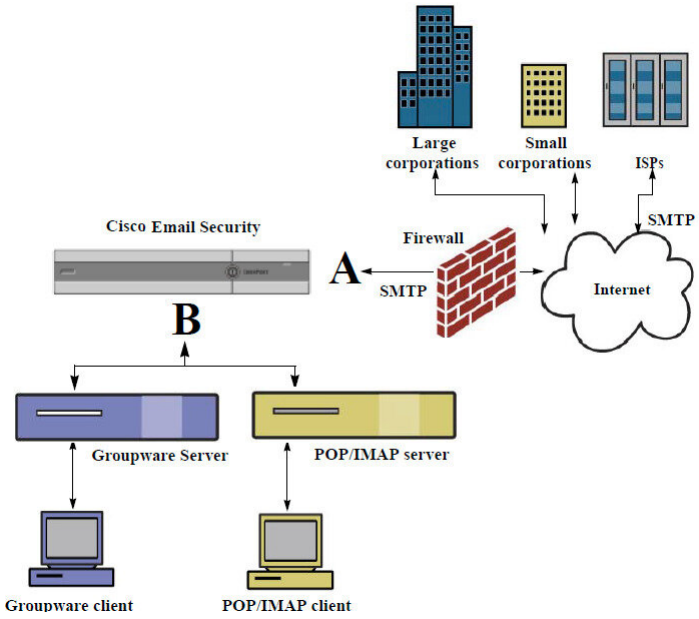
パラメータ	構文	値	値の例
接続あたりの最大メッセージ数	`max_msgs_per_session`	番号	`1000`
メッセージあたりの最大受信者数	`max_rcpts_per_msg`	番号	`10000` `1k`
最大メッセージ サイズ	`max_message_size`	番号	`1048576` `20M`
このリスナーに許可された最大同時接続数	`max_concurrency`	番号	`1000`
SMTP バナー コード	`smtp_banner_code`	番号	`220`
SMTP バナー テキスト（*）	`smtp_banner_text`	文字列	`Accepted`
SMTP 拒否バナー コード	`smtp_banner_code`	番号	`550`

パラメータ	構文	値	値の例
SMTP 拒否バナー テキスト（*）	`smtp_banner_text`	文字列	`Rejected`
SMTPバナーホスト名を上書き	`use_override_hostname`	on | off | default	`default`
	`override_hostname`	文字列	`newhostname`
TLS を使用	`tls`	on | off | required	`on`
スパム対策スキャンの使用	`spam_check`	on | off	`off`
ウイルス スキャンの使用	`virus_check`	on | off	`off`
1時間あたりの最大受信者数	`max_rcpts_per_hour`	番号	`5k`
1時間あたりのエラーコードの最大受信者数	`max_rcpts_per_hour_code`	番号	`452`
1時間あたりのテキストの最大受信者数（*）	`max_rcpts_per_hour_text`	文字列	`Too manyrecipients`
SenderBase の使用	`use_sb`	on | off	`on`
IP レピュテーションスコアの定義	`sbrs[`*`value1`*`:`*`value2`*`]`	-10.0 ～ 10.0	`sbrs[-10:-7.5]`
ディレクトリ獲得攻撃防止：1時間あたりの最大無効受信大数	`dhap_limit`	番号	`150`

エンタープライズ ゲートウェイ構成

この設定では、エンタープライズ ゲートウェイの設定はインターネットからメールを受け取り、グループウェア サーバ、POP/IMAP サーバまたは他の MTA に電子メールをリレーします。エンタープライズ ゲートウェイは、それと同時に、グループウェア サーバおよびその他の電子メール サーバからの SMTP メッセージを受け付け、インターネット上の受信者に中継します。

図 *12 :* エンタープライズ ゲートウェイのパブリック リスナーとプライベート リスナー

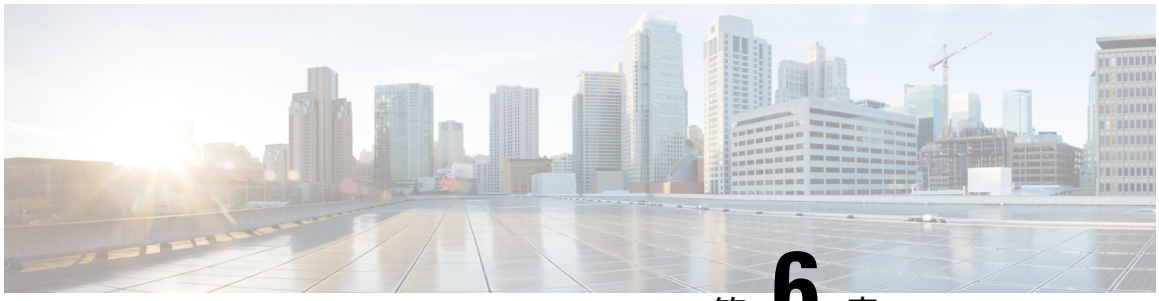


この設定では、少なくとも 2 つのリスナーが必要です。

- インターネットからのメールだけを受け入れるように設定されたリスナー 1 つ
- 内部グループウェアおよび電子メール サーバ（POP/IMAP）からのメールだけを受け入れるように設定されたリスナー 1 つ

異なるパブリック ネットワークとプライベート ネットワーク用に個別のパブリック リスナーとプライベート リスナーを作成することで、セキュリティ、ポリシー強制、レポーティング、管理用に電子メールを区別できます。たとえば、パブリック リスナーで受信した電子メールは、設定されたスパム対策エンジンおよびウイルス対策スキャンエンジンによってデフォルトでスキャンされますが、プライベート リスナーで受信される電子メールはスキャンされません。

図：エンタープライズ ゲートウェイのパブリックリスナーとプライベートリスナーは、このエンタープライズ ゲートウェイ構成の電子メールゲートウェイで構成されている 1 つのパブリック リスナー（A）と 1 つのプライベートリスナー（B）を示しています。



第 6 章

IP レピュテーション フィルタリング

この章は、次の項で構成されています。

- 送信者 IP レピュテーション フィルタリングの概要 （99 ページ）
- IP レピュテーションサービス （99 ページ）
- リスナーの IP レピュテーション フィルタリング スコアのしきい値の編集 （102 ページ）
- メッセージサブジェクトへの低 IP レピュテーションスコアの入力 （105 ページ）

送信者 IP レピュテーション フィルタリングの概要

送信者 IP レピュテーション フィルタリングは、スパム対策の最初のレイヤです。の送信者 IP レピュテーションサービスにより決定される送信者の信頼性に基づいて、電子メールゲートウェイ経由で送信されるメッセージを制御できます。

電子メールゲートウェイは、既知または信頼性の高い送信者、つまりお客様やパートナーなどからのメッセージを受け取り、コンテンツスキャンを一切実施しないでエンドユーザに直接配信できます。未知または信頼性の低い送信者からのメッセージは、アンチスパムおよびアンチウイルス スキャンなどのコンテンツ スキャンの対象にできます。また、各送信者から受け入れるメッセージの数をスロットリングすることもできます。信頼性の最も低い電子メール送信者に対しては、設定に基づいて接続を拒否したり、その送信者からのメッセージを送り返したりできます。

（注） ファイル レピュテーション フィルタリングは別のサービスです。詳細については、ファイル レピュテーション フィルタリングとファイル分析 （585 ページ）を参照してください。

IP レピュテーションサービス

Talos 関係会社のネットワークからのグローバルデータを使用する IP レピュテーションサービスは、クレーム率、メッセージ量の統計情報、および公開ブロックリストやオープンプロキシリストからのデータに基づいて、電子メール送信者に IP レピュテーションスコア（IPRS）を

割り当てます。IP レピュテーションスコアは、正当な送信者とスパム発信元を区別する際に役立ちます。レピュテーション スコアの低い送信者からのメッセージをブロックするしきい値を指定することも可能です。

Talos セキュリティネットワーク Web サイト（https://talosintelligence.com）では、最新の電子メールおよび Web ベースのグローバルな脅威の概要を提供し、現在の電子メールトラフィック量を国別に表示します。また、IP アドレス、URI、またはドメインに基づいてレピュテーションスコアを検索できます。

関連項目

- IP レピュテーションスコア （100 ページ）
- 送信者 IP レピュテーションフィルタの仕組み （101 ページ）
- さまざまな送信者 IP レピュテーション フィルタリング手法の推奨設定 （102 ページ）
- アウトブレイク フィルタ （513 ページ）
- 電子メール セキュリティ モニタの使用方法 （1009 ページ）

IP レピュテーションスコア

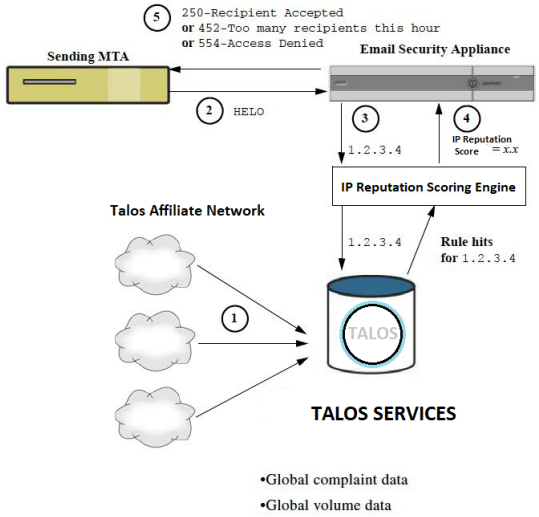
IP レピュテーションスコアは、IP レピュテーションサービスからの情報に基づいて、IP アドレスに割り当てられる数値です。IP レピュテーションサービスは、25 個を超える公開ブロックリストおよびオープンプロキシリストのデータを集約し、さらにこのデータを Talos のグローバルデータと組み合わせて、次のように -10.0 ～ +10.0 のスコアを割り当てます。

スコア（Score）	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い

スコアが低いほど、メッセージがスパムである可能性は高くなります。スコアが -10.0 であれば、そのメッセージはスパムであると「保証」されていることを意味し、スコアが 10.0 であれば、そのメッセージは正規であると「保証」されていることを意味します。

IP レピュテーションスコアを使用して、信頼性に基づいてメールフローポリシーを送信者に適用するように電子メールゲートウェイを設定します。メッセージフィルタを作成して IP レピュテーションスコアに「しきい値」を指定し、システムで処理されるメッセージにさらにアクションを実行できます詳細については、IP レピュテーションルール（202 ページ）およびアンチスパム システムのバイパス アクション （253 ページ）を参照してください）。

図 *13* : *IP* レピュテーションサービス



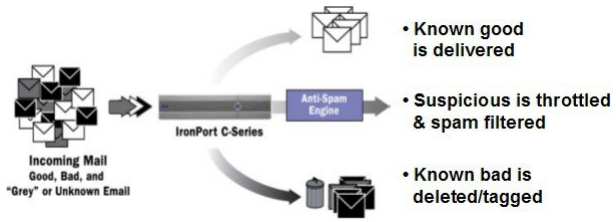
1. Talos 関連会社から、リアルタイムのグローバル データを送信します。
2. 送信側 MTA により、 電子メールゲートウェイとの接続が開始されます。
3. 電子メールゲートウェイにより、接続 IP アドレスのグローバルデータがチェックされます。
4. IP レピュテーションサービスにより、このメッセージがスパムである可能性が計算され、IP レピュテーションスコアが割り当てられます。
5. シスコにより、IP レピュテーションスコアに基づいて応答が返されます。

送信者 IP レピュテーションフィルタの仕組み

送信者 IP レピュテーション フィルタ テクノロジーは、電子メールゲートウェイに搭載されているその他のセキュリティサービスの処理から、できる限り多くのメールを切り離すことを目的としています。（電子メール パイプラインについて （67 ページ） を参照。）

送信者レピュテーションフィルタリングがイネーブルになっている場合は、既知の悪質な送信者からのメールだけが拒否されます。世界中の 2000 社から送信された既知の良好なメールは自動的にスパム フィルタを避けてルーティングされるため、誤検出の可能性が低減されます。未知、または「灰色」の電子メールは、アンチスパム スキャン エンジンにルーティングされます。送信者 IP レピュテーションフィルタは、この方法を使用して、コンテンツフィルタにかかる負荷を最大 50 % 低減できます。

図 *14* : 送信者 *IP* レピュテーション フィルタリングの例



さまざまな送信者 IP レピュテーション フィルタリング手法の推奨設定

企業の目的に応じて、Conservative、Moderate、Aggressive のいずれかの方法を選択できます。

アプローチ	特性	Allowed _List	Blocked_ List	SUSPECTLIST	UNKNOWNLIST
		送信者 IP レピュテーションスコア範囲：			
Conservative	誤検出はほぼ 0。良好なパフォーマンス。	7 ～ 10	-10 ～ -4	-4 ～ -2	-2 ～ 7
Moderate（インストール時のデフォルト）	誤検出は非常に少ない。高パフォーマンス。	送信者 IP レピュテーションスコアは使用されません。	-10 ～ -3	-3 ～ -1	-1 ～ +10
アグレッシブ	誤検出はいくらか発生。パフォーマンスは最大。 このオプションは、ほとんどのメールをアンチスパム処理から切り離します。	4 ～ 10	-10 ～ -2	-2 ～ -1	-1 ～ 4
すべての方式		メール フロー ポリシー：			
		信頼できる	ブロック	スロットル	承認（Accepted）

リスナーの IP レピュテーション フィルタリング スコアのしきい値の編集

デフォルトの IP レピュテーションサービススコアのしきい値を変更またはレピュテーション フィルタリングに送信者グループを追加する場合は、この手順を使用します。

（注） IP レピュテーションスコアのしきい値に関連するその他の設定およびメールフローポリシーの設定については、ホスト アクセス テーブルを使用した接続を許可するホストの定義 （107 ページ）に記載されています。

はじめる前に

- 電子メールゲートウェイがローカル MX/MTA から電子メールを受信するように設定されている場合は、送信者の IP アドレスをマスクする可能性のあるアップストリームホストを特定してください。詳細については、着信リレー構成における送信者の IP アドレスの決定 （497 ページ）を参照してください。
- IP レピュテーションスコアについて理解します。IP レピュテーションスコアを使用した送信者グループの定義 （113 ページ）を参照してください。
- 組織のフィルタリング方法を選択し、このアプローチの推奨設定を確認します。さまざまな送信者 IP レピュテーション フィルタリング手法の推奨設定 （102 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] を選択します。

ステップ 2 [送信者グループ（リスナー）（Sender Groups (Listener)）] メニューからパブリック リスナーを選択します。

ステップ 3 送信者グループのリンクをクリックします。

たとえば、「SUSPECTLIST」のリンクをクリックします。

ステップ 4 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 5 送信者グループの IP レピュテーションスコアの範囲を入力します。

たとえば、「ALLOWED_LIST」に 7.0 ～ 10 の範囲を入力します。

ステップ 6 **[送信（Submit）]** をクリックします。

ステップ 7 必要に応じてこのリスナーの各送信者グループに対し、繰り返し実行します。

ステップ 8 変更を確定します。

次のタスク

関連項目

- IP レピュテーションスコアを使用したIP レピュテーション フィルタリングのテスト （103 ページ）
- ホスト アクセス テーブルを使用した接続を許可するホストの定義 （107 ページ）
- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法 （462 ページ）

IP レピュテーションスコアを使用したIP レピュテーション フィルタリングのテスト

常時大量のスパムを受信しているか、または組織に対するスパムを受信するために「ダミー」のアカウントを特に設定していない限り、実装した IP レピュテーションポリシーをただちに

テストすることは困難です。ただし、次の表に示すように、リスナーの HAT に IP レピュテーションスコアによるレピュテーションフィルタリングのエントリを追加した場合は、受信メールのうち「未分類」になるパーセンテージが低くなります。

このポリシーは、任意の IP レピュテーションスコアを指定し、`trace` コマンドを使用してテストします。「テストメッセージを使用したメールフローのデバッグ：トレース（1515ページ）」を参照してください。`trace` コマンドは、GUI だけでなく CLI でも使用できます。

表 *10 : IP* レピュテーションスコア実装の推奨メールフローポリシー

ポリシー名	主な動作（アクセス ルール）	パラメータ	値
`$BLOCKED`	`REJECT`	`None`	
`$THROTTLED`	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	10 20 1 MB 10 オン オフ **20**（推奨） オン
`$ACCEPTED` （パブリック リスナー）	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Use SenderBase:	1,000 1,000 100 MB 1,000 オン オフ 点灯
`$TRUSTED`	`ACCEPT`	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	1,000 1,000 100 MB 1,000 オフ 消灯 -1（無効） OFF

（注） $THROTTLED ポリシーでは、リモート ホストから受信する 1 時間あたりの最大受信者数は、デフォルトで 1 時間あたり 20 人に設定されています。この設定により、使用可能な最大スロットリングが制御されることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。デフォルトのホスト アクセス ポリシーの詳細については、定義済みの送信者グループとメール フロー ポリシーの理解 （118 ページ）を参照してください。

メッセージサブジェクトへの低IPレピュテーションスコアの入力

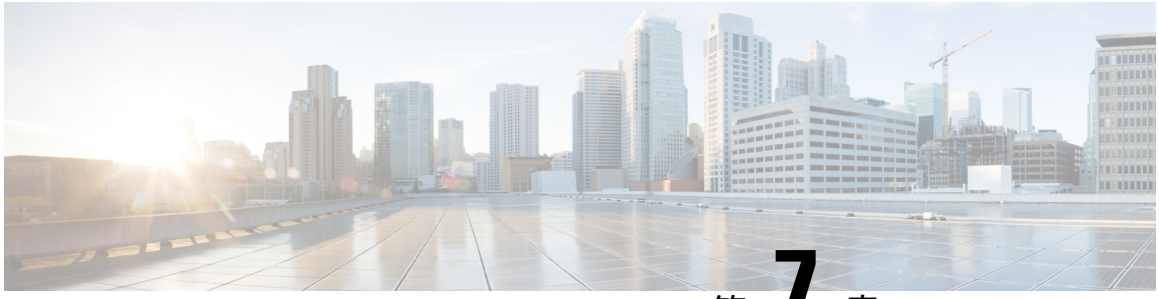
スロットリングを推奨しますが、IP レピュテーションサービスを使用して、スパムの疑いのあるメッセージの件名行を変更するという別の方法もあります。これを行うには、次の表に示すメッセージ フィルタを使用します。このフィルタは、reputation フィルタルール、strip-header および insert-header フィルタアクションを使用して、IP レピュテーションスコアが -2.0 未満のメッセージの件名行を実際の IP レピュテーションスコアを含む件名行に置き換えます。**{Spam *IP Reputation Score*}** のように表されます。この例の *listener_name* を、ご使用のパブリック リスナーの名前に置き換えます（このテキストを切り取って filters コマンドのコマンドライン インターフェイスに直接貼り付けできるように、この行自体にピリオドが含まれています）。

表：件名ヘッダーを IP レピュテーション に変更するメッセージフィルタ：例 1

```
iprs_filter:

if ((recv-inj == "listener_name
" AND subject != "\\{Spam -?[0-9.]+\\}"))

{

        insert-header("X-IPRS", "$REPUTATION");

        if (reputation <= -2.0)

{

        strip-header("Subject");

        insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

      }

 }

.
```

関連項目

- メッセージ フィルタを使用した電子メール ポリシーの適用 （155 ページ）



第 7 章

ホスト アクセス テーブルを使用した接続を許可するホストの定義

この章は、次の項で構成されています。

- 接続を許可するホストの定義の概要 （107 ページ）
- 送信者グループへのリモート ホストの定義 （109 ページ）
- メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （115 ページ）
- 定義済みの送信者グループとメール フロー ポリシーの理解 （118 ページ）
- 送信者グループからのメッセージの同様の処理 （121 ページ）
- ホスト アクセス テーブルの設定の使用 （132 ページ）
- 着信接続ルールへの送信者アドレス リストの使用 （134 ページ）
- SenderBase 設定とメール フロー ポリシー （135 ページ）
- 送信者の検証 （137 ページ）

接続を許可するホストの定義の概要

設定されているすべてのリスナーに対して、リモート ホストからの着信接続を制御する一連の規則を定義します。たとえば、リモート ホストを定義し、リスナーに接続できるかどうかを定義できます。AsyncOS では、ホスト アクセス テーブル（HAT）を使用してリスナーへの接続が許可されるホストを定義できます。

HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。設定されたどのリスナーにも独自の HAT があります。パブリック リスナーおよびプライベート リスナーの両方に HAT を設定します。

リモート ホストからの着信接続を制御するには、次の情報を定義します。

- **リモート ホスト。**リモート ホストがリスナーに接続を試みる方法を定義します。リモート ホスト定義を送信者グループにグループ化します。たとえば、IP アドレスとホスト名の一部を使用して、送信者グループの複数のリモート ホストを定義できます。IP レピュテーションスコアでリモートホストを定義することもできます。詳細については、送信者グループへのリモート ホストの定義 （109 ページ）を参照してください。

- **アクセス ルール。**送信者グループに定義されたリモート ホストがリスナーに接続するのを許可するのか、またどのような条件下なのかを定義できます。アクセス ルールは、メール フロー ポリシーを使って定義します。たとえば、特定の送信者グループのリスナーへの接続を許可するよう定義できますが、接続ごとに最大メッセージ数だけを許可します。詳細については、メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （115 ページ）を参照してください。

[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページで、リスナーへの接続が許可されるホストを定義します。

リスナーが TCP 接続を受信すると、設定された送信者グループに対して送信元 IP アドレスを比較します。また、[HAT概要（HAT Overview）] ページにリストされている順序で送信者グループを評価します。一致が見つかると、設定済みのメール フロー ポリシーを接続に適用します。1 つの送信者グループ内に複数の条件が設定されている場合、いずれかの条件が一致すると、その送信者グループは一致します。

リスナーを作成すると、AsyncOS は、リスナーに定義済みの送信者グループとメール フロー ポリシーを作成します。定義済みの送信者グループとメール フロー ポリシーを編集して新しい送信者グループとメール フロー ポリシーを作成できます。詳細については、定義済みの送信者グループとメール フロー ポリシーの理解 （118 ページ）を参照してください。

ホストアクセステーブルに格納されているすべての情報をファイルにエクスポートし、ファイルに格納されているホストアクセステーブル情報をリスナー用の電子メールゲートウェイにインポートできます。このとき、設定されているすべてのホストアクセステーブル情報は上書きされます。詳細については、ホストアクセステーブルの設定の使用 （132 ページ）を参照してください。

関連項目

- デフォルト HAT エントリ （108 ページ）

デフォルト HAT エントリ

HAT は、デフォルトでは、リスナーのタイプによって異なるアクションを実行するように定義されています。

- **パブリック リスナー。**HAT は、すべてのホストからの電子メールを受け入れるように設定されます。
- **プライベート リスナー。**HAT は、指定したホストからの電子メールをリレーし、他のすべてのホストを拒否するように設定されます。

[HAT概要（HAT Overview）] では、デフォルトのエントリに「ALL」という名前が付けられます。[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページですべての送信者グループのメール フロー ポリシーをクリックしてデフォルト エントリを編集できます。

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

送信者グループへのリモート ホストの定義

リモート ホストがリスナーに接続しようとする方法を定義できます。リモート ホスト定義を送信者グループにグループ化します。送信者グループは、それらの送信者からの電子メールを処理するために定義されたリモート ホストのリストです。

送信者グループは、次のもので識別される送信者のリストです。

- IP アドレス（IPv4 または IPv6）
- IP 範囲
- 具体的なホスト名またはドメイン名
- IP レピュテーションサービスの「組織」分類
- IP レピュテーションスコア（IPRS）の範囲（またはスコアの欠如）
- DNS リスト クエリー応答

送信者グループの受け入れ可能なアドレスのリストの詳細については、送信者グループの構文（110 ページ）を参照してください。

SMTP サーバが電子メールゲートウェイとの SMTP 接続を試みると、リスナーは送信者グループを順番に評価し、IP レピュテーションスコア、ドメイン、または IP アドレスといった送信者グループの任意の条件に一致する場合、送信者グループに SMTP 接続を割り当てます。

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

[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページで送信者グループを定義します。

関連項目

- 送信者グループの構文 （110 ページ）
- ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ （111 ページ）
- IP レピュテーションスコアを使用した送信者グループの定義 （113 ページ）
- DNS リストにクエリーを実行することで定義された送信者グループ （114 ページ）

送信者グループの構文

表 *11 : HAT* 内でのリモート ホストの定義：送信者グループの構文

構文	意味
`n:n:n:n:n:n:n:n`	IPv6 アドレス。先行ゼロを含める必要はありません。
`n:n:n:n:n:n:n:n-n:n:n:n:n:n:n:n` `n:n:n-n:n:n:n:n:n`	IPv6 アドレスの範囲。先行ゼロを含める必要はありません。
`n.n.n.n`	フル（完全な）IPv4 アドレス

`n.n.n.`
`n.n.n.`
`n.n.`
`n.n.`
`n.`
	部分的な IPv4 アドレス

`n.n.n.n-n.`
`n.n.n.n-n.`
`n.n.n-n.`
`n.n-n.`
`n.n-n`
`n-n.`
`n-n`
	IPv4 アドレスの範囲

`yourhost.example.com`	完全修飾ドメイン名
`.partialhost`	部分ホスト ドメイン内のすべてのもの

`n/c`
`n.n/c`
`n.n.n/c`
`n.n.n.n/c`
	IPv4 CIDR アドレス ブロック

`n:n:n:n:n:n:n:n/c`	IPv6 CIDR アドレス ブロック。先行ゼロを含める必要はありません

構文	意味
SBRS[n:n]SBRS[none]	IP レピュテーションスコア詳細については、IP レピュテーションスコアを使用した送信者グループの定義（113ページ）を参照してください。
SBO:n	ネットワークオーナー識別番号。詳細については、IP レピュテーションスコアを使用した送信者グループの定義（113ページ）を参照してください。
dnslist[dnsserver.domain]	DNS リストクエリー。詳細については、DNS リストにクエリーを実行することで定義された送信者グループ（114ページ）を参照してください。
ALL	すべてのアドレスに一致する特殊なキーワード。これは、すべての送信者グループのみに適用され、常に含まれます（ただしリストされません）。

ネットワークオーナー、ドメイン、IPアドレスで定義される送信者グループ

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

IP アドレスは、送信元メール ホストの IP アドレスとして定義します。電子メールゲートウェイは両方のインターネット プロトコル バージョン 4（IPv4）および IP バージョン 6（IPv6）アドレスをサポートします。

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

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

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

関連項目

- HAT に基づくポリシーの設定 （112 ページ）

HAT に基づくポリシーの設定

次の表に、ネットワーク オーナーと組織の例をいくつか示します。

表 *12*：ネットワーク オーナーと組織の例

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

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

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

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

- **この送信者によって、どの IP アドレスが制御されているか。**

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

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

- **その規模に応じて、この送信者に接続数を全体でいくつ割り当てるべきか。**
  - 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。そのため、電子メールゲートウェイへの接続をより多く割り当てる必要があります。
  - 多くの場合、大量の電子メールの送信元は、ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業、迷惑メールの送信元です。ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業は、多数の IP アドレスを管理する組織の例であり、電子メールゲートウェイへの接続をより多く割り当てる必要があります。通常、迷惑メールの送信者は、多数の IP アドレスを管理せず、少数の IP アドレスを通じて大量のメールを送信します。このような送信者には、電子メールゲートウェイへの接続をより少なく割り当てる必要があります。

メールフローモニタ機能は、ネットワークーナーとSENDERBASE組織の差別化を使用して、SENDERBASE内のロジックに基づき、送信者ごとに接続を割り当てる方法を決定します。メール フロー モニタ機能の使用方法の詳細については、「電子メール セキュリティ モニタの使用方法」の章を参照してください。

IP レピュテーションスコアを使用した送信者グループの定義

電子メールゲートウェイは、IP レピュテーションサービスに対してクエリを実行し、IP レピュテーションスコアを決定できます。IP レピュテーションスコアは、IP レピュテーションサービスからの情報に基づき、IPアドレス、ドメイン、または組織に割り当てられた数値です。スコアの範囲は、次の表に示すように、-10.0 ～ +10.0 です。

表 *13 : IP* レピュテーションスコアの定義

スコア（Score）	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い
なし	この送信者のデータがない（一般にスパムの送信元）

IP レピュテーションスコアを使用して、信頼性に基づいてメールフローポリシーを送信者に適用するように 電子メールゲートウェイを設定します。たとえば、スコアが -7.5 未満のすべての送信者を拒否することが考えられます。これは、GUI を使用して実現するのが最も簡単です。メッセージ処理の送信者グループの作成 （122 ページ）を参照してください。エクスポートした HAT をテキストファイルで編集する場合、IP レピュテーションスコアを含めるための構文については次の表を参照してください。

表 *14 : IP* レピュテーションスコアの構文

`SBRS[ n n`	IP レピュテーションスコアIP レピュテーションサービスにクエリを実行すると、送信者が識別され、スコアが範囲内で定義されます。
SBRS[none]	IP がないことを指定します（非常に新しいドメインには、まだ IP レピュテーションスコアがない場合があります）。

（注） GUI を通じて HAT に追加されるネットワークオーナーは、`SBO:n` という構文を使用します。ここで *n* は、IP レピュテーションサービス内のネットワークオーナーの一意の識別番号です。

IP レピュテーションサービスにクエリを実行するようにリスナーを設定するには、[ネットワーク（Network）]>[リスナー（Listeners）] ページを使用するか、CLI で `listenerconfig -> setup` コマンドを使用します。また、 電子メールゲートウェイが IP レピュテーションサービスにクエリを実行するときに待つタイムアウト値を定義することもできます。その後、GUI の [メールポリシー（Mail Policies）] ページの値を使用するか、CLI の `listenerconfig -> edit -> hostaccess` コマンドを使用して、IP レピュテーションサービスに対してルックアップを使用する際のさまざまなポリシーを設定できます。

（注） メッセージフィルタを作成して IP レピュテーションスコアに「しきい値」を指定し、システムで処理されるメッセージにさらにアクションを実行できます詳細については、「アンチスパム」および「アンチウィルス」の章の「IP レピュテーションルール」、「アンチスパムシステムのバイパスアクション」、および「アンチウイルスシステムのバイパスアクション」を参照してください。

DNS リストにクエリーを実行することで定義された送信者グループ

リスナーの HAT では、特定の DNS リスト サーバに対するクエリーに一致するものとして送信者グループを定義することもできます。クエリーは、リモートクライアントの接続時にDNS を通じて実行されます。リモート リストにクエリーを実行する機能は、現在メッセージ フィルタ ルールとしても存在しますが（「メッセージ フィルタを使用した電子メール ポリシーの適用」の章の「DNS リスト ルール」を参照）、メッセージの内容全体が受信されるのは一度だけです。

このメカニズムにより、グループ内で、DNS リストにクエリーを実行する送信者を設定し、それに応じてメール フロー ポリシーを調整できます。たとえば、接続を拒否したり、接続元ドメインの振る舞いを制限したりできます。

（注） いくつかの DNS リストは、可変の応答（たとえば「127.0.0.1」、「127.0.0.2」、「127.0.0.3」）を使用して、クエリー対象の IP アドレスに関するさまざまな事実を示すことができます。メッセージ フィルタ DNS リスト ルール（「メッセージ フィルタを使用した電子メール ポリシーの適用」の章の「DNS リスト ルール」を参照）を使用すると、クエリーの結果をさまざまな値と比較できます。しかし、HAT 内で DNS リスト サーバにクエリーを実行する指定では、簡潔にするためにブール演算のみがサポートされています（つまり、IP アドレスがリストに現れるかどうか）。

（注） CLI のクエリーでは必ず角カッコを含めます。GUI で DNS リスト クエリーを指定する場合には角カッコは不要です。クエリのテスト、DNS クエリの一般的な設定、または現在の DNS リスト キャッシュのフラッシュを行うには、CLI で dnslistconfig コマンドを使用します。

このメカニズムは、「異常な」接続に加えて、「正常な」接続を識別するためにも使用できます。たとえば、query.bondedsender.org に対してクエリを実行すると、その電子メール キャンペーンの健全性を保証するために Cisco Systems の Bonded Sender™ プログラムに供託金を積んだ接続元ホストが照合されます。デフォルトの ALLOWED_LIST の送信者グループを修正して Bonded Sender プログラムの DNS サーバにクエリを実行し（積極的に供託金を拠出したこれら正規の電子メール送信者が一覧表示されます）、その内容に応じてメールフローポリシーを調整することもできます。

メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義

メール フロー ポリシーでは SMTP カンバセーション中の送信者からリスナーへの電子メール メッセージのフローを制御または制限することができます。メール フロー ポリシーに次のパラメータ タイプを定義することで SMTP カンバセーションを制御します。

- 接続ごとの最大メッセージ数などの接続パラメータ。
- 1 時間あたりの受信者の最大数など、レート制限パラメータ。
- SMTP カンバセーション中に通信するカスタム SMTP コードと応答を変更します。
- スパム検出の有効化。
- ウイルス保護の有効化。
- TLS を使った SMTP 接続の暗号化などの暗号化。
- DKIM を使った着信メールの確認などの認証パラメータ。

最後に、メール フロー ポリシーが、リモート ホストからの接続に対し、次のいずれかのアクションを実行します。

- **承認（ACCEPT）**。接続が許可された後、電子メールの許可がさらに受信者アクセステーブル（パブリック リスナーの場合）などのリスナーの設定によって制限されます。
- **拒否（REJECT）**。接続は、最初は許可されますが、接続しようとするクライアントは、4XX または 5XX SMTP のステータス コードを取得します。どの電子メールも許可されません。

（注） また、SMTP カンバセーションの開始時ではなく、メッセージ受信者レベル（RCPT TO）でこの拒否を実行するように、AsyncOS を設定できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。この設定は、CLI の `listenerconfig > setup` コマンドから設定されます。詳細については、CLI を使用してリスナーを作成することによる接続要求のリスニング （95 ページ）を参照してください。

- **TCPREFUSE**。TCP レベルで接続は拒否されます。
- **リレー（RELAY）**。接続は許可されます。すべての受信者の受信は許可され、受信者アクセス テーブルで制限されません。
- **継続（CONTINUE）**。HAT 内のマッピングが無視され、HAT の処理が継続されます。着信接続が、CONTINUE でない後続のエントリに一致する場合、代わりにそのエントリが使用されます。CONTINUE ルールは、GUI での HAT の編集を容易にするために使用されます。詳細については、メッセージ処理の送信者グループの作成 （122 ページ）を参照してください。

関連項目

- HAT 変数の構文 （116 ページ）

HAT 変数の構文

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

表 *15 : HAT* 変数の構文

変数	定義
$Group	HAT 内の一致した送信者グループの名前で置き換えられます。送信者グループに名前がない場合、「None」が表示されます。

変数	定義
$Hostname	電子メールゲートウェイによって検証された場合にのみ、リモートホスト名で置き換えられます。IP アドレスの逆引き DNS ルックアップが成功したもののホスト名が返されない場合、「None」が表示されます。逆引き DNS ルックアップが失敗した場合（DNS サーバに到達できない場合や、DNS サーバが設定されていない場合）、「Unknown」が表示されます。
$OrgID	SenderBase 組織 ID（整数値）で置き換えられます。 電子メールゲートウェイが SENDERBASE 組織 ID を取得できないか、IP レピュテーションサービスが値を返さなかった場合、「None」が表示されます。
$RemoteIP	リモート クライアントの IP アドレスで置き換えられます。
$HATEntry	リモート クライアントが一致した HAT のエントリで置き換えられます。

関連項目

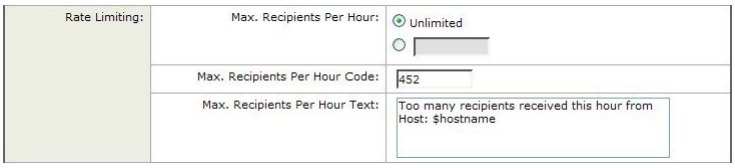
- HAT 変数の使用 （117 ページ）
- HAT 変数のテスト （118 ページ）

HAT 変数の使用

（注） これらの変数は、「ゲートウェイでのメール受信の設定」の章で説明する高度な HAT パラメータ `smtp_banner_text` と `max_rcpts_per_hour_text` と併用できます。

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

図 *15 : HAT* 変数の使用



または、CLI で次のように入力します。

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


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

```
[220]> 200


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

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

HAT 変数のテスト

これらの変数をテストするには、既知の信頼できるマシンの IP アドレスを、電子メールゲートウェイ上のリスナーの $ALLOWED_LIST 送信者グループに追加します。その後、そのマシンから telnet で接続します。SMTP 応答中で変数の置き換えを確認できます。次に例を示します。

```
# telnet
IP_address_of_Email_Security_Appliance port

220 hostname
 ESMTP

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

定義済みの送信者グループとメール フロー ポリシーの理解

次の表では、パブリック リスナーの作成時に設定される定義済みの送信者グループとメール フロー ポリシーをリストします。

表 *16 :* パブリック リスナー用の定義済みの送信者グループとメール フロー ポリシー

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
ALLOWED_LIST	信頼する送信者を ALLOWED_LIST の送信者グループに追加します。メール フロー ポリシー $TRUSTED は、信頼できる送信者からの電子メールのレート制限をイネーブルにせず、それらの送信者からの内容をアンチスパムまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。	$TRUSTED

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
BLOCKED_LIST	BLOCKED_LIST送信者グループ内の送信者は、メールフローポリシー$BLOCKEDで設定されたパラメータによって拒否されます。このグループに送信者を追加すると、SMTP HELOコマンドで5XX SMTP応答が返され、それらのホストからの接続が拒否されます。	$BLOCKED
SUSPECTLIST	送信者グループ SUSPECTLIST には、着信メールの速度をスロットリングする（低下させる）メールフローポリシーが含まれています。送信者が疑わしい場合、送信者グループ SUSPECTLIST に追加することで、メールフローポリシーにより次のことが指示されます。 • レート制限により、セッションあたりの最大メッセージ数、メッセージあたりの最大受信者数、最大メッセージサイズ、リモートホストから受け付ける最大同時接続数が制限されます。 • リモート ホストからの時間あたりの最大受信者数は20に設定されます。この設定は、使用可能な最大のスロットリングであることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。 • メッセージの内容はアンチスパム スキャン エンジンとアンチウイルス スキャン エンジンによってスキャンされます（これらの機能がシステムでイネーブルになっている場合）。 • 送信者に関する詳細情報を得るために、 SenderBase レピュテーション サービスに対してクエリーが実行されます。	$THROTTLED

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
UNKNOWNLIST	送信者グループ UNKNOWNLIST は、特定の送信者に対して使用するメール フロー ポリシーが決まっていない場合に便利です。このグループのメールフローポリシーでは、このグループの送信者についてメールが許可されますが、Anti-Spam ソフトウェア（システムで有効になっている場合）、アンチウイルス スキャン エンジン、および IP レピュテーション サービスをすべて使用して、送信者とメッセージの内容に関する詳細情報を取得することが指示されます。このグループに属する送信者に対するレート制限もデフォルト値を使用してイネーブルになります。ウイルス スキャン エンジンの詳細については、ウイルス スキャン （442 ページ）を参照してください。IP レピュテーション サービスの詳細については、IP レピュテーション サービス （99 ページ）を参照してください。	$ACCEPTED
ALL	その他すべての送信者に適用されるデフォルトの送信者グループ。詳細については、デフォルト HAT エントリ （108 ページ）を参照してください。	$ACCEPTED

次の表では、プライベート リスナーの作成時に設定される定義済みの送信者グループとメール フロー ポリシーをリストします。

表 *17*: プライベート リスナー用の定義済みの送信者グループとメール フロー ポリシー

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
RELAYLIST	中継を許可する必要があることがわかっている送信者を RELAYLIST 送信者グループに追加します。メール フロー ポリシー $RELAYED は、中継を許可する送信者からの電子メールのレート制限を行わず、それらの送信者からの内容をアンチスパム スキャン エンジンまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。 （注） RELAYLIST 送信者グループにはシステム設定ウィザードを実行したときに電子メールのリレーが許可されるシステムが含まれます。	$RELAYED
ALL	その他すべての送信者に適用されるデフォルトの送信者グループ。詳細については、デフォルト HAT エントリ （108 ページ）を参照してください。	$BLOCKED

（注） イーサネットポートが 2 つしかない 電子メールゲートウェイモデルのシステム設定ウィザードを実行すると、1 人のリスナーだけを作成するように促されます。また、内部システム用のメールのリレーに使用される$RELAYED メール フロー ポリシーも含まれるパブリック リスナーを作成します。3 つ以上のイーサネットポートを持つ 電子メールゲートウェイモデルについては、RELAYLIST 送信者グループと $RELAYED メールフローポリシーがプライベートリスナーだけに表示されます。

送信者グループからのメッセージの同様の処理

リスナーが送信者からのメッセージを処理する方法を設定するには、[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] と [メールフローポリシー（Mail Flow Policy）] ページで行います。これは、送信者グループとメール フロー ポリシーを作成、編集、および削除することにより行います。

関連項目

- メッセージ処理の送信者グループの作成 （122 ページ）
- 既存の送信者グループへの送信者の追加 （123 ページ）

- 着信接続のために実行するルールの順序の並べ替え （123 ページ）
- 送信者の検索 （124 ページ）
- メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （115 ページ）
- メール フロー ポリシーのデフォルト値の定義 （132 ページ）

メッセージ処理の送信者グループの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。

ステップ 2 [リスナー（Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 [送信者グループを追加（Add Sender Group）] をクリックします。

ステップ 4 送信者グループの名前を入力します。

ステップ 5 送信者グループのリストに配置する順序を選択します。

ステップ 6 （任意）たとえば、送信者グループまたはその設定についての情報などのコメントを入力します。

ステップ 7 この送信者グループを適用するメール フロー ポリシーを選択します。

（注） このグループに適用すべきメールフローポリシーがわからない場合（またはまだメール フロー ポリシーが存在しない場合）は、デフォルトの「CONTINUE (no policy)」メール フロー ポリシーを使用します。

ステップ 8 （任意）DNS リストを選択します。

ステップ 9 （任意） IP レピュテーションスコアに情報がない送信者を含めます。これは「none」と呼ばれ、一般に疑いがあることを意味します。

ステップ 10 （任意）DNS リストを入力します。

ステップ 11 （任意）ホスト DNS 検証設定を構成します。

詳細については、未検証の送信者へのより厳格なスロットリング設定の実行 （143 ページ）を参照してください。

ステップ 12 [送信（Submit）] をクリックして、送信者グループを作成します。

ステップ 13 新しく作成した送信者グループをクリックします。

ステップ 14 [送信者を追加（Add Sender）] をクリックして、送信者グループに送信者を追加します。

- 送信者の IP アドレスを追加します。[IPアドレス（IP Addresses）] を選択して IPv4 アドレス、IPv6 アドレス、またはホスト名を追加し、変更を送信します。

  送信者は、IP アドレスおよびホスト名の一部の範囲を含めることができます。

- 送信者の国を追加します。 [地理位置情報（Geolocation）] を選択し、変更を送信します。

ステップ 15 変更を送信し、保存します。

次のタスク

関連項目

- リスナーの IP レピュテーション フィルタリング スコアのしきい値の編集 （102 ページ）

既存の送信者グループへの送信者の追加

手順

ステップ 1 ドメイン、IP、またはネットワーク オーナー プロファイル ページで、[送信者グループに追加（Add to Sender Group）] リンクをクリックします。

ステップ 2 各リスナーに対して定義されているリストから送信者グループを選択します。

ステップ 3 変更を送信し、保存します。

（注） ドメインを送信者グループに追加すると、実際には 2 つのドメインが GUI に表示されます。たとえば、ドメイン `example.net` を追加した場合、[送信者グループに追加（Add to Sender Group）] ページには、`example.net` と `.example.net` が追加されます。2 つめのエントリがあることで、`example.net` のサブドメイン内のすべてのホストが送信者グループに追加されます。詳細については、送信者グループの構文 （110 ページ） を参照してください。

送信者グループに追加しようとしている送信者の 1 つ以上がその送信者グループにすでに存在する送信者と重複する場合、重複する送信者は追加されず、確認メッセージが表示されます。

ステップ 4 [保存（Save）] をクリックして送信者を追加し、[受信メールの概要（Incoming Mail Overview）] ページに戻ります。

次のタスク

関連項目

- スパムフィルタからの 電子メールゲートウェイ生成メッセージの保護 （490 ページ）
- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法 （462 ページ）

着信接続のために実行するルールの順序の並べ替え

リスナーに送信者グループを追加すると、送信者グループの順序を編集する必要があります。

リスナーに接続しようとするホストごとに、HAT は上から下へ順番に読み込まれます。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。

ステップ 2 [リスナー（Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 [順番を編集（Edit Order）] をクリックします。

ステップ 4 HAT の送信者グループの既存の行の新しい順序を入力します。

シスコはデフォルトの順序を維持することを推奨します（RELAYLIST（特定のハードウェア モデルのみ）の後に ALLOWED_LIST、BLOCKED_LIST、SUSPECTLIST、および UNKNOWNLIST が続く）。

ステップ 5 変更を送信し、保存します。

送信者の検索

[HAT概要（HAT Overview）] ページの上部にある [送信者を検索（Find Senders）] フィールドにテキストを入力することで送信者を検索できます。検索するテキストを入力し[検索（Find）] をクリックします。

メール フロー ポリシーを使用した着信メッセージのルールの定義

メール フロー ポリシーを作成する前に、次のルールとガイドラインを考慮してください。

- [デフォルトを使用（Use Default）] オプション ボタンがオンの場合、ポリシーのデフォルト値はグレー表示されます。デフォルト値を上書きするには、[On] オプション ボタンを選択して機能または設定をイネーブルにし、新たにアクセス可能になった値を変更します。デフォルト値を定義するには、メール フロー ポリシーのデフォルト値の定義 （132 ページ）を参照してください。
- 一部のパラメータは特定の事前設定値に依存します（たとえば、ディレクトリ獲得攻撃の設定を行うには、LDAP アクセプト クエリーを設定しておく必要があります）。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] ページに移動します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 次の表で説明する情報を入力します。

表 *18* : メール フロー ポリシー パラメータ

パラメータ	説明
接続	
最大メッセージ サイズ（Maximum message size）	このリスナーが許可するメッセージの最大サイズ。最大メッセージサイズの最小値は 1 KB です。
単一 IP からの最大同時接続数（Maximum concurrent connections from a single IP）	単一の IP アドレスからこのリスナーに接続することが許可される最大同時接続数。
接続あたりの最大メッセージ数	リモート ホストからの接続に対して、このリスナーを通じて送信できる最大メッセージ数。
メッセージあたりの最大受信者数	このホストから許可されるメッセージあたりの受信者の最大数。
SMTP バナー	
カスタム SMTP バナー コード（Custom SMTP Banner Code）	このリスナーとの接続が確立されたときに返される SMTP コード。
カスタム SMTP バナー テキスト（Custom SMTP Banner Text）	このリスナーとの接続が確立されたときに返される SMTP バナー テキスト。 （注） このフィールドには一部の変数を使用できます。詳細については、HAT 変数の構文 （116 ページ）を参照してください。
カスタム SMTP 拒否バナー コード（Custom SMTP Reject Banner Code）	このリスナーにより接続が拒否されたときに返される SMTP コード。
カスタム SMTP 拒否バナー テキスト（Custom SMTP Reject Banner Text）	このリスナーにより接続が拒否されたときに返される SMTP バナー テキスト。

パラメータ	説明
SMTP バナー ホスト名を上書き（Override SMTP Banner Host Name）	デフォルトでは、SMTP バナーをリモートホストに表示するときに、リスナーのインターフェイスに関連付けられているホスト名が電子メールゲートウェイに追加されます（たとえば、220- *hostname* ESMTP）。ここに異なるホスト名を入力することで、このバナーを変更できます。また、ホスト名フィールドを空白のままにすることで、ホスト名をバナーに表示しないこともできます。
ホストのレート制限	
1時間あたりの最大受信者数（Max. Recipients per Hour）	このリスナーが 1 台のリモート ホストから受信する、時間あたりの最大受信者数。送信者 IP アドレスあたりの受信者の数は、グローバルに追跡されます。各リスナーは各レート制限のしきい値を追跡します。ただし、すべてのリスナーは単一のカウンタに対して検証するので、同じ IP アドレス（送信者）が複数のリスナーに接続されるとレート制限を超える可能性が高くなります。 （注） このフィールドには一部の変数を使用できます。詳細については、HAT 変数の構文 （116 ページ）を参照してください。
時間コードあたりの最大受信者数（Max. Recipients per Hour Code）	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP コード。
1時間あたりの最大受信者数の超過テキスト（Max. Recipients Per Hour Exceeded Text）	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP バナー テキスト。
送信者のレート制限	
時間間隔あたりの最大受信者数（Max. Recipients per Time Interval）	このリスナーがメール送信者アドレスに基づいて一義的なエンベロープ送信者から受信する指定した期間中の最大受信者数。最大受信者数はグローバルに追跡されません。各リスナーは各レート制限のしきい値を追跡します。ただし、すべてのリスナーは単一のカウンタに対して検証するので、同じメール送信者アドレスからのメッセージが複数のリスナーによって受信されるとレート制限を超える可能性が高くなります。 デフォルトの最大受信者数を使用するか、無制限の受信者を許可するか、または別の最大受信者数を指定するか選択します。 他のメール フロー ポリシーによってデフォルトで使用される、最大受信者数と時間間隔を指定するデフォルトのメール フロー ポリシー設定を使用します。時間間隔はデフォルトのメール フロー ポリシーを使用してしか指定できません。

パラメータ	説明
送信者のレート制限超過エラー コード（Sender Rate Limit Exceeded Error Code）	SMTP コードは、エンベロープがこのリスナーに対して定義された時間間隔の最大受信者数を超えた場合に返されます。
送信者のレート制限超過エラー テキスト（Sender Rate Limit Exceeded Error Text）	SMTP バナー テキストは、エンベロープの送信者がこのリスナーに対して定義された時間間隔の最大受信者数を超えた場合に返されます。
例外	特定のエンベロープ送信者を定義されているレート制限から免除する場合は、そのエンベロープ送信者を含むアドレス リストを選択します。詳細については、着信接続ルールへの送信者アドレス リストの使用 （134 ページ）を参照してください。
フロー制御（Flow Control）	
Use SenderBase for Flow Control	このリスナーに対して IP レピュテーションサービスでの「検索」を有効にします。
IP アドレスの類似性でグループ化：（有効ビット範囲 0 ～ 32）（Group by Similarity of IP Addresses: (significant bits 0-32)）	リスナーのホスト アクセス テーブル（HAT）内のエントリを大規模な CIDR ブロックで管理しつつ、IP アドレスごとに着信メールを追跡およびレート制限するために使用します。レート制限のために類似の IP アドレスをグループ化するための有効ビットの範囲（0～32）を定義しつつ、その範囲内の IP アドレスごとに個別のカウンタを保持します。[SenderBase を使用（Use SenderBase）] をディセーブルにする必要があります。HAT Significant Bits の詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。
ディレクトリ獲得攻撃防御（DHAP）	
ディレクトリ獲得攻撃防止：1 時間あたりの最大無効受信大数	このリスナーがリモート ホストから受け取る無効な受信者の 1 時間あたりの最大数です。このしきい値は、RAT 拒否と SMTP コールアヘッド サーバプロファイル拒否の総数を表します。これは、無効な LDAP 受信者宛てのため SMTP カンバセーション中にドロップされたメッセージの総数と、ワーク キュー内でバウンスされたメッセージの合計です（関連付けられたリスナーの LDAP 承認設定に設定されたとおり）。LDAP アクセプト クエリーの DHAP の設定の詳細については、LDAP クエリに関する作業 （955 ページ）を参照してください。

パラメータ	説明
ディレクトリ獲得攻撃防御：SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ（Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation）	電子メールゲートウェイは、無効な受信者のしきい値に達するとホストへの接続をドロップします。
時間コードあたりの無効な受信者の最大数（Max. Invalid Recipients Per Hour Code）：	接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
時間テキストあたりの無効な受信者の最大数（Max. Invalid Recipients Per Hour Text）：	ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。
SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ（Drop Connection if DHAP threshold is reached within an SMTP Conversation）	SMTP カンバセーション中に DHAP しきい値に達した場合の接続のドロップをイネーブルにします。
時間コードあたりの無効な受信者の最大数（Max. Invalid Recipients Per Hour Code）	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
時間テキストあたりの無効な受信者の最大数（Max. Invalid Recipients Per Hour Text）：	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するテキストを指定します。

パラメータ	説明
スパム検出	
アンチスパム スキャン（Anti-spam scanning）	このリスナー上でアンチスパム スキャンを有効にします。
ウイルス検出	
アンチウイルス スキャン	このリスナー上でアンチウイルス スキャンを有効にします。
送信者ドメインのレピュテーションの検証	
送信者ドメインのレピュテーションの検証	送信者ドメインのレピュテーションの検証を有効にします。
暗号化と認証	
TLS	このリスナーに対する SMTP カンバセーションのトランスポート レイヤ セキュリティ（TLS）の拒否、推奨、必須を設定します。 [推奨（Preferred）] を選択すると、ドメインおよび電子メール アドレスを指定するアドレス リストを選択することによって、特定のドメインまたは特定の電子メールアドレスを持つドメインのエンベロープ送信者に対して TLS を必須に設定できます。このリストのドメインまたはアドレスに一致するエンベロープ送信者が TLS を使用しない接続経由でメッセージを送信しようとすると、 電子メールゲートウェイは接続を拒否し、送信者は再び TLS を使用して送信を試みる必要があります。 [クライアント証明書の検証（Verify Client Certificate）] オプションは、クライアント認証が有効な場合、 電子メールゲートウェイがユーザのメールアプリケーションと TLS 接続を確立するように指示します。TLS 推奨設定にこのオプションを選択した場合、ユーザが証明書を持たない場合にも電子メールゲートウェイは非TLS接続を許可しますが、ユーザが無効な証明書を持っている場合は、接続を拒否します。TLS 必須設定の場合、このオプションを選択すると、電子メールゲートウェイが接続を許可するために有効な証明書が必要になります。 アドレス リストの作成の詳細については、着信接続ルールへの送信者アドレス リストの使用 （134 ページ）を参照してください。 TLS 接続のクライアント証明書を使用する方法については、電子メールゲートウェイからのTLS接続の確立（1003ページ）を参照してください。
SMTP 認証	リスナーに接続するリモート ホストからの SMTP 認証を許可、禁止、義務付けます。SMTP 認証については、「LDAP クエリー」の章で詳細を説明します。

パラメータ	説明
TLS と SMTP 認証の両方が有効化されている場合（If Both TLS and SMTP Authentication are enabled）：	TLS に SMTP 認証を提供するよう義務付けます。
ドメイン キー/DKIM署名（Domain Key/DKIM Signing）	このリスナーでドメイン キーまたは DKIM署名を有効にします。（承認およびリレーのみ）。
DKIM検証	DKIM 検証をイネーブルにします。
S/MIME の復号と検証	
S/MIME の復号/検証	• S/MIME の復号または検証を有効にします。 • S/MIME の検証後、デジタル署名を維持するかメッセージから削除するかを選択します。トリプルラップされたメッセージの場合、内部署名のみが維持または削除されます。
S/MIME 公開キーの収集	
S/MIME公開キーの収集	S/MIME 公開キーの収集をイネーブルにします。
検証エラー時の証明書の収集	署名された着信メッセージの検証に失敗した場合、公開キーを収集するかどうかを選択します。
更新された証明書の保存	更新された公開キーを収集するかどうかを選択します。
SPF/SIDF 検証	
SPF/SIDF検証のイネーブル化（Enable SPF/SIDF Verification）	このリスナーで SPF/SIDF 署名をイネーブルにします。詳細については、電子メール認証 （741 ページ）を参照してください。
準拠レベル（Conformance Level）	SPF/SIDF 準拠レベルを設定します。[SPF]、[SIDF]、[SIDF互換（SIDF Compatible）] のいずれかを選択します。詳細は、電子メール認証 （741 ページ）を参照してください。

パラメータ	説明
「Resent-Sender:」または「Resent-From:」を使用した場合、PRA 検証結果をダウングレードします:（Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:）	準拠レベルとして [SIDF互換（SIDF Compatible）] を選択した場合、メッセージ中に Resent-Sender: ヘッダーまたは Resent-From: ヘッダーが存在する場合に、PRA Identity 検証の結果 Pass を None にダウングレードするかどうかを設定します。このオプションはセキュリティ目的で選択します。
HELOテスト（HELO Test）	HELO ID に対してテストを実行するかどうかを設定します（[SPF] および [SIDF互換（SIDF Compatible）] 準拠レベルで使用します）。
DMARC 検証	
DMARC検証のイネーブル化（Enable DMARC Verification）	このリスナーで DMARK 検証をイネーブルにします。詳細については、DMARC 検証 （777 ページ）を参照してください。
DMARC検証プロファイルを使用（Use DMARC Verification Profile）	このリスナーで使用する DMARK 検証プロファイルを選択します。
DMARCフィードバックレポート（DMARC Feedback Reports）	DMARC 集計フィードバック レポートの送信をイネーブルにします。 DMARC 集計フィードバックレポートの詳細については、DMARC 集計レポート （785 ページ）を参照してください。 （注） DMARC を指定するには、フィードバック レポート メッセージが DMARC に準拠している必要があります。これらのメッセージに DKIM 署名が付いていることを確認するか、または適切な SPF レコードをパブリッシュする必要があります。
タグなしバウンス	
タグなしバウンスを有効と見なす（Consider Untagged Bounces to be Valid）	バウンス検証タギング（「ルーティングおよび配信機能の設定」の章で説明）がイネーブルになっている場合にだけ適用されます。デフォルトでは、アプライアンスはタグのないバウンスを無効とみなし、バウンス検証の設定に応じて、バウンスを拒否するか、カスタムヘッダーを追加します。タグの付いていないバウンスを有効とみなすことを選択した場合、 電子メールゲートウェイはバウンスメッセージを受け入れます。

パラメータ	説明
エンベロープ送信者の DNS 検証	
	送信者の検証 （137 ページ）を参照してください。
例外テーブル	
例外テーブルを使用（Use Exception Table）	送信者検証ドメイン例外テーブルを使用します。例外テーブルは 1 つだけ使用できますが、メール フロー ポリシーごとにイネーブルにできます。詳細については、送信者検証例外テーブル （141 ページ）を参照してください。

（注） アンチスパムまたはアンチウイルススキャンがHATでグローバルに有効な場合、メッセージはアンチスパムまたはアンチウイルススキャンのために電子メールゲートウェイによって受け入れられると同時にフラグが付けられます。メッセージを許可した後にアンチスパムまたはアンチウイルス スキャンが無効にされた場合、メッセージは、ワーク キューを出るときに引き続きスキャン対象になります。

ステップ 4 変更を送信し、保存します。

メール フロー ポリシーのデフォルト値の定義

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] をクリックします。

ステップ 2 [リスナー（Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 設定したメール フロー ポリシーの下の [デフォルトポリシーパラメータ（Default Policy Parameters）] リンクをクリックします。

ステップ 4 このリスナーのすべてのメール フロー ポリシーで使用するデフォルト値を定義します。

プロパティの詳細については、メール フロー ポリシーを使用した着信メッセージのルールの定義 （124 ページ）を参照してください。

ステップ 5 変更を送信し、保存します。

ホスト アクセス テーブルの設定の使用

ホストアクセステーブルに格納されているすべての情報をファイルにエクスポートし、ファイルに格納されているホストアクセステーブル情報をリスナー用の電子メールゲートウェイにイ

ンポートできます。このとき、既存のすべてのホストアクセステーブル情報は上書きされます。

関連項目

- 外部ファイルへの ホスト アクセス テーブル設定のエクスポート （133 ページ）
- 外部ファイルからのホスト アクセス テーブル設定のインポート （133 ページ）

外部ファイルへの ホスト アクセス テーブル設定のエクスポート

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。
ステップ 2 [リスナー（Listener）] メニューで編集するリスナーを選択します。
ステップ 3 [HATをエクスポート（Export HAT）] をクリックします。
ステップ 4 エクスポートする HAT のファイル名を入力します。これは、 電子メールゲートウェイの設定ディレクトリに作成されるファイルの名前になります。
ステップ 5 変更を送信し、保存します。

外部ファイルからのホスト アクセス テーブル設定のインポート

HAT をインポートすると、既存のすべての HAT エントリが現在の HAT から削除されます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。
ステップ 2 [リスナー（Listener）] メニューで編集するリスナーを選択します。
ステップ 3 [HATをインポート（Import HAT）] をクリックします。
ステップ 4 リストからファイルを選択します。

（注） インポートするファイルは、電子メールゲートウェイの configuration ディレクトリに存在する必要があります。

ステップ 5 [送信（Submit）] をクリックします。既存のすべての HAT エントリを削除することを確認する警告メッセージが表示されます。
ステップ 6 [インポート（Import）] をクリックします。
ステップ 7 変更を保存します。

ファイル内に「コメント」を配置できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# File exported by the GUI at 20060530T215438
$BLOCKED
    REJECT {}
[ ... ]
```

着信接続ルールへの送信者アドレス リストの使用

メール フロー ポリシーは、レート制限の除外、および必須 TLS 接続などのエンベロープ送信者グループに適用する特定の設定にアドレス リストを使用できます。アドレス リストは、電子メールアドレス、ドメイン、部分ドメインおよびIPアドレスで構成できます。GUIで[メールポリシー（Mail Policies）]>[アドレスリスト（Address Lists）]のページを使用するか、またはCLIの`addresslistconfig`コマンドを使用し、アドレスリストを作成できます。[アドレスリスト（Address Lists）]ページには、アドレスリストを使用するメールフローポリシーと共に、電子メールゲートウェイのすべてのアドレスリストが表示されます。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[アドレスリスト（Address Lists）]を選択します。

ステップ 2 [アドレスリストの追加（Add Address List）]をクリックします。

ステップ 3 アドレス リストの名前を入力します。

ステップ 4 アドレス リストの説明を入力します。

ステップ 5 （任意）アドレス リストで完全な電子メール アドレスを使用することを義務付けるには、[完全電子メールアドレスのみ（Full Email Addresses only）]を選択します。

ステップ 6 アドレス リストを作成するには、次のオプションのいずれかを選択します。

- アドレスリストで完全な形式の電子メールアドレスを使用することを義務付ける場合は、[完全電子メールアドレスのみ（Full Email Addresses only）]を選択します。
- アドレスリストでドメインを使用することを義務付ける場合は、[ドメインのみ（Domains only）]を選択します。
- アドレス リストでIPアドレスを使用することを義務付ける場合は、[IPアドレスのみ（IP Addresses only）]を選択します。

ステップ 7 追加するアドレスを入力します。次の形式を使用できます。

- 完全な電子メール アドレス：`user@example.com`
- 電子メール アドレスの一部：`user@`

  （注） [完全Eメールアドレスのみ許可（Allow only full Email Addresses）]を選択した場合は、電子メール アドレスの一部は使用できません。

- 電子メール アドレスの IP アドレス：`@[1.2.3.4]`
- ドメインのすべてのユーザ：`@example.com`

- 部分ドメインのすべてのユーザ：`@.example.com`

ドメインおよび IP アドレスは @ 文字で開始する必要があることに注意してください。

カンマで電子メールアドレスを区切ります。新しい行を使ってアドレスを区切る場合、AsyncOS は自動的にエントリをカンマで区切られたリストに変換します。

ステップ 8 変更を送信し、保存します。

SenderBase 設定とメール フロー ポリシー

電子メールゲートウェイへの接続を分類し、メールフローポリシーを適用するには（レート制限が含まれる場合と含まれない場合がある）、リスナーは次の方法を使用します。

[分類（Classification）] -> [送信者グループ（Sender Group）] -> [メールフローポリシー（Mail Flow Policy）] -> [レート制限（Rate Limiting）]

詳細については、ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ （111 ページ）を参照してください。

「分類（Classification）」段階では、送信側ホストの IP アドレスを使用して、（パブリック リスナーで受信した）受信 SMTP セッションを送信者グループに分類します。送信者グループに関連付けられたメール フロー ポリシーには、レート制限をイネーブルにするパラメータがある場合があります。レート制限により、セッションあたりの最大メッセージ数、メッセージあたりの最大受信者数、最大メッセージ サイズ、リモート ホストから受け付ける最大同時接続数が制限されます。

通常、このプロセスでは、対応する名前の送信者グループの各送信者に対して受信者をカウントします。同じ時間帯に複数の送信者からメールを受信した場合、すべての送信者に対する受信者の合計数が制限値と比較されます。

このカウント方法には、次に示すいくつかの例外があります。

- ネットワークオーナーによって分類が行われた場合、IP レピュテーションサービスによってアドレスの大きなブロックが小さなブロックに自動的に分割されます。

このような小さな各ブロックに対して、受信者と受信者レート制限のカウントが別々に実行されます（通常、/24 CIDR ブロックと同じですが、必ずしも同じではありません）。

- HAT Significant Bits 機能を使用する場合について説明します。この場合、ポリシーに関連付けられた significant bits パラメータを適用して、大きなブロックのアドレスが小さなブロックに分割されます。

このパラメータは [メールフローポリシー（Mail Flow Policy）] -> [レート制限（Rate Limiting）] フェーズに関連しています。送信者グループの IP アドレスの分類に使用する「network/bits」CIDR 表記法は、「bits」フィールドとは異なります。

デフォルトでは、IP レピュテーションフィルタおよび IP プロファイリングのサポートが、パブリックリスナーに対しては有効で、プライベートリスナーに対しては無効です。

関連項目

- HAT Significant Bits 機能 （136 ページ）

HAT Significant Bits 機能

AsyncOS の 3.8.3 リリース以降では、大きな CIDR ブロック内のリスナーのホスト アクセス テーブル（HAT）の送信者グループ エントリを管理しながら、IP アドレス単位で受信メールの追跡およびレート制限を実行できます。たとえば、着信接続がホスト「10.1.1.0/24」と一致した場合、すべてのトラフィックを 1 つの大きなカウンタに集約するのではなく、範囲内の個別のアドレスに対してカウンタが生成されます。

（注） HAT ポリシーの significant bits オプションを有効にするには、HAT フロー制御オプションの「User SENDERBASE」を無効にする必要があります（または、CLI の場合、`listenerconfig -> setup` コマンドで SENDERBASE 情報サービスを有効にするための質問「Would you like to enable Reputation Filters and IP Profiling support?」に「no」と回答します）。つまり、Hat Significant Bits 機能と SenderBase IP プロファイリング サポートのイネーブル化は相互に排他的です。

ほとんどの場合、この機能を使用して送信者グループを広く定義し（つまり、「10.1.1.0/24」や「10.1.0.0/16」のような IP アドレスの大きなグループ）、IP アドレスの小さなグループにメール フロー レート制限を狭く適用します。

HAT Significant Bits 機能は、次のようなシステムのコンポーネントに対応します。

- HAT 設定 （136 ページ）
- Significant Bits HAT ポリシー オプション （136 ページ）
- インジェクション制御期間 （137 ページ）

HAT 設定

HAT の設定には、送信者グループとメール フロー ポリシーの 2 つの部分があります。送信者グループの設定では、送信者の IP アドレスの「分類」（送信者グループに入れる）方法を定義します。メール フロー ポリシー設定では IP アドレスからの SMTP セッションの管理方法を定義します。この機能を使用すると、IP アドレスは「CIDR ブロックで分類された」（たとえば、10.1.1.0/24）送信者グループとなり、個々のホスト（/32）として制御されます。これは「signficant_bits」ポリシー設定を使用して実行されます。

Significant Bits HAT ポリシー オプション

HAT 構文では signficant_bits 設定オプションを使用できます。この機能は、[メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] ページの GUI に表示されます。

フロー制御に SenderBase を使用するオプションが [OFF] になっているか、または [ディレクトリ獲得攻撃防御（Directory Harvest Attack Prevention）] がイネーブルになっている場合、

「significant bits」値は、接続している送信者の IP アドレスに適用され、結果的に CIDR 表記法が、HAT 内の定義済みの送信者グループと一致させるためのトークンとして使用されます。CIDR ブロックで囲まれた一番右のビットは、文字列の作成時に「ゼロ設定」になります。そのため、接続が IP アドレス 1.2.3.4 から確立され、significant_bits オプションが 24 に設定されたポリシーと一致する場合、結果として生じる CIDR ブロックは 1.2.3.0/24 になります。この機能を使用すると、HAT 送信者グループエントリ（たとえば、10.1.1.0/24）には、グループに割り当てられたポリシー内の有効ビットエントリ（上記の例では、32）とは異なる数のネットワーク有効ビット（24）が存在する可能性があります。

`listenerconfig` コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

インジェクション制御期間

インジェクション制御カウンタがリセットされた場合に調整できるグローバル設定オプションがあります。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に（たとえば、60 分間隔ではなく 15 分間隔で）リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。

現在のデフォルト値は 3600 秒（1 時間）です。最小 1 分（60 秒）から最大 4 時間（14,400 秒）までの期間を指定できます。

GUI でグローバル設定を使用してこの期間を調整します（詳細については、リスナーのグローバル設定 （85 ページ）を参照してください）。

また、CLI の `listenerconfig -> setup` コマンドを使用してこの期間を調整することもできます。`listenerconfig` コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

送信者の検証

スパムや無用なメールは、多くの場合、DNS で解決できないドメインまたは IP アドレスを持つ送信者によって送信されます。DNS 検証とは、送信者に関する信頼できる情報を取得し、それに従ってメールを処理することを意味します。SMTP カンバセーションの前に送信者検証（送信者の IP アドレスの DNS ルックアップに基づく接続のフィルタリング）を行うことは、電子メールゲートウェイ上のメールパイプラインを介して処理されるジャンクメールの量を減らすことにも役立ちます。

未検証の送信者からのメールは自動的に廃棄されます。代わりに、AsyncOS には、未検証の送信者からのメールを処理する方法を決定する送信者検証設定があります。たとえば、SMTP カンバセーションの前に未検証の送信者からのすべてのメールを自動的にブロックしたり、未検証の送信者をスロットリングしたりするように 電子メールゲートウェイを設定できます。

送信者検証機能は、次のコンポーネントで構成されます。

- **接続ホストの検証（Verification of the connecting host）**。これは、SMTP カンバセーションの前に実行されます。詳細については、送信者検証：ホスト （138 ページ）を参照してください。
- **エンベロープ送信者のドメイン部分の検証（Verification of the domain portion of the envelope sender）**。これは SMTP カンバセーションの中で実行されます。詳細については、送信者検証：エンベロープ送信者 （139 ページ）を参照してください。

関連項目

- 送信者検証：ホスト （138 ページ）
- 送信者検証：エンベロープ送信者 （139 ページ）
- 送信者検証の実装 — 設定例 （141 ページ）
- 未検証送信者からのメッセージの設定テスト （145 ページ）
- 送信者検証とロギング （146 ページ）

送信者検証：ホスト

送信者が未検証となる理由にはさまざまなものがあります。たとえば、DNS サーバが「ダウン」または応答しないか、ドメインが存在しないことが考えられます。送信者グループのホスト DNS 検証設定では、SMTP カンバセーションの前に未検証の送信者を分類し、さまざまな種類の未検証の送信者をさまざまな送信者グループに含めることができます。

電子メールゲートウェイは、着信メールについて、DNS を通じて接続元ホストの送信元ドメインを検証しようとします。この検証は、SMTP カンバセーションの前に実行されます。ダブル DNS ルックアップの実行によって、リモート ホストの IP アドレス（つまり、ドメイン）が取得され、有効性が検証されます。ダブル DNS ルックアップは、接続元ホストの IP アドレスに対する逆引き DNS（PTR）ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS（A）ルックアップからなります。その後、 電子メールゲートウェイは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。PTR ルックアップまたは A ルックアップが失敗するか、結果が一致しない場合、システムは IP アドレスのみを使用して HAT 内のエントリを照合し、送信者は未検証と見なされます。

未検証の送信者は、次のカテゴリに分類されます。

- 接続元ホストの PTR レコードが DNS に存在しない。
- DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。
- 接続元ホストの逆引き DNS ルックアップ（PTR）が正引き DNS ルックアップ（A）に一致しない。

送信者グループの [接続ホストのDNS検証（Connecting Host DNS Verification）] 設定を使用して、未検証の送信者に対する動作を指定できます（送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング （142 ページ）を参照）。

すべての送信者グループの送信者グループ設定でホスト DNS 検証をイネーブルにできますが、ホスト DNS 検証設定を送信者グループに追加するということは、そのグループに未検証の送信者を含めることになるという点に注意してください。つまり、スパムやその他の無用なメールが含まれることになります。そのため、これらの設定は、送信者を拒否またはスロットリン

グする送信者グループに対してのみイネーブルにすることを推奨します。たとえば、送信者グループ ALLOWED_LIST に対してホスト DNS 検証を有効にすると、未検証の送信者からのメールが、ALLOWED_LIST 内の信頼できる送信者からのメールと同様に扱われることを意味します（メールフローポリシーの設定内容に応じて、アンチスパムまたはアンチウイルスチェック、レート制限などのバイパスを含みます）。

送信者検証：エンベロープ送信者

エンベロープ送信者検証を使用すると、エンベロープ送信者のドメイン部分が DNS で検証されます（エンベロープ送信者のドメインが解決されるか。エンベロープ送信者のドメインの A レコードまたは MX レコードが DNS に存在するか）。ドメインは、DNS で確認試行がタイムアウトまたは DNS サーバの障害などの一時的なエラー状態が発生したかを解決できません。これに対し、ドメインをルックアップしようとしたときに明確な「domain does not exist」ステータスが返された場合、ドメインは存在しません。この検証が SMTP カンバセーションの中で実行されるのに対し、ホスト DNS 検証はカンバセーションが開始される前に実行され、接続元 SMTP サーバの IP アドレスに適用されます。

詳細：AsyncOS は、送信者のアドレスのドメインに対して MX レコード クエリーを実行します。次に AsyncOS は、MX レコードのルックアップの結果に基づいて、A レコードのルックアップを行います。DNS サーバが「NXDOMAIN」（このドメインのレコードがない）を返した場合、AsyncOS はそのドメインが存在しないものとして扱います。これは「存在しないドメインのエンベロープ送信者」カテゴリに分類されます。NXDOMAIN は、ルート ネーム サーバがこのドメインの権威ネームサーバを提供していないことを意味する場合があります。

（注） DNS 応答が「NOERROR」の場合、送信者検証は MX レコードのないドメインを拒否します。

ただし DNS サーバが「SERVERFAIL」を返した場合、DNS サーバは「応答がないドメインのエンベロープ送信者」カテゴリに分類されます。SERVFAIL は、ドメインが存在しないが、DNS でレコードのルックアップ中に一時的な問題が発生していることを示します。

スパマーなどの不法なメール送信者が使用する一般的な手法は、MAIL FROM 情報（エンベロープ送信者内）を偽造し、受け付けられた未検証の送信者からのメールが処理されるようにすることです。これにより、MAIL FROM アドレスに送信されたバウンス メッセージが配信不能になるため、問題が生じる可能性があります。エンベロープ送信者検証を使用すると、不正な形式の（ただし空白ではない）MAIL FROM を拒否するように電子メールゲートウェイを設定できます。

各メール フロー ポリシーで、次のことが可能です。

- エンベロープ送信者の DNS 検証をイネーブルにする。
- 不正な形式のエンベロープ送信者に対し、カスタム SMTP コードと応答を渡す。エンベロープ送信者の DNS 検証をイネーブルにした場合、不正な形式のエンベロープ送信者はブロックされます。
- 解決されないエンベロープ送信者ドメインに対しカスタム応答を渡す。

• DNS に存在しないエンベロープ送信者ドメインに対しカスタム応答を渡す。

送信者検証例外テーブルを使用して、ドメインまたはアドレスのリストを格納し、そこからのメールを自動的に許可または拒否することができます（送信者検証例外テーブル （141 ページ）を参照）。送信者検証例外テーブルは、エンベロープ送信者検証とは独立してイネーブルにできます。そのため、たとえば、例外テーブルで指定した特別なアドレスやドメインを、エンベロープ送信者検証をイネーブルにすることなく拒否できます。また、内部ドメインまたはテストドメインからのメールを、他の方法で検証されない場合でも常に許可することもできます。

ほとんどのスパムは未検証の送信者から受信されますが、未検証の送信者からのメールを受け付けることが必要な理由があります。たとえば、すべての正規の電子メールをDNSルックアップで検証できるわけではありません。一時的な DNS サーバの問題により送信者を検証できないことがあります。

未検証の送信者からのメール送信が試みられた場合、送信者検証例外テーブルとメールフローポリシーのエンベロープ送信者 DNS 検証設定を使用して、SMTP カンバセーション中にエンベロープ送信者が分類されます。たとえば、DNSに存在しないために検証されない送信元ドメインからのメールを受け付けてスロットリングすることができます。いったんそのメールを受け付けた後、MAIL FROM の形式が不正なメッセージは、カスタマイズ可能な SMTP コードと応答で拒否されます。これは SMTP カンバセーションの中で実行されます。

任意のメール フロー ポリシーに対し、メール フロー ポリシー設定中で、エンベロープ送信者の DNS 検証（ドメイン例外テーブルを含む）をイネーブルにできます。これには、GUI または CLI（`listenerconfig -> edit -> hostaccess -> < policy >` ）を使用します。

関連項目

- 部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM （140 ページ）
- カスタム SMTP コードと応答 （140 ページ）
- 送信者検証：エンベロープ送信者 （139 ページ）

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

エンベロープ送信者検証をイネーブルにするか、リスナーのSMTPアドレス解析オプションで部分ドメインの許可をディセーブルにすると（「ゲートウェイでのメール受信の設定」の章の「SMTPアドレス解析オプション」の項を参照）、そのリスナーのデフォルトドメイン設定は使用されなくなります。

これらの機能は互いに排他的です。

カスタム SMTP コードと応答

エンベロープ送信者の形式が不正なメッセージ、DNSに存在しないエンベロープ送信者、DNSクエリーで解決できない（DNS サーバがダウンしているなど）エンベロープ送信者に対し、SMTP コードと応答メッセージを指定できます。

SMTP 応答には変数 `$EnvelopeSender` を含めることができます。これは、カスタム応答を送信するときにエンベロープ送信者の値に展開されます。

一般には「Domain does not exist」結果は永続的ですが、これを一時的な状態にすることができます。そのようなケースを扱うために、「保守的な」ユーザは、エラー コードをデフォルトの 5XX から 4XX に変更できます。

送信者検証例外テーブル

送信者検証例外テーブルは、SMTP カンバセーション中に自動的に許可または拒否されるドメインまたは電子メール アドレスのリストです。また、拒否されるドメインについて、オプションの SMTP コードと拒否応答を指定することもできます。 電子メールゲートウェイあたりの送信者検証例外テーブルは 1 つのみであり、メールフローポリシーごとに有効化されます。

送信者検証例外テーブルは、明らかに偽物であるものの、形式が正しいドメインまたは電子メールアドレスをリストし、そこからのメールを拒否するために使用できます。たとえば、形式が正しい MAIL FROM `pres@whitehouse.gov` を送信者検証例外テーブルに格納し、自動的に拒否するように設定できます。また、内部ドメインやテストドメインなど、自動的に許可するドメインをリストすることもできます。これは、受信者アクセステーブル（RAT）で行われるエンベロープ受信者（SMTP RCPT TO コマンド）処理に似ています。

送信者検証例外テーブルは、GUI の [メールポリシー（Mail Policies）]>[例外テーブル（Exception Table）] ページ（または CLI の `exceptionconfig` コマンド）で定義された後、GUI（メール フロー ポリシー ACCEPTED を使用した未検証送信者への送信メッセージの定義 （143 ページ）を参照）または CLI（『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照）でポリシーごとに有効化されます。

送信者検証例外テーブルのエントリの構文は次のとおりです。

例外テーブルの変更については送信者の電子メール アドレスに基づいた送信者検証ルールからの未検証送信者の除外 （144 ページ）を参照してください。

送信者検証の実装 — 設定例

ここでは、ホストとエンベロープ送信者検証の典型的で保守的な実装の例を示します。

この例では、ホスト送信者検証を実装するときに、既存の送信者グループ SUSPECTLIST とメール フロー ポリシー THROTTLED により、逆引き DNS ルックアップが一致しない接続元ホストからのメールがスロットリングされます。

新しい送信者グループ（UNVERIFIED）と新しいメールフローポリシー（THROTTLEMORE）が作成されます。検証されない接続元ホストからのメールは、SMTP カンバセーションの前にスロットリングされます（送信者グループ UNVERIFIED とより積極的なメール フロー ポリシー THROTTLEMORE が使用されます）。

メール フロー ポリシー ACCEPTED に対してエンベロープ送信者検証がイネーブルにされます。

次の表に、送信者検証を実装するための推奨される設定を示します。

表 19 : 送信者検証：推奨される設定

送信者グループ	ポリシー	含める
UNVERIFIED SUSPECTLIST	THROTTLEMORE THROTTLED	SMTP カンバセーションの前。 接続元ホストの PTR レコードが DNS に存在しない。 接続元ホストの逆引き DNS ルックアップ（PTR）が正引き DNS ルックアップ（A）に一致しない。
	ACCEPTED	SMTP カンバセーション中のエンベロープ送信者検証。 - 形式が不正な MAIL FROM:。 - エンベロープ送信者が DNS に存在しない。 - エンベロープ送信者が DNS で解決されない。

関連項目

- 送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング （142 ページ）
- 未検証の送信者へのより厳格なスロットリング設定の実行 （143 ページ）
- メール フロー ポリシー ACCEPTED を使用した未検証送信者への送信メッセージの定義 （143 ページ）
- 送信者の電子メールアドレスに基づいた送信者検証ルールからの未検証送信者の除外 （144 ページ）
- 送信者検証例外テーブル内でのアドレスの検索 （144 ページ）

送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] を選択します。

ステップ 2 送信者グループのリストで [SUSPECTLIST] をクリックします。

ステップ 3 [設定を編集（Edit Settings）] をクリックします。

ステップ 4 リストから [スロットル（THROTTLED）] ポリシーを選択します。

ステップ 5 [接続ホストのDNS検証（Connecting Host DNS Verification）] の中の [接続ホスト逆引きDNS検索（PTR）が転送DNS検索（A）と一致しない（Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)）] チェックボックスをオンにします。

ステップ 6 変更を送信し、保存します。

逆引き DNS ルックアップが失敗した送信者は送信者グループ SUSPECTLIST に一致し、メール フロー ポリシー THROTTLED のデフォルト アクションが実行されます。

未検証の送信者へのより厳格なスロットリング設定の実行

手順

ステップ 1 まず、新しいメール フロー ポリシーを作成し（この例では THROTTLEMORE という名前を付けます）、より厳格なスロットリング設定を行います。

a) [メールフローポリシー（Mail Flow Policies）] ページで [ポリシーを追加（Add Policy）] をクリックします。
b) メール フロー ポリシーの名前を入力し、[接続動作（Connection Behavior）] として [承認（Accept）] を選択します。
c) メールをスロットリングするようにポリシーを設定します。
d) 変更を送信し、保存します。

ステップ 2 次に、新しい送信者グループを作成し（この例では、UNVERIFIED という名前を付けます）、THROTTLEMORE ポリシーを使用するように設定します。

a) [HAT概要（HAT Overview）] ページで [送信者グループを追加（Add Sender Group）] をクリックします。
b) リストから [THROTTLEMORE] ポリシーを選択します。
c) [接続ホストのDNS検証（Connecting Host DNS Verification）] 中の [接続ホストのPTRレコードがDNSに存在しません（Connecting host PTR record does not exist in DNS）] チェックボックスをオンにします。
d) 変更を送信し、保存します。

メール フロー ポリシー **ACCEPTED** を使用した未検証送信者への送信メッセージの定義

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] を選択します。

ステップ 2 [メールフローポリシー（Mail Flow Policies）] ページで、メール フロー ポリシー [承認（ACCEPTED）] をクリックします。

ステップ 3 [送信者の検証（Sender Verification）] セクションまでスクロールします。

ステップ 4 [エンベロープ送信者 DNS の検証（Envelope Sender DNS Verification）] セクションで、次を実行します。

- [On] を選択し、このメール フロー ポリシーに対するエンベロープ送信者の DNS 検証をイネーブルにします。
- カスタム SMTP コードと応答を定義することもできます。

ステップ 5 [ドメイン例外テーブルの使用（Use Domain Exception Table）] セクションで [オン（On）] を選択して、ドメイン例外テーブルを有効にします。

ステップ 6 変更を送信し、保存します。

送信者の電子メール アドレスに基づいた送信者検証ルールからの未検証送信者の除外

手順

ステップ 1 [メールポリシー（Mail Policies）] > [例外テーブル（Exception Table）] を選択します。

（注） 例外テーブルは、[例外テーブルを使用（Use Exception Table）] がイネーブルに設定されているすべてのメール フロー ポリシーにグローバルに適用されます。

ステップ 2 [メールポリシー（Mail Policies）] > [例外テーブル（Exception Table）] ページで [ドメイン例外を追加（Add Domain Exception）] をクリックします。

ステップ 3 電子メールアドレスを入力します。具体的なアドレス（pres@whitehouse.gov）、名前（user@）、ドメイン（@example.com または @.example.com）、または IP アドレスを角カッコで囲んだアドレス（user@[192.168.23.1]）を入力できます。

ステップ 4 そのアドレスからのメッセージを許可するか拒否するかを指定します。メールを拒否する場合、SMTP コードとカスタム応答を指定することもできます。

ステップ 5 変更を送信し、保存します。

送信者検証例外テーブル内でのアドレスの検索

手順

ステップ 1 [例外テーブル（Exception Table）] ページの [ドメイン例外の検索（Find Domain Exception）] セクションに電子メール アドレスを入力します。

ステップ 2 [検索（Find）] をクリックします。

テーブル中のいずれかのエントリにアドレスが一致した場合、最初に一致したエントリが表示されます。

未検証送信者からのメッセージの設定テスト

これで送信者検証設定を完了したため、電子メールゲートウェイの動作を確認できます。

DNS 関連の設定のテストは、本書の範囲を超えていることに注意してください。

関連項目

- 形式が不正な MAIL FROM 送信者アドレスのテスト メッセージの送信 （145 ページ）
- 送信者検証ルールから除外するアドレスからのメッセージの送信 （145 ページ）

形式が不正な MAIL FROM 送信者アドレスのテスト メッセージの送信

THROTTLED ポリシーのさまざまな DNS 関連の設定をテストすることは難しい場合がありますが、形式が不正な MAIL FROM 設定をテストできます。

手順

ステップ 1 電子メールゲートウェイへの Telnet セッションを開きます。

ステップ 2 SMTP コマンドを使用して、形式が不正な MAIL FROM（ドメインなしの「admin」など）を使用したテスト メッセージを送信します。

（注） デフォルトドメインを使用するか、メールを送受信するときに部分ドメインを明示的に許可するように電子メールゲートウェイを設定した場合や、アドレス解析をイネーブルにした場合は（「ゲートウェイでのメール受信の設定」の章を参照）、ドメインがないかドメインの形式が正しくない電子メールを作成、送信、受信できない場合があります。

ステップ 3 メッセージが拒否されることを確認します。

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin
553 #5.5.4 Domain required for sender address
```

SMTP コードと応答が、メール フロー ポリシー THROTTLED のエンベロープ送信者検証設定で設定したものになっていることを確認します。

送信者検証ルールから除外するアドレスからのメッセージの送信

送信者検証例外テーブルに列挙されている電子メール アドレスからのメールに対し、エンベロープ送信者検証が実行されないことを確認するには、次の手順を実行します。

手順

ステップ 1 アドレス admin@zzzaaazzz.com を、例外テーブルに動作「Allow」で追加します。

ステップ 2 変更を保存します。

ステップ 3 電子メールゲートウェイへの Telnet セッションを開きます。

ステップ 4 SMTP コマンドを使用して、送信者検証例外テーブルに入力した電子メール アドレス（admin@zzzaaazzz.com）からテスト メッセージを送信します。

ステップ 5 メッセージが許可されることを確認します。

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin@zzzaaazzz.com
250 sender <admin@zzzaaazzz.com> ok
```

その電子メールアドレスを送信者検証例外テーブルから削除すると、エンベロープ送信者のドメイン部分が DNS で検証されないため、その送信者からのメールが拒否されます。

送信者検証とロギング

次のログ エントリは、送信者検証の判断例を示します。

関連項目

- エンベロープ送信者検証 （146 ページ）

エンベロープ送信者検証

形式が不正なエンベロープ送信者：

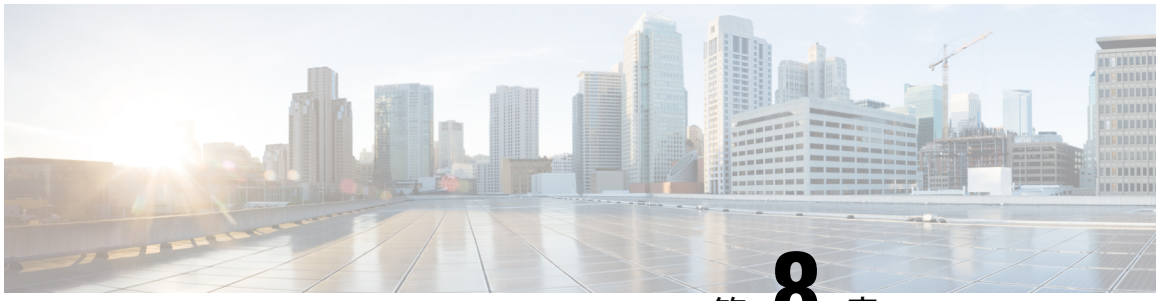
```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected, envelope sender
 domain missing
```

ドメインが存在しない（NXDOMAIN）：

```
Wed Aug  9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com> sender rejected,
envelope sender domain does not exist
```

ドメインが解決されない（SERVFAIL）：

```
Wed Aug  9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com> sender rejected,
envelope sender domain could not be resolved
```



第 8 章

ドメイン名または受信者アドレスに基づく接続の許可または拒否

この章は、次の項で構成されています。

- 受信者のアドレスに基づく接続の許可または拒否の概要 （147 ページ）
- 受信者アクセス テーブル（RAT）の概要 （148 ページ）
- GUI を使用した RAT へのアクセス （148 ページ）
- CLI を使用した RAT へのアクセス （148 ページ）
- デフォルトの RAT エントリの編集 （148 ページ）
- ドメインおよびユーザ （149 ページ）

受信者のアドレスに基づく接続の許可または拒否の概要

AsyncOS では、各パブリック リスナーが受信者アドレスの許可および拒否操作を管理するために受信者アクセステーブル（RAT）を使用します。受信者アドレスには次のものが含まれます。

- ドメイン
- 電子メール アドレス
- 電子メール アドレスのグループ

システム セットアップ ウィザードは、少なくとも 1 つのパブリックリスナー（デフォルト値）を電子メールゲートウェイ上で設定するよう管理者に指示します。セットアップ時にパブリック リスナーを設定すると、メールを受け入れるデフォルトのローカル ドメインまたは特定のアドレスを指定します。これらのローカル ドメインまたは特定のアドレスは、パブリック リスナーの RAT の最初のエントリです。

各パブリック リスナーのデフォルトのエントリである [その他の受信者（All Other Recipients）] は、すべての受信者からの電子メールを拒否します。管理者は、電子メールゲートウェイがメッセージを許可するすべてのローカルドメインを定義します。任意で、電子メールゲートウェイがメッセージを許可または拒否する特定のユーザも定義できます。AsyncOS では、受信者アクセス テーブル（RAT）を使用して適切なローカル ドメインと特定のユーザを定義することができます。

複数ドメインのメッセージを受け入れるように、リスナーの設定が必要になる場合があります。たとえば、組織で currentcompanyname.com ドメインを使用しているが、以前は oldcompanyname.com ドメインを使用していた場合は、currentcompanyname.com と oldcompanyname.com の両方のメッセージを受け入れることができます。この場合、両方のローカル ドメインをパブリック リスナーの RAT に含めます。

（注：ドメインマップ機能によって、あるドメインから別のドメインにメッセージをマップできます。「ルーティングおよびドメイン機能の設定」の章の「ドメインマップ機能」の項を参照してください。）

受信者アクセス テーブル（RAT）の概要

受信者アクセス テーブルは、パブリック リスナーが許可する受信者を定義します。少なくとも、テーブルはアドレスおよびそのアドレスを受け入れるか拒否するかを指定します。

[受信者アクセステーブル(RAT)（Recipient Access Table (RAT)）] ページには、RAT 内のエントリの一覧が、その順序、デフォルトのアクション、エントリが LDAP 許可クエリーをバイパスするように設定されているかどうかと共に表示されます。

GUI を使用した RAT へのアクセス

GUI

手順

[メールポリシー（Mail Policies）] > [受信者アクセステーブル(RAT)（Recipient Access Table (RAT)）] に移動します。

CLI を使用した RAT へのアクセス

CLI

手順

`listenerconfig` コマンドと `edit -> rcptaccess -> new` サブコマンドを使用します。

デフォルトの RAT エントリの編集

はじめる前に

- パブリック リスナーを設定します。
- インターネット上にオープン リレーを作成しないように、編集の計画には注意が必要です。オープンリレー（「セキュアでないリレー」または「サードパーティ リレー」とも呼びます）は、第三者による電子メール メッセージのリレーを許す SMTP 電子メール サーバです。オープン リレーがあると、ローカル ユーザ向けでもローカル ユーザからでもないメールを処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパムを送信することが可能になります。デフォルトでは、RAT はすべての受信者を拒否し、オープン リレーが作成されないようにします。
- デフォルトのエントリを RAT から削除できないことに注意してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信者アクセス テーブル（RAT）（Recipient Access Table（RAT））] に移動します。

ステップ 2 [その他の受信者（All Other Recipients）] をクリックします。

ドメインおよびユーザ

RAT を使用してメッセージを受け入れるドメインを変更する

電子メールゲートウェイがメッセージを許可するすべてのローカルドメインおよび特定のユーザを設定するには、[メールポリシー（Mail Policies）] > [受信者アクセステーブル（RAT）（Recipient Access Table (RAT)）] ページを使用します。このページでは、次の作業を実行できます。

- RAT 内のエントリの追加、削除、変更。
- エントリの順序の変更。
- RAT エントリのテキスト ファイルへのエクスポート。
- RAT エントリのテキスト ファイルからのインポート。テキスト ファイルからのインポートは、既存のエントリを上書きします。

関連項目

- メッセージを受け入れるドメインおよびユーザの追加 （150 ページ）
- 受信者アクセス テーブルでのドメインおよびユーザの順序の入れ替え （152 ページ）
- 受信者アクセス テーブルの外部ファイルへのエクスポート （153 ページ）
- 受信者アクセス テーブルの外部ファイルからのインポート （153 ページ）

メッセージを受け入れるドメインおよびユーザの追加

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信者アクセス テーブル（RAT）（Recipient Access Table (RAT)）] ページに移動します。

ステップ 2 [リスナーの概要（Overview for Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 [受信者を追加...（Add Recipient）] をクリックします。

ステップ 4 エントリの順序を選択します。

ステップ 5 受信者のアドレスを入力します。

ステップ 6 受信者を許可するか拒否するかを選択します。

ステップ 7 （任意）受信者に対する LDAP 許可クエリーをバイパスすることを選択します。

ステップ 8 （任意）このエントリに対してカスタム SMTP 応答を使用します。

a) [カスタムSMTP応答（Custom SMTP Response）] で [はい（Yes）] を選択します。

b) SMTP 応答コードとテキストを入力します。その受信者に対する RCPT TO コマンドへの SMTP 応答を含めます。

ステップ 9 （任意）[受信コントロールのバイパス（Bypass Receiving Control）] で [はい（Yes）] を選択して、スロットリングのバイパスを選択します。

ステップ 10 変更を送信し、保存します。

次のタスク

関連項目

- 受信者アドレスの定義 （150 ページ）
- 特別な受信者での LDAP 許可のバイパス （151 ページ）
- 特別な受信者でのスロットリングのバイパス （152 ページ）

受信者アドレスの定義

RAT では、受信者または受信者のグループを定義できます。受信者は、完全な電子メール アドレス、ドメイン、部分ドメイン、ユーザ名、または IP アドレスで定義できます。

IPv4 address	ホストの特定のインターネット プロトコル バージョン 4（IPv4）アドレス。IP アドレスは文字「[]」で囲む必要があることに注意してください。
IPv6 address	ホストの特定のインターネット プロトコル バージョン 6（IPv6）アドレス。IP アドレスは文字「[]」で囲む必要があることに注意してください。
`division.example.com`	完全修飾ドメイン名。

.partialhost	「partialhost」ドメイン内のすべて。
user@domain	完全な電子メール アドレス。
user@	指定したユーザ名を含むすべてのアドレス。
user@[*IP_address*]	特定の IPv4 または IPv6 アドレスのユーザ名。IP アドレスは文字「[]」で囲む必要があることに注意してください。 「user@*IP_address*」（角カッコ文字なし）は有効なアドレスではないことに注意してください。有効なアドレスを作成するために、メッセージを受信したときに角カッコが追加され、受信者が RAT で一致するかどうかに影響が出ることがあります。

（注） GUI のシステム セットアップ ウィザードの手順 4 でドメインを受信者アクセス テーブルに追加する場合（手順 3：ネットワーク （42 ページ）を参照）、サブドメインを指定するための別のエントリを追加することを検討してください。たとえば、ドメイン example.net を入力する場合、.example.net も入力した方がよい場合があります。第 2 のエントリにより、example.net のすべてのサブドメイン宛てのメールが受信者アクセス テーブルに一致するようになります。RAT で .example.com のみを指定した場合、.example.com のすべてのサブドメイン宛てのメールを許可しますが、サブドメインがない完全な電子メール アドレス受信者（たとえば joe@example.com）宛てのメールは許可されません。

特別な受信者での LDAP 許可のバイパス

LDAP 許可クエリーを設定する場合、特定の受信者について許可クエリーをバイパスすることが必要な場合があります。この機能は、customercare@example.com のように、ある受信者宛に受信した電子メールについて、LDAP クエリの中で遅延させたりキューに格納したりしないことが望ましい場合に便利です。

LDAP 許可クエリーの前にワーク キュー内で受信者アドレスを書き換えるように設定した場合（エイリアシングまたはドメイン マップの使用など）、書き換えられたアドレスは LDAP 許可クエリーをバイパスしません。たとえば、エイリアス テーブルを使用して customercare@example.com を bob@example.com および sue@example.com にマップします。customercare@example.com について LDAP 許可のバイパスを設定した場合、エイリアシングが実行された後に、bob@example.com および sue@example.com に対して LDAP 許可クエリが実行されます。

GUI で LDAP 許可をバイパスするように設定するには、RAT エントリを追加または編集するときに [この受信者のLDAPアクセプトクエリーをバイパスする（Bypass LDAP Accept Queries for this Recipient）] を選択します。

CLI で LDAP アクセプト クエリーをバイパスするように設定するには、listenerconfig -> edit -> rcptaccess コマンドを使用して受信者を入力するときに、次の質問に「y」と答えます。

```
Would you like to bypass LDAP ACCEPT for this entry? [Y]> y
```

LDAP 許可をバイパスするように RAT エントリを設定する場合、RAT エントリの順序が、受信者アドレスの一致のしかたに影響を与えることに注意してください。条件を満たす最初の RAT エントリを使用して受信者アドレスが一致します。たとえば、RAT エントリ postmaster@ironport.com と ironport.com があるとします。postmaster@ironport.com のエントリについては LDAP 許可クエリーをバイパスするように設定し、ironport.com のエントリを ACCEPT に設定します。postmaster@ironport.com 宛てのメールを受信した場合、LDAP 許可がバイパスされるのは、postmaster@ironport.com のエントリが ironport.com のエントリよりも前にある場合のみです。ironport.com のエントリが postmaster@ironport.com のエントリの前にある場合、RAT はこのエントリを介して受信者アドレスと一致し、ACCEPT アクションが適用されます。

特別な受信者でのスロットリングのバイパス

受信者エントリで、リスナーでイネーブルになっているスロットリング制御メカニズムを受信者がバイパスすることを指定できます。

この機能は、特定の受信者のメッセージを制限しない場合に便利です。たとえば、多くのユーザは、メール フロー ポリシーで定義されている受信制御に基づいて送信元ドメインがスロットリングされている場合でも、リスナー上でアドレス「postmaster@domain」の電子メールを受信します。リスナーの RAT 中で受信制御をバイパスするようにこの受信者を指定することで、同じドメイン中の他の受信者用のメール フロー ポリシーを保持しつつ、リスナーは受信者「postmaster@domain」の無制限のメッセージを受信できます。受信者は、送信元ドメインが制限されている場合に、システムが保持している時間あたりの受信者のカウンタでカウントされません。

GUI で特定の受信者が受信制御をバイパスするように指定するには、RAT エントリを追加または編集するときに、[受信コントロールのバイパス（Bypass Receiving Control）] 設定で [はい（Yes）] を選択します。

CLI で特定の受信者が受信制御をバイパスするように指定するには、`listenerconfig -> edit -> rcptaccess` コマンドを使用して受信者を入力するときに、次の質問に「y」と答えます。

```
Would you like to bypass receiving control for this entry?  [N]> y
```

受信者アクセステーブルでのドメインおよびユーザの順序の入れ替え

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信者アクセス テーブル（RAT）（Recipient Access Table (RAT)）] ページに移動します。

ステップ 2 [リスナーの概要（Overview for Listener）] フィールドで、編集するリスナーを選択します。

ステップ 3 [順番を編集（Edit Order）] をクリックします。

ステップ 4 [順番（Order）] 列の値を調整して順序を変更します。

ステップ 5 変更を送信し、保存します。

受信者アクセス テーブルの外部ファイルへのエクスポート

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信者アクセス テーブル（RAT）（Recipient Access Table (RAT)）] ページに移動します。

ステップ 2 [リスナーの概要（Overview for Listener）] フィールドで、編集するリスナーを選択します。

ステップ 3 [RATをエクスポート（Export RAT）] をクリックします。

ステップ 4 エクスポートするエントリのファイル名を入力します。

これは、電子メールゲートウェイの設定ディレクトリに作成されるファイルの名前になります。

ステップ 5 変更を送信し、保存します。

受信者アクセス テーブルの外部ファイルからのインポート

テキスト ファイルから受信者アクセス テーブルエントリをインポートすると、既存のすべてのエントリが受信者アクセス テーブルから削除されます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信者アクセス テーブル（RAT）（Recipient Access Table (RAT)）] ページに移動します。

ステップ 2 [リスナーの概要（Overview for Listener）] フィールドで、編集するリスナーを選択します。

ステップ 3 [RATをインポート（Import RAT）] をクリックします。

ステップ 4 リストからファイルを選択します。

AsyncOS は、電子メールゲートウェイ上の configuration ディレクトリに存在するテキストファイルの一覧を表示します。

ステップ 5 [送信（Submit）] をクリックします。

既存の受信者アクセス テーブル エントリをすべて削除することを確認する警告メッセージが表示されます。

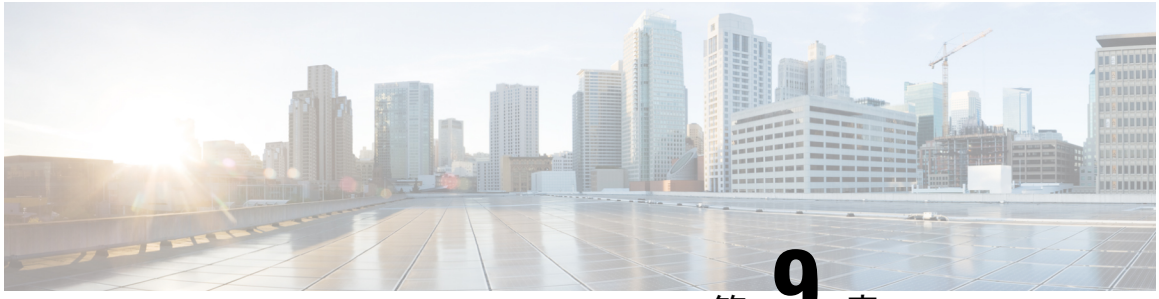
ステップ 6 [インポート（Import）] をクリックします。

ステップ 7 変更を保存します。

ファイル内に「コメント」を配置できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

例：

```
# File exported by the GUI at 20060530T220526
.example.com  ACCEPT
ALL  REJECT
```



第 9 章

メッセージ フィルタを使用した電子メール ポリシーの適用

電子メールゲートウェイは、詳細なコンテンツスキャンおよびメッセージ フィルタリング テクノロジーを備えているため企業のネットワークに参加または退出するときに、企業のポリシーを適用して、特定のメッセージを処理することができます。

この章では、ポリシーの適用のために使用可能な機能（コンテンツ スキャン エンジン、メッセージ フィルタ、添付ファイル フィルタ、コンテンツ ディクショナリ）の強力な組み合わせについて説明します。

この章は、次の項で構成されています。

- 概要 （155 ページ）
- メッセージ フィルタのコンポーネント （157 ページ）
- メッセージ フィルタの処理 （159 ページ）
- メッセージ フィルタ ルール （165 ページ）
- メッセージ フィルタ アクション （223 ページ）
- 添付ファイルのスキャン （260 ページ）
- メッセージフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出 （272 ページ）
- CLI を使用したメッセージ フィルタの管理 （273 ページ）
- メッセージ フィルタの例 （289 ページ）
- スキャン動作の設定 （297 ページ）

概要

メッセージフィルタにより、電子メールゲートウェイでメッセージを受信したときに、それらを処理する方法を記述した特別なルールを作成できます。メッセージフィルタは、特定の種類の電子メール メッセージに指定の特別な処理を施す必要があることを指定します。Cisco メッセージフィルタは、指定の単語に対してメッセージ内容をスキャンすることによって社内メール ポリシーを適用することができます。この章は、次の項で構成されています。

- **メッセージ フィルタのコンポーネント**。メッセージ フィルタにより、メッセージの受信時にそれらを処理する方法を記述した特別なルールを作成できます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージエンベロープ、メッセージヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタアクションにより、通知を生成したり、メッセージのドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、変更を行ったりすることができます。詳細については、メッセージ フィルタのコンポーネント （157 ページ）を参照してください。
- **メッセージ フィルタの処理**。AsyncOS がメッセージ フィルタを処理する場合、AsyncOS がスキャンする内容、処理の順番、実行されるアクションは、メッセージ フィルタの順番、メッセージの内容を変更した可能性のある事前の処理、メッセージの MIME 構造、コンテンツマッチング用に設定されたしきい値スコア、クエリーの構造などのいくつかの要因に基づきます。詳細については、メッセージフィルタの処理 （159 ページ）を参照してください。
- **メッセージ フィルタ ルール**。各フィルタには、フィルタで処理できる一連のメッセージを定義するルールがあります。メッセージフィルタを作成する場合、それらのルールを定義します。詳細については、メッセージフィルタ ルール （157 ページ）を参照してください。
- **メッセージ フィルタ アクション**。各フィルタには、ルールで true に評価された場合に、メッセージに対して実行するアクションがあります。実行できるアクションには、最終アクション（メッセージの配信、ドロップ、バウンスなど）、またはメッセージをさらに処理できる非最終アクション（ヘッダーの除去や挿入など）の 2 つのタイプのアクションがあります。詳細については、メッセージフィルタ アクション （157 ページ）を参照してください。
- **添付ファイル スキャン メッセージ フィルタ**。添付ファイル スキャン メッセージ フィルタを使用して、会社のポリシーと整合しないメッセージから添付ファイルを除去できます。元のメッセージはそのまま配信することができます。添付ファイルは、それらの特定のタイプ、フィンガープリント、内容に基づいてフィルタできます。イメージアナライザを使用して、イメージ添付ファイルをスキャンすることもできます。イメージアナライザは、イメージ属性を測定するアルゴリズムを使用して、不適切なコンテンツの可能性を判断します。これらのアルゴリズムは、たとえば、画像内の形状やカラーパレットを検出できます。アナライザは、不適切なコンテンツの特定に役立つように、画像内の形状のタイプと、画像内の他の色に対する肌色の割合を特定できます。肌色の割合が高い画像は、不適切である可能性が高くなります。アルゴリズムは、いかなる方法でも差別しません。詳細については、添付ファイルのスキャン （260 ページ）を参照してください。
- **CLI を使用したメッセージ フィルタの管理**。CLI は、メッセージ フィルタを操作するためのコマンドを受け入れます。たとえば、メッセージ フィルタのリストを表示、並び替え、インポート、エクスポートする必要がある場合があります。詳細については、CLI を使用したメッセージ フィルタの管理 （273 ページ）を参照してください。
- **メッセージフィルタの例**。この項では、実際のフィルタの例を示し、各フィルタについて簡単に説明します。詳細については、メッセージフィルタの例 （289 ページ）を参照してください。

メッセージ フィルタのコンポーネント

メッセージ フィルタにより、メッセージの受信時にそれらを処理する方法を記述した特別なルールを作成できます。メッセージ フィルタは、メッセージ フィルタ ルールとメッセージ フィルタ アクションから構成されます。

関連項目

- メッセージ フィルタ ルール （157 ページ）
- メッセージ フィルタ アクション （157 ページ）
- メッセージ フィルタの構文例 （158 ページ）

メッセージ フィルタ ルール

メッセージ フィルタ ルールによって、フィルタで処理するメッセージを判断します。ルールは、論理結合子 AND、OR、NOT を使用して組み合わせることで、複雑なテストを作成できます。ルール式は、かっこを使用してグループ化することもできます。

メッセージ フィルタ アクション

メッセージ フィルタの目的は、選択されたメッセージに対してアクションを実行することです。

アクションには、次の 2 つのタイプがあります。

- 最終アクション（deliver、drop、bounce など）はメッセージの処理を終了し、後続のフィルタによるさらなる処理を許可しません。
- 非最終アクションは、メッセージをさらに処理することを許可するアクションを実行します。

（注） 非最終メッセージ フィルタ アクションは、累積的です。各フィルタが異なるアクションを指定する複数のフィルタにメッセージが一致する場合、すべてのアクションが累積され、適用されます。ただし、同じアクションを指定する複数のフィルタにメッセージが一致する場合、前のアクションが上書きされ、最後のフィルタ アクションが適用されます。

関連項目

- フィルタ アクション一覧表 （223 ページ）
- アクション変数 （235 ページ）
- 一致した内容の表示 （238 ページ）
- メッセージ フィルタ アクションの説明と例 （239 ページ）

メッセージ フィルタの構文例

フィルタ仕様の直観的な意味は次のようになります。

メッセージがルールに一致する場合、順番にアクションが適用されます。else 句が存在する場合、メッセージがルールに一致しない場合に else 句内のアクションが実行されます。

指定したフィルタ名によって、フィルタをアクティブ、非アクティブ、削除する場合に、フィルタが管理しやすくなります。

メッセージ フィルタでは次の構文を使用します。

構文例	目的
expedite:	フィルタ名
if (recv-listener == 'InboundMail' or recv-int == 'notmain')	ルールの指定

`{`
`  alt-src-host('outbound1');`
`skip-filters();`
`}`
	アクションの指定

`else`
`{`
`  alt-src-host('outbound2');`
`}`
	（任意）代替アクションの指定

代替アクションは省略できることに注意してください。

構文例	目的
expedite2:	フィルタ名
`if ((not (recv-listener == 'InboundMail')) and` (not (recv-int == 'notmain')))	ルールの指定

`{`
`  alt-src-host('outbound2');`
`skip-filters();`
}
	アクションの指定

複数のフィルタを順番に 1 つずつ並べて 1 つのテキスト ファイルにまとめることができます。

単一引用符または二重引用符で、フィルタの値を囲む必要があります。単一引用符または二重引用符は、値の両側に等しく組み合わせる必要があります。たとえば、式 `notify('customercare@example.com')` と `notify("customercare@example.com")` はどちらも有効ですが、式 `notify("customercare@example.com')` は構文エラーが発生します。

「#」文字で始まる行はコメントと見なされ、無視されます。ただし、それらは `filters -> detail` によってフィルタを表示して確認できるため、AsyncOS では保持されません。

メッセージ フィルタの処理

AsyncOS はメッセージフィルタを処理する場合、AsyncOS がスキャンする内容、処理の順番、実行するアクションは、次のいくつかの要因に基づきます。

- **メッセージ フィルタの順番。**メッセージ フィルタは、順序付けられたリストで維持されます。メッセージの処理時に、AsyncOS は各メッセージ フィルタをそれらがリストに表示されている順番で適用します。最終アクションが行われた場合、そのメッセージに対して、それ以上のアクションは実行されません。詳細については、メッセージフィルタの順番 （160 ページ）を参照してください。
- **事前処理**。メッセージ フィルタが評価される前に、AsyncOS メッセージに対して実行されるアクションによって、ヘッダーが追加または削除されることがあります。AsyncOS は、処理時にメッセージに存在するヘッダーに対してメッセージ フィルタ プロセスを実行します。詳細については、メッセージヘッダールールおよび評価 （160ページ）を参照してください。
- **メッセージの MIME 構造**。メッセージの MIME 構造によって、「本文」として扱われるメッセージの部分と「添付ファイル」として扱われるメッセージの部分が判断されます。多くのメッセージフィルタは、メッセージの本文部分のみに、または添付ファイル部分のみに作用するように設定されます。詳細については、メッセージ本文とメッセージ添付ファイル （160 ページ）を参照してください。
- **正規表現に設定されるしきい値スコア**。正規表現に一致させる場合、フィルタアクションが実行されるまでに、一致が発生しなければならない回数を集計する「スコア」を設定します。これにより、さまざまな用語に対する応答の重み付けをすることができます。詳細については、コンテンツ スキャンの一致のしきい値 （161 ページ）を参照してください。
- **クエリーの構造**。メッセージ フィルタ内で、AND または OR テストを評価する場合、AsyncOS は不要なテストを評価しません。さらに、システムは左から右にテストを評価しないことに注意することが重要です。代わりに、AND および OR テストが評価される場合、最も価値の低いテストが最初に評価されます。詳細については、メッセージフィルタ内の AND テストと OR テスト （164 ページ）を参照してください。

関連項目

- メッセージ フィルタの順番 （160 ページ）
- メッセージ ヘッダー ルールおよび評価 （160 ページ）
- メッセージ本文とメッセージ添付ファイル （160 ページ）
- コンテンツ スキャンの一致のしきい値 （161 ページ）
- メッセージ フィルタ内の AND テストと OR テスト （164 ページ）

メッセージ フィルタの順番

メッセージフィルタは順序付けられたリストに維持され、リスト内のそれらの位置によって番号付けされます。メッセージの処理時に、メッセージフィルタが割り振られた番号順で適用されます。そのため、9 番のフィルタがメッセージに対してすでに最終アクション（バウンスなど）を実行した場合、30番のフィルタは、メッセージの送信元ホストを変更する機会がありません。リストのフィルタの位置は、システム ユーザー インターフェイスによって変更できます。ファイルからインポートされたフィルタは、インポートされたファイル内のそれらの相対的順序に基づきます。

最終アクション後、そのメッセージに対して、それ以上のアクションは実行されません。

メッセージがフィルタ ルールに一致していても、次のいずれかの理由で、フィルタがそのメッセージに対して作用しないことがあります。

- フィルタが非アクティブである。
- フィルタが無効である。
- フィルタが、メッセージの最終アクションを実行した前のフィルタに取って代わられた。

メッセージ ヘッダー ルールおよび評価

フィルタは、ヘッダールールを適用する場合に、元のメッセージのヘッダーではなく、「処理済み」ヘッダーを評価します。つまり、

- 前に実行されたアクションによって、ヘッダーが追加された場合、後続のすべてのヘッダー ルールによって、それを照合できるようになります。
- 前に実行されたアクションによって、ヘッダーが取り除かれた場合、後続のすべてのヘッダー ルールで、それを照合できなくなります。
- 前に実行されたアクションによって、ヘッダーが変更された場合、後続のすべてのヘッダールールで、元のメッセージヘッダーではなく、変更済みのヘッダーが評価されます。

この動作は、メッセージ フィルタとコンテンツ フィルタの両方に共通です。

メッセージ本文とメッセージ添付ファイル

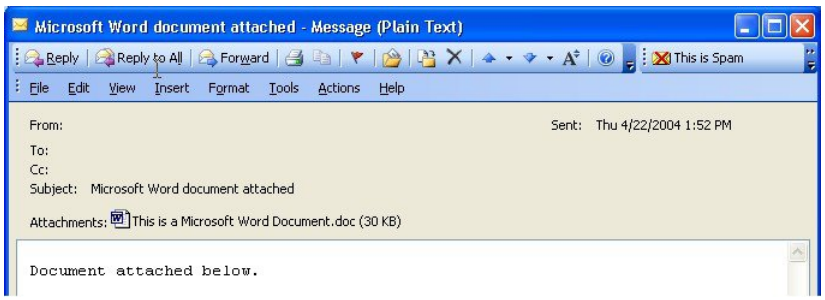
電子メール メッセージは、複数の部分から構成されます。RFC では、メッセージのヘッダーの後に続くすべてのものをマルチパート「メッセージ本文」として規定していますが、多くのユーザはまだメッセージの「本文」と「添付ファイル」を別々のものと捉えています。body-*variable* または `attachment`-*variable* という Cisco メッセージフィルタを使用する場合、電子メールゲートウェイは、ほとんどのユーザが「本文」と「添付ファイル」として考える部分を、多くの MUA がそれらを別々にレンダリングしようと試みるのと同じように区別しようとします。

body-*variable* または `attachment`-*variable* メッセージ フィルタ ルールを書く目的では、メッセージヘッダーの後のすべてのものがメッセージ本文と見なされ、その内容は本文内にある MIME 部分の最初のテキスト部分と見なされます。そのコンテンツの後のすべてのもの（つまり、追

加のMIME部分）は添付ファイルと見なされます。AsyncOSはメッセージのさまざまなMIME部分を評価し、添付ファイルとして処理されるファイルの部分を識別します。

たとえば、 以下の図は、Microsoft Outlook MUA のメッセージを示しています。ここでは「`Document attached below.`」という言葉がプレーン テキストのメッセージ本文として表示され、ドキュメント「`This is a Microsoft Word document.doc`」が添付ファイルとして表示されています。多くのユーザが電子メールをこのように捉えている（最初の部分がプレーンテキストで2番目の部分がバイナリ ファイルであるマルチパート メッセージとしてではなく）ため、Cisco は、メッセージの「本文」（最初のプレーン テキスト部分）と対照的に、.doc ファイル部分（実質的に2番目のMIME部分）を区別して処理するルールを作成するために、メッセージフィルタで「添付ファイル」という用語を使用しています。ただし、RFCS 1521および1522で使われている用語によると、メッセージの本文はすべての MIME 部分から構成されます。

図 *16*：「添付ファイル」を含むメッセージ



電子メールゲートウェイは、マルチパートメッセージの本文と添付ファイルを区別しているため、想定される動作をするためには、*body-variable* または `attachment`-*variable* メッセージフィルタルールを使用する場合に、いくつかのケースで注意が必要です。

- テキスト部分が1つのメッセージ（つまり、「Content-Type: text/plain」または「Content-Type: text/html」のヘッダーを含むメッセージ）がある場合、電子メールゲートウェイはメッセージ全体を本文と見なします。コンテンツタイプが異なる場合、電子メールゲートウェイは、それを単一の添付ファイルと見なします。
- エンコードされたファイル（uuencoded など）は電子メール メッセージの本文に含まれます。これが発生した場合、エンコードされたファイルは添付ファイルとして扱われ、抽出およびスキャンされ、残りのテキストがテキスト本文として見なされます。
- 単一のテキスト以外の部分は常に添付ファイルと見なされます。 たとえば、.zip ファイルのみで構成されるメッセージは、添付ファイルと見なされます。

コンテンツ スキャンの一致のしきい値

メッセージ本文または添付ファイル内のパターンを検索するフィルタ ルールを追加する場合、パターンが見つかる必要がある回数の最初のしきい値を指定できます。AsyncOSはメッセージをスキャンすると、メッセージおよび添付ファイルに見つかった一致の数の「スコア」を集計します。最小しきい値に満たない場合、正規表現はtrueと評価されません。このしきい値は次のフィルタ ルールに指定できます。

- body-contains
- only-body-contains

- attachment-contains
- every-attachment-contains
- dictionary-match
- attachment-dictionary-match

`drop-attachments-where-contains` アクションにしきい値を指定することもできます。

（注） ヘッダーまたはエンベロープの受信者と送信者をスキャンするフィルタ ルールにしきい値を指定できません。

関連項目

- しきい値の構文 （162 ページ）
- メッセージ本文と添付ファイルのしきい値スコア （162 ページ）
- しきい値スコアリング マルチパート/代替 MIME 部分 （163 ページ）
- コンテンツ ディクショナリを使用したしきい値のスコアリング （164 ページ）

しきい値の構文

出現最小回数のしきい値を指定するには、パターンと、true と評価するために必要な一致の最小数を指定します。

```
if(<filter rule>('<pattern>',<minimum threshold>)){
```

たとえば、body-contains フィルタ ルールで、値「Company Confidential」が少なくとも 2 回見つかる必要があることを指定するには、次の構文を使用します。

```
if(body-contains('Company Confidential',2)){
```

デフォルトでは、AsyncOS がコンテンツスキャンフィルタを保存する際に、フィルタをコンパイルし、しきい値が割り当てられていない場合は、1 のしきい値を割り当てます。

コンテンツ ディクショナリの値に対して、パターン マッチの最小数を指定することもできます。コンテンツ ディクショナリの詳細については、「テキスト リソース」の章を参照してください。

メッセージ本文と添付ファイルのしきい値スコア

電子メール メッセージは、複数の部分から構成されることがあります。メッセージ本文または添付ファイル内のパターンを検索するフィルタ ルールのしきい値を指定すると、AsyncOS は、メッセージ部分と添付ファイルの一致の数をカウントして、しきい値「スコア」を判断します。メッセージ フィルタで特定の MIME 部分を指定しない限り（`attachment-contains` フィルタ ルールなど）、AsyncOS はメッセージのすべての部分で見つかった一致を合計し、一致の合計がしきい値に達しているかどうかを判断します。たとえば、しきい値が 2 の `body-contains` メッセージ フィルタがあるとします。本文に 1 つの一致があり、添付ファイルに 1 つの一致があるメッセージを受信します。AsyncOS がこのメッセージを採点した場合、合計が 2 つの一致になり、しきい値スコアを満たしていると判断します。

同様に、複数の添付ファイルがある場合、AsyncOSは添付ファイルごとにスコアを合計して、一致のスコアを判断します。たとえば、しきい値が3の`attachment-contains`フィルタ ルールがあるとします。2つの添付ファイルがあるメッセージを受信し、各添付ファイルに2つの一致が含まれます。AsyncOSはこのメッセージを4つの一致と採点し、しきい値スコアが満たされていると判断します。

しきい値スコアリング マルチパート/代替 MIME 部分

カウントの重複を避けるため、同じコンテンツの2つの表現（プレーン テキストとHTML）がある場合、AsyncOSは重複した部分からの一致を合計しません。代わりに、各部分の一致を比較して、最高値を選択します。AsyncOSはこの値をマルチパート メッセージの他の部分からのスコアに追加して、合計スコアを作成します。

たとえば、`body-contains`フィルタ ルールを設定し、しきい値を4に設定します。プレーン テキスト、HTML、および2つの添付ファイルを含むメッセージを受信します。メッセージは次のような構造を使用します。

```
multipart/mixed

        multipart/alternative

                text/plain

                text/html

        application/octet-stream

        application/octet-stream
```

`body-contains`フィルタ ルールは、メッセージのtext/plainおよびtext/html部分を最初に採点して、このメッセージのスコアを判断します。次に、これらのスコアの結果を比較し、結果から最高のスコアを選択します。さらに、この結果を各添付ファイルからのスコアに追加して、最終スコアを判断します。メッセージに次の数の一致があるとします。

```
multipart/mixed

        multipart/alternative

                text/plain (2 matches)

                text/html (2 matches)

        application/octet-stream (1 match)

        application/octet-stream
```

AsyncOSはtext/plainとtext/html部分の一致を比較するため、スコア3を返します。これは、フィルタ ルールをトリガーする最小しきい値を満たしていません。

コンテンツ ディクショナリを使用したしきい値のスコアリング

コンテンツディクショナリを使用すると、用語の「重み」を設定して、より簡単に特定の用語でフィルタ アクションをトリガーできます。たとえば、「bank」という用語ではメッセージ フィルタをトリガーせず、「bank」の後に「account」という用語があり、さらにABAルーティング番号が含まれていれば、フィルタアクションをトリガーする必要があるとします。これを実現するには、重みを設定したディクショナリを使用して、特定の用語または用語の組み合わせの重要度を高くします。コンテンツ ディクショナリを使うメッセージ フィルタがフィルタ ルールの一致を評価する場合、コンテンツディクショナリの重みを使用して最終的なスコアを決定します。たとえば、次のコンテンツと重みを指定してコンテンツディクショナリを作成したとします。

表 *20*：コンテンツ ディクショナリの例

用語/スマート ID	重み
ABA 送金番号	3
アカウント（Account）	2
バンク	1

このコンテンツ ディクショナリを `dictionary-match` または `attachment-dictionary-match` メッセージ フィルタ ルールに関連付けると、AsyncOS はメッセージ内で検出された一致する用語の各インスタンスの合計「スコア」に、この用語の重みを追加します。たとえば、メッセージ本文に用語「account」のインスタンスが 3 つ含まれているメッセージの合計スコアに、値 6 が追加されます。メッセージ フィルタのしきい値が 6 に設定されている場合、AsyncOS はこのしきい値スコアが満たされたと判断します。または、各用語のインスタンスが 1 つずつ含まれている場合も合計値は 6 になり、このスコアによってフィルタ アクションがトリガーされます。

メッセージ フィルタ内の AND テストと OR テスト

メッセージ フィルタ内で、AND または OR テストを評価する場合、AsyncOS は不要なテストを評価しません。したがって、たとえば、一方の AND テストが false の場合、もう一方のテストは評価されません。テストは左から右に評価されるわけではないため、注意してください。代わりに、AND および OR テストが評価される場合、最も価値の低いテストが最初に評価されます。たとえば、次のフィルタでは、`rcpt-to-group` テストよりも消費リソースの少ない `remote-ip` テストが必ず最初に評価されます（一般に、LDAP テストの方が消費リソースは高くなります）。

```
andTestFilter:

if (remote-ip == "192.168.100.100" AND rcpt-to-group == "GROUP")

  { ... }
```

最もコストの低いテストが最初に実行されるため、項目の順序を入れ替えても影響はありません。テストの実行順序を保証する必要がある場合は、if文をネストさせてください。この方法は、できる限りコストの高いテストを避けるためにも推奨します。

```
expensiveAvoid:

if (<simple tests>)

  { if (<expensive test>)

    { <action> }

  }
```

次に、もう少し複雑な例で説明します。

```
if (test1 AND test2 AND test3) { ... }
```

システムは左から右に式をグループ化するため、次のようになります。

```
if ((test1 AND test2) AND test3) { ... }
```

この場合、システムが最初に行うのは、(`test1` AND `test2`) のコストと `test3` のコストの比較です。最初に 2 番目の AND を評価します。3 つのテストすべてで同じコストがかかる場合、`test3` が最初に実行されます。これは、(`test1` AND `test2`) のコストが 2 倍になるためです。

メッセージ フィルタ ルール

各メッセージフィルタには、フィルタを適用できるメッセージのコレクションを定義するルールが含まれています。フィルタ ルールを定義して、true を返すメッセージへのフィルタ アクションを定義します。

関連項目

- フィルタ ルールの概要の表 （165 ページ）
- ルールで使用する正規表現 （181 ページ）
- スマート ID （186 ページ）
- メッセージ フィルタ アクションの説明と例 （239 ページ）

フィルタ ルールの概要の表

次の表 に、メッセージ フィルタで使用できるルールをまとめます。

表 *21 :* メッセージ フィルタ ルール

ルール	構文	説明
件名ヘッダー（Subject Header）	`subject`	件名ヘッダーが特定のパターンと一致しているか。subject ルール（190ページ）を参照してください。
本文サイズ（Body Size）	`body-size`	本文のサイズは一定の範囲内か。本文サイズ ルール（193ページ）を参照してください。
エンベロープ送信者（Envelope Sender）	`mail-from`	エンベロープ送信者（Envelope From, <MAIL FROM>）が指定したパターンと一致しているか。エンベロープ送信者ルール（192ページ）を参照してください。
グループ内のエンベロープ送信者（Envelope Sender in Group）	`mail-from-group`	エンベロープ送信者（Envelope From <MAIL FROM>）が、指定した LDAP グループ内に存在するか。グループ内エンベロープ送信者ルール（192ページ）を参照してください。
送信者グループ（Sender Group）	`sendergroup`	どの送信者グループが、リスナーのホストアクセステーブル（HAT）に一致するか。送信者グループ ルール（193ページ）を参照してください。

ルール	構文	説明
グループ内エンベロープ（Envelope Recipient）	`rcpt-to`	エンベロープ受信者（Envelope To, <RCPT TO>）が指定したパターンと一致しているか。エンベロープ受信者ルール（191ページ）を参照してください。 （注） `rcpt-to` ルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか 1 人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。
グループ内エンベロープ受信者（Envelope Recipient in Group）	`rcpt-to-group`	エンベロープ受信者（Envelope To, <RCPT TO>）が、指定した LDAP グループ内に存在するか。グループ内エンベロープ受信者ルール（191 ページ）を参照してください。 （注） `rcpt-to-group` ルールはメッセージに基づいています。メッセージに複数の受信者がある場合、グループの受信者が 1 人でも検出されれば、rcptthe により指定されたアクションがメッセージのすべての受信者に適用されます。

ルール	構文	説明
リモートIP（Remote IP）	`remote-ip`	リモート ホストから送信されたメッセージは、指定した IP アドレスまたは IP ブロックに一致しているか。リモート IP ルール（194ページ）を参照してください。
受信インターフェイス（Receiving Interface）	`recv-int`	メッセージは、指定された受信インターフェイス経由で届いたか。を参照してください。受信 IP インターフェイス ルール （195 ページ）
受信リスナー（Receiving Listener）	`recv-listener`	メッセージは、指定されたリスナー経由で届いたか。受信リスナー ルール （194ページ）を参照してください。
日付（Date）	`date`	現在時刻は特定の日時の前か後か。日付ルール （195 ページ）を参照してください。
ヘッダー（Header）	`header(<string>)`	メッセージに特定のヘッダーが含まれているか。ヘッダーの値が特定のパターンと一致しているか。ヘッダー ルール（195ページ）を参照してください。
ランダム（Random）	`random(<integer>)`	ランダム番号は一定の範囲内か。乱数ルール （196ページ）を参照してください。
受信者数（Recipient Count）	`rcpt-count`	この電子メールの受信者の人数。受信者数ルール （197ページ）を参照してください。
アドレス数（Address Count）	`addr-count()`	受信者の累積数。 このフィルタは、エンベロープの受信者ではなくメッセージ本文のヘッダーに対して機能する点が rcpt-count フィルタ ルールと異なります。アドレス数ルール （197ページ）を参照してください。

ルール	構文	説明
SPFステータス（SPF Status）	`spf-status`	SPF 検証ステータスを判別します。このフィルタ ルールでは、さまざまな SPF 検証結果をクエリーできます。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。SPF-Status ルール （204 ページ）を参照してください。
SPF合格（SPF Passed）	`spf-passed`	SPF/SIDF 検証に合格したか。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。SPF-Passed ルール （206ページ）を参照してください。
S/MIME ゲートウェイ メッセージ（S/MIME Gateway Message）	`smime-gateway`	メッセージは S/MIME 署名されているか、暗号化されているか、または署名および暗号化されているか。S/MIME ゲートウェイ メッセージ ルール （206ページ）を参照してください。
S/MIME ゲートウェイ検証済	`smime-gateway-verified`	S/MIME メッセージは正常に検証されているか、復号されているか、または復号および検証されているか。S/MIME ゲートウェイ検証済みルール （206ページ）を参照してください。
イメージ評価（Image verdict）	`image-verdict`	イメージ スキャンの評価の結果。このフィルタ ルールを使用して、さまざまなイメージ分析の評価について問い合わせることができます。イメージ分析 （264ページ）を参照してください。
ワークキュー数（Workqueue count）	`workqueue-count`	ワーク キュー数と指定した値の比較結果（等しい、多い、少ない）。workqueue-count ルール （206ページ）を参照してください。

ルール	構文	説明
本文スキャン（Body Scanning）	`body-contains(<regular expression>)`	指定したパターンと一致するテキストまたは添付ファイルがメッセージに含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 エンジンは、配信ステータス部分と関連する添付ファイルをスキャンします。 本文スキャン （198 ページ）を参照してください。
本文スキャン（Body Scanning）	`only-body-contains (<regular expression>)`	指定したパターンと一致するテキストがメッセージ本文に含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。添付ファイルはスキャンされません。本文スキャン ルール （197 ページ）を参照してください。
暗号化検出（Encryption Detection）	`encrypted`	メッセージは暗号化されているか。暗号化検出ルール （198 ページ）を参照してください。
添付ファイル名（Attachment Filename）	`attachment-filename`	指定したパターンと一致するファイル名の添付ファイルがメッセージに含まれているか。添付ファイル名ルール （200ページ）を参照してください。
添付ファイルのタイプ	`attachment-type`	特定の MIME タイプの添付ファイルがメッセージに含まれているか。添付ファイル タイプ ルール （199 ページ）を参照してください。

ルール	構文	説明
添付ファイル タイプ（Attachment File Type）	`attachment-filetype`	フィンガープリントに基づく特定のパターンと一致するファイル タイプの添付ファイルがメッセージに含まれているか（UNIX の `file` コマンドと同様）。添付ファイルが Excel または Word ドキュメントである場合、埋め込みファイル タイプの .exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、.png、および Photoshop イメージを検索することもできます。 有効なフィルタを作成するには、ファイル タイプを引用符で囲む必要があります。一重引用符または二重引用符を使用できます。たとえば、.exe 添付ファイルを検索するには、次の構文を使用します。 `if (attachment-filetype == "exe")` 詳細については、添付ファイル名とアーカイブ ファイル内の単独の圧縮ファイル （200 ページ）を参照してください。

ルール	構文	説明
Attachment MIME Type	`attachment-mimetype`	特定の MIME タイプの添付ファイルがメッセージに含まれているか。このルールは `attachment-type` ルールに似ていますが、MIME 添付ファイルで指定された MIME タイプのみが評価される点が異なります。（電子メールゲートウェイは、ファイルタイプが明示的に指定されていない場合、拡張子からファイルのタイプを「予測」することはありません。）添付ファイルのスキャン メッセージ フィルタの例（269ページ）を参照してください。
添付ファイルハッシュリスト	`attachment-hashlist-match`	メッセージに、ファイルハッシュリスト内の特定ファイルの SHA-256 値と一致する添付ファイルが含まれているどうかを判別します。ファイル SHA-256 フィルタに一致するメッセージ添付ファイルをドロップする（297ページ）および添付ファイルがファイル SHA-256 フィルタと一致する場合にメッセージをドロップする（297ページ）を参照してください。
保護された添付ファイル（Attachment Protected）	`attachment-protected`	パスワード保護された添付ファイルがメッセージに含まれているか。保護された添付ファイルの隔離（272ページ）を参照してください。

ルール	構文	説明
保護されていない添付ファイル（Attachment Protected）	`attachment-unprotected`	attachment-unprotected フィルタ条件は、保護されていない添付ファイルをスキャン エンジンが検出した場合に true を返します。スキャン エンジンが添付ファイルを読み取ることができた場合、そのファイルは保護されていないと見なされます。zip ファイルに保護されていないメンバが含まれている場合、その zip ファイルは保護されていないと見なされます。 **注**：attachment-unprotected フィルタ条件と attachment-protected フィルタ条件は、相互に排他的ではありません。同じ添付ファイルをスキャンすると、両方のフィルタ条件で true が返される場合があります。これは、たとえば、zip ファイルに保護されたメンバと保護されていないメンバの両方が含まれている場合に発生します。 保護されていない添付ファイルの検出（272ページ）を参照してください。

ルール	構文	説明
添付ファイルのスキャン（Attachment Scanning）	`attachment-contains (<regular expression>)`	指定したパターンと一致するテキストまたは別の添付ファイルが、メッセージの添付ファイルに含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 このルールは`body-contains()`ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。添付ファイルのスキャン メッセージ フィルタの例（269ページ）を参照してください。
添付ファイルのスキャン（Attachment Scanning）	`attachment-binary-contains (<regular expression>)`	指定したパターンと一致するバイナリ データが存在する添付ファイルがメッセージに含まれているか。 このルールは`attachment-contains ()`ルールに似ていますが、バイナリ データ内のパターンのみを検索します。

ルール	構文	説明
添付ファイルのスキャン（Attachment Scanning ）	`every-attachment-contains (<regular expression>)`	このメッセージのすべての添付ファイルに、特定のパターンと一致するテキストが含まれているか。対象のテキストがすべての添付ファイル内に存在する必要があります。つまり実際に実行されるアクションは、各添付ファイルに対する「`attachment-contains()`」の論理AND演算です。本文はスキャンされません。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 添付ファイルのスキャン メッセージフィルタの例（269ページ）を参照してください。
添付ファイルのサイズ	`attachment-size`	メッセージに含まれている添付ファイルのサイズが特定の範囲内に収まっているか。このルールは `body-size` ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。このサイズは、デコードする前に評価されます。添付ファイルのスキャン メッセージフィルタの例（269ページ）を参照してください。
パブリックブロックリスト	`dnslist(<query server>)`	送信者の IP アドレスがパブリック ブラックリスト サーバ（RBL）内に存在するか。DNS リスト ルール （201 ページ）を参照してください。

ルール	構文	説明
IP レピュテーション（IP Reputation）	`reputation`	送信者の IP レピュテーション スコアはいくつか。IP レピュテーションルール （202 ページ）を参照してください。
IP レピュテーションなし（No IP Reputation）	`no-reputation`	IP レピュテーションスコアが「None」の場合に使用されます。IP レピュテーションルール（202ページ）を参照してください。
ディクショナリ	`dictionary-match (<dictionary_name>)`	メッセージ本文に、*dictionary_name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。ディクショナリ ルール（202ページ）を参照してください。
添付ディクショナリ一致（Attachment Dictionary Match）	`attachment-dictionary-match (<dictionary_name>)`	添付ファイルに、*dictionary_name* で指定した名前のコンテンツ ディクショナリの正規表現が含まれているかどうかを判別します。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。ディクショナリ ルール（202ページ）を参照してください。
件名ディクショナリ一致（Subject Dictionary Match）	`subject-dictionary-match (<dictionary_name>)`	件名ヘッダーに、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。ディクショナリ ルール （202 ページ）を参照してください。

ルール	構文	説明
ヘッダーディクショナリ一致（Header Dictionary Match）	`header-dictionary-match (<dictionary_name>, <header>)`	指定したヘッダー（大文字と小文字を区別）に、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。ディクショナリ ルール （202 ページ）を参照してください。
本文ディクショナリ一致（Body Dictionary Match）	`body-dictionary-match (<dictionary_name>)`	このフィルタ条件は、辞書の用語がメッセージ本文に含まれていれば true を返します。このフィルタは、添付ファイルであると判断されないMIME部分の用語に一致します。また、ユーザが定義したしきい値が満たされた場合も true を返します（デフォルトのしきい値は 1 です）。ディクショナリ ルール （202 ページ）を参照してください。
エンベロープ受信者ディクショナリ一致（Envelope Recipient Dictionary Match）	`rcpt-to-dictionary-match (<dictionary_name>)`	エンベロープ受信者に、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。ディクショナリ ルール（202ページ）を参照してください。
エンベロープ送信者ディクショナリ一致（Envelope Sender Dictionary Match）	`mail-from-dictionary-match (<dictionary_name>)`	エンベロープ送信者に、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。ディクショナリ ルール（202ページ）を参照してください。

ルール	構文	説明
SMTP認証済みユーザー一致（SMTP Authenticated User Match）	`smtp-auth-id-matches (<target>[, <sieve-char>])`	エンベロープ送信者のアドレスとメッセージ ヘッダーのアドレスが、送信者の認証済み SMTP ユーザー ID と一致するかどうかを判別します。SMTP認証済みユーザー一致ルール（207ページ）を参照してください。
はい（True）	`true`	すべてのメッセージと一致します。true ルール （190 ページ）を参照してください。
有効（Valid）	`valid`	メッセージに解析不能または無効な MIME 部分がある場合に false を返し、それ以外の場合は true を返します。有効なルール（190ページ）を参照してください。
署名済み（Signed）	`signed`	メッセージが署名済みであるかどうかを判別します。署名付きルール（209ページ）を参照してください。
署名証明書（Signed Certificate）	`signed-certificate (<field> [<operator> <regular expression>])`	メッセージ署名者またはX.509証明書発行者が特定のパターンと一致するかどうかを判別します。署名付き証明書ルール（209ページ）を参照してください。

ルール	構文	説明
ヘッダー繰り返し回数（Header Repeats）	`header-repeats (<target>, <threshold> [, <direction>])`	任意の時点で次の条件のメッセージが指定された数だけ検出されると、`true` を戻します。 • 過去 1 時間の同一件名ヘッダーを持つメッセージ • 過去 1 時間の同一のエンベロープ送信者からのメッセージ ヘッダー繰り返し回数ルール（212ページ）を参照してください。
URLレピュテーション（URL Reputation）	`url-reputation` `url-no-reputation`	メッセージに含まれている任意の URL のレピュテーションスコアが、指定された範囲内にあるかどうか。 URL のレピュテーション スコアが使用できないかどうか。 URL レピュテーション ルール（214ページ）および外部脅威フィードを使用する電子メールゲートウェイの設定 （355ページ）を参照してください。
URL のカテゴリ（URL Category）	`url-category`	メッセージに含まれている任意の URL のカテゴリが、指定されたカテゴリに一致するかどうか。 URL カテゴリ ルール （215ページ）を参照してください。

ルール	構文	説明
破損した添付ファイル（Corrupt Attachment）	`attachment-corrupt`	破損した添付ファイルがメッセージに含まれているかどうか。 破損した添付ファイル ルール（215ページ）を参照してください。
メッセージ言語	`message-language`	メッセージ（件名と本文）は選択したいずれかの言語であるか。 メッセージ言語ルール（216ページ）を参照してください。
マクロ検出	`macro-detection-rule (['file_type-1', 'file_type-2', …,'file_type-n'])`	受信または送信メッセージにマクロが有効な添付ファイルが含まれているか。 マクロ検出ルール（217ページ）を参照してください。
偽装メールの検出	`forged-email-detection ("<dictionary_name>", <threshold>)`	メッセージの送信元アドレスが偽装されているか。メッセージの From: ヘッダーがコンテンツ辞書のユーザに類似している場合にチェックするルールです。 偽造メールの検出ルール（218ページ）を参照してください。
重複境界検証	`duplicate_boundaries`	そのメッセージに、重複する MIME 境界が含まれるか。 重複境界検証ルール（219ページ）を参照してください。
不正な形式の MIME ヘッダーの検出（Malformed MIME Header Detection）	`malformed-header`	メッセージに不正な形式の MIME ヘッダーが含まれているか。 不正な形式の MIME ヘッダー検出ルール（219ページ）を参照してください。

ルール	構文	説明
位置情報（GeoLocation）	`geolocation-rule (['country_name-1', 'country_name-2', 'country_name-n'])`	受信メッセージは、選択した国から発信されましたか。 （注） 位置情報メッセージ フィルタ ルールを使用する前に、アプライアンス上でスパム対策エンジンを有効にします。 地理位置情報ルール（219ページ）を参照してください。

ドメインのレピュテーション	`Sender Domain Reputation: - sdr-reputation (<'sdr_verdict_range'>, <'domain_exception _list'>) - sdr-age (<'unit'>, <'operator'> <'actual value'>) - sdr-unscannable (<'domain_exception _list'>)`
	
	`External Threat Feeds: domain-external- threat-feeds (<'external_threat_ feed_source_name'>, <'header'> , <'domain _exception_list'>)`
		送信者ドメインは、指定された基準と一致していますか?
		• 送信者ドメインのレピュテーション
		• 外部脅威フィード
		ETF のドメイン レピュテーション ルール（220 ページ）またはSDR のドメイン レピュテーション ルール（220 ページ）を参照してください。
		詳細については、外部脅威フィードを使用する電子メール ゲートウェイの設定（355 ページ）または送信者ドメイン レピュテーション フィルタリング（381 ページ）を参照してください。

電子メールゲートウェイに送信されるメッセージはいずれも、すべてのメッセージフィルタで順番に処理されますが、最終アクションを指定した場合はそのアクションによりメッセージに対する以降の処理が停止されます。（メッセージ フィルタ アクション（157 ページ）を参照。）フィルタはすべてのメッセージに適用することもできます。また、ルールは論理接続子（AND、OR、NOT）を使用して結合することもできます。

ルールで使用する正規表現

ルールの定義に使用するアトミックテストの一部では、正規表現照合を行います。正規表現は複雑になる場合があります。次の表は、メッセージ フィルタ ルールで正規表現を適用する場合の目安として使用してください。

表 *22 :* ルールで使用する正規表現

正規表現（abc）	フィルタ ルールの正規表現が文字列と一致すると判断されるのは、正規表現の一連の指示が文字列のいずれかの部分と一致する場合です。 たとえば、正規表現「Georg」は「George Of The Jungle」、「Georgy Porgy」、「La Meson Georgette as well as Georg」の各文字列と一致します。
カレット (^) ドル記号（$）	ドル記号（$）を含むルールは文字列の末尾のみと一致し、キャラット（^）を含むルールは文字列の先頭のみと一致します。 たとえば、正規表現「^Georg$」は文字列「Georg」のみと一致します。 空のヘッダーを検索するには、「"^$"」と指定します。
文字、空白、アットマーク（@）	文字、空白、アットマーク（@）を含むルールは、当該の文字自体と完全に一致します。 たとえば、正規表現「^George@admin$」は文字列「George@admin」のみと一致します。
ピリオド文字（.）	ピリオド（.）を含むルールは任意の 1 文字（改行を除く）と一致します。 たとえば、「^...admin$」という正規表現は「macadmin」および「sunadmin」の各文字列とは一致しますが、「win32admin」とは一致しません。
アスタリスク（*）命令	アスタリスク（*）を含むルールは、「直前に指定されている文字が 0 回を含む任意の回数繰り返されている文字」と一致します。ピリオドとアスタリスクが続く場合（.*）は、任意の文字列（改行を除く）と一致します。 たとえば、「^P.*Piper$」という正規表現は、「PPiper」、「Peter Piper」、「P.Piper」、「Penelope Penny Piper」のどの文字列とも一致します。
バックスラッシュ特殊文字（\）	円記号は特殊文字のエスケープに使用します。シーケンス「\.」はピリオドそのもののみに一致し、「\$」はドル記号のみに一致し、「\^」はキャレット記号のみに一致します。たとえば、「^ik\.ac\.uk$」は「ik.ac.uk」という文字列のみと一致します。 **重要**：円記号はパーサーでも特殊なエスケープ文字として使用します。そのため、正規表現で円記号を使用する場合、2 つの円記号が必要です。解析後には「実際に」使用される円記号 1 つのみが残り、正規表現システムに渡されます。上記の例を照合する場合は「^ik\\.ac\\.uk$」と入力することになります。

大文字と小文字を区別しない（`(?i)`）	トークン (?i) は、正規表現の残りの部分で大文字と小文字が区別されないことを表します。このトークンを、大文字と小文字を区別する正規表現の先頭に配置すると、大文字と小文字が一切区別されない照合が行われます。 たとえば、「`(?i)viagra`」という正規表現は、「`Viagra`」、「`vIaGrA`」、「`VIAGRA`」と一致します。
繰り返し回数 `{min,max}`	1 つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。 たとえば、「`fo{2,3}`」は「`foo`」および「`fooo`」とは一致しますが、「fo」や「fofo」とは一致しません。 `if(header('To') == "^.{500,}")` というステートメントは、500 文字以上が使用されている「To」ヘッダーを検索します。
または (|)	代替、つまり「or」演算子に相当します。「A および B」が正規表現である場合、「`A|B`」は「A」と「B」のいずれかに一致する文字列と一致します。 たとえば、「`foo|bar`」という表現は「`foo`」や「`bar`」とは一致しますが、「`foobar`」とは一致しません。

関連項目

- メッセージのフィルタリングでの正規表現の使用 （183 ページ）
- 正規表現の使用に関するガイドライン （184 ページ）
- 正規表現と非 ASCII 文字セット （184 ページ）
- n テスト （184 ページ）
- 大文字と小文字の区別 （184 ページ）
- 効率的なフィルタの作成 （185 ページ）
- PDF と正規表現 （185 ページ）

メッセージのフィルタリングでの正規表現の使用

フィルタを使用して、ASCII 以外の形式でエンコードされているメッセージの内容（ヘッダーと本文）の文字列とパターンを検索できます。具体的には、本システムでは次の場所にある非 ASCII 文字を検索する正規表現（regex）を使用できます。

- メッセージ ヘッダー
- MIME 添付ファイル名の文字列
- メッセージ本文：
  - MIME ヘッダーがない本文（従来の形式の電子メール）
  - エンコードを示す MIME ヘッダーがあり、MIME 部分がない本文
  - エンコードが指定されているマルチパート MIME メッセージ
  - 上記の本文のうち、MIME ヘッダーでエンコードが指定されていないもの

メッセージまたは本文の任意の部分（添付ファイルを含む）の照合に正規表現を使用できます。添付ファイルのタイプとして HTML、MS Word、Excel など多数のタイプを対象にできます。対象となる文字セットとして、gb2312、HZ、EUC、JIS、Shift-JIS、Big5、Unicode などがあります。正規表現のメッセージ フィルタ ルールを作成するには、コンテンツ フィルタ GUI を使用するか、テキストエディタでファイルを作成してからシステムにインポートします。詳細については、「CLI を使用したメッセージ フィルタの管理 （273 ページ）」および「スキャン動作の設定 （297 ページ）」を参照してください。

正規表現の使用に関するガイドライン

プレフィックスではなく文字列全体を照合する場合は、正規表現の先頭にキャレット（^）、末尾にドル記号（$）をそれぞれ配置する必要があります。

（注） 空の文字列を照合する場合に「」を使用すると、実際にはすべての文字列が一致します。代わりに、「^$」を使用してください。たとえば、subject ルール （190 ページ）の 2 番目の例がこれに該当します。

また、文字としてのピリオドを照合するには、正規表現でピリオドをエスケープする必要があります。たとえば、sun.com という正規表現は「thegodsunocommando」という文字列と一致しますが、^sun\.com$ という正規表現は「sun.com」という文字列のみと一致します。

技術的には、ここで使用する正規表現のスタイルは **Python re Module** モジュール スタイルの正規表現です。Python スタイルの正規表現の詳細については、http://www.python.org/doc/howto/ からアクセスできる「Python Regular Expression HOWTO」を参考にしてください。

正規表現と非 ASCII 文字セット

一部の言語では、「単語」や「単語境界」、「大文字と小文字」という概念が存在しません。

単語を構成する文字（正規表現で「\w」と表される文字）の識別などが必要になる複雑な正規表現では、ロケールが不明な場合、またはエンコードが不明な場合、問題が発生します。

n テスト

正規表現の照合テストは、シーケンス == とシーケンス != を使用して行うことができます。次に例を示します。

```
rcpt-to ==
 "^goober@dev\\.null\\....$" (matching)


rcpt-to != "^goober@dev\\.null\\....$" (non-matching)
```

大文字と小文字の区別

特に明記されている場合を除き、正規表現では大文字と小文字が区別されます。正規表現で foo を検索する場合、FOO や Foo は一致しません。

効率的なフィルタの作成

次の例は、同じ処理を行う 2 つのフィルタですが、最初の例の方が CPU の使用率が高くなります。2 番目のフィルタの方が効率的な正規表現を使用しています。

```
attachment-filter: if ((recv-listener == "Inbound") AND
((((((((((((((((((((((((((((((((((((((((((((((((((attachment-filename ==

"\\.386$") OR (attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.ad$"))
 OR
(attachment-filename == "\\.ade$")) OR (attachment-filename == "\\.adp$")) OR
(attachment-filename == "\\.asp$")) OR (attachment-filename == "\\.bas$")) OR
(attachment-filename == "\\.bat$")) OR (attachment-filename == "\\.chm$")) OR
(attachment-filename == "\\.cmd$")) OR (attachment-filename == "\\.com$")) OR
(attachment-filename == "\\.cpl$")) OR (attachment-filename == "\\.crt$")) OR
(attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.hlp$")) OR
(attachment-filename == "\\.hta$")) OR (attachment-filename == "\\.inf$")) OR
(attachment-filename == "\\.ins$")) OR (attachment- filename == "\\.isp$")) OR
(attachment-filename == "\\.js$")) OR (attachment-filename == "\\.jse$")) OR
(attachment- filename == "\\.lnk$")) OR (attachment-filename == "\\.mdb$")) OR
(attachment-filename == "\\.mde$")) OR (attachment-filename == "\\.msc$")) OR
(attachment-filename == "\\.msi$")) OR (attachment-filename == "\\.msp$")) OR
(attachment-filename == "\\.mst$")) OR (attachment-filename == "\\.pcd$")) OR
(attachment-filename == "\\.pif$")) OR (attachment-filename == "\\.reg$")) OR
(attachment-filename == "\\.scr$")) OR (attachment-filename == "\\.sct$")) OR
(attachment-filename == "\\.shb$")) OR (attachment-filename == "\\.shs$")) OR
(attachment-filename == "\\.url$")) OR (attachment-filename == "\\.vb$")) OR
(attachment-filename == "\\.vbe$")) OR (attachment-filename == "\\.vbs$")) OR
(attachment-filename == "\\.vss$")) OR (attachment-filename == "\\.vst$")) OR
(attachment-filename == "\\.vsw$")) OR (attachment-filename == "\\.ws$")) OR
(attachment-filename == "\\.wsc$")) OR (attachment-filename == "\\.wsf$")) OR
(attachment-filename == "\\.wsh$"))) { bounce(); }
```

この例では、AsyncOS は正規表現エンジンを 30 回（添付ファイルタイプと recv-listener のそれぞれに 1 回ずつ）起動する必要があります。

かわりに、次のようなフィルタを作成します。

```
attachment-filter: if (recv-listener == "Inbound") AND (attachment-filename == "\\.
(386|exe|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|l
nk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|
url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") {
```

正規表現エンジンの起動回数は 2 回だけで、「()」の追加やスペルの誤りについて心配する必要がなくなるためフィルタの管理も大幅に簡単になります。また、最初の例に比べて CPU オーバーヘッドが低下します。

PDF と正規表現

PDF の生成方法によっては、スペースや改行がないことがあります。このような場合、スキャン エンジンは、ページ内の単語の位置に基づき、論理的なスペースと改行の挿入を試みます。たとえば、1 つの単語の中に複数のフォントやフォント サイズが混在する場合、生成される PDF コードからスキャン エンジンが単語と改行を判別するのが難しくなります。このように生成された PDF ファイルで正規表現による照合を行うと、スキャン エンジンは予期しない結果を返す場合があります。

たとえば、PowerPoint 文書に挿入した単語の中に、単語内の文字ごとに異なるフォントやフォントサイズが設定されているものがあるとします。このアプリケーションから生成された PDF をスキャン エンジンが読み取ると、論理的なスペースと改行が挿入されます。PDF の構造が原因で、「callout」という単語が「call out」または「c a l lout」と解釈されることがあります。このいずれかの表現を正規表現「callout」と照合しようとすると、一致なしという結果になります。

スマート ID

メッセージの内容をスキャンするメッセージ ルールを使用する場合、スマート ID を使用するとデータ内の特定のパターンを検出できます。

スマート ID で、データ内の次のパターンを検出できます。

- クレジット カード番号
- 米国社会保障番号
- CUSIP ナンバー
- ABA ナンバー

フィルタでスマート ID を使用するには、本文または添付ファイルのコンテンツをスキャンするフィルタ ルールで次のキーワードを使用します。

表 *23 :* メッセージ フィルタのスマート *ID*

キーワード	スマート ID	説明
*credit	クレジット カード番号	14、15、および 16 桁のクレジット カード番号を識別します。 注意：スマート ID は enRoute カードを識別しません。
*aba	ABA 送金番号	ABA 送金番号を識別します。
*ssn	社会保障番号	米国社会保障番号を識別します。*ssn スマート ID はダッシュ、ピリオド、スペースがある社会保障番号を識別します。
*cusip	CUSIP 番号	CUSIP 番号を識別します。

関連項目

- スマート ID の構文 （186 ページ）

スマート ID の構文

フィルタ ルールでスマート ID を使用する場合、次の例のように、本文または添付ファイルをスキャンするフィルタ ルールの中でスマート ID キーワードを引用符で囲みます。

```
ID_Credit_Cards:
```

```
if(body-contains("*credit")){

notify("legaldept@example.com");

}
.
```

また、コンテンツ ディクショナリの一部としてコンテンツ フィルタ内でスマート ID を使用することもできます。

（注） スマート ID キーワードは通常の正規表現や他のキーワードと組み合わせて使用できません。たとえば、「`*credit|*ssn`」というパターンは有効ではありません。

（注） *ssn スマート ID による誤判定を防ぐため、*ssn スマート ID は他のフィルタ条件とあわせて使用すると有用な場合があります。たとえば、「only-body-contains」フィルタ条件を使用することができます。この場合、検索文字列がメッセージ本文のすべての MIME 部分に存在する場合のみ式が true であると判定されます。たとえば、次のようなフィルタを作成できます。

```
SSN-nohtml: if only-body-contains(“*ssn”) { duplicate-quarantine(“Policy”);}
```

（注） 電子メールゲートウェイは、メッセージコンテンツのプレフィックスとして追加されたキーワード(「credit」、「ssn」、「cusip」、または「aba」)の有無にかかわらず、スマート識別子を検出します。

例：メッセージに次のいずれかの形式の社会保障番号が含まれている場合、電子メールゲートウェイは社会保障番号をスマート識別子として検出します：

(「XXX-XX-XXXX」「ssn XXX-XX-XXXX」、「ssn: XXX-XX-XXXX」など。)

例：プレフィックスのないスマート識別子

次のフィルターを作成して、スマート識別子の前にキーワードが存在しないスマート識別子を検出します。

```
ID_Credit_Cards:
if(body-contains("*credit", 1))
{
notify("legaldept@example.com");
}
```

引数の説明

「 credit」はクレジットカード番号のスマート識別子を示し、

「1」は、ルールを「true」と評価するために必要な最低の一致数を示します。

例：プレフィックス付きのスマート識別子

次のフィルタを作成して、スマート識別子の前にキーワード((「credit」、「ssn」、「cusip」、または「aba」)が存在する場合にのみ、スマート識別子を検出します。

```
ID_Credit_Cards:
if(body-contains("*credit", 1, “prefix”))
{
notify("legaldept@example.com");
}
```

引数の説明

「 credit」はクレジットカード番号のスマート識別子を示し、

「1」は、ルールを「true」と評価するために必要な最低の一致数を示し、

「プレフィックス」は、スマート識別子の前にキーワードが付いている場合にのみ、ルールが「true」であることを示します。

メッセージ フィルタ ルールの説明と例

次のセクションでは、使用されるさまざまなメッセージ フィルタ ルールについて説明し、その例を示します。

関連項目

- true ルール （190 ページ）

• 有効なルール （190 ページ）
• subject ルール （190 ページ）
• エンベロープ受信者ルール （191 ページ）
• グループ内エンベロープ受信者ルール （191 ページ）
• エンベロープ送信者ルール （192 ページ）
• グループ内エンベロープ送信者ルール （192 ページ）
• 送信者グループ ルール （193 ページ）
• 本文サイズ ルール （193 ページ）
• リモート IP ルール （194 ページ）
• 受信リスナー ルール （194 ページ）
• 受信 IP インターフェイス ルール （195 ページ）
• 日付ルール （195 ページ）
• ヘッダー ルール （195 ページ）
• 乱数ルール （196 ページ）
• 受信者数ルール （197 ページ）
• アドレス数ルール （197 ページ）
• 本文スキャン ルール （197 ページ）
• 本文スキャン （198 ページ）
• 暗号化検出ルール （198 ページ）
• 添付ファイル タイプ ルール （199 ページ）
• 添付ファイル名ルール （200 ページ）
• DNS リスト ルール （201 ページ）
• IP レピュテーションルール （202 ページ）
• ディクショナリ ルール （202 ページ）
• SPF-Status ルール （204 ページ）
• SPF-Passed ルール （206 ページ）
• S/MIME ゲートウェイ メッセージ ルール （206 ページ）
• S/MIME ゲートウェイ検証済みルール （206 ページ）
• workqueue-count ルール （206 ページ）
• SMTP 認証済みユーザー一致ルール （207 ページ）
• 署名付きルール （209 ページ）
• ヘッダー繰り返し回数ルール （212 ページ）
• URL レピュテーション ルール （214 ページ）
• URL カテゴリ ルール （215 ページ）
• 破損した添付ファイル ルール （215 ページ）
• メッセージ言語ルール （216 ページ）
• マクロ検出ルール （217 ページ）
• 偽造メールの検出ルール （218 ページ）
• 重複境界検証ルール （219 ページ）
• 不正な形式の MIME ヘッダー検出ルール （219 ページ）
• 地理位置情報ルール （219 ページ）

- ETF のドメイン レピュテーション ルール （220 ページ）
- SDR のドメイン レピュテーション ルール （220 ページ）

true ルール

true ルールはすべてのメッセージと一致します。たとえば、次のルールはテスト対象となるすべてのメッセージについて、IP インターフェイスを external に変更します。

```
externalFilter:

   if (true)

   {

        alt-src-host('external');

   }
```

有効なルール

valid ルールは、メッセージに解析不能または無効な MIME 部分が含まれている場合に false を返し、それ以外の場合は true を返します。たとえば、次のルールはテスト対象のメッセージのうち解析不能なメッセージをすべてドロップします。

```
not-valid-mime:

if not valid

{

drop();

}
```

subject ルール

subject ルールは、件名ヘッダーの値が指定した正規表現と一致するメッセージを選択します。

たとえば、次のフィルタは、件名が「Make Money...」という語句で始まるすべてのメッセージを廃棄します。

```
not-valid-mime:

if not valid

{

drop();

}
```

ヘッダーの値で検索する非 ASCII 文字を指定することができます。

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してくだ

さい。詳細については、メッセージヘッダー ルールおよび評価（160 ページ）を参照してください。

次のフィルタは、ヘッダーが空の場合、またはメッセージにヘッダーがない場合にtrueを返します。

```
EmptySubject_To_filter:

if (header('Subject') != ".") OR

(header('To') != ".") {

drop();

}
```

（注） このフィルタはSubjectヘッダーとToヘッダーが空の場合にtrueを返しますが、ヘッダーがない場合もtrueを返します。指定したヘッダーがメッセージ内にない場合でも、このフィルタはtrueを返します。

エンベロープ受信者ルール

rcpt-toルールは、いずれかのエンベロープ受信者が指定した正規表現と一致するメッセージを選択します。たとえば、次のフィルタは「scarface」という文字列を含む電子メールアドレス宛てに送信されたすべてのメッセージをドロップします。

（注） rcpt-toルールで使用する正規表現では、大文字と小文字は区別されません。

```
scarfaceFilter:

if (rcpt-to == 'scarface')

{

drop();

}
```

（注） rcpt-toルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか1人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

グループ内エンベロープ受信者ルール

rcpt-to-groupルールは、いずれかのエンベロープ受信者が指定したLDAPグループのメンバであるメッセージを選択します。たとえば、次のフィルタは「ExpiredAccounts」というLDAPグループ内の電子メールアドレス宛てに送信されたすべてのメッセージをドロップします。

```
expiredFilter:

if (rcpt-to-group == 'ExpiredAccounts')

{

drop();

}
```

（注） rcpt-to-group ルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか 1 人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

エンベロープ送信者ルール

mail-from ルールは、エンベロープ送信者が指定した正規表現と一致するメッセージを選択します。たとえば、次のフィルタを実行すると admin@yourdomain.com により送信されたすべてのメッセージがただちに出力されます。

（注） mail-from ルールで使用する正規表現では、大文字と小文字は区別されません。次の例では、ピリオドがエスケープ処理されています。

```
kremFilter:

if (mail-from == '^admin@yourdomain\\.com$')

{

skip-filters();

}
```

グループ内エンベロープ送信者ルール

mail-from-group ルールは、エンベロープ送信者が演算子の右辺で指定した LDAP グループに属している（不一致を検索する場合は、送信者の電子メールアドレスが指定した LDAP グループに属していない）メッセージを選択します。たとえば、次のフィルタを実行すると、「KnownSenders」という LDAP グループの電子メールアドレスにより送信されたすべてのメッセージがただちに出力されます。

```
SenderLDAPGroupFilter:

if (mail-from-group == 'KnownSenders')

{

skip-filters();

}
```

送信者グループ ルール

sendergroup メッセージ フィルタは、リスナーのホスト アクセス テーブル（HAT）でどの送信者グループが一致するかに基づいて、メッセージを選択します。このルールは「==」（一致を検索する場合）または「!=」（不一致を検索する場合）を使用して、指定した正規表現（式の右辺）との一致をテストします。たとえば、次のメッセージ フィルタ ルールは、メッセージの送信者グループが正規表現「Internal」と一致する場合に true を返し、その場合はメッセージを代替メール ホストに送信します。

```
senderGroupFilter:

if (sendergroup == "Internal")

{

alt-mailhost("[172.17.0.1]");

}
```

本文サイズ ルール

本文サイズとはメッセージのサイズのことで、ヘッダーと添付ファイルも含みます。body-size ルールは、本文サイズを指定された数値と比較し、条件に一致するメッセージを選択します。たとえば、次のフィルタは本文サイズが 5 メガバイトを超えるすべてのメッセージをバウンスします。

```
BigFilter:

if (body-size > 5M)

{

bounce();

}
```

body-size を使用すると次のような比較ができます。

例	比較の種類
`body-size < 10M`	より少ない
`body-size <= 10M`	以下
`body-size > 10M`	右辺と比較して大きい
`body-size >= 10M`	以上
`body-size == 10M`	等しい
`body-size != 10M`	等しくない

サイズ指定にはサフィクスを使用すると便利です。

数量	説明
10b	10 バイト（「10」に同じ）
13k	13 キロバイト
5M	5 メガバイト
40G	40 ギガバイト（注：電子メールゲートウェイでは 100 メガバイトを超えるメッセージを処理できません）

リモート IP ルール

remote-ip ルールは、メッセージを送信したホストの IP アドレスが特定のパターンと一致するかどうかを確認するためのテストを実行します。IP アドレスは、インターネット プロトコル バージョン 4（IPv4）またはインターネット プロトコル バージョン 6（IPv6）を指定できます。IP アドレスパターンは、「送信者グループの構文」に記載されている allowed hosts 表記を使用して指定されます。ただし、SBO、IPR、dnslist 表記および特殊キーワード ALL を除きます。

allowed hosts 表記では、IP アドレス（ホスト名ではない）の順序と数値での範囲のみを指定できます。たとえば、次のフィルタは 10.1.1. の形式の IP アドレスからインジェクトされていない任意のメッセージをバウンスします。*x*、X は 50、51、52、53、54、または 55。

```
notMineFilter:

if (remote-ip != '10.1.1.50-55')

{

bounce();

}
```

受信リスナー ルール

recv-listener ルールは、名前付きリスナーで受信したメッセージを選択します。リスナー名は、現在システム上で設定されているリスナーのいずれかのニックネームである必要があります。たとえば、次のフィルタを実行すると、expedite という名前のリスナーから受信したすべてのメッセージがただちに出力されます。

```
expediteFilter:

if (recv-listener == 'expedite')

{

skip-filters();

}
```

受信 IP インターフェイス ルール

recv-int ルールは、名前付きインターフェイス経由で受信したメッセージを選択します。インターフェイス名は、現在システムに設定されているインターフェイスのいずれかのニックネームである必要があります。たとえば、次のフィルタは、outside という名前のインターフェイスから受信したすべてのメッセージをバウンスします。

```
outsideFilter:

if (recv-int == 'outside')

{

bounce();

}
```

日付ルール

date ルールは、現在の日時と指定した時刻を照合します。日付ルールは、*MM/DD/YYYY hh:mm:ss* という形式のタイムスタンプを含む文字列と比較されます。このルールは、特定の日時（米国形式）の前または後に実行する処理を指定する場合に便利です。（米国以外の日付形式を使用しているメッセージを検索する場合は問題が発生することがあります。）次のフィルタは、2003 年 7 月 28 日の午後 1 時より後に campaign1@yourdomain.com から送信されたすべてのメッセージをバウンスします。

```
TimeOutFilter:

if ((date > '07/28/2003 13:00:00') and (mail-from ==

'campaign1@yourdomain\\.com'))

{

bounce();

}
```

（注） date ルールを $Date メッセージ フィルタ処理変数と混同しないようにしてください。

ヘッダー ルール

header() ルールは、メッセージ ヘッダーがかっこ内で引用されている特定のヘッダー（“ヘッダー名”）と一致するかどうかを確認します。このルールは subject ルールと同様に正規表現と比較することもできますが、比較を行わずに使用することもできます。この場合、メッセージにそのヘッダーがあれば「true」、なければ「false」となります。たとえば、次の例ではヘッダー X-Sample の有無、およびこのヘッダーの値に「sample text」という文字列が含まれているかどうかを確認しています。一致する場合は、メッセージがバウンスされます。

```
FooHeaderFilter:

if (header('X-Sample') == 'sample text')
```

```
{

bounce();

}
```

ヘッダーの値で検索する非 ASCII 文字を指定することができます。

次の例では、比較を行わずにヘッダー ルールを適用しています。この場合、ヘッダー `X-DeleteMe` が見つかると、そのヘッダーがメッセージから削除されます。

```
DeleteMeHeaderFilter:

if header('X-DeleteMe')

{

strip-header('X-DeleteMe');

}
```

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージヘッダー ルールおよび評価（160 ページ）を参照してください。

乱数ルール

`random` ルールは、0 から N-1（N はルール名の後のかっこで指定される整数値）までの乱数を生成します。このルールでは `header()` ルールと同様に比較を行うこともできますが、「単項」形式で単独使用することもできます。単項形式では、生成された乱数が 0 でない場合に `true` と評価されます。たとえば、次のフィルタはいずれも内容としては同じもので、2 分の 1 の確率で Virtual Gateway アドレス A が選択され、残り 2 分の 1 の確率で Virtual Gateway アドレス B が選択されます。

```
load_balance_a:

if (random(10) < 5)
{

alt-src-host('interface_a');
}

else

{

alt-src-host('interface_b');

}

load_balance_b:

if (random(2))

{

alt-src-host('interface_a');

}
```

```
else

{

alt-src-host('interface_b');

}
```

受信者数ルール

rcpt-count ルールは、body-size ルールと同様に、メッセージの受信者の数を整数値と比較します。このルールを使用すると、ユーザが一度に多数のユーザに電子メールを送信することを防止でき、また大規模なメール送信キャンペーンが特定の Virtual Gateway アドレス経由で行われるようにすることができます。次の例では、受信者数が 100 件を超える電子メールが特定の Virtual Gateway アドレスを経由して送信されます。

```
large_list_filter:

if (rcpt-count > 100) {

alt-src-host('mass_mailing_interface');

}
```

アドレス数ルール

addr-count() メッセージ フィルタ ルールは、1 つ以上のヘッダー文字列を対象に、各行の受信者数を計算し、受信者の累積数をレポートします。このフィルタは、エンベロープの受信者ではなくメッセージ本文のヘッダーに対して機能する点が rcpt-count フィルタ ルールと異なります。次の例では、このフィルタ ルールにより長い受信者リストが「undisclosed-recipients」というエイリアスに置き換えられています。

```
count: if (addr-count("To", "Cc") > 30)
{
 strip-header("To");
 strip-header("Cc");
 insert-header("To", "undisclosed-recipients");
}
```

本文スキャン ルール

body-contains() ルールは、受信する電子メールとその添付ファイルをスキャンし、パラメータで定義された特定のパターンの有無を確認します。これには、配信ステータス部および関連付けられている添付ファイルが含まれます。body-contains() ルールでは複数行を対象とした照合は行われません。スキャンのロジックを [スキャン動作（Scan Behavior）] ページまたは CLI の scanconfig コマンドで変更することにより、スキャンの対象となる、またはスキャンの対象から除外する MIME タイプを定義できます。また、スキャン結果を true と評価するために検出する必要がある一致の最小数を指定することもできます。

デフォルトでは、MIME タイプが video/*、audio/*、image/* 以外であるすべての添付ファイルがスキャンされます。複数のファイルが含まれている .zip、.bzip、.compress、.tar、.gzip の

各アーカイブ添付ファイルがスキャンされます。スキャン対象となる、「ネストされた」アーカイブ添付ファイル（.zip に格納されている .zip など）の数を設定できます。

詳細については、スキャン動作の設定 （297 ページ）を参照してください。

本文スキャン

AsyncOS が本文スキャンを実行する場合、正規表現を使用して本文のテキストと添付ファイルをスキャンします。式には最小しきい値を指定することができ、スキャンエンジンがこの最小回数だけ正規表現との一致を検出すると、この式は true と評価されます。

AsyncOS はメッセージの各種の MIME 部分を評価し、テキスト形式になっているすべての MIME 部分をスキャンします。最初の部分で MIME タイプがテキストに指定されている場合、AsyncOS はテキスト部分を識別します。AsyncOS はメッセージで指定されたエンコードに基づいてエンコードを決定し、テキストを Unicode に変換します。その後、Unicode 領域で正規表現を検索します。メッセージでエンコードが指定されていない場合は、[スキャン動作（Scan Behavior）] ページまたは scanconfig コマンドで指定されたエンコードが使用されます。

メッセージのスキャン時に AsyncOS が MIME 部分を評価する方法の詳細については、メッセージ本文とメッセージ添付ファイル （160 ページ）を参照してください。

MIME 部分がテキストでない場合、AsyncOS は .zip または .tar からファイルを抽出するか、圧縮されたファイルを抽出します。データを抽出した後、スキャン エンジンはファイルのエンコードを識別し、ファイルのデータを Unicode 形式で返します。その後、AsyncOS は Unicode 領域で正規表現を検索します。

次の例では、本文のテキストと添付ファイルで「Company Confidential」という文字列を検索します。この例では、最小しきい値が 2 件に設定されているため、スキャンエンジンがこの文字列を 2 件以上検出すると、該当するメッセージをすべてバウンスし、法務部門に通知します。

```
ConfidentialFilter:

if (body-contains('Company Confidential',2)) {

notify ('legaldept@example.domain');

bounce();

}
```

メッセージの本文のみをスキャンする場合は、only-body-contains を使用します。

```
disclaimer:

if (not only-body-contains('[dD]isclaimer',1) ) {

notify('hresource@example.com');

}
```

暗号化検出ルール

encrypted ルールは、メッセージの内容に暗号化データが存在するかどうかを調査します。このルールは暗号化データのデコードは行わず、メッセージの内容に暗号化データが存在するか

どうかのみを調査します。このルールは、ユーザが暗号化された電子メールを送信できないようにする場合に便利です。

（注） 暗号化されたルールは、メッセージの内容の暗号化されたデータのみを検出できます。暗号化された添付ファイルは検出しません。

encrypted は `true` ルールと同様に、パラメータを使用せず、比較も行いません。暗号化されたデータが検出された場合に `true`、検出されなかった場合に `false` を返します。この機能を実行するにはメッセージのスキャンが必要になるため、[スキャン動作（Scan Behavior）] ページまたは `scanconfig` コマンドで定義されたスキャン設定が使用されます。オプションの設定の詳細については、スキャン動作の設定 （297 ページ）を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、メッセージに暗号化されたデータが含まれる場合は、該当するメッセージが BCC で法務部門宛てに送信され、バウンスされます。

```
prevent_encrypted_data:

if (encrypted) {

bcc ('legaldept@example.domain');

bounce();

}
```

添付ファイル タイプ ルール

`attachment-type` ルールはメッセージ内の各添付ファイルの MIME タイプを確認し、指定されたパターンと一致するかどうかを判別します。このパターンは[スキャン動作（Scan Behavior）] ページまたは `scanconfig` コマンドで使用する形式（スキャン動作の設定 （297 ページ）を参照）と同じ形式である必要があり、スラッシュ（/）の左右の一方でアスタリスクをワイルドカードとして使用できます。メッセージの添付ファイルがここで指定した MIME タイプと一致する場合、このルールは「true」を返します。

この機能を実行するにはメッセージのスキャンが必要となるため、スキャン動作の設定 （297 ページ）で説明されているすべてのオプションが適用されます。

メッセージの添付ファイルを操作するために使用できるメッセージ フィルタ ルールの詳細については、添付ファイルのスキャン （260 ページ）を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、MIME タイプが `video/*` である添付ファイルがメッセージに含まれる場合は、該当するメッセージがバウンスされます。

```
bounce_video_clips:

if (attachment-type == 'video/*') {

bounce();
```

```
}
```

添付ファイル名ルール

attachment-filename ルールはメッセージ内の各添付ファイルの名前を確認し、指定されたパターンと一致するかどうかを判別します。この比較では大文字と小文字は区別されます。この比較ではスペースの有無も区別されるため、ファイル名の末尾にスペースがある状態でエンコードされていると、フィルタはその添付ファイルをスキップします。メッセージの添付ファイルのいずれかが指定したファイル名と一致すると、このルールは true を返します。

次の点に注意してください。

- 各添付ファイルの名前はMIMEヘッダーからキャプチャされます。MIMEヘッダーにあるファイル名の末尾にはスペースがある場合があります。
- 添付ファイルがアーカイブの場合、電子メールゲートウェイはアーカイブの内部からファイル名を取得し、スキャン設定ルール（スキャン動作の設定 （297 ページ）を参照）を適用します。
  - 添付ファイルが 1 個の圧縮ファイル（拡張子を問わず）である場合、アーカイブであるとは見なされず、この圧縮ファイルの名前は取得されません。つまり、このファイルは attachment-filename ルールでは処理されません。このようなファイルの例としては、gzip で圧縮された実行可能ファイル（.exe）などがあります。
  - 添付ファイルが単独の圧縮ファイルである場合（foo.exe.gz など）、正規表現を使用して圧縮ファイル内の特定のファイルタイプを検索します。添付ファイル名とアーカイブ ファイル内の単独の圧縮ファイル （200 ページ）を参照してください。

メッセージの添付ファイルを操作するために使用できるメッセージ フィルタ ルールの詳細については、添付ファイルのスキャン （260 ページ）を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、ファイル名が *.mp3 である添付ファイルがメッセージに含まれる場合は、該当するメッセージがバウンスされます。

```
block_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

bounce();

}
```

関連項目

- 添付ファイル名とアーカイブ ファイル内の単独の圧縮ファイル （200 ページ）

添付ファイル名とアーカイブ ファイル内の単独の圧縮ファイル

次に、アーカイブ（gzip で作成したものなど）にある単独の圧縮ファイルを照合する例を示します。

```
quarantine_gzipped_exe_or_pif:

if (attachment-filename == '(?i)\\.(exe|pif)($|.gz$)') {

quarantine("Policy");

}
```

DNS リスト ルール

dnslist() ルールは、クエリの実行に DNSBL 方式（「ip4r ルックアップ」とも呼ばれます）を使用するパブリック DNS リスト サーバを照会します。着信接続の IP アドレスは反転され（IP が 1.2.3.4 の場合は 4.3.2.1 になり）、かっこ内のサーバ名にプレフィックスとして追加されます（サーバ名の先頭がピリオドでない場合は、サーバ名とプレフィックスを区切るためのピリオドが追加されます）。DNS クエリーが生成され、システムには DNS 失敗応答（接続の IP アドレスがサーバのリストにないことを示す）または IP アドレス（アドレスが見つかったことを示す）が返されます。返される IP アドレスは、通常、127.0.0 の形式でxx。ここで、x は、0 から 255 までのほぼ任意の数字です（IP アドレス範囲は許可されていません）。一部のサーバは、リスト生成の理由に基づいてそれぞれ異なる数字を返しますが、それ以外のサーバはすべての一致に対して同じ結果を返します。

dnslist() は、header() ルールと同様に、単項または二項比較で使用できます。単独では、応答を受信すると true を返し、応答がない場合（DNS サーバが到達不能の場合など）は false を返します。

次のフィルタを実行すると、送信者が Cisco Bonded Sender 情報サービス プログラムにボンドされている場合、そのメッセージがただちに出力されます。

```
allowedlist_bondedsender:

if (dnslist('query.bondedsender.org')) {

skip-filters();

}
```

オプションで、等式（==）または不等式（!=）を使用して結果を文字列と比較することもできます。

次のフィルタは、サーバから「127.0.0.2」が返されるメッセージをドロップします。応答がそれ以外の内容であれば、このルールは false を返し、フィルタは無視されます。

```
blockedlist:

if (dnslist('dnsbl.example.domain') == '127.0.0.2') {

drop();

}
```

IP レピュテーションルール

reputation ルールにより、IP レピュテーションスコアが他の値と比較してチェックされます。>、==、<= などのすべての比較演算子を使用できます。メッセージに IP レピュテーションスコアがない場合（これまでスコアがまったく確認されていないか、IP レピュテーション サービス クエリ サーバから応答を取得できなかった場合）、レピュテーションスコアとの比較はすべて失敗します（数値がいずれかの値より大きいまたは小さい、いずれかの値と等しいまたは等しくないという判別ができません）。次に説明する no-reputation ルールを使用すると、IP レピュテーションスコアが「none」であるかどうかを確認できます。次の例では、IP レピュテーションサービスから返されるレピュテーションスコアがしきい値の -7.5 を下回る場合に、メッセージの「Subject:」行の先頭に「*** BadRep ***」が付加されます。

```
note_bad_reps:

if (reputation < -7.5) {
strip-header ('Subject');
insert-header ('Subject', '*** BadRep $Reputation *** $Subject');
}
```

詳細については、「送信者レピュテーション フィルタリング」の章を参照してください。アンチスパム システムのバイパス アクション （253 ページ）も参照してください。

IP レピュテーションルールの値は -10 ～ 10 ですが、NONE という値が返される場合もあります。NONE について特に確認が必要な場合は、no-reputation ルールを使用します。

```
none_rep:

if (no-reputation) {

strip-header ('Subject');

insert-header ('Subject', '*** Reputation = NONE *** $Subject');

}
```

ディクショナリ ルール

メッセージ本文に、「dictonary_name」という名前のコンテンツ ディクショナリにある正規表現または用語が含まれている場合、dictionary-match(<dictonary_name>) ルールは true と評価されます。該当のディクショナリが存在しない場合は、ルールは false と評価されます。辞書の定義の詳細については（大文字と小文字の区別や単語境界の設定など）、「テキスト リソース」の章を参照してください。

次のフィルタは、シスコが「secret_words」という辞書にある単語を含むメッセージをスキャンすると、管理者にブラインド カーボン コピーを送信します。

```
copy_codenames:

if (dictionary-match ('secret_words')) {

bcc('administrator@example.com');

}
```

次の例では、メッセージの本文に、「secret_words」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。only-body-contains 条件とは異なり、body-dictionary-match 条件では、すべてのコンテンツ部分がそれぞれ個別に辞書に一致する必要はありません。各コンテンツ部分のスコア（マルチパート/代替部分も考慮されます）は合計されます。

```
quarantine_data_loss_prevention:

if (body-dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

次のフィルタでは、件名が指定した辞書にある単語と一致すると隔離されます。

```
quarantine_policy_subject:

if (subject-dictionary-match ('gTest'))

{

quarantine('Policy');

}
```

次の例では、「To」ヘッダーの電子メール アドレスを照合し、管理者にブラインド コピーを送信しています。

```
headerTest:

if (header-dictionary-match ('competitorsList', 'to'))

{

bcc('administrator@example.com');

}
```

attachment-dictionary-match(<dictonary_name>) ルールは上記の dictionary-match ルールと同様に機能しますが、検索対象は添付ファイルです。

次のフィルタでは、メッセージの添付ファイルに「secret_words」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。

```
quarantine_codenames_attachment:

if (attachment-dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

`header-dictionary-match(<dictonary_name>,<header>)` ルールは上記の dictionary-match ルールと同様に機能しますが、検索対象は *<header>* で指定したヘッダーです。ヘッダー名の大文字と小文字は区別されないため、たとえば「subject」でも「Subject」でも機能します。

次のフィルタでは、メッセージの「cc」ヘッダーに「ex_employees」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。

```
quarantine_codenames_attachment:

if (header-dictionary-match ('ex_employees', 'cc'))

{

quarantine('Policy');

}
```

辞書用語内でワイルドカードを使用することができます。電子メールアドレスのピリオドをエスケープする必要はありません。

SPF-Status ルール

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。spf-status ルールを使用すると、複数の SPF 検証結果との照合が可能になります。詳細については、検証結果（773 ページ）を参照してください。

（注） SPF 識別情報なしで SPF 検証メッセージ フィルタ ルールを設定している場合、メッセージに判定が異なる別の SPF 識別情報が含まれているときは、そのルールは、メッセージ内の判定のいずれかがルールと一致するとトリガーされます。

SPF/SIDF 検証結果との照合を行うには、次の構文を使用します。

```
if (spf-status == "Pass")
```

1 つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```

次の例に、spf-status フィルタの使用例を示します。

```
skip-spam-check-for-verified-senders:

if (sendergroup == "TRUSTED" and spf-status == "Pass"){
```

```
skip-spamcheck();
}
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
if (spf-status("mailfrom") == "Fail"){
# completely malicious mail
quarantine("Policy");
} else {
if(spf-status("mailfrom") == "SoftFail") {
# malicious mail, but tempting
quarantine("Policy");
}
}
} else {
if(spf-status("pra") == "SoftFail"){
if (spf-status("mailfrom") == "Fail"
or spf-status("mailfrom") == "SoftFail"){
# malicious mail, but tempting
quarantine("Policy");
}
}
}
stamp-mail-with-spf-verification-error:
if (spf-status("pra") == "PermError, TempError"

or spf-status("mailfrom") == "PermError, TempError"
or spf-status("helo") == "PermError, TempError"){
# permanent error - stamp message subject
strip-header("Subject");
insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }
.
```

SPF-Passed ルール

次の例に、spf-passed とマークされていない電子メールを隔離するための spf-passed ルールを示します。

```
quarantine-spf-unauthorized-mail:

if (not spf-passed) {

quarantine("Policy");

}
```

（注） spf-status ルールと異なり spf-passed ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、spf-passed ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、spf-status ルールを使用します。

S/MIME ゲートウェイ メッセージ ルール

S/MIME ゲートウェイ メッセージ ルールでは、メッセージが S/MIME 署名されているか、暗号化されているか、または署名および暗号化されているかを確認します。次のメッセージフィルタでは、メッセージが S/MIME メッセージであるかどうかを確認し、S/MIME を使用した検証または復号に失敗した場合は隔離します。

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

詳細については、S/MIME セキュリティ サービス （681 ページ）を参照してください。

S/MIME ゲートウェイ検証済みルール

S/MIME ゲートウェイ メッセージ検証済みルールでは、メッセージが正常に検証されているか、復号されているか、または復号および検証されているかを確認します。次のメッセージフィルタでは、メッセージが S/MIME メッセージであるかどうかを確認し、S/MIME を使用した検証または復号に失敗した場合は隔離します。

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

詳細については、「S/MIME セキュリティ サービス （681 ページ）」を参照してください。

workqueue-count ルール

workqueue-count ルールは、ワークキュー数を特定の値と照合します。>、==、<= などのすべての比較演算子を使用できます。

次のフィルタは、ワークキュー数を確認し、指定した値より多ければスパムの確認を省略します。

```
wqfull:

if (workqueue-count > 1000) {

skip-spamcheck();

}
```

SPF/SIDF の詳細については、SPF および SIDF 検証の概要（765 ページ）を参照してください。

SMTP 認証済みユーザー致ルール

電子メールゲートウェイがメッセージの送信に SMTP 認証を使用している場合、`smtp-auth-id-matches` (*<target> [, <sieve-char>]*) ルールはメッセージのヘッダーとエンベロープ送信者を送信者の SMTP 認証ユーザ ID と照合し、スプーフィングされたヘッダーを含む送信メッセージを識別します。このフィルタを使用すると、なりすましの可能性のあるメッセージを隔離またはブロックできます。

`smtp-auth-id-matches` ルールは、SMTP 認証 ID を次の比較対象と比較します。

ターゲット	説明
*EnvelopeFrom	SMTP 対話のエンベロープ送信者のアドレス（MAIL FROM）を比較します。
*FromAddress	From ヘッダーから解析されたアドレスを比較します。From ヘッダーには複数のアドレスを使用できるため、そのうち 1 つが一致すれば一致と見なされます。
*Sender	Sender ヘッダーで指定されているアドレスを比較します。
*Any	ID にかかわらず、認証済み SMTP セッション中に作成されたメッセージと一致します。
*None	認証済み SMTP セッション中に作成されなかったメッセージと一致します。認証がオプションの場合に便利です（推奨）。

フィルタによる照合は厳密ではありません。大文字と小文字は区別されません。オプションで *sieve-char* パラメータが指定されている場合、特定の文字の後に続くアドレスの最後の部分は比較時に無視されます。たとえば、パラメータに「+」が含まれている場合、アドレス `joe+folder@example.com` のうち「+」より後の部分がフィルタでは無視されます。アドレスが `joe+smith+folder@example.com` の場合は、「`+folder`」のみが無視されます。SMTP 認証ユーザ ID 文字列が単純なユーザ名で、完全修飾電子メール アドレスでない場合は、比較対象のユーザ名部分のみが照合されます。ドメイン部分は別のルールで検証する必要があります。

また、$SMTPAuthID 変数を使用して SMTP 認証ユーザ ID をヘッダーに挿入することができます。

次の表は、SMTP 認証 ID と電子メールの比較の例で、`smtp-auth-id-matches` フィルタ ルールによる比較で一致するかどうかを示しています。

SMTP 認証 ID	Sieve 文字	比較するアドレス	一致の可否
someuser		otheruser@example.com	×
someuser		someuser@example.com	○
someuser		someuser@another.com	○
SomeUser		someuser@example.com	○
someuser		someuser+folder@example.com	×
someuser	+	someuser+folder@example.com	○
someuser@example.com		someuser@forged.com	×
someuser@example.com		someuser@example.com	○
SomeUser@example.com		someuser@example.com	○

次のフィルタは、認証済み SMTP セッション中に作成されたすべてのメッセージを確認し、From ヘッダーのアドレスとエンベロープ送信者が SMTP 認証ユーザ ID と一致するか検証します。アドレスと ID が一致すると、フィルタはドメインを許可します。一致しない場合、電子メールゲートウェイはメッセージを隔離します。

```
Msg_Authentication:

if (smtp-auth-id-matches("*Any"))

{

# Always include the original authentication credentials in a

# special header.

insert-header("X-Auth-ID","$SMTPAuthID");

if (smtp-auth-id-matches("*FromAddress", "+") and

smtp-auth-id-matches("*EnvelopeFrom", "+"))

{

# Username matches. Verify the domain

if header('from') != "(?i)@(?:example\\.com|alternate\\.com)" or

mail-from != "(?i)@(?:example\\.com|alternate\\.com)"

{

# User has specified a domain which cannot be authenticated

quarantine("forged");

}
```

```
} else {

# User claims to be an completely different user

quarantine("forged");

}

}
```

署名付きルール

signedルールはメッセージの署名を確認します。このルールは、メッセージの署名の有無を示すブール値を返します。このルールは、署名がASN.1 DERエンコーディング ルールに従っているか、およびCMS署名データ型構造（RFC 3852、セクション5.1）に準拠しているかを評価します。署名がコンテンツと一致するかどうかは検証されず、証明書の有効性も確認されません。

次の例では、signedルールを使用してヘッダーを署名済みメッセージに挿入します。

```
signedcheck: if signed { insert-header("X-Signed", "True"); }
```

次の例では、signedルールを使用して、特定の送信者グループから受信した未署名のメッセージの添付ファイルをドロップします。

```
Signed: if ((sendergroup == "NOTTRUSTED") AND NOT signed) {

html-convert();

if (attachment_size > 0)

{

drop_attachments("");

}

}
```

署名付き証明書ルール

signed-certificateルールは、X.509証明書発行者またはメッセージ署名者が、指定した正規表現と一致しているS/MIMEメッセージを選択します。このルールが対応しているのはX.509証明書のみです。

このルールの構文はsigned-certificate (<field> [<operator> <regular expression>]) です。各項目の内容は次のとおりです。

- <field>：引用符で囲まれた文字列 “issuer”（発行者）または “signer”（署名者）。
- <operator>：== または !=。
- <regular expression>：発行者または署名者を照合するための値。

メッセージに複数の署名が使用されている場合、いずれかの発行者または署名者が正規表現と一致すると true が返されます。このルールを一番短い形で signed-certificate(“issuer”) および signed-certificate(“signer”) のように指定すると、S/MIME メッセージに発行者または署名者が設定されている場合に true が返されます。

関連項目

- 署名者 （210 ページ）
- 発行元（Issuer） （210 ページ）
- 正規表現でのエスケープ処理 （210 ページ）
- $CertificateSigners アクション変数 （211 ページ）
- 例 1 （211 ページ）

署名者

メッセージ署名者に関して、このルールは X.509 証明書の subjectAltName 拡張から rfc822Name 名のシーケンスを抽出します。署名証明書に subjectAltName フィールドがない場合、またはこのフィールドに rfc822Name 名がない場合、signed-certificate(“signer”) ルールは false を返します。まれではありますが、rfc822Name 名が複数使用されている場合、このルールはすべての名前を正規表現と照合しようと試み、最初に一致した時点で true を返します。

発行元（Issuer）

発行者は X.509 証明書の空でない識別名です。AsyncOS は証明書から発行者を取得し、LDAP-UTF8 Unicode 文字列に変換します。次に例を示します。

- C=US,S=CA,O=IronPort
- C=US,CN=Bob Smith

X.509 証明書では発行者フィールドが必要なため、signed-certificate(“issuer”) は S/MIME メッセージに X.509 証明書があるかどうかを評価します。

正規表現でのエスケープ処理

LDAP-UTF8 では、正規表現で使用できるエスケープ方式が定義されています。LDAP-UTF8 での文字のエスケープ処理の詳細については、『Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names』（http://www.ietf.org/rfc/rfc4514.txt）を参照してください。

signed-certificate ルールでのエスケープ ルールは、LDAP-UTF8 で定義されたエスケープ ルールとは異なり、エスケープ処理が必要な文字のみをエスケープします。LDAP-UTF8 では、エスケープ処理なしで表示できる文字をオプションでエスケープすることができます。たとえば、次の 2 つの文字列は、LDAP-UTF8 のエスケープ ルールではいずれも「Example, Inc.」を正しく表すものとされます。

- Example\, Inc.
- Example\,\ Inc\.

一方で、signed-certificate ルールでは「Example\, Inc.」のみが一致します。スペースやピリオドのエスケープ処理は LDAP-UTF8 では許可されていますが、必要ではないため、正規表現では

許可されません。signed-certificateルールで使用する正規表現を作成する場合は、エスケープ処理がなくても表示できる文字はエスケープしないでください。

$CertificateSigners アクション変数

アクション変数 `$CertificateSigners` は、署名証明書の `subjectAltName` 要素から取得した、カンマ区切り形式の署名者のリストです。1人の署名者に複数の電子メールアドレスがある場合、重複を除去した上でリストに収録されます。

たとえば、Alice が自分の 2 つの証明書でメッセージに署名したとします。Bob は自分の 1 つの証明書でメッセージに署名しています。すべての証明書は1件の社内機関により発行されています。メッセージが S/MIME スキャンを通過すると、抽出されるデータには3 つの項目が含まれます。

```
[
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['alice@example.com', 'al@private.example.com']
},
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['alice@example.com', 'al@private.example.com']
},
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['bob@example.com', 'bob@private.example.com']
}
]
```

`$CertificateSigners` 変数は次のように拡張されます。

```
"alice@example.com, al@private.example.com, bob@example.com, bob@private.example.com"
```

例 1

次の例では、証明書発行者が米国にいる場合、新しいヘッダーが挿入されます。

```
Issuer: if signed-certificate("issuer") == "(?i)C=US" {
insert-header("X-Test", "US issuer");
}
```

次の例では、署名者のドメインが example.com でない場合、管理者に通知されます。

```
NotOurSigners: if signed-certificate("signer") AND
signed-certificate("signer") != "example\\.com$" {
notify("admin@example.com");
}
```

次の例では、メッセージに X.509 証明書がある場合、ヘッダーが追加されます。

```
AnyX509: if signed-certificate ("issuer") {
insert-header("X-Test", "X.509 present");
}
```

次の例では、メッセージの証明書に署名者がない場合、ヘッダーが追加されます。

```
NoSigner: if not signed-certificate ("signer") {
insert-header("X-Test", "Old X.509?");
}
```

ヘッダー繰り返し回数ルール

ヘッダー繰り返し回数ルールは、任意の時点で次の条件のメッセージが指定された数だけ検出されると、true と判断します。

- 過去 1 時間以内に同じ件名のものが検出された。
- 過去 1 時間以内に同じエンベロープ送信者からのものが検出された。

このルールを使用することで、大量送信メールを検出できます。たとえば、特定の Web サイトで行われる政治キャンペーンで、組織に大量の電子メールが送信されることがあります。アンチスパムエンジンはこのような電子メールを正常なメールとして扱い、電子メールの配信は停止されません。

このルールの構文は header-repeats (<target>, <threshold> [, <direction>]) です。各項目の意味は次のとおりです。

- <target> には subject または mail-from を指定します。AsyncOS はターゲットの値の繰り返し回数をカウントします。
- <threshold> は、過去 1 時間に受信した、指定した target に同じ値を持つメッセージの数です。この数を超えると、ルールは true と評価されます。
- <direction> は incoming、outgoing、またはこの両方です。このルールで direction が指定されていない場合、着信メッセージと発信メッセージがルール評価対象としてカウントされます。

ヘッダー繰り返し回数ルールが true と評価されるたびに、システム アラートが送信されます。システム アラート （1285 ページ）を参照。

（注） ヘッダーフィールドにカンマまたはセミコロンで区切られた値が含まれている場合、ルールは完全な文字列をトラッキング対象とみなします。このルールでは、件名ヘッダーが空白のメッセージは無視されます。

ヘッダー繰り返し回数ルールは、変化するメッセージの合計数を 1 分単位の精度で維持します。このため、設定されているしきい値に達してからこのルールがトリガーされるまでに、1 分の遅れが生じることがあります。

関連項目

- ヘッダー繰り返し回数ルールとその他のルールの併用 （213 ページ）
- 例 （213 ページ）

ヘッダー繰り返し回数ルールとその他のルールの併用

ヘッダー繰り返し回数ルールとその他のルールを組み合わせて使用するには、AND 演算子または OR 演算子を使用します。たとえば、メッセージのサブセットの許可リストを分類するには、次のフィルタを使用します。

```
F1: if (recv_listener == 'Gray')  AND (header-repeats('subject', X, 'incoming') { drop();}
```

AND または OR 演算子を使用してヘッダー繰り返し回数ルールとその他のルールを組み合わせて使用する場合は、ヘッダー繰り返し回数ルールが必要な場合にだけ最後に評価されます。特定のメッセージに対してヘッダー繰り返し回数ルールが評価されない場合、subject または mail-from は指定されたしきい値との比較対象としてカウントされません。

ヘッダー繰り返し回数ルールは必要な場合に限り最後に評価されるため、OR 演算子で他のルールと組み合わせて使用される場合はこのルールの動作は異なります。次のフィルタの例では、OR 演算子を使用して署名付きルールとヘッダー繰り返し回数ルールが組み合わせられています。

```
f1: if signed OR (header-repeats('subject', 10)) { drop();}
```

この例では、このフィルタで処理される最初の 9 件のメッセージが同じ件名の署名付きメッセージである場合、ヘッダー繰り返し回数ルールはこれらのメッセージを処理しません。10 番目のメッセージが、9 番目までのメッセージと同じ件名ヘッダーの未署名メッセージである場合、しきい値に達していても、フィルタは設定されたアクションを実行します。

例

次の例では、任意の時点で、フィルタが過去 1 時間において同じ件名の着信メッセージを X 件以上検出した場合に、それ以降受信する同じ件名のメッセージが、ポリシー隔離に送信されます。

```
f1 : if header-repeats('subject', X, 'incoming') { quarantine('Policy');}
```

次の例では、フィルタが任意の時点で、過去1時間において同じエンベロープ送信者からの発信メッセージをX件以上検出した場合に、それ以降同じエンベロープ送信者から送信されるメッセージがドロップされ、破棄されます。

```
f2 :  if header-repeats('mail-from', X, 'outgoing') {drop();}
```

次の例では、フィルタが任意の時点で、過去1時間において同じ件名の着信メッセージまたは発信メッセージをX件以上検出した場合に、それ以降同じ件名を持つすべてのメッセージが管理者に通知されます。

```
f3: if header-repeats('subject', X) {notify('admin@xyz.com');}
```

URL レピュテーション ルール

URL レピュテーション ルールでは、メッセージに含まれているURLのレピュテーション スコアに基づいてメッセージ アクションを定義します。重要な詳細については、悪意のあるURLまたは望ましくないURLからの保護（543ページ）のURL レピュテーションまたはURL カテゴリによるフィルタリング：条件およびルール （554ページ） を参照してください。

このルールの各部分は次のとおりです。

- `msg_filter_name` はこのメッセージ フィルタの名前です。
- `allowedlist` は（urllistconfig コマンドを使用して）定義されている URL リストの名前です。許可リストの指定は任意です。

レピュテーション サービスからスコアが提供される場合にアクションを実行するには

`url-reputation` ルールを使用します。

url-reputation ルールを使用する場合のフィルタの構文を次に示します。

```
<msg_filter_name>:

if url-reputation('<min_score'>, <'max_score'>, '<allowedlist>',
'<include_attachments>','<include_message_body_subject>')

{<action>}
```

ここで、

- `min_score` および `max_score` は、アクション適用範囲の最小スコアと最大スコアです。指定する値は範囲に含まれます。

最小スコアと最大スコアは `-10.0` から `10.0` までの範囲内の数値である必要があります。

- メッセージの添付ファイル内のURLをスキャンするには、`include_attachments` を指定します。値「1」はメッセージ添付ファイルのURL スキャンが有効であり、値「0」はメッセージ添付ファイルのURL スキャンが有効でないことを示します。
- メッセージの本文と件名内のURLをスキャンするには、`include_message_body_subject` を指定します。値「1」はメッセージ本文と件名のURL スキャンが有効であり、値「0」はメッセージ本文と件名のURL スキャンが有効でないことを示します。

レピュテーション サービスからスコアが提供されない場合にアクションを実行するには

`url-no-reputation` ルールを使用します。

`url-no-reputation` ルールを使用する場合のフィルタの構文を次に示します。

```
<msg_filter_name>:

if url_no_reputation('<allowedlist>',
'<include_attachments>','<include_message_body_subject>')

{<action>}
```

URL カテゴリ ルール

メッセージに含まれている URL のカテゴリに基づいてメッセージ アクションを定義するときに、URL カテゴリを使用します。重要な詳細については、悪意のある URL または望ましくない URL からの保護 （543 ページ）のURL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール （554 ページ） を参照してください。

`url-category` ルールを使用する場合のフィルタの構文を次に示します。

```
<msg_filter_name>: if url-category (['<category-name1>','<category-name2>',...,
'<category-name3>'],'<url_allowed_list>','<include_attachments>','<include_message_body_subject>')

<action>
```

ここで、

- `msg_filter_name` はこのメッセージ フィルタの名前です。
- `action` はメッセージ フィルタ アクションです。
- `category-name` は URL カテゴリです。複数のカテゴリを指定する場合は、各カテゴリをカンマで区切ります。正しいカテゴリ名を確認するには、コンテンツ フィルタの URL カテゴリ条件またはアクションを確認してください。カテゴリの説明と例については、URL カテゴリについて （568 ページ）を参照してください。
- `url_allowed_list` は（urllistconfig コマンドを使用して）定義されている URL リストの名前です。
- メッセージの添付ファイル内の URL をスキャンするには、`include_attachments` を指定します。値「1」はメッセージ添付ファイルの URL スキャンが有効であり、値「0」はメッセージ添付ファイルの URL スキャンが有効でないことを示します。
- メッセージの本文と件名内の URL をスキャンするには、`include_message_body_subject` を指定します。値「1」はメッセージ本文と件名の URL スキャンが有効であり、値「0」はメッセージ本文と件名の URL スキャンが有効でないことを示します。

破損した添付ファイル ルール

破損した添付ファイル ルールは、破損している添付ファイルがメッセージに含まれている場合に true と評価します。破損した添付ファイルとは、スキャン エンジンがスキャンできないため破損として識別する添付ファイルのことです。

関連項目

- 例 （216 ページ）

例

次の例では、メッセージに含まれている破損した添付ファイルが検出されると、メッセージは Policy 隔離エリアに隔離されます。

```
quar_corrupt_attach: if (attachment-corrupt) { quarantine("Policy"); }
```

メッセージ言語ルール

メッセージの言語に基づいて異なるメッセージアクションを取る場合があります。たとえば、次のような場合があります。

- ロシアにあるメッセージにロシア語で免責事項を追加します
- 言語が確定できないメッセージをドロップします

メッセージ言語ルールを使用して、メッセージの件名と本文の言語に応じたメッセージ アクションを取ります。

（注） このルールでは、添付ファイルおよびヘッダーの言語は確認しません。

言語の検出動作の仕組み

電子メールゲートウェイは、メッセージの言語を検出するのに組み込みの言語検出エンジンを使用します。電子メールゲートウェイは、件名とメッセージ本文を抽出し、言語検出エンジンに渡します。

言語検出エンジンは、抽出されたテキスト内の各言語の確率を決定し、それを電子メールゲートウェイに渡します。電子メールゲートウェイは、最も高い確率をもつ言語をメッセージの言語とみなします。電子メールゲートウェイは、次のシナリオのいずれかで、メッセージの言語を「判別不能」とみなします。

- 検出された言語が電子メールゲートウェイでサポートされていない場合
- 電子メールゲートウェイがメッセージの言語を検出できない場合
- 言語検出エンジンに送られた抽出されたテキストの合計サイズが 50 バイト未満の場合。

メッセージ フィルタの構文

```
<msg_filter_name>: if (message-language <operator> "<language1>, <language2>,..., <language n>") {<action>}
```

ここで、

- `msg_filter_name` はこのメッセージ フィルタの名前です。
- 演算子は、`==` または `!=` です。

- language は、このメッセージ フィルタに指定するメッセージ言語の値です。複数のエントリを指定する場合は、カンマで区切ります。サポートされているメッセージ言語と値のリストについては、コンテンツ フィルタのメッセージ言語の条件を参照してください。値は、角かっこ（[ ]）で囲まれています。
- action はメッセージ フィルタ アクションです。

例

次の例では、言語が特定できなかったメッセージをドロップする方法を示しています。

```
DropMessagesWithUndeterminedLanguage: if (message-language == "unknown") { drop(); }
```

次の例では、ロシア語のメッセージにロシア語の免責事項を追加する方法を示しています。

```
ussianDisclaimerRule: if (message-language == "ru") { add-heading("RussianDisclaimer");
```

マクロ検出ルール

マクロ検出ルールを使用すると、メッセージに添付されたマクロが有効な添付ファイルを、指定したファイル タイプについて検出できます。

（注） アーカイブまたは埋め込みファイルにマクロが含まれている場合、親ファイルはメッセージからドロップされます。

マクロ検出構文

```
<msg_filter_name>: if (macro-detection-rule (['file_type-1', 'file_type-2',...
,'file_type-n'])) {<action>}
```

ここで、

- msg_filter_name はこのメッセージ フィルタの名前です。
- file_type には、次のサポートされているファイル タイプのいずれかを指定できます。
  - Adobe Portable Document Format
  - Microsoft Office Files
  - OLE File types
- action はメッセージ フィルタ アクションです。

例

次の例は、マクロが有効なMicrosoft Office添付ファイルを含むメッセージをドロップする方法を示しています。

```
Drop_Messages_With_Macro-enabled_Office_Files: if (macro-detection-rule (['Microsoft
Office Files'])) { drop(); }
```

次の例では、マクロが有効な PDF 形式の添付ファイルを含むメッセージが特定のユーザに送信されると、そのメッセージはドロップされます。

```
Strip_Macro_enabled_PDF: if (rcpt-to == "joe@example.com") {
drop-macro-enabled-attachments(['Adobe Portable Document Format']); }
```

偽造メールの検出ルール

偽造された送信者アドレス（From: ヘッダー）を持つ不正なメッセージを検出し、そのようなメッセージに対してアクションを取ることが必要になる場合があります。

そのようなメッセージを検出するには、forged-email-detection ルールを使用します。このルールを設定する際には、コンテンツディクショナリと、メッセージに偽造の可能性があると見なすためのしきい値（1 ～ 100）を指定する必要があります。

forged-email-detection ルールは、From: ヘッダーをコンテンツ ディクショナリ内のユーザと比較します。このプロセス中に、類似により、電子メールゲートウェイはディクショナリ内の各ユーザに類似性スコアを割り当てます。次に例を示します。

- From: ヘッダーが <j0hn.sim0ns@example.com> で、コンテンツディクショナリにユーザ「John Simons」が含まれている場合、 電子メールゲートウェイによってこのユーザに 82 の類似性スコアが割り当てられます。
- From: ヘッダーが <john.simons@diff-example.com> で、コンテンツディクショナリにユーザ「John Simons」が含まれている場合は、このユーザに 100 の類似性スコアが割り当てられます。

類似性スコアが高くなればなるほど、メッセージが偽装されている確立が高くなります。類似性スコアが指定したしきい値以上の場合は、フィルタ アクションがトリガーされます。

詳細については、偽装メールの検出 （787 ページ）を参照してください。

メッセージ フィルタの構文

```
<filter_name>: if (forged-email-detection(“<content_dictionary>”, threshold)) {<action>;}
```

ここで、

- filter_name はメッセージ フィルタの名前です
- content_dictionary はコンテンツ ディクショナリの名前です
- threshold は、メッセージに偽造の可能性があるとみなすためのしきい値（1 ～ 100）です

例

次のメッセージフィルタは、メッセージ内の From: ヘッダーをディクショナリ内の用語と比較します。コンテンツディクショナリ内のユーザの類似性スコアが 70 以上である場合、このメッセージ フィルタは From: ヘッダーを削除し、エンベロープ送信者に置き換えます。

```
FED_CF: if (forged-email-detection("Execs", 70)) { fed("from", ""); }
```

重複境界検証ルール

duplicate_boundaries ルールを使用すると、重複する MIME 境界が含まれるメッセージを検出できます。

（注） 添付ファイルベースのルール（attachment-contains など）またはアクション（drop-attachments-where-contains など）は形式異常のメッセージ（重複する MIME 境界を含む）では動作しません。

メッセージ フィルタの構文

```
<filter_name>: if (duplicate_boundaries){<action>;}
```

例

次のメッセージ フィルタは、重複する MIME 境界が含まれるすべてのメッセージを隔離します。

```
DuplicateBoundaries: if (duplicate_boundaries) { quarantine("Policy"); }
```

不正な形式の MIME ヘッダー検出ルール

不正形式ヘッダー ルールを使用して、不正な形式の MIME ヘッダーを含むメッセージを検出できます。

メッセージ フィルタの構文

```
<filter_name>: if (malformed-header){<action>;}
```

例

次の例では、不正な形式の MIME ヘッダーがあるすべてのメッセージを隔離する方法を示しています。

```
quarantine_malformed_headers: if (malformed-header)
{
quarantine("Policy");
}
```

地理位置情報ルール

地理位置情報ルールを使用すると、選択した特定の国からの着信メッセージを処理できます。

地理位置情報構文

```
<msg_filter_name>: if (geolocation-rule (['country_name-1', 'country_name-2',...
,'country_name-n'])) {<action>}
```

ここで、

- msg_filter_name はこのメッセージ フィルタの名前です。
- country_name は選択した国の名前です。
- action はメッセージ フィルタ アクションです。

例

次の例は、Country1 と Country2 から受信したメッセージを検疫する方法を示します。

```
Quarantine_Incoming_Messages_from_Country1_and_Country2: if (geolocation-rule
(['Country1', 'Country2'])) {quarantine("Policy");}
```

ETF のドメイン レピュテーション ルール

例として、以下のメッセージ フィルタ ルール構文を使用して、ETF エンジンを使用してメッセージ内の悪意のあるドメインを検出し、そのようなメッセージに対して適切な対応をします。

構文：

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

引数の説明

- 'domain-external-threat-feeds' は、ドメイン レピュテーション メッセージ フィルタのルールです。
- 'etf_source1'は、メッセージのヘッダーの悪意のあるドメインを検出するために使用される ETF ソースです。
- 'mail-from'、'from' は、ドメインのレピュテーションを確認するために使用される必須ヘッダーです。
- 'domain_exception_list' は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。

例

以下の例では、'Errors To:' カスタム ヘッダーのドメインが ETF によって悪意があるとして検出された場合、メッセージが検疫されます。

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

SDR のドメイン レピュテーション ルール

ドメイン レピュテーション ルールを使用して SDR に基づいてメッセージをフィルタ処理し、そのようなメッセージに対して適切な対応ができます。

- 送信者のドメインの判定
- 送信者のドメインの経過時間

- 送信者のドメインがスキャン不可

送信者ドメインの判定に基づいてメッセージをフィルタ処理

（注） 推奨されるブロッキングのしきい値は「Poor」です。SDRの詳細については、Cisco Talos（https://www.talosintelligence.com）にお問い合わせください。

構文：

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['awful', 'poor'], "<domain_exception_list>")
{drop();}
```

それぞれの説明は次のとおりです。

- 'drop_msg_based_on_sdr_verdict' は、メッセージ フィルタの名前です。
- 'sdr-reputation' は、ドメイン レピュテーション メッセージ フィルタのルールです。
- 'awful'、'poor' は、SDR に基づいてメッセージをフィルタ処理するための送信者のドメイン判定の範囲です。
- 'domain_exception_list' は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。
- 'drop' は、メッセージに適用されるアクションです。

例

以下のメッセージでは、SDR 判定が 'Unknownr' の場合、メッセージが検疫されます。

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

送信者ドメインの経過時間に基づいてメッセージをフィルタ処理

（注） [送信者ドメインの経過時間（Sender Domain Age）] オプションは、次の AsyncOS リリースで削除されます。

構文：

```
<msg_filter_name>
if sdr-age (<'unit'>, <'operator'> <'actual value’>)
{<action>}
```

それぞれの説明は次のとおりです。

- 'sdr-reputation' は、ドメイン レピュテーション メッセージ フィルタのルールです。
- 'sdr_age'は、SDR に基づいてメッセージをフィルタ処理するために使用される送信者ドメインの経過時間です。

- 'unit' は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための ‘days’、‘years’、‘months’、'weeks' オプションです。
- 'operator' は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための比較演算子です。
  - – >（次の値より大きい）
  - – >=（次の値以上）
  - – <（次の値より小さい）
  - – <=（次の値以下）
  - – ==（次の値と等しい）
  - – !=（次の値と等しくない）
  - – Unknown
- 'actual value' は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するために使用される数字です。

例

以下のメッセージでは、送信者ドメインの経過時間が不明な場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("unknown", "")) {drop();}
```

以下のメッセージでは、送信者ドメインの経過時間が1ヵ月よりも短い場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("months", <, 1, "")) { drop(); }
```

送信者ドメインのスキャン不可能性に基づいてメッセージをフィルタ処理

構文：

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

それぞれの説明は次のとおりです。

- 'sdr-unscannable' は、ドメイン レピュテーション メッセージ フィルタのルールです。

  'domain_exception_list' は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。

例

以下のメッセージでは、メッセージが SDR チェックに不合格の場合、メッセージが検疫されます。

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

メッセージ フィルタ アクション

メッセージ フィルタの目的は、選択されたメッセージに対してアクションを実行することです。

アクションには、次の 2 つのタイプがあります。

- 最終アクション（deliver、drop、bounce など）はメッセージの処理を終了し、後続のフィルタによるさらなる処理を許可しません。
- 非最終アクションは、メッセージをさらに処理することを許可するアクションを実行します。

（注） 非最終メッセージ フィルタ アクションは、累積的です。各フィルタが異なるアクションを指定する複数のフィルタにメッセージが一致する場合、すべてのアクションが累積され、適用されます。ただし、同じアクションを指定する複数のフィルタにメッセージが一致する場合、前のアクションが上書きされ、最後のフィルタ アクションが適用されます。

関連項目

- フィルタ アクション一覧表 （223 ページ）
- アクション変数 （235 ページ）
- 一致した内容の表示 （238 ページ）
- メッセージ フィルタ アクションの説明と例 （239 ページ）

フィルタ アクション一覧表

メッセージ フィルタは、電子メール メッセージに対し、次の表に示すアクションを適用することができます。

表 *24*：メッセージ フィルタ アクション

操作	構文	説明
送信元ホストの変更	alt-src-host	メッセージの送信に使用する送信元ホスト名と IP インターフェイス（Virtual Gateway アドレス）を変更します。送信元ホスト（Virtual Gateway アドレス）変更アクション （248 ページ）を参照してください。
受信者の変更	alt-rcpt-to	メッセージの受信者を変更します。受信者変更アクション （247 ページ）を参照してください。

操作	構文	説明
メールホストの変更	alt-mailhost	メッセージの送信先メール ホストを変更します。配信ホスト変更アクション （247 ページ）を参照してください。
通知	notify	メッセージに関する報告を別の受信者に送信します。通知およびコピー通知アクション （241 ページ）を参照してください。
コピーの通知	notify-copy	notify アクションと同様ですが、bcc-scan アクションのようにコピーを送信します。通知およびコピー通知アクション （241 ページ）を参照してください。
BCC	bcc	メッセージをコピーし（メッセージ レプリケーション）、このコピーを匿名で別の受信者に送信します。ブラインド カーボン コピー アクション （244 ページ）を参照してください。
BCC（スキャン処理あり）	bcc-scan	メッセージを秘密で他の受信者に送信し、そのメッセージを新しいメッセージであるかのようにワーク キューで処理します。ブラインド カーボン コピー アクション （244 ページ）を参照してください。
アーカイブ（Archive）	archive	メッセージを mbox 形式のファイルにアーカイブします。アーカイブ アクション （249 ページ）を参照してください。
検疫（Quarantine）	`quarantine (`*`quarantine_name`*	*quarantine_name* で指定した隔離エリアにメッセージを送信するようフラグを設定します。隔離および複製アクション （246 ページ）を参照してください。
複製（隔離）	`duplicate-quarantine (`*`quarantine_name`*	指定された隔離エリアにメッセージのコピーを送信します。隔離および複製アクション （246 ページ）を参照してください。

操作	構文	説明
ヘッダーの削除	strip-header	メッセージの配信前に、指定したヘッダーをメッセージから削除します。ヘッダー削除アクション （250 ページ）を参照してください。
ヘッダーの挿入	insert-header	メッセージの配信前に、ヘッダーと値の対をメッセージに挿入します。ヘッダー挿入アクション （250ページ）を参照してください。
ヘッダーテキストの編集	edit-header-text	指定したヘッダー テキストを、フィルタ条件として指定した文字列に置き換えます。ヘッダー テキスト編集アクション （251ページ）を参照してください。
本文の編集	edit-body-text()	メッセージ本文から正規表現に一致する部分を削除し、指定したテキストに置き換えます。このフィルタは、メッセージ本文内の URL などの特定のコンテンツを削除および置換する場合に使用できます。本文編集アクション （251ページ）を参照してください。
HTML の変換	html-convert()	メッセージ本文から HTML タグを削除し、メッセージのプレーン テキスト部分を残します。このフィルタは、メッセージ内のすべての HTML テキストをプレーン テキストに変換する場合に使用します。HTML 変換アクション （252 ページ）。
バウンスプロファイルの割り当て	bounce-profile	特定のバウンス プロファイルをメッセージに割り当てます。バウンス プロファイル アクション （253 ページ）を参照してください。
アンチスパム システムのバイパス	skip-spamcheck	Cisco システムのアンチスパム システムがメッセージに適用されないようにします。アンチスパム システムのバイパス アクション （253ページ）を参照してください。

操作	構文	説明
グレイメールアクションのバイパス	skip-marketingcheck	マーケティング メールに対するアクションのバイパス。グレイメール アクションのバイパス （254ページ）を参照してください。
	skip-socialcheck	ソーシャル ネットワーク メールに対するアクションのバイパス。グレイメール アクションのバイパス （254ページ）を参照してください。
	skip-bulkcheck	バルク メールに対するアクションのバイパス。グレイメール アクションのバイパス （254ページ）を参照してください。
アンチウイルス システムのバイパス	`skip-viruscheck`	Cisco システムのアンチウイルス システムがメッセージに適用されないようにします。アンチウイルス システムのバイパス アクション （254ページ）を参照してください。
ファイル レピュテーション フィルタリングおよびファイル分析のバイパス	`skip-ampcheck`	このメッセージにファイル レピュテーション フィルタリングおよびファイル分析が適用されていないことを確認します。ファイル レピュテーション フィルタリングおよびファイル分析システムのバイパス アクション （255ページ）を参照してください。
ウイルス アウトブレイク フィルタのスキャニング処理のスキップ	`skip-vofcheck`	このメッセージがウイルス アウトブレイク フィルタでスキャニング処理されないようにします。アンチウイルス システムのバイパス アクション （254ページ）を参照してください。

操作	構文	説明
添付ファイルのドロップ（名前別）	`drop-attachments-by-name`	メッセージの添付ファイルのうち、指定した正規表現と一致する名前のファイルをすべてドロップします。一致するファイルが含まれている場合、アーカイブ形式の添付ファイル（zip、tar）、Microsoft Office の添付ファイル（doc、docx）、電子メールの添付ファイル（winmail.dat）はドロップされます。添付ファイルのスキャン メッセージ フィルタの例（269 ページ）を参照してください。
添付ファイルのドロップ（タイプ別）	`drop-attachments-by-type`	メッセージの添付ファイルのうち、指定した MIME タイプまたはファイル拡張子に該当する MIME タイプのファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。添付ファイルのスキャン メッセージ フィルタの例（269 ページ）を参照してください。
添付ファイルのドロップ（ファイル タイプ別）	`drop-attachments-by-filetype`	メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。詳細については、添付ファイルのスキャン メッセージ フィルタの例（269 ページ）を参照してください。
添付ファイルのドロップ（MIME タイプ別）	`drop-attachments-by-mimetype`	メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。このアクションではファイル拡張子による MIME タイプの判別は行われず、アーカイブの内容の確認もされません。添付ファイルのスキャン メッセージ フィルタの例（269 ページ）を参照してください。

操作	構文	説明
ファイルハッシュリストに基づく添付ファイルのドロップ	`drop-attachments-by-hash`	ファイルハッシュリスト内の特定のファイル SHA-256 値と一致するメッセージ内のすべてのメッセージ添付ファイルをドロップします。ファイル SHA-256 フィルタに一致するメッセージ添付ファイルをドロップする （297 ページ）および添付ファイルがファイル SHA-256 フィルタと一致する場合にメッセージをドロップする （297 ページ）を参照してください。
添付ファイルのドロップ（サイズ別）	`drop-attachments-by-size`	メッセージの添付ファイルのうち、ロー エンコード形式で指定したサイズ（バイト単位）以上のサイズであるファイルをすべてドロップします。アーカイブや圧縮ファイルの場合、このアクションでは非圧縮状態でのサイズは計測されず、デコードを行う前の実際の添付ファイルのサイズが計測されます。添付ファイルのスキャン メッセージ フィルタの例 （269 ページ）を参照してください。
添付ファイルのドロップ（内容別）	`drop-attachments-where-contains`	メッセージの添付ファイルのうち、指定した正規表現を含むファイルをすべてドロップします。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。アーカイブ ファイル（zip、tar）は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。添付ファイルのスキャン メッセージ フィルタの例 （269 ページ）を参照してください。 オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。

操作	構文	説明
マクロが含まれる添付ファイルのドロップ	drop-macro-enabled-attachments	指定したファイル タイプのマクロが有効になった添付ファイルをすべてドロップします。 （注） アーカイブまたは埋め込みファイルにマクロが含まれている場合、親ファイルはメッセージからドロップされます。 **構文** drop-macro-enabled-attachments (['file_type-1', 'file_type-2', …,'file_type-n'], "custom_replacement_message") ここで、 • file_type には、次のサポートされているファイル タイプのいずれかを指定できます。 • Adobe Portable Document Format • Microsoft Office Files • OLE File types • **custom replacement** メッセージとは、添付ファイルが削除されるときはメッセージ本文の一番下に既定のシステム生成メッセージが追加されますが、それに代わって追加される任意のメッセージです。 マクロ検出ルール （217ページ）を参照してください。

操作	構文	説明
添付ファイルのドロップ（辞書との一致別）	`drop-attachments-where-dictionary-match`	辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。添付ファイルのスキャン メッセージ フィルタの例（269 ページ） を参照してください。
フッターの追加	`add-footer(`*`footer-name`*`)`	メッセージのフッターとして免責条項を追加します。詳細については、「テキスト リソース」の章の「メッセージ免責事項スタンプ」を参照してください。
見出しの追加	`add-heading(`*`heading-name`*`)`	メッセージの見出しとして免責条項を追加します。詳細については、「テキスト リソース」の章の「メッセージ免責事項スタンプ」を参照してください。
配信時の暗号化	`encrypt-deferred`	配信時にメッセージを暗号化します。メッセージはそのまま次の処理に進み、すべての処理が完了した時点で暗号化され、配信されます。
配信時の S/MIME 署名/暗号化	`smime-gateway-deferred ("sending_profile")`	配信時に、指定された送信プロファイルを使用して、メッセージの S/MIME 署名または暗号化を実行します。配信時の S/MIME 署名/暗号化アクション（241 ページ） を参照してください。
S/MIME 署名/暗号化	`smime-gateway("sending_profile")`	指定された送信プロファイルを使用して S/MIME 署名または暗号化を実行してメッセージを配信し、その後の処理はスキップします。S/MIME 署名または暗号化アクション（241 ページ） を参照してください。

操作	構文	説明
メッセージ タグの追加	`tag-message(tag-name)`	DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに追加します。DLP ポリシーを設定して、スキャン対象をメッセージ タグがあるメッセージに限定することができます。メッセージ タグは受信者側では表示されません。メッセージ タグ追加アクション（256ページ）と「データ消失防止」の章を参照してください。
ログ エントリの追加	`log-entry`	カスタマイズしたテキストを、テキスト メール ログに INFO レベルで追加します。このテキストにはアクション変数を使用することができます。ログ エントリはメッセージ トラッキングに表示されます。詳細については、「ログ エントリ追加アクション（256ページ）」を参照してください。
URL レピュテーションに基づき URL をテキストに置換	• `url-reputation-replace` • `url-no-reputation-replace`	URL またはその動作を URL のレピュテーションに基づいて変更します。 レピュテーション サービスから URL のスコアが提供されない状況を処理するには、個別のアクションを使用します。 URL レピュテーション アクション（256ページ）を参照してください。
URL レピュテーションに基づき URL の危険を取り除く	• `url-reputation-defang` • `url-no-reputation-defang`	
URL レピュテーションに基づいてシスコのセキュリティ プロキシに URL をリダイレクト	• `url-reputation-proxy-redirect` • `url-no-reputation-proxy-redirect`	

操作	構文	説明
URLカテゴリに基づき URL をテキストに置換	`url-category-replace`	URL またはその動作を URL のカテゴリに基づいて変更します。 URL カテゴリ アクション （259 ページ）を参照してください。
URLカテゴリに基づき URL の危険を取り除く	`url-category-defang`	
URLカテゴリに基づき Cisco セキュリティプロキシに URLをリダイレクトする	`url-category-proxy-redirect`	
偽装メールの検出	`fed`	偽装されたメッセージから From: ヘッダーを削除し、エンベロープ送信者で置き換えます。偽造メールの検出アクション （260ページ）を参照してください。
オペレーションなし	`no-op`	操作は実行されません。オペレーションなし （260ページ）を参照してください。
*残りのメッセージ フィルタをスキップ	`skip-filters`	メッセージに対して他のメッセージ フィルタによる処理は行われず、メッセージは電子メール パイプラインをそのまま通過します。「残りのメッセージフィルタをスキップ」アクション （239 ページ）を参照してください。
*メッセージのドロップ	`drop`	メッセージをドロップし、廃棄します。ドロップ アクション （240 ページ）を参照してください。
*メッセージのバウンス	`bounce`	メッセージを送信者に戻します。バウンスアクション （240ページ）を参照してください。
*すぐに暗号化して配信	`encrypt`	Cisco Email Encryption を使用して、送信メッセージを暗号化します。暗号化アクション （241 ページ）を参照してください。
* 最終アクション		

関連項目

- 添付ファイル グループ （233 ページ）

添付ファイル グループ

特定のファイル タイプ（「exe」など）や一般的な添付ファイルのグループを `attachment-filetype` ルールや `drop-attachments-by-filetype rules` ルールで指定できます。AsyncOS は添付ファイルを以下の表に記載されているグループに分類します。

特定のファイルタイプの添付ファイルを含まないメッセージと照合させる `!=`演算子を使うメッセージ フィルタを作成する場合は、フィルタで除外するファイル タイプの添付ファイルが少なくとも1つあると、フィルタはメッセージへのアクションを実行しません。たとえば、次のフィルタは **`.exe`** ファイル タイプではない添付ファイルを含むメッセージをドロップします。

```
exe_check: if (attachment-filetype != "exe") {

drop();

}
```

メッセージに複数の添付ファイルがある場合、電子メールゲートウェイは他の添付ファイルが `.exe` ファイルでない場合でも、添付ファイルの少なくとも 1 つが .exe ファイルの場合はメッセージをドロップしません。

表 *25*：添付ファイル グループ

添付ファイルグループ名	スキャン対象のファイル タイプ
マニュアル	• doc • docx • mdb • mpp • ole • pdf • ppt • pptx • rtf • wps • x-wmf • xls • xlsx

添付ファイルグループ名	スキャン対象のファイル タイプ
実行可能ファイル	• exe • java • msi • pif （注） Executable グループをフィルタリングすると、.dll ファイルと .scr ファイルもスキャンされます。これらのファイル タイプは個別にスキャンできません。
圧縮	• ace（ACE アーカイバ圧縮ファイル） • arc（SQUASH 圧縮アーカイブ） • arj（Robert Jung ARJ 圧縮アーカイブ） • binhex • bz（Bzip 圧縮ファイル） • bz2（Bzip 圧縮ファイル） • cab（Microsoft キャビネット ファイル） • gzip*（圧縮ファイル - UNIX gzip） • lha（圧縮アーカイブ [LHA/LHARC/LZH]） • rar（圧縮アーカイブ） • sit（圧縮アーカイブ - Macintosh ファイル [Stuffit]） • tar*（圧縮アーカイブ） • unix（UNIX 圧縮アーカイブ） • zip*（圧縮アーカイブ - Windows） • zoo（ZOO 圧縮アーカイブ ファイル） * これらのファイルは「本文スキャン」の対象にすることができます。
テキスト（Text）	• txt • html • xml
画像	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff

添付ファイルグループ名	スキャン対象のファイル タイプ
メディア	• aac • aiff • asf • avi • flash • midi • mov • mp3 • mpeg • ogg • ram • snd • wav • wma • wmv

アクション変数

bcc()、bcc-scan()、notify()、notify-copy()、add-footer()、add-heading()、insert-headers() の各アクションには、アクションの実行時に元のメッセージの情報に自動的に置き換えられる所定の変数を使用しているパラメータがあります。これらの特殊な変数はアクション変数と呼ばれます。 電子メールゲートウェイでは次のアクション変数がサポートされています。

表 *26 :* メッセージ フィルタ アクション変数

変数	構文	説明
すべてのヘッダー（All Headers）	`$AllHeaders`	メッセージのヘッダーを返します。
本文サイズ（Body Size）	`$BodySize`	メッセージのサイズをバイト単位で返します。
証明書の署名者（Certificate Signers）	`$CertificateSigners`	署名付き証明書の subjectAltName 要素から取得した署名者を返します。詳細については、$CertificateSigners アクション変数（211 ページ）を参照してください。
日付（Date）	`$Date`	現在の日付を MM/DD/YYYY 形式で返します。
ドロップされたファイル名（Dropped File Name）	`$dropped_filename`	直近にドロップされたファイル名のみを返します。

変数	構文	説明
ドロップされたファイル名（Dropped File Names）	`$dropped_filenames`	ドロップされたファイルのリストを表示します（$filenames と同様です）。
ドロップされたファイルタイプ（Dropped File Types）	`$dropped_filetypes`	ドロップされたファイルのタイプを表示します（$filetypes と同様です）。
エンベロープ送信者（Envelope Sender）	`$EnvelopeFrom`	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）を返します。
エンベロープ受信者（Envelope Recipients）	`$EnvelopeRecipients`	メッセージのすべてのエンベロープ受信者（Envelope To、<RCPT TO>）を返します。
ファイル名（File Names）	`$filenames`	メッセージの添付ファイルの名前のリストをカンマ区切りで返します。
ファイルサイズ（File Sizes）	`$filesizes`	メッセージの添付ファイルのサイズのリストをカンマ区切りで返します。
ファイルタイプ（File Types）	`$filetypes`	メッセージの添付ファイルのタイプのリストをカンマ区切りで返します。
フィルタ名（Filter Name）	`$FilterName`	処理中のフィルタの名前を返します。
GMT 日時（GMTimeStamp）	`$GMTimeStamp`	メッセージの Received: 行に表示される現在の日時を GMT 形式で返します。
HATグループ名（HAT Group Name）	`$Group`	メッセージの送信時に送信者が属していた送信者グループの名前を返します。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
一致した内容（Matched Content）	`$MatchedContent`	スキャン フィルタ ルール（body-contains などのフィルタ ルールやコンテンツディクショナリを含む）をトリガーした内容を返します。
メールフローポリシー（Mail Flow Policy）	`$Policy`	メッセージの送信時に送信者に適用された HAT ポリシーの名前を返します。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。

変数	構文	説明
ヘッダー（Header）	`$Header['string']`	引用符で囲まれたヘッダーの値を返します（元のメッセージに該当するヘッダーがある場合）。二重引用符が使用される場合もあります。
ホストネーム	`$Hostname`	電子メールゲートウェイのホスト名を返します。
内部メッセージID（Internal Message ID）	`$MID`	内部でメッセージを識別するため使用されているメッセージ ID（MID）を返します。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。
受信リスナー（Receiving Listener）	`$RecvListener`	メッセージを受信したリスナーのニックネームに置き換えられます。
受信インターフェイス（Receiving Interface）	`$RecvInt`	メッセージを受信したインターフェイスのニックネームを返します。
リモート IP アドレス（Remote IP Address）	`$RemoteIP`	電子メールゲートウェイにメッセージを送信したシステムの IP アドレスを返します。
リモートホストアドレス（Remote Host Address）	`$remotehost`	電子メールゲートウェイにメッセージを送信したシステムのホスト名を返します。
IP レピュテーションスコア	`$Reputation`	送信者の IP レピュテーションスコアを返します。レピュテーション スコアがない場合は「None」に置き換えられます。
Subject	`$Subject`	メッセージの件名を返します。
時刻	`$Time`	現在地の時間帯での現在時刻を返します。
Timestamp	`$Timestamp`	メッセージの Received: 行に表示される現在の日時を現在地の時間帯に従って返します。

関連項目

- 非 ASCII 文字セットとメッセージ フィルタ アクション変数 （237 ページ）

非 ASCII 文字セットとメッセージ フィルタ アクション変数

このシステムでは、ISO-2022 スタイル文字コード（ヘッダー値で使用されるエンコードのスタイル）を含むアクション変数の拡張をサポートしています。また、通知内で多言語テキストを

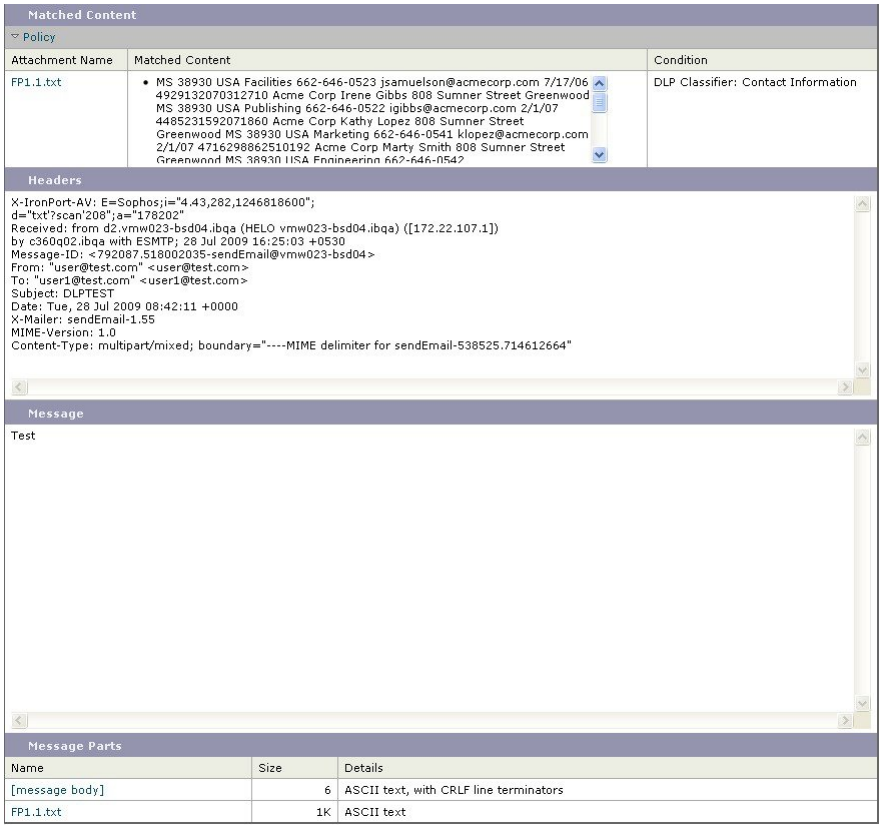
使用できます。これらの内容が統合されて通知が生成され、UTF-8形式の、引用符で囲まれた印刷可能なメッセージとして送信されます。

一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示すると、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。

メッセージフィルタまたはコンテンツフィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタアクションをトリガーした内容と共に）GUIで表示されることがあります。GUIの表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。これは、GUIで使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールと共に一覧表示するテーブルは正しく表示されます。

図 *17 : Policy* 検疫エリア内で表示されたー致内容



メッセージ フィルタ アクションの説明と例

次のセクションでは、使用されるさまざまなメッセージフィルタアクションについて説明し、その例を示します。

- 「残りのメッセージ フィルタをスキップ」アクション （239 ページ）
- ドロップ アクション （240 ページ）
- バウンス アクション （240 ページ）
- 暗号化アクション （241 ページ）
- 通知およびコピー通知アクション （241 ページ）
- ブラインド カーボン コピー アクション （244 ページ）
- 隔離および複製アクション （246 ページ）
- 受信者変更アクション （247 ページ）
- 配信ホスト変更アクション （247 ページ）
- 送信元ホスト（Virtual Gateway アドレス）変更アクション （248 ページ）
- アーカイブ アクション （249 ページ）
- ヘッダー削除アクション （250 ページ）
- ヘッダー挿入アクション （250 ページ）
- ヘッダー テキスト編集アクション （251 ページ）
- 本文編集アクション （251 ページ）
- HTML 変換アクション （252 ページ）
- バウンス プロファイル アクション （253 ページ）
- アンチスパム システムのバイパス アクション （253 ページ）
- グレイメール アクションのバイパス （254 ページ）
- アンチウイルス システムのバイパス アクション （254 ページ）
- ファイル レピュテーション フィルタリングおよびファイル分析システムのバイパス アクション （255 ページ）
- アンチウイルス システムのバイパス アクション （254 ページ）
- メッセージ タグ追加アクション （256 ページ）
- ログ エントリ追加アクション （256 ページ）
- URL レピュテーション アクション （256 ページ）
- URL カテゴリ アクション （259 ページ）
- オペレーションなし （260 ページ）
- 偽造メールの検出アクション （260 ページ）

「残りのメッセージ フィルタをスキップ」アクション

`skip-filters`アクションを実行すると、メッセージフィルタによるメッセージの処理がスキップされ、メッセージは電子メールパイプラインを通過します。電子メールゲートウェイでアンチスパムスキャンとアンチウイルススキャンが使用できる場合、`skip-filters`アクションを実行したメッセージはこれらのスキャンの対象となります。`skip-filters` アクションは、メッセージ フィルタのデフォルトの最終アクションです。

次のフィルタは、customercare@example.com に通知を送信し、boss@admin 宛てのメッセージをただちに送信します。

```
bossFilter:

if(rcpt-to == 'boss@admin$')

{

notify('customercare@example.com');

skip-filters();

}
```

ドロップ アクション

drop アクションを実行すると、メッセージは送信されずに破棄されます。メッセージは送信者には戻されず、メッセージの本来の宛先にも送信されず、それ以外の処理も一切行われません。

次のフィルタは、まず george@whitehouse.gov に通知を送信し、その後件名が「SPAM」で始まるメッセージを破棄します。

```
spamFilter:

if(subject == '^SPAM.*')

{

notify('george@whitehouse.gov');

drop();

}
```

バウンス アクション

bounce アクションは、メッセージを送信者（エンベロープ送信者）に戻し、それ以降の処理は行いません。

次のフィルタは、@yahoo\\.com で終わる電子メール アドレスから送信されたすべてのメッセージを戻します（バウンスします）。

```
yahooFilter:

if(mail-from == '@yahoo\\.com$')

{

bounce();

}
```

暗号化アクション

encrypt アクションは、設定された暗号化プロファイルを使用して、電子メール受信者に暗号化されたメッセージを送信します。

次のフィルタは、メッセージの件名に [encrypt] という語句が含まれている場合に、そのメッセージを暗号化します。

```
Encrypt_Filter:

if ( subject == '\\[encrypt\\]' )

{

encrypt('My_Encryption_Profile');

}
```

（注） このフィルタ アクションを使用するには、ネットワークに Cisco 暗号化アプライアンスがあるか、ホスト キー サービスが設定されている必要があります。また、このフィルタ アクションを使用するには、暗号化プロファイルの設定が必要です。

配信時の S/MIME 署名/暗号化アクション

smime-gateway-deferred アクションでは、配信時に、指定された送信プロファイルを使用して、メッセージの S/MIME 署名または暗号化を実行しますメッセージは次の処理段階に進み、すべての処理が完了した時点で署名または暗号化されて、配信されます。

次のフィルタでは、配信時に、特定の送信者からのすべての発信メッセージに対して S/MIME 暗号化を実行します。

```
smime-deferred:if(mail-from ==
"user@example.com"){smime-gateway-deferred("smime-encrypt");}
```

S/MIME 署名または暗号化アクション

smime-gateway アクションでは、指定された送信プロファイルを使用して S/MIME 署名または暗号化を実行してメッセージを配信し、その後の処理はスキップします。

次のフィルタでは、特定の送信者からのすべての発信メッセージに対して S/MIME 暗号化を実行して、即時に配信します。

```
smime-deliver-now:if(mail-from == "user@example.com"){smime-gateway("smime-sign");}
```

通知およびコピー通知アクション

notify および notify-copy アクションは、指定した電子メールに対して、メッセージの概要を電子メールで送信します。notify-copy アクションは、bcc-scan アクションと同様に、元のメッセージのコピーも送信します。通知概要には次の内容が含まれます。

- メッセージのメール転送プロトコル対話から取得したエンベロープ送信者およびエンベロープ受信者（MAIL FROM および RCPT TO）指定の内容。
- メッセージのヘッダー。
- メッセージを検出したメッセージ フィルタの名前。

受信者、件名行、送信元アドレス、および通知テンプレートを指定できます。次のフィルタは、サイズが 4 MB を超えるメッセージを選択し、一致するメッセージのそれぞれについて通知メッセージを admin@example.com に送信し、最後にメッセージを破棄します。

```
bigFilter:

if(body-size >= 4M)

{

notify('admin@example.com');

drop();

}
```

または

```
bigFilterCopy:

if(body-size >= 4M)

{

notify-copy('admin@example.com');

drop();

}
```

エンベロープ受信者パラメータとして、有効な任意の電子メール アドレス（上の例では admin@example.com）を指定できます。また、メッセージのすべてのエンベロープ受信者を指定するアクション変数 $EnvelopeRecipients（アクション変数（235 ページ）を参照）を指定することもできます。

```
bigFilter:

if(body-size >= 4M)

{

notify('$EnvelopeRecipients');

drop();

}
```

notify アクションでは最大で 3 つのオプション引数を使用でき、件名ヘッダー、エンベロープ送信者、通知メッセージに使用する定義済みテキスト リソースを指定できます。これらのパラ

メータはこの順序で指定する必要があるため、エンベロープ送信者を設定する場合や通知テンプレートを指定する場合は件名を指定する必要があります。

件名パラメータにはアクション変数（アクション変数（235ページ）を参照）を指定できます。この変数は元のメッセージから取得したデータで置き換えられます。デフォルトでは、件名は「Message Notification」に設定されています。

エンベロープ送信者パラメータとして、有効な任意の電子メールアドレスを指定できます。また、メッセージのリターンパスを元のメッセージと同じに設定する $EnvelopeFrom アクション変数を指定することもできます。

通知テンプレート パラメータは、既存の通知テンプレートの名前になります。詳細については、通知 （268 ページ）を参照してください。

次の例は前の例を拡張したものですが、件名が「[bigFilter] Message too large」となるように変更し、リターンパスを元の送信者に設定し、「message.too.large」テンプレートを使用しています。

```
bigFilter:

if (body-size >= 4M)

{

notify('admin@example.com', '[$FilterName] Message too large',

'$EnvelopeFrom', 'message.too.large');

drop();

}
```

また、$MatchedContent アクション変数を使用して、送信者または管理者にコンテンツ フィルタがトリガーされたことを通知することもできます。$MatchedContent アクション変数は、フィルタをトリガーしたコンテンツを表示します。たとえば、次のフィルタは、電子メールにABAアカウント情報が含まれる場合に、管理者に通知します。

```
ABA_filter:

if (body-contains ('*aba')){

notify('admin@example.com','[$MatchedContent]Account Information Displayed');

}
```

関連項目

- 通知テンプレート （243 ページ）

通知テンプレート

[テキストリソース（Text Resources）] ページまたは textconfig CLI コマンドを使用して、notify() および notify-copy() アクションで使用するテキストリソースとなるカスタム通知テ

ンプレートを設定できます。カスタム通知テンプレートを作成しない場合、デフォルトのテンプレートが使用されます。デフォルトのテンプレートにはメッセージ ヘッダーが含まれますが、デフォルトではカスタム通知テンプレートにはメッセージヘッダーは含まれません。カスタム通知にメッセージ ヘッダーを含めるには、`$AllHeaders` アクション変数を使用します。

詳細については、「テキスト リソース」の章を参照してください。

次の例では、メッセージのサイズが大きい場合に次のフィルタがトリガーされると、本来の受信者に対して、メッセージが大きすぎることを示す電子メールが送信されます。

```
bigFilter:

if (body-size >= 4M)

{

notify('$EnvelopeRecipients', '[$FilterName] Message too large',

'$EnvelopeFrom', 'message.too.large');

drop();

}
```

ブラインド カーボン コピー アクション

`bcc` アクションは、メッセージの無記名コピーを、指定した受信者に送信します。この処理はメッセージ レプリケーションとも呼ばれています。元のメッセージにはコピーに関する通知は含まれず、無記名コピーが受信者にバウンスされることはないため、メッセージの元の送信者と受信者はコピーが送信されたことを関知しない場合があります。

次のフィルタは、`johnny` から sue に送信されるメッセージのそれぞれについて、ブラインド カーボン コピーを `mom@home.org` に送信します。

```
momFilter:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc('mom@home.org');

}
```

bcc アクションでは最大で 3 つのオプション引数を使用でき、コピーしたメッセージに使用する件名ヘッダーとエンベロープ送信者、および alt-mailhost を指定できます。これらのパラメータはこの順序で指定する必要があるため、エンベロープ送信者を設定する場合は件名を指定する必要があります。

件名パラメータにはアクション変数（アクション変数（235 ページ）を参照）を指定できます。この変数は元のメッセージから取得したデータで置き換えられます。デフォルトでは、元のメッセージの件名（`$Subject` と同じ内容）が設定されます。

エンベロープ送信者パラメータとして、有効な任意の電子メールアドレスを指定できます。また、メッセージのリターンパスを元のメッセージと同じに設定する `$EnvelopeFrom` アクション変数を指定することもできます。

次の例は前の例を拡張したもので、件名は「`[Bcc] <original subject>`」に設定され、リターンパスは `badbounce@home.org` に設定されています。

```
momFilter:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc('mom@home.org', '[Bcc] $Subject', 'badbounce@home.org');

}
```

4 番目のパラメータは alt-mailhost です。

```
momFilterAltM:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc('mom@home.org', '[Bcc] $Subject', '$EnvelopeFrom',

'momaltmailserver.example.com');

}
```

注意 `Bcc()`、`notify()`、`bounce()` の各フィルタ アクションを実行すると、ネットワーク内にウイルスが侵入する場合があります。ブラインドカーボンコピーフィルタアクションは、元のメッセージの完全なコピーであるメッセージを新規作成します。通知フィルタ アクションは、元のメッセージのヘッダーを含むメッセージを新規作成します。まれにではありますが、ヘッダーにウイルスが含まれている場合があります。バウンス フィルタ アクションは、元のメッセージの最初の 10 キロバイトを含むメッセージを新規作成します。3 つのうちいずれの場合についても、新しいメッセージはアンチウイルス スキャンやアンチスパム スキャンの処理対象とはなりません。

複数のホストに送信する場合は、`bcc()` アクションを複数回呼び出すことができます。

```
multiplealthosts:

if (recv-listener == "IncomingMail")

{

insert-header('X-ORIGINAL-IP', '$remote_ip');

bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.4');
```

```
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.5');
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.6');
}
```

関連項目

- 競合他社に送信されたメールの BCC およびスキャン （290 ページ）

bcc-scan() アクション

bcc-scan アクションは bcc アクションと同様に機能しますが、送信されるメッセージは新しいメッセージとして扱われるため、電子メール パイプライン全体を経由して送信されます。

```
momFilter:
if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
{
bcc-scan('mom@home.org');
}
```

隔離および複製アクション

quarantine('quarantine_name') アクションは、隔離エリアと呼ばれるキューに入れるメッセージにフラグを設定します。隔離についての詳細については、「隔離」の章を参照してください。duplicate-quarantine ('quarantine_name') アクションを実行すると、メッセージのコピーが指定されている隔離エリアにただちに配置されます。隔離エリア名の大文字と小文字は区別されます。

隔離フラグの付けられたメッセージは、電子メールパイプラインの残りの処理を継続します。メッセージがパイプラインの末尾に到達すると、メッセージに 1 つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。それ以外の場合は配信されます。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

したがって、メッセージ フィルタに quarantine() アクションがあり、その後に bounce() または drop() アクションが続く場合、最後のアクションによりメッセージはパイプラインの末尾に到達しないため、メッセージは隔離エリアに配置されません。メッセージフィルタに隔離アクションが含まれる場合も同様ですが、メッセージはアンチスパムまたはアンチウイルス スキャン、またはコンテンツ フィルタによりドロップされます。skip-filters() アクションによりメッセージは残りのメッセージ フィルタをとばしますが、コンテンツ フィルタが適用される場合があります。たとえば、メッセージフィルタがメッセージに隔離フラグを設定し、同時に最後の skip-filters() アクションも設定している場合、電子メール パイプラインの他のアクションによりメッセージがドロップされる場合を除き、メッセージは残りのメッセージフィルタをすべてスキップした上で隔離されます。

次の例では、メッセージに「secret_word」という辞書にあるいずれかの単語が含まれていると、そのメッセージは Policy 隔離エリアに送信されます。

```
quarantine_codenames:

if (dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

次の例では、ある会社に.mp3ファイル形式の添付ファイルをすべてドロップする公式ポリシーがあるものと仮定しています。受信メッセージに .mp3 形式の添付ファイルがある場合、この添付ファイルは削除され、残りのメッセージ（本文と他の添付ファイル）は本来の受信者に送信されます。元のメッセージにすべての添付ファイルが添付されているコピーが隔離（Policy 隔離エリアに送信）されます。ブロックされた添付ファイルを受信する必要がある場合、本来の受信者はメッセージを隔離エリアからリリースするよう要求することができます。

```
strip_all_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

duplicate-quarantine('Policy');

drop-attachments-by-name('(?i)\\.mp3$');

}
```

受信者変更アクション

alt-rcpt-to アクションは、メッセージの配信時にメッセージのすべての受信者を指定した受信者に変更します。

次のフィルタは、エンベロープ受信者のアドレスに .freelist.com が含まれているすべてのメッセージを送信し、そのメッセージのすべての受信者を system-lists@myhost.com に変更します。

```
freelistFilter:

if(rcpt-to == '\\.freelist\\.com$')

{

alt-rcpt-to('system-lists@myhost.com');

}
```

配信ホスト変更アクション

alt-mailhost アクションは、選択したメッセージのすべての受信者の IP アドレスを、指定した数値 IP アドレスまたはホスト名に変更します。

（注） alt-mailhost アクションを実行すると、アンチスパム スキャンによりスパムと分類されたメッセージが隔離されないようにすることができます。alt-mailhost アクションは quarantine アクションに優先して実行され、指定したメール ホストにメッセージを送信します。

次のフィルタは、すべての受信者について、受信者のアドレスをホスト example.com に変更します。

```
localRedirectFilter:

if(true)

{

alt-mailhost('example.com');

}
```

これにより、joe@anywhere.com に送信されるメッセージの Envelope To アドレスが joe@anywhere.com になり、メッセージは example.com のメールホストに送信されます。smtproutes コマンドで指定された追加ルーティング情報は、引き続きメッセージのルーティングに適用されます。（ローカル ドメインの電子メールのルーティング （853 ページ） を参照。）

（注） alt-mailhost アクションではポート番号を指定できません。この操作を行うには、かわりに SMTP ルートを追加します。

次のフィルタは、すべてのメッセージを 192.168.12.5 にリダイレクトします。

```
local2Filter:

if(true)

{

alt-mailhost('192.168.12.5');

}
```

送信元ホスト（Virtual Gateway アドレス）変更アクション

alt-src-host アクションは、メッセージの送信元ホストを指定した送信元に変更します。送信元ホストは、メッセージの送信元となる IP インターフェイス、または IP インターフェイスのグループにより構成されます。IP インターフェイスのグループが選択された場合、システムは電子メールの配信時に、グループ内のすべての IP インターフェイスを送信元インターフェイスとして使用する処理を繰り返します。つまり、これにより 1 台の電子メールゲートウェイに複数の仮想ゲートウェイアドレスを設定できます。詳細については、Virtual Gateway™ テクノ

ロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （912 ページ）を参照してください。

IP インターフェイスは、現在システムで設定されている IP インターフェイスまたは IP インターフェイス グループだけに変更できます。次のフィルタは、IP アドレスが `1.2.3.4` であるリモート ホストから受信したすべてのメッセージに対して、発信（配信）IP インターフェイス `outbound2` を使用する仮想ゲートウェイを作成します。

```
externalFilter:

if(remote-ip == '1.2.3.4')

{

alt-src-host('outbound2');

}
```

次のフィルタは、IP アドレスが `1.2.3.4` であるリモート ホストから受信したすべてのメッセージに対して、IP インターフェイスのグループ Group1 を使用します。

```
groupFilter:

if(remote-ip == '1.2.3.4')

{

alt-src-host('Group1');

}
```

アーカイブ アクション

`archive` アクションは、元のメッセージ（すべてのメッセージヘッダーと受信者を含む）のコピーを、電子メールゲートウェイ上の mbox 形式のファイルに保存します。このアクションでは、メッセージを保存するログ ファイルの名前がパラメータとして使用されます。システムはフィルタの作成時に、指定したファイル名で自動的にログ サブスクリプションを作成します。また、既存のフィルタ ログ ファイルを指定することもできます。フィルタとフィルタ ログ ファイルの作成後は、`filters -> logconfig` サブコマンドでフィルタ ログ オプションを編集できます。

（注） `logconfig` コマンドは `filters` のサブコマンドです。このサブコマンドの完全な説明については、CLI を使用したメッセージ フィルタの管理 （273 ページ）を参照してください。

mbox 形式は標準の UNIX メールボックス形式で、メッセージを簡単に表示するためのユーティリティが多数用意されています。ほとんどの UNIX システムでは、「`mail -f` *mbox.filename*」と入力して、ファイルを表示できます。mbox 形式はプレーン テキストであるため、普通のテキスト エディタを使用してメッセージの内容を表示することができます。

次の例では、エンベロープ送信者が joesmith@yourdomain.com と一致する場合に、メッセージのコピーが joesmith というログに保存されます。

```
logJoeSmithFilter:

if(mail-from == '^joesmith@yourdomain\\.com$')

{

archive('joesmith');

}
```

ヘッダー削除アクション

strip-header アクションは、メッセージの特定のヘッダーを調べ、配信する前に該当する行をメッセージから削除します。ヘッダーが複数ある場合は、ヘッダーのすべてのインスタンス（「Received:」ヘッダーなど）が削除されます。

次の例では、すべてのメッセージで送信前に X-DeleteMe ヘッダーが削除されます。

```
stripXDeleteMeFilter:

if (true)

{

strip-header('X-DeleteMe');

}
```

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージヘッダー ルールおよび評価（160 ページ）を参照してください。

ヘッダー挿入アクション

insert-header アクションは、メッセージに新しいヘッダーを挿入します。AsyncOS は、挿入したヘッダーが規格を満たしているかどうかを検証しません。生成されるメッセージが電子メールのインターネット規格を満たしているかどうかは、ユーザが自分で確認する必要があります。

次の例では、X-Company というヘッダーがメッセージにない場合に、このヘッダーに My Company Name という値が設定されます。

```
addXCompanyFilter:

if (not header('X-Company'))

{

insert-header('X-Company', 'My Company Name');
```

```
}
```

insert-header() アクションでは、ヘッダーのテキストに非 ASCII 文字を使用できます。ただし、ヘッダー名には（規格遵守のため）ASCII 文字しか使用できません。可読性を最大限に高めるため、トランスポート エンコードは Quoted-Printable となります。

（注） strip-headers アクションと insert-header アクションを組み合わせることにより、元のメッセージにある任意のメッセージ ヘッダーを書き換えることができます。場合によっては、同じヘッダーを複数回使用することができますが（Received: など）、それ以外の場合は同じヘッダーを複数回使用すると MUA が混乱する場合があります（Subject: ヘッダーを複数回使用する場合など）。

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージヘッダー ルールおよび評価（160 ページ）を参照してください。

ヘッダー テキスト編集アクション

edit-header-text アクションを実行すると、正規表現の置換機能を使用して、指定したヘッダーテキストを書き換えることができます。このフィルタはヘッダー内で正規表現と一致するテキストを検索し、指定した正規表現に置き換えます。

たとえば、電子メールに次のような件名ヘッダーがあるものとします。

```
Subject: SCAN Marketing Messages
```

次のフィルタは、「SCAN」というテキストを削除し、「Marketing Messages」というテキストをヘッダー内に残します。

```
Remove_SCAN: if true

{

edit-header-text ('Subject', '^SCAN\\s*','');

}
```

フィルタはメッセージを処理した後、次のヘッダーを返します。

```
Subject: Marketing Messages
```

本文編集アクション

edit-body-text() メッセージ フィルタの機能は Edit-Header-Text() フィルタと同様ですが、メッセージのヘッダーではなく本文が処理対象です。

edit-body-text() メッセージフィルタは次の構文を使用します。最初のパラメータは検索のための正規表現で、2 番目のパラメータは置換のためのテキストです。

```
Example: if true {

edit-body-text("parameter 1","parameter 2");

}
```

`edit-body-text()` メッセージ フィルタはメッセージ本文のみが処理対象です。特定の MIME 部分がメッセージの「本文」と見なされるか「添付ファイル」と見なされるかの詳細については、メッセージ本文とメッセージ添付ファイル （160 ページ）を参照してください。

次の例では、メッセージから URL が削除され、「URL REMOVED」というテキストに置き換えられています。

```
URL_Replaced: if true {

edit-body-text("(?i)(?:https?|ftp)://[^\\s\">]+", "URL REMOVED");

}
```

次の例では、メッセージの本文から社会保障番号が削除され、「XXX-XX-XXXX」というテキストに置き換えられています。

```
ssn: if true {

edit-body-text("(?!000)(?:[0-6]\\d{2}|7(?:[0-6]\\d|7[012]))([
-]?)(?!00)\\d\\d\\1(?!0000)\\d{4}",

"XXX-XX-XXXX");

}
```

（注） 現時点では、`edit-body-text()` フィルタではスマート ID を使用できません。

HTML 変換アクション

RFC 2822 では電子メール メッセージのテキスト形式が規定されていますが、RFC 2822 メッセージ内の他のコンテンツのトランスポートを実現するための拡張機能（MIME など）があります。AsyncOS は `html-convert()` メッセージ フィルタを使用して、次の構文により HTML をプレーン テキストに変換できます。

```
Convert_HTML_Filter:

if (true)

{

html-convert();

}
```

Cisco メッセージ フィルタは、特定の MIME 部分がメッセージの「本文」であるか「添付ファイル」であるかを判別します。`html-convert()` メッセージ フィルタはメッセージ本文のみが処理対象です。メッセージの本文と添付ファイルの詳細については、メッセージ本文とメッセージ添付ファイル （160 ページ）を参照してください。

`html-convert()` フィルタが文書内の HTML を削除する方式は、形式によって異なります。

メッセージがプレーンテキスト（text/plain）である場合、メッセージは変更されずにフィルタを通過します。メッセージが単純な HTML メッセージ（text/html）である場合、すべての HTML タグはメッセージから削除され、残りの本文が HTML メッセージにかわり使用されます。各行の再フォーマットは行われず、HTML がプレーン テキストになることはありません。構造が MIME（multipart/alternative 構造）で、同じコンテンツに text/plain 部分と text/html 部分が含まれている場合、フィルタはメッセージの text/html 部分を削除して text/plain 部分を残します。その他の MIME タイプ（multipart/mixed など）では、すべての HTML 本文部分のタグが削除され、メッセージに再挿入されます。

メッセージ フィルタでは、`html-convert()` フィルタ アクションは処理対象のメッセージにタグを設定するだけで、メッセージ構造の変更はすぐには行われません。メッセージの変更は、すべての処理が完了した後に行われます。これにより、変更前に他のフィルタ アクションが元のメッセージを処理することができます。

バウンス プロファイル アクション

`bounce-profile` アクションは、設定済みのバウンス プロファイルをメッセージに割り当てます。（バウンスした電子メールの処理 （884 ページ） を参照。）メッセージを配信できない場合、バウンス プロファイルで設定されたバウンス オプションが使用されます。この機能は、リスナーの設定から割り当てられているバウンスプロファイル（割り当てられている場合）に優先して適用されます。

次のフィルタの例では、送信される電子メールのうち、ヘッダーに「`X-Bounce-Profile: fastbounce`」があるすべての電子メールにバウンス プロファイル「fastbounce」が割り当てられます。

```
fastbounce:

if (header ('X-Bounce-Profile') == 'fastbounce') {

bounce-profile ('fastbounce');

}
```

アンチスパム システムのバイパス アクション

`skip-spamcheck` アクションは、システムに設定されたコンテンツベースのアンチスパム フィルタリングをすべてバイパスするようシステムに指示します。コンテンツベースのアンチスパム フィルタリングが設定されていない場合、またはメッセージがあらかじめスパム スキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、メッセージの IP レピュテーションスコアが高い場合に、メッセージに対するコンテンツベースのアンチスパムフィルタリング機能がバイパスされます。

```
allowed_list_on_reputation:

if (reputation > 7.5)

{

skip-spamcheck();

}
```

関連項目

- 着信リレーが機能にどのように影響するか （505 ページ）
- スパムフィルタからの 電子メールゲートウェイ生成メッセージの保護 （490 ページ）

グレイメール アクションのバイパス

特定のメッセージにグレイメール アクションを適用しない場合、次のメッセージ フィルタ アクションを使用してバイパスできます。

メッセージ フィルタ アクション	説明
skip-marketingcheck	マーケティング メールに対するアクションのバイパス
skip-socialcheck	ソーシャル ネットワーク メールに対するアクションのバイパス
skip-bulkcheck	バルク メールに対するアクションのバイパス

次の例では、リスナー “private_listener” で受信したメッセージは、ソーシャル ネットワーク メールに対するグレイメール アクションをバイパスする必要があること指定しています。

```
internal_mail_is_safe:

if (recv-listener == 'private_listener')

{

skip-socialcheck();

}
```

アンチウイルス システムのバイパス アクション

skip-viruscheck アクションは、システムに設定されたウイルス保護システムをすべてバイパスするようシステムに指示します。アンチウイルス システムが設定されていない場合、またはメッセージがあらかじめウイルス スキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、「private_listener」というリスナーで受信したメッセージに対して、アンチスパム システムとアンチウイルス システムによる処理がバイパスされています。

```
internal_mail_is_safe:

if (recv-listener == 'private_listener')

{

skip-spamcheck();

skip-viruscheck();

}
```

ファイル レピュテーション フィルタリングおよびファイル分析システムのバイパス アクション

skip-ampcheck アクションは、メッセージがシステムで設定されたファイル レピュテーション フィルタリングおよびファイル分析をバイパスすることを許可するよう、システムに指示します。ファイル レピュテーション フィルタリングおよびファイル分析が設定されていない場合、またはメッセージがあらかじめファイル レピュテーション フィルタリングおよびファイル分析スキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、PDF 添付ファイルを含むメッセージがファイル レピュテーション フィルタリングおよびファイル分析をバイパスすることを指定します。

```
skip_amp_scan:
if (attachment-filetype == 'pdf')
{
skip-ampcheck();
}
```

ウイルス アウトブレイク フィルタのスキャニング処理バイパス アクション

skip-vofcheck アクションは、メッセージのウイルス アウトブレイク フィルタによるスキャニング処理がバイパスされるようシステムに指示します。ウイルス アウトブレイク フィルタのスキャニング処理がイネーブルになっていない場合、このアクションを実行してもメッセージに影響はありません。

次の例では、「private_listener」というリスナーで受信したメッセージに対して、ウイルス アウトブレイク フィルタのスキャニング処理がバイパスされています。

```
internal_mail_is_safe:

if (recv-listener == 'private_listener') Outbreak Filters

{

skip-vofcheck();

}
```

メッセージ タグ追加アクション

tag-message アクションは、DLP ポリシー フィルタリングで使用するカスタム用語を送信メッセージに挿入します。DLP ポリシーを設定して、スキャン対象をメッセージ タグがあるメッセージに限定することができます。メッセージ タグは受信者側では表示されません。タグ名には、[a-zA-Z0-9_-.] の範囲の文字のうち任意のものを組み合わせて使用できます。.

メッセージのフィルタリングに使用する DLP ポリシーの設定の詳細については、「データ消失防止」の章を参照してください。

次の例では、件名に「[Encrypt]」が含まれるメッセージにメッセージ タグを挿入しています。Cisco Email Encryption が使用できる場合は、メッセージの配信前にメッセージをこのメッセージ タグで暗号化する DLP ポリシーを作成できます。

```
Tag_Message:

if (subject == '^\\[Encrypt\\]')

{

tag-message('Encrypt-And-Deliver');

}
```

ログ エントリ追加アクション

log-entry アクションは、カスタマイズしたテキストを、テキスト メール ログに INFO レベルで追加します。このテキストにはアクション変数を使用することができます。このアクションを使用すると、デバッグ時に便利なテキストや、メッセージフィルタがアクションを実行した理由に関する情報を挿入できます。ログ エントリはメッセージ トラッキングにも表示されます。

次の例では、メッセージに会社の機密情報が含まれていると判断されたためメッセージがバウンスされたことを示すログ エントリが挿入されます。

```
CompanyConfidential:

if (body-contains('Company Confidential'))

{

log-entry('Message may have contained confidential information.');

bounce();

}
```

URL レピュテーション アクション

メッセージに含まれる URL のレピュテーション スコアを使用して、URL またはその動作を変更します。重要な詳細と例については、悪意のある URL または望ましくない URL からの保護

（543 ページ）のメッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （555 ページ） を参照してください。

これらのアクションでは、ルールは不要です。

URL レピュテーション アクションの各部分は次のとおりです。

- `msg_filter_name` はこのメッセージ フィルタの名前です。
- `min_score` および `max_score` は、アクション適用範囲の最小スコアと最大スコアです。適用範囲には、指定する値も含まれます。

最小スコアと最大スコアは `-10.0` から `10.0` までの範囲内の数値でなければなりません。

- レピュテーション サービスからスコアが提供されない場合のアクションを指定するには、このアクションの「no-reputation」バージョンを使用します。これについては以降の項で説明します。
- `allowedlist` は（`urllistconfig` コマンドを使用して）定義されている URL リストの名前です。許可リストの指定は任意です。
- `Preserve_signed` の位置に 0 または 1 を入力します。
  - 1 - このアクションを未署名のメッセージだけに適用する
  - 0 - このアクションをすべてのメッセージに適用する

`preserve_signed` 値を指定しないと、アクションは未署名のメッセージだけに適用されます。

関連項目

- URL レピュテーションに基づき URL をテキストに置換する （257 ページ）
- URL レピュテーションに基づき URL の危険を取り除く （258 ページ）
- URL レピュテーションに基づき Cisco セキュリティ プロキシに URL をリダイレクトする （258 ページ）

URL レピュテーションに基づき URL をテキストに置換する

レピュテーション サービスからスコアが提供される場合にアクションを実行するには

`url-reputation-replace` アクションを使用します。

`url-reputation-replace` アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:
if <condition>
{url-reputation-replace(<min_score>, <max_score>,'<replace_text>', '< allowedlist>',<
Preserve_signed> );}
```

`replace_text` は、URL を置き換えるテキストです。

レピュテーション サービスからスコアが提供されない場合にアクションを実行するには

`url-no-reputation-replace` アクションを使用します。

url-no-reputation-replace アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:
if <condition>
{url-no-reputation-replace ('<replace_text>', '<allowedlist>', <Preserve_signed>);}
```

replace_text は、URL を置き換えるテキストです。

URL レピュテーションに基づき URL の危険を取り除く

レピュテーション サービスからスコアが提供される場合にアクションを実行するには

url-reputation-defang アクションを使用します。

url-reputation-defang アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:
if <condition>
{url-reputation-defang (<min_score>, <max_score>, '<allowedlist>', <Preserve_signed>);}
```

レピュテーション サービスからスコアが提供されない場合にアクションを実行するには

url-no-reputation-defang アクションを使用します。

url-no-reputation-defang アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:
if <condition>
{url-no-reputation-defang ('<allowedlist>', <Preserve_signed>);}
```

URL レピュテーションに基づき Cisco セキュリティ プロキシに URL をリダイレクトする

レピュテーション サービスからスコアが提供される場合にアクションを実行するには

url-reputation-proxy-redirect アクションを使用します。

url-reputation-proxy-redirect アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:
if <condition>
{url-reputation-proxy-redirect (<min_score>, <max_score>, '<allowedlist>',
<Preserve_signed>);}
```

レピュテーション サービスからスコアが提供されない場合にアクションを実行するには

url-no-reputation-proxy-redirect アクションを使用します。

url-no-reputation-proxy-redirect アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:
if <condition>
```

```
{url-no-reputation-proxy-redirect ('<allowedlist>', <Preserve_signed>);}
```

URL カテゴリ アクション

メッセージに含まれる URL のカテゴリを使用して、URL またはその動作を変更します。重要な詳細については、悪意のある URL または望ましくない URL からの保護（543 ページ）のメッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （555 ページ） を参照してください。

これらのアクションでは、ルールは不要です。

すべての URL カテゴリ アクションの各部分は次のとおりです。

- msg_filter_name はメッセージ フィルタの名前です。
- category-name は URL カテゴリです。複数のカテゴリを指定する場合は、各カテゴリをカンマで区切ります。正しいカテゴリ名を確認するには、コンテンツ フィルタの URL カテゴリ条件またはアクションを確認してください。カテゴリの説明と例については、URL カテゴリについて （568 ページ）を参照してください。
- url_allowed_list は（urllistconfig コマンドを使用して）定義されている URL リストの名前です。
- unsigned-only：0 または 1 を入力します。
  - 1 - このアクションを未署名のメッセージだけに適用する
  - 0 - このアクションをすべてのメッセージに適用する

関連項目

- URL カテゴリに基づき URL をテキストに置換する （259 ページ）
- URL カテゴリに基づき URL の危険を取り除く （259 ページ）
- URL カテゴリに基づき Cisco セキュリティ プロキシに URL をリダイレクトする （260 ページ）

URL カテゴリに基づき URL をテキストに置換する

`url-category-replace` アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:

if <condition>

url-category-replace(['<category-name1>','<category-name2>',...,
'<category-name3>'],'<replacement-text>', '<url_allowed_list>', <unsigned-only>);
```

`replacement-text` は、URL を置き換えるテキストです。

URL カテゴリに基づき URL の危険を取り除く

`url-category-defang` アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:

if <condition>
```

```
url-category-defang(['<category-name1>','<category-name2>',..., '<category-name3>'],
'<url_allowed_list>', <unsigned-only>);
```

URL カテゴリに基づき Cisco セキュリティ プロキシに URL をリダイレクトする

`url-category-proxy-redirect` アクションを使用するフィルタの構文を次に示します。

```
<msg_filter_name>:

if <condition>

url-category-proxy-redirect(['<category-name1>','<category-name2>',...,
'<category-name3>'], '<url_allowed_list>', <unsigned-only>);
```

オペレーションなし

オペレーションなしアクションは、操作を実行しません（no-op）。通知、隔離、ドロップなどその他のアクションを使用しない場合にメッセージフィルタでこのアクションを使用できます。たとえば、作成した新しいメッセージ フィルタの動作を確認する場合に、操作なしアクションを使用できます。メッセージ フィルタが動作したら、[メッセージフィルタ（Message Filters）] レポート ページを使用して新しいメッセージ フィルタの動作をモニタし、要件に対応するようにフィルタを調整できます。

次に、操作なしアクションをメッセージ フィルタで使用する例を示します。

```
new_filter_test: if header-repeats ('subject', X, 'incoming') {no-op();}
```

偽造メールの検出アクション

偽装されたメッセージから From: ヘッダーを削除し、エンベロープ送信者で置き換えます。

次のメッセージフィルタは、メッセージ内の From: ヘッダーと辞書の用語を比較し、コンテンツ辞書の用語のマッチング スコアが 70 以上である場合、メッセージ フィルタは From: ヘッダーを除去し、エンベロープ送信者と置き換えます。

```
FED_CF: if (forged-email-detection("Execs", 70)) { fed("from", ""); }
```

添付ファイルのスキャン

電子メールゲートウェイではコンテンツスキャナを使用して、会社のポリシーと整合しないメッセージから添付ファイルを削除できます。元のメッセージはそのまま配信できます。

添付ファイルのフィルタリングは、特定のファイルタイプ、フィンガープリント、添付ファイルの内容に基づいて行うことができます。フィンガープリントを使用して添付ファイルの正確な種類を判別することにより、ユーザは悪意のある添付ファイルの拡張子（.exeなど）を一般的な拡張子（.docなど）に変更して、名前が変更されたファイルが添付ファイル フィルタを通過できるようにすることができなくなります。

添付ファイルのコンテンツをスキャンする際、コンテンツ スキャナは添付ファイルからデータを抽出し、正規表現による検索を実行します。添付ファイルのデータとメタデータの両方が検査対象となります。Excel または Word 文書をスキャンする場合、添付ファイル スキャン エン

ジンは .exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、.png、Photoshop 画像の各埋め込みファイルも検出できます。

電子メールゲートウェイのコンテンツスキャナでは、次のアーカイブファイル形式でコンテンツスキャンを実行できます。

- ACE アーカイブ
- ALZ アーカイブ
- Apple ディスク イメージ
- ARJ アーカイブ
- bzip2 アーカイブ
- EGG アーカイブ
- GNU Zip
- ISO ディスク イメージ
- Java アーカイブ
- LZH
- Microsoft キャビネット アーカイブ
- RAR マルチパート ファイル
- RedHat パッケージ マネージャ アーカイブ
- Roshal アーカイブ（RAR）
- UNIX AR アーカイブ
- UNIX 圧縮アーカイブ
- UNIX cpio
- UNIX Tar
- XZ アーカイブ
- ZIP アーカイブ
- 7-Zip
- ARC

（注） コンテンツ スキャナ関連ファイルの詳細を表示するには、Web インターフェイスで [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] ページを使用するか、CLI で contentscannerstatus コマンドを使用します。これらのファイルは、アップデート サーバを使用して自動的に更新されます。これらのファイルを手動で更新する場合は、スキャン動作の設定 （297 ページ）を参照してください。

関連項目

- 添付ファイルのスキャンで使用するメッセージ フィルタ （262 ページ）
- イメージ分析 （264 ページ）
- イメージ分析スキャン エンジンの設定 （264 ページ）
- イメージ分析結果に基づいたアクション実行のメッセージフィルタの構成 （266 ページ）
- 通知 （268 ページ）
- 添付ファイルのスキャン メッセージ フィルタの例 （269 ページ）

添付ファイルのスキャンで使用するメッセージ フィルタ

次の表に記載されているメッセージフィルタアクションは、最終でないアクションです。（添付ファイルはドロップされ、メッセージの処理が続行されます）。

オプションのコメントは、フッターのようにメッセージに追加されるテキストで、メッセージ フィルタ アクション変数（添付ファイルのスキャン メッセージ フィルタの例 （269 ページ）を参照）を使用することもできます。

表 *27*：添付ファイルのスキャンで使用するメッセージ フィルタ アクション

操作	構文	説明
添付ファイルのドロップ（名前別）	`drop-attachments-by-name (<regular expression >[, <optional comment >])`	メッセージの添付ファイルのうち、指定した正規表現と一致する名前のファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。添付ファイルのスキャン メッセージ フィルタの例 （269 ページ）を参照してください。
添付ファイルのドロップ（タイプ別）	`drop-attachments-by-type (<MIME type >[, <optional comment >])`	メッセージの添付ファイルのうち、指定したMIMEタイプまたはファイル拡張子に該当するMIMEタイプのファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。

操作	構文	説明
添付ファイルのドロップ（ファイル タイプ別）	`drop-attachments-by-filetype (<fingerprint name >[, <optional comment >])`	メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。
添付ファイルのドロップ（MIME タイプ別）	`drop-attachments-by-mimetype (<MIME type >[, <optional comment >])`	メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。このアクションではファイル拡張子による MIME タイプの判別は行われず、アーカイブの内容の確認もされません。
添付ファイルのドロップ（サイズ別）	`drop-attachments-by-size (<number >[, <optional comment >])`	メッセージの添付ファイルのうち、ローエンコード形式で指定したサイズ（バイト単位）以上のサイズであるファイルをすべてドロップします。アーカイブ ファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の自体のサイズが計測されます。
添付ファイルのスキャン	`drop-attachments-where-contains (<regular expression >[, <optional comment >])`	メッセージの添付ファイルのうち、指定した正規表現を含むファイルをすべてドロップします。アーカイブ ファイル（zip、tar）は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。
添付ファイルのドロップ（辞書との一致別）	`drop-attachments-where-dictionary-match(<dictionary name>)`	このフィルタ アクションは、辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。添付ファイルのスキャン メッセージ フィルタの例（269 ページ） を参照してください。

イメージ分析

メッセージによってはイメージを含むものがあり、適切でないコンテンツがないかスキャンすることが必要になる場合があります。イメージ分析エンジンを使用して、電子メール内の適切でないコンテンツを検索します。

イメージアナライザは、イメージ属性を測定するアルゴリズムを使用して、不適切なコンテンツの可能性を判断します。これらのアルゴリズムは、たとえば、画像内の形状やカラーパレットを検出できます。アナライザは、不適切なコンテンツの特定に役立つように、画像内の形状のタイプと、画像内の他の色に対する肌色の割合を特定できます。肌色の割合が高い画像は、不適切である可能性が高くなります。アルゴリズムは、いかなる方法でも差別しません。

イメージ分析は、アンチウイルスおよびアンチスパム スキャン エンジンの補完または代替を目的とするものではありません。この機能は、電子メール内の適切でないコンテンツを特定することにより、許容範囲での使用を促進するためのものです。イメージ分析スキャンエンジンを使用すると、メールの隔離と分析、および傾向の認識ができます。

電子メールゲートウェイでイメージ分析を設定すると、イメージ分析フィルタルールを使用して、疑わしい電子メールまたは不適切な電子メールに対してアクションを実行できます。イメージ スキャンでは、次のタイプの添付ファイルをスキャンできます：BMP、JPG、TIF、PNG、GIF、TGA、PCX。

イメージ添付ファイルをスキャンすると、Cisco フィンガープリントによりファイル タイプが特定され、イメージアナライザはイメージコンテンツを分析するアルゴリズムを使用します。イメージが他のファイルに埋め込まれている場合、コンテンツ スキャナはファイルを抽出します。イメージ分析の結果は、メッセージ全体で計算されます。メッセージにイメージがない場合、メッセージのスコアは0となります。これは分析結果が「Clean」であることを表します。そのため、イメージがないメッセージに対する分析結果は「Clean」となります。

イメージ分析スキャン エンジンの設定

GUI からイメージ分析をイネーブル化するには、次の手順を実行します。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[IronPortイメージ分析（IronPort Image Analysis）]の順に進みます。

ステップ 2 [有効（Enable）] をクリックします。

成功したことを示すメッセージが表示され、分析結果設定が表示されます。

イメージ分析フィルタルールを使用すると、次の各分析結果に基づいてアクションを決定できます。

- [正常（Clean）]：イメージに適切でないコンテンツはありません。イメージ分析の結果はメッセージ全体で計算されるため、イメージがないメッセージをスキャンすると分析結果は [正常（Clean）] となります。

- [疑わしい（Suspect）]：イメージに適切でないコンテンツがある可能性があります。
- [不適切（Inappropriate）]：イメージに適切でないコンテンツがあります。

これらの計算結果には、イメージアナライザのアルゴリズムにより、適切でないコンテンツがある可能性を示す数値が割り当てられます。

次の値が推奨されます。

- [正常（Clean）]：0 ～ 49
- [疑わしい（Suspect）]：50 ～ 74
- [不適切（Inappropriate）]：75 ～ 100

次のタスク

精度を設定することによりイメージスキャンを微調整できます。これにより、誤判定を減らすことができます。たとえば、誤判定が発生している場合は、精度を低くします。逆に、イメージスキャンで適切でないコンテンツが検出されていない場合は、精度を高く設定します。精度設定は 0（一切検出しない）と 100（精度が最高である）の間の値です。デフォルトの精度の 65 に設定することを推奨します。

関連項目

- イメージ分析設定の調整 （265 ページ）

イメージ分析設定の調整

手順

ステップ 1 [セキュリティサービス（Security Services）]> [IronPortイメージ分析（IronPort Image Analysis）]の順に進みます。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 イメージ分析の精度を設定します。デフォルトの精度の 65 に設定することを推奨します。

ステップ 4 [正常（Clean）]、[疑わしい（Suspect）]、および [不適切（Inappropriate）] の評価を設定します。

値の範囲を設定する場合、値が重ならないようにしてください。また、すべて整数を使用してください。

ステップ 5 任意で、最小サイズの要件を満たさないイメージのスキャンをバイパスするように、AsyncOS を設定します（推奨）。デフォルトで、この設定は 100 ピクセルに設定されています。100 ピクセル未満のイメージをスキャンすると、誤検知が発生する可能性があります。

imageanalysisconfig コマンドを使用して CLI でイメージ分析設定を有効にすることもできます。

次のタスク

関連項目

- 特定のメッセージの判定スコアの表示 （266 ページ）

特定のメッセージの判定スコアの表示

特定のメッセージのレピュテーション スコアを確認するには、メール ログを参照します。メール ログにはイメージ名またはファイル名、特定のメッセージの添付ファイルのスコアが表示されます。また、ログにはファイル内のイメージがスキャン可能かどうかについての情報も表示されます。このログには、各イメージではなく、各メッセージの添付ファイルの結果に関する情報が表示されます。たとえば、メッセージに JPEG イメージを含む zip ファイルが添付されていた場合、ログのエントリにはJPEGの名前ではなく、zipファイルの名前が表示されます。また、zip ファイルに複数のイメージが含まれている場合、ログ エントリにはすべてのイメージの最大スコアが表示されます。「unscannable」の通知は、いずれかのイメージがスキャンできないことを意味します。

ログには、スコアがどのように特定の評価（[正常（clean）]、[疑わしい（suspect）]、または [不適切（inappropriate）]）に反映されるかに関する情報はありません。ただし、メール ログを使用して特定のメッセージの配信を追跡できるため、メッセージに対して実行されたアクションによって、メールに不適切なイメージまたは疑わしいイメージが含まれていたかどうかがわかります。

たとえば、次のメール ログでは、イメージ分析スキャンの結果、メッセージ フィルタ ルールによってドロップされた添付ファイルを示しています。

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
is unscannable.

Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
'Unscannable.jpg' score 0 unscannable

Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
drop-attachments-where-image-verdict filter 'f-001'

Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

イメージ分析結果に基づいたアクション実行のメッセージフィルタの構成

イメージ分析をイネーブルにしたら、メッセージフィルタを作成して、さまざまなメッセージの評価に対してさまざまなアクションを実行する必要があります。たとえば、問題ないと評価されたメッセージを配信し、不適切なコンテンツを含むと判断されたメッセージを隔離する必要があるとします。

（注） シスコでは、不適切または疑わしいと評価されたメッセージをドロップまたはバウンスしないことを推奨します。代わりに、後で確認してトレンド分析について把握するために、違反したメッセージのコピーを隔離します。

次のフィルタは、コンテンツが不適切または疑わしい場合にタグを付けられるメッセージを示しています。

```
image_analysis: if image-verdict == "inappropriate" {

strip-header("Subject");

insert-header("Subject", "[inappropriate image] $Subject");

}

else {

if image-verdict == "suspect" {

strip-header("Subject");


insert-header("Subject", "[suspect image] $Subject");

}

}
```

関連項目

- イメージ分析の評価に基づいて添付ファイルを除去するコンテンツ フィルタの作成 （267 ページ）

イメージ分析の評価に基づいて添付ファイルを除去するコンテンツ フィルタの作成

イメージ分析をイネーブルにすると、コンテンツ フィルタを作成してイメージ分析の評価に基づいて添付ファイルを削除するか、さまざまなメッセージの評価に対してさまざまなアクションを実行するようにフィルタを設定できます。たとえば、不適切なコンテンツを含むメッセージを隔離することに決定したとします。

イメージ分析の評価に基づいて添付ファイルを削除するには、次の手順を実行します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。

ステップ 2 [フィルタを追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前を入力します。

ステップ 4 [アクション（Actions）] で、[アクションを追加（Add Action）] をクリックします。

ステップ 5 [ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] で、[イメージ分析判定（Image Analysis Verdict is）] をクリックします。

ステップ 6 次のイメージ分析の評価から選択します。

- 疑わしい（Suspect）
- 不適切（Inappropriate）
- 不適切もしくは疑わしい（Suspect or Inappropriate）
- スキャン不可（Unscannable）
- 正常（Clean）

イメージ分析判定に基づくアクションの設定

イメージ分析の評価に基づくアクションを設定するには、次の手順を実行します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。

ステップ 2 [フィルタを追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前を入力します。

ステップ 4 [条件（Conditions）] で、[条件を追加（Add Condition）] をクリックします。

ステップ 5 [添付ファイルのファイル情報（Attachment File Info）] で、[イメージ分析判定（Image Analysis Verdict）] をクリックします。

ステップ 6 次のいずれかの評価を選択します。

- 疑わしい（Suspect）
- 不適切（Inappropriate）
- 不適切もしくは疑わしい（Suspect or Inappropriate）
- スキャン不可（Unscannable）
- 正常（Clean）

ステップ 7 [アクションを追加（Add Action）] をクリックします。

ステップ 8 イメージ分析の評価に基づいてメッセージに対して実行するアクションを選択します。

ステップ 9 変更を送信し、保存します。

通知

GUI の [テキストリソース（Text Resources）] ページまたは `textconfig` CLI コマンドを使用して、カスタム通知テンプレートをテキストリソースとして設定することもできます。これも、

添付ファイルのフィルタ ルールと組み合わせて使用すると便利なツールです。通知テンプレートは非ASCII文字をサポートしています（テンプレートを作成するとき、エンコードを選択するように要求されます）。

次の例では、最初に `textconfig` コマンドを使用して、`strip.mp3` という名前の通知テンプレートを作成します。これは、通知メッセージの本文に挿入されます。次に、添付ファイルのフィルタ ルールを作成し、.mp3 ファイルがメッセージから削除された場合、予定していた受信者宛てに .mp3 ファイルが削除されたことを通知する電子メールが送信されるように設定できます。

```
drop-mp3s:

if (attachment-type == '*/mp3')

{ drop-attachments-by-filetype('Media');

notify ('$EnvelopeRecipients', 'Your mp3 has been removed', '$EnvelopeFrom',

'strip.mp3');

}
```

詳細については、通知およびコピー通知アクション （241 ページ）を参照してください。

添付ファイルのスキャン メッセージ フィルタの例

次に、添付ファイルに対して実行されるアクションの例を示します。

- ヘッダーの挿入 （269 ページ）
- ファイル タイプによる添付ファイルのドロップ （270 ページ）
- ディクショナリの一致による添付ファイルのドロップ （271 ページ）
- 保護された添付ファイルの隔離 （272 ページ）
- 保護されていない添付ファイルの検出 （272 ページ）

ヘッダーの挿入

この例では、添付ファイルに指定したコンテンツが含まれている場合に、AsyncOSがヘッダーを挿入します。

次の例では、あるキーワードが含まれるかどうか、メッセージのすべての添付ファイルをスキャンします。すべての添付ファイルにキーワードが存在する場合、カスタムの `X-Header` が挿入されます。

```
attach_disclaim:

if (every-attachment-contains('[dD]isclaimer') ) {

insert-header("X-Example-Approval", "AttachOK");

}
```

次の例では、特定のバイナリ データのパターンがあるかどうか、添付ファイルをスキャンします。フィルタは attachment-binary-contains フィルタ ルールを使用して、PDF ドキュメントが暗号化されていることを示すパターンを検索します。バイナリ データ内にそのパターンが存在する場合、カスタム ヘッダーが挿入されます。

```
match_PDF_Encrypt:

if (attachment-filetype == 'pdf' AND

attachment-binary-contains('/Encrypt')){

strip-header (‘Subject’);

insert-header (‘Subject’, ‘[Encrypted] $Subject’);

}
```

ファイル タイプによる添付ファイルのドロップ

次の例では、添付ファイルの「executable」グループ（.exe、.dll、および .scr）がメッセージから削除され、削除されたファイルの名前をリストするテキストがメッセージに追加されます（$dropped_filename アクション変数を使用して）。drop-attachments-by-filetype アクションは添付ファイルを確認し、3 文字のファイル拡張子だけではなく、ファイルのフィンガープリントに基づいて添付ファイルを削除します。1 つのファイル タイプ（「mpeg」）を指定したり、あるファイル タイプのすべてのメンバ（「Media」）を参照したりできます。

```
strip_all_exes: if (true) {

drop-attachments-by-filetype ('Executable', “Removed attachment:

$dropped_filename”);

}
```

次の例では、エンベロープ送信者がドメイン example.com 内に存在しないメッセージから、同じ「executable」グループの添付ファイル（.exe、.dll、および .scr）が、削除されます。

```
strip_inbound_exes: if (mail-from != "@example\\.com$") {

drop-attachments-by-filetype ('Executable');

}
```

次の例では、エンベロープ送信者がドメイン example.com 内に存在しないメッセージから、ファイル タイプの特定のメンバ（「wmf」）および同じ「executable」グループの添付ファイル（.exe、.dll、および .scr）が削除されます。

```
strip_inbound_exes_and_wmf: if (mail-from != "@example\\.com$") {

drop-attachments-by-filetype ('Executable');

drop-attachments-by-filetype ('x-wmf');
```

```
}
```

次の例では、添付ファイルの「executable」事前定義グループが、より多くの添付ファイルの名前を含むように拡張されています（このアクションでは、添付ファイルのファイルタイプは確認されません）。

```
strip_all_dangerous: if (true) {

drop-attachments-by-filetype ('Executable');

drop-attachments-by-name('(?i)\\.(cmd|pif|bat)$');

}
```

drop-attachments-by-name アクションでは、非 ASCII 文字をサポートしています。

（注） drop-attachments-by-name アクションは、MIME ヘッダーでキャプチャされたファイル名に対して正規表現照合を実行します。MIME ヘッダーからキャプチャされたファイル名は、最後にスペースが存在する場合があります。

次の例では、添付ファイルがメッセージに .exe 実行ファイルのファイル タイプでない場合はドロップされます。ただし、フィルタは、除外するファイル タイプを備えた少なくとも 1 つの添付ファイルがあるメッセージへのアクションを実行しません。たとえば、次のフィルタは **.exe** ファイル タイプではない添付ファイルを含むメッセージをドロップします。

```
exe_check: if (attachment-filetype != "exe") {

drop();

}
```

メッセージに複数の添付ファイルがある場合、電子メールゲートウェイは他の添付ファイルが .exe ファイルでない場合でも、添付ファイルの少なくとも 1 つが .exe ファイルの場合はメッセージをドロップしません。

ディクショナリの一致による添付ファイルのドロップ

この drop-attachments-where-dictionary-match アクションでは、辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。次の例では、「secret_words」辞書内の単語が添付ファイル内で検出されると、添付ファイルが削除されます。一致のしきい値は 1 に設定されている点に注意してください。

```
Data_Loss_Prevention: if (true) {

drop-attachments-where-dictionary-match("secret_words", 1);
```

```
}
```

保護された添付ファイルの隔離

attachment-protected フィルタでは、メッセージ内の添付ファイルがパスワード保護されているかをテストします。受信メールに対してこのフィルタを使用して、添付ファイルがスキャン可能かどうかを確認できます。この定義に従い、1 つの暗号化されたメンバと複数の暗号化されていないメンバーを含む zip ファイルは、保護されていると見なされます。同様に、オープン パスワードが設定されていない PDF ファイルは、コピーや印刷がパスワード保護されていたとしても、保護されているとは見なされません。次の例では、保護された添付ファイルが隔離エリア「Policy」に送信されます。

```
quarantine_protected:

if attachment-protected

{

quarantine("Policy");

}
```

保護されていない添付ファイルの検出

attachment-unprotected フィルタは、メッセージ内の添付ファイルがパスワード保護されていないかをテストします。このメッセージフィルタは、attachment-protected フィルタと補完関係にあります。このフィルタを送信メールに使用して、保護されていないメールを検出することができます。次の例では、AsyncOS が送信リスナーで保護されていない添付ファイルを検出し、メッセージを隔離しています。

```
quarantine_unprotected:

if attachment-unprotected

{

quarantine("Policy");

}
```

メッセージフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出

例として、以下のメッセージフィルタ ルール構文を使用して、ETF エンジンによってメッセージの添付ファイル内で悪意があるとして分類されるファイルを検出し、そのようなメッセージに対して適切な対応をします。

構文：

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'],
<'file_hash_exception_list'>))
{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

それぞれの説明は次のとおりです。

- `'file-hash-etf-rule'` は、添付ファイル情報のメッセージ フィルタのルールです。
- `'etf_source1'` は、ファイルのハッシュに基づいてメッセージの悪意のあるファイルを検出するために使用される ETF ソースです。
- `'file_hash_exception_list'` は、ファイル ハッシュの例外リストの名前です。ファイル ハッシュの例外リストが存在しない場合は「""」と表示されます。
- `'file-hash-etf-strip-attachment-action'` は、悪意のあるファイルが含まれるメッセージに対して適用するアクションです。

以下の例では、メッセージに ETF エンジンによって悪意があるとして検出された添付ファイルが含まれる場合、添付ファイルが除去されます。

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", "Malicious message attachment has been stripped from
the message.");}
```

CLI を使用したメッセージ フィルタの管理

CLI を使用して、メッセージフィルタの追加、削除、アクティブ化/非アクティブ化、インポート/エクスポート、ログ オプションの設定が可能です。次の表で、コマンドとサブコマンドについてまとめて説明します。次の表で、コマンドとサブコマンドについてまとめて説明します。

表 *28*：メッセージ フィルタ サブコマンド

構文	説明
`filters`	メイン コマンド。このコマンドは対話形式で、詳細情報を入力するよう要求されます（たとえば、new、delete、import など）。
`new`	新しいフィルタを作成します。場所を指定しない場合、現在のシーケンスにフィルタが追加されます。場所を指定した場合、シーケンスの特定の場所にフィルタが挿入されます。詳細については、新しいメッセージ フィルタの作成 （275 ページ）を参照してください。
`delete`	名前またはシーケンス番号を指定して、フィルタを削除します。詳細については、メッセージ フィルタの削除 （275 ページ）を参照してください。
`move`	既存のフィルタを並べ替えます。詳細については、新しいメッセージ フィルタの作成 （275 ページ）を参照してください。

構文	説明
`set`	フィルタをアクティブまたは非アクティブ状態に設定します。詳細については、新しいメッセージ フィルタの作成 （275 ページ）を参照してください。
`import`	フィルタの現在のセットを、ファイル（電子メールゲートウェイの/configuration ディレクトリ）内に保存されている新しいセットに置き換えます。詳細については、新しいメッセージ フィルタの作成 （275 ページ）を参照してください。
`export`	フィルタの現在のセットを（電子メールゲートウェイの /configuration ディレクトリ内の）ファイルにエクスポートします。詳細については、メッセージ フィルタのエクスポート （280 ページ）を参照してください。
`list`	1 つ以上のフィルタに関する情報を一覧表示します。詳細については、メッセージ フィルタ リストの表示 （280 ページ）を参照してください。
`detail`	特定のフィルタに関する詳細情報（フィルタ ルール自体の本文など）を出力します。詳細については、メッセージ フィルタの詳細の表示 （280 ページ）を参照してください。
`logconfig`	フィルタの logconfig サブメニューを入力すると、archive() フィルタ アクションからログ サブスクリプションを編集できます。詳細については、フィルタ ログ サブスクリプションの構成 （281 ページ）を参照してください。

（注） フィルタを有効にするには、commit コマンドを発行する必要があります。

パラメータには、次の 3 つのタイプがあります。

表 *29*：フィルタ管理パラメータ

seqnum	フィルタのリスト内の位置に基づいてフィルタを表す整数です。たとえば、*seqnum* が 2 の場合、リスト内の 2 番目のフィルタを表します。
filtname	フィルタの表示名。
range	range は、複数のフィルタを表す場合に使用することがあり、「*X*-Y」の形式で表されます。X と Y は、範囲を指定するための最初と最後の *seqnums* です。たとえば、「`2-4`」は、2、3、4 番目の位置にあるフィルタを表します。X または Y のいずれかを省略すると、無制限のリストを表します。たとえば、「`-4`」は最初から 4 つのフィルタを表し、「`2-`」は、先頭以外のすべてのフィルタを表します。キーワード all を使用して、フィルタ リスト内のすべてのフィルタを表すこともできます。

関連項目

- 新しいメッセージ フィルタの作成 （275 ページ）
- メッセージ フィルタの削除 （275 ページ）
- メッセージ フィルタの移動 （276 ページ）
- メッセージ フィルタのアクティベーションとディアクティベーション （276 ページ）
- 事前ポリシーフィルタのインポート （279 ページ）
- メッセージ フィルタのエクスポート （280 ページ）
- 非 ASCII 文字セットの表示 （280 ページ）
- メッセージ フィルタ リストの表示 （280 ページ）
- メッセージ フィルタの詳細の表示 （280 ページ）
- フィルタ ログ サブスクリプションの構成 （281 ページ）
- メッセージのエンコードの変更 （282 ページ）
- サンプル メッセージ フィルタ （284 ページ）

新しいメッセージ フィルタの作成

`new [seqnum|filtname|last]`

新しいフィルタを挿入する位置を指定します。省略するか、キーワード last を指定すると、入力されたフィルタがフィルタ リストの最後に追加されます。シーケンス番号は連続させる必要があります。現在のリストの範囲を超える *seqnum* は入力できません。不明な *filtname* を入力すると、有効な *filtname*、*seqnum*、または last を入力するように求められます。

フィルタを入力したら、手動でフィルタ スクリプトを入力する必要があります。入力を終了したら、その行自体にピリオド（.）を入力してエントリを終了します。

次の条件ではエラーが発生します。

- シーケンス番号が現在のシーケンス番号の範囲を超えている。
- フィルタに付けた *filtname* が一意ではない。
- フィルタに付けた *filtname* が予約語である。
- フィルタに構文エラーが発生している。
- インターフェイスなど、存在しないシステム リソースを参照するアクションを実行するフィルタ。

メッセージ フィルタの削除

`delete [seqnum|filtname|range]`

指定したフィルタを削除します。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

メッセージ フィルタの移動

```
move [seqnum|filtname|rangeseqnum|last]
```

最初のパラメータで指定したフィルタを、2 番目のパラメータで指定した場所に移動します。2 番目のパラメータがキーワード last である場合、フィルタはフィルタ リストの最後に移動されます。複数のフィルタを移動する場合、それらのフィルタの相対的な順序は変わりません。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。
- シーケンス番号が現在のシーケンス番号の範囲を超えている。
- 移動してもシーケンスが変更されない。

メッセージフィルタのアクティベーションとディアクティベーション

指定されるメッセージ フィルタは、*active* または *inactive* のいずれかであり、さらに *valid* または *invalid* のいずれかです。メッセージ フィルタは、*active* と *valid* の両方の状態である場合にのみ処理に使用されます。CLI を使用して、既存のフィルタを active から inactive に変更します（その後、再び戻します）。存在しない（または削除された）リスナーまたはインターフェイスを参照している場合、そのフィルタは invalid です。

（注） フィルタが inactive であるかどうかは、構文から判断できます。AsyncOS では、inactive であるフィルタのフィルタ名に続くコロンが、感嘆符に変更されます。フィルタを入力またはインポートするときにこの構文を使用すると、AsyncOS はフィルタを inactive としてマークします。

たとえば、次のように無害な「filterstatus」という名前のフィルタを入力します。`filter -> set` サブコマンドを使用して、このフィルタを inactive にします。フィルタの詳細が表示され、コロンが感嘆符に変わっている点に注目してください（以下の例で、太字で示されています）。

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

filterstatus: if true{skip-filters();}

.

1 filters added.
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list
Num Active Valid Name
1 Y Y filterstatus
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> set
Enter the filter name, number, or range:
[all]> all
Enter the attribute to set:
[active]> inactive
1 filters updated.
Choose the operation you want to perform:
```

```
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> detail
Enter the filter name, number, or range:
[]> all
Num Active Valid Name
1 N Y filterstatus
filterstatus! if (true) {
skip-filters();
}
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
```

関連項目

- メッセージフィルタのアクティベーションまたはディアクティベーション （279ページ）

メッセージ フィルタのアクティベーションまたはディアクティベーション

```
set [seqnum|filtname|range] active|inactive
```

指定したフィルタを指定した状態に設定します。状態のルールは次のとおりです。

- active：選択したフィルタの状態を active に設定します。
- inactive：選択したフィルタの状態を inactive に設定します。

次の条件ではエラーが発生します。

- 指定した *filtname* のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

（注） inactive であるフィルタは、構文からも判断できます。ラベル（フィルタ名）の後のコロンが、感嘆符（!）に変更されます。CLI から手動で入力された、またはインポートされたフィルタにこの構文が含まれる場合、自動的に inactive とマークされます。たとえば、mailfrompm! が、mailfrompm: の代わりに表示されます。

事前ポリシーフィルタのインポート

```
import filename
```

処理されるフィルタを含むファイルの名前です。このファイルは、アプライアンスのFTP/SCPルートディレクトリのconfigurationディレクトリ内に存在する必要があります（`interfaceconfig` コマンドを使用してインターフェイスの FTP/SCP アクセスを有効にしている場合）。ファイルは取り込まれて解析され、エラーが存在すれば報告されます。現在のフィルタ セット内に存在するすべてのフィルタは、インポートされたフィルタに置き換わります。詳細については、FTP、SSH、およびSCPアクセス （1573ページ）を参照してください。現在のフィルタ リストをエクスポートし（メッセージフィルタのエクスポート （280ページ）を参照）、そのファイルを編集してインポートすることを推奨します。

メッセージ フィルタをインポートする場合、使用するエンコードを選択するよう求められます。

次の条件ではエラーが発生します。

- ファイルが存在しない。
- フィルタ名が一意ではない。
- フィルタに付けた *filtname* が予約語である。
- フィルタに構文エラーが発生している。
- インターフェイスなど、存在しないシステム リソースを参照するアクションを実行するフィルタ。

メッセージ フィルタのエクスポート

`export filename[seqnum|filtname|range]`

既存のフィルタセットを、電子メールゲートウェイの FTP/SCP ルートディレクトリにある configuration ディレクトリ内のファイルに所定の形式で出力します。詳細については、FTP、SSH、および SCP アクセス （1573 ページ）を参照してください。

メッセージフィルタをエクスポートする場合、使用するエンコードを選択するよう求められます。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

非 ASCII 文字セットの表示

このシステムでは、CLI で非 ASCII 文字が UTF-8 で表示されます。お使いのターミナル/ディスプレイが UTF-8 をサポートしていない場合、フィルタが正常に表示されません。

フィルタ内の非 ASCII 文字を管理する最も良い方法は、フィルタをテキストファイルで編集してから、そのテキストファイルを電子メールゲートウェイにインポートすることです（事前ポリシーフィルタのインポート （279 ページ）を参照）。

メッセージ フィルタ リストの表示

`list [seqnum|filtname|range]`

指定したフィルタの本文を出力せずに、概要を表形式で表示します。表示される情報は次のとおりです。

- フィルタ名
- フィルタ シーケンス番号
- フィルタの active/inactive 状態
- フィルタの valid/invalid 状態

次の条件ではエラーが発生します。

- 範囲の指定が不正である。

メッセージ フィルタの詳細の表示

`detail [seqnum|filtname|range]`

フィルタの本文や追加の状態情報など、指定したフィルタの情報をすべて表示します。

フィルタ ログ サブスクリプションの構成

`logconfig`

サブメニューを入力し、`archive()` アクションによって生成されたメールボックス ファイルのフィルタ ログ オプションを設定できます。これらのオプションは、通常の `logconfig` コマンドで使用されるオプションとよく似ていますが、ログを参照するフィルタを追加または削除することによってのみ、ログを作成または削除できます。

各フィルタ ログ サブスクリプションには次のデフォルト値が設定されています。この値は、logconfig サブコマンドを使用して変更できます。

- 取得方法：FTP Poll
- ファイル サイズ：10MB
- ファイルの最大数：10

詳細については、「ロギング」の章を参照してください。

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> logconfig

Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll

Choose the operation you want to perform:

- EDIT - Modify a log setting.

[]> edit

Enter the number of the log you wish to edit.

[]> 1
```

```
Choose the method to retrieve the logs.

1. FTP Poll

2. FTP Push

3. SCP Push

[1]> 1

Please enter the filename for the log:

[joesmith.mbox]>

Please enter the maximum file size:

[10485760]>

Please enter the maximum number of files:

[10]>

Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll

Enter "EDIT" to modify or press Enter to go back.

[]>
```

メッセージのエンコードの変更

localeconfig コマンドを使用して、メッセージ処理中のメッセージのヘッダーおよびフッターのエンコードの変更に関する AsyncOS の動作を設定できます。

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
 encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?

(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
 of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main
```

```
body in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
 or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body
whenever possible.
However, if the disclaimer is encoded differently than the message body, and if imposing
 a single encoding
will cause loss of characters, it will be added as an attachment. The system will always
 try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit
the message body to
use an encoding that is compatible with the message body as well as the disclaimer.
Should the system try to
re-encode the message body in such a case? [Y]>

If the disclaimer that is added to the footer or header of the message generates an error
 when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added
as an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
 content is split into
separate email attachments. Should the system try to ignore such errors when decoding
the message body? [N]>

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
 encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]>
```

最初のプロンプトは、ヘッダーが（たとえばフィルタによって）変更されていた場合、メッセージヘッダーのエンコードをメッセージ本文に一致するように変更するかどうかを指定します。

2番目のプロンプトは、ヘッダーの文字セットが適切にタグで指定されていない場合、電子メールゲートウェイがヘッダーに対してメッセージ本文のエンコードを強制する必要があるかどうかを制御します。

3 番目のプロンプトは、免責事項のスタンプ（および複数のエンコード）がメッセージ本文でどのように機能するかを制御するために使用されます。詳細については、「テキスト リソース」の章の「免責事項スタンプと複数エンコード方式」を参照してください。

4 番目のプロンプトは、メッセージ本文のデコード時にエラーが生成された場合に、免責事項スタンプの動作を設定するために使用されます。[はい（Yes）] を選択するとデコード エラーは無視され、免責事項スタンプが行われます。[いいえ（No）]を選択すると、メッセージに免責事項テキストが添付されます。

サンプル メッセージ フィルタ

次の例では、filter コマンドを使用して新しいフィルタを 3 つ作成します。

- 最初のフィルタの名前は、**big_messages** です。これは body-size ルールを使用して、10 MB より大きいメッセージをドロップします。
- 2 番目のフィルタの名前は、**no_mp3s** です。これは attachment-filename ルールを使用して、.mp3 ファイル拡張子が付いた添付ファイルを含むメッセージをドロップします。
- 3 番目のフィルタの名前は、**mailfrompm** です。これは mail-from ルールを使用して、postmaster@example.com からのメールをすべて調べ、administrator@example.com のブラインド カーボン コピーを作成します。

filter -> list サブコマンドを使用し、フィルタのリストを表示して、フィルタがアクティブで有効であることを確認します。次に、move サブコマンドを使用して、最初と最後のフィルタの位置を入れ替えます。最後に、変更を確定してフィルタを有効にします。

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

big_messages:

if (body-size >= 10M) {

drop();

}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.
```

```
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
no_mp3s:
if (attachment-filename == '(?i)\\.mp3$') {
drop();
}
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
mailfrompm:
if (mail-from == "^postmaster$")
{ bcc ("administrator@example.com");}
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
```

```
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list
Num Active Valid Name
1 Y Y big_messages
2 Y Y no_mp3s
3 Y Y mailfrompm
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> move
Enter the filter name, number, or range to move:
[]> 1
Enter the target filter position number or name:
[]> last
1 filters moved.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
```

```
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list
Num Active Valid Name
1 Y Y no_mp3s
2 Y Y mailfrompm
3 Y Y big_messages
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> move
Enter the filter name, number, or range to move:
[]> 2
Enter the target filter position number or name:
[]> 1
1 filters moved.
Choose the operation you want to perform:
- NEW - Create a new filter.
```

```
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

[]> list
Num Active Valid Name
1 Y Y mailfrompm
2 Y Y no_mp3s
3 Y Y big_messages
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.

- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> entered and enabled 3 filters: no_mp3s, mailfrompm, big_messages
Do you want to save the current configuration for rollback? [Y]> n
```

```
Changes committed: Fri May 23 11:42:12 2014 GMT
```

メッセージ フィルタの例

この項では、実際のフィルタの例を示し、各フィルタについて簡単に説明します。

関連項目

- オープンリレー防止フィルタ （289 ページ）
- ポリシー適用フィルタ （290 ページ）
- ルーティングおよびドメイン スプーフィング （293 ページ）
- ファイル SHA-256 フィルタに一致するメッセージ添付ファイルをドロップする （297 ページ）
- 添付ファイルがファイル SHA-256 フィルタと一致する場合にメッセージをドロップする （297 ページ）

オープンリレー防止フィルタ

このフィルタは、次のように電子メール アドレスに %、余分な @、および ! 文字が含まれているメッセージをバウンスします。

- `user%otherdomain@validdomain`
- `user@otherdomain@validdomain:`
- `domain!user@validdomain`

```
sourceRouted:

if (rcpt-to == "(%|@|!)(.*)@") {

bounce();

}
```

電子メールゲートウェイは、従来の Sendmail/Qmail システムを活用するためによく使用される、このようなサードパーティ製のリレーハックの影響を受けません。これらの記号の多く（% など）は正当な電子メールアドレスの一部である可能性があるため、電子メールゲートウェイはこれらを有効なアドレスとして受け入れ、設定済みの受信者リストと照合し、次の内部サーバに渡します。電子メールゲートウェイは、これらのメッセージを外部にリレーしません。

このようなフィルタは、このタイプのメッセージをリレーできるように誤って設定されたオープンソース MTA を使用しているユーザを保護するために所定の場所に設定されます。

（注） このようなタイプのアドレスを処理するように、リスナーを設定することもできます。詳細については、Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング （88 ページ）を参照してください。

ポリシー適用フィルタ

- 件名に基づき通知するフィルタ （290 ページ）
- 競合他社に送信されたメールの BCC およびスキャン （290 ページ）
- 特定のユーザをブロックするフィルタ （291 ページ）
- メッセージのアーカイブおよびドロップ フィルタ （291 ページ）
- 大きい「To:」ヘッダーのフィルタ （291 ページ）
- 空白の「From:」フィルタ （292 ページ）
- IP レピュテーションフィルタ （292 ページ）
- IP レピュテーションフィルタの変更 （292 ページ）
- ファイル名の正規表現フィルタ （292 ページ）
- ヘッダー内の IP レピュテーションスコアの表示フィルタ （293 ページ）
- ポリシーのヘッダーへの挿入フィルタ （293 ページ）
- 多数の受信者のバウンス フィルタ （293 ページ）

件名に基づき通知するフィルタ

このフィルタは、件名に特定の用語が含まれているかどうかに基づいて通知を送信します。

```
search_for_sensitive_content:

if (Subject == "(?i)plaintiff|lawsuit|judge" ) {

notify ("admin@company.com");

}
```

競合他社に送信されたメールの BCC およびスキャン

このフィルタは、競合他社に送信されたメッセージをスキャンし、ブラインドコピーを作成します。辞書と `header-dictionary-match()` ルールを使用して、柔軟性の高い競合他社のリストを指定できます（ディクショナリ ルール （202 ページ）を参照）。

```
competitorFilter:

if (rcpt-to == '@competitor1.com|@competitor2.com') {

bcc-scan('legal@example.com');
```

```
}
```

特定のユーザをブロックするフィルタ

このフィルタを使用すると、特定のアドレスからの電子メールをブロックします。

```
block_harrasing_user:

if (mail-from == "ex-employee@hotmail\\.com") {

notify ("admin@company.com");

drop ();

}
```

メッセージのアーカイブおよびドロップ フィルタ

ファイルタイプが一致するメッセージのみをログ記録およびドロップします。

```
drop_attachments:

if (mail-from != "user@example.com") AND (attachment-filename ==

'(?i)\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$')

{

archive("Drop_Attachments");

insert-header("X-Filter", "Dropped by: $FilterName MID: $MID");

drop-attachments-by-name("\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$");

}
```

大きい「To:」ヘッダーのフィルタ

「To」ヘッダーが非常に大きいメッセージを検索します。

`archive()` 行を使用して適切なアクションを検証し、drop() をイネーブルまたはディセーブルにして安全性を高めます。

```
toTooBig:

if(header('To') == "^.{500,}") {

archive('tooTooBigdropped');

drop();

}
```

空白の「From:」フィルタ

空白の「From」ヘッダーを特定します。

このフィルタは、「from」アドレスが空白であるさまざまな形式に対応できます。

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND header("From") == "^$|<\\s*>") {

drop ();

}
```

また、Envelope Fromが空欄のメッセージをドロップする場合は、次のフィルタを使用します。

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND (mail-from == "^$|<\\s*>" OR header ("From") ==
"^$|<\\s*>"))

{

drop ();
}
```

IP レピュテーションフィルタ

IP レピュテーションフィルタ：

```
note_bad_reps:
if (reputation < -2) {
strip-header ('Subject');

insert-header ('Subject', '***BadRep $Reputation *** $Subject');
}
```

IP レピュテーションフィルタの変更

特定のドメインの IP レピュテーションスコアしきい値の変更：

```
mod_ipr:
if ( (rcpt-count == 1) AND (rcpt-to == "@domain\\.com$") AND (reputation < -2) ) {
drop ();
}
```

ファイル名の正規表現フィルタ

このフィルタは、メッセージ本文のサイズの範囲を指定し、正規表現に一致する添付ファイルを検索します（このパターンに一致するファイル名は、「readme.zip」、「readme.exe」、「attach.exe」、など）。

```
filename_filter:
if ((body-size >= 9k) AND (body-size <= 20k)) {
if (body-contains ("(?i)(readme|attach|information)\\.(zip|exe)$")) {
drop ();

}

}
```

ヘッダー内の IP レピュテーションスコアの表示フィルタ

ヘッダーのログが記録されるので、メール ログで表示できます（「ロギング」の章を参照）。

```
Check_ipr:

if (true) {

insert-header('X-ipr', '$Reputation');

}
```

ポリシーのヘッダーへの挿入フィルタ

どのメール フロー ポリシーが接続を受け入れたかを示します。

```
Policy_Tracker:

if (true) {

insert-header ('X-HAT', 'Sender Group $Group, Policy $Policy applied.');

}
```

多数の受信者のバウンス フィルタ

3 つ以上の固有ドメインから 50 人を超える受信者が指定されている発信電子メール メッセージをすべてバウンスします。

```
bounce_high_rcpt_count:

if ( (rcpt-count > 49) AND (rcpt-to != "@example\\.com$") ) {

bounce-profile ("too_many_rcpt_bounce"); bounce ();

}
```

ルーティングおよびドメイン スプーフィング

- Virtual Gateway フィルタの使用 （294 ページ）
- 配信とリスナーのフィルタに対する同じリスナーの使用 （294 ページ）

• 単一のリスナーのフィルタ （294 ページ）
• スプーフィング ドメインのドロップ フィルタ（単一のリスナー） （295 ページ）
• スプーフィング ドメインのドロップ フィルタ（複数のリスナー） （295 ページ）
• 別のスプーフィング ドメインのドロップ フィルタ （295 ページ）
• ルーピングの検出フィルタ （296 ページ）

Virtual Gateway フィルタの使用

仮想ゲートウェイを使用してトラフィックを区分します。システムに2つのインターフェイス「public1」と「public2」が存在するとします。デフォルトの配信インターフェイスは「public1」です。これにより、発信トラフィックはすべて2番目のインターフェイスを介すように強制されます。バウンスおよびその他同様のタイプのメールはフィルタを通過しないため、そのようなメールは public1 から配信されます。

```
virtual_gateways:

if (recv-listener == "OutboundMail") {

alt-src-host ("public2");

}
```

配信とリスナーのフィルタに対する同じリスナーの使用

配信と受信に同じリスナーを使用します。このフィルタでは、パブリック リスナー「listener1」で受信したメッセージを、インターフェイス「listener1」から送信できます（設定したパブリック インジェクタごとに、固有のフィルタをセットアップする必要があります）。

```
same_listener:

if (recv-inj == 'listener1') {

alt-src-host('listener1');

}
```

単一のリスナーのフィルタ

単一のリスナーでフィルタを機能させます。たとえば、システム全体で実行するのではなく、メッセージ フィルタを処理する専用のリスナーを指定します。

```
textfilter-new:

if (recv-inj == 'inbound' and body-contains("some spammy message")) {

alt-rcpt-to ("spam.quarantine@spam.example.com");

}
```

スプーフィング ドメインのドロップ フィルタ（単一のリスナー）

スプーフィング ドメイン（内部のアドレスからであると偽り、単一のリスナーで機能する）が使用されている電子メールをドロップします。以下の IP アドレスは、架空のドメイン mycompany.com を表しています。

```
DomainSpoofed:
if (mail-from == "mycompany\\.com$") {
if ((remote-ip != "1.2.") AND (remote-ip != "3.4.")) {
drop();
}
}
```

スプーフィング ドメインのドロップ フィルタ（複数のリスナー）

前述と同じですが、複数のリスナーを使用して動作します。

```
domain_spoof:
if ((recv-listener == "Inbound") and (mail-from == "@mycompany\\.com")) {
archive('domain_spoof');
drop ();
}
```

別のスプーフィング ドメインのドロップ フィルタ

概要：ドメイン スプーフィング対策フィルタ：

```
reject_domain_spoof:
if (recv-listener == "MailListener") {
insert-header("X-Group", "$Group");
if ((mail-from == "@test\\.mycompany\\.com") AND (header("X-Group") != "RELAYLIST")) {
notify("me@here.com");
drop();
strip-header("X-Group");
}
```

ループピングの検出フィルタ

このフィルタを使用して、メールループを発生させている要因を検出、停止、および判断します。このフィルタは、Exchangeサーバまたはそれ以外の場所で発生している構成の問題を判断するために役立ちます。

```
External_Loop_Count:

if (header("X-ExtLoop1")) {


if (header("X-ExtLoopCount2")) {

if (header("X-ExtLoopCount3")) {

if (header("X-ExtLoopCount4")) {

if (header("X-ExtLoopCount5")) {

if (header("X-ExtLoopCount6")) {

if (header("X-ExtLoopCount7")) {

if (header("X-ExtLoopCount8")) {

if (header("X-ExtLoopCount9")) {

notify ('joe@example.com');

drop();

}

else {insert-header("X-ExtLoopCount9", "from
$RemoteIP");}}

else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}

else {insert-header("X-ExtLoop1", "1");

}
```

（注） デフォルトでは、AsyncOS は自動的にメールのループを検出し、100 回ループしたメッセージをドロップします。

ファイルSHA-256フィルタに一致するメッセージ添付ファイルをドロップする

ファイルハッシュリスト内の特定のファイル SHA-256 値と一致するメッセージ内のすべてのメッセージ添付ファイルをドロップするには、このフィルタを使用します

```
File_Hash_Message_Filter: if (true)
{ drop-attachments-by-hash("SHA-256_hash_list"); }
```

添付ファイルがファイル SHA-256 フィルタと一致する場合にメッセージをドロップする

メッセージ添付ファイルがファイルハッシュリスト内の特定のファイル SHA-256 値と一致する場合にすべてのメッセージをドロップするには、このフィルタを使用します。

```
File_Hash_Message_Filter: if (attachment-hashlist-match("SHA-256_hash_list"))
{ drop(); }
```

スキャン動作の設定

スキャンパラメータを設定することで、本文と添付ファイルのスキャン動作（スキャン中にスキップする添付ファイルのタイプなど）を制御できます。これらのパラメータを設定するには、[スキャン動作（Scan Behavior）] ページまたは `scanconfig` コマンドを使用します。スキャン動作の設定はグローバルな設定であるため、すべてのスキャンの動作に影響します。

（注） zip などの圧縮ファイルに含まれる MIME タイプをスキャンする場合、スキャン リストに「compressed」または「zip」または「application/zip」リストを含める必要があります。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] をクリックします。

ステップ 2 添付ファイル タイプのマッピングを定義します。次のいずれかを実行します。

- 新しい添付ファイル タイプのマッピングを追加する。[マッピングの追加（Add Mappin）] をクリックします。
- 設定ファイルを使用して添付ファイル タイプ マッピングのリストをインポートする。[インポートリスト（Import List）] をクリックし、configuration ディレクトリから該当する設定ファイルをインポートします。

  （注） この手順を実行するためには、設定ファイルが、電子メールゲートウェイの configuration ディレクトリに存在する必要があります。設定ファイルの管理（1243 ページ）を参照してください。

• 既存の添付ファイルタイプマッピングを変更するには[編集（Edit）]をクリックします。

ステップ 3 グローバル設定を行います。次の手順を実行します。

a) [グローバル設定（Global Settings）] で、[グローバル設定を編集（Edit Global Settings）] をクリックします。

b) 以下の必須フィールドを編集します。

フィールド	説明
上記の表にある MIME タイプ/フィンガープリントの添付ファイルの場合のアクション（**Action for attachments with MIME types / fingerprints in table above**）	添付ファイル タイプ マッピングで定義されている添付ファイル タイプをスキャンするか、またはスキップするかを選択します。
スキャンする添付ファイル繰り返しの最大深度（**Maximum depth of attachment recursion to scan**）	スキャンする添付ファイルの繰り返しの最大レベルを指定します。
スキャンする最大添付ファイルサイズ（**Maximum attachment size to scan**）	スキャンする添付ファイルの最大サイズを指定します。
添付ファイルメタデータスキャン（**Attachment Metadata scan**）	添付ファイルのメタデータをスキャンするか、またはスキップするかを指定します。
添付ファイルスキャンタイムアウト（**Attachment scanning timeout**）	スキャンのタイムアウト期間を指定します。
何らかの理由でスキャンされない場合、添付ファイルがパターンに一致するものと仮定します（**Assume attachment matches pattern if not scanned for any reason**）	スキャンされない添付ファイルを検索パターンに一致するものとみなすかどうかを指定します。
メッセージを分解し、指定の添付ファイルを削除できないときのアクション（**Action when message cannot be deconstructed to remove specified attachments**）	指定の添付ファイルを削除するためにメッセージを分解できないときに実行するアクションを指定します。
コンテンツまたはメッセージフィルタエラーの場合、すべてのフィルタをバイパスします（**Bypass all filters in case of a content or message filter error**）	コンテンツまたはメッセージ フィルタ エラーの場合にすべてのフィルタをバイパスするかどうかを指定します。
何も指定されていないときに使用する符号化（**Encoding to use when none is specified**）	エンコーディングが指定されていない場合に使用するエンコーディングを指定します。
不透明な署名の付いたメッセージを明瞭な署名のものに変換する(S/MIME アンパック)（**Convert opaque-signed messages to clear-signed (S/MIME unpacking)**）	不透明な署名の付いたメッセージを明瞭な署名のものに変換する(S/MIME アンパック)かどうかを指定します。
Safe Print の設定	

フィールド	説明
最大ファイル サイズ（Maximum File Size）	Safe Print で出力される添付ファイルの最大添付ファイル サイズを入力します。 （注） [最大ファイルサイズ（Maximum File Size）] 値が電子メール ゲートウェイの [アウトブレイクフィルタ（Outbreak Filters）] に設定した [スキャンする最大メッセージサイズ（Maximum Message Size to Scan）] 値を超える場合、メッセージとメッセージ添付ファイルは電子メール パイプラインのアウトブレイク フィルタではスキャンされません。
最大ページ数（Maximum Page Count）	メッセージの添付ファイルで Safe Print を使用して出力するページの最大数を入力します。
ドキュメントの品質（Document Quality）	Safe Print で出力される添付ファイルに推奨されるイメージ品質値を使用するには、[デフォルト値（70）の使用（Use Default Value (70)）] オプションを選択します。 （注） [カスタム値の入力（Enter Custom Value）] オプションを選択して、Safe Print で出力される添付ファイルのカスタムイメージ品質値を入力することもできます。
ファイルタイプの選択（File Type Selection）	メッセージの添付ファイルを Safe Print で出力する場合に使用可能なファイル グループ（「Microsoft Documents」など）から必要なファイル タイプを選択します。
Watermark	Safe Print で出力される添付ファイルに Watermark を追加するには、[有効（Enabled）] オプションを選択します。 （注） [カスタムテキストの入力（Enter Custom Text）] フィールドに Watermark のカスタム テキストを入力します。

フィールド	説明
カバーページ（Cover Page）	Safe Print で出力される添付ファイルにカバーページを追加するには、[有効（Enabled）] オプションを選択します。 （注） [カスタムテキストの入力（Enter Custom Text）] フィールドにカバーページのカスタムテキストを入力します。
詳細については、メッセージの添付ファイルを Safe Print で出力する場合の電子メールゲートウェイの設定方法 （414 ページ）を参照してください。	
パスワードで保護された添付ファイルのスキャン	

フィールド	説明
パスワードで保護された添付ファイルのスキャンを有効にします。	[受信メールトラフィック（Inbound Mail Traffic）] または [発信メールトラフィック（Outbound Mail Traffic）] の下の [有効（Enabled）] オプションを選択して、電子メールゲートウェイのコンテンツスキャナを設定し、着信メッセージまたは発信メッセージ内のパスワードで保護された添付ファイルの内容をスキャンできます。 （注） 電子メールゲートウェイでDLPスキャンエンジンが有効になっているとします。この場合、パスワードの抽出に成功すると、パスワードで保護された添付ファイルの内容が、設定されたDLPポリシーに従ってDLPエンジンでスキャンされます。 重要 • コンテンツスキャナがメッセージの本文からパスワードを抽出し、添付ファイルの内容を正常にスキャンできるとします。この場合、パスワードと添付ファイルがCisco AMP Threat Gridに送信されます（電子メールゲートウェイで設定されている場合）。このファイルはファイル分析に推奨されます。 • コンテンツスキャナは、ベストエフォートでメッセージの本文からパスワードを抽出します。スキャンが完了すると、抽出されたパスワードは電子メールゲートウェイに保存されません。

フィールド	説明
分析用ユーザー定義パスワード候補：	

フィールド	説明
	[有効（Enabled）] オプションを選択してユーザ定義のパスフレーズを作成し、着信メッセージまたは発信メッセージ内のパスワードで保護された添付ファイルを開きます。 複数のユーザ定義パスフレーズを追加する場合は、[行を追加（Add Row）] をクリックします。 （注） • 最大 128 文字のユーザ定義パスフレーズを作成できます。。 • 最大 5 つのユーザ定義パスフレーズを作成できます。 • 必要な優先度に対応するユーザ定義のパスフレーズを [パスワード（Password）] フィールドに入力して、ユーザ定義のパスフレーズの優先度を変更できます。 • （着信メールのみ）メッセージ本文から抽出されたパスフレーズは、着信メッセージのパスワード保護された添付ファイルを開くために使用されるユーザ定義のパスフレーズよりも優先されます。 • （発信メールのみ）ユーザ定義のパスフレーズは、発信メッセージのパスワード保護された添付ファイルを開くために使用されるメッセージ本文から抽出されたパスフレーズよりも優先されます。 （オプション）[ユーザー定義のパスワードのみを適用（Apply User-defined Passwords Only）] チェックボックス：ユーザー定義のパスフレーズのみを使用して、受信および送信メッセージでパスワードで保護された添付ファイルを開く場合は、このチェックボックスを選択します。このチェックボックスを選択すると、電子メールゲートウェイは、パスワードで保護された添付ファイルを開く際に電子メール本文から抽出されたパスフレーズを使用しません。

フィールド	説明
	（注） [ユーザー定義の分析用パスワード候補（Probable User-defined Password for Analysis）] オプションボタンを有効にしない場合、[ユーザー定義のパスワードのみを適用（Apply User-defined Passwords Only）] チェックボックスはデフォルトで無効になります。
URL フィルタリング アクション中に検出された復号エラーによるスキャン不可メッセージに対するアクション	URL フィルタリング アクション中に検出された復号エラーが原因で、コンテンツ スキャナによってスキャンできないメッセージに対して実行するアクションを指定します。
抽出エラーによるスキャン不可メッセージに対するアクション	添付ファイル抽出エラーが原因で、メッセージをコンテンツ スキャナでスキャンできない場合に実行するアクションを指定します。
RFC 違反によるスキャン不可メッセージに対するアクション	RFC 違反が原因で、メッセージをコンテンツ スキャナでスキャンできない場合に実行するアクションを指定します。

c) [送信（Submit）] をクリックします。

ステップ 4 （任意）コンテンツ スキャナ ファイルを手動で更新します。[現在のコンテンツ スキャナ ファイル（Current Content Scanner files）] で [今すぐ更新（Update Now）] をクリックします。

通常、これらのファイルは、アップデート サーバを使用して自動的に更新されます。

（注） CLI で `contentscannerupdate` を使用して、これらのファイルを手動で更新することもできます。

ステップ 5 変更を確定します。

スキャンできないメッセージのメッセージ処理アクションの設定

電子メールゲートウェイのコンテンツスキャナを使用して、以下の理由によりスキャンされないメッセージを処理できるようになりました。

- ファイル抽出失敗
- RFC 違反
- URL フィルタリング アクション中に検出された復号エラー

コンテンツ スキャナによってスキャンされないメッセージに対する、次のいずれかのメッセージ処理アクションを構成できます。

- メッセージのドロップ
- メッセージをそのまま配信
- ポリシー隔離へのメッセージの送信

Web インターフェイスの [セキュリティ サービス（Security Services）] > [スキャン動作（Scan Behavior）] ページで [グローバル設定の編集（Edit Global Settings）] ボタンをクリックして、コンテンツ スキャナによってスキャンされないメッセージに対するメッセージ処理アクションを有効にして構成することができます。

メッセージの配信

メッセージを配信する場合に、次の操作を実行できます。

- メッセージの件名を変更します。
- メッセージへのカスタム ヘッダーの追加
- メッセージの受信者の変更
- 代替宛先ホストへのメッセージの送信

（注） これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。

メッセージの件名を修正

コンテンツ スキャナによってスキャンされないメッセージのテキストを、特定のテキスト文字列を前に付加または後に付加することにより変更して、ユーザが容易に識別でき、識別されたメッセージを並べ替えることができるようになります。

（注） [メッセージの件名を修正（Modify message subject）] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、`[WARNING: UNSCANNABLE EXTRACTION FAILURE]` というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

コンテンツ スキャナによってスキャンされないメッセージの件名に追加されるデフォルトのテキストは次のとおりです。

理由	件名へのデフォルトのテキストの追加
抽出エラー	[WARNING: UNSCANNABLE EXTRACTION FAILED]
RFC 違反	[WARNING: UNSCANNABLE RFC NON-COMPLIANT]
URL フィルタリング アクション中に検出された復号エラー	[WARNING: DECODING ERRORS WHEN APPLYING URL FILTERING ACTIONS]

メッセージへのカスタム ヘッダーの追加

コンテンツ スキャナによってスキャンされないすべてのメッセージに追加する、追加のカスタム ヘッダーを定義できます。[はい（Yes）] をクリックし、ヘッダー名およびテキストを定義します。

メッセージの受信者の変更

メッセージの受信者を変更して、コンテンツ スキャナによってスキャンされないメッセージが別のアドレスに送信されるようにできます。[はい（Yes）] をクリックして、新しい受信者のアドレスを入力します。

代替宛先ホストへのメッセージの送信

コンテンツ スキャナによってスキャンされないメッセージに対し、別の受信者または宛先ホストに通知を送信することができます。[はい（Yes）] をクリックして代替アドレスまたはホストを入力します。

たとえば、コンテンツ スキャナによってスキャンされないメッセージを、管理者のメールボックスまたは特別なメール サーバに、その後の調査のためにルーティングできます。受信者が複数のメッセージの場合は、代替受信者に送信されるコピーは 1 つのみです。

ポリシー隔離へメッセージの送信

隔離に関するフラグが設定されると、コンテンツ スキャナによってスキャンされないメッセージは、電子メール パイプラインのそれ以降の部分を引き続き通過していきます。メッセージがパイプラインの末尾に到達すると、メッセージに1つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

たとえば、コンテンツ フィルタはメッセージをドロップまたは返送する場合がありますが、その場合、メッセージは隔離されません。

（注） 電子メールゲートウェイにポリシー隔離が定義されていない場合、メッセージを隔離エリアに送ることはできません。

メッセージをポリシー隔離に送ることを選択すると、次の追加アクションを実行できます。

- メッセージの件名を変更します。
- メッセージへのカスタム ヘッダーの追加

メッセージの件名ヘッダーの変更

特定のテキスト文字列を前後に追加することで、ポリシー隔離に送られたメッセージを変更すると、ユーザは、識別されたメッセージを判別したり、ソートしたりすることが簡単にできるようになります。

（注） [メッセージの件名を修正（Modify message subject）] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、`[WARNING: UNSCANNABLE EXTRACTION FAILURE]` というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

ポリシー隔離に送られたメッセージの件名に追加される既定のテキスト。

理由	件名へのデフォルトのテキストの追加
抽出エラー	[WARNING: UNSCANNABLE EXTRACTION FAILED]
RFC 違反	[WARNING: UNSCANNABLE RFC NON-COMPLIANT]
URL フィルタリング アクション中に検出された復号エラー	[WARNING: DECODING ERRORS WHEN APPLYING URL FILTERING ACTIONS]

メッセージへのカスタム ヘッダーの追加

ポリシー隔離に送られたすべてのメッセージに追加する、追加のカスタムヘッダーを定義できます。[はい（Yes）] をクリックし、ヘッダー名およびテキストを定義します。

第 10 章

メール ポリシー

この章は、次の項で構成されています。

- メール ポリシーの概要 （309 ページ）
- メール ポリシーをユーザ単位で適用する方法 （310 ページ）
- 着信メッセージと発信メッセージの異なる処理 （311 ページ）
- メール ポリシーへのユーザの一致 （312 ページ）
- メッセージ分裂 （314 ページ）
- メール ポリシーの設定 （316 ページ）
- メッセージ ヘッダーの優先順位の設定 （322 ページ）

メール ポリシーの概要

電子メールゲートウェイはメールポリシーを使用して、組織とユーザとの間で送信されるメッセージについての組織のポリシーを適用します。これらは、組織が社内のネットワークに入ったり出たりして欲しくない、疑わしい、機密な、または悪意のあるコンテンツのタイプを指定する一連のルールです。このコンテンツは次のようなものがあります。

- スパム
- 問題のないマーケティング メッセージ
- グレーメール
- ウイルス
- フィッシングおよび他のメール攻撃のターゲット
- 機密企業データ
- 個人情報

組織内の異なるユーザ グループの個別のセキュリティ ニーズを満たすために複数のポリシーを作成できます。電子メールゲートウェイはこれらのポリシーに定義されているルールを使用して各メッセージをスキャンし、必要に応じて、ユーザを保護するアクションを実行します。たとえば、ポリシーは、スパムの疑いのあるメッセージが幹部に配信されないようにすると共に、そのコンテンツについて警告する件名に変更して IT スタッフへの配信を許可することができます。システム管理者グループ以外のすべてのユーザで、危険な実行可能プログラムの添付ファイルをドロップします。

メール ポリシーをユーザ単位で適用する方法

手順

	コマンドまたはアクション	目的
ステップ 1	電子メールゲートウェイが着信または発信メッセージに使用するコンテンツスキャン機能をイネーブルにします。	この機能で、次の1つ以上をイネーブル化し、設定できます。 • アンチウイルス （439 ページ） • ファイル レピュテーション フィルタリングとファイル分析 （585 ページ） （着信メッセージのみ） • スパムおよびグレイメールの管理 （461 ページ） • グレイメールの検出と安全な配信停止。「スパムおよびグレイメールの管理 （461 ページ）」を参照してください。 • アウトブレイク フィルタ （513 ページ） • データ損失の防止 （625 ページ） （発信メッセージのみ） • コンテンツ フィルタ （325 ページ）
ステップ 2	（任意）特定のデータを含むメッセージに対して実行するアクションの場合にコンテンツ フィルタを作成します。	コンテンツ フィルタ （325 ページ） を参照してください
ステップ 3	（任意）メール ポリシーのルールが適用されるユーザを指定する LDAP グループ クエリーを定義します。	受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （968 ページ） を参照してください。
ステップ 4	（任意）着信または発信メッセージのデフォルトのメール ポリシーを定義します。	着信または発信メッセージのデフォルトのメール ポリシーの設定 （316 ページ） を参照してください。
ステップ 5	ユーザ特定のメール ポリシーを設定するユーザ グループを定義します。	着信または発信メール ポリシーを作成します。 詳細については、メール ポリシーの設定 （316 ページ） を参照してください。
ステップ 6	コンテンツセキュリティ機能と電子メールゲートウェイがメッセージに対して実	メール ポリシーの異なるコンテンツのセキュリティ機能を設定します。

	コマンドまたはアクション	目的
	行するコンテンツ フィルタ アクションを設定します。	• コンテンツ フィルタ（Content Filters）：特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用 （351 ページ） • ウイルス対策（Anti-Virus）：ユーザのウイルス スキャン アクションの設定 （447 ページ） • ファイル レピュテーション フィルタリングおよびファイル分析：ファイル レピュテーション フィルタリングとファイル分析 （585ページ） • スパム対策（Anti-Spam）：スパム対策ポリシーの定義 （481ページ） • グレイメールの検出と安全な配信停止：グレイメールの検出と安全な配信停止の着信メール ポリシーの設定 （476 ページ） • アウトブレイク フィルタ（Outbreak Filters）：アウトブレイク フィルタ機能とアウトブレイク隔離 （536 ページ） • データ漏洩防止（DLP）：発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て （650 ページ）。

着信メッセージと発信メッセージの異なる処理

電子メールゲートウェイはメッセージコンテンツセキュリティに2つの異なるメールポリシーのセットを使用します。

- メッセージの着信メール ポリシーは、リスナーの ACCEPT HAT ポリシーに一致する接続から受信されるメッセージです。
- メッセージの発信メール ポリシーは、リスナーの RELAY HAT ポリシーに一致する接続からのメッセージです。この接続には、SMTP AUTH で認証された任意の接続が含まれます。

異なるポリシーのセットを持つことで、ユーザに送信またはユーザから送信されたメッセージに対し異なるセキュリティ ルールを定義することができます。これらのテーブルを管理するには、GUI の [メールポリシー（Mail Policies）]>[着信メールポリシー（Incoming Mail Policies）] ページまたは [発信メールポリシー（Outgoing Mail Policies）] ページ、あるいは CLI の policyconfig コマンドを使用します。

（注） 一部の機能は発信メール ポリシーのみ、または着信メール ポリシーのみに適用できます。データ消失防止スキャンは、発信メッセージに対してのみ実行できます。高度なマルウェア防御（ファイル レピュテーション スキャンおよびファイルの分析）は着信メール ポリシーおよび発信メール ポリシーで使用できます。

特定のインストールでは、Cisco アプライアンスを経由する「内部」メールは、すべての受信者が内部アドレスにアドレス指定されている場合でも、発信と見なされます。たとえばデフォルトでは、システム セットアップ ウィザードによって C170 および C190 アプライアンスに対して、着信電子メールの受信および発信電子メールのリレー用に、リスナー 1 つの物理イーサネット ポート 1 つのみが設定されます。

メール ポリシーへのユーザの一致

メッセージが電子メールゲートウェイによって受信されると同時に、電子メールゲートウェイは、メッセージが着信か発信かによって、各メッセージ受信者と送信者を着信または発信メールポリシーテーブルのメールポリシーに一致させようとします。

一致は受信者のアドレス、送信者のアドレス、または両方に基づきます。

- 受信者アドレスは、エンベロープ受信者アドレスとマッチングされます。

  受信者アドレスが一致すると、入力された受信者アドレスは、電子メール パイプラインの先行部分による処理後の最終アドレスです。たとえば、イネーブルの場合、デフォルト ドメイン、LDAP ルーティングまたはマスカレード、エイリアス テーブル、ドメイン マップ、メッセージ フィルタ機能はエンベロープ受信者アドレスを書き換えることができ、メッセージがメール ポリシーに一致するかどうかに影響することがあります。

- 送信者アドレスは、次のアドレスと照合されます。
  - エンベロープ送信者（RFC821 MAIL FROM アドレス）
  - RFC822 From: ヘッダーのアドレス
  - RFC822 Reply-To: ヘッダーのアドレス

アドレス マッチングは、完全な電子メール アドレス、ユーザー、ドメインまたは部分的なドメインのいずれか、あるいは LDAP グループ メンバーシップで行われます。

関連項目

- 最初に一致したものが有効 （312 ページ）
- ポリシー マッチングの例 （313 ページ）

最初に一致したものが有効

各ユーザは（送信者または受信者）トップダウン方式の適切なメール ポリシー テーブルで定義したメール ポリシーごとに評価されます。

ユーザごとに、最初に一致したポリシーが適用されます。ユーザが特定のポリシーと一致しない場合、ユーザは自動的にテーブルのデフォルト ポリシーと一致します。

送信者アドレスに基づいて一致する場合、メッセージの残りのすべての受信者がそのポリシーに一致します。（これは、メッセージごとに存在する送信者が 1 人だけのためです）。

エンベロープ送信者とエンベロープ受信者は、メッセージをメールポリシーに突き合わせるときに送信者ヘッダーよりも高いプライオリティを持ちます。メールポリシーを特定のユーザに合わせて構成すると、メッセージはエンベロープ送信者とエンベロープ受信者に基づいてメール ポリシーに自動的に分類されます。

ポリシー マッチングの例

次の例では、ポリシー テーブルがどのように上から順に照合されるかを説明します。

次の表に示す着信メールの電子メール セキュリティ ポリシーの表では、着信メッセージはさまざまなポリシーとマッチングされます。

表 *30*：ポリシー マッチングの例

順序	ポリシー名	ユーザー	
		送信者（Sender）	受信者（Recipient）
1	special_people	ANY	joe@example.com ann@example.com
2	from_lawyers	@lawfirm.com	ANY
3	acquired_domains	ANY	@newdomain.com @anotherexample.com
4	engineering	ANY	PublicLDAP.ldapgroup: engineers
5	sales_team	ANY	jim@john@larry@
6	デフォルト ポリシー	ANY	ANY

関連項目

- 例 1 （313 ページ）
- 例 2 （314 ページ）
- 例 3 （314 ページ）

例 1

送信者 bill@lawfirm.com から受信者 jim@example.com に送信されるメッセージは次に一致します。

- ポリシー#2、ユーザの説明が送信者（@lawfirm.com）と受信者（ANY）に一致する場合。
- ポリシー #2、エンベロープ送信者が bill@lawfirm.com である場合。
- ポリシー#5、ヘッダー送信者はbill@lawfirm.comだが、エンベロープ送信者が@lawfirm.comと一致しない場合。

例 2

送信者 joe@yahoo.com は、3 人の受信者、john@example.com、jane@newdomain.com および bill@example.com に着信メッセージを送信します。

- 受信者 jane@newdomain.com へのメッセージは、ポリシー #3 で定義されたスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。
- 受信者 john@example.com へのメッセージはポリシー #5 で定義されている設定を受信します。
- 受信者bill@example.comはエンジニアリングLDAPクエリーに一致しないため、メッセージはデフォルト ポリシーで定義された設定を受け取ります。

次の例では、受信者が複数あるメッセージでメッセージ分裂がどのように発生するかについて示します。 詳細については、メッセージ分裂 （314 ページ）を参照してください。

例 3

送信者 bill@lawfirm.com（bill@lawfirm.com はエンベロープ送信者に使用される）は、メッセージを受信者 ann@example.com および larry@example.com に送信します。

- 受信者 ann@example.com は、ポリシー#1 で定義されているスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。
- 受信者 larry@example.com は、ポリシー#2 で定義されているスパム対策、ウイルス対策、アウトブレイク フィルタおよびコンテンツ フィルタを受信します。これは、送信者（@lawfirm.com）と受信者（jim@）が一致するためです。

メッセージ分裂

インテリジェントなメッセージ分裂は、受信者に基づいたコンテンツの異なるセキュリティ ルールを複数の受信者に対するメッセージに個別に適用できるメカニズムです。

各受信者は、該当するメール ポリシー テーブル（着信または発信）の各ポリシーに対して上から順に評価されます。

メッセージに一致する各ポリシーは、これらの受信者に新しいメッセージを作成します。このプロセスが、「メッセージ分裂」と定義されます。

- 一部の受信者が異なるポリシーと一致する場合、受信者は一致したポリシーに基づいてグループ化され、メッセージは一致したポリシー数と同数のメッセージに分裂されます。これらの受信者は、それぞれ適切な「分裂先」に設定されます。

- すべての受信者が同じポリシーと一致する場合、メッセージは分裂されません。反対に、最も多くの分裂が行われるのは、単一のメッセージがメッセージ受信者1人1人に分裂される場合です。
- その後、各メッセージ分裂は、アンチスパム、アンチウイルス、高度なマルウェア防御（着信メッセージのみ）、DLP スキャン（発信メッセージのみ）、アウトブレイク フィルタおよびコンテンツ フィルタにより電子メール パイプラインで個別に処理されます。

次の表に、電子メール パイプラインでメッセージが分裂されるポイントを示します。

ワーク キュー	**メッセージ フィルタ** **（filters）**	電子メール セキュリティ マネージャ スキャン（受信者1人あたり）	**↓すべての受信者のメッセージ**
	スパム対策 **（antispamconfig、antispamupdate）**		メッセージは、メッセージフィルタ処理直後の、スパム対策処理前に分裂されます。 ポリシー 1 に一致するすべての受信者のメッセージ ポリシー 2 に一致するすべての受信者のメッセージ すべてのその他の受信者向けのメッセージ（デフォルトのポリシーに一致） （注） DLP スキャンは、発信メッセージだけに実行されます。
	ウイルス対策 **(antivirusconfig、antivirusupdate)**		
	ファイル レピュテーションとファイル分析（高度なマルウェア防御） **(ampconfig)**		
	グレイメール管理		
	コンテンツ フィルタ **（policyconfig -> filters）**		
	アウトブレイク フィルタ **（outbreakconfig、outbreakflush、outbreakstatus、outbreakupdate）**		
	データ損失の防止 **（policyconfig）**		

（注） 新しい MID（メッセージ ID）が、各メッセージ分裂用に作成されます（たとえば、MID 1 は、MID 2 および MID 3 になります）。詳細については、「ロギング」の章を参照してください。また、trace機能は、メッセージを分裂したポリシーを示します。

電子メールセキュリティマネージャポリシーのポリシーマッチングおよびメッセージ分裂は、電子メールゲートウェイで使用できるメッセージ処理の管理に影響を与えます。

関連項目

- 管理例外 （316 ページ）

管理例外

各分裂メッセージの反復処理はパフォーマンスに影響するため、シスコは管理例外単位で十分なコンテンツ セキュリティ ルールを設定することを推奨します。つまり、組織のニーズを評価し、大多数のメッセージがデフォルト ポリシーで処理され、少数のメッセージが、追加の「例外」ポリシーで処理されるように機能を設定します。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

メール ポリシーの設定

メール ポリシーはスパム対策やウイルス対策などの特定のセキュリティ設定に、異なるユーザ グループをマップします。

関連項目

- 着信または発信メッセージのデフォルトのメール ポリシーの設定 （316 ページ）
- 送信者および受信者のグループのメール ポリシーの作成 （317 ページ）
- 送信者または受信者に適用するポリシーの検索 （321 ページ）

着信または発信メッセージのデフォルトのメール ポリシーの設定

デフォルトのメール ポリシーは他のメール ポリシーに該当しないメッセージに適用されます。他のポリシーが設定されていない場合、デフォルト ポリシーはすべてのメッセージに適用されます。

はじめる前に

個々のセキュリティ サービスをメール ポリシーに定義する方法を理解します。メール ポリシーをユーザ単位で適用する方法 （310 ページ）を参照してください。

手順

ステップ 1 要件に応じて、次のいずれかを選択します。

- **[メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）]**
- **[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] を選択します。**

ステップ 2 デフォルトのメール ポリシーに設定するセキュリティ サービスのリンクをクリックします。

（注） デフォルトのセキュリティ サービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。[無効（Disable）] をクリックしてすべてのサービスをディセーブルにできます。

ステップ 3 セキュリティ サービスの設定値を設定します。

ステップ 4 **[送信（Submit）]** をクリックします。

ステップ 5 変更を送信し、保存します。

送信者および受信者のグループのメール ポリシーの作成

はじめる前に

- 個々のセキュリティ サービスをメール ポリシーに定義する方法を理解します。メール ポリシーをユーザ単位で適用する方法 （310 ページ）を参照してください。
- 各受信者は、適切なテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。詳細については、最初に一致したものが有効（312ページ）を参照してください。
- （任意）メール ポリシーの管理を担当する委任管理者を定義します。委任管理者は、ポリシーのアンチスパム、アンチウイルス、高度なマルウェア防御、アウトブレイク フィルタの設定を編集し、ポリシーのコンテンツ フィルタを有効化または無効化できます。オペレータおよび管理者のみがメール ポリシーの名前または送信者、受信者、またはグループを変更できます。メール ポリシーへのフル アクセス権があるカスタム ユーザー ロールはメール ポリシーに自動的に割り当てられます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] または [メール ポリシー（Mail Policies）] > [送信メール ポリシー（Outgoing Mail Policies）] を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 メール ポリシーの名前を入力します。

ステップ 4 （任意）[編集可能なユーザ(役割)（Editable by (Roles)）] のリンクをクリックし、メール ポリシーの管理を担当する委任管理者のカスタム ユーザ役割を選択します。

ステップ 5 ポリシーのユーザを定義します。ユーザを定義する手順については、メール ポリシーの送信者および受信者の定義 （318 ページ）を参照してください。

ステップ 6 **[送信（Submit）]** をクリックします。

ステップ 7 メールポリシーを設定するコンテンツ セキュリティ サービスのリンクをクリックします。

ステップ 8 ドロップダウン リストから、デフォルト設定を使用する代わりに、ポリシーの設定をカスタマイズするオプションを選択します。

ステップ 9 セキュリティ サービスの設定をカスタマイズします。

ステップ 10 変更を送信し、保存します。

次のタスク

関連項目

- メール ポリシーの送信者および受信者の定義 （318 ページ）
- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法 （462 ページ）

メール ポリシーの送信者および受信者の定義

次の方法で、ポリシーを適用する送信者と受信者を定義できます。

- 完全な電子メール アドレス：`user@example.com`
- 電子メール アドレスの一部：`user@`
- ドメインのすべてのユーザ：`@example.com`
- 部分ドメインのすべてのユーザ：`@.example.com`
- LDAP クエリーとのマッチング

（注） ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 `Joe@` を入力すると、`joe@example.com` に送信されるメッセージが一致します。

メール ポリシーの送信者と受信者を定義する際、次の点に注意してください。

- 少なくとも 1 人の送信者と受信者を指定する必要があります。
- 次の場合に一致するポリシーを設定できます。
  - メッセージが、任意の送信者、指定した 1 人以上の送信者からのものであるか、指定した送信者からのものでない場合。
  - メッセージが、任意の受信者、指定した 1 人以上の受信者、指定したすべての受信者に送信されるか、指定した受信者に送信されない場合。

手順

ステップ 1 [ユーザー（Users）] セクションで [ユーザーの追加（Add User）] をクリックします。

ステップ 2 ポリシーの送信者を定義します。次のいずれかのオプションを選択します。

- **任意の送信者（Any Sender）**。メッセージが任意の送信者からのものである場合、ポリシーと一致します。

- **次の送信者（Following Senders）**。メッセージが指定した 1 人以上の送信者からのものである場合、ポリシーと一致します。このオプションを選択して、テキストボックスに送信者の詳細を入力するか、LDAP グループ クエリーを選択します。
- **次の送信者は該当しません（Following Senders are Not）**。メッセージが指定した送信者からのものでない場合、ポリシーと一致します。このオプションを選択して、テキストボックスに送信者の詳細を入力するか、LDAP グループ クエリーを選択します。

上記のフィールドを選択する際にどのように送信者の条件が設定されるかを把握するには、例（319 ページ）を参照してください。

ステップ 3 ポリシーの受信者を定義します。次のいずれかのオプションを選択します。

- **任意の受信者（Any Recipient）**。メッセージが任意の受信者に送信される場合、ポリシーと一致します。
- **次の受信者（Following Recipients）**。メッセージが指定した受信者に送信される場合、ポリシーと一致します。このオプションを選択して、テキストボックスに受信者の詳細を入力するか、LDAP グループ クエリーを選択します。

メッセージが指定した 1 人以上の受信者または指定したすべての受信者に送信される場合、ポリシーが一致するかどうかを選択できます。ドロップダウン リストから [1つ以上の条件が一致した場合（If One or More Conditions Match）] または [すべての条件が一致した場合のみ（Only if all conditions match）] のいずれかのオプションを選択します。

- **次の受信者は該当しません（Following Recipients are Not）**。メッセージが指定した受信者に送信されない場合、ポリシーと一致します。このオプションを選択して、テキストボックスに受信者の詳細を入力するか、LDAP グループ クエリーを選択します。

（注） このオプションは、[次の受信者（Following Recipients）] を選択し、ドロップダウン リストから [すべての条件が一致した場合のみ（Only if all conditions match）] を選択した場合にのみ設定できます。

上記のフィールドを選択する際にどのように受信者の条件が設定されるかを把握するには、例（319 ページ）を参照してください。

ステップ 4 **[送信（Submit）]** をクリックします。

ステップ 5 [ユーザー（Users）] セクションで選択した条件を確認します。

次のタスク

関連項目

- 送信者および受信者のグループのメール ポリシーの作成 （317 ページ）
- 例 （319 ページ）

例

次の表で、[ユーザの追加（Add User）] ページでさまざまなオプションを選択する際に、どのように条件が設定されるかを示します。

送信者（Sender）			受信者（Recipient）			条件
任意の送信者	次の送信者	次の送信者は該当しません	任意の受信者	次の受信者	次の受信者は該当しません	
オン	-	-	-	オン （デフォルト）[すべての条件が一致した場合のみ（Only if all conditions match）] が選択されています。 値： user1@、 user2@	-	**送信者**：任意 **受信者**： user1@[AND]user2@
-	オン 値： u1@a.com、 u2@a.com	-	-	オン （デフォルト）[すべての条件が一致した場合のみ（Only if all conditions match）] が選択されています。 値： u1@b.com、 u2@b.com	オン 値： u3@b.com、 u4@b.com	**送信者**： u1@a.com[OR]u2@a.com **受信者**： [u1@b.com[AND]u2@b.com] [AND] [[NOT] [u3@b.com[AND]u4@b.com]]

-	-	オン 値： u1@a.com、 u2@a.com	-	オン [1つ以上の条件が一致した場合（If One or More Conditions Match）] オプションも選択されます 値： u1@b.com、 u2@b.com	-	**送信者：** [NOT] [u1@a.com[OR]u2@a.com] **受信者：** u1@b.com [OR] u2@b.com

関連項目

- メール ポリシーの送信者および受信者の定義 （318 ページ）

送信者または受信者に適用するポリシーの検索

すでに着信または発信メール ポリシーに定義されているユーザを検索するには、[メールポリシー（Mail Policies）] ページの上部にある [ポリシー検索（Find Policies）] セクションを使用します。

たとえば、bob@example.com と入力して、[ポリシー検索（Find Policies）] ボタンをクリックすると、ポリシーに一致する定義済みのユーザが含まれるポリシーが表示されます。

そのポリシーのユーザを編集するには、ポリシーの名前をクリックします。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

関連項目

- 管理例外 （316 ページ）

管理例外

前述の2つの例で示されている手順を使用して、管理例外に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルト ポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザ グループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。次の表に、いくつかのポリシーの例の概要を示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達するスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、偽陽性を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 *31* : 積極的および保守的な電子メール セキュリティ マネージャ設定

	積極的な設定	保守的な設定
スパム対策	陽性と判定されたスパム：ドロップ 陽性と疑わしいスパム：隔離 マーケティング メール：メッセージの件名の前に「[Marketing]」が追加されて配信	陽性と判定されたスパム：隔離 陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信 マーケティング メール：ディセーブル
アンチウイルス	修復されたメッセージ：配信 暗号化されたメッセージ：ドロップ スキャンできないメッセージ：ドロップ 感染メッセージ：ドロップ	修復されたメッセージ：配信 暗号化されたメッセージ：隔離 スキャンできないメッセージ：隔離 感染メッセージ：ドロップ
Advanced Malware Protection **（ファイル レピュテーション フィルタリングおよびファイル分析）**	スキャンされていない添付ファイル：ドロップ マルウェア ファイルが添付されたメッセージ：ドロップ 保留中のファイル分析のあるメッセージ：隔離	スキャンされていない添付ファイル：メッセージの件名の前に「[WARNING: ATTACHMENT UNSCANNED]」が追加されて配信。 マルウェア ファイルが添付されたメッセージ：ドロップ 保留中のファイル分析のあるメッセージ：メッセージの件名の前に「[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]」が追加されて配信。
ウイルス フィルタ	イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし すべてのメッセージのメッセージ変更の有効化	バイパスできるファイル名拡張子またはドメインの有効化 未署名のメッセージのメッセージ変更の有効化

メッセージ ヘッダーの優先順位の設定

メッセージヘッダーの優先順位を設定して、電子メールゲートウェイの受信メッセージと送信メッセージを一致させることができます。

重要 電子メールゲートウェイが受信メッセージと送信メッセージのメッセージヘッダーをチェックする際の優先順位を設定できます。最初に、電子メールゲートウェイはすべてのメールポリシーで優先順位の最も高いメッセージヘッダーをチェックします。いずれのメールポリシーとも一致するヘッダーがない場合、電子メールゲートウェイはすべてのメールポリシーの優先順位リスト内の次のメッセージヘッダーを検索します。いずれのメールポリシーとも一致するメッセージヘッダーがない場合は、デフォルトのメールポリシー設定が使用されます。

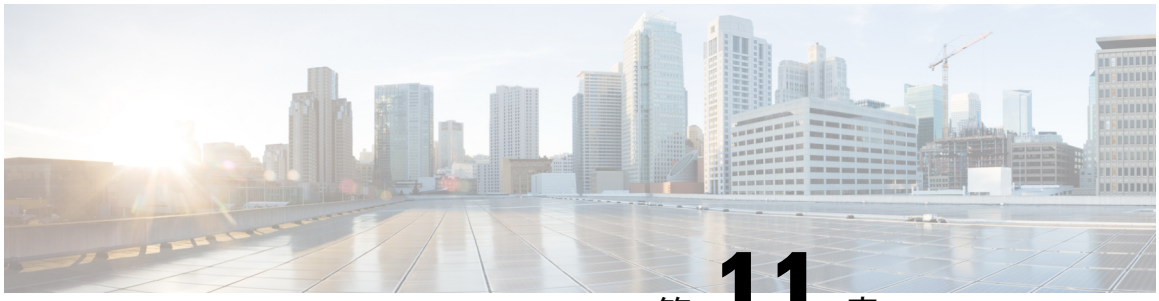
手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールポリシー設定（Mail Policy Settings）] に移動します。

デフォルトでは、[エンベロープ送信者（Envelope Sender）] ヘッダーは優先度 1 に設定されています。[エンベロープ送信者（Envelope Sender）] リンクをクリックして優先度を変更できます。

ステップ 2 [優先順位の追加（Add Priority）] をクリックし、適切なヘッダー名（たとえば、ヘッダー「送信元（From）」）のチェックボックスをオンにして、新しい優先順位を追加します。

ステップ 3 [送信（Submit）] をクリックし、変更をコミットします。



第 11 章

コンテンツ フィルタ

この章は、次の項で構成されています。

- コンテンツ フィルタの概要 （325 ページ）
- コンテンツ フィルタの仕組み （325 ページ）
- コンテンツ フィルタの条件 （327 ページ）
- コンテンツ フィルタのアクション （338 ページ）
- コンテンツに基づくメッセージのフィルタリング方法 （349 ページ）

コンテンツ フィルタの概要

コンテンツ フィルタを使用して、アンチウイルス スキャンやDLP などのコンテンツ セキュリティ機能によって処理される標準ルーチン以上に、メッセージの処理をカスタマイズします。たとえばコンテンツ フィルタは、後で調査するためにコンテンツを隔離する必要がある場合や、企業のポリシーで特定メッセージを配信する前に暗号化する必要がある場合に使用できます。

コンテンツ フィルタの仕組み

コンテンツ フィルタは、電子メール パイプラインで後ほど適用される点、つまり、メッセージ フィルタリングの後で、1 つのメッセージが、各メール ポリシーに対応する個々の複数のメッセージに「分裂」された後で（詳細はメッセージ分裂（314ページ）を参照）、およびメッセージがアンチスパムおよびアンチウイルス スキャンされた後で適用される点を除いては、メッセージ フィルタとほぼ同じです。

コンテンツフィルタは、着信または発信メッセージをスキャンします。両方のメッセージをスキャンするフィルタを定義することはできません。電子メールゲートウェイには、各メッセージタイプのコンテンツフィルタに個別の「プライマリリスト」が用意されています。また、プライマリリストは、アプライアンスがコンテンツフィルタを実行する順序も決定します。ただし個々のメールポリシーは、メッセージがポリシーに一致するときに、実行される特定のフィルタを決定します。

コンテンツ フィルタは、ユーザー（送信者または受信者）単位でメッセージをスキャンします。

コンテンツ フィルタには次のコンポーネントがあります。

- どのような場合に電子メールゲートウェイがコンテンツフィルタを使用してメッセージをスキャンするかを決定する条件（任意）
- 電子メールゲートウェイがメッセージに実行するアクション（必須）
- メッセージを変更した場合に、電子メールゲートウェイがメッセージに追加できるアクション変数（任意）

関連項目

- コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法 （326 ページ）
- コンテンツ フィルタの条件 （327 ページ）
- コンテンツ フィルタのアクション （338 ページ）
- アクション変数 （346 ページ）

コンテンツ フィルタを使用したメッセージ コンテンツのスキャン方法

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）コンテンツ フィルタがサポートする機能を定義します。	コンテンツ フィルタで使用する次の項目を作成します。 • 暗号化プロファイル • 免責事項テンプレート • 通知テンプレート • Policy 隔離 • URL 許可リスト
ステップ 2	着信または発信コンテンツ フィルタを定義します。	コンテンツ フィルタは以下で構成されることもあります。 • コンテンツ フィルタの条件 （327 ページ） （任意） • コンテンツ フィルタのアクション （338 ページ） • アクション変数 （346ページ） （任意） コンテンツ フィルタの作成 （349 ページ）

	コマンドまたはアクション	目的
ステップ 3	コンテンツ セキュリティ ルールを設定するユーザ グループを定義します。	着信または発信メール ポリシーを作成します。
ステップ 4	フィルタを使用する着信または発信メッセージのユーザのグループにコンテンツ フィルタを割り当てます。	メール ポリシー（309ページ）を参照してください

コンテンツ フィルタの条件

条件は、電子メールゲートウェイが関連するメールポリシーに一致するメッセージにフィルタを使用するかどうかを決定する「トリガー」です。コンテンツ フィルタの条件の指定はオプションです。条件のないコンテンツ フィルタは関連するメール ポリシーに一致するすべてのメッセージに適用されます。

コンテンツ フィルタの条件では、メッセージ本文または添付ファイルで特定のパターンを検索するフィルタ ルールを追加する場合、パターンが検出される回数の最小しきい値を指定できます。AsyncOS はメッセージをスキャンすると、メッセージおよび添付ファイルに見つかった一致の数の「スコア」を集計します。最小しきい値に満たない場合、正規表現は true と評価されません。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。

各フィルタには、複数の条件を定義できます。複数の条件が定義されている場合、条件を論理 OR（「次の任意の条件...」）または論理 AND（「次のすべての条件」）のいずれで結合するかを選択できます。

表 *32*：コンテンツ フィルタの条件

条件	説明
（条件なし）	コンテンツ フィルタでの条件の指定はオプションです。条件が指定されていない場合、true ルールが適用されます。true ルールはすべてのメッセージに一致し、必ずアクションが実行されます。

条件	説明
メッセージ本文または添付ファイル	[テキストを含む（Contains text）]：メッセージ本文に、特定のパターンと一致するテキストまたは添付ファイルが含まれているかどうかを判別します。 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文または添付ファイルのコンテンツが、スマート ID と一致するかどうかを判別します。 • クレジット カード番号 • 米国社会保障番号 • Committee on Uniform Security Identification Procedures（CUSIP）番号 • American Banking Association（ABA; 米国銀行協会）ルーティング番号 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文または添付ファイルのコンテンツが、プレフィックス（「credit」、「ssn」、「cusip」、または「aba」）を含むスマート識別子と一致するかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains term in content dictionary）]：メッセージ本文に、<*dictionary name*> という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID、またはコンテンツ ディクショナリの用語に対して指定できます。 これには、配信ステータス部および関連付けられている添付ファイルが含まれます。

条件	説明
メッセージ本文	[テキストを含む（Contains text）]：メッセージ本文に、特定のパターンと一致するテキストが含まれているかどうかを判別します。 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文のコンテンツが、スマート ID と一致するかどうかを判別します。スマート ID は、次のパターンを検出できます。 • クレジット カード番号 • 米国社会保障番号 • Committee on Uniform Security Identification Procedures（CUSIP）番号 • American Banking Association（ABA; 米国銀行協会）ルーティング番号 [スマート識別子を含む（Contains smart identifier）]：メッセージ本文のコンテンツが、プレフィックス（「credit」、「ssn」、「cusip」、または「aba」）を含むスマート識別子と一致するかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains term in content dictionary）]：メッセージ本文に、<*dictionary name*> という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキストまたはスマート ID に対して指定できます。 このルールは、メッセージの本文だけに適用されます。添付ファイルまたはヘッダーは含まれません。
URL カテゴリ（URL Category）	URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール （554 ページ）およびURL カテゴリについて （568 ページ）を参照してください。
メッセージ サイズ	本文サイズが、指定範囲内にあるかどうかを判別します。本文サイズとはメッセージのサイズのことで、ヘッダーと添付ファイルも含みます。本文サイズ ルールは、本文サイズが指定数と比較されるメッセージを選択します。

条件	説明
マクロ検出	受信または送信メッセージにマクロが有効な添付ファイルが含まれているか。 マクロ検出の条件を使用すると、選択したファイル タイプのメッセージのマクロが有効な添付ファイルを検出できます。
添付ファイルの内容	**[テキストを含む（Contains text）]**：指定したパターンと一致するテキストまたは別の添付ファイルが、メッセージの添付ファイルに含まれているか。このルールは body-contains() ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。 **[スマート識別子を含む（Contains a smart identifier）]**：メッセージ添付ファイルの内容が、指定されたスマート ID と一致するかどうかを判別します。 [スマート識別子を含む（Contains smart identifier）]：メッセージの添付ファイルのコンテンツが、プレフィックス（「credit」、「ssn」、「cusip」、または「aba」）を含むスマート識別子と一致するかどうかを判別します。 **[コンテンツ辞書の単語を含む（Contains terms in content dictionary）]**：添付ファイルに、<*dictionary name*> という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。

条件	説明
添付ファイルのファイル情報	

条件	説明
	[ファイル名（Filename）]：メッセージに、ファイル名が特定のパターンと一致する添付ファイルがあるかどうかを判別します。 **[コンテンツ辞書の単語を含むファイル名（Filename contains term in content dictionary）]**：メッセージに、<ディクショナリ名> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれるファイル名の添付ファイルがあるかどうかを判別します。 このオプションをイネーブルにするには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。 [ファイルタイプ（File type）]：メッセージに、フィンガープリントに基づいて特定のパターンと一致するファイル タイプの添付ファイルがあるかどうかを判別します（UNIX file コマンドと似ています）。 [MIMEタイプ（MIME type）]：メッセージに、特定の MIME タイプの添付ファイルがあるかどうかを判別します。このルールは attachment-type ルールに似ていますが、MIME 添付ファイルで指定された MIME タイプのみが評価される点が異なります。（電子メールゲートウェイは、ファイルタイプが明示的に指定されていない場合、拡張子からファイルのタイプを「予測」することはありません。） [ファイルハッシュリスト（File Hash List）]：メッセージに、特定のファイルの SHA-256 値と一致する添付ファイルがあるかどうかを判別します。ドロップダウンリストから必要なファイルハッシュリストを選択します。 （注） SHA-256 ファイルハッシュタイプを含むファイルハッシュリストのみ選択できます。 **[イメージ分析（Image Analysis）]**：メッセージに、指定されているイメージ判定と一致するイメージ添付ファイルがあるかどうかを判別します。有効なイメージ分析判定には、[疑わしい（Suspect）]、[不適切（Inappropriate）]、[不適切もしくは疑わしい（Suspect or Inappropriate）]、[スキャン不可（Unscannable）] または [正常（Clean）] があります。 [外部脅威フィード（External Threat Feeds）]：ファイルは選択した外部脅威フィードソースからの脅威情報と 一致していますか? [ファイルハッシュ例外リストの選択（Select a File Hash Exception List）]：（オプション） 電子メールゲートウェイで脅威を検出しない許可リスト登録済みファイルハッシュのリストを選択します。

条件	説明
	詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定 （355 ページ）を参照してください。 **添付ファイルが破損しています（Attachment is Corrupt）**：破損した添付ファイルがメッセージに含まれているかどうか。 （注） 破損した添付ファイルとは、スキャンエンジンがスキャンできないため破損として識別する添付ファイルのことです。
添付ファイル保護	**[パスワードで保護されたまたは暗号化された添付ファイルが添付されている（Contains an attachment that is password-protected or encrypted）]**： （この条件は、たとえば、スキャンできない可能性がある添付ファイルを識別する場合に使用します）。 **[パスワードで保護されたまたは暗号化された添付ファイルが添付されていない（Contains an attachment that is NOT password-protected or encrypted）]**：
件名ヘッダー（Subject Header）	[件名ヘッダー（Subject Header）]：件名ヘッダーに、特定のパターンが含まれているかどうかを判別します。 [コンテンツ辞書の単語を含む（Contains terms in content dictionary）]：件名ヘッダーに、<ディクショナリ名>という名前のコンテンツディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。

条件	説明
その他のヘッダー	[ヘッダー名（Header name）]：メッセージに、特定のヘッダーが含まれているかどうかを判別します。 [ヘッダーの値（Header value）]：ヘッダーの値が、特定のパターンと一致するかどうかを判別します。 **[ヘッダーの値がコンテント辞書内の単語を含みます（Header value contains terms in the content dictionary）]**：指定されたヘッダーに、<ディクショナリ名> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。 このオプションを使用する方法を説明する例については、カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）を参照してください。
エンベロープ送信者（Envelope Sender）	**[エンベロープ送信者（Envelope Sender）]**：エンベロープ送信者（Envelope From, <MAIL FROM>）が指定したパターンと一致しているか。 [LDAPグループに一致（Matches LDAP group）]：エンベロープ送信者（つまり、Envelope From、<MAIL FROM>）が、特定の LDAP グループに含まれるかどうかを判別します。 **[コンテンツ辞書の単語を含む（Contains term in content dictionary）]**：エンベロープ送信者に、<ディクショナリ名> という名前のコンテンツ ディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。

条件	説明
エンベロープ受信者	[エンベロープ受信者（Envelope Recipient）]：エンベロープ受信者（Envelope To, <RCPT TO>）が指定したパターンと一致しているか。 [LDAPグループに一致（Matches LDAP group）]：エンベロープ受信者（Envelope To, <RCPT TO>）が、指定した LDAP グループ内に存在するか。 **[コンテンツ辞書の単語を含む（Contains term in content dictionary）]**：エンベロープ受信者に、<ディクショナリ名>という名前のコンテンツディクショナリのいずれかの正規表現または用語が含まれているかどうかを判別します。 ディクショナリ用語を検索するには、ディクショナリがすでに作成されている必要があります。コンテンツ ディクショナリ （791 ページ）を参照してください。 （注） ディクショナリに関連する条件は、1 つ以上のディクショナリがイネーブルにされている場合だけ使用できます。コンテンツ ディクショナリの作成の詳細については、コンテンツ ディクショナリ （791 ページ）を参照してください。 [エンベロープ受信者（Envelope Recipient）] ルールは、メッセージ単位です。メッセージに複数の受信者がある場合、グループの受信者が 1 人でも検出されれば、指定されたアクションがメッセージのすべての受信者に適用されます。 エンベロープ送信者（Envelope From <MAIL FROM>）が、指定した LDAP グループ内に存在するか。
受信リスナー（Receiving Listener）	メッセージは、指定されたリスナー経由で届いたか。リスナー名は、システムで現在設定されているリスナーの名前である必要があります。
リモートIP（Remote IP）	リモートホストから送信されたメッセージは、指定したIPアドレスまたはIPブロックに一致しているか。[リモートIP（Remote IP）] ルールは、メッセージを送信したホストのIPアドレスが特定のパターンと一致するかどうかをテストします。これは、インターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）アドレスを指定できます。IP アドレスパターンは、「送信者グループの構文 （110 ページ）」で説明されているように、許可されたホスト表記を使用して指定します。ただし、SBO、IPR、dnslist表記および特殊キーワードALLを除きます
レピュテーション スコア	送信者のIPレピュテーションスコアはいくつか。レピュテーションスコア ルールにより、IP レピュテーションスコアが別の値と比較してチェックされます。

条件	説明
DKIM 認証	DKIM 認証に合格したか、部分的に検証されたか、一時的に検証不可能として返されたか、失敗したか、DKIM 結果が返されていないかどうかを判別します。
偽装メールの検出	メッセージの送信元アドレスが偽装されているか。メッセージの From: ヘッダーがコンテンツ辞書のユーザに類似している場合にチェックするルールです。 コンテンツ ディクショナリを選択し、偽装の可能性ありとみなされるメッセージに、しきい値（1 ～ 100）を入力します。 偽装電子メール検出の条件は、From: ヘッダーとコンテンツディクショナリのユーザを比較します。このプロセス中に、類似により、 電子メールゲートウェイはディクショナリ内の各ユーザに類似性スコアを割り当てます。次に例を示します。 • From: ヘッダーが <j0hn.sim0ns@example.com> で、コンテンツディクショナリにユーザ「John Simons」が含まれている場合、 電子メールゲートウェイによってこのユーザに 82 の類似性スコアが割り当てられます。 • From: ヘッダーが <john.simons@diff-example.com> で、コンテンツディクショナリにユーザ「John Simons」が含まれている場合は、このユーザに 100 の類似性スコアが割り当てられます。 類似性スコアが高くなればなるほど、メッセージが偽装されている確立が高くなります。類似性スコアが指定したしきい値以上の場合は、フィルタ アクションがトリガーされます。 特定の送信者からのメッセージの偽装メールの検出フィルタをスキップする場合、[例外リスト（Exception List）] ドロップダウン リストからアドレス リストを選択します。 （注） 完全な電子メール アドレスを使用して作成したアドレス リストのみを選択できます。詳細については、着信接続ルールへの送信者アドレス リストの使用 （134 ページ）を参照してください。 詳細については、偽装メールの検出 （787 ページ）を参照してください。
SPF 検証	SPF 検証ステータスを判別します。このフィルタ ルールでは、さまざまな SPF 検証結果をクエリーできます。SPF 検証の詳細については、「電子メール認証」の章を参照してください。 （注） SPF ID を含まずに SPF 検証コンテンツ フィルタ条件を設定した場合、また異なる判定を含む異なる SPF ID がメッセージに含まれている場合は、メッセージ内のいずれかの判定と一致した条件がトリガーされます。

条件	説明
S/MIME ゲートウェイ メッセージ（S/MIME Gateway Message）	メッセージは S/MIME 署名されているか、暗号化されているか、または署名および暗号化されているか。詳細については、S/MIME セキュリティ サービス （681 ページ）を参照してください。
S/MIME ゲートウェイ 検証済	S/MIME メッセージは正常に検証されているか、復号されているか、または復号および検証されているか。詳細については、S/MIME セキュリティ サービス （681 ページ）を参照してください。
メッセージ言語	メッセージ（件名と本文）は選択したいずれかの言語であるか。この条件では、添付ファイルおよびヘッダーの言語は確認しません。 **言語の検出の動作の仕組み** 電子メールゲートウェイは、メッセージの言語を検出するのに組み込みの言語検出エンジンを使用します。電子メールゲートウェイは、件名とメッセージ本文を抽出し、言語検出エンジンに渡します。 言語検出エンジンは、抽出されたテキスト内の各言語の確率を決定し、それを電子メールゲートウェイに渡します。電子メールゲートウェイは、最も高い確率をもつ言語をメッセージの言語とみなします。 電子メールゲートウェイは、次のシナリオのいずれかで、メッセージの言語を「判別不能」とみなします。 • 検出された言語が 電子メールゲートウェイでサポートされていない場合 • 電子メールゲートウェイがメッセージの言語を検出できない場合 • 言語検出エンジンに送られた抽出されたテキストの合計サイズが 50 バイト未満の場合。
重複境界検証	そのメッセージに、重複する MIME 境界が含まれるか。 重複する MIME 境界が含まれるメッセージにアクションを実行する場合は、この条件を使用します。 （注） 添付ファイルベースの条件（たとえば、添付ファイルの内容）や操作（たとえば、コンテンツによる添付ファイルの除去）は、（重複する MIME 境界を含む）不正なメッセージでは動作しません。
位置情報	メッセージが選択した国で作成されたものかどうかを判別します。 位置情報条件を使用すると、選択した特定の国からの着信メッセージを処理できます。 （注） 位置情報コンテンツフィルタを使用する前に、 電子メールゲートウェイでスパム対策エンジンを有効にします。

条件	説明
ドメインのレピュテーション	送信者ドメインは、指定された基準と一致していますか? • 送信者ドメインのレピュテーション • 外部脅威フィード 詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定 （355 ページ）または送信者ドメイン レピュテーション フィルタリング （381 ページ）を参照してください。

コンテンツ フィルタのアクション

アクションは、電子メールゲートウェイがコンテンツフィルタの条件に一致するメッセージに行うことです。メッセージの変更、隔離またはドロップなどさまざまなタイプのアクションが用意されています。メッセージで配信またはドロップといった「最終アクション」が実行されることで、E メール セキュリティ アプライアンスで強制的にアクションが即時実行され、アウトブレイク フィルタまたは DLP スキャンなどのその後のすべての処理が実施されません。

各コンテンツ フィルタには、少なくとも 1 つのアクションを定義する必要があります。

アクションは、順序に従いメッセージで実行されるため、コンテンツ フィルタの複数のアクションを定義する場合、アクションの順序を考慮します。

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示すると、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。詳細については、「テキスト リソース」の章を参照してください。

フィルタごとに定義できる最終アクションは1つだけです。最終アクションは、リストの最後のアクションです。バウンス、配信、およびドロップは、最終アクションです。コンテンツフィルタのアクションを入力する場合、GUIおよびCLIにより、最終アクションが強制的に最後に配置されます。

アクション変数 （346 ページ）も参照してください。

表 *33*：コンテンツ フィルタのアクション

アクション	説明
検疫（Quarantine）	[隔離（Quarantine）]。いずれかの Policy 隔離エリアに保持されるメッセージにフラグを付けます。 [重複するメッセージ（Duplicate message）]：メッセージのコピーを指定された隔離エリアに送信して、オリジナル メッセージの処理を続行します。任意の追加アクションが、オリジナル メッセージに適用されます。
配信時の暗号化	メッセージは、次の処理段階に進みます。すべての処理が完了すると、メッセージが暗号化され、配信されます。 [暗号化ルール（Encryption rule）]：メッセージを常に暗号化するか、TLS接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、TLS 接続を暗号化の代わりに使用 （672 ページ）を参照してください。 **[暗号化プロファイル（Encryption Profile）]**：処理が完了したら、指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco 暗号化アプライアンスまたはホステッド キー サービスと併用します。 **[件名（Subject）]**：暗号化されたメッセージの件名です。デフォルト値は **`$Subject`** です。
内容によって添付ファイルを除去	**[次を含む添付ファイル（Attachment contains）]**：正規表現を含むメッセージのすべての添付ファイルをドロップします。アーカイブ ファイル（zip、tar）は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。 **[スマート識別子を含む（Contains smart identifier）]**：指定されたスマート ID を含むメッセージのすべての添付ファイルをドロップします。 **[コンテンツ辞書の単語を含む添付ファイル（Attachment contains terms in the content dictionary）]**：添付ファイルに、*<dictionary name>* という名前のコンテンツ辞書のいずれかの正規表現または用語が含まれているかどうかを判別します。 [要求された一致数（Number of matches required）]：true と評価するためにルールで必要な一致数を指定します。このしきい値は、テキスト、スマート ID またはコンテンツ ディクショナリの一致回数に対して指定できます。 **[メッセージ差し替え（Replacement message）]**：オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。

アクション	説明
ファイル情報によって添付ファイルを除去	

アクション	説明
	[ファイル名（File name）]：指定された正規表現とファイル名が一致するメッセージのすべての添付ファイルをドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。 [ファイルサイズ（File size）]：メッセージの添付ファイルのうち、ロー エンコード形式で指定したサイズ（バイト単位）以上のサイズであるファイルをすべてドロップします。アーカイブ ファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の自体のサイズが計測されます。 [ファイルタイプ（File type）]：メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。 [MIMEタイプ（MIME type）]：メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。 [ファイルハッシュリスト（File Hash List）]：選択したファイルハッシュリスト内のファイルの SHA-256 値と一致するメッセージにあるすべての添付ファイルをドロップします。ドロップダウンリストから必要なファイルハッシュリストを選択します。 （注） SHA-256 ファイルハッシュタイプを含むファイルハッシュリストのみ選択できます。 [イメージ分析判定（Image Analysis Verdict）]：指定されたイメージ判定と一致するイメージ添付ファイルをドロップします。有効なイメージ分析判定には、[疑わしい（Suspect）]、[不適切（Inappropriate）]、[不適切もしくは疑わしい（Suspect or Inappropriate）]、[スキャン不可（Unscannable）] または [正常（Clean）] があります。 **外部脅威フィード**。ETF エンジンによって悪意のあるファイルとして分類されたメッセージのすべてのメッセージ添付ファイルをドロップします。 **ファイル ハッシュ例外リストを選択します。**（任意）Cisco E メール セキュリティ ゲートウェイで脅威を検出しない許可リスト登録済みファイルハッシュのリストを選択します。 詳細については、外部脅威フィードを使用する電子メールゲートウェイの設定 （355 ページ）を参照してください。 **[メッセージ差し替え（Replacement message）]**：オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追

アクション	説明
	加されるだけです。
マクロが含まれる添付ファイルを削除	指定したファイル タイプのマクロが有効になった添付ファイルをすべてドロップします。 （注） アーカイブまたは埋め込みファイルにマクロが含まれている場合、親ファイルはメッセージからドロップされます。 [カスタム差し替えメッセージ（Custom Replacement Message）]（任意）：添付ファイルが削除されるとき、デフォルトでは、システム生成のメッセージがメッセージ本文の一番下に追加されます。 以下は、マクロが有効な添付ファイルがメッセージから削除されるときにシステムによって生成されるメッセージのサンプルです。 **A MIME attachment of type <application/vnd.ms-excel> was removed here by a drop-macro-enabled-attachments filter rule on the host <mail.example.com>.** [カスタム差し替えメッセージ（Custom Replacement Message）] フィールドにカスタム メッセージを入力すると、システム生成のメッセージは入力されたメッセージに差し替えられます。
URLレピュテーション（URL Reputation）	メッセージに含まれるURLの変更：フィルタでのURLレピュテーションまたはURLカテゴリのアクションの使用 （555ページ）およびURL フィルタリングの許可リストの作成 （550ページ）を参照してください。 レピュテーションを判断できないURLには、「スコアなし」を使用してアクションを指定します。 （注） S/MIMEを使用して暗号化されている場合またはS/MIME署名が含まれる場合、電子メールゲートウェイはメッセージを署名済みとみなします。
URL カテゴリ（URL Category）	メッセージに含まれるURLの変更：フィルタでのURLレピュテーションまたはURLカテゴリのアクションの使用 （555ページ）およびURL カテゴリについて （568ページ）を参照してください。 （注） S/MIMEを使用して暗号化されている場合またはS/MIME署名が含まれる場合、電子メールゲートウェイはメッセージを署名済みとみなします。

アクション	説明
免責条項文の追加	[上に配置（Above）]：メッセージ上部に免責事項を追加します（ヘッダー）。 **[下に配置（Below）]**：メッセージ下部に免責事項を追加します（フッター）。 **注**：このコンテンツ フィルタ アクションを使用するには、免責事項テキストをすでに作成している必要があります。 詳細については、免責事項テンプレート（806 ページ）を参照してください。
アウトブレイク フィルタによるスキャンのバイパス	メッセージに対してアウトブレイク フィルタによるスキャンをスキップします。
DKIM 署名のバイパス	メッセージに対して DKIM 署名をバイパスします。
コピー（Bcc:）を送信	[電子メールアドレス（Email addresses）]：指定受信者にメッセージを匿名でコピーします。 **[件名（Subject）]**：コピーされたメッセージの件名を追加します。 **[リターンパス（オプション）（Return path (optional)）]**：リターン パスを指定します。 **[代替メールホスト（オプション）（Alternate mail host (optional)）]**：代替メール ホストを指定します。
通知	**[通知（Notify）]**：指定された受信者にこのメッセージを報告します。オプションで送信者および受信者に通知できます。 **[件名（Subject）]**：コピーされたメッセージの件名を追加します。 **[リターンパス（オプション）（Return path (optional)）]**：リターン パスを指定します。 [テンプレート利用（Use template）]：作成したテンプレートからテンプレートを選択します。 [オリジナル メッセージを添付ファイルとして含めます（Include original message as an attachment）]：オリジナル メッセージを添付ファイルとして追加します。
受信者を変更	**電子メール アドレス**メッセージの受信者を指定電子メール アドレスに変更します。

アクション	説明
代替送信ホストにメッセージを送信	[メールホスト（Mail host）]：メッセージの宛先メール ホストを指定メール ホストに変更します。 （注） このアクションは、アンチスパム スキャン エンジンによりスパムとして分類されたメッセージが隔離されないようにします。このアクションは、隔離を無効にして、指定メール ホストに送信します。
IP インターフェイスから送信	**[次の IP インターフェイスから送信（Send from IP interface）]**：指定 IP インターフェイスから送信します。[IP インターフェイスから送信（Deliver from IP Interface）] アクションは、メッセージのソース ホストを指定ソースに変更します。ソース ホストは、メッセージが配信される IP インターフェイスで構成されます。
ヘッダーの除去	**[ヘッダー名（Header name）]**：指定ヘッダーを配信前にメッセージから削除します。
ヘッダーの追加/編集	**メッセージに新しいヘッダーを挿入または既存のヘッダーを変更します。** [ヘッダー名（Header name）]：新規または既存のヘッダーの名前。 **[新しいヘッダーの値を指定（Specify value of new header）]**：新しいヘッダーの値を配信前にメッセージに挿入します。 **[既存のヘッダーの値の前に付加（Prepend to the Value of Existing Header）]**：配信前に既存のヘッダーの前に値を追加します。 **[既存のヘッダーの値の後ろに付加（Append to the Value of Existing Heade）]**：配信前に既存のヘッダーの後ろに値を追加します。 [既存のヘッダーの値から検索して置換（Search & Replace from the Value of Existing Header）]：[検索対象（Search for）] フィールドに、既存のヘッダーで置き換える値を見つけるための検索語を入力します。ヘッダーに挿入する値を [次で置換（Replace with）] フィールドに入力します。値を検索するために正規表現を使用できます。ヘッダーから値を削除する場合は、[次で置換（Replace with）] フィールドを空白のままにしてください。
偽装メールの検出	偽装されたメッセージから From: ヘッダーを削除し、エンベロープ送信者で置き換えます。 偽装メールの検出 （787 ページ）を参照してください。

アクション	説明
メッセージ タグの追加	DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに挿入します。DLP ポリシーを設定して、スキャン対象をメッセージタグがあるメッセージに限定することができます。メッセージタグは受信者側では表示されません。DLPポリシーでのメッセージ タグの使用については、データ損失防止のポリシー （629 ページ）を参照してください。
ログ エントリの追加	カスタマイズされたテキストを INFO レベルで IronPort テキスト メール ログに挿入します。このテキストにはアクション変数を使用することができます。ログ エントリはメッセージ トラッキングにも表示されます。
配信時の S/MIME 署名/暗号化	配信時にメッセージの S/MIME 署名または暗号化を実行します。メッセージは次の処理段階に進み、すべての処理が完了した時点で署名または暗号化されて、配信されます。 **S/MIME 送信プロファイル**：指定された S/MIME 送信プロファイルを使用して、S/MIME 署名または暗号化を実行します。S/MIME 送信プロファイルの管理 （693 ページ）を参照してください。
暗号化して今すぐ配信（最終アクション）	メッセージを暗号化および配信し、その後の任意の処理をスキップします。 [暗号化ルール（Encryption rule）]：メッセージを常に暗号化するか、TLS接続を介した送信試行が最初に失敗した場合だけ暗号化します。詳細については、TLS 接続を暗号化の代わりに使用 （672 ページ）を参照してください。 **[暗号化プロファイル（Encryption Profile）]**：指定された暗号化プロファイルを使用してメッセージを暗号化し、メッセージを配信します。このアクションは、Cisco 暗号化アプライアンスまたはホステッド キー サービスと併用します。 **[件名（Subject）]**：暗号化されたメッセージの件名です。デフォルト値は **`$Subject`** です。
S/MIME 署名/暗号化（最終アクション）	S/MIME 署名または暗号化を実行してメッセージを配信し、その後の処理はスキップします。 **S/MIME 送信プロファイル**：指定された S/MIME 送信プロファイルを使用して、S/MIME 署名または暗号化を実行します。S/MIME 送信プロファイルの管理 （693 ページ）を参照してください。
バウンスする（最終アクション）	メッセージを送信者に戻します。

アクション	説明
残りのコンテンツ フィルタをスキップ（最終アクション）	メッセージを次の処理段階に配信し、その後の任意のコンテンツ フィルタをスキップします。設定に応じて、メッセージが受信者に配信されるか、隔離が実行されるか、アウトブレイク フィルタによるスキャンが開始されます。
ドロップする（最終アクション）	メッセージをドロップして廃棄します。
Safe Print	「Safe Print」コンテンツ フィルタ アクションを使用して、メッセージの添付ファイルを Safe Print で出力します。 Safe Print コンテンツ フィルタ アクションは、次のいずれかの方法で使用できます。 • 一致する添付ファイルをSafe Printで出力（Safe print matching attachments）：このオプションを使用すると、設定されたコンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力します。 • すべての添付ファイルをSafe Printで出力（Safe print all attachments）：このオプションを使用すると、設定されたコンテンツ フィルタ条件が true の場合にすべてのメッセージの添付ファイルを Safe Print で出力します。 [はい（Yes）] を選択して、スキャン不可とマークされているメッセージの添付ファイルを削除します。 （注） デフォルトでは、添付ファイルがスキャンできない場合、システム生成のメッセージが添付テキスト ファイルとして追加されます。[カスタム差し替えメッセージ（Custom Replacement Message）] フィールドにカスタム メッセージを入力します。 詳細については、メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定方法（414 ページ）を参照してください。

関連項目

- アクション変数 （346 ページ）

アクション変数

コンテンツ フィルタにより処理されるメッセージに追加されるヘッダーには、アクション実行時にオリジナル メッセージの情報に自動的に置換される変数を含めることができます。これら

の特殊な変数はアクション変数と呼ばれます。電子メールゲートウェイでは次のアクション変数がサポートされています。

表 *34* : アクション変数

変数	構文	説明
すべてのヘッダー（All Headers）	`$AllHeaders`	メッセージ ヘッダーに置き換えられます。
本文サイズ（Body Size）	`$BodySize`	メッセージのサイズ（バイト単位）に置き換えられます。
日付（Date）	`$Date`	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
ドロップされたファイル名（Dropped File Name）	`$dropped_filename`	直近にドロップされたファイル名のみを返します。
ドロップされたファイル名（Dropped File Names）	`$dropped_filenames`	$filenames と同様に、ドロップされたファイルのリストを表示します。
ドロップされたファイルタイプ（Dropped File Types）	`$dropped_filetypes`	$filetypes と同様に、ドロップされたファイルタイプのリストを表示します。
エンベロープ送信者（Envelope Sender）	`$envelopefrom` or `$envelopesender`	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
エンベロープ受信者（Envelope Recipients）	`$EnvelopeRecipients`	メッセージのエンベロープ受信者すべて（Envelope To、<RCPT TO>）に置き換えられます。
ファイル名（File Names）	`$filenames`	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
ファイルサイズ（File Sizes）	`$filesizes`	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。
ファイルタイプ（File Types）	`$filetypes`	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
フィルタ名（Filter Name）	`$FilterName`	処理されるフィルタの名前に置き換えられます。
GMT 日時（GMTimeStamp）	`$GMTimeStamp`	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

変数	構文	説明
HATグループ名（HAT Group Name）	`$Group`	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
メールフローポリシー（Mail Flow Policy）	`$Policy`	メッセージのインジェクト時に、送信者に適用したHATポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
一致した内容（Matched Content）	`$MatchedContent`	コンテンツスキャンフィルタをトリガーした1つ以上の値に置き換えられます。一致した内容は、コンテンツディクショナリマッチ、スマートIDまたは正規表現との一致になります。
ヘッダー（Header）	`$Header['`*string*`']`	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
ホストネーム	`$Hostname`	電子メールゲートウェイのホスト名に置き換えられます。
内部メッセージID（Internal Message ID）	`$MID`	メッセージを内部で識別するために使用するメッセージID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには$Headerを使用します）。
受信リスナー（Receiving Listener）	`$RecvListener`	メッセージを受信したリスナーのニックネームに置き換えられます。
受信インターフェイス（Receiving Interface）	`$RecvInt`	メッセージを受信したインターフェイスのニックネームに置き換えられます。
リモートIPアドレス（Remote IP Address）	`$RemoteIP`	メッセージを電子メールゲートウェイに送信したシステムのIPアドレスに置き換えられます。
リモートホストアドレス（Remote Host Address）	`$remotehost`	メッセージを電子メールゲートウェイに送信したシステムのホスト名に置き換えられます。

変数	構文	説明
SenderBase レピュテーション スコア	`$Reputation`	送信者の SenderBase レピュテーション スコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
Subject	`$Subject`	メッセージの件名に置き換えられます。
時刻	`$Time`	現在の時刻（ローカル時間帯）に置き換えられます。
Timestamp	`$Timestamp`	現在の時刻および日付（ローカル時間帯）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

コンテンツに基づくメッセージのフィルタリング方法

関連項目

- コンテンツ フィルタの作成 （349 ページ）
- デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化 （351 ページ）
- 特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用 （351 ページ）
- GUI でのコンテンツ フィルタの設定に関する注意事項 （352 ページ）

コンテンツ フィルタの作成

はじめる前に

- コンテンツ フィルタに一致するメッセージを暗号化する場合は、暗号化プロファイルを作成します。
- 一致メッセージに免責事項を追加する場合は、免責事項の生成に使用する免責事項テンプレートを作成します。
- 一致するメッセージについてユーザに通知メッセージを送信する場合は、通知を生成するための通知テンプレートを作成します。
- メッセージを隔離する場合は、これらのメッセージに対する新しい Policy 隔離を作成するか、または既存のものを使用します。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] をクリックします。

または

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] をクリックします。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 フィルタの名前と説明を入力します。

ステップ 4 （相互参照）[編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックして、ポリシーの管理者を選択し、[OK] をクリックします。

ポリシー管理者ユーザ ロールに属する委任管理者はこのコンテンツ フィルタを編集し、自身のメール ポリシーで使用できます。

ステップ 5 （任意）フィルタをトリガーするための条件を追加します。

a) [条件を追加（Add Condition）] をクリックします。
b) 条件のタイプを選択します。
c) 条件のルールを定義します。
d) [OK] をクリックします。
e) フィルタに追加する追加条件について、上記の手順を繰り返して行ってください。コンテンツ フィルタに複数の条件を定義する場合、コンテンツ フィルタが一致したと見なされるために、定義されるアクションのすべて（論理 AND）、または定義されたいずれかのアクション（論理 OR）の適用が必要かどうかを定義できます。

（注） 条件を追加しない場合、電子メールゲートウェイはフィルタに関連するメールポリシーの 1 つと一致するあらゆるメッセージにコンテンツフィルタのアクションを実行します。

ステップ 6 フィルタの条件に一致するメッセージに対して実行する電子メールゲートウェイのアクションを追加します。

a) [アクションを追加（Add Action）] をクリックします。
b) アクション タイプを選択します。
c) アクションを定義します。
d) [OK] をクリックします。
e) 電子メールゲートウェイに実行する追加のアクションについて、上記の手順を繰り返して行ってください。
f) 複数のアクションに対して、電子メールゲートウェイがメッセージに適用する順序でアクションを配置します。フィルタごとに 1 個だけ「最終」アクションがあり、AsyncOS は自動的に最終アクションを順番の最後に移動します。

ステップ 7 変更を送信し、保存します。

次のタスク

- デフォルトの着信または発信メール ポリシーでコンテンツ フィルタをイネーブルにできます。
- 特定のユーザ グループのメールポリシーのコンテンツフィルタをイネーブルにできます。

デフォルトでのすべての受信者のコンテンツフィルタのイネーブル化

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] をクリックします。

または

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] をクリックします。

ステップ 2 デフォルト ポリシー行のコンテンツ フィルタ セキュリティ サービスのリンクをクリックします

ステップ 3 コンテンツ フィルタ セキュリティ サービス ページで、[コンテンツフィルタリング：デフォルトポリシー（Content Filtering for Default Policy）] の値を [コンテンツフィルタを無効にする（Disable Content Filters）] から [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更します。

プライマリリストで定義されているコンテンツ フィルタ（コンテンツ フィルタの概要 （325 ページ）で作成されたフィルタ）が、このページに表示されます。値を [コンテンツ フィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更すると、各フィルタのチェックボックスがイネーブルになります。

ステップ 4 イネーブルにする個々のコンテンツ フィルタの [有効（Enable）] チェックボックスをオンにします。

ステップ 5 変更を送信し、保存します。

特定のユーザ グループに対するメッセージへのコンテンツ フィルタの適用

はじめる前に

- ユーザー グループのメッセージに対してコンテンツ フィルタを使用する場合、着信または発信メールポリシーを作成します。詳細については、送信者および受信者のグループのメール ポリシーの作成 （317 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] をクリックします。

または

[メールポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] をクリックします。

ステップ 2 コンテンツ フィルタに適用するメール ポリシーのコンテンツ フィルタ セキュリティ サービス（[コンテンツ フィルタ（Content Filters）] 列）のリンクをクリックします。

ステップ 3 コンテンツ フィルタ セキュリティ サービス ページで、[ポリシーのコンテンツフィルタリング: エンジニアリング（Content Filtering for Policy: Engineering）] の値を [コンテンツフィルタを有効にする（デフォルトのメールポリシー設定を継承）（Enable Content Filtering (Inherit default policy settings)）] から [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更します。

ステップ 4 ユーザが使用するコンテンツ フィルタのチェックボックスを選択します。

ステップ 5 変更を送信し、保存します。

GUI でのコンテンツ フィルタの設定に関する注意事項

- コンテンツ フィルタを作成するときに条件を指定する必要はありません。アクションが定義されていない場合、定義されるアクションは常にルールに適用されます（条件を指定しないことは、true() メッセージフィルタ ルールを使用すること同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます）。
- カスタム ユーザー ロールをコンテンツ フィルタに割り当てていない場合、パブリックのコンテンツ フィルタになり、メール ポリシーの任意の委任管理者が使用できます。委任管理者とコンテンツ フィルタの詳細については、「Common Administrative Tasks」の章を参照してください。
- 管理者とオペレータは、コンテンツフィルタがカスタムユーザロールに割り当てられている場合でも、電子メールゲートウェイのすべてのコンテンツフィルタを表示および編集できます。
- フィルタ ルールおよびアクションのテキストを入力する場合、正規表現照合において、次のメタ文字に特殊な意味があります。^ $ * + ? { [ ] \ | ( )

  正規表現を使用しない場合、「\」（バックスラッシュ）を使用して、これらの任意の文字をエスケープする必要があります。たとえば、「*Warning*」と入力します。

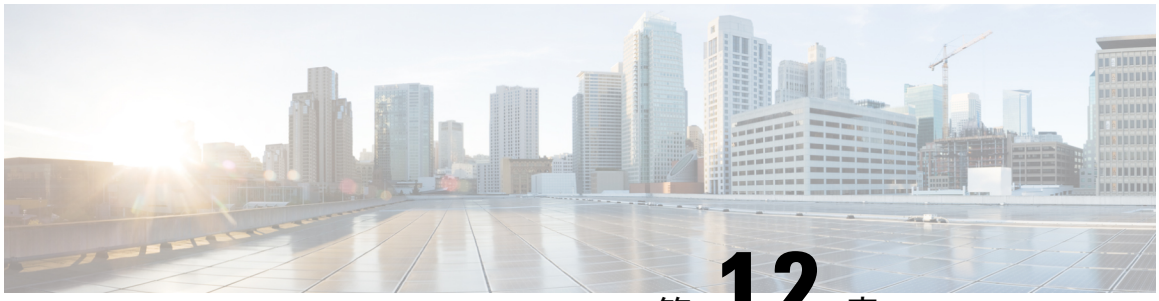
- 「benign」コンテンツ フィルタを作成して、メッセージ分裂およびコンテンツ フィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツ フィルタを作成できます。このコンテンツ フィルタは、メール処理に影響を与えませんが、このフィルタを使用して、電子メール セキュリティ マネージャ ポリシー処理が、システムの他の要素（たとえば、メール ログ）に影響を与えているかテストできます。
- 逆に、着信コンテンツまたは発信コンテンツフィルタの「プライマリリスト」の概念を使用して、電子メールゲートウェイにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツフィルタを作成できます。このコンテンツ フィルタは次のように作成できます。

  - [受信コンテンツフィルタ（Incoming Content Filters）] または [送信コンテンツフィルタ（Outgoing Content filters）] ページを使用して、順序が 1 の新しいコンテンツ フィルタを作成します。
  - [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページを使用して、デフォルト ポリシーの新しいコンテンツ フィルタをイネーブルにします。
  - 残りすべてのポリシーでこのコンテンツ フィルタをイネーブルにします。

- コンテンツ フィルタで使用できる [Bcc:] および [隔離（Quarantine）] アクションは、作成する隔離エリアの保持設定に役に立ちます（詳細については、ポリシー、ウイルス、およびアウトブレイク隔離（1129ページ）を参照してください）。メッセージがすぐにはシステムからリリースされないようにするため（つまり、隔離エリアの割り当てディスク領域がすぐにいっぱいにならないようにするため）、ポリシー隔離とのメールフローをシミュレートするフィルタを作成できます。
- **scanconfig** コマンドと同じ設定が使用されるため、「Entire Message」条件は、メッセージのヘッダーをスキャンしません。「Entire Message」を選択すると、メッセージ本文および添付ファイルだけがスキャンされます。特定のヘッダー情報を検索するには、「Subject」または「Header」条件を使用します。
- LDAP クエリによるユーザの設定は、電子メールゲートウェイで LDAP サーバが設定されている場合（つまり、**ldapconfig** コマンドを使用して特定の文字列を含む特定の LDAP サーバをクエリするようにアプライアンスが設定されている場合）だけ GUI に表示されます。
- リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、GUI に表示されません。たとえば、通知テンプレートおよびメッセージ免責事項は、[テキストリソース（Text Resources）] ページまたは CLI の **textconfig** コマンドを使用して事前に設定されていない場合、オプションとして表示されません。
- コンテンツフィルタ機能は、次の文字エンコーディングのテキストを認識し、これらを追加およびスキャンできます。
  - Unicode（UTF-8）
  - Unicode（UTF-16）
  - Western European/Latin-1（ISO 8859-1）
  - Western European/Latin-1（Windows CP1252）
  - 中国語（繁体字）（Big 5）
  - 中国語（簡体字）（GB 2312）
  - 中国語（簡体字）（HZ GB 2312）
  - 韓国語（ISO 2022-KR）
  - 韓国語（KS-C-5601/EUC-KR）
  - 日本語（Shift-JIS（X0123））
  - 日本語（ISO-2022-JP）
  - 日本語（EUC）

複数の文字セットを1つのコンテンツ フィルタ内で組み合わせてマッチングできます。複数の文字エンコーディングでのテキストの表示および入力については、Webブラウザのマニュアルを参照してください。ほとんどのブラウザでは、複数の文字セットを同時にレンダリングできます。

- 着信または発信コンテンツ フィルタの要約ページで、[説明（Description）]、[ルール（Rules）] および [ポリシー（Policies）] のリンクを使用して、コンテンツ フィルタに提供されているビューを変更します。
  - [説明（Description）] ビューには、各コンテンツ フィルタの説明フィールドに入力したテキストが表示されます（これはデフォルト ビューです）。
  - [ルール（Rules）] ビューには、ルール ビルダ ページにより構築されたルールおよび正規表現が表示されます。
  - [ポリシー（Policies）] ビューには、イネーブルにされている各コンテンツ フィルタのポリシーが表示されます。



第 12 章

外部脅威フィードを使用する電子メールゲートウェイの設定

この章は、次の項で構成されています。

- 外部脅威フィードの概要 （355 ページ）
- 外部脅威フィードを使用する電子メールゲートウェイの設定方法 （356 ページ）
- 外部脅威フィード機能キーの取得 （358 ページ）
- 電子メールゲートウェイでの外部脅威フィードエンジンの有効化 （359 ページ）
- 外部脅威フィード ソースの設定 （360 ページ）
- SecureX Threat Response フィードソースの設定 （364 ページ）
- 脅威が含まれているメッセージの処理 （369 ページ）
- 脅威が含まれているメッセージの処理に向けた送信者グループの設定 （369 ページ）
- 脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージフィルタの設定 （370 ページ）
- 受信メール ポリシーへのコンテンツ フィルタのアタッチ （378 ページ）
- 外部脅威フィードおよびクラスタ （379 ページ）
- 外部脅威フィード エンジンの更新のモニタリング （379 ページ）
- アラートの表示 （379 ページ）
- メッセージ トラッキングの脅威詳細の表示 （380 ページ）

外部脅威フィードの概要

外部の脅威フィード（ETF）フレームワークによって、電子メールゲートウェイは次の外部脅威情報を使用できます。

- TAXII プロトコルで通信される STIX 形式。
- Cisco SecureX Threat Response ポータルからの JavaScript Object Notation（JSON）形式。

電子メールゲートウェイで外部脅威情報を使用する機能によって、組織は以下が可能です。

- マルウェア、ランサムウェア、フィッシング攻撃、標的型攻撃などのサイバー脅威にプロアクティブに対応する。
- ローカルおよびサードパーティの脅威インテリジェンス ソースに登録する。
- 電子メールゲートウェイの有効性を向上する。

電子メールゲートウェイで ETF 機能を使用するには、有効な機能キーが必要です。機能キーの入手方法の詳細は、シスコの販売担当者にお問い合わせください。

STIX（構造化された脅威情報表現）は、サイバー脅威情報を表す業界標準の構造化言語です。STIX ソースは、悪意のある、または疑わしいサイバー アクティビティを検出するために使用されるパターンを含むインジケータで構成されています。

TAXII（検知指標情報自動交換手順）は、異なる組織または製品ラインにかけて、サービス（TAXII サーバ）によってサイバー脅威情報を交換するための一連の仕様を定義します。

本リリースでは、STIX 1.1.1 および 1.2 と TAXII 1.1 の STIX/TAXII バージョンがサポートされています。

Cisco SecureX Threat Response ポータルでは、監視対象を継続的に収集するためのカスタムフィードを作成し、フィード URL を使用して電子メールゲートウェイでそれらを利用できます。フィードは、JSON 形式の監視対象の単純なリストです。フィードは、SecureX Threat Response ポータルの [インテリジェンス（Intelligence）] > [フィード（Feeds）] ページで作成および管理されます。

以下は、本リリースでサポートされる STIX および SecureX Threat Response のセキュリティ侵害の指標（IOC）のリストです。

- ファイル ハッシュ ウォッチリスト（疑わしい、悪意のあるファイルの一連のハッシュを説明）
- IP ウォッチリスト（疑わしい、悪意のある一連の IP アドレスを説明）
- ドメイン ウォッチリスト（疑わしい、悪意のある一連のドメインを説明）
- URL ウォッチリスト（疑わしい、悪意のある一連の URL を説明）

外部脅威フィードを使用する電子メールゲートウェイの設定方法

次の手順を順番に実行します。

手順	操作手順	詳細情報
ステップ 1	外部脅威フィード機能キーを取得します。	外部脅威フィード機能キーの取得 （358 ページ）

手順	操作手順	詳細情報
ステップ 2	電子メールゲートウェイで ETF エンジンを有効化します。	電子メールゲートウェイでの外部脅威フィードエンジンの有効化 （359 ページ）
ステップ 3	ETF ソースを設定して、電子メールゲートウェイが TAXII サーバから STIX 形式で脅威フィードを取得することを許可します。	外部脅威フィード ソースの設定 （360 ページ）
（ SecureX Threat Response フィードの設定にのみ適用可能）ステップ 4	（SecureX Threat Response ポータル上）：フィード URL を作成します。 （注） フィード URL を作成する場合は、フィード URL の出力を [監視対象（Observables）] のみとして選択していることを確認します。	フィード URL の作成方法の詳細については、次の SecureX Threat Response ヘルプページを参照してください。 • https://visibility.amp.cisco.com/help/create-feed-url（米国のユーザに適用） • https://visibility.eu.amp.cisco.com/help/create-feed-url（欧州連合（EU）のユーザに適用） • https://visibility.apjc.amp.cisco.com/help/create-feed-url（APJC のユーザに適用）
（SecureX Threat Response フィードの設定にのみ適用可能）ステップ 5	（SecureX Threat Response ポータル上）：システムで、ステップ 4 で作成したフィード URL の詳細を表示してコピーします。 （注） フィード URL の詳細は、SecureX Threat Response フィード ソースの作成に使用されます。	ステップ 4 で作成したフィード URL の詳細を表示する方法の詳細については、次の SecureX Threat Response ヘルプページを参照してください。 • https://visibility.amp.cisco.com/help/intelligence-view-feeds（米国のユーザに適用） • https://visibility.eu.amp.cisco.com/help/intelligence-view-feeds（欧州連合（EU）のユーザに適用） • https://visibility.apjc.amp.cisco.com/help/intelligence-view-feeds（APJC のユーザに適用）

手順	操作手順	詳細情報
（SecureX Threat Response フィードの設定にのみ適用可能）ステップ 6	SecureX Threat Response フィードソースを設定して、電子メールゲートウェイが SecureX Threat Response フィードを SecureX Threat Response ポータルから取得できるようにします。	SecureX Threat Response フィードソースの設定 （364 ページ）
ステップ 7	以下を使用して、脅威を含むメッセージを処理します。 • HAT • コンテンツ フィルタまたはメッセージ フィルタ	脅威が含まれているメッセージの処理 （369 ページ）
ステップ 8	メッセージの悪意のあるドメイン、URL、ファイル ハッシュを検出するように設定したコンテンツ フィルタを受信メール ポリシーにアタッチします。	受信メール ポリシーへのコンテンツ フィルタのアタッチ （378 ページ）

外部脅威フィード機能キーの取得

クラシックライセンスモードを使用した電子メールゲートウェイの管理

クラシックライセンシングモードを使用していて、外部脅威フィードの機能キーをお持ちでない場合は、以下の手順でシスコの Global Licensing Operations（GLO）チームに連絡して機能キーを取得してください。

手順

ステップ 1 件名を「外部脅威フィード機能キーのリクエスト」にして、GLO チーム（licensing@cisco.com）に電子メールを送信します。

ステップ 2 電子メールには製品認証キー（PAK）ファイルと発注書（PO）の詳細を入力します。

GLO チームが機能キーを手動でプロビジョニングし、電子メールゲートウェイにインストール可能なライセンスキーを電子メールで送信します。

次のタスク

（注）
- ハードウェアモデルまたは仮想電子メールゲートウェイモデルのユーザで、シスコ サーバから機能キーやソフトウェアライセンスを直接取得できる場合、外部脅威フィード機能キーは自動的に提供されます。
- 仮想電子メールゲートウェイモデルのユーザで、シスコ サーバから機能キーやライセンスを直接取得できない場合は、次の手順に従って外部脅威フィード機能キーを取得します。
  1. LRP ユーザアカウントのログイン情報を使用して、ライセンス登録ポータル（LRP）にログインします。
  2. [ライセンスの取得（Get License）] を選択します。
  3. [移行（Migration）] を選択します。
  4. [セキュリティ製品（Security Products）] を選択します。
  5. [Eメールセキュリティ（ESA）（Email Security (ESA)）] を選択します。
  6. VLN 番号を入力し、ライセンスファイルを生成します。

     生成されたライセンスファイルには、ETF機能が含まれています。ETF機能を使用するには、電子メールゲートウェイに新しいライセンスファイルをインストールする必要があります。

     （注） LRP アカウントにログインできない場合は、GLO チーム（licensing@cisco.com）に連絡してライセンスファイルを生成してください。

スマート ソフトウェア ライセンス モードを使用した電子メールゲートウェイの管理

電子メールゲートウェイでスマートライセンスモードをすでに使用している場合、または新規ユーザの場合、自動的に外部脅威フィード機能キーが提供されます。

電子メールゲートウェイでの外部脅威フィードエンジンの有効化

始める前に

電子メールゲートウェイで ETF 機能を使用するための、有効な機能キーがあることを確認します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [外部脅威フィード（External Threat Feeds）] をクリックします。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

（注） ライセンス契約に合意しない場合、Cisco E メール セキュリティ ゲートウェイで ETF が有効になりません。

ステップ 4 [外部脅威フィードの有効化] をチェックします。

ステップ 5 （任意）[はい（Yes）] を選択して、ETF エンジンのルックアップの失敗のために ETF エンジンによって脅威をスキャンされなかったすべてのメッセージにカスタム ヘッダーを追加します。

ステップ 6 変更を送信し、保存します。

次のタスク

ETF ソースを設定します。外部脅威フィード ソースの設定 （360 ページ） を参照してください。

外部脅威フィード ソースの設定

TAXII サーバで利用可能な脅威のコレクションについての情報をダウンロードするために、ETF ソースが使用されます。ETF ソースを設定して、電子メールゲートウェイが TAXII サーバから STIX 形式で脅威フィードを取得することを許可する必要があります。

（注） 電子メールゲートウェイでは、最大 8 個の ETF ソースを設定できます。

ETF ソースは、「ポーリングパス」と「コレクション名」で構成されるポーリング サービスを使用して設定できます。

始める前に

- 電子メールゲートウェイで ETF エンジンを有効化していることを確認します。
- ゲートウェイが外部脅威フィードを使用することを許可するために、ファイアウォールで HTTP（80）と HTTPS（443）のポートが開いていることを確認します。詳細については、ファイアウォール情報 （1607 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] をクリックします。

ステップ 2 [ソースに追加（Add to Source）] をクリックします。

ステップ 3 以下の表に記載される必須パラメータを入力して、ETF ソースを設定します。

パラメータ ソースの詳細	説明
ソース名（Source Name）	ETF ソースの名前を入力します。
説明（Description）	ETF ソースの説明を入力します。
TAXII の詳細（TAXII Details）	
ホスト名（Hostname）	完全修飾ドメイン名のホスト名または TAXII サーバの IP アドレスを入力します。
ポーリングパス（Polling Path）	TAXII サーバのポーリング サービスを特定するポーリング パスを入力します（例：/taxii-data）。
コレクション名（Collection Name）	TAXII サーバでホストされる脅威フィードのコレクション名を入力します（例：guest.Abuse_ch）。
ポーリング間隔（Polling Interval）	TAXII サーバから脅威フィードを取得する頻度を定義するポーリング間隔を入力します。最小値は 15 分で、デフォルト値は 60 分です。
脅威フィードの期間経過（Age of Threat Feeds）	TAXII サーバから取得できる脅威フィードの最大経過時間を入力します。経過時間の値は、365 日以内にする必要があります。

パラメータ ソースの詳細	説明
ポーリング セグメントの期間（Time Span for Poll Segment）	各ポーリングセグメントの期間を入力します。 ポーリングセグメントの最小期間は1日です。ポーリングセグメントの最大期間は、[脅威フィードの経過時間（Age of Threat Feeds）] フィールドに入力した値です。 以下のシナリオでは、[ポーリングセグメントの期間（Time Span for Poll Segment）] オプションを使用できます。 • TAXII サーバに脅威フィードの経過時間の既知の制限が存在しない場合、[脅威フィードの経過時間（Age of Threat Feeds）] オプションに入力した値を使用します。 • TAXII サーバに脅威フィードの経過時間の既知の制限が存在する場合、既知の制限値を使用します。 • TAXII サーバに脅威フィードの経過時間の既知の制限が不明な場合は、デフォルト値の 30 日を使用します。 • [脅威フィードの経過時間（Age of Threat Feeds）] オプションに入力した値が TAXII サーバにサポートされていない場合、脅威フィードの経過時間を入力した期間に基づく異なるポーリング セグメントに分割できます。 たとえば、脅威フィードの経過時間が 100 日間で、 TAXII サーバに脅威フィードの経過時間の固定の制限（「40 日」など）が設定されている場合、ポーリング セグメントの期間として 40 を入力します。 （注） ポーリングセグメントの期間が小さい値 （「5 日」など）の場合、脅威フィードソースのポーリングが完了するまでに長い時間がかかる場合があります。これにより、ゲートウェイのパフォーマンスに影響が出る可能性があります。

パラメータ ソースの詳細	説明
HTTPS の使用（Use HTTPS）	HTTPS を使用して TAXII サーバに接続する場合は [はい（Yes）] を選択します。
クレデンシャルの設定（Configure Credentials）	TAXII サーバで作成したユーザ クレデンシャルを使用して TAXII サーバにアクセスする場合は [はい（Yes）] を選択します。 ユーザ名とパスワードを入力します。
プロキシの詳細	
グローバル プロキシの使用（Use Global Proxy）	電子メールゲートウェイがプロキシサーバを介して TAXII サーバに接続されるようにするには **[はい（Yes）]** を選択します。 次のいずれかの方法でプロキシ サーバを設定できます。 • Web インターフェイスの [セキュリティ サービス（Security Services）]>[サービス アップデート（Service Updates）] ページ • CLI の *updateconfig* コマンド **[いいえ（No）]** を選択すると、電子メールゲートウェイは直接 TAXII サーバに接続されます。

ステップ 4 変更を送信し、保存します。

ETF ソースを設定した後、電子メールゲートウェイは TAXII ソースからの脅威フィードの取得を開始します。

次のタスク

- CLI で **threatfeedsconfig > sourceconfig** サブコマンドを使用して ETF ソースを設定することもできます。
- （任意）[メールポリシー（Mail Policies）]>[外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで**ポーリングの一時停止**（ ）アイコンをクリックして、設定した ETF ソースのポーリング サービスを一時停止します。
- （任意）[メールポリシー（Mail Policies）]>[外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで**ポーリングの再開**（ ）アイコンをクリックして、ETF ソースのポーリング サービスを再開します。

- （任意）（任意）[メールポリシー（Mail Policies）]>[外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで [今すぐポーリング（Poll Now）] をクリックして、最後に成功したポーリング間隔ですぐに脅威フィードを取得します。
- 脅威が含まれているメッセージの処理 （369 ページ） を参照してください。

SecureX Threat Response フィードソースの設定

SecureX Threat Response フィードソースは、SecureX Threat Response ポータルで利用可能な脅威のコレクションに関する情報をダウンロードするために使用されます。電子メールゲートウェイが SecureX Threat Response ポータルから脅威フィードを取得できるように、SecureX Threat Response フィードソースを設定する必要があります。

（注） 電子メールゲートウェイには、最大 8 つの SecureX Threat Response フィードソースを設定できます。

始める前に

次の前提条件を満たしていることを確認してください。

- 電子メールゲートウェイで ETF エンジンがイネーブルである。
- ゲートウェイが SecureX Threat Response フィードを使用できるように、ファイアウォールで HTTP（80）と HTTPS（443）のポートが開かれている。詳細については、ファイアウォール情報 （1607 ページ）を参照してください。
- 管理者アクセス権を使用して、Cisco SecureX でユーザアカウントが作成されている。新しいユーザアカウントを作成するには、URL（https://securex.us.security.cisco.com/login）を使用して **Cisco SecureX のログイン**ページに移動し、ログインページで [SecureXサインオンアカウントの作成（Create a SecureX Sign-on Account）] をクリックします。新しいユーザアカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。
- SecureX Threat Response ポータルでフィード URL が作成されている。詳細については、次の SecureX Threat Response ヘルプページを参照してください。
  - https://visibility.amp.cisco.com/help/create-feed-url（米国のユーザに適用）
  - https://visibility.eu.amp.cisco.com/help/create-feed-url（欧州連合（EU）のユーザに適用）
  - https://visibility.apjc.amp.cisco.com/help/create-feed-url（APJC のユーザに適用）
- システムで、SecureX Threat Response ポータルで作成されたフィード URL の詳細が表示およびコピーされている。詳細については、次の SecureX Threat Response ヘルプページを参照してください。
  - https://visibility.amp.cisco.com/help/intelligence-view-feeds（米国のユーザに適用）

- https://visibility.eu.amp.cisco.com/help/intelligence-view-feeds（欧州連合（EU）のユーザに適用）
- https://visibility.apjc.amp.cisco.com/help/intelligence-view-feeds（APJC のユーザに適用）

手順

ステップ 1 [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] をクリックします。

ステップ 2 [ソースに追加（Add to Source）] をクリックします。

ステップ 3 以下の表に記載される必須パラメータを入力して、SecureX Threat Response フィードソースを設定します。

パラメータ ソースの詳細	説明
ソース名（Source Name）	SecureX Threat Response フィードソースの名前を入力します。
説明（Description）	SecureX Threat Response フィードソースの説明を入力します。

パラメータ ソースの詳細	説明
TAXII の詳細（TAXII Details） SecureX Threat Response フィードソースは、一般的な TAXII フィードソースとは異なります。ただし、SecureX Threat Response サーバからの監視対象のポーリングをイネーブルにするには、SecureX Threat Response フィード URL を次の TAXII ソースパラメータにマッピングする必要があります。 • ホスト名 • ポーリングパス（Polling Path） • コレクション名（Collection Name） **例**：SecureX Threat Response ポータルで作成された SecureX Threat Response フィード URL の例を以下に示します。 *<https://private.intel.amp.cisco.com/ctia/feed/feed-d78e1eba-cbe6-5* *e13-8d47-197b344e41c9/view.txt?s=e8f3f519-9170-4b76-8b58 bda0be540ff3>* 例の SecureX Threat Response フィード URL の詳細を次の TAXII ソースパラメータにマッピングできます。 • ホスト名（Hostname）：SecureX Threat Response フィード URL の「*private.intel.amp.cisco.com*」部分で構成されます。 • ポーリングパス（Polling Path）：SecureX Threat Response フィード URL の「*/ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view*」部分で構成されます。 （注） ポーリングパスには SecureX Threat Response フィード URL の「*.txt*」部分を含めないでください。 • コレクション名（Collection Name）：SecureX Threat Response フィード URL の「*e8f3f519-9170-4b76-8b58-bda0be540ff3*」部分で構成されます。 上記の例を使用して、「ホスト名」、「ポーリングパス」、および「コレクション名」パラメータを設定できます。これらのパラメータを設定する方法については、以下を参照してください。	

パラメータ ソースの詳細	説明
ホスト名	SecureX Threat Response サーバリージョンに基づいて、SecureX Threat Response フィード URL のホスト名を入力します。 SecureX Threat Response サーバリージョンに基づいて選択できるホスト名は次のとおりです。 • `private.intel.amp.cisco.com`（米国のユーザに適用可能） • `private.intel.eu.amp.cisco.com`（EU のユーザに適用可能） • `private.intel.apjc.amp.cisco.com` （APJC のユーザに適用可能）
ポーリングパス（Polling Path）	SecureX Threat Response サーバーのポーリングサービスを識別するポーリングパスを入力します。 例：/ctia/feed/feed-d78e1eba-cbe6-5e13-8d47-197b344e41c9/view
コレクション名（Collection Name）	SecureX Threat Response サーバでホストされている SecureX Threat Response フィードのコレクションの名前を入力します。 例：e8f3f519-9170-4b76-8b58-bda0be540ff3
ポーリング間隔（Polling Interval）	SecureX Threat Response サーバから SecureX Threat Response フィードを取得する頻度を定義するポーリング間隔を入力します。最小値は 15 分で、デフォルト値は 60 分です。 （注） フルポーリングの上限は 100 mb であり、フィード監視対象のサイズが上限を超えると、電子メールゲートウェイは ETF ログにエラーメッセージを表示します。
脅威フィードの経過期間、ポーリングセグメントの期間	SecureX Threat Response サーバからの監視対象のポーリングは時間間隔に基づいていないため、これらのパラメータは SecureX Threat Response フィードソースに設定する必要はありません。監視対象の取得には、フルポーリング方式が使用されます。

パラメータ ソースの詳細	説明
HTTPS の使用（Use HTTPS）	HTTPS プロキシサーバーを使用して電子メールゲートウェイを SecureX サーバーに接続する場合は、[はい（Yes）] を選択します。 （注） このパラメーターは、電子メールゲートウェイでプロキシサーバーを有効にして設定する場合にのみ使用されます。
クレデンシャルの設定（Configure Credentials）	このパラメータは、 SecureX Threat Response フィードソースの設定には必要ありません。
プロキシの詳細	
グローバル プロキシの使用（Use Global Proxy）	電子メールゲートウェイがプロキシサーバを介して SecureX Threat Response サーバに接続されるようにする場合は、[はい（Yes）] を選択します。 次のいずれかの方法でプロキシ サーバを設定できます。 • Web インターフェイスの [セキュリティ サービス（Security Services）] > [サービス アップデート（Service Updates）] ページ • CLI の *updateconfig* コマンド [いいえ（No）] を選択すると、電子メールゲートウェイは直接 SecureX Threat Response サーバに接続されます。

ステップ 4 変更を送信し、保存します。

SecureX Threat Response フィードソースの設定後、電子メールゲートウェイが SecureX Threat Response ソースから脅威フィードを取得し始めます。

次のタスク

- CLI で **threatfeedsconfig > sourceconfig** サブコマンドを使用して SecureX Threat Response フィードソースを設定することもできます。
- （任意）[メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで [ポーリングの一時停止（Suspend Polling）]（ ）アイコンをクリックして、設定した SecureX Threat Response フィードソースのポーリングサービスを一時停止します。

- （任意）[メールポリシー（Mail Policies）]>[外部脅威フィードマネージャ（External Threat Feeds Manager）]ページで[ポーリングの再開（Resume Polling）]（ ）アイコンをクリックして、設定した SecureX Threat Response フィードソースのポーリングサービスを再開します。
- （任意）[メールポリシー（Mail Policies）]>[外部脅威フィードマネージャ（External Threat Feeds Manager）] ページで [今すぐポーリング（Poll Now）] をクリックして、最後に成功したポーリング間隔ですぐに SecureX Threat Response フィードを取得します。
- 脅威が含まれているメッセージの処理 （369 ページ） を参照してください。

脅威が含まれているメッセージの処理

電子メールゲートウェイで以下を使用して、脅威が含まれているメッセージを処理できます。

- HAT
- コンテンツ フィルタまたはメッセージ フィルタ

関連項目

- 脅威が含まれているメッセージの処理に向けた送信者グループの設定 （369 ページ）。
- 脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージ フィルタの設定 （370 ページ）。

脅威が含まれているメッセージの処理に向けた送信者グループの設定

既存の送信者グループを設定して、ETF エンジンから取得した判定を使用して悪意のある IP を起源とするメッセージを処理できます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。
ステップ 2 脅威を含むメッセージを処理するために設定する既存の送信者グループをクリックします。
ステップ 3 [設定の編集（Edit Settings）] をクリックします。
ステップ 4 悪意のある IP アドレスをフィルタ処理するために必要な ETF ソースを選択します。
ステップ 5 （任意）[行の追加（Add Row）] をクリックして別の ETF ソースを追加します。
ステップ 6 変更を送信し、保存します。

脅威が含まれているメッセージの処理に向けたコンテンツまたはメッセージ フィルタの設定

ETFエンジンから取得した判定に基づいて脅威を含むメッセージに適切なアクションを実行するために、以下の 1 つ以上のコンテンツまたはメッセージ フィルタを設定できます。

- URL レピュテーション - ETF エンジンによって悪意があるとして分類された URL を検出します。
- ドメイン レピュテーション - ETF エンジンによって悪意があるとして分類されたドメインを検出します。
- ファイル情報による添付ファイル - ファイルのハッシュに基づいて ETF エンジンによって悪意があるとして分類されたファイルを検出します。

関連項目

- コンテンツ フィルタを使用した、メッセージの悪意のあるドメインの検出（370ページ）。
- メッセージフィルタを使用した、メッセージの悪意のあるドメインの検出（372ページ）
- コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出（372 ページ）
- メッセージ フィルタを使用した、メッセージの悪意のある URL の検出（374 ページ）
- コンテンツフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出（376 ページ）。
- メッセージフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出（272 ページ）。

コンテンツフィルタを使用した、メッセージの悪意のあるドメインの検出

‘Domain Reputation’ コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージのドメインを検出し、これらのメッセージに対して適切なアクションを実行します。

始める前に

- （任意）ドメインのみが含まれたアドレス リストを作成します。作成するには、Web インターフェイスの [メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）] ページに移動するか、CLI で `addresslistconfig` コマンドを使用します。詳細については、メール ポリシー （309 ページ）を参照してください。

- （任意）ドメインの例外リストを作成します。詳細については、ドメインの例外リストの作成を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [ドメインレピュテーション（Domain Reputation）] をクリックします。

ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 7 メッセージのヘッダーの悪意のあるドメインを検出するための ETF ソースを選択します。

ステップ 8 ドメインのレピュテーションの確認に必要なヘッダーを選択します。

ステップ 9 （任意）電子メールゲートウェイで、このコンテンツフィルタによる脅威の検出を避ける許可リストに登録されているドメインのリストを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [アクションの追加（Add Action）] をクリックして、悪意のあるドメインを含むメッセージに対して実行する適切なアクションを設定します。

ステップ 12 変更を送信し、保存します。

ドメインの例外リストの作成

ドメインの例外リストは、ドメインのみが含まれるアドレスのリストで構成されています。電子メールゲートウェイで、設定されているすべてのドメインレピュテーションのコンテンツまたはメッセージフィルタでのドメインチェックをスキップするには、ドメインの例外リストを使用します。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ドメインレピュテーション（Domain Reputation）] に移動します。

ステップ 2 [ドメインの例外リスト（Domain Exception List）] の下の [設定の編集（Edit Settings）] をクリックします。

ステップ 3 ドメインのみが含まれている必要なアドレス リストを選択します。

ステップ 4 変更を送信し、保存します。

次のタスク

CLI で domainrepconfig コマンドを使用してドメインの例外リストを作成することもできます。詳細については、『*CLI Reference Guide for AsyncOS 12.0 for Cisco Email Security Appliances*』を参照してください。

メッセージフィルタを使用した、メッセージの悪意のあるドメインの検出

例として、以下のメッセージ フィルタ ルール構文を使用して、ETF エンジンを使用してメッセージ内の悪意のあるドメインを検出し、そのようなメッセージに対して適切な対応をします。

構文：

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

引数の説明

- `'domain-external-threat-feeds'` は、ドメイン レピュテーション メッセージ フィルタのルールです。
- `'etf_source1'`は、メッセージのヘッダーの悪意のあるドメインを検出するために使用される ETF ソースです。
- `'mail-from'`、`'from'` は、ドメインのレピュテーションを確認するために使用される必須ヘッダーです。
- `'domain_exception_list'` は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。

例

以下の例では、‘Errors To:’ カスタム ヘッダーのドメインが ETF によって悪意があるとして検出された場合、メッセージが検疫されます。

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出

‘URL Reputation’ コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージの URL を検出し、これらのメッセージに対して適切なアクションを実行します。

ETF の ‘URL Reputation’ コンテンツ フィルタは、以下のいずれかの方法で設定できます。

- 'URL Reputation' の条件と適切なアクションを使用する。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない。

- 'URL Reputation' の条件とアクションを使用する。

'URL Reputation' の条件とアクションを使用して悪意のある URL を検出するには、以下の手順を使用します。

（注）
- 'URL Reputation' の条件と任意の適切なアクションを使用するには、手順のステップ 11 ～ 20 は無視してください。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない場合は、手順のステップ 4 ～ 10 は無視してください。

始める前に

- 電子メールゲートウェイで URL フィルタリングが有効にされていることを確認します。URL フィルタリングを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）] > [URLフィルタリング（URL Filtering）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護 （543 ページ）を参照してください。
- 電子メールゲートウェイでアウトブレイクフィルタが有効にされていることを確認します。アウトブレイク フィルタを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）]>[アウトブレイクフィルタ（Outbreak Filters）] ページに移動します。詳細については、アウトブレイク フィルタ （513 ページ）を参照してください。
- 電子メールゲートウェイでスパム対策エンジンが有効にされていることを確認します。スパム対策エンジンを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）]>[スパム対策（Anti-Spam）] ページに移動します。詳細については、スパムおよびグレイメールの管理 （461 ページ）を参照してください。
- （任意）URL リストを作成します。作成するには、Web インターフェイスで [メールポリシー（Mail Polices）]>[URLリスト（URL Lists）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護 （543 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 7 悪意のある URL を検出する ETF ソースを選択します。

ステップ 8 （任意）電子メールゲートウェイで脅威を検出しない許可リストに登録されている URL のリストを選択します。

ステップ 9 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [アクションを追加（Add Action）] をクリックします。

ステップ 12 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 13 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 14 条件（ステップ 7）で選択した ETF ソースと同じ ETF ソースを選択したことを確認します。

ステップ 15 （任意）ステップ 8 で選択したものと同じ許可リストに登録されている URL のリストを選択します。

ステップ 16 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 17 メッセージの本文および件名および/またはメッセージの添付ファイルの URL に対して実行する必要なアクションを選択します。

（注） ステップ 16 で [（次に含まれるURLを確認）Check URLs within] オプションに [添付ファイル（Attachments）] を選択した場合、メッセージから添付ファイルを除去することのみが可能です。

ステップ 18 すべてのメッセージにアクションを実行するか、未署名のメッセージにアクションを実行するかを選択します。

ステップ 19 [OK] をクリックします。

ステップ 20 変更を送信し、保存します。

（注） Webベースのレピュテーションスコア（WBRS）と電子メールゲートウェイのETFに対してURL レピュテーション コンテンツ フィルタを設定している場合は、電子メールゲートウェイのパフォーマンスを向上するために、WBRS URL レピュテーション コンテンツ フィルタの順序を ETF URL レピュテーションフィルタの順序よりも高く設定することをお勧めします。

メッセージフィルタを使用した、メッセージの悪意のあるURLの検出

例として、ETF エンジンを使用して悪意のあるメッセージの URL を検出し、URL を無効化するには、‘URL Reputation’ のメッセージ フィルタ ルール構文を使用します。

構文：

```
defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
<'URL_allowedlist'>,
```

```
<’message_attachments'> , <’message_body_subject’> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <’URL_allowedlist’> ,
<’Preserve_signed’>)}
```

引数の説明

- ‘url-external-threat-feeds’ は、URL レピュテーションのルールです。
- ‘etf_source1’ は、メッセージまたはメッセージの添付ファイルの悪意のある URL を検出するために使用される ETF ソースです。
- 「URL_allowedlist」は、URL 許可リストの名前です。URL の許可リストが存在しない場合は「""」と表示されます。
- 'message_attachments' は、メッセージの添付ファイルの悪意のある URL をチェックするために使用します。メッセージの添付ファイルの悪意のある URL を検出するには '1' の値を使用します。
- 'message_body_subject' は、メッセージ本文と件名の悪意のある URL をチェックするために使用します。メッセージの本文と件名の悪意のある URL を検出するには '1' の値を使用します。

（注） メッセージの本文、件名、添付ファイルの悪意のある URL を検出するには '1,1' の値を使用します。

- ‘url-etf-defang’ は、悪意のある URL を含むメッセージに対して実行できるアクションの 1 つです。

  以下の例は、悪意のある URL を含むメッセージに対して適用できる ETF ベースのアクションです。

  - url-etf-strip(['etf_source1'],"None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- ‘Preserve_signed’ は、‘1’ または ‘0’ で表されます。‘1’ は、このアクションが未署名のメッセージのみに適用されることを示し、‘0’ はこのアクションがすべてのメッセージに適用されることを示します。

以下の例では、ETFエンジンによってメッセージの添付ファイルで悪意のあるURLが検出された場合、添付ファイルが除去されます。

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

コンテンツフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出

'Attachment File Info' コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージの添付ファイルを検出し、これらのメッセージに対して適切なアクションを実行します。

（注） ETF エンジンは、ファイルのファイル ハッシュに基づいてルックアップを実行します。

ETF の 'Attachment File Info' コンテンツ フィルタは、以下のいずれかの方法で設定できます。

- 'Attachment File Info' の条件と適切なアクションを使用する。
- 'Strip Attachment by File Info' のアクションと任意の条件を使用するか、条件を使用しない。
- 'Attachment File Info' の条件と 'Strip Attachment by File Info' のアクションを使用する。

'Attachment by File Info' の条件と 'Strip Attachment by File Info' のアクションを使用してメッセージの悪意のある添付ファイルを検出するには、以下の手順を使用します。

（注）
- 'Attachment File Info' の条件と任意の適切なアクションを使用するには、手順のステップ 10 ～ 15 は無視してください。
- 'Strip Attachment by File Info' のアクションと任意の条件を使用するか、条件を使用しない場合は、手順のステップ 4 ～ 9 は無視してください。

始める前に

（任意）ファイル ハッシュの例外リストを作成します。作成するには、Web インターフェイスで [メールポリシー（Mail Polices）] > [ファイルハッシュリスト（File Hash Lists）] ページに移動します。詳細については、ファイル ハッシュのリストの作成（377 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。
ステップ 3 コンテンツ フィルタの名前と説明を入力します。
ステップ 4 [条件を追加（Add Condition）] をクリックします。
ステップ 5 [添付ファイル情報（Attachment File Info）] をクリックします。
ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。
ステップ 7 ファイル ハッシュを使用して悪意のある ファイル を検出する ETF ソースを選択します。
ステップ 8 （任意）電子メールゲートウェイで脅威を検出しないファイルハッシュのリストを選択します。
ステップ 9 [OK] をクリックします。
ステップ 10 [アクションを追加（Add Action）] をクリックします。
ステップ 11 [ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] をクリックします。
ステップ 12 [外部脅威フィード（External Threat Feeds）] を選択します。
ステップ 13 条件（ステップ 7）で選択した ETF ソースと同じ ETF ソースを選択したことを確認します。
ステップ 14 （任意）ステップ 8 で選択したものと同じファイル ハッシュのリストを選択します。
ステップ 15 変更を送信し、保存します。

ファイル ハッシュのリストの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [ファイルハッシュのリスト（File Hash Lists）] に移動します。
ステップ 2 [ファイルハッシュのリストの追加（Add File Hash List）] を選択します。
ステップ 3 必要なファイル ハッシュのタイプ（‘SHA256’ または ‘MD5'、または上記のすべて）をチェックします。
ステップ 4 （ステップ 3 で選択した）ファイル ハッシュをカンマで区切って、または改行して入力します。
ステップ 5 変更を送信し、保存します。

メッセージフィルタを使用した、メッセージの添付ファイルの悪意のあるファイルの検出

例として、以下のメッセージフィルタ ルール構文を使用して、ETF エンジンによってメッセージの添付ファイル内で悪意があるとして分類されるファイルを検出し、そのようなメッセージに対して適切な対応をします。

構文：

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'],
<'file_hash_exception_list'>))
{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

それぞれの説明は次のとおりです。

- `'file-hash-etf-rule'` は、添付ファイル情報のメッセージ フィルタのルールです。
- `'etf_source1'` は、ファイルのハッシュに基づいてメッセージの悪意のあるファイルを検出するために使用される ETF ソースです。
- `'file_hash_exception_list'` は、ファイル ハッシュの例外リストの名前です。ファイル ハッシュの例外リストが存在しない場合は「""」と表示されます。
- `'file-hash-etf-strip-attachment-action'` は、悪意のあるファイルが含まれるメッセージに対して適用するアクションです。

以下の例では、メッセージに ETF エンジンによって悪意があるとして検出された添付ファイルが含まれる場合、添付ファイルが除去されます。

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", "Malicious message attachment has been stripped from
the message.");}
```

受信メール ポリシーへのコンテンツ フィルタのアタッチ

メッセージの悪意のあるドメイン、URL、ファイル ハッシュを検出するように設定した 1 つ以上のコンテンツ フィルタを受信メール ポリシーにアタッチできます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 2 特定のメール ポリシーの [コンテンツフィルタ（Content Filters）] の下のリンクをクリックします。

ステップ 3 [コンテンツフィルタを有効にする（カスタマイズ設定）（Enable Content Filters (Customize Settings)）] を選択します。

ステップ 4 悪意のあるドメイン、URL、ファイル ハッシュを検出するために作成したコンテンツ フィルタを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

コンテンツフィルタをメールポリシーにアタッチした後、電子メールゲートウェイは、ETF エンジンから受け取った判定に基づいてメッセージに対するアクションの実行を開始します。

外部脅威フィードおよびクラスタ

一元管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、ETFエンジンとメール ポリシーを有効化できます。

外部脅威フィード エンジンの更新のモニタリング

サービス アップデートを有効にすると、ETF エンジンのアップデートがシスコのアップデートサーバから取得されます。しかし、一部のシナリオでは（たとえば、サービスの自動アップデートを無効にした場合またはサービスの自動アップデートが機能していない場合）、ETFエンジンを手動で更新する必要があります。

ETF エンジンは、以下のいずれかの方法で手動アップデートできます。

- Web インターフェイスの [セキュリティサービス（Security Services）] > [外部脅威フィード（External Threat Feeds）] ページに移動し、[今すぐアップデート（Update Now）] をクリックします。
- CLI では、`threatfeedupdate` コマンドを使用します。

既存の ETF エンジンの詳細を確認するには、Web インターフェイスの [セキュリティサービス（Security Services）] > [外部脅威フィード（External Threat Feeds）] ページの [外部脅威フィードのアップデート（External Threat Feeds Engine Updates）] セクションを表示するか、CLI で threatfeedstatus コマンドを使用します。

アラートの表示

以下の表では、ETFエンジンによって生成されるアラート、アラートの説明、アラートの重大度を記載します。

コンポーネント/アラート名	メッセージと説明	パラメータ
ETF ENGINE ALERT	Unable to fetch the observables from the source: $source_name after 3 failed attempts. Reason for failure: $reason	**'source'** - TAXII ソースの名前。 **'reason'** - ポーリングに失敗した理由。
	情報。TAXII ソースからのフィードのポーリングが失敗した場合に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
ETF ENGINE ALERT	The storage limit of $count observables exceeded for the observable type: $type.	**$count** - タイプごとに許可された監視対象の数。 **$ type** - は、監視対象のタイプ。
	情報。許可された監視対象の数を超過した場合に送信されます。	

メッセージ トラッキングの脅威詳細の表示

選択した ETF の選択した IOC に対応する、脅威を含むメッセージの詳細を表示できます。

始める前に

- E メール ゲートウェイでメッセージ トラッキング機能が有効にされていることを確認します。メッセージ トラッキングを有効にするには、Web インターフェイスで [セキュリティサービス（Security Services）] > [集中管理サービス（Centralized Services）] > [メッセージトラッキング（Message Tracking）] ページに移動します。
- メッセージの脅威を検出するためのコンテンツまたはメッセージフィルタが動作していることを確認します。

手順

ステップ 1 [モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] に移動します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [メッセージイベント（Message Event）] の下の [外部脅威フィード（External Threat Feeds）] をクリックします。

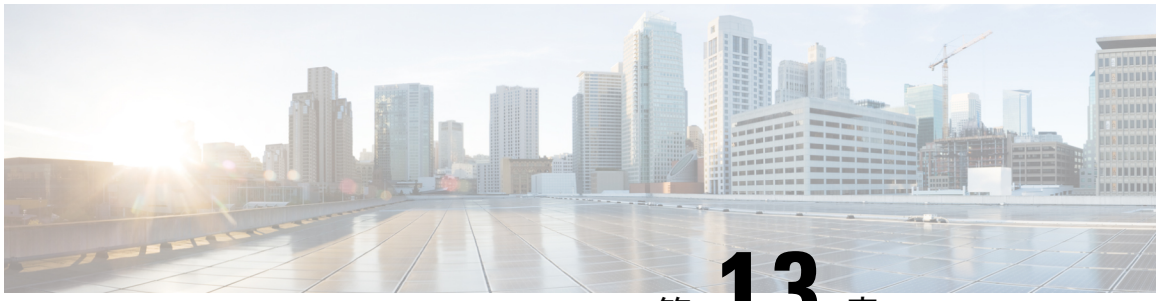
ステップ 4 選択した IOC に対応する、脅威を含むメッセージをトラッキングするために必要な IOC を選択します。

ステップ 5 （任意）**[すべての外部脅威フィードソース（All External Threat Feed Sources）]** を選択して、電子メールゲートウェイで設定した、利用可能および消去された ETF ソースに基づいて脅威を含むメッセージを表示します。

ステップ 6 （任意）**[現在の外部脅威フィードソース（Current External Threat Feed Sources）]** と必要な ETF ソースを選択して、電子メールゲートウェイで設定した、利用可能な ETF ソースに基づいて脅威を含むメッセージを表示します。

ステップ 7 （任意）[外部脅威フィードソース（External Threat Feed Sources）] に特定の ETF ソースの名前を入力して、その ETF ソースに基づいて脅威を含むメッセージを表示します。

ステップ 8 **[検索（Search）]** をクリックします。



第 13 章

送信者ドメイン レピュテーション フィルタリング

この章は、次の項で構成されています。

- 送信者ドメイン レピュテーション フィルタリングの概要 （381 ページ）
- 送信者ドメイン レピュテーションに基づいてメッセージをフィルタリングする方法 （385 ページ）
- 電子メールゲートウェイでの送信者ドメイン レピュテーション フィルタリングの有効化 （385 ページ）
- 送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定 （387 ページ）
- 受信メール ポリシーへのコンテンツ フィルタのアタッチ （391 ページ）
- 送信者ドメイン レピュテーション フィルタリングおよびクラスタ （392 ページ）
- メッセージ トラッキングの送信者ドメイン レピュテーション詳細の表示 （392 ページ）
- アラートの表示 （393 ページ）
- ログの表示 （393 ページ）

送信者ドメイン レピュテーション フィルタリングの概要

Cisco Talos の送信者ドメイン レピュテーション（SDR）は、電子メールのエンベロープおよびヘッダーに入力されたドメインに基づいて、電子メール メッセージのレピュテーション判定を提供するクラウド サービスです。たとえば、HELO/EHLO 文字列、エンベロープとヘッダーの「From」アドレス、「Reply-to」アドレス、および「List-Unsubscribe」ヘッダーに含まれるドメインが使用されます。

ドメイン ベースのレピュテーション分析では、共有 IP、ホスティングまたはインフラストラクチャ プロバイダーのレピュテーションよりも詳しい情報を調べることでより高いスパム検出率を達成し、完全修飾ドメイン名（FQDN）や Simple Mail Transfer Protocol（SMTP）通信およびメッセージ ヘッダーのその他の送信者情報に関連する特徴に基づいて判定を取得します。

詳細については、シスコのカスタマー連携プログラム（http://www.cisco.com/go/ccp）のセキュリティ トラックで、Cisco Talos の送信者ドメイン レピュテーション（SDR）のホワイト ペーパーをご覧ください。

（注）
- SDR のホワイト ペーパーにアクセスするには、シスコのカスタマー連携プログラムのアカウントを作成する必要があります。
- Cisco IPAS のクレームについては、Cisco Technical Assistance Center（TAC）のサポート リクエストを開いて SDR のクレームを送信してください。

SDR 判定

以下の表に、SDR 判定の名前、説明、推奨処置を記載します。

表 *35 : SDR* 判定

判定名	説明	推奨処置
非常に問題がある（Awful）	最も問題のあるレピュテーション判定です。 ブロッキングのしきい値がこの判定のみに設定されている場合、検出漏れ（FN）が発生し、セキュリティよりも配信が優先されます。	メッセージをブロックする。
不良（Poor）	推奨されるブロッキングのしきい値です。 これにより、検出漏れ（FN）と誤検出（FP）の長所と短所のバランスを取ることができます。Talos は SDR を調整し、「不良」または「非常に問題がある」の判定のいずれかを持つメッセージが SDR によってブロックされるようにします。 この判定でブロッキングをしない場合はセキュリティよりも配信が優先されますが、お客様はこの判定に基づいてブロックしない場合の検出漏れを許容することになります。	電子メールゲートウェイに設定されている他のエンジンでメッセージをスキャンする。

判定名	説明	推奨処置
汚染されている（Tainted）	疑わしい送信者レピュテーションです。 これらの判定に基づくブロッキングは積極的で、Talos では推奨されていません。配信よりもセキュリティが優先されますが、この判定に基づいてブロックすると、許容できる誤検出が発生します。	電子メールゲートウェイに設定されている他のエンジンでメッセージをスキャンする。
弱い（Weak）	ニュートラルな判定を除外した弱いインジケータに関連付けられる多くのドメイン（正規および混在使用を含む）に一般的な判定です。Talos は、この判定でのブロッキングを推奨していません。 配信よりもセキュリティが優先されますが、この判定に基づいてメッセージをブロックする場合、（Talos の基準で）許容できない数の誤検出が発生します。	電子メールゲートウェイに設定されている他のエンジンでメッセージをスキャンする。

判定名	説明	推奨処置
不明（Unknown）	送信者が新しく登録したドメインか、SDR が認識できないドメインを使用しています。この判定不可能なステータスのドメインに対して、Talos は詳細な分析を実行してすばやく判定を確立します。Talos は、この判定でのブロッキングを推奨していません。この判定でブロックすると、しきい値をこの判定に調整した場合の多くの誤検出を許容することになります。Talos では、「不明」の判定でメッセージを検疫することを推奨しています。 Talos がドメインを調査するため、メッセージが後続のエンジンにスキャンされる前に、メッセージの配信が少し遅延します。	電子メールゲートウェイに設定されている他のエンジンでメッセージをスキャンする。
ニュートラル	送信者が新しいドメインを使用しておらず、送信者のベストプラクティスに従っている場合に通常期待される判定です。送信者のベストプラクティスには、SPF を使用する、DKIM 署名を使用する、スパムを送信しないなどがあります。	電子メールゲートウェイに設定されている他のエンジンでメッセージをスキャンする。
良好	送信者が、メッセージにDKIM署名（「`From:` ヘッダー ドメインに並列」）がある認定済みのドメインを使用している稀な判定です。	電子メールゲートウェイに設定されている他のエンジンでメッセージをスキャンする。

送信者ドメインレピュテーションに基づいてメッセージをフィルタリングする方法

手順	操作手順	詳細情報
ステップ 1	Cisco E メール セキュリティ ゲートウェイで SDR フィルタリングを有効化します。 （注） AsyncOS 12.0 にアップグレードすると、SDR クエリがデフォルトで有効化されます。	電子メールゲートウェイでの送信者ドメイン レピュテーション フィルタリングの有効化 （385 ページ）
ステップ 2	SDR に基づいてメッセージを処理するためのメッセージまたはコンテンツ フィルタを設定します。	送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定 （387 ページ）
ステップ 3	SDR に基づいてメッセージをフィルタ処理するために設定したコンテンツ フィルタを受信メール ポリシーにアタッチします。	受信メール ポリシーへのコンテンツ フィルタのアタッチ （391 ページ）

電子メールゲートウェイでの送信者ドメインレピュテーション フィルタリングの有効化

（注） AsyncOS 12.0 にアップグレードすると、SDR クエリがデフォルトで有効化されます。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ドメインレピュテーション（Domain Reputation）] に移動します。

ステップ 2 [有効化（Enable）] をクリックします。

ステップ 3 [送信者ドメインレピュテーションフィルタリングの有効化（Enable Sender Domain Reputation Filtering）] をチェックします。

ステップ 4 （任意）SDR サービスによって、メッセージの追加の属性によって SDR を確認する場合は [追加属性を含める（Include Additional Attributes）] をチェックします。

このオプションを有効にすると、メッセージの次の追加属性が SDR の確認に追加され、有効性が向上します。

- 「`Envelope From:`」ヘッダー、「`From:`」ヘッダー、および「`Reply-To:`」ヘッダーに存在する電子メールアドレスのユーザ名の部分。
- 「`From:`」ヘッダーと「`Reply-To:`」ヘッダーの表示名。

ステップ 5 （任意）レピュテーション クエリーがタイムアウトになるまでの経過秒数を入力します。

（注） SDR クエリのタイムアウト値を変更すると、メール処理のパフォーマンスに影響を与える可能性があります。

ステップ 6 （任意）電子メールゲートウェイで「Envelope From：」ヘッダーのドメインのみに基づく SDR の確認をスキップする場合は、[Envelope Fromのドメインに基づいてドメイン例外リストと一致（Match Domain Exception List based on Domain in Envelope From）] をチェックします。

ステップ 7 **範囲スライダ**を動かして、SMTP カンバセーションレベルでメッセージを許可または拒否するために必要な SDR 判定範囲を選択します。

（注） AsyncOS 14.x 以降にアップグレードした後、デフォルトでは範囲スライダは Awful 判定を示します。「Awful」判定のメッセージはすべて、SMTP カンバセーションレベルでドロップされます。

（注） 「Good」判定は送信者が認証済みドメインを使用していることを示すため、メッセージを拒否するために「Good」判定を選択することはできません。

ステップ 8 [送信] をクリックします。

ステップ 9 （任意）「SDR には追加属性契約が含まれます」のメッセージを許可する場合は [同意（I Agree）] をクリックします。

（注） 「SDR には追加属性契約が含まれます」のメッセージは、[追加属性を含める（Include Additional Attributes）] オプションを選択した場合のみ表示されます。

ステップ 10 [確定する（Commit）] をクリックして変更を保存します。

次のタスク

SDR に基づいてメッセージを処理するためのメッセージまたはコンテンツ フィルタを設定します。送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定 （387 ページ） を参照してください。

送信者ドメイン レピュテーションに基づいてメッセージを処理するためのコンテンツまたはメッセージ フィルタの設定

以下のいずれかの方法で 'Domain Reputation' のメッセージまたはコンテンツ フィルタを使用して、SDR に基づいてメッセージをフィルタ処理し、そのようなメッセージに対して適切なアクションを実行できます。

- 送信者のドメインの判定
- 送信者のドメインの経過時間
- 送信者のドメインがスキャン不可

関連項目

- メッセージ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング （387 ページ）
- コンテンツ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング （389 ページ）

メッセージ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング

送信者ドメインの判定に基づいてメッセージをフィルタ処理

（注） 推奨されるブロッキングのしきい値は「Awful」です。SDR 判定の詳細は、SDR 判定 （382 ページ）を参照してください。

構文：

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['awful', 'poor'], "<domain_exception_list>")
{drop();}
```

それぞれの説明は次のとおりです。

- `'drop_msg_based_on_sdr_verdict'` は、メッセージ フィルタの名前です。
- `'sdr-reputation'` は、ドメイン レピュテーション メッセージ フィルタのルールです。

- 'awful'、'poor' は、SDR に基づいてメッセージをフィルタ処理するための送信者のドメイン判定の範囲です。
- 'domain_exception_list' は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。
- 'drop' は、メッセージに適用されるアクションです。

例

以下のメッセージでは、SDR 判定が 'Unknown' の場合、メッセージが検疫されます。

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

送信者ドメインの経過時間に基づいてメッセージをフィルタ処理

（注） [送信者ドメインの経過時間（Sender Domain Age）] オプションは、次の AsyncOS リリースで削除されます。

構文：

```
<msg_filter_name>
if sdr-age (<‘unit'>, <‘operator'> <‘actual value’>)
{<action>}
```

それぞれの説明は次のとおりです。

- ‘sdr-reputation' は、ドメイン レピュテーション メッセージ フィルタのルールです。
- 'sdr_age'は、SDR に基づいてメッセージをフィルタ処理するために使用される送信者ドメインの経過時間です。
- ‘unit' は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための ‘days’、‘years’、‘months’、'weeks' オプションです。
- ‘operator'は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための比較演算子です。
  - – >（次の値より大きい）
  - – >=（次の値以上）
  - – <（次の値より小さい）
  - – <=（次の値以下）
  - – ==（次の値と等しい）
  - – !=（次の値と等しくない）
  - – Unknown

- 'actual value' は、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するために使用される数字です。

例

以下のメッセージでは、送信者ドメインの経過時間が不明な場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("unknown", "")) {drop();}
```

以下のメッセージでは、送信者ドメインの経過時間が1ヵ月よりも短い場合、メッセージはドロップされます。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("months", <, 1, "")) { drop(); }
```

送信者ドメインのスキャン不可能性に基づいてメッセージをフィルタ処理

構文：

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

それぞれの説明は次のとおりです。

- 'sdr-unscannable' は、ドメイン レピュテーション メッセージ フィルタのルールです。

  'domain_exception_list' は、ドメインの例外リストの名前です。ドメインの例外リストが存在しない場合は「""」と表示されます。

例

以下のメッセージでは、メッセージが SDR チェックに不合格の場合、メッセージが検疫されます。

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

コンテンツ フィルタを使用した、送信者ドメイン レピュテーションに基づくメッセージのフィルタリング

始める前に

- （任意）ドメインのみが含まれたアドレス リストを作成します。作成するには、Web インターフェイスの [メールポリシー（Mail Policies）] > [アドレスリスト（Address Lists）] ページに移動するか、CLI で addresslistconfig コマンドを使用します。詳細については、メール ポリシー （309 ページ）を参照してください。
- （任意）ドメインの例外リストを作成します。詳細については、ドメインの例外リストの作成 （390 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [ドメインレピュテーション（Domain Reputation）] をクリックします。

ステップ 6 SDRに基づいてメッセージをフィルタ処理するために、以下のいずれかの条件を選択します。

- 判定範囲を選択し、SDRサービスから受け取った判定に基づいてメッセージをフィルタ処理するには [送信者ドメインレピュテーション判定（Sender Domain Reputation Verdict）] を選択します。

  （注） 推奨されるブロッキングのしきい値は「Awful」です。SDR 判定の詳細は、SDR 判定 （382 ページ）を参照してください。

- [送信者ドメインの経過時間（Sender Domain Age）] を選択し、比較演算子を選択します。数字を入力し、送信者ドメインの経過時間に基づいてメッセージをフィルタ処理するための期間を選択します。

  （注） [送信者ドメインの経過時間（Sender Domain Age）] オプションは、次の AsyncOS リリースで削除されます。

- [送信者ドメインレピュテーションスキャン不可（Sender Domain Reputation Unscannable）] を選択し、SDR の確認に失敗したメッセージをフィルタ処理します。

ステップ 7 （任意）電子メールゲートウェイで、SDRに基づくメッセージのフィルタ処理を避ける許可リストに掲載されたドメインのリストを選択します。

ステップ 8 [アクションの追加（Add Action）] をクリックして、SDR に基づいてメッセージに実行する適切なアクションを設定します。

ステップ 9 変更を送信し、保存します。

ドメインの例外リストの作成

ドメインの例外リストは、ドメインのみが含まれるアドレスのリストで構成されています。ドメインの例外リストを使用して、Cisco E メール セキュリティ ゲートウェイで設定したメールポリシーにかかわらず、すべての受信メッセージに対するSDRチェックをスキップできます。

（注） 特定のメール ポリシーで受信メッセージに対する SDR コンテンツ フィルタ アクションをスキップする場合は、ドメイン レピュテーション コンテンツ フィルタでドメインの例外リストを選択する必要があります。

ドメインの例外のリストを使用するための条件

SDRチェックをスキップするには、デフォルトで、メッセージの「Envelope From:」ヘッダー、「From:」ヘッダー、および「Reply-To:」ヘッダーが同じで、ドメイン例外リストに設定されているドメインと一致する必要があります。アプライアンスで「Envelope From：」ヘッダーのドメインのみに基づく SDR の確認をスキップする場合は、ドメイン レピュテーションの設定ページで [Envelope Fromのドメインに基づいてドメイン例外リストと一致] を選択します。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ドメインレピュテーション（Domain Reputation）] に移動します。

ステップ 2 [ドメインの例外リスト（Domain Exception List）] の下の [設定の編集（Edit Settings）] をクリックします。

ステップ 3 ドメインのみが含まれている必要なアドレス リストを選択します。

ステップ 4 変更を送信し、保存します。

次のタスク

CLI で domainrepconfig コマンドを使用してドメインの例外リストを作成することもできます。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

受信メール ポリシーへのコンテンツ フィルタのアタッチ

SDR に基づいてメッセージをフィルタ処理するために設定したコンテンツ フィルタを受信メール ポリシーにアタッチできます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 2 コンテンツ フィルタの下のリンクをクリックします。

ステップ 3 [コンテンツフィルタを有効にする（カスタマイズ設定）（Enable Content Filters (Customize Settings)）] を確実に選択します。

ステップ 4 SDR に基づいてメッセージをフィルタリングするために作成したコンテンツ フィルタを選択します。

ステップ 5 変更を送信し、保存します。

送信者ドメイン レピュテーション フィルタリングおよびクラスタ

一元管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、SDR フィルタリングとメール ポリシーを有効化できます。

メッセージ トラッキングの送信者ドメイン レピュテーション詳細の表示

メッセージ トラッキングを使用して、SDR に基づくメッセージの詳細を表示できます。

始める前に

- E メール ゲートウェイでメッセージ トラッキング機能が有効にされていることを確認します。メッセージ トラッキングを有効にするには、Web インターフェイスで [セキュリティサービス（Security Services）] > [メッセージトラッキング（Message Tracking）] ページに移動します。
- SDR に基づいてメッセージをフィルタリングするためのコンテンツまたはメッセージフィルタが動作していることを確認します。

手順

ステップ 1 [モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] に移動します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 [メッセージイベント（Message Event）] の下の [送信者ドメインレピュテーション（Sender Domain Reputation）] をクリックします。

ステップ 4 必要な SDR 判定を選択して、SDR サービスから受け取った判定に基づいてメッセージを表示します。

ステップ 5 （任意）SDR チェックに失敗した場合にメッセージを表示するには [スキャン不可（Unscannable）] をチェックします。

ステップ 6 （任意）必要な SDR の脅威カテゴリを選択して、脅威カテゴリに基づいてメッセージを表示します。

ステップ 7 **[検索（Search）]** をクリックします。

アラートの表示

以下の表では、SDRに対して生成されるアラート、アラートの説明、アラートの重大度を記載します。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.IMH.SENDER_DOMAIN_LOOKUP_FAILURE_ALERTS	The SDR lookup failed. Reason - <$reason> 警告。SDR クエリが失敗した場合に送信されます。	**'reason'** - SDR クエリが失敗した理由。

ログの表示

SDR フィルタリング情報はメール ログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

SDR フィルタリングのログ エントリの例

SDR フィルタリング情報はメール ログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

- 送信者ドメイン レピュテーションの認証の失敗 （393 ページ）
- 送信者ドメイン レピュテーションのリクエストのタイムアウト （394 ページ）
- 送信者ドメイン レピュテーションの無効なホスト （394 ページ）
- 送信者ドメインのレピュテーションの一般的なエラー （394 ページ）

送信者ドメイン レピュテーションの認証の失敗

この例のログは、SDR サービスに接続する際の認証失敗のために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Authentication failure.
```

ソリューション

CLI で sdradvancedconfig コマンドを使用すると、電子メールゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメイン レピュテーションのリクエストのタイムアウト

この例のログは、SDR サービスと通信する際のリクエスト タイムアウトのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Request timed out.
```

ソリューション

SDR リクエストがタイムアウトになると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。

送信者ドメイン レピュテーションの無効なホスト

この例のログは、電子メールゲートウェイで無効な SDR サービス ホストが設定されたために SDR に基づいてフィルタ処理されなかったメッセージが表示しています。

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Invalid host configured.
```

ソリューション

CLI で sdradvancedconfig コマンドを使用すると、電子メールゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメインのレピュテーションの一般的なエラー

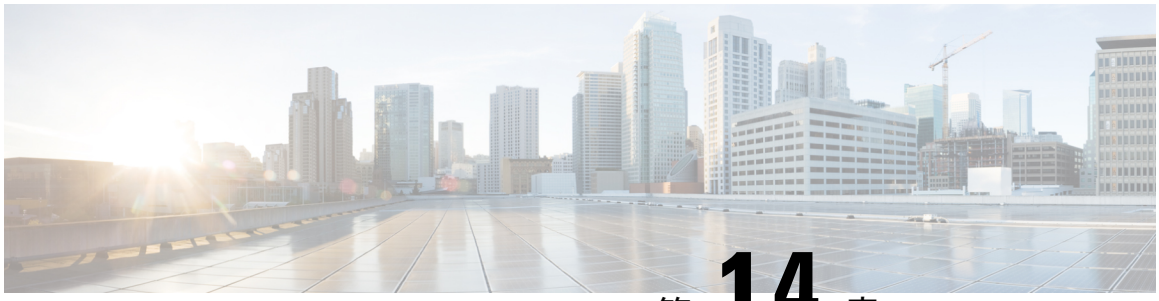
この例のログは、不明なエラーのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
```

```
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Unknown error.
```

ソリューション

不明なエラーが発生すると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。



第 14 章

Cisco SecureX Threat Response との統合

この章は、次の項で構成されています。

- 電子メールゲートウェイと Cisco SecureX Threat Response の統合 （397 ページ）
- 電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （398 ページ）
- Cisco Cloud Services ポータルへの電子メールゲートウェイの登録 （403 ページ）
- Cisco SecureX Ribbon を使用した攻撃分析の実行 （404 ページ）
- Cisco SecureX Threat Response 内のメッセージに対する修復アクションの実行 （408 ページ）
- Cisco Success Network を使用した電子メールゲートウェイのユーザエクスペリエンスの向上 （409 ページ）

電子メールゲートウェイと Cisco SecureX Threat Response の統合

Cisco SecureXは、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。これは新しいテクノロジーを導入する必要のないクラウドネイティブです。Cisco SecureX は、可視性を統合し、自動化を可能にして、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティを強化するプラットフォームを提供することで、脅威からの保護の要求を簡素化します。統合プラットフォームで技術を連携することで、Cisco SecureXは測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。Cisco SecureX では、セキュリティ インフラストラクチャを連携させて機能を拡張できます。

電子メールゲートウェイと Cisco SecureX Threat Response の統合には、次のセクションが含まれています。

- 電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （398 ページ）
- Cisco SecureX Ribbon を使用した攻撃分析の実行 （404 ページ）

電子メールゲートウェイを Cisco SecureX Threat Response と統合し、Cisco SecureX Threat Response で以下のアクションを実行できます。

- 組織内の複数の電子メールゲートウェイから電子メールデータを表示および送信します。
- 電子メールレポート、送信者とターゲットの関係、複数の電子メールアドレスと件名行の検索、およびメッセージトラッキングで確認された脅威を特定、調査、修復します。
- 侵害されたユーザまたは発信電子メールポリシーに違反するユーザをブロックします。
- 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。
- 脅威をドキュメント化して調査内容を保存し、他のデバイスと情報を共有します。
- 悪意のあるドメインのブロック、不審な観測対象の追跡、承認ワークフローの開始、または電子メールポリシーを更新するための IT チケットの作成を行います。

Cisco SecureX Threat Response には、次の URL を使用してアクセスできます。

https://securex.us.security.cisco.com/login

Cisco Secure Email Gateway は高度な脅威からの保護機能を備えており、脅威を迅速に検出、ブロック、修復します。また、データ損失を防ぎ、送信中の重要な情報をエンドツーエンド暗号化によって保護します。ESA モジュールで強化できる観測対象の詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動し、Cisco SecureX と統合するモジュールに移動して、[詳細情報（Learn More）] をクリックしてください。

電子メールゲートウェイと Cisco SecureX Threat Response の統合方法

表 *36 :* 電子メールゲートウェイと *Cisco SecureX Threat Response* の統合方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	前提条件 （400 ページ）

	操作内容	詳細
ステップ 2	（クラシックライセンスモードを使用するユーザにのみ適用されます）。 （注） スマートライセンスモードを使用している場合は、Cisco Cloud Services ポータルが電子メールゲートウェイで自動的に有効になるため、この手順は省略できます。 電子メールゲートウェイで Cisco Cloud Services ポータルを有効にします。	電子メールゲートウェイでの Cisco Cloud Services ポータルの有効化 （401 ページ）
ステップ 3	Cisco SecureX で、電子メールゲートウェイをデバイスとして追加し、登録して、登録トークンを生成します。	詳細については、次を参照してください。https://securex.us.security.cisco.com/help/settings-devices
ステップ 4	（クラシックライセンスモードを使用するユーザにのみ適用されます）。 （注） スマートライセンスモードを使用している場合は、電子メールゲートウェイが Cisco Cloud Services ポータルに自動的に登録されるため、この手順は省略できます。 Cisco Cloud Services ポータルに電子メールゲートウェイを登録します。	Cisco Cloud Services ポータルへの電子メールゲートウェイの登録 （402 ページ）
ステップ 5	登録が成功したかどうかを確認します。	登録が成功したかどうかの確認 （402 ページ）
ステップ 6	電子メールゲートウェイでの Cisco SecureX Threat Response の有効化	電子メールゲートウェイでの Cisco SecureX Threat Response の有効化 （403 ページ）

	操作内容	詳細
ステップ 7	Cisco SecureX で、Cisco Secure Email Gateway モジュールを追加します。	詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するために必要な Cisco Secure Email Gatewayモジュールを選択し、**[新しいモジュールの追加（Add New Module）]** をクリックして、そのページに記載されている手順を参照してください。

前提条件

（注） すでに Cisco Threat Response ユーザアカウントを持っている場合は、Cisco SecureX ユーザアカウントを作成する必要はありません。Cisco Threat Response ユーザアカウントのクレデンシャルを使用して Cisco SecureX にログインできます。

- 管理者アクセス権を使用して、Cisco SecureX でユーザアカウントを作成していることを確認します。新しいユーザアカウントを作成するには、URL（https://securex.us.security.cisco.com/login）を使用して **Cisco SecureX のログイン**ページに移動し、ログインページで [SecureXサインオンアカウントの作成（Create a SecureX Sign-on Account）] をクリックします。新しいユーザアカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。
- 電子メールゲートウェイにアクセスするために指定したホスト名を、設定した DNS サーバーが解決できることを確認します。
- （プロキシサーバを使用していない場合のみ）電子メールゲートウェイを Cisco SecureX Threat Response に登録する場合、ファイアウォールで HTTPS（インおよびアウト）443 ポートが次の FQDN に対してオープンになっていることを確認してください。
  - api-sse.cisco.com（NAM ユーザのみに対応）
  - api.eu.sse.itd.cisco.com（欧州連合（EU）のユーザのみに対応）
  - api.apj.sse.itd.cisco.com（APJC ユーザのみに対応）
  - est.sco.cisco.com（APJC、EU、および NAM ユーザに対応）

  詳細については、ファイアウォール情報 （1607 ページ）を参照してください。
- （電子メールゲートウェイにスマートライセンスが登録されているユーザの場合）（Cisco Smart Software Manager ポータルで作成された）スマートアカウントが Cisco Security Services Exchange にすでにリンクされていることを確認します。詳細については、次の資料を参照してください。

- （NAM ユーザに適用）https://admin.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
- （欧州連合（EU）のユーザに適用）https://admin.eu.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html
- （APJC ユーザに適用）https://admin.apj.sse.itd.cisco.com/assets/static/online-help/index.html#!t_link_accounts.html

電子メールゲートウェイでの Cisco Cloud Services ポータルの有効化

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [ネットワーク（Networks）]>[クラウドサービス設定（Cloud Service Settings）] を選択します。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 [Cisco Cloud Servicesの有効化（Enable Cisco Cloud Services）] チェックボックスをオンにします。

ステップ 5 必要な Cisco Secure サーバを選択して、電子メールゲートウェイを Cisco Cloud Services ポータルに接続します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分待ってから、**[登録（Register）]** ボタンが [クラウドサービス設定（Cloud Services Settings）] ページに表示されるかどうかを確認します。

クラスタ化された設定では、ログイン中の電子メールゲートウェイはマシンモードの Cisco Cloud Services ポータルにのみ登録できます。電子メールゲートウェイを Cisco Cloud Services ポータルにスタンドアロンモードですでに登録している場合は、電子メールゲートウェイをクラスタに参加させる前に手動で登録を解除してください。

（注） CLI を使用して Cisco Cloud Services ポータルを有効にするには、`cloudserviceconfig` コマンドを使用します。

次のタスク

Cisco Cloud Services ポータルに電子メールゲートウェイを登録します。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するモジュールを選択し、**[新しいモジュールの追加（Add New Module）]** をクリックしてページに記載されている手順を参照してください。

Cisco Cloud Services ポータルへの電子メールゲートウェイの登録

手順

ステップ 1 [ネットワーク（Networks）] > [クラウドサービスの設定（Cloud Service Settings）] に移動します。

ステップ 2 [クラウドサービス設定（Cloud Services Settings）] の下に、登録トークンを入力し、**[登録（Register）]** をクリックします。

（注） CLI を使用して電子メールゲートウェイを Cisco Cloud Services ポータルに登録するには、`cloudserviceconfig` サブコマンドを使用します。

次のタスク

登録が成功したかどうかの確認 （402 ページ）

登録が成功したかどうかの確認

- Security Services Exchange で、Security Services Exchange のステータスを確認して、正常に登録されたことを確認します。
- Cisco SecureX で、[デバイス（Devices）] ページに移動し、Security Services Exchange に登録されている ESA を表示します。

（注） 別の Cisco SecureX Threat Response サーバ（欧州用の「api.eu.sse.itd.cisco.com」など）に切り替える場合は、最初に Cisco SecureX Threat Response から電子メールゲートウェイの登録を解除して、電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （398 ページ）のステップを実行する必要があります。

電子メールゲートウェイを Cisco SecureX Threat Response と統合した後は、Cisco Secure Manager Email and Web Gateway を Cisco SecureX Threat Response と統合する必要はありません。

Security Services Exchange に電子メールゲートウェイが正常に登録されたら、Cisco SecureX に ESA 電子メールモジュールを追加します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動して、Cisco SecureX と統合するモジュールを選択し、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

電子メールゲートウェイでの Cisco SecureX Threat Response の有効化

手順

ステップ 1 電子メールゲートウェイにログインします。
ステップ 2 [ネットワーク（Networks）]>[クラウドサービス設定（Cloud Service Settings）] を選択します。
ステップ 3 SecureX の下の **[有効（Enable）]** チェックボックスをオンにします。
ステップ 4 変更を送信し、保存します。

Cisco Cloud Services ポータルへの電子メールゲートウェイの登録

次のいずれかのシナリオに基づいて、電子メールゲートウェイを Cisco Cloud Services ポータルに再登録できます。

- 電子メールゲートウェイを Cisco Cloud Services ポータルに自動的に登録するときに、Cisco Cloud Services ポータルに追加されたデバイス（電子メールゲートウェイ）を表示または管理できない場合。
- 電子メールゲートウェイを Cisco Cloud Services ポータルに自動的に登録するときに、スマートアカウントと Cisco Cloud Services アカウントがリンクされていない場合。

CLI で `cloudserviceconfig` > `register` サブコマンドを使用して電子メールゲートウェイを Cisco Cloud Services ポータルに登録することもできます。

始める前に

次の前提条件を満たしていることを確認してください。

- 電子メールゲートウェイでスマート ソフトウェア ライセンシングをイネーブル化している。
- Cisco Smart Software Manager に電子メールゲートウェイを登録済みである。

手順

ステップ 1 電子メールゲートウェイの [ネットワーク（Networks）]>[クラウドサービス設定（Cloud Service Settings）] ページに移動します。
ステップ 2 [再登録（Reregister）] をクリックします。

（注） [再登録（Reregister）]をクリックした後、要件に応じてステップ 3 または 4 のいずれかまたは両方でタスクを実行するかどうかを選択できます。

ステップ 3 （任意）電子メールゲートウェイが誤った Cisco Secure サーバに自動的に登録された場合は、適切な Cisco Secure サーバを選択して、電子メールゲートウェイを Cisco Cloud Services ポータルに接続します。

ステップ 4 （任意）電子メールゲートウェイが誤ったスマートアカウントで自動的に登録された場合は、Cisco Cloud Services ポータルから取得した登録トークンを入力します。

ステップ 5 [送信（Submit）]をクリックすると、ステップ 4 で登録トークンを入力しない場合にのみ、[再登録の確認（Confirm reregistration）] ダイアログボックスが表示されます。

ステップ 6 [再登録の確認（Confirm reregistration）] ダイアログボックスで [送信（Submit）] をクリックすると、Cisco Cloud Services が Cisco Cloud Services ポータルから自動生成されたトークンをスマートアカウント情報とともに使用して、電子メールゲートウェイを Cisco Cloud Services ポータルに再登録できます。

Cisco SecureX Ribbon を使用した攻撃分析の実行

（注） Cisco Secure Email Gateway 13.5.1 以前のバージョンからアップグレードする場合、**[ケースブック（Casebook）]** は Cisco SecureX Ribbon の一部となります。

Cisco SecureX は、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能をサポートします。Cisco SecureX の分散機能は、SecureX リボンでアプリケーションおよびツールの形式で利用できます。

この章で説明する内容は、次のとおりです。

- Cisco SecureX Ribbon へのアクセス （405 ページ）
- Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （406 ページ）

Cisco SecureX Ribbon はページの下部ペインにあり、ダッシュボードと環境内の他のセキュリティ製品間を移動しても保持されます。Cisco SecureX Ribbon は、次のアイコンと要素で構成されています。

- [リボンの展開/縮小（Expand/Collapse Ribbon）]
- Home
- ケースブックアプリ
- Incidents アプリ
- Orbital アプリ

- [エンリッチメント（Enrichment）] 検索ボックス
- 観測対象の検索
- 設定

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco SecureX Ribbon へのアクセス

始める前に

前提条件（400ページ）に記載されているすべての前提条件を満たしていることを確認してください。

（注） Cisco Secure Email Gateway 13.5.1 以前のバージョンで [ケースブック（Casebook）] を設定していたものとします。次の手順で説明するように、追加のスコープを持つCisco SecureX API クライアントで新しい [クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成する必要があります。

ボタンを使用して、ページの下部ペインにある Cisco SecureX リボンを右からドラッグできます。

手順

ステップ 1 電子メールゲートウェイの新しいWebインターフェイスにログインします。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス（37ページ）を参照してください。

ステップ 2 [Cisco SecureX Ribbon] をクリックします。

ステップ 3 **SecureX API クライアント**で [クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成します。API クライアントのクレデンシャルを生成する方法の詳細については、「Creating an API Client」を参照してください。

クライアント ID とクライアントパスワードの作成時には、次の範囲を選択してください。

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read

- profile
- private-intel
- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (アクセス権がある場合)

ステップ 4 電子メールゲートウェイの **[SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）]** ダイアログボックスのステップ 3 で取得したクライアント ID とクライアントパスワードを入力します。

ステップ 5 [SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）] ダイアログボックスで必要な Cisco SecureX サーバを選択します。

ステップ 6 [認証（Authenticate）] をクリックします。

（注） クライアント ID、クライアントパスワード、および Cisco SecureX サーバを編集する場合は、Cisco SecureX リボンを右クリックして詳細を追加します。

次のタスク

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （406 ページ）

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加

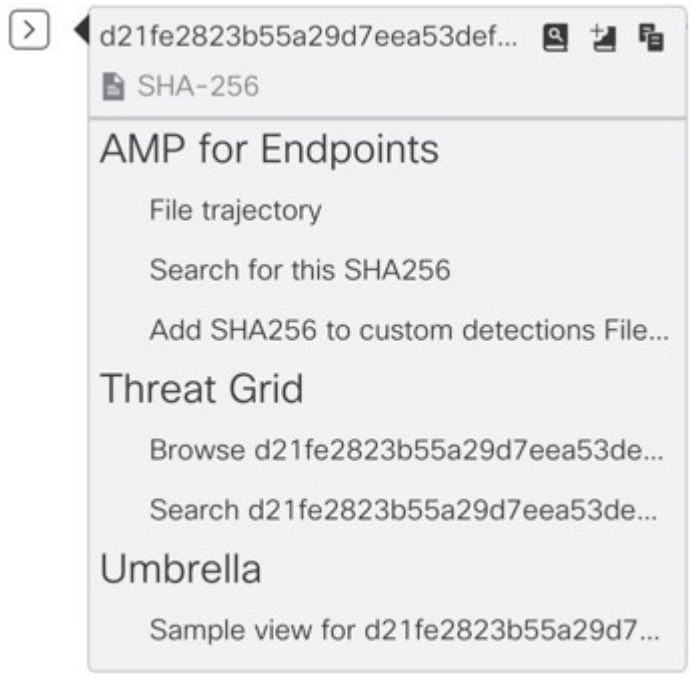
始める前に

電子メールゲートウェイの Cisco SecureX Ribbon とピボット メニュー ウィジェットにアクセスするには、クライアント ID とクライアントパスワードを取得します。詳細については、Cisco SecureX Ribbon へのアクセス （405 ページ）を参照してください。

手順

ステップ 1 電子メールゲートウェイの新しい Web インターフェイスにログインします。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス （37 ページ）を参照してください。

ステップ 2 [メールレポート（Email Reporting）] ページへ移動して、該当する観測対象（bit.ly など）の横にあるピボットメニュー ボタンをクリックします。



次の手順を実行します。

- アクティブなケースに観測対象を追加するには、 ボタンをクリックします。
- 新しいケースに観測対象を追加するには、 ボタンをクリックします。

（注） ピボット メニュー ボタンを使用して、ポータルに登録された他のデバイスの観測対象（AMP for Endpoints など）をピボットし、攻撃分析の調査を実行します。

ステップ 3 アイコンにカーソルを合わせ、ボタンをクリックして**ケースブック**を開きます。観測対象が新しいまたは既存のケースに追加されたかどうかを確認します。

ステップ 4 （オプション） ボタンをクリックして、タイトル、説明、またはメモを**ケースブック**に追加します。

（注） 脅威分析の観測対象を検索するには、次の 2 つの方法があります。

- Cisco SecureX の[エンリッチメント（Enrichment）] 検索ボックスをクリックし、観測対象を検索します。
- Cisco SecureX Ribbon 内の [ケースブック（Casebook）] アイコンをクリックし、 フィールドで観測対象を検索します。

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco SecureX Threat Response 内のメッセージに対する修復アクションの実行

Cisco SecureX Threat Response では、電子メールゲートウェイで処理されたメッセージに対して次の修復アクションを調査して適用できるようになりました。

- 削除（Delete）
- 転送（Forward）
- 転送と削除（Forward and Delete）

始める前に

Cisco SecureX Threat Response のメッセージに対して修復アクションを実行する前に、次の前提条件を満たしていることを確認します。

- Cisco SecureX サーバで電子メールゲートウェイを有効にし、登録した。詳細については、電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （398 ページ）を参照してください。
- 電子メール ゲートウェイ モジュールを Cisco SecureX に追加し、Cisco SecureX で修復転送アドレスを指定した。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するために必要な Cisco Secure Email Gateway モジュールを選択し、[新しいモジュールの追加（Add New Module）] をクリックして、そのページに記載されている手順を参照してください。
- 電子メールゲートウェイの [システム管理（System Administration）] > [アカウント設定（Account Settings）] ページで修復プロファイルを有効にして設定します。詳細については、メールボックスでのメッセージの修復 （709 ページ）を参照してください。

手順

ステップ 1 クレデンシャルを使用して Cisco SecureX にログインします。

ステップ 2 [調査（Investigate）] パネルで必要な IOC（URL、電子メールメッセージ ID など）を入力して脅威分析の調査を実行し、**[調査（Investigate）]** をクリックします。詳細については、https://visibility.amp.cisco.com/help/investigate で「ヘルプ」セクションの「調査」のトピックを参照してください。

ステップ 3 対応する **[シスコメッセージID（Cisco Message ID）]** または **[電子メールメッセージID（Email MessageID）]** を使用して、調査結果に基づいて必要なメッセージを選択します。詳細については、https://visibility.amp.cisco.com/help/investigate で「ヘルプ」セクションの「調査」のトピックを参照してください。

ステップ 4 [シスコメッセージID（Cisco Message ID）] または [電子メールメッセージID（Email MessageID）] の横にあるピボットメニュー ボタンをクリックし、必要な修復アクション（[転送（Forward）] など）を選択します。詳細については、https://visibility.amp.cisco.com/help/investigate で「ヘルプ」セクションの「調査」のトピックを参照してください

Cisco Success Network を使用した電子メールゲートウェイのユーザエクスペリエンスの向上

概要

Cisco Success Network（CSN）機能を使用して、電子メールゲートウェイや機能の使用状況の詳細をシスコに送信できます。これらの詳細情報は、電子メールゲートウェイのバージョンと、電子メールゲートウェイでアクティブになっているが有効になっていない機能を識別するために使用されます。

電子メールゲートウェイや機能の使用状況の詳細をシスコに送信する機能により、組織は次のことを行うことができます。

- 収集されたテレメトリデータの分析を実行し、デジタルキャンペーンを使用してユーザに推奨事項を提示することによって、ユーザネットワークでの製品の有効性を向上させます。
- 電子メールゲートウェイの使用により、ユーザエクスペリエンスが向上します。

次の表に、シスコに送信される電子メールゲートウェイと機能の使用状況の詳細情報のサンプルデータを示します。

統計情報	サンプルデータ
電子メールゲートウェイの詳細	
UID	4215XXXXXXXXXXXXXXX-XXXXXXXXXXX
モデル	C100V

統計情報	サンプルデータ
sIVAN	電子メールゲートウェイ（スマートライセンスの場合）または null（クラシックライセンスの場合）
配置	クラスタ/スタンドアロン
userAccountID	SLPIID（スマートライセンスの場合）または VLNID（クラシックライセンスの場合）を入力します。
バージョン（Version）	1X.X.X-XXX
インストール日	1582535814000（エポックからミリ秒単位）
機能情報	
名前	電子メールゲートウェイ機能
イネーブル	Yes
ステータス	コンプライアンス
有効期限日	1831591683（エポックからの秒数）
機能 ID	a4deXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

関連項目

- 電子メールゲートウェイでの CSN での有効化 （410 ページ）
- 電子メールゲートウェイでの CSN の無効化 （411 ページ）

電子メールゲートウェイでの CSN での有効化

始める前に

電子メールゲートウェイが Cisco Cloud Service ポータルに登録され、有効になっていることを確認します。詳細については、電子メールゲートウェイと Cisco SecureX Threat Response の統合方法 （398 ページ）を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [グローバル設定の編集（Edit Global Settings）] をクリックします。

ステップ 3 をオンにします。[Cisco Success Network] の下にある [有効化（Enable）] チェックボックス。

ステップ 4 変更を送信し、保存します。

電子メールゲートウェイでの CSN の無効化

手順

ステップ 1 [セキュリティサービス（Security Services）]>[クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [グローバル設定の編集（Edit Global Settings）] をクリックします。

ステップ 3 [Cisco Success Network] の下にある [有効化（Enable）] チェックボックスをオフにします。

ステップ 4 変更を送信し、保存します。

第 15 章

メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定

この章は、次の項で構成されています。

- 概要 （413 ページ）
- メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定方法 （414 ページ）
- 電子メール ゲートウェイで Safe Print 設定を構成 （414 ページ）
- メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタの設定 （416 ページ）
- 受信メール ポリシーへのコンテンツ フィルタのアタッチ （420 ページ）
- Safe Print の設定とクラスタ （420 ページ）
- Safe Print で出力された添付ファイル付きメッセージのモニタリング （420 ページ）
- ログの表示 （421 ページ）
- メッセージトラッキングでの Safe Print 詳細の表示 （422 ページ）

概要

悪意のあるまたは疑わしいと検出されたメッセージの添付ファイルの安全なビュー（Safe Print で出力される PDF バージョン）を提供するように電子メール ゲートウェイを構成できます。メッセージの添付ファイルの安全なビューがエンド ユーザに配信され、元の添付ファイルはメッセージから削除されます。「Safe Print」コンテンツ フィルタ アクションを使用すると、設定されたコンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力できます。

電子メールゲートウェイでメッセージの添付ファイルを Safe Print で出力する機能は、組織が次のことを行うのに役立ちます。

- 悪意のあるコンテンツや疑わしいコンテンツを含むメッセージの添付ファイルが組織のネットワークに侵入するのを防ぎます。

- 悪意のあるメッセージや疑わしいメッセージの添付ファイルをマルウェアの影響を受けずに表示します。
- エンドユーザの要求に応じて元のメッセージ添付ファイルを配信します。

Safe-Print機能では、英語、イタリア語、ポルトガル語、スペイン語、ドイツ語、フランス語、日本語、中国語（PRC および台湾）、ロシア語および韓国語がサポートされています。

メッセージの添付ファイルを Safe Print で出力する場合の電子メール ゲートウェイの設定方法

手順	操作手順	詳細情報
ステップ 1	電子メール ゲートウェイで Safe Print の設定値を設定します。	電子メール ゲートウェイで Safe Print 設定を構成（414 ページ）
ステップ 2	メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタを設定します。	メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタの設定（416 ページ）
ステップ 3	メッセージの添付ファイルを Safe Print で出力するために設定したコンテンツ フィルタを受信メール ポリシーにアタッチします。	受信メール ポリシーへのコンテンツ フィルタのアタッチ（420 ページ）

電子メール ゲートウェイで Safe Print 設定を構成

手順

ステップ 1 [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] をクリックします。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 以下の表に記載される必須パラメータを入力して、電子メール ゲートウェイに Safe Print 設定を構成します。

パラメータ ソースの詳細	説明
Safe Print の設定	

パラメータ ソースの詳細	説明
最大ファイル サイズ（Maximum File Size）	Safe Print で出力される添付ファイルの最大添付ファイル サイズを入力します。 （注） [最大ファイルサイズ（Maximum File Size）] の値が、[スキャン動作（Scan Behavior）] > [グローバル設定（Global Settings）] ページで設定されている [スキャンする最大添付ファイルサイズ（Maximum attachment size to scan）] の値を超えていないことを確認します。 （注） [最大ファイルサイズ（Maximum File Size）] 値が電子メール ゲートウェイの [アウトブレイクフィルタ（Outbreak Filters）] に設定した [スキャンする最大メッセージサイズ（Maximum Message Size to Scan）] 値を超える場合、メッセージとメッセージ添付ファイルは電子メール パイプラインのアウトブレイク フィルタではスキャンされません。
最大ページ数（Maximum Page Count）	メッセージの添付ファイルで Safe Print を使用して出力するページの最大数を入力します。
ドキュメントの品質（Document Quality）	Safe Print で出力される添付ファイルに推奨されるイメージ品質値を使用するには、[デフォルト値（70）の使用（Use Default Value (70)）] オプションを選択します。 （注） [カスタム値の入力（Enter Custom Value）] オプションを選択して、Safe Print で出力される添付ファイルのカスタム イメージ品質値を入力することもできます。
ファイルタイプの選択（File Type Selection）	メッセージの添付ファイルを Safe Print で出力する場合に使用可能なファイル グループ（「Microsoft Documents」など）から必要なファイル タイプを選択します。
Watermark	Safe Print で出力される添付ファイルに Watermark を追加するには、[有効（Enabled）] オプションを選択します。 （注） [カスタムテキストの入力（Enter Custom Text）] フィールドに Watermark のカスタム テキストを入力します。

パラメータ ソースの詳細	説明
カバーページ（Cover Page）	Safe Print で出力される添付ファイルにカバー ページを追加するには、[有効（Enabled）] オプションを選択します。 （注） [カスタムテキストの入力（Enter Custom Text）] フィールドにカバー ページのカスタム テキストを入力します。

ステップ 4 変更を送信し、保存します。

次のタスク

メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタを設定します。詳細については、メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタの設定 （416 ページ）を参照してください。

メッセージの添付ファイルを Safe Print で出力するためのコンテンツ フィルタの設定

「Safe Print」コンテンツ フィルタ アクションを使用して、メッセージの添付ファイルを Safe Print で出力

Safe Print コンテンツ フィルタ アクションは、次のいずれかの方法で使用できます。

- [一致する添付ファイルをSafe Printで出力（Safe print matching attachments）] オプション
- [すべての添付ファイルをSafe Printで出力（Safe print all attachments）] オプション

表 *37*:

Safe Print アクション オプション	使用方法	例	サポートされるコンテンツ フィルタ条件
一致する添付ファイルをSafe Printで出力（Safe print matching attachments）	[一致する添付ファイルをSafe Printで出力（Safe print matching attachments）] オプションを使用すると、設定されたコンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力します。	[マクロ検出（Macro Detection）] コンテンツ フィルタ条件を設定し、[一致する添付ファイルをSafe Printで出力（Safe print matching attachments）] オプションを選択します。 受信メッセージに 3 つのメッセージ添付ファイル「docx1」、「docx2」、および「docx3」が含まれ、電子メールゲートウェイによって「docx1」でマクロが検出された場合は、「docx1」のみが Safe Print で出力されます。	次に、[一致する添付ファイルをSafe Printで出力（Safe print matching attachments）] オプションでのみ使用できるコンテンツ フィルタ条件を示します。 • URL レピュテーション • URL Category • マクロ検出 • 添付ファイルの内容 • 添付ファイルのファイル情報

Safe Print アクション オプション	使用方法	例	サポートされるコンテンツ フィルタ条件
すべての添付ファイルをSafe Printで出力（Safe print all attachments）	[すべての添付ファイルをSafe Printで出力（Safe print all attachments）] オプションを使用すると、設定されたコンテンツ フィルタ条件が true の場合にすべてのメッセージの添付ファイルを Safe Print で出力します。	[エンベロープ送信者（Envelope Sender）] コンテンツ フィルタ条件を設定し、[すべての添付ファイルをSafe Printで出力（Safe print all attachments）] オプションを選択します。 送信者「user1@example.com」からの受信メッセージに 3 つのメッセージ添付ファイル「docx1」、「docx2」、および「ppt1」が含まれている場合、すべてのメッセージ添付ファイル「docx1」、「docx2」、および「ppt1」が以下の条件に基づいて Safe Print で出力されます。 • [スキャン動作（Scan Behavior）] > [Safe Printの設定（Safe Print Settings）] ページで選択されたファイル タイプ。 • 送信者 user1@example.com は、[エンベロープ送信者（Envelope Sender）] コンテンツ フィルタ条件で設定された LDAP グループ ディレクトリに一致します。	[すべての添付ファイルをSafe Printで出力（Safe print all attachments）] オプションを設定した電子メールゲートウェイで使用可能なコンテンツ フィルタ条件であればどれでも使用できます。

たとえば、[マクロ検出（Macro Detection）] 条件および「Safe Print」アクションを使用して、マクロを含むメッセージ添付ファイルを Safe Print で出力するには、次の手順を実行します。

始める前に

電子メール ゲートウェイで Safe Print 設定を構成したことを確認します。電子メール ゲートウェイで Safe Print 設定を構成 （414 ページ）を参照してください

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [マクロ検出（Macro Detection）] をクリックします。

ステップ 6 電子メール ゲートウェイでマクロを検出するファイル タイプを選択して、[追加（Add）] をクリックします。

ステップ 7 [OK] をクリックします。

ステップ 8 [アクションを追加（Add Action）] をクリックします。

ステップ 9 [Safe Print] をクリックします。

ステップ 10 メッセージの添付ファイルに対して実行するアクションは、次のいずれかを選択します。

- [一致する添付ファイルをSafe Printで出力（Safe print matching attachments）] オプションを選択すると、設定された [マクロ検出（Macro Detection）] コンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力します。
- [すべての添付ファイルをSafe Printで出力（Safe print all attachments）] オプションを選択すると、設定された [マクロ検出（Macro Detection）] コンテンツ フィルタ条件が true の場合に、すべてのメッセージの添付ファイルを Safe Print で出力します。

ステップ 11 [はい（Yes）] を選択して、スキャン不可とマークされているメッセージの添付ファイルを削除します。

メッセージの添付ファイルは、次のいずれかの理由により、スキャン不可とマークされます。

- メッセージに暗号化された添付ファイルが含まれている。
- メッセージに破損した添付ファイルが含まれている。
- メッセージの添付ファイルに対して Safe Print アクションを実行したときに I/O エラーが発生する。
- メッセージの添付ファイルに対して Safe Print アクションを実行したときにタイムアウト エラーが発生する。

（注） デフォルトでは、添付ファイルがスキャンできない場合、システム生成のメッセージが添付テキストファイルとして追加されます。[カスタム差し替えメッセージ（Custom Replacement Message）] フィールドにカスタム メッセージを入力します。

ステップ 12 [OK] をクリックします。

ステップ 13 変更を送信し、保存します。

受信メールポリシーへのコンテンツフィルタのアタッチ

メッセージの添付ファイルを Safe Print で出力するために設定したコンテンツ フィルタを受信メール ポリシーにアタッチできます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 2 コンテンツ フィルタの下のリンクをクリックします。

ステップ 3 [コンテンツフィルタを有効にする（カスタマイズ設定）（Enable Content Filters (Customize Settings)）] を確実に選択します。

ステップ 4 メッセージの添付ファイルを Safe Print で出力するために作成したコンテンツ フィルタを選択します。

ステップ 5 変更を送信し、保存します。

Safe Print の設定とクラスタ

中央管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、電子メールゲートウェイとメールポリシーで Safe Print を設定できます。

Safe Print で出力された添付ファイル付きメッセージのモニタリング

[Safe Print] レポート ページを使用して、次の内容を表示できます。

- ファイル タイプ別の、Safe Print で出力された添付ファイルの数（グラフ形式）。
- ファイル タイプ別の、Safe Print で出力された添付ファイルの概要（表形式）。

[Safe Printで出力されたファイル種類の概要（Summary of Safe Print File Types）] セクションで Safe Print で出力された添付ファイルの合計数をクリックすると、[メッセージトラッキング（Message Tracking）] にメッセージの詳細が表示されます。

ログの表示

Safe Print に関するログ情報はメールログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

Safe Print ログエントリの例

Safe Print に関する情報はメールログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

- 入出力エラー
  - 一時ディレクトリを作成できない （421 ページ）
  - Safe Print 対象の PDF 添付ファイルを作成できない （421 ページ）
- 破損ファイル （422 ページ）
- 暗号化ファイル （422 ページ）
- タイムアウトエラー （422 ページ）

一時ディレクトリを作成できない

この例では、電子メールゲートウェイがファイルを保存するための一時ディレクトリを作成できなかったため、メッセージの添付ファイルが Safe Print で出力されなかったことがログに示されます。

```
Sat Jul 20 05:53:48 2019 Info: MID 5 Unable to safe print the attachment,
Filename:test_file.docx, Reason: IO error occurred during safeprinting of the attachment
Sat Jul 20 05:53:48 2019 Trace: MID 5 Unable to safe print the attachment,
Filename:test_file.docx, Exception: Unable to create tmp directory for safeprinting
document:
[Errno 2] No such file or directory: '/tmp/test_file.docx'
```

Safe Print 対象の PDF 添付ファイルを作成できない

この例では、電子メールゲートウェイが Safe Print 対象の PDF 添付ファイルを作成できなかったため、メッセージの添付ファイルが Safe Print で出力されなかったことがログに示されています。

```
Thu Jul 11 07:19:01 2019 Info: MID 132 Unable to safe print the attachment,
Filename:test_file.docx, Reason: IO error occurred during safeprinting of the attachment
Thu Jul 11 07:19:01 2019 Trace: MID 132 Unable to safe print the attachment,
Filename:test_file.docx, Exception: Error while creating safeprinted PDF document:
[Errno 2] No such file or directory: '/tmp/test_file.docx/safe_print_test_file.pdf'
```

破損ファイル

この例では、ファイルが破損したため、メッセージの添付ファイルが Safe Print で出力されなかったことがログに示されています。

```
Thu Jul 11 08:34:31 2019 Info: MID 142 Unable to safe print the attachment,
Filename:corrupt_file=20(1).docx, Reason: The attachment is corrupted
```

暗号化ファイル

この例では、ファイルが暗号化されたため、メッセージの添付ファイルが Safe Print に出力されなかったことがログに示されています。

```
Thu Jul 11 08:34:31 2019 Info: MID 142 Unable to safe print the attachment,
Filename:sept_subscription.pdf, Reason: The attachment is encrypted.
```

タイムアウトエラー

この例では、タイムアウトエラーにより、メッセージの添付ファイルが SafePrint で出力されなかったことがログに示されています。

```
Thu Jul 11 10:32:29 2019 Info: MID 165 Unable to safe print the attachment,
Filename:20_page.docx, Reason: A timeout error occurred when trying to safe print the
attachment
```

メッセージトラッキングでの Safe Print 詳細の表示

メッセージトラッキングを使用して、Safe Print で出力された添付ファイルを含むメッセージの詳細を表示します。

始める前に

- E メール ゲートウェイでメッセージ トラッキング機能が有効にされていることを確認します。メッセージトラッキングを有効にするには、電子メールゲートウェイのレガシー Web インターフェイスで **[セキュリティサービス（Security Services）] > [メッセージトラッキング（Message Tracking）]** ページに移動します。
- メッセージの添付ファイルを Safe Print で出力するためのコンテンツフィルタが設定されている必要があります。

手順

ステップ 1 （新しい Web インターフェイスのみ）[トラッキング（Tracking）] > [メッセージトラッキング（Message Tracking）] に移動します。

または

（レガシー Web インターフェイスのみ）[モニタ（Monitor）] > [メッセージトラッキング（Message Tracking）] に移動します。

ステップ 2 （新しい Web インターフェイスのみ） [詳細検索（Advanced Search）] をクリックします。
または
（レガシー Web インターフェイスのみ）[詳細（Advanced）] をクリックします。

ステップ 3 Safe Print に出力された添付ファイルを含むメッセージの詳細を表示するには、[メッセージイベント（Message Event）] で [Safe Print] チェックボックスをオンにします。

ステップ 4 必要な検索オプションを入力して [Search（検索）] をクリックします。

第 16 章

電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合

この章は、次の項で構成されています。

- 概要 （425 ページ）
- 電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合方法 （426 ページ）
- Cisco Secure Awareness クラウドサービスアカウントの作成 （427 ページ）
- Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 （428 ページ）
- 電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成 （429 ページ）
- Cisco Secure Awareness クラウドサービスからの認証トークンの取得 （430 ページ）
- 電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化 （431 ページ）
- リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成 （432 ページ）
- Cisco Secure Awareness クラウドサービスとクラスタ （433 ページ）
- ログの表示 （433 ページ）
- アラートの表示 （435 ページ）

概要

Cisco Secure Awareness クラウドサービスを使用すると、フィッシング シミュレーション、意識向上トレーニング、またはその両方を効果的に展開して、結果を測定およびレポートできます。これにより、セキュリティ運用チームは、エンドユーザの状況緩和ではなく、リアルタイムの脅威に集中できます。

Cisco Secure Awareness クラウドサービスは、リピートクリッカー（任意の URL またはメッセージ内の添付ファイルを繰り返しクリックするユーザ）のレポートを提供します。これらのユーザは、Cisco Secure Awareness クラウドサービスによって定義されたフィッシング シミュレーション キャンペーンによって識別されます。

Cisco Secure Awareness クラウドサービスの詳細については、https://secat.cisco.com を参照してください。

電子メールゲートウェイと Cisco Secure Awareness クラウドサービスを統合することで、次のことが可能になります。

- 実際のフィッシング攻撃に対するエンドユーザの認識が向上します。
- 電子メール管理者は、リピートクリッカーと識別されたエンドユーザに対して厳格なポリシーを設定できます。

電子メールゲートウェイと Cisco Secure Awareness クラウドサービスの統合方法

次の手順を順番に実行します。

手順	操作手順	詳細情報
ステップ 1	（Cisco Secure Awareness で）地域に基づいて、組織の Cisco Security Awareness クラウドサービスアカウントを作成します。	Cisco Secure Awareness クラウドサービスアカウントの作成（427 ページ）
ステップ 2	電子メールゲートウェイが Cisco Secure Awareness クラウドサービスにアクセスできるようにファイアウォールを設定します。	Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 （428 ページ）
ステップ 3	電子メールゲートウェイで Cisco Secure Awareness クラウドサービスからのフィッシングメッセージをシミュレートできるように、新しい送信者グループを作成します。	電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成 （429 ページ）
ステップ 4	（Cisco Secure Awareness で）Cisco Secure Awareness クラウドサービスの新しいユーザを作成し、リピートクリッカーを識別します。 ：	次の URL にある 『CSA Administrator Guide』を参照してください。 • https://secat.cisco.com/portal/Support（米国のユーザに適用） • https://secat-eu.cisco.com/portal/Support（欧州連合（EU）のユーザに適用）

手順	操作手順	詳細情報
ステップ 5	（Cisco Secure Awareness で）Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内のエンドユーザに送信します。このプロセスは、メッセージ内の添付ファイルまたはURLを繰り返しクリックするエンドユーザを追跡するために使用されます。	次の URL にある『CSA Administrator Guide』を参照してください。 • https://secat.cisco.com/portal/Support（米国のユーザに適用） • https://secat-eu.cisco.com/portal/Support（欧州連合（EU）のユーザに適用）
ステップ 6	Cisco Secure Awareness クラウドサービスから認証トークンを取得します。	Cisco Secure Awareness クラウドサービスからの認証トークンの取得 （430 ページ）
ステップ 7	電子メールゲートウェイで Cisco Secure Awareness クラウドサービスを有効にします。	電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化（431 ページ）
ステップ 8	カスタム着信メールポリシーを作成して、リピートクリッカーとして分類されるエンドユーザのアグレッシブメールポリシーを設定します。	リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成 （432 ページ）

Cisco Secure Awareness クラウドサービスアカウントの作成

地域に応じて、次のいずれかのURLを使用して、組織の管理者権限を持つCisco Secure Awareness クラウドサービスアカウントを作成します。

- https://secat.cisco.com（アメリカ地域のユーザに適用）
- https://secat-eu.cisco.com（欧州連合（EU）のユーザに適用）

次のタスク

電子メールゲートウェイが Cisco Secure Awareness クラウドサービスに接続できるようにファイアウォールを設定します。詳細については、「Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成 （428 ページ）」を参照してください。

Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成

電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります（以下の表を参照）。

サービス	アメリカ地域		欧州連合	
	ホスト名（Hostname）	IP アドレス（IP Address）	ホスト名（Hostname）	IP アドレス（IP Address）
Cisco Secure Awareness クラウドサービス	secat.cisco.com	52.242.31.199	secat-eu.cisco.com	40.127.163.97
コース通知（アウトバウンド）	-	167.89.98.161	-	40.127.163.97
ランディングページとフィードバックページ（アウトバウンド）	-	52.242.31.199	-	
電子メール添付ファイル（アウトバウンド）	-		-	

（注） 上記の表に記載されている IP アドレスは変更される場合があります。IP アドレスの最新のリストについては、Cisco Secure Awareness クラウドサービスの「IP Allowlist Guide」https://secat.cisco.com/portal/Support/IpWhitelistingGuide を参照してください

次のタスク

電子メールゲートウェイで Cisco Secure Awareness クラウドサービスからのフィッシングメッセージをシミュレートできるように、新しい送信者グループを作成します。詳細については、「電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成 （429 ページ）」を参照してください。

電子メールゲートウェイでシミュレートされたフィッシングメッセージを許可する送信者グループの作成

電子メールゲートウェイで Cisco Secure Awareness クラウドサービスからのフィッシングメッセージをシミュレートできるように、新しい送信者グループを作成する必要があります。

始める前に

電子メールゲートウェイが Cisco Secure Awareness クラウドサービスにアクセスできるようにファイアウォールが設定されていることを確認します。詳細については、Cisco Secure Awareness クラウドサービスにアクセスするためのファイアウォール設定の構成（428 ページ）を参照してください。

手順

ステップ 1 **[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）]** の順にクリックします。

ステップ 2 [送信者グループを追加（Add Sender Group）] をクリックします。

ステップ 3 送信者グループの名前を入力します。

ステップ 4 優先順位を **1** に選択します。

ステップ 5 **CYBERSEC_AWARENESS_ALLOWED** としてポリシーを選択します。

ステップ 6 **[SBRSを未使用にする（SBRS to Not in Use）]** チェックボックスをオンにして、IP レピュテーション フィルタリングを無効にします。

ステップ 7 **[送信者を送信して追加（Submit and Add Senders）]** をクリックします。

ステップ 8 次の Cisco Secure Awareness クラウドサービスの IP アドレスのいずれかを追加して、地域に基づく送信元 IP アドレスとして設定します。

- アメリカ地域 - 207.200.3.14 または 173.244.184.143
- 欧州連合（EU）- 77.32.150.153

（注） Cisco Secure Awareness クラウドサービスの IP アドレスは、電子メールゲートウェイがシミュレートされたフィッシングメッセージを実際のフィッシングとして解釈しないようにするために使用されます。

ステップ 9 変更を送信し、保存します。

次のタスク

1. Cisco Secure Awareness クラウドサービスで新しいユーザを作成し、リピートクリッカーを識別します。

2. Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内のエンドユーザに送信します。

   上記の2つのタスクを完了する方法の詳細については、次のURLにある『CSA Administrator Guide』を参照してください：

   - https://secat.cisco.com/portal/Support（米国のユーザに適用）
   - https://secat-eu.cisco.com/portal/Support（欧州連合（EU）のユーザに適用）

3. Cisco Secure Awareness クラウドサービスから認証トークンを取得し、Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードします。詳細については、「Cisco Secure Awareness クラウドサービスからの認証トークンの取得 （430ページ）」を参照してください。

Cisco Secure Awareness クラウドサービスからの認証トークンの取得

Cisco Secure Awareness クラウドサービスから認証トークンを取得し、それを使用して Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードする必要があります。

始める前に

管理者権限を持つ Cisco Secure Awareness クラウドサービスのアカウントがあることを確認します。詳細については、Cisco Secure Awareness クラウドサービスアカウントの作成 （427ページ）を参照してください。Cisco Secure Awareness クラウドサービスにアクセスできない場合は、Cisco サポートにお問い合わせください。

手順

ステップ 1 Cisco Secure Awareness クラウドサービスにログインします。

ステップ 2 [環境（Environment）] > [設定（Settings）] に移動します

ステップ 3 [レポートAPI（Reports API）] タブをクリックします。

ステップ 4 **[レポートAPIを有効にする（Enable Report API）]** チェックボックスをオンにします。

ステップ 5 認証トークンをコピーします。

この認証トークンを使用して、Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードします。

次のタスク

電子メールゲートウェイで Cisco Secure Awareness クラウドサービスを有効にします。詳細については、「電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化（431 ページ）」を参照してください。

電子メールゲートウェイでの Cisco Secure Awareness クラウドサービスの有効化

始める前に

次のように設定されていることを確認します。

- 管理者権限を持つ Cisco Secure Awareness クラウドサービスの有効なアカウント。
- Cisco Secure Awareness クラウドサービスから有効な認証トークンを取得しました。詳細については、Cisco Secure Awareness クラウドサービスからの認証トークンの取得（430 ページ）を参照してください。

手順

ステップ 1 **[セキュリティサービス（Security Services）] > [Cisco Secure Awareness]** に移動します。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 **[Cisco Security Awarenessの有効化（Enable Cisco Secure Awareness）]** チェックボックスをオンにします。

ステップ 4 必要なサーバを選択して、電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続します。

ステップ 5 Cisco Secure Awareness クラウドサービスから取得した認証トークンを入力します。

ステップ 6 （任意）Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードするためのポーリング間隔を入力します。

ステップ 7 変更を送信し、保存します。

次のタスク

- Cisco Secure Awareness クラウドサービスを有効にすると、電子メールゲートウェイは Cisco Secure Awareness クラウドサービスからリピートクリッカーリストを自動的にダウンロードします。電子メールゲートウェイの Web インターフェイスで **[セキュリティサービス（Security Services）] > [Cisco Secure Awareness] > [リピートクリッカーリストの設定（Repeat Clickers List Settings）]** セクションに移動すると、リピートクリッカーリストのリピートクリッカーユーザの数を表示できます。リピートクリッカーリストの詳細については、Cisco Secure Awareness クラウドサービスにログインし、[分析（Analytics）] > [標準

レポート（Standard Reports）] > [フィッシングシミュレーション（Phishing Simulations）] > [リピートクリッカー（Repeat Clickers）] セクションに移動します。

- カスタム着信メールポリシーを作成して、リピートクリッカーとして分類されるエンドユーザのアグレッシブメールポリシーを設定します。詳細については、「リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成（432ページ）」を参照してください。
- Cisco Secure Email Submission Add-In は、Cisco Secure Awareness（CSA）クラウドサービスポータルを介して送信されるシミュレートされたフィッシングメッセージの送信をサポートするようになりました。Secure Email Submission Add-In 自体を使用して、シミュレートされたフィッシングメッセージを送信できるようになりました。詳細については、『Cisco Secure Email Submission Add-In ユーザーガイド』を参照してください。

リピートクリッカーとして分類されたエンドユーザのカスタム着信メールポリシーの作成

リピートクリッカーとして分類されるエンドユーザのアグレッシブメールポリシーを設定するには、カスタム着信メールポリシーを作成する必要があります。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 ポリシーの名前を入力します。

ステップ 4 **[ユーザの追加（Add User）]** をオンにします。

ステップ 5 **[次の受信者（Following Recipients）]** を選択します。

ステップ 6 **[リピートクリッカーリストを含める（Include Repeat Clicker List）]** チェックボックスをオンにして、Cisco Secure Awareness クラウドサービスによってリピートクリッカーとして分類された受信者のリストを含めます。

ステップ 7 [OK] をクリックします。

ステップ 8 **[送信（Submit）]** をクリックします。

ステップ 9 メールポリシーに必要なサービスエンジン（アンチウイルス、グレイメールなど）を設定します。

ステップ 10 変更を保存します。

Cisco Secure Awareness クラウドサービスとクラスタ

一元管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、Cisco Secure Awareness クラウドサービスを有効化できます。スタンドアロンモードで Cisco Secure Awareness クラウドサービスを使用して電子メールゲートウェイを有効にしている場合は、Cisco Secure Awareness クラウドサービスに登録されているクラスタに参加することを選択できます。

（注） マシンレベルで Cisco Secure Awareness クラウドサービスを無効にすると、ログインした電子メールゲートウェイに対してのみ無効になり、クラスタ内の他のマシンはまだ Cisco Secure Awareness クラウドサービスに接続されています。

ログの表示

Cisco Secure Awareness クラウドサービスの情報はメールログに記録されます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

Cisco Secure Awareness ログエントリの例：

- この例では、無効なトークンが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an invalid token.
```

解決策：Cisco Secure Awareness クラウドサービスから有効な認証トークンを取得してください。

- この例では、接続エラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of a connection error.
```

解決策：電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続するために使用するファイアウォール設定を確認します。

- この例では、内部サーバエラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
of an internal server error.
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

- この例では、SSL 証明書の検証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed because
the SSL certificate verification failed.
```

解決策：必要なプロキシサーバの CA 証明書を電子メールゲートウェイのカスタム認証局リストに追加します。

- この例では、プロキシ認証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Secure Awareness cloud service failed
because the proxy authentication failed.
```

解決策：電子メールゲートウェイでプロキシサーバが正しい認証ログイン情報を使用して設定されているかどうかを確認します。

- この例では、Cisco Secure Awareness クラウドサービスでレポート API が有効になっていなかったことが原因で、Cisco Secure Awareness クラウドサービスへの要求が失敗したことがログに示されています。

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

解決策：Cisco Secure Awareness クラウドサービスの [環境（Environment）] > [設定（Settings）] > [レポートAPI（Report API）] タブで [レポートAPIを有効にする（Enable Report API）] チェックボックスをオンにします。

- この例では、Cisco Secure Awareness 機能が特定の日付で期限切れになることがログに示されています。

```
2020-10-15 08:00:11,968 INFO csa The Cisco Secure
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、Cisco Secure Awareness 機能のライセンスの有効期限が切れており、電子メールゲートウェイでこの機能が無効になっていることがログに示されています。

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Secure
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、ダウンロードされたリピートクリッカーリストが空であることがログに示されています。

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

解決策：Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内の受信者に送信します。

- この例では、ダウンロード試行の最大数に達したため、Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Secure Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

解決策：Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードする試行回数を増やすには、シスコサポートに連絡してください。

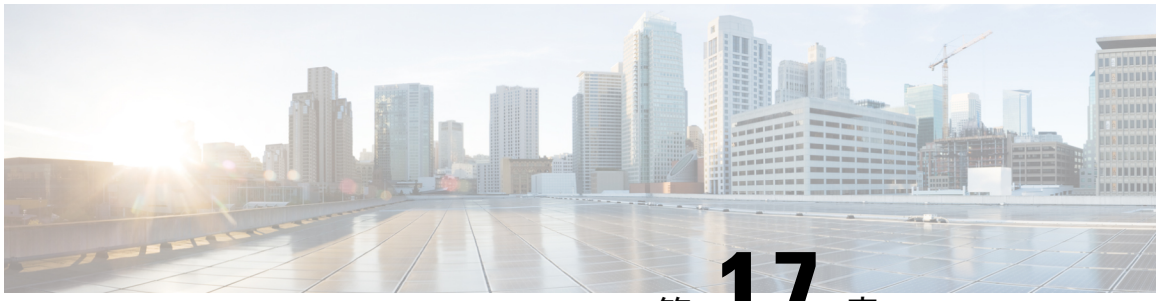
アラートの表示

以下の表では、Cisco Secure Awareness クラウドサービスに対して生成されるアラート、アラートの説明、アラートの重大度を記載します。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.CSA.DOWNLOAD_FAILURE	アラートテキスト：Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードに失敗しました。$reason。 アラートレベル：警告（WARNING）。 説明：Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードに失敗するとアラートが送信されます。	パラメータ：reason 理由：Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードできなかった理由。 例：「無効なトークン」、「最大試行回数に達しました」など。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.CSA.EMPTY_ EMAIL_LIST	アラートテキスト：ダウンロードされたリピートクリッカーリストは空です。 アラートレベル：情報（INFO）。 説明：ダウンロードされたリピートクリッカーリストが空の場合にアラートが送信されます。このアラートは、Cisco Secure Awareness クラウドサービスにリピートクリッカーがリストされていないことを示します。	該当なし。
MAIL.CSA.LICENSE_ EXPIRING	アラートテキスト：Cisco Secure Awareness 機能のライセンスは $expiry で期限切れになります。シスコアカウントマネージャに連絡して、ライセンスを更新する必要があります。 リージョン：$region サーバ：$server アラートレベル：情報（INFO） 説明：有効期限の 7 日前、有効期限の 3 日前、および有効期限の 1 日前にアラートが送信されます。	パラメータ：expiry、region、server expiry：Cisco Secure Awareness ライセンスの有効期限が切れる日付。 region：期限が切れる Cisco Secure Awareness ライセンスのリージョン。リージョンは、AMERICAS、EUROPE などです。 server：サーバ URL の名前（例：https://secat.cisco.com）

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.CSA.LICENSE_ EXPIRED	アラートテキスト：Cisco Secure Awareness 機能ライセンスの有効期限が切れており、この機能は電子メールゲートウェイで無効になっています。シスコアカウントマネージャに連絡して、ライセンスを更新してください。 リージョン：$region サーバ：$server アラートレベル：クリティカル（Critical） 説明：Cisco Secure Awareness ライセンスの有効期限が切れるとアラートが送信されます。	パラメータ：region、server region：期限が切れた Cisco Secure Awareness ライセンスのリージョン。リージョンは、AMERICAS、EUROPE などです。 server：サーバ URL の名前（例：https://secat.cisco.com）。
MAIL.CSA.LICENSE_ RETRIVAL_FAILURE	アラートテキスト：Cisco Secure Awareness クラウドサービスからのライセンス有効期限の詳細の取得に失敗しました（$reason） アラートレベル：警告（WARNING） 説明：Cisco Secure Awareness クラウドサービスからライセンスの有効期限の詳細を 3 回連続で取得できなかった場合にアラートが送信されます。ライセンスの有効期限の詳細が正常に取得されるまで、ライセンスの有効期限の詳細の取得が毎日試行されます。	パラメータ：reason reason：Cisco Secure Awareness クラウドサービスからライセンスの有効期限の詳細を取得できなかった理由。 例：「無効なトークン」、「最大試行回数に達しました。」



第 17 章

アンチウイルス

この章は、次の項で構成されています。

- アンチウイルス スキャンの概要 （439 ページ）
- Sophos アンチウイルス フィルタリング （441 ページ）
- McAfee アンチウイルス フィルタリング （444 ページ）
- 電子メールゲートウェイでのウイルスのスキャンの設定方法 （445 ページ）
- アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信（457 ページ）
- ウイルス定義ファイルの更新 （459 ページ）

アンチウイルス スキャンの概要

電子メールゲートウェイには、サードパーティの企業の Sophos および McAfee の統合されたウイルススキャンエンジンが含まれます。電子メールゲートウェイのライセンスキーを取得して、これらのウイルススキャンエンジンのいずれかまたは両方を使用してメッセージのウイルスをスキャンし、どちらかのアンチウイルス スキャン エンジンを使用してウイルスをスキャンするように電子メールゲートウェイを設定できます。

McAfee および Sophos のエンジンには、特定のポイントでのファイルのスキャン、ファイルで発見されたデータとウイルス定義のパターン照合と処理、エミュレーション環境でのウイルスコードの復号および実行、新しいウイルスを認識するための発見的手法の適用、および正規ファイルからの感染コードの削除に必要なプログラム ロジックが含まれています。

（一致する着信または発信メールポリシーに基づいて）メッセージのウイルスをスキャンし、ウイルスが見つかった場合はメッセージに対してさまざまなアクション（たとえば、ウイルスの発見されたメッセージの「修復」、件名ヘッダーの変更、X-Header の追加、代替アドレスまたはメールホストへのメッセージの送信、メッセージのアーカイブ、またはメッセージの削除など）を実行するように電子メールゲートウェイを設定できます。

ウイルススキャンをイネーブルにした場合は、アンチスパムスキャンの直後に、電子メールゲートウェイ上の「ワークキュー」でウイルススキャンが実行されます。（電子メール パイプラインとセキュリティ サービス （73 ページ） を参照。）

デフォルトでは、ウイルス スキャンはデフォルトの着信および発信メール ポリシーに対してイネーブルになります。

関連項目

- 評価キー （440 ページ）
- 複数のアンチウイルス スキャンエンジンによるメッセージのスキャン （440 ページ）

評価キー

電子メールゲートウェイには、使用可能な各アンチウイルス スキャン エンジンに対して 30 日間有効な評価キーが同梱されています。評価キーは、システム セットアップ ウィザードまたは [セキュリティサービス（Security Services）] > [Sophos] または [McAfee ウイルス対策（McAfee Anti-Virus）] ページのライセンス契約書にアクセスするか（GUI）、または `antivirusconfig` または `systemsetup` コマンドを実行して（CLI）有効にします。デフォルトでは、ライセンス契約書に同意すると、アンチウイルス スキャン エンジンはデフォルトの着信および発信メール ポリシーに対してただちにイネーブルになります。30 日間の評価期間後もこの機能を有効にする場合の詳細については、Cisco の営業担当者にお問い合わせください。残りの評価期間は、[システム管理（System Administration）] > [ライセンスキー（Feature Keys）] ページを表示するか、または `featurekey` コマンドを発行することによって確認できます。（詳細については、ライセンス キー （1231 ページ）を参照してください。）

複数のアンチウイルススキャンエンジンによるメッセージのスキャン

AsyncOS は、複数のアンチウイルス スキャン エンジンによるメッセージのスキャン（マルチレイヤ アンチウイルス スキャン）をサポートしています。メールポリシーごとに、ライセンスを受けたアンチウイルス スキャンエンジンのいずれかまたは両方を使用するように電子メールゲートウェイを設定できます。たとえば、経営幹部用のメールポリシーを作成し、そのポリシーでは Sophos および McAfee の両方のエンジンを使用してメールをスキャンするように設定することもできます。

複数のスキャンエンジンでメッセージをスキャンすることにより、Sophos および McAfee のアンチウイルス スキャン エンジン双方の利点を組み合わせた「多重防衛」が実現します。各エンジンともに業界をリードするアンチウイルス捕捉率を誇りますが、各エンジンは別々のテクノロジー基盤（McAfee アンチウイルス フィルタリング （444 ページ）および Sophos アンチウイルス フィルタリング （441 ページ）を参照）に依存してウイルスを検出しているため、マルチスキャン方式を使用することで、より効果が高まります。複数のスキャンエンジンを使用することで、システム スループットが低下する場合があります。詳細は、シスコのサポート担当者にお問い合わせください。

ウイルス スキャンの順序は設定できません。マルチレイヤ アンチウイルス スキャンをイネーブルにした場合、最初に McAfee エンジンによるウイルス スキャンが実行され、次に Sophos エンジンによるウイルス スキャンが実行されます。McAfee エンジンがメッセージはウイルスに感染していないと判断した場合は、Sophos エンジンはさらにメッセージをスキャンして、別の保護層を追加します。McAfee エンジンがメッセージはウイルスを含んでいると判断した場

合は、電子メールゲートウェイは Sophos によるスキャンをスキップし、構成した設定に応じてウイルスメッセージに対してアクションを実行します。

Sophos アンチウイルス フィルタリング

電子メールゲートウェイには、Sophos の総合的なウイルス スキャン テクノロジーが含まれています。Sophos Anti-Virus は、プラットフォーム間のアンチウイルス保護、検出、および除去を提供します。

Sophos Anti-Virus は、ファイルをスキャンしてウイルス、トロイの木馬、およびワームを検出するウイルス検出エンジンを提供します。これらのプログラムは、「悪意のあるソフトウェア」を意味するマルウェアと総称されます。ウイルス対策スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

関連項目

- ウイルス検出エンジン （441 ページ）
- ウイルス スキャン （442 ページ）
- 検出方法 （442 ページ）
- ウイルスの記述 （443 ページ）
- Sophos アラート （443 ページ）
- ウイルスが発見された場合 （443 ページ）

ウイルス検出エンジン

Sophos ウイルス検出エンジンは、Sophos Anti-Virus テクノロジーの中心的役割を担います。このエンジンは、Microsoft の Component Object Model（COM; コンポーネント オブジェクト モデル）と同様の、多くのオブジェクトと明確に定義されたインターフェイスで構成された独自のアーキテクチャを使用します。エンジンで使用されるモジュラ ファイリング システムは、それぞれが異なる「ストレージ クラス」（たとえばファイル タイプなど）を処理する、個別の内蔵型動的ライブラリに基づいています。この方法では、タイプに関係なく汎用のデータ ソースにウイルス スキャン操作を適用できます。

エンジンは、データのロードおよび検索に特化したテクノロジーにより、非常に高速なスキャンを実現できます。次の機能が内蔵されています。

- ポリモーフィック型ウイルスを検出するためのフル コード エミュレータ。
- アーカイブ ファイル内をスキャンするためのオンライン解凍プログラム。
- マクロ ウイルスを検出および駆除するための OLE2 エンジン。

電子メールゲートウェイは、SAV インターフェイスを使用してウイルスエンジンを統合しています。

ウイルス スキャン

大まかにいうと、エンジンのスキャン機能は、検索する場所を特定する分類子と、検索する対象を特定するウイルスデータベースという2つの重要なコンポーネントの高性能な組み合わせにより管理されています。エンジンは、識別子に依存せずに、タイプでファイルを分類します。

ウイルスエンジンは、システムが受信したメッセージの本文および添付ファイルでウイルスを検索しますが、スキャンの実行方法の決定には、添付ファイルのタイプが役立ちます。たとえば、メッセージの添付ファイルが実行ファイルであれば、エンジンは実行コードの開始場所が記述されているヘッダーを調べて、その場所を検索します。ファイルが Word ドキュメントであれば、エンジンはマクロ ストリームを調べます。MIME ファイル（メール メッセージに使用される形式）であれば、添付ファイルが保存されている場所を調べます。

検出方法

ウイルスの検出方法は、ウイルスのタイプに応じて異なります。スキャン処理中に、エンジンは各ファイルを分析してタイプを特定してから、該当する手法を適用します。すべての方法の根幹には、特定のタイプの命令または特定の命令の順序を検索するという基本概念があります。

関連項目

- パターン照合 （442 ページ）
- 発見的手法 （442 ページ）
- エミュレーション （443 ページ）

パターン照合

パターン照合の手法では、エンジンは特定のコードシーケンスを知っており、そのコードシーケンスと完全一致するコードをウイルスとして特定します。たいていの場合、エンジンは既知のウイルス コードのシーケンスに類似した（必ずしも完全に同一である必要はありません）コードのシーケンスを検索します。スキャン実行中にファイルを比較する対象となる記述を作成する際、Sophos のウイルス研究者達は、エンジンが（次で説明する発見的手法を使用して）オリジナルのウイルスだけでなく、後の派生的なウイルスも発見できるように、識別コードを可能な限り一般的なものに維持することに努めています。

発見的手法

ウイルスエンジンは、基本的なパターン照合手法と発見的手法（特定のルールではなく一般的なルールを使用する手法）を組み合わせることで、Sophos の研究者があるファミリの1種類のウイルスしか分析していなかったとしても、そのファミリの複数のウイルスを検出できます。この手法では、記述を1つ作成すれば、ウイルスの複数の派生形を捕らえることができます。Sophos は、発見的手法にその他の手法を加味することで、false positive の発生を最低限に抑えています。

エミュレーション

エミュレーションは、ポリモーフィック型ウイルスに対して、ウイルスエンジンによって適用される手法です。ポリモーフィック型ウイルスは、ウイルスを隠す目的のために、ウイルス自体を別の形に変更する暗号化されたウイルスです。明らかな定型的ウイルス コードは存在せず、拡散するたびにウイルス自体が別の形に暗号化されます。このウイルスは、実行されたときに自己復号します。ウイルス検出エンジンのエミュレータは、DOS または Windows 実行ファイルに使用されますが、ポリモーフィック型マクロは Sophos のウイルス記述言語で記述された検出コードによって発見されます。

この復号の出力は実際のウイルス コードであり、エミュレータで実行された後に Sophos のウイルス検出エンジンによって検出されるのは、この出力です。

スキャン用にエンジンに送信された実行ファイルは、エミュレータ内で実行されます。エミュレータでは、ウイルス本文の復号がメモリに書き込まれ、これに応じて復号が追跡されます。通常、ウイルスの侵入ポイントはファイルのフロントエンドにあり、最初に実行される部分です。ほとんどの場合、ウイルスであることを認識するためには、ウイルス本文のほんのわずかな部分を復号するだけで十分です。クリーンな実行ファイルの多くは、数個の命令をエミュレートするだけでエミュレーションを停止して、負担を軽減します。

エミュレータは制限された領域で実行されるため、コードがウイルスであるとわかっても、電子メールゲートウェイに感染することはありません。

ウイルスの記述

Sophos は、他の信用されているアンチウイルス企業と毎月ウイルスを交換しています。さらに、顧客から毎月数千の疑わしいファイルが直接 Sophos に送られ、そのうち約 30 % はウイルスであると判明しています。各サンプルは、非常にセキュアなウイルス ラボで厳しく分析され、ウイルスかどうか判断されます。Sophos は、新しく発見された各ウイルスまたはウイルスのグループに対して、記述を作成します。

Sophos アラート

Sophos Anti-Virus スキャンをイネーブルにしているお客様に対して、Sophos のサイト（http://www.sophos.com/virusinfo/notifications/）から Sophos アラートを購読することを推奨しています。購読して Sophos から直接アラートを受け取ることにより、最新のウイルスの発生および利用可能な解決方法が確実に通知されます。

ウイルスが発見された場合

ウイルスが検出されたら、Sophos Anti-Virus はファイルを修復（駆除）できます。通常、Sophos Anti-Virus は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に

戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、E メール セキュリティ機能（[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページ（GUI）または `policyconfig -> antivirus` コマンド（CLI）を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、ユーザのウイルス スキャン アクションの設定 （447 ページ）を参照してください。

McAfee アンチウイルス フィルタリング

McAfee®スキャン エンジン:

- ファイルのデータとウイルス シグニチャをパターン照合することにより、ファイルをスキャンします。
- エミュレーション環境でウイルス コードを復号および実行します。
- 発見的手法を適用して新しいウイルスを認識します。
- ファイルから感染性のコードを削除します。

関連項目

- ウイルス シグニチャとのパターン照合 （444 ページ）
- 暗号化されたポリモーフィック型ウイルスの検出 （444 ページ）
- 発見的分析 （445 ページ）
- ウイルスが発見された場合 （443 ページ）

ウイルス シグニチャとのパターン照合

McAfee は、アンチウイルス定義（DAT）ファイルをスキャン エンジンで使用して、特定のウイルス、ウイルスのタイプ、またはその他の潜在的に望ましくないソフトウェアを検出します。また、ファイル内の既知の場所を開始点としてウイルス固有の特徴を検索することにより、単純なウイルスを検出できます。多くの場合、ファイルのほんの一部を検索するだけで、ファイルがウイルスに感染していないと判断できます。

暗号化されたポリモーフィック型ウイルスの検出

複雑なウイルスは、次の2つの一般的な手法を使用して、シグニチャ スキャンによる検出を回避します。

- **暗号化**。ウイルス内部のデータは、アンチウイルス スキャナがメッセージまたはウイルスのコンピュータ コードを判読できないように、暗号化されます。ウイルスがアクティブになると、ウイルス自体が自発的に実行バージョンに変化し、自己実行します。
- **ポリモーフィック化**。この処理は暗号化に似ていますが、ウイルスが自己複製する際に、その形が変わる点で暗号化とは異なります。

このようなウイルスに対抗するために、エンジンはエミュレーションと呼ばれる手法を使用します。エンジンは、ファイルにこのようなウイルスが含まれていると疑った場合、ウイルスが

他に害を及ぼすことなく自己実行して、本来の形が判読できる状態まで自分自身をデコードする人工的な環境を作成します。その後、エンジンは通常どおりウイルス シグニチャをスキャンして、ウイルスを特定します。

発見的分析

新しいウイルスの署名は未知であるため、ウイルス シグニチャを使用するだけでは、新しいウイルスは検出できません。そのため、エンジンは追加で発見的分析という手法を使用します。

ウイルスを運ぶプログラム、ドキュメント、または電子メール メッセージには、多くの場合、特異な特徴があります。これらは、自発的にファイルの変更を試行したり、メール クライアントを起動したり、またはその他の方法を使用して自己複製します。エンジンはプログラム コードを分析して、この種のコンピュータ命令を検出します。また、エンジンは、アクションを実行する前にユーザの入力を求めたりするようなウイルスらしくない正規の動作も検索して、誤ったアラームを発行しないようにしています。

このような手法を使用することで、エンジンは多くの新しいウイルスを検出できます。

ウイルスが発見された場合

ウイルスが検出されたら、Sophos Anti-Virus はファイルを修復（駆除）できます。通常、Sophos Anti-Virus は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、E メール セキュリティ機能（[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページ（GUI）または `policyconfig -> antivirus` コマンド（CLI）を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、ユーザのウイルス スキャン アクションの設定 （447 ページ）を参照してください。

電子メールゲートウェイでのウイルスのスキャンの設定方法

メッセージのウイルスのスキャン方法

	操作内容	詳細
ステップ 1	電子メールゲートウェイでアンチウイルススキャンをイネーブルにします。	ウイルス スキャンのイネーブル化およびグローバル設定の構成 （446 ページ）

	操作内容	詳細
ステップ 2	メッセージのウイルスをスキャンするユーザ グループを定義します。	送信者および受信者のグループのメール ポリシーの作成 （317 ページ）
ステップ 3	（任意）ウイルス隔離でのメッセージの処理方法を設定します。	ポリシー、ウイルス、およびアウトブレイク隔離の設定 （1135 ページ）
ステップ 4	電子メールゲートウェイでのウイルスに感染したメッセージの処理方法を決定します。	ユーザのウイルス スキャン アクションの設定 （447 ページ）
ステップ 5	定義したユーザ グループに対するアンチウイルス スキャンのルールを設定します。	送信者および受信者のグループごとのアンチウイルス ポリシーの設定 （454 ページ）
ステップ 6	（任意）設定をテストするために電子メール メッセージを送信します。	アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信 （457 ページ）

関連項目

- ウイルス スキャンのイネーブル化およびグローバル設定の構成 （446 ページ）
- ユーザのウイルス スキャン アクションの設定 （447 ページ）
- 送信者および受信者のグループごとのアンチウイルス ポリシーの設定 （454 ページ）
- ウイルス対策設定に関する注意事項 （455 ページ）
- アンチウイルス アクションのフロー ダイアグラム （456 ページ）

ウイルス スキャンのイネーブル化およびグローバル設定の構成

ウイルス スキャン エンジンは、システム セットアップ ウィザードを実行したときにイネーブルになった可能性があります。これにかかわらず、次の手順で設定をします。

（注） ライセンス キーによって、Sophos、McAfee、またはその両方をイネーブルにできます。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [McAfee] ページに移動します。

または

[セキュリティサービス（Security Services）] > [Sophos] ページに移動します。

ステップ 2 [有効（Enable）] をクリックします。

（注） [有効（Enable）] をクリックすると、電子メールゲートウェイで機能がグローバルにイネーブルになります。ただし、後で [メールポリシー（Mail Policies）] で受信者ごとの設定をイネーブルにする必要があります。

ステップ 3 ライセンス契約書を読み、ページの最後までスクロールしてから [承認（Accept）] をクリックして契約に同意します。

ステップ 4 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 5 ウイルス スキャンの最大タイムアウト値を選択します。

システムがメッセージに対するアンチウイルス スキャンの実行を停止する、タイムアウト値を設定します。デフォルト値は 60 秒です。

ステップ 6 （任意）[自動アップデートを有効にする（Enable Automatic Updates）] をクリックして、エンジンの自動アップデートを有効にします。

電子メールゲートウェイは、アップデートサーバから特定のエンジンに必要なアップデートを取得します。

ステップ 7 変更を送信し、保存します。

次のタスク

アンチウイルス設定を受信者ごとに設定します。ユーザのウイルス スキャン アクションの設定 （447 ページ） を参照してください。

ユーザのウイルス スキャン アクションの設定

電子メールゲートウェイに統合されているウイルススキャンエンジンは、[電子メールセキュリティマネージャ（Email Security Manager）] 機能を使用して設定したポリシー（設定オプション）に基づいて、着信および発信メールメッセージのウイルスを処理します。アンチウイルス アクションは、[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページ（GUI）または `policyconfig > antivirus` コマンド（CLI）を使用して受信者ごとにイネーブルにします。

関連項目

- メッセージ スキャン設定 （447 ページ）
- メッセージ処理設定 （448 ページ）
- メッセージ処理アクションの設定の構成 （449 ページ）

メッセージ スキャン設定

- [ウイルス スキャンのみ（Scan for Viruses Only）] :

  システムにより処理されるメッセージには、ウイルス スキャンが実行されます。感染している添付ファイルがあっても、修復は試行されません。ウイルスが含まれるメッセージま

たは修復できなかったメッセージについて、添付ファイルをドロップしてメールを配信するかどうかを選択できます。

- [ウイルスをスキャンして修復（Scan and Repair Viruses）]：

  システムにより処理されるメッセージには、ウイルス スキャンが実行されます。添付ファイルにウイルスが発見された場合は、システムは添付ファイルの「修復」を試行します。

- [添付ファイルをドロップ（Dropping Attachments）]：

  感染した添付ファイルをドロップするように選択できます。

  アンチウイルス スキャン エンジンにより、メッセージの添付ファイルがスキャンされ感染したファイルがドロップされると、代わりに「Removed Attachment」という名前の新しいファイルが添付されます。この添付ファイルのタイプはテキストまたはプレーンで、次の内容が含まれています。

```
This attachment contained a virus and was stripped.
 Filename: filename
Content-Type: application/filetype
```

悪質な添付ファイルによりメッセージが感染していたため、ユーザのメッセージに何らかの修正が加えられた場合は、必ずユーザに通知されます。二次的な通知アクションを設定することもできます（通知の送信（452ページ）を参照）。感染した添付ファイルをドロップするように選択した場合は、通知アクションにより、ユーザにメッセージが修正されたことを通知する必要はありません。

- [X-IronPort-AVヘッダー（X-IronPort-AV Header）]：

  電子メールゲートウェイのアンチウイルス スキャン エンジンにより処理されたすべてのメッセージには、X-IronPort-AV: というヘッダーが追加されます。このヘッダーは、特に「スキャンできない」と見なされたメッセージについて、アンチウイルス設定に関する問題をデバッグする際の追加情報となります。X-IronPort-AVヘッダーをスキャンされたメッセージに含めるかどうかは、切り替えできます。このヘッダーを含めることを推奨します。

メッセージ処理設定

ウイルス スキャン エンジンは、リスナーにより受信される 4 つの独立したメッセージ クラスについて、それぞれ別々のアクションを実行して処理するように設定できます。「図：ウイルスをスキャンするメッセージを処理するオプション」は、ウイルス スキャン エンジンが有効なときに、システムが実行するアクションの概要を示します。

次の各メッセージタイプについて、それぞれ実行するアクションを選択できます。アクションについては後述します（メッセージ処理アクションの設定の構成（449ページ）を参照）。たとえば、ウイルスに感染したメッセージについて、感染した添付ファイルがドロップされ、電子メールの件名が変更されて、カスタムアラートがメッセージの受信者に送信されるように、ウイルス対策を設定できます。

修復されたメッセージの処理

メッセージが完全にスキャンされ、すべてのウイルスが修復または削除された場合は、そのメッセージは修復されたと見なされます。これらのメッセージはそのまま配信されます。

暗号化されたメッセージの処理

メッセージ内に暗号化または保護されたフィールドがあるために、エンジンがスキャンを完了できなかった場合は、そのメッセージは暗号化されていると見なされます。暗号化されているとマークされたメッセージも、修復可能です。

暗号化検出のメッセージフィルタルール（暗号化検出ルール（198ページ）を参照）と、「暗号化された」メッセージに対するウイルス スキャン アクションの違いに注意してください。暗号化メッセージ フィルタ ルールは、PGP または S/MIME で暗号化されたすべてのメッセージを「true」と評価します。暗号化ルールで検出できるのは、PGP および S/MIME で暗号化されたデータのみです。パスワードで保護された ZIP ファイル、もしくは暗号化されたコンテンツを含む Microsoft Word または Excel ドキュメントは検出できません。ウイルス スキャン エンジンは、パスワードで保護されたメッセージまたは添付ファイルはすべて「暗号化されている」と見なします。

（注） AsyncOS バージョン 3.8 以前からアップグレードして、Sophos Anti-Virus スキャンを設定する場合は、アップグレード後に「暗号化されたメッセージの処理」の項を設定する必要があります。

スキャンできないメッセージの処理

スキャン タイムアウト値に到達した場合、または内部エラーによりエンジンが使用不可能になった場合は、メッセージはスキャンできないと見なされます。スキャンできないとマークされたメッセージも、修復可能です。

ウイルスに感染したメッセージの処理

システムが添付ファイルをドロップできない、またはメッセージを完全に修復できない場合があります。このような場合は、依然としてウイルスが含まれるメッセージのシステムでの処理方法を設定できます。

暗号化メッセージ、スキャンできないメッセージ、およびウイルス メッセージの設定オプションは、どれも同じです。

メッセージ処理アクションの設定の構成

- 適用するアクション （450 ページ）
- 隔離およびウイルス対策スキャン （450 ページ）
- メッセージの件名ヘッダーの変更 （451 ページ）
- オリジナル メッセージのアーカイブ （451 ページ）
- 通知の送信 （452 ページ）
- メッセージへのカスタム ヘッダーの追加 （452 ページ）

- メッセージ受信者の変更 （452 ページ）
- 代替送信ホストにメッセージを送る （453 ページ）
- カスタム アラート通知の送信 （453 ページ）

適用するアクション

暗号化されたメッセージ、スキャンできないメッセージ、またはウイルス陽性のメッセージの各タイプについて、全般的にどのアクションを実行するか（メッセージをドロップする、新しいメッセージの添付ファイルとしてメッセージを配信する、メッセージをそのまま配信する、またはメッセージをアンチウイルス隔離エリアに送信する（隔離およびウイルス対策スキャン（450 ページ）を参照））を選択します。

感染したメッセージを新しいメッセージの添付ファイルとして配信するように電子メールゲートウェイを設定すると、受信者がオリジナルの感染した添付ファイルをどのように処理するか、選択できるようになります。

メッセージをそのまま配信するか、またはメッセージを新しいメッセージの添付ファイルとして配信することを選択した場合は、追加で次の処理を設定できます。

- メッセージの件名の変更
- オリジナル メッセージのアーカイブ
- 一般的な通知の送信。次のアクションは、GUI の [詳細（Advanced）] セクションから実行できます。
- メッセージへのカスタム ヘッダーの追加
- メッセージ受信者の変更
- 代替宛先ホストへのメッセージの送信
- カスタム アラート通知の送信

（注） これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。これらのオプションを使用した、さまざまなスキャンポリシーの定義に関する詳細については、後述のセクションおよびウイルス対策設定に関する注意事項 （455 ページ）を参照してください。

修復されたメッセージに対する拡張オプションは、[カスタムヘッダーを追加（Add custom header）] および [カスタムアラート通知を送信（Send custom alert notification）] の 2 つのみです。その他すべてのメッセージ タイプについては、すべての拡張オプションにアクセスできます。

隔離およびウイルス対策スキャン

隔離フラグの付けられたメッセージは、電子メールパイプラインの残りの処理を継続します。メッセージがパイプラインの末尾に到達すると、メッセージに 1 つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

たとえば、コンテンツ フィルタはメッセージをドロップまたは返送する場合がありますが、その場合、メッセージは隔離されません。

オリジナル メッセージのアーカイブ

システムにより、ウイルスが含まれている（または含まれている可能性がある）と判断されたメッセージは、「avarchive」ディレクトリにアーカイブできます。この形式は、mbox 形式のログ ファイルです。「Anti-Virus Archive」ログ サブスクリプションを設定して、ウイルスが含まれているメッセージまたは完全にスキャンできなかったメッセージをアーカイブする必要があります。詳細については、ログ （1391 ページ）を参照してください。

（注） GUI では、場合により [詳細（Advanced）] リンクをクリックして [オリジナルのメッセージをアーカイブ（Archive original message）] を表示する必要があります。

メッセージの件名ヘッダーの変更

特定のテキスト文字列を前後に追加することで、識別されたメッセージを変更すると、ユーザがより簡単に識別されたメッセージを判別したり、ソートしたりできるようになります。

（注） [メッセージの件名を修正（Modify message subject）] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、`[WARNING: VIRUS REMOVED]` というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

デフォルトのテキストは次のとおりです。

アンチウイルス件名行変更のデフォルト件名行テキスト

判定	件名に追加されるデフォルトのテキスト
暗号化	`[WARNING: MESSAGE ENCRYPTED]`
感染している	`[WARNING: VIRUS DETECTED]`
修復されている	`[WARNING: VIRUS REMOVED]`
スキャン不可（Unscannable）	`[WARNING: A/V UNSCANNABLE]`

複数のステートが該当するメッセージについては、電子メールゲートウェイがメッセージに対して実行したアクションをユーザに知らせる、複数部分で構成された通知メッセージが作成さ

れます（たとえば、ユーザに対してはメッセージがウイルスを修復されていると通知されていても、メッセージの他の部分は暗号化されている場合があります）。

通知の送信

システムにより、メッセージにウイルスが含まれていると識別されたときに、デフォルトの通知を送信者、受信者、およびその他のユーザまたはそのいずれかに送信できます。その他のユーザを通知対象に指定する場合は、複数のアドレスをコンマで区切ります（CLI および GUI の両方）。デフォルトの通知、メッセージは次のとおりです。

アンチウイルス通知のデフォルト通知

判定	通知
修復されている	次のウイルスがメールメッセージで検出されました: <ウイルス名>（The following virus(es) was detected in a mail message: <virus name(s)>） 実行するアクション:感染している添付ファイルがドロップされました（または感染している添付ファイルが修復されました）。（Actions taken: Infected attachment dropped (or Infected attachment repaired).）
暗号化	暗号化されているため、次のメッセージをウイルス対策エンジンによって完全にスキャンできませんでした。（The following message could not be fully scanned by the anti-virus engine due to encryption.）
スキャン不可	次のメッセージをウイルス対策エンジンによって完全にスキャンできませんでした。（The following message could not be fully scanned by the anti-virus engine.）
感染している	次の修復不可能なウイルスがメールメッセージで検出されました:<ウイルス名>。（The following unrepairable virus(es) was detected in a mail message: <virus name(s)>.）

メッセージへのカスタム ヘッダーの追加

アンチウイルス スキャン エンジンによってスキャンされたすべてのメッセージに追加する、追加のカスタム ヘッダーを定義できます。[はい（Yes）] をクリックし、ヘッダー名およびテキストを定義します。

また、`skip-viruscheck` アクションを使用するフィルタを作成して、特定のメッセージはウイルス スキャンを回避するようにもできます。アンチウイルス システムのバイパス アクション（254 ページ） を参照してください。

メッセージ受信者の変更

メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようにできます。[はい（Yes）] をクリックして、新しい受信者のアドレスを入力します。

代替送信ホストにメッセージを送る

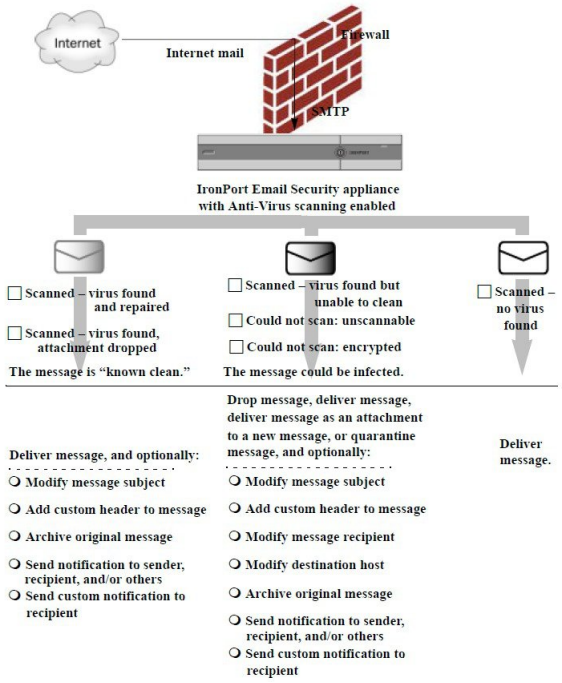
暗号化されたメッセージ、スキャンできないメッセージ、またはウイルスに感染したメッセージについて、異なる受信者または宛先ホストに通知を送信するように選択できます。[はい（Yes）] をクリックして代替アドレスまたはホストを入力します。

たとえば、疑わしいメッセージを管理者のメールボックスまたは専用のメールサーバに送信して、後で調査することができます。受信者が複数のメッセージの場合は、代替受信者に送信されるコピーは 1 つのみです。

カスタム アラート通知の送信

送信者、受信者、およびその他のユーザ（メールアドレス）にカスタム通知を送信できます。そのためには、この設定を構成する前に、まずカスタム通知を作成する必要があります。詳細については、テキスト リソースについて （800 ページ）を参照してください。

図 *18 :* ウイルス スキャンを実行したメッセージの処理に関するオプション



（注） デフォルトでは、アンチウイルススキャンは、ALLOWED_LIST 送信者グループが参照するパブリックリスナーの $TRUSTED メールフローポリシーで有効になっています。メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （115 ページ）を参照してください。

送信者および受信者のグループごとのアンチウイルスポリシーの設定

メールポリシーのユーザごとのアンチウイルス設定を編集する処理は、着信メールと発信メールで基本的に同じです。

個々のポリシー（デフォルト以外）には、[デフォルトを使用（Use Default）] 設定値という追加のフィールドがあります。この設定は、デフォルトのメールポリシー設定を継承するように選択します。

アンチウイルス アクションは、[受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] を使用して受信者ごとにイネーブルにします。GUI または CLI の policyconfig > antivirus コマンドを使用してメール ポリシーを設定できます。アンチウイルス設定をグローバルにイネーブルにした後は、作成した各メール ポリシーに対して、これらのアクションを別々に設定します。さまざまなメールポリシーに対して、異なるアクションを設定できます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページに移動します。

ステップ 2 ポリシーを設定するアンチウイルス セキュリティ サービスのリンクをクリックします。

（注） デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。

ステップ 3 [はい（Yes）] または [デフォルトを使用（Use Default）] をクリックして、そのポリシーのアンチウイルス スキャンをイネーブルにします。

このページの最初の設定値は、そのポリシーに対してサービスがイネーブルであるかどうかを定義します。[無効（Disable）] をクリックしてすべてのサービスをディセーブルにできます。

デフォルト以外のメール ポリシーでは、[はい（Yes）] を選択することで、[修復されたメッセージ（Repaired Messages）]、[暗号化されたメッセージ（Encrypted Messages）]、[スキャン不能なメッセージ（Unscannable Messages）]、および [ウイルス感染したメッセージ（Virus Infected Messages）] 領域内の各フィールドがイネーブルになります。

ステップ 4 アンチウイルス スキャン エンジンを選択します。McAfee または Sophos のエンジンを選択できます。

ステップ 5 [メッセージのスキャン（Message Scanning）] 設定を構成します。

詳細については、メッセージ スキャン設定 （447 ページ）を参照してください。

ステップ 6 [修復されたメッセージ（Repaired Messages）]、[暗号化されたメッセージ（Encrypted Messages）]、[スキャン不能なメッセージ（Unscannable Messages）]、および [ウイルス感染したメッセージ（Virus Infected Messages）] の設定を構成します。

メッセージ処理設定 （448 ページ）およびメッセージ処理アクションの設定の構成 （449 ページ）を参照してください。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 変更を保存します。

ウイルス対策設定に関する注意事項

添付ファイルのドロップフラグにより、アンチウイルス スキャンの動作は大きく異なります。システムが、[ウイルスが検出され修復できない場合、感染した添付ファイルをドロップする（Drop infected attachments if a virus is found and it could not be repaired）] ように設定されている場合は、ウイルス性またはスキャンできない MIME 部分はすべてメッセージから削除されます。そのため、アンチウイルス スキャンの出力は、ほとんど常にクリーンなメッセージになります。GUI ペインに表示された [スキャン不能なメッセージ（Unscannable Messages）] で定義されるアクションは、実行されることはほとんどありません。

[ウイルスのみスキャン（Scan for Viruses only）] 環境では、これらのアクションは悪質なメッセージ部分をドロップすることで、メッセージを「クリーンに」します。RFC822 ヘッダーに限り、RFC822 ヘッダー自体が攻撃された、またはその他の問題に遭遇した場合は、スキャンできなかった場合のアクションが実行されます。ただし、アンチウイルス スキャンが [ウイルスのみスキャン（Scan for Viruses only）] に設定されていながら、[ウイルスが検出され修復できない場合、感染した添付ファイルをドロップする（Drop infected attachments if a virus is found and it could not be repaired）] が選択されていない場合は、スキャンできなかった場合のアクションが実行される可能性は非常に高くなります。

次の表に、一般的なアンチウイルス設定オプションを示します。

一般的なアンチウイルス設定オプション

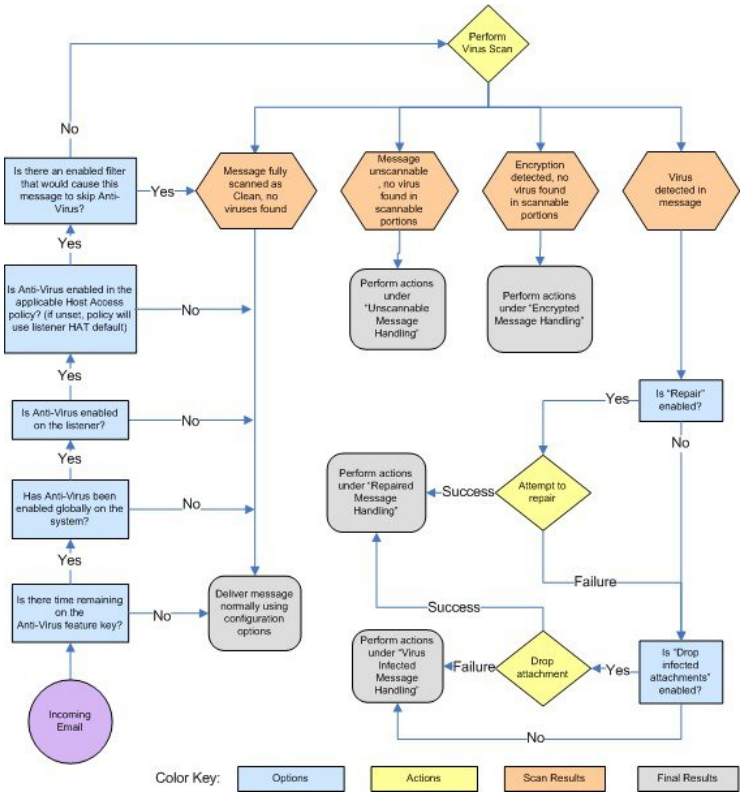
状況	アンチウイルス設定
ウイルスが広範囲に発生 ウイルス性のメッセージは単純にシステムからドロップされ、他の処理が実行されることはほとんどありません。	**添付ファイルのドロップ**：しない。 **スキャン**：スキャンのみ。 **クリーンアップされたメッセージ**：配信する。 **スキャンできないメッセージ**：メッセージをドロップする。 暗号化されたメッセージ：管理者に送るか隔離して、後で確認する。 ウイルス性のメッセージ：メッセージをドロップする。

状況	アンチウイルス設定
リベラルなポリシー できる限り多くのドキュメントを送信します。	**添付ファイルのドロップ**：する。 **スキャン**：スキャンして修復。 **クリーンアップされたメッセージ**：[VIRUS REMOVED] として配信する **スキャンできないメッセージ**：添付ファイルとして転送する。 暗号化されたメッセージ：マークして転送する。 ウイルス性のメッセージ：隔離するか、マークして転送する。
より保守的なポリシー	**添付ファイルのドロップ**：する。 **スキャン**：スキャンして修復。 **クリーンアップされたメッセージ**：[VIRUS REMOVED] として配信する （より慎重なポリシーでは、クリーンアップしたメッセージをアーカイブします）。 **スキャンできないメッセージ**：通知を送る、隔離する、またはドロップしてアーカイブする。 暗号化されたメッセージ：マークして転送する、またはスキャンできないメッセージとして処理する。 ウイルス性のメッセージ：アーカイブしてドロップする。
保守的なポリシーでレビューを実施する ウイルス メッセージの可能性があるものは、後で管理者が内容を確認できるように、隔離メールボックスに送信されます。	**添付ファイルのドロップ**：しない。 **スキャン**：スキャンのみ。 **クリーンアップされたメッセージ**：配信する（通常、このアクションは実行されません）。 スキャンできないメッセージ：添付ファイル、alt-src-host、または alt-rcpt-to アクションとして転送する。 暗号化されたメッセージ：スキャンできないメッセージとして処理する。 ウイルス性のメッセージ：隔離するか管理者に転送する。

アンチウイルス アクションのフロー ダイアグラム

次の図に、アンチウイルスアクションおよびオプションが、電子メールゲートウェイで処理されるメッセージにどのように影響を及ぼすかを示します。

図 *19* : アンチウイルス アクションのフロー ダイアグラム



（注） マルチレイヤ アンチウイルス スキャンを設定した場合は、Cisco アプライアンスは最初に McAfee エンジンでウイルス スキャンを実行し、次に Sophos エンジンでウイルス スキャンを実行します。アプライアンスは、McAfee エンジンがウイルスを検出しない限りは、両方のエンジンを使用してメッセージをスキャンします。McAfee エンジンがウイルスを検出した場合は、電子メールゲートウェイは、メールポリシーで定義されたアンチウイルスアクション（修復、隔離など）を実行します。

アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信

手順

ステップ 1 メール ポリシーのウイルス スキャンをイネーブルにします。

[セキュリティサービス（Security Services）] > [Sophos] または [McAfeeウイルス対策（McAfee Anti-Virus）] ページ、または `antivirusconfig` コマンドを使用してグローバル設定を行ってか

ら、[電子メールセキュリティマネージャ（Email Security Manager）] ページ（GUI）または policyconfig の antivirus サブコマンドを使用して、特定のメール ポリシーの設定を構成します。

ステップ 2 標準のテキスト エディタを開き、次の文字列をスペースまたは改行を使用せず、1 行で入力します。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

（注） 上記の行は、テキスト エディタ ウィンドウで 1 行で表示される必要があります。そのため、必ずテキスト エディタのウィンドウは最大にして、改行はすべて削除します。また、テスト メッセージ開始部の「X5O...」には、数字の「0」ではなく必ず文字の「O」を入力します。

このマニュアルをコンピュータでお読みの場合は、PDF ファイルまたは HTML ファイルから直接この行をコピーして、テキスト エディタに貼ることができます。この行をコピーする場合は、必ずすべての余分な復帰文字またはスペースを削除します。

ステップ 3 ファイルを **EICAR.COM** という名前で保存します。

ファイルのサイズは 68 ～ 70 バイトになります。

（注） このファイルはウイルスではありません。拡散したり、他のファイルに感染したり、またはコンピュータに害を与えたりするものではありません。ただし、他のユーザにアラームを与えないために、テストを終了したらこのファイルは削除してください。

ステップ 4 ファイル EICAR.COM を電子メール メッセージに添付して、ステップ 1 で設定したメール ポリシーに一致するリスナーに送信します。

テスト メッセージで指定した受信者が、リスナーで許可されることを確認します（詳細については、メッセージを受け入れるドメインおよびユーザの追加（150 ページ）を参照してください。）

シスコ以外のゲートウェイ（たとえば Microsoft Exchange サーバ）で発信メールに対するウイルス スキャン ソフトウェアをインストールしている場合は、ファイルを電子メールで送信することが難しいことがあるため、注意してください。

（注） テスト ファイルは、常に修復不可能としてスキャンされます。

ステップ 5 リスナー上のウイルス スキャンに設定したアクションを評価して、そのアクションがイネーブルであり、予想どおりに動作していることを確認します。

これは、次のいずれかのアクションを実行することで、最も簡単に達成できます。

1. ウイルス スキャンを、[スキャンして修復（Scan and Repair）] モードまたは [スキャンのみ（Scan Only）] モードにして、添付ファイルをドロップしないように設定します。
   - EICAR テスト ファイルを添付ファイルとした電子メールを送信します。実行されたアクションが、[ウイルス感染したメッセージ（Virus Infected Messages）] の処理で設定した内容（ウイルスに感染したメッセージの処理（449 ページ）の設定）と一致していることを確認します。

2. ウイルス スキャンを、[スキャンして修復（Scan and Repair）] モードまたは [スキャンのみ（Scan Only）] モードにして、添付ファイルをドロップするように設定します。
   - EICAR テスト ファイルを添付ファイルとした電子メールを送信します。
   - 実行されたアクションが、[修復されたメッセージ（Repaired Messages）] の処理で設定した内容（修復されたメッセージの処理 （449 ページ）の設定）と一致していることを確認します。

アンチウイルス スキャンのテスト用ウイルス ファイルの取得に関する詳細については、次の URL を参照してください。http://www.eicar.org/anti_virus_test_file.htm

このページでは、ダウンロード可能な4つのファイルを提供しています。クライアント側にウイルス スキャン ソフトウェアをインストールしている場合は、これらのファイルをダウンロードして抽出するのは難しいため、注意してください。

ウイルス定義ファイルの更新

関連項目

- HTTP を使用したアンチウイルス アップデートの取得について （459 ページ）
- アップデート サーバ設定の構成 （460 ページ）
- モニタリングおよび手動での Anti-Virus アップデート チェック （460 ページ）
- 電子メールゲートウェイでのアンチウイルスファイルの更新の確認 （460 ページ）

HTTP を使用したアンチウイルス アップデートの取得について

Sophos および McAfee は新たに識別されたウイルスのウイルス定義を頻繁にアップデートします。これらの更新は、電子メールゲートウェイに渡す必要があります。

デフォルトでは、電子メールゲートウェイは、5 分ごとにアップデートをチェックするように設定されています。Sophos および McAfee のアンチウイルス エンジンの場合は、サーバは動的 Web サイトからアップデートします。

アップデートを電子メールゲートウェイにダウンロードしている間は、アップデートのタイムアウトにはなりません。アップデートのダウンロードが長時間中断すると、ダウンロードがタイムアウトします。

システムがタイムアウトせずに、アップデートが完了するまで待機する最大時間は、アンチウイルス アップデート間隔より 1 分短い値に定義された、動的な値です（[セキュリティ サービス（Security Services）]>[サービスのアップデート（Service Updates）] で定義されています）。この設定値は、接続速度の遅いアプライアンスが、完了まで 10 分を超える大きいアップデートをダウンロードする場合に役立ちます。

アップデート サーバ設定の構成

[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページでウイルス更新設定を設定できます。たとえば、システムがアンチウイルスの更新を受ける方法や更新を確認する頻度を設定できます。追加設定に関する詳細については、サービス アップデート （1253 ページ）を参照してください。

モニタリングおよび手動での Anti-Virus アップデート チェック

[セキュリティサービス（Security Services）] > [Sophos] または [McAfee] ページまたは CLI の `antivirusstatus` コマンドを使用して、電子メールゲートウェイに最新のアンチウイルスエンジンおよび識別ファイルがインストールされていることを確認し、いつ最終のアップデートが実行されたか確認できます。

また、手動でアップデートを実行することもできます。手動でのアンチウイルス エンジンの更新 （460 ページ）を参照してください

手動でのアンチウイルス エンジンの更新

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Sophosウイルス対策（Sophos Anti-Virus）] または [McAfeeウイルス対策（McAfee Anti-Virus）] ページに移動します。

ステップ 2 [現在のMcAfee/Sophosウイルス対策ファイル（Current McAfee/Sophos Anti-Virus Files）] テーブルで、[今すぐ更新（Update Now）] をクリックします。

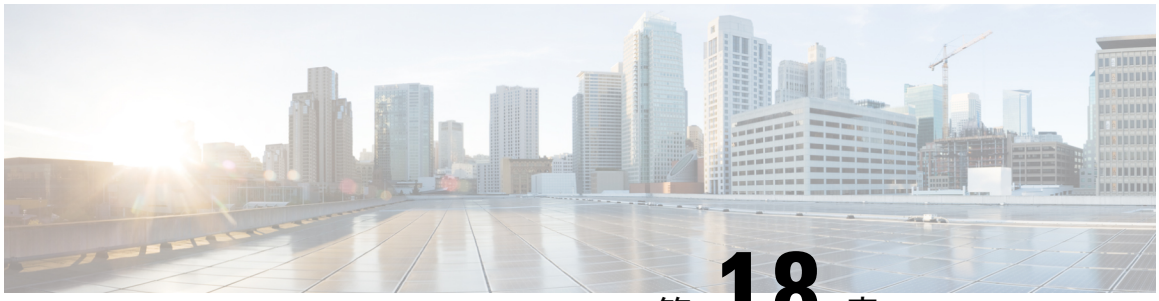
電子メールゲートウェイは最新のアップデートを確認してダウンロードします。

次のタスク

これは、antivirusstatus および antivirusupdate コマンドを使用してコマンドライン インターフェイスでも構成できます。

電子メールゲートウェイでのアンチウイルスファイルの更新の確認

アップデータ ログを表示して、アンチウイルス ファイルが、すべて正常にダウンロード、抽出、またはアップデートされたことを確認できます。アップデータ ログ サブスクリプションの最終的なエントリを表示して、ウイルス アップデートが取得できていることを確認するには、tail コマンドを使用します。



第 18 章

スパムおよびグレイメールの管理

この章は、次の項で構成されています。

- スパム対策スキャンの概要 （461 ページ）
- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法 （462 ページ）
- IronPort スパム対策フィルタリング （464 ページ）
- Intelligent Multi-Scan とグレイメール検出の設定 （467 ページ）
- スパム対策ポリシーの定義 （481 ページ）
- スパムフィルタからの 電子メールゲートウェイ生成メッセージの保護 （490 ページ）
- スパム対策スキャン中に追加されるヘッダー （490 ページ）
- 誤って分類されたメッセージのシスコへの報告 （491 ページ）
- 着信リレー構成における送信者の IP アドレスの決定 （497 ページ）
- モニタリング ルールのアップデート （507 ページ）
- スパム対策のテスト （508 ページ）

スパム対策スキャンの概要

スパム対策プロセスは、設定するメールポリシーに基づいて着信（および発信）のメールの電子メールをスキャンします。

- 1 つ以上のスキャン エンジンはフィルタ モジュールによってメッセージをスキャンします。
- スキャン エンジンは、各メッセージにスコアを割り当てます。スコアが高いほど、メッセージがスパムである可能性が高くなります。
- スコアに基づいて、各メッセージは次のいずれかに分類されます。
  - スパムではない電子メール
  - スパムだと疑われる電子メール
  - 陽性と判定されたスパム
- 結果に基づいてアクションが実行されます。

陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティング メッセージとして識別されたメッセージに対して実行されるアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションの数個またはすべてを、さまざまに組み合わせることができます。同じポリシーで、陽性と判定されたスパムと陽性と疑わしいスパムを別々に扱うことができます。たとえば、陽性と判定されたスパムであるメッセージをドロップする一方で、陽性と疑わしいスパム メッセージを隔離する必要がある場合があります。

各メールポリシーで、カテゴリの複数のしきい値を指定し、各カテゴリに対して実行するアクションを指定できます。異なるメールポリシーに異なるユーザを割り当て、各ポリシーに対して異なるスキャン エンジン、スパム定義しきい値、スパム処理アクションを定義できます。

（注） スパム対策スキャンの適用方法および適用時期の詳細については、電子メール パイプラインとセキュリティ サービス （73 ページ）を参照してください。

関連項目

- スパム対策ソリューション （462 ページ）

スパム対策ソリューション

電子メールゲートウェイは次のスパム対策ソリューションを提供します。

- IronPort スパム対策フィルタリング （464 ページ）。
- Intelligent Multi-Scan とグレイメール検出の設定 （467 ページ）。

電子メールゲートウェイの両方のソリューションを認可して有効にできますが、特定のメールポリシーでは 1 つしか使用できません。ユーザのグループごとに異なるスパム対策ソリューションを指定できます。

メッセージがスパムかどうかスキャンするための 電子メールゲートウェイの設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	電子メールゲートウェイのスパム対策スキャニングをイネーブルにします。	（注） この表の残りの手順は、両方のスキャン エンジンにオプションに適用されます。

	コマンドまたはアクション	目的
		Cisco IronPort Anti-Spam および Intelligent Multi-Scan の両方のライセンスキーがある場合は、電子メールゲートウェイの両方のソリューションをイネーブルにできます。 • IronPort スパム対策フィルタリング（464 ページ） • Intelligent Multi-Scan とグレイメール検出の設定 （467 ページ）
ステップ 2	ローカルの電子メールゲートウェイからスパムを隔離するか、 Cisco Secure Email and Web Manager の外部隔離を使用するかどうかを設定します。	• ローカルのスパム隔離の設定（1154 ページ） • 外部スパム隔離の操作 （1560 ページ）
ステップ 3	メッセージのスパムをスキャンするユーザ グループを定義します。	送信者および受信者のグループのメール ポリシーの作成 （317 ページ）
ステップ 4	定義したユーザ グループのスパム対策スキャン ルールを設定します。	スパム対策ポリシーの定義 （481 ページ）
ステップ 5	特定のメッセージに対する Cisco Anti-Spam スキャンをスキップし、skip-spamcheck アクションを使用するメッセージ フィルタを作成します。	アンチスパム システムのバイパス アクション （253 ページ）
ステップ 6	（推奨）IP レピュテーションスコアに基づいて接続を拒否しない場合でも、IP レピュテーションスコアを各受信メールフローポリシーで有効にします。	各受信メール フロー ポリシーで、[フロー制御にSenderBaseを使用（Use SenderBase for Flow Control）] がオンになっていることを確認します。 「メール フロー ポリシーを使用した着信メッセージのルールの定義（124 ページ）」を参照してください。
ステップ 7	電子メールゲートウェイが着信電子メールを受信するために外部送信者に直接接続しない代わりに、メール交換、メール転送エージェント、ネットワークの他のマシンからリレーされたメッセージを受信する場合は、リレーされた着信メッセージに元の送信者の IP アドレスが含まれていることを確認します。	着信リレー構成における送信者の IP アドレスの決定 （497 ページ）

	コマンドまたはアクション	目的
ステップ 8	電子メールゲートウェイで生成されたアラートや他のメッセージがスパムとして間違って識別されないようにします。	スパムフィルタからの電子メールゲートウェイ生成メッセージの保護 （490 ページ）
ステップ 9	（任意）メッセージ内の悪意のある URL に対する保護を強化するため、URL フィルタリングをイネーブルにします。	URL フィルタリングを有効にする （545 ページ）
ステップ 10	設定をテストします。	スパム対策のテスト （508 ページ）
ステップ 11	（任意）サービスの更新を設定します（スパム対策ルールも含め）。	両方のスパム対策ソリューションのスキャン ルールが Cisco 更新サーバからデフォルトで取得されます。 • サービス アップデート （1253 ページ） • プロキシ サーバを経由したアップデート （1259 ページ） • アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）

IronPort スパム対策フィルタリング

関連項目

- 評価キー （464 ページ）
- Cisco Anti-Spam：概要 （465 ページ）
- IronPort Anti-Spam スキャンの設定 （465 ページ）

評価キー

電子メールゲートウェイには、Cisco Anti-Spam ソフトウェアの 30 日間有効な評価キーが付属しています。このキーは、システム セットアップ ウィザードまたは [セキュリティサービス（Security Services）] > [IronPort Anti-Spam] ページ（GUI）か、systemsetup コマンドまたは antispamconfig コマンド（CLI）で、ライセンス契約書を受諾して初めてイネーブルになります。デフォルトでは、ライセンス契約書に同意すると、デフォルト着信メール ポリシーに対して Cisco Anti-Spam がイネーブルになります。設定した管理者アドレス（システム設定ウィザード、手順 2：システム （40 ページ）を参照）に対して、Cisco Anti-Spam のライセンスの期限

が30日後に切れることを通知するアラートの送信も行われます。アラートは、期限切れの30、15、5、および0日前に送信されます。30日間の評価期間後もこの機能を有効にする場合の詳細については、Ciscoの営業担当者にお問い合わせください。残りの評価期間は、[システム管理（System Administration）]>[ライセンスキー（Feature Keys）]ページを表示するか、またはfeaturekeyコマンドを発行することによって確認できます。（詳細については、ライセンス キー（1231 ページ）を参照してください。）

Cisco Anti-Spam：概要

IronPort Anti-Spamでは、スパム、フィッシング、ゾンビ攻撃などの既知のあらゆる脅威に対応するだけでなく、「419」詐欺など検出が難しく、少量で、短期間の電子メール脅威にも対応します。さらに、IronPort Anti-Spamでは、ダウンロードURLまたは実行ファイルを介して不正なコンテンツを配布するスパム攻撃など、新しい脅威や混合された脅威を識別します。

これらの脅威を特定するには、IronPort Anti-Spamはそのメッセージ コンテンツの完全なコンテキスト、メッセージの構築方法、送信者のレピュテーション、メッセージでなどによりアドバタイズされるWebサイトのレピュテーションを検査します。IronPort Anti-Spamは世界最大の電子メールおよびWebモニタリング ネットワークであるSenderBaseを最大限に活用する電子メールおよびWebレピュテーション データを組み合わせ、開始と同時に新しい攻撃を検出します。

IronPort Anti-Spamは次の分野における100,000以上のメッセージ属性を分析します。

- 電子メール レピュテーション：このメッセージの送信者は誰か。
- メッセージの内容：このメッセージに含まれている内容は何か。
- メッセージ構造：このメッセージはどのように構築されているか。
- Web レピュテーション：遷移先はどこか。

多次元的な関係を分析することにより、精度を維持しながら、システムは多様な脅威を検出できます。たとえば、正規金融機関から送信されたと断言する内容を持ちながら、消費者向けのブロードバンド ネットワークに属しているIPアドレスから送信されたメッセージや、「ゾンビ」PCによってホストされているURLを含むメッセージは、疑わしいメッセージであると見なされます。これとは対照的に、肯定的なレピュテーションが与えられている製薬会社からのメッセージは、スパムとの関連性が強い単語を含んでいたとしても、スパムであるとタグ付けされません。

関連項目

- URL 関連の保護および制御 （543 ページ）

IronPort Anti-Spam スキャンの設定

手順

ステップ1 [セキュリティサービス（Security Services）]>[IronPort Anti-Spam]を選択します。

ステップ 2 システム セットアップ ウィザードで [IronPort Anti-Spam] をイネーブルにしなかった場合：

a) **[有効（Enable）]** をクリックします。

b) ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

ステップ 3 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 4 [IronPort Anti-Spamスキャニングを有効にする（Enable IronPort Anti-Spam Scanning）] チェックボックスを選択します。

このボックスをオンにすると、電子メールゲートウェイの機能がグローバルにイネーブルになります。

ステップ 5 スパム送信者から続々と送信される大量メッセージをスキャンする能力を備えながらも、電子メールゲートウェイのスループット最適化を図るため、Cisco Anti-Spam によるメッセージスキャンのしきい値を設定します。

オプション	説明
メッセージのスキャンのしきい値（Message Scanning Thresholds）	**1.** [次のサイズより小さい場合は常にメッセージをスキャン（Always scan messages smaller than）] に値を入力します。推奨値は 1 MB 以下です。「初期終了」の場合を除き、*always scan* サイズより小さいメッセージは完全にスキャンします。このサイズより大きいメッセージは、never scan サイズより小さい場合、部分的にスキャンします。 *always scan* メッセージ サイズは 3 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。 **2.** [次のサイズより大きい場合はメッセージをスキャンしない（Never scan messages larger than）] に値を入力します。推奨値は 2 MB 以下です。このサイズより大きいメッセージは Cisco Anti-Spam によってスキャンされず、X-IronPort-Anti-Spam-Filtered: true というヘッダーはメッセージに追加されません。 *never scan* メッセージ サイズは 10 MB を超えないようにしてください。値が大きくなると、パフォーマンスが低下する可能性があります。 *always scan* サイズより大きいか、または *never scan* サイズより小さいメッセージについては、限定的な高速スキャンを実行します。 （注） アウトブレイク フィルタの最大メッセージサイズが Cisco Anti-Spam の always scan メッセージよりも大きい場合、アウトブレイク フィルタの最大サイズよりも小さいメッセージは完全にスキャンされます。

オプション	説明
1 つのメッセージのスキャンのタイムアウト（Timeout for Scanning Single Message）	メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。 1 ～ 120 の整数を入力します。デフォルト値は 60 秒です。
スキャンプロファイル（Scanning Profile）	スパム メッセージを捕捉するには、次のスキャン プロファイルのいずれかを選択します。 • 通常（Normal）：スパムをブロックするためのバランスの取れたアプローチを使用するには、このオプションを有効にします。 • アグレッシブ（Aggressive）：スパムのブロックを強化するには、このオプションを有効にします。有効にすると、スパム対策ポリシーしきい値を調整したときに、[通常（Normal）]プロファイルよりも、スパム検出に対する影響が大きくなり、誤検出の可能性が高くなります。 （注） 新しいアグレッシブ スキャン プロファイルを使用している場合、メールポリシーを調整してスパム対策のしきい値を変更すると、以前よりも与える影響が大きくなります。したがって、アグレッシブプロファイルを有効にする際、以前に調整したスパム対策ポリシーのしきい値がある場合はデフォルト設定にリセットし、スパム検出率と誤検出の可能性のバランスが最適になるように再評価する必要があります。

ステップ 6 変更を送信し、保存します。

Intelligent Multi-Scan とグレイメール検出の設定

このセクションでは、Cisco Intelligent Multi-Scan と、グレイメール検出および安全な配信停止を設定する方法を説明します。

• Cisco Intelligent Multi-Scan の設定 （468 ページ）
• Intelligent Multi-Scan とグレイメール検出のグローバル設定 （481 ページ）
• グレイメールの管理 （469 ページ）

Cisco Intelligent Multi-Scan の設定

Cisco Intelligent Multi-Scan では、Cisco Anti-Spam を含めた複数のスキャン対策エンジンを組み込むことにより、多層スパム対策ソリューションを実現しています。

Cisco Intelligent Multi-Scan によって処理された場合：

- メッセージは、サードパーティ製スパム対策エンジンによって最初にスキャンされます。
- Cisco Intelligent Multi-Scan は次に、メッセージおよびサードパーティ製エンジンによる判定を Cisco Anti-Spam に渡し、最終判定が下されます。
- Cisco Anti-Spam がスキャンを実行した後、結合された複数のスキャン スコアを AsyncOS に返します。
- Cisco Anti-Spam の低い誤検出率を維持したまま、サードパーティ製スキャン エンジンおよびシスコのスパム対策の結果を組み合わせることで、より多くのスパムが検出されます。

Cisco Intelligent Multi-Scan で使用されるスキャン エンジンの順序は設定できません。Cisco Anti-Spam は、常に最後にメッセージをスキャンするエンジンであり、サードパーティ製エンジンによってスパムであると判定されたメッセージを Cisco Intelligent Multi-Scan がスキップすることはありません。

Cisco Intelligent Multi-Scan を使用すると、システムのスループットが低下する場合があります。詳細については、シスコのサポート担当者にお問い合わせください

（注） Cisco Intelligent Multi-Scan 機能キーによって、電子メールゲートウェイで Cisco Anti-Spam も有効になります。その結果、メールポリシーで Cisco Intelligent MultiScan または Cisco Anti-Spam のいずれかを有効にできるようになります。

重要 Cisco Intelligent Multi-Scan をシステム セットアップ時にイネーブルにすると、グローバル設定のデフォルト値を使用し、デフォルトの着信メール ポリシーでイネーブルにされます。

始める前に

この機能のライセンス キーをアクティブにします。ライセンス キー（1231 ページ）を参照してください。これを行った場合にだけ [IronPortインテリジェントマルチスキャン（IronPort Intelligent Multi-Scan）] オプションが表示されます。

手順

ステップ 1 **[セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）]** を選択します。

ステップ 2 システム セットアップ ウィザードで Cisco Intelligent Multi-Scan をイネーブルにしていない場合：

a) **[有効（Enable）]** をクリックします。

b) ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

ステップ 3 [IMS設定の編集（Edit IMS Settings）] をクリックします。

ステップ 4 [Intelligent Multi-Scanの有効化（Enable Intelligent Multi-Scan）] のチェックボックスをオンにして、 電子メールゲートウェイ全体で機能を有効化します。ただし、メール ポリシーの受信者ごとの設定値は依然として有効にする必要があります。

ステップ 5 （任意）[グローバル設定の編集（Edit Global Settings）] をクリックして、メッセージ スキャンのしきい値を設定します。グローバル設定の詳細については、Intelligent Multi-Scan とグレイメール検出のグローバル設定 （481 ページ） を参照してください。

ステップ 6 変更を送信し、保存します。

グレイメールの管理

- グレイメールの概要 （469 ページ）
- 電子メールゲートウェイでのグレイメール管理ソリューション （470 ページ）
- グレイメール管理ソリューションの仕組み （471 ページ）
- グレイメールの検出および安全な配信停止の設定 （474 ページ）
- グレイメールの検出および安全な配信停止のトラブルシューティング （480 ページ）

グレイメールの概要

グレイメール メッセージとは、ニュースレター、メーリング リストのサブスクリプション、ソーシャル メディア通知など、スパムの定義に適合しないメッセージです。これらのメッセージは、ある時点では役に立ちますが、その後エンドユーザがもはや受信したくないところまで価値が減少します。

グレイメールとスパムの違いは、エンドユーザが購読していないメッセージであるスパムと異なり、いずれかの時点（エンド ユーザが e-コマース Web サイトでニュースレターを購読したり、会議中に組織に連絡先詳細を提供した場合など）でエンド ユーザが意図的に電子メール アドレスを提供した点です。

電子メールゲートウェイでのグレイメール管理ソリューション

電子メールゲートウェイのグレイメール管理ソリューションは、統合されたグレイメール スキャン エンジンとクラウドベースの登録解除サービスの 2 つのコンポーネントで構成されます。

組織でグレイメール管理ソリューションを使用すると、以下が可能になります。

- 統合グレイメールエンジンを使用してグレイメールを識別し、適切なポリシー制御を適用します。
- 登録解除サービスを使用して、不要なメッセージを配信停止にする簡単なメカニズムをエンド ユーザに提供します。

これらに加えて、グレイメール管理ソリューションでは、組織に以下を提供することもできます。

- **エンドユーザへの安全な配信停止オプション。**配信停止オプションを模倣することは、よくあるフィッシング技法です。そのため、一般にエンドユーザは、不明な購読解約リンクのクリックに慎重になります。このようなシナリオでは、クラウドベースの登録解除サービスが元の配信停止 URI を抽出し、URI のレピュテーションをチェックして、エンドユーザに代わって配信停止プロセスを実行します。これにより、配信停止リンクを装った悪意のある脅威からエンド ユーザを保護します。
- **エンドユーザを対象として統一されたサブスクリプション管理インターフェイス。**さまざまなグレイメール送信者が、ユーザに配信停止リンクを表示するためのさまざまなレイアウトを使用しています。ユーザは、メッセージ本文で配信停止リンクを探して、配信停止を行う必要があります。グレイメール送信者に関係なく、グレイメール管理ソリューションは、配信停止リンクを表示するための共通のレイアウトを提供します。
- **管理者にさまざまなグレイメール カテゴリに対するより良い可視性を提供。**グレイメール エンジンでは、各グレイメールを3つのカテゴリに分類し（グレイメールの分類 （470ページ）を参照）、管理者はこれらのカテゴリに基づいてポリシー制御を設定できます。
- **スパムに対する有効性の改善**

関連項目

- グレイメールの分類 （470 ページ）

グレイメールの分類

グレイメール エンジンでは、各グレイメールを次のいずれかのカテゴリに分類します。

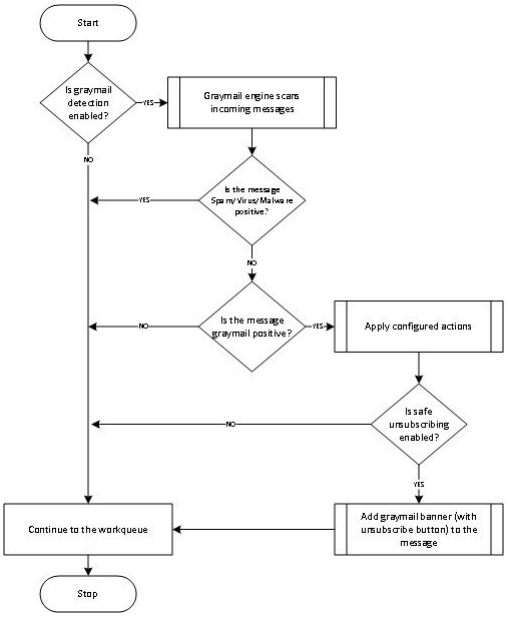
- **マーケティング メール。**Amazon.com からの新たに販売される製品の詳細に関する記事など、プロフェッショナル マーケティング グループから送信された広告メッセージ。
- **ソーシャル ネットワーク メール。**ソーシャル ネットワーク、出会い系/結婚 Web サイト、フォーラムなどからの通知メッセージ。例として、以下からのアラートなどが挙げられます。
  - LinkedIn。関心があると思われるジョブについて
  - CNET Forum。ユーザが投稿に応答した場合。

- **バルク メール**。認識されないマーケティング グループから送信された広告メッセージ（テクノロジー メディア企業の TechTarget からのニュースレターなど）。

グレイメール管理ソリューションの仕組み

次の手順では、グレイメール管理ソリューションのワークフローを示します。

図 *20*：グレイメール管理ソリューションのワークフロー



ワークフロー（Workflow）

手順

ステップ 1 電子メールゲートウェイは、着信メッセージを受信します。

ステップ 2 電子メールゲートウェイは、グレイメール検出が有効かどうかを確認します。グレイメール検出が有効になっている場合は、ステップ 3 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 3 電子メールゲートウェイは、メッセージがスパム、ウイルス、またはマルウェア陽性かどうかを確認します。陽性の場合は、ステップ 8 に進みます。それ以外の場合は、ステップ 4 に進みます。

ステップ 4 電子メールゲートウェイは、メッセージがグレイメールかどうかを確認します。メッセージがグレイメールの場合は、ステップ 5 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 5 電子メールゲートウェイは、削除、配信、バウンス、スパム隔離エリアへの隔離など、設定されたポリシーアクションを適用します。

ステップ 6 電子メールゲートウェイは、安全な配信停止が有効になっているかどうかを確認します。安全な配信停止が有効になっている場合は、ステップ 7 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 7 電子メールゲートウェイは、配信停止ボタン付きのバナーをメッセージに追加します。また、電子メールゲートウェイは、メッセージ本文内の既存の配信停止リンクを書き換えます。

ステップ 8 電子メールゲートウェイは、電子メールのワークキューの次の段階でメッセージを処理します。

次のタスク

受信から配信へのルーティングまで、電子メールがシステムで処理される様子の概要については、電子メール パイプラインについて （67 ページ）を参照してください。

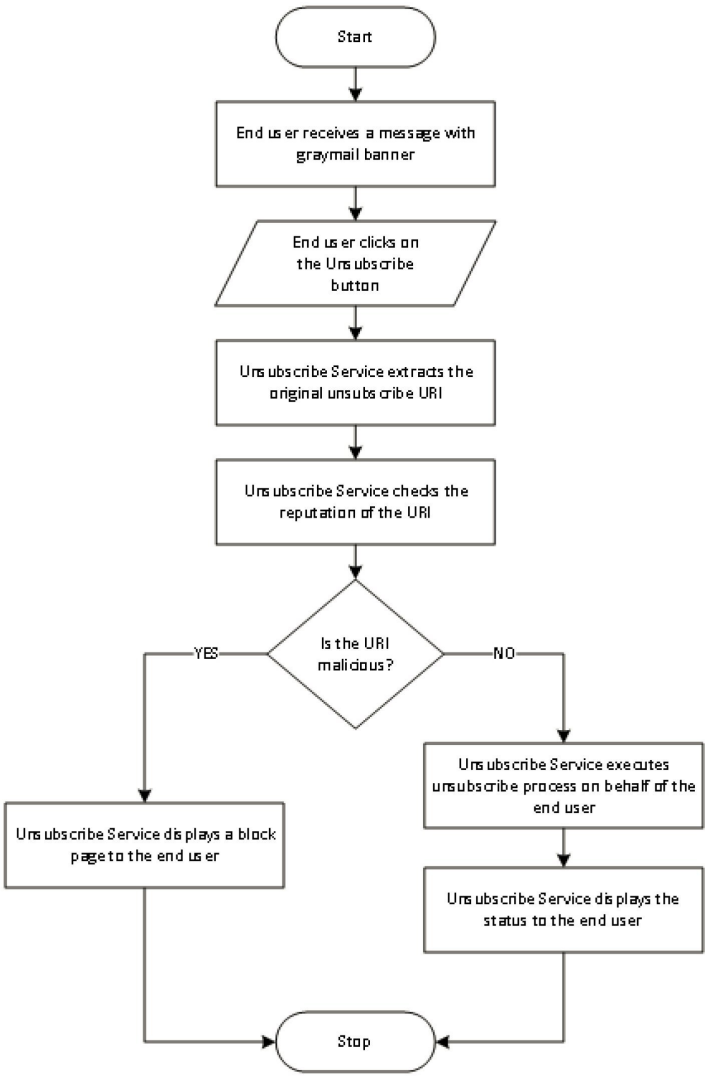
関連項目

- 安全な登録解除の仕組み （472 ページ）
- 電子メール パイプラインについて （67 ページ）

安全な登録解除の仕組み

次のフロー チャートで、安全な配信停止のしくみを示します。

図 *21* : 安全な配信停止のワークフロー



ワークフロー（Workflow）

手順

ステップ 1 エンドユーザがグレイメール バナーを含むメッセージを受信します。
ステップ 2 エンドユーザが [購読解約（Unsubscribe）] リンクをクリックします。
ステップ 3 登録解除サービスは、元の配信停止 URI を抽出します。
ステップ 4 登録解除サービスは、URI のレピュテーションを確認します。

ステップ 5 URI のレピュテーションに応じて、登録解除サービスは次のいずれかのアクションを実行します。

- URI に悪意がある場合、登録解除サービスは配信停止プロセスを実行せず、エンドユーザにブロック ページを表示します。
- URI に悪意がない場合、URI のタイプ（http または mailto）に応じて、登録解除サービスはグレイメール送信者に配信停止要求を送信します。
  - 要求が成功した場合、登録解除サービスはエンド ユーザに [登録が解除されました（Successfully unsubscribed）] というステータスを表示します。
  - 最初の配信停止要求が失敗した場合、登録解除サービスは [配信停止プロセスの進行中（Unsubscribe process in progress）] というステータスを表示し、配信停止のステータスを追跡できる URL を示します。

    エンドユーザはこの URL を使用して後でステータスを追跡することができます。最初の試行失敗後、登録解除サービスは 4 時間の間、定期的に配信停止要求を送信します。

    エンドユーザが後から配信停止プロセスのステータスを確認した場合、次のようになります。

  - （最初の試行失敗から）4 時間以内にいずれかの要求が成功した場合、登録解除サービスはエンド ユーザに [登録が解除されました（Successfully unsubscribed）] というステータスを表示します。
  - （最初の試行失敗から）4 時間以内にいずれの要求も成功しなかった場合、登録解除サービスはエンド ユーザに [登録できません（Unable to subscribe）] というステータスを表示し、グレイメールを手動で配信停止するための URL を示します。

グレイメールの検出および安全な配信停止の設定

- グレイメールの検出と安全な配信停止の要件 （475 ページ）
- クラスタ構成でのグレイメールの検出および安全な登録解除 （475 ページ）
- グレイメールの検出および安全な配信停止の有効化 （475 ページ）
- グレイメールの検出と安全な配信停止の着信メール ポリシーの設定 （476 ページ）
- グレイメール スキャン中に追加された IronPort-PHdr ヘッダー （477 ページ）
- メッセージ フィルタを使用したグレイメール アクションのバイパス （477 ページ）
- グレイメールのモニタリング （478 ページ）
- グレイメール ルールの更新 （479 ページ）
- エンドユーザに表示される [登録解除（Unsubscribe）] ページのカスタマイズ （480 ページ）
- エンドユーザのセーフリスト （480 ページ）
- ログの表示 （480 ページ）

グレイメールの検出と安全な配信停止の要件

- グレイメールを検出するには、アンチスパム スキャンをグローバルにイネーブルにする必要があります。これにはIronPort Anti-Spam機能、インテリジェント マルチスキャン機能、またはアウトブレイク フィルタのいずれかを使用できます。「スパムおよびグレイメールの管理 （461 ページ）」を参照してください。
- 安全な配信停止の場合、
  - 安全な配信停止機能キーを追加します。
  - エンドユーザのマシンは、インターネット経由で直接クラウドベースの登録解除サービスに接続できる必要があります。

クラスタ構成でのグレイメールの検出および安全な登録解除

グレイメールの検出および安全な配信停止は、マシン レベル、グループ レベルまたはクラスタ レベルでイネーブルにできます。

グレイメールの検出および安全な配信停止の有効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] を選択します。

ステップ 2 [グレイメール設定（Graymail Settings）] をクリックします。

ステップ 3 [グレイメール検出を有効にする（Enable Graymail Detection）] をオンにします。

ステップ 4 [安全な配信停止を有効にする（Enable Safe Unsubscribe）] をオンにします。

ステップ 5 （任意）[自動アップデートを有効にする（Enable Automatic Updates）] をチェックして、エンジンの自動アップデートを有効にします。

電子メールゲートウェイは、アップデートサーバから特定のエンジンに必要なアップデートを取得します。

ステップ 6 **[送信（Submit）]** をクリックします。

ステップ 7 （任意）[グローバル設定の編集（Edit Global Settings）] をクリックして、メッセージ スキャンのしきい値を設定します。詳細については、Intelligent Multi-Scan とグレイメール検出のグローバル設定 （481 ページ）を参照してください。

ステップ 8 変更を送信し、保存します。

次のタスク

CLI でグレイメールの検出および安全な配信停止のグローバル設定を構成するには、`imsandgraymailconfig` の CLI コマンドを使用します。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

グレイメールの検出と安全な配信停止の着信メール ポリシーの設定

はじめる前に

グレイメールの検出および安全な配信停止の有効化 （475 ページ）

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] をクリックします。

ステップ 2 変更するメール ポリシーの [グレイメール（Graymail）] 列のリンクをクリックします。

ステップ 3 要件に応じて、次のオプションを選択します。

- グレイメール検出の有効化
- 安全な配信停止の有効化
- 上記のアクションをすべてのメッセージまたは未署名のメッセージのいずれに適用するかを選択します。

  （注） S/MIME を使用して暗号化されている場合または S/MIME 署名が含まれる場合、電子メールゲートウェイはメッセージを署名済みとみなします。

- さまざまなグレイメール カテゴリ（マーケティング メール、ソーシャル ネットワーク メール、およびバルク メール）に対して実行するアクション。
  - メッセージの削除、配信、バウンス、または（スパム隔離エリアへの）隔離

    （注） 安全な配信停止オプションを使用する場合、配信または隔離するアクションを設定する必要があります。

  - 代替ホストへのメッセージの送信
  - メッセージの件名の変更
  - カスタム ヘッダーの追加
  - 代替エンベロープ受信者へのメッセージの送信

    （注） グレイメール陽性メッセージを代替エンベロープ受信者に送信する場合、バナーは追加されません。

  - メッセージのアーカイブ

    （注） 検出されたグレイメールのみをモニタする場合、ポリシーごとにグレイメール検出を有効にできます。さまざまなグレイメール カテゴリに対するアクションを設定する必要はありません。このシナリオでは、電子メールゲートウェイは、検出されたグレイメールに対して何もアクションを実行しません。

ステップ 4 変更を送信し、保存します。

次のタスク

（注） グレイメール検出の発信メールポリシーを設定することもできます。このシナリオでは、安全な配信停止は設定できないことに注意してください。

CLIでグレイメールの検出および安全な配信停止用のポリシーを設定するには、**policyconfig**を使用します。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

グレイメール スキャン中に追加された IronPort-PHdr ヘッダー

次の場合、グレイメール エンジンによって処理されるすべてのメッセージに、IronPort PHdr ヘッダーが追加されます。

- 電子メールゲートウェイでグレイメールエンジンがグローバルに有効である。
- グレイメール スキャンが特定のメール ポリシーに対して有効である。

（注） グレイメールスキャンが特定のメールポリシーに対して有効になっていない場合、電子メールゲートウェイでグレイメールエンジンがグローバルに有効であれば、すべてのメッセージに IronPort-PHdr ヘッダーが追加されます。

IronPort-PHdrヘッダーには符号化された独自の情報が含まれており、顧客による復号はできません。このヘッダーは、グレイメールの設定に関する問題のデバッグに関する追加情報を提供します。

（注） スパム対策エンジンまたはアウトブレイク フィルタが特定のメール ポリシーに対して有効な場合、IronPort-PHdrヘッダーは、特定のメールポリシーを通過するすべてのメッセージに追加されます。

メッセージ フィルタを使用したグレイメール アクションのバイパス

特定のメッセージにグレイメール アクションを適用しない場合、次のメッセージ フィルタを使用してグレイメール アクションをバイパスできます。

メッセージフィルタ アクション	説明
skip-marketingcheck	マーケティング メールに対するアクションのバイパス
skip-socialcheck	ソーシャル ネットワーク メールに対するアクションのバイパス

メッセージフィルタ アクション	説明
skip-bulkcheck	バルク メールに対するアクションのバイパス

次の例では、リスナー “private_listener” で受信したメッセージは、ソーシャル ネットワーク メールに対するグレイメール アクションをバイパスする必要があること指定しています。

```
internal_mail_is_safe:
if (recv-listener == 'private_listener')
{
skip-socialcheck
();
}
```

グレイメールのモニタリング

次のレポートを使用して、検出されたグレイメールに関するデータを表示できます。

レポート	含まれるグレイメール データ	詳細
[概要（Overview）] ページ > [受信メールサマリー（Incoming Mail Summary）]	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、グレーメール メッセージの総数。	[概要（Overview）] ページ（1015ページ）
[受信メール（Incoming Mail）] ページ > [グレーメール メッセージの上位送信者（Top Senders by Graymail Messages）]	グレーメールの上位送信者。	[受信メール（Incoming Mail）] ページ（1020ページ）
[受信メール（Incoming Mail）] ページ > [受信メールの詳細（Incoming Mail Details）]	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、すべての IP アドレス、ドメイン名、またはネットワーク オーナーのグレーメール メッセージの総数。	
[受信メール（Incoming Mail）] ページ > [受信メールの詳細（Incoming Mail Details）] > [送信者プロファイル（Sender Profile）]（ドリル ダウン ビュー）	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、指定されたIPアドレス、ドメイン名、またはネットワーク オーナーのグレーメール メッセージの総数。	

レポート	含まれるグレイメール データ	詳細
[内部ユーザ（Internal Users）] ページ > [グレーメールの上位ユーザ（Top Users by Graymail）]	グレーメールを受信する上位エンドユーザ。	[内部ユーザ（Internal Users）] ページ（1030ページ）
[内部ユーザー（Internal Users）] ページ > [ユーザー メール フローの詳細（User Mail Flow Details）]	グレーメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレーメール メッセージの数と、すべてのユーザのグレーメール メッセージの総数。	
[内部ユーザー（Internal Users）] ページ > [ユーザー メール フローの詳細（User Mail Flow Details）] > [内部ユーザー（Internal User）]（ドリルダウン ビュー）	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの受信グレイメール メッセージの数と、指定されたユーザのグレイメール メッセージの総数。	

AsyncOS 9.5 以降にアップグレード後、メール ポリシーのアンチスパム設定でマーケティング メールのスキャンをイネーブルにした場合は、次の点に注意してください。

- マーケティング メッセージの数は、アップグレードの前後に検出されたマーケティング メッセージの合計です。
- グレイメール メッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数は含まれません。
- 試行されたメッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数も含まれます。

グレイメール ルールの更新

サービスのアップデートをイネーブルにした場合、シスコのアップデート サーバからグレイメール管理ソリューションのスキャン ルールを取得できます。しかし、一部のシナリオでは（たとえば、サービスの自動アップデートをディセーブルにした場合またはサービスの自動アップデートが機能していない場合）、グレイメール ルールを手動で更新できます。

グレイメール ルールを手動で更新するには、次のいずれかを実行します。

- Web インターフェイスで、[セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] ページに移動して [今すぐ更新（Update Now）] をクリックします。
- CLI で graymailupdate コマンドを実行します。

既存のグレイメール ルールの詳細を確認するには、Web インターフェイスで [IMSおよびグレイメール（IMS and Graymail）] ページの [ルールの更新（Rule Updates）] を確認するか、または CLI で graymailstatus コマンドを使用します。

エンドユーザに表示される [登録解除（Unsubscribe）] ページのカスタマイズ

エンドユーザが配信停止リンクをクリックすると、登録解除サービスにより、配信停止プロセスのステータスを示すシスコブランドの配信停止ページが表示されます（安全な登録解除の仕組み（472ページ）を参照）。[セキュリティサービス（Security Services）]>[ブロックページカスタマイズ（Block Page Customization）] を使用して、配信停止ページの外観および組織のブランディングの表示（企業ロゴ、連絡先情報など）をカスタマイズできます。この説明については、サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ（552ページ）を参照してください。

エンドユーザのセーフリスト

組織のエンドユーザが自分の電子メールアカウントのセーフリストを設定している場合は、セーフリストの送信者からのグレイメールメッセージはグレイメールスキャンエンジンによってスキャンされません。セーフリストの詳細については、セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御（1161ページ）を参照してください。

ログの表示

グレイメールの検出および安全な配信停止情報は、次のログに書き込まれます。

- **グレイメール エンジン ログ**。グレイメールエンジン、ステータス、設定などの情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。
- **グレイメール アーカイブ**。アーカイブされたメッセージ（スキャン済みの「アーカイブメッセージ」アクションに関連付けられているメッセージ）が含まれます。この形式は、mbox 形式のログファイルです。
- **メール ログ**。グレイメールの検出および安全な配信停止用のバナーの追加についての情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

グレイメールの検出および安全な配信停止のトラブルシューティング

安全な配信停止を実行できない（480ページ）

安全な配信停止を実行できない

問題

配信停止リンクをクリックした後、エンドユーザに「...を配信停止できません」というメッセージが表示されます。

ソリューション

この問題は、登録解除サービスがエンドユーザの代わりに安全な配信停止を実行できない場合に発生することがあります。次に、登録解除サービスが安全な配信停止を実行できない一般的なシナリオをいくつか示します。

- 配信停止 URI または mailto アドレスが間違っている。
- 配信停止にエンドユーザのクレデンシャルを要求する Web サイト。
- エンドユーザに自分の電子メールアカウントにログインし、配信停止要求を確認するように要求する Web サイト。

- Web サイトで captcha を解決するよう要求され、登録解除サービスで captcha を解決できない。
- インタラクティブな配信停止を必要とする Web サイト。

エンドユーザは [購読解約（Unsubscribe）] ページの下部に表示されている URL を使用して購読解約を手動で行えます。

Intelligent Multi-Scan とグレイメール検出のグローバル設定

電子メールゲートウェイのスループットを最適化するために、Cisco Intelligent Multi-Scan とグレイメールによってメッセージをスキャンするしきい値とタイムアウトを設定できます。これらの設定は、Cisco Intelligent Multi-Scan とグレイメールの設定に共通です。

1. [セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] を選択します。
2. [グローバル設定を編集（Edit Global Settings）] をクリックします。
3. Cisco Intelligent Multi-Scan とグレイメール検出でスキャンするしきい値を選択します。

   デフォルトの値は次のとおりです。

   - 512 K 以下は常にスキャンします。

   （注） この設定は、グレイメール検出と安全な配信停止には適用されません。

   - 1 M 超はスキャンしないでください。

4. メッセージをスキャンするときにタイムアウトを待機する秒数を入力します。

   秒数を指定する場合は、1 ～ 120 の整数を入力します。デフォルト値は 60 秒です。

   大部分のユーザでは、スキャンする最大メッセージサイズもタイムアウト値も変更する必要がありません。最大メッセージサイズの設定を小さくして、電子メールゲートウェイのスループットを最適化できる可能性があります。

5. 変更を送信して確定します。

スパム対策ポリシーの定義

各メールポリシーで、スパムと見なされるメッセージと、これらのメッセージで行われるアクションを指定します。また、ポリシーが適されるメッセージをスキャンするエンジンを指定します。

デフォルトの着信および発信メールポリシーに対して、異なる設定を設定できます。別のユーザに異なるスパム対策ポリシーが必要な場合は、異なるスパム対策設定を持つ複数のメールポ

リシーを使用します。ポリシーごとに1つのスパム対策ソリューションだけをイネーブルにできます。同じポリシーに両方をイネーブルにすることはできません。

はじめる前に

- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法（462ページ）のテーブルの、ここまでのすべてのステップを実行します。
- 次の概念を十分に理解してください。
  - 陽性および陽性と疑わしいスパムのしきい値について （485 ページ）
  - 設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション （486 ページ）
  - 正規の送信元からの不要なマーケティング メッセージ （486 ページ）
  - 複数のスパム対策ソリューションをイネーブルにした場合：異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例 （488 ページ）
  - スパム対策スキャン中に追加されるヘッダー （490 ページ）
- 「スパム対策アーカイブ」ログにスパムをアーカイブする場合は、ログ（1391ページ）も参照してください。
- 代替メール ホストにメッセージを送信する場合は、配信ホスト変更アクション （247ページ）も参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] ページに移動します。

または

ステップ 2 [メールポリシー（Mail Policies）] > [発信メールポリシー（Outgoing Mail Policies）] ページに移動します。

ステップ 3 [スパム対策（Anti-Spam）] 列で、任意のメール ポリシーのリンクをクリックします。

ステップ 4 [このポリシーのスパム対策スキャンを有効にする（Enable Anti-Spam Scanning for this Policy）] セクションでは、ユーザがポリシーで使用するスパム対策ソリューションを選択します。

表示されるオプションは、イネーブルにしたスパム対策スキャン ソリューションに基づきます。

デフォルト以外のメールポリシーの場合、デフォルトのポリシーを使用すると、そのページの他のオプションはディセーブルになります。

このメールポリシーに対してスパム対策スキャンをまとめてディセーブルにすることもできます。

ステップ 5 スパムであることが確実な電子メール、スパムだと疑われる電子メール、およびマーケティング メッセージの設定を行います。

オプション	説明
スパムだと疑われる電子メールのスキャンを有効にする（Enable Suspected Spam Scanning） マーケティング電子メールのスキャンを有効にする（Enable Marketing Email Scanning）	オプションを選択します。 陽性と判定されたスパムのスキャンはスパム対策スキャンが有効の場合は常に有効です。
このアクションをメッセージに適用する（Apply This Action to Message）	陽性と判定されたスパム、陽性と疑わしいスパム、または不要なマーケティング メッセージに対する全般的なアクションを選択します。 • デリバリ • ドロップ（Drop） • バウンス（Bounce） • 検疫（Quarantine）
（任意）代替ホストに送信（Send to Alternate Host）	識別されたメッセージを別の宛先メールホスト（SMTPルートまたはDNSに示されているもの以外のメール サーバ）に送信できます。 IP アドレスまたはホスト名を入力します。ホスト名を入力すると、Mail Exchange（MX）が最初に検索されます。キーが見つからない場合、DNS サーバの A レコードが使用されます（SMTP ルートと同じ）。 たとえば、追加の検査のサンドボックスのメールサーバなど、メッセージの方向を変更するにはこのオプションを使用します。 重要な詳細情報については、配信ホスト変更アクション （247 ページ）を参照してください。

オプション	説明
件名へテキストを追加（Add Text to Subject）	特定のテキスト文字列を前または後に追加して、識別されたメッセージ上の件名のテキストを変更することにより、スパムおよび不要なマーケティング メッセージをユーザが識別およびソートしやすくできます。 （注） このフィールドでは空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば付加した場合、少数の末尾にスペースを含むテキスト `[SPAM]` を追加します。 [件名へテキストを追加（Add Text to Subject）] フィールドでは US-ASCII 文字だけが許可されます。
[詳細オプション（Advanced Options）]（カスタム ヘッダーとメッセージ配信用）	
カスタムヘッダーを追加(オプション)（Add Custom Header (Optional)）	識別されたメッセージにカスタム ヘッダーを追加できます。 [詳細（Advanced）] をクリックし、ヘッダーと値を定義します。 カスタム ヘッダーとコンテンツ フィルタを併用することで、陽性と疑わしいスパム メッセージ内の URL をリダイレクトして Cisco Web セキュリティ プロキシ サービスにパススルーするなどのアクションを実行できます。詳細については、カスタムヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）を参照してください。
（任意）代替エンベロープ受信者に送信（Send to an Alternate Envelope Recipient）	識別されたメッセージを代替エンベロープ受信者アドレスに送信できます。 [詳細（Advanced）] をクリックして代替アドレスを定義します。 たとえば、スパムであると識別されたメッセージを後で調査するために、管理者のメールボックスにルーティングできます。複数受信者メッセージの場合は、単一のコピーだけが代替受信者に送信されます。
アーカイブ メッセージ（Archive Message）	識別されたメッセージを「スパム対策アーカイブ」ログにアーカイブできます。この形式は、mbox 形式のログ ファイルです。
スパムしきい値（Spam Thresholds）	デフォルトのしきい値を使用するか、陽性と判定されたスパムのしきい値および陽性と疑わしいスパムの値を入力します。

ステップ 6 変更を送信し、保存します。

次のタスク

発信メールのスパム対策スキャンをイネーブルにした場合は、特にプライベートリスナーに関連するホストアクセステーブルのスパム対策設定を確認します。メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （115 ページ） を参照してください。

関連項目

- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法（462 ページ）
- 陽性および陽性と疑わしいスパムのしきい値について （485 ページ）
- 設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション （486 ページ）
- 正規の送信元からの不要なマーケティング メッセージ （486 ページ）
- カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）
- 異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例 （488 ページ）

陽性および陽性と疑わしいスパムのしきい値について

メッセージがスパムであるかどうかを評価するときに、両方のスパム対策スキャン ソリューションは、メッセージの総合スパム評点に達するために何千ものルールを適用します。スコアは、メッセージをスパムとして見なすかどうかを決定するため、該当するメールポリシーで指定されたしきい値と比較されます。

最高精度では、スパムとして陽性と識別する精度はデフォルトでかなり高く設定されています。90～100の範囲のメッセージスコアは、陽性と判定されたスパムであると見なされます。陽性と疑わしいスパムのデフォルトのしきい値は 50 です。

- 陽性と疑わしいスパムのしきい値未満のスコアを持つメッセージは正規のメッセージと見なされます。
- 陽性と疑わしいスパムのしきい値を超えているが、陽性と識別されたしきい値未満のメッセージは、スパムの疑いがあると見なされます。

各メールポリシーで陽性および陽性と疑わしいスパムのしきい値をカスタマイズし、組織のスパムの許容レベルを反映するスパム対策ソリューションを設定できます。

50～99 の値に陽性と判定されたスパムのしきい値を変更できます。25 から陽性と判定されたスパムに指定した値までの範囲の任意の値に、陽性と疑わしいスパムのしきい値を変更できます。

しきい値を変更する場合：

- 低い番号（より積極的な設定）を指定すると、より多くのメッセージをスパムとして識別し、より多くの誤検出が生成される場合があります。これによって、ユーザがスパムを受けるリスクは低くなりますが、スパムとしてマークされた正規のメールを受けるリスクは高くなります。

- より高い数（より保守的な設定）を指定すると、より少ないメッセージをスパムとして識別し、より多くのスパムを配信する可能性があります。これによって、ユーザがスパムを受けるリスクは高くなりますが、正規のメールがスパムとして除かれるリスクは低くなります。理想的には、正しく設定した場合、メッセージの件名はそのメッセージがスパムである可能性が高いことを識別し、メッセージは配信されます。

陽性と判定されたスパムと陽性と疑わしいスパムに対して異なるアクションを定義できます。たとえば、「陽性と判定された」スパムをドロップしますが、「陽性と疑わしい」スパムは隔離します。

関連項目

- スパム対策ソリューション （462 ページ）
- 設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション （486 ページ）

設定例：陽性と判定されたスパムに対するアクションと陽性と疑わしいスパムに対するアクション

スパム	サンプル アクション（**Aggressive**）	サンプル アクション（**Conservative**）
陽性と判定された	削除	• メッセージの件名に「`[Positive Spam]`」を追加して配信、または • 検疫（Quarantine）
陽性と疑わしい	メッセージの件名に「`[Suspected Spam]`」を追加して配信	メッセージの件名に「`[Suspected Spam]`」を追加して配信

積極的な例では、陽性と識別されたメッセージをドロップし、スパムの疑いのあるメッセージだけにタグを付けます。管理者およびエンドユーザは、着信メッセージの件名行を調べて、誤検出でないかどうかを確認でき、管理者は必要に応じて、陽性と疑わしいスパムのしきい値を調整できます。

保守的な例では、陽性と判定されたスパムと陽性と疑わしいスパムは、件名を変更して通過されます。ユーザは、陽性と疑わしいスパムおよび陽性と判定されたスパムを削除できます。この方式は、1 番目の方式よりも保守的です。

メール ポリシーの積極的および保守的なポリシーの詳細については、管理例外 （321 ページ）を参照してください。

正規の送信元からの不要なマーケティング メッセージ

マーケティング電子メール設定をメール ポリシーのアンチスパム設定の下に構成した場合、AsyncOS 9.5 for Email へのアップグレード後、アンチスパム設定の下のマーケティング電子メー

ル設定は同じポリシーのグレイメール設定の下に移動されます。スパムおよびグレイメールの管理 （461 ページ） を参照してください。

カスタムヘッダーを使用して、陽性と疑わしいスパム内のURLをCisco Web セキュリティ プロキシにリダイレクトする：設定例

受信者が陽性と疑わしいスパム内のリンクをクリックしたときに、その要求が Cisco Web セキュリティ プロキシ サービスにルーティングされるように、メッセージ内の URL を書き換えることができます。これにより、クリック時にサイトの安全性が評価され、既知の悪意のあるサイトへのアクセスがブロックされます。

はじめる前に

URL フィルタリング機能とその前提条件をイネーブルにしてください。URL フィルタリングの設定 （544 ページ）を参照してください。

手順

ステップ 1 陽性と疑わしいスパム メッセージにカスタム ヘッダーを適用します。

a) [メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policies）] を選択します。
b) [スパム対策（Anti-Spam）]列で、ポリシー（デフォルト ポリシーなど）のリンクをクリックします。
c) [サスペクトスパムの設定（Suspected Spam Settings）] セクションで、陽性と疑わしいスパムのスキャンをイネーブルにします。
d) [詳細（Advanced）] をクリックして、[カスタムヘッダーを追加（Add Custom Header）] オプションを表示します。
e) url_redirect などのカスタム ヘッダーを追加します。
f) 変更を送信し、保存します。

ステップ 2 カスタム ヘッダーを持つメッセージ内の URL をリダイレクトするコンテンツ フィルタを作成します。

a) [メールポリシー（Mail Policies）]>[受信コンテンツフィルタ（Incoming Content Filters）] を選択します。
b) [フィルタの追加（Add Filter）] をクリックします。
c) フィルタに url_redirect という名前を付けます。
d) [条件を追加（Add Condition）] をクリックします。
e) [その他のヘッダー（Other Header）] をクリックします。
f) ヘッダー名 url_redirect を入力します。

これが上記で作成したヘッダーと正確に一致することを確認してください。

g) [ヘッダーが存在（Header exists）] を選択します。
h) [OK] をクリックします。

i) [アクションを追加（Add Action）] をクリックします。
j) [URLカテゴリ（URL Category）] をクリックします。
k) [利用可能なカテゴリ（Available Categories）] ですべてのカテゴリを選択し、[選択したカテゴリ（Selected Categories）] に追加します。
l) [URLに対するアクション（Action on URL）] で、[Cisco Security Proxyにリダイレクト（Redirect to Cisco Security Proxy）] を選択します。
m) [OK] をクリックします。

ステップ 3 メール ポリシーにコンテンツ フィルタを追加します。

a) [メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policies）] を選択します。
b) [コンテンツフィルタ（Content Filters）] 列で、前の手順で選択したポリシーのリンクをクリックします。
a) [コンテンツフィルタを有効にする（Enable Content Filters）] を選択します（選択されていない場合）。
b) チェックボックスを選択して、**url_filtering** コンテンツ フィルタをイネーブルにします。
c) 変更を送信し、保存します。

次のタスク

関連項目

- URL のリダイレクト （518 ページ）
- コンテンツ フィルタ （325 ページ）

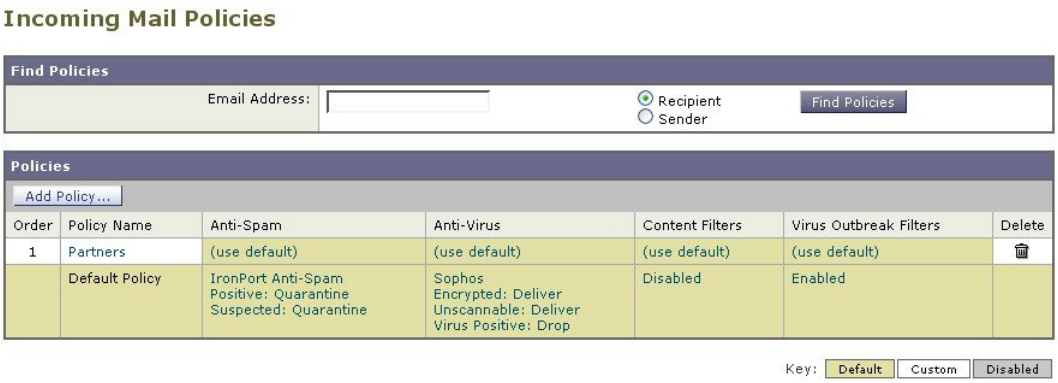
異なるメール ポリシーでの異なるスパム対策スキャン エンジンの有効化：設定例

システム セットアップ ウィザード（またはCLI の systemsetup コマンド）を使用すると、Cisco Intelligent Multi-Scan または Cisco Anti-Spam エンジンのいずれかをイネーブルにするオプションが示されます。システムセットアップ中に両方をイネーブルにできませんが、システムセットアップが完了した後に[セキュリティサービス（Security Services）]メニューを使用して、選択しなかったスパム対策ソリューションをイネーブルにできます。

システムのセットアップが終了すれば、[メール ポリシー（Mail Policies）]>[着信メール ポリシー（Incoming Mail Policies）] ページから着信メール ポリシー用のスパム対策スキャン ソリューションを設定できます（スパム対策スキャンは、発信メール ポリシーでは通常無効です）。ポリシーのスパム対策スキャンもディセーブルにできます。

この例では、デフォルトのメールポリシーおよび「パートナー」ポリシーで、陽性スパムおよび陽性と疑わしいスパムを隔離するために Cisco Anti-Spam スキャン エンジンを使用しています。

図 *22 :* メール ポリシー：受信者ごとのスパム対策エンジン

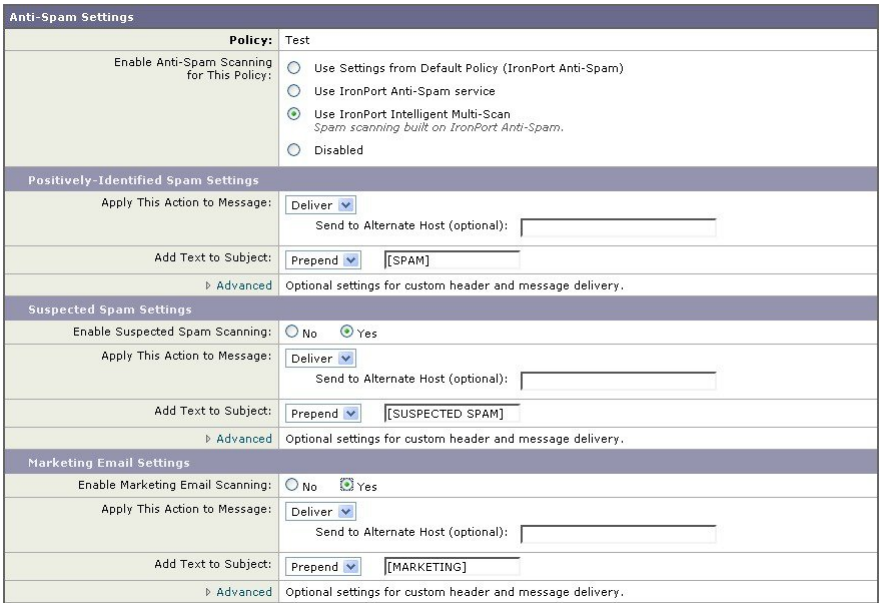


パートナーのポリシーを変更して、不要なマーケティング メッセージに対して Cisco Intelligent Multi-Scan とスキャンを使用するには、パートナーの行に対応する [スパム対策（Anti-Spam）] 列のエントリ（[デフォルトを使用（Use Default）]）をクリックします。

スキャン エンジンに Cisco Intelligent Multi-Scan を選択し、不要なマーケティング メッセージの検出をイネーブルにする場合は [はい（Yes）] を選択します。不要なマーケティング メッセージの検出にデフォルト設定を使用します。

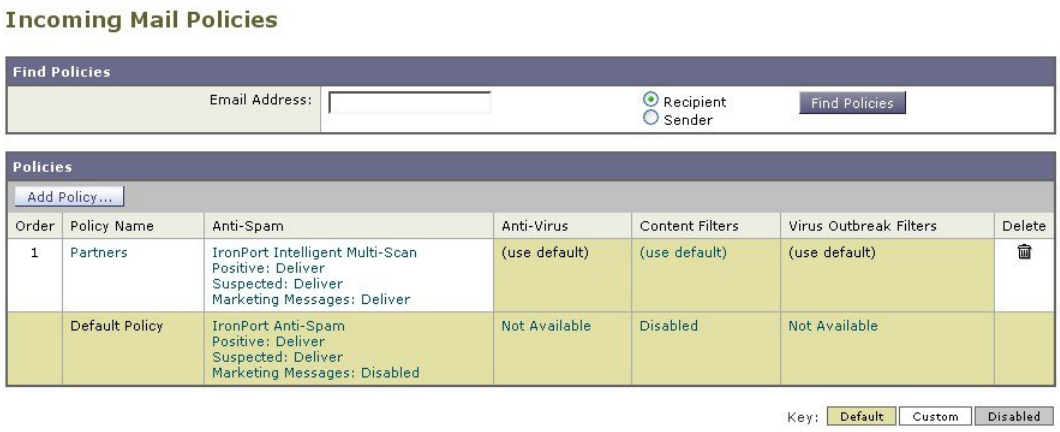
次の図は、Cisco Intelligent Multi-Scan と不要なマーケティング メッセージの検出がポリシーでイネーブルに設定されていることを示します。

図 *23 :* メール ポリシー：*Cisco Intelligent Multi-Scan* のイネーブル化



変更の送信と確定後のメール ポリシーは次のようになります。

図 *24 :* メール ポリシー：***Intelligent Multi-Scan*** がイネーブルにされたポリシー



スパムフィルタからの電子メールゲートウェイ生成メッセージの保護

電子メールゲートウェイから自動送信された電子メールメッセージ（メールアラートおよびスケジュールレポートなど）には、誤ってスパムとして識別される可能性のある URL または他の情報が含まれることがあるため、確実に配信されるよう次を実行します。

スパム対策スキャンをバイパスする着信メールポリシーにこれらのメッセージの送信者を含めます。送信者および受信者のグループのメール ポリシーの作成 （317ページ）およびアンチスパム システムのバイパス アクション （253 ページ）を参照してください。

スパム対策スキャン中に追加されるヘッダー

- いずれかのスパム対策スキャン エンジンがメール ポリシーでイネーブルにされている場合、そのポリシーを通過した各メッセージは次のヘッダーをメッセージに追加します。

  X-IronPort-Anti-Spam-Filtered: true

  X-IronPort-Anti-Spam-Result

  2 番目のヘッダーには、メッセージのスキャンに使用されたルールとエンジンのバージョンをシスコ サポートで識別するための情報が含まれます。結果の情報は、符号化された独自の情報であり、顧客による復号は可能ではありません。

- Cisco Intelligent Multi-Scan では、サードパーティ製アンチスパム スキャン エンジンからのヘッダーも追加します。
- 陽性と判定されたスパム、陽性と疑わしいスパム、不要なマーケティング メールとして識別される特定のメールポリシーのすべてのメッセージに追加する追加のカスタムヘッダーを定義できます。スパム対策ポリシーの定義 （481 ページ） を参照してください。

関連項目

- カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）

誤って分類されたメッセージのシスコへの報告

分類が誤っていると思われるメッセージを、分析用にシスコに報告できます。報告されたメッセージは、製品の精度および有効性を高めるために使用されます。

誤って分類されたメッセージは、次のカテゴリに属するものを報告いただけます。

- 検出されなかったスパム
- スパムとしてマークされたがスパムではないメッセージ
- 検出されなかったマーケティング メッセージ
- マーケティング メッセージとしてマークされたがマーケティング メッセージではないメッセージ
- 検出されなかったフィッシング メッセージ

関連項目

- 誤って分類されたメッセージのシスコへの報告方法 （491 ページ）
- 送信を追跡する方法 （497 ページ）

誤って分類されたメッセージのシスコへの報告方法

はじめる前に

誤って分類されたメッセージをシスコに報告する前に、次の手順を実行する必要があります。この手順は一度だけ実行してください。

手順

ステップ 1 Cisco Talos 電子メールステータスポータルで管理者として登録するには、次のいずれかの方法を使用します。

（注） Cisco Talos 電子メールステータスポータルは、電子メール管理者がポータル上で電子メール送信を表示および追跡できる Web ベースのツールです。

- 組織内で初めてポータルにアクセスする管理者である場合の登録：

  1. シスコのクレデンシャルを使用して Cisco Talos 電子メールステータスポータル（https://talosintelligence.com/email_status_portal）にログインします。
  2. [アカウントの管理（Manage Account）] をクリックします。
  3. [ドメインの追加（Add Domain）] をクリックします。

4. ドメインをポータルに登録するには、[ドメイン（Domain）]フィールドに組織のドメイン名を入力します。

   （注） 必ず有効なドメイン名を入力します。たとえば、example.com は電子メールアドレス user@example.com のドメイン名です。組織内に複数のドメインがある場合は、必ずすべてのドメインを追加します。

5. ステップ「d」で入力したドメインの所有者である場合は、[所有するドメイン（I own this domain）] チェックボックスをオンにします。

   （注） [所有するドメイン（I own this domain）] チェックボックスをオンにしない場合、ドメインの表示アクセス権のみが付与されます。詳細については、次の URL にある Cisco Talos 電子メールステータスポータルのヘルプページを参照してください。 https://talosintelligence.com/tickets/email_submissions/help

6. **[送信（Submit）]** をクリックします。

   [送信（Submit）] をクリックすると、6 桁の文字の確認コードを示す電子メールが自動的に postmaster@domain.com（domain.com はステップ「d」で入力したドメイン）に送信され、ドメインの所有権が確認されます。

   組織が postmaster@domain.com を使用していないか、または管理者に postmaster メールボックスへのアクセス権がない場合には、メッセージフィルタを（すべての電子メールゲートウェイ上で）作成して、SubmissionPortal@cisco.com から postmaster@domain.com に送信されるメッセージを別の電子メールアドレスにリダイレクトします。次に示すのは、サンプルのメッセージ フィルタです。

   ```
   redirect_postmaster: if (rcpt-to == "postmaster@domain.com") AND (mail-from ==
   "^SubmissionPortal@cisco.com$") { alt-rcpt-to ("admin@domain.com"); }
   ```

7. [ドメイン所有者確認コード（Domain Ownership Verification Code）] ダイアログボックスに 6 桁の文字の確認コードを入力して、ドメインの所有権を確認します。
8. [確認コードの送信（Submit Verification Code）] をクリックします。

   [確認コードの送信（Submit Verification Code）] ボタンをクリックすると、自動的に管理者アクセス権が付与されます。登録 ID が自動的に生成され、ポータルの [アカウントの管理（Manage Accounts）] セクションで確認できます。この登録 ID は組織内すべての電子メールゲートウェイで使用できます。

   （注） 登録 ID は、特定の組織に属している Cisco E メールセキュリティ ゲートウェイから行われた送信を識別するための一意の ID です。

- 組織内の管理者がポータルにすでに登録されている場合の登録：

1. シスコのクレデンシャルを使用して Cisco Talos 電子メールステータスポータル（https://talosintelligence.com/email_status_portal）にログインします。
2. [アカウントの管理（Manage Account）] をクリックします。
3. [ドメインの追加（Add Domain）] をクリックします。

4. ドメインをポータルに登録するには、[ドメイン（Domain）]フィールドに組織のドメイン名を入力します。

   （注） 必ず有効なドメイン名を入力します。たとえば、`example.com` は電子メールアドレス `user@example.com` のドメイン名です。組織内に複数のドメインがある場合は、必ずすべてのドメインを追加します。

5. **[送信（Submit）]** をクリックします。

[登録（Register）]をクリックすると、すでにポータルに登録されている管理者に電子メール通知が送信されます。この管理者はポータルにログインし、[アカウントの管理（Manage Accounts）] の [権限要求（Permission Requests）] セクションで [承認（Approve）] をクリックして、登録要求を承認する必要があります。

登録要求が承認されると、登録IDが自動的に生成され、ポータルの[アカウントの管理（Manage Accounts）]セクションに表示できます。この登録 ID は組織内すべての電子メールゲートウェイで使用できます。

（注） 登録 ID は、特定の組織に属している Cisco E メール セキュリティ ゲートウェイから行われた送信を識別するための一意の ID です。

ステップ 2 組織内のすべての電子メールゲートウェイについて、Cisco Talos 電子メールステータスポータルから生成された登録 ID を追加します。

1. Web インターフェイスを使用して 電子メールゲートウェイにログインします。
2. [システム管理（System Administration）] > [Cisco Talos 電子メールステータスポータル登録（Cisco Talos Email Status Portal Registration）] に移動します。
3. 電子メールゲートウェイがクラスタの一部である場合は、モードをクラスタレベルに設定します。
4. [登録 ID の設定（Set Registration ID）] をクリックします。
5. [登録ID（Registration ID）] フィールドに、Cisco Talos 電子メールステータスポータルから取得した登録 ID を入力します。
6. 変更を送信し、保存します。
7. 電子メールゲートウェイがクラスタの一部ではない場合、組織内すべての電子メールゲートウェイでステップ 1 ～ 6 を繰り返す必要があります。

CLI で `portalregistrationconfig` コマンドを使用して登録 ID を設定することもできます。

誤って分類されたメッセージのシスコへの報告方法

詳細については、以下を参照してください。

- 『How to Submit Email Messages to Cisco』ドキュメント（https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html#anc5）。
- Cisco Talos 電子メールステータスポータルのヘルプページ（https://talosintelligence.com/tickets/email_submissions/help）。

手順

ステップ 1 誤って分類されたメッセージのシスコへの報告方法 （491 ページ）の「**はじめる前に**」の項に記載されている手順を実行します。

ステップ 2 誤って分類されたメッセージをシスコに報告するには、次の方法のいずれかを使用します。

- Cisco E メール セキュリティ プラグインの使用 （494 ページ）
- 誤って分類されたメッセージの添付ファイルとしての転送 （495 ページ）

誤って分類されたメッセージをシスコに報告すると、ポータルの [アカウントの管理（Manage Account）] セクションにある [電子メール通知とレポート（Email Notification and Reports）] ボタンで選択したオプションに基づいた電子メール通知を受信します。

（注） [電子メール通知とレポート（Email Notification and Reports）] ボタンの下にある [マイ送信通知（My Submission Notifications）] および [マイ送信レポート（My Submission Reports）] オプションは、デフォルトでオフに設定されています。詳細については、次の URL にある Cisco Talos 電子メールステータスポータルのヘルプページを参照してください。 https://talosintelligence.com/tickets/email_submissions/help

次のタスク

送信を追跡する方法 （497 ページ）

Cisco E メール セキュリティ プラグインの使用

Cisco Email Security Plug-In は、Microsoft Outlook を使用してユーザー（電子メール管理者とエンドユーザー）が誤って分類されたメッセージをシスコへ報告できるようにするツールです。このプラグインを Microsoft Outlook の一部として展開する場合、レポート メニューが Microsoft Outlook の Web インターフェイスに追加されます。このプラグインのメニューを使用して、誤って分類されたメッセージをレポートできます。

その他の情報

- 次のページから Cisco Email Security Plug-In をダウンロードできます：https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=284900944&flowid=41782&softwareid=283090986。
- 詳細については、『Cisco Email Security Plug-In Administrator Guide』http://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.htmlを参照してください。

誤って分類されたメッセージの添付ファイルとしての転送

メッセージのカテゴリに応じて、以下の表に表示されているアドレスにRFC 822添付ファイルとしてそれぞれの誤って分類されたメッセージを転送できます。

電子メールの送信	定義	送信方法	送信に関するユーザの考慮事項
スパム/フィッシング	未承認および望ましくないメール。スパム/フィッシングは正当ではなく、悪意のあるもの（フィッシング、ウイルス、マルウェア、詐欺など）である可能性もあります。	spam@access。 ironport.com phish@access。 ironport.com virus@access。 ironport.com Outlookプラグインの[迷惑メール（Spam）]、[フィッシング（Phish）]、または[ウイルス（Virus）]ボタン	ユーザの受信トレイに配信されますが、ユーザはメッセージをスパムまたはフィッシングと見なします。 スパムとして検出されましたが、ユーザは正当なメッセージと見なします。
正当mate	スパムではなく、正当な（正常な）電子メール。「ハム」とも呼ばれます。	ham@access。 ironport.com Outlookプラグインの[迷惑メールではない（Not Spam）]ボタン	マーケティング/グレイメールメッセージはマーケティング/グレイメールとして検出されない。

電子メールの送信	定義	送信方法	送信に関するユーザの考慮事項
マーケティング/グレイメール	マーケティングは、商用のバルク電子メールである正当な（スパムではない）電子メールです。通常はサブスクリプションベースで、不要な場合もあります。 ユーザは、送信者に対し故意または無意識にメールを要求した可能性があります。たとえば、会議でバッジをスワイプしたり、オンラインで購入した場合が考えられます。正当なサブスクリプションベースのマーケティング電子メールには、購読解除メカニズムがあります。 グレイメールは、マーケティングおよびその他の正当なバルク電子メールを含むより広範囲なカテゴリです。	ads@access。 ironport.com Outlook プラグインの[マーケティング（Marketing）] ボタン	スパムとして検出されても、ユーザは正当なメッセージと見なします。
非マーケティング/グレイメール	バルクでもサブスクリプションベースでもない正規の電子メール（スパムではない）。通常、個人間や取引に関するものです。	not_ads@access。 ironport.com	マーケティング/グレイメールとしてとして検出されても、ユーザはメッセージを取引関連またはマーケティング/グレイメールではないものと見なします。

次の電子メールプログラムのいずれかを使用してメッセージを転送すると、最適な結果を得ることができます。

- Apple Mail
- Microsoft Outlook for Mac
- Microsoft Outlook Web App
- Mozilla Thunderbird

⚠

注意 Microsoft Outlook 2010、2013、2016 for Microsoft Windows を使用している場合は、誤って分類されたメッセージを報告するのに、Cisco Email Security Plug-In または Microsoft Outlook Web App を使用する必要があります。これは、Windows 用の Outlook が必要なヘッダーをそのままにしてメッセージを転送できないためです。また、添付ファイルとして元のメッセージを転送することができる場合にのみ、モバイル プラットフォームを使用します。

送信を追跡する方法

送信の詳細が示された電子メール通知を受け取ったら、Cisco Talos 電子メールステータスポータルで送信を表示および追跡できます。

手順

ステップ 1 シスコのクレデンシャルを使用して Cisco Talos 電子メールステータスポータル（https://talosintelligence.com/email_status_portal）にログインします。

ステップ 2 Cisco Talos 電子メールステータスポータルで [送信（Submissions）] をクリックします。

ステップ 3 [フィルタオプション（Filter Options）] をクリックし、適切なフィルタオプションを選択します。

ステップ 4 （オプション）カレンダーボタンをクリックして、特定の日付を選択します。

次のタスク

詳細については、Cisco Talos 電子メールステータスポータルのヘルプページ（https://talosintelligence.com/tickets/email_submissions/help）を参照してください。

着信リレー構成における送信者の IP アドレスの決定

1 つ以上のメール交換/転送エージェント（MX または MTA）、フィルタサービスなどが 電子メールゲートウェイと着信メールを送信する外部マシンとの間のネットワークのエッジに配置されている場合、 電子メールゲートウェイは送信元マシンの IP アドレスを決定することはできません。代わりに、メールはローカル MX/MTA から送信されたように見えます。ただし、IronPort Anti-Spam および Cisco Intelligent Multi-Scan（IP レピュテーションサービスを使用）は外部送信者の正確な IP アドレスに依存します。

ソリューションは、着信リレーを使用するように 電子メールゲートウェイを設定することです。 電子メールゲートウェイに接続するすべての内部 MX/MTA の名前と IP アドレス、発信元 IP アドレスを保管するのに使用するヘッダーを指定します。

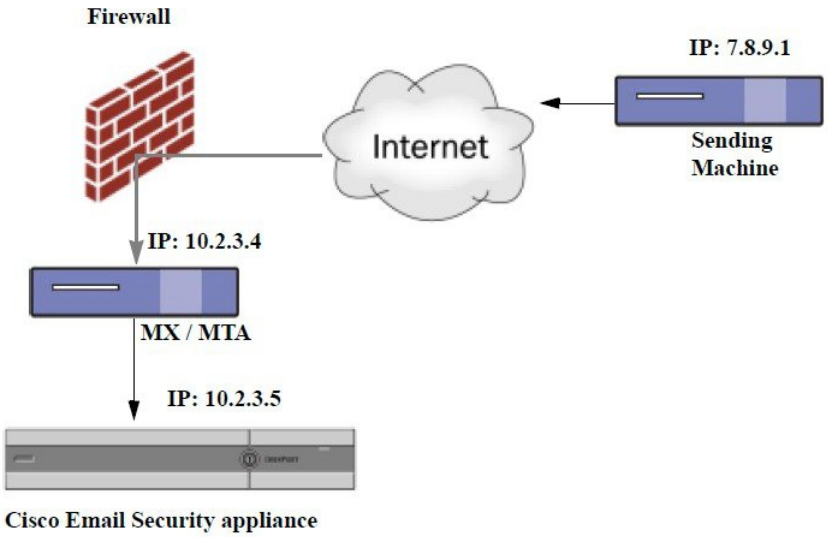
関連項目

- 着信リレーを使用した環境例 （498 ページ）
- 着信リレーを使用する 電子メールゲートウェイの設定 （499 ページ）
- 着信リレーが機能にどのように影響するか （505 ページ）
- 使用するヘッダーを指定するログの設定 （507 ページ）

着信リレーを使用した環境例

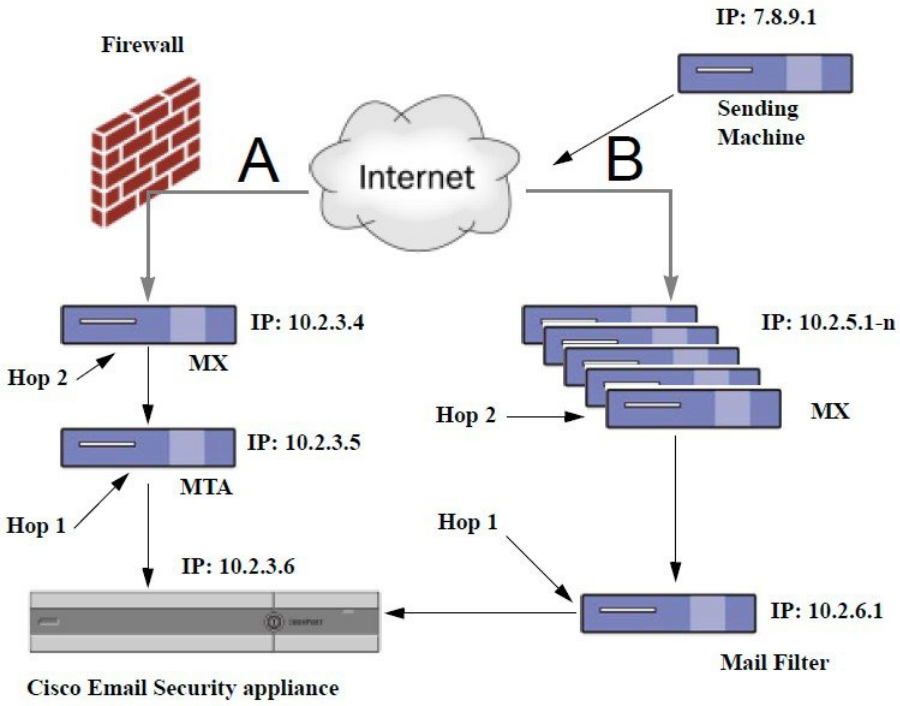
次の図に、着信リレーの非常に基本的な例を示します。ローカル MX/MTA によってメールが電子メールゲートウェイにリレーされているため、IP アドレス 7.8.9.1 からのメールは IP アドレス 10.2.3.4 からのように見えます。

図 *25 : MX/MTA* によるメール リレー：簡易



次の図に別の 2 つの例を示します。この例は、少し複雑であり、ネットワーク内でのメールのリレー方法と、電子メールゲートウェイへの受け渡し前に実施できる、ネットワーク内の複数サーバにおけるメールの処理方法を示します。例 A では、7.8.9.1 からのメールがファイアウォールを通過し、MX および MTA で処理されてから、 電子メールゲートウェイに配信されます。例 B では、7.8.9.1 からのメールがロードバランサまたは他のタイプのトラフィック シェーピング アプライアンスに送信され、一連の MX のいずれかに送信されてから、 電子メールゲートウェイに配信されます。

図 *26 : MX/MTA* によるメール リレー：拡張



着信リレーを使用する 電子メールゲートウェイの設定

関連項目

- 着信リレー機能のイネーブル化 （499 ページ）
- 着信リレーの追加 （500 ページ）
- リレーされたメッセージのメッセージ ヘッダー （501 ページ）

着信リレー機能のイネーブル化

（注） ローカル MX/MTA がメールを 電子メールゲートウェイにリレーする場合のみ、着信リレー機能をイネーブルにしてください。

手順

ステップ 1 [ネットワーク（Network）] > [着信リレー（Incoming Relays）] を選択します。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 変更を保存します。

着信リレーの追加

識別する着信リレーを追加します。

- 電子メールゲートウェイに着信メッセージをリレーするネットワークの各マシン、および
- 元の外部送信者の IP アドレスが分類されるヘッダー。

はじめる前に

これらの前提条件を完了するために必要な情報は、リレーされたメッセージのメッセージヘッダー （501 ページ）を参照してください。

- 元の外部送信者の IP アドレスを識別するカスタムまたは Received ヘッダーを使用するかどうかを設定します。
- カスタム ヘッダーを使用する場合：
  - リレーされたメッセージの発信元 IP アドレスを分類する正確なヘッダーを設定します。
  - 各 MX、MTA、または元の外部送信元に接続している他のマシンは、受信メッセージに元の外部送信者のヘッダー名と IP アドレスを追加するには、そのマシンを設定します。

手順

ステップ 1 [ネットワーク（Network）] > [着信リレー（Incoming Relays）] を選択します。

ステップ 2 [リレーの追加（Add Relay）] をクリックします。

ステップ 3 このリレーの名前を入力します。

ステップ 4 MTA、MX、または着信メッセージをリレーするために電子メールゲートウェイに接続している他のマシンの IP アドレスを入力します。

IPv4 または IPv6 アドレス、標準 CIDR 形式、または IP アドレス範囲を使用できます。たとえば、電子メールを受信する複数の MTA をネットワークのエッジに配置している場合に、すべての MTA を含む IP アドレスの範囲、たとえば 10.2.3.1/8 や 10.2.3.1-10 を入力する場合があります。

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

ステップ 5 元の外部送信者の IP アドレスを識別するヘッダーを指定します。

ヘッダーを入力する場合に、末尾のコロンを入力する必要はありません。

a) ヘッダー タイプの選択：

カスタム ヘッダー（推奨）または Received ヘッダーを選択します。

b) カスタム ヘッダーの場合：

リレーされたメッセージに追加するリレー マシンを設定したヘッダー名を入力します。

次に例を示します。

```
SenderIP
```

または

```
X-CustomHeader
```

c) Received ヘッダーの場合：

IPアドレスの前に配置される文字または文字列を入力します。IPアドレスを調査する「ホップ」数を入力します。

ステップ 6 変更を送信し、保存します。

次のタスク

次を行うことを検討します。

- DHAP の無制限のメッセージがあるメール フロー ポリシーを送信者グループにリレーするマシンを追加します。説明については、着信リレーおよびディレクトリ ハーベスト攻撃防止 （505 ページ）を参照してください。
- トラッキングおよびトラブルシューティングを容易にするには、使用されるヘッダーを示すように電子メールゲートウェイのロギングを設定します。使用するヘッダーを指定するログの設定 （507 ページ） を参照してください。

関連項目

- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法（462 ページ）

リレーされたメッセージのメッセージ ヘッダー

リレーされたメッセージの元の送信者の識別にヘッダーのタイプが次のいずれかを使用するように 電子メールゲートウェイを設定します。

- カスタム ヘッダー （502 ページ）
- Received ヘッダー （502 ページ）

カスタム ヘッダー

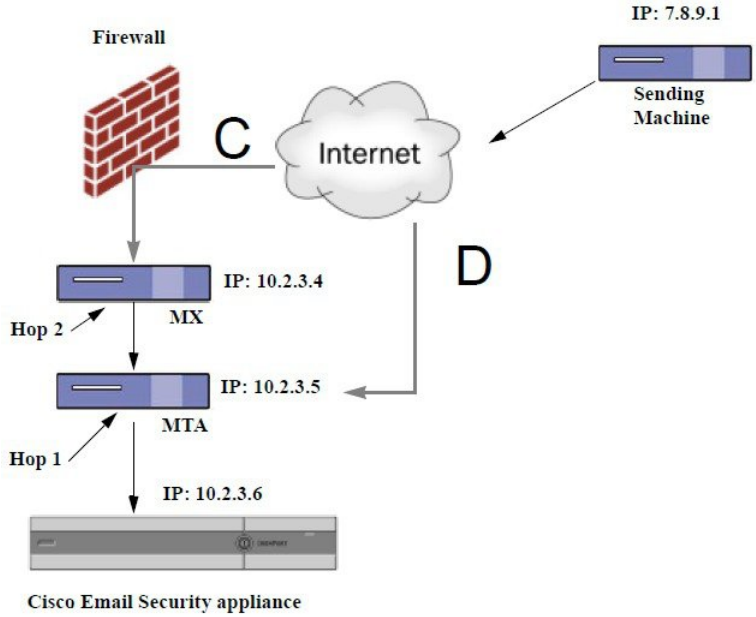
カスタムヘッダーを使用して元の送信者を識別する推奨される方法です。元の送信者に接続するマシンでは、このカスタムヘッダーを追加する必要があります。このヘッダーの値は、外部の送信マシンの IP アドレスになることが予期されます。例：

```
SenderIP: 7.8.9.1
```

```
X-CustomHeader: 7.8.9.1
```

ローカル MX/MTA で不定ホップ数のメールを受信する場合は、カスタム ヘッダーを挿入することが、着信リレー機能をイネーブルにする唯一の方法です。たとえば、次の図では、パス C とパス D の両方が IP アドレス 10.2.3.5 まで至る一方で、パス C は 2 ホップ、パス D は 1 ホップです。この状況では、ホップ数が異なる場合があるため、カスタムヘッダーを使用して、着信リレーが正しく設定されるようにする必要があります。

図 *27 : MX/MTA* によるメール リレー：不定ホップ数



関連項目

- 着信リレーの追加 （500 ページ）

Received ヘッダー

MX/MTA を設定する際に、送信 IP アドレスを含むカスタム ヘッダーの組み込みは選択肢にならない場合、着信リレー機能は、メッセージの「Received:」ヘッダーを調査することによって送信 IP アドレスの判別を試行するように設定できます。「Received:」ヘッダーを使用する方法は、ネットワーク「ホップ」の数が常に一定である IP アドレスの場合に限り機能します。つまり、最初のホップにあるマシン（「図：*MX/MTA* によるメール リレー：拡張」の 10.2.3.5）は、ネットワークのエッジからのホップ数が常に等しい必要があります。受信メールがお使いの電子メールゲートウェイに接続しているマシンへの別のパスを取ることができる場合（「図：

MX/MTA によるメールリレー：不定ホップ数」で説明しているように、異なるホップ数になる）、カスタムヘッダーを使用する必要があります（カスタム ヘッダー （502 ページ）を参照）。

解析対象文字または文字列および逆行して検索するネットワーク ホップ数（または Received: ヘッダー数）を指定します。ホップは、基本的に、メッセージがマシン間で転送されることを指します（電子メールゲートウェイによる受信はホップとしてカウントされません。詳細については、使用するヘッダーを指定するログの設定 （507 ページ）を参照してください）。AsyncOS は、指定されたホップ数に対応する Received: ヘッダー内の解析対象文字または文字列の最初のオカレンスに続く最初の IP アドレスを参照します。たとえば、2 ホップを指定した場合は、 電子メールゲートウェイから逆行して 2 つめの Received: ヘッダーが解析されます。解析対象文字も有効な IP アドレスも見つからない場合、 電子メールゲートウェイは接続マシンの実際の IP アドレスを使用します。

次の例のメール ヘッダーの場合、左角カッコ（[）と 2 ホップを指定した場合は、外部マシンの IP アドレスは 7.8.9.1 です。ただし、右カッコ（]）および解析対象文字を指定した場合は、有効な IP アドレスが見つかりません。この場合、着信リレー機能はディセーブルであると見なされ、接続元マシンの IP（10.2.3.5）が使用されます。

「図：*MX/MTA* によるメール リレー：拡張」の例で着信リレーは次のとおりです。

- パス A：10.2.3.5（Received ヘッダーを使用して 2 ホップ）および
- パス B：10.2.6.1（Received ヘッダーを使用して 2 ホップ）

「図：*MX/MTA* によるメールリレー：拡張」に示すように、電子メールゲートウェイまでにいくつかのホップを通過するメッセージの電子メールヘッダーの例を次の表に示します。この例は、受信者の受信箱に到着したメッセージで表示される、外部からのヘッダー（ 電子メールゲートウェイでは無視）を示します。指定するホップ数は 2 になります。

表 *38*：一連の *Received:* ヘッダー（パス *A* 例 *1*）

1	Microsoft Mail Internet Headers Version 2.0 Received: from smemail.rand.org ([10.2.2.7]) by smmail5.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713); Received: from ironport.customerdomain.org ([10.2.3.6]) by smemail.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713);
2	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTP; 21 Sep 2005 13:46:07 -0700
3	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>
4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>

5	Received: from linux1.thespammer.com (HELO linux1.thespammer.com) ([10.1.1.89]) by sending-machine.spamham.com with ESMTP; Received: from exchange1.thespammer.com ([10.1.1.111]) by linux1.thespammer.com with Microsoft SMTPSVC(6.0.3790.1830); Subject: Would like a bigger paycheck? Date: Wed, 21 Sep 2005 13:46:07 -0700 From: "A. Sender" <asend@otherdomain.com> To: <joefoo@customerdomain.org>

上記の表のメモ：

- 電子メールゲートウェイでは、これらのヘッダーを無視します。
- 電子メールゲートウェイがメッセージを受信します（ホップとしてカウントされない）。
- 最初のホップ（着信リレー）。
- 第 2 ホップ。これは、送信側 MTA です。IP アドレスは 7.8.9.1 です。
- 電子メールゲートウェイでは、これらの Microsoft Exchange ヘッダーを無視します。

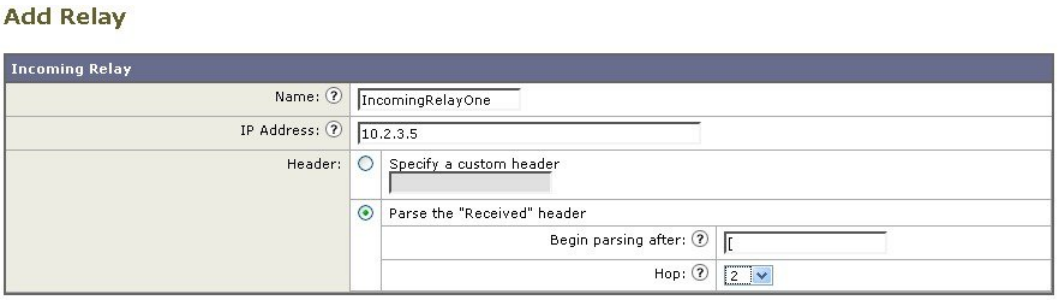
次の表に、外部ヘッダーを除く、同じ電子メール メッセージのヘッダーを示します

表 *39 :* 一連の *Received:* ヘッダー（パス *A* 例 *2*）

1	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTP; 21 Sep 2005 13:46:07 -0700
2	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>;
3	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;

次の図 に、GUI の [リレーの追加（Add Relay）] ページで設定されたパス A（前述）の着信リレーを示します。

図 *28 : Received* ヘッダー付きで設定された着信リレー



関連項目

- 着信リレーの追加 （500 ページ）

着信リレーが機能にどのように影響するか

- 着信リレーとフィルタ （505 ページ）
- 着信リレー、HAT、IP レピュテーションスコア、および送信者グループ （505 ページ）
- 着信リレーおよびディレクトリ ハーベスト攻撃防止 （505 ページ）
- 着信リレーおよびトレース （506 ページ）
- 着信リレーと電子メール セキュリティ モニタ（レポート） （506 ページ）
- 着信リレーおよびメッセージ トラッキング （506 ページ）
- 着信リレーとロギング （506 ページ）

着信リレーとフィルタ

着信リレー機能では、IP レピュテーションサービスに関連するさまざまなフィルタルール（reputation、no-reputation）にさまざまな IP レピュテーションスコアを提供します。

着信リレー、HAT、IP レピュテーションスコア、および送信者グループ

HAT ポリシー グループは、着信リレーからの情報は現在は使用していません。ただし、着信リレー機能では レピュテーションスコアが提供されるため、メッセージフィルタおよび $reputation 変数を使用して HAT ポリシーグループ機能をシミュレートできます。

着信リレーおよびディレクトリ ハーベスト攻撃防止

リモートホストが、ネットワーク上で着信リレーとして使われている MX または MTA にメッセージを送ることでディレクトリ獲得攻撃防止を試みる場合、 電子メールゲートウェイは、ディレクトリ獲得攻撃防止（DHAP）がイネーブルに設定されたメールフローポリシーを持つ送信者グループにリレーが割り当てられていると、その着信リレーからの接続をドロップします。これは、リレーからすべてのメッセージが、正規のメッセージも含め 電子メールゲートウェイに接続されないよう防止します。電子メールゲートウェイはリモートホストが攻撃者であると認識できず、着信リレーとして機能する MX または MTA は攻撃元ホストからメールを

受信し続けます。この問題を回避して、着信リレーからメッセージを受信し続けるためにDHAP の無制限のメッセージがあるメールフローポリシーを送信者グループにリレーを追加します。

着信リレーおよびトレース

トレースは、送信元 IP アドレスのレピュテーションスコアの代わりに、結果の着信リレーの IP レピュテーションスコアを返します。

着信リレーと電子メール セキュリティ モニタ（レポート）

着信リレーを使用する場合：

- 電子メール セキュリティ モニタ レポートには外部 IP および MX/MTA の両方のデータが含まれます。たとえば、外部マシン（IP 7.8.9.1）から内部 MX/MTA（IP 10.2.3.4）を介して 5 通の電子メールが送信された場合、[メールフローサマリー（Mail Flow Summary）] には、IP 7.8.9.1 からの 5 個のメッセージに加えて、内部リレー MX/MTA（IP 10.2.3.5）からの 5 個のメッセージが表示されます。
- IP レピュテーションスコアは、電子メール セキュリティ モニタ レポートで正しく報告されません。送信者グループが正しく解決されない場合もあります。

着信リレーおよびメッセージ トラッキング

着信リレーを使用すると、メッセージトラッキングの詳細ページに、外部送信元の IP アドレスおよびレピュテーションスコアの代わりに、メッセージのリレーの IP アドレスおよびリレーの IP レピュテーションスコアが表示されます。

着信リレーとロギング

次のログの例で、送信者の IP レピュテーショスコアは、当初 1 行目に示されます。その後、着信リレーの処理が行われて、正しい IP レピュテーションスコアが 5 行目に示されます。

1	Fri Apr 28 17:07:29 2006 Info: ICID 210158 ACCEPT SG UNKNOWNLIST match nx.domain IPR rfc1918
2	Fri Apr 28 17:07:29 2006 Info: Start MID 201434 ICID 210158
3	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 From: <joe@sender.com>
4	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 RID 0 To: <mary@example.com>
5	Fri Apr 28 17:07:29 2006 Info: MID 201434 IncomingRelay(senderdotcom): Header Received found, IP 192.192.108.1 being used, IPR **6.8**
6	Fri Apr 28 17:07:29 2006 Info: MID 201434 Message-ID '<7.0.1.0.2.20060428170643.0451be40@sender.com>'
7	Fri Apr 28 17:07:29 2006 Info: MID 201434 Subject 'That report...'

8	Fri Apr 28 17:07:29 2006 Info: MID 201434 ready 2367 bytes from <joe@sender.com>
9	Fri Apr 28 17:07:29 2006 Info: MID 201434 matched all recipients for per-recipient policy DEFAULT in the inbound table
10	Fri Apr 28 17:07:34 2006 Info: ICID 210158 close
11	Fri Apr 28 17:07:35 2006 Info: MID 201434 using engine: CASE spam negative
12	Fri Apr 28 17:07:35 2006 Info: MID 201434 antivirus negative
13	Fri Apr 28 17:07:35 2006 Info: MID 201434 queued for delivery

着信リレーとメール ログ

次の例は、着信リレー情報を含む、一般的なログ エントリを示します。

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay): Header Received found,
 IP 192.168.230.120 being used
```

使用するヘッダーを指定するログの設定

電子メールゲートウェイでは、メッセージが受信された時点で存在していたヘッダーのみ検査します。したがって、ローカルで追加されるヘッダー（Microsoft Exchange のヘッダーなど）や、電子メールゲートウェイがメッセージを受信するときに追加する追加のヘッダーは、処理されません。使用されるヘッダーを特定する方法の 1 つは、使用するヘッダーを AsyncOS ロギングに含めるよう設定することです。

ヘッダーのロギング設定を設定するには、ロギングのグローバル設定（1469ページ）を参照してください。

モニタリング ルールのアップデート

使用許諾契約に同意すると、最新の Cisco Anti-Spam および Cisco Intelligent Multi-Scan ルールのアップデートを確認できます。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [IronPort Anti-Spam] を選択します。

または

ステップ 2 [セキュリティサービス（Security Services）] > [IMSおよびグレイメール（IMS and Graymail）] を選択します。

ステップ 3 [ルールの更新（Rule Updates）] セクションを表示し、次を行います。

目的 (To)	詳細情報
各コンポーネントの最新の更新について参照	アップデートが実行されていないか、サーバが設定されていない場合は、「Never Updated」という文字列が表示されます。
アップデートが使用可能かどうかを確認	—
アップグレードが入手可能な場合はルールを更新	[今すぐ更新（Update Now）] をクリックします。

次のタスク

関連項目

- サービス アップデート （1253 ページ）
- プロキシ サーバを経由したアップデート （1259 ページ）
- アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）

スパム対策のテスト

目的	操作手順	詳細情報
設定をテストします。	`X-advertisement: spam` ヘッダーを使用して、設定をテストします。 テストを目的として、Cisco Anti-Spam では、`X-Advertisement: spam` という形式の X-Header を含むすべてのメッセージをスパムであると見なします。	このヘッダーを付けて送信したテストメッセージには、Cisco Anti-Spam によってフラグが設定され、メールポリシーに対して設定したアクション（スパム対策ポリシーの定義 （481 ページ）） が実行されることを確認できます。 次のいずれかをこのヘッダーに使用します。 • このヘッダーを含むテストメッセージを送信する SMTP コマンドを使用します。Cisco Anti-Spam をテストするための電子メールゲートウェイへのメール送信 （509 ページ） を参照してください。 • trace コマンドを使用してこのヘッダーを含めます。テストメッセージを使用したメールフローのデバッグ：トレース （1515 ページ） を参照してください。

目的	操作手順	詳細情報
スパム対策エンジンの有効性を評価します。	インターネットから直接本物のメール ストリームを使用して製品を評価します。	回避すべき非効率的な評価のアプローチの一覧については、スパム対策の有効性をテストできない方法（510 ページ）を参照してください。

関連項目

- Cisco Anti-Spam をテストするための 電子メールゲートウェイへのメール送信 （509 ページ）
- スパム対策の有効性をテストできない方法 （510 ページ）

Cisco Anti-Spam をテストするための電子メールゲートウェイへのメール送信

はじめる前に

スパム対策設定のテスト：SMTP の使用例 （510 ページ）の例を確認してください。

手順

ステップ 1 メール ポリシーで Cisco Anti-Spam を有効にします。

ステップ 2 X-Advertisement: spam というヘッダーを含むテスト電子メールをそのメール ポリシーに含まれているユーザに送信します。

Telnet で SMTP コマンドを使用して、アクセスできるアドレスにこのメッセージを送信します。

ステップ 3 次に、テスト アカウントのメールボックスを調べて、メール ポリシーに設定したアクションに基づいてテスト メッセージが正しく配信されたことを確認します。

次に例を示します。

- 件名行が変更されている。
- 追加のカスタム ヘッダーが追加されている。
- メッセージが代替アドレスに配信された。
- メッセージがドロップされた。

関連項目

- スパム対策設定のテスト：SMTP の使用例 （510 ページ）

スパム対策設定のテスト：SMTP の使用例

この例では、テスト アドレスのメッセージを受信するようにメール ポリシーを設定し、HAT でテスト接続を許可する必要があります。

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam port

220 hostname ESMTP

helo example.com

250 hostname

mail from: <test@example.com>

250 sender <test@example.com> ok

rcpt to: <test@address>

250 recipient <test@address>
ok

data

354 go ahead

Subject: Spam Message Test


X-Advertisement: spam

spam test

.

250 Message MID accepted

221 hostname

quit
```

スパム対策の有効性をテストできない方法

IronPort Anti-Spam と Cisco Intelligent Multi-Scan のルールは、活発なスパム攻撃を防ぐためにすぐに追加され、攻撃が終結するとすぐに期限切れになるため、次の方法のいずれかを使用して有効性をテストしないでください。

- 再送信されたか、転送されたメールまたはカット アンド ペーストされたスパム メッセージによる評価。

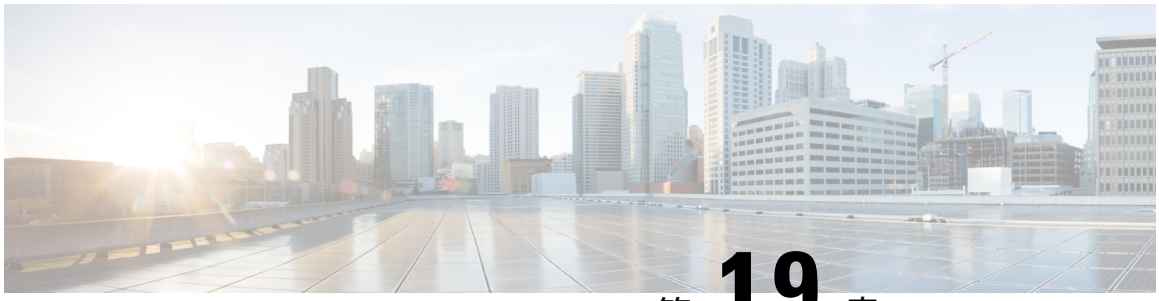
  適切なヘッダー、接続IP、シグニチャなどを持たないメールを使用すると、評点が不正確になります。

- 「難易度の高いスパム」だけをテストする。

  IP レピュテーションサービス、ブロックリスト、メッセージフィルタなどを使用して「難易度の低いスパム」を取り除くと、全体の検出率が低くなります。

- 別のスパム対策ベンダーによって検出されたスパムの再送信。
- 以前のメッセージのテスト。

  スキャンエンジンは現在の脅威に基づき、迅速にルールを追加し、排除します。したがって、古いメッセージを使用してテストすると、テスト結果が不正確になります。



第 19 章

アウトブレイク フィルタ

この章は、次の項で構成されています。

- アウトブレイク フィルタの概要 （513 ページ）
- アウトブレイク フィルタの動作 （514 ページ）
- アウトブレイク フィルタの機能概要 （522 ページ）
- アウトブレイク フィルタの管理 （526 ページ）
- アウトブレイク フィルタのモニタリング （539 ページ）
- アウトブレイク フィルタ機能のトラブルシューティング （540 ページ）

アウトブレイク フィルタの概要

アウトブレイク フィルタは大規模なウイルスの拡散、および小規模のフィッシング詐欺およびマルウェア配布といった、非ウイルス性の攻撃が発生した際にネットワークを保護します。データが収集され、ソフトウェアの更新が公開されるまで新たな拡散を検知できない通常のアンチマルウェア セキュリティ ソフトウェアとは異なり、シスコは感染が拡散したときにデータを収集し、ユーザにこれらのメッセージが到達することを防ぐためにリアルタイムで電子メールゲートウェイに更新情報を送信します。

シスコは着信メッセージは、着信メッセージが安全またはアウトブレイクの一部であることを判断するルールを開発するためにグローバル トラフィック パターンを使用します。アウトブレイクの一部となる可能性があるメッセージは、シスコからアップデートされたアウトブレイクの情報またはSophosおよびMcAfeeによって発行される新しいアンチウイルス定義に基づいて安全と判断されるまで隔離されます。

小規模な非ウイルス性の攻撃で使用されるメッセージは、正当に見える外見、受信者情報、そして短期間だけオンラインに存在し Web セキュリティ サービスが知らないフィッシングおよびマルウェア Web サイトを参照するカスタム URL を使用します。アウトブレイク フィルタはメッセージの内容を分析し、この種の非ウイルス性の攻撃を検出するために URL リンクを検索します。アウトブレイク フィルタは Web セキュリティ プロキシによって潜在的に危険な Web サイトへのトラフィックをリダイレクトするために URL を書き換え、ユーザがアクセスしようとしている Web サイトが悪意があるかもしれないことを警告するかまたは Web サイトを完全にブロックします。

アウトブレイク フィルタの動作

関連項目

- メッセージの遅延、リダイレクトおよび修正 （514 ページ）
- 脅威カテゴリ （515 ページ）
- Cisco Security Intelligence Operations （516 ページ）
- コンテキスト適応スキャン エンジン （517 ページ）
- メッセージの遅延 （517 ページ）
- URL のリダイレクト （518 ページ）
- メッセージの変更 （519 ページ）
- ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール （519 ページ）
- アウトブレイク （520 ページ）
- 脅威レベル （521 ページ）

メッセージの遅延、リダイレクトおよび修正

アウトブレイク フィルタ機能は、ウイルス感染からユーザを保護するために3つの戦略を使用します。

- **遅延。**アウトブレイク フィルタは、ウイルス感染の一部または非ウイルス性の攻撃である可能性のあるメッセージを隔離します。隔離の間、電子メールゲートウェイはアップデートされたアウトブレイク情報を受信し、攻撃の一部であるかどうか確認するためにメッセージを再スキャンします。

（注） スパム検出のメッセージがアウトブレイクフィルタによってアウトブレイク検出と識別されても、そのメッセージはアウトブレイク検疫に送信されません。

- **リダイレクト。**リンクされた Web サイトのいずれかにアクセスしようとすると、Cisco Web セキュリティ プロキシによって受信者をリダイレクトするように非ウイルス性の攻撃のメッセージ内の URL を書き換えます。プロキシは、Web サイトがまだ動作中である場合は、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ画面を表示し、Web サイトがオフラインになっている場合は、エラー メッセージを表示します。URLのリダイレクトの詳細については、URLのリダイレクト （518 ページ）を参照してください。
- **変更。**非ウイルス性の脅威メッセージの URL 書き換えに加えて、アウトブレイク フィルタはユーザにメッセージの内容についてユーザに警告するためにメッセージの件名を変更して、メッセージ本文の上に免責事項を追加できます。詳細については、メッセージの変更 （519 ページ）を参照してください。

脅威カテゴリ

アウトブレイク フィルタ機能は、メッセージに基づくアウトブレイクの次の2つのカテゴリからの保護を提供します。ウイルスアウトブレイクは、添付ファイルに見たことのないウイルスが含まれるメッセージで、非ウイルス性の脅威には、外部 Web サイトへのリンクを経由するフィッシング試行、詐欺、およびマルウェア配布が含まれます。

デフォルトでアウトブレイクフィルタ機能は、アウトブレイク中の可能性があるウイルスがあるかどうか送受信メッセージをスキャンします。電子メールゲートウェイでアンチスパムスキャンをイネーブルにする場合は、ウイルスアウトブレイクに加えて、非ウイルス性の脅威のスキャンをイネーブルにできます。

（注） アウトブレイクフィルタが非ウイルス性の脅威をスキャンするために、電子メールゲートウェイには、Anti-Spam または Intelligent Multi-Scan のライセンスキーが必要です。

関連項目

- ウイルス アウトブレイク （515 ページ）
- フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威 （515 ページ）

ウイルス アウトブレイク

アウトブレイク フィルタ機能を使用することで、ウイルス アウトブレイクとの格闘において優位なスタートを切ることができます。アウトブレイクは、見たことのないウイルスまたは既存のウイルスの変異型を含む添付ファイルを持つメッセージがプライベート ネットワークおよびインターネットを経由してすばやく拡散するときに発生します。これらの新しいウイルスまたはウイルスの変異型がインターネットを攻撃した場合、最も危機的な期間はウイルスがリリースされてからアンチウイルス ベンダーがアップデートしたウイルス定義をリリースするまでの期間です。たとえ数時間でも、事前に通知を受けることは、マルウェアまたはウイルスの拡散を抑えるうえで非常に重要です。ウイルス定義がリリースされるまでの間に、新しく発見されたウイルスはグローバルに伝播し、電子メール インフラストラクチャを停止に追い込むことが可能です。

フィッシング、マルウェア配布、およびその他の非ウイルス性の脅威

非ウイルス性の脅威を含んでいるメッセージは、正規の送信元からのメッセージのように設計されていて、多くの場合、少数の受信者に送信されます。これらのメッセージには、信頼できると見せるために次の 1 つまたは複数の特徴がある場合があります。

- 受信者の連絡先情報。
- HTML コンテンツは、ソーシャル ネットワークおよびオンライン販売などの正規の送信元からの電子メールを模倣するように設計されています。
- 新しい IP アドレスを持ち、短期間だけオンラインである Web サイトを指している URL。これは電子メールおよび Web セキュリティ サービスに、その Web サイトが不正かどうか判断するための十分な情報がないことを意味します。

- URL 短縮サービスを指している URL。

これらの特徴すべてによって、これらのメッセージをスパムとして検出するのがさらに難しくなります。アウトブレイク フィルタ機能によって、これらの非ウイルス性の脅威に対するマルチレイヤの防衛が提供され、ユーザがマルウェアをダウンロードしたり、個人情報を新しい不審な Web サイトに提供したりすることを防ぎます。

CASE はメッセージ内に URL を発見すると、そのメッセージを既存のアウトブレイク ルールと比較して、そのメッセージが小規模の非ウイルス性のアウトブレイクの一部かどうか判断し、次に脅威レベルを割り当てます。脅威レベルに応じて、電子メールゲートウェイは、より多くの脅威のデータを集められるまで受信者への配信を遅らせ、Web サイトにアクセスしようとすると Cisco Web セキュリティプロキシへ受信者をリダイレクトするようにメッセージ内の URL を書き換えます。プロキシは、その Web サイトにマルウェアが含まれる可能性があることをユーザに警告するスプラッシュ ページを表示します。

Cisco Security Intelligence Operations

Cisco Security Intelligence Operations（SIO）は、グローバルな脅威情報、レピュテーションに基づくサービス、および高度な分析を電子メールゲートウェイに結び付け、より強力な保護をより迅速な応答時間で提供するセキュリティエコシステムです。

SIO は次の 3 種類のコンポーネントからなります。

- SenderBase。世界有数の規模を誇る脅威モニタリング ネットワークおよび脆弱性データベース。
- Threat Operations Center（TOC）。セキュリティ専門家のグローバル チームおよび SenderBase によって収集された実行可能な情報を抽出する自動システム。
- Dynamic Update。アウトブレイク発生時に、電子メールゲートウェイに自動的に配信されるリアルタイムアップデート。

SIO は、グローバル SenderBase ネットワークからのリアルタイム データを、共通のトラフィック パターンと比較して、アウトブレイクの確かな前兆である異常を識別します。TOC は、データをレビューしてアウトブレイクの可能性の脅威レベルを発行します。電子メールゲートウェイは、アップデートされた脅威レベルとアウトブレイクルールをダウンロードし、それらを使用してすでにアウトブレイク隔離エリアにあるメッセージと同様に送受信メッセージをスキャンします。

現在のウイルス アウトブレイクに関する情報は、次の SenderBase の Web サイトで入手できます。

http://www.senderbase.org/

次の SIO Web サイトに、スパム、フィッシング、およびマルウェア配布の試行を含む現在の非ウイルス性の脅威のリストが記載されています。

http://tools.cisco.com/security/center/home.x

コンテキスト適応スキャン エンジン

アウトブレイク フィルタには、シスコ独自のコンテキスト適応スキャンエンジン（CASE）が使用されています。CASE は、メッセージング脅威に対するリアルタイムの分析に基づいて自動的かつ定期的に調整されている、100,000 を超える適応メッセージ属性を活用しています。

ウイルスアウトブレイクの場合、CASEはメッセージの内容、コンテキスト、および構造を分析してアダプティブ ルールのトリガーである可能性のあるものを、正確に識別します。CASE は、アダプティブ ルールと SIO から発行されるリアルタイムのアウトブレイク ルールを組み合わせて、各メッセージを評価し、独自の脅威レベルを割り当てます。

非ウイルス性の脅威を検出するために、CASE はURL に対してメッセージをスキャンし、1 つまたは複数の URL が発見されると SIO が提供するアウトブレイク ルールを使用してメッセージの脅威レベルを評価します。

メッセージの脅威レベルに基づいて、CASE は、アウトブレイクを防ぐためにメッセージを一定期間隔離することを推奨します。SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージを再評価できるように、CASE は再スキャンの間隔も決定します。脅威レベルが高くなるほど、隔離中のメッセージの再スキャンの頻度が高くなります。

メッセージが隔離解除されるときに、CASE はメッセージの再スキャンも行います。再スキャン時に、CASE によりメッセージがスパムであるか、ウイルスを含むと判断された場合、メッセージを再度隔離できます。

CASE の詳細については、Cisco Anti-Spam：概要 （465 ページ）を参照してください。

メッセージの遅延

アウトブレイクまたは電子メール攻撃の発生と、ソフトウェアベンダーによるアップデートしたルールのリリースの間の期間は、ネットワークとユーザが最も脆弱なときです。この期間に、現代のウイルスはグローバルに伝播でき、また不正な Web サイトはマルウェアを配信したり、ユーザの機密情報を収集したりすることができます。限られた期間に疑わしいメッセージを隔離することによって、アウトブレイク フィルタは、ユーザおよびネットワークを保護し、シスコおよびその他のベンダーに新しいアウトブレイクを調査する時間を与えます。

ウイルス アウトブレイクが発生すると、アップデートされたアウトブレイク ルールおよび新しいアンチウイルス シグニチャにより、その電子メールの添付ファイルがクリーン、またはウイルスであることが証明されるまで添付ファイルを含む疑わしいメッセージは隔離されます。

小規模の非ウイルス性の脅威には、Web セキュリティ サービスによる検出を回避するために短期間オンラインになる可能性のある不正な Web サイトへの URL、または Web セキュリティを回避するため、信頼できる Web サイトを途中に置いて URL 短縮サービスを経由する URL が含まれます。脅威レベルのしきい値を満たすURL を含んでいるメッセージの隔離によって、CASE は SIO が提供するアップデートされたアウトブレイク ルールに基づいてメッセージの内容を再評価できるだけでなく、リンクされた Web サイトがオフラインになるか、Web セキュリティ ソリューションによってブロックできるほど長く、メッセージを隔離のままにしておくことができます。

疑いのあるメッセージに対するアウトブレイク フィルタの隔離方法の詳細については、動的隔離 （524 ページ）を参照してください。

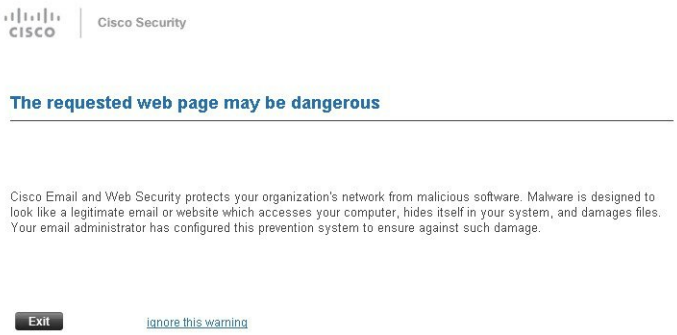
URL のリダイレクト

CASEがアウトブレイク フィルタの段階でメッセージをスキャンする場合、他の疑わしい内容に加えてメッセージ本文に URL があるかどうか検索します。CASE は、発行されたアウトブレイク ルールを使用して、そのメッセージが脅威であるかどうかを評価して、次に適切な脅威レベルでメッセージをスコアリングします。脅威レベルに応じて、アウトブレイク フィルタは、受信者が Cisco Web セキュリティ プロキシにリダイレクトされるように、バイパスされたドメインを指している URL を除くすべての URL を書き換えることによって受信者を保護します。メッセージがより大きなアウトブレイクの一部であると思われる場合は、TOC が Web サイトについてさらに詳しく調べるためにメッセージの配信を遅らせます。信頼ドメインへの URL のバイパスの詳細については、URL 書き換えおよびドメインのバイパス （535 ページ）を参照してください。

電子メールゲートウェイがメッセージをリリースおよび配信した後で、受信者による Web サイトへのアクセスの試行があれば、Cisco Web セキュリティプロキシによってリダイレクトされます。これは、シスコによってホストされている外部プロキシで、Web サイトが引き続き使用可能な場合、その Web サイトが危険である可能性があることをユーザに警告するスプラッシュ画面を表示します。Web サイトがオフラインになった場合は、スプラッシュ画面にエラーメッセージが表示されます。

受信者がメッセージの URL をクリックすることにした場合、Cisco Web セキュリティ プロキシは、ユーザの Web ブラウザにスプラッシュ画面を表示して、メッセージの内容について警告します。次の図は、スプラッシュ画面の警告の例を示しています。受信者は、[この警告を無視する（Ignore this warning）] をクリックして Web サイトへ進むか、[終了（Exit）] をクリックして退出し、ブラウザ ウィンドウを安全に閉じることができます。

図 *29 :* シスコのセキュリティによるスプラッシュ画面の警告（*proxy_splash_screen*）



Cisco Web セキュリティ プロキシにアクセスする唯一の方法は、メッセージ内の URL を書き換えることです。Web ブラウザで URL を入力しても、プロキシにはアクセスできません。

（注） このスプラッシュ画面の外観をカスタマイズして、会社のロゴ、連絡先情報などの自社のブランディングを表示することができます。サイトに悪意がある場合にエンド ユーザに表示する通知のカスタマイズ （552 ページ）を参照してください。

ヒント スパムの可能性があるメッセージの URL をすべて Cisco Web セキュリティ プロキシ サービスにリダイレクトするには、カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）を参照してください。

メッセージの変更

アウトブレイク フィルタ機能は、非ウイルス性の脅威であるメッセージのメッセージ本文を変更して、URL を書き換えるだけでなく、メッセージが疑わしい脅威であるというアラートをユーザに出します。アウトブレイク フィルタ機能は、件名ヘッダーを変更したり、メッセージ本文上部にメッセージの内容について免責事項を追加したりできます。詳細については、メッセージ変更 （533 ページ）を参照してください。

脅威の免責事項は、[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページから免責事項テンプレートを使用して作成されます。詳細については、テキスト リソース管理の概要 （802 ページ）を参照してください。

ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール

アウトブレイク フィルタでは、アダプティブ ルールおよびアウトブレイク ルールの 2 つのタイプのルールを使用して、潜在的なアウトブレイクを検出します。アウトブレイク フィルタ機能は、これらの 2 つのルールセットを使用して、高い有効性を持ち、綿密に的を絞った、一連の脅威検出基準を提供することで、フィルタが確実に特定のアウトブレイクに正確に照準を合わせることができるようにしています。アウトブレイク フィルタのルールおよびアクションは、水面下に隠されているものではなく、管理者の目に見えるようになっており、隔離されたメッセージにただちにアクセスしたり、隔離された理由を確認したりできるようになっています。

関連項目

- 適応ルール （520 ページ）
- アウトブレイクのルール （519 ページ）

アウトブレイクのルール

アウトブレイク ルールは、Cisco Security Intelligence Operations の一部である、Cisco Threat Operations Center（TOC）で作成されるもので、添付ファイルのタイプだけでなく、メッセー

ジ全体に焦点を当てています。アウトブレイク ルールは、SenderBaseデータ（リアルタイムおよび履歴のトラフィック データ）およびその他のあらゆるメッセージ パラメータの組み合わせ（添付ファイル タイプ、ファイル名のキーワード、またはアンチウイルス エンジンのアップデート）を使用して、リアルタイムでアウトブレイクを認識し、防止します。アウトブレイク ルールには一意の ID が付けられ、GUI のさまざまな場所（たとえばアウトブレイク隔離など）でルールを参照するために使用されます。

グローバル SenderBase ネットワークからのリアルタイム データは、このベースラインと比較され、アウトブレイクの確かな前兆である異常を識別します。TOCは、データをレビューして脅威のインジケータまたは脅威レベルを発行します。脅威レベルは 0（脅威なし）から 5（非常に危険）の範囲の数値で表し、メッセージがシスコのお客様による他のゲートウェイの防御が広く導入されていない脅威である可能性を判断します（詳細については、脅威レベル （521 ページ）を参照してください）。脅威レベルは、TOC によりアウトブレイク ルールとして発行されます。

アウトブレイク ルール内で組み合わせることができる特性には、たとえば次のようなものがあります。

- ファイル タイプ、ファイル タイプとサイズ、ファイル タイプとファイル名キーワードなど
- ファイル名キーワードとファイル サイズ
- ファイル名キーワード
- メッセージ URL
- ファイル名と Sophos IDE

適応ルール

アダプティブ ルールは、CASE内の一連のルールであり、メッセージの属性を既知のウイルス アウトブレイク メッセージの属性と正確に比較します。これらのルールは、広範なウイルス コーパスの中で、既知の脅威のメッセージおよび既知の良好なメッセージを研究し、作成されたものです。アダプティブ ルールは、コーパスの評価に合わせて、頻繁にアップデートされます。アダプティブ ルールは、既存のアウトブレイク ルールを補完して、常にアウトブレイク メッセージを検出します。アウトブレイク ルールは、アウトブレイクの可能性がある状態が発生したときに有効になりますが、アダプティブ ルールは（いったんイネーブルにされると）「常時オン」となり、グローバルな規模で本格的な異常が起きる前にローカルでアウトブレイク メッセージを捕捉します。さらに、アダプティブ ルールは、電子メール トラフィックおよび構造の小規模および微小な変化にも継続的に対応し、お客様にアップデートした保護を提供します。

アウトブレイク

アウトブレイク フィルタ ルールは、基本的に、電子メールのメッセージおよび添付ファイルの一連の特性（ファイル サイズ、ファイル タイプ、ファイル名、メッセージの内容など）に関連付けられた脅威レベル（例：4）です。たとえば、ファイル名に特定のキーワード（たとえば「hello」）が含まれた .exe 形式のファイル（サイズは 143 KB）が添付された、疑わしい電子メール メッセージの発生が増加していることを、Cisco SIO が通知したと想定します。こ

の基準に一致するメッセージに対する脅威レベルを上げたアウトブレイク ルールが発行されます。デフォルトでは、電子メールゲートウェイは、新しく発行されたアウトブレイクルールおよびアダプティブルールを5分ごとにチェックし、ダウンロードします（アウトブレイク フィルタ ルールのアップデート （531ページ）を参照）。アダプティブ ルールは、アウトブレイク ルールほど頻繁にはアップデートされません。電子メールゲートウェイで、疑わしいメッセージの隔離についてしきい値を設定します。メッセージの脅威レベルが隔離のしきい値以上の場合、メッセージはアウトブレイク 隔離エリアに送信されます。非ウイルス性の脅威のメッセージの変更についてしきい値を設定して、疑わしいメッセージで発見された URL すべてを書き換えたり、メッセージ本文の上部に通知を追加したりできます。

脅威レベル

次の表に、各レベルの基本的なガイドラインまたは定義のセットを示します。

レベル	リスク	意味
0	なし	メッセージが脅威であるリスクはありません。
1	低	メッセージが脅威であるリスクは低です。
2	低または中	メッセージが脅威であるリスクは低から中です。これは「疑わしい」脅威です。
3	中	メッセージが確認されているアウトブレイクの一部であるか、メッセージの内容が脅威である中から高のリスクがあります。
4	高	メッセージが大規模アウトブレイクの一部であることが確認されているか、メッセージの内容が非常に危険です。
5	最高	メッセージの内容が、非常に大規模または大規模な、かつ非常に危険なアウトブレイクの一部であることが確認されています。

脅威レベルおよびアウトブレイク ルールの詳細については、アウトブレイク フィルタ ルール （530 ページ）を参照してください。

関連項目

- 隔離脅威レベルのしきい値設定ガイドライン （521 ページ）
- コンテナ：特定ルールおよび常時ルール （522 ページ）

隔離脅威レベルのしきい値設定ガイドライン

隔離脅威レベルのしきい値を使用することで、管理者は疑いのあるメッセージをより積極的または消極的に隔離できるようになります。低い値（1 または 2）は、より積極的な設定値で、多くのメッセージが隔離されます。反対に、高いスコア（4 または 5）は消極的な設定値で、不正である可能性がきわめて高いメッセージのみが隔離されます。

ウイルスアウトブレイクおよび非ウイルス性の脅威の両方に同じしきい値が適用されますが、ウイルス攻撃およびその他の脅威に対して、異なる隔離の保持期間を指定できます。詳細については、動的隔離 （524 ページ）を参照してください。

シスコは、デフォルト値の 3 を推奨します。

コンテナ：特定ルールおよび常時ルール

コンテナ ファイルとは、他のファイルを含む zip（.zip）アーカイブなどのファイルです。TOC は、アーカイブ ファイル内の特定のファイルを処理するルールを発行できます。

たとえば、TOC により、あるウイルス アウトブレイクが、1 つの .exe を含む 1 つの .zip ファイルで構成されていると判別された場合は、.zip ファイル内の .exe ファイル（.zip(exe)）に脅威レベルを設定する特定のアウトブレイク ルールが発行されます。ただし .zip ファイル内に含まれるその他のファイル タイプ（たとえば .txt ファイル）には特定の脅威レベルを設定しません。2 番目のルール（.zip(*)）は、コンテナ ファイル タイプ内のその他すべてのファイル タイプをカバーします。コンテナに対する常時ルールは、コンテナ内にあるファイルのタイプに関係なく、メッセージの脅威レベル計算に常に使用されます。そのようなコンテナ タイプが危険であると判明した場合は、常時ルールが SIO により発行されます。

表 *40*：フォールバック ルールおよび脅威レベル スコア

アウトブレイク ルール	脅威レベル	説明
.zip(exe)	4	このルールは、.zip ファイル内の .exe ファイルの脅威レベルを 4 に設定します。
.zip(doc)	0	このルールは、.zip ファイル内の .doc ファイルの脅威レベルを 0 に設定します。
zip(*)	2	このルールは、含まれているファイルのタイプに関係なく、すべての .zip ファイルの脅威レベルを 2 に設定します。

アウトブレイク フィルタの機能概要

電子メールメッセージは、電子メールゲートウェイで処理される際に、「電子メールパイプライン」と呼ばれる一連の手順を通過します（電子メールパイプラインの詳細については、電子メール パイプラインについて （67 ページ）を参照してください）。メッセージは電子メールパイプラインを通過するので、これらのエンジンがメール ポリシーをイネーブルにしている場合、アンチスパムおよびアンチウイルス スキャンを実行します。言い換えると、認識されているウイルスが含まれる既知のスパムまたはメッセージは、アウトブレイク フィルタ機能でスキャンされる前に、アンチスパムおよびアンチウイルス設定に基づいてメール ストリームから除去（削除、隔離など）されているため、アウトブレイク フィルタ機能ではスキャンされません。このため、アウトブレイク フィルタ機能に到達するメッセージは、スパムおよびウイルスを含まないとマークされています。アウトブレイク フィルタによって隔離されたメッセージは、CASEによって隔離解除されて、再スキャンされる際、アップデートされたスパム ルール

およびウイルス定義に基づいて、スパムまたはウイルスを含んでいるとしてマークされる可能性があることに注意してください。

（注） フィルタおよびエンジンがディセーブルになっていることでアンチスパムおよびアンチウイルス スキャンをスキップするメッセージでも、アウトブレイク フィルタによってスキャンされます。

関連項目

- メッセージ スコアリング （523 ページ）
- 動的隔離 （524 ページ）

メッセージ スコアリング

新しいウイルス攻撃または非ウイルス性の脅威がコンピュータ ネットワークに放たれた時点では、脅威を認識できるアンチウイルスやアンチスパム ソフトウェアはまだありません。アウトブレイク フィルタ機能が非常に重要となるのは、このときです。着信メッセージは、発行されているアウトブレイクおよびアダプティブルールを使用して、CASEによりスキャンおよびスコアリングされます（ルールのタイプ：アダプティブ ルールおよびアウトブレイク ルール（519ページ）を参照）。メッセージスコアはメッセージの脅威レベルに対応しています。メッセージに該当するルールがあった場合は、どのルールに一致したかに従って、CASE は対応する脅威レベルを割り当てます。関連する脅威レベルが存在しない（メッセージに一致するルールが存在しない）場合は、メッセージには脅威レベル 0 が割り当てられます。

その計算が完了すると、電子メールゲートウェイは、メッセージの脅威レベルが隔離またはメッセージ変更のしきい値以上であるかどうかをチェックし、メッセージを隔離するかメッセージの URL を書き換えます。脅威レベルがしきい値を下回る場合、パイプラインの後続の処理が継続されます。

さらに、CASE は既存の隔離されているメッセージを最新のルールに照らして再評価し、メッセージの最新の脅威レベルを決定します。これにより、アウトブレイク メッセージに整合する脅威レベルを持つメッセージのみが隔離され続け、脅威と見なされなくなったメッセージは自動再評価の後に隔離エリアから解放されます。

1 つのアウトブレイク メッセージで複数のスコアが存在する場合（1 つのスコアが、あるアダプティブ ルールに基づいたもの（または該当するアダプティブ ルールが複数ある場合はそのうちの最も高いスコア）で、別のスコアはあるアウトブレイク ルールに基づいたもの（または該当するアウトブレイク ルールが複数ある場合はそのうちの最も高いスコア）である場合）は、インテリジェント アルゴリズムを使用して最終的な脅威レベルが決定されます。

アウトブレイクフィルタ機能は、電子メールゲートウェイでアンチウイルススキャンをイネーブルにしなくても使用できます。この2つのセキュリティ サービスは、お互いを補完するように設計されていますが、別々に動作しています。ただし、電子メールゲートウェイでアンチウイルススキャンをイネーブルにしていない場合は、アンチウイルスベンダーのアップデートをモニタリングして、アウトブレイク隔離エリアにあるメッセージの一部を手動で隔離解除した

り、再評価したりする必要があります。アンチウイルス スキャンをイネーブルにしないでアウトブレイク フィルタを使用する場合は、次の点に注意してください。

- アダプティブ ルールはディセーブルにする必要があります。
- メッセージはアウトブレイク ルールに従って隔離されます。
- 脅威レベルが引き下げられたり、隔離時間の期限が過ぎたりした場合は、メッセージは隔離解除されます。

ダウンストリームのアンチウイルス ベンダー（デスクトップ/グループウェア）は、隔離解除されたメッセージを捕捉する場合があります。

（注） アウトブレイクフィルタ機能が非ウイルス性の脅威をスキャンするために、Anti-Spam スキャンを電子メールゲートウェイでグローバルにイネーブルにする必要があります。

動的隔離

アウトブレイク フィルタ機能のアウトブレイク隔離エリアは、メッセージが脅威であると確認されるか、ユーザに配信しても安全であることが確認されるまで、一時的にメッセージを保管しておくための保持領域です。（詳細については、アウトブレイク ライフサイクルおよびルール発行（525 ページ）を参照してください。）隔離されたメッセージは、複数の方法でアウトブレイク隔離エリアから解放できます。新しいルールがダウンロードされると、アウトブレイク隔離エリアにあるメッセージは、CASE によって計算された推奨再スキャン間隔に基づいて再評価されます。更新されたメッセージの脅威レベルが隔離保持のしきい値よりも低くなった場合、メッセージは自動的に（アウトブレイク隔離の設定に関係なく）隔離解除されるため、メッセージが隔離されている時間を最小限に抑えることができます。メッセージの再評価中に新しいルールが発行された場合は、再スキャンが開始されます。

ウイルス攻撃として隔離されるメッセージは、新しいアンチウイルス シグニチャが使用可能な場合は、自動的にアウトブレイク隔離エリアからリリースされることはないため、注意してください。新しいルールは、新しいアンチウイルス シグニチャを参照している場合と、参照していない場合があります。ただし、アウトブレイク ルールによりメッセージの脅威レベルが設定されている脅威レベルのしきい値よりも低いスコアに変更されない限り、アンチウイルス エンジンがアップデートされたことによって、メッセージが隔離解除されることはありません。

CASE の推奨保持期間が経過した場合も、メッセージはアウトブレイク隔離エリアから解放されます。CASE は、メッセージの脅威レベルに基づいて保持期間を計算します。ウイルス アウトブレイクおよび非ウイルス性の脅威に対して別々の最大保持期間を定義できます。CASE の推奨保持期間がその脅威タイプの最大保持期間を超える場合、電子メールゲートウェイは、最大保持期間が経過した時点でメッセージを解放します。ウイルス性のメッセージのデフォルトの最大隔離期間は 1 日です。非ウイルス性の脅威を隔離するデフォルト期間は 4 時間です。メッセージを、手動で隔離解除できます。

また、隔離エリアがいっぱいであるときに、追加のメッセージが挿入されると、 電子メールゲートウェイもメッセージを解放します（これはオーバーフローと呼ばれます）。オーバーフローは、アウトブレイク隔離エリアが容量の 100 % まで使用されているときに、新しいメッ

セージが隔離エリアに追加された場合のみ発生します。このとき、メッセージが隔離解除される優先順位は次のとおりです。

- アダプティブ ルールにより隔離されたメッセージ（最も早く隔離解除されるようにスケジュール設定されているものから）
- アウトブレイク ルールにより隔離されたメッセージ（最も早く隔離解除されるようにスケジュール設定されているものから）

アウトブレイク隔離エリアの使用量が容量の100％を下回った時点で、オーバーフローは停止します。隔離エリアのオーバーフローの処理方法に関する詳細については、隔離内のメッセージの保持期間 （1134ページ）および隔離メッセージに自動的に適用されるデフォルト アクション （1135 ページ）を参照してください。

アウトブレイク隔離エリアから解放されたメッセージは、アンチウイルスおよびアンチスパム エンジンがメール ポリシーでイネーブルとなっている場合、アンチウイルスおよびアンチスパム エンジンによって再度スキャンされます。このときに既知のウイルスまたはスパムとしてマークされた場合は、このメッセージはメール ポリシー設定に従って処理されます（ウィルス隔離エリアまたはスパム隔離エリアに隔離される場合もあります）。詳細については、アウトブレイク フィルタ機能とアウトブレイク隔離 （536 ページ）を参照してください。

このため、メッセージのライフタイムの間に、メッセージは2回隔離される場合がある（1回はアウトブレイク フィルタ機能により、もう1回はアウトブレイク隔離エリアから解放されたとき）と注意しておくことが重要です。各スキャン（アウトブレイク フィルタの前およびアウトブレイク隔離エリアから解放されたとき）照合の結果、何らかの判断がなされたメッセージは、2回隔離されることはありません。また、アウトブレイク フィルタ機能により、メッセージに対して最終的なアクションが実行されることはないことにも注意してください。アウトブレイク フィルタ機能は、（後続の処理のために）メッセージを隔離するか、またはメッセージをパイプラインの次の手順に移動します。

関連項目

- アウトブレイク ライフサイクルおよびルール発行 （525 ページ）

アウトブレイク ライフサイクルおよびルール発行

ウイルスのアウトブレイク ライフサイクルの非常に初期の段階では、メッセージを隔離するために広範なルールが多く使用されます。より詳しい情報が判明していくと、より的を絞ったルールが発行され、隔離する対象の定義が絞り込まれていきます。新しいルールが発行されると、その時点でウイルス メッセージの可能性があると見なされなくなったメッセージは、隔離解除されます（アウトブレイク隔離エリアにあるメッセージは、新しいルールが発行されると再スキャンされます）。

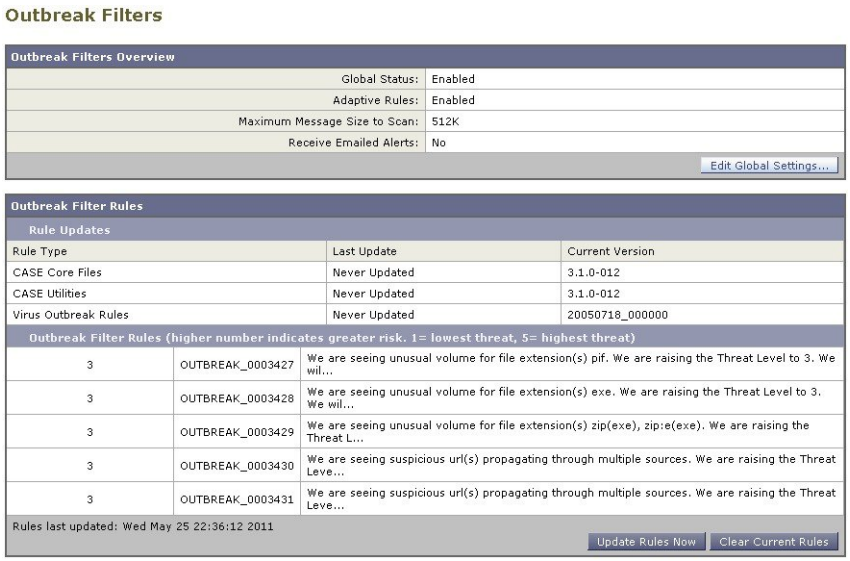
表 *41 :* アウトブレイク ライフサイクルのルールの例

時刻	ルール タイプ	ルールの説明	操作
T=0	アダプティブ ルール（過去のアウトブレイクに基づく）	10 万を超えるメッセージ属性に基づく、統合されたルールセットで、メッセージの内容、コンテキスト、および構造を分析します。	アダプティブ ルールに一致したメッセージは、自動的に隔離されます。
T=5 分	アウトブレイク ルール	.zip（exe）ファイルが含まれるメッセージを隔離します。	.exe が含まれる .zip 形式の添付ファイルはすべて隔離されます。
T=10 分	アウトブレイク ルール	50 KB を超える .zip（exe）ファイルが含まれるメッセージを隔離します。	50 KB 未満の .zip（exe）ファイルが含まれたメッセージはすべて隔離解除されます。
T=20 分	アウトブレイク ルール	ファイル名に「Price」が含まれる 50 ～ 55 KB の .zip（exe）ファイルが含まれるメッセージを隔離します。	この基準に一致しないメッセージはすべて隔離解除されます。
T=12 時間	アウトブレイク ルール	新しいシグニチャを使用してスキャンします。	残っているすべてのメッセージを、最新のアンチウイルス シグニチャを使用してスキャンします

アウトブレイク フィルタの管理

グラフィカル ユーザー インターフェイス（GUI）にログインし、メニューの [セキュリティ サービス（Security Services）] を選択して、[アウトブレイクフィルタ（Outbreak Filters）] をクリックします。

図 *30 : [*アウトブレイク フィルタ（***Outbreak Filters***）*]* メインページ



[アウトブレイクフィルタ（Outbreak Filters）] ページには、[アウトブレイクフィルタの概要（Outbreak Filters Overview）] と現在の [アウトブレイクフィルタのルール（Outbreak Filter Rules）]（存在する場合）のリストの 2 つのセクションが表示されます。

上の図で、アウトブレイク フィルタはイネーブル、Adaptive Scanning はイネーブル、また最大メッセージ サイズは 512 K に設定されています。これらの設定を変更するには、[グローバル設定を編集（Edit Global Settings）] をクリックします。グローバル設定の編集に関する詳細については、アウトブレイク フィルタのグローバル設定の構成（528 ページ）を参照してください。

[アウトブレイクフィルタのルール（Outbreak Filter Rules）] セクションには、各種コンポーネント（ルール自体だけでなくルールエンジンも含む）の最新アップデートの時刻、日付、およびバージョンのリストと、脅威レベルと共にアウトブレイク フィルタ ルールのリストが示されます。

アウトブレイク ルールの詳細については、アウトブレイク フィルタ ルール （530 ページ）を参照してください。

関連項目

- アウトブレイク フィルタのグローバル設定の構成 （528 ページ）
- アウトブレイク フィルタ ルール （530 ページ）
- アウトブレイク フィルタ機能とメール ポリシー （531 ページ）
- アウトブレイク フィルタ機能とアウトブレイク隔離 （536 ページ）

アウトブレイク フィルタのグローバル設定の構成

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [アウトブレイク フィルタ（Outbreak Filters）] をクリックします。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 要件に応じて、次を実行します。

- アウトブレイク フィルタをグローバルにイネーブルにします。
- アダプティブ ルールのスキャンをイネーブルにします。
- スキャンするファイルの最大サイズを設定します（サイズをバイトで入力することに注意してください）。
- アウトブレイク フィルタのアラートをイネーブルにします。
- Web インタラクション トラッキングをイネーブルにします。Web インタラクション トラッキング （549 ページ）を参照してください。

ステップ 4 変更を送信し、保存します。

次のタスク

この機能は、outbreakconfig CLI コマンドによっても使用可能です（『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照）。変更を加えたら、送信して確定します。

（注） Web インターフェイスを使用して URL のロギングをイネーブルにすることはできません。CLI を使用して URL のロギングをイネーブルにする手順については、URL のロギングと URL のメッセージ トラッキングの詳細の有効化 （529 ページ）を参照してください。

関連項目

- アウトブレイク フィルタ機能の有効化 （528 ページ）
- アダプティブ ルールの有効化 （529 ページ）
- アウトブレイク フィルタのアラートの有効化 （529 ページ）
- URL のロギングと URL のメッセージ トラッキングの詳細の有効化 （529 ページ）

アウトブレイク フィルタ機能の有効化

アウトブレイク フィルタ機能をグローバルに有効にするには、[アウトブレイクフィルタのグローバル設定（Outbreak Filters Global Settings）] ページの [アウトブレイクフィルタを有効にす

る（Enable Outbreak Filters）] の横にあるボックスをオンにして、[送信（Submit）] をクリックします。事前にアウトブレイク フィルタのライセンス契約書に同意しておく必要があります。

いったんグローバルにイネーブルにした後は、アウトブレイク フィルタ機能は、各送受信メール ポリシー（デフォルト ポリシーも含む）に対して個別にイネーブルまたはディセーブルにできます。詳細については、アウトブレイク フィルタ機能とメール ポリシー（531 ページ）を参照してください。

アウトブレイクフィルタ機能は、アンチスパムスキャンがイネーブルになっているかどうかに関係なく、コンテキスト適応スキャンエンジン（CASE）を使用してウイルス性の脅威を検出します。ただし、非ウイルス性の脅威をスキャンするために、 電子メールゲートウェイで Anti-Spam または Intelligent Multi-Scan をグローバルにイネーブルにする必要があります。

（注） システムのセットアップ中にライセンスに同意しなかった場合（手順 4：セキュリティ（46 ページ）を参照）は、[セキュリティサービス（Security Services）] > [アウトブレイクフィルタ（Outbreak Filters）] ページで [有効（Enable）] をクリックして、ライセンス契約を読み、同意する必要があります。

アダプティブ ルールの有効化

Adaptive Scanning は、アウトブレイク フィルタのアダプティブ ルールをイネーブルにします。メッセージの内容に関するウイルス シグニチャまたはスパム基準が使用できない場合は、一連の係数または特性（ファイルサイズなど）が使用されて、メッセージがアウトブレイクの一部である可能性が決定されます。Adaptive Scanning を有効にするには、[アウトブレイクフィルタのグローバル設定（Outbreak Filters Global Settings）] ページの [適応ルールを有効にする（Enable Adaptive Rules）] の横にあるボックスをオンにして、**[送信（Submit）]** をクリックします。

アウトブレイク フィルタのアラートの有効化

[アラート メール（Emailed Alerts）] というラベルの付いたボックスをオンにして、アウトブレイク フィルタ機能のアラートをイネーブルにします。アウトブレイク フィルタの電子メール アラートのイネーブル化は、単にアラートエンジンをイネーブルにして、アウトブレイクフィルタに関するアラートが送信されるようにするためのものです。送信されるアラートおよび送信先の電子メール アドレスの指定は、[アラート（Alerts）] ページの [システム管理（System Administration）] タブで設定します。アウトブレイク フィルタのアラートの設定に関する詳細については、アラート、SNMP トラップ、およびアウトブレイク フィルタ（540 ページ）を参照してください。

URL のロギングと URL のメッセージ トラッキングの詳細の有効化

URL 関連のログのログ収集と、メッセージ トラッキングの詳細のこの情報の表示は、デフォルトで無効になっています。これには、次のイベントのログが含まれます。

- メッセージ内の特定の URL のカテゴリが URL カテゴリ フィルタと一致した
- メッセージ内の特定の URL のレピュテーション スコアが URL レピュテーション フィルタと一致した

- アウトブレイク フィルタによってメッセージ内の特定の URL が書き換えられた

これらのイベントのロギングをイネーブルにするには、CLI で `websecurityadvancedconfig` コマンドを使用するか、Web インターフェイスで [セキュリティサービス（Security Services）] > [URL フィルタリング（URL Filtering）] ページに移動します。

関連項目

- アウトブレイク フィルタ ルールの管理 （530 ページ）

アウトブレイク フィルタ ルール

アウトブレイクルールは、Cisco Security Intelligence Operations から発行されます。電子メールゲートウェイは新しいアウトブレイクルールを 5 分ごとにチェックおよびダウンロードします。このアップデート間隔を変更できます。詳細については、アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）を参照してください。

関連項目

- アウトブレイク フィルタ ルールの管理 （530 ページ）

アウトブレイク フィルタ ルールの管理

アウトブレイク フィルタ ルールは自動的にダウンロードされるため、ユーザによる管理は一切必要ありません。

ただし、何らかの理由で電子メールゲートウェイが一定期間シスコのアップデートサーバの新しいルールにアクセスできない場合は、ローカルでキャッシュされているスコアが有効でなくなっている（つまり、既知のウイルス性の添付ファイルタイプが現在ではアンチウイルスソフトウェアのアップデートに含まれている、またはすでに脅威ではなくなっている、またはその両方の場合）可能性があります。この場合は、これらの特性を持つメッセージを隔離しておく必要はありません。

[ルールを今すぐアップデート（Update Rules Now）] をクリックすることによって、シスコのアップデートサーバから、アップデートされたアウトブレイクルールを手動でダウンロードできます。

（注） [ルールを今すぐアップデート（Update Rules Now）] ボタンは、電子メールゲートウェイの既存のアウトブレイクルールを「フラッシュ」しません。アップデートされたアウトブレイク ルールを置き換えるだけです。シスコのアップデートサーバに利用可能なアップデートがない場合、電子メールゲートウェイはこのボタンをクリックするまでアウトブレイクルールをダウンロードしません。

関連項目

- アウトブレイク フィルタ ルールのアップデート （531 ページ）

アウトブレイク フィルタ ルールのアップデート

デフォルトでは、 電子メールゲートウェイは 5 分ごとに新しいアウトブレイク フィルタ ルールのダウンロードを試行します。この間隔は、[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで変更できます。詳細については、サービス アップデート （1253 ページ）を参照してください。

アウトブレイク フィルタ機能とメール ポリシー

アウトブレイク フィルタ機能の設定には、メールポリシーごとに設定できるものがあります。アウトブレイクフィルタ機能は、電子メールゲートウェイでメールポリシーごとにイネーブルまたはディセーブルにできます。メールポリシーごとに、特定のファイル拡張子およびドメインをアウトブレイク フィルタ機能の処理から除外できます。この機能は、policyconfig CLI コマンドによっても使用可能です（『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照）。

（注） アウトブレイクフィルタ機能が非ウイルス性の脅威をスキャンするために、Anti-Spam または Intelligent Multi-Scan スキャンを 電子メールゲートウェイでグローバルにイネーブルにする必要があります。

特定のメール ポリシーに対するアウトブレイク フィルタ機能の設定を変更するには、変更するポリシーの [アウトブレイクフィルタ（Outbreak Filters）] 列のリンクをクリックします。

特定のメール ポリシーに対してアウトブレイク フィルタ機能をイネーブルにし、カスタマイズするには、[アウトブレイクフィルタを有効にする（設定をカスタマイズ）（Enable Outbreak Filtering (Customize Settings)）] を選択します。

メール ポリシーに対して次のアウトブレイク フィルタ設定を構成できます。

- 隔離脅威レベル
- 最大隔離保持期間
- 非ウイルス性の脅威メッセージを隔離に追加せずに即時に配信
- バイパスするファイル拡張子のタイプ
- メッセージ変更のしきい値
- カスタム テキストおよびアウトブレイク フィルタ変数（$threat_verdict、$threat_category、$threat_type、$threat_description、および $threat_level など）を使用して件名ヘッダーを変更します。
- 次の電子メール ヘッダーを組み込みます。
  - X-IronPort-Outbreak-Status
  - X-IronPort-Outbreak-Description
- 電子メールゲートウェイまたは Exchange サーバなどの代替宛先にメッセージを送信します。
- URL 書き換え
- 脅威の免責事項

[アウトブレイクフィルタを有効にする（デフォルトのメールポリシー設定を継承）（Enable Outbreak Filtering (Inherit Default mail policy settings)）] を選択して、デフォルトのメール ポリシーについて定義されているアウトブレイク フィルタ設定を使用します。デフォルト メール ポリシーでアウトブレイク フィルタ機能をイネーブルにしている場合は、その他すべてのメール ポリシーはカスタマイズしない限り同じアウトブレイク フィルタ設定を使用します。

設定を変更したら、変更を確定します。

関連項目

- 隔離レベルのしきい値の設定 （532 ページ）
- 最大隔離保持 （532 ページ）
- ファイル拡張子タイプのバイパス （532 ページ）
- メッセージ変更 （533 ページ）

隔離レベルのしきい値の設定

リストからアウトブレイクの脅威に対する[隔離する脅威レベル（Quarantine Threat Level）]のしきい値を選択します。数字が小さいほど隔離されるメッセージは多くなり、数字が大きいほど隔離されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

詳細については、隔離脅威レベルのしきい値設定ガイドライン （521 ページ）を参照してください。

最大隔離保持

メッセージがアウトブレイク隔離エリアに留まる最大時間を指定します。ウイルス性の添付ファイルを含む可能性のあるメッセージ、およびフィッシングやマルウェア リンクなどその他の脅威を含む可能性のあるメッセージに対して異なる保持期間を指定できます。非ウィルス性の脅威の場合は、メッセージを隔離に追加せずに即時に配信するには [隔離に追加せずにメッセージを送信します（Deliver messages without adding them to quarantine）] チェックボックスをオンにします。

（注） ポリシーで [メッセージの変更（Message Modification）] をイネーブルにしない限り、非ウイルス性の脅威を隔離できません。

CASEは、メッセージに脅威レベルを割り当てるときに隔離保持期間を推奨しています。電子メールゲートウェイは、脅威タイプに対する最大隔離保持期間を超えない限り、CASE が推奨する時間の長さの間、隔離されるメッセージを保持します。

ファイル拡張子タイプのバイパス

特定のファイル タイプをバイパスするようにポリシーを変更できます。バイパスされたファイル拡張子は、CASE によるメッセージの脅威レベルの計算から除外されます。ただし、添付ファイルに対する残りの電子メール セキュリティ パイプラインの処理は行われます。

ファイル拡張子をバイパスするには、[添付ファイルのスキャンのバイパス（Bypass Attachment Scanning）] をクリックし、ファイル拡張子を選択または入力してから、[拡張子を追加（Add Extension）] をクリックします。AsyncOS は、[バイパスするファイル拡張子（File Extensions to Bypass）] リストに拡張子タイプを表示します。

バイパスされる拡張子のリストから拡張子を削除するには、[バイパスするファイル拡張子（File Extensions to Bypass）] リストの拡張子の横のゴミ箱アイコンをクリックします。

関連項目

- ファイル拡張子のバイパス：コンテナ ファイルのタイプ （533 ページ）

ファイル拡張子のバイパス：コンテナ ファイルのタイプ

ファイル拡張子をバイパスする場合、コンテナ ファイル内のファイル（たとえば .zip 内の .doc ファイル）もバイパスする拡張子のリストに含まれていれば、バイパスされます。たとえば、バイパスする拡張子のリストに .doc を追加した場合は、コンテナ ファイルに含まれているものも含めて、すべての .doc ファイルがバイパスされます。

メッセージ変更

電子メールゲートウェイがフィッシングの試行またはマルウェア Web サイトへのリンクなど非ウイルス性の脅威を持つメッセージをスキャンする場合は、[メッセージの変更（Message Modification）] をイネーブルにします。

メッセージの脅威レベルに基づいて、AsyncOS はメッセージを変更し、すべての URL を書き換えて、メッセージから Web サイトを開こうとすると Cisco Web セキュリティ プロキシを経由して受信者をリダイレクトすることができます。電子メールゲートウェイはメッセージに免責事項を追加して、ユーザにメッセージの内容が疑わしい、または不正であることを警告することもできます。

非ウイルス性の脅威メッセージを隔離するために、メッセージ変更をイネーブルにする必要があります。

関連項目

- メッセージ変更の脅威レベル （533 ページ）
- メッセージの件名 （534 ページ）
- アウトブレイク フィルタの電子メール ヘッダー （534 ページ）
- 代替宛先メール ホスト （535 ページ）
- URL 書き換えおよびドメインのバイパス （535 ページ）
- 脅威の免責事項 （536 ページ）

メッセージ変更の脅威レベル

リストから [メッセージの変更 - 脅威レベル（Message Modification Threat Level）] のしきい値を選択します。この設定は、CASE によって返される脅威レベルに基づいて、メッセージを変更するかどうかを決定します。数字が小さいほど変更されるメッセージは多くなり、数字が大

きいほど変更されるメッセージは少なくなります。シスコは、デフォルト値の 3 を推奨します。

メッセージの件名

変更されたリンクを含む非ウイルス性の脅威メッセージで件名ヘッダーのテキストを変更すると、ユーザにメッセージが保護のために変更されたことを通知できます。カスタムテキストとアウトブレイク フィルタ変数（`$threat_verdict`、`$threat_category`、`$threat_type`、`$threat_description`、および `$threat_level` など）のいずれかまたは両方を、件名ヘッダーの前または後に追加します。変数を挿入するには、[変数の挿入（Insert Variables）] をクリックし、変数のリストから選択します。

[メッセージの件名（Message Subject）] フィールドでは、空白は無視されません。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、`[MODIFIED FOR PROTECTION]` というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

（注） [メッセージの件名（Message Subject）] フィールドでは、US-ASCII 文字だけを使用できます。

アウトブレイク フィルタの電子メール ヘッダー

次のヘッダーをメッセージに追加できます。

ヘッダー	フォーマット	例	オプション
X-IronPort-Outbreak-Status	`X-IronPort-Outbreak-Status: $threat_verdict, level $threat_level, $threat_category - $threat_type`	`X-IronPort-Outbreak-Status: Yes, level 4, Phish - Password`	• すべてのメッセージで有効（Enable for all messages） • 非ウイルス性アウトブレイクでのみ有効（Enable only for non-viral outbreak） • 無効（Disable）
X-IronPort-Outbreak-Description	`X-IronPort-Outbreak-Description: $threat_description`	`X-IronPort-Outbreak-Description: It may trick victims into submitting their username and password on a fake website.`	• 有効 • 無効

（注） これらのヘッダーに基づいてメッセージをフィルタリングする場合は、（代替宛先メールホストを設定して）アウトブレイクフィルタで処理されたメッセージを電子メールゲートウェイに戻し、これらのヘッダーに一致するコンテンツフィルタを使用してメッセージをスキャンする必要があります。

代替宛先メール ホスト

アウトブレイクフィルタにより処理されたメッセージに対してコンテンツフィルタベースのスキャンを実行する場合は、処理されたメッセージを電子メールゲートウェイに戻すようにアウトブレイクフィルタを設定する必要があります。これは、処理パイプラインではコンテンツフィルタ スキャンの後にアウトブレイク フィルタ スキャンが実行されるためです。

[代替宛先メールホスト（Alternate Destination Mail Host）] フィールドに、処理後のメッセージをさらにスキャンするために送信する 電子メールゲートウェイの IP アドレス（IPv4 または IPv6）または FQDN を入力します。

URL 書き換えおよびドメインのバイパス

メッセージの脅威レベルがメッセージ変更のしきい値を超える場合、アウトブレイク フィルタ機能はメッセージ内のすべての URL を書き換え、これらの URL をクリックするとユーザを Cisco Web セキュリティ プロキシのスプラッシュ ページにリダイレクトします。（詳細については、URL のリダイレクト（518 ページ）を参照してください。）メッセージの脅威レベルが隔離のしきい値を超える場合、アプライアンスがメッセージの隔離も行います。小規模の非ウイルス性のアウトブレイクが進行中の場合、メッセージの隔離は TOC に、アウトブレイクの可能性があるメッセージからリンクされるすべての疑わしい Web サイトを分析し、その Web サイトが不正であるかどうか判断する時間を与えます。CASE は、SIO が提供するアップデートされたアウトブレイク ルールを使用してメッセージを再スキャンし、メッセージがアウトブレイクの一部であるかを判断します。保持期間が過ぎると、 電子メールゲートウェイはメッセージを隔離から解放します。

AsyncOS は、バイパスされるドメインを指している URL を除き、メッセージ内のすべての URL を書き換えます。

[URLの書き換え（URL Rewriting）] では次のオプションを使用できます。

- [未署名のメッセージでのみ有効（Enable only for unsigned messages）]：このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超える未署名のメッセージ内の URL を書き換えられるようになります。ただし、署名されたメッセージは含まれません。URL 書き換えについて、シスコはこの設定の使用を推奨します。

（注） 電子メールゲートウェイ以外のネットワーク上のサーバまたはアプライアンスが DomainKeys/DKIM 署名の検証を担当する場合、電子メールゲートウェイは、DomainKeys/DKIM-signed メッセージ内の URL を書き換えたり、メッセージの署名を無効にしたりすることができます。

S/MIME を使用して暗号化されている場合または S/MIME 署名が含まれる場合、電子メールゲートウェイはメッセージを署名済みとみなします。

- **[すべてのメッセージで有効（Enable for all messages）]**：このオプションによって、AsyncOS は、メッセージ変更のしきい値を満たすか超えるすべてのメッセージ内の URL を書き換えられるようになります。署名されたメッセージも含まれます。AsyncOS が署名されたメッセージを変更すると、署名は無効になります。
- **[無効（Disable）]**：このオプションはアウトブレイク フィルタに対して URL 書き換えをディセーブルにします。

ポリシーを変更して、特定のドメインへの URL を変更から除外できます。ドメインをバイパスするには、IPv4 アドレス、IPv6 アドレス、CIDR 範囲、ホスト名、部分ホスト名、またはドメインを [ドメインのスキャンをバイパス（Bypass Domain Scanning）] フィールドに入力します。複数のエントリを指定する場合は、カンマで区切ります。

バイパスドメインスキャン機能は、URL フィルタリングで使用されるグローバル許可リストに似ていますが、無関係です。許可リストの詳細については、URL フィルタリングの許可リストの作成 （550 ページ）を参照してください。

脅威の免責事項

電子メールゲートウェイは、疑わしいメッセージのヘッダーの上部に免責事項メッセージを追加して、ユーザにメッセージの内容を警告することができます。この免責事項には、メッセージのタイプに応じて HTML またはプレーン テキストが使用できます。

[脅威に関する免責事項（Threat Disclaimer）] リストから使用する免責事項のテキストを選択するか、[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] リンクをクリックし、[免責事項テンプレート（Disclaimer Template）] を使用して新しい免責事項を作成します。[免責事項テンプレート（Disclaimer Template）] には、アウトブレイク脅威情報に関する変数が含まれます。[免責事項のプレビュー（Preview Disclaimer）] をクリックすると、脅威免責事項のプレビューを表示できます。カスタム免責事項メッセージでは、変数を使用してメッセージの脅威レベル、脅威のタイプ、および脅威の説明を表示できます。免責事項メッセージの作成については、テキストリソース管理の概要 （802 ページ）を参照してください。

アウトブレイク フィルタ機能とアウトブレイク隔離

アウトブレイク フィルタ機能により隔離されたメッセージは、アウトブレイク隔離エリアに送信されます。この隔離エリアは、メッセージを隔離するために使用されるルール（アウトブレ

イク ルールの場合はアウトブレイク ID、アダプティブ ルールの場合は一般名称が表示されます）に基づいて、隔離エリアからすべてのメッセージを削除または解放する際に役立つ「サマリー」ビューがあることを除けば、その他のあらゆる隔離と同様に機能します（隔離の操作方法の詳細については、ポリシー、ウイルス、およびアウトブレイク隔離（1129ページ）を参照してください）。サマリー ビューの詳細については、[アウトブレイク隔離（Outbreak Quarantine）]および[ルールサマリーによる管理（Manage by Rule Summary）] ビュー（538 ページ）を参照してください。

関連項目

- アウトブレイク隔離のモニタリング （537 ページ）
- [アウトブレイク隔離（Outbreak Quarantine）]および[ルールサマリーによる管理（Manage by Rule Summary）] ビュー （538 ページ）

アウトブレイク隔離のモニタリング

適切に設定された隔離エリアはほとんどモニタリングを必要としませんが、特にウイルスアウトブレイクの発生中または発生後の、正規のメッセージが遅延する可能性がある間は、アウトブレイク隔離エリアに注意を払うことを推奨します。

正規のメッセージが隔離された場合、アウトブレイク隔離の設定によっては、次のいずれかが発生します。

- 隔離のデフォルト アクションが [リリース（Release）] に設定されている場合は、保持期間の期限が切れたとき、または隔離エリアがオーバーフローしたときにメッセージが解放されます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクションがメッセージに対して実行されるように、アウトブレイク隔離を設定できます。これらのアクションの詳細については、隔離メッセージに自動的に適用されるデフォルトアクション （1135ページ）を参照してください。
- 隔離のデフォルト アクションが [削除（Delete）] に設定されている場合は、保持期間の期限が切れたとき、または隔離エリアがオーバーフローしたときにメッセージが削除されます。
- オーバーフローは、隔離エリアがいっぱいのときにさらにメッセージが追加された場合に発生します。この場合は、有効期限日に近いメッセージから（必ずしも最も古いメッセージからとは限りません）、新しいメッセージに十分な領域が空くまで、メッセージが解放されていきます。オーバーフローのためにメッセージが解放される前に、添付ファイルの削除、件名の変更、X-Header の追加といったアクションがメッセージに対して実行されるように、アウトブレイク隔離を設定できます。

隔離されているメッセージは、新しいルールが発行されるたびに再スキャンされるため、アウトブレイク隔離エリアにあるメッセージは有効期限が切れる前に解放されることがほとんどです。

それでも、デフォルト アクションが [削除（Delete）] に設定されている場合は、アウトブレイク隔離エリアをモニタすることが重要です。シスコは、ほとんどのユーザに対して、デフォルト アクションを [削除（Delete）] に設定しないことを推奨します。アウトブレイク隔離エリアからのメッセージの解放、またはアウトブレイク隔離のデフォルト アクションの変更に関する

詳細については、隔離メッセージに自動的に適用されるデフォルトアクション （1135ページ）を参照してください。

反対に、新しいルールのアップデートを待つ間、アウトブレイク隔離エリアに長時間留めておきたいメッセージがある場合は、たとえばそのメッセージの有効期限を遅らせることもできます。メッセージの保持期間を増やすことにより、隔離エリアのサイズが大きくなる場合があるため、注意してください。

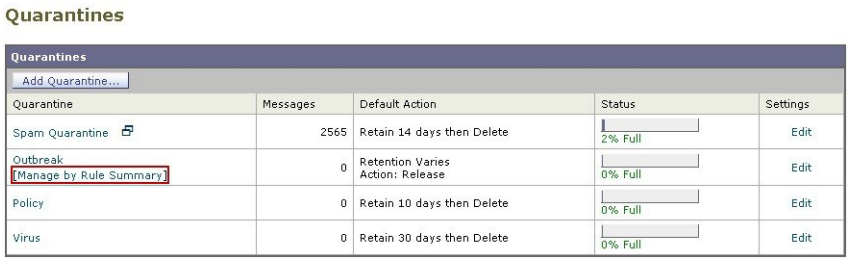
（注） メッセージが アウトブレイク隔離エリアに留まっている間にアンチウイルス スキャンが（メールポリシーごとではなく）グローバルにディセーブルにされた場合は、たとえメッセージが解放される前にもう一度アンチウイルス スキャンを再度イネーブルにしたとしても、そのメッセージが解放されたときのアンチウイルス スキャンは実行されません。

（注） アウトブレイクフィルタ機能は、 電子メールゲートウェイでアンチウイルススキャンをイネーブルにしなくても使用できます。ただし、アプライアンスでアンチスパム スキャンがイネーブルでない場合は、アウトブレイク フィルタは非ウイルス性の脅威をスキャンできません。

[アウトブレイク隔離（OutbreakQuarantine）]および[ルールサマリーによる管理（Manage by Rule Summary）] ビュー

GUI の [モニタ（Monitor）] メニューにあるリスト内の隔離名をクリックすることで、アウトブレイク隔離エリアの内容を表示できます。アウトブレイク隔離には、追加のビューである、アウトブレイク隔離の [ルールサマリーによる管理（Manage by Rule Summary）] リンクもあります。

図 *31* : アウトブレイク隔離の *[ルールサマリーによる管理（Manage by Rule Summary）]* リンク



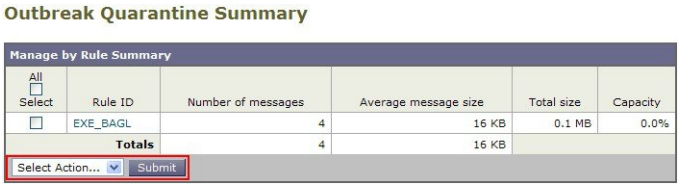
関連項目

- サマリー ビューの使用によるアウトブレイク隔離エリア内のメッセージに対するルール ID に基づいたメッセージ アクションの実行 （539 ページ）

サマリー ビューの使用によるアウトブレイク隔離エリア内のメッセージに対するルール ID に基づいたメッセージ アクションの実行

[ルールサマリーによる管理（Manage by Rule Summary）] リンクをクリックして、ルール ID ごとにグループ化されたアウトブレイク隔離の内容のリストを表示します。

図 *32*：アウトブレイク隔離の *[*ルールサマリーによる管理（*Manage by Rule Summary*）*]* ビュー



個別にメッセージを選択しなくても、このビューから特定のアウトブレイクまたはアダプティブルールに関するすべてのメッセージに対して、解放、削除、または保持期間延長を実行するように選択できます。また、検索またはリストのソートも実行できます。

この機能は、quarantineconfig -> outbreakmanage CLI コマンドからも使用できます。詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

アウトブレイク フィルタのモニタリング

電子メールゲートウェイには、アウトブレイクフィルタ機能のパフォーマンスおよび活動をモニタする複数のツールが含まれています。

関連項目

- アウトブレイク フィルタ レポート （539 ページ）
- アウトブレイク フィルタの概要とルール リスト （539 ページ）
- アウトブレイク隔離 （540 ページ）
- アラート、SNMP トラップ、およびアウトブレイク フィルタ （540 ページ）

アウトブレイク フィルタ レポート

電子メールゲートウェイのアウトブレイクフィルタの現在のステータスおよび設定に加えて、最近のアウトブレイクやアウトブレイクフィルタによって隔離されたメッセージに関する情報が表示されるアウトブレイク フィルタ レポートです。この情報は、[モニタ（Monitor）] > [アウトブレイクフィルタ（Outbreak Filters）] ページで表示します。詳細については、「電子メール セキュリティ モニタ」の章を参照してください。

アウトブレイク フィルタの概要とルール リスト

概要およびルール リストは、アウトブレイク フィルタ機能の現在の状態に関して役立つ情報を提供します。この情報は、[セキュリティサービス（Security Services）] > [アウトブレイクフィルタ（Outbreak Filters）] ページで表示します。

アウトブレイク隔離

アウトブレイク隔離を使用して、アウトブレイク フィルタの脅威レベルのしきい値により、フラグ付けされているメッセージの数をモニタします。また、ルールごとの隔離メッセージのリストも使用できます。詳細については、[アウトブレイク隔離（Outbreak Quarantine）] および [ルールサマリーによる管理（Manage by Rule Summary）] ビュー （538 ページ）およびポリシー、ウイルス、およびアウトブレイク隔離 （1129 ページ）を参照してください。

アラート、SNMP トラップ、およびアウトブレイク フィルタ

アウトブレイク フィルタ機能は、定期的な AsyncOS アラートと SNMP トラップという 2 つの異なるタイプの通知をサポートしています。

SNMP トラップは、ルールのアップデートが失敗したときに作成されます。AsyncOS の SNMP トラップの詳細については、「CLI を使用した管理とモニタ」の章を参照してください。

AsyncOS のアウトブレイク フィルタ機能には、2 つのタイプのアラート（サイズおよびルール）が用意されています。

AsyncOS アラートは、アウトブレイク隔離エリアのサイズが最大サイズの 5、50、75、および 95 を超えるたびに生成されます。95 % のしきい値を超えたときに生成されるアラートの重大度は CRITICAL、その他のアラートしきい値の場合は WARNING です。アラートは、隔離エリアのサイズが大きくなり、しきい値を超えたときに生成されます。隔離エリアのサイズが小さくなり、しきい値を下回ったときは生成されません。アラートの詳細については、アラート（1275 ページ）を参照してください。

また、AsyncOS はルールが発行されたとき、しきい値が変更されたとき、またはルールまたは CASE エンジンのアップデート中に問題が発生したときにもアラートを生成します。

アウトブレイク フィルタ機能のトラブルシューティング

この項では、アウトブレイク フィルタ機能の基本的なトラブルシューティングに関するヒントをいくつか紹介します。

関連項目

- 誤って分類されたメッセージのシスコへの報告 （540 ページ）
- 複数の添付ファイルおよびバイパスされるファイル タイプ （541 ページ）
- メッセージ フィルタ、コンテンツ フィルタ、および電子メール パイプライン （541 ページ）

誤って分類されたメッセージのシスコへの報告

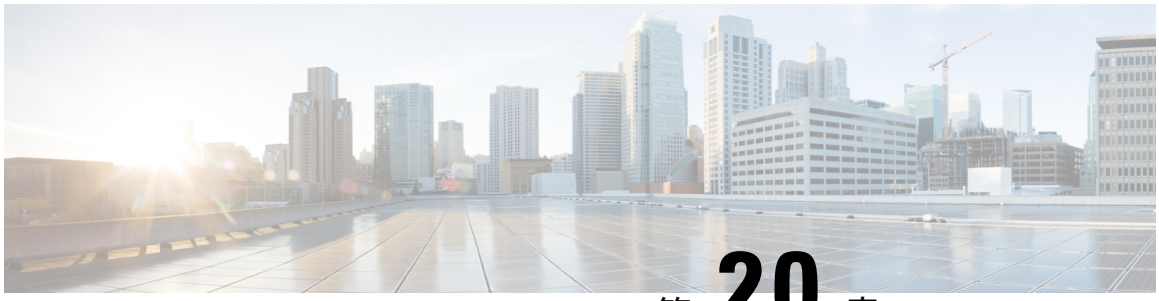
[隔離の管理（Manage Quarantine）] ページのチェックボックスを使用すると、アウトブレイク隔離がシスコに対して誤分類を通知するようになります。

複数の添付ファイルおよびバイパスされるファイル タイプ

バイパスされるファイル タイプは、メッセージに1つだけ添付されているファイルのタイプが指定したタイプであった場合、または、メッセージに複数のファイルが添付されている場合は、その他の添付ファイルに対して既存のルールが存在しない場合のみ、除外されます。これ以外の場合は、メッセージはスキャンされます。

メッセージ フィルタ、コンテンツ フィルタ、および電子メール パイプライン

メッセージ フィルタおよびコンテンツ フィルタは、アウトブレイク フィルタによるスキャンが実行される前にメッセージに適用されます。フィルタを適用することにより、メッセージがアウトブレイク フィルタ スキャンをスキップしたり、バイパスしたりする場合があります。



第 20 章

悪意のある URL または望ましくない URL からの保護

この章は、次の項で構成されています。

- URL 関連の保護および制御 （543 ページ）
- URL フィルタリングの設定 （544 ページ）
- メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （553 ページ）
- URL フィルタリング用にスキャンできないメッセージの処理 （558 ページ）
- コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出 （558 ページ）
- メッセージ フィルタを使用した、メッセージの悪意のある URL の検出 （560 ページ）
- URL フィルタリング結果のモニタ （562 ページ）
- メッセージ トラッキングの URL 詳細の表示 （562 ページ）
- URL フィルタリングのトラブルシューティング （562 ページ）
- URL カテゴリについて （568 ページ）

URL 関連の保護および制御

作業キューのアンチスパム、アウトブレイク、コンテンツおよびメッセージ フィルタリング プロセスには、悪意のあるリンクまたは望ましくないリンクに対する制御および保護が組み込まれています。これらは、以下を制御します。

- メッセージおよび添付ファイルの悪意のある URL からの保護を強化する。

  URL フィルタリングはアウトブレイク フィルタリングに組み込まれています。組織にすでに Cisco Web Security Appliance や、類似する Web ベースの脅威からの保護機能を導入している場合でも、この保護強化機能は脅威をその侵入時点でブロックするため、有用です。

  また、コンテンツ フィルタやメッセージ フィルタを使用して、メッセージに含まれる URL に対してその URL の Web ベース レピュテーション スコア（WBRS）に基づいてアクションを実行することができます。

（注） ベストプラクティスとして、疑わしい、ニュートラル、好ましいまたは不明なレピュテーションを持つ URL は、クリック時の URL の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトするように書き換えることをお勧めします。

- スパムの識別の改善

  電子メールゲートウェイは、メッセージのリンクのレピュテーションとカテゴリを、その他のスパム特定アルゴリズムと組み合わせて使用し、スパムを特定します。たとえば、メッセージのリンクがマーケティングの Web サイトに属している場合、メッセージはマーケティングに関するメッセージである可能性が高いです。

- 企業のアクセプタブル ユース ポリシーの適用のサポート

  URL のカテゴリ（アダルト コンテンツや違法行為など）を、コンテンツ フィルタおよびメッセージ フィルタと組み合わせて使用して、企業のアクセプタブル ユース ポリシーの適用を強化できます。

- 保護のために書き換えられたメッセージに含まれる URL を最も頻繁にクリックした組織内のユーザ、および最も頻繁にクリックされたリンクを識別できます。

関連項目

- 評価される URL （544 ページ）
- [Webインタラクショントラッキング（Web Interaction Tracking）] ページ （1039 ページ）

評価される URL

着信メッセージと発信メッセージ（添付ファイルを含む）に含まれる URL が評価されます。URL を表す有効な文字列（次を含む文字列）が評価されます。

- http、https、www
- ドメインまたは IP アドレス
- コロン（:）が先頭に付いたポート番号
- 大文字または小文字

メッセージがスパムであるかどうかを判定するために URL を評価するときに、これがロード管理に必要である場合は、着信メッセージのスクリーニングが発信メッセージよりも優先されます。

URL フィルタリングの設定

- URL フィルタリングの要件 （545 ページ）
- URL フィルタリングを有効にする （545 ページ）

• Talos インテリジェンスサービスへの接続について （548 ページ）
• Web インタラクション トラッキング （549 ページ）
• クラスタ構成での URL フィルタリング （550 ページ）
• URL フィルタリングの許可リストの作成 （550 ページ）
• サイトに悪意がある場合にエンド ユーザに表示する通知のカスタマイズ （552 ページ）

URL フィルタリングの要件

URL フィルタリングをイネーブルにする他に、必要な機能に応じてその他の機能をイネーブルにする必要があります。

スパムに対する保護の強化：

- スパム対策スキャンは、グローバルにイネーブルにするか、または該当するメール ポリシーごとにイネーブルにする必要があります。これには IronPort Anti-Spam 機能またはインテリジェント マルチスキャン機能のいずれかを使用できます。スパム対策の章を参照してください。

マルウェアに対する保護の強化：

- アウトブレイク フィルタ機能はグローバルにイネーブルにするか、または該当するメール ポリシーごとにイネーブルにする必要があります。アウトブレイク フィルタに関する章を参照してください。

URL のレピュテーションに基づいてアクションを実行するか、またはメッセージ フィルタとコンテンツ フィルタを使用してアクセプタブル ユース ポリシーを適用する場合：

- アウトブレイク フィルタ機能はグローバルにイネーブルにする必要があります。アウトブレイク フィルタに関する章を参照してください。

URL フィルタリングを有効にする

URL フィルタリングは、Web インターフェイスの **[セキュリティ サービス（Security Services）] > [URL フィルタ（URL Filtering）]** ページまたは CLI の **`websecurityconfig`** コマンドを使用してイネーブルにできます。

はじめる前に

- 使用する各 URL フィルタ機能の要件を満たしていることを確認してください。URL フィルタリングの要件 （545 ページ）を参照してください。
- （任意）すべての URL フィルタリング機能で無視する URL のリストを作成します。URL フィルタリングの許可リストの作成 （550 ページ）を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] を選択します。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 [URLカテゴリおよびレピュテーションのフィルタの有効化（Enable URL Category and Reputation Filters）] チェックボックスをオンにします。

ステップ 4 （任意）メッセージを評価し、スパムやマルウェアが含まれているかどうかを確認するときに URL フィルタリングから除外する URL、およびすべてのコンテンツ フィルタリングとメッセージ フィルタリングから除外する URL のリストを作成した場合は、そのリストを選択します。

この設定により、メッセージがスパム対策またはアウトブレイク フィルタの処理をバイパスすることは通常はありません。

ステップ 5 （任意）Web インタラクション トラッキングをイネーブルにします。Web インタラクション トラッキング （549 ページ）を参照してください。

ステップ 6 （任意）[詳細設定（Advanced Settings）] をクリックし、次の表に示す必須パラメータを入力して、URL フィルタリングの詳細設定を行います。

パラメータ	説明
URL ルックアップタイムアウト（URL Lookup Timeout）	URL が特定のドメイン名の IP アドレスを要求するためにかかる時間を入力します。
メッセージ本文でスキャンされる URL の最大数（Maximum Number of URLs scanned in Message Body）	電子メールゲートウェイがメッセージ本文内でスキャンする URL の最大数を入力します。
メッセージ添付ファイルでスキャンされるURL の最大数（Maximum Number of URLs scanned in Message Attachments）	電子メールゲートウェイがメッセージの添付ファイルでスキャンするURLの最大数を入力します。
メッセージ内の URL テキストと HREF の書き換え（Rewrite URL text and HREF in Message）	書き換えられた URL 全体をメッセージ本文に表示する場合は、[はい（Yes）] オプションボタンを選択します。 または 書き換えられた URL 全体を HTML メッセージの HREF にのみ表示する場合は、[いいえ（No）] オプションボタンを選択します。

パラメータ	説明
URL Logging	メールログとメッセージトラッキングに URL の詳細を表示する場合は、[イネーブル化（Enable）] オプションボタンを選択します。 URLの詳細は、次のいずれかの条件に基づいてメールログとメッセージトラッキングに記録されます。 • メッセージ内のいずれかの URL のカテゴリが URL カテゴリフィルタと一致した • メッセージ内のいずれかの URL のレピュテーションスコアが URL レピュテーションフィルタと一致した • アウトブレイクフィルタ（イネーブルな場合）によってメッセージ内のずれかの URL が書き換えられた

ステップ 7 変更を送信し、保存します。

該当する前提条件を満たしており、すでにアウトブレイク フィルタとスパム対策保護を設定している場合は、スパムまたは悪意のある URL の拡張自動検出を利用するために、追加の設定を行う必要はありません。

次のタスク

- メッセージに含まれている URL のレピュテーションに基づいてアクションを実行する場合は、メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （553 ページ）を参照してください。
- コンテンツ フィルタおよびメッセージ フィルタで URL カテゴリを使用するには（アクセプタブル ユース ポリシーを適用する場合など）、メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （553 ページ）を参照してください。
- スパムの可能性があるメッセージの URL をすべて Cisco Web セキュリティ プロキシ サービスにリダイレクトするには、カスタムヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）を参照してください。
- （任意）エンドユーザ通知ページの外観をカスタマイズするには、サイトに悪意がある場合にエンド ユーザに表示する通知のカスタマイズ （552 ページ）を参照してください。
- この機能に関連する問題についてのアラートを受信することを確認します。将来の URL カテゴリ セットの変更 （584 ページ）、ご使用の AsyncOS リリースのリリース ノート、およびアラート受信者の追加 （1277 ページ）を参照してください。

Talos インテリジェンスサービスへの接続について

URL レピュテーションとカテゴリは、クラウドベースの Talos インテリジェンスサービスによって提供されます。

電子メールゲートウェイは、ファイアウォール情報（1607ページ）でURLフィルタリングサービス用に指定したポートを使用して、Talos インテリジェンスサービスに直接または Web プロキシ経由で接続します。通信は HTTPS 経由で相互証明書認証を使用して行われます。証明書は自動的に更新されます（サービスアップデート （1253ページ）を参照）。必要な証明書の詳細については、URLフィルタリング機能の証明書 （548ページ）に示されている場所から入手できるリリース ノートを参照してください。

[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで HTTP または HTTPS プロキシを設定している場合は、電子メールゲートウェイが Talos インテリジェンスサービスとの通信時にそのプロキシ設定を使用します。プロキシ サーバの使用の詳細については、アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）を参照してください。

（注） 証明書はコンフィギュレーション ファイルには保存されません。

関連項目

- URL フィルタリング機能の証明書 （548 ページ）
- アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） （563 ページ）
- アラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） （564 ページ）

URL フィルタリング機能の証明書

AsyncOS は、URL フィルタリング機能に使用するクラウド サービスとの通信に必要な証明書を自動的に導入、更新するように設計されています。ただし、何らかの理由でシステムがこれらの証明書を更新できない場合には、ユーザのアクションを必要とするアラートがユーザに送信されます。

これらのアラート（[システム（System）] タイプ、[警告（Warning）] 重大度）を送信するように 電子メールゲートウェイが設定されていることを確認します。この説明については、アラート （1275 ページ） を参照してください。

無効な証明書に関するアラートを受信した場合は、Cisco TAC に連絡してください。Cisco TAC は必要な代替証明書を提供できます。代替証明書の使用手順については、Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 （567 ページ）を参照してください。

Web インタラクション トラッキング

Web インタラクション トラッキング機能は、書き換えられた URL をクリックしたエンド ユーザおよび各ユーザ クリックに関連するアクション（許可、ブロック、不明）に関する情報を提供します。この機能をイネーブルにすると、Web インタラクション トラッキング レポートを使用して、クリックされた悪意のある上位 URL、悪意のある URL をクリックした上位ユーザなどの情報を確認できます。Web インタラクション トラッキング レポートの詳細については、[Web インタラクション トラッキング（Web Interaction Tracking）] ページ（1039 ページ）を参照してください。

Web インタラクション トラッキング データは、クラウドベースの Cisco Aggregator Server によって提供されます。

関連項目

- Web インタラクション トラッキングの設定 （549 ページ）
- Cisco Aggregator Server への接続について （549 ページ）

Web インタラクション トラッキングの設定

要件に応じて、いずれかのグローバル設定ページで Web インタラクション トラッキングをイネーブルにできます。

- **アウトブレイク フィルタ**。アウトブレイク フィルタによって書き換えられた URL をクリックしたエンド ユーザを追跡します。アウトブレイク フィルタのグローバル設定の構成 （528 ページ）を参照してください。
- **URL フィルタリング**。ポリシーによって書き換えられた URL をクリックしたエンド ユーザを追跡します（コンテンツ フィルタおよびメッセージ フィルタを使用して）。URL フィルタリングを有効にする （545 ページ） を参照してください。

Cisco Aggregator Server への接続について

電子メール ゲートウェイは 30 分（構成不能）ごとに、ファイアウォール情報 （1607 ページ）でURL フィルタリング サービス用に指定したポートを使用して、Cisco Aggregator Server に直接または Web プロキシ経由で接続します。通信は HTTPS 経由で相互証明書認証を使用して行われます。証明書は自動的に更新されます（サービス アップデート （1253 ページ）を参照）。

[セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで HTTP または HTTPS プロキシが設定されている場合、 電子メール ゲートウェイは Cisco Aggregator Server との通信にこれらを使用します。プロキシ サーバの使用の詳細については、アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）を参照してください。

（注） 証明書はコンフィギュレーション ファイルには保存されません。

クラスタ構成での URL フィルタリング

- URL フィルタリングは、マシンごと、グループごと、またはクラスタごとに有効にできます。
- URL フィルタリングがマシンレベルで有効になっている場合、URL 許可リストおよび Web インタラクション トラッキングをマシン、グループ、またはクラスタレベルで設定できます。
- URL フィルタリングがグループレベルで有効になっている場合、URL 許可リストおよび Web インタラクション トラッキングをグループまたはクラスタレベルで設定する必要があります。
- URL フィルタリングがクラスタレベルで有効になっている場合、URL 許可リストおよび Web インタラクション トラッキングをクラスタレベルで設定する必要があります。
- メッセージ フィルタとコンテンツ フィルタのクラスタの標準ルールが適用されます。

URL フィルタリングの許可リストの作成

URL フィルタリング機能の設定時にグローバル許可リストを指定すると、その許可リストに含まれている URL は、レピュテーション、カテゴリ、アンチスパム、アウトブレイク フィルタリング、コンテンツフィルタリング、およびメッセージフィルタリングの対象として評価されません。ただし、これらの URL を含むメッセージは、アンチスパム スキャンおよびアウトブレイク フィルタによって通常どおりに評価されます。グローバル URL 許可リストを補足する目的で、コンテンツフィルタとメッセージフィルタの各 URL フィルタリング条件（ルール）およびアクションに URL 許可リストを指定することもできます。

アウトブレイク フィルタリングから許可リストの URL を分類するには通常、[メールポリシー：アウトブレイクフィルタ（Mail Policies: Outbreak Filters）] ページで設定した [ドメインのスキャンをバイパス（Bypass Domain Scanning）] オプションを使用します。URL フィルタリング用の URL 許可リストは、[ドメインのスキャンをバイパス（Bypass Domain Scanning）] に似ていますが、このオプションとは関係ありません。この機能の詳細については、URL 書き換えおよびドメインのバイパス （535 ページ）を参照してください。

この項で説明する URL フィルタリング許可リストと、IP レピュテーションスコアに基づく送信者レピュテーション フィルタリングに使用される許可リストは無関係です。

はじめる前に

Web インターフェイスで URL リストを作成する代わりに、リストをインポートすることを検討してください。URL リストのインポート （551 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [URL リスト（URL Lists）] を選択します。

ステップ 2 [URL リストの追加（Add URL List）] を選択するか、または編集するリストをクリックします。

グローバルに指定するすべての URL が許可リストとして 1 つのリストにまとめられていることを確認します。URL フィルタリングにはグローバル許可リストを 1 つだけ選択できます。

ステップ 3 URL リストを作成して送信します。

サポートされる URL 形式のリストを表示するには、[URL（URL s）] ボックスにセミコロン（:）を入力し、[送信（Submit）] をクリックします表示される [詳細...（more...）] リンクをクリックします。

各 URL、ドメイン、または IP アドレスを 1 行ずつ入力するか、またはコンマで区切って入力することができます。

ステップ 4 変更を保存します。

次のタスク

- URL リストをグローバル許可リストとして指定するには、URL フィルタリングを有効にする （545 ページ）を参照してください。
- URL リストを、コンテンツフィルタまたはメッセージフィルタの特定の条件（ルール）またはアクションのための許可リストとして指定するには、メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （553 ページ）およびコンテンツ フィルタのアクション （338 ページ）を参照してください。メッセージフィルタについてはURL カテゴリ アクション （259 ページ）およびURL カテゴリ ルール （215 ページ）も参照してください。

関連項目

- URL リストのインポート （551 ページ）

URL リストのインポート

URL リストをインポートし、URL フィルタリングの許可リストとして使用できます。

手順

ステップ 1 インポートするテキスト ファイルを作成します。

- 最初の行には URL リストの名前を指定する必要があります。
- 各 URL はそれぞれ別の行に入力する必要があります。

ステップ 2 ファイルをアプライアンスの `/configuration` ディレクトリにアップロードします。

ステップ 3 コマンドライン インターフェイスで `urllistconfig > new` コマンドを使用します。

サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ

アウトブレイク フィルタまたはポリシー（コンテンツ フィルタまたはメッセージ フィルタを使用して）で識別された悪意のある URL をエンドユーザがクリックすると、Cisco Web セキュリティ プロキシによってエンドユーザの Web ブラウザに通知が表示されます。この通知には、サイトに悪意があり、サイトへのアクセスがブロックされている旨が記載されています。

アウトブレイク フィルタを使用して書き換えられた URL をエンドユーザがクリックすると、通知ページが 10 秒間表示された後、クリック時の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトされます。

この通知ページの外観をカスタマイズして、企業ロゴ、連絡先情報など、組織のブランディングを表示できます。

（注） 通知ページをカスタマイズしない場合、エンドユーザにはシスコ ブランドの通知ページが表示されます。

はじめる前に

- URL フィルタリングをイネーブルにします。URL フィルタリングを有効にする（545 ページ）を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [ブロック ページ カスタマイズ（Block Page Customization）] を選択します。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 [ブロック ページ カスタマイズを有効にする（Enable Block Page customization）] チェックボックスをオンにして、次の詳細を入力します。

- 組織のロゴの URL。ロゴ イメージは、公にアクセス可能なサーバでホストすることが推奨されます。
- 組織名
- 組織の連絡先情報

ステップ 4 通知の言語を選択します。Web インターフェイスでサポートされるいずれかの言語を選択できます。

（注） エンドユーザのブラウザのデフォルト言語は、ここで選択した言語より優先されます。また、エンドユーザのブラウザのデフォルト言語が AsyncOS でサポートされていない場合は、ここで選択した言語で通知が表示されます。

ステップ 5 （任意）[ブロック ページ カスタマイズのプレビュー（Preview Block Page Customization）] をクリックして通知ページをプレビューします。

ステップ 6 変更を送信し、保存します。

次のステップ

次のいずれかの方法で URL の書き換えを設定します。

- アウトブレイク フィルタを使用します。URL のリダイレクト（518 ページ）を参照してください。
- コンテンツ フィルタまたはメッセージ フィルタを使用します。メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （553 ページ）を参照してください。

メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行

メッセージ本文またはメッセージの添付ファイルに含まれる URL リンクのレピュテーションまたはカテゴリに基づき、着信および発信電子メール ポリシーのメッセージ フィルタまたはコンテンツ フィルタを使用してアクションを実行できます。

アウトブレイク フィルタでは、マルウェアについてメッセージを評価するときにさまざまな要因が考慮されるため、URL レピュテーションだけではアグレッシブなメッセージ処理はトリガーされません。URL レピュテーションに基づいてフィルタを作成することをお勧めします。

たとえば、URL レピュテーション フィルタを使用して次のことを実行できます。

- （メッセージ本文に含まれる URL の場合のみ）ニュートラルまたは不明なレピュテーションの URL を書き換えて、クリック時の安全性評価のために Cisco Cloud Web Security プロキシ サービスにリダイレクトします。
- レピュテーションスコアが 信頼できないレピュテーションの範囲に該当する URL を含むメッセージをドロップします。

URL カテゴリ フィルタを使用して、次のことを実行できます。

- URL カテゴリをフィルタリングして、許容される Web の使用に関する組織のポリシーを適用します。たとえば、ユーザがオフィスでアダルト サイトやギャンブル サイトにアクセスできないようにする場合などです。
- 分類が可能となる十分な期間にわたって存在しない可能性がある、悪意のあるサイトからの保護を強化します。（メッセージ本文に含まれる URL の場合のみ）ユーザがリンクをクリックした時点で評価できるように、[未分類（Unclassified）] カテゴリの URL をすべて Cisco Cloud Web Security プロキシ サービスにリダイレクトできます。

関連項目

- URL 関連の条件(ルール）およびアクションの使用 （554 ページ）
- URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール（554 ページ）

- メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （555 ページ）
- リダイレクト URL：エンドユーザのエクスペリエンス （557 ページ）

URL 関連の条件(ルール）およびアクションの使用

目的	例	操作内容
メッセージ全体に対してアクションを実行する。	メッセージを削除または検疫する。	URL レピュテーションまたは URL カテゴリの条件またはルールを作成し、URL レピュテーションまたは URL カテゴリのアクション以外のアクションと組み合わせます。 例外：URL レピュテーション条件またはルールをバウンスアクションと組み合わせないでください。
（メッセージ本文の URl の場合のみ）メッセージに含まれる URL を変更またはその動作を変更します。	メッセージに含まれる URL をテキストに置換するか、URL をクリックできない状態にします。	URL レピュテーションまたは URL カテゴリのアクションのみを作成します。個別の URL フィルタリング条件は使用しないでください。

コンテンツ フィルタを使用するには、メール ポリシーにそのフィルタを指定する必要があります。

関連項目

- URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール （554 ページ）
- メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （555 ページ）

URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール

メッセージの本文および添付ファイルに含まれる URL のレピュテーションまたはカテゴリに基づいて、メッセージに対するアクションを実行できます。URL または URL の動作の変更以外のアクションを実行するには、**URL レピュテーション**または **URL カテゴリ**の条件を追加し、アクションを適用するレピュテーション スコアまたは URL カテゴリを選択します。

たとえば、[成人向け（Adult）] カテゴリの URL が含まれているすべてのメッセージに対して [ドロップする（最終アクション）（Drop (Final Action)）] アクションを適用するには、[成人向け（Adult）] カテゴリが選択されている [URL カテゴリ（URL Category）] タイプの条件を追加します。

カテゴリを指定しない場合、選択したアクションはすべてのメッセージに適用されます。

信頼できる URL、ニュートラルな URL、および信頼できない URL の URL レピュテーション スコア範囲が事前定義されているため、編集できません。ただし、代わりにカスタム範囲を指定できます。指定されたエンドポイントは、指定した範囲に含まれます。たとえば、-8 から -10 までのカスタム範囲を作成する場合、-8 と -10 はこの範囲に含まれます。レピュテーション スコアを判断できない URL には 「不明」 を使用します。

（注） ニュートラルな URL レピュテーションとは、URL は現在はクリーンであるが、攻撃に陥りやすいため、今後悪意のある URL に変化する可能性があることを示します。このような URL に対して、管理者はノンブロッキング ポリシー（クリック時の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトするなど）を作成できます

選択した URL 許可リストまたはグローバル URL 許可リストに含まれている URL は評価されません。

この条件と組み合わせるアクションは、メッセージに含まれる URL が、レピュテーション スコアまたは条件に指定されているカテゴリに一致する場合に実行されます。

メッセージに含まれる URL またはその動作を変更するには、URL レピュテーションまたは URL カテゴリのアクションのみを設定します。この目的のための別個の URL レピュテーションまたは URL カテゴリの条件またはルールは不要です。

（注） URL レピュテーションの条件をバウンス アクションと組み合わせないでください。

ヒント 特定の URL カテゴリを確認するには、未分類の URL と誤って分類された URL の報告（584 ページ）のリンクを参照してください。

関連項目

- URL フィルタリングの許可リストの作成 （550 ページ）
- コンテンツ フィルタ （325 ページ）

メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用

URL レピュテーションまたは URL カテゴリのアクションを使用し、URL のレピュテーションまたはカテゴリに基づいて、メッセージに含まれる URL またはその動作を変更します。

URL レピュテーションおよびURL カテゴリのアクションには、個別の条件は必要ありません。代わりに、URL レピュテーションまたはURL カテゴリのアクションで選択するレピュテーションまたはカテゴリに基づいて、選択したアクションが適用されます。

アクションは、そのアクションに指定された条件に一致する URL だけに適用されます。メッセージに含まれるその他の URL は変更されません。

カテゴリを指定しない場合、選択したアクションはすべてのメッセージに適用されます。

信頼できる URL、ニュートラルな URL、および信頼できない URL の URL レピュテーションスコア範囲は事前定義されているため、編集できません。ただし、代わりにカスタム範囲を指定できます。指定されたエンドポイントは、指定した範囲に含まれます。たとえば、-8 から -10 までのカスタム範囲を作成する場合、-8 と -10 はこの範囲に含まれます。レピュテーションスコアを判断できない URL には 「不明」を使用します。

（注） ニュートラルなURL レピュテーションとは、URL は現在はクリーンであるが、攻撃に陥りやすいため、今後悪意のある URL に変化する可能性があることを示します。このようなURL に対して、管理者はノンブロッキング ポリシー（クリック時の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトするなど）を作成できます

次の URL 関連のアクションは、メッセージ本文に含まれる URL のみに適用されます。

- URL を無効化して、クリックできないようにします。メッセージ受信者は、引き続きその URL を表示およびコピーできます。
- メッセージ受信者がリンクをクリックすると、トランザクションがクラウド内のCisco Web セキュリティ プロキシにルーティングされるように URL をリダイレクトします。このプロキシでは、悪意のあるサイトである場合はアクセスがブロックされます。

  例：フィッシング攻撃で使用される悪意のあるサイトは、分類が可能となる十分な期間にわたって存在しないことがよくあるため、[未分類（Uncategorized）] カテゴリに含まれるすべての URL を Cisco Cloud Web Security プロキシ サービスにリダイレクトするとします。

  リダイレクト URL：エンドユーザのエクスペリエンス （557 ページ）も参照してください。

  URL を別のプロキシにリダイレクトするには、次の箇条書き項目の例を参照してください。

（注） このリリースでは、Cisco Cloud Web Security プロキシ サービスには設定可能なオプションがありません。たとえば、調整する脅威スコアのしきい値や、脅威スコアに基づいて指定するアクションがありません。

- URL を任意のテキストで置き換えます。

  メッセージに示されるテキストに元の URL を含めるには、$URL 変数を使用します。

次に、例を示します。

- [違法ダウンロード（Illegal Downloads）] カテゴリのすべての URL を次のテキストに置き換えます。

  ```
  Message from your system administrator: A link to an illegal downloads web site has been removed from this message.
  ```

- 元の URL と次の警告を組み込みます。

  ```
  警告! The following URL may contain malware: $URL
  ```

  次のようになります。警告：次の URL にはマルウェアが含まれている可能性があります。http://example.com。

- カスタム プロキシまたは Web セキュリティ サービスにリダイレクトします。

  ```
  http://custom_proxy/$URL
  ```

  これは http://custom_proxy/http://example.com となります。

選択した URL 許可リストまたはグローバル URL 許可リストに含まれている URL のレピュテーションまたはカテゴリは評価されません。

URL の危険を取り除くか、URL を置き換える場合は、署名メッセージで URL を無視することを選択できます。

URL レピュテーションまたは URL カテゴリのアクションを URL レピュテーションまたは URL カテゴリの条件（またはルール）と組み合わせることは推奨されません。組み合わせる条件 (ルール）とアクションに異なるカテゴリが含まれている場合、一致することはありません。

ヒント 特定の URL カテゴリを確認するには、未分類の URL と誤って分類された URL の報告（584 ページ）のリンクを参照してください。

関連項目

- URL フィルタリングの許可リストの作成 （550 ページ）
- カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例 （487 ページ）
- コンテンツ フィルタ （325 ページ）
- URL レピュテーション ルール （214 ページ）
- URL カテゴリ ルール （215 ページ）

リダイレクト URL：エンドユーザのエクスペリエンス

Cisco Cloud Web Security プロキシ サービスの評価に基づいて、次の処理が行われます。

- サイトが安全である場合、ユーザはターゲット Web サイトに誘導され、リンクがリダイレクトされたことを認識しません。

- 悪意のあるサイトの場合、そのサイトは悪意のあるサイトであり、アクセスがブロックされたことを示す通知がユーザに対して表示されます。

  エンドユーザ通知ページの外観をカスタマイズして、企業ロゴ、連絡先情報など、組織のブランディングを表示できます。サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ （552 ページ）を参照してください。

- Cisco Cloud Web Security プロキシ サービスとの通信がタイムアウトになった場合、ユーザに対しターゲット Web サイトへのアクセスが許可されます。
- その他のエラーが発生した場合、ユーザに対して通知が表示されます。

関連項目

- メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （555 ページ）

URL フィルタリング用にスキャンできないメッセージの処理

次のシナリオでは、URL フィルタリング スキャンが失敗し、次のヘッダー *X-URL-LookUp-ScanningError* がメッセージに追加されます。

- URL レピュテーションとカテゴリを取得できない
- メッセージで短縮 URL を展開できない
- メッセージ本文や添付ファイル内の URL の数が最大 URL スキャンの制限を超えている

コンテンツ フィルタを追加、[その他のヘッダー（Other Header）] 条件に *X-URL-LookUp-ScanningError* ヘッダーを選択、およびメッセージで実行する適切な処置を設定できます。

コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出

‘URL Reputation’ コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージの URL を検出し、これらのメッセージに対して適切なアクションを実行します。

ETF の ‘URL Reputation’ コンテンツ フィルタは、以下のいずれかの方法で設定できます。

- 'URL Reputation' の条件と適切なアクションを使用する。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない。
- 'URL Reputation' の条件とアクションを使用する。

'URL Reputation' の条件とアクションを使用して悪意のある URL を検出するには、以下の手順を使用します。

（注）
- 'URL Reputation' の条件と任意の適切なアクションを使用するには、手順のステップ 11 ～ 20 は無視してください。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない場合は、手順のステップ 4 ～ 10 は無視してください。

始める前に

- 電子メールゲートウェイで URL フィルタリングが有効にされていることを確認します。URL フィルタリングを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）] > [URLフィルタリング（URL Filtering）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護 （543 ページ）を参照してください。
- 電子メールゲートウェイでアウトブレイクフィルタが有効にされていることを確認します。アウトブレイク フィルタを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）]>[アウトブレイクフィルタ（Outbreak Filters）] ページに移動します。詳細については、アウトブレイク フィルタ （513 ページ）を参照してください。
- 電子メールゲートウェイでスパム対策エンジンが有効にされていることを確認します。スパム対策エンジンを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）]>[スパム対策（Anti-Spam）] ページに移動します。詳細については、スパムおよびグレイメールの管理 （461 ページ）を参照してください。
- （任意）URL リストを作成します。作成するには、Web インターフェイスで [メールポリシー（Mail Polices）]>[URLリスト（URL Lists）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護 （543 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 7 悪意のある URL を検出する ETF ソースを選択します。

ステップ 8 （任意）電子メールゲートウェイで脅威を検出しない許可リストに登録されている URL のリストを選択します。

ステップ 9 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [アクションを追加（Add Action）] をクリックします。

ステップ 12 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 13 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 14 条件（ステップ 7）で選択した ETF ソースと同じ ETF ソースを選択したことを確認します。

ステップ 15 （任意）ステップ 8 で選択したものと同じ許可リストに登録されている URL のリストを選択します。

ステップ 16 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 17 メッセージの本文および件名および/またはメッセージの添付ファイルの URL に対して実行する必要なアクションを選択します。

（注） ステップ 16 で [（次に含まれるURLを確認）Check URLs within] オプションに [添付ファイル（Attachments）] を選択した場合、メッセージから添付ファイルを除去することのみが可能です。

ステップ 18 すべてのメッセージにアクションを実行するか、未署名のメッセージにアクションを実行するかを選択します。

ステップ 19 [OK] をクリックします。

ステップ 20 変更を送信し、保存します。

（注） Webベースのレピュテーションスコア（WBRS）と電子メールゲートウェイのETFに対してURL レピュテーション コンテンツ フィルタを設定している場合は、電子メールゲートウェイのパフォーマンスを向上するために、WBRS URL レピュテーション コンテンツ フィルタの順序を ETF URL レピュテーションフィルタの順序よりも高く設定することをお勧めします。

メッセージフィルタを使用した、メッセージの悪意のある URL の検出

例として、ETF エンジンを使用して悪意のあるメッセージの URL を検出し、URL を無効化するには、‘URL Reputation’ のメッセージ フィルタ ルール構文を使用します。

構文：

```
 defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
 <'URL_allowedlist'>,
<’message_attachments'> , <’message_body_subject’> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <’URL_allowedlist’> ,
<’Preserve_signed’>)}
```

引数の説明

- ‘url-external-threat-feeds’ は、URL レピュテーションのルールです。
- ‘etf_source1’ は、メッセージまたはメッセージの添付ファイルの悪意のある URL を検出するために使用される ETF ソースです。
- 「URL_allowedlist」は、URL 許可リストの名前です。URL の許可リストが存在しない場合は「""」と表示されます。
- 'message_attachments' は、メッセージの添付ファイルの悪意のある URL をチェックするために使用します。メッセージの添付ファイルの悪意のある URL を検出するには '1' の値を使用します。
- 'message_body_subject' は、メッセージ本文と件名の悪意のある URL をチェックするために使用します。メッセージの本文と件名の悪意のある URL を検出するには '1' の値を使用します。

（注） メッセージの本文、件名、添付ファイルの悪意のある URL を検出するには '1,1' の値を使用します。

- ‘url-etf-defang’ は、悪意のある URL を含むメッセージに対して実行できるアクションの 1 つです。

  以下の例は、悪意のある URL を含むメッセージに対して適用できる ETF ベースのアクションです。

  - url-etf-strip(['etf_source1'],"None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- 'Preserve_signed' は、'1' または '0' で表されます。'1' は、このアクションが未署名のメッセージのみに適用されることを示し、'0' はこのアクションがすべてのメッセージに適用されることを示します。

以下の例では、ETF エンジンによってメッセージの添付ファイルで悪意のある URL が検出された場合、添付ファイルが除去されます。

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

URL フィルタリング結果のモニタ

検出された悪意のある URL およびニュートラルな URL に関するデータを表示するには、[モニタ（Monitor）] > [URL フィルタ（URL Filtering）] を選択します。このページのデータの詳細については、[URL フィルタリング（URL Filtering）] ページ （1038 ページ）を参照してください。

メッセージ トラッキングの URL 詳細の表示

アウトブレイク フィルタおよび関連するコンテンツ フィルタによって取得された URL のメッセージ トラッキングの詳細を表示するには、以下のことが必要です。

- メッセージ トラッキングが有効になっている必要があります。
- アウトブレイク フィルタおよび/または、URL レピュテーションもしくは URL カテゴリに基づくコンテンツ フィルタが稼働している必要があります。
- アウトブレイク フィルタについては、URL 書き換えが有効になっている必要があります。URL 書き換えおよびドメインのバイパス （535 ページ）を参照してください。
- URL ロギングが有効になっている必要があります。URL のロギングと URL のメッセージ トラッキングの詳細の有効化 （529 ページ）を参照してください。

表示されるデータの詳細については、メッセージ トラッキングの詳細 （1122 ページ） を参照してください。

これらの潜在的な機密情報に対する管理ユーザのアクセスを管理するには、メッセージ トラッキングでの機密情報へのアクセスの制御 （1197 ページ）を参照してください。

URL フィルタリングのトラブルシューティング

関連項目

- ログの表示 （563 ページ）
- アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） （563 ページ）

- アラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） （564 ページ）
- Talos インテリジェンスサービスに接続できない （564 ページ）
- アラート：シスコ アグリゲータ サーバに接続できない（Unable to Connect to the Cisco Aggregator Server） （565 ページ）
- アラート：シスコ アグリゲータ サーバから Web インタラクション トラッキング情報を取得できない（Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server） （565 ページ）
- websecurityadvancedconfig コマンドの使用 （566 ページ）
- メッセージ トラッキング検索で指定のカテゴリのメッセージが見つからない （566 ページ）
- 悪意のある URL とマーケティング メッセージがアンチスパム フィルタまたはアウトブレイク フィルタでキャプチャされない （566 ページ）
- フィルタリングされたカテゴリの URL が正しく処理されない （566 ページ）
- エンドユーザが書き換え後の URL から悪意のあるサイトにアクセスする （567 ページ）
- Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 （567 ページ）

ログの表示

URL フィルタリング情報は、次のログに書き込まれます。

- メール ログ（mail_logs）。URL のスキャン結果に関する情報は（URL に応じてメッセージに対して実行されるアクション）、このログに書き込まれます。
- URL フィルタリング ログ（web_client）。URL ルックアップの試行時のエラー、タイムアウト、ネットワークの問題などに関する情報は、このログに書き込まれます。

ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。ログの詳細については、ログ （1391 ページ）を参照してください。

ユーザがメッセージに含まれているリダイレクト リンクをクリックしたときに発生する動作に関する情報は、ログには記録されません。

ログ内の「SDS」は、URL レピュテーションサービスを示します。「Beaker コネクタ」は Talos エンジンを指します。

アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate）

問題

登録クライアント証明書の取得中に発生したエラーに関する情報レベルのアラートを受信します。

ソリューション

この証明書は、Talos インテリジェンスサービス（URL レピュテーションと URL カテゴリを取得するため）および Cisco Aggregator Server（Web インタラクション トラッキング データを取

得するため）のクラウドベースのサービスに接続する必要があります。次のことを試してください。

1. ネットワークの問題（誤ったプロキシ設定やファイアウォールの問題など）が発生しているかどうかを確認します。
2. URL フィルタリング機能キーが有効であり、アクティブであることを確認します。
3. 問題が解決しない場合は、Cisco TAC にご連絡ください。

アラート：Beakerコネクタ：証明書が無効です（CertificateIsInvalid）

問題

無効な Beaker コネクタの証明書に関する重大なアラートを受信しました。

ソリューション

この証明書は、URL レピュテーションとカテゴリを取得する目的でクラウド内の Talos インテリジェンスサービスに接続する際に必要です。

証明書を取得して手動でインストールする場合は、Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 （567 ページ）を参照してください。

Talos インテリジェンスサービスに接続できない

問題

[セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] ページに、Talos インテリジェンスサービスへの接続の問題が継続的に示されます。

解決方法

- URL フィルタリングを有効にしているが変更をまだ確定していない場合は、変更を確定します。
- Talos インテリジェンスサービスとの接続に関する最新のアラートを確認します。最新アラートの表示（1279 ページ）を参照してください。該当する場合は、アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） （563 ページ）およびアラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） （564 ページ）を参照してください。
- [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] で指定されたプロキシを経由して接続している場合は、これが設定されており、正常に機能していることを確認します。
- 接続を妨げている可能性があるネットワークの問題が他にあるかどうかを確認します。
- URL フィルタリングログで、Talos クライアントへのタイムアウト要求に関連するエラーが示されている場合は、コマンドライン インターフェイスで websecuritydiagnostics コマンドおよび **websecurityadvancedconfig** コマンドを使用し、調査および変更を行います。
  - 応答時間が、設定されている URL ルックアップタイムアウト以上である場合は、URL ルックアップタイムアウトの値を適宜増やします。

- URL スキャナ、Cisco Web セキュリティサービス、または Talos クライアントとの通信でタイムアウト以外のエラーが発生しているかどうかを URL フィルタリングログで確認します。ログに「Talos client」と記録されている場合、これは Talos インテリジェンスサービスを示します。このようなログ メッセージを見つけた場合は、TACにご連絡ください。

アラート：シスコ アグリゲータ サーバに接続できない（Unable to Connect to the Cisco Aggregator Server）

問題

次の警告アラートを受信：Cisco Aggregator Server に接続できません。

ソリューション

次の手順を実行します。

1. 電子メールゲートウェイからサーバのホスト名を ping して、電子メールゲートウェイと Cisco Aggregator Server との接続を確認します。CLI で aggregatorconfig コマンドを使用して、Cisco Aggregator Server のホスト名を表示します。
2. [セキュリティサービス（Security Services）]>[サービスのアップデート（Service Updates）]で指定されたプロキシを経由して接続している場合は、これが設定されており、正常に機能していることを確認します。
3. 接続を妨げている可能性があるネットワークの問題が他にあるかどうかを確認します。
4. DNS サービスが実行されているかどうかを確認します。
5. 問題が解決しない場合は、Cisco TAC にご連絡ください。

アラート：シスコ アグリゲータ サーバから Web インタラクション トラッキング情報を取得できない（Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server）

問題

次の警告アラートを受信：Cisco Aggregator Server から Web インタラクション トラッキング情報を取得できません。

ソリューション

次の手順を実行します。

1. [セキュリティ サービス（Security Services）]>[サービスのアップデート（Service Updates）]で指定されたプロキシを経由して接続している場合は、これが設定されており、正常に機能していることを確認します。
2. 接続を妨げている可能性があるネットワークの問題が他にあるかどうかを確認します。
3. DNS サービスが実行されているかどうかを確認します。
4. 問題が解決しない場合は、Cisco TAC にご連絡ください。

websecurityadvancedconfig コマンドの使用

本書で明示的に説明する変更を除き、TAC からの指示を受けずに websecurityadvancedconfig コマンドを使用して変更を行わないでください。

メッセージトラッキング検索で指定のカテゴリのメッセージが見つからない

問題

特定のカテゴリの URL が含まれているメッセージが、そのカテゴリでの検索で見つかりませんでした。

ソリューション

予想されるメッセージが検索結果に表示されない （1126 ページ） を参照してください。

悪意のある URL とマーケティング メッセージがアンチスパム フィルタまたはアウトブレイク フィルタでキャプチャされない

問題

マーケティング リンクを含むメッセージと悪意のある URL が、アンチスパム フィルタまたはアウトブレイク フィルタによってキャプチャされません。

解決方法

- これは、Web サイトのレピュテーションとカテゴリは、アンチスパム フィルタとアウトブレイク フィルタがサイトについて判定するときに使用する多数の条件の 2 つに過ぎないために発生することがあります。アクション（URL の書き換え、URL のテキストでの置き換え、メッセージの隔離またはドロップなど）の実行に必要なしきい値を低くすることで、これらのフィルタの感度を上げることができます。詳細については、アウトブレイク フィルタ機能とメール ポリシー （531 ページ） および スパム対策ポリシーの定義 （481 ページ） を参照してください。あるいは、URL レピュテーション スコアに基づくコンテンツ フィルタまたはメッセージ フィルタを作成します。
- またこれは、電子メールゲートウェイが Talos インテリジェンスサービスに接続できない場合に発生することもあります。Talos インテリジェンスサービスに接続できない （564 ページ） を参照してください。

フィルタリングされたカテゴリの URL が正しく処理されない

問題

URL カテゴリに基づくコンテンツ フィルタまたはメッセージ フィルタで定義されているアクションは、適用されません。

解決方法

- トレース機能を使用してメッセージ処理パスを追跡します（トレース機能についてはトラブルシューティングに関する章で説明します）。
- これは、電子メールゲートウェイが Talos インテリジェンスサービスに接続できない場合に発生することがあります。Talos インテリジェンスサービスに接続できない （564 ページ）を参照してください。
- 接続に問題がない場合でも、URL を分類できないか、誤って分類することがあります。未分類の URL と誤って分類された URL の報告 （584 ページ）を参照してください。URL のカテゴリを判別するときにこのサイトを使用できます。

エンドユーザが書き換え後の URL から悪意のあるサイトにアクセスする

問題

悪意のある URL が Cisco Web セキュリティ プロキシにリダイレクトされましたが、エンドユーザがそのサイトにアクセスできます。

解決方法

これは次の場合に発生する可能性があります。

- サイトが悪意のあるサイトとして識別されていない。
- Cisco Web セキュリティ プロキシへの接続がタイムアウトした。このタイムアウトが発生することは非常にまれです。ネットワークの問題が原因で接続が妨げられていないことを確認します。

Talos インテリジェンスサービスとの通信に必要な証明書の手動設定

この手順は、 電子メールゲートウェイが Talos インテリジェンスサービスとの通信に必要な証明書を自動的に取得できない場合に使用します。

手順

ステップ 1 必須の証明書の取得

ステップ 2 [ネットワーク（Network）]>[証明書（Certificates）] を使用するか、またはコマンドライン インターフェイスで certconfig コマンドを使用して、証明書をアップロードします。

ステップ 3 コマンドライン インターフェイスで **websecurityconfig** コマンドを入力します。

ステップ 4 プロンプトに従って、Talos インテリジェンスサービス認証用のクライアント証明書を設定します。

URL カテゴリについて

関連項目

- URL カテゴリについて （568 ページ）
- URL のカテゴリの判別 （584 ページ）
- 未分類の URL と誤って分類された URL の報告 （584 ページ）
- 将来の URL カテゴリ セットの変更 （584 ページ）

URL カテゴリについて

これらの URL カテゴリは、AsyncOS の最近のリリースで Web セキュリティ アプライアンスに使用されているカテゴリと同じです。

URL カテゴリ	省略形	コード	説明	URL の例
アダルト（Adult）	adlt	1006	アダルト コンテンツを指しますが、ポルノだけではありません。アダルト向けのナイトクラブ（ストリップ クラブ、スワッピング クラブ、同伴サービス、ストリッパーなど）、セックスに関する全般情報（ポルノとは限らない）、性器ピアス、アダルト向けの製品やグリーティング カード、健康や疾病関連以外の性行為に関する情報なども含まれることがあります。	www.adultentertainmentexpo.com www.adultnetline.com
アドバタイズメント（Advertisements）	adv	1027	Web ページに表示されることの多いバナー広告やポップアップ広告。広告コンテンツを提供しているその他の広告関連 Web サイト。広告サービスおよび広告営業は、[事業および産業（Business and Industry）] カテゴリに分類されます。	www.adforce.com www.doubleclick.com

URL カテゴリ	省略形	コード	説明	URL の例
アルコール（Alcohol）	alc	1077	嗜好品としてのお酒、ビールやワインの醸造、カクテルのレシピ、リキュール販売、ワイナリー、ブドウ園、ビール工場、アルコール類の販売元など。アルコール中毒は[健康および栄養（Health and Nutrition）]カテゴリに分類されます。バーおよびレストランは[飲食（Dining and Drinking）]カテゴリに分類されます。	www.samueladams.com www.whisky.com
芸術（Arts）	art	1002	画廊および展示会、芸術家および芸術作品、写真、文学および書籍、舞台芸術および劇場、ミュージカル、バレエ、美術館、デザイン、建築。映画およびテレビは [エンターテイメント（Entertainment）] に分類されます。	www.moma.org www.nga.gov
占星術（Astrology）	astr	1074	占星術、ホロスコープ、占い、数霊術、霊能者による助言、タロット。	www.astro.com www.astrology.com
オークション（Auctions）	auct	1088	オンラインまたはオフラインのオークション、オークション会社、オークション案内広告など。	www.craigslist.com www.ebay.com

URL カテゴリ	省略形	コード	説明	URL の例
ビジネスおよび産業（Business and Industry）	busi	1019	マーケティング、商業、企業、ビジネス手法、労働力、人材、運輸、給与、セキュリティとベンチャーキャピタル、オフィス用品、産業機器（プロセス用機器）、機械と機械系、加熱装置、冷却装置、資材運搬機器、包装装置、製造、立体処理、金属製作、建築と建築物、旅客輸送、商業、工業デザイン、建築、建築資材、出荷と貨物（貨物取扱業務、トラック輸送、運送会社、トラック輸送業者、貨物ブローカと輸送ブローカ、優先サービス、荷高と貨物のマッチング、追跡とトレース、鉄道輸送、海上輸送、ロードフィーダ サービス、移動と保管）。	www.freightcenter.com www.staples.com
チャットおよびインスタントメッセージ（Chat and Instant Messaging）	chat	1040	Web ベースのインスタントメッセージングおよびチャット ルーム。	www.icq.com www.meebo.com
不正および盗用（Cheating and Plagiarism）	plag	1051	不正行為を助長し、学期末論文（盗用したもの）などの書物を販売したりします。	www.bestessays.com www.superiorpapers.com
児童虐待コンテンツ（Child Abuse Content）	cprn	1064	世界中の違法な児童性的虐待コンテンツ。	—
コンピュータセキュリティ（Computer Security）	csec	1065	企業ユーザおよび家庭ユーザ向けのセキュリティ製品およびセキュリティ サービス。	www.computersecurity.com www.symantec.com

URL カテゴリ	省略形	コード	説明	URL の例
コンピュータおよびインターネット（Computers and Internet）	comp	1003	コンピュータおよびソフトウェアに関する情報（ハードウェア、ソフトウェア、ソフトウェア サポートなど）、ソフトウェア エンジニア向けの情報、プログラミング、ネットワーク、Web サイト設計、Web およびインターネット全般、コンピュータ科学、コンピュータ グラフィック、クリップアートなど。フリーウェアとシェアウェアは、[フリーウェアおよびシェアウェア（Freeware and Shareware）] カテゴリに分類されます。	www.xml.com www.w3.org
出会い系（Dating）	date	1055	出会い系サイト、結婚紹介所など。	www.eharmony.com www.match.com
デジタル ポストカード（Digital Postcards）	card	1082	デジタルはがきおよび電子カードの送信。	www.all-yours.net www.delivr.net
飲食（Dining and Drinking）	food	1061	飲食店、レストラン、バー、居酒屋、パブ、レストラン ガイド、レストラン レビューなど。	www.hideawaybrewpub.com www.restaurantrow.com
ダイナミックおよびレジデンシャル（Dynamic and Residential）	dyn	1091	ブロードバンド リンクの IP アドレス。通常は、ホーム ネットワークへのアクセスを試みているユーザを指します。たとえば、ホーム コンピュータへのリモート セッションの場合などです。	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net

URL カテゴリ	省略形	コード	説明	URL の例
教育（Education）	edu	1001	教育関連の Web サイト。たとえば、学校、短大、大学、教材、教師用資料、技術訓練、職業訓練、オンライントレーニング、教育問題、教育政策、学資援助、学校助成金、規範、試験など。	www.education.com www.greatschools.org
エンターテイメント（Entertainment）	ent	1093	映画、音楽、バンド、テレビ、芸能人、ファンサイト、エンターテイメントニュース、芸能界のゴシップ、エンターテイメントの会場などに関する詳細や批評など。[芸術（Arts）] カテゴリとの違いを確認してください。	www.eonline.com www.ew.com
過激（Extreme）	extr	1075	性的暴力または犯罪性のあるもの、暴力および暴力的行為、悪趣味な写真や血まみれの写真（解剖写真など）、犯行現場、犯罪被害者、事故被害者の写真、過度にわいせつな文章や写真、衝撃的な内容の Web サイトなど。	www.car-accidents.com www.crime-scene-photos.com
ファッション（Fashion）	fash	1076	衣料、服飾、美容室、化粧品、アクセサリ、宝飾品、香水、身体改造に関連する図表や文章、タトゥー、ピアス、モデル事務所など。皮膚科関連製品は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。	www.fashion.net www.findabeautysalon.com
ファイル転送サービス（File Transfer Services）	fts	1071	ダウンロードサービスおよびホスティングによるファイル共有を主目的とするファイル転送サービス	www.rapidshare.com www.yousendit.com

URL カテゴリ	省略形	コード	説明	URL の例
フィルタリング回避（Filter Avoidance）	filt	1025	検出されない匿名の Web 利用を促進および支援する Web サイト。例：cgi、php、および glype を使用した匿名プロキシ サービス。	www.bypassschoolfilter.com www.filterbypass.com
金融（Finance）	fnnc	1015	会計実務、会計士、課税、税、銀行、保険、投資、国家経済、個人資産管理（各種保険、クレジット カード、個人退職金積立計画、遺産相続計画、ローン、住宅ローン）などの金融や財務関連のもの。株は[オンライン トレード（Online Trading）]に分類されます。	finance.yahoo.com www.bankofamerica.com
フリーウェアおよびシェアウェア（Freeware and Shareware）	free	1068	フリー ソフトウェアおよびシェアウェア ソフトウェアのダウンロードを提供します。	www.freewarehome.com www.shareware.com
ギャンブル（Gambling）	gamb	1049	カジノ、オンライン ギャンブル、ブックメーカー、オッズ、ギャンブルに関する助言、ギャンブルの対象となっているレース、スポーツ ブッキング、スポーツ ギャンブル、株式スプレッドベッティング サービス。ギャンブル中毒に関する Web サイトは、[健康および栄養（Health and Nutrition）] カテゴリに分類されます。国営宝くじは、[宝くじ（Lotteries）] カテゴリに分類されます。	www.888.com www.gambling.com

URL カテゴリ	省略形	コード	説明	URL の例
ゲーム（Games）	game	1007	さまざまなカードゲーム、ボードゲーム、ワードゲーム、ビデオ ゲーム、戦闘ゲーム、スポーツ ゲーム、ダウンロード型ゲーム、ゲーム批評、攻略本、コンピュータ ゲーム、インターネット ゲーム（ロールプレイング ゲームなど）。	www.games.com www.shockwave.com
政府および法律（Government and Law）	gov	1011	政府 Web サイト、外交関係、政府および選挙に関するニュースや情報、法律家、法律事務所、法律関連の出版物、法律関連の参考資料、裁判所、訴訟事件一覧表、法律関連の協会などの法律分野に関する情報、立法および判例、市民権問題、移民関連、特許、著作権、法執行制度および矯正制度に関する情報、犯罪報道、法的措置、犯罪統計、軍事（軍隊、軍事基地、軍組織）/テロ対策など。	www.usa.gov www.law.com
ハッキング（Hacking）	hack	1050	Web サイト、ソフトウェア、およびコンピュータのセキュリティを回避する方法に関する議論。	www.hackthissite.org www.gohacking.com
ヘイト スピーチ（Hate Speech）	hate	1016	社会集団、肌の色、宗教、性的指向、障がい、階級、民族、国籍、年齢、性別、性同一性を基に、憎悪、不寛容、差別を助長する Web サイト。人種差別を扇動するサイト、性差別、人種差別の神学、人種差別の音楽、ネオナチ組織、特定民族至上主義、ホロコースト否定論。	www.kkk.com www.nazi.org

URL カテゴリ	省略形	コード	説明	URL の例
健康および栄養（Health and Nutrition）	hlth	1009	健康管理、疾病および障がい、医療、病院、医師、医薬品、精神衛生、精神医学、薬理学、エクササイズおよびフィットネス、身体障がい、ビタミン剤およびサプリメント、健康にかかわる性行為（疾病および健康管理）、喫煙、飲酒、薬物使用、健康にかかわるギャンブル（疾病および健康管理）、食物全般、飲食、調理およびレシピ、食物と栄養、健康維持および食事療法、レシピや料理に関する Web サイトを含む料理全般、代替医療など。	www.health.com www.webmd.com
ユーモア（Humor）	lol	1079	ジョーク、スケッチ、コミック、その他のユーモラスなコンテンツ。不快感を与える可能性のあるアダルト ユーモアは [アダルト（Adult）] に分類されます。	www.humor.com www.jokes.com
違法行為（Illegal Activities）	ilac	1022	窃盗、不正行為、電話ネットワークへの不法アクセスなどの犯罪を助長するサイト、コンピュータ ウィルス、テロリズム、爆弾、無秩序、殺人や自殺を描写したものやその実行方法を記述した Web サイト。	www.ekran.no www.thedisease.net

URL カテゴリ	省略形	コード	説明	URL の例
違法ダウンロード（Illegal Downloads）	ildl	1084	著作権契約に違反してソフトウェア保護を回避するための、ソフトウェア、シリアル番号、キー生成ツールなどをダウンロードできる Web サイト。Torrent は [ピアファイル転送（Peer File Transfer）] に分類されます。	www.keygenguru.com www.zcrack.com
違法ドラッグ（Illegal Drugs）	drug	1047	気晴らしのためのドラッグ、ドラッグ摂取の道具、ドラッグの購入と製造に関する情報。	www.cocaine.org www.hightimes.com
インフラストラクチャおよびコンテンツ配信ネットワーク（Infrastructure and Content Delivery Networks）	infr	1018	コンテンツ配信インフラおよび動的に生成されるコンテンツ、セキュリティで保護されているか、または分類が困難なために細かく分類できない Web サイトなど。	www.akamai.net www.webstat.net
インターネット電話（Internet Telephony）	v oip	1067	インターネットを利用した電話サービス。	www.evaphone.com www.skype.com
求職（Job Search）	job	1004	職業に関する助言、履歴書の書き方、面接に関するスキル、就職斡旋サービス、求人データバンク、職業紹介所、人材派遣会社、雇用主の Web サイトなど。	www.careerbuilder.com www.monster.com
下着および水着（Lingerie and Swimsuits）	ling	1031	下着および水着。特にモデルが着用している Web サイト。	www.swimsuits.com www.victoriassecret.com
宝くじ（Lotteries）	lotr	1034	宝くじ、コンテストおよび国が運営する宝くじ。	www.calottery.com www.flalottery.com

URL カテゴリ	省略形	コード	説明	URL の例
携帯電話（Mobile Phones）	cell	1070	Short Message Services（SMS; ショート メッセージ サービス）、着信音などの携帯電話用ダウンロード サービス。携帯電話会社の Web サイトは、[ビジネスおよび産業（Business and Industry）] カテゴリに分類されます。	www.cbfsms.com www.zedge.net
自然（Nature）	natr	1013	天然資源、生態学および自然保護、森林、原生地、植物、草花、森林保護、森林、原生林および林業、森林管理（再生、保護、保全、伐採、森林状態、間伐、計画的火入れ）、農作業（農業、ガーデニング、園芸、造園、種まき、除草、灌漑、剪定、収穫）、環境汚染問題（大気質、有害廃棄物、汚染防止、リサイクル、廃棄物処理、水質、環境産業）、動物、ペット、家畜、動物学、生物学、植物学。	www.enature.com www.nature.org
ニュース（News）	news	1058	ニュース、ヘッドライン、新聞、テレビ局、雑誌、天気、スキー場の状態。	www.cnn.com news.bbc.co.uk
非政府組織（Non-Governmental Organizations）	ngo	1087	クラブ、圧力団体、コミュニティ、非営利組織および労働組合などの非政府組織。	www.panda.org www.unions.org
性的でないヌード（Non-Sexual Nudity）	nsn	1060	ヌーディズム、ヌード、自然主義、ヌーディスト キャンプ、芸術的ヌードなど。	www.artenuda.com www.naturistsociety.com

URL カテゴリ	省略形	コード	説明	URL の例
オンライン コミュニティ（Online Communities）	comm	1024	アフィニティ グループ、Special Interest Group（SIG; 同じ興味を持つ人々の集まり）、Web ニュースグループ、Web 掲示板など。[プロフェッショナルネットワーキング（Professional Networking）] カテゴリまたは[ソーシャルネットワーキング（Social Networking）] カテゴリに分類される Web サイトはここには含まれません。	www.igda.org www.ieee.org
オンライン ストレージおよびバックアップ（Online Storage and Backup）	osb	1066	バックアップ、共有、およびホスティングを目的とした、オフサイト ストレージおよびピアツーピア型ストレージ	www.adrive.com www.dropbox.com
オンライン トレード（Online Trading）	trad	1028	オンライン証券会社、ユーザがオンラインで株取引できる Web サイト、株式市場、株式、債券、投資信託会社、ブローカー、株式市場の分析と解説、株式審査、株価チャート、IPO、株式分割に関する情報。株式スプレッド ベッティング サービスは [ギャンブル（Gambling）] に分類されます。その他の金融サービスは、[財務（Finance）] に分類されます。	www.tdameritrade.com www.scottrade.com
業務用電子メール（Organizational Email）	pem	1085	Outlook Web Access（OWA）などで業務用のメールを利用する際に使用する Web サイト。	—

URL カテゴリ	省略形	コード	説明	URL の例
パーク ドメイン（Parked Domains）	park	1092	広告ネットワークの有料リスティング サービスを利用してそのドメインのトラフィックから収益を得ようとする Web サイト、またはドメイン名を販売して収益を得ようと考えている「不正占拠者」が所有する Web サイト。有料広告リンクを返す偽の検索サイトも含まれます。	www.domainzaar.com www.parked.com
ピア ファイル転送（Peer File Transfer）	p2p	1056	ピアツーピア型のファイル要求 Web サイト。ファイル転送自体のトラッキングは行いません。	www.bittorrent.com www.limewire.com
個人サイト（Personal Sites）	pers	1081	個人が運営している個人関連の Web サイト、個人用ホームページ サーバ、個人的コンテンツが公開されている Web サイト、特定のテーマがない個人ブログなど。	www.karymullis.com www.stallman.org
写真検索および画像（Photo Searches and Images）	img	1090	画像、写真、クリップ アートの保存と検索を促進します。	www.flickr.com www.photobucket.com
政治（Politics）	pol	1083	政治家、政党、政治、選挙、民主主義、投票などに関連するニュースや情報の Web サイト。	www.politics.com www.thisnation.com

URL カテゴリ	省略形	コード	説明	URL の例
ポルノ（Pornography）	porn	1054	性的表現が露骨な文章または画像。性的表現が露骨なアニメや漫画、性的表現が露骨な描写全般、フェチ志向の文章や画像、性的表現が露骨なチャットルーム、セックスシミュレータ、ストリップポーカー、アダルト映画、わいせつな芸術、性的表現が露骨な Web メールなど。	www.redtube.com www.youporn.com
プロフェッショナル ネットワーキング（Professional Networking）	pnet	1089	キャリア開発や専門性開発を目的としたソーシャルネットワーキング。[ソーシャルネットワーキング（Social Networking）] も参照してください。	www.linkedin.com www.europeanpwn.net
不動産（Real Estate）	rest	1045	不動産の検索に役立つ情報、事務所および商業区画、賃貸、アパート、戸建てなどの不動産物件一覧、住宅建築など。	www.realtor.com www.zillow.com
参照（Reference）	ref	1017	都道府県および市区町村の案内情報、地図、時刻、参照文献、辞書、図書館など	www.wikipedia.org www.yellowpages.com
宗教（Religion）	rel	1086	宗教に関するコンテンツ、宗教に関する情報、宗教団体。	www.religionfacts.com www.religioustolerance.org
SaaS および B2B（SaaS and B2B）	saas	1080	オンライン ビジネス サービス用 Web ポータル、オンライン会議など。	www.netsuite.com www.salesforce.com
子供向け（Safe for Kids）	kids	1057	幼児や児童向けに作成されているか、明示的に幼児や児童向けと認められている Web サイト。	kids.discovery.com www.nickjr.com

URL カテゴリ	省略形	コード	説明	URL の例
科学技術（Science and Technology）	sci	1012	科学技術（航空宇宙、電子工学、工学、数学など）、宇宙探査、気象学、地理学、環境、エネルギー（化石燃料、原子力、再生可能エネルギー）、通信（電話、電気通信）など。	www.physorg.com www.science.gov
検索エンジンおよびポータル（Search Engines and Portals）	srch	1020	検索エンジンなど、インターネット上の情報にアクセスするための起点となるサイト。	www.bing.com www.google.com
性教育（Sex Education）	sxed	1052	事実に基づいて性的情報を扱う Web サイト、性的健康、避妊、妊娠など	www.avert.org www.scarleteen.com
ショッピング（Shopping）	shop	1005	物々交換、オンライン購入、クーポン、無料提供、事務用品、オンライン カタログ、オンライン モールなど。	www.amazon.com www.shopping.com
ソーシャル ネットワーキング（Social Networking）	snet	1069	ソーシャル ネットワーキング関連。[プロフェッショナル ネットワーキング（Professional Networking）] も参照してください。	www.facebook.com www.twitter.com
社会科学（Social Science）	socs	1014	社会に関係する科学と歴史、考古学、文化人類学、カルチュラル スタディーズ、歴史学、言語学、地理学、哲学、心理学、女性学。	www.archaeology.org www.anthropology.net
社会および文化（Society and Culture）	scty	1010	家族および家族関係、民族性、社会組織、家系、高齢者、保育など。	www.childcare.gov www.familysearch.org

URL カテゴリ	省略形	コード	説明	URL の例
ソフトウェアアップデート（Software Updates）	swup	1053	ソフトウェア パッケージに対する更新プログラムを提供している Web サイト。	www.softwarepatch.com www.versiontracker.com
スポーツおよびレクリエーション（Sports and Recreation）	sprt	1008	すべてのプロ スポーツおよびアマチュア スポーツ、レクリエーション活動、釣り、ファンタジー スポーツ（ゲーム）、公園、遊園地、レジャープール、テーマ パーク、動物園、水族館、温泉施設など。	www.espn.com www.recreation.gov
ストリーミング オーディオ（Streaming Audio）	aud	1073	リアルタイム ストリーミング オーディオ コンテンツ（インターネット ラジオやオーディオ フィードなど）。	www.live-radio.net www.shoutcast.com
ストリーミング ビデオ（Streaming Video）	vid	1072	リアルタイム ストリーミング ビデオ（インターネット テレビ、Web キャスト、動画共有など）。	www.hulu.com www.youtube.com
タバコ（Tobacco）	tob	1078	愛煙家の Web サイト、タバコ製造会社、パイプ、喫煙製品（違法薬物吸引用でないもの）など。タバコ依存は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。	www.bat.com www.tobacco.org
乗り物（Transportation）	trns	1044	個人用の乗り物、自動車およびバイクに関する情報、新車、中古車、オートバイの購入、自動車愛好会、小型船舶、航空機、レジャー用自動車（RV）など。自動車レースおよびバイク レースは [スポーツおよびレクリエーション（Sports and Recreation）] に分類されます。	www.cars.com www.motorcycles.com

URL カテゴリ	省略形	コード	説明	URL の例
旅行（Travel）	trvl	1046	ビジネス旅行と個人旅行、旅行情報、トラベル リソース、旅行代理店、休暇利用のパック旅行、船旅、宿泊施設、交通手段、航空便の予約、航空運賃、レンタカー、別荘など。	www.expedia.com www.lonelyplanet.com
未分類（Unclassified）	—	—	シスコのデータベースに存在しない Web サイトは、レポートのために未分類として記録されます。誤入力された URL もこれに含まれます。	—
武器（Weapons）	weap	1036	一般的な武器の購入および使用に関する情報（銃販売店、銃オークション、銃の案内広告、銃の付属品、銃の展示会、銃の訓練など）、銃に関する全般情報、その他の武器や狩猟関連画像のサイトなども含まれる場合があります。政府の軍に関する Web サイトは、[政府および法律（Government and Law）] カテゴリに分類されます。	www.coldsteel.com www.gunbroker.com
Web ホスティング（Web Hosting）	whst	1037	Web サイトのホスティング、帯域幅サービスなど。	www.bluehost.com www.godaddy.com
Web ページ翻訳（Web Page Translation）	tran	1063	Web ページの翻訳。	babelfish.yahoo.com translate.google.com
Web メール（Web-Based Email）	メール アドレス	1038	Web メール サービス。個人が自分の会社の電子メール サービスを利用するための Web サイトは、[業務用電子メール（Organizational Email）] カテゴリに分類されます。	mail.yahoo.com www.hotmail.com

URL のカテゴリの判別

特定の URL のカテゴリを確認するには、未分類の URL と誤って分類された URL の報告 （584 ページ）に示されているサイトを参照してください。

未分類の URL と誤って分類された URL の報告

誤って分類された URL や、未分類だが分類する必要がある URL を報告するには、次のサイトにアクセスしてください。

https://talosintelligence.com/reputation_center/support

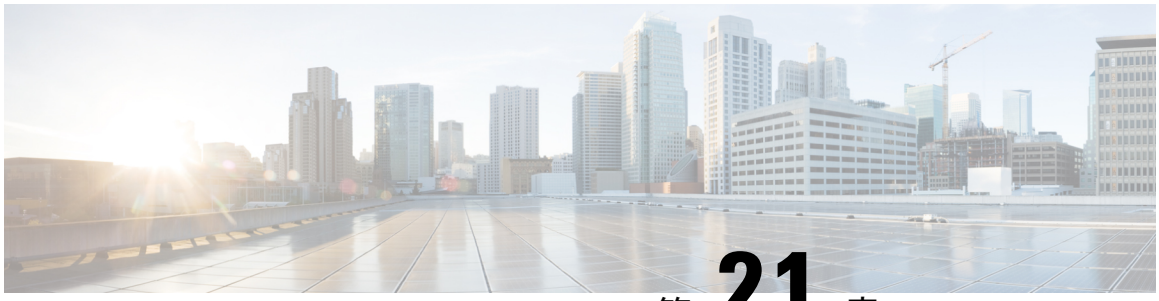
送信された URL のステータスを確認するには、このページの [送信したURLのステータス（Status on Submitted URLs）] タブをクリックします。

将来の URL カテゴリ セットの変更

新たな流行やテクノロジーの出現に伴い、URL カテゴリ セットが変更されることがまれにあります。たとえば、カテゴリの追加、削除、名前変更、別のカテゴリとの結合、2 つのカテゴリへの分割などです。このような変更は既存のフィルタの結果に影響することがあるので、変更が生じた場合は、 電子メールゲートウェイからアラート（[システム（System）] タイプ、[警告（Warning）] 重大度）が送信されます。このようなアラートを受信したら、コンテンツ フィルタとメッセージフィルタを評価し、場合によっては、更新されたカテゴリで機能するようにこれらのフィルタを更新する必要があります。既存のフィルタは自動的には変更されません。確実にアラートが届くようにするには、アラート受信者の追加 （1277 ページ）を参照してください。

次の変更では、カテゴリ セットの変更は不要であり、アラートは生成されません。

- 新たに分類されたサイトの定期的な分類。
- 誤って分類されたサイトの再分類



第 21 章

ファイル レピュテーション フィルタリングとファイル分析

この章は、次の項で構成されています。

- ファイル レピュテーション フィルタリングとファイル分析の概要 （585 ページ）
- ファイル レピュテーションと分析機能の設定 （590 ページ）
- ファイル レピュテーションおよびファイル分析のレポートとトラッキング （616ページ）
- ファイルの脅威判定の変更時のアクションの実行 （620 ページ）
- ファイル レピュテーションと分析のトラブルシューティング （620 ページ）

ファイル レピュテーション フィルタリングとファイル分析の概要

Advanced Malware Protection は、次によりゼロデイや電子メールの添付ファイル内のファイル ベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を常に評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

この機能は着信メッセージと発信メッセージ。

ファイル レピュテーションおよびファイル分析サービスでは、パブリック クラウドまたはプライベート クラウド（オンプレミス）を選択できます。

- プライベートクラウド ファイル レピュテーション サービスは Cisco AMP 仮想プライベートクラウドアプライアンスにより提供され、「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードで動作します。「オンプレミスのファイル レピュテーション サーバの設定 （592 ページ）」を参照してください。

- プライベートクラウド ファイル分析サービスは、オンプレミス Cisco AMP マルウェア分析アプライアンスにより提供されます。オンプレミスのファイル分析サーバの設定 （593 ページ） を参照してください。

ファイル脅威判定のアップデート

新しい情報の出現に伴い、脅威の判定は変化します。最初にファイルが不明または正常として評価されると、ファイルは受信者に対して解放されます。新しい情報が利用可能になるのに伴い脅威判定が変更されると、アラートが送信され、ファイルとその新しい判定が [AMP判定のアップデート（AMP Verdict Updates）] レポートに示されます。脅威の影響に対処する最初の作業として、侵入のきっかけとなったメッセージを調査できます。

判定が「悪意がある」から「正常」に変更されることもあります。

ファイル分析の後でファイルに動的なコンテンツが見つからない場合、判定は「低リスク」です。ファイル分析用にファイルは送信されず、メッセージは電子メールパイプラインを通過します。

アプライアンスが同じファイルの後続インスタンスを処理するときに、更新された結果がただちに適用されます。

判定アップデートのタイミングに関する情報は、ファイル基準のドキュメント（ファイル レピュテーションおよび分析サービスでサポートされるファイル （588ページ）を参照）に記載されています。

関連項目

- ファイル レピュテーションおよびファイル分析のレポートとトラッキング （616ページ）
- ファイルの脅威判定の変更時のアクションの実行 （620 ページ）

ファイル処理の概要

メッセージに対して最終アクションが実行されていない場合は、以前のスキャンエンジンの判定に関係なく、アンチウィルス スキャンの完了直後に、ファイル レピュテーションが評価され、ファイルが分析目的で送信されます。

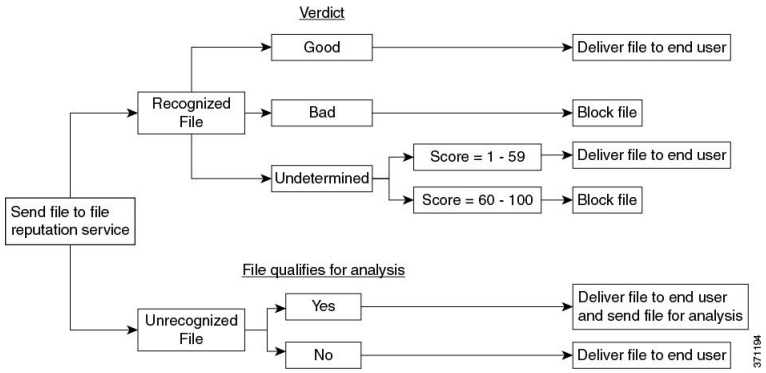
（注） メッセージの MIME ヘッダーの形式が正しくない場合、ファイル レピュテーション サービスはデフォルトで「スキャン不可」の判定を返します。アプライアンスは、このメッセージからも添付ファイルを抽出しようとします。アプライアンスが添付ファイルを抽出できない場合、判定は「スキャン不可」のままです。アプライアンスが添付ファイルを抽出できる場合は、添付ファイルのファイル レピュテーションが評価されます。添付ファイルが悪意のあるものである場合、判定は「スキャン不可」から「悪意のある」に変わります。

アプライアンスとファイル レピュテーション サービス間の通信は暗号化され、改ざんされないように保護されます。

ファイル レピュテーションの評価後：

- メッセージに添付ファイルが含まれていない場合、ファイル レピュテーション サービスは「スキップ」の判定を返します。
- ファイルがファイル レピュテーション サービスに対して既知であり、正常であると判断された場合、メッセージは引き続きワークキューに残ります。
- ファイル レピュテーション サービスからメッセージの添付ファイルについて悪意があるという判定が返されると、該当するメールポリシーで指定したアクションが、アプライアンスにより適用されます。
- レピュテーションサービスがファイルを認識しているが、決定的な判定を下すための十分な情報がない場合、レピュテーションサービスはファイルの特性（脅威のフィンガープリントや動作分析など）に基づき、レピュテーションスコアを戻します。このスコアが設定されたレピュテーションしきい値を満たすか、または超過した場合、マルウェアが含まれるファイルに関するメールポリシーで設定したアクションがアプライアンスによって適用されます。
- レピュテーションサービスにそのファイルに関する情報がなく、そのファイルが分析の基準を満たしていない場合（ファイル レピュテーションおよび分析サービスでサポートされるファイル （588 ページ）を参照）、そのファイルは正常と見なされ、メッセージはワークキューに残ります。
- ファイル分析サービスがイネーブルな状態で、レピュテーションサービスにはファイルに関する情報がなく、そのファイルが分析可能なファイルの条件を満たしている場合（ファイル レピュテーションおよび分析サービスでサポートされるファイル （588 ページ）を参照）、メッセージは隔離され（分析のために送信した添付ファイルがあるメッセージの隔離 （610 ページ）を参照）、ファイルは分析用に送信される可能性があります。添付ファイルが分析のために送信されるとき、またはファイルが分析のために送信されない場合にメッセージを隔離するようにアプライアンスを設定していない場合、そのメッセージはユーザに解放されます。
- オンプレミスのファイル分析での展開では、レピュテーション評価とファイル分析は同時に実行されます。レピュテーションサービスから判定が返された場合は、その判定が使用されます。これは、レピュテーションサービスにはさまざまなソースからの情報が含まれているためです。レピュテーションサービスがファイルを認識していない場合、ファイル分析の判定が使用されます。
- サーバとの接続がタイムアウトしたためにファイル レピュテーションの判定の情報が利用できない場合、そのファイルはスキャン不可と見なされ、設定されたアクションが適用されます。

図 *33* : パブリッククラウドファイル分析の展開における ***Advanced Malware Protection*** ワークフロー



ファイルが分析のために送信される場合：

- 分析用にクラウドに送信される場合、ファイルは HTTPS 経由で送信されます。
- 分析には通常、数分かかりますが、さらに時間がかかることもあります。
- ファイル分析で悪意があるとしてフラグ付けされたファイルが、レピュテーションサービスでは悪意があると識別されない場合があります。ファイル レピュテーションは、1 回のファイル分析結果でなく、さまざまな要因によって経時的に決定されます。
- オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用して分析されたファイルの結果は、ローカルにキャッシュされます。

判別のアップデートの詳細については、ファイル脅威判定のアップデート （586ページ）を参照してください。

ファイルレピュテーションおよび分析サービスでサポートされるファイル

レピュテーション サービスはほとんどのタイプのファイルを評価します。ファイル タイプの識別はファイル コンテンツによって行われ、ファイル拡張子には依存していません。

レピュテーションが不明な一部のファイルは、分析して脅威の特性を調べることができます。ファイル分析機能を設定すると、分析するファイルタイプを選択できます。新しいタイプを動的に追加できます。アップロード可能なファイルタイプのリストが変更された場合はアラートを受け取るので、追加されたファイル タイプを選択してアップロードできます。

ファイル レピュテーションおよび分析サービスでサポートされているファイルの詳細は、登録済みのお客様に限り提供しています。評価と分析の対象となるファイルについて詳しくは、『*File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*』を参照してください。このドキュメントは、https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html から入手できます。ファイル レピュテーションの評価基準、および分析用ファイルの送信基準はいつでも変更できます。

このドキュメントにアクセスするには、シスコの顧客アカウントとサポート契約が必要です。登録するには、https://tools.cisco.com/RPF/register/register.do にアクセスしてください。

Advanced Malware Protectionが対応しないファイルの配信をブロックするには、ポリシーを設定する必要があります。

（注） どこかのソースからすでに分析用にアップロードしたことのある（着信メールまたは発信メールのいずれかの）ファイルは、再度アップロードされません。このようなファイルの分析結果を表示するには、[ファイル分析（File Analysis）] レポート ページから SHA-256 を検索します。

関連項目

- ファイル レピュテーションと分析サービスの有効化と設定 （594 ページ）
- Advanced Malware Protection の問題に関するアラートの確実な受信 （615 ページ）
- アーカイブ ファイルまたは圧縮ファイルの処理 （589 ページ）

アーカイブ ファイルまたは圧縮ファイルの処理

ファイルが圧縮またはアーカイブされている場合：

- 圧縮ファイルまたはアーカイブ ファイルのレピュテーションが評価されます。

ファイル形式を含めて、検査対象となるアーカイブ ファイルや圧縮ファイルについて詳しくは、ファイル レピュテーションおよび分析サービスでサポートされるファイル （588 ページ）の情報を参照してください。

このシナリオでは、次のようになります。

- 抽出されたファイルのいずれかが悪意のあるファイルである場合、ファイル レピュテーション サービスは、その圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します。
- 圧縮/アーカイブ ファイルが悪意のあるファイルであり、抽出されたすべてのファイルが正常である場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します。
- 抽出されたファイルのいくつかの判定が「不明（unknown）」である場合、それらの抽出ファイルは、状況に応じて、分析のために送信されます（そのように設定されており、ファイル タイプがファイル分析でサポートされている場合）。
- 抽出されたファイルまたは添付ファイルのいくつかの判定が「低リスク（low risk）」である場合、そのファイルはファイル分析に送信されません。
- 圧縮/アーカイブ ファイルの圧縮解除中にファイルの抽出に失敗した場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「スキャン不可（Unscannable）」という判定を返します。ただし、抽出されたファイルの 1 つが悪意のあるファイルである場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します（「悪意がある

（Malicious）」という判定は「スキャン不可（Unscannable）」よりも順位が高くなります）。

- アーカイブまたは圧縮ファイルは、次のシナリオではスキャン不可として処理されます。
  - データ圧縮率が 20 を超える。
  - アーカイブ ファイルに 5 を超えるレベルのネストが含まれる。
  - アーカイブ ファイルに 200 を超える子ファイルが含まれる。
  - アーカイブ ファイルのサイズが 50 MB を超える。
  - アーカイブ ファイルがパスワードで保護されているか、または読み取り不可である。

（注） セキュア MIME タイプの抽出ファイル（テキストやプレーンテキストなど）のレピュテーションは、評価されません。

クラウドに送信される情報のプライバシー

- クラウド内のレピュテーション サービスには、ファイルを一意に識別する SHA のみが送信されます。ファイル自体は送信されません。
- クラウド内のファイル分析サービスを使用している場合、ファイルが分析の要件を満たしていれば、ファイル自体がクラウドに送信されます。
- 分析用にクラウドに送信されて「悪意がある」と判定されたすべてのファイルに関する情報は、レピュテーション データベースに追加されます。この情報は他のデータと共にレピュテーション スコアを決定するために使用されます。

  オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスで分析されたファイルの情報は、レピュテーションサービスと共有されません。

ファイル レピュテーションと分析機能の設定

- ファイル レピュテーションと分析サービスとの通信の要件 （591 ページ）
- オンプレミスのファイル レピュテーション サーバの設定 （592 ページ）
- オンプレミスのファイル分析サーバの設定 （593 ページ）
- ファイル レピュテーションと分析サービスの有効化と設定
- （パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定 （605 ページ）

- ファイル レピュテーション スキャンおよびファイル分析のメール ポリシーの設定 （607 ページ）
- 分析のために送信した添付ファイルがあるメッセージの隔離 （610 ページ）
- ファイル分析隔離の使用 （612 ページ）
- 中央集中型のファイル分析の隔離 （614 ページ）
- ファイル レピュテーションと分析の X ヘッダー （614 ページ）
- ドロップされたメッセージまたは添付ファイルに関する通知のエンドユーザへの送信 （614 ページ）
- 高度なマルウェア防御とクラスタ （615 ページ）
- Advanced Malware Protection の問題に関するアラートの確実な受信 （615 ページ）
- Advanced Malware Protection 機能の集約管理レポートの設定 （616 ページ）

ファイル レピュテーションと分析サービスとの通信の要件

- これらのサービスを使用する Web セキュリティアプライアンス E メール セキュリティ アプライアンスはすべて（オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用するよう設定されたファイル分析サービスは除く）、インターネット経由で直接サービスに接続できる必要があります。
- デフォルトでは、ファイル レピュテーションおよび分析サービス を参照してください。
- デフォルトでは、ファイル レピュテーションとクラウドベースの分析サービスとの通信は、デフォルト ゲートウェイに関連付けられているインターフェイス経由でルーティングされます。トラフィックを異なるインターフェイス経由でルーティングするには、[セキュリティ サービス（Security Services）]>[ファイル レピュテーションと分析（File Reputation and Analysis）] ページの [詳細設定（Advanced）] セクションで、各アドレスにスタティック ルートを作成します。
- 以下のファイアウォール ポートが開いている必要があります。

ファイアウォール ポート	説明	プロトコル	入力 / 出力	ホストネーム	アプライアンス インターフェイス
32137（デフォルト）または 443	ファイル レピュテーション取得のためのクラウド サービスへのアクセス。	TCP	発信	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクションの [クラウド サーバ プール（Cloud Server Pool）] パラメータで設定された名前。	管理（データ ポート経由でこのトラフィックをルーティングするようにスタティック ルートが設定されている場合を除く）。
443	ファイル分析のためのクラウド サービスへのアクセス。	TCP	発信	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクションで設定された名前。	

オンプレミスのファイル レピュテーション サーバの設定

プライベートクラウドのファイル分析サーバーとして Cisco AMP 仮想プライベート クラウド アプライアンスを使用する場合は、以下のように設定します。

- FireAMP プライベートクラウドのインストールおよび設定に関するガイドを含む、Cisco Advanced Malware Protection 仮想プライベート クラウド アプライアンスのドキュメントは、http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html から取得できます。

  この項目に記載されているタスクはこのドキュメントを参照して実行します。

  AMP 仮想プライベート クラウド アプライアンスのヘルプリンクを使用して、その他のドキュメントも入手できます。

- 「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードでの Cisco AMP 仮想プライベート クラウド アプライアンスを設定および構成します。

- Cisco AMP 仮想プライベート クラウド アプライアンスのソフトウェアバージョンが、Cisco E メール セキュリティ アプライアンスWeb セキュリティアプライアンス との統合を可能にするバージョン 2.2 であることを確認します。

- AMP 仮想プライベートクラウドの証明書およびキーをそのアプライアンスにダウンロードして、このEメール セキュリティ アプライアンスWeb セキュリティアプライアンス にアップロードします。
- E メール セキュリティ アプライアンスで信頼されているルート認証局がトンネル プロキシ サーバの証明書に署名していない場合は、[ルート証明書（Root Certificate）] オプションを使用して標準の検証をスキップします。

（注） オンプレミスのファイル レピュテーション サーバーを設定した後に、このE メール セキュリティ アプライアンスWeb セキュリティアプライアンス からこのサーバーへの接続を設定します。以下ファイル レピュテーションと分析サービスの有効化と設定 （594 ページ）のステップ 6 を参照してください。

オンプレミスのファイル分析サーバの設定

Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合：

- 『Cisco Secure Endpoint Malware Analytics Appliance Setup and Configuration Guide』および『Cisco Secure Endpoint Malware Analytics Appliance Administration Guide』を入手してください。Cisco Secure Endpoint マルウェア分析アプライアンスのドキュメントは、http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides%20-list.html から入手できます。

  この項目に記載されているタスクはこのドキュメントを参照して実行します。

  追加のドキュメントは、Cisco Secure Endpoint マルウェア分析アプライアンスのヘルプリンクから入手できます。

  Administration Guide で、次のすべての情報を検索します：他の Cisco アプライアンス（CSA、Cisco Sandbox API、ESA、およびEメールセキュリティアプライアンス Web セキュリティアプライアンス）との統合。

- Cisco Secure Endpoint マルウェア分析アプライアンスを設定および構成します。
- 必要に応じて、Cisco Secure Endpoint マルウェア分析アプライアンスのソフトウェアバージョンをバージョン 1.2.1 に更新します。これにより、Cisco E メール セキュリティ アプライアンスWeb セキュリティアプライアンス との統合がサポートされます。

  バージョン番号を確認し更新を実行する方法については、 AMP マルウェア分析のドキュメントを参照してください。

- アプライアンスがネットワーク上で相互に通信できることを確認します。Cisco E メール セキュリティ アプライアンスWeb セキュリティアプライアンス は、Cisco Secure Endpoint マルウェア分析アプライアンスの正常な（CLEAN）インターフェイスに接続可能である必要があります。

- 自己署名証明書を展開する場合は、E メール セキュリティ アプライアンス Web セキュリティアプライアンス で使用される Cisco Secure Endpoint マルウェア分析アプライアンスから自己署名 SSL 証明書を生成します。SSL 証明書とキーをダウンロードする手順については、Cisco Secure Endpoint マルウェア分析アプライアンスの管理者ガイドを参照してください。CN として Cisco Secure Endpoint マルウェア分析アプライアンスのホスト名がある証明書を生成してください。Cisco Secure Endpoint マルウェア分析アプライアンスからのデフォルトの証明書は機能しません。
- マルウェア分析アプライアンスへの E メール セキュリティ アプライアンス Web セキュリティアプライアンス の登録は、「ファイル レピュテーションと分析サービスの有効化と設定」で説明したように、ファイル分析の設定を送信したときに自動的に実行されます。ただし、同じ手順に記載されているように、登録をアクティブ化する必要があります。

ファイル レピュテーションと分析サービスの有効化と設定

始める前に

- ファイル レピュテーション サービスとファイル分析サービスの機能キーを取得して、このアプライアンスに転送します。
- ファイル レピュテーションと分析サービスとの通信の要件 （591 ページ）を満たします。
- [更新（Updates）] ページで 設定したアップデート サーバへの接続を確認します。
- Cisco AMP 仮想プライベート クラウド アプライアンスをプライベートクラウドのファイルレピュテーション サーバーとして使用する場合は、オンプレミスのファイル レピュテーション サーバの設定 （592 ページ） を参照してください。
- Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合は、オンプレミスのファイル分析サーバの設定 （593 ページ） を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ファイルレピュテーションと分析（File Reputation and Analysis）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [ファイル レピュテーション フィルタを有効にする（Enable File Reputation Filtering）] をクリックし、必要に応じて [ファイル分析を有効にする（Enable File Analysis）] をクリックします。

- [ファイル レピュテーション フィルタを有効にする（Enable File Reputation Filtering）] をオンにする場合、[ファイル レピュテーション サーバ（File Reputation Server）] セクションを設定するために（**ステップ 6**）、外部パブリック レピュテーション クラウド サーバの URL を入力するか、プライベート レピュテーション クラウド サーバの接続情報を入力する必要があります。

- 同様に、[ファイル分析を有効にする（Enable File Analysis）] をオンにする場合、[ファイル分析サーバの URL（File Analysis Server URL）] セクションを設定するために（**ステップ 7**）、外部クラウドサーバの URL を入力するか、プライベート分析クラウドの接続情報を入力する必要があります。

  （注） 新しいファイル タイプがアップグレード後に追加される場合がありますが、デフォルトでは有効になっていません。ファイル分析を有効にしており、新しいファイル タイプを分析に含めることが必要な場合には、それらを有効にする必要があります。

ステップ 4 ライセンス契約が表示された場合は、それに同意します。

ステップ 5 [ファイル分析（File Analysis）] セクションで、適切なファイル グループ（たとえば、「Microsoft Documents」）からファイル分析のために送信する必要があるファイル タイプを選択します。

サポートされるファイル タイプについては、次のドキュメントの説明を参照してください。
ファイル レピュテーションおよび分析サービスでサポートされるファイル （588 ページ）

（注） シスコは、ゼロデイの脅威を阻止するために、潜在的な悪意のあるファイル タイプを定期的にチェックしています。新しい脅威が特定されると、アップデータ サーバを介してファイル タイプなどの詳細がアプライアンスに送信されます。[その他の潜在的な悪意のあるファイル タイプ（Other potentially malicious file types）] オプションを選択して、この機能を有効にします。この機能を有効にすると、アプライアンスは選択したファイル タイプに加えて分析用のファイル タイプを送信します。

ステップ 6 [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] パネルを展開し、必要に応じて以下のオプションを調整します。

オプション	説明
クラウド ドメイン（Cloud Domain）	ファイル レピュテーション クエリーに使用するドメインの名前。

オプション	説明
ファイル レピュテーションサーバ（File Reputation Server）	パブリック レピュテーション クラウド サーバまたはプライベート レピュテーション クラウド クラウドのホスト名を選択します。 プライベート レピュテーション クラウドを選択する場合は、次の情報を入力します。 • [サーバー（Server）]：Cisco AMP 仮想プライベート クラウド アプライアンスのホスト名または IP アドレス。 • [公開キー（Public Key）]：このアプライアンスとプライベート クラウドアプライアンスとの間の暗号化通信に使用する公開キーを入力します。これは、プライベート クラウド サーバで使用されるキーと同じである必要があります。このアプライアンス上のキー ファイルの位置を指定して、[ファイルのアップロード（Upload File）] をクリックします。 （注） 事前にサーバからこのアプライアンスにキー ファイルをダウンロードしておく必要があります。
AMP for Endpoints コンソールの統合	お使いのアプライアンスを AMP for Endpoints コンソールと統合するには、[AMP for Endpointsコンソールでのアプライアンスの登録（Register the Appliance with Secure Endpoint AMP for Endpoints console）] をクリックします。詳細な手順については、AMP for Endpoints コンソールとアプライアンスの統合 （602 ページ）を参照してください。

オプション	説明
ファイル レピュテーション用の SSL 通信（SSL Communication for File Reputation）	デフォルト ポート（32137）ではなくポート 443 で通信するには、[SSL（ポート 443）の使用（Use SSL (Port 443)）] をオンにします。サーバーへの SSH アクセスを有効にする方法については、Cisco AMP 仮想プライベート クラウド アプライアンスのユーザーガイドを参照してください。 （注） ポート 32137 で SSL 通信を行うには、ファイアウォールでこのポートを開く必要があります。 このオプションを使用すると、ファイル レピュテーション サービスとの通信用にアップストリーム プロキシを設定できます。オンにする場合、[サーバ（Server）]、[ユーザ名（Username）]、[パスフレーズ（Passphrase）] に適切な情報を入力します。 [SSL（ポート 443）の使用（Use SSL (Port 443)）] がオンにされている場合、[証明書検証の緩和（Relax Certificate Validation）] もオンにすると、（トンネル プロキシ サーバの証明書に信頼できるルート認証局の署名がない場合に）標準の証明書検証をスキップできます。たとえば信頼できる内部トンネル プロキシ サーバの自己署名証明書を使用している場合は、このオプションをオンにします。 （注） [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] の [ファイルレピュテーションの SSL 通信（SSL Communication for File Reputation）] セクションで [SSL（ポート 443）の使用（Use SSL (Port 443)）] をオンにした場合、CLI コマンド certconfig > CERTAUTHORITY > CUSTOM、または Web インターフェイスの [ネットワーク（Network）] > [証明書（カスタム認証局）（Certificates (Custom Certificate Authorities)）] を使用して AMP オンプレミス レピュテーション サーバー CA 証明書をこのアプライアンスに追加する必要があります。この証明書をサーバから取得します（[設定（Configuration）] > [SSL] > [クラウド サーバ（Cloud server）] > [ダウンロード（download）]）。
ハートビート間隔（Heartbeat Interval）	レトロスペクティブなイベントを確認するための ping の送信頻度（分単位）。
クエリー タイムアウト（Query Timeout）	レピュテーション クエリーがタイムアウトになるまでの経過秒数。
処理のタイムアウト（Processing Timeout）	ファイルの処理がタイムアウトになるまでの経過秒数。

オプション	説明
ファイル レピュテーションクライアントID（File Reputation Client ID）	ファイル レピュテーション サーバ上のこのアプライアンスのクライアント ID（読み取り専用）
ファイルレトロスペクティブ（File Retrospective）	メッセージ受信者に配信されなかった、ドロップ、または隔離されたメッセージに関するレトロスペクティブ判定アラートを抑制するには、[レトロスペクティブ判定アラートの抑制（Suppress the retrospective verdict alerts）] をオンにします。

（注） このセクションの他の設定は、シスコのサポートのガイダンスなしに変更しないでください。

ステップ 7 ファイル分析にクラウド サービスを使用する場合は、[ファイル分析の詳細設定（Advanced Settings for File Analysis）] パネルを展開し、必要に応じて次のオプションを調整します。

オプション	説明
ファイル分析サーバの URL（File Analysis Server URL）	

オプション	説明
	外部クラウド サーバの名前（URL）、または [プライベート分析クラウド（Private analysis cloud）] を選択します。 外部クラウド サーバを指定する場合、アプライアンスに物理的に近いサーバを選択します。新たに使用可能になったサーバは、標準の更新プロセスを使用して、このリストに定期的に追加されます。 ファイル分析にオンプレミス Cisco Secure Endpoint マルウェア分析アプライアンスを使用するプライベート分析クラウドを選択し、次の情報を入力します。 • [TG サーバー（TG Servers）]：スタンドアロンの、またはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの IPv4 アドレスまたはホスト名を入力します。最大 7 つの Cisco Secure Endpoint マルウェア分析アプライアンスを追加できます。 （注） シリアル番号は、スタンドアロンまたはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの追加順序を示しています。アプライアンスの優先順位を示すものではありません。 （注） 1 つのインスタンスにスタンドアロン サーバとクラスタ サーバを追加することはできません。スタンドアロンまたはクラスタのいずれかにする必要があります。 1 つのインスタンスに追加できるスタンドアロン サーバは 1 台のみです。クラスタ モードの場合は 7 台までサーバを追加できますが、すべてのサーバが同じクラスタに属している必要があります。複数のクラスタを追加することはできません。 • [認証局（Certificate Authority）]：[シスコのデフォルト認証局を使用する（Use Cisco Default Certificate Authority）] または [アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択します。 [アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択する場合、[参照（Browse）] をクリックし、このアプライアンスとプライベート クラウド アプライアンスとの間の暗号化通信に使用する有効な証明書ファイルをアップロードします。これは、プライベート クラウド サーバで使用される証明書と同じである必要があります。 （注） ファイル分析のためにアプライアンスで Cisco Secure Endpoint マルウェア分析ポータルを設定している場合は、Cisco Secure Endpoint マルウェア分析ポータル（https://panacea.threatgrid.eu など）にアクセスし、ファイ

オプション	説明
	ル分析用に送信されたファイルを表示および追跡できます。Cisco Secure Endpoint マルウェア分析ポータルにアクセスする方法については、Cisco TAC にお問い合わせください。
プロキシの設定	ファイル分析用アップストリーム プロキシとして設定済みの、同じファイル レピュテーション トンネル プロキシを使用するには、[ファイル レピュテーション プロキシを使用する（Use File Reputation Proxy）] チェックボックスをオンにします。 別のアップストリーム プロキシを設定するには、[ファイル レピュテーション プロキシを使用する（Use File Reputation Proxy）] チェックボックスをオフにして、適切な [サーバ（Server）]、[ポート（Port）]、[ユーザ名（Username）]、および [パスフレーズ（Passphrase）] の情報を入力します。
ファイル分析クライアント ID（File Analysis Client ID）	ファイル分析サーバ上のこのアプライアンスのクライアント ID（読み取り専用）

ステップ 8 （任意）ファイル レピュテーション判定結果の値にキャッシュ有効期限を設定する場合は、[キャッシュ設定（Cache Settings）] パネルを展開します。

ステップ 9 許容されるファイル分析スコアの上限を設定するには、[しきい値の設定（Threshold Settings）] パネルを展開します。スコアがこのしきい値を超えた場合は、ファイルが感染していることを示しています。次のいずれかのオプションを選択します。

- クラウド サービスの値を使用（95）（Use value from Cloud Service (60)）
- [カスタム値の入力（Enter Custom Value）]：デフォルトでは 95 に設定されます。

ステップ 10 変更を送信し、保存します。

ステップ 11 オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用している場合は、Cisco Secure Endpoint マルウェア分析アプライアンスでこのアプライアンスのアカウントをアクティブ化します。

「ユーザー」アカウントをアクティブ化するための詳細な手順は、Cisco Secure Endpoint マルウェア分析のドキュメントで説明しています。

a) ページセクションの下部に表示されたファイル分析クライアント ID を書き留めます。ここにはアクティブ化する「ユーザー」が表示されます。
b) Cisco Secure Endpoint マルウェア分析アプライアンスにサインインします。
c) **[ようこそ…（Welcome…）] > [ユーザの管理（Manage Users）]** を選択し、[ユーザの詳細（User Details）] に移動します。
d) E メール セキュリティ アプライアンスWeb セキュリティアプライアンス のファイル分析クライアント ID に応じた「ユーザー」アカウントを指定します。

e) アプライアンスの「ユーザー」アカウントをアクティブにします。

AMP for Endpoints コンソールとアプライアンスの統合

お使いのアプライアンスを AMP for Endpoints コンソールと統合すると、 AMP for Endpoints コンソールで以下の操作を実行できます。

- シンプル カスタム検出リストを作成する。
- シンプル カスタム検出リストに新しい悪意のあるファイル SHA を追加する。
- アプリケーション許可リストを作成する。
- アプリケーション許可トリストに新しいファイル SHA を追加する。
- カスタム ポリシーを作成する。
- カスタムポリシーにシンプルカスタム検出リストおよびアプリケーション許可リストを関連付ける。
- カスタム グループを作成する。
- カスタム グループにカスタム ポリシーを関連付ける。
- 登録済みのアプライアンスをデフォルトのグループからカスタム グループに移動する。
- 特定のファイル SHA のファイル トラジェクトリの詳細を表示する。

アプライアンスを AMP for Endpoints コンソールと統合するには、アプライアンスをコンソールに登録する必要があります。

統合後に、ファイル SHA がファイル レピュテーション サーバに送信されると、ファイル SHA に対してファイル レピュテーション サーバーから得られた判定は、AMP for Endpoints コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。

ファイル SHA がすでにグローバルに悪意のあるものとしてマークされている場合、AMP for Endpoints コンソールで同じファイル SHA をブロックリストに追加すると、ファイルの判定結果は「悪意のあるもの」になります。

[高度なマルウェア防御（Advanced Malware Protection）] レポートページには、新しいセクション、[カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] があります。このセクションには、AMP for Endpoints コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出（Custom Detection）] として表示されます。ブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションに [シンプルカスタム検出（Simple Custom Detection）] として表示されます。レポートの [詳細（More Details）] セクションのリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。

始める前に

AMP for Endpoints コンソールの管理アクセス権を伴うユーザーアカウントがあることを確認してください。AMP for Endpoints コンソールのユーザーアカウントを作成する方法の詳細については、Cisco TAC にお問い合わせください。

（クラスタ化された設定の場合）クラスタ化された設定では、ログインしているアプライアンスを AMP for Endpoints コンソールにのみ登録できます。アプライアンスを AMP for Endpoints コンソールにスタンドアロンモードですでに登録している場合は、アプライアンスをクラスタに参加させる前に手動で登録を解除してください。

ファイル レピュテーション フィルタリングが有効化され、設定されていることを確認してください。ファイル レピュテーション フィルタリングを有効にして設定する方法については、「ファイル レピュテーションと分析サービスの有効化と設定」を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）]>[ファイル レピュテーションと分析（File Reputation and Analysis）] を選択します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 Web インターフェイスの [ファイルレピュテーションとファイル分析（File Reputation and File Analysis）] ページで、[ファイルレピュテーション（File Reputation）] の [詳細設定（Advanced Settings）] パネルにある [AMP for Endpointsへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックします。

[AMP for Endpointsへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックすると、 AMP for Endpoints コンソールのログインページが表示されます。

ステップ 4 ご使用のユーザーログイン情報で、AMP for Endpoints コンソールにログインします。

ステップ 5 AMP for Endpoints の認証ページで [許可（Allow）] をクリックして、アプライアンスを登録します。

[許可（Allow）] をクリックすると登録が完了し、アプライアンスの [ファイルレピュテーションと分析（File Reputation and Analysis）] ページにリダイレクトされます。[AMP for Endpoints コンソールの統合（Secure Endpoint AMP for Endpoints Console Integration）] フィールドに、お使いのアプライアンスの名前が表示されます。アプライアンス名は、 AMP for Endpoints のコンソールページでアプライアンス設定をカスタマイズする際に使用できます。

次のタスク

次の手順：

- AMP for Endpoints コンソールページの [アカウント（Accounts）] > [アプリケーション（Applications）] セクションに移動すると、アプライアンスが AMP for Endpoints コンソー

ルに登録されているかどうかを確認できます。アプライアンス名は、 AMP for Endpoints コンソールページの [アプリケーション（Applications）] セクションに表示されます。

- 登録されたアプライアンスは、デフォルトのポリシー（ネットワーク ポリシー）が関連付けられたデフォルトのグループ（監査グループ）に追加されます。デフォルトポリシーには、ブロックリストまたは許可リストに追加されるファイルSHAが含まれています。AMP for Endpoints の設定をお使いのアプライアンス用にカスタマイズして、ブロックリストまたは許可リストに追加されている独自のファイル SHA を追加する場合は、https://console.amp.cisco.com/docs で AMP for Endpoints のユーザーマニュアルを参照してください。
- [ファイルレピュテーション設定（File Reputation Settings）] ページの 「ファイルレピュテーションクライアント ID」の値と、 AMP for Endpoints コンソールポータルで登録したアプライアンスの「デバイス GUID」の値が同じであることを確認します。値が異なっていると、アプライアンスと AMP for Endpoints の統合が、マシンレベルまたはクラスタレベルで正しく機能しません。AMP for Endpoints機能を使用するには、アプライアンスの登録を解除して登録しなおす必要があります。
- アプライアンス接続を AMP for Endpoints コンソールから登録解除するには、アプライアンスの [ファイルレピュテーション（File Reputation）] セクションの [詳細設定（Advanced Settings）] で [登録解除（Deregister）] をクリックするか、または AMP for Endpoints のコンソールページ（https://console.amp.cisco.com/）にアクセスする必要があります。詳細については、https://console.amp.cisco.com/docs で AMP for Endpoints のユーザーマニュアルを参照してください。

（注） ファイル レピュテーション サーバーを別のデータセンターに変更すると、アプライアンスは AMP for Endpoints コンソールから自動的に登録解除されます。ファイル レピュテーション サーバーに選択された同じデータセンターを使用して、アプライアンスを AMP for Endpoints コンソールに再登録する必要があります。

（注） クラスタレベルでファイル レピュテーション サーバーを変更すると、ログインしているアプライアンスは自動的に AMP for Endpoints コンソールから登録解除されます。クラスタ内の他のすべてのマシンの登録を解除してください。ファイル レピュテーション サーバーに選択された同じデータセンターを使用して、すべてのアプライアンスを AMP for Endpoints コンソールに再登録する必要があります。

（注） 悪意のあるファイル SHA がクリーンと判定される場合、そのファイル SHA が AMP for Endpoints コンソールで許可リストに追加されていないか確認する必要があります。

重要：ファイル分析設定に必要な変更

新しいパブリック クラウド ファイル分析サービスを使用する場合は、次の説明を読み、データセンターの分離を維持するようにしてください。

- 既存のアプライアンスのグループ化情報は、新しいファイル分析サーバには保存されません。新しいファイル分析サーバでアプライアンスを再グループ化する必要があります。
- ファイル分析隔離エリアに隔離されたメッセージは、保存期間が経過するまで保存されます。隔離エリアでの保存期間が経過すると、メッセージはファイル分析隔離エリアから解放され、 AMP エンジンによって再スキャンされます。その後、ファイルは分析のために新しいファイル分析サーバにアップロードされますが、メッセージがもう一度ファイル分析隔離エリアに送信されることはありません。

詳細については、
http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html から Cisco AMP マルウェア分析のマニュアルを参照してください。

（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の任意のアプライアンスから分析用に送信されるファイルに関するクラウド内の分析結果の詳細が表示されるようにするには、すべてのアプライアンスを同じアプライアンスグループに結合する必要があります。

（注） マシン レベルでアプライアンスのグループを設定できます。アプライアンスのグループは、クラスタ レベルで設定することはできません。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ファイルレピュテーションと分析（File Reputation and Analysis）] を選択します。

ステップ 2 （電子メールゲートウェイでスマートライセンスが無効になっている場合に適用）[アプライアンスID/名前（Appliance ID/Name）] フィールドにグループ ID を手動で入力し、[今すぐグループ化（Group Now）] をクリックします。

または

（電子メールゲートウェイでスマートライセンスが有効になっている場合に適用）システムによりスマートアカウント ID がグループ ID として自動的に登録され、[アプライアンスグループID/名前（Appliance Group ID/Name）] フィールドに表示されます。

注：

- アプライアンスは 1 つのグループだけに属することができます。
- マシンはいつでもグループに追加できます。
- マシンレベルまたはクラスタレベルでアプライアンスのグループを設定できます。
- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすい ID を指定します。この ID は大文字と小文字が区別され、スペースを含めることはできません。
- アプライアンスグループ ID は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、ID はグループ内の以降のアプライアンスでは検証されません。
- アプライアンスグループ ID を更新すると、変更はすぐに有効になります。確定は必要ありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバーを使用するように設定する必要があります。
- スマートライセンシングが有効になっている場合、アプライアンスはスマートアカウント ID を使用してグループ化されます。

ステップ 3 [ファイル分析クラウド レポートのためのアプライアンスのグループ化（Appliance Grouping for File Analysis Cloud Reporting）] セクションで、ファイル分析グループ ID を入力します。

- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすい ID を指定します。
- この ID は大文字と小文字が区別され、スペースを含めることはできません。
- 指定した ID は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、ID は以降のグループ アプライアンスでは検証されません。
- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバを使用するように設定する必要があります。
- アプライアンスは 1 つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

ステップ 4 [今すぐグループ化（Group Now）] をクリックします。

分析グループ内のアプライアンスの確認

手順

ステップ 1 [セキュリティサービス（Security Services）]>[ファイル レピュテーションと分析（File Reputation and Analysis）] を選択します。

ステップ 2 [ファイル分析クラウド レポートの用のアプライアンスのグループ化（Appliance Grouping for File Analysis Cloud Reporting）] セクションで、**[アプライアンスの表示（View Appliances）]** をクリックします。

ステップ 3 特定のアプライアンスの**ファイル分析クライアント ID** を表示するには、以下の場所を参照します。

アプライアンス	ファイル分析クライアント ID の場所
E メール セキュリティ アプライアンス	[セキュリティ サービス（Security Services）] > [ファイル レピュテーションと分析（File Reputation and Analysis）] ページの [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション
Web セキュリティアプライアンス	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページの [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション
セキュリティ管理アプライアンス	[管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）]>[セキュリティアプライアンス（Security Appliances）] ページの下部

ファイル レピュテーション スキャンおよびファイル分析のメール ポリシーの設定

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] または [メール ポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] を選択します（どちらか該当するほう）。

ステップ 2 変更するメール ポリシーの [高度なマルウェア防御（Advanced Malware Protection）] カラム内のリンクをクリックします。

ステップ 3 オプションを選択します。

- オンプレミスの Cisco AMP Threat Grid アプライアンスがなく、機密上の理由などからクラウドにファイルを送信したくない場合は、[ファイル分析を有効にする（Enable File Analysis）] をオフにします。
- 添付ファイルがスキャン不可であると見なされる場合にアプライアンスが実行するアクションを選択します。アプライアンスが以下の理由でファイルをスキャンできない場合、添付ファイルはスキャン不能とみなされます。
  - **メッセージ エラー**：
    - パスワードで保護されたアーカイブまたは圧縮ファイル
    - RFC 違反のあるメッセージ。
    - 200 を超える子ファイルを含むメッセージ
    - 5 回以上ネストされた子ファイルを含むメッセージ
    - 抽出が失敗したメッセージ
  - **レート制限**：アプライアンスがファイルのアップロード制限に達したために、ファイル分析サーバによってスキャンされていないファイル。
  - **AMP サービスが使用不可**：
    - ファイル レピュテーション サービスが使用不可
    - ファイル分析サービスが使用不可
    - ファイル レピュテーション クエリーのタイムアウト
    - ファイル アップロード クエリーのタイムアウト
- AMP エンジンによってスキャンされないメッセージに対する、次のいずれかのメッセージ処理アクションを設定できます。
  - メッセージのドロップ
  - メッセージをそのまま配信
  - ポリシー隔離へのメッセージの送信
- メッセージを配信する場合は、次の追加の操作を選択します。
  - 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの amparchive ディレクトリに保管されます。事前設定された AMP アーカイブ（amparchive）ログ サブスクリプションが必要です。
  - メッセージの件名を変更して（例：[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]）エンドユーザに警告するかどうか。
  - 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。

- メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようするかどうか。[はい（Yes）] をクリックして、新しい受信者のアドレスを入力します。
- スキャンできないメッセージを代替の宛先ホストに送信するかどうか。[はい（Yes）] をクリックして代替 IP アドレスまたはホスト名を入力します。

- ポリシー隔離にメッセージを送信する場合は、次の追加の操作を選択します。
  - ドロップダウン リストからポリシー隔離を選択するかどうか。隔離のフラグが立てられている場合、メッセージは電子メール パイプラインの最後に到達すると隔離に置かれ、電子メール パイプラインの他のすべてのエンジンによってスキャンされます。
  - 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの amparchive ディレクトリに保管されます。事前設定された AMP アーカイブ（`amparchive`）ログ サブスクリプションが必要です。
  - メッセージの件名を変更して（例：[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]）エンドユーザに警告するかどうか。
  - 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。

- 添付ファイルが悪意のあるファイルであると見なされる場合に AsyncOS が実行する必要があるアクションを選択します。次のことを選択します。
  - メッセージを配信するか、またはドロップするか。
  - 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの amparchive ディレクトリに保管されます。事前設定された AMP アーカイブ（amparchive）ログ サブスクリプションが必要です。
  - マルウェア添付ファイルを削除した後で、メッセージを配信するかどうか。
  - メッセージの件名を変更して（例：[WARNING: MALWARE DETECTED IN ATTACHMENT(S)]）エンドユーザに警告するかどうか。
  - 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。
  - メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようするかどうか。[はい（Yes）] をクリックして、新しい受信者のアドレスを入力します。
  - 悪意のあるメッセージを代替の宛先ホストに送信するかどうか。[はい（Yes）] をクリックして代替 IP アドレスまたはホスト名を入力します。

- ファイル分析のために添付ファイルを送信する場合は、AsyncOS が実行すべきアクションを選択します次のことを選択します。
  - メッセージを配信するか、または隔離するか。

- 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの amparchive ディレクトリに保管されます。事前設定された AMP アーカイブ（amparchive）ログ サブスクリプションが必要です。
- メッセージの件名を変更して（例：[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]）エンドユーザに警告するかどうか。
- 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。
- メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようするかどうか。[はい（Yes）] をクリックして、新しい受信者のアドレスを入力します。
- ファイル分析のために送信されるメッセージを代替の宛先ホストに送信するかどうか。[はい（Yes）] をクリックして代替 IP アドレスまたはホスト名を入力します。

- （着信メール ポリシーの場合のみ）脅威の判定が「悪意がある」に変更された時点でエンドユーザに送信されるメッセージに対して実行する修復アクションを設定します。[メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）] をオンにして、以下のいずれかのアクションを選択します。
  - [電子メール アドレスに転送（Forward to an email address）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送する場合は、このオプションを選択します。
  - メッセージを削除します。悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。
  - [指定した電子メール アドレスに転送してメッセージを削除（Forward to an email address and delete the message）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送して、悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。

    （注） Office 365 サービスでは特定のフォルダからのメッセージの削除をサポートしていないため、それらのフォルダ（[削除済みアイテム（Deleted Items）] など）からメッセージを削除することはできません。

    重要 [メールボックス自動修復（Mailbox Auto Remediation）] の設定を確定する前に、メールボックスでのメッセージの修復 （709 ページ） を確認します。

ステップ 4 変更を送信し、保存します。

分析のために送信した添付ファイルがあるメッセージの隔離

分析用に送信されたファイルをただちにワークキューにリリースする代わりに、隔離するようにアプライアンスを設定できます。隔離されたメッセージとそれらの添付ファイルは、隔離か

らの解放時に脅威について再スキャンされます。ファイル分析結果がレピュテーション スキャナで使用できるようになった後にメッセージが解放された場合は、特定された脅威は再スキャン中に補足されます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] または [メール ポリシー（Mail Policies）] > [送信メールポリシー（Outgoing Mail Policies）] を選択します（どちらか該当するほう）。

ステップ 2 変更するメール ポリシーの [高度なマルウェア防御（Advanced Malware Protection）] カラム内のリンクをクリックします。

ステップ 3 [ファイル分析が保留中のメッセージ（Messages with File Analysis Pending）] セクションで、[メッセージに適用するアクション（Action Applied to Message）] ドロップダウンから [隔離（Quarantine）] を選択します。

隔離されたメッセージはファイル分析隔離エリアに保存されます。ファイル分析隔離の使用（612 ページ）を参照してください。

ステップ 4 （任意）[ファイル分析が保留中のメッセージ（Messages with File Analysis Pending）] セクションで、以下のオプションを選択します。

- 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの amparchive ディレクトリに保管されます。事前設定された AMP アーカイブ（amparchive）ログ サブスクリプションが必要です。
- メッセージの件名を変更して（例：[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]）エンドユーザに警告するかどうか。
- アプライアンスからの最終メッセージの配信中にファイル分析の判定が保留された場合、添付ファイルをドロップするかどうかを選択できます。デフォルトのオプションは [いいえ（No）] です。
- 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。

（注） ステップ 4 で説明した上記のアクションが適用されるのは、メッセージが隔離エリアからリリースされるときだけです。メッセージが隔離エリアに送信されるときには適用されません。

- 元のメッセージのアーカイブ。
- メッセージ件名の変更。
- カスタム ヘッダーの追加。

ステップ 5 変更を送信し、保存します。

次のタスク

関連項目

ファイル分析隔離の使用 （612 ページ）

ファイル分析隔離の使用

- ファイル分析隔離の設定の編集 （612 ページ）
- ファイル分析隔離領域内のメッセージの手動処理 （613 ページ）

ファイル分析隔離の設定の編集

手順

ステップ 1 [モニタ（Monitor）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2 [ファイル分析（File Analysis）] 隔離リンクをクリックします。

ステップ 3 保留期間を指定します。

デフォルトの 1 時間から変更することはお勧めしません。

ステップ 4 保留期間経過後に AsyncOS が実行する必要があるデフォルトのアクションを指定します。

ステップ 5 隔離ディスクに空き領域がなくなった場合でも、指定した保持期間前にその隔離内のメッセージが処理されなくなるように設定するには、[容量オーバーフロー時にメッセージにデフォルトのアクションを適用して容量を解放します（Free up space by applying default action on messages upon space overflow）] の選択を解除します。

ステップ 6 デフォルトのアクションとして [リリース（Release）] を選択する場合は、保留期間が経過する前にリリースされるメッセージに適用する追加のアクションを任意で指定できます。

オプション	情報
件名の変更（Modify Subject）	追加するテキストを入力し、そのテキストを元の件名の前と後ろのどちらに追加するかを選択します。 たとえば、受信者にマルウェアが添付されている可能性があるメッセージであることを警告します。 （注） 非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。

オプション	情報
[X-Header の追加（Add X-Header）]	X-Header にはメッセージに対して実行されたアクションを記録できます。この情報は、特定のメッセージが配信された理由についての照会を処理するときなどに役立ちます。 名前と値を入力します。 例： Name = Inappropriate-release-early Value = True
添付ファイルを除去（Strip Attachments）	添付ファイルを削除することで、メッセージに添付されたマルウェアから保護します。

ステップ 7 この隔離へのアクセスを付与するユーザを指定します。

ユーザー	情報
ローカル ユーザー（Local Users）	ローカルユーザのリストには、隔離にアクセスできるロールを持つユーザだけが含まれます。 すべての管理者は隔離に完全なアクセス権限を持つため、リストでは管理者が除外されます。
外部認証されたユーザ（Externally Authenticated Users）	外部認証を設定しておく必要があります。
カスタムユーザロール（Custom User Roles）	このオプションは、隔離へのアクセス権限を持つ少なくとも 1 つのカスタムユーザー ロールを作成している場合にのみ表示されます。

ステップ 8 変更を送信し、保存します。

ファイル分析隔離領域内のメッセージの手動処理

手順

ステップ 1 [モニタ（Monitor）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2 表のファイル分析隔離の行で、[メッセージ（Messages）] 列の青い番号をクリックします。

ステップ 3 要件に応じて、メッセージに以下のアクションを実行します。

- 削除（Delete）
- リリース

- 隔離からのリリースの遅延
- 指定した電子メール アドレスにメッセージのコピーを送信

中央集中型のファイル分析の隔離

中央集中型ファイル分析の隔離の詳細については、『*Cisco Email Security Appliance Guide*』の章「*Centralized Policy, Virus and Outbreak Quarantine*」を参照してください。

ファイル レピュテーションと分析の X ヘッダー

Xヘッダーを使用して、メッセージ処理ステップのアクションと結果でメッセージをマークできます。メール ポリシーでメッセージに X ヘッダーをタグ付けし、次にコンテンツ フィルタを使用して、これらのメッセージの処理オプションと最終アクションを選択します。

値では大文字/小文字が区別されます。

ヘッダー名	有効な値（大文字と小文字を区別）	説明
X-Amp-Result	正常（Clean） 悪意のある（Malicious） スキャン不可（Unscannable）	ファイル レピュテーション サービスにより処理されたメッセージに適用される判定。
X-Amp-Original-Verdict	file unknown verdict unknown	レピュテーションしきい値に基づく調整の前の判定。このヘッダーは、元の判定が有効な値のいずれかである場合にだけ存在します。
X-Amp-File-Uploaded	true false	メッセージに添付されたファイルが分析目的で送信されている場合、このヘッダーは「true」です。

ドロップされたメッセージまたは添付ファイルに関する通知のエンドユーザへの送信

疑わしい添付ファイルまたはその親メッセージが、ファイル レピュテーション スキャンに基づいてドロップされる場合に、エンドユーザに対して通知を送信するには、Xヘッダーまたはカスタム ヘッダーとコンテンツ フィルタを使用します。

高度なマルウェア防御とクラスタ

一元管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、高度なマルウェア防御とメール ポリシーをイネーブルにできます。

ライセンス キーはマシン レベルで追加する必要があります。

アプライアンス グループをクラスタ レベルで設定しないでください。

Advanced Malware Protection の問題に関するアラートの確実な受信

Advanced Malware Protectionに関連するアラートを送信するようにアプライアンスが設定されていることを確認します。

以下の場合にアラートを受信します。

アラートの説明	タイプ	重大度
オンプレミス（プライベートクラウド）の Cisco Secure Endpoint マルウェア分析アプライアンスへの接続をセットアップし、ファイル レピュテーションと分析サービスの有効化と設定 に説明されているようにアカウントをアクティブ化する必要があります。	マルウェア対策	警告
機能キーが期限切れになりました	（すべての機能に対する標準）	
ファイル レピュテーションまたはファイル分析サービスに到達できません。	ウイルス対策および AMP（Anti-Virus and AMP）	警告
クラウドサービスとの通信が確立されました。	ウイルス対策および AMP（Anti-Virus and AMP）	情報（Info）
レピュテーションおよび分析エンジンがウォッチドッグ サービスにより再起動される	ウイルス対策および AMP（Anti-Virus and AMP）	情報（Info）
ファイル レピュテーションの判定が変更されました。	ウイルス対策および AMP（Anti-Virus and AMP）	情報（Info）
分析用に送信できるファイル タイプが変更された。新しいファイル タイプのアップロードをイネーブルにできます。	ウイルス対策および AMP（Anti-Virus and AMP）	情報（Info）

アラートの説明	タイプ	重大度
一部のファイル タイプの分析が一時的に利用できません。	ウイルス対策および AMP（Anti-Virus and AMP）	警告
サポートされているすべてのファイル タイプの分析が一時停止後に復旧されます。	ウイルス対策および AMP（Anti-Virus and AMP）	情報（Info）
無効なファイル分析サービスキーです。このエラーを修正するには、Cisco TAC にファイル分析 ID の詳細を連絡する必要があります。	AMP	エラー（Error）

関連項目

- ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート （621 ページ）
- ファイルの脅威判定の変更時のアクションの実行 （620 ページ）

Advanced Malware Protection 機能の集約管理レポートの設定

セキュリティ管理アプライアンスでレポートを集約管理する場合は、管理アプライアンスに関するオンラインヘルプまたはユーザーガイドのEメールレポーティングのトピックの「Advanced Malware Protection」セクションで、重要な設定要件を確認してください。

ファイル レピュテーションおよびファイル分析のレポートとトラッキング

- SHA-256 ハッシュによるファイルの識別 （616 ページ）
- ファイル レピュテーションとファイル分析レポートのページ （617 ページ）
- その他のレポートでのファイル レピュテーション フィルタ データの表示 （619 ページ）
- メッセージ トラッキング機能と Advanced Malware Protection 機能について （619 ページ）

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数

のアプライアンスが同じファイルを処理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルはその SHA-256 値でリストされます（短縮形式

ファイル レピュテーションとファイル分析レポートのページ

レポート	説明
Advanced Malware Protection	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 判定が変更されたファイルについては、[AMP 判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。 圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。 [カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] セクションは、[カスタム検出（Custom Detection）] に分類される、AMP for Endpoints コンソールから受信したブロックリストに登録されたファイル SHA の割合を示しています。 AMP for Endpoints コンソールから取得されるブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで [シンプルカスタム検出（Simple Custom Detection）] として表示されます。 レポートの [詳細（More Details）] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。 [リスク低（Low Risk）] 判定の詳細をレポートの [AMP により渡された受信ファイル（Incoming Files Handed by AMP）] セクションに表示できます。

レポート	説明
Advanced Malware Protection [ファイル分析（File Analysis）]	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。 1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。 ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。 SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。 （注） 圧縮/アーカイブ ファイルから抽出したファイルが分析用に送信される場合は、それらの抽出ファイルの SHA 値だけが [ファイル分析（File Analysis）] レポートに含まれます。
Advanced Malware Protection レピュテーション	Advanced Malware Protection は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。 [AMP レピュテーション（AMP Reputation）] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、ファイル脅威判定のアップデート （586 ページ） を参照してください。 1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。 1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。 使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。

その他のレポートでのファイル レピュテーション フィルタ データの表示

該当する場合は、ファイル レピュテーションおよびファイル分析のデータを他のレポートでも使用できます。デフォルトでは、[]列は適用可能なレポートに表示されません。追加列を表示するには、テーブルの下の [列（Columns）] リンクをクリックします。

メッセージ トラッキング機能と Advanced Malware Protection 機能について

メッセージトラッキングでファイル脅威情報を検索するときには、以下の点に注意してください。

- ファイル レピュテーション サービスにより検出された悪意のあるファイルを検索するには、Web メッセージ トラッキングの [詳細設定（Advanced）] セクションの [メッセージ イベント（Message Event）] オプションで **[高度なマルウェア防御反応ポジティブ（Advanced Malware Protection Positive）]** を選択します。
- メッセージ トラッキングには、ファイル レピュテーション処理に関する情報と、トランザクションメッセージの処理時点で戻された元のファイル レピュテーション判定だけが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

  メッセージ トラッキングの詳細の [処理詳細（Action Details）] セクションには、以下の情報が表示されます。

  - メッセージの各添付ファイルの SHA-256
  - メッセージ全体での最終的な Advanced Malware Protection 判定。
  - マルウェアが検出された添付ファイル

- 判定の更新は [AMP 判定の更新（AMP Verdict Updates）] レポートだけに表示されます。メッセージ トラッキングの元の メッセージの詳細は、判定の変更によって更新されません。特定の添付ファイルが含まれているメッセージを確認するには、判定アップデート レポートで SHA-256 リンクをクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

  分析済みファイルのその他の情報は、クラウドまたはオンプレミスのファイル分析サーバーから入手できます。ファイルについて使用可能なすべてのファイル分析情報を確認するには、[レポート（Reporting）][モニタリング（Monitor）]>[ファイル分析（File Analysis）] を選択し、ファイルで検索する SHA-256 を入力します。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

分析目的で送信されたファイルの後続インスタンスがアプライアンスにより処理される場合、これらのインスタンスは、 メッセージ トラッキング検索結果に表示されます。

ファイルの脅威判定の変更時のアクションの実行

手順

ステップ 1 [AMP 判定の更新（AMP Verdict updates）] レポートを表示します。

ステップ 2 該当する SHA-256 リンクをクリックします。ファイルを含むメッセージの トラッキング データが表示されます。

ステップ 3 トラッキングデータを使用して、侵害された可能性があるユーザと、違反に関連するファイルの名前やなどの情報を特定します。

ステップ 4 ファイルの脅威の動作を詳細に把握するために、[ファイル分析（File Analysis）] レポートを検証して、この SHA-256 が分析用に送信されたかどうかを確認します。

次のタスク

関連項目

ファイル脅威判定のアップデート （586 ページ）

ファイル レピュテーションと分析のトラブルシューティング

- ログ ファイル （620 ページ）
- トレースの使用 （621 ページ）
- ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート （621 ページ）
- API キーのエラー（オンプレミスのファイル分析） （622 ページ）
- ファイルが予想どおりにアップロードされない （622 ページ）
- 分析のために送信できるファイル タイプに関するアラート （623 ページ）

ログ ファイル

ログの説明：

- `AMP` と `amp` は、ファイル レピュテーション サービスまたはエンジンを示しています。
- `Retrospective` は判定のアップデートを示しています。

- `VRT` と `sandboxing` はファイル分析サービスを示しています。

ファイル分析を含む Advanced Malware Protectionに関する情報は、または AMP エンジンのログ。

ファイル レピュテーション フィルタリングおよび分析のイベントは、 AMP エンジンログとメールログに記録されます。

ログ メッセージ「ファイル レピュテーション クエリーに対する受信応答（Response received for file reputation query）」の「アップロードアクション（upload action）」の値は以下のようになります。

- 1：送信。（1: SEND.）この場合、ファイル分析のためにファイルを送信する必要があります。
- 2：送信しない。（2: DON'T SEND.）この場合は、ファイル分析用にファイルを送信しません。
- 3：メタデータのみを送信。（3: SEND ONLY METADATA.）この場合、ファイル分析のためにファイル全体ではなく、メタデータのみを送信します。
- 0：アクションなし。（0: NO ACTION.）この場合、他のアクションは不要です。

メール ログの「処理（Disposition）」の値は、以下のようになります。

- 1：マルウェアが検出されない、または正常であると推測される（正常として処理）
- 2：正常
- 3：マルウェア

「Spyname」は脅威の名前です。

トレースの使用

ファイル レピュテーション フィルタおよび分析機能ではトレースは使用できません。代わりに、組織外のアカウントからテスト メッセージを送信します。

ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート

問題

ファイル レピュテーション サービスまたは分析サービスへの接続の失敗に関するアラートをいくつか受信した。（単一のアラートは一時的な問題のみを示していることがあります。）

ソリューション

- ファイル レピュテーションと分析サービスとの通信の要件 （591 ページ）に記載されている要件を満たしていることを確認します。

- アプライアンスとクラウドサービスとの通信を妨げている可能性があるネットワークの問題を確認します。
- [クエリー タイムアウト（Query Timeout）] の値を大きくします。

  [セキュリティサービス（Security Services）] [ファイルレピュテーションと分析（File Reputation and Analysis）] を選択します。の [詳細設定（Advanced settings）] エリアの [クエリタイムアウト（Query Timeout）] の値。

API キーのエラー（オンプレミスのファイル分析）

問題

ファイル分析レポートの詳細を表示しようとした場合や、分析用ファイルをアップロードするのに E メール セキュリティ アプライアンスWeb セキュリティアプライアンス が AMP マルウェア分析サーバーに接続できない場合、API キーのアラートを受信します。

解決方法

このエラーは、 AMP マルウェア分析サーバのホスト名を変更し、 AMP マルウェア分析サーバーの自己署名証明書を使用する場合に発生します。また、他の状況でも発生する可能性があります。この問題を解決するには、次の手順を実行します。

- 新しいホスト名がある AMP マルウェア分析アプライアンスから新しい証明書を生成します。
- E メール セキュリティ アプライアンスWeb セキュリティアプライアンス に新しい証明書をアップロードします。
- AMP マルウェア分析アプライアンスの API キーをリセットします。手順については、AMP マルウェア分析アプライアンスのオンラインヘルプを参照してください。

関連項目

- ファイル レピュテーションと分析サービスの有効化と設定

ファイルが予想どおりにアップロードされない

問題

ファイルが予想どおりに評価または分析されていません。アラートまたは明らかなエラーはありません。

解決方法

以下の点に注意してください。

- ファイルが他のアプライアンスによる分析用に送信されているために、すでにファイル分析サーバ、またはそのファイルを処理するアプライアンスのキャッシュに存在している可能性があります。

分析のために送信できるファイル タイプに関するアラート

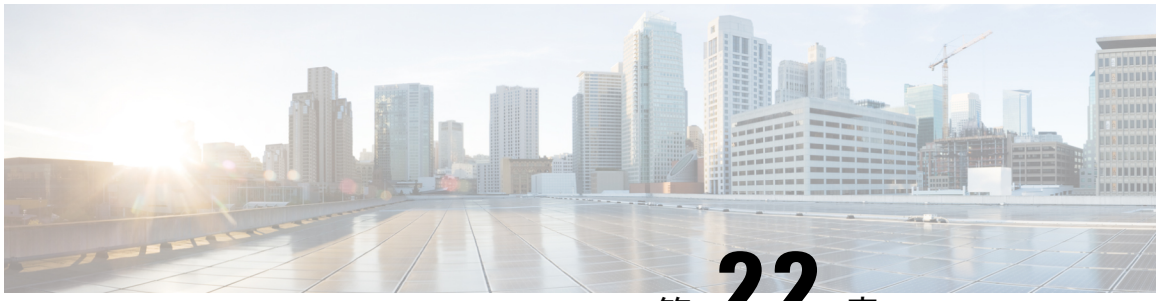
問題

ファイル分析のために送信できるファイルタイプに関する重大度情報のアラートを受け取れます。

解決方法

このアラートは、サポート対象のファイル タイプが変更された場合や、アプライアンスがサポート対象のファイルタイプを確認した場合に送信されます。これは、以下の場合に発生する可能性があります。

- 自分または別の管理者が分析用に選択されているファイル タイプを変更した。
- サポート対象のファイル タイプがクラウド サービスでの可用性に基づいて一時的に変更された。この場合、アプライアンスで選択されたファイルタイプのサポートは可能な限り迅速に復旧されます。どちらのプロセスも動的であり、ユーザによる操作は必要ありません。
- アプライアンスが再起動した（たとえば、AsyncOS のアップグレードの一環として）。



第 22 章

データ損失の防止

この章は、次の項で構成されています。

- データ消失防止の概要 （625 ページ）
- データ消失防止のシステム要件 （627 ページ）
- データ漏洩防止の設定方法 （627 ページ）
- データ消失防止の有効化（DLP） （628 ページ）
- データ損失防止のポリシー （629 ページ）
- メッセージ アクション （650 ページ）
- メッセージ トラッキングでの機密性の高い DLP データの表示 （657 ページ）
- DLP エンジンおよびコンテンツ照合分類子の更新について （657 ページ）
- DLP インシデントのメッセージとデータの使用 （659 ページ）
- トラブルシューティング データ消失防止 （660 ページ）

データ消失防止の概要

データ消失防止（DLP）機能により、ユーザが悪意を持ってまたは過失によって機密データを電子メールで送付しないように防止することで、組織の情報と知的財産を保護し、規制と組織のコンプライアンスを実施します。法または会社のポリシーに違反するデータがないか送信メッセージをスキャンするのに使われる DLP ポリシーを作成して、従業員が電子メールで送付できないデータの種類を定義します。

関連項目

- DLP スキャン プロセスの概要 （626 ページ）
- データ消失防止の動作 （626 ページ）

DLP スキャン プロセスの概要

	操作	詳細情報
1.	組織のユーザは組織外部の受信者に電子メールでメッセージを送信します。	電子メールゲートウェイ は、ネットワークに出入りするメッセージを処理します。 ネットワーク内の他のユーザに送信されるメッセージはスキャンされません。
2.	電子メールゲートウェイは DLP スキャン段階に到達する前に電子メールの「ワークキュー」の段階でメッセージを処理します。	DLP スキャン前プロセスは、たとえばメッセージにスパムやマルウェアが含まれていないことを確認します。 DLP 処理がワークキューのどこで発生するかを確認するには、電子メール パイプラインのフロー （67 ページ）のワークキュー フロー図を参照してください。
3.	電子メールゲートウェイは、DLPポリシーで特定した重要なコンテンツのメッセージ本文、ヘッダー、添付ファイルをスキャンします。	データ消失防止の動作 （626 ページ）を参照してください。
4.	重要なコンテンツが見つかった場合、電子メールゲートウェイはメッセージを隔離するか、廃棄または制限をかけて提供するなどのデータを保護するための処理を行います。 それ以外は、メッセージは電子メールゲートウェイのワークキューを通じて継続され、問題がない場合は、電子メールゲートウェイで受信者に配信されます。	実行されるアクションを定義します。メッセージ アクション （650 ページ）を参照してください。

データ消失防止の動作

組織内の誰かが組織外部の受信者にメッセージを送信する場合、電子メールゲートウェイは、定義したルールに基づいてどの発信メールポリシーをメッセージの送信者または受信者に適用するかを決定します。電子メールゲートウェイは、その発信メールポシリーに指定されたDLPポリシーを使用してメッセージの内容を評価します。

具体的には、電子メールゲートウェイは、単語、語句、社会保障番号などの定義済みのパターン、または適用される DLP ポリシーで機密内容として特定される正規表現と一致するテキストがないかメッセージ内容（ヘッダーと添付ファイルを含む）をスキャンします。

また、電子メールゲートウェイは、誤検出の一致を最小限に抑えるため拒否されたコンテキストを評価します。たとえば、クレジットカード番号のパターンに一致する番号は、有効期限、クレジット カード会社名（VISA、AMEX など）、または個人の名前や住所が伴っている場合のみ違反になります。

メッセージ内容が複数の DLP ポリシーに一致したら、指定された順序に基づいてリストの最初に一致した DLP ポリシーが適用されます。内容が違反であるかどうかを判断するために同じ基準を使用する複数の DLP ポリシーが発信メール ポリシーにある場合でも、すべてのポリシーは、1 つの内容スキャンの結果を使用します。

機密である可能性のある内容がメッセージに表示されると、電子メールゲートウェイは 0 ～ 100 間のリスク要因スコアを潜在的違反に割り当てます。このスコアは、メッセージに DLP 違反が含まれる確率を示します。

電子メールゲートウェイは、そのリスク要因スコアに定義した重大度レベル（クリティカルまたは低いなど）を割り当て、適切な DLP ポリシーでその重大度に指定したメッセージアクションを実行します。

データ消失防止のシステム要件

データ損失の防止は、D-Mode ライセンスを使用するアプライアンスを除き、サポートされるすべての C シリーズおよび X-Series アプライアンスでサポートされています。

データ漏洩防止の設定方法

次の手順を順番に実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	DLP 機能を有効にします。	データ消失防止の有効化（DLP）（628 ページ）
ステップ 2	違反が見つかったか疑いがあるメッセージに対して実行できるアクションを定義します。たとえば、そのようなメッセージを隔離できます。	メッセージ アクション（650 ページ）
ステップ 3	DLP ポリシーの作成について次を行います。 • 組織から電子メールで送信しないコンテンツを識別します。 • 各違反について実行するアクションを指定します。	方法を選択します。 • ウィザードを使用した DLP 防止の設定（630 ページ） • 事前定義されたテンプレートを使用した DLP ポリシーの作成（632 ページ）

	コマンドまたはアクション	目的
		• カスタム DLP ポリシーの作成（詳細） （633 ページ）
ステップ 4	コンテンツが 1 つ以上の DLP ポリシーに一致する可能性がある場合に、DLP 違反のメッセージの評価に使用する DLP ポリシーを指定する場合は、DLP ポリシーの順序を設定します。	違反との一致に対する Email DLP ポリシーの順序の調整 （648 ページ）
ステップ 5	DLP 違反をスキャンするメッセージの送信者と受信者グループごとに発信メール ポリシーを作成したことを確認します。	メール ポリシー（309 ページ）を参照してください さらに個々の DLP ポリシーの許可および制限されたメッセージ送信者と受信者を改善するには、DLP ポリシーのメッセージのフィルタリング （646 ページ）を参照してください。
ステップ 6	DLP ポリシーを発信メール ポリシーに割り付けることによって、どの DLP ポリシーをどの送信者と受信者に適用するかを指定します。	発信メール ポリシーとの DLP ポリシーの関連付け （649 ページ）
ステップ 7	ストレージの設定を構成し、機密 DLP 情報にアクセスします。	• メッセージ トラッキングでの機密性の高い DLP データの表示 （657 ページ） • メッセージ トラッキングでの機密情報へのアクセスの制御 （1197 ページ）

データ消失防止の有効化（DLP）

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 ライセンス契約書ページの下部にスクロールし、[承認（Accept）] をクリックしてライセンス契約に合意します。

（注） ライセンス契約に合意しない場合、DLP は 電子メールゲートウェイ上で有効になりません。

ステップ 4 [データ漏洩防止グローバル設定（Data Loss Prevention Global Settings）] の下の [データ漏洩防止を有効にする（Enable Data Loss Prevention）] を選択します。

ステップ 5 （推奨）現段階では、このページの他のオプションの選択を解除します。

これらの設定は、後でこの章で説明する手順に従って変更できます。

ステップ 6 変更を送信し、保存します。

次のタスク

データ漏洩防止の設定方法 （627 ページ） を参照してください。

関連項目

- メッセージ トラッキングでの機密性の高い DLP データの表示 （657 ページ）
- ウィザードを使用した DLP 防止の設定 （630 ページ）
- DLP エンジンおよびコンテンツ照合分類子の更新について （657 ページ）

データ損失防止のポリシー

関連項目

- DLP ポリシーの説明 （629 ページ）
- 定義済み DLP ポリシー テンプレート （630 ページ）
- ウィザードを使用した DLP 防止の設定 （630 ページ）
- 事前定義されたテンプレートを使用した DLP ポリシーの作成 （632 ページ）
- カスタム DLP ポリシーの作成（詳細） （633 ページ）
- コンテンツ照合分類子を使用した拒否されたコンテンツの定義について （635 ページ）
- DLP ポリシーのメッセージのフィルタリング （646 ページ）
- 違反の重大度の評価について （647 ページ）
- 違反との一致に対する Email DLP ポリシーの順序の調整 （648 ページ）
- デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け （649 ページ）
- DLP ポリシーの編集または削除に関する重要な情報 （650 ページ）

DLP ポリシーの説明

DLP ポリシーは次が含まれます。

- 発信メッセージが機密データが含んでいるかどうかを判断する一連の条件
- メッセージがそのようなデータを含んでいる場合に実行するアクション。

メッセージ コンテンツの評価方法を以下から指定します。

- 拒否された特定のコンテンツまたは情報のパターン。ポリシーによっては、識別番号を検索する正規表現の作成が必須の場合があります。コンテンツ照合分類子を使用した拒否されたコンテンツの定義について （635 ページ）を参照してください。
- メッセージフィルタリング用の特定の送信者および受信者のリスト。DLP ポリシーのメッセージのフィルタリング （646 ページ）を参照してください。
- メッセージ フィルタリング用の添付ファイルのタイプ一覧。DLP ポリシーのメッセージのフィルタリング （646 ページ）を参照してください。
- 発生するさまざまなアクションを許可する設定は違反の重大度に基づいています。違反の重大度の評価について （647 ページ）を参照してください。

発信メール ポリシーの DLP ポリシーをイネーブルにする場合に、各ポリシーを適用するメッセージ送信者と受信者を決定します。

定義済み DLP ポリシー テンプレート

DLP ポリシーの作成を簡素化するために、電子メールゲートウェイには、定義済みのポリシーテンプレートの大規模なコレクションが含まれます。

テンプレートのカテゴリには次が含まれます。

- **[規制コンプライアンス（Regulatory Compliance）]。**これらのテンプレートは、個人識別情報、クレジット情報、その他の保護または非公開情報を含む添付ファイル、メッセージを識別します。
- **[許可された使用（Acceptable Use）]。**これらのテンプレートは、組織の機密情報が含まれる制限された受信者または競合他社に送信されたメッセージを指定します。
- **[プライバシー保護（Privacy Protection）]。**金融口座、税金記録、国民 ID の識別番号を含むメッセージおよび添付ファイルを識別します。
- **[知的財産保護（Intellectual Property Protection）]。**これらのテンプレートは、よく使われるパブリッシングおよびデザイン ドキュメント ファイル タイプで、組織が保護する知的財産を含む可能性があるものを識別します。
- **[企業機密情報（Company Confidential）]。**これらのテンプレートは、会社の財務情報や近い将来の合併および買収に関する情報を含むドキュメントとメッセージを識別します。
- **[カスタム ポリシー（Custom Policy）]。**この「テンプレート」を使用すると、定義済みのコンテンツ照合分類子または組織が指定した違反識別基準を使用して、独自のポリシーを最初から作成できます。このオプションは高度であり、事前定義されたポリシー テンプレートではユーザのネットワーク環境の独自の要件を満たせない、まれな場合にのみ使用されることを想定しています。

これらのテンプレートの中にはカスタマイズが必要になものもあります。

ウィザードを使用した DLP 防止の設定

DLP 評価ウィザードでは一般的な DLP ポリシーを設定し、 電子メールゲートウェイのデフォルトの発信メールポリシーでイネーブルにします。

（注） DLP Assessment Wizard を使って追加された DLP ポリシーでは、検出された DLP 違反の重大度にかかわらず、メッセージはすべて配信されます。ウィザードを使用して作成されたポリシーを編集する必要があります。

はじめる前に

- 電子メールゲートウェイから既存の DLP ポリシーを削除します。DLP ポリシーが 電子メールゲートウェイに存在しない場合は、DLP評価ウィザードのみ使用することができます。
- クレジットカード番号、米国社会保障番号、および米国運転免許証番号以外の生徒識別番号またはアカウント番号を含むメッセージを検出する必要がある場合、それらの番号を特定する正規表現を作成します。詳細については、識別番号を識別する正規表現 （639ページ）を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[データ漏洩防止（Data Loss Prevention）] を選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 [有効（Enable）] を選択し、[DLP 評価ウィザードを使用して DLP を設定します。（DLP using the DLP Assessment Wizard）] チェックボックスをオンにします。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 ウィザードを完了します。

次の点を考慮してください。

- カリフォルニアでビジネスを営み、カリフォルニア州民のコンピュータ化した個人情報（PII）データを保有またはライセンスしている企業は、物理的な所在地にかかわらず、**米国の規則（カリフォルニア SB-1386）**に準拠することが必須となっています。この法律は、ウィザードのポリシーの選択肢の 1 つです。
- 自動生成されたスケジュール済み DLP インシデント サマリー レポートを受信する電子メール アドレスを入力しない場合、レポートは生成されません。
- 設定を確認し、変更を加える手順まで戻った場合は、再度このレビュー ページに至るまで、残りの手順を進める必要があります。以前に入力した設定は、すべて残っています。
- ウィザードを完了すると、デフォルトの送信メール ポリシーで DLP ポリシーがイネーブルな [送信メール ポリシー（Outgoing Mail Policies）] ページが表示されます。DLP ポリシー設定の要約が、ページの上部に表示されます。

ステップ 6 変更を保存します。

次のタスク

- （任意）これらの DLP ポリシーを編集し、追加ポリシーを作成し、メッセージの全体的な処理を変更するか、または重大度レベルの設定を変更するには、[メールポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。詳細については、事前定義されたテンプレートを使用した DLP ポリシーの作成 （632 ページ）、カスタム DLP ポリシーの作成（詳細） （633 ページ）、および重大度スケールの調整（648 ページ）を参照してください。
- （任意）他の発信メール ポリシーのある既存の DLP ポリシーをイネーブルにするには、発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て （650 ページ）を参照してください。

関連項目

- 事前定義されたテンプレートを使用した DLP ポリシーの作成 （632 ページ）
- カスタム DLP ポリシーの作成（詳細） （633 ページ）

事前定義されたテンプレートを使用した DLP ポリシーの作成

手順

ステップ 1 **[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）]** を選択します。

ステップ 2 [DLP ポリシーの追加（Add DLP Policy）] をクリックします。

ステップ 3 カテゴリ名をクリックし、使用可能な DLP ポリシー テンプレートの一覧を表示します。

（注） 各テンプレートの説明を表示するには、[ポリシーの説明を表示（Display Policy Descriptions）] をクリックします。

ステップ 4 使用する DLP ポリシー テンプレートの [追加（Add）] をクリックします。

ステップ 5 （任意）テンプレートの定義済みの名前と説明を変更します。

ステップ 6 ポリシーで、1つ以上のコンテンツ照合分類子のカスタマイズが要求または推奨される場合は、組織の識別番号付けシステムのパターンを定義するための正規表現と、使用される識別番号に関連する、または通常は関連付けられている単語や語句のリストを入力します。

詳細については、次を参照してください。

コンテンツ照合分類子を使用した拒否されたコンテンツの定義について （635ページ）および識別番号を識別する正規表現 （639 ページ）。

（注） 定義済みのテンプレートに基づいたポリシーのコンテンツの分類子は追加または削除できません。

ステップ 7 （任意）特定の受信者、送信者、添付ファイルの種類、または以前に追加されたメッセージタグを持つメッセージにのみ DLP ポリシーを適用します。

詳細については、DLP ポリシーのメッセージのフィルタリング（646 ページ）を参照してください。

改行やカンマで、複数のエントリを分離できます。

ステップ 8 [重大度設定（Severity Settings）] の項で、以下を行います。

- 違反の重大度レベルごとに実行するアクションを選択します。詳細については、違反の重大度の評価について （647 ページ）を参照してください。
- （任意）ポリシーに対して違反の重大度基準を調整する場合は、[スケールの編集（Edit Scale）] をクリックします。詳細については、重大度スケールの調整 （648 ページ）を参照してください。

ステップ 9 変更を送信し、保存します。

次のタスク

関連項目

- ウィザードを使用した DLP 防止の設定 （630 ページ）
- カスタム DLP ポリシーの作成（詳細） （633 ページ）

カスタム DLP ポリシーの作成（詳細）

（注） カスタム ポリシーの作成は非常に複雑です。定義済み DLP ポリシー テンプレートが組織のニーズを満たさない場合のみ、カスタム ポリシーを作成します。

Custom Policy テンプレートを使用して、カスタム DLP ポリシーを最初から作成し、定義されたコンテンツ照合分類子またはカスタム分類子をポリシーに追加できます。

ポリシーの定義によって、コンテンツが 1 つの分類子またはすべての分類子に一致した場合に、カスタム ポリシーは DLP 違反を返すことができます。

はじめる前に

推奨：コンテンツ違反を識別する基準を定義します。カスタム DLP ポリシーに対するコンテンツ照合分類子の作成 （637ページ）を参照してください。次の手順の中で、これらの基準を定義することもできます。

手順

ステップ 1 **[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）]** を選択します。

ステップ 2 [DLP ポリシーの追加（Add DLP Policy）] をクリックします。

ステップ 3 [カスタムポリシー（Custom Policy）] をクリックします。

ステップ 4 Custom Policy テンプレートの [追加（Add）] をクリックします。

ステップ 5 ポリシーの名前と説明を入力します。

ステップ 6 DLP 違反を構成するコンテンツとコンテキストを特定します。

a) コンテンツ照合分類子を選択します。

b) [追加（Add）] をクリックします。

- [分類子を作成（Create a Classifier）] を選択した場合、カスタム DLP ポリシーに対するコンテンツ照合分類子の作成 （637 ページ）を参照してください。
- それ以外の場合は、選択された分類子がテーブルに追加されます。

c) （任意）ポリシーに追加分類子を追加します。

たとえば、別の分類子を追加し、[NOT] を選択して、既知の誤検出である可能性の高い一致を削除できます。

d) 複数の分類子を追加した場合、テーブル見出しのオプションを選択し、インスタンスを違反としてカウントするために分類子の**一部**または**すべて**を一致させるかどうかを指定します。

ステップ 7 （任意）特定の受信者、送信者、添付ファイルの種類、または以前に追加されたメッセージタグを持つメッセージにのみ DLP ポリシーを適用します。

詳細については、DLP ポリシーのメッセージのフィルタリング （646 ページ）を参照してください。

改行やカンマで、複数のエントリを分離できます。

ステップ 8 [重大度設定（Severity Settings）] の項で、以下を行います。

- 違反の重大度レベルごとに実行するアクションを選択します。詳細については、違反の重大度の評価について （647 ページ）を参照してください。
- （任意）ポリシーに対して違反の重大度基準を調整する場合は、[スケールの編集（Edit Scale）] をクリックします。詳細については、重大度スケールの調整 （648 ページ）を参照してください。

ステップ 9 変更を送信し、保存します。

次のタスク

関連項目

- ウィザードを使用した DLP 防止の設定 （630 ページ）
- 事前定義されたテンプレートを使用した DLP ポリシーの作成 （632 ページ）

コンテンツ照合分類子を使用した拒否されたコンテンツの定義について

コンテンツ一致分類子は、電子メールで送信できないコンテンツと、任意選択でそのコンテンツがデータ消失防止違反と見なされるために発生する必要があるコンテキストを定義します。

患者識別番号が組織から電子メールで送信されることを回避する必要があるとします。

これらの番号を電子メールゲートウェイに認識させるために、1つ以上の正規表現を使用して組織の記録番号付けシステムのパターンを指定する必要があります。補足情報として記録番号を伴うかもしれない単語およびフレーズのリストを追加できます。分類子が発信メッセージ内に番号パターンを検出すると、補足情報を検索し、そのパターンが識別番号か、また、ランダムな番号の文字列でないかを確認します。コンテキストと一致する情報を含むことにより、誤検出の一致が減少します。

この例では、HIPAA および HITECH テンプレートを使用する DLP ポリシーを作成します。このテンプレートには、患者識別番号コンテンツ照合分類子という患者識別番号を検出するようにカスタマイズ可能な分類子が含まれます。パターン 123-CL456789 の番号を検出するには、分類子の正規表現 [0-9]{3}\-[A-Z]{2}[0-9]{6} を入力します。関連フレーズとして「Patient ID」と入力します。ポリシーの作成を完了し、発信メールポリシーでイネーブルにします。変更を送信し、保存します。フレーズ「患者 ID」が番号パターンの近くに設定された発信メッセージからポリシーが番号パターンを検出した場合、DLP ポリシーは DLP 違反を返します。

DLP ポリシーでのコンテンツ照合分類子の使用方法について

定義済み DLP ポリシーテンプレートの多くは、コンテンツ照合分類子が含まれます。これらの分類子の一部は、組織のデータに使用されるパターンを識別するためにカスタマイズする必要があります。

カスタム DLP ポリシーを作成すると、事前定義された分類子を選択するか、独自の分類子を作成できます。

関連項目

- コンテンツ照合分類子の例 （635 ページ）
- カスタム DLP ポリシーに対するコンテンツ照合分類子の作成 （637 ページ）
- 機密情報を特定する分類子検出ルール（カスタム DLP ポリシーのみ） （639 ページ）
- 識別番号を識別する正規表現 （639 ページ）
- 機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用 （641 ページ）
- 疑わしい違反のリスク要因の判別子 （643 ページ）
- カスタム コンテンツ分類子が使用されるポリシーの表示 （646 ページ）

コンテンツ照合分類子の例

次の例は、分類子がメッセージの内容を照合する方法を示します。

- クレジット カード番号 （636 ページ）

- 米国社会保障番号 （636 ページ）
- 米国銀行協会銀行支店コード （636 ページ）
- 運転免許証番号（米国） （636 ページ）
- 国内のプロバイダー ID（米国） （637 ページ）
- 学歴（英語） （637 ページ）
- 財務諸表（英語） （637 ページ）

クレジット カード番号

DLP ポリシーテンプレートのいくつかは、クレジット カード番号分類子を含みます。クレジットカード番号はそれ自体、数と句読点のパターン、発行者固有のプレフィックス、最後のチェックデジットなどさまざまな制約があります。この分類子で一致するには、有効期限やカード発行者の名前など、追加の補足情報が必要です。これで false positive の数が減ります。

例：

- `378734493671000`（補足情報がないため一致せず）
- `378734493671000 VISA`（一致）
- `378734493671000 exp: 12/2019`（一致）

米国社会保障番号

米国社会保障番号分類子では、正しい形式の番号と誕生日や名前および「SSN」という文字列などの補足データが必要です。

例：

- `321-02-3456`（補足情報がないため一致せず）
- `SSN: 132-45-6788`（一致）

米国銀行協会銀行支店コード

ABA 送金番号分類子は、クレジット カード番号分類子とほぼ同じです。

例：

- `119999992`（補足情報がないため一致せず）
- `ABA No. 800000080`（一致）

運転免許証番号（米国）

米国運転免許証分類子を使用するポリシーは多数あります。デフォルトでは、この分類子は、米国で発行された運転免許証を検索します。カリフォルニア州の AB-1298 およびモンタナ州の HB-732 など米国の州固有のポリシーでは、それぞれの州の米国運転免許のみを検索します。

各州の分類子はその州のパターンと照合し、対応する州の名前または略称および追加の補足データを定めています。

例：

- `CA DL# C3452362`（番号と補足データのパターンが正しいため一致）
- `California DL# C3452362`（一致）

- `DL: C3452362`（補足データ不足のため一致せず）
- `California C3452362`（補足データ不足のため一致せず）
- `OR DL# C3452362`（一致）
- `OR DL# 3452362`（オレゴン州の正しいパターンのため一致）
- `WV DL# D654321`（ウェスト バージニア州の正しいパターンのため一致）
- `WV DL# G654321`（一致）

国内のプロバイダー ID（米国）

米国の国内のプロバイダー ID の分類子は、チェック デジットを含む 10 桁の数字である国家プロバイダー認証（NPI）をスキャンします。

例：

- `NPI No. 1245319599`（NPI があるため一致）
- `NPI No. 1235678996`（NPI があるため一致）
- `3459872347`（補足情報がないため一致せず）
- `NPI: 3459872342`（誤ったチェック デジットのため一致せず）

学歴（英語）

事前定義された Family Educational Rights and Privacy Act（FERPA; 家族教育権とプライバシー法）DLP ポリシー テンプレートは、生徒記録分類子を使用します。より正確に検出するため、この分類子とカスタマイズされた生徒識別番号分類子を組み合わせて、特定の生徒 ID パターンを検出します。

例：

- `Fall Semester Course Numbers: CHEM101, ECON102, MATH103`（一致）

財務諸表（英語）

事前定義された Sarbanes-Oxley（SOX）ポリシー テンプレートは、企業財務情報分類子を使用し、非公開の企業の財務情報を検索します。

例：

`Gross Profits, Current Assets, and Cash Flow Statement for the Quarter ended June 30, 2016.`（一致）

カスタム DLP ポリシーに対するコンテンツ照合分類子の作成

作成したカスタム分類子は、カスタム DLP ポリシーの作成時に使用できる分類子のリストに追加されます。

手順

	コマンドまたはアクション	目的
ステップ 1	潜在的な DLP 違反を特定するためにコンテンツ照合分類子がどのように使用されているかを理解します。	参照先： • コンテンツ照合分類子を使用した拒否されたコンテンツの定義について（635 ページ） • コンテンツ照合分類子の例 （635 ページ）
ステップ 2	[メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択し、[カスタム分類子の追加（Add Custom Classifier）] をクリックします。分類子の名前と説明を入力します。	—
ステップ 3	近接性および最小合計スコアを入力します。	疑わしい違反のリスク要因の判別子（643 ページ）を参照してください
ステップ 4	次の検出規則タイプから 1 つを選択し、関連するコンテンツの一致基準を定義します。 • 単語またはフレーズ • ディクショナリのテキスト • 正規表現、または • 既存のデータ消失防止エンティティ	参照先： • 機密情報を特定する分類子検出ルール（カスタム DLP ポリシーのみ）（639 ページ） • 機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用 （641 ページ） • 識別番号を識別する正規表現 （639 ページ）
ステップ 5	（任意）[ルールの追加（Add Rule）] をクリックして、追加ルールを追加します。	重み付けや最大スコアの詳細については、疑わしい違反のリスク要因の判別子（643 ページ）を参照してください。
ステップ 6	複数のルールを含める場合は、ルールの**すべて一致**と**いずれか一致**を指定します。	この設定は、[ルール（Rules）] セクションの上部にあります。
ステップ 7	変更を送信し、保存します。	—

次のタスク

カスタム DLP ポリシーでカスタム コンテンツ分類子を使用します。カスタム DLP ポリシーの作成（詳細） （633 ページ） を参照してください。

関連項目

• カスタム コンテンツ分類子が使用されるポリシーの表示 （646 ページ）

機密情報を特定する分類子検出ルール（カスタム DLP ポリシーのみ）

コンテンツ照合分類子では、メッセージやドキュメント内の DLP 違反を検出するルールが必要となります。分類子では、次の検出ルールの 1 つ以上のルールを使用できます。

- **単語またはフレーズ**（Words or Phrases）。分類子が探す単語およびフレーズの一覧。複数のエントリは、カンマまたは改行で区切ります。
- **正規表現**（Regular Expression）。メッセージや添付ファイルの検索パターンを定義する正規表現。false positive を防止するため、照合から除外するパターンも定義できます。詳細については、「識別番号を識別する正規表現 （639 ページ）」と「識別番号を識別する正規表現の例 （641 ページ）」を参照してください。
- **ディクショナリ（Dictionary）**。単語とフレーズに関連するディクショナリ。 電子メールゲートウェイには定義済みディクショナリがあります。または独自に作成できます。機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタムディクショナリの使用 （641 ページ）を参照してください。
- **エンティティ（Entity）**。定義済みのパターンは、クレジットカード番号、アドレス、社会保障番号、または ABA 送金番号などの機密データの一般的なタイプを識別します。エンティティの説明については、[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] に移動し、[DLP ポリシーの追加（Add DLP Policy）] をクリックし、[プライバシー保護（Privacy Protection）] をクリックして、[ポリシーの説明を表示（Display Policy Descriptions）] をクリックします。

識別番号を識別する正規表現

ポリシーテンプレートによっては、1 つ以上のコンテンツ照合分類子をカスタマイズする必要であり、カスタマイズには、カスタムアカウント番号、患者識別番号または生徒識別番号などの極秘情報に結び付く可能性がある識別番号を検索するための正規表現の作成があります。**Perl 互換正規表現（PCRE2）**構文を使用して、コンテンツ照合分類子または DLP ポリシー テンプレートに一致する正規表現を追加できます。 電子メールゲートウェイで DLP 機能が有効な場合にのみ、PCRE2 互換の正規表現が検証されます。

（注） 正規表現では大文字と小文字は区別されるため、`[a-zA-Z]` のように大文字と小文字を含める必要があります。特定の文字のみ使用する場合は、その文字に合わせて正規表現を定義します。

8 桁の数字など、あまり特殊ではないパターンほど、ランダムな 8 桁の数字を実際の顧客番号と区別するため、追加の単語とフレーズを検索するポリシーが必要になります。

次の表を、分類子用の正規表現の作成ガイドとして使用してください。

要素	説明
正規表現（abc）	正規表現の一連の命令が文字列の一部に一致すると、分類子用の正規表現はその文字列に一致するということになります。 たとえば、正規表現**ACC**は、文字列**ACCOUNT**と**ACCT**に一致します。
[ ]	大カッコは文字のセットを示すために使用します。文字は個々または範囲で定義できます。 たとえば、**[a-z]**は、aからzまでのすべての小文字に一致し、**[a-zA-Z]**は、A から Z までのすべての大文字と小文字に一致します。**[xyz]**は、x、y または z の文字のみに一致します。
バックスラッシュ特殊文字（\）	円記号は特殊文字のエスケープに使用します。シーケンス「\.」はピリオドそのもののみに一致し、「\$」はドル記号のみに一致し、「\^」はキャレット記号のみに一致します。 円記号は、「\d」などトークンの始まりともなります。 **重要**：円記号はパーサーでも特殊なエスケープ文字として使用します。そのため、正規表現で円記号を使用する場合、*2*つの円記号が必要です。解析後には「実際に」使用される円記号 1 つのみが残り、正規表現システムに渡されます。
\d	数字（0 ～ 9）に一致するトークン。複数の数字に一致させるには、整数を {} に入れ、数の長さを規定します。 たとえば、「\d」は、5 などの 1 桁の数字のみに一致しますが、55 には一致しません。\d{2} を使うと、55 などの 2 桁の数に一致しますが、5 には一致しません。
\D	数字以外の文字に一致するトークン。複数の数字以外の文字に一致させるには、{} で囲んだ整数で長さを定義します。
\w	任意の英数字と下線に一致するトークン（a ～ z、A ～ Z、0 ～ 9、および _）。
繰り返し回数 {min,max}	1 つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。 たとえば、式「\d{8}」は 12345678 および 11223344 と一致しますが、8 とは一致しません。

要素	説明
または (|)	代替、つまり「or」演算子に相当します。「AおよびB」が正規表現である場合、式「A|B」は「A」または「B」のいずれかと一致する文字列と一致します。これは、正規表現で複数の数値パターンを組み合わせるために使用できます。 たとえば、「foo|bar」という表現は「foo」や「bar」とは一致しますが、「foobar」とは一致しません。

関連項目

- 識別番号を識別する正規表現の例 （641 ページ）

識別番号を識別する正規表現の例

識別または口座番号に数字と文字のパターンを記述する単純な正規表現には、次のように表示される可能性があります。

- 8 桁の数：`\d{8}`
- 数字のセットの間にハイフンがある識別コード：`\d{3}-\d{4}-\d`
- 大文字または小文字の英字 1 つで始まる識別コード：`[a-zA-Z]\d{7}`
- 3 桁の数字で始まり、大文字が 9 つ続く識別コード：`\d{3}[A-Z]{9}`
- | を使い、検索する 2 つの異なる数字パターンを定義：`\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用

AsyncOS には、事前定義された一連のディクショナリが提供されますが、DLP スキャン機能に一致する用語を指定するカスタム DLP ディクショナリを作成することもできます。

複数の方法でカスタム DLP ディクショナリを作成できます。

- カスタム DLP ディクショナリの直接追加 （641 ページ）
- テキスト ファイルとして DLP ディクショナリを作成 （642 ページ）、その後にDLP ディクショナリのインポート （642 ページ）。
- 別の 電子メールゲートウェイからDLP ディクショナリのエクスポート （642 ページ）、次にDLP ディクショナリのインポート （642 ページ）。

カスタム DLP ディクショナリの直接追加

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）] を選択します。

ステップ 2 [詳細設定（Advanced Settings）] セクションで、[カスタム DLP ディクショナリ（Custom DLP Dictionaries）] の側のリンクをクリックします。

ステップ 3 [ディクショナリを追加（Add Dictionary）] をクリックします。

ステップ 4 カスタム ディクショナリの名前を入力します。

ステップ 5 用語のリストに新規ディクショナリのエントリ（単語とフレーズ）を入力します。

ディクショナリの単語は大文字と小文字が区別され、非ASCII 文字を含めることができます。

複数のエントリを入力する場合は、改行でエントリを区切ります。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 変更を送信し、保存します。

テキスト ファイルとして DLP ディクショナリを作成

ユーザ独自のディクショナリをテキストファイルとしてローカルマシンに作成し、電子メールゲートウェイにインポートできます。ディクショナリのテキスト ファイルにおける各単語には、強制改行を使用します。ディクショナリの単語は大文字と小文字が区別され、非ASCII 文字を含めることができます。

DLP ディクショナリのエクスポート

（注） 事前定義された DLP ディクショナリはエクスポートできません。

手順

ステップ 1 **[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）]** を選択します。

ステップ 2 [詳細設定（Advanced Settings）] の **[カスタム DLP ディクショナリ（Custom DLP Dictionaries）]** セクションのリンクをクリックします。

ステップ 3 **[ディクショナリをエクスポート（Export Dictionary）]** をクリックします。

ステップ 4 エクスポートするディクショナリを選択します。

ステップ 5 ディクショナリのファイル名を入力します。

ステップ 6 エクスポートされたディクショナリを保存する場所（ローカルコンピュータまたは電子メールゲートウェイの configuration ディレクトリのいずれか）を選択します。

ステップ 7 ファイルのエンコード方式を選択します。

ステップ 8 **[送信（Submit）]** をクリックし、ファイルを保存します。

DLP ディクショナリのインポート

はじめる前に

電子メールゲートウェイに非 DLP ディクショナリからエクスポートしたファイルをインポートする場合は、最初にテキストファイルから重み値を削除し、正規表現を単語または語句に変換する必要があります。

手順

ステップ 1 **[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）]** を選択します。

ステップ 2 [詳細設定（Advanced Settings）] セクションで、[カスタム DLP ディクショナリ（Custom DLP Dictionaries）] の側のリンクをクリックします。

ステップ 3 [ディクショナリをインポート（Import Dictionary）] をクリックします。

ステップ 4 ファイルをローカルマシンからインポートするか、 電子メールゲートウェイの configuration ディレクトリからインポートするかを選択します。

ステップ 5 エンコード方式を選択します。

ステップ 6 **[Next]** をクリックします。

「成功」を伝えるメッセージが表示され、インポートされたディクショナリが [ディクショナリの追加（Add Dictionary）] ページに表示されます。ただし、このプロセスはまだ完全ではありません。

ステップ 7 ディクショナリの名前を指定し、編集します。

ステップ 8 **[送信（Submit）]** をクリックします。

疑わしい違反のリスク要因の判別子

電子メールゲートウェイは DLP 違反に対してメッセージをスキャンすると、メッセージにリスク要因スコアを割り当てます。このスコアは、メッセージに DLP 違反が含まれる確率を示します。スコアが 0 であれば、メッセージにはほぼ確実に違反が含まれないことを意味します。スコアが 100 であれば、ほぼ確実に違反が含まれます。

定義済みのテンプレートに基づいた DLP ポリシーについて

定義済みのテンプレートから作成された DLP ポリシーに対するリスク要因のスコアリング パラメータを表示または変更することはできません。ただし、特定 DLP ポリシーに大量の誤検出の一致がある場合、そのポリシーに対して重大度スケールを調整できます。違反の重大度の評価について （647 ページ）を参照してください。コンテンツ照合分類子のないテンプレート（SOX（Sarbanes-Oxley）テンプレートなど）に基づくポリシーの場合、メッセージがポリシーに違反していると、スキャン エンジンは常にリスク要因の値として「75」を返します。

カスタム DLP ポリシーについて

カスタム DLP ポリシーに対するコンテンツ照合分類子を作成すると、リスク要因スコアを決定するために使用される値を指定します。

- **近接性**。違反と見なすには、メッセージや添付ファイルの中でルールと一致する箇所がどのくらい近くで発生する必要があるかを定義します。たとえば、長いメッセージの先頭近くに社会保障番号のような数値パターンが出現し、一番下の送信者の署名にアドレスが含まれている場合、この数値パターンとアドレスには関連性がないと見なされ、一致としてカウントされません。
- **最小総合スコア**。機密情報が DLP 違反として分類されるために必要な最小限のリスク要因スコア。メッセージの一致スコアが最小総合スコアに満たない場合、そのデータは機密データとして見なされません。
- **重み**。作成するカスタムルールのそれぞれに、ルールの重要度を表す「重み」を指定します。スコアは検出ルールに一致した数にルールの重みを乗算することで取得できます。重みが 10 のルールで違反が 2 つある場合は、スコアは 20 となります。あるルールが分類子にとって他より重要であれば、より大きい重みをアサインすることになります。
- **最大スコア**。ルールの最大スコアは、多数の低い重みのルールによってスキャンの最終スコアにゆがみが生じるのを防ぎます。
- **最小スコア**。[DLPポリシーのカスタマイズ（DLP Policy Customizations）] ページの [カスタム分類子設定（Custom Classifiers Settings）] セクションにある [エンティティベースのルールで推奨される最小スコアを使用（Use recommended minimum scores for entity-based rules）] チェックボックスの選択に応じて、推奨される最小スコアを使用するか、またはウェイトの使用を選択することができます。詳細については、エンティティベースのルールで最小スコアを使用する（カスタム DLP ポリシーのみ）（645 ページ）を参照してください。

リスク要因を計算するため、分類子は検出ルールに一致する数にルールの重みを乗算します。この値が検出ルールの最大スコアを超えている場合、分類子では最大スコアの値が使用されます。分類子が複数の検出ルールを持つ場合、すべての検出ルールのスコアを合計して1つの値にします。分類子は次の表にあるように、検出ルールのスコア（10 ～ 10000）を 10 ～ 100 の対数目盛りにマッピングし、リスク要因を算出します。

表 *42*：検出ルール スコアからのリスク要因スコアの計算方法

ルールのスコア	リスク要因
0	0
1	1
2	2
3	3
5	6
6	7
7	8
8	9

ルールのスコア	リスク要因
9	10
10	11
15	16
20	20
25	24
30	26
40	32
50	36
75	44
100	50
125	54
150	58
257	67
300	70
400	75
500	78
750	84
1000	87
5000	98
8000	99
10000	99
20000	100

エンティティベースのルールで最小スコアを使用する（カスタム DLP ポリシーのみ）

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DLPポリシーのカスタマイズ（DLP Policy Customizations）] に移動します。

ステップ 2 [カスタム分類子設定（Custom Classifiers Settings）] セクションで、**[エンティティベースのルールで推奨される最小スコアを使用（Use recommended minimum scores for entity-based rules）]** チェックボックスを選択します。

このオプションを選択すると、エンティティベースのルールのスコアは、ウェイトの代わりに設定した最小スコアを使用して計算されます。

たとえば、このオプションを無効にして、メッセージがウェイトを 10 に設定した特定のエンティティの 5 つのルールと一致した場合、ルールのスコアは、5 つの一致と 10 回の出現を掛け合わせて 50 になります。エンティティの最小スコアが 10 に設定されたこのオプションを有効にすると、設定した最小スコアおよび一部の一致と完全一致の数に基づいてスコアが計算されます。

（注） [エンティティベースのルールで推奨される最小スコアを使用（Use recommended minimum scores for entity-based rules）] オプションを選択した場合は、エンティティベースのルールを使用してすべての分類子の最小合計スコアを確認する必要があります。

ステップ 3 [送信（Submit）] をクリックし、変更をコミットします。

このオプションを有効にすると、カスタム分類子のエンティティベースのルールの最小スコアを確認する必要があります。詳細については、カスタム DLP ポリシーに対するコンテンツ照合分類子の作成 （637 ページ）を参照してください。

カスタム コンテンツ分類子が使用されるポリシーの表示

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択します。

ステップ 2 [カスタム分類子（Custome Classifiers）] セクションで、[カスタム分類子（Custome Classifiers）] テーブルの見出しにある [ポリシー（Policies）] をクリックします。

次のタスク

関連項目

- カスタム DLP ポリシーに対するコンテンツ照合分類子の作成 （637 ページ）

DLP ポリシーのメッセージのフィルタリング

パフォーマンスや精度を向上させるために、次の基準に基づいて特定のメッセージだけに適用されるように DLP ポリシーを制限できます。

オプション	説明
送信者および受信者に基づいたフィルタリング	DLP ポリシーを制限し、次のいずれかを使用して指定する送信者または受信者を含むまたは含まないメッセージに適用する。 • 完全な電子メール アドレス：`user@example.com` • 電子メール アドレスの一部：`user@` • ドメインのすべてのユーザ：`@example.com` • 部分ドメインのすべてのユーザ：`@.example.com` 改行やカンマで、複数のエントリを分離できます。 AsyncOS は最初に発信メッセージの受信者または送信者が発信メール ポリシーと一致するか照合し、次に送信者または受信者がそのメール ポリシーでイネーブルとなっている DLP ポリシーで指定した送信者および受信者フィルタと一致するか照合します。 たとえば、パートナー ドメインの受信者を除いて、すべての送信者に対し特定のタイプの情報を送信することを拒否する場合があります。パートナー ドメイン内のすべてのユーザを除外するフィルタを含め、その情報に対し DLP ポリシーを作成し、すべての送信元に適用される発信メール ポリシーにこの DLP ポリシーを含めます。
添付ファイルの種類に基づいたフィルタリング	特定の種類の添付ファイルを含むまたは含まないメッセージのみをスキャンするよう DLP ポリシーを限定できます。添付ファイルのカテゴリを選択し、次に定義済みのファイル タイプを選択するか、リストされていないファイル タイプを指定します。事前定義されていないファイル タイプを指定した場合、AsyncOS は添付ファイルの拡張子に基づいてファイル タイプを検索します。 DLP のスキャンを、最小ファイル サイズの添付ファイルに限定することができます。
メッセージ タグによるフィルタリング	DLP ポリシーを特定のフレーズを含むメッセージのスキャンに限定する場合は、メッセージまたはコンテンツ フィルタを使って発信メッセージにそのフレーズがないか検索し、カスタム メッセージ タグを当該メッセージに挿入することができます。詳細については、コンテンツ フィルタのアクション （338 ページ）およびメッセージ フィルタを使用した電子メール ポリシーの適用 （155 ページ）を参照してください。

違反の重大度の評価について

DLP スキャン エンジンが潜在的な DLP 違反を検出すると、そのインスタンスが実際に DLP 違反である確率を表すリスク要因スコアを計算します。ポリシーでは、リスク要因スコアをその

ポリシーに定義されている重大度スケールと比較して、重大度レベル（たとえば、[低（Low）]、[重大（Critical）] など）を判別します。各重大度レベルでの違反に対して実行するアクションは、ユーザが指定します（ただし、[無視（Ignore）] の場合に実行されるアクションはありません）。各重大度レベルに達するために必要なリスク要因スコアは、調整することができます。

関連項目

- 重大度スケールの調整 （648 ページ）

重大度スケールの調整

すべてのポリシーにはデフォルトの重大度スケールがあります。各ポリシーに対してこのスケールを調整できます。

たとえば、リスク要因スコアが 90 から 100 の場合、デフォルトで違反の重大度レベルはクリティカルになります。ただし、特定のポリシーに一致する違反についてはデータ消失の可能性があり、機密度を上げることが必要になることがあります。このDLPポリシーには、クリティカルな重大度レベルを 75 ～ 100 のリスク要因スコアを持つ違反に変更できます。

手順

ステップ 1 **[メール ポリシー（Mail Policies）] > [DLP ポリシー マネージャ（DLP Policy Manager）]** を選択します。

ステップ 2 編集するポリシーの名前をクリックします。

ステップ 3 [重大度設定（Severity Settings）] セクションで、[スケールの編集（Edit Scale）] をクリックします。

ステップ 4 スケールの矢印を使用して、重大度レベルのスコアを調整します。

ステップ 5 **[完了（Done）]** をクリックします。

ステップ 6 [重大度スケール（Severity Scale）] のテーブルで、必要なときにスコアがあることを確認します。

ステップ 7 **[送信（Submit）]** をクリックします。

次のタスク

関連項目

- 違反の重大度の評価について （647 ページ）

違反との一致に対する Email DLP ポリシーの順序の調整

DLP 違反が、発信メール ポリシーでイネーブルな DLP ポリシーに 1 つ以上一致する場合、リストで最初に一致した DLP ポリシーのみが使用されます。

手順

ステップ 1 [DLP ポリシー マネージャ（DLP Policy Manager）] ページで、[ポリシーの順番の編集（Edit Policy Order）] をクリックします。

ステップ 2 移動するポリシーの行をクリックし、新しい順序の場所にドラッグします。

ステップ 3 ポリシーの順序の変更を完了したら、変更内容を送信し、確定します。

発信メール ポリシーとの DLP ポリシーの関連付け

関連項目

- デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け （649 ページ）
- 発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て （650 ページ）

デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け

デフォルトの発信メール ポリシーは、他の発信メール ポリシーが送信者または受信者に一致しない場合に使用されます。

はじめる前に

データ漏洩防止の設定方法 （627 ページ）のテーブルの、ここまでのすべてのアクティビティを実行します。たとえば、デフォルトの発信メール ポリシーに含める DLP ポリシーを作成したことを確認します。

手順

ステップ 1 **[メール ポリシー（Mail Policies）] > [メール ポリシー（Mail Policies）]** を選択します。

ステップ 2 テーブルの **[デフォルト ポリシー（Default Policy）]** の行で、**[DLP]** の列の **[ディセーブル（Disabled）]** リンクをクリックします。

ステップ 3 [DLP を有効にする（設定をカスタマイズ）（Enable DLP（Customize Settings））] を選択します。

ステップ 4 デフォルトの発信メール ポリシーでイネーブルにする DLP ポリシーを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

追加の発信メール ポリシーの DLP ポリシーを選択します。発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て （650 ページ） を参照してください。

発信メール ポリシーを使用した送信者および受信者への DLP ポリシーの割り当て

発信メール ポリシーでイネーブルにすることによって、どの送信者と受信者にどの DLP ポリシーを適用するかを指定します。発信メール ポリシー内で DLP ポリシーだけを使用することができます。

はじめる前に

デフォルトの発信メール ポリシーの DLP ポリシーを設定します。デフォルトの発信メール ポリシーとの DLP ポリシーの関連付け （649 ページ）を参照してください。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [メール ポリシー（Mail Policies）] を選択します。
ステップ 2 テーブルの任意の行の DLP 列のリンクをクリックします。
ステップ 3 この発信メール ポリシーに関連付ける DLP ポリシーを選択します。
ステップ 4 変更を送信します。
ステップ 5 他の発信メール ポリシーに対して、必要に応じて繰り返します。
ステップ 6 変更を保存します。

次のタスク

データ漏洩防止の設定方法 （627 ページ）を参照してください。

DLP ポリシーの編集または削除に関する重要な情報

操作	情報
DLP ポリシーの編集	ポリシーの名前を変更すると、発信メール ポリシーで再度イネーブルにする必要があります。
DLP ポリシーの削除	ポリシーを削除すると、DLP ポリシーが 1 つ以上の発信メール ポリシーで使用された場合に、通知を受信します。DLP ポリシーの削除により、このようなメール ポリシーからポリシーが削除されます。

メッセージ アクション

発信メッセージから DLP 違反の可能性が検出されると、 電子メールゲートウェイが実行するプライマリおよびセカンダリアクションを指定します。さまざまなアクションに対して、異なる違反タイプおよび重大度を割り当てることができます。

プライマリ アクションは次のとおりです。

- デリバリ
- ドロップ（Drop）
- 検疫（Quarantine）

セカンダリ アクションは次のとおりです。

- メッセージを配信する場合は、コピーをポリシー隔離に送信します。このコピーは、メッセージ ID を含む元のメッセージの完全なクローンです。コピーの隔離は、DLP 違反を監視する別の方法を提供する他、導入前に DLP システムをテストすることができます。隔離からコピーをリリースすると、電子メールゲートウェイはすでに元のメッセージを受信した受信者にコピーを配信します。
- メッセージの暗号化この 電子メールゲートウェイは、メッセージ本文だけを暗号化します。メッセージ ヘッダーは暗号化されません。
- DLP 違反があるメッセージの件名ヘッダーの変更
- メッセージへの免責事項の追加。
- 代替宛先メールホストへのメッセージの送信。
- 他の受信者にメッセージのコピー（bcc）の送信。（たとえば、重大なDLP違反があるメッセージを調べてもらうために、そのメッセージをコンプライアンス担当者のメールボックスにコピーできます）。
- DLP 違反の通知メッセージを、送信者や、マネージャまたは DLP コンプライアンス責任者といった他の連絡先に送信します。DLP 通知のドラフト （654 ページ）を参照してください。

（注） これらのアクションは相互排他的ではなく、各ユーザ グループのさまざまな要求を処理するために、異なる DLP ポリシー内でアクションをいくつか組み合わせることができます。また、同じポリシーの異なる重大度レベルに基づいて別の処理を設定できます。たとえば、重大な DLP 違反を含むメッセージを隔離し、コンプライアンス担当者に通知を送信しますが、重大度レベルの低いメッセージを配信することもできます。

関連項目

- DLP 違反アクション（メッセージアクション）に対して実行するアクションの定義 （651 ページ）
- メッセージ アクションの表示および編集 （653 ページ）
- DLP 通知のドラフト （654 ページ）

DLP 違反アクション（メッセージアクション）に対して実行するアクションの定義

はじめる前に

- DLP ポリシーに違反したメッセージ（またはメッセージのコピー）を保持する専用隔離を少なくとも 1 つ作成します。

ここでは、 電子メールゲートウェイでローカルに隔離するか、または Cisco Secure Email and Web Manager で一元的に隔離するかを指定できます。

詳細については、ポリシー、ウイルス、およびアウトブレイク隔離（1129ページ）を参照してください。

- 配信前にメッセージを暗号化する場合は、暗号化プロファイルを設定してください。Cisco 電子メール暗号化 （663 ページ）を参照してください
- DLP違反またはその疑いがあるメッセージを配信する場合、免責事項を含めるには、[メール ポリシー（Mail Policies）] > [テキスト リソース（Text Resources）] で、免責事項のテキストを指定します。詳細については、免責事項テンプレート （806ページ）を参照してください。
- DLP違反の送信者またはコンプライアンス責任者などの他の人に通知を送信するには、まず DLP 通知テンプレートを作成します。DLP 通知のドラフト （654 ページ）を参照してください。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択します。

ステップ 2 [メッセージアクション（Message Actions）] セクションで [メッセージアクションの追加（Add Message Action）] をクリックします。

ステップ 3 メッセージ アクションの名前を入力します。

ステップ 4 メッセージ アクションの説明を入力します。

ステップ 5 DLP 違反を含むメッセージをドロップ、配信、または隔離するか選択します。

（注） [配信（Deliver）] を選択すると、ポリシー隔離に送信されたメッセージのコピーを取ることを選択できます。メッセージのコピーはメッセージ ID を含む完全なクローンです

ステップ 6 配信にメッセージの隔離からリリースを暗号化する場合は、[暗号化を有効にする（Enable Encryption）] チェックボックスを選択して、次のオプションを選択します。

- [暗号化ルール（Encryption Rule）]。メッセージを常に暗号化するか、TLS 接続を介した送信試行が最初に失敗した場合だけ暗号化します。
- [暗号化プロファイル（Encryption Profile）]。Cisco IronPort 暗号化アプライアンスまたはまたはホステッド キー サービスを使用する場合、指定した暗号化プロファイルを使用してメッセージを暗号化し、配信します。
- [暗号化されたメッセージの件名（Encrypted Message Subject）]。暗号化されたメッセージの件名です。既存のメッセージ件名を保持するには、$Subject の値を使用します。

ステップ 7 アクションとして隔離を選択した場合は、DLP違反を含むメッセージに使用するポリシー隔離を選択します。

ステップ 8 次のオプションのいずれかを使用してメッセージを変更する場合は、[詳細（Advanced）] をクリックします。

- カスタム ヘッダーを追加します。
- メッセージの件名を変更します。
- 代替ホストに配信します
- 他の受信者にコピー（bcc）を送信します
- DLP 通知メッセージを送信します。

ステップ 9 変更を送信し、保存します。

メッセージ アクションの表示および編集

手順

ステップ 1 [メール ポリシー（Mail Policies）]>[DLP ポリシーのカスタマイズ（DLP Policy Customizations）] を選択します。

ステップ 2 [メッセージ アクション（Message Actions）] セクションでアクションを選択します。

目的	操作手順
各アクションが割り当てられているメール ポリシーを表示します。	メッセージ アクション表の見出しで [ポリシー（Policies）] のリンクをクリックします。
アクションごとに入力した説明を表示します。	メッセージ アクション表の見出しで [説明（Description）] のリンクをクリックします。
メッセージ アクションの詳細を表示または編集します。	メッセージ アクションの名前をクリックします。
メッセージ アクションを削除します。	削除対象のメッセージアクションの横にあるゴミ箱のアイコンをクリックします。 確認メッセージは、1 つ以上の DLP ポリシーでメッセージアクションが使用されているかどうかを通知します。

目的	操作手順
メッセージ アクションを複製します。 この機能は、メッセージ アクションを変更する前にバックアップコピーを作成するか、または新たな、または類似のメッセージ アクションの出発点として使用するために使用できます。	複製するメッセージ アクションの横にある [重複（Duplicate）] アイコンをクリックします。

ステップ 3 変更を送信し、確定します。

DLP 通知のドラフト

以下の手順に従って、組織のデータ漏洩防止ポリシーに違反する情報がメール メッセージに含まれている場合に送信する通知のテンプレートを作成します。この通知は、DLP ポリシーに違反しているメッセージの送信者、または別のアドレス（マネージャまたは DLP コンプライアンス責任者）に送信できます。

はじめる前に

- DLP 通知テンプレートの変数の定義 （655 ページ） の内容についてよく理解しておきます。各違反についての詳細を含む通知をカスタマイズするためにこれらの変数を使用できます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [テキスト リソース（Text Resources）] を選択します。

ステップ 2 [テキスト リソースを追加（Add Text Resource）] をクリックします。

ステップ 3 [タイプ（Type）] に、[DLP 通知テンプレート（DLP Notification Template）] を選択します。

DLP 変数は通常の通知テンプレートでは利用可能ではありません。

ステップ 4 通知テキストおよび変数を入力します。

この通知で受信者に対し、発信メッセージに組織のデータ漏洩防止ポリシーに違反する機密データが含まれている可能性があることを知らせる必要があります。

次のタスク

DLP Policy Manager の DLP ポリシーで [メッセージ アクション（Message Action）] にこの DLP 通知テンプレートを指定します。

関連項目

• DLP 通知テンプレートの変数の定義 （655 ページ）

DLP 通知テンプレートの変数の定義

通知に、各 DLP 違反に関する特定の情報を含めるには、次の変数を使用します。

変数	置き換える値
$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
$DLPSeverity	違反の重大度に置き換えられます。値は [低（Low）]、[中（Medium）]、[高（High）]、または [重大（Critical）] のいずれかです。
$DLPRiskFactor	メッセージの機密内容のリスク要因スコアに置き換えられます（スコア 0 ～ 100）。
$To	メッセージの To: ヘッダーに置き換えられます（エンベロープ受信者には置き換えられません）。
$From	メッセージの From: ヘッダーに置き換えられます（エンベロープ送信者には置き換えられません）。
$Subject	元のメッセージの件名に置き換えられます。
$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$GMTimestamp	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
$MID	メッセージを内部で識別するために使用するメッセージ ID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。
$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
$Reputation	送信者の IP レピュテーションスコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
$filenames	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
$filesizes	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。

変数	置き換える値
$remotehost	メッセージを Cisco アプライアンスに送信したシステムのホスト名に置き換えられます。
$AllHeaders	メッセージ ヘッダーに置き換えられます。
$EnvelopeFrom	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
$Hostname	電子メールゲートウェイのホスト名に置き換えられます。
$bodysize	メッセージのサイズ（バイト単位）に置き換えられます。
$header[‘*string* ’]	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
$remoteip	メッセージを 電子メールゲートウェイに送信したシステムの IP アドレスに置き換えられます。
$recvlistener	メッセージを受信したリスナーのニックネームに置き換えられます。
$dropped_filenames	$filenames と同様に、ドロップされたファイルのリストを表示します。
$dropped_filename	直近にドロップされたファイル名のみを返します。
$recvint	メッセージを受信したインターフェイスのニックネームに置き換えられます。
$timestamp	現在の時刻および日付（ローカル時間帯）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$orgid	SenderBase 組織 ID（整数値）で置き換えられます。
$enveloperecipients	メッセージのエンベロープ受信者すべて（Envelope To、<RCPT TO>）に置き換えられます。
$dropped_filetypes	$filetypes と同様に、ドロップされたファイル タイプのリストを表示します。
$dropped_filetype	直近にドロップされたファイルのファイル タイプのみを返します。

メッセージ トラッキングでの機密性の高い DLP データの表示

DLP 導入では、DLP ポリシーに違反するコンテンツを、周囲のコンテンツとともにログに記録するオプションが提供され、これは後でメッセージ トラッキングで表示できます。この内容は、クレジット カード番号や社会保障番号などの機密データを含む場合があります。

はじめる前に

メッセージ トラッキングをイネーブルにします。メッセージ トラッキングの有効化（1113 ページ）を参照してください

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 [一致したコンテンツのログへの記録（Enable Matched Content Logging）] チェックボックスを選択します。

ステップ 4 変更を送信し、保存します。

次のタスク

この情報を表示できる管理者ユーザを指定します。メッセージ トラッキングでの機密情報へのアクセスの制御 （1197 ページ） を参照してください。

関連項目

- メッセージ トラッキングの詳細 （1122 ページ）

DLP エンジンおよびコンテンツ照合分類子の更新について

Cisco DLP エンジンと 電子メールゲートウェイの定義済みコンテンツ照合分類子の更新は別のセキュリティサービスの更新に依存しません。

関連項目

- DLP エンジンの現在のバージョンの決定 （658 ページ）
- DLP エンジンとコンテンツ照合分類子の手動による更新 （658 ページ）
- 自動アップデートの有効化（推奨されません） （658 ページ）

- 一元化された（クラスタ化された） 電子メールゲートウェイの DLP 更新 （659 ページ）

DLP エンジンの現在のバージョンの決定

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 [最新 DLP バージョン ファイル（Current DLP Version Files）] のセクションを参照してください。

（注） また、`dlpstatus` CLI コマンドを使用して、DLP エンジンの現在のバージョンを表示することもできます。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

DLP エンジンとコンテンツ照合分類子の手動による更新

はじめる前に

その場合は、次のトピックを参照してください。

- （該当する場合）一元化された（クラスタ化された） 電子メールゲートウェイの DLP 更新 （659 ページ）

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 [最新 DLP バージョンファイル（Current DLP Version Files）] セクションで [今すぐ更新（Update Now）] をクリックします。

このボタンは、ダウンロード可能な新規アップデートがある場合にだけ使用できます。

（注） DLP エンジンを更新するには、`dlpupdate` CLI コマンドも使用できます。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

自動アップデートの有効化（推奨されません）

電子メールゲートウェイが定期的に更新をチェックし、ダウンロードできるようにするには、この手順を使用します。

（注） シスコは、自動更新を使用しないことを推奨します。これらの更新は、DLP ポリシーで使用されるコンテンツ照合分類子を変更する場合があります。代わりに、手動で DLP 更新をダウンロードし、実稼働環境で使われる 電子メールゲートウェイを更新する前に、ラボ環境でテストします。

はじめる前に

- [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで、自動アップデートをイネーブルにし、すべてのサービス契約更新に更新間隔を指定してください。
- 一元化された（クラスタ化された） 電子メールゲートウェイの DLP 更新 （659 ページ）を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [データ損失の防止（Data Loss Prevention）] の順に選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 [自動アップデートを有効にする（Enable automatic updates）] チェックボックスを選択します。

ステップ 4 変更を送信し、保存します。

一元化された（クラスタ化された） 電子メールゲートウェイの DLP 更新

次の点に注意してください。

- クラスタ化された導入での 電子メールゲートウェイでは、自動 DLP 更新を有効にできません。
- DLP の更新は、クラスタ、マシンまたはグループ レベルで設定されている DLP に関係なく、マシン レベルで常に実行されます。
- マシンレベルで **dlpstatus** CLI コマンドを使用したときのみ、 電子メールゲートウェイの DLP エンジンの状態をチェックできます。

DLP インシデントのメッセージとデータの使用

（注） 導入が該当する場合は、 Cisco Secure Email and Web Manager に関するドキュメントも参照してください。

目的	操作手順
DLP ポリシー名、違反の重大度、行われるアクションなどの基準を使って DLP 違反が含まれるメッセージを検索し、検出されたメッセージの詳細情報を表示します。	メッセージ トラッキング （1113 ページ）を参照してください。
疑わしい DLP 違反として隔離されたメッセージを表示または管理できます。	ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作 （1143 ページ）を参照してください。
DLPインシデントのサマリーを表示します。	DLP インシデント サマリー レポートについては、電子メール セキュリティ モニタの使用方法 （1009 ページ）を参照してください。
発信メールで検出された DLP 違反に関する情報を表示します。	DLP インシデント レポートについては、電子メール セキュリティ モニタの使用方法 （1009 ページ）を参照してください。

関連項目

- メッセージ トラッキングでの機密性の高い DLP データの表示 （657 ページ）
- メッセージ トラッキングでの機密情報へのアクセスの制御 （1197 ページ）

トラブルシューティング データ消失防止

- DLP が電子メールの添付ファイルの違反を検出しない （660 ページ）

DLP が電子メールの添付ファイルの違反を検出しない

問題

定義済みの DLP ポリシーを使用すると、DLP は電子メールの添付違反を検出しません。次の原因が考えられます。

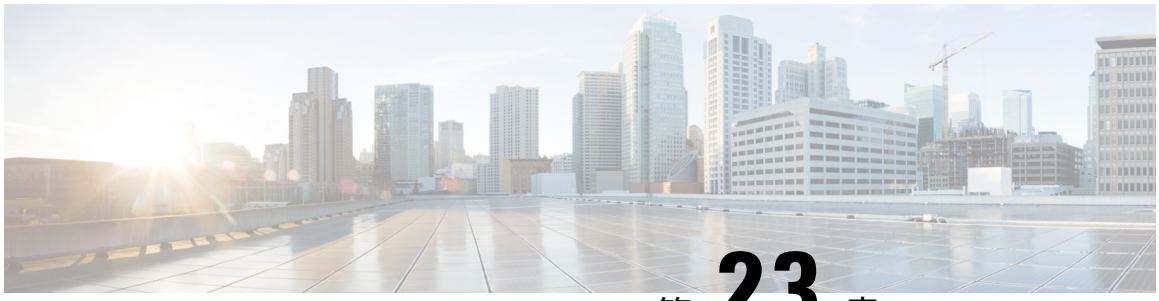
- 定義済みの DLP ポリシーのプロキシミティ パラメータの値が小さい

（注） 定義済みの DLP ポリシーのプロキシミティは変更できません。

- 定義済みの DLP ポリシーで定義されている重大度スケール パラメータが大きい

解決方法

- カスタム ポリシーを作成し、プロキシミティを必要に応じて調整します。カスタム DLP ポリシーの作成（詳細） （633 ページ）を参照してください。
- 定義済みの DLP ポリシーの重大度スケール パラメータを小さくします。重大度スケールの調整 （648 ページ）を参照してください



第 23 章

Cisco 電子メール暗号化

この章は、次の項で構成されています。

- Cisco 電子メール暗号化の概要 （663 ページ）
- Cisco Secure Email Encryption Service でメッセージを暗号化する方法 （664 ページ）
- 電子メールゲートウェイを使用したメッセージの暗号化 （665 ページ）
- 暗号化するメッセージの決定 （672 ページ）
- メッセージへの暗号化ヘッダーの挿入 （675 ページ）

Cisco 電子メール暗号化の概要

AsyncOS は暗号化を使用して着信電子メールと発信電子メールをサポートします。この機能を使用するには、暗号化されたメッセージの特性および、 Cisco Secure Email Encryption Service （マネージドサービス）のキー（鍵）サーバーの接続性の情報を指定する暗号化プロファイルを作成します。

次に、暗号化するメッセージを作成するために、コンテンツ フィルタ、メッセージ フィルタ、データ漏洩防止ポリシーを作成します。

1. フィルタ条件に合致する発信メッセージは、電子メールゲートウェイの暗号化処理のキューに入れられます。
2. メッセージが暗号化されると、暗号化に使われたキーがキー サーバーに保存され、暗号化されたメッセージが配信のキューに入れられます。
3. キューの中の電子メールの暗号化を妨げるような条件（つまり、一時的な C シリーズのビジー状態や Cisco Secure Email Encryption Service が使用できない状態）が一時的に存在すると、メッセージはキューに入れられ、しばらくしてから再度暗号化が試行されます。

（注） また、メッセージを暗号化する前に、まず TLS 接続経由で送信を試みるように電子メールゲートウェイを設定することもできます。詳細については、TLS 接続を暗号化の代わりに使用 （672 ページ）を参照してください。

Cisco Secure Email Encryption Service でメッセージを暗号化する方法

表 *43 : Cisco Secure Email Encryption Service* でメッセージを暗号化する方法

手順	操作手順	詳細
ステップ 1	ネットワークの Cisco IronPort 暗号化アプライアンスを設定します。	セットアップおよび設置 （19 ページ）を参照してください。
ステップ 2	メッセージ暗号化をイネーブルにします。	電子メールゲートウェイでのメッセージの暗号化のイネーブル化 （666 ページ）。
ステップ 3	暗号化プロファイルを作成して、暗号化キーサーバーと暗号化されたメッセージのセキュリティ設定を指定します。	キーサービスによる暗号化メッセージの処理方法の設定 （667 ページ）。
ステップ 4	電子メールゲートウェイが暗号化できるように、メッセージが満たす必要のある条件を定義します。	暗号化するメッセージの決定 （672 ページ）。
ステップ 5	電子メールのワークフローにおいてメッセージを暗号化するタイミングを決定します。	• コンテンツ フィルタを使用したメッセージの暗号化と即時配信 （673 ページ）。 または • コンテンツ フィルタを使用した配信時のメッセージの暗号化 （674 ページ）。
ステップ 6	（任意）メッセージに追加セキュリティのフラグを付けます。	メッセージへの暗号化ヘッダーの挿入 （675 ページ）。
ステップ 7	メッセージを暗号化するユーザ グループを定義します。	メール ポリシーを作成します。 メール ポリシー （309 ページ）を参照してください
ステップ 8	定義したユーザ グループに定義済みの暗号化アクションを関連付けます。	メール ポリシーにコンテンツ フィルタを関連付けます。 メール ポリシー （309 ページ）を参照してください

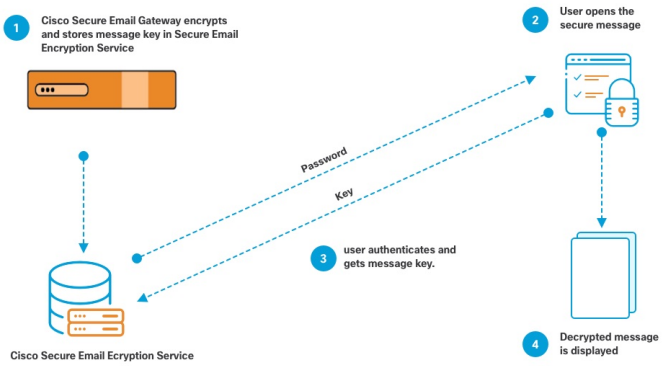
関連項目

- 暗号化ワークフロー （665 ページ）

暗号化ワークフロー

電子メール暗号化を使用する場合、電子メールゲートウェイはメッセージを暗号化し、 Cisco Secure Email Encryption Service（ホステッドキーサービス）にメッセージキーを格納します。受信者が暗号化されたメッセージを開封すると、キーサービスによって受信者が認証され、復号されたメッセージが表示されます。

図 *34* : 暗号化ワークフロー



暗号化されたメッセージを開封する基本的なワークフローは次のとおりです。

1. 暗号化プロファイルを設定するときは、メッセージ暗号化のパラメータを指定します。暗号化されたメッセージでは、メッセージキーが電子メールゲートウェイによりホステッドキーサービス（Cisco Secure Email Encryption Service）に作成および格納されます。
2. 受信者はブラウザで安全なエンベロープを開封します。
3. ブラウザで暗号化されたメッセージを開封するとき、受信者の本人確認のためパスワードが必要となります。キー サーバはメッセージに関連付けられた暗号化キーを返します。

（注） 暗号化された電子メール メッセージの初回開封時に、受信者は安全なエンベロープを開封するためのキー サービスに登録する必要があります。登録後、暗号化プロファイルの設定によっては、受信者が暗号化されたメッセージを認証なしで開封することも可能です。暗号化プロファイルでは、パスワード不要と指定できますが、特定の機能が使用できなくなります。

4. 復号したメッセージが表示されます。

電子メールゲートウェイを使用したメッセージの暗号化

電子メールゲートウェイによる暗号化を使用するには、暗号化プロファイルを設定する必要があります。encryptionconfig CLI コマンド、または GUI の [セキュリティサービス（Security Services）] > [Cisco IronPortメール暗号化（Cisco IronPort Email Encryption）] で、暗号化プロファイルをイネーブルにして設定することができます。

（注） 電子メールゲートウェイでPXE暗号化とS/MIME暗号化が有効になっている場合、AsyncOSではまず S/MIME を使用して、次に PXE を使用してメッセージが暗号化されます。

関連項目

- 電子メールゲートウェイでのメッセージの暗号化のイネーブル化 （666 ページ）
- キー サービスによる暗号化メッセージの処理方法の設定 （667 ページ）
- エンベロープのデフォルト ロケールの設定 （670 ページ）
- PXE エンジンの最新バージョンへの更新 （671 ページ）

電子メールゲートウェイでのメッセージの暗号化のイネーブル化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Cisco IronPort電子メール暗号化（Cisco IronPort Email Encryption）] をクリックします。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 （任意）次のオプションを設定するには、[設定の編集（Edit Settings）] をクリックしてください。

- 暗号化する最大メッセージ サイズ。シスコが推奨するメッセージ サイズは 10 MB です。電子メールゲートウェイが暗号化するメッセージの最大サイズは 25 MB です。

  （注） 推奨される 10 MB の制限を超えてメッセージを暗号化すると、電子メールゲートウェイのパフォーマンスが遅くなる可能性があります。Cisco Registered Envelope サービスを使用する場合、メッセージ受信者は 10 MB より大きい添付ファイルのある暗号化メッセージへは返信できません。

- 暗号化アカウント管理者のメールアドレス。暗号化プロファイルをプロビジョニングすると、この電子メール アドレスが自動的に暗号化サーバに登録されます。

- プロキシ サーバを設定します。

（注） Secure Emali Encryption Service 管理ポータルで[メッセージからの読み取り（Read from Message）]機能を有効にすることで、暗号化されたエンベロープのコピーを保存する優先ストレージを設定できます。次のストレージオプションを使用できます。

- Cisco Storage
- Microsoft OneDrive Storage

詳細については、このページの『*Cisco Secure Email Encryption Service Account Administrator Guide*』を参照してください。

キー サービスによる暗号化メッセージの処理方法の設定

キー サービスを使用する場合、1 つ以上の暗号化プロファイルを作成できます。さまざまな電子メール グループに異なるセキュリティ レベルを使用する場合、それぞれ別の暗号化プロファイルを作成することもできます。たとえば、機密資料を含んだメッセージを高レベルのセキュリティで送信し、他のメッセージを中レベルのセキュリティで送信するという場合です。この場合、特定のキー ワード（「confidential」など）を含むメッセージには高レベルのセキュリティ暗号化プロファイルを作成し、他の発信メッセージには別の暗号化プロファイルを作成します。

暗号化プロファイルをカスタム ユーザー ロールに割り当て、そのロールに割り当てられた委任管理者が DLP ポリシーとコンテンツ フィルタで暗号化プロファイルを使用できるようにします。DLP ポリシーとコンテンツ フィルタを設定する場合は、管理者、オペレータ、および委任ユーザだけが暗号化プロファイルを使用できます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。詳細については、管理タスクの分散 （1191 ページ）を参照してください。

（注） 1 つのホステッド キー サービスに複数の暗号化プロファイルを設定できます。組織に複数のブランドがある場合、PXE エンベロープ用にキー サーバに格納された異なるロゴを参照することができます。

暗号化プロファイルは次の設定を保存します。

- [キーサーバ設定（Key server settings）]。キー サーバとそのキー サーバに接続するための情報を指定します。
- [エンベロープ設定（Envelope settings）]。セキュリティ レベル、開封確認を返すか、暗号化キューにあるメッセージがタイムアウトするまでの時間、使用する暗号化アルゴリズムのタイプ、および復号アプレットをブラウザで動作可能にするかなど、メッセージエンベロープの詳細を指定します。
- [メッセージ設定（Message settings）]。安全なメッセージ転送や安全な「全員に返信」をイネーブルにするかなど、メッセージに関する詳細を指定します。

- [通知設定（Notification settings）]。暗号化失敗通知と同様、テキスト形式およびHTML形式の通知を使う通知テンプレートを指定します。暗号化プロファイル作成時に、テキストリソース内のテンプレートを作成し、テンプレートを選択します。エンベロープをローカライズし、暗号化失敗通知のメッセージの件名を指定することもできます。通知の詳細については、暗号化通知テンプレート（817ページ）およびバウンス通知および暗号化失敗通知テンプレート（816ページ）を参照してください。

手順

ステップ1 [メール暗号化プロファイル（Email Encryption Profiles）] のセクションで [暗号化プロファイルの追加（Add Encryption Profile）] をクリックします。

ステップ2 暗号化プロファイルの名前を入力します。

ステップ3 [使用者（役割）（Used By (Roles)）] リンクをクリックし、暗号化プロファイルへのアクセス権を設定するカスタム ユーザー ロールを選択して、[OK] をクリックします。

このカスタム ロールに割り当てられた委任管理者は、責任があるすべての DLP ポリシーとコンテンツ フィルタに対して暗号化プロファイルを使用できます。

ステップ4 [キーサーバー設定（Key Server Settings）] セクションで、[Cisco Secure Email Encryption Service] を選択します。

ステップ5 [Cisco Secure Email Encryption Service] を選択した場合は、ホステッドキーサービスの URL を入力します。キー サービスの URL は、https://res.cisco.com です。

ステップ6 [キーサーバ設定（Key Server Settings）] で [詳細（Advanced）] をクリックし、受信者がエンベロープを開封した場合、エンベロープの暗号化ペイロードの転送に HTTP または HTTPS を使用するかどうかを指定します。次のいずれかを選択してください。

- [キーサービスをHTTPで使用する（Use the Key Service with HTTP）]。受信者がエンベロープを開封すると、HTTP を使用してキー サービスから暗号化ペイロードを転送します。Cisco Secure Email Encryption Service の場合、これはステップ 5 で指定した URL です。
- ペイロードがすでに暗号化されているため、HTTPに転送しても安全であり、HTTPSに送信するよりも迅速です。これは、HTTPS経由でイメージ要求を送信するよりも、パフォーマンスがさらに向上します。
- [キーサービスをHTTPSで使用する（Use the Key Service with HTTPS）]。受信者がエンベロープを開封すると、HTTPS を使用してキー サービスから暗号化ペイロードを転送します。Cisco Secure Email Encryption Service の場合、これはステップ 5 で指定した URL です。
- [ペイロードトランスポートの個別のURLを指定します（Specify a separate URL for payload transport）]。暗号化ペイロードにキー サーバを使用しない場合は、ペイロード転送には HTTP または HTTPS を使用するかどうかを別の URL を使用して指定できます。

ステップ7 [エンベロープ設定（Envelope Settings）] のセクションで、メッセージのセキュリティ レベルを選択します。

- [セキュリティ（高）（High Security）]。受信者は、暗号化されたメッセージを開封するには、パスフレーズを必ず入力する必要があります。

- [セキュリティ（中）（Medium Security）]。受信者の資格情報がキャッシュされていれば、受信者は暗号化されたメッセージを開封するために資格情報を入力する必要はありません。
- [パスフレーズは不要です（No Passphrase Required）]。暗号化されたメッセージの最も低いセキュリティ レベルです。暗号化されたメッセージを開封するために受信者がパスフレーズを入力する必要はありません。それでも、パスフレーズ保護されないエンベロープの [開封確認（Read Receipts）]、[全員への安全な返信（Secure Reply All）]、および [メッセージの安全な転送（Secure Message Forwarding）] 機能を有効にできます。

ステップ 8 ユーザが組織のロゴをクリックするとその組織の URL が開くようにするように、ロゴのリンクを追加できます。次のオプションから選択します。

- **[リンクなし（No link）]。**実際のリンクは、メッセージエンベロープに追加されません。
- [カスタムリンクURL（Custom link URL）]。URL を入力し、メッセージ エンベロープへの実際のリンクを追加します。

ステップ 9 （任意）開封確認をイネーブルにします。このオプションをイネーブルにすると、受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。

ステップ 10 （任意）次の設定を行うために、任意で [エンベロープ設定（Envelope Settings）] の [詳細設定（Advanced）] をクリックしてください。

- 暗号化キューにあるメッセージがタイムアウトするまでの時間（秒単位）を入力します。メッセージがタイムアウトになると、電子メールゲートウェイはメッセージをバウンスし、送信者に通知を送信します。
- 暗号化アルゴリズム「AES 192」または「AES 256」 を選択します。

  （注） AESは、より強力な暗号化を実現しますが、復号により長い時間がかかるため、受信者には遅延が発生します。AESは、通常、政府や銀行業務のアプリケーションで使用されます。

- 復号アプレットをイネーブルまたはディセーブルにします。このオプションをイネーブルにすると、メッセージの添付ファイルがブラウザ環境で開かれるようになります。このオプションをディセーブルにすると、メッセージの添付ファイルがキーサーバで復号されるようになります。ディセーブルの場合、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。

ステップ 11 [メッセージ設定（Message settings）] セクションで、次のようにします。

- 全員へのセキュアな返信機能をイネーブルにするには、[全員にセキュアな返信を有効にする（Enable Secure Reply All）] チェックボックスをオンにします。
- セキュアなメッセージ転送機能をイネーブルにするには、[セキュアなメッセージ転送を有効にする（Enable Secure Message Forwarding）] チェックボックスをオンにします。

ステップ 12 （任意）Cisco Secure Email Encryption Service を選択しており、このサービスでエンベロープのローカリゼーションがサポートされている場合は、エンベロープのローカリゼーションをイ

ネーブルにします。[通知設定（Notification Settings）] セクションで [ローカライズされたエンベロープの使用（Use Localized Envelope）] チェックボックスをオンにします。

（注） エンベロープのローカリゼーションをイネーブルにすると、暗号化されたメッセージの HTML またはテキストによる通知を選択できません。

エンベロープのデフォルト ロケールを設定する場合は、エンベロープのデフォルト ロケールの設定 （670 ページ）を参照してください。

ステップ 13 HTML 形式またはテキスト形式の通知テンプレートを選択します。

（注） キー サーバは、受信者の電子メール アプリケーションによって、HTML またはテキスト形式の通知を使います。両方の通知を設定する必要があります。

次の手順を実行します。

a) HTML 形式の通知テンプレートを選択します。テキスト リソースで設定した HTML 形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。

b) テキスト形式の通知テンプレートを選択します。テキストリソースで設定したテキスト形式の通知から選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。

（注） これらのオプションは、ローカライズされたエンベロープを使用している場合には使用できません。

ステップ 14 暗号化失敗通知用の件名ヘッダーを入力します。暗号化プロセスがタイムアウトした場合、電子メールゲートウェイは通知を送信します。

ステップ 15 メッセージ本文の暗号化失敗通知テンプレートを選択します。テキストリソースで設定した暗号化失敗通知テンプレートから選択します。テンプレートが設定されていなかった場合、システムはデフォルトのテンプレートを使用します。

ステップ 16 変更を送信し、保存します。

ステップ 17 Cisco Registered Envelope Service を使用する場合、電子メールゲートウェイをプロビジョニングする手順を追加で実行する必要があります。電子メールゲートウェイをプロビジョニングすると、暗号化プロファイルがホステッドキーサービスと共に登録されます。電子メールゲートウェイをプロビジョニングするには、登録する暗号化プロファイルの [プロビジョニング（Provision）] ボタンをクリックします。

エンベロープのデフォルト ロケールの設定

エンベロープのデフォルト ロケールは英語です。[Cisco Secure Email Encryption Service] を選択しており、このサービスでエンベロープのローカリゼーションがサポートされている場合は、エンベロープのロケールを次のいずれかに変更できます。

- 英語
- フランス語

- ドイツ語
- 日本語
- ポルトガル語
- スペイン語
- イタリア語
- 韓国語
- オランダ語
- ポーランド語
- ロシア語
- 中国語

はじめる前に

- キーサービスタイプとして Cisco Secure Email Encryption Service を使用し、エンベロープのローカリゼーションがイネーブルな状態で、暗号化プロファイルを作成します。キーサービスによる暗号化メッセージの処理方法の設定（667ページ）を参照してください。
- Cisco Secure Email Encryption Service でエンベロープのローカリゼーションがサポートされていることを確認します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [Cisco IronPort電子メール暗号化（Cisco IronPort Email Encryption）] をクリックします。

ステップ 2 既存の暗号化プロファイルを開きます。

ステップ 3 [通知設定（Notification Settings）] セクションの [ローカライズされたエンベロープ（Localized Envelopes）] ドロップダウンリストからロケールを選択します。

ステップ 4 **[送信（Submit）]** をクリックします。

ステップ 5 [変更を確定（Commit Changes）] をクリックします。

PXE エンジンの最新バージョンへの更新

[Ciscoメール暗号化設定（Cisco Email Encryption Settings）] ページには、PXE エンジンの現在のバージョンおよび電子メールゲートウェイで使用するドメインマッピングファイルが表示されます。[セキュリティサービス（Security Services）] > [サービスアップデート（Service Updates）] ページ（または CLI の updateconfig コマンド）を使って、自動的に PXE エンジンを更新するように電子メールゲートウェイを設定できます。詳細については、サービス アップデート （1253 ページ）を参照してください。

また、[IronPortメール暗号化設定（IronPort Email Encryption Settings）] ページの [PXEエンジンの更新（PXE Engine Updates）] セクションの [今すぐ更新（Update Now）] ボタン（またはCLIの**encryptionupdate**コマンド）を使用して、手動でエンジンを更新することもできます。

暗号化するメッセージの決定

暗号化プロファイルの作成後、どの電子メールメッセージを暗号化すべきかを決める発信コンテンツフィルタを作成する必要があります。コンテンツフィルタは、発信電子メールをスキャンしてメッセージが指定された条件に一致するか判断します。コンテンツフィルタによりメッセージが条件に一致すると判断されたら、電子メールゲートウェイはメッセージを暗号化し、生成されたキーをキーサーバに送信します。このアプライアンスは、使用するキーサーバを決定するための、暗号化プロファイルで指定された設定と、他の暗号化設定を使用します。

データ漏洩防止スキャン後に解放された後でも、メッセージを暗号化できます。詳細については、DLP違反アクション（メッセージアクション）に対して実行するアクションの定義 （651ページ）を参照してください。

関連項目

- TLS 接続を暗号化の代わりに使用 （672 ページ）
- コンテンツ フィルタを使用したメッセージの暗号化と即時配信 （673 ページ）
- コンテンツ フィルタを使用した配信時のメッセージの暗号化 （674 ページ）

TLS 接続を暗号化の代わりに使用

ドメイン用に指定された送信先コントロールに基づき、電子メールゲートウェイは、メッセージを暗号化する代わりに TLS 接続を介してメッセージをセキュアにリレーできます（TLS 接続が使用可能な場合）。電子メールゲートウェイは、送信先コントロール（必須（Required）、推奨（Preferred）、またはなし（None））の TLS 設定と暗号化コンテンツフィルタで定義されたアクションに基づいて、メッセージを暗号化するか TLS 接続で送信するか決定します。

コンテンツ フィルタ作成時に、必ずメッセージを暗号化するか、まず TLS 接続で送信を試みて、TLS接続が使用不可であればメッセージを暗号化するかを指定できます。次の表では、暗号化制御フィルタが最初に TLS 接続でのメッセージの送信を試みる場合、 電子メールゲートウェイが、ドメインの送信先コントロールの TLS 設定に基づいてどのようにメッセージを送信するかを示しています。

表 *44 :* 電子メールゲートウェイの *TLS* サポート

送信先コントロール TLS 設定	TLS接続が使用可能である場合のアクション	TLS 接続が使用不可である場合のアクション
なし	エンベロープを暗号化して送信します。	エンベロープを暗号化して送信します。

送信先コントロール TLS 設定	TLS 接続が使用可能である場合のアクション	TLS 接続が使用不可である場合のアクション
TLS 推奨	TLS 経由で送信します。	エンベロープを暗号化して送信します。
TLS 必須	TLS 経由で送信します。	リトライまたはメッセージのバウンス

送信先コントロールで TLS をイネーブルにする方法については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

コンテンツ フィルタを使用したメッセージの暗号化と即時配信

はじめる前に

- コンテンツ フィルタを構築するための条件の概念を理解するには、コンテンツ フィルタの概要 （325 ページ）を参照してください。
- （任意）メッセージへの暗号化ヘッダーの挿入 （675 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [発信コンテンツフィルタ（Outgoing Content Filters）] に移動します。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。

ステップ 5 [OK] をクリックします。

ステップ 6 任意で、[アクションを追加（Add Action）] をクリックし、[ヘッダーの追加（Add Header）] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

ステップ 7 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックします。

ステップ 8 [アクションを追加（Add Action）] リストから [暗号化して今すぐ配信(最終アクション)（Encrypt and Deliver Now (Final Action)）] を選択します。

ステップ 9 条件に合致するメッセージを常に暗号化するか、TLS 接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。

ステップ 10 コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。

暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

ステップ 11 メッセージの件名を入力します。

ステップ 12 [OK] をクリックします。

次の図のコンテンツ フィルタは、メッセージ本文で ABA コンテンツを検索するコンテンツ フィルタを示します。コンテンツ フィルタで定義されているアクションは、電子メールを暗号化して配信すると指定しています。

図 *35*：暗号化コンテンツ フィルタ

ステップ 13 暗号化アクションを追加した後、[送信（Submit）] をクリックします。

ステップ 14 変更を保存します。

次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、メール ポリシーの概要 （309 ページ）を参照してください。

コンテンツ フィルタを使用した配信時のメッセージの暗号化

配信時にメッセージを暗号化するコンテンツ フィルタを作成するには、次の手順に従ってください。配信時の暗号化とは、メッセージが次の処理の段階に進み、すべての処理が完了した時点で、メッセージが暗号化され、配信されることを意味します。

はじめる前に

- コンテンツ フィルタを構築するための条件の概念を理解するには、コンテンツ フィルタの概要 （325 ページ）を参照してください。
- （任意）メッセージへの暗号化ヘッダーの挿入 （675 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [発信コンテンツフィルタ（Outgoing Content Filters）] に移動します。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 暗号化するメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。

ステップ 5 [OK] をクリックします。

ステップ 6 任意で、[アクションを追加（Add Action）] をクリックし、[ヘッダーの追加（Add Header）] を選択し、追加の暗号化設定を指定する暗号化ヘッダーをメッセージに挿入します。

ステップ 7 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックします。

ステップ 8 [アクションを追加（Add Action）] リストから [配信時の暗号化（Encrypt on Delivery）] を選択します。

ステップ 9 条件に合致するメッセージを常に暗号化するか、TLS接続を介した送信の試行が失敗したときのみメッセージを暗号化するかを選択します。

ステップ 10 コンテンツ フィルタに関連付ける暗号化プロファイルを選択します。

暗号化プロファイルは、使用するキー サーバ、セキュリティ レベル、およびメッセージ エンベロープのフォーマット化に関する設定、および他のメッセージ設定を指定します。暗号化プロファイルをコンテンツ フィルタに関連付けた場合、コンテンツ フィルタはこれらの格納された設定を暗号化メッセージに使用します。

ステップ 11 メッセージの件名を入力します。

ステップ 12 [OK] をクリックします。

ステップ 13 暗号化アクションを追加した後、[送信（Submit）] をクリックします。

ステップ 14 変更を保存します。

次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、メール ポリシーの概要 （309 ページ）を参照してください。

メッセージへの暗号化ヘッダーの挿入

AsyncOS では、コンテンツ フィルタまたはメッセージ フィルタを使って SMTP ヘッダーをメッセージに挿入することで、暗号化設定をメッセージに追加できます。暗号化ヘッダーは、関連

付けられた暗号化プロファイルで定義されている暗号化設定を上書きすることが可能で、指定された暗号化機能をメッセージに適用できます。

（注） Cisco 暗号化アプライアンスはフラグ付きのメッセージを処理するように設定する必要があります。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[発信コンテンツフィルタ（Outgoing Content Filters）] または [受信コンテンツフィルタ（Incoming Content Filters）] に進みます。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックして [ヘッダーの追加/編集（ヘッダーの追加/編集）] を選択し、追加の暗号化設定を指定するためにメッセージに暗号化ヘッダーを挿入します。

たとえば、Registered Envelope を送信後 24 時間で期限切れにする場合は、ヘッダー名として X-PostX-ExpirationDate、ヘッダーの値として +24:00:00 を入力します。

次のタスク

関連項目

- 暗号化ヘッダー （676 ページ）
- 暗号化ヘッダーの例 （678 ページ）
- 暗号化コンテンツ フィルタの作成の詳細については、コンテンツ フィルタを使用したメッセージの暗号化と即時配信 （673 ページ）を参照してください。
- メッセージ フィルタを使用したヘッダー挿入については、メッセージ フィルタを使用した電子メール ポリシーの適用 （155 ページ）を参照してください。

暗号化ヘッダー

次の表に、メッセージに追加可能な暗号化ヘッダーを示します。

表 *45*：電子メール暗号化ヘッダー

MIME ヘッダー	説明	値
`X-PostX-Reply- Enabled`	メッセージで安全な返信をイネーブルにするかを示し、メッセージ バーに [返信（Reply）] ボタンを表示します。このヘッダーは、メッセージに暗号化設定を追加します。	[返信（Reply）] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。

MIME ヘッダー	説明	値
X-PostX-Reply-All-Enabled	メッセージで安全な「全員に返信」をイネーブルにするかを示し、メッセージバーに[全員に返信（Reply All）] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[全員に返信（Reply All）] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。
X-PostX-Forward-Enabled	メッセージの安全な転送をイネーブルにするかを示し、メッセージ バーに [転送（Forward）] ボタンを表示します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	[転送（Forward）] ボタンを表示または非表示にするかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。
X-PostX-Send-Return-Receipt	開封確認をイネーブルにするかを示します。受信者が安全なエンベロープを開くと、送信者は開封確認を受信します。このヘッダーは、デフォルトのプロファイル設定を上書きします。	開封確認を送信するかしないかを示すブール値。true に設定するとボタンを表示します。デ フォルト値は true です。
X-PostX-Expiration Date	送信前に Registered Envelope の有効期限の日付を設定します。有効期限後は、キー サーバにより Registered Envelope へのアクセスが制限されます。Registered Envelope は、メッセージの期限が切れたというメッセージを表示します。このヘッダーは、メッセージに暗号化設定を追加します。 Cisco Registered Envelope Service を使用している場合、メッセージ送信後に http://res.cisco.com の Web サイトにログインして、メッセージ管理機能でメッセージの有効期限を設定、調整、削除できます。	相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。
X-PostX-ReadNotification Date	送信前に Registered Envelope の「開封期限」の日付を設定します。Registered Envelope がこの期限までに読まれなかった場合、ローカル キー サーバは通知を生成します。このヘッダーを持つ Registered Envelope は、Cisco Registered Envelope Service では機能せず、ローカル キー サーバでのみ機能します。このヘッダーは、メッセージに暗号化設定を追加します。	相対的な日付や時間を含む文字列値。相対的な時間、分、秒には +HH:MM:SS 形式、相対的な日付には +D 形式を使います。デフォルトでは、有効期限はありません。

MIME ヘッダー	説明	値
X-PostX-Suppress-Applet-For-Open	復号アプレットをディセーブルにするかしないかを示します。復号アプレットにより、ブラウザ環境でメッセージの添付ファイルが開かれます。アプレットをディセーブルにすると、メッセージの添付ファイルはキー サーバで復号されます。このオプションをディセーブルにすると、メッセージの開封により時間がかかるようになりますが、ブラウザ環境に依存しなくなります。このヘッダーは、デフォルトのプロファイル設定を上書きします。	復号アプレットをディセーブルにするかしないかのブール値。アプレットをディセーブルにするには true に設定します。デ フォルト値は true です。
X-PostX-Use-Script	JavaScript を含まないエンベロープを送信するかしないかを示します。JavaScript を含まないエンベロープとは、受信者のコンピュータ上でエンベロープをローカルに開封するために使われる JavaScript を含まない Registered Envelope のことです。受信者は、メッセージを見るには Open Online メソッド、または Open by Forwarding メソッドのいずれかを使用する必要があります。受信者のドメインのゲートウェイにより JavaScript が削除され、暗号化されたメッセージを開封できない場合、このヘッダーを使います。このヘッダーはメッセージに暗号化設定を追加します。	JavaScript アプレットを含めるか含めないかのブール値。JavaScript を含まないエンベロープを送信するには、false に設定します。デフォルト値は true です。
X-PostX-Remember-Envelope-Key-Checkbox	オフラインでエンベロープを開封するため、エンベロープ固有のキーのキャッシュを許可するかしないかを示します。エンベロープ キーのキャッシングでは、受信者が正しいパスフレーズを入力し、[このエンベロープのパスワードを記憶する（Remember the password for this envelope）] チェックボックスをオンにした場合、個別のエンベロープの復号キーが受信者のコンピュータでキャッシュされます。これ以降、受信者はそのコンピュータでエンベロープを再開封するためにパスフレーズをもう一度入力する必要はありません。このヘッダーは、メッセージに暗号化設定を追加します。	エンベロープ キーのキャッシュをイネーブルにするか、[このエンベロープのパスワードを記憶する（Remember the password for this envelope）] チェックボックスを表示するかしないかのブール値。デ フォルト値は true です。

暗号化ヘッダーの例

この項では、暗号化ヘッダーの例を示します。

関連項目

- JavaScript を含まないエンベロープのイネーブル化 （679 ページ）
- オフラインでの開封のためエンベロープ キーをイネーブルにする （679 ページ）
- メッセージ有効期限のイネーブル化 （679 ページ）
- 復号アプレットの無効化 （679 ページ）

オフラインでの開封のためエンベロープ キーをイネーブルにする

エンベロープ キーのキャッシュをイネーブルにして Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

[このエンベロープのパスワードを記憶する（Remember the password for this envelope）] チェックボックスが Registered Envelope に表示されます。

JavaScript を含まないエンベロープのイネーブル化

JavaScript を含めずに Registered Envelope を送信するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Use-Script: false
```

受信者が securedoc.html 添付ファイルを開くと、Registered Envelope が [オンラインで開く（Open Online）] リンクと共に表示され、[開く（Open）] ボタンがディセーブルになります。

メッセージ有効期限のイネーブル化

送信後、24 時間で有効期限が切れるようにメッセージを設定するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-ExpirationDate: +24:00:00
```

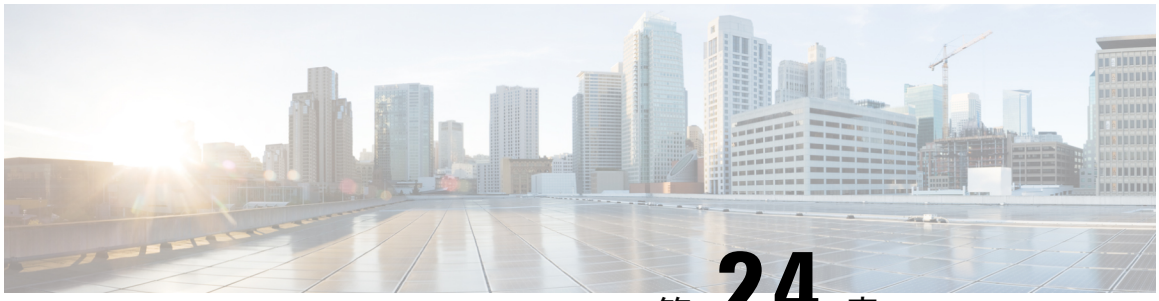
送信後 24 時間は、受信者はその暗号化されたメッセージを開封して内容を見ることができます。それ以降、Registered Envelope では、エンベロープの有効期限が切れたことを示すメッセージが表示されます。

復号アプレットの無効化

復号アプレットをディセーブルにし、メッセージの添付ファイルをキー サーバで復号するには、次のヘッダーをメッセージに挿入します。

```
X-PostX-Suppress-Applet-For-Open: true
```

（注） 復号アプレットをディセーブルにしている場合、メッセージの開封には時間がかかりますが、ブラウザ環境には依存しなくなります。



第 24 章

S/MIME セキュリティ サービス

この章は、次の項で構成されています。

- S/MIME セキュリティ サービスの概要 （681 ページ）
- 電子メールゲートウェイでの S/MIME セキュリティサービス （682 ページ）
- S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化 （685 ページ）
- S/MIME を使用した着信メッセージの検証、復号、または復号と検証 （698 ページ）
- S/MIME 証明書の要件 （704 ページ）
- 公開キーの管理 （706 ページ）

S/MIME セキュリティ サービスの概要

Secure/Multipurpose Internet Mail Extensions（S/MIME）は、安全な検証済みの電子メール メッセージを送受信するための標準ベースの方式です。S/MIME では、公開/秘密キーのペアを使用してメッセージを暗号化または署名します。この方法により、

- メッセージが暗号化されている場合、メッセージ受信者のみが暗号化されたメッセージを開くことができます。
- メッセージが署名されている場合、メッセージ受信者は送信者のドメインのアイデンティティを検証して、転送中にメッセージが変更されていないことを確信できます。

S/MIME の詳細については、次の RFC を確認してください。

- RFC 5750：Secure/Multipurpose Internet Mail Extensions（S/MIME）Version 3.2 - Certificate Handling
- RFC 5751：Secure/Multipurpose Internet Mail Extensions（S/MIME）Version 3.2 - Message Specification
- RFC 3369：Cryptographic Message Syntax

電子メールゲートウェイでの S/MIME セキュリティサービス

組織では、すべてのエンドユーザが独自の証明書を所有していなくても、S/MIMEを使用して安全に通信したいと考えています。このような組織に対して電子メールゲートウェイは、個々のユーザではなく組織を識別する証明書を使用して、ゲートウェイレベルでS/MIMEセキュリティサービス（署名、暗号化、検証および復号）をサポートします。

電子メールゲートウェイは、Business-to-Business（B2B）および Business-to-Consumer（B2C）シナリオに次の S/MIME セキュリティサービスを提供します。

- S/MIME を使用したメッセージの署名、暗号化、または署名と暗号化S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化（685ページ）を参照してください。
- S/MIME を使用したメッセージの検証、復号、または復号と検証S/MIME を使用した着信メッセージの検証、復号、または復号と検証 （698 ページ） を参照してください。

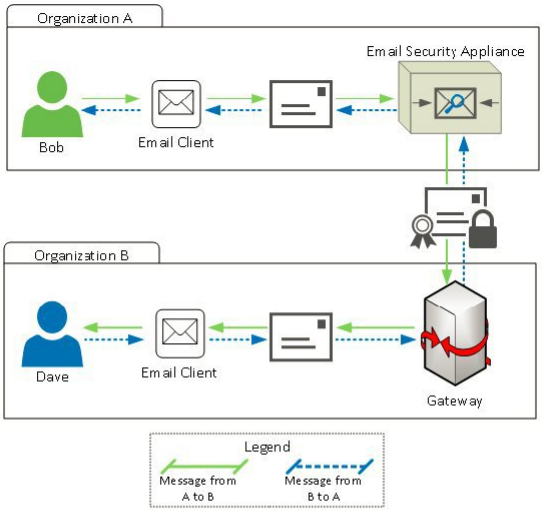
関連項目

- S/MIME セキュリティ サービスのしくみについて （682 ページ）

S/MIME セキュリティ サービスのしくみについて

- シナリオ：Business-to-Business（B2B） （683 ページ）
- シナリオ：Business-to-Consumer （684 ページ）

シナリオ：Business-to-Business（B2B）



企業 A と B は、両社の間でやり取りするすべてのメッセージを、S/MIME を使用して署名および暗号化したいと考えています。企業 A は、ゲートウェイ レベルで S/MIME セキュリティ サービスを実行するように Cisco Secure Email Gateway を設定しています。企業 B は、ゲートウェイ レベルで S/MIME セキュリティ サービスを実行するようにサードパーティ アプリケーションを設定しています。

（注） 現在の例では、企業 B はサードパーティ アプリケーションを使用して S/MIME セキュリティ サービスを実行していると仮定します。実際には、これはゲートウェイ レベルで S/MIME セキュリティサービスを実行できる任意のアプリケーションまたは電子メール ゲートウェイ（ Cisco Secure Email Gateway を含む）になります。

企業 A が企業 B にメッセージを送信：

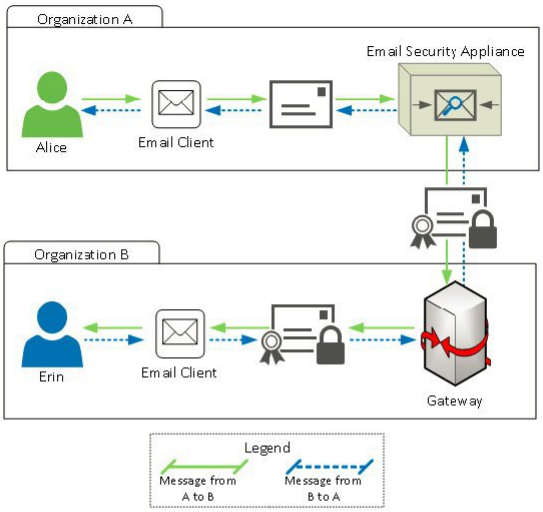
1. Bob（企業 A）は電子メール クライアントを使用して、未署名の暗号化されていないメッセージを Dave（企業 B）に送信します。
2. 企業 A の Cisco Secure Email Gateway は、メッセージを署名および暗号化して企業 B に送信します。

3. 企業Bのゲートウェイで、サードパーティアプリケーションはメッセージを復号および検証します。
4. Dave は暗号化されていない署名付きメッセージを受信します。

企業 B が企業 A にメッセージを送信：

1. Dave（企業B）は電子メール クライアントを使用して、未署名の暗号化されていないメッセージを Bob（企業 A）に送信します。
2. 企業Bのゲートウェイで、サードパーティアプリケーションはメッセージを署名および暗号化して企業 A に送信します。
3. 企業 A の Cisco Secure Email Gateway は、メッセージを復号および検証します。
4. Bob は暗号化されていない署名付きメッセージを受信します。

シナリオ：Business-to-Consumer



企業 A と B は、両社の間でやり取りするすべてのメッセージを、S/MIME を使用して署名および暗号化したいと考えています。企業 A は、ゲートウェイレベルで S/MIME セキュリティサービスを実行するように Cisco Secure Email Gateway を設定しています。企業 B は、すべてのユーザの電子メール クライアントを、S/MIME セキュリティ サービスを実行するように設定しています。

企業 A が企業 B にメッセージを送信：

1. Alice（企業 A）は電子メール クライアントを使用して、未署名の暗号化されていないメッセージを Erin（企業 B）に送信します。
2. 企業 A の Secure Email Gateway は、メッセージを署名および暗号化して企業 B に送信します。
3. 企業 B の電子メール クライアントは、メッセージを復号および検証して Erin に表示します。

企業 B が企業 A にメッセージを送信：

1. Erin（企業 B）は電子メール クライアントを使用し、メッセージを署名および暗号化して Alice（企業 A）に送信します。
2. 企業 A の Secure Email Gateway は、メッセージを復号および検証します。
3. Alice は暗号化されていない未署名のメッセージを受信します。

S/MIME を使用した発信メッセージの署名、暗号化、または署名と暗号化

- 電子メールゲートウェイでの S/MIME 署名および暗号化ワークフロー （685 ページ）
- S/MIME を使用して発信メッセージの署名、暗号化、または署名と暗号化を行う方法 （686 ページ）
- S/MIME 署名用の証明書の設定 （688 ページ）
- S/MIME 暗号化用の公開キーの設定 （691 ページ）
- S/MIME 送信プロファイルの管理 （693 ページ）
- 署名、暗号化、または署名と暗号化を行うメッセージの決定 （696 ページ）
- コンテンツ フィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信 （696 ページ）
- コンテンツ フィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化 （697 ページ）

（注） 電子メールゲートウェイを使用して、発信および着信メッセージの署名、暗号化、および署名と暗号化を行うことができます。

電子メールゲートウェイでの S/MIME 署名および暗号化ワークフロー

- S/MIME 署名ワークフロー （686 ページ）
- S/MIME 暗号化ワークフロー （686 ページ）

S/MIME 署名ワークフロー

次のプロセスでは、電子メールゲートウェイでS/MIME署名を実行する方法について説明します。

1. メッセージにハッシュアルゴリズムを適用して、メッセージダイジェストを作成します。
2. 電子メールゲートウェイの S/MIME 証明書の秘密キーを使用して、メッセージダイジェストを暗号化します。
3. 暗号化されたメッセージダイジェストおよび電子メールゲートウェイの S/MIME 証明書の公開キーを使用して、PKCS7 署名を作成します。
4. メッセージに PKCS7 署名を添付して、メッセージに署名します。
5. 署名されたメッセージを受信者に送信します。

S/MIME 暗号化ワークフロー

次のプロセスでは、電子メールゲートウェイでS/MIME暗号化を実行する方法について説明します。

1. 疑似乱数セッション キーを作成します。
2. セッション キーを使用してメッセージ本文を暗号化します。
3. 受信者（ゲートウェイまたはコンシューマ）の S/MIME 証明書の公開キーを使用して、セッション キーを暗号化します。
4. 暗号化されたセッション キーをメッセージに添付します。
5. 暗号化されたメッセージを受信者に送信します。

（注） 電子メールゲートウェイで PXE 暗号化と S/MIME 暗号化が有効になっている場合、まず S/MIME を使用して、次に PXE を使用してメッセージが暗号化されます。

S/MIME を使用して発信メッセージの署名、暗号化、または署名と暗号化を行う方法

手順	操作手順	詳細
ステップ 1	S/MIME 証明書の要件を把握します。	S/MIME 証明書の要件 （704 ページ）を参照してください。

手順	操作手順	詳細
ステップ 2	要件に応じて、次のいずれかを実行します。 • S/MIME 署名の場合、S/MIME 署名証明書を設定します。 • S/MIME 暗号化の場合、受信者の S/MIME 証明書の公開キーを設定します。 • S/MIME 署名および暗号化の場合、S/MIME 署名証明書と受信者の S/MIME 証明書の公開キーをそれぞれ設定します。	参照先： • S/MIME 署名用の証明書の設定（688 ページ） • S/MIME 暗号化用の公開キーの設定 （691 ページ）
ステップ 3	メッセージの署名、暗号化、または署名と暗号化を行うためのプロファイルを作成します。	メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成 （694 ページ）を参照してください。
ステップ 4	電子メールゲートウェイでメッセージの署名、暗号化、または署名と暗号化を行うために、メッセージが満たすべき条件を定義します。	署名、暗号化、または署名と暗号化を行うメッセージの決定 （696 ページ）を参照してください。
ステップ 5	電子メールのワーク フローでいつメッセージの署名、暗号化、または署名と暗号化を行うかを決定します。	参照先： • コンテンツ フィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信 （696 ページ） • コンテンツ フィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化 （697 ページ）
ステップ 6	メッセージを署名または暗号化するユーザ グループを定義します。	メール ポリシーを作成します。 メール ポリシー （309 ページ）を参照してください
ステップ 7	定義した署名または暗号化アクションを、定義したユーザ グループに関連付けます。	メール ポリシーにコンテンツ フィルタを関連付けます。 メール ポリシー （309 ページ）を参照してください

（注） CLI を使用して S/MIME 署名、暗号化、または署名と暗号化を実行する場合は、**smimeconfig** コマンドを使用します。『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

S/MIME 署名用の証明書の設定

メッセージに署名するための S/MIME 証明書を設定する必要があります。電子メールゲートウェイでは、次のいずれかの方法を使用して S/MIME 署名証明書を設定できます。

- 電子メールゲートウェイを使用して自己署名 S/MIME 証明書を作成します。自己署名 S/MIME 証明書の作成 （688 ページ）を参照してください。
- 既存の S/MIME 証明書を電子メールゲートウェイにインポートします。S/MIME 署名証明書のインポート （690 ページ）を参照してください。

（注） 署名されたメッセージを企業内のユーザに送信、またはテスト環境で送信するには、自己署名 S/MIME 証明書を使用することが推奨されます。署名されたメッセージを外部ユーザに送信、または実稼働環境で送信するには、信頼できる CA から取得した有効な S/MIME 証明書を使用します。

S/MIME の証明書要件については、S/MIME 証明書の要件 （704 ページ）を参照してください。

自己署名 S/MIME 証明書の作成

Web インターフェイスまたは CLI を使用して、RFC 5750（Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 - Certificate Handling）に準拠する自己署名 S/MIME 証明書を生成できます。

（注） 署名されたメッセージを企業内のユーザに送信、またはテスト環境で送信するには、自己署名 S/MIME 証明書を使用することが推奨されます。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] をクリックします。

ステップ 2 [証明書の追加（Add Certificate）] をクリックします。

ステップ 3 [自己署名S/MIME証明書の作成（Create Self-Signed S/MIME Certificate）] を選択します。

ステップ 4 自己署名証明書に、次の情報を入力します。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
サブジェクトの別名（ドメイン）	このフィールドを設定した場合、指定したドメインのユーザは署名されたメッセージを送信できます。 署名されたメッセージの送信元のドメイン名。たとえば、domain.com や *.domain.net などです。複数エントリの場合、カンマ区切りリストを使用します。
サブジェクトの別名（E メール）	このフィールドを設定した場合、指定したユーザのみが署名されたメッセージを送信できます。 署名されたメッセージを送信するユーザの電子メール アドレス（例：user@somedomain.com）。複数エントリの場合、カンマ区切りリストを使用します。
秘密キーサイズ	証明書署名要求（CSR）を生成する秘密キーのサイズ。

（注） S/MIME署名証明書には、サブジェクトの別名（ドメイン）とサブジェクトの別名（E メール）の両方を含めることができます。

ステップ 5 [次へ（Next）] をクリックして、証明書および署名情報を確認します。

ステップ 6 要件に応じて、次を実行します。

- [FQDN検証（FQDN Validation）] チェックボックスをオンにすると、証明書に存在する [共通名（Common Name）] フィールド、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式であるかどうかを電子メールゲートウェイで確認できます。
- 証明書の名前を入力します。
- 自己署名証明書の CSR を認証局に送信する場合、[証明書署名要求をダウンロード（Download Certificate Signing Request）] をクリックしてローカルまたはネットワーク マシンに PEM 形式で CSR を保存します。

ステップ 7 変更を送信し、保存します。

次のタスク

（注） CLI を使用して自己署名 S/MIME 証明書を生成するには、**certconfig** コマンドを使用します。

S/MIME 署名証明書のインポート

メッセージに署名するための S/MIME 証明書がすでにある場合、インポートして電子メールゲートウェイに追加できます。

はじめる前に

インポートする S/MIME 証明書が、S/MIME 証明書の要件 （704 ページ）に記載されている要件を満たしていることを確認します。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] をクリックします。

ステップ 2 [証明書の追加（Add Certificate）] をクリックします。

ステップ 3 [証明書のインポート（Import Certificate）] を選択します。

ステップ 4 ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。

ステップ 5 ファイルのパスフレーズを入力します。

ステップ 6 [次へ（Next）] をクリックして証明書の情報を表示します。

ステップ 7 （任意）**[FQDN検証（FQDN Validation）]** チェックボックスをオンにして、証明書にある [共通名（Common Name）] フィールド、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式であるかどうかを確認できるようにします。

ステップ 8 証明書の名前を入力します。

ステップ 9 変更を送信し、保存します。

次のタスク

（注） CLI を使用して S/MIME 証明書をインポートするには、**certconfig** コマンドを使用します。

S/MIME 暗号化用の公開キーの設定

メッセージを暗号化するには、受信者のS/MIME証明書の公開キーを電子メールゲートウェイに追加する必要があります。組織のポリシーおよびプロセスに応じて、次のいずれかの方法を使用して公開キーを電子メールゲートウェイに追加できます。

- 受信者に、電子メールなどの電子チャネルを使用して公開キーを送信するよう要求します。その後、Web インターフェイスまたは CLI を使用して公開キーを追加できます。

  公開キーを追加する手順については、S/MIME 暗号化用の公開キーの追加 （691 ページ）を参照してください。

- WebインターフェイスまたはCLIを使用して公開キーの収集をイネーブルにし、受信者に署名されたメッセージを送信するよう要求します。Eメールセキュリティ電子メールゲートウェイは、署名されたメッセージから公開キーを収集できます。

  署名された着信メッセージから公開キーを収集する方法については、公開キーの収集 （692 ページ）を参照してください。

S/MIME 暗号化用の公開キーの追加

はじめる前に

- 公開キーがS/MIME 証明書の要件 （704 ページ）に説明されている要件を満たしていることを確認します。
- 公開キーが PEM 形式であることを確認します。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [公開キー（Public Keys）] をクリックします。
ステップ 2 [公開キーを追加（Add Public Key）] をクリックします。
ステップ 3 公開キーの名前を入力します。
ステップ 4 公開キーを入力します。
ステップ 5 変更を送信し、保存します。

次のタスク

（注） CLI を使用して公開キーを追加するには、**smimeconfig** コマンドを使用します。

S/MIME 収集済み公開キー

公開キーを着信S/MIME署名済みメッセージから取得（収集）し、収集したキーを使用して暗号化済みメッセージを収集したキーの所有者（ビジネスまたはコンシューマ）に送信するように、電子メールゲートウェイを設定できます。

公開キーの収集は、メール フロー ポリシーでイネーブルにできます。収集したすべての公開キーは、[S/MIME収集済み公開キー（S/MIME Harvested Public Key）]ページに表示されます。

関連項目

- 公開キーの収集 （692 ページ）

公開キーの収集

公開キーを着信S/MIME署名済みメッセージから取得（収集）し、これを使用して暗号化済みメッセージを収集したキーの所有者（ビジネスまたはコンシューマ）に送信するように、電子メールゲートウェイを設定できます。

（注） デフォルトでは、期限切れまたは自己署名S/MIME証明書の公開キーは収集されません。

はじめる前に

送信者の S/MIME 証明書の公開キーが、S/MIME 証明書の要件 （704 ページ）に説明されている要件を満たしていることを確認します。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [メール フロー ポリシー（Mail Flow Policies）] をクリックします。

ステップ 2 新しいメール フロー ポリシーを作成するか、既存のポリシーを変更します。

ステップ 3 [セキュリティサービス（Security Features）] セクションまでスクロールします。

ステップ 4 [S/MIME 公開キーの収集（S/MIME Public Key Harvesting）] で以下を実行します。

- S/MIME 公開キーの収集をイネーブルにします。
- （任意）署名された着信メッセージの検証に失敗した場合、公開キーを収集するかどうかを選択します。
- （任意）更新された公開キーを収集するかどうかを選択します。

（注） 48時間以内に同じドメインまたはメッセージから複数の更新された公開キーを受信すると、電子メールゲートウェイは警告アラートを送信します。

ステップ 5 変更を送信し、保存します。

次のタスク

（注） 電子メールゲートウェイ上の、収集された公開キーのリポジトリのサイズは 512 MB です。リポジトリが一杯になると、電子メールゲートウェイにより未使用の公開キーが自動的に削除されます。

CLI を使用してキーの収集をイネーブルにするには、**listenerconfig** コマンドを使用します。

次のステップ

署名されたメッセージを電子メールゲートウェイの管理者に送信するよう、受信者に要求します。電子メールゲートウェイは、署名されたメッセージから公開キーを収集し、[メールポリシー（Mail Policies）] > [収集済み公開キー（Harvested Public Keys）] ページに表示します。

関連項目

- S/MIME 収集済み公開キー （692 ページ）

S/MIME 送信プロファイルの管理

S/MIME 送信プロファイルでは、次のようなパラメータを定義できます。

- 署名、暗号化など、使用する S/MIME モード。
- 署名を行うための S/MIME 証明書
- 不透明、分離など、使用する S/MIME 署名モード。
- 受信者の S/MIME 証明書の公開キーを 電子メールゲートウェイで利用できない場合に実行するアクション。

たとえば、ある組織に送信するメッセージはすべて署名済みである必要があり、別の組織に送信するメッセージはすべて署名済みかつ暗号化済みである必要があるとします。このシナリオでは、署名のみ、および署名および暗号化の2つの送信プロファイルを作成する必要があります。

Web インターフェイスまたは CLI を使用して、S/MIME 送信プロファイルを作成、編集、削除、インポート、エクスポート、および検索できます。

関連項目

- メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成 （694 ページ）
- S/MIME 送信プロファイルの編集 （695 ページ）

メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [送信プロファイル（Sending Profiles）] をクリックします。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 次のフィールドを設定します。

S/MIME プロファイル名	**送信プロファイルの名前を入力します。**
S/MIME モード（S/MIME Mode）	S/MIME モードを選択します。値は次のとおりです。 • **署名** • **暗号化** • **署名/暗号化（Sign/Encrypt）**。署名してから暗号化します • **3 倍（Triple）**。署名、暗号化してから再度署名します （注） [署名（Sign）]、[署名/暗号化（Sign/Encrypt）] または [3 倍（Triple）] のいずれかの S/MIME モードを使用している場合、署名に失敗するとメッセージはバウンスされます。
署名付き証明書（Signing Certificate）	使用する署名付き証明書を選択します。 （注） このフィールドを設定する必要があるのは、[署名（Sign）]、[署名/暗号化（Sign/Encrypt）] または [3 倍（Triple）] のいずれかの S/MIME モードを選択した場合のみです。
S/MIME 署名モード（S/MIME Sign Mode）	S/MIME 署名モードを選択します。値は次のとおりです。 • **不透明（Opaque）**。不透明署名メッセージでは、メッセージと署名が 1 番目の部分に結合されて含められ、署名を検証することでのみ読み取ることができます。 • **分離（Detached）**。署名情報は、署名されるテキストと分離されます。この MIME タイプは 2 番目の部分に application/(x-)pkcs7-mime の MIME サブタイプを持つ multipart/signed です。 （注） このフィールドを設定する必要があるのは、[署名（Sign）]、[署名/暗号化（Sign/Encrypt）] または [3 倍（Triple）] のいずれかの S/MIME モードを選択した場合のみです。

S/MIME プロファイル名	送信プロファイルの名前を入力します。
S/MIME アクション（S/MIME Action）	受信者の公開キーを利用できない場合に 電子メールゲートウェイが実行する必要のあるアクションを選択します。値は次のとおりです。 • **バウンス（Bounce）**。いずれかの受信者の公開キーを利用できない場合、メッセージは送信者にバウンスされます。 • **ドロップ（Drop）**。いずれかの受信者の公開キーを利用できない場合、メッセージはドロップされます。 • **分割（Split）**。メッセージが分割されます。公開キーを利用できない受信者へのメッセージは暗号化されずに配信され、公開キーを利用できる受信者へのメッセージは暗号化されて配信されます。 **例**：bob@example1.com と dave@example2.com にメッセージを送信し、dave@example2.com の公開キーを利用できないとします。このシナリオで [分割（Split）] を選択した場合、 電子メールゲートウェイは次の処理を行います。 • メッセージを暗号化してから bob@example1.com に配信します。 • メッセージを暗号化せずに dave@example2.com に配信します。 （注） このフィールドを設定する必要があるのは、[暗号化（Encrypt）]、[署名/暗号化（Sign/Encrypt）] または [3 倍（Triple）] のいずれかの S/MIME モードを選択した場合のみです。

ステップ 4 変更を送信し、保存します。

次のタスク

（注） CLI を使用して送信プロファイルを作成するには、**smimeconfig** コマンドを使用します。

S/MIME 送信プロファイルの編集

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [送信プロファイル（Sending Profiles）] をクリックします。

ステップ 2 変更する送信プロファイルをクリックします。

ステップ 3 メッセージの署名、暗号化、または署名および暗号化用の S/MIME 送信プロファイルの作成（694 ページ）に説明されているように、フィールドを編集します。

ステップ 4 変更を送信し、保存します。

署名、暗号化、または署名と暗号化を行うメッセージの決定

送信プロファイルを作成したら、署名、暗号化、または署名と暗号化を行うメッセージを決定する発信コンテンツ フィルタを作成する必要があります。コンテンツ フィルタは、発信電子メールをスキャンしてメッセージが指定された条件に一致するか判断します。コンテンツフィルタによってメッセージが条件に一致すると判断されたら、電子メールゲートウェイはメッセージの署名、暗号化、または署名と暗号化を行います。

関連項目

- コンテンツに基づくメッセージのフィルタリング方法 （349 ページ）

コンテンツフィルタを使用したメッセージの署名、暗号化、または署名と暗号化および即時配信

はじめる前に

コンテンツ フィルタの条件を作成する概念を理解します。コンテンツ フィルタの仕組み （325 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [発信コンテンツフィルタ（Outgoing Content Filters）] に移動します。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 署名、暗号化、または署名と暗号化を行うメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックします。

ステップ 7 [アクションを追加（Add Action）] リストから [S/MIME 署名/暗号化（最終アクション）（S/MIME Sign/Encrypt（Final Action））] を選択します。

ステップ 8 コンテンツ フィルタに関連付ける送信プロファイルを選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 変更を送信し、保存します。

次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルト ポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、メール ポリシーの概要 （309 ページ）を参照してください。

コンテンツフィルタを使用した配信時のメッセージの署名、暗号化、または署名と暗号化

配信時にメッセージを署名、暗号化、または署名および暗号化するコンテンツ フィルタを作成します。すなわち、メッセージは次の処理段階に進み、すべての処理が完了したら、メッセージは署名、暗号化、または署名および暗号化されて配信されます。

はじめる前に

- コンテンツ フィルタの条件を作成する概念を理解します。コンテンツ フィルタの概要（325 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [発信コンテンツフィルタ（Outgoing Content Filters）] に移動します。

ステップ 2 [フィルタ（Filters）] セクションで、[フィルタを追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 署名、暗号化、または署名と暗号化を行うメッセージをフィルタリングする条件を追加します。たとえば、機密資料を暗号化するために、件名または本文に特定の単語またはフレーズ（「Confidential」など）を含むメッセージを識別する条件を追加できます。

ステップ 5 [OK] をクリックします。

ステップ 6 [アクション（Actions）] セクションで、[アクションを追加（Add Action）] をクリックします。

ステップ 7 [アクションを追加（Add Action）] リストから [S/MIME 署名/配信時に暗号化（S/MIME Sign/Encrypt on Delivery）] を選択します。

ステップ 8 コンテンツ フィルタに関連付ける送信プロファイルを選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 変更を送信し、保存します。

次のタスク

コンテンツ フィルタを追加したら、フィルタを発信メール ポリシーに追加する必要があります。組織のニーズに応じて、デフォルトポリシーでコンテンツ フィルタをイネーブルにする、またはフィルタを特定のメール ポリシーに適用することを選択します。メール ポリシーの操作については、メール ポリシーの概要 （309 ページ）を参照してください。

S/MIMEを使用した着信メッセージの検証、復号、または復号と検証

- 電子メールゲートウェイでの S/MIME 検証および復号ワークフロー （698 ページ）
- S/MIMEを使用して着信メッセージの検証、復号、または復号と検証を行う方法 （699ページ）
- メッセージを復号するための証明書の設定 （700 ページ）
- 署名されたメッセージを検証するための公開キーの設定 （701 ページ）
- S/MIME 復号および検証のイネーブル化 （703 ページ）
- S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定 （704 ページ）

（注） 電子メールゲートウェイの S/MIME セキュリティサービスを使用して、発信および着信メッセージの検証、復号、または復号と検証を行うことができます。

電子メールゲートウェイでの S/MIME 検証および復号ワークフロー

- S/MIME 検証ワークフロー （698 ページ）
- S/MIME 復号ワークフロー （699 ページ）

S/MIME 検証ワークフロー

次のプロセスでは、電子メールゲートウェイでS/MIME検証を実行する方法について説明します。

1. 署名されたメッセージにハッシュ アルゴリズムを適用して、メッセージ ダイジェストを作成します。
2. 送信者のS/MIME証明書の公開キーを使用し、署名されたメッセージに添付されたPKCS7署名を復号してメッセージ ダイジェストを取得します。
3. 生成されたメッセージ ダイジェストを、署名されたメッセージから取得したメッセージ ダイジェストと比較します。メッセージダイジェストが一致した場合、メッセージは検証されます。
4. 認証局で送信者ドメインの S/MIME 証明書を検証します。

S/MIME 復号ワークフロー

次のプロセスでは、電子メールゲートウェイでS/MIME復号を実行する方法について説明します。

1. 電子メールゲートウェイの S/MIME 証明書の秘密キーを使用して、セッションキーを復号します
2. セッション キーを使用してメッセージ本文を復号します。

S/MIME を使用して着信メッセージの検証、復号、または復号と検証を行う方法

手順	操作手順	詳細
ステップ 1	S/MIME 証明書の要件を把握します。	S/MIME 証明書の要件 （704 ページ）を参照してください。

ステップ 2	要件に応じて、次のいずれかを実行します。
	• S/MIME 復号の場合、組織の S/MIME 証明書（復号の実行に必要な秘密キーを含む）を電子メールゲートウェイに追加します。
	• S/MIME 検証の場合、検証の実行に必要な送信者の S/MIME 証明書の公開キーを電子メールゲートウェイに追加します。
	• S/MIME 復号および検証の場合、以下を電子メールゲートウェイに追加します。
	  • 組織の S/MIME 証明書（復号の実行に必要な秘密キーを含む）を電子メールゲートウェイに追加します。
	  • 送信者ドメインの認証局。
	  • 検証の実行に必要な送信者 S/MIME 証明書の公開キー。
		参照先
		• メッセージを復号するための証明書の設定 （700 ページ）
		• 署名されたメッセージを検証するための公開キーの設定 （701 ページ）
		• カスタム認証局リストのインポート （850 ページ）

ステップ 3	S/MIME を使用して着信メッセージの検証、復号、または復号と検証を行うメール フロー ポリシーを設定します。	S/MIME 復号および検証のイネーブル化（703ページ）を参照してください。
ステップ 4	（任意）電子メールゲートウェイが復号済みまたは検証済みのメッセージに対して実行するアクションを定義します。	S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定（704ページ）を参照してください。

（注） CLI を使用して S/MIME 検証、復号、または復号と検証を実行する場合は、**listenerconfig > hostaccess** コマンドを使用します。詳細については、CLI インライン ヘルプを参照してください。

メッセージを復号するための証明書の設定

組織の S/MIME 証明書（復号の実行に必要な秘密キーを含む）を電子メールゲートウェイに追加する必要があります。

はじめる前に

- 次のいずれかの方法で、電子メールゲートウェイの S/MIME 証明書の公開キーを送信者（ビジネスまたはコンシューマ）と共有します。
  - 電子メールなどの電子チャネルを使用して、公開キーを送信します。
  - キー収集を使用して公開キーを取得するように、送信者に要求します。

  送信者はこの公開キーを使用して、暗号化されたメッセージを電子メールゲートウェイに送信できます。

（注） B2C のシナリオでは、組織の S/MIME 証明書がドメイン証明書の場合、一部の電子メールクライアント（Microsoft Outlook など）は組織の S/MIME 証明書の公開キーを使用して暗号化済みメッセージを送信できないことがあります。これは、これらの電子メールクライアントがドメイン証明書の公開キーを使用した暗号化をサポートしていないためです。

- インポートする S/MIME 証明書が、S/MIME 証明書の要件 （704 ページ）に記載されている要件を満たしていることを確認します。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] をクリックします。
ステップ 2 [証明書の追加（Add Certificate）] をクリックします。
ステップ 3 [証明書のインポート（Import Certificate）] を選択します。
ステップ 4 ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。
ステップ 5 ファイルのパスフレーズを入力します。
ステップ 6 [次へ（Next）] をクリックして証明書の情報を表示します。
ステップ 7 証明書の名前を入力します。

ステップ 8 変更を送信し、保存します。

次のタスク

（注） CLI を使用して S/MIME 証明書を追加するには、**certconfig** コマンドを使用します。

署名されたメッセージを検証するための公開キーの設定

署名されたメッセージを検証するには、送信者の S/MIME 証明書の公開キーを電子メールゲートウェイに追加する必要があります。組織のポリシーおよびプロセスに応じて、次のいずれかの方法を使用して公開キーを電子メールゲートウェイに追加できます。

- 送信者に、電子メールなどの電子チャネルを使用して公開キーを送信するよう要求します。その後、Web インターフェイスまたは CLI を使用して公開キーを追加できます。

  公開キーを追加する手順については、S/MIME 暗号化用の公開キーの追加 （691 ページ）を参照してください。

- キー収集を使用して公開キーを取得します。公開キーの収集 （692 ページ） を参照してください。

S/MIME 検証用の公開キーの追加

はじめる前に

- 公開キーがS/MIME 証明書の要件 （704 ページ）に説明されている要件を満たしていることを確認します。
- 公開キーが PEM 形式であることを確認します。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [公開キー（Public Keys）] をクリックします。
ステップ 2 [公開キーを追加（Add Public Key）] をクリックします。
ステップ 3 公開キーの名前を入力します。
ステップ 4 公開キーを入力します。
ステップ 5 変更を送信し、保存します。

次のタスク

（注） CLI を使用して公開キーを追加するには、**smimeconfig** コマンドを使用します。

S/MIME 検証用の公開キーの収集

公開キーを着信 S/MIME 署名済みメッセージから取得（収集）し、これを使用して収集したキーの所有者（ビジネスまたはコンシューマ）からの署名済みメッセージを検証するように、電子メールゲートウェイを設定できます。

（注） デフォルトでは、期限切れまたは自己署名 S/MIME 証明書の公開キーは収集されません。

1. Web インターフェイスまたは CLI を使用して、公開キーの収集をイネーブルにします。公開キーの収集のイネーブル化 （702 ページ）を参照してください。
2. 送信者に、署名されたメッセージを送信するよう要求します。
3. 収集が完了したら、収集した公開キーを電子メールゲートウェイに追加します。S/MIME 検証用の収集された公開キーの追加 （703 ページ）を参照してください。

この手順により、メッセージは確実にゲートウェイ レベルで検証されます。

公開キーの収集のイネーブル化

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [メール フロー ポリシー（Mail Flow Policies）] をクリックします。

ステップ 2 新しいメール フロー ポリシーを作成するか、既存のポリシーを変更します。

ステップ 3 [セキュリティサービス（Security Features）] セクションまでスクロールします。

ステップ 4 [S/MIME 公開キーの収集（S/MIME Public Key Harvesting）] で以下を実行します。

- S/MIME 公開キーの収集をイネーブルにします。
- （任意）署名された着信メッセージの検証に失敗した場合、公開キーを収集するかどうかを選択します。
- （任意）更新された公開キーを収集するかどうかを選択します。

（注） 48 時間以内に同じドメインまたはメッセージから複数の更新された公開キーを受信すると、電子メールゲートウェイは警告アラートを送信します。

ステップ 5 変更を送信し、保存します。

次のタスク

（注） 電子メールゲートウェイ上の、収集された公開キーのリポジトリのサイズは 512 MB です。リポジトリが一杯になると、電子メールゲートウェイにより未使用の公開キーが自動的に削除されます。

CLI を使用してキーの収集をイネーブルにするには、**listenerconfig** コマンドを使用します。

S/MIME 検証用の収集された公開キーの追加

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [収集済み公開キー（Harvested Public Keys）] をクリックします。

ステップ 2 目的の収集された公開キーをクリックして、公開キーをコピーします。

ステップ 3 公開キーを電子メールゲートウェイに追加します。S/MIME 検証用の公開キーの追加（701 ページ）を参照してください。

ステップ 4 変更を送信し、保存します。

S/MIME 復号および検証のイネーブル化

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [メール フロー ポリシー（Mail Flow Policies）] をクリックします。

ステップ 2 新しいメール フロー ポリシーを作成するか、既存のポリシーを変更します。

ステップ 3 [セキュリティサービス（Security Features）] セクションまでスクロールします。

ステップ 4 [S/MIME の復号/検証（S/MIME Decryption/Verification）] で以下を行います。

- S/MIME 復号および検証をイネーブル化します。
- S/MIME の検証後、デジタル署名を維持するかメッセージから削除するかを選択します。エンド ユーザに S/MIME ゲートウェイ検証について知られたくない場合は、[削除（Remove）] を選択します。

トリプル ラップされたメッセージの場合、内部署名のみが維持または削除されます。

ステップ 5 変更を送信し、保存します。

次のタスク

ヒント S/MIME 復号および検証がメール フロー ポリシーでイネーブルになっている場合、すべてのS/MIMEメッセージは、復号および検証ステータスに関係なく配信されます。S/MIME暗号化済みまたは検証済みメッセージを処理するアクションを設定する場合は、メッセージ フィルタ ルール smime-gateway-verified および smime-gateway を使用できます。詳細については、S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定 （704 ページ）を参照してください。

S/MIME 暗号化済みまたは検証済みメッセージ用のアクションの設定

電子メールゲートウェイでS/MIME復号、検証、またはその両方を実行した後、結果に応じて異なるアクションを行うことできます。メッセージ フィルタ ルール smime-gateway-verified および smime-gateway を使用して、復号、検証、またはその両方の結果に基づいてメッセージに対してアクションを実行できます。詳細については、メッセージフィルタを使用した電子メール ポリシーの適用 （155 ページ）を参照してください。

（注） また、復号または検証、あるいはその両方の結果に基づいたアクションをメッセージで実行するには、コンテンツ フィルタ条件の [S/MIME ゲートウェイ メッセージ（S/MIME Gateway Message）] および [S/MIME ゲートウェイ検証済み（S/MIME Gateway Verified）] も使用できます。詳細については、コンテンツ フィルタ （325 ページ）を参照してください。

例：検証、検証、復号、またはその両方に失敗した S/MIME メッセージの隔離

次のメッセージ フィルタでは、メッセージが S/MIME メッセージであるかどうかを確認し、S/MIME を使用した検証または復号に失敗した場合は隔離します。

```
quarantine_smime_messages:if (smime-gateway-message and not smime-gateway-verified)
{ quarantine("Policy"); }
```

S/MIME 証明書の要件

- 署名のための証明書の要件 （704 ページ）
- 暗号化のための証明書の要件 （705 ページ）

署名のための証明書の要件

署名を行うための S/MIME 証明書には、次の情報を含める必要があります。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
サブジェクトの別名（ドメイン）	署名されたメッセージの送信元のドメイン名。たとえば、domain.com や *.domain.net などです。複数エントリの場合、カンマ区切りリストを使用します。
サブジェクトの別名（E メール）	署名されたメッセージを送信するユーザの電子メールアドレス（例：user@somedomain.com）。複数エントリの場合、カンマ区切りリストを使用します。
秘密キーサイズ	CSR 用に生成する秘密キーのサイズ。
キーの使途	キーの使用状況は、証明書を何に使用できるかを決定する制約方式です。キーの使用状況の拡張が指定されている場合は、digitalSignature および nonRepudiation ビットが設定されている必要があります。 キーの使用状況の拡張が指定されていない場合、受信側クライアントは、digitalSignature および nonRepudiation ビットが設定されていると推定する必要があります。

S/MIME 証明書の詳細については、RFC 5750：Secure/Multipurpose Internet Mail Extensions（S/MIME）Version 3.2 - Certificate Handling を参照してください。

暗号化のための証明書の要件

暗号化を行うための S/MIME 証明書には、次の情報を含める必要があります。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。

共通名	完全修飾ドメイン名
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
サブジェクトの別名（ドメイン）	暗号化されたメッセージの送信先のドメイン名。たとえば、domain.com や *.domain.net などです。複数エントリの場合、カンマ区切りリストを使用します。 暗号化されたメッセージをドメイン内のすべてのユーザに送信する場合は、公開キーに SAN ドメインを含める必要があります。
サブジェクトの別名（E メール）	暗号化されたメッセージを送信するユーザの電子メールアドレス（例：user@somedomain.com）。複数エントリの場合、カンマ区切りリストを使用します。
秘密キーサイズ	CSR 用に生成する秘密キーのサイズ。
キーの使途	キーの使用状況は、証明書を何に使用できるかを決定する制約方式です。キーの使用状況の拡張が指定され、keyEncipherment ビットが設定されている必要があります。

S/MIME 証明書の詳細については、RFC 5750：Secure/Multipurpose Internet Mail Extensions（S/MIME）Version 3.2 - Certificate Handling を参照してください。

公開キーの管理

電子メールゲートウェイでは次が必要です。

- 発信メッセージを暗号化するための、受信者の S/MIME 暗号化証明書の公開キー。
- 署名済み着信メッセージを検証するための、送信者の S/MIME 署名証明書の公開キー。

次のいずれかの方法で、公開キーを電子メールゲートウェイに追加できます。

- 目的の PEM 形式の公開キーがある場合は、Web インターフェイスまたは CLI を使用して追加できます。公開キーの追加 （707 ページ）を参照してください。
- 目的の公開キーが含まれたエクスポートファイルがある場合は、そのエクスポートファイルを /configuration ディレクトリにコピーし、Web インターフェイスまたは CLI を使用してインポートできます。既存のエクスポートファイルからの公開キーのインポート （707 ページ）を参照してください。

電子メールゲートウェイでは、キーの収集もサポートしています（署名済み着信メッセージから自動的に公開キーを取得）。詳細については、S/MIME 収集済み公開キー （692 ページ）を参照してください。

公開キーの追加

はじめる前に

- 公開キーがS/MIME 証明書の要件 （704 ページ）に説明されている要件を満たしていることを確認します。
- 公開キーが PEM 形式であることを確認します。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [公開キー（Public Keys）] をクリックします。
ステップ 2 [公開キーを追加（Add Public Key）] をクリックします。
ステップ 3 公開キーの名前を入力します。
ステップ 4 公開キーを入力します。
ステップ 5 変更を送信し、保存します。

次のタスク

（注） CLI を使用して公開キーを追加するには、**smimeconfig** コマンドを使用します。

既存のエクスポート ファイルからの公開キーのインポート

はじめる前に

エクスポートファイルを電子メールゲートウェイの /configuration ディレクトリにコピーします。エクスポート ファイルを作成する手順については、公開キーのエクスポート （708 ページ）を参照してください。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [公開キー（Public Keys）] をクリックします。
ステップ 2 [公開キーをインポート（Import Public Keys）] をクリックします。
ステップ 3 エクスポート ファイルを選択して [送信（Submit）] をクリックします。

（注） 多数の公開キーを持つファイルをインポートする場合、インポートプロセスに時間がかかることがあります。WebインターフェイスまたはCLI無活動タイムアウトを適宜調整してください。

ステップ 4 変更を保存します。

公開キーのエクスポート

電子メールゲートウェイのすべての公開キーは、1つのテキストファイルにまとめてエクスポートされ、/configuration ディレクトリに保存されます。

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [公開キー（Public Keys）] を選択します。
ステップ 2 [公開キーをエクスポート（Export Public Keys）] をクリックします。
ステップ 3 ファイルの名前を入力し、**[送信（Submit）]** をクリックします。

第 25 章

メールボックスでのメッセージの修復

この章は、次の項で構成されています。

- 概要 （709 ページ）
- ワークフロー （710 ページ）
- メールボックス内のメッセージに対する修復アクションの実行 （714 ページ）
- 電子メールゲートウェイでのメールボックス修復機能の設定 （722 ページ）
- AsyncOS 13.0 以降のリリースへのアップグレード （734 ページ）
- メールボックス修復結果のモニタリング （735 ページ）
- メッセージ トラッキングでのメールボックス修復の詳細の表示 （735 ページ）
- メールボックス修復のトラブルシューティング （735 ページ）

概要

電子メールゲートウェイは、ユーザメールボックスにすでに配信されている悪意のあるメッセージを修復する機能を提供します。電子メールゲートウェイを設定し、次の方法でメッセージを修復できます。

- AMP が電子メールゲートウェイにレトロスペクティブアラートを送信すると、メッセージを自動的に修復する
- メッセージ トラッキング フィルタを使用してメッセージを手動で検索して修正する。

ファイルは常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。AMP は、新しい情報が発生する際にこの変化を識別し、電子メールゲートウェイにレトロスペクティブアラートを送信することができます。脅威判定が変更されたときにユーザのメールボックス内のメッセージに対して自動修復アクションを実行するように電子メールゲートウェイを設定できます。たとえば、添付ファイルに対する判定が「正常」から「悪意がある」に変更されたときには受信者のメールボックスからメッセージを削除するように電子メールゲートウェイを設定することができます。

また、[メッセージトラッキング（Message Tracking）]ページを使用して、ユーザのメールボックスに配信されたメッセージを検索して修正することもできます。[メッセージトラッキング（Message Tracking）]ページは、メールボックスに配信されたすべてのメッセージを対象にし

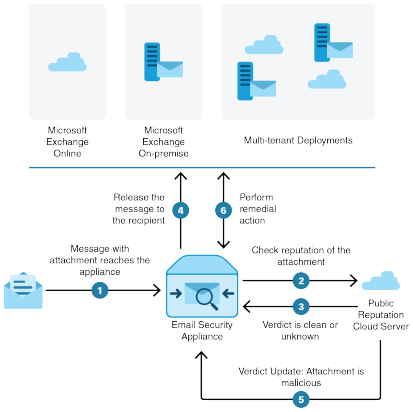
た検索を実行するための統合された場所です。検索結果から修復するメッセージを選択し、そのメッセージに対して実行するアクションを適用できます。

電子メールゲートウェイは、次のメールボックスに展開されたメッセージに対して修復アクション（手動または自動）を実行できます。

- Microsoft Exchange Online：Microsoft Office 365 でホストされたメールボックス
- Microsoft Exchange オンプレミス：ローカルの Microsoft Exchange サーバ
- ハイブリッド/マルチテナント構成：Microsoft Exchange Online 展開および Microsoft Exchange オンプレミス展開で設定されたメールボックスの組み合わせ

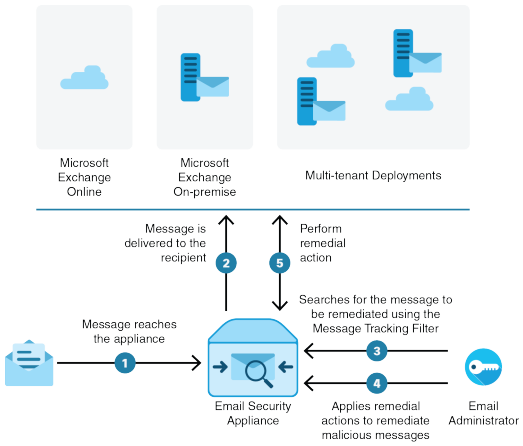
ワークフロー

メールボックス自動修復ワークフロー



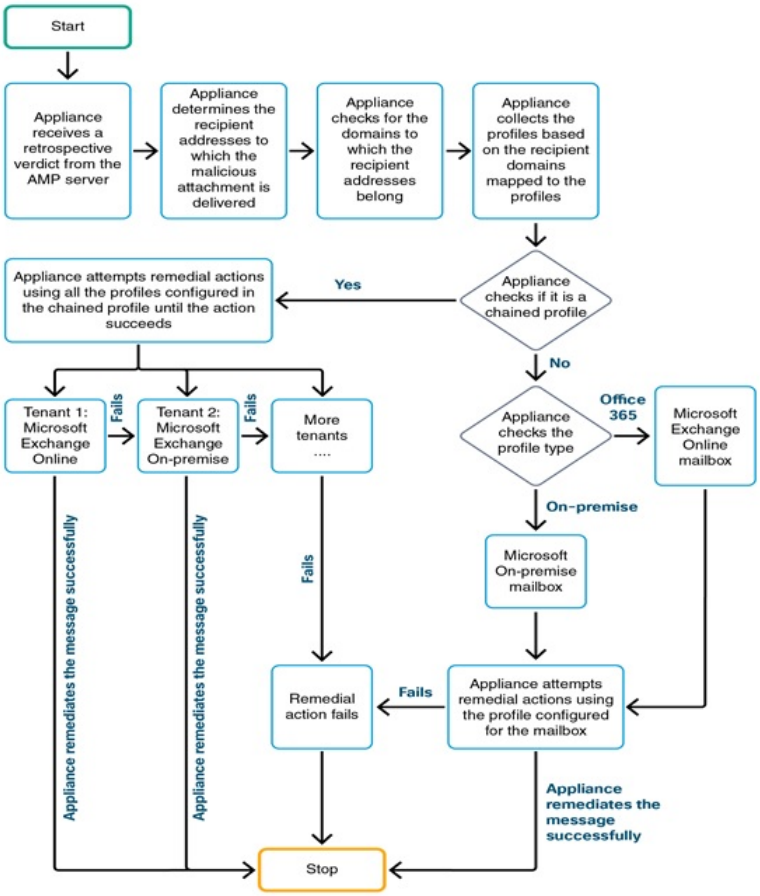
1. 添付ファイル付きメッセージが電子メールゲートウェイに到達します。
2. 電子メールゲートウェイは、添付ファイルのレピュテーションを評価するため、パブリック ファイル レピュテーション クラウド サーバにクエリを実行します。
3. パブリック ファイル レピュテーション クラウド サーバは、判定を電子メールゲートウェイに送信します。判定は、[正常（clean）] または [不明（unknown）] です。
4. 電子メールゲートウェイは、受信者へメッセージをリリースします。
5. 一定期間後に、電子メールゲートウェイはパブリック ファイル レピュテーション クラウド サーバから判定の更新を受け取ります。新しい判定は、[悪意のある（malicious）] です。
6. 電子メールゲートウェイは、受信者のメールボックスに存在する（悪意のある添付ファイルを含む）メッセージに対し、設定された修復アクションを実行します。

メッセージワークフローの検索と修復



1. メッセージが電子メールゲートウェイに到達します。
2. メッセージは受信者に配信されます。
3. 管理者はメッセージ トラッキング フィルタを使用して、受信者に配信されたメッセージを検索します。
4. ユーザは受信者のメールボックスから修正するメッセージを選択し、メッセージに修正アクションを適用します。
5. 電子メールゲートウェイは、受信者のメールボックスに存在するメッセージに対し、設定された修復アクションを実行します。

電子メールゲートウェイによる自動修復アクションの実行の仕組み



1. （メッセージを検索して修復する場合のみ）ユーザは、メッセージ トラッキング フィルタを使用して、ユーザメールボックスに配信されたメッセージを検索します。
2. （メッセージを検索して修復する場合のみ）：ユーザは修復するメッセージを選択し、そのメッセージに修復アクションを適用します。
3. （メッセージを自動修復する場合のみ）電子メールゲートウェイがパブリック ファイル レピュテーション クラウド サーバからレトロスペクティブな判定を受信すると、電子メールゲートウェイはメールボックスの修復プロセスを開始します。
4. （メッセージを自動修復する場合のみ）電子メールゲートウェイは、悪意のあるメッセージが配信された電子メールアドレスを特定します。
5. アプライアンスは、電子メール アドレスが属する受信者ドメインを識別します。

6. その受信者ドメインに基づいて、電子メールゲートウェイはドメインにマッピングされているアカウントプロファイルを収集します。

   アカウント プロファイルは、アプライアンスがメールボックスに接続して自動修復アクションを実行するために使用するメールボックス設定を定義します。メールボックスからメッセージを正常に修復するには、アカウントプロファイルを作成して受信者ドメインにマッピングする必要があります。

7. 電子メールゲートウェイは、ドメインにマッピングされたプロファイルをチェックします。

   - （ハイブリッドまたはマルチテナント展開のみ）連結プロファイルの場合、電子メールゲートウェイは連結プロファイル内のすべてのアカウントプロファイルを使用して修復アクションを実行しようとします。

     連結プロファイルとは、複数のアカウントプロファイルを組み合わせたものです。複数の展開にメールボックスが存在するハイブリッドまたはマルチテナント展開の場合は、展開内のメールボックスが定義されているすべてのプロファイルを組み合わせた連結プロファイルを作成する必要があります。電子メールゲートウェイは、アカウントプロファイルが連結プロファイルに追加された順序に基づいて、修復アクションの実行を試みます。

   - 連結プロファイルでない場合、電子メールゲートウェイはプロファイルタイプが Microsoft Exchange Online プロファイルか Microsoft Exchange オンプレミスプロファイルかを確認します。

8. 電子メールゲートウェイは、識別されたプロファイルを使用して修復アクションを実行し、メッセージを修復します。

（注） メールボックスの修復は、さまざまな理由で失敗することがあります。詳細については、メールボックス修復のトラブルシューティング （735 ページ）を参照してください。

目次

- Microsoft Exchange Online メールボックス内のメッセージに対する修復アクションの実行（714 ページ）
- Microsoft Exchange オンプレミスメールボックス内のメッセージに対する修復アクションの実行 （717 ページ）
- ハイブリッド展開のメールボックス内のメッセージに対する修復アクションの実行 （719 ページ）

メールボックス内のメッセージに対する修復アクションの実行

修復アクションは、次のメールボックス展開のメッセージに対して実行できます。

- Microsoft Exchange Online（Office 365）：Microsoft Exchange Online メールボックス内のメッセージに対する修復アクションの実行 （714 ページ）
- Microsoft Exchange オンプレミス：Microsoft Exchange オンプレミスメールボックス内のメッセージに対する修復アクションの実行 （717 ページ）
- ハイブリッド/マルチテナント展開：ハイブリッド展開のメールボックス内のメッセージに対する修復アクションの実行 （719 ページ）

Microsoft Exchange Online メールボックス内のメッセージに対する修復アクションの実行

ユーザメールボックスのメッセージの修復を実行するように電子メールゲートウェイを設定できます。

組織でメールボックスの管理に Microsoft Exchange Online を使用している場合、脅威判定が変更されたときにユーザのメールボックス内のメッセージに対して自動修復アクションを実行するように電子メールゲートウェイを設定できます。たとえば、添付ファイルに対する判定が「正常」から「悪意がある」に変更されたときには受信者のメールボックスからメッセージを削除するように電子メールゲートウェイを設定することができます。

ユーザメールボックスにすでに配信されているメッセージに対して、手動で修復アクションを実行できます。たとえば、着信メッセージをモニタする管理者は、メッセージ トラッキング フィルタを使用して、ユーザメールボックス内のメッセージに対して修復アクションを実行できます。

目次

- Microsoft Exchange Online メールボックスのメッセージに対する修復アクションの設定方法 （714 ページ）

Microsoft Exchange Online メールボックスのメッセージに対する修復アクションの設定方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	Microsoft Exchange Online メールボックスのメッセージ修復の前提条件 （723 ページ）

	操作内容	詳細
ステップ 2	Azure AD（Azure 管理ポータル）上のアプリケーションとして、電子メールゲートウェイを登録します。	Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録（725 ページ）
ステップ 3	電子メールゲートウェイでアカウント設定を有効にします。	電子メールゲートウェイでメールボックスの修復機能を有効にします。 電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）

	操作内容	詳細
ステップ 4	電子メールゲートウェイで [Office 365/ハイブリッド（Graph API）（Office 365/Hybrid (Graph API)）] タイプのアカウントプロファイルを作成します。	ユーザメールボックスの Office 365 プロファイルを作成し、電子メールゲートウェイでメールボックスの設定を定義します。 手順を開始する前に、次の点を確認してください。 • 次のパラメータの値 - Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録（725 ページ） のステップ 9 を参照してください。 • クライアント証明書ベースの通信の場合は、次のパラメータの値を取得します。 • .pem 形式の証明書の秘密キー。「セキュアな通信の証明書」を参照してください • 証明書サムプリント（$base64Thumbprint）。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録（725 ページ） のステップ 8 を参照してください。 • クライアント シークレット ベースの通信の場合は、Azure 管理ポータルで作成したアプリケーションの生成されたクライアントシークレットの値を取得します。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録（725 ページ） のステップ 8 を参照してください。 アカウントプロファイルの作成 （728 ページ）を参照してください。

	操作内容	詳細
ステップ 5	受信者ドメインを追加し、ドメインを Office 365 プロファイルにマッピングします。	受信者メールボックスが属するドメインを追加し、ドメインを Office 365 アカウントプロファイルにマッピングします。 アカウント プロファイルへのドメインのマッピング （731 ページ）を参照してください。
ステップ 6	（自動的にメッセージを修復する場合のみ）脅威の判定が「悪意がある」に変更された時点でエンドユーザに送信されるメッセージに対して修復アクションを実行するように、電子メールゲートウェイを設定します。	メールボックス内のメッセージに対する自動修復アクションの設定 （732 ページ）
ステップ 7	（メッセージを検索して修復する場合のみ）エンドユーザに送信されるメッセージに対して修復アクションを手動で実行するように電子メールゲートウェイを設定します。	メールボックス内のメッセージの検索と修復 （733 ページ）

MicrosoftExchangeオンプレミスメールボックス内のメッセージに対する修復アクションの実行

Exchange オンプレミスサーバ上のメールボックスからメッセージを修復するように電子メールゲートウェイを設定できます。メッセージは、電子メールゲートウェイによって自動的に修復することも、ユーザがメッセージ トラッキング フィルタを使用して手動で修復することもできます。

電子メールゲートウェイは、偽装権限があるユーザアカウントを使用して Exchange オンプレミスメールボックスにアクセスし、メッセージに対して修復アクションを実行します。偽装権限があるこのユーザアカウントは、電子メールゲートウェイが接続してメッセージを修復する必要があるメール交換サーバで作成する必要があります。

（注） シスコでは、Microsoft Exchange 2013、2016 および 2019 でのみメールボックス自動修復機能を検証しました。

目次

• Microsoft Exchange オンプレミス メールボックスのメッセージに対する修復アクションの設定方法 （718 ページ）

Microsoft Exchange オンプレミス メールボックスのメッセージに対する修復アクションの設定方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	オンプレミス アカウントのメッセージ修復の前提条件 （724 ページ）
ステップ 2	電子メールゲートウェイでアカウント設定を有効にします。	電子メールゲートウェイでメールボックスの修復機能を有効にします。 電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）
ステップ 3	電子メールゲートウェイで [オンプレミス（On-Premise）] タイプのアカウントプロファイルを作成します。	ユーザメールボックスのオンプレミスプロファイルを作成し、電子メールゲートウェイでメールボックスの設定を定義します。 手順を開始する前に、次の点を確認してください。 • 偽装ユーザ アカウントの詳細 • ローカル メール交換サーバのホスト名 アカウントプロファイルの作成 （728 ページ）。
ステップ 4	受信者ドメインを追加し、ドメインをオンプレミス アカウント プロファイルにマッピングします。	受信者メールボックスが属するドメインを追加し、ドメインをオンプレミス アカウント プロファイルにマッピングします。 アカウント プロファイルへのドメインのマッピング （731 ページ）を参照してください。
ステップ 5	（自動的にメッセージを修復する場合のみ）脅威の判定が「悪意がある」に変更された時点でエンドユーザに送信されるメッセージに対して修復アクションを実行するように、電子メールゲートウェイを設定します。	メールボックス内のメッセージに対する自動修復アクションの設定 （732 ページ）
ステップ 6	（メッセージの検索と修復のみ）オンプレミスのメールボックスのメッセージに対する修復アクションを設定します。	メールボックス内のメッセージの検索と修復 （733 ページ）

ハイブリッド展開のメールボックス内のメッセージに対する修復アクションの実行

単一の電子メールゲートウェイでハイブリッド Exchange 展開または複数の Exchange テナントからメッセージを修復するように設定できます。たとえば、組織がメールボックスを Microsoft Exchange オンプレミスから Microsoft Exchange Online に移行中の場合、移行が完了するまでは、Microsoft Exchange Online と Microsoft Exchange オンプレミスにメールボックスが展開されることになります。メッセージは、電子メールゲートウェイによって自動的に修復することも、ユーザがメッセージ トラッキング フィルタを使用して手動で修復することもできます。

異なる展開で設定された複数のメールボックスからメッセージを自動的に修復するには、連結プロファイルを作成します。連結プロファイルは、ハイブリッドまたはマルチテナント展開のすべてのアカウントプロファイルを統合します。プロファイルが連結プロファイルに追加される順序によって、電子メールゲートウェイがメッセージを修復するためにプロファイルを確認する優先順位が定義されます。

電子メールゲートウェイは AMP サーバからレトロスペクティブ判定を受信すると、連結プロファイルで定義されている優先順に連結プロファイル内の各プロファイルを使用して修復アクションの実行を試みます。

ユーザメールボックスに配信されるメッセージを手動で検索して修正するには、メッセージ トラッキング フィルタを使用します。このフィルタを使用すると、修復するメッセージを選択して、修復アクションを設定し、メッセージに修復アクションを適用できます。

目次

• ハイブリッド展開のメールボックスのメッセージに対する修復アクションの実行方法（719 ページ）

ハイブリッド展開のメールボックスのメッセージに対する修復アクションの実行方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	ハイブリッドまたはマルチテナント展開で、Microsoft Exchange Online および Microsoft Exchange オンプレミスのメールボックスに対して自動修復アクションを実行するためのすべての前提条件が満たされていることを確認します。 前提条件（723 ページ）を参照してください。
ステップ 2	Azure AD（Azure 管理ポータル）上のアプリケーションとして、電子メールゲートウェイを登録します。	Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録（725 ページ）

	操作内容	詳細
ステップ 3	電子メールゲートウェイでアカウント設定を有効にします。	電子メールゲートウェイでメールボックスの修復機能を有効にします。 電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）を参照してください。

	操作内容	詳細
ステップ 4	ハイブリッド/マルチテナント展開内の全メールボックスのアカウント プロファイルを作成します。	ユーザメールボックスのアカウントプロファイルを作成し、電子メールゲートウェイでメールボックスの設定を定義します。 手順を開始する前に、次の点を確認してください。 • 次のパラメータの値 - Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （725 ページ） のステップ 9 を参照してください。 • クライアント証明書ベースの通信の場合は、次のパラメータの値を取得します。 • .pem 形式の証明書の秘密キー。「セキュアな通信の証明書」を参照してください • 証明書サムプリント（$base64Thumbprint）。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （725 ページ） のステップ 8 を参照してください。 • クライアント シークレット ベースの通信の場合は、Azure 管理ポータルで作成したアプリケーションの生成されたクライアントシークレットの値を取得します。Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （725 ページ） のステップ 8 を参照してください。 • 偽装ユーザアカウントの詳細。 • ローカルメール交換サーバのホスト名。 アカウントプロファイルの作成 （728 ページ） を参照してください。

	操作内容	詳細
ステップ 5	連結プロファイルを作成します。	連結プロファイルを作成し、ハイブリッド/マルチテナント展開のすべてのプロファイルを追加します。 連結プロファイルの作成 （730ページ）を参照してください。
ステップ 6	受信者のドメインを追加して連結プロファイルにマッピングします。	受信者のメールボックスが属するドメインを追加し、そのドメインを連結プロファイルにマッピングします。 アカウント プロファイルへのドメインのマッピング （731 ページ）を参照してください。
ステップ 7	（自動的にメッセージを修復する場合のみ）脅威の判定が「悪意がある」に変更された時点でエンドユーザに送信されるメッセージに対して修復アクションを実行するように、電子メールゲートウェイを設定します。	メールボックス内のメッセージに対する自動修復アクションの設定 （732 ページ）
ステップ 8	（メッセージを検索して修復する場合のみ）メッセージに修復アクションを適用します。	メールボックス内のメッセージの検索と修復 （733 ページ）

電子メールゲートウェイでのメールボックス修復機能の設定

- 前提条件 （723 ページ）
- Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （725 ページ）
- 電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）
- アカウント プロファイルの作成 （728 ページ）
- 連結プロファイルの作成 （730 ページ）
- アカウント プロファイルへのドメインのマッピング （731 ページ）
- メールボックス内のメッセージに対する自動修復アクションの設定 （732 ページ）
- メールボックス内のメッセージの検索と修復 （733 ページ）

前提条件

- Microsoft Exchange Online メールボックスのメッセージ修復の前提条件 （723 ページ）
- オンプレミス アカウントのメッセージ修復の前提条件 （724 ページ）

Microsoft Exchange Online メールボックスのメッセージ修復の前提条件

- （メールボックス自動修復の場合のみ） ファイル レピュテーション サービスとファイル分析サービスの機能キー （723 ページ）
- Office 365 アカウント （723 ページ）
- セキュアな通信のクライアントシークレットまたは証明書 （723 ページ）

ファイル レピュテーション サービスとファイル分析サービスの機能キー

（注） ファイル レピュテーション サービスおよびファイル分析サービスの機能キーは、ユーザメールボックス内のメッセージに対して検索および修復アクションを実行する際には必要ありません。

ユーザメールボックス内のメッセージに対する修復アクションをメールボックス自動修復機能で設定するには、次の条件を満たしていることを確認してください。

- ファイル レピュテーション サービスおよびファイル分析サービスの機能キーをお使いの電子メールゲートウェイに追加していること。
- 電子メールゲートウェイでのファイルレピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析 （585 ページ） を参照してください。

Office 365 アカウント

Azure AD に、電子メールゲートウェイを登録する必要がある次のアカウントがあることを確認します。

- Office 365 のビジネス アカウント
- Office 365 のビジネス アカウントに関連付けられた Azure AD サブスクリプション

詳細については、Office 365 のシステム管理者にお問い合わせください。

セキュアな通信のクライアントシークレットまたは証明書

Office 365 サービスと電子メールゲートウェイ間の通信を保護するには、次のタスクのいずれかを実行する必要があります。

- Azure 管理ポータルで生成したアプリケーションのクライアントシークレットを生成します。

- 自己署名証明書を作成する、または信頼された CA から証明書を取得する方法のいずれかで証明書を設定します。

  次のものが必要です。

  - .crt または .p12 形式の公開キー。emailAddress に Office 365 の管理者の電子メールアドレス（<admin_username>@<domain>.com）が設定されていること。
  - キーサイズが少なくとも 2048 ビットで、関連付けられた .pem 形式の秘密キー。

（注） パスフレーズを含む秘密キーはこのリリースではサポートされません。

詳細については、https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/211404-How-to-configure-Azure-AD-and-Office-365.htmlを参照してください。

オンプレミス アカウントのメッセージ修復の前提条件

- （メールボックス自動修復の場合のみ） ファイル レピュテーション サービスとファイル分析サービスの機能キー （723 ページ）
- （任意）Microsoft Exchange Web サービス（EWS）証明書のインポート （724 ページ）
- 偽装ロールへのユーザの追加 （725 ページ）

ファイル レピュテーション サービスとファイル分析サービスの機能キー

（注） ファイル レピュテーション サービスおよびファイル分析サービスの機能キーは、ユーザメールボックス内のメッセージに対して検索および修復アクションを実行する際には必要ありません。

ユーザメールボックス内のメッセージに対する修復アクションをメールボックス自動修復機能で設定するには、次の条件を満たしていることを確認してください。

- ファイル レピュテーション サービスおよびファイル分析サービスの機能キーをお使いの電子メールゲートウェイに追加していること。
- 電子メールゲートウェイでのファイルレピュテーションと分析機能が有効になっている。ファイル レピュテーション フィルタリングとファイル分析 （585 ページ） を参照してください。

（任意）Microsoft Exchange Web サービス（EWS）証明書のインポート

EWS サービス用に Microsoft Exchange オンプレミスサーバで自己署名証明書を使用している場合は、Microsoft Exchange オンプレミスサーバから電子メールゲートウェイに証明書をインポー

トする必要があります。証明書をインポートするには、証明書のインポート （835ページ） を参照してください。

偽装ロールへのユーザの追加

電子メールゲートウェイは偽装権限があるユーザアカウントを使用して、Microsoft Exchange オンプレミスのメールボックスにアクセスします。メール交換管理者は、ローカル交換サーバで偽装権限があるユーザ アカウントを作成する必要があります。 電子メールゲートウェイはこのユーザアカウントを使用して、メールボックスからメッセージを修復します。

手順

ステップ 1 偽装権限を割り当てる必要があるユーザアカウントを作成します。このユーザアカウントは、電子メールゲートウェイがメッセージの修復を目的にメールボックスにアクセスして操作するために使用されます。

ステップ 2 管理者クレデンシャルを使用して、Microsoft Exchange コントロール パネル インターフェイスにログインします。

ステップ 3 [権限（Permissions）] -> [管理者ロール（Admin Roles）] に移動します。

ステップ 4 ロールを作成し、そのロールに「ApplicationImpersonation」権限を割り当てます。

ステップ 5 この新しいロールのメンバーとして、偽装権限を割り当てる必要があるユーザアカウントを追加します。

Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録

Office 365 サービスは、ユーザのメールボックスへのセキュアなアクセスを提供する Azure Active Directory（Azure AD）を使用します。Office 365 のメールボックスに電子メールゲートウェイがアクセスするには、Azure AD で電子メールゲートウェイを登録しなければなりません。Azure AD で電子メールゲートウェイを登録するために実行する必要がある手順の概要を次に示します。詳細な手順については、Microsoft のマニュアルを参照してください（https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app）。

はじめる前に

Microsoft Exchange Online メールボックスのメッセージ修復の前提条件 （723ページ） で説明されている作業を行います。

手順

ステップ 1 Office 365 のビジネス アカウントの資格情報を使用して Azure 管理ポータルにログインします。

ステップ 2 Office 365 のサブスクリプションにリンクされているディレクトリに新しいアプリケーションを追加します。

ステップ 3 [アプリケーションの登録（App Registrations）] > [新規登録（New Registration）] に移動して、新しいアプリケーションを追加します。

ステップ 4 新しいアプリケーションを追加している間に、次のことを確認します。

- アプリケーション名、およびアプリケーションがサポートする必要があるアカウントタイプを指定します。
- （任意）アプリケーションタイプとして [Web] を選択し、ユーザがサインインして電子メールゲートウェイを使用できる URL を指定します。

ステップ 5 アプリケーションに必要な権限を割り当てます。ナビゲーションウィンドウで[API権限（API permissions）] をクリックし、[権限の追加（Add a permission）] をクリックします。

ステップ 6 [Microsoft Graph] > [アプリケーション権限（Application permissions）] を選択し、次の権限を割り当てます。

- Mail.Read：すべてのメールボックスのメールを読み取ります。
- Mail. ReadWrite：すべてのメールボックスのメールの読み取りと書き込みを行います。
- Mail.Send：任意のユーザとしてメールを送信します。

ステップ 7 組織内のすべてのアカウントで必要なすべての権限に対して管理者の同意を付与します。

ステップ 8 次のタスクのいずれかを実行して、Office 365 サービスと電子メールゲートウェイ間の通信を保護します。

- Azure 管理ポータルで生成したアプリケーションのクライアントシークレットを生成します。

  （注） クライアントシークレットの値は、Azure 管理ポータルへの後続のログイン時に表示されないため、必ずコピーしてください。

- 公開キー証明書のキークレデンシャルでアプリケーションマニフェストを更新します。次の操作を行ってください。

  1. Windows PowerShell プロンプトを使用して、公開キー証明書の `$base64Thumbprint`、`$base64Value`、および `$keyid` の値を取得します。次の例を参照してください。Windows PowerShell プロンプトから公開キー証明書を含むディレクトリに移動し、次を実行します。

     例

     ```
     $cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
     $cer.Import(".\mycer.cer")
     $bin = $cer.GetRawCertData()
     $base64Value = [System.Convert]::ToBase64String($bin)
     $bin = $cer.GetCertHash()
     $base64Thumbprint = [System.Convert]::ToBase64String($bin)
     $keyid = [System.Guid]::NewGuid().ToString()
     ```

     上記のコマンドを実行した後、次のコマンドを実行して、その値を抽出します。

     ```
     $keyid
     $base64Value
     $base64Thumbprint
     ```

2. 登録済みアプリケーション ペインの左ペインにある [マニフェスト（manifest）] をクリックして、アプリケーションのマニフェストを開きます。
3. マニフェスト テキスト エディタを使用して、空の KeyCredentials プロパティを次の JSON で置き換えます。

   例

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint_from_step_1",
"keyId": "$keyid_from_step1",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value_from_step1"
}
],
```

例：

上記の JSON スニペットでは、`$base64Thumbprint`、`$base64Value`、および `$keyid` の値が、手順 a で取得した値で置き換えられていることを確認します。各値は 1 行で入力する必要があります。

ステップ 9 アプライアンスを Azure AD に登録した後、Azure 管理ポータルで、登録したアプリケーションの [概要（Overview）] ペインにある次の詳細を書き留めてください。

- Client ID
- テナント ID テナント ID は、このページに記載されているすべての URL で使用できる一意の値です。たとえば、このページに記載されている次のような URL です。
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

この例では、テナント ID は abcd1234-bcdd-469d-8545-a0662708cbc3 です。

次のタスク

電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）

電子メールゲートウェイでのアカウント設定の有効化

はじめる前に

次の内容について確認してください。

- （メールボックスの自動修復でのみ必要）電子メールゲートウェイでファイルレピュテーションと分析機能が有効になっていること。ファイル レピュテーション フィルタリングとファイル分析 （585 ページ）を参照してください。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 [アカウント設定の有効化（Enable Account Settings）] を選択します。

ステップ 5 （オプション）電子メールゲートウェイがメッセージを修復するためにメールボックスへの接続を試行する最大回数を入力します。許容値は 1 ～ 5 の整数です。

ステップ 6 （オプション）ハイブリッドメール交換サーバへの接続がタイムアウトする前に 電子メールゲートウェイが待機する秒数を入力します。許容値は 15 ～ 90 の整数です。

ステップ 7 （オプション）ローカルメール交換サーバへの接続がタイムアウトする前に電子メールゲートウェイが待機する秒数を入力します。許容値は 15 ～ 90 の整数です。

ステップ 8 変更を送信し、保存します。

次のタスク

アカウント プロファイルの作成 （728 ページ）

アカウント プロファイルの作成

アカウントプロファイルは、メールボックス内のメッセージの脅威判定が「悪意のある」に変わったときに、電子メールゲートウェイがメールボックスに接続して修復アクションを実行するために必要なメールボックスパラメータを定義します。

各プロファイルのクレデンシャルは、1 つのテナントに関連しています。複数のテナント間で修復を実行する場合は、テナントごとにプロファイルを設定し、チェーンプロファイルを使用してそれらを連結する必要があります。ただし、マルチテナント展開でロードバランサを使用している場合は、1 つのプロファイルを設定し、ロード バランサのホスト名を使用してプロファイルを作成することができます。

はじめる前に

次の内容について確認してください。

- 有効化されたアカウント設定。電子メールゲートウェイでのアカウント設定の有効化（727 ページ）を参照してください。
- Microsoft Exchange Online サーバまたは Microsoft Exchange オンプレミス サーバの有効な電子メール アドレス。

- Microsoft Exchange Online アカウントまたは Microsoft Exchange オンプレミス アカウントを設定するために必要なパラメータ。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 [アカウントプロファイルの作成（Create Account Profile）] をクリックします。

ステップ 4 プロファイルの名前および説明を入力します。

ステップ 5 メールボックスの展開に基づいてプロファイル タイプを選択します。

- [Office 365/ハイブリッド（Graph API）（Office 365/Hybrid (Graph API)）]：Microsoft Exchange Online 上に展開されたメールボックスを設定し、次の詳細情報を入力する場合に選択します。
  - Azure 管理ポータルで登録したアプリケーションのクライアント ID とテナント ID。
  - クライアントのクレデンシャルを検証するには、次のいずれかの方法を選択します。
    - [クライアントシークレット（Client Secret）]：Azure 管理ポータルで生成したアプリケーションのクライアントシークレットを入力する場合に選択します。
    - [クライアント証明書（Client Certificate）]：証明書のサムプリント（$base64Thumbprint の値）を入力し、[ファイルの選択（Choose File）] をクリックして、証明書の秘密キーを .pem 形式でアップロードする場合に選択します。
- [Exchangeオンプレミス（Exchange On-premise）]：Microsoft Exchange オンプレミスで展開されたメールボックスを設定し、次の詳細情報を入力する場合に選択します。
  - 偽装権限を持つユーザアカウントのユーザ名とパスワードを入力します。詳細については、偽装ロールへのユーザの追加 （725 ページ）を参照してください。
  - Microsoft Exchange オンプレミス サーバのホスト名を入力します。

    （注） マルチテナント展開でロード バランサを使用する場合は、ロード バランサのホスト名を設定する必要があります。

ステップ 6 電子メールゲートウェイが Microsoft Exchange Online サーバまたは Microsoft Exchange オンプレミスサーバに接続できるかどうかを確認します。

a) [テスト接続（Test Connection）] をクリックします。
b) 電子メール アドレスを入力します。これは、Microsoft Exchange Online または Microsoft Exchange オンプレミスの有効な電子メール アドレスである必要があります。
c) [テスト接続（Test Connection）] をクリックします。
電子メールゲートウェイがメールボックス サーバに接続できるかどうかを示すステータスが表示されます。

d) 4. [完了（Done）] をクリックします。エラーのトラブルシューティングについては、メールボックス修復のトラブルシューティング （735 ページ）を参照してください。

ステップ 7 変更を送信し、保存します。

次のタスク

- 連結プロファイルの作成 （730 ページ）
- アカウント プロファイルへのドメインのマッピング （731 ページ）

連結プロファイルの作成

このタスクは、ハイブリッド展開またはマルチテナント展開のメールボックスにあるメッセージを修復する場合にのみ必須です。

はじめる前に

少なくとも 1 つのアカウントプロファイルが電子メールゲートウェイに追加されていることを確認してください。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 [連結プロファイルの作成（Create Chained Profile）] をクリックします。

ステップ 4 連結プロファイルの名前および説明を入力します。

ステップ 5 連結プロファイルに追加するアカウント プロファイルをドロップダウン メニューから選択します。さらにプロファイルを追加するには、[アカウントプロファイルの追加（Add Account Profile）] をクリックします。

（注）
- 電子メールゲートウェイがメッセージを修復するためにプロファイルを確認する優先順にプロファイルを追加する必要があります。
- 電子メールゲートウェイには、一度に最大 5 つの連結プロファイルを作成できます。
- 連結プロファイルごとに最大 10 個のアカウントプロファイルを追加できます。

ステップ 6 変更を送信し、保存します。

次のタスク

アカウント プロファイルへのドメインのマッピング （731 ページ）

アカウント プロファイルへのドメインのマッピング

受信者のメールボックスが属するドメインを定義する必要があります。次に、電子メールゲートウェイがメールボックス内のメッセージを修復する際に使用するアカウントプロファイルにドメインをマッピングします。

（注）
- ドメイン マッピングを編集して、プロファイルにマッピングされた既存のドメインに新しいドメインを追加することができます。
- ドメイン マッピングはプロファイルに固有です。あるプロファイルにマップされたドメインは、別のプロファイルにマップできません。

はじめる前に

少なくとも1つのアカウントプロファイルが電子メールゲートウェイに追加されていることを確認してください。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [アカウントの設定（Account Settings）] をクリックします。

ステップ 3 [ドメインマッピングの作成（Create Domain Mapping）] をクリックします。

ステップ 4 ドメイン名をカンマで区切って入力します。すべてのドメインにプロファイルをマッピングする場合は、「ALL」という文字列を入力します。

ステップ 5 ドメインにマッピングするプロファイルを選択します。また、連結プロファイルをドメインにマッピングすることもできます。

ステップ 6 変更を送信し、保存します。

次のタスク

- メールボックス内のメッセージに対する自動修復アクションの設定 （732 ページ）
- メールボックス内のメッセージの検索と修復 （733 ページ）

メールボックス内のメッセージに対する自動修復アクションの設定

（注） メールボックス自動修復機能でメールボックス内のメッセージに対する修復アクションを設定する場合は、次の手順を実行します。

はじめる前に

メールボックスの自動修復機能が有効になっており、アプライアンスでアカウントの設定が完了していることを確認します。電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] を選択します。

ステップ 2 変更するメール ポリシーの [高度なマルウェア防御（Advanced Malware Protection）] カラム内のリンクをクリックします。

ステップ 3 [メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）] を選択します。

ステップ 4 脅威の判定が悪意に変更されたときにエンドユーザに配信されたメッセージ基づいて実行するアクションを指定します。要件に応じて、次のいずれかの修復アクションを選択します。

- [電子メール アドレスに転送（Forward to an email address）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送する場合は、このオプションを選択します。
- メッセージを削除します。悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。
- [指定した電子メール アドレスに転送してメッセージを削除（Forward to an email address and delete the message）]。指定したユーザ（たとえば、電子メール管理者など）に悪意のある添付ファイルを転送して、悪意のある添付ファイルをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

関連項目

- メールボックス修復結果のモニタリング （735 ページ）
- メッセージ トラッキングでのメールボックス修復の詳細の表示 （735 ページ）
- メールボックス修復のトラブルシューティング （735 ページ）

メールボックス内のメッセージの検索と修復

はじめる前に

- 電子メールゲートウェイでメールボックスの修復機能が有効になっていること、およびアカウントの設定が完了していることを確認します。電子メールゲートウェイでのアカウント設定の有効化 （727 ページ）を参照してください。
- 電子メールゲートウェイでメッセージトラッキングを有効にします。メッセージトラッキングの有効化 （1113 ページ）を参照してください。
- 中央集中型メッセージトラッキングサービスを使用している場合は、管理対象の電子メールゲートウェイで Trailblazer ポートと AsyncOS API HTTP ポートが有効になっていること、および Cisco Secure Email and Web Manager が Trailblazer ポートにアクセスできることを確認します。Trailblazer ポートが無効になっている場合は、 Cisco Secure Email and Web Manager が、管理対象の 電子メールゲートウェイの AsyncOS API HTTP ポートにアクセスできることを確認します。

（注） 次の手順は、 電子メールゲートウェイの新しい Web インターフェイスでのみ実行できます。

手順

ステップ 1 レガシー Web インターフェイスの [Eメールセキュリティアプライアンスの外観が新しくなりました。お試しください（Email Security Appliance is getting a new look. Try it!!）] リンクをクリックします。Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス （37 ページ）を参照してください。

ステップ 2 [Tracking] タブをクリックします。

ステップ 3 [メッセージ（Messages）] タブをクリックし、検索結果を絞り込みます。詳細については、新しい Web インターフェイスでの電子メール メッセージの検索 （1118 ページ）を参照してください。

ステップ 4 修復するメッセージを選択します。一度に最大 1000 件のメッセージを選択できます。配信済みのメッセージのみを修復できます。

ステップ 5 [修復（Remediate）] をクリックします。

ステップ 6 次の詳細を入力します。

- 修正対象のバッチ名を入力します。
- 次の修復アクションのいずれかを選択します
  - メッセージを削除する。悪意のあるメッセージをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。

- 1 つの電子メールアドレス、またはセミコロン（;）で区切った複数の電子メールアドレスに転送する。指定したユーザ（電子メール管理者など）に悪意のあるメッセージを転送する場合は、このオプションを選択します。
- 1 つの電子メールアドレス、またはセミコロン（;）で区切った複数の電子メールアドレスに転送してからメッセージを削除する。指定したユーザ（電子メール管理者など）に悪意のあるメッセージを転送した後に、そのメッセージをエンドユーザのメールボックスから完全に削除する場合は、このオプションを選択します。

ステップ 7 [適用（Apply）] をクリックします。

[適用（Apply）] をクリックすると、[メッセージトラッキング（Message Tracking）] ページの右下隅にある [修復レポートのステータス（Remediation Report Status）] ウィジェットを表示できます。このウィジェットを使用して修復レポートの生成ステータスを確認します。修復レポートの生成が完了したら、ウィジェットの [詳細の表示（View Details）] をクリックして修復レポートに移動し、修復結果を表示します。

（注） また、[レポート（Reports）] > [ユーザレポート（User Reports）] > [修復レポート（Remediation Report）] に移動し、[メールボックスの検索と修復（Mailbox Search And Remediate）] タブをクリックして、修復レポートを直接表示することもできます。

次のタスク

関連項目

- メールボックス修復結果のモニタリング （735 ページ）
- メッセージ トラッキングでのメールボックス修復の詳細の表示 （735 ページ）
- メールボックス修復のトラブルシューティング （735 ページ）

AsyncOS 13.0 以降のリリースへのアップグレード

以前の AsyncOS バージョンで定義されたメールボックスの設定は、アップグレード中にシームレスに移行されます。このメールボックスは、「Default」というプロファイル名で作成されて「すべて」のドメインにマッピングされます。このプロファイルは、アップグレード後に必要に応じて編集できます。アプリケーションが Azure Active Directory の Microsoft Graph API にアクセスして、Microsoft Exchange Online メールボックスからメッセージを修復できることを確認します。詳細については、Azure AD 上のアプリケーションとしての電子メールゲートウェイの登録 （725 ページ）を参照してください。

メールボックス修復結果のモニタリング

[修復（Remediation）] レポートページを使用して、メールボックスの修復結果の詳細を表示できます。レポートを表示するには、次の手順を行います。

1. **レガシー Web インターフェイスの [Eメールセキュリティアプライアンスの外観が新しくなりました。**お試しください（Email Security Appliance is getting a new look. Try it!!）] リンクをクリックします。
2. [モニタリング（Monitoring）] タブをクリックします。
3. [レポート（Reports）] ドロップダウンメニューをクリックし、[修復レポート（Remediation Report）] を選択します。

このレポートを使用して次の詳細情報を表示します。

- [メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] を使用して修復が試行されたメッセージの合計数。
- 設定された修正アクションに対して正常に修復されたメッセージの数。
- 修復が失敗したメッセージの数。
- 修復が試行されたメッセージの詳細。

詳細については、[修復レポート（Remediation Report）] ページ（1101 ページ）を参照してください。

メッセージトラッキングでのメールボックス修復の詳細の表示

[メッセージトラッキング（Message Tracking）] ページの [メールボックスの検索と修復（Mailbox Search and Remediate）] を使用して、修復されたメッセージの詳細を表示できます。修復を開始する前に、[メッセージトラッキング（Message Tracking）] が有効になっていることを確認します。

（注） メールボックス自動修復機能を使用して修復が試みられたメッセージは、トラッキングの検索結果に含まれません。

表示されるデータの詳細については、メッセージトラッキングの詳細 （1122 ページ）を参照してください。

メールボックス修復のトラブルシューティング

- 接続エラー （736 ページ）

- ログの表示 （738 ページ）
- アラート （738 ページ）
- 設定された是正措置が実行されない （739 ページ）

接続エラー

問題

[アカウントの設定（Account Settings）] ページ（[システム管理（System Administration）] > [メールボックスの設定（Mailbox Settings）][アカウントの設定（Account Settings）]）で 電子メールゲートウェイと受信者メールボックスとの接続を確認しようとすると、エラーメッセージ `Connection Unsuccessful` が表示されます。

ソリューション

サーバからの応答に応じて、次のいずれかを実行します。

エラー メッセージ	理由とソリューション
`The SMTP address has no mailbox associated with it`	関連付けられたメール ドメインに属していない電子メール アドレスを入力しました。 有効な電子メール アドレスを入力して、接続を再度確認します。
`The mailbox cannot be accessed using this profile or the required permissions may be missing`	以下を確認します。 • ユーザー メールボックスにアクセスするために必要な権限があります。Micrsoft Exchange Online アカウントには Microsoft Graph API でのみアクセスでき、Microsoft Exchange オンプレミス アカウントには偽装権限を持つユーザ アカウントを使用してアクセスできます。 • 誤ったプロファイル タイプを選択しました。[アカウントプロファイルの編集（Edit Account Profile）] ページでプロファイルの詳細を変更し、接続を再度確認します。
`Access is denied. Check credentials and try again`	Microsoft Azure に設定された Office 365 アプリケーションに、Microsoft Exchange Online メールボックスにアクセスするために必要な権限がありません。
`Application with identifier '<client_id>' was not found in the directory <tenant_id>`	無効なクライアント ID を入力しました。 [アカウントプロファイル（Account Profile）] ページでクライアント ID を変更し、接続を再度確認します。
`No service namespace named '<tenant_id>' was found in the data store.`	無効なテナント ID を入力しました。 [アカウントプロファイル（Account Profile）] ページでテナント ID を変更し、接続を再度確認します。

エラー メッセージ	理由とソリューション
`Error validating credentials. Credential validation failed`	無効な証明書サムプリントを入力しました。 [アカウントプロファイル（Account Profile）] ページで証明書サムプリントを変更し、接続を再度確認します。
`Error validating credentials. Client assertion contains an invalid signature.`	誤った証明書サムプリントを入力したか、または無効なあるいは誤った証明書秘密キーをアップロードしました。 以下を確認します。 • 正しいサムプリントを入力しました。 • 正しい証明書の秘密キーをアップロードしました。 • 証明書の秘密キーは有効期限が切れていません。 • 電子メールゲートウェイの時間帯は、証明書の秘密キーの時間帯と一致します。
`The requested user <email address> is invalid`	入力された電子メール アドレスが、アカウント プロファイルのプロファイル タイプと一致しません。有効な電子メールアドレスを入力するか、[アカウントプロファイル（Account Profile）] ページでアカウント プロファイルを変更して、接続を再度確認します。
`Failed to verify exchange server('<host name>') certificate. If self-signed certificate is used on exchange server install its custom CA certificate`	• Microsoft Exchange オンプレミス サーバで、無効な CA または自己署名証明書を入力しました。証明書を検証してから、接続を再度確認します。 （注） 使用している証明書が、プロファイルで指定されたホスト名に対応していることを確認します。たとえば、プロファイル設定でExchange Server の IP アドレスを指定した場合に証明書がホスト名に基づいていると、接続は失敗します。 • Microsoft Exchange オンプレミスサーバから 電子メールゲートウェイに自己署名証明書がインポートされていません。詳細については、証明書のインポート （835 ページ）を参照してください。
`Invalid username or password entered for exchange server ('<email address>')`	Microsoft Exchange オンプレミスのメールボックスに接続するために使用される偽装ユーザ アカウントの無効なユーザ名またはパスワードを入力しました。
`The account does not have permission to impersonate the requested user`	Microsoft Exchange オンプレミスのメールボックスに接続するために使用されるユーザ アカウントは、偽装ロールのメンバーではありません（偽装権限を持っていません）。

エラー メッセージ	理由とソリューション
`Please check host <hostname> is valid exchange server address.`	Microsoft Exchange オンプレミス サーバの誤ったホスト名を入力しました。[アカウントプロファイル（Account Profile）] ページでホスト名を変更し、接続を再度確認します。

ログの表示

メールボックスの修復情報は、次のログに書き込まれます。

- メール ログ（mail_logs）。メールボックスの修復プロセスの開始時刻は、このログに転記されます。メールボックスの自動修復機能またはメールボックス検索と修復アクションに関する情報：
  - メールボックスの修復プロセスの開始時刻は、このログに転記されます。
  - 修復ステータス
  - 修復が失敗した理由。
  - 修復が成功および失敗した受信者。
  - 検索および修復アクションが開始された送信元。
  - 検索および修復アクションを開始したユーザ。
  - メッセージに対して実行された修復アクション。
- 修復ログ。修復状態、実行された操作、エラーに関連する情報などがこのログに転記されます。

アラート

アラート：検出された 電子メールゲートウェイと Microsoft Exchange サービスとの間の接続の問題

問題

電子メールゲートウェイと Microsoft Exchange Online サービスまたは Microsoft Exchange オンプレミスサービスの間に接続の問題があり、設定された修復アクションを電子メールゲートウェイが実行できないことを示す情報レベルのアラートを受け取ります。

ソリューション

次の手順を実行します。

- 電子メールゲートウェイと Microsoft Exchange Online サービスまたは Microsoft Exchange オンプレミスサービスとの通信を妨げている可能性があるネットワークの問題を確認します。

  電子メールゲートウェイのネットワーク設定を確認します。ネットワーク設定値の変更（1303 ページ）を参照してください。

- アプリケーションに Azure Active Directory 上の Microsoft Graph API へのアクセス権があることを確認します。
- Exchange オンプレミスのメールボックスへのアクセスに使用されるユーザ アカウントに偽装権限があることを確認します。
- 対応するプロファイルに設定されているパラメータが有効であることを確認し、接続をテストします。
- ファイアウォールの問題を確認します。ファイアウォール情報（1607ページ）を参照してください。
- Microsoft Exchange Online サービスまたは Microsoft Exchange オンプレミス サービスが動作しているかどうかを確認します。

設定された是正措置が実行されない

問題

AMP サーバからレトロスペクティブ アラートを受信した後、設定済みの修復アクションが Exchange Online および Exchange オンプレミスのメールボックスにある悪意のあるメッセージに対して実行されません。

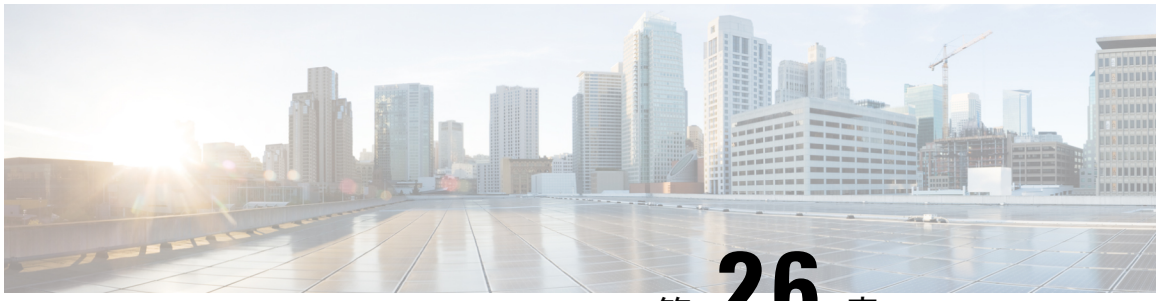
または

ユーザは、[メッセージトラッキング（Message Tracking）] ページの [修復（Remediate）] オプションを使用してメッセージを手動で修復できません。

ソリューション

次の手順を実行します。

- 電子メールゲートウェイと Exchange Online サービスおよび Exchange オンプレミスサービスの接続をテストします。アカウント プロファイルの作成 （728 ページ） を参照してください。
- （メールボックス自動修復の場合のみ）「電子メールゲートウェイと Exchange Online サービスおよびExchange オンプレミスサービス間の接続の問題が検出されました。（Connectivity Issues Between Appliance and Exchange online and Exchange on-premise Services Detected.）」というアラートを受信しているかどうかを確認します。アラート （738 ページ） を参照してください。



第 26 章

電子メール認証

この章は、次の項で構成されています。

- 電子メール認証の概要 （741 ページ）
- DomainKeys および DKIM 署名の構成 （744 ページ）
- DKIM を使用した受信メッセージの検証方法 （759 ページ）
- SPF および SIDF 検証の概要 （765 ページ）
- SPF/SIDF を使用した受信メッセージの検証方法 （767 ページ）
- SPF と SIDF のイネーブル化 （768 ページ）
- SPF/SIDF 検証済みメールに対して実行するアクションの決定 （773 ページ）
- SPF/SIDF 結果のテスト （776 ページ）
- DMARC 検証 （777 ページ）
- 偽装メールの検出 （787 ページ）

電子メール認証の概要

AsyncOS では、電子メールの偽造を防止するために、電子メール検証と署名をサポートします。着信メールを検証するために、AsyncOS は SPF（Sender Policy Framework）、SIDF（Sender ID Framework）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting and Conformance）、および偽装電子メール検出をサポートします。送信メールを認証するために、AsyncOS は DomainKeys および DKIM 署名をサポートしています。

関連項目

- DomainKeys と DKIM 認証 （742 ページ）
- SPF および SIDF 検証の概要 （765 ページ）
- DMARC 検証 （777 ページ）
- 偽装メールの検出 （787 ページ）

DomainKeys と DKIM 認証

DomainKeysまたはDKIM電子メール認証では、送信側が公開キー暗号化を使用して、電子メールに署名します。これにより、検証済みのドメインを使用して、電子メールの From:（または Sender:）ヘッダーのドメインと比較して、偽造を検出できます。

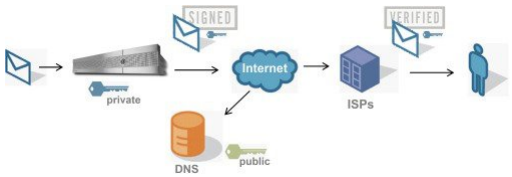
DomainKeys と DKIM は、署名と検証の 2 つの主要部分から構成されます。AsyncOS では、DomainKeys の「署名」部分のプロセスをサポートし、DKIM の署名と検証の両方をサポートします。バウンスおよび遅延メッセージで DomainKeys および DKIM 署名を使用することもできます。

関連項目

- DomainKeys と DKIM 認証ワークフロー （742 ページ）
- AsyncOS の DomainKeys および DKIM 署名 （742 ページ）

DomainKeys と DKIM 認証ワークフロー

図 *36 :* 認証ワーク フロー



1. 管理者（ドメイン所有者）が公開キーを DNS 名前空間にパブリッシュします。
2. 管理者は発信メール転送エージェント（MTA）に秘密キーをロードします。
3. そのドメインの権限のあるユーザによって送信される電子メールが、各秘密キーによってデジタル署名されます。署名は DomainKey または DKIM 署名ヘッダーとして電子メールに挿入され、電子メールが送信されます。
4. 受信側 MTA は、電子メールのヘッダーから DomainKeys または DKIM 署名と、要求された送信側ドメイン（Sender: または From: ヘッダーによって）を抽出します。DomainKeysまたはDKIM署名ヘッダーフィールドから抽出された要求された署名ドメインから、公開キーが取得されます。
5. 公開キーは、DomainKeys または DKIM 署名が適切な秘密キーによって生成されているかどうかを確認するために使われます。

Yahoo! または Gmail アドレスを使用して、送信 DomainKeys 署名をテストできます。これらのサービスは無料で提供され、DomainKeys 署名されている着信メッセージを検証します。

AsyncOS の DomainKeys および DKIM 署名

AsyncOS の DomainKeysおよびDKIM署名は、ドメインプロファイルによって実装され、メール フロー ポリシー（一般に、発信「リレー」ポリシー）によってイネーブルにされます。詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。メッセー

ジの署名は、メッセージ送信前に電子メールゲートウェイによって実行される最後の操作です。

ドメイン プロファイルはドメインとドメイン キー情報（署名キーと関連情報）を関連付けます。電子メールは、電子メールゲートウェイで、メールフローポリシーによって送信され、いずれかのドメインプロファイルに一致する送信側電子メールアドレスが、ドメインプロファイルに指定されている署名キーを使用して DomainKeys 署名されます。DKIM と DomainKeys の両方の署名をイネーブルにすると、DKIM 署名が使われます。DomainKeys および DKIM プロファイルは、domainkeysconfig CLI コマンドまたは GUI の [メールポリシー（Mail Policies）] > [ドメインプロファイル（Domain Profiles）] および [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] ページを使用して実装します。

DomainKeys および DKIM 署名は次のように機能します。ドメイン所有者はパブリック DNS（そのドメインに関連付けられた DNS TXT レコード）に格納される公開キーと、電子メールゲートウェイに格納され、そのドメインから送信されるメール（発信されるメール）の署名に使われる秘密キーの 2 つのキーを生成します。

メッセージがメッセージの送信（発信）に使われるリスナーで受信されると、電子メールゲートウェイはドメインプロファイルが存在するかどうかを調べます。電子メールゲートウェイに作成された（およびメールフローポリシー用に実装された）ドメインプロファイルが存在する場合、メッセージの有効な Sender: または From: アドレスがスキャンされます。両方が存在する場合、DomainKeys 署名および DKIM 署名には常に Sender: ヘッダーが使用され、From: ヘッダーも、DKIM 署名には使用されないものの、必要です。Sender: ヘッダーしか存在しない場合は、DomainKeys 署名または DKIM 署名のプロファイルが一致しません。From: ヘッダーは、次の場合のみ使用されます。

- Sender: ヘッダーがない。
- Web インターフェイスの [DKIMグローバル設定（DKIM Global Setting）] ページで [DKIM署名のFromヘッダーの使用（Use From Header for DKIM Signing）] オプションを選択している。

（注） AsyncOS 10.0 以降、Web インターフェイスの [DKIMグローバル設定（DKIM Global Setting）] ページで [DKIM署名へのFromヘッダーの使用（Use From Header for DKIM Signing）] オプションを選択できるようになっています。DKIM 署名に From ヘッダーを使用することが重要なのは、主に、適切な DMARC 検証のためです。

有効なアドレスが見つからない場合、メッセージは署名されず、イベントが mail_logs に記録されます。

（注） DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

有効な送信側アドレスが見つかった場合、送信側アドレスが既存のドメインプロファイルに対して照合されます。一致しているものが見つかった場合、メッセージは署名されます。見つからない場合、メッセージは署名なしで送信されます。メッセージに既存の DomainKeys（「DomainKey-Signature:」ヘッダー）がある場合、メッセージは、元の署名の後に新しい送信側アドレスが追加されている場合にのみ、署名されます。メッセージに既存の DKIM 署名がある場合、新しい DKIM 署名がメッセージに追加されます。

AsyncOS はドメインに基づいて電子メールに署名するメカニズムに加えて、署名キーを管理する（新しいキーの作成または既存のキーの入力）方法を提供します。

このマニュアルのコンフィギュレーションの説明は、署名と検証の最も一般的な使用方法を示しています。着信電子メールのメール フロー ポリシーで DomainKeys および DKIM 署名をイネーブルにすることも、発信電子メールのメール フロー ポリシーで DKIM 検証をイネーブルにすることもできます。

（注） クラスタ環境にドメイン プロファイルと署名キーを設定する場合、[ドメイン キー プロファイル（Domain Key Profile）] 設定と [署名キー（Signing Key）] 設定がリンクしていることに注意します。そのため、署名キーをコピー、移動、または削除した場合、同じ操作が関連プロファイルに対して行われます。

DomainKeys および DKIM 署名の構成

関連項目

- 署名キー （744 ページ）
- 公開キー （745 ページ）
- ドメイン プロファイル （746 ページ）
- バウンスおよび遅延メッセージの署名のイネーブル化 （747 ページ）
- 送信メールの署名のイネーブル化 （747 ページ）
- DomainKeys/DKIM 署名の設定（GUI） （748 ページ）
- ドメイン キーとロギング （758 ページ）

署名キー

署名キーは電子メールゲートウェイに格納されている秘密キーです。署名キーの作成時に、キー サイズを指定します。キー サイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性もあります。電子メールゲートウェイでは 512 ～ 2048 ビットのキーをサポートしています。768 ～ 1024 ビットのキー サイズは安全であると見なされ、現在ほとんどの送信側で使われています。大きなキーサイズに基づいたキーはパフォーマンスに影響する可能性があるため、2048 ビットを超えるキーはサポートされていません。署名キーの作成方法については、署名キーの作成または編集 （752 ページ）を参照してください。

既存のキーを入力する場合、それをフォームに貼り付けるだけです。既存の署名キーの別の使用方法は、キーをテキストファイルとしてインポートすることです。既存の署名キーの追加の詳細については、既存の署名キーのインポートまたは入力 （753 ページ）を参照してください。

キーを入力すると、ドメイン プロファイルで使用できるようになり、ドメイン プロファイルの [署名キー（Signing Key）] ドロップダウン リストに表示されます。

関連項目

- 署名キーのエクスポートとインポート （745 ページ）

署名キーのエクスポートとインポート

署名キーを電子メールゲートウェイ上のテキストファイルにエクスポートできます。キーをエクスポートすると、電子メールゲートウェイに現在存在するすべてのキーがテキストファイルに挿入されます。キーのエクスポートの詳細については、署名キーのエクスポート （753 ページ）を参照してください。

エクスポートされたキーをインポートすることもできます。

（注） キーをインポートすると、電子メールゲートウェイ上のすべての現在のキーが置き換えられます。

詳細については、既存の署名キーのインポートまたは入力 （753 ページ）を参照してください。

公開キー

署名キーをドメイン プロファイルに関連付けると、公開キーが含まれる DNS テキスト レコードを作成できます。これは、ドメイン プロファイルのリストの [DNSテキストレコード（DNS Text Record）] 列の [生成（Generate）] リンクから（または CLI の **domainkeysconfig -> profiles -> dnstxt** から）実行します。

DNS テキスト レコードの生成の詳細については、DNS テキスト レコードの生成 （755 ページ）を参照してください。

[署名キー（Signing Keys）] ページの [ビュー（View）] リンクから、公開キーを表示することもできます。

図 *37 : [*署名キー（*Signing Keys***）*] *ページの公開キーの表示リンク***

ドメイン プロファイル

ドメインプロファイルは送信側ドメインを署名に必要なその他の情報と共に署名キーに関連付けます。

- ドメイン プロファイルの名前。
- ドメイン名（「d=」ヘッダーに含まれるドメイン）。
- セレクタ（セレクタは公開キーのクエリを形成するために使用されます。DNS クエリータイプでは、この値が送信側ドメインの「_domainkey」名前空間の前に付けられます）。
- 正規化方法（署名アルゴリズムに提示するためにヘッダーと内容が準備される方法）。AsyncOS は DomainKeys に対して「simple」と「nofws」、DKIM に対して「relaxed」と「simple」をサポートしています。
- 署名キー（詳細については、署名キー （744 ページ）を参照してください）。
- 署名するヘッダーのリストと本文の長さ（DKIM のみ）。
- 署名のヘッダー（DKIM のみ）に含めるタグのリスト。これらのタグは次の情報を保持します。
  - 署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。
  - 公開キーを取得するために使用されるクエリー方法のカンマ区切りリスト。
  - 署名が作成されたときのタイムスタンプ。
  - 秒による署名の有効期限。
  - 垂直バー（|）によって区切られているヘッダー フィールドのリストには、メッセージが署名された時が示されます。
- 署名（DKIM のみ）に含めるタグ。
- プロファイル ユーザのリスト（署名用にドメイン プロファイルの使用を許可されたアドレス）。

（注） プロファイル ユーザに指定されたアドレスのドメインは [ドメイン（Domain）] フィールドに指定されたドメインに一致している必要があります。

既存のすべてのドメインプロファイルで、特定の用語を検索できます。詳細については、ドメイン プロファイルの検索 （757 ページ）を参照してください。

さらに、次のことを行うかどうか選択することができます。

- DKIM 署名を持つシステム生成メッセージへの署名
- DKIM 署名の From ヘッダーの使用

この説明については、DKIM グローバル設定の編集 （758 ページ） を参照してください。

関連項目

- ドメイン プロファイルのエクスポートとインポート （747 ページ）

ドメイン プロファイルのエクスポートとインポート

既存のドメインプロファイルを電子メールゲートウェイ上のテキストファイルにエクスポートできます。ドメインプロファイルをエクスポートすると、電子メールゲートウェイに存在するすべてのプロファイルが1つのテキストファイルに挿入されます。ドメイン プロファイルのエクスポート （756 ページ）を参照してください。

以前にエクスポートしたドメイン プロファイルをインポートできます。ドメイン プロファイルをインポートすると、マシン上のすべての現在のドメイン プロファイルが置き換えられます。ドメイン プロファイルのインポート （756 ページ） を参照してください。

送信メールの署名のイネーブル化

DomainKeys および DKIM 署名は発信メールのメール フロー ポリシーでイネーブルにします。詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。

手順

ステップ 1 [メール フロー ポリシー（Mail Flow Policies）] ページ（[メール ポリシー（Mail Policies）] メニューから）で、[リレー（RELAYED）] メール フロー ポリシー（送信）をクリックします。

ステップ 2 [セキュリティ サービス（Security Features）] セクションから、[オン（On）] を選択して、[DomainKeys/DKIM 署名（DomainKeys/DKIM Signing）] をイネーブルにします。

ステップ 3 変更を送信し、保存します。

バウンスおよび遅延メッセージの署名のイネーブル化

発信メッセージに署名するだけでなく、バウンスおよび遅延メッセージに署名したい場合があります。これにより、会社から受信するバウンスおよび遅延メッセージが正当なものであることを受信者に警告したい場合があります。バウンスおよび遅延メッセージの DomainKeys および DKIM 署名をイネーブルにするには、公開リスナーに関連付けられたバウンス プロファイルの DomainKeys/DKIM 署名をイネーブルにします。

手順

ステップ 1 署名された発信メッセージを送信する公開リスナーに関連付けられているバウンス プロファイルで、[ハード バウンスと遅延警告メッセージ（Hard Bounce and Delay Warning Messages）] に移動します。

ステップ 2 [バウンスおよび遅延メッセージに対してドメインキー署名を使用（Use Domain Key Signing for Bounce and Delay Messages）] をイネーブルにします。

（注） バウンスおよび遅延メッセージに署名するには、DomainKeys/DKIM 署名の設定（GUI）（748 ページ）に示されたすべての手順を完了している必要があります。

ドメイン プロファイルの [差出人：（From:）] アドレスは、バウンス返信アドレスに使用されているアドレスと一致している必要があります。これらのアドレスを一致させるには、バウンス プロファイルの返信アドレスを設定し（[システム管理（System Administration）] > [返信先アドレス（Return Addresses）]）、ドメイン プロファイルの [ユーザのプロファイリング（Profile Users）] リストで同じ名前を使用します。たとえば、バウンス返信アドレスに MAILER-DAEMON@example.com の返信アドレスを設定し、ドメイン プロファイルにプロファイル ユーザとして MAILER-DAEMON@example.com を追加します。

DomainKeys/DKIM 署名の設定（GUI）

手順

ステップ 1 新規の秘密キーを作成するか、既存の秘密キーをインポートします。署名キーの作成またはインポートについては、署名キー （744 ページ）を参照してください。

ステップ 2 ドメイン プロファイルを作成し、キーをドメイン プロファイルに関連付けます。ドメイン プロファイルの作成については、ドメイン プロファイル （746 ページ）を参照してください。

ステップ 3 DNS テキスト レコードを作成します。DNS テキスト レコードの作成については、DNS テキスト レコードの生成 （755 ページ）を参照してください。

ステップ 4 発信メールのメール フロー ポリシーで、DomainKeys/DKIM 署名をまだイネーブルにしていない場合は、イネーブルにします（送信メールの署名のイネーブル化（747 ページ）を参照してください）。

ステップ 5 任意で、バウンスおよび遅延メッセージの DomainKeys/DKIM 署名をイネーブルにします。バウンスおよび遅延メッセージの署名のイネーブル化については、バウンスおよび遅延メッセージの署名のイネーブル化 （747 ページ）を参照してください。

ステップ 6 電子メールを送信します。ドメインプロファイルに一致するドメインから送信されたメールは DomainKeys/DKIM 署名されます。さらに、バウンスおよび遅延メッセージの署名を設定した場合は、バウンスまたは遅延メッセージに署名されます。

（注） DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

次のタスク

関連項目

• DomainKeys 署名のドメイン プロファイルの作成 （749 ページ）
• DKIM 署名の新しいドメイン プロファイルの作成 （750 ページ）
• 署名キーの作成または編集 （752 ページ）
• 既存の署名キーのインポートまたは入力 （753 ページ）
• ドメイン プロファイルのテスト （756 ページ）
• DKIM グローバル設定の編集 （758 ページ）

DomainKeys 署名のドメイン プロファイルの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profile）] セクションで、[プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します

ステップ 4 [ドメインキータイプ（Domain Key Type）] については、[ドメインキー（Domain Keys）] を選択します。

新しいオプションがページに表示されます。

ステップ 5 ドメイン名を入力します。

ステップ 6 セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メール ヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。

ステップ 7 正規化（[no forwarding whitespaces] または [simple]）を選択します。

ステップ 8 すでに署名キーを作成している場合、署名キーを選択します。それ以外の場合は、次のステップに進みます。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。署名キーの作成または編集 （752 ページ）を参照してください。

ステップ 9 署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。

ステップ 10 変更を送信し、保存します。

ステップ 11 この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（送信メールの署名のイネーブル化 （747 ページ）を参照してください）。

（注） DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

DKIM 署名の新しいドメイン プロファイルの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profile）] セクションで、[プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します

ステップ 4 [ドメインキータイプ（Domain Key Type）] に対して、[DKIM] を選択します。

新しいオプションがページに表示されます。

ステップ 5 ドメイン名を入力します。

ステップ 6 セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メール ヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。

ステップ 7 ヘッダーの正規化を選択します。次のオプションから選択します。

- [Relaxed]。「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。ヘッダー名を小文字に変更し、ヘッダーを展開して、連続した空白を 1 つの空白に短縮し、先頭と末尾の空白を取り除きます。
- [Simple]。 ヘッダーは変更されません。

ステップ 8 本文の正規化を選択します。次のオプションから選択します。

- [Relaxed]。「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。本文末尾の空の行を取り除き、行中の空白を 1 つの空白に短縮し、行の末尾の空白を取り除きます。
- **[Simple]。**本文末尾の空の行を取り除きます。

ステップ 9 すでに署名キーを作成している場合、署名キーを選択します。それ以外の場合は、次のステップに進みます。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。署名キーの作成または編集 （752 ページ）を参照してください。

ステップ 10 署名するヘッダーのリストを選択します。次のヘッダーから選択できます。

- [すべて（All）]。 AsyncOS は署名時に存在するすべてのヘッダーに署名します。送信中にヘッダーの追加や削除が予想されない場合は、すべてのヘッダーに署名することが考えられます。
- [標準（Standard）]。 送信中にヘッダーの追加や削除が予想される場合は、標準ヘッダーを選択することが考えられます。AsyncOS は次の標準ヘッダーにのみ署名します（メッセージにそのヘッダーが存在しない場合、DKIM 署名は、そのヘッダーにヌル値を示します）。

- From
- Sender、Reply To-
- Subject
- Date、Message-ID
- To、Cc
- MIME-Version
- Content-Type、Content-Transfer-Encoding、Content-ID、Content-Description
- Resent-Date、Resent-From、Resent-Sender、Resent-To、Resent-cc、Resent-Message-ID
- In-Reply-To、References
- List-Id、List-Help、List-Unsubscribe、LIst-Subscribe、List-Post、List-Owner、List-Archive

（注） [標準（Standard）] を選択した場合、署名するヘッダーを追加できます。

ステップ 11 メッセージ本文に署名する方法を指定します。メッセージ本文に署名するか、署名するバイト数を選択できます。次のオプションのいずれかを選択します。

- [本文全体を含む（Whole Body Implied）]。本文の長さを判断するために「l=」タグを使用しないでください。メッセージ全体に署名し、変更を許可しません。
- [本文全体を自動判断（Whole Body Auto-determined）]。メッセージ本文全体に署名し、送信中に本文の末尾へのデータの追加を許可します。
- **[最初に署名 _ バイト（Sign first _ bytes）]**。指定したバイト数まで、メッセージ本文に署名します。

ステップ 12 メッセージ署名のヘッダーフィールドに含めるタグを選択します。これらのタグに格納されている情報はメッセージ署名の検証に使用されます。次のオプションから 1 つ以上を選択します。

- ["i" タグ]。署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。ドメイン @example.com など、@記号が付加されたドメイン名を入力します。
- ["q" タグ]。公開キーを取得するために使用されるクエリー方法のコロン区切りリスト。現在、唯一有効な値は dns/txt です。
- ["t" タグ]。署名が作成されたときのタイムスタンプを表示します。
- ["x" タグ]。署名が終了する絶対的な日時。署名の有効期限（秒単位）を指定します。デフォルトは 31536000 秒です。
- ["z" タグ]。垂直バー（|）によって区切られているヘッダーフィールドのリストには、メッセージが署名された時が示されます。これには、ヘッダーフィールドの名前と値が含まれます。次に例を示します。

z=From:admin@example.come|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700

ステップ 13 署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。

（注） ドメインプロファイルを作成する場合、特定のユーザに関連付けるプロファイルの決定において、階層を使用することに注意してください。たとえば、example.com のプロファイルと joe@example.com の別のプロファイルを作成するとします。joe@example.com からメールが送信される場合、joe@example.com のプロファイルが使われます。しかし、メールが adam@example.com から送信される場合は、example.com のプロファイルが使われます。

ステップ 14 変更を送信し、保存します。

ステップ 15 この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（送信メールの署名のイネーブル化（747 ページ）を参照してください）。

（注） DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

署名キーの作成または編集

- 新しい署名キーの作成 （752 ページ）
- 既存の署名キーの編集 （753 ページ）

新しい署名キーの作成

署名キーは DomainKeys および DKIM 署名のドメイン プロファイルに必要です。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。

ステップ 2 [キーを追加（Add Key）] をクリックします。

ステップ 3 キーの名前を入力します。

ステップ 4 [生成（Generate）] をクリックし、キー サイズを選択します。

ステップ 5 変更を送信し、保存します。

（注） キーを割り当てるドメインプロファイルを編集していない場合は、編集する必要がある場合があります。

既存の署名キーの編集

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 目的の署名キーをクリックします。
ステップ 3 新しい署名キーの作成 （752 ページ）の説明に従って、目的のフィールドを編集します。
ステップ 4 変更を送信し、保存します。

署名キーのエクスポート

電子メールゲートウェイのすべてのキーは、1 つのテキストファイルとしてエクスポートされます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 [キーをエクスポート（Export Keys）] をクリックします。
ステップ 3 ファイルの名前を入力し、**[送信（Submit）]** をクリックします。

既存の署名キーのインポートまたは入力

関連項目

- キーの貼り付け （753 ページ）
- 既存のエクスポート ファイルからのキーのインポート （754 ページ）

キーの貼り付け

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 [キーを追加（Add Key）] をクリックします。
ステップ 3 [貼り付けキー（Paste Key）] フィールドにキーを貼り付けます（PEM フォーマットされ、RSA キーのみである必要があります）。
ステップ 4 変更を送信し、保存します。

既存のエクスポート ファイルからのキーのインポート

（注） キー ファイルを取得するには、署名キーのエクスポート （753 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 [キーをインポート（Import Keys）] をクリックします。
ステップ 3 エクスポートされた署名キーを含むファイルを選択します。
ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存の署名キーが置き換えられることが警告されます。テキスト ファイルのすべてのキーがインポートされます。
ステップ 5 [インポート（Import）] をクリックします。

署名キーの削除

関連項目

- 選択した署名キーの削除 （754 ページ）
- すべての署名キーの削除 （754 ページ）

選択した署名キーの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 削除する各署名キーの右のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

すべての署名キーの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] を選択します。
ステップ 2 [署名キー（Signing Keys）] ページの [すべてのキーを消去（Clear All Keys）] をクリックします。

ステップ 3 削除を確認します。

DNS テキスト レコードの生成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profiles）] セクションの [DNSテキストレコード（DNS Text Record）] 列で、対応するドメイン プロファイルの [生成（Generate）] リンクをクリックします。

ステップ 3 DNS テキスト レコードに含める属性のチェックボックスをオンにします。

ステップ 4 [再生成（Generate Again）] をクリックして、変更を含めてキーを再生成します。

ステップ 5 DNS テキスト レコードがウィンドウの下部のテキスト フィールド（コピーできます）に表示されます。場合によっては、複数の文字列の DNS テキスト レコードが生成されます。複数の文字列の DNS テキスト レコード （755 ページ）を参照してください。

ステップ 6 [完了（Done）] をクリックします。

次のタスク

関連項目

- 複数の文字列の DNS テキスト レコード （755 ページ）

複数の文字列の DNS テキスト レコード

DNS テキスト レコードの生成に使用される署名キーのサイズが 1024 ビットより大きい場合は、複数の文字列の DNS テキスト レコードが生成されることがあります。これは、DNS テキスト レコードの単一の文字列に含めることができるのは、255 文字以下であるためです。一部の DNS サーバでは複数の文字列の DNS テキスト レコードが受け入れられないか、実行されないため、DKIM 認証は失敗する可能性があります。

このシナリオを回避するために、二重引用符を使用して、複数の文字列の DNS テキスト レコードを、255 バイト未満の文字列に分割することを推奨します。次に、例を示します。

```
s._domainkey.domain.com. IN TXT "v=DKIM1;"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE"
"A4Vbhjq2n/3DbEk6EHdeVXlIXFT7OEl81amoZLbvwMX+bej"
"CdxcsFV3uS7G8oOJSWBP0z++nTQmy9ZDWfaiopU6k7tzoi"
"+oRDlKkhCQrM4oP2B2F5sTDkYwPY3Pen2jgC2OgbPnbo3o"
"m3c1wMWgSoZxoZUE4ly5kPuK9fTtpeJHNiZAqkFICiev4yrkL"
"R+SmFsJn9MYH5+lchyZ74BVm+16Xq2mptWXEwpiwOxWI"
"YHXsZo2zRjedrQ45vmgb8xUx5ioYY9/yBLHudGc+GUKTj1i4"
"mQg48yCD/HVNfsSRXaPinliEkypH9cSnvgvWuIYUQz0dHU;"
```

このようにして分割された DNS テキスト レコードが、DKIM 実装により、処理前に元の単一の文字列に再構築されます。

ドメイン プロファイルのテスト

署名キーを作成し、それをドメイン プロファイルに関連付け、DNS テキストを生成して、権限のある DNS に挿入したら、ドメイン プロファイルをテストできます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメイン署名プロファイル（Domain Signing Profiles）] セクションの [テストプロファイル（Test Profile）] 列で、ドメイン プロファイルの [テスト（Test）] リンクをクリックします。

ステップ 3 成功または失敗を示すメッセージがページの上部に表示されます。テストが失敗した場合、エラー テキストを含む警告メッセージが表示されます。

ドメイン プロファイルのエクスポート

電子メールゲートウェイのすべてのドメインプロファイルは、単一のテキストファイルにエクスポートされます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメインプロファイルのエクスポート（Export Domain Profiles）] をクリックします。

ステップ 3 ファイルの名前を入力し、**[送信（Submit）]** をクリックします。

ドメイン プロファイルのインポート

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [ドメインプロファイルのインポート（Import Domain Profiles）] をクリックします。

ステップ 3 エクスポートされたドメイン プロファイルを含むファイルを選択します。

ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存のドメインプロファイルが置き換えられることが警告されます。テキスト ファイルのすべてのドメイン プロファイルがインポートされます。

ステップ 5 [インポート（Import）] をクリックします。

ドメイン プロファイルの削除

関連項目

- ドメイン プロファイルの削除 （757 ページ）
- すべてのドメイン プロファイルの削除 （757 ページ）

ドメイン プロファイルの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。
ステップ 2 削除する各ドメイン プロファイルの右のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

すべてのドメイン プロファイルの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。
ステップ 2 [すべて消去（Clear All）] をクリックします。
ステップ 3 削除を確認します。

ドメイン プロファイルの検索

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。
ステップ 2 [ドメインプロファイルの検索（Find Domain Profiles）] セクションで、検索条件を指定します。
ステップ 3 [プロファイルの検索（Find Profiles）] をクリックします。
ステップ 4 検索では、各ドメイン プロファイルの email、domain、selector、signing key name のフィールドがスキャンされます。

（注） 検索語を入力しない場合、検索エンジンはすべてのドメイン プロファイルを返します。

DKIM グローバル設定の編集

DKIM のグローバル設定を使用して、次のことを行うかどうかを選択できます。

- DKIM 署名でシステムによって生成されたメッセージに署名します。電子メールゲートウェイは、次のメッセージに署名します。
  - Cisco IronPort スパム隔離通知
  - コンテンツ フィルタで生成された通知
  - 設定メッセージ
  - サポート リクエスト
- DKIM 署名の From ヘッダーの使用

手順

ステップ 1 [メールポリシー（Mail Policies）] > [署名プロファイル（Signing Profiles）] を選択します。

ステップ 2 [DKIMグローバル設定（DKIM Global Settings）] の下の [設定の編集（Edit Settings）] をクリックします。

ステップ 3 要件に応じて、次のフィールドを設定します。

- システム生成メッセージのDKIM署名（DKIM Signing of System Generated Messages）
- DKIM 署名の From ヘッダーの使用

（注） DKIM 署名に From ヘッダーを使用していない場合、または有効な From ヘッダーが存在しない場合は、Sender ヘッダーが使用されます。DKIM 署名済みメッセージの DMARC 検証の場合、DKIM 署名中は From ヘッダーを使用する必要があります。

ステップ 4 変更を送信し、保存します。

ドメイン キーとロギング

DomainKeys 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

DKIM 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

DKIM を使用した受信メッセージの検証方法

DKIM を使用した受信メッセージの検証方法

	操作内容	詳細
ステップ 1	DKIMを使用してメッセージを検証するプロファイルを作成します。	DKIM検証プロファイルの作成 （761 ページ）
ステップ 2	（任意）DKIMを使用した受信メッセージの検証に使用されるカスタムのメール フローポリシーを作成します。	メール フロー ポリシーを使用した着信メッセージのルールの定義 （124 ページ）
ステップ 3	DKIMを使用して受信メッセージを検証するようにメールフローポリシーを設定します。	メール フロー ポリシーでの DKIM 検証の設定 （763 ページ）
ステップ 4	電子メールゲートウェイが確認されたメッセージで実行するアクションを定義します。	DKIM 検証済みメールのアクションの設定 （764 ページ）
ステップ 5	特定の送信者または受信者のグループにアクションを関連付けます。	メール ポリシーの設定 （316 ページ）

関連項目

- AsyncOS による DKIM 検証チェック （759 ページ）
- DKIM 検証プロファイルの管理 （760 ページ）
- メール フロー ポリシーでの DKIM 検証の設定 （763 ページ）
- DKIM 検証済みメールのアクションの設定 （764 ページ）

AsyncOS による DKIM 検証チェック

DKIM 検証用に AsyncOS 電子メールゲートウェイを設定すると、次のチェックが実行されます。

手順

ステップ 1 AsyncOS は受信メールの [DKIMシグネチャ（DKIM-Signature）] フィールド、署名ヘッダーの構文、有効なタグ値、必須タグを調べます。署名がこれらのいずれかのチェックで失敗すると、AsyncOS は *permfail* を返します。

ステップ 2 署名チェックの実行後、公開 DNS レコードから公開キーが取得され、TXT レコードが検証されます。このプロセス中にエラーが検出されると、AsyncOS は *permfail* を返します。公開キーの DNS クエリーで応答を取得できない場合、*tempfail* が発生します。

ステップ 3 公開キーの取得後、AsyncOS はハッシュ値をチェックし、署名を検証します。この手順中にエラーが発生すると、AsyncOS は *permfail* を返します。

ステップ 4 チェックにすべて合格すると、AsyncOS は *pass* を返します。

（注） メッセージ本文が指定された長さより長い場合、AsyncOS は次の判定を返します。

```
dkim = pass (partially verified [x bytes])
```

ここで *X* は検証されたバイト数を表します。

最終検証結果は、*Authentication-Results* ヘッダーとして入力されます。たとえば、次のいずれかのようなヘッダーを受け取ることがあります。

```
Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (signature verified)

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```

（注） 現在の DKIM 検証は最初の有効な署名で停止します。最後に検出された署名を使用して、検証できません。この機能は、後のリリースで使用できるようになる可能性があります。

ドメインに DKIM テストモードでその DNS TXT レコードがあるとき（`t=y`）、電子メールゲートウェイは DKIM 検証と操作を完全にスキップします。

DKIM 検証プロファイルの管理

DKIM 検証プロファイルは電子メールゲートウェイのメールフローポリシーが DKIM 署名を保証するために使用されるパラメータのリストです。たとえば、クエリーがタイムアウトする前に 30 秒取る検証プロファイルと、クエリーがタイムアウトする前に 3 秒だけ取る検証プロファイルの、2 つの検証プロファイルを作成できます。THROTTLED メール フロー ポリシーに 2 つ目の検証プロファイルを割り当てて、DDoS の場合の接続スタベーションを防止できます。検証プロファイルは次の情報で構成されます。

- 検証プロファイルの名前。
- 許容できる公開キーの最小、最大サイズ。デフォルトのキーのサイズは 512 および 2048 です。
- メッセージの中で検証できる署名の最大数。メッセージに定義した署名の最大数よりも多くの署名がある場合、電子メールゲートウェイは残りの署名の検証をスキップし、メッセージの処理を続行します。デフォルトは、5 つの署名です。
- 送信者のシステム時刻と検証者のシステム時刻との間の時間の最大許容差（秒単位）。たとえば、メッセージ署名が 05:00:00 に期限切れとなり、検証者のシステム時刻が 05:00:30 である場合、時間の許容差が 60 秒であればメッセージ署名は有効なままですが、許容差が 10 秒であれば無効になります。デフォルトは 60 秒です。
- 本文の長さのパラメータを使用するかどうかを指定するオプション。

- 一時的な障害の場合に実行する SMTP アクション。
- 永続的な障害の場合に実行する SMTP アクション。

プロファイル名ですべての既存の検証プロファイルを検索できます。

電子メールゲートウェイの configuration ディレクトリに DKIM 検証プロファイルをテキストファイルとしてエクスポートできます。検証プロファイルをエクスポートすると、電子メールゲートウェイに存在するすべてのプロファイルが 1 つのテキストファイルに挿入されます。詳細については、DKIM 検証プロファイルのエクスポート （762 ページ）を参照してください。

以前エクスポートした DKIM 検証プロファイルをインポートできます。DKIM 検証プロファイルをインポートすると、マシンの現在のすべての DKIM 検証プロファイルを置き換えることになります。詳細については、DKIM 検証プロファイルのインポート （762 ページ）を参照してください。

関連項目

- DKIM 検証プロファイルの作成 （761 ページ）
- DKIM 検証プロファイルのエクスポート （762 ページ）
- DKIM 検証プロファイルのインポート （762 ページ）
- DKIM 検証プロファイルの削除 （762 ページ）
- DKIM 検証プロファイルの検索 （763 ページ）

DKIM 検証プロファイルの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] をクリックします。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 電子メールゲートウェイが許可する署名キーの最小キーサイズを選択します。

ステップ 5 電子メールゲートウェイが許可する署名キーの最大キーサイズを選択します。

ステップ 6 1 つのメッセージで検証する署名の最大数を選択します。デフォルトは 5 つの署名です。

ステップ 7 キー クエリーがタイムアウトするまでの時間（秒）を選択します。デフォルトは 10 秒です。

ステップ 8 送信者のシステム時刻と検証者のシステム時刻との間の時間の最大許容差（秒単位）を選択します。デフォルトは 60 秒です。

ステップ 9 メッセージの検証に、署名の本文の長さのパラメータを使用するかどうか選択します。

ステップ 10 署名を確認するときに一時的な障害がある場合、電子メールゲートウェイがメッセージを受け入れるか、拒否するかを選択します。電子メールゲートウェイがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。

ステップ 11 署名を確認するときに永続的な障害がある場合は、電子メールゲートウェイがメッセージを受け入れるか、拒否するかを選択します。電子メールゲートウェイがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。

ステップ 12 変更を送信します。

新しいプロファイルが DKIM 検証プロファイルのテーブルに表示されます。

ステップ 13 変更を保存します。

ステップ 14 この時点で着信メールフローポリシーでDKIM検証をイネーブルにし、使用する検証プロファイルを選択する必要があります。

DKIM 検証プロファイルのエクスポート

電子メールゲートウェイのすべてのDKIM検証プロファイルは単一のテキストファイルとしてエクスポートされ、電子メールゲートウェイの configuration ディレクトリに保存されます。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[検証プロファイル（Verification Profiles）] を選択します。

ステップ 2 [プロファイルをエクスポート（Export Profiles）] をクリックします。

ステップ 3 ファイルの名前を入力し、**[送信（Submit）]** をクリックします。

DKIM 検証プロファイルのインポート

手順

ステップ 1 [メールポリシー（Mail Policies）]>[検証プロファイル（Verification Profiles）] を選択します。

ステップ 2 [プロファイルをインポート（Import Profiles）] をクリックします。

ステップ 3 DKIM 検証プロファイルを含むファイルを選択します。

ステップ 4 [送信（Submit）] をクリックします。インポートによってすべての既存の DKIM 検証プロファイルが置き換えられることが警告されます。

ステップ 5 [インポート（Import）] をクリックします。

DKIM 検証プロファイルの削除

関連項目

- 選択した DKIM 検証プロファイルの削除 （763 ページ）

• すべての DKIM 検証プロファイルの削除 （763 ページ）

選択した DKIM 検証プロファイルの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 削除する各 DKIM 検証プロファイルの右のチェックボックスをオンにします。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

すべての DKIM 検証プロファイルの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 [すべて消去（Clear All）] をクリックします。
ステップ 3 削除を確認します。

DKIM 検証プロファイルの検索

すべての DKIM 検証プロファイルについてプロファイル名から特定の用語を検索します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] を選択します。
ステップ 2 [次のDKIM検証プロファイルを検索（Search DKIM Verification Profiles）] セクションで、検索条件を指定します。
ステップ 3 [プロファイルの検索（Find Profiles）] をクリックします。

検索では、各 DKIM 検証プロファイル名をスキャンします。

検索語を入力しない場合、検索エンジンはすべての DKIM 検証プロファイルを返します。

メール フロー ポリシーでの DKIM 検証の設定

DKIM 検証は、受信メールのメール フロー ポリシーでイネーブルにします。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] を選択します。

ステップ 2 検証を実行するリスナーの着信メール ポリシーをクリックします。

ステップ 3 メール フロー ポリシーの [セキュリティサービス（Security Features）] セクションで、[オン（On）] を選択して、[DKIM検証（DKIM Verification）] をイネーブルにします。

ステップ 4 ポリシーで使用する DKIM 検証プロファイルを選択します。

ステップ 5 変更を保存します。

次のタスク

関連項目

- DKIM 検証とロギング （764 ページ）

DKIM 検証とロギング

DKIM 検証時には、次のような行がメール ログに追加されます。

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature

mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

DKIM 検証済みメールのアクションの設定

DKIM メールを検証すると、メールに Authentication-Results ヘッダーが追加されますが、認証結果に関係なく、メールは受け入れられます。これらの認証結果に基づいてアクションを設定するには、コンテンツ フィルタを作成して、DKIM 検証済みメールに対するアクションを実行します。たとえば、DKIM 検証が失敗した場合、メールを配信、バウンス、ドロップ、または隔離エリアに送るように設定できます。これを実行するには、コンテンツ フィルタを使用して、アクションを設定する必要があります。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] を選択します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 [条件（Conditions）] セクションで、[条件を追加（Add Condition）] をクリックします。

ステップ 4 条件のリストから [DKIM認証（DKIM Authentication）] を選択します。

ステップ 5 DKIM 条件を選択します。次のオプションのいずれかを選択します。

- **[Pass]**。メッセージは認証テストに合格しました。

- [Neutral]。認証が実行されませんでした。
- [Temperror]。 修復可能なエラーが発生しました。
- [Permerror]。 修復不可能なエラーが発生しました。
- [Hardfail]。 認証テストが失敗しました。
- [None]。 メッセージは署名されていません。

ステップ 6 条件に関連付けるアクションを選択します。たとえば、DKIM検証が失敗した場合、受信者に通知し、メッセージをバウンスさせることができます。またはDKIM検証に合格した場合、それ以上処理せずに、メッセージをすぐに配信できます。

ステップ 7 新しいコンテンツ フィルタを送信します。

ステップ 8 適切な受信メール ポリシーでコンテンツ フィルタをイネーブルにします。

ステップ 9 変更を保存します。

SPF および SIDF 検証の概要

AsyncOS は、Sender Policy Framework（SPF）および Sender ID Framework（SIDF）検証をサポートしています。SPF と SIDF は DNS レコードに基づいて電子メールの信頼性を検証する方法です。SPF と SIDF により、インターネット ドメインの所有者は、特別な形式の DNS TXT レコードを使用して、そのドメインに電子メールを送信する権限のあるマシンを指定することができます。準拠したメール受信側は、パブリッシュされた SPF レコードを使用して、メール トランザクション中に、送信側のメール転送エージェントの ID の権限をテストします。

SPF/SIDF 認証を使用すると、送信側はそれらの名前の使用が許可されるホストを指定する SPF レコードをパブリッシュし、準拠するメール受信側はパブリッシュされた SPF レコードを使用して、メール トランザクション中に送信側のメール転送エージェントの ID の権限をテストします。

（注） SPF チェックでは、解析と評価が必要であるため、AsyncOS のパフォーマンスに影響する場合があります。さらに、SPF チェックによって、DNS インフラストラクチャの負荷が増えることに注意してください。

SPF と SIDF を操作する場合、SIDF は SPF に似ていますが、いくつかの違いがあります。SIDF と SPF の違いに関する詳しい説明については、RFC 4406 を参照してください。このマニュアルの目的のため、この 2 つの用語は、1 つのタイプの検証のみを適用する場合を除いて、まとめて説明しています。

（注） AsyncOS は着信リレーに対して SPF をサポートしていません。

関連項目

- 有効な SPF レコードに関する注意 （766 ページ）

有効な SPF レコードに関する注意

電子メールゲートウェイで SPF および SIDF を使用するには、RFC 4406、4408 および 7208 に従って、SPF レコードをパブリッシュします。PRA ID の決定方法の定義については、RFC 4407 を確認してください。さらに、SPF レコードと SIDF レコードを作成する場合に犯しやすい誤りについては、次の Web サイトを参照してください。

http://www.openspf.org/FAQ/Common_mistakes

関連項目

- 有効な SPF レコード （766 ページ）
- 有効な SIDF レコード （766 ページ）
- SPF レコードのテスト （767 ページ）

有効な SPF レコード

SPF HELO チェックに合格するには、各送信側 MTA に（ドメインとは別に）「v=spf1 a –all」SPF レコードを含めます。このレコードを含めないと、HELO チェックは HELO ID に None 判定を下す可能性があります。ドメインへの SPF 送信側が大量の None 判定を返した場合、これらの送信側は各送信側 MTA に「v=spf1 a –all」SPF レコードを含めていない可能性があります。

有効な SIDF レコード

SIDF フレームワークをサポートするには、「v=spf1」レコードと「spf2.0」レコードの両方をパブリッシュする必要があります。たとえば、DNS レコードは次の例のようになります。

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"

smtp-out.example.com TXT "v=spf1 a -all"

example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF は HELO ID を検証しないため、この場合、各送信側 MTA に SPF v2.0 レコードをパブリッシュする必要はありません。

（注） SIDF をサポートしない場合は、「spf2.0/pra ~all」レコードをパブリッシュします。

SPF レコードのテスト

RFC の確認に加えて、電子メールゲートウェイに SPF 検証を実装する前に、SPF レコードをテストすることを推奨します。openspf.org Web サイトでは、いくつかのテスト ツールが提供されています。

http://www.openspf.org/Tools

次のツールを使用して、電子メールが SPF レコードチェックに失敗した理由を判断できます。

http://www.openspf.org/Why

さらに、テストリスナーで SPF をイネーブルにし、シスコの trace CLI コマンドを使用して（または GUI からトレースを実行して）、SPF 結果を表示できます。トレースを使用すると、さまざまな送信側 IP を簡単にテストできます。

SPF/SIDF を使用した受信メッセージの検証方法

	操作内容	詳細
ステップ 1	（任意）SPF/SIDF を使用した受信メッセージの検証に使用されるカスタムのメール フロー ポリシーを作成します。	メール フロー ポリシーを使用した着信メッセージのルールの定義（124 ページ）
ステップ 2	SPF/SIDF を使用して受信メッセージを検証するようにメール フロー ポリシーを設定します。	SPF と SIDF のイネーブル化 （768 ページ）
ステップ 3	電子メールゲートウェイが確認されたメッセージで実行するアクションを定義します。	SPF/SIDF 検証済みメールに対して実行するアクションの決定 （773 ページ）
ステップ 4	特定の送信者または受信者のグループにアクションを関連付けます。	メール ポリシーの設定 （316 ページ）
ステップ 5	（任意）メッセージの検証の結果をテストします。	SPF/SIDF 結果のテスト （776 ページ）

注意 シスコでは、グローバルな電子メール認証を強く奨励していますが、業界での採用途上にある現時点では、SPF/SIDF 認証の失敗に対して慎重な処理を行うよう提案しています。さらに多くの組織で社内公認のメール送信インフラストラクチャの制御能力が向上するまでは、シスコは電子メールのバウンスを回避し、代わりに SPF/SIDF 検証に失敗した電子メールを隔離できます。

（注） AsyncOS コマンドライン インターフェイス（CLI）では、Web インターフェイスよりも詳細な SPF レベルの制御設定を提供しています。SPF 判定に基づいて、電子メールゲートウェイは、リスナー単位で SMTP カンバセーションにおいてメッセージを許可または拒否できます。SPF の設定は、listenerconfig コマンドを使用してリスナーのホスト アクセス テーブルのデフォルト設定を編集するときに変更できます。設定の詳細については、CLI を使用した SPF および SIDF のイネーブル化 （769 ページ）を参照してください。

SPF と SIDF のイネーブル化

SPF/SIDF を使用するには、受信リスナーでメール フロー ポリシーの SPF/SIDF をイネーブルにする必要があります。デフォルトのメール フロー ポリシーから、リスナーで SPF/SIDF をイネーブルにするか、特定の受信メール ポリシーについて SPF/SIDF をイネーブルにすることができます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policy）] を選択します。

ステップ 2 [デフォルトポリシーパラメータ（Default Policy Parameters）] をクリックします。

ステップ 3 デフォルトのポリシーパラメータで、[セキュリティサービス（Security Features）]セクションを表示します。

ステップ 4 [SPF/SIDF検証（SPF/SIDF Verification）] セクションで、[オン（On）] をクリックします。

ステップ 5 準拠のレベルを設定します（デフォルトは SIDF 互換）。このオプションを使用して、使用する SPF または SIDF 検証の規格を判断できます。SIDF 準拠に加えて、SPF と SIDF を組み合わせた SIDF 互換を選択できます

SPF/SIDF 準拠レベル

準拠レベル	説明
SPF	SPF/SIDF 検証は RFC4408 および RFC7208 に従って動作します。 - PRA（Purported Responsible Address）ID 検証は行われません。 **注**：HELO ID に対してテストするには、この準拠オプションを選択します。

準拠レベル	説明
SIDF	SPF/SIDF 検証は RFC4406 に従って動作します。 - PRA ID は規格への完全準拠によって判断されます。 - SPF v1.0 レコードは spf2.0/mfrom,pra として扱われます。 - 存在しないドメインや形式が誤った ID については、Fail の判定が返されます。
SIDF 互換（SIDF Compatible）	SPF/SIDF 検証は、次の違いを除き、RFC4406 に従って動作します。 - SPF v1.0 レコードは spf2.0/mfrom として扱われます。 - 存在しないドメインや形式が誤った ID については、None の判定が返されます。 **注**：この準拠オプションは、OpenSPF コミュニティ（www.openspf.org）の要求に応じて導入されました。

（注） CLI からはさらに多くの設定を使用できます。詳細については、CLI を使用した SPF および SIDF のイネーブル化 （769 ページ）を参照してください。

ステップ 6 SIDF 互換の準拠レベルを選択した場合、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうかを設定します。このオプションをセキュリティ目的で選択できます。

ステップ 7 SPF の準拠レベルを選択した場合、HELO ID に対してテストを実行するかどうかを設定します。このオプションを使用して、HELOチェックをディセーブルにすることによって、パフォーマンスが向上することがあります。これは、spf-passed フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。電子メールゲートウェイは SPF 準拠レベルに対してのみ HELO チェックを実行します。

次のタスク

関連項目

- Received-SPF ヘッダー （772 ページ）
- CLI を使用した SPF および SIDF のイネーブル化 （769 ページ）

CLI を使用した SPF および SIDF のイネーブル化

AsyncOS CLI では各 SPF/SIDF 準拠レベルのより詳細な制御設定をサポートしています。リスナーのホストアクセステーブルのデフォルトの設定をする場合、リスナーの SPF/SIDF 準拠レベルと、電子メールゲートウェイが SPF/SIDF 検証結果に基づいて実行する SMTP アクション（ACCEPT または REJECT）を選択できます。電子メールゲートウェイがメッセージを拒否する場合に送信する SMTP 応答を定義することもできます。

準拠レベルに応じて、電子メールゲートウェイは HELO ID、MAIL FROM ID、または PRA ID に対してチェックを実行します。電子メールゲートウェイが、次の各 ID チェックの各 SPF/SIDF 検証結果に対し、セッションを続行する（ACCEPT）か、セッションを終了する（REJECT）かを指定できます。

- **なし。**情報の不足のため、検証を実行できません。
- **[Neutral]。**ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- **[SoftFail]。**ドメイン所有者は、ホストが指定された ID を使用する権限がないと思うが、断言を避けたいと考えています。
- **[失敗]**：クライアントは、指定された ID でメールを送信する権限がありません。
- **[TempError]。**検証中に一時的なエラーが発生しました。
- **[Permerror]。**検証中に永続的なエラーが発生しました。

電子メールゲートウェイは、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、PRA ID の Pass 結果を None にダウングレードするように SIDF 互換準拠レベルを設定していない限り、Pass 結果のメッセージを受け入れます。電子メールゲートウェイは PRA チェックで None が返された場合に指定された SMTP アクションを実行します。

ID チェックに対して SMTP アクションを定義していない場合、電子メールゲートウェイは Fail を含むすべての検証結果を自動的に受け入れます。

イネーブルにされたいずれかの ID チェックの ID 検証結果が REJECT アクションに一致する場合、電子メールゲートウェイはセッションを終了します。たとえば、管理者は、すべての HELO ID チェック結果に基づいてメッセージを受け入れるようにリスナーを設定しますが、MAIL FROM ID チェックからの Fail 結果に対してはメッセージを拒否するようにリスナーを設定するとします。メッセージが HELO ID チェックに失敗しても、電子メールゲートウェイはその結果を受け入れるため、セッションが続行します。次に、メッセージが MAIL FROM ID チェックで失敗した場合、リスナーはセッションを終了し、REJECT アクションの STMP 応答を返します。

SMTP 応答は、電子メールゲートウェイが SPF/SIDF 検証結果に基づいてメッセージを拒否する場合に返すコード番号とメッセージです。TempError 結果は、他の検証結果と異なる SMTP 応答を返します。TempError の場合、デフォルトの応答コードは 451 で、デフォルトのメッセージ テキストは「`#4.4.3 Temporary error occurred during SPF verification`」です。他のすべての検証結果では、デフォルトの応答コードは 550 で、デフォルトのメッセージ テキストは「`#5.7.1 SPF unauthorized mail is prohibited`」です。TempError や他の検証結果に独自の応答コードとメッセージ テキストを指定できます。

任意で、Neutral、SoftFail、または Fail 検証結果に対して REJECT アクションが実行された場合に、SPF パブリッシャドメインから、サードパーティの応答を返すように、電子メールゲートウェイを設定することができます。デフォルトで、電子メールゲートウェイは次の応答を返します。

```
550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:
```

550 <Response text from SPF domain publisher>

これらの SPF/SIDF 設定をイネーブルにするには、`listenerconfig -> edit` サブコマンドを使用し、リスナーを選択します。次に、`hostaccess -> default` サブコマンドを使用して、ホスト アクセス テーブルのデフォルトの設定を編集します。

ホスト アクセス テーブルでは、次の SPF 制御設定を使用できます。

CLI を使用した SPF 制御設定

準拠レベル	使用可能な SPF 制御設定

SPF のみ（SPF Only）	• HELO ID チェックを実行するかどうか
	• 次の ID チェックの結果に基づいて実行される SMTP アクション
	  • HELO ID（イネーブルの場合）
	  • MAIL FROM ID
	• REJECT アクションに対して返される SMTP 応答コードとテキスト
	• 秒単位の検証タイムアウト

SIDF 互換（SIDF Compatible）	• HELO ID チェックを実行するかどうか
	• メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうか
	• 次の ID チェックの結果に基づいて実行される SMTP アクション
	  • HELO ID（イネーブルの場合）
	  • MAIL FROM ID
	  • PRA Identity
	• REJECT アクションに対して返される SMTP 応答コードとテキスト
	• 秒単位の検証タイムアウト

準拠レベル	使用可能な SPF 制御設定

SIDF 厳格（SIDF Strict）	• 次の ID チェックの結果に基づいて実行される SMTP アクション
	  • MAIL FROM ID
	  • PRA Identity
	• SPF REJECT アクションの場合に返される SMTP 応答コードとテキスト
	• 秒単位の検証タイムアウト

電子メールゲートウェイは HELO ID チェックを実行し、None および Neutral 検証結果を受け入れ、その他の結果を拒否します。SMTP アクションの CLI プロンプトはすべての ID タイプで同じです。ユーザは MAIL FROM ID の SMTP アクションを定義しません。電子メールゲートウェイは、その ID のすべての検証結果を自動的に受け入れます。電子メールゲートウェイはすべての REJECT 結果に対して、デフォルトの拒否コードとテキストを使用します。

また、コマンドライン インターフェイスで `listenerconfig` コマンドを使用して、これを設定することもできます。

Received-SPF ヘッダー

AsyncOS で SPF/SIDF 検証を設定すると、電子メールに SPF/SIDF 検証ヘッダー（`Received-SPF`）が配置されます。さらに、`Received-SPF` ヘッダーには、次の情報が含まれます。

- **検証結果**：SPF 検証結果（検証結果 （773 ページ）を参照してください）。
- **ID**：SPF 検証でチェックされた ID：HELO、MAIL FROM、PRA。
- **レシーバ**：検証するホスト名（チェックを実行する）。
- **クライアント IP アドレス**：SMTP クライアントの IP アドレス。
- **ENVELOPE FROM**：エンベロープ送信者メールボックス。（MAIL FROM ID は空にすることができないため、これは、MAIL FROM ID と異なることがあります）。
- **x-sender**：HELO、MAIL FROM、または PRA ID の値。
- **x-conformance**：準拠のレベル（表「SPF/SIDF 準拠レベル」を参照）と PRA チェックのダウングレードが実行されたかどうか。

次の例に、SPF/SIDF チェックに合格したメッセージに追加されるヘッダーを示します。

```
Received-SPF: Pass identity=pra; receiver=box.example.com;

client-ip=1.2.3.4; envelope-from="alice@fooo.com";

x-sender="alice@company.com"; x-conformance=sidf_compatible
```

（注） `spf-status` および `spf-passed` フィルタ ルールでは、received-SPF ヘッダーを使用して、SPF/SIDF 検証の状態が判断されます。

SPF/SIDF 検証済みメールに対して実行するアクションの決定

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。次のメッセージおよびコンテンツ フィルタ ルールを使用して、SPF/SIDF 検証済みメールの状態を判断し、検証結果に基づいてメッセージへのアクションを実行できます。

- `spf-status`。このフィルタ ルールは SPF/SIDF 状態に基づいてアクションを決定します。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。
- `spf-passed`。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。

（注） `spf-passed` フィルタ ルールはメッセージ フィルタでのみ使用できます。

より詳細な結果に対処する必要がある場合は、`spf-status` ルールを使用し、簡単なブール値を作成する必要がある場合は spf-passed ルールを使用できます。

関連項目

- 検証結果 （773 ページ）
- CLI での spf-status フィルタ ルールの使用 （774 ページ）
- GUI での spf-status コンテンツ フィルタ ルール （775 ページ）
- spf-passed フィルタ ルールの使用 （775 ページ）

検証結果

`spf-status` フィルタ ルールを使用する場合、次の構文を使用して、SPF/SIDF 検証結果に対してチェックできます。

```
if (spf-status == "Pass")
```

1 つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```

（注） spf-status メッセージ フィルタ ルールは、HELO、MAIL FROM、PRA ID に対して結果をチェックする場合にのみ使用できます。spf-status コンテンツ フィルタ ルールは、ID に対してチェックする場合に使用できません。spf-status コンテンツ フィルタは、PRA ID のみをチェックします。

次のいずれかの検証結果を受け取る可能性があります。

- None：情報の不足のため、検証を実行できません。
- Pass：クライアントは、指定された ID でメールを送信する権限があります。
- Neutral：ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- SoftFail：ドメイン所有者は、指定された ID を使用する権限がホストにないと思うが、断言を避けたいと考えています。
- Fail：クライアントは、指定された ID でメールを送信する権限がありません。
- TempError：検証中に一時的なエラーが発生しました。
- PermError：検証中に永続的なエラーが発生しました。

CLI での spf-status フィルタ ルールの使用

次の例に、spf-status メッセージ フィルタの使用例を示します。

```
skip-spam-check-for-verified-senders:

if (sendergroup == "TRUSTED" and spf-status == "Pass"){
skip-spamcheck();
}
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
if (spf-status("mailfrom") == "Fail"){
# completely malicious mail
quarantine("Policy");
} else {
if(spf-status("mailfrom") == "SoftFail") {
# malicious mail, but tempting
quarantine("Policy");
}
}
} else {
```

```
if(spf-status("pra") == "SoftFail"){
if (spf-status("mailfrom") == "Fail"
or spf-status("mailfrom") == "SoftFail"){
# malicious mail, but tempting
quarantine("Policy");
}
}
}
stamp-mail-with-spf-verification-error:
if (spf-status("pra") == "PermError, TempError"
or spf-status("mailfrom") == "PermError, TempError"
or spf-status("helo") == "PermError, TempError"){
# permanent error - stamp message subject
strip-header("Subject");
insert-header("Subject", "[POTENTIAL PHISHING] $Subject");
}
.
```

GUI での spf-status コンテンツ フィルタ ルール

GUI でコンテンツ フィルタから spf-status ルールをイネーブルにすることもできます。ただし、spf-status コンテンツ フィルタ ルールを使用した場合、HELO、MAIL FROM、PRA ID に対して結果をチェックできません。

GUI から spf-status コンテンツ フィルタ ルールを追加するには、[メール ポリシー（Mail Policies）]>[受信コンテンツ フィルタ（Incoming Content Filters）] をクリックします。次に [条件を追加（Add Condition）] ダイアログボックスから、[SPF検証（SPF Verification）] フィルタ ルールを追加します。条件に、1 つ以上の検証結果を指定します。

SPF 検証条件を追加したら、SPF 状態に基づいて実行するアクションを指定します。たとえば、SPF 状態が SoftFail の場合、メッセージを隔離します。

spf-passed フィルタ ルールの使用

`spf-passed` ルールは SPF 検証の結果をブール値として表示します。次の例に、`spf-passed` とマークされていない電子メールを隔離するための `spf-passed` ルールを示します。

```
quarantine-spf-unauthorized-mail:
if (not spf-passed) {
```

```
quarantine("Policy");

}
```

（注） spf-status ルールと異なり spf-passed ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、spf-passed ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、spf-status ルールを使用します。

SPF/SIDF 結果のテスト

組織によって SPF/SIDF の実装方法が異なるため、SPF/SIDF 検証の結果をテストし、これらの結果を使用して、SPF/SIDF の失敗の処理方法を決定します。コンテンツ フィルタ、メッセージ フィルタ、Email Security Monitor - Content Filters レポートを組み合わせて使用し、SPF/SIDF 検証の結果をテストします。

SPF/SIDF 検証の依存度によって、SPF/SIDF 結果をテストする詳細レベルが決まります。

関連項目

- SPF/SIDF 結果の基本の詳細度のテスト （776 ページ）
- SPF/SIDF 結果の高い詳細度のテスト （777 ページ）

SPF/SIDF 結果の基本の詳細度のテスト

受信メールの SPF/SIDF 検証結果の基本評価基準を取得するため、コンテンツ フィルタと [メールセキュリティモニタ-コンテンツフィルタ（Email Security Monitor - Content Filters）] ページを使用できます。このテストでは、SPF/SIDF 検証結果のタイプごとに受信されたメッセージ数が表示されます。

手順

ステップ 1 受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにし、コンテンツ フィルタを使用して、実行するアクションを設定します。SPF/SIDF をイネーブルにする方法については、SPF と SIDF のイネーブル化 （768 ページ）を参照してください。

ステップ 2 SPF/SIDF 検証のタイプごとに **spf-status** コンテンツ フィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには「SPF-Passed」を使用し、検証中の一時的エラーのために合格しなかったメッセージには、「SPF-TempErr」を使用します。**spf-status** コンテンツ フィルタの作成については、GUI での spf-status コンテンツ フィルタ ルール （775 ページ）を参照してください。

ステップ 3 多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ（Monitor）] > [コンテンツフィルタ（Content Filters）] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。

SPF/SIDF 結果の高い詳細度のテスト

SPF/SIDF 検証結果のより包括的な情報を得るには、送信者の特定のグループの SPF/SIDF 検証をイネーブルにし、それらの特定の送信者の結果を確認するだけです。次に、その特定のグループのメール ポリシーを作成し、メール ポリシーで SPF/SIDF 検証をイネーブルにします。SPF/SIDF 結果の基本の詳細度のテスト （776 ページ）で説明するように、コンテンツ フィルタを作成し、Content Filters レポートを確認します。検証が有効であることがわかったら、この指定した送信者のグループの電子メールをドロップするかバウンスするかの決断の基準として、SPF/SIDF 検証を使用できます。

手順

ステップ 1 SPF/SIDF 検証のメール フロー ポリシーを作成します。受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにします。SPF/SIDF をイネーブルにする方法については、SPF と SIDF のイネーブル化 （768 ページ）を参照してください。

ステップ 2 SPF/SIDF 検証の送信者グループを作成し、命名規則を使用して、SPF/SIDF 検証を示します。送信者グループの作成については、「Configuring the Gateway to Receive Mail」の章を参照してください。

ステップ 3 SPF/SIDF 検証のタイプごとに **spf-status** コンテンツ フィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには「SPF-Passed」を使用し、検証中の一時的エラーのために合格しなかったメッセージには、「SPF-TempErr」を使用します。**spf-status** コンテンツ フィルタの作成については、GUI での spf-status コンテンツ フィルタ ルール （775 ページ）を参照してください。

ステップ 4 多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ（Monitor）] > [コンテンツフィルタ（Content Filters）] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。

DMARC 検証

Domain-based Message Authentication, Reporting and Conformance（DMARC）は、電子メールベースの不正利用の可能性を減らすために作成された技術仕様です。DMARC では、電子メールの受信者が SPF および DKIM メカニズムを使用して電子メール認証を行う方法が標準化されています。DMARC 検証に合格するには、電子メールがこれらの認証メカニズムのうち少なくとも 1 つに合格し、認証 ID が RFC 5322 に準拠している必要があります。

電子メールゲートウェイでは、次のことができます。

- DMARC を使用して着信電子メールを検証する。
- ドメイン所有者のポリシーを上書き（受け入れ、隔離、または拒否）するプロファイルを定義する。
- ドメイン所有者に認証の導入環境の強化に役立つフィードバック レポートを送信する。
- DMARC 集計レポートのサイズが 10 MB または DMARC レコードの RUA タグで指定されたサイズを超えた場合に、ドメイン所有者に配信エラー レポートを送信します。

AsyncOS では、2013 年 3 年 31 日に Internet Engineering Task Force（IETF）に提出された DMARC 仕様に準拠する電子メールを処理できます。詳細については、http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02 を参照してください。

（注） 電子メールゲートウェイでは、不正な形式の DMARC レコードを持つドメインからのメッセージの DMARC 検証は実行しません。ただし、 電子メールゲートウェイでもこうしたメッセージを受信して処理することはできます。

関連項目

- DMARC 検証のワークフロー （778 ページ）
- DMARC を使用した受信メッセージの検証方法 （779 ページ）

DMARC 検証のワークフロー

次に、AsyncOS による DMARC 検証の実行方法について説明します。

1. AsyncOS に設定されたリスナーが SMTP 接続を受信します。
2. AsyncOS は、メッセージに対して SPF および DKIM 検証を実行します。
3. AsyncOS は、DNS から送信者のドメインの DMARC レコードを取得します。
   - レコードが見つからない場合、AsyncOS は DMARC 検証をスキップし、処理を続行します。
   - DNS ルックアップが失敗した場合、AsyncOS は指定された DMARC 検証プロファイルに基づいてアクションを実行します。
4. DKIM および SPF 検証の結果に応じて、AsyncOS はメッセージに対して DMARC 検証を実行します。

（注） DKIM および SPF 検証がイネーブルの場合は、DKIM および SPF 検証の結果が DMARC 検証で再利用されます。

5. DMARC 検証の結果と指定された DMARC 検証プロファイルに応じて、AsyncOS はメッセージを受け入れるか、隔離するか、または拒否します。DMARC 検証の失敗によってメッセージが拒否されなかった場合、AsyncOS は処理を続行します。
6. AsyncOS は適切な SMTP 応答を送信し、処理を続行します。

7. 集計レポートの送信がイネーブルの場合、AsyncOS は DMARC 検証のデータを収集し、それをドメイン所有者に送信する日次レポートに追加します。DMARC 集計フィードバック レポートの詳細については、DMARC 集計レポート （785 ページ）を参照してください。

（注） 集計レポートのサイズが 10 MB または DMARC レコードの RUA タグで指定されたサイズを超えた場合、AsyncOS はドメイン所有者に配信エラー レポートを送信します。

DMARC を使用した受信メッセージの検証方法

DMARC を使用した受信メッセージの検証方法

	操作手順	詳細情報
ステップ 1	新しい DMARC 検証プロファイルを作成するか、デフォルトの DMARC 検証プロファイルを要件に合わせて変更します。	DMARC 検証プロファイルの作成 （780 ページ） DMARC 検証プロファイルの編集 （781 ページ）
ステップ 2	（任意）DMARC のグローバル設定を要件に合わせて設定します。	DMARC のグローバル設定 （783 ページ）
ステップ 3	DMARC を使用して受信メッセージを検証するようにメール フロー ポリシーを設定します。	メール フロー ポリシーでの DMARC 検証の設定 （784 ページ）
ステップ 4	（任意）DMARC フィードバック レポートの返信アドレスを設定します。	DMARC フィードバック レポートの返信アドレスの設定 （785 ページ）
ステップ 5	（任意）以下を確認します。 • DMARC 検証レポートと着信メール レポート • DMARC 検証に失敗したメッセージ（メッセージ トラッキングを使用）	• [DMARC検証（DMARC Verification）]ページ （1034 ページ） • [受信メール（Incoming Mail）]ページ （1020 ページ） • レガシー インターフェイスでのメッセージの検索 （1115 ページ）

関連項目

- DMARC 検証プロファイルの管理 （780 ページ）
- DMARC 集計レポート （785 ページ）
- DMARC のグローバル設定 （783 ページ）
- メール フロー ポリシーでの DMARC 検証の設定 （784 ページ）
- DMARC フィードバック レポートの返信アドレスの設定 （785 ページ）

DMARC 検証プロファイルの管理

DMARC 検証プロファイルは、 電子メールゲートウェイのメールフローポリシーが DMARC を検証するために使用するパラメータのリストです。たとえば、特定のドメインからの非準拠メッセージをすべて拒否する厳格なプロファイルと、別のドメインからの非準拠メッセージをすべて隔離するあまり厳格でないプロファイルを作成できます。

DMARC 検証プロファイルは次の情報で構成されます。

- 検証プロファイルの名前。
- DMARC レコード内のポリシーが拒否のときに実行するメッセージ アクション。
- DMARC レコード内のポリシーが隔離のときに実行するメッセージ アクション。
- 一時的な障害の場合に実行するメッセージ アクション。
- 永続的な障害の場合に実行するメッセージ アクション。

関連項目

- DMARC 検証プロファイルの作成 （780 ページ）
- DMARC 検証プロファイルの編集 （781 ページ）
- DMARC 検証プロファイルのエクスポート （782 ページ）
- DMARC 検証プロファイルのインポート （782 ページ）
- DKIM 検証プロファイルの削除 （762 ページ）

DMARC 検証プロファイルの作成

新しい DMARC 検証プロファイルを作成するには、次の手順を使用します。

（注） デフォルトでは、AsyncOS はデフォルトの DMARC 検証プロファイルを提供します。新しい DMARC 検証プロファイルを作成しない場合は、デフォルトの DMARC 検証プロファイルを使用できます。デフォルトの DMARC 検証プロファイルは、[メールポリシー（Mail Policies）] > [DMARC] ページで使用可能です。デフォルトの DMARC 検証プロファイルを編集する手順については、DMARC 検証プロファイルの編集 （781 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 DMARC レコード内のポリシーが拒否のときに AsyncOS が実行するメッセージ アクションを設定します。次のいずれかを実行します。

- [アクションなし（No Action）]。AsyncOS は、DMARC 検証に失敗したメッセージに対してアクションを実行しません。

- [隔離（Quarantine）]。AsyncOS は、DMARC 検証に失敗したメッセージを指定された隔離領域に隔離します。
- [拒否（Reject）]。 AsyncOS は、DMARC 検証に失敗したすべてのメッセージを拒否し、指定された SMTP コードと応答を返します。デフォルト値は、それぞれ `550 and #5.7.1 DMARC unauthenticated mail is prohibited` です。

ステップ 5 DMARC レコード内のポリシーが隔離のときに AsyncOS が実行するメッセージ アクションを設定します。次のいずれかを実行します。

- [アクションなし（No Action）]。AsyncOS は、DMARC 検証に失敗したメッセージに対してアクションを実行しません。
- [隔離（Quarantine）]。AsyncOS は、DMARC 検証に失敗したメッセージを指定された隔離領域に隔離します。

ステップ 6 DMARC 検証中に一時的な障害が発生したメッセージに対して AsyncOS が実行するメッセージ アクションを設定します。次のいずれかを実行します。

- [承認（Accept）]。 AsyncOS は、DMARC 検証中に一時的な障害が発生したメッセージを受け入れます。
- [拒否（Reject）]。 AsyncOS は、DMARC 検証中に一時的な障害が発生したメッセージを拒否し、指定された SMTP コードと応答を返します。デフォルト値は、それぞれ `451 and #4.7.1 Unable to perform DMARC verification` です。

ステップ 7 DMARC 検証中に永続的な障害が発生したメッセージに対して AsyncOS が実行するメッセージ アクションを設定します。次のいずれかを実行します。

- [承認（Accept）]。 AsyncOS は、DMARC 検証中に永続的な障害が発生したメッセージを受け入れます。
- [拒否（Reject）]。 AsyncOS は、DMARC 検証中に永続的な障害が発生したメッセージを拒否し、指定された SMTP コードと応答を返します。デフォルト値は、それぞれ `550 and #5.7.1 DMARC verification failed` です。

ステップ 8 変更を送信し、保存します。

DMARC 検証プロファイルの編集

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。

ステップ 2 目的の検証プロファイル名をクリックします。

ステップ 3 DMARC 検証プロファイルの作成 （780 ページ）の説明に従って、目的のフィールドを編集します。

ステップ 4 変更を送信し、保存します。

DMARC 検証プロファイルのエクスポート

電子メールゲートウェイ上のすべての DMARC 検証プロファイルを configuration ディレクトリ内の単一のテキストファイルにエクスポートできます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。
ステップ 2 [プロファイルをエクスポート（Export Profiles）] をクリックします。
ステップ 3 ファイルの名前を入力します。
ステップ 4 **[送信（Submit）]** をクリックします。

DMARC 検証プロファイルのインポート

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。
ステップ 2 [プロファイルをインポート（Import Profiles）] をクリックします。
ステップ 3 DMARC 検証プロファイルを含むファイルを選択します。
ステップ 4 **[送信（Submit）]** をクリックします。インポートによってすべての既存の DMARC 検証プロファイルが置き換えられることが警告されます。
ステップ 5 [インポート（Import）] をクリックします。
ステップ 6 変更を保存します。

DMARC 検証プロファイルの削除

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。
ステップ 2 削除する検証プロファイルを選択します。
ステップ 3 [削除（Delete）] をクリックします。
ステップ 4 削除を確認します。

DMARC のグローバル設定

手順

ステップ 1 [メールポリシー（Mail Policies）] > [DMARC] を選択します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 次の表に定義された設定を変更します。

DMARC のグローバル設定

グローバル設定	説明
特定の送信者はアドレスリストをバイパスします（Specific senders bypass address list）	特定の送信者から受信したメッセージの DMARC 検証をスキップします。ドロップダウンリストからアドレス一覧を選択します。 （注） 完全な電子メール アドレスまたはドメインのみを使用して作成したアドレス リストを使用すると、DMARC 検証を回避することができます。詳細については、着信接続ルールへの送信者アドレス リストの使用 （134 ページ）を参照してください。
次のヘッダーのあるメッセージの場合、検証をバイパスする（Bypass verification for messages with headers）	特定のヘッダーを含むメッセージの DMARC 検証をスキップします。たとえば、メーリングリストや信頼できるフォワーダからのメッセージの DMARC 検証をスキップするには、このオプションを使用します。 ヘッダーを入力します。複数の場合はカンマで区切ります。
レポート生成のスケジュール（Schedule for report generation）	AsyncOS が DMARC 集計レポートを生成する時間。たとえば、集計レポートを生成する時間として非ピーク時間を選択することで、メール フローへの影響を回避できます。
レポートを生成するエンティティ（Entity generating reports）	DMARC 集計レポートを生成するエンティティ。これは、DMARC 集計レポートを受け取ったドメイン所有者がレポートを生成したエンティティを特定するのに役立ちます。 有効なドメイン名を入力します。
レポートの追加連絡先情報（Additional contact information for reports）	DMARC 集計レポートを受け取ったドメイン所有者がレポートを生成したエンティティと連絡を取る場合の、追加の連絡先情報（組織のカスタマー サポートの詳細など）。
すべての集計レポートのコピーの送信先（Send copy of all aggregate reports to）	すべての DMARC 集計レポートのコピーを特定のユーザ（集計レポートの分析を実行する内部ユーザなど）に送信します。 電子メールアドレスを入力します。複数の場合はカンマで区切ります。

グローバル設定	説明
エラーレポート（Error Reports）	DMARC集計レポートのサイズが10 MBまたはDMARCレコードのRUAタグで指定されたサイズを超えた場合に、ドメイン所有者に配信エラー レポートを送信します。 チェックボックスをオンにします。

ステップ 4 変更を送信し、保存します。

メール フロー ポリシーでの DMARC 検証の設定

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] を選択します。

ステップ 2 検証を実行するリスナーの着信メール ポリシーをクリックします。

ステップ 3 メール フロー ポリシーの [セキュリティサービス（Security Features）] セクションで、[オン（On）] を選択して、[DMARC検証（DMARC Verification）] をイネーブルにします。

ステップ 4 ポリシーで使用する DMARC 検証プロファイルを選択します。

ステップ 5 （任意）メッセージの送信元である DMARC 対応ドメインの RUA タグで指定された電子メール アドレスに対する DMARC 集計フィードバック レポートの送信をイネーブルにします。

集計フィードバック レポートは毎日生成されます。

ステップ 6 変更を送信し、保存します。

次のタスク

関連項目

- DMARC 検証ログ （784 ページ）

DMARC 検証ログ

DMARC 検証の次の段階で、メール ログにログ メッセージが追加されます。

- メッセージに対して DMARC 検証が試行されたとき
- DMARC 検証が完了したとき
- DKIM および SPF の調整結果を含む DMARC 検証の詳細が出力されるとき
- メッセージに対する DMARC 検証がスキップされたとき
- DMARC レコードが取得および解析されたとき、または DNS に障害が発生したとき
- ドメインに対する DMARC 集計レポートの配信が失敗したとき

- ドメインに対してエラー レポートが生成されたとき
- ドメインに対するエラー レポートの配信が成功したとき
- ドメインに対するエラー レポートの配信が失敗したとき

DMARC フィードバック レポートの返信アドレスの設定

手順

ステップ 1 **[システム管理（System Administration）]** > **[返信先アドレス（Return Addresses）]** を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 DMARC 集計フィードバック レポートの返信アドレスを入力します。

ステップ 4 変更を送信し、保存します。

DMARC 集計レポート

DMARC では、フィードバック メカニズムを利用して、ドメイン所有者のポリシーを安全かつスケーラブルな方法で適用します。このフィードバック メカニズムは、ドメイン所有者が認証の導入環境を強化するのに役立ちます。

メールフローポリシーで集計フィードバック レポートの送信をイネーブルにしてから、AsyncOS を使用して DMARC 検証を実行すると、AsyncOS は集計フィードバック レポートを毎日生成し、それをドメイン所有者に送信します。これらのレポートは、XML 形式で生成され、GZip ファイルにアーカイブされます。

（注） AsyncOS が生成するすべての DMARC 集計フィードバック レポートは、DMARC に準拠しています。

DMARC 集計フィードバック レポートには次のセクションが含まれています。

- レポート送信者のメタデータ（電子メール アドレスやレポート ID 番号など）。
- 公開済みの DMARC ポリシーの詳細。
- DMARC ポリシー処理の詳細（送信元 IP アドレスや処理のサマリーなど）。
- ドメイン ID
- DMARC 検証の結果と認証のサマリー。

関連項目

- DMARC 集計フィードバック レポートの例 （786 ページ）

DMARC 集計フィードバック レポートの例

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <version>1.0</version>
  <report_metadata>
    <org_name>cisco.com</org_name>
    <email>noreply-dmarc-support@cisco.com</email>
    <extra_contact_info>http://cisco.com/dmarc/support</extra_contact_info>
    <report_id>b1d925$4ecceab=0694614b826605cd@cisco.com</report_id>
    <date_range>
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>1.1.1.1</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
   <envelope_from>example.com</envelope_from>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
     <selector>ny</selector>
        <result>fail</result>
      </dkim>
      <dkim>
        <domain>example.net</domain>
<selector></selector>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>example.com</domain>
<scope>mfrom</scope>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

偽装メールの検出

電子メール偽造（スプーフィング、CEO 詐欺、またはビジネス メール詐欺とも呼ばれる）とは、送信者の実際の身元を隠すためにメッセージヘッダーを変更し、それを既知の相手からの本物のメッセージのように見せかけるプロセスのことです。組織の幹部になりすましている詐欺師が、クライアントとその個人情報（PII）のリストを送信するように求める偽造メッセージを従業員に送信しているとしましょう。送信者の本当の身元に気づいていない従業員は、クライアントとその PII のリストを送信します。詐欺師はその PII を使用して個人情報の盗難を行います。

電子メールゲートウェイは、偽装送信者のアドレス（From: ヘッダー）がある詐欺メッセージを検出し、そのようなメッセージに対して指定されたアクションを実行することができます。たとえば、 電子メールゲートウェイは偽装送信者のアドレスがあるメッセージを検出して、From: ヘッダーをエンベロープ送信者に置き換えることができます。この場合、従業員には偽装電子メール アドレスではなく、実際の送信者（詐欺師）の電子メール アドレスが表示されます。

関連項目

- 偽造メールの検出の設定 （787 ページ）
- 偽装メールの検出結果の監視 （788 ページ）
- メッセージ トラッキングでの偽装メールの詳細の表示 （789 ページ）

偽造メールの検出の設定

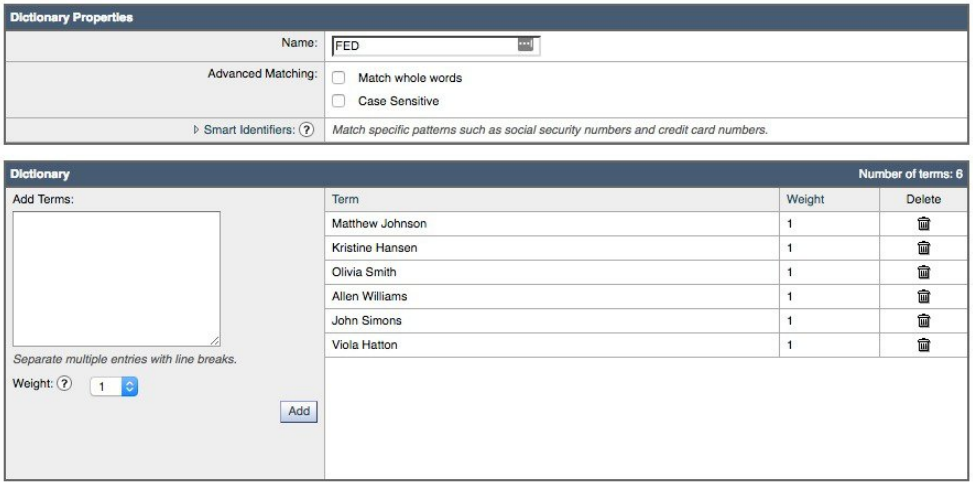
1. メッセージが偽造される可能性がある組織内のユーザ（幹部など）を特定します。新しいコンテンツ ディクショナリを作成し、特定したユーザの名前をそれに追加します。

   コンテンツ ディクショナリの作成時には、

   - ユーザの名前（電子メール アドレスではない）を入力します。たとえば、"olivia.smith@example.com" ではなく "Olivia Smith" を入力します。
   - 高度なマッチングとスマート ID は構成しないでください。
   - 使用する用語の重みは選択しないでください。
   - 正規表現は使用しないでください。

   次の図は、偽造メールの検出用に作成されたサンプル コンテンツ ディクショナリを示しています。

図 *38* : 偽造メールの検出用のコンテンツ ディクショナリ



コンテンツ ディクショナリを構成する手順については、ディクショナリの追加 （796 ページ）を参照してください。

2. 偽造メールを検出するための受信コンテンツフィルタまたはメッセージフィルタと、そのようなメッセージに対して電子メールゲートウェイが取る必要があるアクションを作成します。次のように指定します。

   - [条件/ルール（Condition/Rule）]：偽造メールの検出（コンテンツ フィルタの条件 （327 ページ）およびメッセージ フィルタ ルール （157 ページ）を参照）

（注） 特定の送信者からのメッセージの偽装メールの検出フィルタをスキップする場合、[例外リスト（Exception List）] ドロップダウン リストからアドレス リストを選択します。完全な電子メール アドレスを使用して作成したアドレス リストのみを選択できます。例外アドレス リストの追加方法の詳細については、着信接続ルールへの送信者アドレス リストの使用 （134 ページ）を参照してください。

   - [アクション（Action）]：偽造メールの検出またはユーザの要求に基づく他のアクション。 （コンテンツ フィルタの条件 （327 ページ） およびメッセージ フィルタ ルール （157 ページ） を参照）。

3. 新しく作成されたコンテンツ フィルタを受信メール ポリシーに追加します。メール ポリシーをユーザ単位で適用する方法 （310 ページ） を参照してください。

偽装メールの検出結果の監視

検出された偽装メッセージについてのデータを表示するには、[偽造メールの一致（Forged Email Matches）] レポートのページ（[モニタ（Monitor）] > [偽造メールの一致（Forged Email

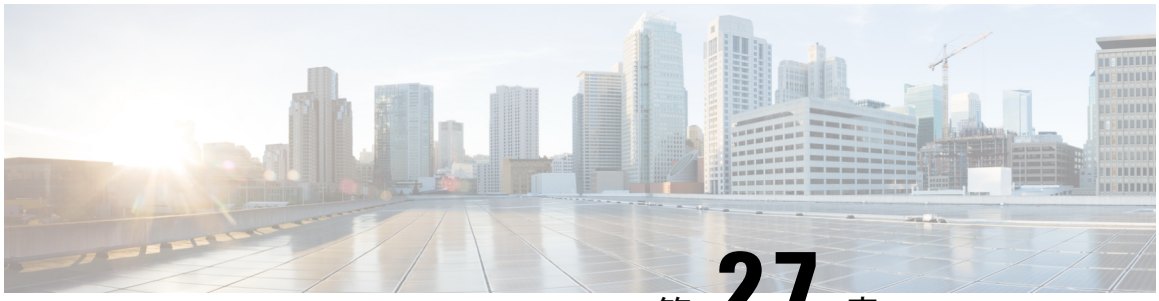
Matches）]）を参照してください。このレポートページに表示されるレポートは、次のとおりです。

- 偽装メール一致の上位（Top Forged Email Matches）受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。
- 偽装メールの一致：詳細（Forged Email Matches: Details）受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。メッセージトラッキングのメッセージ一覧を表示するには、番号をクリックします。

メッセージ トラッキングでの偽装メールの詳細の表示

メッセージトラッキングで電子メールゲートウェイによって検出された偽装メッセージの詳細を表示するには、次のことを確認します。

- メッセージトラッキングが有効である。メッセージトラッキング（1113ページ）を参照してください。
- 偽装メッセージを検出するためのコンテンツまたはメッセージフィルタが動作している。



第 27 章

テキスト リソース

この章は、次の項で構成されています。

- テキスト リソースの概要 （791 ページ）
- コンテンツ ディクショナリ （793 ページ）
- コンテンツ ディクショナリ フィルタ ルールの使用方法およびテスト方法 （798 ページ）
- テキスト リソースについて （800 ページ）
- テキスト リソース管理の概要 （802 ページ）
- テキスト リソースの使用 （805 ページ）

テキスト リソースの概要

この章では、コンテンツディクショナリ、免責事項、およびテンプレートなどのさまざまなテキスト リソースの作成および管理について説明します。

関連項目

- コンテンツ ディクショナリ （791 ページ）
- テキスト リソース （792 ページ）
- メッセージの免責事項スタンプ （793 ページ）
- 機密 DLP 用語（カスタム DLP ポリシーのみ）のカスタム ディクショナリの使用 （641 ページ）

コンテンツ ディクショナリ

コンテンツディクショナリは、電子メールゲートウェイの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツフィルタおよびメッセージフィルタの両方に利用できます。定義したディクショナリを使用し、ディクショナリに含まれる単語に対してメッセージ、メッセージ ヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行できます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語を含むメッセージをスキャンし、メッセージをドロップ、アーカイブ、または隔離できます。

テキスト リソース

AsyncOS オペレーティング システムには、GUI（[メール ポリシー（Mail Policies）] > [辞書（Dictionaries）]）または CLI の **dictionaryconfig** コマンドを使用して、合計 100 個のコンテンツディクショナリを定義する能力があります。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。

コンテンツディクショナリを使用して、企業のポリシーに沿った適切なアクションを実行できるようにメッセージまたはコンテンツ フィルタに対してメッセージをスキャンできます。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。ディクショナリごとに、大文字と小文字の区別および単語の区切りの検出方法を決定することもできます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語に対してメッセージをスキャンし、一致する単語を含むメッセージをドロップまたはアーカイブできます。また、単語によってフィルタ アクションをより簡単にトリガーできるように、ディクショナリに「重み」の条件を追加できます。

ディクショナリには、非 ASCII 文字を含めることができます。

効率的に処理するため、次のコンテンツディクショナリのエントリは単語として処理されることに注意してください。

- 英数字のみを含むエントリ
- 0 ～ 9、A ～ Z、a ～ z、ドット、アンダースコア、ハイフン、アット マークを含む電子メール アドレス
- 0 ～ 9、A ～ Z、a ～ z、ドット、アンダースコア、ハイフン、アット マークを含むドメイン名

このような単語を正規表現として 電子メールゲートウェイに処理させる場合は、(user@example.com) のように、その単語をカッコで囲みます。

関連項目

- ディクショナリの内容 （794 ページ）
- テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 （795 ページ）
- ディクショナリの追加 （796 ページ）
- ディクショナリの削除 （797 ページ）
- ディクショナリのインポート （797 ページ）
- ディクショナリのエクスポート （798 ページ）

テキスト リソース

テキスト リソースは、免責事項、通知テンプレート、アンチウイルス テンプレートなどのテキスト オブジェクトです。AsyncOS のさまざまなコンポーネントで使用できる新規オブジェクトを作成できます。テキスト リソースをインポートおよびエクスポートできます。

メッセージの免責事項スタンプ

メッセージの免責事項スタンプを使用すると、免責事項のテキストリソースをメッセージに追加できます。たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

コンテンツ ディクショナリ

コンテンツディクショナリは、電子メールゲートウェイの本文スキャン機能と連携して動作する単語またはエントリのグループであり、コンテンツフィルタおよびメッセージフィルタの両方に利用できます。定義したディクショナリを使用し、ディクショナリに含まれる単語に対してメッセージ、メッセージ ヘッダー、およびメッセージの添付ファイルをスキャンすることで、企業のポリシーに沿った適切なアクションを実行できます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語を含むメッセージをスキャンし、メッセージをドロップ、アーカイブ、または隔離できます。

AsyncOS オペレーティング システムには、GUI（[メール ポリシー（Mail Policies）] > [辞書（Dictionaries）]）または CLI の **dictionaryconfig** コマンドを使用して、合計 100 個のコンテンツディクショナリを定義する能力があります。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。

コンテンツディクショナリを使用して、企業のポリシーに沿った適切なアクションを実行できるようにメッセージまたはコンテンツ フィルタに対してメッセージをスキャンできます。ディクショナリの作成、削除、および表示、ディクショナリからのエントリの追加または削除、およびディクショナリ全体のインポートまたはエクスポートができます。ディクショナリごとに、大文字と小文字の区別および単語の区切りの検出方法を決定することもできます。たとえば、機密性の高い単語や野卑な単語のリストを作成し、フィルタ ルールを使用してリスト内の単語に対してメッセージをスキャンし、一致する単語を含むメッセージをドロップまたはアーカイブできます。また、単語によってフィルタ アクションをより簡単にトリガーできるように、ディクショナリに「重み」の条件を追加できます。

ディクショナリには、非 ASCII 文字を含めることができます。

効率的に処理するため、次のコンテンツディクショナリのエントリは単語として処理されることに注意してください。

- 英数字のみを含むエントリ
- 0 ～ 9、A ～ Z、a ～ z、ドット、アンダースコア、ハイフン、アット マークを含む電子メール アドレス
- 0 ～ 9、A ～ Z、a ～ z、ドット、アンダースコア、ハイフン、アット マークを含むドメイン名

このような単語を正規表現として 電子メールゲートウェイに処理させる場合は、(user@example.com) のように、その単語をカッコで囲みます。

関連項目

- ディクショナリの内容 （794 ページ）
- テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 （795 ページ）
- ディクショナリの追加 （796 ページ）
- ディクショナリの削除 （797 ページ）
- ディクショナリのインポート （797 ページ）
- ディクショナリのエクスポート （798 ページ）

ディクショナリの内容

ディクショナリの単語は 1 行につき 1 つのテキスト文字列で作成し、エントリはプレーン テキストまたは正規表現の形式で記載できます。ディクショナリには、非 ASCII 文字を含めることもできます。正規表現のディクショナリを定義すると、より柔軟に単語を照合させることができます。ただし、このためには適切に単語を区切る方法を理解する必要があります。Python スタイルの正規表現の詳細については、次の URL からアクセスできる「Python Regular Expression HOWTO」を参考にしてください。

http://www.python.org/doc/howto/

（注） ディクショナリのエントリの最初に特殊文字 # を使用すると、文字クラス [#] をコメントとして扱われることなく使用できます。

単語によってフィルタ条件をより簡単にトリガーできるように、各単語に「重み」を指定できます。AsyncOS では、コンテンツ ディクショナリの単語に対してメッセージをスキャンし、単語インスタンスの数に単語の重みを掛けることでメッセージのスコアを付けます。2 つの単語インスタンスに 3 の重みが付いている場合、スコアは 6 になります。AsyncOS は、このスコアをコンテンツ フィルタまたはメッセージ フィルタに関連するしきい値と比較し、メッセージがフィルタ アクションをトリガーするかどうかを決定します。

コンテンツ ディクショナリにスマート ID を追加することもできます。スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。これらの ID はポリシーの拡張に便利です。正規表現の詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Regular Expressions in Rules」を参照してください。スマート ID の詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Smart Identifiers」を参照してください。

（注） 端末の CLI に非 ASCII 文字を含むディクショナリが正しく表示される場合とされない場合があります。非ASCII文字を含むディクショナリを表示および変更する最適な方法は、ディクショナリをテキストファイルにエクスポートし、テキストファイルを編集して、新しいファイルを再び 電子メールゲートウェイにインポートする方法です。詳細については、テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 （795 ページ）を参照してください。

関連項目

- 単語境界と 2 バイト文字セット （795 ページ）

単語境界と 2 バイト文字セット

一部の言語（2バイト文字セット）では、単語または単語の区切りに関する概念や、大文字/小文字がありません。単語を構成する文字（正規表現で「\w」と表される文字）の識別などが必要になる複雑な正規表現では、ロケールが不明な場合、またはエンコードが不明な場合、問題が発生します。この理由から、単語境界の拡張をディセーブルにできます。

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

コンテンツディクショナリ機能には、デフォルトで 電子メールゲートウェイの configuration ディレクトリに配置されている次のテキストファイルが含まれます。

- **config.dtd**
- **profanity.txt**
- **proprietary_content.txt**
- **sexual_content.txt**

これらのテキスト ファイルは、コンテンツ ディクショナリ機能と組み合わせて使用することで、新規ディクショナリの作成をサポートすることを目的としています。これらのコンテンツディクショナリは重み付けされており、スマート ID を使用することでデータ内のパターンを高い精度で検出し、コンプライアンスの問題となるパターンの場合にはフィルタをトリガーします。

（注） ディクショナリをインポートおよびエクスポートする場合は、完全に一致する単語の設定と大文字と小文字を区別する設定が保持されません。この設定は、設定ファイルにのみ保持されます。

configuration ディレクトリへのアクセスの詳細については、FTP、SSH、および SCP アクセス（1573 ページ）を参照してください。

ユーザ独自のディクショナリファイルを作成して、電子メールゲートウェイにインポートすることもできます。非 ASCII 文字をディクショナリに追加する最善の方法は、 電子メールゲートウェイ以外の場所でテキストファイルのディクショナリに単語を追加し、電子メールゲートウェイ上にファイルを移動してから新しいディクショナリとしてファイルをインポートすることです。ディクショナリのインポートの詳細については、ディクショナリのインポート （797 ページ）を参照してください。ディクショナリのエクスポートについては、ディクショナリのエクスポート （798 ページ）を参照してください。

注意 これらのテキスト ファイルには、一部の人の間では卑猥、下品または不快に感じられる単語が含まれています。これらのファイルからコンテンツディクショナリに単語をインポートした場合、 電子メールゲートウェイに設定したコンテンツディクショナリを後で閲覧する際にこれらの単語が表示されます。

ディクショナリの追加

手順

ステップ 1 [メールポリシー（Mail Policies）] > [辞書（Dictionaries）] ページに移動します。

ステップ 2 [ディクショナリを追加（Add Dictionary）] をクリックします。

ステップ 3 ディクショナリの名前を入力します。

ステップ 4 （任意）高度なマッチングを設定します。

（注） AsyncOS は、設定ファイルに保存する際に、[単語全体の一致（Match Whole Words）] と [大文字小文字を区別（Case Sensitive）] の設定を保持します。ディクショナリをインポートおよびエクスポートするときは、AsyncOS はこれらの設定は保持しません。

ステップ 5 （任意）ディクショナリにスマート ID を追加します。

スマート ID は、社会保障番号や ABA ルーティング番号など共通の数字パターンに一致するパターンをデータ内から検索するアルゴリズムです。スマート ID の詳細については、「Using Message Filters to Enforce Email Policies」の章を参照してください。

ステップ 6 新規ディクショナリのエントリを単語のリストに入力します。

追加する複数の新しいエントリがあり、フィルタ アクションを同じ様にトリガーにする場合は、1 行につき 1 つずつ新しい語を入力します。

（注） 正規表現「.*」をエントリの最初または最後に使用したコンテンツディクショナリのエントリがあると、その「単語」に一致する MIME パートが見つかった場合にシステムがロックされます。コンテンツディクショナリのエントリの最初または最後に「.*」を使用しないことを推奨します。

ステップ 7 単語に対する重みを指定します。

フィルタ アクションを他の単語よりトリガーしやすくなるように、ディクショナリの単語に「重み」を付けられます。この重みがフィルタ アクションの決定に使用される仕組みの詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Threshold Scoring for Content Dictionaries」を参照してください。

ステップ 8 [追加（Add）] をクリックします。

ステップ 9 変更を送信し、保存します。

次のタスク

関連項目

- ディクショナリの内容 （794 ページ）。

ディクショナリの削除

はじめる前に

AsyncOS は、削除されたディクショナリを参照しているすべてのメッセージ フィルタを無効としてマークすることに注意してください。AsyncOS は削除されたディクショナリを参照しているすべてのコンテンツ フィルタをイネーブルのままにしますが、今後無効と判断します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [辞書（Dictionaries）] ページに移動します。

ステップ 2 ディクショナリの横にあるゴミ箱アイコンをクリックして、ディクショナリのリストから削除します。

確認メッセージには、ディクショナリを現在参照しているフィルタがすべて表示されます。

ステップ 3 確認メッセージで [削除（Delete）] をクリックします。

ステップ 4 変更を保存します。

ディクショナリのインポート

はじめる前に

インポートするファイルが、電子メールゲートウェイの configuration ディレクトリに存在することを確認します。

手順

ステップ 1 **[メールポリシー（Mail Policies）] > [辞書（Dictionaries）]** ページに移動します。

ステップ 2 [辞書をインポート（Import Dictionary）] をクリックします。
ステップ 3 インポート元の場所を選択します。
ステップ 4 インポートするファイルを選択します。
ステップ 5 ディクショナリの単語に使用するデフォルトの重みを選択します。

AsyncOS では、重みが指定されていない単語に対してデフォルトの重みを割り当てます。ファイルのインポート後に重みを編集できます。

ステップ 6 エンコード方式を選択します。
ステップ 7 **[Next]** をクリックします。
ステップ 8 ディクショナリの名前を指定し、編集します。
ステップ 9 変更を送信し、保存します。

ディクショナリのエクスポート

手順

ステップ 1 [メールポリシー（Mail Policies）] > [辞書（Dictionaries）] ページに移動します。
ステップ 2 **[ディクショナリをエクスポート（Export Dictionary）]** をクリックします。
ステップ 3 エクスポートするディクショナリを選択します。
ステップ 4 エクスポートされたディクショナリのファイル名を入力します。

これは、 電子メールゲートウェイの設定ディレクトリに作成されるファイルの名前になります。

ステップ 5 エクスポート先の場所を選択します。
ステップ 6 テキスト ファイルのエンコード方式を選択します。
ステップ 7 変更を送信し、保存します。

コンテンツ ディクショナリ フィルタ ルールの使用方法およびテスト方法

ディクショナリは、さまざまな dictionary-match() メッセージ フィルタ ルールおよびコンテンツ フィルタに使用できます。

関連項目

- ディクショナリの照合フィルタ ルール （799 ページ）

ディクショナリの照合フィルタ ルール

dictionary-match(<*dictionary_name*>) という名前のメッセージ フィルタ ルール（および同様のルール）は、メッセージの本文にコンテンツ ディクショナリ（*dictionary_name*）に存在するいずれかの正規表現が含まれる場合に有効と判断されます。該当のディクショナリが存在しない場合は、ルールは無効と判断されます。

dictionary-match() ルールは、body-contains() 本文スキャン ルールと同様にメッセージ本文と添付ファイルのみをスキャンし、ヘッダーをスキャンしないことに注意してください。

ヘッダーのスキャンには、適切な *-dictionary-match() タイプのルールを使用できます（subject-dictionary-match() や、より一般的なルールでカスタム ヘッダーを含むすべてのヘッダーを指定できる header-dictionary-match() など、特定のヘッダーに対するルールが存在します）。ディクショナリの照合の詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Dictionary Rules」を参照してください。

表 *46*：コンテンツ ディクショナリのメッセージ フィルタ ルール

ルール	構文	説明
ディクショナリ照合	dictionary-match (<*dictionary_name*>)	指定したディクショナリに存在するすべての正規表現に一致した単語がメッセージに含まれているか。

次の例では dictionary-match() ルールを使用して、電子メールゲートウェイが（前回の例で作成した）「secret_words」という名前のディクショナリ内の単語を含むメッセージをスキャンした際に、管理者にメッセージをブラインドカーボンコピーで送信する新規メッセージフィルタが作成されます。設定値によっては、大文字/小文字も含めて「codename」と完全に一致する単語を含むメッセージのみが、このフィルタで有効と判断されることに注意してください。

```
bcc_codenames:

if (dictionary-match ('secret_words'))

{

bcc('administrator@example.com');

}
```

この例では、ポリシー隔離にメッセージを送信します。

```
quarantine_codenames:

if (dictionary-match ('secret_words'))

{

quarantine('Policy');


}
```

関連項目

- ディクショナリ エントリの例 （800 ページ）
- コンテンツ ディクショナリのテスト方法 （800 ページ）

ディクショナリ エントリの例

表 *47*: ディクショナリ エントリの例

説明	例
ワイルドカード	
アンカー	末尾：foo $、先頭：^ foo
電子メールアドレス（ピリオドをエスケープしない）	**foo@example.com**, **@example.com** **example.com$**（次で終わる）**@example.***
件名	**電子メールの件名**（電子メールの件名に ^ アンカーを使用する際は、件名の先頭に「RE:」や「FW:」などが多く付いていることを覚えておいてください）

コンテンツ ディクショナリのテスト方法

`trace` 関数を使用すると、`dictionary-match()` ルールを使用しているメッセージ フィルタに対して迅速なフィードバックが得られます。詳細については、テストメッセージを使用したメールフローのデバッグ：トレース （1515ページ）を参照してください。上記の `quarantine_codenames` フィルタの例のように、`quarantine()` アクションを使用してフィルタをテストすることもできます。

テキスト リソースについて

テキスト リソースは、メッセージへの添付や、メッセージとしての送信が可能なテキスト テンプレートです。テキスト リソースは、次のいずれかの種類になります。

- **メッセージ免責事項**：メッセージに追加されるテキスト。詳細については、免責事項テンプレート （806 ページ）を参照してください。
- 通知テンプレート：通知として送信されるメッセージ（notify() および notify-bcc() アクションで使用されます）。詳細については、通知テンプレート （812 ページ）を参照してください。
- **アンチウイルス通知テンプレート**：メッセージにウイルスが見つかったときに、通知として送信されるメッセージ。コンテナ用のテンプレート（元のメッセージに付加）、またはメッセージに付加せず通知として送信されるテンプレートを作成できます。詳細については、アンチウイルス通知テンプレート （812 ページ）を参照してください。

- **バウンスおよび暗号化失敗通知テンプレート**：メッセージがバウンスされたときやメッセージの暗号化に失敗したときに通知として送信されるメッセージ。詳細については、バウンス通知および暗号化失敗通知テンプレート （816 ページ）を参照してください。
- **暗号化通知テンプレート**：発信電子メールを暗号化するように電子メールゲートウェイを設定した場合に送信されるメッセージ。このメッセージは、受信者が暗号化されたメッセージを受信したことを受信者に通知し、メッセージを読む手順を示します。詳細については、暗号化通知テンプレート （817 ページ）を参照してください。

CLI（**textconfig**）または GUI を使用して、テキスト リソースの追加、削除、編集、インポート、およびエクスポートを含むテキスト リソースの管理ができます。GUI を使用したテキスト リソースの管理については、テキスト リソース管理の概要 （802 ページ）を参照してください。

テキスト リソースには、非 ASCII 文字を含めることができます。

（注） 非 ASCII 文字を含むテキスト リソースは端末の CLI に正しく表示される場合とされない場合があります。非 ASCII 文字を含むテキストリソースを表示および変更するには、テキストリソースをテキストファイルにエクスポートし、テキストファイルを編集して、新しいファイルを再び 電子メールゲートウェイにインポートします。詳細については、テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 （795 ページ）を参照してください。

関連項目

- テキスト ファイルとしてディクショナリをインポートおよびエクスポートする方法 （795 ページ）

テキスト ファイルとしてのテキスト リソースのインポートおよびエクスポート

電子メールゲートウェイの configuration ディレクトリに対するアクセス権を持っている必要があります。インポートするテキストファイルは、電子メールゲートウェイ上の configuration ディレクトリに存在する必要があります。エクスポートされたテキストファイルは、configuration ディレクトリに配置されます。

configuration ディレクトリへのアクセスの詳細については、FTP、SSH、および SCP アクセス （1573 ページ）を参照してください。

非ASCII 文字をテキストリソースに追加するには、電子メールゲートウェイ以外の場所でテキストファイルのテキストリソースに単語を追加し、電子メールゲートウェイ上にファイルを移動し、新しいテキストリソースとしてファイルをインポートします。テキストリソースのインポートの詳細については、テキスト リソースのインポート （803 ページ）を参照してください。テキスト リソースのエクスポートについては、テキスト リソースのエクスポート （804 ページ）を参照してください。

テキスト リソース管理の概要

GUI または CLI を使用してテキスト リソースを管理できます。この項では、GUI について説明します。

textconfig コマンドを使用して CLI からテキスト リソースを管理します。

テキスト リソース管理には、次のタスクが含まれます。

- 追加
- 編集および削除
- エクスポートおよびインポート
- すべてのテキスト リソース タイプのプレーン テキスト メッセージの定義
- 一部のテキスト リソース タイプの HTML ベースのメッセージの定義

関連項目

- テキスト リソースの追加 （802 ページ）
- テキスト リソースの削除 （803 ページ）
- テキスト リソースのエクスポート （804 ページ）
- テキスト リソースのインポート （803 ページ）
- HTML ベースのテキスト リソースの概要 （804 ページ）。

テキスト リソースの追加

手順

ステップ 1 [メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] に移動します。

ステップ 2 [テキスト リソースを追加（Add Text Resource）] をクリックします。

ステップ 3 [名前（Name）] フィールドにテキスト リソースの名前を入力します。

ステップ 4 [タイプ（Type）] フィールドからテキスト リソースのタイプを選択します。

ステップ 5 [テキスト（Text）] または [HTMLおよびプレーンテキスト（HTML and Plain Text）] のどちらかのフィールドに、メッセージ テキストを入力します。

テキストリソースがプレーンテキストメッセージのみを許可する場合は、[テキスト（Text）] フィールドを使用します。テキスト リソースが HTML およびプレーン テキスト メッセージの両方を許可する場合は、[HTMLおよびプレーンテキスト（HTML and Plain Text）] フィールドを使用します。

ステップ 6 変更を送信し、保存します。

次のタスク

関連項目

- HTML ベースのテキスト リソースの概要 （804 ページ）。

テキスト リソースの削除

はじめる前に

テキスト リソースの削除の影響に注意してください。

- 削除されたテキスト リソースを参照しているすべてのメッセージ フィルタは、無効としてマークされます。
- 削除されたテキスト リソースを参照しているすべてのコンテンツ フィルタはイネーブルのままになりますが、今後無効と判断されます。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページに移動し、削除するテキスト リソースの [削除（Delete）] 列にあるゴミ箱アイコンをクリックします。確認メッセージが表示されます。

ステップ 2 [削除（Delete）] をクリックして、テキスト リソースを削除します。

（注） コンテンツまたはメッセージ フィルタのいずれかの設定で参照されているテキスト リソースは削除できません。

ステップ 3 変更を保存します。

テキスト リソースのインポート

はじめる前に

インポートするファイルが、電子メールゲートウェイの configuration ディレクトリに存在することを確認します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページに移動し、[テキストリソースのインポート（Import Text Resource）] をクリックします。

ステップ 2 インポートするファイルを選択します。

ステップ 3 エンコード方式を指定します。

ステップ 4 **[Next]** をクリックします。

ステップ 5 名前を選択し、テキスト リソース タイプを編集および選択します。

ステップ 6 変更を送信し、保存します。

テキスト リソースのエクスポート

はじめる前に

テキストリソースをエクスポートする場合は、テキストファイルが電子メールゲートウェイの configuration ディレクトリに作成されることに注意してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページに移動し、[テキストリソースのエクスポート（Export Text Resource）] をクリックします。

ステップ 2 エクスポートするテキスト リソースを選択します。

ステップ 3 テキスト リソースのファイル名を入力します。

ステップ 4 テキスト ファイルのエンコード方式を選択します。

ステップ 5 [送信（Submit）] をクリックしてテキスト リソースを含むテキスト ファイルを configuration ディレクトリに作成します。

HTML ベースのテキスト リソースの概要

免責事項などの一部のテキスト リソースは、HTML ベースのメッセージおよびプレーン テキスト メッセージの両方を使用して作成できます。HTML ベースのメッセージとプレーン テキスト メッセージの両方を含むテキスト リソースが電子メール メッセージに適用された場合、HTML ベースのテキスト リソース メッセージは電子メール メッセージのテキストまたは HTML 部分に適用され、プレーン テキスト メッセージは電子メール メッセージのテキストまたはプレーン部分に適用されます。

HTML ベースのテキスト リソースを追加または編集する場合、GUI には、HTML コードを手動で記述せずにリッチ テキストの入力を可能にするリッチ テキスト編集が含まれます。

HTML ベースのテキスト リソースを追加および編集する場合は、次の点に留意してください。

- HTML バージョンに基づいて、メッセージのプレーン テキスト バージョンを自動的に生成するよう選択できます。または、プレーンテキストバージョンを個別に定義できます。
- [コードビュー（Code View）] ボタンをクリックすることにより、リッチ テキスト エディタと HTML コード間を切り替えることができます。
- リッチ テキスト エディタでサポートされない HTML コードを GUI で入力するには、コードビューに切り替え、HTML コードを手動で入力します。たとえば、これは、**<img src>** HTML タグを使用して外部サーバにあるイメージ ファイルへの参照を挿入する場合に行います。

関連項目

- HTML ベースのテキスト リソースのインポートおよびエクスポート （805 ページ）

HTML ベースのテキスト リソースのインポートおよびエクスポート

HTML ベースのテキスト リソースをテキスト ファイルにエクスポートしたり、テキスト ファイルから HTML ベースのテキスト リソースをインポートしたりできます。HTML ベースのテキストリソースをファイルにエクスポートする場合、ファイルにはテキストリソースの各バージョンに対する次のセクションが含まれます。

- `[html_version]`
- `[text_version]`

これらのセクションの順序は重要ではありません。

たとえば、エクスポートされたファイルには、次のテキストが含まれることがあります。

```
[html_version]
 <p>Sample <i>message.</i></p>
 [text_version]
 Sample message.
```

HTML ベースのテキスト リソースをエクスポートおよびインポートする場合は、次のルールとガイドラインに留意してください。

- プレーン テキスト メッセージが HTML バージョンから自動的に生成される HTML ベースのテキスト リソースをエクスポートする場合、エクスポートされたファイルには `[text_version]` セクションが含まれません。
- テキスト ファイルからインポートするとき、[html_version] セクション下のすべての HTML コードは作成されたテキスト リソースの HTML メッセージに変換されます（テキスト リソース タイプが HTML メッセージをサポートする場合）。同様に、`[text_version]` セクション下のすべてのテキストは、作成されたテキスト リソースのプレーン テキスト メッセージに変換されます。
- HTML ベースのテキストリソースを作成するために、空の、または存在しない `[html_version]` セクションを含むファイルからインポートする場合、 電子メールゲートウェイは `[text_version]` セクションのテキストを使用して HTML およびプレーンテキストメッセージの両方を作成します。

テキスト リソースの使用

すべてのタイプのテキスト リソースは、[テキストリソース（Text Resources）] ページまたは CLI の textconfig コマンドを使用して、同じ方法で作成されます。一度作成されると、各タイプで異なる使われ方をします。免責事項テンプレートおよび通知テンプレートは、フィルタおよびリスナーで使用されます。一方、アンチウイルス通知テンプレートは、メール ポリシーおよびアンチウイルス設定値で使用されます。

関連項目

- 免責事項テンプレート （806 ページ）
- 免責事項スタンプと複数エンコード方式 （809 ページ）
- 通知テンプレート （812 ページ）
- アンチウイルス通知テンプレート （812 ページ）
- バウンス通知および暗号化失敗通知テンプレート （816 ページ）
- 暗号化通知テンプレート （817 ページ）

免責事項テンプレート

電子メールゲートウェイは、リスナーが受信した一部またはすべてのメッセージのテキストの上または下（ヘッダーまたはフッター）にデフォルトの免責事項を追加できます。次の方法を使用して、 電子メールゲートウェイでメッセージに免責事項を追加できます。

- リスナーから、GUI または `listenerconfig` コマンドを使用する方法（リスナーからの免責事項テキストの追加 （806 ページ） を参照）。
- コンテンツ フィルタ アクション `Add Disclaimer Text` を使用する方法（コンテンツ フィルタのアクション （338 ページ） を参照）。
- メッセージ フィルタ アクション `add-footer()` を使用する方法（「Using Message Filters to Enforce Email Policies」の章を参照）。
- データ消失防止プロファイルを使用する方法（データ損失の防止 （625ページ） を参照）。
- メッセージの目的がフィッシングまたはマルウェアの配布である可能性があることをユーザに通知するようアウトブレイク フィルタに対してメッセージの修正を使用する方法（メッセージの変更 （519ページ） を参照）。このタイプの通知に追加される免責事項は、テキストの上に追加されます。

たとえば、企業内から送信される各メッセージに著作権宣言文、宣伝メッセージ、または免責事項を付加できます。

免責事項テキストを使用する前に、免責事項テンプレートを作成する必要があります。GUI で [テキストリソース（Text Resources）]ページを使用（テキスト リソースの追加 （802 ページ） を参照）または `textconfig` コマンドを使用（『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照）して、使用するテキスト文字列のセットを作成および管理します。

関連項目

- フィルタからの免責事項の追加 （807 ページ）
- リスナーからの免責事項テキストの追加 （806 ページ）
- 免責事項およびフィルタ アクション変数 （807 ページ）

リスナーからの免責事項テキストの追加

免責事項テキスト リソースを作成したら、リスナーで受信するメッセージに付加するテキスト文字列を選択します。免責事項テキストをメッセージの上部または下部に追加できます。この機能は、パブリック（インバウンド）リスナーとプライベート（アウトバウンド）リスナーの両方に使用できます。

テキストおよびHTMLから構成されるメッセージ（Microsoft Outlookでは、このタイプのメッセージを「multipart alternative」と呼びます）を送信する場合、電子メールゲートウェイは、メッセージの両方の部分に免責事項をスタンプします。ただし、メッセージが署名済みのコンテンツである場合、署名が無効になるためコンテンツは変更されません。代わりに、免責事項スタンプによって「Content-Disposition inline attachment」という新規パートが作成されます。マルチパート メッセージの詳細については、「Using Message Filters to Enforce Email Policies」の章の「Message Bodies vs. Message Attachments」を参照してください。

フィルタからの免責事項の追加

フィルタ アクション `add-footer()` またはコンテンツ フィルタ アクション「免責条項文の追加」を使用して、メッセージの免責事項に特定の定義済みテキスト文字列を付加することができます。たとえば、次のメッセージフィルタルールは、LDAPグループ「Legal」に属するユーザから送信されるすべてのメッセージに、`legal.disclaimer` というテキスト文字列を付加します。

```
Add-Disclaimer-For-Legal-Team:

if (mail-from-group == 'Legal')

{

add-footer('legal.disclaimer');

}
```

免責事項およびフィルタ アクション変数

メッセージ フィルタ アクション変数を使用することもできます（詳細については、「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照してください）。

免責事項テンプレートには、次の変数を使用できます。

表 *48*：アンチウイルス通知変数

変数	置き換える値
$To	メッセージの To: ヘッダーに置き換えられます（エンベロープ受信者には置き換えられません）。
$From	メッセージの From: ヘッダーに置き換えられます（エンベロープ送信者には置き換えられません）。
$Subject	元のメッセージの件名に置き換えられます。
$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$GMTimestamp	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。

変数	置き換える値
$MID	メッセージを内部で識別するために使用するメッセージID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。
$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
$Policy	メッセージのインジェクト時に、送信者に適用した HAT ポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
$Reputation	送信者の IP レピュテーションスコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
$filenames	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
$filetypes	メッセージの添付ファイルのファイルタイプを示すカンマ区切りリストに置き換えられます。
$filesizes	メッセージの添付ファイルサイズのカンマ区切りリストに置き換えられます。
$remotehost	メッセージを電子メールゲートウェイに送信したシステムのホスト名に置き換えられます。
$AllHeaders	メッセージ ヘッダーに置き換えられます。
$EnvelopeFrom	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
$Hostname	電子メールゲートウェイのホスト名に置き換えられます。
$header[‘*string* ’]	元のメッセージに一致するヘッダーが含まれる場合、引用符付きヘッダーの値に置き換えられます。二重引用符が使用される場合もあります。
$enveloperecipients	メッセージのエンベロープ受信者すべて（Envelope To、<RCPT TO>）に置き換えられます。
$bodysize	メッセージのサイズ（バイト単位）に置き換えられます。
$FilterName	処理中のフィルタの名前を返します。
$MatchedContent	スキャン フィルタ ルール（body-contains などのフィルタ ルールやコンテンツ ディクショナリを含む）をトリガーした内容を返します。

変数	置き換える値
$DLPPolicy	違反があった Email DLP ポリシーの名前に置き換えられます。
$DLPSeverity	違反の重大度に置き換えられます。値は[低（Low）]、[中（Medium）]、[高（High）]、または [重大（Critical）] のいずれかです。
$DLPRiskFactor	メッセージの機密内容のリスク要因スコアに置き換えられます（スコア 0 ～ 100）。
$threat_category	フィッシング、ウイルス、詐欺、マルウェアなどのアウトブレイク フィルタ脅威のタイプに置き換えられます。
$threat_type	アウトブレイク フィルタ脅威カテゴリのサブカテゴリに置き換えられます。たとえば、チャリティ詐欺、金銭目的のフィッシング、偽の取引などがあります。
$threat_description	アウトブレイク フィルタ脅威の説明に置き換えられます。
$threat_level	メッセージの脅威レベル（スコア 0 ～ 5）に置き換えられます。
$threat_verdict	[メッセージの変更 - 脅威レベル（Message Modification Threat Level）] しきい値によって、「はい」または「いいえ」に置き換えられます。メッセージに含まれるウイルスまたは非ウイルスの脅威レベルが [メッセージの変更 - 脅威レベル（Message Modification Threat Level）] しきい値以上の場合、この変数の値は「はい」に設定されます。

メッセージ フィルタ アクション変数を免責事項で使用するには、（GUI の [テキストリソース（Text Resource）] ページまたは **textconfig** コマンドから）メッセージの免責事項を作成し、変数を参照します。

add-footer() アクションでは、フッターを inline attachment、UTF-8 coded attachment、quoted printable attachment として追加することで、非 ASCII テキストをサポートします。

免責事項スタンプと複数エンコード方式

AsyncOS には、異なる文字エンコード方式を含む免責事項スタンプの動作を変更するために使用される設定値が存在します。デフォルトでは、AsyncOS は電子メール メッセージの本文パート内に添付されるように、免責事項を配置します。`localeconfig` コマンド内で設定した設定値を使用して、本文パートと免責事項のエンコード方式が異なる場合の動作を設定できます。数個のパートから構成される電子メール メッセージを確認することで、この設定が理解しやすくなります。

To: joe@example.com From: mary@example.com Subject: Hi!	ヘッダー
<空白行>	

Hello!	本文パート
このメッセージはスキャンされました。	最初の添付パート
Example.zip	2 番目の添付パート

最初の空白行に続くメッセージの本文には、多くのMIMEパートが含まれている場合があります。多くの場合、最初のパートは「本文」または「テキスト」と呼ばれ、2 番目以降のパートは「アタッチメント」と呼ばれます。

免責事項は「アタッチメント」（上記の例）または本文の一部として、電子メールに含めることができます。

To: joe@example.com From: mary@example.com Subject: Hi!	ヘッダー
<空白行>	
Hello!	本文パート
このメッセージはスキャンされました。	本文に含められた免責事項
Example.zip	最初の添付パート

一般的に、メッセージの本文と免責事項の間でエンコード方式の不一致が起こると、免責事項が本文に含まれ（インライン）個別のアタッチメントとして含まれないように、AsyncOS はメッセージ全体をメッセージの本文と同じエンコード方式でエンコードしようとします。つまり、免責事項と本文のエンコード方式が一致する場合、または免責事項のテキストに（本文の）インラインに表示できる文字が含まれている場合は、免責事項はインラインに含められます。たとえば、US-ASCII 文字のみを含む ISO-8859-1 エンコードされた免責事項が生成される可能性があります。結果的に、この免責事項は問題なく「インライン」に表示されます。

ただし、免責事項が本文と組み合わせられない場合、`localeconfig` コマンドを使用し、本文テキストを昇格または変換して免責事項のエンコード方式と一致させるように AsyncOS を設定することで、免責事項をメッセージの本文に含めることができます。

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
 encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
```

```
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?

(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
 of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main
body in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
 or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body
whenever possible.
However, if the disclaimer is encoded differently than the message body, and if imposing
 a single encoding
will cause loss of characters, it will be added as an attachment. The system will always
 try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit
the message body to
use an encoding that is compatible with the message body as well as the disclaimer.
Should the system try to
re-encode the message body in such a case? [Y]>

If the disclaimer that is added to the footer or header of the message generates an error
 when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added
as an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
 content is split into
separate email attachments. Should the system try to ignore such errors when decoding
the message body? [N]>

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
 encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]>
```

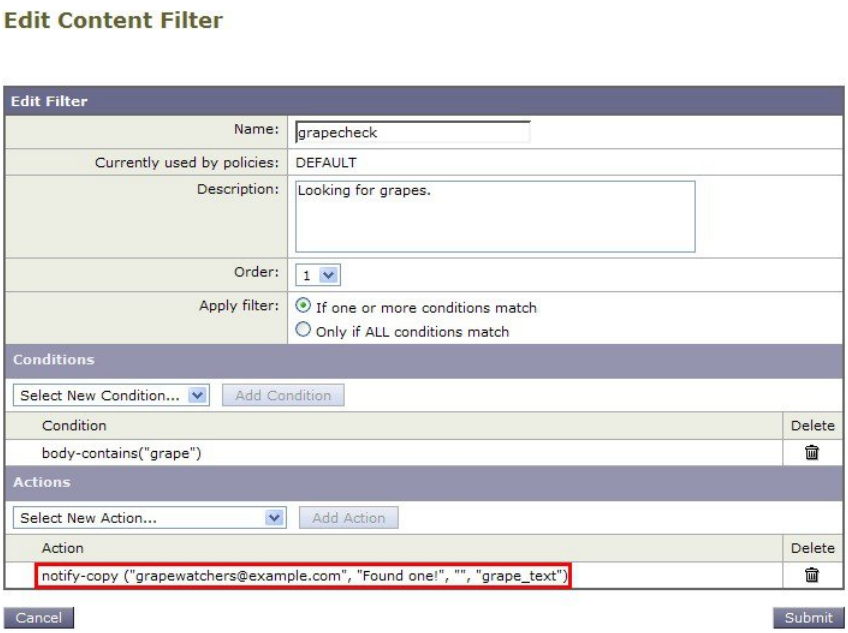
localeconfig コマンドの詳細については、「電子メールゲートウェイでのメール受信の設定」の章を参照してください。

通知テンプレート

通知テンプレートは、**notify()** および **notify-copy()** フィルタ アクションで使用されます。通知テンプレートには、アンチウイルス通知により使用されるアンチウイルス関連の変数を含む非 ASCII テキストおよびアクション変数を含めることができます（「Using Message Filters to Enforce Email Policies」の章にある「Action Variables」を参照）。たとえば、**$Allheaders** アクション変数を使用して、元のメッセージのヘッダーを含めることができます。通知用の From: アドレスを設定できます。電子メールゲートウェイに生成されるメッセージの返信アドレスの設定 （1272 ページ）を参照してください。

通知テンプレートを作成したら、コンテンツ フィルタおよびメッセージ フィルタから参照させることができます。次の図は、「grapewatchers@example.com」に「grape_text」通知が送信されるように **notify-copy()** フィルタ アクションを設定したコンテンツ フィルタを示しています。

図 *39*：コンテンツ フィルタによる通知の例



アンチウイルス通知テンプレート

アンチウイルス通知テンプレートには、次の 2 つのタイプがあります。

- **アンチウイルス通知テンプレート**。アンチウイルス通知テンプレートは、元のメッセージがウイルス通知に添付されていない場合に使用されます。
- **アンチウイルス コンテナ テンプレート**。コンテナ テンプレートは、元のメッセージが添付ファイルとして送信される際に使用されます。

アンチウイルス通知テンプレートは、フィルタの代わりにアンチウイルスエンジンで使用される以外は、基本的に通知テンプレートと同様に使用されます。メール ポリシーの編集中に送信するカスタム通知を指定できます。ウイルス対策通知用の From: アドレスを設定できます。詳

細については、電子メールゲートウェイに生成されるメッセージの返信アドレスの設定（1272 ページ）を参照してください。

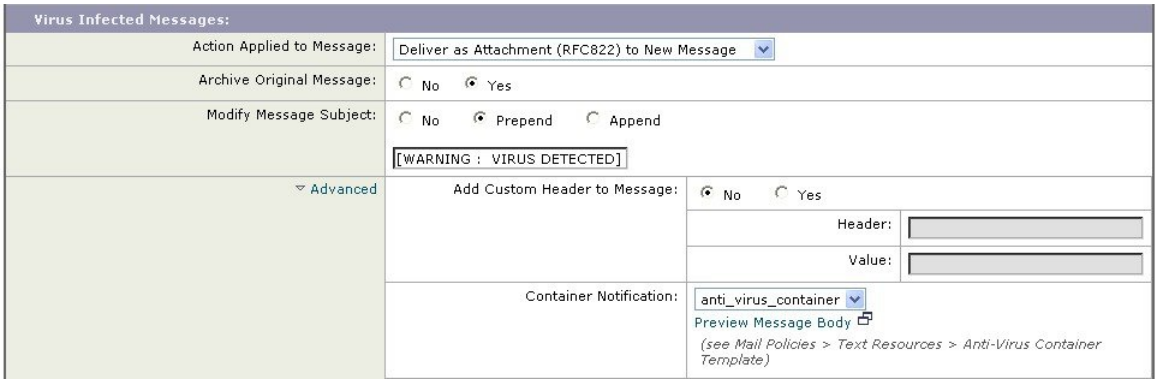
関連項目

- カスタム アンチウイルス通知テンプレート （813 ページ）

カスタム アンチウイルス通知テンプレート

次の図は、カスタム アンチウイルス通知が指定されたメール ポリシーを示しています。

図 *40 :* メール ポリシーでのアンチウイルス コンテナ テンプレートの通知例



関連項目

- アンチウイルス通知変数 （813 ページ）

アンチウイルス通知変数

ウイルス対策通知を作成する際に、次の表に記載されている通知変数を使用できます。

表 *49 :* アンチウイルス通知変数

変数	置き換える値
$To	メッセージの To: ヘッダーに置き換えられます（エンベロープ受信者には置き換えられません）。
$From	メッセージの From: ヘッダーに置き換えられます（エンベロープ送信者には置き換えられません）。
$Subject	元のメッセージの件名に置き換えられます。
$AV_VIRUSES	メッセージで発見されたすべてのウイルスのリストに置き換えられます。 例：“Unix/Apache.Trojan”, “W32/Bagel-F”

変数	置き換える値
$AV_VIRUS_TABLE	パートごとに MIME-Part/Attachment 名とウイルスを示すテーブルに置き換えられます。 例：“HELLO.SCR” : “W32/Bagel-F” <unnamed part of the message> : “Unix/Apache.Trojan”
$AV_VERDICT	アンチウイルスの判定に置き換えられます。
$AV_DROPPED_TABLE	ドロップされた添付ファイルのテーブルに置き換えられます。各行は、パートまたはファイル名とパートに付随するウイルスのリストにより構成されます。 例：“HELLO.SCR” : “W32/Bagel-f”, “W32/Bagel-d” “Love.SCR” : “Netsky-c”, “W32/Bagel-d”
$AV_REPAIRED_VIRUSES	発見および修復されたすべてのウイルスのリストに置き換えられます。
$AV_REPAIRED_TABLE	発見および修復されたすべてのパーツとウイルスのテーブルに置き換えられます。例："HELLO.SCR" : "W32/Bagel-F"
$AV_DROPPED_PARTS	ドロップされたファイル名のリストに置き換えられます。 例：“HELLO.SCR”, “CheckThisOut.exe”
$AV_REPAIRED_PARTS	修復されたファイル名またはパートのリストに置き換えられます。
$AV_ENCRYPTED_PARTS	暗号化されたファイル名またはパートのリストに置き換えられます。
$AV_INFECTED_PARTS	ウイルスを含むファイルのファイル名のカンマ区切りリストに置き換えられます。
$AV_UNSCANNABLE_PARTS	スキャンできなかったファイル名またはパートのリストに置き換えられます。
$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$GMTimestamp	現在の時刻および日付（GMT）に置き換えられます。電子メールメッセージの Received: 行で見られる形式と同様です。
$MID	メッセージを内部で識別するために使用するメッセージ ID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。

変数	置き換える値
$Group	メッセージのインジェクト時に、送信者が一致する送信者グループの名前に置き換えられます。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。
$Policy	メッセージのインジェクト時に、送信者に適用したHATポリシーの名前に置き換えられます。事前に定義されているポリシー名が使用されていない場合、文字列「>Unknown<」が挿入されます。
$Reputation	送信者のIPレピュテーションスコアに置き換えられます。レピュテーション スコアがない場合は「None」に置き換えられます。
$filenames	メッセージの添付ファイルのファイル名のカンマ区切リストに置き換えられます。
$filetypes	メッセージの添付ファイルのファイル タイプを示すカンマ区切りリストに置き換えられます。
$filesizes	メッセージの添付ファイル サイズのカンマ区切りリストに置き換えられます。
$remotehost	メッセージを電子メールゲートウェイに送信したシステムのホスト名に置き換えられます。
$AllHeaders	メッセージ ヘッダーに置き換えられます。
$EnvelopeFrom	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）に置き換えられます。
$Hostname	電子メールゲートウェイのホスト名に置き換えられます。

（注） 変数名は大文字/小文字を区別しません。たとえば、テキストリソースで「$to」と「$To」は同等です。元のメッセージで「AV_」変数が空の場合、文字列 <None> で置き換えられます。

テキスト リソースを定義した後、[メールポリシー（Mail Policies）] > [送受信メールポリシー（Incoming/Outgoing Mail Policies）] > [ウイルス対策設定を編集（Edit Anti-Virus Settings）] ページまたは **policyconfig -> edit -> antivirus** コマンドを使用して、修復されたメッセージ、スキャンできなかったメッセージ、暗号化されたメッセージ、またはウイルスが陽性のメッセージに対して、元のメッセージがRFC 822のアタッチメントとして含まれるように指定します。詳細については、カスタム アラート通知の送信 （453 ページ）を参照してください。

バウンス通知および暗号化失敗通知テンプレート

バウンス通知および暗号化失敗通知テンプレートは、バウンス通知およびメッセージ暗号化失敗通知で使用される以外は、基本的に通知テンプレートと同様に使用されます。暗号化プロファイルを編集中に、バウンス プロファイルおよびカスタム メッセージ暗号化失敗通知を編集していた場合に送信するカスタム バウンス通知を指定できます。

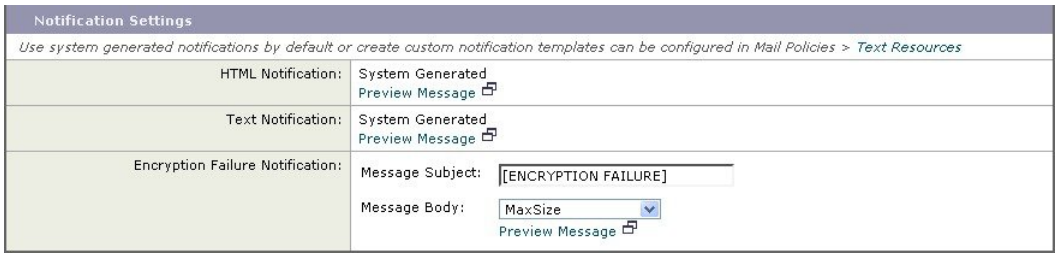
次の図は、バウンス プロファイルで指定されたバウンス通知テンプレートを示しています。

図 *41* : バウンス プロファイルのバウンス通知の例

（注） カスタム テンプレートを使用する場合は、RFC-1891 の DSN を使用してください。

次の図は、暗号化プロファイルで指定された暗号化失敗テンプレートを示しています。

図 *42* : 暗号化プロファイルの暗号化失敗通知の例



関連項目

- バウンス通知および暗号化失敗通知変数 （816 ページ）

バウンス通知および暗号化失敗通知変数

バウンス通知または暗号化失敗通知を作成する際に、次の表に記載されている通知変数を使用できます。

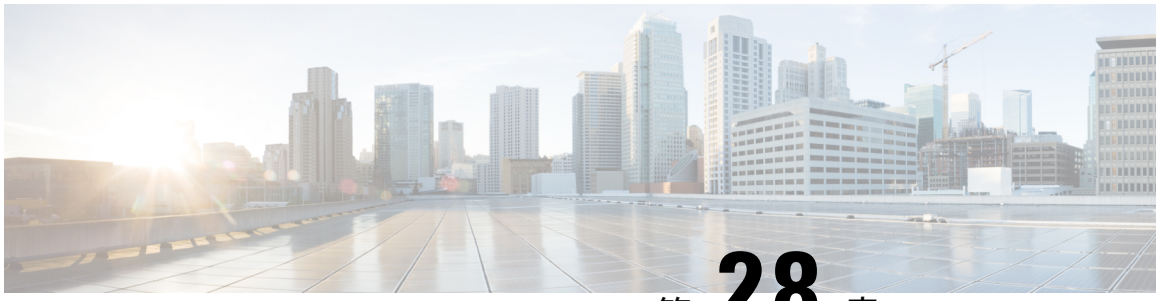
表 *50* : バウンス通知変数

変数	置き換える値
$Subject	元のメッセージの件名。

変数	置き換える値
$Date	現在の日付（MM/DD/YYYY 形式）に置き換えられます。
$Time	現在の時刻（ローカル時間帯）に置き換えられます。
$GMTimeStamp	現在の時刻および日付（GMT）に置き換えられます。電子メール メッセージの Received: 行で見られる形式と同様です。
$MID	メッセージを内部で識別するために使用するメッセージ ID（MID）に置き換えられます。RFC822「Message-Id」の値とは異なるため注意してください（「Message-Id」を取得するには $Header を使用します）。
$BouncedRecipient	バウンスされた受信者のアドレス。
$BounceReason	通知理由。
$remotehost	メッセージを 電子メールゲートウェイに送信したシステムのホスト名に置き換えられます。

暗号化通知テンプレート

暗号化通知テンプレートは、アウトバウンド電子メールを暗号化するように Cisco 電子メール暗号化を設定した際に使用されます。この通知では、受信者が暗号化されたメッセージを受信したことを通知し、メッセージを読む手順を説明しています。暗号化メッセージと一緒に送信するカスタム暗号化通知を指定できます。暗号化プロファイルを作成する際は、HTML 形式およびテキスト形式の両方の暗号化通知を指定します。このため、カスタムプロファイルを作成する場合は、テキスト形式および HTML 形式の両方の通知を作成する必要があります。



第 28 章

SMTP サーバを使用した受信者の検証

この章は、次の項で構成されています。

- SMTP コールアヘッド受信者検証の概要 （819 ページ）
- SMTP コールアヘッド受信者検証のワークフロー （819 ページ）
- 外部 SMTP サーバを使用した受信者の検証方法 （821 ページ）
- リスナーでの SMTP サーバ経由の着信メール検証のイネーブル化 （826 ページ）
- LDAP ルーティング クエリの構成 （826 ページ）
- SMTP コールアヘッド クエリのルーティング （827 ページ）
- 特定のユーザまたはグループの SMTP コールアヘッド検証のバイパス （828 ページ）

SMTP コールアヘッド受信者検証の概要

SMTP コールアヘッド受信者検証機能では、受信者宛ての着信メールを受け入れる前に、外部 SMTP サーバにクエリを実行します。LDAP 承認または Recipient Access Table（RAT; 受信者アクセステーブル）を使用できない場合、受信者を検証するためにこの機能を使用します。たとえば、それぞれ別のドメインを使用する多数のメール ボックスのメールをホストしていて、LDAP インフラストラクチャが各受信者を検証するために LDAP サーバにクエリーすることを許可していないとします。この場合、電子メールゲートウェイが SMTP サーバにクエリーを実行して、SMTP 通信を続ける前に受信者を検証できます。

SMTP コールアヘッド受信者検証を使用して、無効な受信者宛てのメッセージの処理を減らします。通常、無効な受信者宛てのメッセージは、ドロップする前にワーク キューを通して処理します。代わりに、電子メール パイプラインの着信および受信部分で追加処理を行わずに無効なメッセージをドロップまたはバウンスできます。

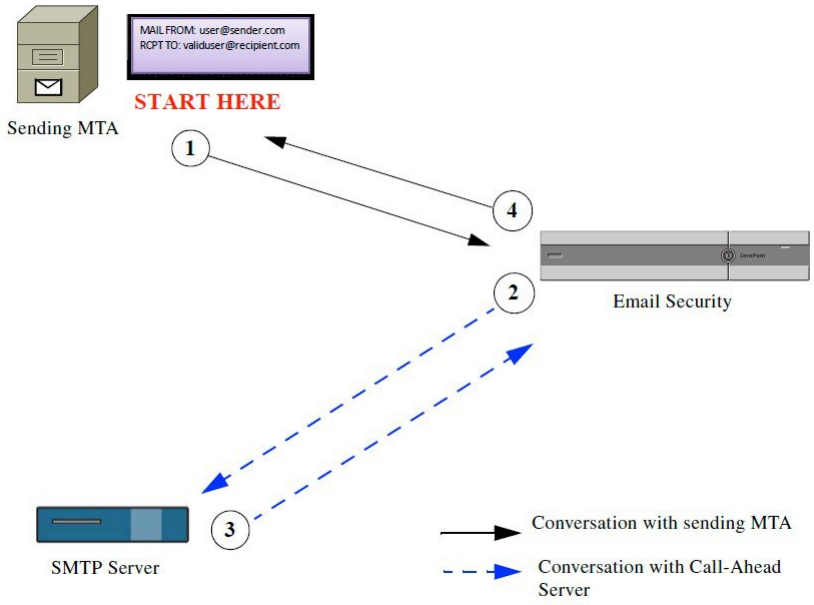
SMTP コールアヘッド受信者検証のワークフロー

電子メールゲートウェイ で SMTP コールアヘッド受信者検証を設定すると、電子メールゲートウェイ は、SMTP サーバに「事前に電話して」受信者を検証する間、送信側の MTA との SMTP 通信を中断します。電子メールゲートウェイは、SMTP サーバにクエリーを実行するとき、SMTP サーバの応答を E メール セキュリティ アプライアンスに返し、ユーザの設定に基

づいて、メールを受け入れるか、コードとカスタム応答で接続をドロップすることができます。

次の図に、SMTP コールアヘッド検証通信の基本的なワークフローを示します。

図 *43 : SMTP* コールアヘッド サーバ通信のワークフロー



1. 送信側の MTA が SMTP 通信を開始します。
2. 電子メールゲートウェイは、SMTP サーバにクエリーを送信して受信者 validuser@recipient.com を検証する間、SMTP 通信を中断します。

（注） SMTP ルートまたは LDAP ルーティング クエリーが設定されている場合、SMTP サーバへのクエリーにはこれらのルートが使用されます。

3. SMTP サーバは、電子メールゲートウェイにクエリーの応答を返します。
4. 電子メールゲートウェイは SMTP 通信を再開し、送信側の MTA に応答を送信し、SMTP サーバの応答（および SMTP コールアヘッドプロファイルの設定）に基づいて接続を続行するかドロップします。

電子メールパイプラインでの処理の順序が決まっているため、特定の受信者宛てのメッセージが RAT によって拒否された場合、SMTP コールアヘッド受信者検証は発生しません。たとえば、RAT で *example.com* 宛てのメールのみを受け入れるように指定した場合、SMTP コールアヘッド受信者検証が発生する前に、*recipient@domain2.com* 宛てのメールは拒否されます。

（注） HAT でディレクトリ ハーベスト攻撃防止（DHAP）を設定した場合、SMTP コールアヘッド サーバの拒否は、指定した 1 時間あたりの最大無効受信者数の中の拒否数に含まれるので注意してください。SMTP サーバによって拒否が増える場合を考慮してこの数を調整する必要があります。DHAP の詳細については、「ゲートウェイでのメール受信の設定」を参照してください。

外部 SMTP サーバを使用した受信者の検証方法

	操作内容	詳細
ステップ 1	電子メールゲートウェイの SMTP サーバへの接続およびサーバの応答の解釈方法を決定します。	コールアヘッド サーバ プロファイルの設定（821 ページ）
ステップ 2	SMTP サーバが受信者を検証するようにパブリック リスナーを設定します。	リスナーでの SMTP サーバ経由の着信メール検証のイネーブル化（826 ページ）
ステップ 3	（任意）メールの別のホストにルーティングする際に使用する SMTP サーバを決定するには、LDAP ルーティング クエリーを更新します。	LDAP ルーティング クエリの構成（826 ページ）
ステップ 4	（任意）特定の受信者に対してコールアヘッド検証をバイパスするように電子メールゲートウェイを設定します	特定のユーザまたはグループの SMTP コールアヘッド検証のバイパス（828 ページ）

関連項目

- コールアヘッド サーバ プロファイルの設定（821 ページ）

コールアヘッド サーバ プロファイルの設定

SMTP コールアヘッド サーバ プロファイルの設定では、電子メールゲートウェイと SMTP サーバの接続方法と SMTP サーバから返される応答の解釈方法を設定します。

手順

ステップ 1 [ネットワーク（Network）]>[SMTP コールアヘッド（SMTP Call-Ahead）] をクリックします。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイルの設定値を入力します。詳細については、表「SMTP コールアヘッド サーバ プロファイルの設定」を参照してください。

ステップ 4 プロファイルの高度な設定を指定します。詳細については、表「SMTP コールアヘッドサーバプロファイルの詳細設定」を参照してください。

ステップ 5 変更を送信し、保存します。

次のタスク

- SMTP コールアヘッド サーバ プロファイルの設定 （822 ページ）
- コールアヘッド サーバの応答 （825 ページ）

SMTP コールアヘッド サーバ プロファイルの設定

SMTP コールアヘッドサーバプロファイルの設定時に、電子メールゲートウェイと SMTP サーバの接続方法を設定する必要があります。

表 *51 : SMTP* コールアヘッド サーバ プロファイルの設定

設定	説明
プロファイル名（Profile Name）	コールアヘッド サーバ プロファイルの名前。

設定	説明
コールアヘッド サーバ タイプ（Call-Ahead Server Type）	コールアヘッド サーバへの接続方法を次から 1 つ選択します。 • [配信ホストを使用（Use Delivery Host）]。SMTP コールアヘッド クエリーに配信電子メール アドレスのホストを使用するように指定する場合は、このオプションを選択します。たとえば、メールの受信アドレスが recipient@example.com の場合、SMTP クエリーは example.com に関連付けられた SMTP サーバに対して実行されます。SMTP ルートまたは LDAP ルーティング クエリーを設定した場合、クエリー先の SMTP サーバの決定には、これらのルートが使用されます。LDAP ルーティング クエリーの設定についての詳細は、LDAP ルーティング クエリの構成 （826 ページ）を参照してください。 • [スタティック コールアヘッドサーバ（Static Call-Ahead Server）]。クエリー先のコールアヘッド サーバのスタティック リストを作成する場合は、このオプションを使用します。コールアヘッド サーバの名前や場所が頻繁に変わらないと思われる場合は、このオプションを使用できます。このオプションを使用すると、電子メール ゲートウェイは、リストの最初のスタティック コールアヘッド サーバからラウンドロビン方式でホストにクエリーを送信します。 （注） スタティック コールアヘッド サーバ タイプを選択すると、クエリーに SMTP ルートは適用されないので注意してください。その代わり MX ルックアップが実行され、その後、ホストでスタティック サーバのコールアヘッド IP アドレスを取得するためのルックアップが実行されます。
スタティック コールアヘッドサーバ（Static Call-Ahead Servers）	スタティック コールアヘッド サーバ タイプを使用する場合は、このフィールドにホストとポートの組み合わせのリストを入力します。次の構文を使用して、サーバとポートのリストを作成します。 ironport.com:25 複数のエントリがある場合は、カンマで区切ります。

次の表に、SMTP コールアヘッド サーバ プロファイルの高度な設定を示します。

表 *52 : SMTP* コールアヘッド サーバ プロファイルの高度な設定

設定	説明
インターフェイス（Interface）	SMTP サーバと SMTP 通信を開始するときに使用されるインターフェイス。 [管理インターフェイス（Management interface）] または [自動（Auto）] のどちらを使用するかを選択します。[自動（Auto）] を選択すると、電子メールゲートウェイは、使用するインターフェイスを自動的に検出しようとします。Cisco IronPort インターフェイスは、次の方法で SMTP サーバとの接続を試みます。 • コールアヘッドサーバが設定済みインターフェイスの1つと同じサブネット上にある場合、接続は一致するインターフェイスによって開始されます。 • 設定済みの任意の SMTP ルートが、クエリーのルートに使用されます。 • それ以外の場合、デフォルト ゲートウェイと同じサブネット上にあるインターフェイスが使用されます。
受信者検証の TLS サポート	TLS を使用して SMTP コールアヘッド受信者検証を実行する場合は、[イネーブル化（Enabled）] オプションボタンを選択します。 （注） SMTP コールアヘッド受信者検証では、電子メールゲートウェイの [SSL 設定（SSL Configuration）] ページの [その他の TLS クライアントサービス（Other TLS Client Services）] オプションで選択したものと同じ TLS バージョンを使用します。 （注） [受信者検証の TLS サポート（TLS Support for Recipient Validation）] オプションを選択した場合は、TLS を使用した SMTP コールアヘッド受信者検証を確立するために、電子メールゲートウェイに有効なクライアント証明書を追加します。 （注） SMTP コールアヘッド受信者検証の TLS サポートでは、DEFAULT SSL 暗号リストを使用します。DEFAULT キーワードは OpenSSL DEFAULT 暗号ストリングで、通常は `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2` です。
MAIL FROMアドレス（MAIL FROM Address）	SMTP サーバとの SMTP 通信に使用される MAIL FROM: アドレス。
検証要求タイムアウト（Validation Request Timeout）	SMTP サーバからの結果を待機する秒数。このタイムアウト値は、複数のコールアヘッドサーバにアクセスする可能性のある1つの受信者検証要求に対する値です。コールアヘッドサーバの応答 （825 ページ）を参照してください。

設定	説明
検証エラーのアクション（Validation Failure Action）	受信者検証要求が失敗した場合（タイムアウト、サーバの障害、ネットワークの問題、または不明な応答により）に実行するアクション。電子メールゲートウェイでのさまざまな応答の処理方法を設定できます。コールアヘッド サーバの応答 （825 ページ）を参照してください。
一時的なエラーのアクション（Temporary Failure Action）	受信者検証要求が一時的に失敗した場合（リモート SMTP サーバから 4xx 応答が返された）に実行するアクション。メールボックスが一杯の場合、メールボックスを利用できない場合、またはサービスを利用できない場合に発生することがあります。 コールアヘッド サーバの応答 （825 ページ）を参照してください。
セッションあたりの最大受信者数（Max. Recipients per Session）	1 つの SMTP セッションで検証する最大受信者数。 1 ～ 25,000 セッションの間で指定します。
サーバあたりの最大接続数（Max. Connections per Server）	1 台のコールアヘッド SMTP サーバへの最大接続数。 1 ～ 100 接続の間で指定します。
キャッシュ（Cache）	SMTP 応答のキャッシュのサイズ。100 ～ 1,000,000 エントリの間で指定します。
キャッシュ TTL（Cache TTL）	キャッシュ内でのエントリの存続可能時間値。このフィールドのデフォルト値は 900 秒です。60 ～ 86400 秒の間で指定します。

コールアヘッド サーバの応答

SMTP サーバからは、次の応答が返されます。

- **2xx**：コールアヘッド サーバから 2 で始まる SMTP コードを受け取った場合、受信者は受け入れられます。たとえば、応答が 250 の場合、メーリング アクションを続行できます。
- **4xx**：4 で始まる SMTP コードは、SMTP 要求の処理中に一時的な障害が発生したことを示します。後で再試行すると正常に処理されることがあります。たとえば、応答 451 は、要求されたアクションが中止されたか、処理中にローカル エラーが発生したことを示します。
- **5xx**：5 で始まる SMTP コードは、SMTP 要求の処理中に永続的な障害が発生したことを示します。たとえば、応答 550 は、要求されたアクションが実行されなかったか、メールボックスを使用できなかったことを示します。
- **タイムアウト。**コールアヘッドサーバから応答が戻されない場合、タイムアウトが発生する前に再試行する時間を設定できます。
- **接続エラー。**コールアヘッドサーバへの接続に失敗した場合、受信者アドレスへの接続を受け入れるか拒否するかを設定できます。

- **カスタム応答**。検証エラーおよび一時エラーのためにカスタムSMTP応答（コードとテキスト）との接続を拒否するよう設定できます。

リスナーでのSMTPサーバ経由の着信メール検証のイネーブル化

SMTP コールアヘッド サーバ プロファイルを作成したら、そのプロファイルをリスナーでイネーブルにして、リスナーがSMTPサーバ経由の着信メールを検証できるようにする必要があります。プライベート リスナーでは受信者の検証は必要ないので、SMTP コールアヘッド機能はパブリック リスナーでのみ使用できます。

手順

ステップ 1 [ネットワーク（Network）] > [リスナー（Listeners）] に移動します。

ステップ 2 SMTP コールアヘッド機能をイネーブルにするリスナーの名前をクリックします。

ステップ 3 [SMTPコールアヘッドプロファイル（SMTP Call Ahead Profile）] フィールドで、イネーブルにする SMTP コールアヘッド プロファイルを選択します。

ステップ 4 変更を送信し、保存します。

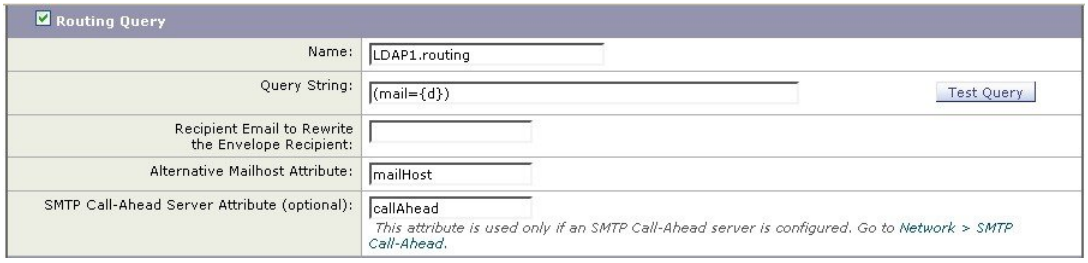
LDAP ルーティング クエリの構成

LDAP ルーティング クエリーを使用して、メールを異なるメール ホストにルーティングする場合、AsyncOS は、代替メールホスト属性を使用して、クエリー先の SMTP サーバを決定します。ただし、この処理が不適切な場合があります。たとえば、次のスキーマでは、メール ホスト属性（mailHost）には、コールアヘッド SMTP サーバの属性（callAhead）で指定されているサーバとは異なる SMTP アドレスがあります。

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

この場合、[SMTPコールアヘッド（SMTP Call-Ahead）] フィールドを使用して、SMTP コールアヘッド クエリーを callAhead 属性で指定されているサーバに転送するルーティング クエリーを作成できます。たとえば、次の属性でルーティング クエリーを作成できます。

図 *44 : SMTP* コールアヘッド用に設定された *LDAP* ルーティング クエリー



このクエリーでは、{d} は受信者アドレスのドメイン部分を表し、SMTP コールアヘッド サーバ属性は、クエリーに使用するコールアヘッド サーバとポートの値として、ポート 9025 の smtp2.mydomain.com、smtp3.mydomain.com を返します。

（注） この例は、LDAP ルーティング クエリーを使用して SMTP コールアヘッド クエリーを正しい SMTP サーバに転送できるクエリーの設定例の 1 つです。この例で説明したクエリー文字列や特定の LDAP 属性を使用する必要はありません。

SMTP コールアヘッド クエリのルーティング

SMTP コールアヘッドクエリーのルーティング時、AsyncOS は次の順序で情報をチェックします。

1. ドメイン名をチェックします。
2. LDAP ルーティング クエリーをチェックします。
3. SMTP ルートをチェックします。
4. DNS ルックアップを実行します（MX ルックアップ、A ルックアップの順に実行）。

ドメインに LDAP ルーティング クエリーまたは SMTP ルートが設定されていない場合、前の状態の結果は次のステージに渡されます。SMTP ルートが存在しない場合は、DNS ルックアップが実行されます。

SMTP コールアヘッド クエリーの代わりに LDAP ルーティング クエリーを使用するときに、SMTP ルートも設定されている場合、ルーティング動作は、ルーティング クエリーから返される値によって異なります。

- LDAP ルーティング クエリーからポートなしで 1 つのホスト名が返された場合、SMTP コールアヘッドクエリーは SMTP ルートを適用します。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。
- LDAP ルーティング クエリーからポートと共に 1 つのホスト名が返された場合、その SMTP ルートが使用されますが、SMTP ルートでポートが指定されていても、LDAP クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。

- LDAP ルーティング クエリーからポートと共に、またはポートなしで複数のホストが返された場合、SMTP ルートが適用されますが、SMTP ルートでポートが指定されていても、LDAP ルーティング クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。

特定のユーザまたはグループの SMTP コールアヘッド検証のバイパス

リスナーで SMTP コールアヘッド検証をイネーブルにしたまま、特定のユーザまたはユーザグループに対して SMTP コールアヘッド検証を省略する必要がある場合があります。

SMTP コールアヘッド クエリー中にメールを遅延させてはならない受信者に対する SMTP コールアヘッド検証を省略する場合です。たとえば、有効であることが明確であり、迅速な対応を必要とするカスタマー サービスのエイリアスに RAT エントリを追加できます。

SMTP コールアヘッド検証のバイパスを GUI から設定するには、RAT エントリを追加または編集するときに [SMTPコールアヘッドをバイパス（Bypass SMTP Call-Ahead）] を選択します。

第 29 章

他の MTA との暗号化通信

この章は、次の項で構成されています。

- 他の MTA との暗号化通信の概要 （829 ページ）
- 証明書の使用 （830 ページ）
- リスナー HAT の TLS の有効化 （837 ページ）
- 配信時の TLS および証明書検証の有効化 （840 ページ）
- 名前付きエンティティの DNS ベースの認証 （844 ページ）
- 認証局のリストの管理 （848 ページ）
- HTTPS の証明書のイネーブル化 （852 ページ）

他の MTA との暗号化通信の概要

エンタープライズゲートウェイ（またはメッセージ転送エージェント、つまり MTA）は通常、インターネット上で「素性が判別している相手」と通信します。つまり、通信は暗号化されません。場合によっては、悪意のあるエージェントが、送信者または受信者に知られることなく、この通信を傍受する可能性があります。通信は第三者によってモニタされる可能性や、変更される可能性さえあります。

Transport Layer Security（TLS）はセキュア ソケット レイヤ（SSL）テクノロジーを改良したバージョンです。これは、インターネット上での SMTP カンバセーションの暗号化に広く使用されているメカニズムです。AsyncOS では SMTP への STARTTLS 拡張（セキュアな SMTP over TLS）がサポートされます。詳細については、RFC 3207 を参照してください（これは、廃止になった RFC 2487 に代わるバージョンです）。

AsyncOS の TLS 実装では、暗号化によってプライバシーが確保されます。これによって、X.509 証明書および証明書認証局サービスからの秘密キーをインポートしたり、 電子メールゲートウェイ上で使用する自己署名証明書を作成したりできます。AsyncOS では、パブリック リスナーおよびプライベート リスナーに対する個々の TLS 証明書、インターフェイス上の セキュア HTTP（HTTPS）管理アクセス、LDAP インターフェイス、およびすべての発信 TLS 接続がサポートされます。

関連項目

- TLS を使用した SMTP カンバセーションの暗号化方法 （830 ページ）

TLS を使用した SMTP カンバセーションの暗号化方法

TLS を使用した SMTP カンバセーションの暗号化方法

	操作内容	詳細
ステップ 1	公認の認証局からの X.509 証明書と秘密キーを取得します。	証明書の使用 （830 ページ）
ステップ 2	電子メールゲートウェイに証明書をインストールします。	次のいずれかで証明書をインストールします。 • 自己署名証明書の作成 （833 ページ） • 証明書のインポート （835 ページ）
ステップ 3	メッセージ受信用、またはメッセージ配信用、またはその両方の TLS をイネーブルにします。	• リスナー HAT の TLS の有効化 （837 ページ） • 配信時の TLS および証明書検証の有効化 （840 ページ）
ステップ 4	（任意）リモート ドメインからの証明書を検証し、ドメインのクレデンシャルを確立するためにアプライアンスが使用する信頼できる認証局のリストをカスタマイズします。	認証局のリストの管理 （848 ページ）
ステップ 5	（任意）TLS 接続が必要なドメインにメッセージを送信できない場合に警告を送信するよう 電子メールゲートウェイを設定します。	要求された TLS 接続が失敗した場合のアラートの送信 （843 ページ）

証明書の使用

TLS を使用するには、電子メールゲートウェイに対する受信および配信のための X.509 証明書および一致する秘密キーが必要です。SMTP での受信および配信の両方には同じ証明書を使用し、インターフェイス（LDAP インターフェイス）上での HTTPS サービスや宛先ドメインへのすべての発信 TLS 接続には別の証明書を使用することも、それらのすべてに対して 1 つの証明書を使用することもできます。

certconfig を使用して証明書を設定した後で、Web インターフェイスの [ネットワーク（Network）] > [証明書（Certificates）] ページおよび CLI の print コマンドを使用して証明書の

リスト全体を表示できます。print コマンドでは中間証明書が表示されないことに注意してください。

注意 電子メールゲートウェイには TLS および HTTPS 機能がテスト済みであることを示すデモ証明書が同梱されますが、デモ証明書付きのサービスのいずれかをイネーブルにすることはセキュアではないため、通常の使用には推奨できません。デフォルトのデモ証明書が付属しているいずれかのサービスをイネーブルにすると、CLI に警告メッセージが表示されます。

関連項目

- 署名付き証明書の導入 （831 ページ）
- 自己署名証明書の導入 （831 ページ）

署名付き証明書の導入

たとえば、マシンがドメインにないために電子メールゲートウェイと他のマシン間で自己署名証明書を交換できない場合、署名付き証明書を使用します。企業のセキュリティ部門には、他にも要件が存在する場合があります。

	操作内容	詳細
ステップ 1	クラスタに導入する場合は、次の手順に従います。	証明書と集中管理 （832 ページ）
ステップ 2	自己署名証明書および証明書署名要求（CSR）を生成します。	自己署名証明書の作成 （833 ページ）
ステップ 3	生成された証明書を、署名のために既知の認証局に送信します。	認証局への証明書署名要求（CSR）の送信について （834 ページ）
ステップ 4	署名付き証明書をアップロードします。	認証局によって署名された証明書のアップロード （834 ページ）
ステップ 5	証明書に署名した認証局が、信頼できる認証局のリストにあることを確認します。	認証局のリストの管理 （848 ページ）
ステップ 6	該当する場合、中間証明書を使用します。	中間証明書 （832 ページ）

自己署名証明書の導入

自己署名証明書は一般に、企業のファイアウォールの背後にある電子メールゲートウェイ間の通信に使用できます。企業のセキュリティ部門には、他にも要件が存在する場合があります。

	操作内容	詳細
ステップ 1	クラスタに導入する場合は、次の手順に従います。	証明書と集中管理 （832 ページ）
ステップ 2	電子メールゲートウェイから自己署名証明書を生成します。	自己署名証明書の作成 （833 ページ）
ステップ 3	自己署名証明書をエクスポートします。	証明書のエクスポート （836 ページ）
ステップ 4	自己署名証明書を、 電子メールゲートウェイと通信するマシンにインポートします。	他のマシンのマニュアルを参照してください。
ステップ 5	他のマシンから自己署名証明書を生成し、エクスポートします。	他のマシンのマニュアルを参照してください。
ステップ 6	自己署名証明書を別のマシンから 電子メールゲートウェイにインポートします。	証明書のインポート （835 ページ） または そのマシンとの通信の設定については、このマニュアルの章を参照してください。 たとえば、Cisco AMP Threat Grid アプライアンスとのセキュアな通信を構成するには、オンプレミスのファイル分析サーバの設定 （593 ページ）の詳細設定を構成する手順を参照してください。

証明書と集中管理

証明書は通常、証明書の共通名にローカル マシンのホスト名を使用します。 電子メールゲートウェイがクラスタの一部である場合は、クラスタレベルでインストールできるワイルドカードの証明書またはサブジェクト代替名（SAN）の証明書を除いてマシンレベルとして各クラスタメンバの証明書をインポートする必要があります。メンバーのリスナーが別のマシンと通信するときにクラスタが参照できるように、各クラスタ メンバの証明書は、同じ証明書の名前を使用する必要があります。

中間証明書

ルート証明書の検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、信頼の連鎖を効率的に作成することによって、追加の証明書を作成するために使用されます。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた godaddy.com によって証明書が発行されたとします。godaddy.com によって発行された証明書では、信頼できるルート認証局の秘密キーと同様に godaddy.com の秘密キーが検証される必要があります。

自己署名証明書の作成

次のいずれかの理由により、電子メールゲートウェイで自己署名証明書を作成する可能性があります。

- 他の MTA との SMTP カンバセーションを TLS（着信と発信カンバセーションの両方）を使用して暗号化するため。
- HTTPS を使用して GUI にアクセスするための 電子メールゲートウェイの HTTPS サービスをイネーブルにするため。
- LDAP サーバがクライアント認証を要求した場合に LDAPS のクライアント証明書として使用するため。
- 電子メールゲートウェイと Cisco AMP Threat Grid アプライアンスとのセキュアな通信を許可するため。

CLI を使用して自己署名証明書を作成するには、certconfig コマンドを使用します。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] を選択します。

ステップ 2 [証明書の追加（Add Certificate）] をクリックします。

ステップ 3 [自己署名証明書の作成（Create Self-Signed Certificate）] を選択します。

ステップ 4 自己署名証明書に、次の情報を入力します。

共通名	完全修飾ドメイン名
組織	組織の正確な正式名称。
組織単位	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
秘密キーサイズ	CSR 用に生成する秘密キーのサイズ。2048 ビットおよび 1024 ビットだけがサポートされます。

ステップ 5 [Next] をクリックします。

ステップ 6 [FQDN検証（FQDN Validation）] チェックボックスをオンにして、電子メールゲートウェイで証明書に存在する共通名が FQDN 形式であるかどうかを確認できるようにします。

ステップ 7 証明書の名前を入力します。デフォルトでは、前に入力された共通名が割り当てられます。

ステップ 8 この証明書を証明書署名要求（CSR）として送信するには、[証明書署名要求のダウンロード（Download Certificate Signing Request）] をクリックして CSR を PEM 形式でローカルまたはネットワーク マシンに保存します。

ステップ 9 変更を送信し、保存します。

次のタスク

該当する次のステップを参照してください。

- 署名付き証明書の導入　（831 ページ）
- 自己署名証明書の導入　（831 ページ）

認証局への証明書署名要求（CSR）の送信について

認証局は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。証明書および秘密キーは認識されている認証局から購入できます。シスコでは、サービスの重複を推奨しません。

電子メールゲートウェイでは、自己署名証明書を作成して、公開証明書を取得するために認証局に送信する証明書署名要求（CSR）を生成できます。認証局は、秘密キーによって署名された信頼できる公開証明書を返送します。Web インターフェイスの [ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の certconfig コマンドを使用して自己署名証明書を作成し、CSR を生成して、信頼できる公開証明書をインストールします。

初めて証明書を取得または作成する場合は、インターネットで「certificate authority services SSL Server Certificates（SSL サーバ証明書を提供している認証局）」を検索して、お客様の環境のニーズに最も適したサービスを選択してください。サービスの手順に従って、証明書を取得します。

次のタスク

署名付き証明書の導入　（831 ページ） を参照してください。

認証局によって署名された証明書のアップロード

認証局から秘密キーで署名された信頼できる公開証明書が返されたら、証明書を 電子メールゲートウェイにアップロードします。

パブリック リスナーまたはプライベート リスナー、IP インターフェイスの HTTPS サービス、LDAP インターフェイス、または宛先ドメインへのすべての発信 TLS 接続に証明書を使用できます。

手順

ステップ 1 受信した信頼できる公開証明書が PEM 形式であるか、または 電子メールゲートウェイにアップロードする前にPEMを使用するように変換できる形式であることを確認します。（変換ツールは http://www.openssl.org の無料のソフトウェア OpenSSL に含まれています。）

ステップ 2 署名付き証明書を 電子メールゲートウェイにアップロードします。

（注） 証明書を認証局からアップロードすると、既存の自己署名証明書が上書きされます。

a) [ネットワーク（Network）] > [証明書（Certificates）] を選択します。
b) 署名のために認証局に送信した証明書の名前をクリックします。
c) ローカル マシンまたはネットワーク ボリューム上のファイルへのパスを入力します。

ステップ 3 自己署名証明書に関連する中間証明書をアップロードすることもできます。

次のタスク

関連項目

- 署名付き証明書の導入 （831 ページ）

証明書のインポート

AsyncOS では、 電子メールゲートウェイで使用するために、PKCS #12 形式で保存された証明書を他のマシンからインポートすることもできます。

CLI を使用して証明書をインポートするには、**certconfig** コマンドを使用します。

（注） 署名付き証明書を導入する場合、この手順を使用して署名付き証明書をインポートしないでください。代わりに、認証局によって署名された証明書のアップロード （834 ページ）を参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] を選択します。

ステップ 2 [証明書の追加（Add Certificate）] をクリックします。

ステップ 3 [証明書のインポート（Import Certificate）] オプションを選択します。

ステップ 4 ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。

ステップ 5 ファイルのパスフレーズを入力します。

ステップ 6 [次へ（Next）] をクリックして証明書の情報を表示します。

ステップ 7 [FQDN検証（FQDN Validation）] チェックボックスをオンにすると、証明書に存在する [共通名（Common Name）] フィールド、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式であるかどうかを電子メールゲートウェイで確認できます。

ステップ 8 証明書の名前を入力します。

AsyncOS のデフォルトでは、共通の名前が割り当てられます。

ステップ 9 変更を送信し、保存します。

次のタスク

- 自己署名証明書を導入する場合は、自己署名証明書の導入 （831 ページ）を参照してください。

証明書のエクスポート

AsyncOS では、証明書をエクスポートし、PKCS #12 形式で保存することも可能です。

（注） 署名付き証明書を導入する場合、この手順を使用して証明書署名要求（CSR）を生成しないでください。代わりに、署名付き証明書の導入 （831 ページ）を参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [証明書のエクスポート（Export Certificate）] をクリックします。

ステップ 3 エクスポートする証明書を選択します。

ステップ 4 証明書のファイル名を入力します。

ステップ 5 証明書ファイルのパスフレーズを入力して確認します。

ステップ 6 [エクスポート（Export）] をクリックします。

ステップ 7 ファイルをローカル マシンまたはネットワーク マシンに保存します。

ステップ 8 さらに証明書をエクスポートするか、または [キャンセル（Cancel）] をクリックして [ネットワーク（Network）] > [証明書（Certificates）] ページに戻ります。

次のタスク

- 自己署名証明書を導入する場合は、自己署名証明書の導入 （831 ページ）を参照してください。

リスナー HAT の TLS の有効化

暗号化が必要なリスナーに対して TLS をイネーブルにする必要があります。インターネットに対するリスナー（つまり、パブリック リスナー）には TLS をイネーブルにしますが、内部システムのリスナー（つまり、プライベート リスナー）には必要ありません。また、すべてのリスナーに対して暗号化をイネーブルにすることもできます。

リスナーの TLS に次の設定を指定できます。

表 *53*：リスナーの *TLS* 設定

TLS 設定	意味
1. No	TLS では着信接続を行えません。リスナーに対する接続では、暗号化された SMTP カンバセーションは必要ありません。これは、電子メールゲートウェイ上で設定されるすべてのリスナーに対するデフォルト設定です。
2. Preferred	TLS で MTA からのリスナーへの着信接続が可能です。
3. Required	TLS で MTA からリスナーへの着信接続が可能です。また、STARTTLS コマンドを受信するまで電子メールゲートウェイは NOOP、EHLO、または QUIT 以外のすべてのコマンドに対してエラーメッセージで応答します。この動作は RFC 3207 によって指定されています。RFC 3207 では、Secure SMTP over Transport Layer Security の SMTP サービス拡張が規定されています。TLS が「必要」であることは、送信側で TLS の暗号化を行わない電子メールが、送信前に電子メールゲートウェイによって拒否されることを意味し、このため、暗号化されずにクリアテキストで転送されることが回避されます。

デフォルトでは、プライベート リスナーとパブリック リスナーのどちらも TLS 接続を許可しません。電子メールの着信（受信）または発信（送信）の TLS をイネーブルにするには、リスナーの HAT の TLS をイネーブルにする必要があります。また、プライベート リスナーおよびパブリック リスナーのすべてのデフォルト メール フロー ポリシー設定で tls 設定が「off」になっています。

リスナーの作成時に、個々のパブリック リスナーに TLS 接続の専用の証明書を割り当てることができます。詳細については、Webインターフェイスを使用してリスナーを作成することによる接続要求のリスニング （88 ページ）を参照してください。

関連項目

- GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て （838 ページ）
- CLI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て （838 ページ）
- ログ （843 ページ）

• GUI の例：リスナーの HAT の TLS 設定の変更 （839 ページ）
• CLI の例：リスナーの HAT の TLS 設定の変更 （839 ページ）

GUI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て

手順

ステップ 1 [ネットワーク（Network）] > [リスナー（Listeners）] ページに移動します。
ステップ 2 編集するリスナーの名前をクリックします。
ステップ 3 [証明書（Certificate）] フィールドから、証明書を選択します。
ステップ 4 変更を送信し、保存します。

CLI を使用したパブリックまたはプライベートのリスナーへの TLS 接続のための証明書の割り当て

手順

ステップ 1 `listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。
ステップ 2 `certificate` コマンドを使用して、使用できる証明書を表示します。
ステップ 3 プロンプトが表示されたら、リスナーを割り当てる証明書を選択します。
ステップ 4 リスナーの設定が完了したら、`commit` コマンドを発行して、変更をイネーブルにします。

ログ

TLS が必要であるにもかかわらず、リスナーで使用できない場合は、E メール セキュリティ アプライアンスがメール ログ インスタンスに書き込みます。次の条件のいずれかを満たす場合、メール ログが更新されます。

- リスナーに対して TLS が「必須（required）」と設定されている。
- E メール セキュリティ アプライアンスは、「STARTTLS コマンドを最初に発行（Must issue a STARTTLS command first）」コマンドを送信した。
- 正常な受信者が受信せずに接続が終了した。

TLS 接続が失敗した理由に関する情報がメール ログに記録されます。

GUI の例：リスナーの HAT の TLS 設定の変更

手順

ステップ 1 [メール ポリシー（Mail Policies）] > [メール フロー ポリシー（Mail Flow Policies）] ページに移動します。

ステップ 2 変更するポリシーを持つリスナーを選択し、編集するポリシーの名前へのリンクをクリックします。（デフォルト ポリシー パラメータも編集可能）。

ステップ 3 [暗号化と認証（Encryption and Authentication）] セクションの [TLS:] フィールドで、リスナーに必要な TLS のレベルを選択します。

ステップ 4 変更の送信と保存

選択した TLS 設定が反映されてリスナーのメール フロー ポリシーが更新されます

CLI の例：リスナーの HAT の TLS 設定の変更

手順

ステップ 1 `listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。

ステップ 2 リスナーのデフォルトの HAT 設定を編集するには、`hostaccess -> default` コマンドを使用します。

ステップ 3 次の質問が表示されたら、次の選択肢のいずれかを入力して TLS 設定を変更します。

```
Do you want to allow encrypted TLS connections?

1. No

2. Preferred

3. Required

[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to

ensure that there is a valid certificate configured.
```

ステップ 4 この例では、リスナーで使用できる有効な証明書があるかどうかを確認するために `certconfig` コマンドを使用するかどうかを質問しています。証明書を作成していない場合、リスナーでは電子メールゲートウェイにあらかじめインストールされているデモ証明書を使用します。テスト目的でデモ証明書で TLS をイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。リスナーに証明書を割り当てるには、`listenerconfig -> edit -> certificate` コマンドを使用します。TLS を設定すると、CLI でリスナーの概要に設定が反映されます。

```
Name: Inboundmail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

ステップ 5 変更をイネーブルにするには、`commit` コマンドを発行します

配信時の TLS および証明書検証の有効化

[送信先コントロール（Destination Controls）]ページまたは`destconfig`コマンドを使用すると、TLS をイネーブルにして、特定のドメインに電子メールを配信するように要求できます。

TLSだけでなく、ドメインのサーバ証明書の検証も要求できます。このドメイン証明書は、ドメインのクレデンシャルを確立するために使用されるデジタル証明書に基づいています。検証プロセスには、次の 4 つの要件が含まれます。

- 信頼できる認証局（CA）によって発行された証明書で終わる SMTP セッションの証明書発行者のチェーン。
- 受信マシンの DNS 名またはメッセージの宛先ドメインのいずれかと一致する証明書に表示された Common Name（CN）。

  または

  メッセージの宛先ドメインが、証明書のサブジェクト代替名（subjectAltName）の拡張の DNS 名のいずれかと一致している（RFC 2459 を参照）。この一致では、RFC 2818 のセクション 3.1 で説明されているワイルドカードがサポートされます。

- [オプション - FQDN検証がSSL設定で有効な場合のみ（Optional - Only if FQDN validation enabled in SSL Configuration settings）]：サーバ証明書にある [共通名（Common Name）]、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式かどうかを確認します。
- [オプション - SSL構成時の設定でX 509検証が有効になっている場合のみ（Optional - Only if X 509 validation enabled in SSL Configuration settings）]：サーバ証明書の署名アルゴリズムを確認します。

信頼できるCAは、IDの検証および公開キーの配布に使用されるデジタル証明書を発行する、第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。

エンベロープ暗号化の代わりに TLS 接続を介してドメインにメッセージを送信するように 電子メールゲートウェイを設定できます。詳細については、「Cisco 電子メール暗号化」の章を参照してください。

すべての発信 TLS 接続に対して 電子メールゲートウェイで使用する証明書を指定できます。証明書を指定するには、[送信先コントロール（Destination Controls）] ページの [グローバル設定の編集（Edit Global Settings）] をクリックするか、または CLI で `destconfig -> setup` を使用します。証明書はドメインごとの設定ではなく、グローバル設定です。

[送信先コントロール（Destination Controls）] ページまたは `destconfig` コマンドを使用してドメインを含める場合、指定されたドメインの TLS に 5 つの異なる設定を指定できます。TLS のエンコードにドメインとの交換が必須であるか、または推奨されるかの指定に加えて、ドメインの検証が必要かどうかも指定できます。設定の説明については、次の表を参照してください。

表 *54* : 配信の *TLS* 設定

TLS 設定	意味
デフォルト	デフォルトの TLS 設定では、リスナーからドメインの MTA への発信接続に [送信先コントロール（Destination Controls）] ページまたは `destconfig -> default` サブコマンドを使用するように設定されています。 質問の "Do you wish to apply a specific TLS setting for this domain?" に対して "no" と回答すると、値の "Default" が設定されます。
1. ×	インターフェイスからドメインの MTA への発信接続には、TLS がネゴシエートされません。
2. 推奨（Preferred）	電子メールゲートウェイ インターフェイスからドメインの MTA への TLS がネゴシエートされます。ただし、（220 応答を受信する前に）TLS ネゴシエーションに失敗すると、SMTP トランザクションはクリアテキストにフォールバックしません。証明書が信頼できる認証局によって発行された場合、検証は行われません。220 応答を受信した後でエラーが発生して TLS ネゴシエーションに失敗すると、SMTP トランザクションは「クリアな」（暗号化されない）ままです。
3. 必須（Required）	電子メールゲートウェイ インターフェイスからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証は行われません。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。ネゴシエーションに成功すると、暗号化されたセッションを経由して電子メールが配信されます。

TLS 設定	意味
4. 推奨（検証）	電子メールゲートウェイからドメインの MTA への TLS がネゴシエートされます。 電子メールゲートウェイはドメインの証明書の検証を試行します。 次の 3 つの結果が考えられます。 • TLS がネゴシエートされ、証明書が検証される。暗号化されたセッションによってメールが配信される。 • TLS がネゴシエートされるものの、証明書は検証されない。暗号化されたセッションによってメールが配信される。 • TLS 接続が確立されず、証明書は検証されない。電子メール メッセージがプレーン テキストで配信される。
5. 必須（検証）	電子メールゲートウェイからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証が必要です。次の結果が考えられます。 • TLS 接続がネゴシエートされ、証明書が検証される。暗号化されたセッションによって電子メール メッセージが配信される。 • TLS 接続がネゴシエートされるが、信頼できる認証局（CA）によって証明書が検証されない。メールは配信されない。 • TLS 接続がネゴシエートされない。メールは配信されない。
6. 必須 - ホステッドドメインの検証	[必要な TLS（TLS Required）]、[検証と必要な TLS（Verify and TLS Required）]、[ホステッド ドメインの検証（Verify Hosted Domain）] の各オプションは、ID 検証プロセスに相違があります。提示される ID を処理する方法および使用が許可される参照識別子の種類によって、最終的な結果に相違が生じます。 提示される ID は、最初に、`dNSName` タイプの `subjectAltName` 拡張子から派生されます。`dNSName` と承認された参照識別子（`REF-ID`）のいずれかとの間が一致しない場合、`CN` が件名フィールドに存在し、さらなる ID 検証に合格するかどうかに関係なく、検証は失敗します。件名フィールドから派生した `CN` は、証明書に `dNSName` タイプの `subjectAltName` 拡張子が含まれない場合のみ検証されます。

グッド ネイバー テーブルに指定された受信者ドメインの指定されたエントリがない場合、または指定されたエントリが存在するものの、そのエントリに対して指定された TLS 設定が存在しない場合、[送信先コントロール（Destination Controls）] ページまたは `destconfig -> default` サブコマンド（"No"、"Preferred"、"Required"、"Preferred (Verify)"、または "Required (Verify)"）を使用して動作を設定する必要があります。

関連項目

- 要求された TLS 接続が失敗した場合のアラートの送信 （843 ページ）
- ログ （843 ページ）
- 認証局のリストの管理 （848 ページ）

要求された TLS 接続が失敗した場合のアラートの送信

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、電子メールゲートウェイがアラートを送信するかどうかを指定できます。アラート メッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。電子メールゲートウェイは、システムアラートのタイプの警告重大度レベルアラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。GUI の [システム管理（System Administration）] > [アラート（Alerts）] ページ（または CLI の alertconfig コマンド）を使用してアラートの受信者を管理できます。

関連項目

- TLS 接続アラートの有効化 （843 ページ）

TLS 接続アラートの有効化

手順

ステップ 1 メール ポリシーの [送信先コントロール（Destination Controls）] ページに移動します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 [必要な TLS 接続に失敗した場合にアラートを送信：（Send an alert when a required TLS connection fails:）] の **[有効（Enable）]** をクリックします。

これは、ドメイン単位ではなく、グローバルな設定です。電子メールゲートウェイが配信を試行したメッセージの情報については、[モニタ（Monitor）]>[メッセージトラッキング（Message Tracking）] ページまたはメールログを使用します。

ステップ 4 変更を送信し、保存します。

次のタスク

これはコマンドライン インターフェイスでも構成できます。CLI で destconfig -> setup コマンドを使用して TLS 接続アラートを有効化します。

ログ

ドメインに TLS が必要であるにもかかわらず、使用できない場合、電子メールゲートウェイによってメールログインスタンスで通知されます。TLS接続を使用できなかった理由も記載されています。次の条件のいずれかを満たす場合、メール ログが更新されます。

- リモート MTA で ESMTP がサポートされない（たとえば、 電子メールゲートウェイからの EHLO コマンドが理解できない）。
- リモート MTA で ESMTP がサポートされるものの、「STARTTLS」が EHLO 応答でアドバタイズされる拡張のリストにない。

- リモート MTA で「STARTTLS」拡張がアドバタイズされたものの、 電子メールゲートウェイで STARTTLS コマンドを送信した際にエラーが返される。

名前付きエンティティの DNS ベースの認証

- 名前付きエンティティの SMTP DNS ベースの認証の概要 （844 ページ）
- DANE をサポートする配信に向けた TLS の有効化 （846 ページ）
- DANE 失敗時のアラートの送信 （848 ページ）

名前付きエンティティの SMTP DNS ベースの認証の概要

証明書を使用して認証された TLS 接続は、以下のいずれかの方法でセキュリティ侵害に対して脆弱となる可能性があります。

- 信頼できる認証局（CA）は任意のドメイン名に証明書を発行できます。
- 攻撃者は、中間者（man-in-the-middle）攻撃を使用して、TLS 接続をプレーン テキスト通信にダウングレードできます。
- DNS サーバで DNSSEC が設定されていない場合、攻撃者は偽の DNS MX レコードで DNS レスポンスを偽って安全でないサーバにメッセージをリダイレクトし、DNS キャッシュ ポイズニング攻撃を仕掛けます。
- 受信側のメール転送エージェント（MTA）に信頼できる認証局（CA）のリストが設定されていない場合は、自己署名の証明書またはプライベート認証局によって発行された証明書を使用できます。

名前付きエンティティの SMTP DNS ベースの認証（DANE）プロトコルは、DNS サーバで設定したドメイン ネーム システム セキュリティ（DNSSEC）拡張と、TLSA としても知られる DNS リソース レコードを使用して、X.509 証明書と DNS 名を検証します。

TLSA レコードは RFC 6698 で記述される DNS 名に対して使用される認証局（CA）、エンドエンティティの証明書、トラスト アンカーのいずれかの詳細が含まれる証明書に追加されます。詳細については、TLSA レコードの作成 （846 ページ）を参照してください。ドメイン ネーム システム セキュリティ（DNSSEC）拡張は、DNS セキュリティの脆弱性に対応することで、DNS のセキュリティを強化します。暗号化キーおよびデジタル署名を使用する DNSSEC は、ルックアップ データが正確で、適切なサーバに接続されていることを保証します。

以下は、送信 TLS 接続に SMTP DANE を使用する利点です。

- 中間者（MITM）ダウングレード攻撃、傍受、DNS キャッシュ ポイズニング攻撃を防ぎ、メッセージを安全に配信します。
- DNSSEC によって保護することで、TLS 証明書と DNS 情報の信憑性を保証します。

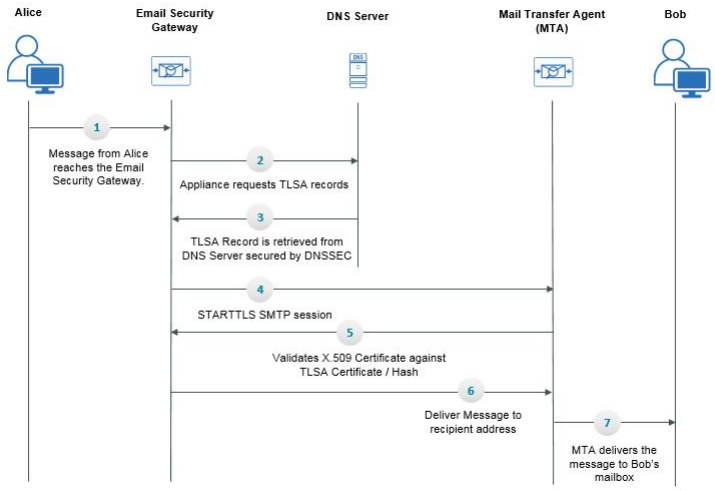
関連項目

- SMTP DANE ワークフロー （845 ページ）
- TLSA レコードの作成 （846 ページ）
- DANE をサポートする配信に向けた TLS の有効化 （846 ページ）
- DANE 失敗時のアラートの送信 （848 ページ）

SMTP DANE ワークフロー

以下の図は、送信 TLS 接続と DANE サポートを使用したメッセージのフローを説明しています。

図 *45 : TLS* と *DANE* サポートを使用したメッセージの配信



1. 送信側（アリス）は、組織外の受信者（ボブ）にメッセージを送信します。
2. メッセージが電子メールゲートウェイに到達します。
3. 電子メールゲートウェイが、DNS の TLSA レコードとしても知られる DNS リソースレコードを DNS サーバからリクエストします。
4. 証明書と TLSA レコードは DNS サーバから取得され、DNSSEC によって保護されます。
5. 電子メールゲートウェイが、受信者のアドレスに対する STARTTLS SMTP セッションを確立します。
6. X.509 証明書が、受信者のアドレスの完全な TLSA レコードまたは TLSA レコードのハッシュ値に対して検証されます。検証に成功した後、メッセージは受信者のメール転送エージェント（MTA）に配信されます。証明書の検証が失敗すると、メッセージが後ほど配信されるか、メッセージがバウンスされます。
7. MTA が受信者の、メールボックスにメッセージを配信します。

TLSA レコードの作成

DNSSEC で署名した DNS レコード上で、希望する認証局（CA）の TLSA レコードを作成できます。以下は、完全修飾ドメイン名（FQDN）`www.example.com:` の TLSA レコードのサンプルです。

```
_443._tcp.www.example.com。IN TLSA (0 0 1
91751cee0a1ab8414400238a761411daa29643ab4b8243e9a91649e25be53ada)
```

上記の例 TLSA レコードには、暗号化は、次のフィールドがあります。

- **証明書の使用状況**：証明書のタイプを指定します。
  - サンプルでは、最初の「0」の桁は CA の証明書を指定しており、RFC 6698 に記述される PKIX 証明書パスと一致する必要があります。
  - 「1」の場合はエンド エンティティの証明書を指定しており、TLS のサーバによって提供されるエンド エンティティの証明書と一致する必要があります。
  - 「2」の場合は、TLS のサーバによって提供されるエンド エンティティの証明書を検証する際にトラスト アンカーとして使用する必要がある証明書を指定します。
  - 「3」の場合は、TLS のサーバによって提供されるエンド エンティティの証明書と一致する必要がある証明書を指定します。
- **セレクタ フィールド**：関連データと一致する TLS 証明書の部分を指定します。
  - サンプルでは、2つ目の「0」は、完全な証明書が一致する必要があることを指定しています。
  - 「1」の場合は、「SubjectPublicKeyInfo」フィールドのみが一致する必要があることを指定します。
- **一致タイプ**：使用されるハッシュ値のタイプを指定します。
  - サンプルでは、3 番目の「1」は選択したコンテンツの SHA-256 ハッシュを指定しています。
  - 「0」の場合は、選択したコンテンツの完全一致を指定します。
  - 「2」の場合は、選択したコンテンツの SHA-512 ハッシュを指定します。

DANE をサポートする配信に向けた TLS の有効化

始める前に

- エンベロープ送信者と TLSA リソース レコードが DNSSEC で検証されていることを確認します。

- 電子メールゲートウェイで DANE を設定するために TLS を有効にしていることを確認します。詳細については、配信時の TLS および証明書検証の有効化（840 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[送信先コントロール（Destination Controls）]ページに移動します。

ステップ 2 [送信先コントロールの追加（Add Destination Controls）]をクリックするか、既存のエントリを変更します。

ステップ 3 [TLSサポート（TLS Support）]フィールドから[推奨（Preferred）]、[必要（Required）]、[必須（Mandatory）]のいずれかを選択し、電子メールゲートウェイでDANEサポートを有効にします。

ステップ 4 [DANEサポート（DANE Support）]フィールドから、特定の TLS 接続に対する DANE に以下の設定を指定できます。

DANE 設定	説明
デフォルト	送信先コントロール ページを使用して設定するデフォルトの DANE 設定は、リスナーからドメインの MTA への送信 TLS 接続に使用されます。 [デフォルト（Default）] の DANE 設定は、送信先コントロールのデフォルト TLS 設定から継承されます。この設定は、カスタムの送信先コントロール エントリに上書きできます。
なし	インターフェイスからドメインの MTA への送信接続のネゴシエートに DANE を使用しない場合は、[なし（None）] を選択します。
状況対応型	[状況対応型（Opportunistic）]を選択し、リモートホストが DANE をサポートしていない場合、SMTP カンバセーションの暗号化に状況対応型の TLS が使用されます。 [状況対応型（Opportunistic）]を選択し、リモートホストがDANEをサポートしている場合、SMTPカンバセーションの暗号化の優先モードとなります。

DANE 設定	説明
必須	[必須（Mandatory）] を選択し、リモート ホストが DANE をサポートしていない場合、送信先ホストに対する接続が確立されません。 「[必須（Mandatory）] を選択し、リモート ホストが DANE をサポートしている場合、SMTP カンバセーションの暗号化の優先モードとなります。

ステップ 5 変更を [実行（Submit）] して [確定する（Commit）] します。

DANE 失敗時のアラートの送信

TLS 接続と DANE サポートが必要なドメインにメッセージを配信する際に、すべての MX ホストに対して DANE の検証が失敗した場合、電子メールゲートウェイがアラートを送信するかどうかを指定できます。電子メールゲートウェイは、システムアラートのタイプの警告重大度レベルアラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。

DANE アラートの有効化

手順

ステップ 1 [システム管理（System Administration）] > [アラート（Alerts）] ページに移動します。

ステップ 2 アラートを有効にするアラートの受信者を選択します。

ステップ 3 アラート タイプに対応する [メッセージ配信（Message Delivery）] チェック ボックスを選択します。

ステップ 4 変更を送信し、保存します。

認証局のリストの管理

電子メールゲートウェイは、保存済みの信頼できる認証局を使用してリモートドメインからの証明書を検証し、ドメインのクレデンシャルを確立します。次の信頼できる認証局を使用するように 電子メールゲートウェイを設定できます。

- **プレインストールされたリスト。** 電子メールゲートウェイには信頼できる認証局のリストがあらかじめインストールされています。これは、システム リストと呼ばれます。
- **ユーザ定義のリスト。** 信頼できる認証局のリストをカスタマイズし、 電子メールゲートウェイにリストをインポートできます。

システム リストまたはカスタマイズされたリストのいずれか、または両方のリストを使って、リモート ドメインからの証明書を検証できます。

GUI の [ネットワーク（Network）] > [証明書（Certificates）] > [認証局の編集（Edit Certificate Authorities）] ページまたは CLI の certconfig > certauthority コマンドを使用してリストします。

[ネットワーク（Network）] > [証明書（Certificates）] > [認証局の編集（Edit Certificate Authorities）] ページで、次のタスクを実行できます。

- **認証局のシステム リスト（インストール済み）を参照します。**詳細については、プレインストールされた認証局リストの参照 （849 ページ）を参照してください。
- **システム リストを使用するかどうかを選択します。**システム リストはイネーブルまたはディセーブルにできます。詳細については、システム認証局リストの無効化 （850ページ）を参照してください。
- **カスタム認証局リストを使用するかどうかを選択します。**カスタムリストを使用してテキストファイルからリストをインポートするように、電子メールゲートウェイをイネーブルにできます。詳細については、カスタム認証局リストのインポート （850ページ）を参照してください。
- **ファイルに、認証局のリストをエクスポートします。**テキスト ファイルに、認証局のシステム リストまたはカスタム リストをエクスポートできます。詳細については、認証局リストのエクスポート （850 ページ）を参照してください。

関連項目

- プレインストールされた認証局リストの参照 （849 ページ）
- システム認証局リストの無効化 （850 ページ）
- カスタム認証局リストのインポート （850 ページ）
- 認証局リストのエクスポート （850 ページ）
- 証明書の更新 （851 ページ）
- 信頼できるルート証明書の管理 （851 ページ）

プレインストールされた認証局リストの参照

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [システム認証局を表示（View System Certificate Authorities）] をクリックします。

システム認証局リストの無効化

事前にインストールされたシステム認証局リストは電子メールゲートウェイから削除できませんが、イネーブルまたはディセーブルにできます。リストをディセーブルにして、電子メールゲートウェイがリモートホストからの証明書を確認するためにカスタムリストのみを使用することを許可する場合があります。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [システム リスト（System List）] で [ディセーブル（Disable）] をクリックします。

ステップ 4 変更を送信し、保存します。

カスタム認証局リストのインポート

信頼できる認証局のカスタムリストを作成して、電子メールゲートウェイにインポートできます。ファイルは PEM 形式にして、 電子メールゲートウェイで信頼する認証局の証明書が含まれている必要があります。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [カスタム リスト（Custom List）] の [有効（Enable）] をクリックします。

ステップ 4 ローカル マシンまたはネットワーク マシンのカスタム リストへのフル パスを入力します。

ステップ 5 **[FQDN検証（FQDN Validation）]** チェックボックスをオンにすると、証明書に存在する [共通名（Common Name）] フィールド、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式であるかどうかを電子メールゲートウェイで確認できます。

ステップ 6 変更を送信し、保存します。

認証局リストのエクスポート

システム内の信頼できる認証局のサブセットのみを使用するか、既存のカスタム リストの編集を行う場合、リストを .txt ファイルにエクスポートして、認証局を追加または削除するように

編集できます。リストの編集が完了したら、ファイルをカスタムリストとして電子メールゲートウェイにインポートします。

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 [認証局（Certificate Authorities）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 [リストのエクスポート（Export List）] をクリックします。

[認証局リストのエクスポート（Export Certificate Authority List）] ページが表示されます。

ステップ 4 自分がエクスポートするリストを選択します。

ステップ 5 リストのファイル名を入力します。

ステップ 6 [エクスポート（Export）] をクリックします。

AsyncOS では、.txt ファイルとしてリストを開くか、または保存するかを確認するダイアログボックスが表示されます。

証明書の更新

[証明書リスト（Certificate Lists）] の下の [更新（Updates）] セクションには、電子メールゲートウェイ上のシスコの信頼できるルート証明書（システム CA 証明書）バンドルについて、バージョン情報および最終更新情報が表示されます。バンドルは定期的に更新されます。

[証明書（Certificates）] ページの [今すぐ更新（Update Now）] をクリックして、既存のシスコの信頼できるルート証明書（システム CA 証明書）バンドルを最新バージョンに更新します。

信頼できるルート証明書の管理

電子メールゲートウェイに次の証明書の数と詳細を表示できます。

- カスタムの信頼できるルート（カスタム CA）証明書
- シスコの信頼できるルート（システム CA）証明書

手順

ステップ 1 [ネットワーク（Network）] > [証明書（Certificates）] ページに移動します。

ステップ 2 カスタム CA 証明書またはシステム CA 証明書の詳細を表示するには、[証明書リスト（Certificate Lists）] セクションの下で [信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3 証明書の詳細を表示するには、[シスコの信頼できるルート証明書リスト（Cisco Trusted Root Certificate List）] セクションで必要な証明書リンク（[Admin-Root-CA] など）をクリックします。

ステップ 4 （オプション）証明書（[Admin-Root-CA] など）の詳細の下にある [証明書をダウンロード（Download Certificate）] リンクをクリックして、証明書をダウンロードします。

（注） また、[カスタムの信頼できるルート証明書リスト（Custom Trusted Root Certificates List）]セクションの下にある必要な証明書のリンクをクリックして、証明書の詳細を表示またはダウンロードすることもできます。

（注） 必要に応じて、カスタムの信頼できるルート（カスタム CA）証明書を削除することもできます。

HTTPS の証明書のイネーブル化

GUI の [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] ページまたは CLI の **interfaceconfig** コマンドのいずれかを使用して、IP インターフェイスで HTTPS サービスの証明書をイネーブルにできます。

手順

ステップ 1 [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページに移動します。

ステップ 2 HTTPS サービスを有効化するインターフェイスを選択します。

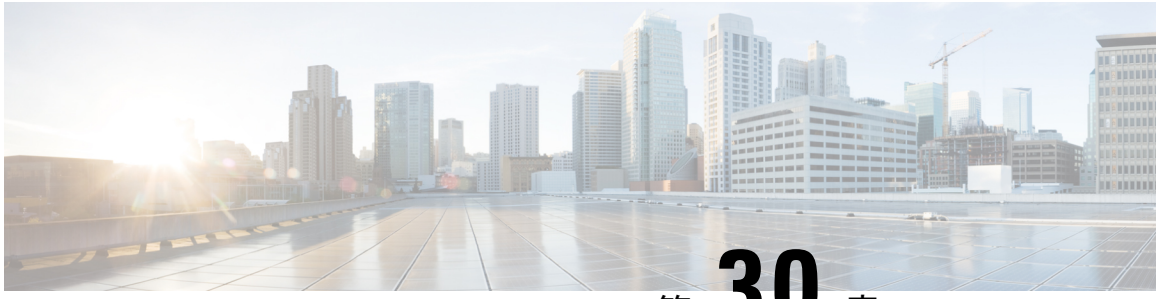
ステップ 3 [アプライアンス管理（Appliance Management）] で、[HTTPS] チェック ボックスをオンにし、ポート番号を入力します。

ステップ 4 変更を送信し、保存します。

次のタスク

（注） 電子メールゲートウェイにあらかじめインストールされているデモ証明書。テスト目的でデモ証明書で HTTPS サービスをイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。

GUI のシステム設定ウィザードを使用して HTTPS サービスをイネーブルにできます。詳細については、セットアップおよび設置 （19 ページ）を参照してください。



第 30 章

ルーティングおよび配信機能の設定

この章は、次の項で構成されています。

- ローカル ドメインの電子メールのルーティング （853 ページ）
- アドレスの書き換え （859 ページ）
- エイリアス テーブルの作成 （860 ページ）
- マスカレードの構成 （868 ページ）
- ドメイン マップ機能 （878 ページ）
- バウンスした電子メールの処理 （884 ページ）
- 宛先制御による電子メール配信の管理 （894 ページ）
- バウンス検証 （904 ページ）
- 電子メール配信パラメータの設定 （909 ページ）
- Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （912 ページ）
- グローバル配信停止機能の使用 （922 ページ）
- 確認：電子メール パイプライン （926 ページ）

ローカル ドメインの電子メールのルーティング

電子メールを受信するためのゲートウェイの設定 （81 ページ）では、エンタープライズ ゲートウェイ設定に対して SMTP 接続を提供するようにプライベート リスナーとパブリック リスナーをカスタマイズしました。これらのリスナーは、特定の接続を処理したり（HAT 変更経由）、特定ドメインのメールを受信したり（パブリック リスナーの RAT 変更経由）するようにカスタマイズされています。

電子メールゲートウェイでは、メールをローカルドメイン経由で、[ネットワーク（Network）] > [SMTPルート（SMTP Routes）] ページ（または `smtproutes` コマンド）を使用して指定されたホストにルーティングします。この機能は、sendmail の `mailertable` 機能に似ています。

（注） GUI でシステム セットアップ ウィザード（またはコマンドライン インターフェイスで systemsetup コマンド）を実行し（「セットアップとインストール」の章を参照）、変更内容を確定した場合、そのときに入力した RAT エントリごとに、電子メールゲートウェイで最初の SMTP ルートエントリが定義されています。

関連項目

- SMTP ルートの概要 （854 ページ）
- デフォルトの SMTP ルート （855 ページ）
- SMTP ルートの定義 （855 ページ）
- SMTP ルートの制限 （856 ページ）
- SMTP ルートと DNS （856 ページ）
- SMTP ルートおよびアラート （856 ページ）
- SMTP ルート、メール配信、およびメッセージ分裂 （856 ページ）
- SMTP ルートと発信 SMTP 認証 （857 ページ）
- GUI を使用した発信電子メール送信の SMTP ルート管理 （857 ページ）

SMTP ルートの概要

SMTP ルートを使用すると、特定ドメインのすべての電子メールを別の Mail eXchange（MX; メール交換）ホストへリダイレクトできます。たとえば、example.com から groupware.example.com へのマッピングを作成できます。このマッピングにより、エンベロープ受信者アドレスに @example.com が含まれる電子メールは、代わりに groupware.example.com に転送されます。システムは、通常の電子メール配信のように、groupware.example.com で「MX」ルックアップを実行し、次にホストで「A」ルックアップを実行します。この代替MX ホストは、DNS の MX レコードにリストされている必要はなく、電子メールがリダイレクトされているドメインのメンバである必要もありません。AsyncOS オペレーティングシステムでは、 電子メールゲートウェイで最大 4 万の SMTP ルートマッピングを設定できます。（SMTP ルートの制限 （856 ページ）を参照）。

この機能を使用すると、ホストを「ひとかたまりにする」ことができます。.example.com などの部分ドメインを指定すると、example.com で終わるすべてのドメインがエントリに一致します。たとえば、fred@foo.example.com と wilma@bar.example.com は、両方ともマッピングに一致します。

SMTP ルート テーブルにホストがない場合は、DNS を使用して MX ルックアップが実行されます。結果は、SMTP ルート テーブルに対して再チェックされません。foo.domain の DNS MX エントリが bar.domain の場合、foo.domain に送信されるすべての電子メールが bar.domain に配信されます。bar.domain から他のホストへのマッピングを作成した場合、foo.domain へ送信される電子メールは影響を受けません。

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがその後にある場合、メー

ルのループは作成されません。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

すべての電子メール配信で、SMTP ルートテーブルは、上から順に読み取られます。マッピングと一致する最も具体的なエントリが選択されます。たとえば、SMTP ルート テーブルで host1.example.com と .example.com の両方についてマッピングがある場合は、host1.example.com のエントリが使用されます。これは、具体的ではない .example.com エントリの後に出現した場合であっても、このエントリの方が具体的なエントリであるためです。そうでない場合は、エンベロープ受信者のドメインで通常の MX ルックアップが実行されます。

デフォルトの SMTP ルート

特殊キーワードの ALL を使用して、デフォルト SMTP ルートを定義することもできます。ドメインが SMTP ルート リストで前のマッピングと一致しない場合のデフォルトは、ALL エントリで指定された MX ホストにリダイレクトされます。

SMTP ルート エントリを印刷する場合、デフォルトの SMTP ルートは ALL: として一覧表示されます。デフォルトの SMTP ルートは削除できません。入力した値をクリアすることのみ可能です。

デフォルトの SMTP ルートを設定するには、[ネットワーク（Network）] > [SMTPルート（SMTP Routes）] ページまたは smtproutes コマンドを使用します。

SMTP ルートの定義

ルートを構築するには、[ネットワーク（Network）] > [SMTPルート（SMTP Routes）] ページ（または smtproutes コマンド）を使用します。新しいルートを作成するには、まず、永続的なルートを作成するドメインまたはドメインの一部を指定する必要があります。次に、宛先ホストを指定します。宛先ホストは、完全修飾ホスト名として入力することも、IP アドレスとして入力することもできます。IP アドレスは、インターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）を指定できます。

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

エントリと一致するメッセージをドロップするために、特殊な宛先ホスト /dev/null を指定することもできます（つまり、デフォルトルートに /dev/null を指定することで、 電子メール ゲートウェイで受信されたメールが配信されないようにすることができます）。

受信側のドメインに複数の宛先ホストを設定できます。MX レコードと同様に、それぞれの宛先ホストにはプライオリティ番号が割り当てられています。最低番号が割り当てられた宛先ホストは、受信側ドメインのプライマリ宛先ホストであることを示します。一覧にある他の宛先ホストは、バックアップとして使用されます。

プライオリティが同じ宛先は、「ラウンドロビン」方式で使用されます。ラウンドロビン処理は、SMTP 接続に基づいていて、必ずしもメッセージに基づくものではありません。また、1 つ以上の宛先ホストが応答しない場合は、到達可能ないずれかのホストにメッセージが配信されます。設定されているすべての宛先ホストが応答しない場合、メールは受信側ドメインのキューに入れられ、宛先ホストへの配信が後で試みられます。（MX レコードの使用へのフェールオーバーは行われません）。

CLI で `smtproutes` コマンドを使用してルートを構築するときは、ホスト名または IP アドレスに続けて `/pri=` とその後にプライオリティを割り当てるための整数 `0` ～ `65535`（`0` は最高のプライオリティ）を使用して、各宛先ホストにプライオリティを設定できます。たとえば、`host1.example.com/pri=0` のプライオリティは、`host2.example.com/pri=10` よりも高くなります。複数のエントリを指定する場合は、カンマで区切ります。

SMTP ルートの制限

ルートは、最大 40,000 個定義できます。ALL による最終的なデフォルト ルートは、この制限に含まれます。したがって、39,999 個までのカスタム ルートと、特別なキーワードである ALL を使用する 1 つのルートを定義できます。

SMTP ルートと DNS

特殊なキーワード USEDNS を使用して、MX ルックアップの実行により特定ドメインの次のホップを決定するよう電子メールゲートウェイに指示します。これは、サブドメイン宛のメールを特定ホストへルーティングする必要があるときに便利です。たとえば、example.com へのメールが企業の Exchange サーバに送信されるようにする場合、SMTP ルートは次のようになります。

example.com exchange.example.com

ただし、さまざまなサブドメイン（foo.example.com）宛のメールの場合は、次のような SMTP ルートを追加します。

.example.com USEDNS

SMTP ルートおよびアラート

[システム管理（System Administration）] > [アラート（Alerts）] ページ（または alertconfig コマンド）で指定されたアドレスに電子メールゲートウェイから送信されたアラートは、これらの宛先に対して定義された SMTP ルートに従います。

SMTP ルート、メール配信、およびメッセージ分裂

着信：1 つのメッセージに 10 人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を 1 つ開き、メール ストアには 10 の別々のメッセージではなく、メッセージを 1 つのみ配置します。

発信：動作は同様ですが、1 つのメッセージが 10 の異なるドメインの 10 人の受信者に送信される場合、AsyncOS では 10 の MTA に対する 10 の接続を開き、それぞれ 1 つの電子メールを配信します。

分裂：1 つの着信メッセージに 10 人の受信者がいて、全員が別々の着信ポリシー グループ（10 グループ）に属する場合、10 人の受信者全員が同じ Exchange サーバに属していても、メッセージは分裂されます。つまり、10 の別々の電子メールが 1 つの TCP 接続で配信されます。

SMTP ルートと発信 SMTP 認証

発信 SMTP 認証プロファイルを作成したら、SMTP ルートに適用できます。これによって、ネットワークエッジにあるメールリレーサーバの背後に電子メールゲートウェイが配置されている場合に、発信メールを認証できます。発信 SMTP 認証の詳細については、発信 SMTP 認証（987 ページ）を参照してください。

GUI を使用した発信電子メール送信の SMTP ルート管理

電子メールゲートウェイの SMTP ルートを管理するには、[ネットワーク（Network）]>[SMTP ルート（SMTP Routes）]ページを使用します。テーブルでマッピングの追加、変更、および削除ができます。SMTP ルートエントリをエクスポートまたはインポートすることができます。

関連項目

- SMTP ルートの追加 （857 ページ）
- SMTP ルートのエクスポート （858 ページ）
- SMTP ルートのインポート （858 ページ）

SMTP ルートの追加

手順

ステップ 1 [ネットワーク（Network）] > [SMTPルート（SMTP Routes）] ページの [ルートを追加（Add Route）] をクリックします。

ステップ 2 受信ドメインを入力します。ここには、ホスト名、ドメイン、IPv4 アドレス、または IPv6 アドレスを指定できます。

ステップ 3 宛先ホストを入力します。ここには、ホスト名、IPv4 アドレス、または IPv6 アドレスを指定できます。複数の宛先ホストを追加するには、[行の追加（Add Row）] をクリックし、新しい行に次の宛先ホストを入力します。

（注） ポート番号を指定するには、宛先ホストに「:<port number>」を追加します（例：example.com:25）。

ステップ 4 複数の宛先ホストを追加する場合は、0 ～ 65535 の整数を入力してホストのプライオリティを割り当てます。0 が最も高いプライオリティです。詳細については、SMTP ルートの定義 （855 ページ）を参照してください。

ステップ 5 変更を送信し、保存します。

SMTP ルートのエクスポート

Host Access Table（HAT）および Recipient Access Table（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをエクスポートするには、次の手順に従います。

手順

ステップ 1 [SMTPルート（SMTP Routes）] ページの **[SMTPルートをエクスポート（Export SMTP Routes）]** をクリックします。

ステップ 2 ファイルの名前を入力し、**[送信（Submit）]** をクリックします。

SMTP ルートのインポート

Host Access Table（HAT）および Recipient Access Table（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをインポートするには、次の手順に従います。

手順

ステップ 1 [SMTPルート（SMTP Routes）] ページの [SMTPルートをインポート（Import SMTP Routes）] をクリックします。

ステップ 2 エクスポートした SMTP ルートを含むファイルを選択します。

ステップ 3 **[送信（Submit）]** をクリックします。インポートによって既存の SMTP ルートがすべて置き換えられることが警告されます。テキスト ファイル内のすべての SMTP ルートがインポートされます。

ステップ 4 **[インポート（Import）]** をクリックします。

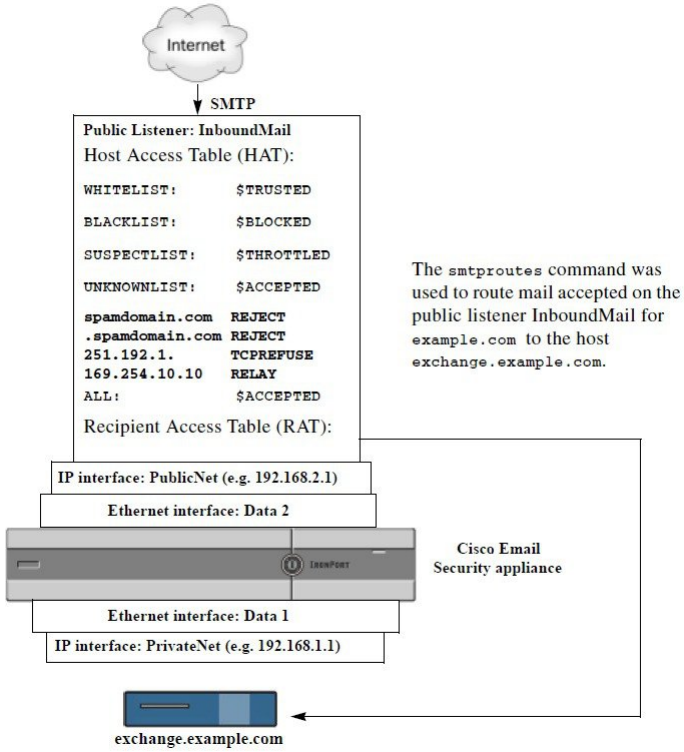
ファイル内に「コメント」を配置できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# this is a comment, but the next line is not

ALL:
```

次のタスク

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 *46* : パブリック リスナー用に定義された *SMTP* ルート



アドレスの書き換え

AsyncOS では、電子メール パイプラインでエンベロープ送信者および受信者のアドレスを書き換える方法が複数あります。アドレスの書き換えは、たとえばパートナードメインに送信されたメールをリダイレクトする場合や、社内インフラストラクチャを隠す（マスクする）場合に使用できます。

次の表に、送信者および受信者の電子メールアドレスを書き換えるために使用される各種機能の概要を示します。

表 *55* : アドレスの書き換え方法

元のアドレス	変更後	機能	作業対象
*@anydomain	user@domain	エイリアス テーブル（エイリアス テーブルの作成（860 ページ）を参照）	• エンベロープ受信者のみ • グローバルに適用 • エイリアスを電子メール アドレスまたは他のエイリアスにマッピング

元のアドレス	変更後	機能	作業対象
*@olddomain	*@newdomain	ドメイン マッピング（ドメイン マップ機能 （878 ページ）を参照）	• エンベロープ受信者のみ • リスナーごとに適用
*@olddomain	*@newdomain	マスカレード（マスカレードの構成 （868 ページ）を参照）	• エンベロープ送信者、および To:、From:、または CC: ヘッダー • リスナーごとに適用

エイリアス テーブルの作成

エイリアステーブルを使用すると、1 人または複数の受信者にメッセージをリダイレクトできます。エイリアスからユーザ名や他のエイリアスへのマッピング テーブルは、一部の UNIX システムで sendmail コンフィギュレーションの `/etc/mail/aliases` 機能と同様の方法で作成できます。

リスナーが受信した電子メールのエンベロープ受信者（Envelope To または `RCPT TO` とも呼ばれます）がエイリアステーブルで定義されているエイリアスと一致すると、電子メールのエンベロープ受信者アドレスが書き換えられます。

（注） RAT チェックの後からメッセージ フィルタの前までに、リスナーはエイリアス テーブルをチェックし、受信者を変更します。「電子メール パイプラインについて」の章を参照してください。

（注） エイリアス テーブル機能により、電子メールのエンベロープ受信者が実際に書き換えられます。これは、電子メールのエンベロープ受信者を書き換えず、電子メールを指定されたドメインに再ルーティングするだけの `smtproutes` コマンド（バウンスした電子メールの処理 （884 ページ）を参照）とは異なります。

関連項目

- コマンド ラインによるエイリアス テーブルの設定 （861 ページ）
- エイリアス テーブルのエクスポートおよびインポート （862 ページ）
- エイリアス テーブルのエントリの削除 （862 ページ）

コマンド ラインによるエイリアス テーブルの設定

エイリアス テーブルはセクションで定義します。各セクションの先頭にはドメイン コンテキスト（そのセクションに関連するドメインのリスト）があり、その後にマップのリストが続きます。

ドメイン コンテキストは、1つ以上のドメインまたは部分ドメインのリストです。カンマで区切り、角カッコ（「[」および「]」）で囲みます。ドメインは、文字、数字、ハイフン、およびピリオドで構成される文字列です（RFC 1035、セクション 2.3.1 の「優先される名前構文」を参照）。部分ドメイン（.example.com など）は、ピリオドで始まるドメインです。部分ドメインに一致するサブ文字列で終わるようなすべてのドメインは、一致であると見なされます。たとえば、ドメイン コンテキスト `.example.com` は、`mars.example.com` および `venus.example.com` と一致します。ドメイン コンテキストの後には、マップ（エイリアスと受信者リスト）のリストがあります。マップは、次のように構成されます。

表 *56* : エイリアス テーブルの構文

左辺（LHS）	区切り文字	右辺（RHS）
一致する1つ以上のエイリアスのリスト	コロン文字「:」	1つ以上の受信者アドレスまたはエイリアスのリスト

左辺のエイリアスでは、次の形式を使用できます。

`username`	一致するエイリアスを指定します。先行する「ドメイン」属性がテーブルで指定されている必要があります。このパラメータがないと、エラーになります。
`user@domain`	一致する正確な電子メール アドレスを指定します。

左辺 1 行あたり複数のエイリアスをカンマで区切って入力できます。

右辺の各受信者は、`user@domain` 形式の完全な電子メール アドレス、または別のエイリアスを指定できます。

エイリアス ファイルには、暗黙的なドメインのない「グローバルな」エイリアス（特定ドメインではなく、グローバルに適用されるエイリアス）、エイリアスに1つ以上の暗黙的なドメインのあるドメイン コンテキスト、またはその両方を指定できます。

エイリアスの「チェーン」（再帰的なエントリ）を作成することはできますが、完全な電子メール アドレスで終わる必要があります。

sendmail コンフィギュレーションのコンテキストと互換性を持たせるために、メッセージをドロップするための特殊な宛先である `/dev/null` がサポートされています。エイリアス テーブルによってメッセージが `/dev/null` にマッピングされると、廃棄済みカウンタが増分します（「CLI による管理およびモニタリング」の章を参照）。受信者は受け入れられますが、キューには入れられません。

関連項目

- エイリアス テーブルの例 （862 ページ）
- aliasconfig コマンドの例 （864 ページ）

エイリアス テーブルのエクスポートおよびインポート

エイリアステーブルをインポートするには、先にFTP、SSH、およびSCPアクセス （1573ページ）を確認し、電子メールゲートウェイにアクセスできるようにします。

既存のエイリアステーブルを保存するには、`aliasconfig`コマンドの`export`サブコマンドを使用します。ファイル（ファイル名は自分で指定）は、リスナーの`/configuration`ディレクトリに書き込まれます。このファイルをCLIの外部で変更し、インポートし直すことができます。（ファイルに不正な形式のエントリがある場合は、ファイルのインポート時にエラーが出力されます）。

エイリアステーブル ファイルを`/configuration`ディレクトリに配置し、`aliasconfig`コマンドの`import`サブコマンドを使用してファイルをアップロードします。

テーブルの行の先頭でナンバー記号（#）を使用すると、その行がコメントアウトされます。

コンフィギュレーションの変更が反映されるように、必ずエイリアス テーブル ファイルをインポートした後で`commit`コマンドを発行してください。

エイリアス テーブルのエントリの削除

コマンドラインインターフェイス（CLI）を使用してエイリアステーブルからエントリを削除する場合は、先にドメイン グループを選択するように求められます。「ALL (any domain)」エントリを選択すると、すべてのドメインに適用されるエイリアスの番号付きリストが表示されます。その後、削除するエイリアスの番号を選択します。

エイリアス テーブルの例

（注） このテーブル例のすべてのエントリは、コメントアウトされています。

```
# sample Alias Table file

# copyright (c) 2001-2005, IronPort Systems, Inc.

#

# Incoming Envelope To addresses are evaluated against each

# entry in this file from top to bottom. The first entry that

# matches will be used, and the Envelope To will be rewritten.

#

# Separate multiple entries with commas.
```

```
#
# Global aliases should appear before the first domain
# context. For example:
#
# admin@example.com: administrator@example.com
# postmaster@example.net: administrator@example.net
#
# This alias has no implied domain because it appears
# before a domain context:
#
# someaddr@somewhere.dom: specificperson@here.dom
#
# The following aliases apply to recipients @ironport.com and
# any subdomain within .example.com because the domain context
# is specified.
#
# Email to joe@ironport.com or joe@foo.example.com will
# be delivered to joseph@example.com.
#
# Similarly, email to fred@mx.example.com will be
# delivered to joseph@example.com
#
# [ironport.com, .example.com]
#
# joe, fred: joseph@example.com
#
# In this example, email to partygoers will be sent to
# three addresses:
#
# partygoers: wilma@example.com, fred@example.com, barney@example.com
#
# In this example, mail to help@example.com will be delivered to
```

```
# customercare@otherhost.dom. Note that mail to help@ironport.com will
# NOT be processed by the alias table because the domain context
# overrides the previous domain context.
#
# [example.com]
#
# help: customercare@otherhost.dom
#
# In this example, mail to nobody@example.com is dropped.
#
# nobody@example.com: /dev/null
#
# "Chains" may be created, but they must end in an email address.
# For example, email to "all" will be sent to 9 addresses:
#
# [example.com]
#
# all: sales, marketing, engineering
# sales: joe@example.com, fred@example.com, mary@example.com
# marketing:bob@example.com, advertising
# engineering:betty@example.com, miles@example.com, chris@example.com
# advertising:richard@example.com, karen@advertising.com
```

aliasconfig コマンドの例

この例では、aliasconfig コマンドを使用してエイリアス テーブルを作成します。まず、**example.com** のドメイン コンテキストを指定します。次に、**customercare** のエイリアスを作成し、customercare@example.com に送信されたすべての電子メールが bob@example.com、frank@example.com、および sally@example.com にリダイレクトされるようにします。さらに、**admin** のグローバル エイリアスを作成し、admin に送信された電子メールが administrator@example.com にリダイレクトされるようにします。最後に、確認用にエイリアス テーブルが出力されます。

テーブルの出力時に、admin のグローバル エイリアスは、example.com の最初のドメイン コンテキストの前に出力されます。

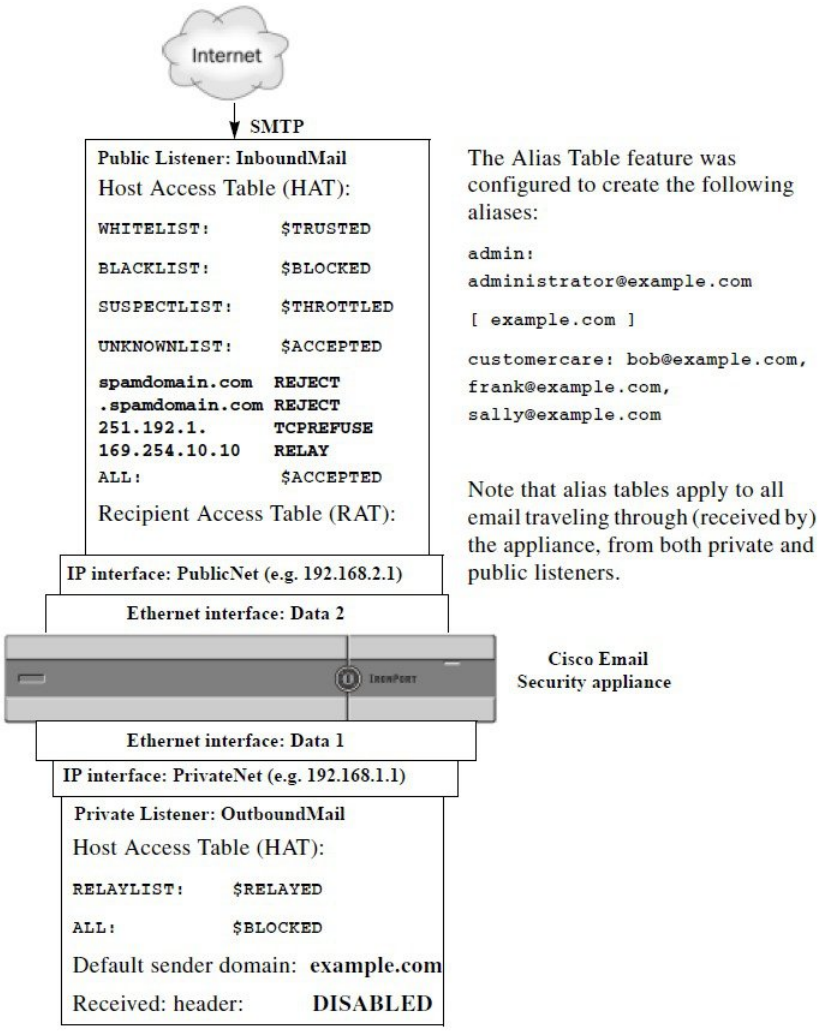
```
mail3.example.com> aliasconfig

No aliases in table.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import aliases from a file.

[]> new


How do you want your aliases to apply?

1. Globally

2. Add a new domain context


[1]> 2

Enter new domain context.

Separate multiple domains with commas.

Partial domains such as .example.com are allowed.

[]> example.com


Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

- "user" - This user in this domain context.

- "user@domain" - This email address.

[]> customercare


Enter address(es) for "customercare".

Separate multiple addresses with commas.

[]> bob@example.com, frank@example.com, sally@example.com


Adding alias customercare: bob@example.com,frank@example.com,sally@example.com

Do you want to add another alias? [N]> n

There are currently 1 mappings defined.

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.
```

```
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> new
How do you want your aliases to apply?
1. Globally
2. Add a new domain context
3. example.com
[1]> 1
Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
- "user@domain" - This email address.
- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.
[]> admin
Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com
Adding alias admin: administrator@example.com
Do you want to add another alias? [N]> n

There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
```

```
- CLEAR - Clear the table.
[]> print
admin: administrator@example.com
[ example.com ]
customercare: bob@example.com, frank@example.com, sally@example.com
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]>
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 *47 :* 電子メールゲートウェイに定義されたエイリアステーブル



マスカレードの構成

マスカレードは、作成したテーブルに従って、エンベロープ送信者（送信者またはMAIL FROMとも呼ばれます）、およびリスナーで処理される電子メールのTo:、From:、CC:ヘッダーを書き換える機能です。この機能の一般的な実装例の1つが「仮想ドメイン」であり、これによって複数のドメインを1つのサイトからホスティングできるようになります。他の一般的な実装としては、ネットワーク インフラストラクチャを「隠す」ために、電子メール ヘッダーの文字列からサブドメインを取り除く（「ストリッピング」）というものがあります。マスカレード機能は、プライベート リスナーとパブリック リスナーの両方で利用できます。

（注） マスカレード機能は、システム全体に対して設定するエイリアス テーブル機能とは異なり、リスナー単位で設定します。

リスナーは、LDAP受信者受け入れクエリーの直後でLDAPルーティング クエリーの前、メッセージがワーク キュー内にある間に、マスカレード テーブルで一致を探して受信者を変更します。「電子メール パイプラインについて」の章を参照してください。

マスカレード機能により、エンベロープ送信者および受信した電子メールの To:、From:、CC: フィールドのアドレスが実際に書き換えられます。作成するリスナーごとに別々のマスカレード パラメータを指定できます。2 つある方法のいずれかを使用します。

- 作成したマッピングのスタティック テーブルを使用
- LDAP クエリを使用。

この項では、スタティック テーブルを使用する方法について説明します。テーブルの形式は、一部の UNIX システムで sendmail コンフィギュレーションの /etc/mail/genericstable 機能と上位互換性があります。LDAPマスカレードクエリの詳細については、LDAP クエリ （943 ページ）を参照してください。

関連項目

- マスカレードと altsrchost （869 ページ）

マスカレードと altsrchost

一般に、マスカレード機能ではエンベロープ送信者が書き換えられ、メッセージで実行されるそれ以降のアクションは、マスカレードされたアドレスから「トリガー」されます。ただし、CLI から altscrchost コマンドを実行した場合、altscrchost マッピングは元のアドレスからトリガーされます（つまり変更後のマスカレードされたアドレスではない）。

詳細については、Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （912ページ）および確認：電子メール パイプライン （926ページ）を参照してください。

関連項目

- スタティック マスカレード テーブルの構成 （869 ページ）
- プライベート リスナー用マスカレード テーブルの例 （871 ページ）
- マスカレード テーブルのインポート （871 ページ）
- マスカレードの例 （871 ページ）

スタティック マスカレード テーブルの構成

マッピングのスタティック マスカレード テーブルを設定するには、listenerconfig コマンドの edit -> masquerade サブコマンドを使用します。また、マッピングが含まれるファイルをインポートできます。マスカレードテーブルのインポート （871ページ）を参照してください。こ

のサブコマンドにより、入力アドレス、ユーザ名、およびドメインを新しいアドレスおよびドメインにマッピングするテーブルを作成および維持します。LDAPマスカレードクエリの詳細については、LDAP クエリ （943 ページ）を参照してください。

メッセージがシステムに挿入されるときは、テーブルが参照され、ヘッダーに一致が見つかるとメッセージが書き換えられます。

ドメインのマスカレード テーブルは、次のように構成されます。

表 *57*：マスカレード テーブルの構文

左辺（LHS）	区切り文字	右辺（RHS）
一致する 1 つ以上のユーザ名やドメインのリスト	空白文字（スペースまたはタブ文字）	書き換え後のユーザ名やドメイン

次の表に、マスカレード テーブルで有効なエントリを示します。

左辺（LHS）	右辺（RHS）
username	username@domain
このエントリは、一致するユーザ名を指定します。左辺のユーザ名に一致する着信電子メール メッセージは、一致となり、右辺のアドレスで書き換えられます。右辺は、完全なアドレスである必要があります。	
user@domain	username@domain
このエントリは、一致する正確なアドレスを指定します。左辺の完全なアドレスに一致する着信メッセージは、右辺のアドレスで書き換えられます。右辺は、完全なアドレスである必要があります。	
@domain	@domain
このエントリは、特定のドメインの任意のアドレスを指定します。左辺の元のドメインは、右辺のドメインで置き換えられますが、ユーザ名は変更ありません。	
@.partialdomain	@domain
このエントリは、特定のドメインの任意のアドレスを指定します。左辺の元のドメインは、右辺のドメインで置き換えられますが、ユーザ名は変更ありません。	
ALL	@domain
ALL エントリは、そのままのアドレスに一致し、右辺のアドレスで書き換えます。右辺は、ドメインの先頭に「@」を付ける必要があります。このエントリは、テーブル内の位置に関係なく、常に優先度最低になります。 （注） ALL エントリは、プライベート リスナーのみに使用できます。	

- ルールは、マスカレード テーブルでの出現順序に従って一致します。

- デフォルトでは受信時にヘッダーのFrom:、To:、およびCC:フィールド内のアドレスが一致し、書き換えられます。エンベロープ送信者に一致して書き換えるようにオプションを設定することもできます。エンベロープ送信者および書き換え対象ヘッダーは、configサブコマンドを使用して有効と無効を切り替えます。
- テーブルの行の先頭でナンバー記号（#）を使用すると、その行がコメントアウトされます。#から行の末尾まで、すべてコメントであると見なされて無視されます。
- マスカレードテーブルは、newサブコマンドで作成したか、ファイルからインポートしたかによって、400,000エントリに制限されます。

プライベート リスナー用マスカレード テーブルの例

```
# sample Masquerading file

@.example.com @example.com # Hides local subdomains in the header

sales sales_team@success.com

@techsupport tech_support@biggie.com

user@localdomain user@company.com

ALL @bigsender.com
```

マスカレード テーブルのインポート

従来のsendmailの`/etc/mail/genericstable`ファイルをインポートできます。`genericstable`ファイルをインポートするには、先にFTP、SSH、およびSCPアクセス（1573ページ）を確認し、電子メールゲートウェイにアクセスできるようにします。

`genericstable`ファイルをconfigurationディレクトリに配置し、`masquerade`サブコマンドの`import`サブコマンドを使用してファイルをアップロードします。コマンドは、次の順序で使用します。

```
listenerconfig -> edit -> listener_number -> masquerade -> import
```

または、`export`サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル（ファイル名は自分で指定）は、configurationディレクトリに書き込まれます。このファイルをCLIの外部で変更し、インポートし直すことができます。

`import`サブコマンドを使用するときは、ファイルに有効なエントリのみが含まれているようにしてください。無効なエントリ（左辺があって右辺がない場合など）があると、ファイルのインポート時にCLIで構文エラーが発生します。インポート中に構文エラーが発生すると、ファイル全体でマッピングがインポートされません。

リスナーのコンフィギュレーションの変更内容が反映されるように、`genericstable`ファイルをインポートした後で必ず`commit`コマンドを発行してください。

マスカレードの例

この例では、`listenerconfig`の`masquerade`サブコマンドを使用して、PrivateNetインターフェイス上にある「OutboundMail」という名前のプライベートリスナー用に、ドメインマスカレード テーブルを作成します。

まず、マスカレードにLDAPを使用するオプションを宣言します。（LDAPマスカレードクエリの詳細については、LDAP クエリ （943 ページ）を参照してください）。

次に、**@.example.com** の部分ドメイン表記が **@example.com** にマッピングされます。これにより、サブドメイン .example.com 内にある任意のマシンから送信されるすべての電子メールが example.com にマッピングされます。さらに、ユーザ名 **joe** がドメイン **joe@example.com** にマッピングされます。両方のエントリを確認するためにドメイン マスカレード テーブルが出力されて、masquerade.txt という名前のファイルにエクスポートされます。config サブコマンドを使用して、CC: フィールドのアドレスの書き換えが無効になり、最後に変更が確定されます。

```
mail3.example.com> listenerconfig

Currently configured listeners:

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

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

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.

[]> 2

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.
```

```
- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or

recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]> masquerade

Do you want to use LDAP for masquerading? [N]> n

Domain Masquerading Table

There are currently 0 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.
```

```
Hosts like @training and @.sales are allowed.
[]> @.example.com
Enter the masqueraded address or domain.
Domains like @example.com are allowed.
Full addresses such as user@example.com are allowed.
[]> @example.com
Entry mapping @.example.com to @example.com created.
Domain Masquerading Table
There are currently 1 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> new

Enter the source address or domain to masquerade.
Usernames like "joe" are allowed.
Full addresses like "user@example.com" are allowed.
Full addresses with subdomain wildcards such as "username@.company.com" are allowed.
Domains like @example.com and @.example.com are allowed.
Hosts like @training and @.sales are allowed.
[]> joe
Enter the masqueraded address.
Only full addresses such as user@example.com are allowed.
[]> joe@example.com
Entry mapping joe to joe@example.com created.
Domain Masquerading Table
```

```
There are currently 2 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> print
@.example.com @example.com

joe joe@example.com
Domain Masquerading Table
There are currently 2 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> export
Enter a name for the exported file:
[]> masquerade.txt
Export completed.
Domain Masquerading Table
There are currently 2 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
```

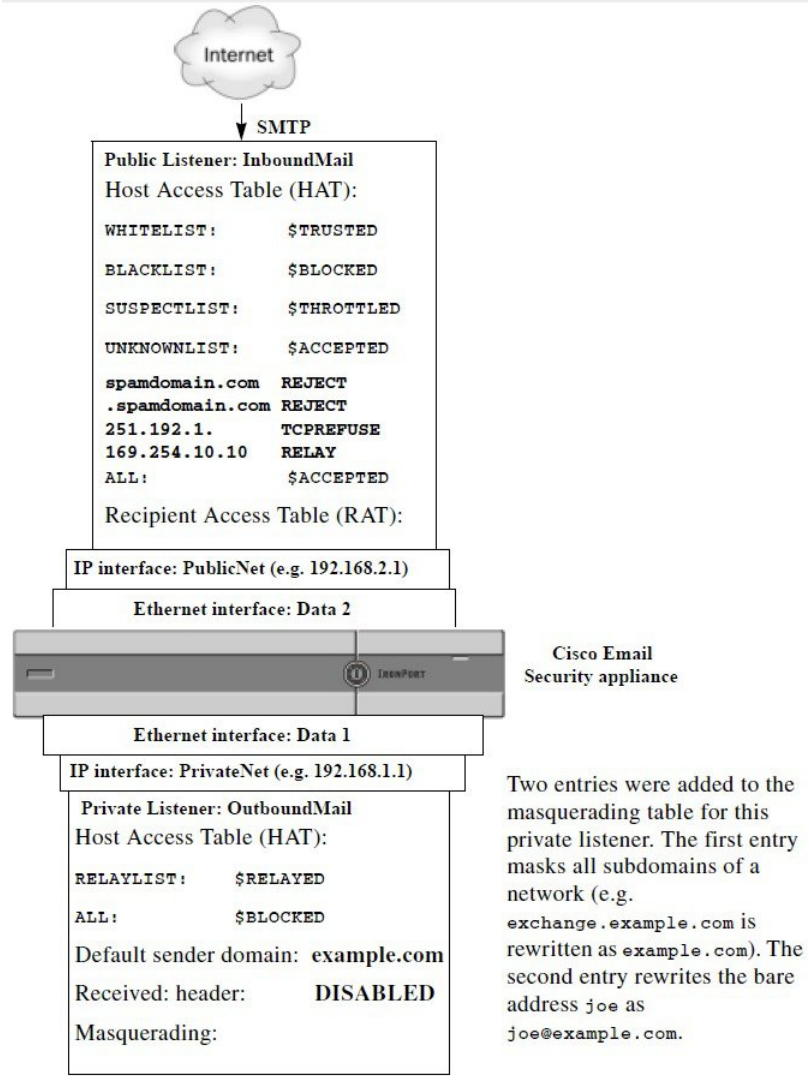
```
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.

[]> config
Do you wish to masquerade Envelope Sender?
[N]> y
Do you wish to masquerade From headers?
[Y]> y
Do you wish to masquerade To headers?
[Y]> y
Do you wish to masquerade CC headers?
[Y]> n
Do you wish to masquerade Reply-To headers?
[Y]> n
Domain Masquerading Table
There are currently 2 entries.
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]>
Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
```

```
Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or
recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.


[]>

Currently configured listeners:

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

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

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.
```

```
- SETUP - Change global settings.

[]>
```

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 *48 :* プライベート リスナー用に定義されたマスカレード



ドメイン マップ機能

リスナー用に「ドメイン マップ」を設定できます。設定するリスナーごとにドメイン マップ テーブルを作成できます。ドメイン マップ テーブルに含まれているドメインと一致するメッセージでは、各受信者のエンベロープ受信者が書き換えられます。この機能は、sendmail の

「ドメイン テーブル」機能または Postfix の「仮想テーブル」機能に似ています。この機能では、エンベロープ受信者のみが影響を受け、「To:」ヘッダーは書き換えられません。

（注） ドメイン マップ機能の処理は、RAT の直前でデフォルト ドメインの評価直後に発生します。「電子メール パイプラインについて」の章を参照してください。

ドメイン マップ機能でよくある実装では、複数のレガシー ドメインの着信メールを受け入れます。たとえば、会社が他の会社を買収した場合に、電子メールゲートウェイにドメインマップを作成して買収したドメインのメッセージを受け入れ、エンベロープ受信者を会社の現在のドメインに書き換えることができます。

（注） 最大 20,000 の別個の固有ドメイン マッピングを設定できます。

表 *58*：ドメイン マップ テーブルの構文の例

左側	右側	説明
`username@example.com`	**username2@example.net**	右側は完全なアドレスのみ
`user@.example.com`	**user2@example.net**	
`@example.com`	**user@example.net** または **@example.net**	完全なアドレス、または完全修飾ドメイン名。
`@.example.com`	**user@example.net** または **@example.net**	

次の例では、`listenerconfig` コマンドの `domainmap` サブコマンドを使用して、パブリック リスナー「InboundMail」用のドメイン マップを作成します。`oldcompanyname.com` ドメインおよびそのサブドメイン宛のメールは、`example.com` ドメインにマッピングされます。マッピングは、確認のために出力されます。この例は、両方のドメインをリスナーの RAT に配置するコンフィギュレーションとは異なります。ドメイン マップ機能により、実際にエンベロープ受信者 `joe@oldcomapanyname.com` が `joe@example.com` に書き換えられます。一方、リスナーの RAT 内にドメイン `oldcompanyname.com` を置くと、`joe@oldcompanyname.com` のメールが受け入れられて、エンベロープ受信者を書き換えずにルーティングされます。また、エイリアステーブル機能とも異なります。エイリアス テーブルでは、明示的なアドレスに解決されることが必要です。「任意のユーザ名`@domain`」を「同じユーザ名`@newdomain`」にマップするように構築することはできません。

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

```
Currently configured listeners:

1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

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

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.

[]> 1

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.
```

```
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> domainmap
Domain Map Table
There are currently 0 Domain Mappings.
Domain Mapping is: disabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import domain mappings from a file.
[]> new

Enter the original domain for this entry.
Domains such as "@example.com" are allowed.
Partial hostnames such as "@.example.com" are allowed.
Email addresses such as "test@example.com" and "test@.example.com"
are also allowed.
[]> @.oldcompanyname.com
Enter the new domain for this entry.
The new domain may be a fully qualified
such as "@example.domain.com" or a complete
email address such as "test@example.com"
[]> @example.com
Domain Map Table
There are currently 1 Domain Mappings.
Domain Mapping is: enabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
- IMPORT - Import domain mappings from a file.
- EXPORT - Export domain mappings to a file.
```

```
- CLEAR - Clear all domain mappings.

[]> print

@.oldcompanyname.com --> @example.com

Domain Map Table

There are currently 1 Domain Mappings.

Domain Mapping is: enabled

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display all domain mappings.

- IMPORT - Import domain mappings from a file.

- EXPORT - Export domain mappings to a file.

- CLEAR - Clear all domain mappings.

[]>

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Enabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.
```

```
- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]>
```

関連項目

- ドメイン マップ テーブルのインポートおよびエクスポート （883 ページ）

ドメイン マップ テーブルのインポートおよびエクスポート

ドメインマップテーブルをインポートまたはエクスポートするには、先に FTP、SSH、および SCP アクセス（1573 ページ） を確認し、電子メールゲートウェイにアクセスできるようにします。

マッピングするドメインのエントリが含まれるテキストファイルを作成します。エントリは空白文字（タブ文字またはスペース）で区切ります。テーブルの行の先頭でナンバー記号（#）を使用すると、その行がコメントアウトされます。

ファイルを configuration ディレクトリに配置し、domain サブコマンドの `import` サブコマンドを使用してファイルをアップロードします。コマンドは、次の順序で使用します。

```
listenerconfig ->  edit ->  inejctor_number -> domainmap -> import
```

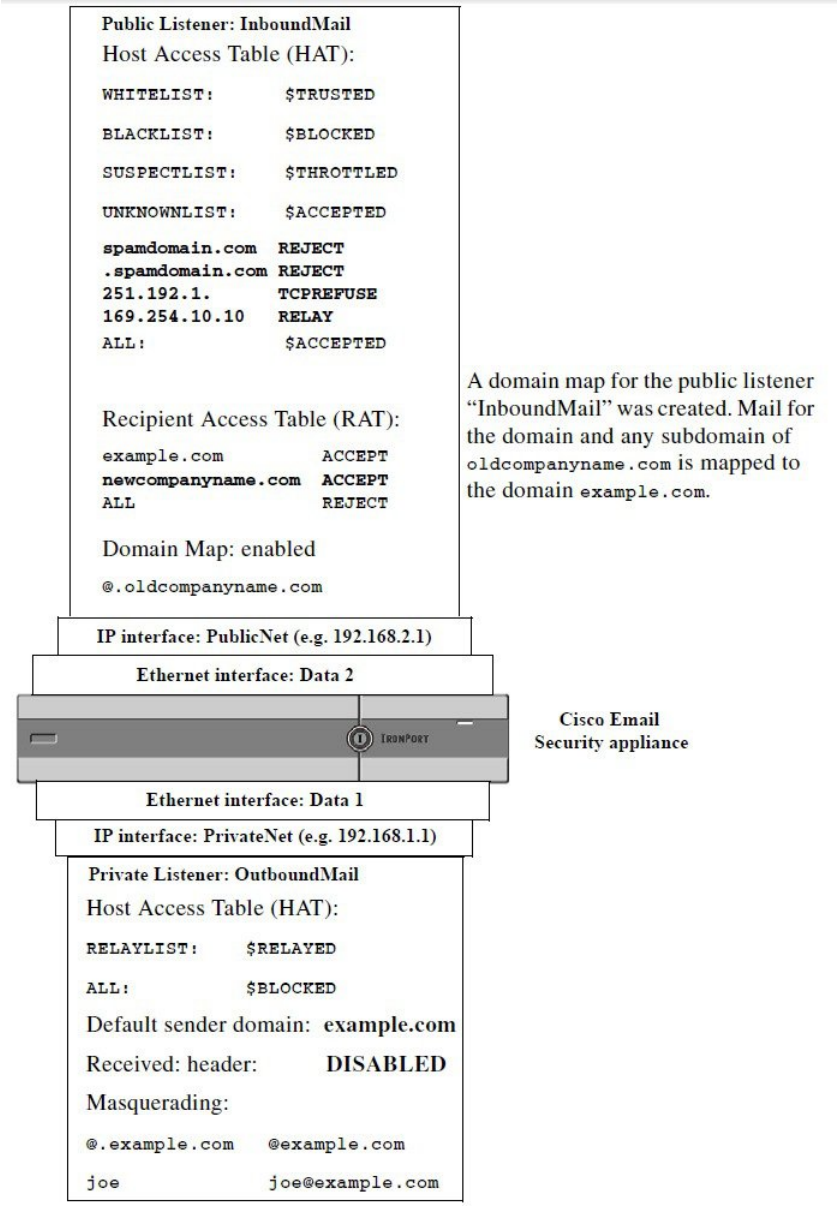
または、`export` サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル（ファイル名は自分で指定）は、configuration ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。

`import` サブコマンドを使用するときは、ファイルに有効なエントリのみが含まれているようにしてください。無効なエントリ（左辺があって右辺がない場合など）があると、ファイルのインポート時に CLI で構文エラーが発生します。インポート中に構文エラーが発生すると、ファイル全体でマッピングがインポートされません。

リスナーのコンフィギュレーションの変更が反映されるように、ドメインマップテーブルファイルをインポートした後で `commit` コマンドを発行してください。

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 *49 :* パブリック リスナー用に定義されたドメイン マップ



バウンスした電子メールの処理

バウンスした電子メールは、あらゆる電子メール配信においてやむを得ないものです。電子メールゲートウェイでは、詳細に設定できるさまざまな方法で、バウンスした電子メールを処理できます。

この項では、電子メールゲートウェイで着信メールに基づいて発信バウンスを生成する方法の制御について説明していることに注意してください。電子メールゲートウェイが発信メールに

基づいて着信バウンスを制御する方法について管理するには、バウンス検証を使用します（バウンス検証 （895 ページ）を参照）。

関連項目

- 配信不可能な電子メールの処理 （885 ページ）
- 新しいバウンス プロファイルの作成 （893 ページ）
- リスナーへのバウンス プロファイルの適用 （893 ページ）

配信不可能な電子メールの処理

AsyncOS オペレーティング システムでは、配信不可能な電子メール（「バウンスしたメッセージ」）は、次のカテゴリに分類されます。

「カンバセーション」バウンス： **最初の SMTP カンバセーションで、リモート ドメインがメッセージをバウンスします。**	
ソフト バウンス	一時的に配信不可能なメッセージ。たとえば、ユーザのメールボックスがいっぱいです。これらのメッセージは、後で再試行できます。（例：SMTP 4XX エラー コード。）
ハード バウンス	永続的に配信できないメッセージ。たとえば、そのユーザはそのドメインにはもう存在しません。これらのメッセージは、再試行されません。（例：SMTP 5XX エラー コード。）
「遅延」（または「カンバセーションでない」）バウンス: **リモート ドメインは、メッセージを配信するために受け入れて、後でのみバウンスします。**	
ソフト バウンス	一時的に配信不可能なメッセージ。たとえば、ユーザのメールボックスがいっぱいです。これらのメッセージは、後で再試行できます。（例：SMTP 4XX エラー コード。）
ハード バウンス	永続的に配信できないメッセージ。たとえば、そのユーザはそのドメインにはもう存在しません。これらのメッセージは、再試行されません。（例：SMTP 5XX エラー コード。）

GUI の [ネットワーク（Network）] メニューの [バウンスプロファイル（Bounce Profiles）] ページ（または `bounceconfig` コマンド）を使用して、作成するリスナーごとにハードおよびソフトのカンバセーション バウンスの AsyncOS の処理方法を設定します。バウンス プロファイルを作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページ（または `listenerconfig` コマンド）を使用して、プロファイルを各リスナーに適用します。メッセージ フィルタを使用して、特定のメッセージにバウンス プロファイルを割り当てることもできます。（詳細については、メッセージ フィルタを使用した電子メール ポリシーの適用 （155 ページ）を参照してください。）

関連項目

- ソフト バウンスおよびハード バウンスに関する注意 （886 ページ）
- バウンス プロファイルのパラメータ （886 ページ）
- ハード バウンスと status コマンド （890 ページ）
- カンバセーション バウンスおよび SMTP ルートのメッセージ フィルタ アクション （891 ページ）
- バウンス プロファイルの例 （891 ページ）
- 配信ステータス通知形式 （892 ページ）
- 遅延警告メッセージ （892 ページ）
- 遅延警告メッセージとハード バウンス （892 ページ）

ソフト バウンスおよびハード バウンスに関する注意

- カンバセーション ソフト バウンスの場合、ソフト バウンス イベントは、受信者への配信が一時的に失敗するたびに定義されます。単一の受信者が複数のソフト バウンス イベントを繰り返し発生させることがあります。[バウンスプロファイル（Bounce Profiles）]ページまたは bounceconfig コマンドを使用して、各ソフト バウンス イベントのパラメータを設定します。（バウンス プロファイルのパラメータ （886 ページ） を参照。）
- デフォルトでは、ハード バウンスした受信者ごとにバウンス メッセージが生成され、元の送信者に送信されます。（メッセージは、メッセージエンベロープのエンベロープ送信者アドレスで定義されたアドレスに送信されます。Envelope From も通常エンベロープ送信者を意味します）。この機能をディセーブルにし、代わりにハードバウンスに関する情報をログ ファイルに頼ることもできます。（「ロギング」の章を参照。）
- キュー内での最大時間または再試行の最大回数のどちらかに達すると、ソフトバウンスはハード バウンスになります。

バウンス プロファイルのパラメータ

バウンスプロファイルを設定するときは、次のパラメータを使用して、メッセージごとにカンバセーション バウンスを処理する方法を制御します。

表 *59*：バウンス プロファイルのパラメータ

最大再試行回数（Maximum number of retries）	ソフトバウンスしたメッセージを配信し直すために、ハードバウンス メッセージとして扱われるようになる前に、受信者のホストに再接続が試みられる回数。デフォルトの再試行回数は 100 です。
キューの最大時間（秒）（Maximum number of seconds in queue）	ソフト バウンスしたメッセージを配信し直すために、ハード バウンスしたメッセージとして扱われるようになる前に、受信者のホストに再接続が試みられるのに費やされる時間。デフォルトは 259,200 秒（72 時間）です。

メッセージを再試行するまでの初回待機時間（秒）（**Initial number of seconds to wait before retrying a message**）	ソフト バウンスしたメッセージを最初に配信し直すまでの待機時間。デフォルトは 60 秒です。初回再試行時間を大きい値に設定すると、ソフト バウンスの試行頻度が低下します。逆に頻度を上げるには、小さい値にします。
メッセージを再試行するまでの最大待機時間（秒）（**Maximum number of seconds to wait before retrying a message**）	ソフトバウンスしたメッセージを配信し直すまでに待機する最大時間。デフォルトは 3,600 秒（1 時間）です。これは、次の試行までの間隔ではなく、再試行回数を制御するために使用できるもう 1 つのパラメータです。初回再試行間隔の上限は、最大再試行間隔に制限されます。計算された再試行間隔が最大再試行間隔を超える場合は、最大再試行間隔が使用されます。

ハード バウンス メッセージの送信（Send Hard Bounce Messages）	ハード バウンスに対してバウンス メッセージを送信するかどうかを指定します。このオプションが有効な場合は、バウンス メッセージの形式を選択できます。デフォルトでは、バウンス メッセージで DSN 形式（RFC 1894）が使用されます。 元のメッセージ（件名と本文）の言語に基づいてカスタマイズされたバウンス メッセージを送信することもできます。たとえば、中国語のメッセージには中国語でバウンス メッセージを送信し、他の言語のすべてのメッセージには英語のバウンス メッセージを送信することができます。 [通知テンプレート（Notification Template）] の下で [行の追加（Add Row）] をクリックして、メッセージの言語と使用するテンプレートを選択します。 （注） デフォルトのエントリが削除されていないことを確認します（[メッセージの言語（Message Language）] を [デフォルト（Default）] に設定）。デフォルト エントリのバウンス通知テンプレートは変更できます。 メッセージの言語は、次のシナリオではデフォルトと見なされます。 • メッセージの言語が、他の通知テンプレート エントリで選択した言語と異なる場合。 • メッセージの言語が、電子メール ゲートウェイでサポートされていない場合。 • 電子メール ゲートウェイがメッセージの言語を検出できない場合。 • メッセージの内容（件名と本文）が 50 バイト未満である場合。 前述の例（中国語のメッセージには中国語のバウンス メッセージを送信し、他の言語のすべてのメッセージには英語のバウンス メッセージを送信する）を設定する場合、通知テンプレートのテーブルは次のようになります。 バウンス応答から DSN の status フィールドを解析するかどうかを選択することもできます。「はい」の場合、電子メール ゲートウェイは DSN ステータス コード（RFC 3436）を検索し、そのコードを配信ステータス通知の Status フィールドで使用します。

遅延警告メッセージの送信（Send Delay Warning Messages）	配信遅延に対して警告メッセージを送信するかどうかを指定します。このオプションが有効な場合は、元のメッセージ（件名と本文）の言語に基づいてカスタムの遅延警告メッセージを構成できます。たとえば、中国語のメッセージには中国語で遅延警告メッセージを送信し、他の言語のすべてのメッセージには英語の遅延警告メッセージを送信することができます。 [通知テンプレート（Notification Template）] の下で [行の追加（Add Row）] をクリックして、メッセージの言語と使用するテンプレートを選択します。 （注） デフォルトのエントリが削除されていないことを確認します（[メッセージの言語（Message Language）] を [デフォルト（Default）] に設定）。デフォルトエントリのバウンス通知テンプレートは変更できます。 メッセージの言語は、次のシナリオではデフォルトと見なされます。 • メッセージの言語が、他の通知テンプレートエントリで選択した言語と異なる場合。 • メッセージの言語が、電子メールゲートウェイでサポートされていない場合。 • 電子メールゲートウェイがメッセージの言語を検出できない場合。 • メッセージの内容（件名と本文）が 50 バイト未満である場合。 前述の例（中国語のメッセージには中国語の遅延警告メッセージを送信し、他の言語のすべてのメッセージには英語の遅延警告メッセージを送信する）を設定する場合、通知テンプレートのテーブルは次のようになります。 メッセージ間の最小間隔、および送信する最大再試行回数を指定することもできます。
バウンス先の受信者の指定（Specify Recipient for Bounces）	メッセージのバウンス先としてデフォルトのエンベロープ送信者アドレスではなく、別のアドレスにすることができます。

バウンスおよび遅延メッセージへの DomainKeys 署名の使用（Use DomainKeys signing for bounce and delay messages）	バウンス メッセージおよび遅延メッセージの署名に使用する DomainKeys プロファイルを選択できます。DomainKeys の詳細については、DomainKeys と DKIM 認証 （742 ページ）を参照してください。
グローバル設定（Global Settings）	
これらの設定を行うには、[バウンスプロファイル（Bounce Profiles）] ページの [グローバル設定を編集（Edit Global Settings）] リンクを使用するか、または CLI で `bounceconfig` コマンドを使用してデフォルトのバウンス プロファイルを編集します。	
到達不能ホストをリトライするまでの最初の待機時間（秒）（Initial number of seconds to wait before retrying an unreachable host）	システムが到達不可能なホストへの再試行を 待機する時間。デフォルトは 60 秒です。
到達不能ホストの最大許容再試行間隔（Max interval allowed between retries to an unreachable host）	システムが到達不可能なホストへの再試行を待機する最大時間。デフォルトは 3,600 秒（1 時間）です。ホストがダウンしているために配信が最初に失敗すると、再試行値の最小秒数で開始し、ダウンしたホストに対するその後の再試行では、間隔を徐々に延ばしていきます。最大で、この最大秒数になります。

ハード バウンスと status コマンド

ハードバウンスメッセージの生成がイネーブルの場合、電子メールゲートウェイで配信用のハードバウンスメッセージが生成されるたびに、status および status detail コマンドの次のカウンタが増えていきます。

Counters:	Reset	Uptime	Lifetime
Receiving			
Messages Received	0	0	0

Recipients Received	0	0	0
Gen. Bounce Recipients	0	0	0

詳細については、「CLIによる管理およびモニタリング」の章を参照してください。ハードバウンス メッセージの生成がディセーブルの場合、受信者でハード バウンスが発生しても、これらのカウンタはどれも増えません。

（注） メッセージ エンベロープのエンベロープ送信者アドレスは、メッセージ ヘッダーの「From:」とは異なります。AsyncOS では、ハード バウンス メッセージをエンベロープ送信者アドレスとは異なる電子メール アドレスに送信するように設定できます。

カンバセーション バウンスおよび SMTP ルートのメッセージ フィルタ アクション

SMTP ルートマッピングおよびメッセージ フィルタ アクションは、カンバセーションバウンスの結果として電子メールゲートウェイで生成されたSMTPバウンスメッセージのルーティングには適用されません。電子メールゲートウェイでカンバセーション バウンス メッセージが受信されると、元のメッセージのエンベロープ送信者に返送するSMTPバウンスメッセージが生成されます。この場合、電子メールゲートウェイでは実際にメッセージが生成されるため、リレー用に挿入されたメッセージに適用されるすべての SMTP ルートは適用されません。

バウンス プロファイルの例

これら 2 つの例では、異なるバウンス プロファイル パラメータが使用されます。

表 *60* : 例 *1* : バウンス プロファイル パラメータ

パラメータ	値
最大再試行回数（Max number of retries）	2
キューの最大時間（秒）（Maximum number of seconds in queue）	259,200 秒（72 時間）
再試行するまでの初回最大時間（秒）（Initial number of seconds before retrying）	60 秒
再試行するまでの最大待機時間（秒）（Max number of seconds to wait before retrying）	60 秒

例 1 では、受信者への最初の配信は、t = 0 で実行されます。これは、メッセージが電子メールゲートウェイに挿入された直後です。デフォルトの初回再試行時間は 60 秒であるため、最初の再試行は約 1 分後の t = 60 で実行されます。再試行間隔が計算されます。再試行間隔は、最大再試行間隔である 60 秒を使用して決定されます。そのため、2 回めの再試行は、t = 約 120 で実行されます。最大再試行回数は2であるため、この再試行の直後にその受信者のハードバウンス メッセージが生成されます。

表 *61 : 例 2* : バウンス プロファイル パラメータ

パラメータ	値
最大再試行回数（Max number of retries）	100
キューの最大時間（秒）（Maximum number of seconds in queue）	100 秒
再試行するまでの初回最大時間（秒）（Initial number of seconds before retrying）	60 秒
再試行するまでの最大待機時間（秒）（Max number of seconds to wait before retrying）	120 秒

例 2 では、最初の配信は t = 0、最初の再試行は t = 60 で実行されます。2 回目の配信（t = 120 で発生するようにスケジュール）の直前にメッセージがハードバウンスされます。なぜなら、この時点でキュー内での最大時間である 100 秒を超過しているためです。

配信ステータス通知形式

システムによって生成されるバウンス メッセージは、デフォルトではハードとソフトの両方のバウンスで Delivery Status Notification（DSN; 配信ステータス通知）形式を使用します。DSN は、RFC 1894（http://www.faqs.org/rfcs/rfc1894.html を参照）で規定されている形式であり、「メッセージを 1 人以上の受信者に配信したときの結果をレポートするために、Message Transfer Agent（MTA; メッセージ転送エージェント）または電子的なメール ゲートウェイで使用できる MIME コンテンツ タイプを定義」します。デフォルトでは、配信ステータス通知には配信ステータスの説明、およびメッセージのサイズが 10 k よりも小さい場合は元のメッセージが含まれます。メッセージ サイズが 10 k よりも大きい場合、配信ステータス通知には、メッセージ ヘッダーのみが含まれます。メッセージ ヘッダーが 10 k を超える場合は、配信ステータス通知ではヘッダーが切り捨てられます。DSN に 10 k よりも大きいメッセージ（またはメッセージ ヘッダー）を含める場合は、bounceconfig コマンドの max_bounce_copy パラメータを使用できます（このパラメータは CLI からのみ利用できます）。

遅延警告メッセージ

システムで生成される [遅延通知メッセージ（Time in Queue Message）] でも、DSN 形式が使用されます。デフォルト パラメータを変更するには、[ネットワーク（Network）] メニューの [バウンスプロファイル（Bounce Profiles）] ページ（または bounceconfig コマンド）を使用して、既存のバウンス プロファイルを編集するか新規に作成し、以下のパラメータのデフォルト値を変更します。

- 遅延警告メッセージが送信される最小間隔。（The minimum interval between sending delay warning messages.）
- 遅延警告メッセージが送信される受信者あたりの最大数。（The maximum number of delay warning messages to send per recipient.）

遅延警告メッセージとハード バウンス

[キューでの最大保持時間（Maximum Time in Queue）] 設定と [遅延警告メッセージの送信（Send Delay Warning Messages）] の最小間隔設定の両方を非常に小さい時間に設定した場合は、同じ

メッセージに対して遅延警告とハードバウンスの両方を同時に受信することが可能です。シスコでは、遅延警告メッセージの送信をイネーブルにする場合は、これらの設定のデフォルト値を最小設定として使用することを推奨します。

さらに、電子メールゲートウェイによって生成される遅延警告メッセージおよびバウンスメッセージは、処理中に最大で 15 分遅延することがあります。

新しいバウンス プロファイルの作成

次の例では、[バウンスプロファイル（Bounce Profiles）] ページを使用して、bouncepr1 という名前のバウンス プロファイルが作成されます。このプロファイルでは、ハード バウンスされたすべてのメッセージが代替アドレスである bounce-mailbox@example.com に送信されます。遅延警告メッセージはイネーブルです。受信者あたり警告メッセージが 1 つ送信されます。警告メッセージ間のデフォルト値は 4 時間（14400 秒）です。

関連項目

- デフォルトのバウンス プロファイルの編集 （893 ページ）
- minimalist バウンス プロファイルの例 （893 ページ）

デフォルトのバウンス プロファイルの編集

バウンス プロファイルを編集するには、バウンス プロファイルのリストで名前をクリックします。デフォルトのバウンスプロファイルを編集することもできます。この例では、デフォルトプロファイルを編集して、`maximum number of seconds to wait before retrying unreachable hosts` を 3600（1 時間）から 10800（3 時間）に増やします。

minimalist バウンス プロファイルの例

次の例では、minimalist という名前のバウンス プロファイルが作成されます。このプロファイルでは、メッセージがバウンスされるときに再試行されず（最大再試行回数が 0）、再試行を待機する最大時間が指定されます。ハード バウンス メッセージはディセーブルであり、ソフト バウンス警告は送信されません。

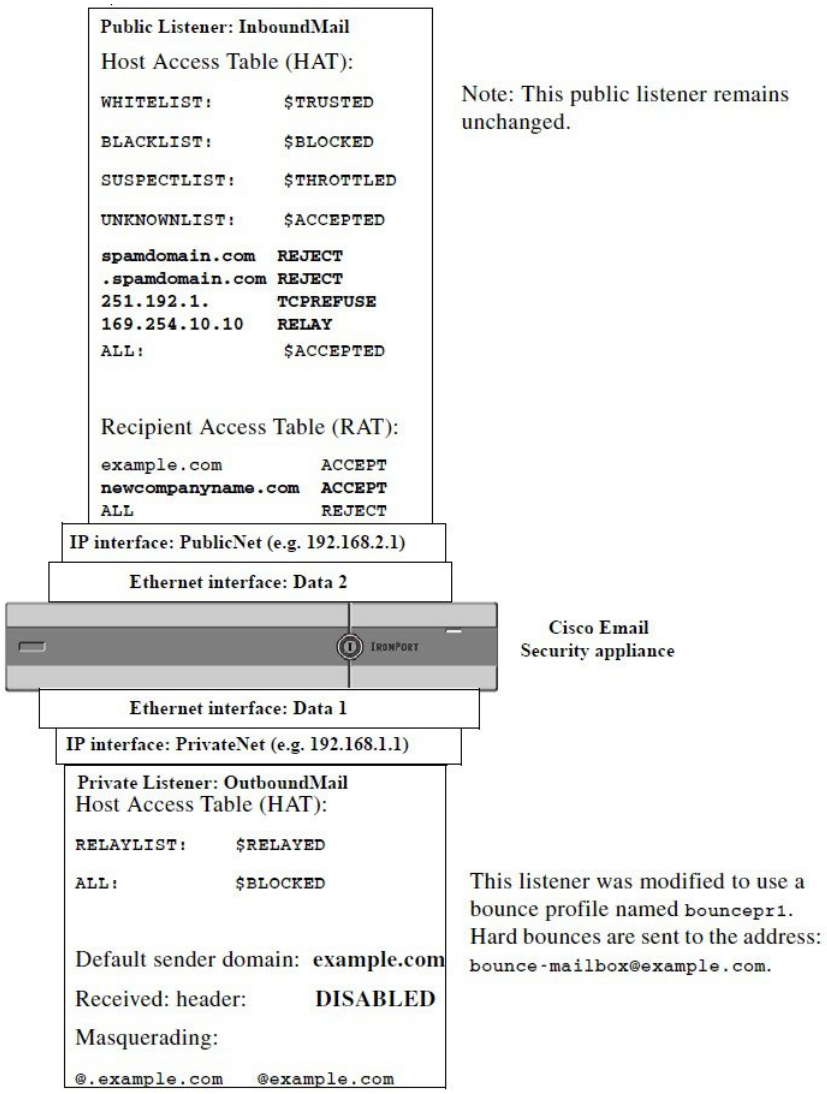
リスナーへのバウンス プロファイルの適用

バウンス プロファイルを作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページまたは **`listenerconfig`** コマンドを使用して、そのプロファイルをリスナーに適用できます。

次の例では、bouncepr1 プロファイルが OutgoingMail リスナーに適用されます。

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 *50 :* プライベート リスナーへのバウンス プロファイルの適用



宛先制御による電子メール配信の管理

大量の電子メールが未管理で配信されると、受信者ドメインで混乱が生じることがあります。AsyncOS では、電子メールゲートウェイで開く接続数や電子メールゲートウェイで各宛先ドメイン宛に送信されるメッセージ数を定義することにより、メッセージ配信を詳細に管理できます。

送信先コントロール機能（GUI では [メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）]、CLI では destconfig コマンド）を使用すると、次の項目を制御できます。

- レート制限 （895 ページ）

- TLS （895 ページ）
- バウンス検証 （895 ページ）
- [バウンス プロファイル（Bounce Profile）] （895 ページ）

レート制限

- [同時接続（Concurrent Connections）]：リモートホストに対して電子メールゲートウェイが開こうとする同時接続数。
- [接続あたりの最大メッセージ数（Maximum Messages Per Connection）]：電子メールゲートウェイが新しい接続を開始する前に、宛先ドメインに送信するメッセージ数。
- [受信者（Recipients）]：電子メールゲートウェイが特定の期間に特定のリモートホストに対して送信する受信者数。
- [制限（Limits）]：宛先ごと、および MGA ホスト名ごとに、制限を適用する方法。

TLS

- リモート ホストに対する TLS 接続を受入、可能、必須のいずれにするか（TLS の管理 （899 ページ） を参照）。
- TLS 接続が必要なリモート ホストに対してメッセージが配信されるときに、TLS ネゴシエーションが失敗した場合にアラートを送信するかどうか。これは、ドメイン単位ではなく、グローバルな設定です。
- リモート ホストに対するすべての発信 TLS 接続で使用する TLS 証明書の割り当て。

バウンス検証

- バウンス検証を使用して、アドレス タギングを実行するかどうか（バウンス検証 （904 ページ） を参照）。

[バウンス プロファイル（Bounce Profile）]

- 特定のリモートホストに対して電子メールゲートウェイで使用されるバウンスプロファイル（デフォルトのバウンスプロファイルは、[ネットワーク（Network）] > [バウンスプロファイル（Bounce Profiles）] ページで設定します）。

未指定のドメインに対するデフォルト設定を制御することもできます。

関連項目

- メール配信に使用するインターフェイスの決定 （896 ページ）
- デフォルトの配信制限 （896 ページ）
- 送信先コントロールの使用 （896 ページ）

メール配信に使用するインターフェイスの決定

出力インターフェイスを deliveryconfig コマンド、メッセージフィルタ（alt-src-host）、または仮想ゲートウェイを使用して指定しない場合は、出力インターフェイスは AsyncOS ルーティングテーブルによって選択されます。基本的には、「自動」を選択すると AsyncOS によって選択されます。

詳細は次のとおりです。ローカル アドレスは、インターフェイスのネットマスクをインターフェイスの IP アドレスに適用することで識別されます。どちらも、[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページまたは interfaceconfig コマンドを使用して（あるいはシステムのセットアップ時に）設定されます。アドレス空間が重なる場合は、より具体的なネットマスクが使用されます。宛先がローカルの場合、パケットは適切なローカルインターフェイス経由で送信されます。

宛先がローカルではない場合、パケットはデフォルトのルータ（[ネットワーク（Network）]> [ルーティング（Routing）] ページまたは setgateway コマンドを使用して設定）に対して送信されます。デフォルト ルータの IP アドレスはローカルです。出力インターフェイスは、ローカルアドレスの出力インターフェイスの選択ルールに従って決まります。たとえば、AsyncOS では、デフォルト ルータの IP アドレスが含まれていて最も具体的な IP アドレスおよびネットマスクが選択されます。

ルーティングテーブルは、[ネットワーク（Network）]>[ルーティング（Routing）]ページ（または routeconfig コマンド）を使用して設定されます。ルーティングテーブルで一致するエントリが、デフォルトルートよりも優先されます。ルートが具体的になるほど、優先度が高くなります。

デフォルトの配信制限

発信宛先ドメインごとに、専用の発信キューがあります。そのため、ドメインごとに別々の同時接続制限（[送信先コントロール（Destination Controls）] テーブルで指定）があります。さらに、[送信先コントロール（Destination Controls）] テーブルで具体的に示されていない一意のドメインごとに、テーブルで設定した別の「デフォルト（Default）」制限を使用します。

送信先コントロールの使用

GUI で [メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）] ページ、または CLI で destconfig コマンドを使用して、送信先コントロールエントリを作成、編集、および削除します。

関連項目

- IP アドレス バージョンの管理 （897 ページ）
- ドメインに対する接続、メッセージ、受信者の数の管理 （897 ページ）
- TLS の管理 （899 ページ）
- バウンス検証タギングの管理 （899 ページ）
- バウンスの管理 （900 ページ）

• 新しい送信先コントロール エントリの追加 （900 ページ）
• 宛先制御設定のインポートおよびエクスポート （900 ページ）
• 宛先制御と CLI （904 ページ）

IP アドレス バージョンの管理

ドメイン接続に使用する IP アドレスのバージョンを設定できます。電子メールゲートウェイはインターネットプロトコルバージョン4（IPv4）およびインターネットプロトコルバージョン（IPv6）の両方を使用します。電子メールゲートウェイのリスナーをプロトコルの両方または 1 つのバージョンを使用するように設定できます。

IPv4 または IPv6 に対して [必須（Required）] 設定を指定した場合、電子メールゲートウェイは指定されたバージョンのアドレスを使用してドメインへの接続をネゴシエーションします。ドメインが IP アドレスのバージョンを使わない場合、電子メールは送信されません。IPv4 または IPv6 の [推奨（Preferred）] 設定を指定した場合、電子メールゲートウェイは最初に指定されたバージョンのアドレスを使用してドメインへの接続をネゴシエーションし、最初の試みが到達可能でない場合は他にフォールバックします。

ドメインに対する接続、メッセージ、受信者の数の管理

アプライアンスで電子メールを配信する方法を制限することにより、電子メールゲートウェイからの電子メールを扱うリモートホストや独自の社内グループウェアサーバに負荷がかかり過ぎないようにできます。

ドメインごとに、特定の期間にシステムで超過しないようにする接続、発信メッセージ、受信者の最大数を割り当てることができます。この「グッドネイバー」テーブルは、送信先コントロール機能（[メールポリシー（Mail Policies）]>[送信先コントロール（Destination Controls）]、または `destconfig` コマンド（以前の `setgoodtable` コマンド））を使用して定義します。ドメイン名を指定するには、次の構文を使用します。

```
domain.com
```

または

```
.domain.com
```

この構文を使用すると、AsyncOS で sample.server.domain.com のようなサブドメインの送信先コントロールを指定できるようになります。詳細なサブドメインアドレスを個別に入力する必要はありません。

接続、メッセージ、受信者については、定義する制限が各 Virtual Gateway アドレスとシステム全体のどちらに対して適用されるのかを設定します。（Virtual Gateway アドレス制限では、IP インターフェイスごとの同時接続数を管理します。システム全体の制限では、電子メールゲートウェイで許可される接続の合計数を管理します。）

また、定義した制限がドメイン全体に適用されるかどうかを設定します。

（注） 現在のシステム デフォルトは、ドメインあたり 500 接続、接続あたり 50 メッセージです。

これらの値については、次の表で説明します。

表 *62 : [*送信先コントロール（*Destination Controls***）*]* テーブルの値**

フィールド	説明
同時接続（Concurrent Connections）	電子メールゲートウェイによって特定のホストに対して行われる発信接続の最大数。（ドメインには、社内グループウェアのホストを含めることができます。）
接続あたりの最大メッセージ数（Maximum Messages Per Connection）	新しい接続が開始されるまでに、電子メールゲートウェイから特定のホストに対する単一発信接続に対して許可されるメッセージの最大数。
受信者（Recipients）	特定の期間内に許可される受信者の最大数。[なし（None）] は、当該ドメインに対して、受信者の制限がないことを示します。 電子メールゲートウェイが受信者の数を数える最小期間（1 ～ 60 分）。期間に「0」を指定すると、この機能がディセーブルになります。 （注） 受信者制限を変更すると、すでにキュー内にあるすべてのメッセージのカウンタがリセットされます。電子メールゲートウェイは、新しい受信者制限に基づいてメッセージを配信します。
制限の適用（Apply Limits）	制限がドメイン全体に適用（強制）されるかどうかを指定します。 この設定は、接続、メッセージ、受信者の制限に適用されます。 制限がシステム全体と各 Virtual Gateway アドレスのどちらに適用されるのかを指定します。 （注） IP アドレスのグループを設定しても、仮想ゲートウェイを設定していない場合は、仮想ゲートウェイごとに適用制限を設定しないでください。この設定は、仮想ゲートウェイを使用するように設定されたシステムのみを対象にしています。仮想ゲートウェイの設定方法については、Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ（912 ページ）を参照してください。

（注） 制限が Virtual Gateway アドレスごとに適用される場合でも、システム全体の制限を仮想ゲートウェイの数で除算した値を Virtual Gateway の制限に設定することによって、システム全体の制限を効果的に実装できます。たとえば、4 つの仮想ゲートウェイ アドレスが設定されていて、ドメイン `yahoo.com` に対して 100 より多くの同時接続を開かないようにするには、仮想ゲートウェイの制限を同時接続数 25 に設定します。

`delivernow` コマンドをすべてのドメインに対して実行すると、`destconfig` コマンドで追跡されているすべてのカウンタがリセットされます。

TLS の管理

ドメイン単位で Transport Layer Security（TLS; トランスポート層セキュリティ）を設定することもできます。[必須（Required）]設定が指定された場合、電子メールゲートウェイのリスナーからドメインの MTA に対して TLS 接続がネゴシエートされます。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。詳細については、配信時の TLS および証明書検証の有効化 （840 ページ）を参照してください。

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、電子メールゲートウェイがアラートを送信するかどうかを指定できます。アラート メッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。電子メールゲートウェイは、システムアラートのタイプの警告重大度レベルアラートを受信するよう設定されたすべての受信者にアラートメッセージを送信します。GUI の [システム管理（System Administration）] > [アラート（Alerts）] ページ（または CLI の alertconfig コマンド）を使用してアラートの受信者を管理できます。

TLS 接続アラートをイネーブルにするには、[送信先コントロール（Destination Controls）] ページの [グローバル設定を編集（Edit Global Settings）] をクリックまたは destconfig -> setup サブコマンドを使用します。これは、ドメイン単位ではなく、グローバルな設定です。電子メールゲートウェイが配信を試行したメッセージの情報については、[モニタ（Monitor）]>[メッセージトラッキング（Message Tracking）] ページまたはメールログを使用します。

すべての発信 TLS 接続に使用する証明書を指定する必要があります。[送信先コントロール（Destination Controls）] ページの [グローバル設定を編集（Edit Global Settings）] または destconfig -> setup サブコマンドを使用して、証明書を指定します。証明書の取得方法については、証明書の使用 （830 ページ）を参照してください。

アラートの詳細については、「システム管理」の章を参照してください。

バウンス検証タギングの管理

送信されるメールにバウンス検証のタギングが行われるかどうかを指定できます。デフォルトに対して指定することも、特定の宛先に対して指定することもできます。シスコでは、デフォルトに対してバウンス検証をイネーブルにした後で、具体的な除外対象として新しい宛先を作成することを推奨します。詳細については、バウンス検証（904ページ）を参照してください。

バウンスの管理

リモートホストに配信する接続や受信者の数を制御できるだけでなく、そのドメインで使用されるバウンス プロファイルを指定することもできます。指定すると、バウンス プロファイルは destconfig コマンドの 5 番目のカラムに表示されます。バウンス プロファイルを指定しない場合は、デフォルトのバウンスプロファイルが使用されます。詳細については、新しいバウンス プロファイルの作成 （893 ページ）を参照してください。

新しい送信先コントロール エントリの追加

手順

ステップ 1 [送信先の追加（Add Destination）] をクリックします。

ステップ 2 エントリを設定します。

ステップ 3 変更を送信し、保存します。

宛先制御設定のインポートおよびエクスポート

複数のドメインを管理している場合は、すべてのドメインの送信先コントロールエントリを定義する単一の設定ファイルを作成して、電子メールゲートウェイにインポートできます。設定ファイルの形式は、Windows INI 設定ファイルと似ています。ドメインのパラメータはセクションにまとめられ、セクション名としてドメイン名が使用されます。たとえば、セクション名 [example.com] を使用して、ドメイン `example.com` のパラメータをグループにします。定義されないすべてのパラメータは、デフォルトの送信先コントロールエントリから継承されます。デフォルトの送信先コントロールエントリのパラメータを定義するには、設定ファイルに `[デフォルト（DEFAULT）]` セクションを含めます。

設定ファイルをインポートすると、電子メールゲートウェイの送信先コントロールエントリがすべて上書きされます。ただし、設定ファイルに `[デフォルト（DEFAULT）]` セクションが含まれていない場合、デフォルトエントリは上書きされません。その他すべての既存の送信先コントロール エントリは削除されます。

設定ファイルでは、ドメインに対して次のパラメータを定義できます。`[デフォルト（DEFAULT）]` セクションには `bounce_profile` パラメータを除くすべてのパラメータが必要です。

表 *63* : 送信先コントロール設定ファイルのパラメータ

パラメータ名	説明
ip_sort_pref	ドメインに対してインターネットプロトコルバージョンを指定します。 次のいずれかの値を入力します。 • IPv6「Preferred」の場合の PREFER_V6 • IPv6「Required」の場合の REQUIRE_v6 • IPv4「Preferred」の場合の PREFER_V4 • IPv4「Required」の場合の REQUIRE_v4
max_host_concurrency	電子メールゲートウェイによって特定のホストに対して行われる発信接続の最大数。 ドメインに対してこのパラメータを定義する場合は、limit_type および limit_apply パラメータも定義する必要があります。
max_messages_per_connection	新しい接続が開始されるまでに、電子メールゲートウェイから特定のホストに対する単一発信接続に対して許可されるメッセージの最大数。
recipient_minutes	電子メールゲートウェイが受信者の数を数える期間（1 ～ 60 分）。受信者制限を適用しないようにする場合は、未定義のままにします。
recipient_limit	特定の期間内に許可される受信者の最大数。受信者制限を適用しないようにする場合は、未定義のままにします。 ドメインに対してこのパラメータを定義する場合は、recipient_minutes、limit_type、および limit_apply パラメータも定義する必要があります。
limit_type	制限がドメイン全体とそのドメインに指定された各メール交換 IP アドレスのどちらに適用されるのかを指定します。 次のいずれかの値を入力します。 • 0（または host）：ドメインの場合 • 1（または MXIP）：メール交換 IP アドレスの場合
limit_apply	制限がシステム全体と各 Virtual Gateway アドレスのどちらに適用されるのかを指定します。 次のいずれかの値を入力します。 • 0（または system）：システム全体の場合 • 1（または VG）：Virtual Gateway の場合
bounce_validation	バウンス検証アドレス タギングをオンにするかどうかを指定します。 次のいずれかの値を入力します。 • 0（または off） • 1（または on）

パラメータ名	説明
table_tls	ドメインの TLS 設定を指定します。詳細については、配信時の TLS および証明書検証の有効化 （840 ページ）を参照してください。 次のいずれかの値を入力します。 • 0（または off） • 1（または on）「推奨（Preferred）」の場合 • 2（または required）「必須（Required）」の場合 • 3（または on_verify）「推奨（検証）（Preferred (Verify)）」の場合 • 4（または require_verify）：「必須（検証）（Required (Verify)）」の場合 文字列には、大文字と小文字の区別はありません。
bounce_profile	使用するバウンス プロファイルの名前。[デフォルト（DEFAULT）] 送信先コントロール エントリでは使用できません。
send_tls_req_alert	必須の TLS 接続が失敗した場合にアラートを送信するかどうか。 次のいずれかの値を入力します。 • 0（または off） • 1（または on） これはグローバル設定であり、[デフォルト（DEFAULT）] 送信先コントロール エントリでのみ使用できます。
certificate	発信 TLS 接続で使用される証明書。これはグローバル設定であり、[デフォルト（DEFAULT）] 送信先コントロールエントリでのみ使用できます。 （注） 証明書を指定しない場合は、デモの証明書が割り当てられますが、デモの証明書を使用することはセキュアではないため、通常の使用には推奨できません。

ドメイン example1.com、example2.com、およびデフォルトの送信先コントロール エントリの例を次に示します。

```
[DEFAULT]

ip_sort_pref = PREFER_V6

max_host_concurrency = 500

max_messages_per_connection = 50

recipient_minutes = 60

recipient_limit = 300

limit_type = host

limit_apply = VG
```

```
table_tls = off

bounce_validation = 0

send_tls_req_alert = 0

certificate = example.com

[example1.com]

ip_sort_pref = PREFER_V6

recipient_minutes = 60

recipient_limit = 100

table_tls = require_verify

limit_apply = VG

bounce_profile = tls_failed

limit_type = host

[example2.com]

table_tls = on

bounce_profile = tls_failed
```

上記の例では、example1.com および example2.com について次の送信先コントロール エントリが生成されます。

```
example1.com

IP Address Preference: IPv6 Preferred

Maximum messages per connection: 50

Rate Limiting:

500 concurrent connections

100 recipients per 60 minutes

Limits applied to entire domain, across all virtual gateways

TLS: Required (Verify)

Bounce Profile: tls_failed

example2.com

IP Address Preference: IPv6 Preferred

Maximum messages per connection: Default
```

```
Rate Limiting: Default

TLS: Preferred


Bounce Profile: tls_failed
```

[送信先コントロール（Destination Controls）] ページの [テーブルのインポート（Import Table）] ボタン、または `destconfig -> import` コマンドを使用して、設定ファイルをインポートします。[送信先コントロール（Destination Controls）] ページの [テーブルのエクスポート（Export Table）] ボタン、または `destconfig -> export` コマンドを使用して、送信先コントロール エントリを INI ファイルにエクスポートすることもできます。エクスポートされた INI ファイルには `[デフォルト（Default）]` ドメイン管理エントリも含まれています。

宛先制御と CLI

CLI で destconfig コマンドを使用して、送信先コントロール エントリを設定できます。このコマンドについては、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

バウンス検証

「バウンス」メッセージは、受信側の MTA によって送信される新しいメッセージで、元の電子メールのエンベロープ送信者が新しいエンベロープ受信者として使用されます。このバウンスは、元のメッセージが配信不可能なときに（通常は、受信者アドレスが存在しないため）、通常は空のエンベロープ送信者（MAIL FROM:<>）でエンベロープ受信者に送り返されます。

スパム送信者は、誤った宛先を指定したバウンス攻撃による電子メールインフラストラクチャへの攻撃をますます増やしています。このような攻撃は、未知の正当なメールサーバによって送信される、膨大なバウンスメッセージによって行われます。基本的に、スパム送信者が使用するプロセスでは、オープンリレーおよび「ゾンビ」ネットワークを経由してさまざまなドメインで無効な可能性のあるアドレス（エンベロープ受信者）に電子メールを送信します。このようなメッセージでは、エンベロープ送信者が偽装されるため、スパムは正当なドメインから送信されたように見えます（これは「Joe job（ジョー ジョブ）」とも呼ばれます）。

次に、無効なエンベロープ受信者による着信電子メールごとに、受信側のメールサーバによって新しい電子メール（バウンスメッセージ）が生成され、一緒に無実なドメイン（エンベロープ送信者アドレスが偽装されたドメイン）の電子メール送信者宛に送信されます。その結果、このターゲットドメインは、「誤った宛先が指定された」膨大なバウンスを受信します。このバウンスメッセージは、数百万にもおよぶことがあります。このような分散DoS攻撃により、電子メールインフラストラクチャがダウンして、ターゲットが正当な電子メールの送受信を行えなくなります。

誤った宛先を指定したバウンス攻撃に対処するため、AsyncOS には [バウンス検証（Bounce Verification）] が用意されています。イネーブルにすると、バウンス検証によって、その電子メールゲートウェイから送信されたメッセージのエンベロープ送信者アドレスにタグが付けられます。次に、電子メールゲートウェイで受信したバウンスメッセージで、エンベロープ受信者にこのタグが付いているかどうかがチェックされます。正当なバウンス（このタグが付いて

いる）であれば、タグが外されて配信されます。タグが付いていないバウンス メッセージは、別の処理を行えます。

バウンス検証を使用して、発信メールに基づいて着信バウンス メッセージを管理できます。電子メールゲートウェイで着信メールに基づいて発信バウンスを生成する方法の制御については、バウンスした電子メールの処理 （884 ページ）を参照してください。

関連項目

- 概要：タギングとバウンス検証 （905 ページ）
- バウンス検証を使用してバウンス メッセージ ストームを防止 （907 ページ）
- タグなしのバウンスされたメッセージの合法的受け入れ （906 ページ）

概要：タギングとバウンス検証

バウンス検証をイネーブルにして電子メールを送信すると、電子メールゲートウェイにより、メッセージのエンベロープ送信者アドレスが書き換えられます。たとえば、MAIL FROM: joe@example.com が MAIL FROM: prvs=joe=123ABCDEFG@example.com になるとします。この例の 123... という文字列は、「バウンス検証タグ」であり、電子メールゲートウェイによって送信されるときに、エンベロープ送信者に追加されます。このタグは、バウンス検証設定で定義されたキーを使用して生成されます（キーの指定については、バウンス検証アドレスのタギング キー （906 ページ）を参照してください）。このメッセージがバウンスすると、バウンス内のエンベロープ受信者アドレスに通常はこのバウンス検証タグが含まれます。

デフォルトではシステム全体でバウンス検証タギングをイネーブルまたはディセーブルにできます。特定のドメインに対してバウンス検証タギングをイネーブルまたはディセーブルにすることもできます。ほとんどの場合、デフォルトでイネーブルにしておき、除外する具体的なドメインを [送信先コントロール（Destination Controls）] テーブルに列挙します（送信先コントロールの使用 （896 ページ）を参照）。

メッセージにタグ付きのアドレスがすでに含まれている場合は、別のタグが追加されません（電子メールゲートウェイがバウンスメッセージを DMZ 内の電子メールゲートウェイに配信する場合）。

関連項目

- 着信バウンス メッセージの処理 （905 ページ）
- バウンス検証アドレスのタギング キー （906 ページ）

着信バウンス メッセージの処理

有効なタグが含まれているバウンスは配信されます。タグが削除され、エンベロープ受信者が復元されます。これは、電子メールパイプラインのドメインマップ処理の直後に発生します。電子メールゲートウェイでタグの付いていないバウンスやタグが無効に付いたバウンスの処理方法として、拒否するのか、それともカスタムヘッダーを追加するのかを定義できます。詳細については、バウンス検証設定値の設定 （908 ページ）を参照してください。

バウンス検証タグが存在しない場合、タグの生成に使用されたキーが変更された場合、またはメッセージが7日より古い場合、そのメッセージはバウンス検証で定義された設定に従って扱われます。

たとえば、次のメールログには、電子メールゲートウェイで拒否されたバウンスメッセージが示されています。

```
Fri Jul 21 16:02:19 2006 Info: Start MID 26603 ICID 125192

Fri Jul 21 16:02:19 2006 Info: MID 26603 ICID 125192 From: <>

Fri Jul 21 16:02:40 2006 Info: MID 26603 ICID 125192 invalid bounce, rcpt address
<bob@example.com> rejected by bounce verification.
Fri Jul 21 16:03:51 2006 Info: Message aborted MID 26603 Receiving aborted by sender

Fri Jul 21 16:03:51 2006 Info: Message finished MID 26603 aborted
```

（注） 非バウンス メールを独自の社内メール サーバ（Exchange など）に配信する場合は、その社内ドメインに対してバウンス検証タギングを無効にしてください。

AsyncOS では、バウンスがヌルの MAIL FROM アドレス（<>）が設定されたメールであると見なされます。タグ付きのエンベロープ受信者が含まれる可能性のある非バウンス メッセージの場合は、より緩やかなポリシーが適用されます。そのような場合、7 日でのキー失効は無視され、古いキーとの一致も調べられます。

バウンス検証アドレスのタギング キー

タギングキーは、バウンス検証タグを生成するときに電子メールゲートウェイで使用されるテキスト文字列です。ドメインから発信されるすべてのメールには一貫してタグが付けられるため、すべての電子メールゲートウェイで同じキーを使用することが理想的です。そのようにして、ある電子メールゲートウェイで発信メッセージのエンベロープ送信者にタグが付けられる場合、別の電子メールゲートウェイからバウンスを受信しても、その着信バウンスが検証および配信されます。

タグには7日間の猶予期間があります。たとえば、7 日間のうちにタギング キーを複数回変更できます。その場合、電子メールゲートウェイは7日よりも新しいこれまでのすべてのキーを使用して、タグの付いたメッセージを検証しようとします。

タグなしのバウンスされたメッセージの合法的受け入れ

AsyncOS には、バウンス検証に関連して、タグの付いていないバウンスを有効とするかどうかを検討する HAT 設定もあります。デフォルト設定は「いいえ」であり、タグの付いていないバウンスは無効であると見なされます。さらに、電子メールゲートウェイでは[メールポリシー（Mail Policies）]>[バウンス検証（Bounce Verification）]ページで選択されたアクションに従って、メッセージが拒否されるか、またはカスタムヘッダーが付加されます。「はい」を選択した場合、電子メールゲートウェイではタグの付いていないバウンスは有効であると見なされ、受け入れられます。これは、次のようなシナリオで使用できます。

電子メールをメーリング リストに送信することを検討しているユーザがいるとします。しかし、メーリングリストでは、エンベロープ送信者の固定セットからのメッセージのみを受け入れています。そのような場合、ユーザからのタグ付きメッセージは受け入れられません（タグは定期的に変更されるため）。

手順

ステップ 1 ユーザがメールを送信しようとするドメインを [送信先コントロール（Destination Controls）] テーブルに追加し、そのドメインに対するタギングをディセーブルにします。この時点で、ユーザは問題なくメールを送信できます。

ステップ 2 しかし、そのドメインからのバウンスにはタグが付いていないため、バウンス受信を適切にサポートするには、そのドメインの送信者グループを作成し、[承認（Accept）] メール フロー ポリシーの [タグなしバウンスを有効と見なす（Consider Untagged Bounces to be Valid）] パラメータをイネーブルにします。

バウンス検証を使用してバウンス メッセージ ストームを防止

手順

ステップ 1 タギング キーを入力します。詳細については、バウンス検証アドレスのタグ付けキーの設定（907 ページ）を参照してください。

ステップ 2 バウンス検証設定を編集します。詳細については、バウンス検証設定値の設定（908 ページ）を参照してください。

ステップ 3 [送信先コントロール（Destination Controls）] を使用したバウンス検証をイネーブルにします。詳細については、送信先コントロールの使用（896 ページ）を参照してください。

次のタスク

関連項目

- バウンス検証アドレスのタグ付けキーの設定（907 ページ）
- バウンス検証設定値の設定（908 ページ）
- CLI を使用したバウンス検証の構成（908 ページ）
- バウンス検証とクラスタ設定（909 ページ）

バウンス検証アドレスのタグ付けキーの設定

[バウンス検証アドレスのタグ付けキー（Bounce Verification Address Tagging Keys）] のリストには、現在のキー、および過去に使用してまだ削除されていないキーが示されます。新規のキーを追加するには、次の手順を実行します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [バウンス検証（Bounce Verification）] ページで、[キーを追加（New Key）] をクリックします。

ステップ 2 テキスト文字列を入力し、[送信（Submit）] をクリックします。

ステップ 3 変更を保存します。

次のタスク

関連項目

- キーの削除 （908 ページ）

キーの削除

古いアドレス タギング キーを削除するには、プルダウン メニューから削除するルールを選択し、[除去（Purge）] をクリックします。

バウンス検証設定値の設定

バウンス検証設定では、無効なバウンスを受信したときに実行するアクションを指定します。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [バウンス検証（Bounce Verification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 無効なバウンスを拒否するのか、カスタム ヘッダーをメッセージに追加するのかを選択します。ヘッダーを追加する場合は、ヘッダーの名前と値を入力します。

ステップ 4 必要に応じて、スマート例外機能をイネーブルにします。この設定を使用すると、（着信メールと発信メールの両方で1つのリスナーを使用している場合であっても）着信メール メッセージ、および社内メール サーバで生成されるバウンス メッセージをバウンス検証処理から自動的に除外できるようにします。

ステップ 5 変更を送信し、保存します。

CLI を使用したバウンス検証の構成

CLI で bvconfig コマンドおよび destconfig コマンドを使用して、バウンス検証を設定できます。これらのコマンドについては、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

バウンス検証とクラスタ設定

バウンス検証は、両方の電子メールゲートウェイで同じ「バウンスキー」を使用している限り、クラスタ設定で動作します。同じキーを使用する場合は、どちらのシステムでも正当なバウンスを受け入れられる必要があります。変更後のヘッダータグ/キーは、各電子メールゲートウェイに固有ではありません。

電子メール配信パラメータの設定

deliveryconfig コマンドは、電子メールゲートウェイから電子メールを配信するときに使用されるパラメータを設定します。

電子メールゲートウェイは、SMTP と QMQP という複数のメールプロトコルを使用してメールを受信します。ただし、すべての発信電子メールは、SMTP を使用して配信されます。このため、deliveryconfig コマンドではプロトコルの指定が不要です。

（注） このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、付録「ネットワークと IP アドレスの割り当て」を参照してください。

関連項目

- デフォルトの配信 IP インターフェイス （909 ページ）
- 配信可能性あり機能 （910 ページ）
- デフォルトの最大同時接続数 （910 ページ）
- deliveryconfig の例 （910 ページ）

デフォルトの配信 IP インターフェイス

デフォルトで、電子メール配信には IP インターフェイスまたは IP インターフェイス グループが使用されます。現在設定されているどの IP インターフェイスまたは IP インターフェイス グループでも設定できます。特定のインターフェイスが指定されない場合は、AsyncOS は、受信者ホストと通信するときに、SMTP HELO コマンドでデフォルトの配信インターフェイスと関連付けられたホスト名を使用します。IP インターフェイスを設定するには、interfaceconfig コマンドを使用します。

電子メール配信インターフェイスの自動選択を使用するときのルールは次のとおりです。

- リモートの電子メール サーバが設定済みインターフェイスのいずれかと同じサブネット上にある場合、トラフィックは一致するインターフェイス上を流れます。
- auto-select に設定した場合、routeconfig を使用して設定したスタティック ルートが有効になります。

- そうでない場合、デフォルトゲートウェイと同じサブネット上にあるインターフェイスが使用されます。すべての IP アドレスで宛先に対するルートが同等の場合、使用可能なうち最も効率的なインターフェイスが使用されます。

配信可能性あり機能

注意 この機能を有効にすると、メッセージ配信が信頼できなくなり、メッセージの損失につながることがあります。また、電子メールゲートウェイは RFC 5321 に準拠しない状態になります。詳細については、http://tools.ietf.org/html/rfc5321#section-6.1.を参照してください。

配信可能性あり機能が有効になると、AsyncOS では、メッセージ本文が配信されてから受信者ホストがメッセージの受信を確認するまでの間にタイムアウトするすべてのメッセージを「配信可能性あり」であるとみなして扱います。この機能を使用すると、受信者ホストで連続するエラーにより受信の確認が妨げられる場合に、メッセージのコピーを複数受信しなくて済みます。AsyncOS では、この受信を配信可能性ありとしてメール ログに記録し、そのメッセージを完了したものとして見なします。

デフォルトの最大同時接続数

電子メールゲートウェイが発信メッセージの配信で確立するデフォルトの最大同時接続数も指定できます。（システム全体のデフォルトはドメインごとに 10,000 接続です）この制限は、リスナーあたりの最大同時発信メッセージ配信数（リスナーあたりのデフォルトは、プライベート リスナーで 600 接続、パブリック リスナーで 1000 接続です）とともにモニタリングされます。デフォルトよりも小さい値を設定すると、ゲートウェイが弱いネットワークを支配しないようにすることができます。たとえば、特定のファイアウォールが大量の接続をサポートしない場合、そのような環境ではこれが原因で Denial of Service（DoS; サービス拒否）警告が引き起こされることがあります。

deliveryconfig の例

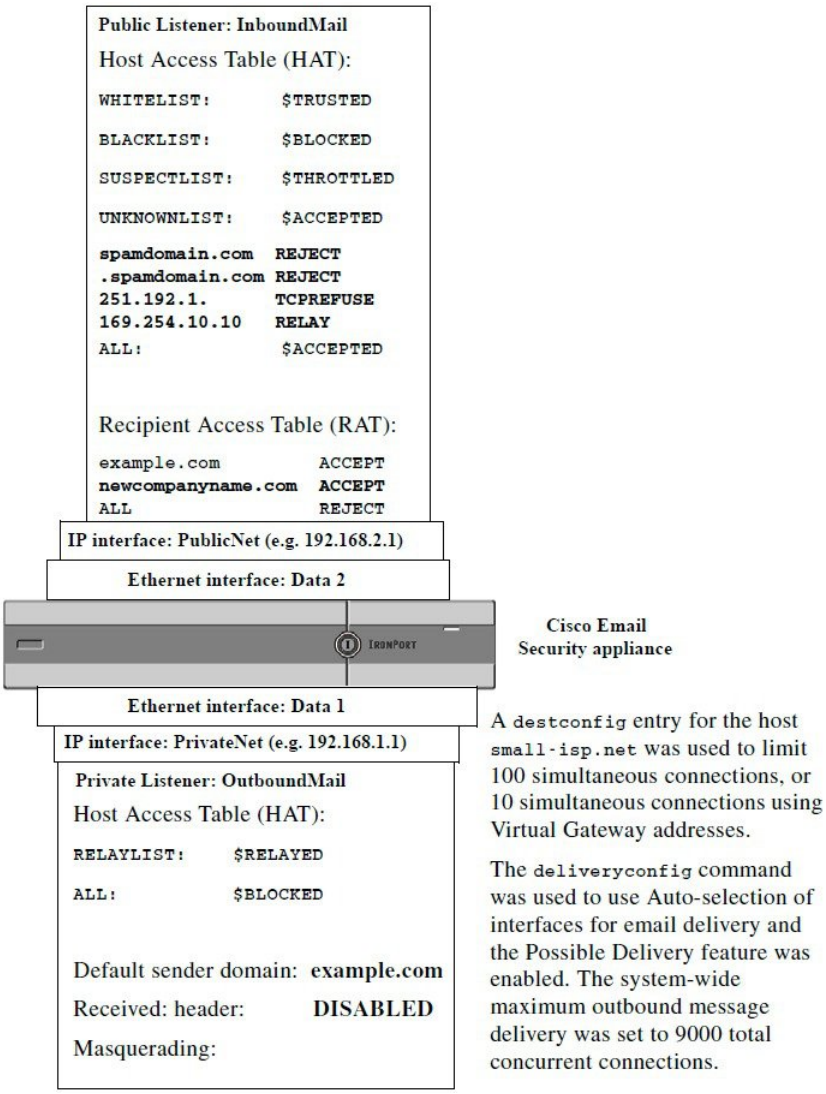
次の例では、`deliveryconfig` コマンドを使用し、[配信可能性あり（Possible Delivery）] をイネーブルにして、デフォルトのインターフェイスを [自動（Auto）] に設定します。システム全体の最大発信メッセージ配信は、9000 接続です。

```
mail3.example.com> deliveryconfig


Choose the operation you want to perform:

- SETUP - Configure mail delivery.

[]> setup

Choose the default interface to deliver mail.
```

```
1. Auto

2. PublicNet2 (192.168.3.1/24: mail4.example.com)

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

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

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


[1]> 1

Enable "Possible Delivery"? [Y]> y

Please enter the default system wide maximum outbound message delivery

concurrency

[10000]> 9000

mail3.example.com>
```

これで電子メール ゲートウェイの設定は次のようになります。

図 *51 :* 宛先および配信パラメータの設定



Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ

この項では、Cisco Virtual Gateway™ テクノロジーとその利点、Virtual Gateway アドレスの設定方法、および Virtual Gateway アドレスのモニタおよび管理方法について説明します。

Cisco Virtual Gateway テクノロジーでは、ホストするすべてのドメインに対して異なる IP アドレス、ホスト名、およびドメインを使用してエンタープライズ メール ゲートウェイを設定し、同じ物理電子メールゲートウェイ内にホストしている場合でも、それらのドメインに対して別々に企業の電子メールポリシー強制およびスパム対策方針を作成できます。すべての電子メールゲートウェイモデルで使用可能な仮想ゲートウェイアドレスの数値は 255 です。

関連項目

- 概要 （913 ページ）
- Virtual Gateway アドレスの設定 （913 ページ）
- Virtual Gateway アドレスのモニタ （921 ページ）
- Virtual Gateway アドレスごとの配信接続の管理 （921 ページ）

概要

企業がカスタマーと電子メールで信頼性の高いコミュニケーションを実現できるように、シスコは独自の Virtual Gateway テクノロジーを開発しました。Virtual Gateway テクノロジーを使用すると、電子メールゲートウェイを複数の Virtual Gateway アドレスに分割し、そのアドレスを使用して電子メールを送受信できます。各 Virtual Gateway アドレスには、別々の IP アドレス、ホスト名、ドメイン、および電子メール キューが与えられます。

別々の IP アドレスとホスト名を各 Virtual Gateway アドレスに割り当てることにより、ゲートウェイ経由で配信される電子メールが受信者ホストで正しく識別され、重要な電子メールがスパムと見なされてブロックされるのを防ぐことができます。電子メールゲートウェイには、Virtual Gateway アドレスごとに SMTP HELO コマンドで正しいホスト名を付与できる高度な機能があります。そのため、受信側の Internet Service Provider（ISP; インターネット サービス プロバイダー）が逆 DNS ルックアップを実行すると、電子メールゲートウェイでは、その Virtual Gateway アドレス経由で送信された電子メールの IP アドレスと一致させることができます。多くの ISP では迷惑電子メールを検出するために逆 DNS ルックアップを使用しているため、この機能は非常に有用です。逆 DNS ルックアップでの IP アドレスが送信側ホストの IP アドレスと一致しない場合、ISP では、送信者が不正であると見なして、電子メールを破棄する頻度が高くなります。Cisco Virtual Gateway テクノロジーでは、逆 DNS ルックアップが送信側の IP アドレスと常に一致するため、メッセージが意図せずブロックされてしまうのを防げます。

各 Virtual Gateway アドレスでのメッセージも、別々のメッセージ キューに割り当てられます。受信者ホストで特定の Virtual Gateway アドレスからの電子メールをブロックしている場合、そのホスト宛のメッセージはキューに残され、最終的にはタイムアウトします。しかしブロックされていない別の Virtual Gateway キュー内にある同じドメイン宛のメッセージは、正常に配信されます。これらのキューは、配信では別のものとして扱われますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。

Virtual Gateway アドレスの設定

Cisco Virtual Gateway アドレスを設定する前に、電子メールの送信元として使用される IP アドレスのセットを割り当てる必要があります。（詳細については、付録「ネットワークと IP アドレスの割り当て」を参照してください。）また、IP アドレスが有効なホスト名に解決されるように DNS サーバが正しく設定されている必要があります。DNS サーバが正しく設定されていれば、受信者ホストで逆 DNS ルックアップが実行されると、有効な IP/ホスト名のペアに解決されます。

関連項目

- 仮想ゲートウェイで使用する新しい IP インターフェイスの作成 （914 ページ）
- メッセージから配信用 IP インターフェイスへのマッピング （916 ページ）
- altsrchost ファイルのインポート （917 ページ）
- altsrchost の制限 （918 ページ）
- altsrchost コマンド用に有効なマッピングが記載されたテキスト ファイルの例 （918 ページ）
- CLI を使用した altsrchost マッピングの追加 （918 ページ）

仮想ゲートウェイで使用する新しい IP インターフェイスの作成

IP アドレスとホスト名が確立したら、Virtual Gateway アドレスを設定するために、まずはその IP/ホスト名のペアで新しい IP インターフェイスを作成します。それには、GUI の [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] ページ、または CLI の interfaceconfig コマンドを使用します。

IP インターフェイスを設定したら、複数の IP インターフェイスをインターフェイス グループへと結合できます。これらのグループは、電子メールの配信時に「ラウンドロビン」方式で順番に使用される Virtual Gateway アドレスに割り当てることができます。

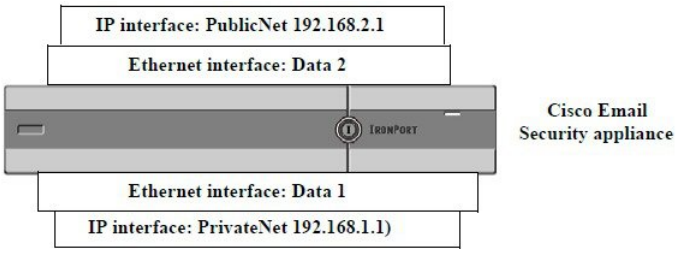
必要な IP インターフェイスを作成したら、2 つの方法で Virtual Gateway アドレスを設定し、各 IP インターフェイスまたはインターフェイス グループから送信される電子メール キャンペーンを定義します。

- altsrchost コマンドを使用すると、特定の送信者 IP アドレスまたはエンベロープ送信者アドレスの情報からホストの IP インターフェイス（Virtual Gateway アドレス）またはインターフェイス グループに電子メールをマッピングして配信できます。
- メッセージ フィルタを使用して、特定ホストの IP インターフェイス（Virtual Gateway アドレス）またはインターフェイス グループを使用してフラグ付きのメッセージを配信するためのフィルタを設定できます。送信元ホスト（Virtual Gateway アドレス）変更アクション （248 ページ）を参照してください。（この方法は前述の方法よりも柔軟性があり、強力です。）

IP インターフェイスを作成する詳細については、付録「電子メールゲートウェイへのアクセス」を参照してください。

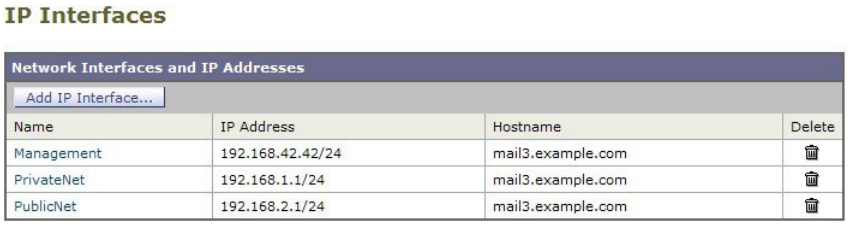
ここまで、次の図に示すように定義された次のインターフェイスを用いて、電子メール ゲートウェイの設定を使用してきました。

図 *52* : パブリック インターフェイスとプライベート インターフェイスの例



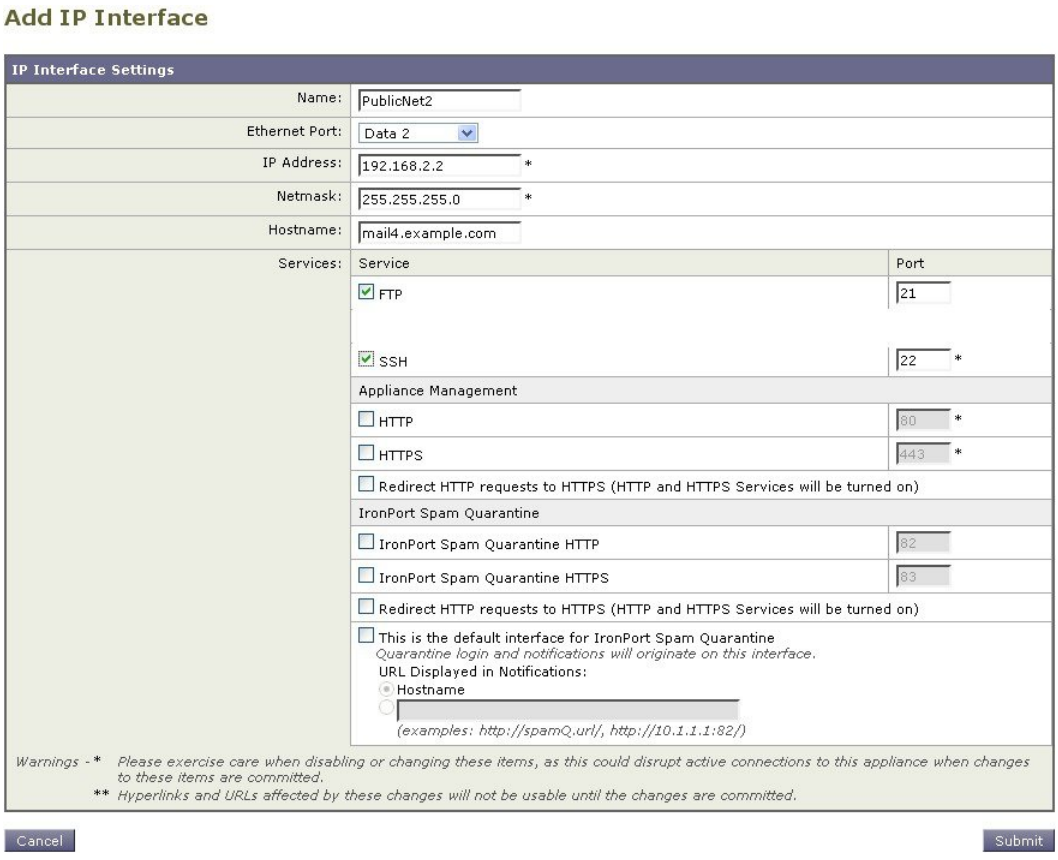
次の例では、[IPインターフェイス（IP Interfaces）] ページで管理インターフェイスの他に 2 つのインターフェイス（PrivateNet および PublicNet）が設定されていることを確認できます。

図 *53 : [IPインターフェイスを編集（ IP Interface）] ページ*



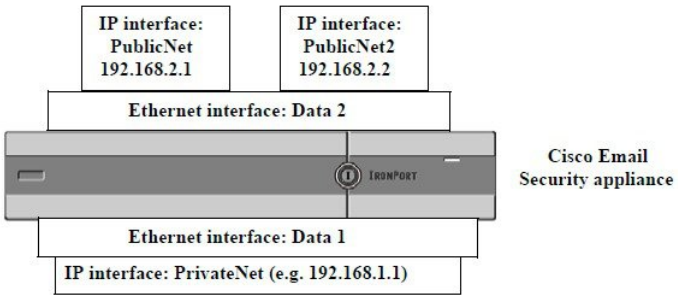
次に、[IPインターフェイスの追加（Add IP Interface）] ページを使用して、Data2 イーサネット インターフェイス上に PublicNet2 という名前の新しいインターフェイスを作成します。IP アドレス 192.168.2.2 が使用され、ホスト名 mail4.example.com が指定されています。さらに、FTP（ポート 21）および SSH（ポート 22）がイネーブルになります。

図 *54 : [IPインターフェイスの追加（Add IP Interface）] ページ*



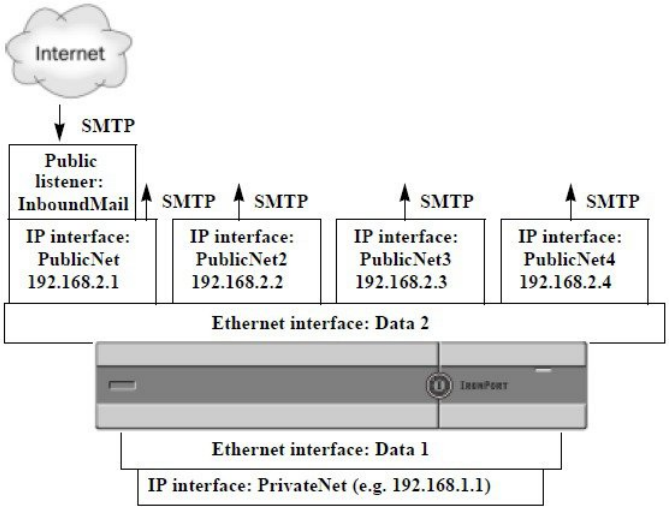
これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 *55 :* 別のパブリック インターフェイスの追加



Virtual Gateway アドレスを使用すると、次の図に示すようなコンフィギュレーションも可能です。

図 *56 : 1* つのイーサネット インターフェイス上にある *4* つの *Virtual Gateway* アドレス



4 つの IP インターフェイスはそれぞれメール配信に使用できますが、インターネットからのメールを受け入れるように設定されるのはパブリック リスナー 1 つだけです。

メッセージから配信用 IP インターフェイスへのマッピング

`altsrchost` コマンドを使用すると、各電子メールゲートウェイを、電子メールの配信元となる複数の IP インターフェイス（Virtual Gateway アドレス）にセグメント化することが最も単純で単刀直入な方法です。ただし、メッセージを特定の Virtual Gateway にマッピングする際にさらに強力で柔軟な方法が必要であれば、メッセージフィルタの使用を検討してください。詳細については、メッセージフィルタを使用した電子メール ポリシーの適用（155 ページ）を参照してください。

`altsrchost` コマンドを使用すると、次のいずれかに基づいて、電子メールの配信中に使用する IP インターフェイスまたはインターフェイス グループを管理できます。

- 送信者の IP アドレス
- エンベロープ送信者アドレス

電子メールの配信元にする IP インターフェイスまたはインターフェイス グループを指定するには、送信者の IP アドレスまたはエンベロープ送信者アドレスを IP インターフェイスまたはインターフェイス グループ（インターフェイス名またはグループ名で指定）とペアにするマッピング キーを作成します。

AsyncOS では、IP アドレスとエンベロープ送信者アドレスの両方をマッピング キーと比較します。IP アドレスまたはエンベロープ送信者アドレスがいずれかのキーと一致する場合、対応する IP インターフェイスが発信配信に使用されます。一致しない場合は、デフォルトの発信インターフェイスが使用されます。

一致する可能性のあるキーを優先順に示します。

送信者の IP アドレス（Sender's IP address）	送信者の IP アドレスは完全一致する必要があります。 例：`192.168.1.5`
完全形式のエンベロープ送信者（Fully-formed Envelope Sender ）	エンベロープ送信者は、アドレス全体が完全一致する必要があります。 例：`username@example.com`
ユーザ名（Username）	エンベロープ送信者アドレスの `@` 記号までの部分に対してユーザ名構文と一致させます。`@`記号を含める必要があります。例：`username@`
ドメイン（Domain）	エンベロープ送信者アドレスの `@` 記号で始まる部分に対してドメイン名構文と一致させます。`@` 記号を含める必要があります。例：`@example.com`

（注） リスナーは `altsrchost` テーブルで情報をチェックし、マスカレード情報をチェックした後からメッセージフィルタがチェックされる前までに、電子メールを特定のインターフェイスに転送します。

`altsrchost` コマンド内のサブコマンドを使用して、CLI で Virtual Gateway にマッピングを作成します。

構文	説明
`new`	新しいマッピングを手動で作成します。
`print`	マッピングの現在のリストを表示します。
`delete`	テーブルからマッピングを 1 つ削除します。

altsrchost ファイルのインポート

HAT、RAT、smtproutes、マスカレード テーブル、エイリアス テーブルと同様に、altsrchost エントリはファイルをエクスポートおよびインポートして変更できます。

手順

ステップ 1 altsrchost コマンドの export サブコマンドを使用して、既存のエントリをファイル（ファイル名は自分で指定）にエクスポートします。

ステップ 2 CLI の外部で、ファイルを取得します。（詳細については、FTP、SSH、および SCP アクセス（1573 ページ）を参照してください。）

ステップ 3 テキスト エディタを使用して、ファイルに新しいエントリを作成します。ルールが altsrchost テーブルに出現する順序が重要です。

ステップ 4 ファイルを保存してインターフェイスの「altsrchost」ディレクトリに配置し、インポートできるようにします。（詳細については、FTP、SSH、およびSCP アクセス（1573 ページ）を参照してください）。

ステップ 5 altsrchost の import サブコマンドを使用して、編集したファイルをインポートします。

altsrchost の制限

altsrchost エントリは、最大 1,000 個まで定義できます。

altsrchost コマンド用に有効なマッピングが記載されたテキスト ファイルの例

```
# Comments to describe the file

@example.com DemoInterface

paul@ PublicInterface

joe@ PublicInterface

192.168.1.5, DemoInterface

steve@example.com PublicNet
```

`import` および `export` サブコマンドは、1 行単位で実行され、送信者 IP アドレスまたはエンベロープ送信者アドレスの行をインターフェイス名にマッピングします。スペース以外の文字からなる 1 番目のブロックがキー、スペース以外の文字からなる 2 番目のブロックがインターフェイス名となり、カンマ（,）またはスペース（ ）で区切ります。コメント行はナンバー記号（#）で始まり、無視されます。

CLI を使用した altsrchost マッピングの追加

次の例では、`altsrchost` テーブルが出力されて、既存のマッピングがないことが示されます。その後、2 つのエントリが作成されます。

- グループウェア サーバ ホスト `@exchange.example.com` からのメールは、PublicNet インターフェイスにマッピングされます。
- 送信者 IP アドレス 192.168.35.35（たとえば、マーケティング キャンペーン メッセージング システム）からのメールは、PublicNet2 インターフェイスにマッピングされます。

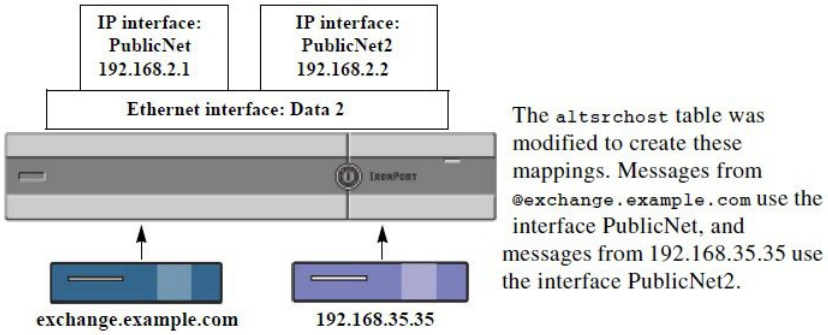
最後に、確認のために altsrchost マッピングが出力されて、変更が確定されます。

```
mail3.example.com> altsrchost

There are currently no mappings configured.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- IMPORT - Load new mappings from a file.

[]> new

Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.

[]> @exchange.example.com

Which interface do you want to send messages for @exchange.example.com from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)

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

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

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 4

Mapping for @exchange.example.com on interface PublicNet created.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.


[]> new


Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.


[]> 192.168.35.35

Which interface do you want to send messages for 192.168.35.35 from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)
```

```
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[1]> 1

Mapping for 192.168.35.35 on interface PublicNet2 created.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> print
1. 192.168.35.35 -> PublicNet2
2. @exchange.example.com -> PublicNet
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:

[]> Added 2 altsrchost mappings
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

この例におけるコンフィギュレーションの変更を次の図に示します。

図 *57* : 例：使用する *IP* インターフェイスまたはインターフェイス グループの選択



Virtual Gateway アドレスのモニタ

Virtual Gateway アドレスごとに独自の配信用電子メール キューがありますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。Virtual Gateway キューごとに受信者ホストのステータスをモニタするには、hoststatus および hostrate コマンドを使用します。「CLI による管理およびモニタリング」の章の「モニタリングに使用できるコンポーネントの読み取り」を参照してください。

hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。

Virtual Gateway テクノロジーを使用している場合は、各 Virtual Gateway アドレスに関する情報も表示されます。このコマンドは、返されるホスト情報のドメインを入力する必要があります。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です。

返される統計情報は、カウンタとゲージの 2 つのカテゴリにグループ化されます。さらに、返される他のデータには、最後のアクティビティ、MX レコード、最後の 5XX エラーがあります。

Virtual Gateway アドレスごとの配信接続の管理

一部のシステム パラメータには、システム レベルと Virtual Gateway アドレス レベルで設定が必要です。

たとえば、一部の受信者 ISP では、各クライアント ホストに許可されている接続数を制限しています。そのため、特に電子メールが複数の Virtual Gateway アドレスで配信されているときに、ISP との関係を管理することが必要です。

destconfig コマンド、および仮想ゲートウェイ アドレスに対する影響については、宛先制御による電子メール配信の管理 （894 ページ）を参照してください。

Virtual Gateway アドレスの「グループ」を作成すると、グループが 254 個の IP アドレスで構成されている場合であっても、Virtual Gateway のグッド ネイバー テーブル設定がグループに適用されます。

たとえば、254 個の発信 IP アドレスのグループを作成して、「ラウンドロビン」方式で順番に使用するようにセットアップされているとします。また、small-isp.com のグッド ネイバー テーブルで、同時接続数がシステムの場合は 100、Virtual Gateway アドレスの場合は 10 であるとします。このコンフィギュレーションでは、そのグループ内の 254 個の IP アドレスすべてに対して、合計で 10 よりも多くの接続が開くことはありません。グループは、単一の Virtual Gateway アドレスとして扱われます。

グローバル配信停止機能の使用

特定の受信者、受信者ドメイン、または IP アドレスが電子メールゲートウェイからメッセージを受信しないようにするには、AsyncOS の [グローバル配信停止（Global Unsubscribe）] 機能を使用します。unsubscribe コマンドを使用すると、[グローバル配信停止（Global Unsubscribe）] リストにアドレスを追加/削除したり、この機能を有効および無効にすることができます。「グローバルに配信停止された」ユーザー、ドメイン、電子メール アドレス、および IP アドレスのリストで、すべての受信者アドレスがチェックされます。受信者がリスト内のアドレスと一致する場合、受信者はドロップされるかハードバウンスされ、Global Unsubscribe（GUS; グローバル配信停止）カウンタが増分されます。（ログ ファイルには、一致する受信者がドロップされたのかハード バウンスされたのかが記録されます。）GUS のチェックは、電子メールを受信者に送信する直前に行われるため、システムで送信されるすべてのメッセージが検査されます。

（注） [グローバル配信停止（Global Unsubscribe）] 機能は、メーリング リストからの名前の削除やメーリング リストの全般的な保守に代わるものではありません。この機能は、不適切なエンティティに電子メールが配信されないようにするフェールセーフ メカニズムとして動作することを目的としています。

[グローバル配信停止（Global Unsubscribe）] には最大 10,000 アドレスを指定できます。[グローバル配信停止（Global Unsubscribe）] に追加されたアドレスは、次の 4 つのうちいずれかの形式をとります。

表 *64 :* グローバル配信停止の構文

username@example.com	完全形式の電子メール アドレス この構文は、特定ドメインの特定受信者をブロックするために使用されます。

username@	ユーザ名 ユーザ名構文は、すべてのドメインで特定ユーザ名を持つすべての受信者をブロックします。構文は、ユーザ名の後にアットマーク（@）を付けます。
@example.com	ドメイン ドメイン構文は、特定ドメイン宛のすべての受信者をブロックするために使用されます。構文は、具体的なドメインの前にアットマーク（@）を付けます。
@.example.com	部分ドメイン 部分ドメイン構文は、特定ドメイン宛およびそのすべてのサブドメイン宛のすべての受信者をブロックするために使用されます。
10.1.28.12	IP アドレス IP アドレス構文は、特定 IP アドレス宛のすべての受信者をブロックするために使用されます。単一 IP アドレスで複数ドメインをホストしている場合に、この構文が便利です。構文は、一般的なドット区切りのオクテット IP アドレスです。

関連項目

- CLI を使用したグローバル配信停止へのアドレスの追加 （923 ページ）
- グローバル配信停止ファイルのエクスポートおよびインポート （925 ページ）

CLI を使用したグローバル配信停止へのアドレスの追加

この例では、アドレス `user@example.net` がグローバル配信停止リストに追加され、メッセージをハードバウンスするように機能が設定されます。このアドレスに送信されるメッセージはバウンスされます。電子メールゲートウェイにより配信の直前にメッセージがバウンスされます。

```
mail3.example.com> unsubscribe


Global Unsubscribe is enabled. Action: drop.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import entries from a file.
```

```
- SETUP - Configure general settings.
[]> new
Enter the unsubscribe key to add. Partial addresses such as
"@example.com" or "user@" are allowed, as are IP addresses. Partial hostnames such as
"@.example.com" are allowed.
[]> user@example.net
Email Address 'user@example.net' added.
Global Unsubscribe is enabled.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup
Do you want to enable the Global Unsubscribe feature? [Y]> y
Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2
Global Unsubscribe is enabled. Action: bounce.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>
```

```
mail3.example.com> commit

Please enter some comments describing your changes:

[]> Added username "user@example.net" to global unsubscribe

Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

グローバル配信停止ファイルのエクスポートおよびインポート

HAT、RAT、smtproutes、スタティック マスカレード テーブル、エイリアス テーブル、ドメイン マップ テーブル、altsrchost エントリと同様に、グローバル配信停止エントリはファイルをエクスポートおよびインポートして変更できます。

手順

ステップ 1 unsubscribe コマンドの export サブコマンドを使用して、既存のエントリをファイル（ファイル名は自分で指定）にエクスポートします。

ステップ 2 CLI の外部で、ファイルを取得します。（詳細については、FTP、SSH、および SCP アクセス（1573 ページ）を参照してください。）

ステップ 3 テキスト エディタを使用して、ファイルに新しいエントリを作成します。

ファイル内でエントリを区切るには、改行します。あらゆるオペレーティング システムの改行表現を使用できます（<CR>、<LF>、または<CR><LF>）。コメント行はナンバー記号（#）で始まり、無視されます。たとえば、次のファイルでは、単一の受信者電子メール アドレス（test@example.com）、特定ドメインのすべての受信者（@testdomain.com）、複数ドメインで同じ名前を持つすべてのユーザ（testuser@）、および特定 IP アドレスの任意の受信者（11.12.13.14）が除外されます。

```
# this is an example of the global_unsubscribe.txt file
test@example.com
@testdomain.com
testuser@
11.12.13.14
```

ステップ 4 ファイルを保存してインターフェイスの configuration ディレクトリに配置し、インポートできるようにします。（詳細については、FTP、SSH、および SCP アクセス（1573 ページ）を参照してください。）

ステップ 5 unsubscribe の import サブコマンドを使用して、編集したファイルをインポートします。

確認：電子メール パイプライン

次の表に、受信から配信へのルーティングまで、電子メールがシステムでルーティングされる様子の概要を示します。各機能は上から順に実行されます。ここでは簡単に説明します。「表：Cisco Secure Email Gateway の電子メールパイプライン：ルーティングおよび配信機能」の影付きの部分は、ワークキューで実行される処理を表します。

このパイプラインに含まれる機能の設定の大部分は、trace コマンドを使用してテストできます。詳細については、「トラブルシューティング」の章の「テストメッセージを使用したメール フローのデバッグ：トレース」を参照してください。

（注） 発信メールの場合は、アウトブレイク フィルタ ステージの後にデータ漏洩防止スキャニングが実行されます。

表 *65 : Cisco Secure Email Gateway* の電子メールパイプライン：電子メール受信機能

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

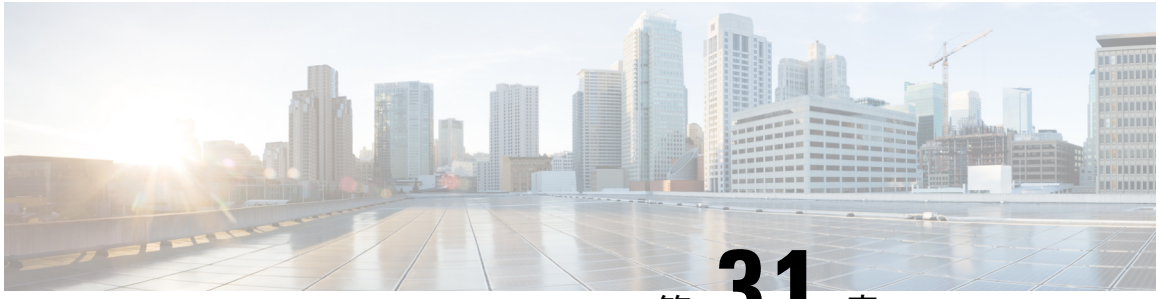
機能	説明
受信者アクセステーブル（RAT）	（パブリック リスナーのみ）RCPT TO およびカスタム SMTP 応答内の受信者の ACCEPT または REJECT。特別な受信者にスロットリングのバイパスを許可します。
エイリアス テーブル（Alias tables）	エンベロープ受信者を書き換えます。（システム全体を対象に設定。aliasconfig は、listenerconfig のサブコマンドではありません）
LDAP 受信者の受け入れ（LDAP Recipient Acceptance）	受信者受け入れの LDAP 検証は、SMTP カンバセーションで行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりにワーク キュー内で LDAP 検証を行うように設定することもできます。

表 *66 : E* メール セキュリティ アプライアンスの電子メール パイプライン：ルーティングおよび配信機能

ワーク キュー	**LDAP** 受信者の受け入れ		受信者受け入れのLDAP検証はワーク キュー内で行われます。受信者がLDAPディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりにSMTPカンバセーションLDAP検証を行うよう設定することもできます。
	マスカレード または **LDAP** マスカレード		マスカレードは、ワーク キューで行われます。マスカレードでは、スタティック テーブルを使用するかLDAP クエリーを使用して、エンベロープ送信者、To:、From:、CC: ヘッダーを書き換えます。
	LDAP ルーティング		LDAPクエリーは、メッセージルーティングまたはアドレス書き換えのために実行されます。グループLDAPクエリーは、メッセージ フィルタ ルール mail-from-group および rcpt-to-group と連携して動作します。
	メッセージ フィルタ（**Message Filters**）*		メッセージフィルタはメッセージの「分裂」よりも前に適用されます。* メッセージを隔離エリアに送信できます。
	アンチスパム**	受信者単位のスキャン（**Per Recipient Scanning**）	アンチスパム スキャン エンジンでは、メッセージを検査して、さらに処理するために判定を返します。
	アンチウイルス*		アンチウイルス スキャンでは、ウイルスを検出するためにメッセージを検査します。メッセージはスキャンされ、可能であれば、任意で修復されます。*メッセージを隔離エリアに送信できます。
	高度なマルウェア防御		高度なマルウェア防御は、添付ファイルからマルウェアを検出するために、ファイル レピュテーション スキャンとファイル分析を実行します。
	コンテンツ フィルタ*		コンテンツ フィルタが適用されます。* メッセージを隔離エリアに送信できます。
	アウトブレイク フィルタ*		アウトブレイク フィルタ機能を使用すると、ウイルス感染から保護できます。* メッセージを隔離エリアに送信できます。
	仮想ゲートウェイ		特定の IP インターフェイスまたは IP インターフェイスのグループを介してメールを送信します。
	配信制限（**Delivery limits**）		1. デフォルト配信インターフェイスを設定します。 2. アウトバウンド接続の合計最大数を設定します。

	ドメインベースの制限値（**Domain-based Limits**）		ドメイン単位で、各仮想ゲートウェイおよびシステム全体の最大アウトバウンド接続数、使用するバウンスプロファイル、配信用の TLS プレファレンス：no/preferred/required を定義します。
	ドメインベースのルーティング（**Domain-based routing**）		エンベロープ受信者を書き換えず、ドメインに基づいてメールをルーティングします。
	グローバル配信停止（**Global unsubscribe**）		特定のリストに従って受信者をドロップします（システム全体を対象に設定）。
	バウンス プロファイル（**Bounce profiles**）		配信不能メッセージの処理です。リスナー単位、送信先コントロールエントリ単位、およびメッセージフィルタ経由で設定可能です。

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



第 31 章

電子メールゲートウェイと Cisco Advanced Phishing Protection の統合

この章は、次の項で構成されています。

- Cisco Advanced Phishing Protection の概要 （931 ページ）
- 電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法 （933 ページ）
- Advanced Phishing Protection およびクラスタ （940 ページ）
- [高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ （940 ページ）
- Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング （941 ページ）
- Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの表示 （942 ページ）

Cisco Advanced Phishing Protection の概要

Cisco Advanced Phishing Protection は、ビジネスメール詐欺（BEC）とフィッシングの検出機能を提供します。高度な機械学習技術および追加されたインテリジェンスを駆使して、送信者アドレスのレピュテーションをチェックし、アイデンティティ詐欺による脅威を検出します。このインテリジェンスは継続的な適応機能を備え、送信者をリアルタイムで把握して、保護を強化します。

電子メールゲートウェイの高度なフィッシング防御エンジンは、組織に送信された過去の電子メールトラフィックに基づいて、すべての正当な送信者固有の動作を確認します。Cisco Advanced Phishing Protection のクラウドサービスインターフェイスは、悪意のある可能性があるメッセージを正常なメッセージと区別するためにリスク分析を実行します。

Cisco Advanced Phishing Protection クラウドサービスは、電子メールゲートウェイを組織への着信メッセージのメタデータのコピーを受信するためのセンサーエンジンとして使用します。このセンサーエンジンが、電子メールゲートウェイから送られるメッセージヘッダーなどのメタデータを収集し、それらを分析するために Cisco Advanced Phishing Protection クラウドサービスに中継します。分析後に、悪意のある可能性があるメッセージは、Advanced Phishing Protection

クラウドサービスで事前に設定したポリシーに基づいて、受信者のメールボックスから自動的に修復されます。

電子メールゲートウェイをセンサーエンジンとして使用できると、組織が次のことを行うときに役立ちます。

- 受信者のメールボックスのメッセージヘッダーで検出された脅威を特定、調査、および修復する。
- 組織内の複数の電子メールゲートウェイからメッセージのメタデータのレポートデータを表示する。

Cisco Advanced Phishing Protection の利点

電子メールゲートウェイに Cisco Advanced Phishing Protection を展開すると、次のような利点があります。

- センサーベースのソリューションを迅速に展開することで、ユーザを侵害による損害から完全に保護できます。
- 電子メール環境をより効果的に保護するための追加の防御層を提供します。
- BEC 攻撃を防御するため、送信者をリアルタイムで把握し、電子メールのアイデンティティと動作関係を学習して認証します。
- 受信者の受信トレイから悪意のある電子メールを自動的に削除し、アイデンティティ偽装の手法に関する注意を呼びかけ、アイデンティティ詐称やその他の高度な攻撃を防御します。
- 保護されたメッセージや防御された攻撃の総数など、電子メール攻撃のアクティビティを詳細に可視化します。
- 次の攻撃を防御します。
  - 侵害されたアカウントやソーシャルエンジニアリングを使用した攻撃。
  - フィッシング、ランサムウェア、ゼロデイ攻撃、スプーフィング。
  - 悪意のあるペイロードや URL がない BEC。

ワークフロー

1. Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのライセンスをアクティブ化します。
2. 電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスのセンサーエンジンとして設定します。これにより、クラウドまたはオンプレミス経由で電子メールゲートウェイが軽量センサーとして展開されます。

3. 電子メールゲートウェイのセンサーエンジンを Cisco Advanced Phishing Protection クラウドサービスに登録します。
4. 電子メールゲートウェイのセンサーエンジンは、正常と見なされたメッセージのメタデータを Cisco Advanced Phishing Protection クラウドサービスに転送します。
5. Cisco Advanced Phishing Protection クラウドサービスは、メッセージのメタデータが悪意のあるものかどうかを判断します。
6. Cisco Advanced Phishing Protection クラウドサービスで事前設定されたポリシーが「適用」センサーで設定されている場合、さらに詳細なインシデント調査のために、メッセージがブロックまたはリダイレクトされます。

電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法

次の手順を順番に実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	前提条件を確認します。	前提条件 （934 ページ）
ステップ 2	Cisco Advanced Phishing Protection クラウドサービスからプロビジョニングキーを取得します。	Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得 （934 ページ）
ステップ 3	電子メールゲートウェイをセンサーエンジンとして Cisco Advanced Phishing Protection クラウドサービスに登録します。	電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （935 ページ）
ステップ 4	電子メールゲートウェイで Advanced Phishing Protection を有効にします。	電子メールゲートウェイでの Advanced Phishing Protection の有効化 （936 ページ）
ステップ 5	Cisco Advanced Phishing Protection クラウドサービスから API アクセスキーを取得します。	Cisco Advanced Phishing Protection クラウドサービスからの API アクセスキーの取得 （937 ページ）
ステップ 6	メッセージメタデータの転送を有効にするための受信メールポリシーを設定します。	メッセージメタデータの転送を有効にするための受信メールポリシーの設定 （938 ページ）

	コマンドまたはアクション	目的
ステップ 7	Advanced Phishing Protection クラウドサービスに転送されたメッセージのメタデータをモニタします。	Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング （940 ページ）

前提条件

- Cisco Advanced Phishing Protection クラウドサービスのアカウントの利用 （934 ページ）
- Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール （934 ページ）

Cisco Advanced Phishing Protection クラウドサービスのアカウントの利用

次の内容について確認してください。

- URL https://www.cisco.com/c/en/us/buy.html から Cisco Advanced Phishing Protection クラウドサービスを利用するためのライセンスを取得していること。
- Cisco Advanced Phishing Protection クラウドサービスでプロビジョニングを行うため、電子メール通知で受信したアクティベーションリンクを使用して、アカウントがアクティブ化されていること。

Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール

組織の要件に従って、センサーエンジンとして電子メールゲートウェイを設定していることを確認します。詳細については、『*Cisco Advanced Phishing Protection* ユーザーガイド』を参照してください。

Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得

始める前に

管理者権限を使用して、Cisco Advanced Phishing Protection クラウドサービスにアクセスできることを確認します。詳細については、前提条件 （934 ページ）を参照してください。Cisco Advanced Phishing Protection クラウドサービスにアクセスできない場合は、Cisco TAC にお問い合わせください。

手順

ステップ 1 Cisco Advanced Phishing Protection クラウドサービスにログインします。

ステップ 2 [管理（Manage）] > [センサー（Sensors）] を選択します。

ステップ 3 [インストール（Installation）] > [センサーインストーラのダウンロード（Download Sensor Installer）] を選択します。

ステップ 4 ドロップダウンから、組織の要件に従って設定したセンサーのインストールスクリプトを選択します（例：Cisco SEG）。

詳細については、Cisco Advanced Phishing Protection クラウドサービスのセンサーのインストール （934 ページ）を参照してください。

ステップ 5 6 文字のプロビジョニングキーをコピーします。

このプロビジョニングキーを使用して、Cisco E メール セキュリティ ゲートウェイをセンサーとして設定します。

（注） 電子メールゲートウェイをセンサーとして登録するには、プロビジョニングキーを生成から 7 日以内に使用する必要があります。

次のタスク

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに登録します。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （935 ページ）を参照してください。

電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録

始める前に

次の内容について確認してください。

- 電子メールゲートウェイを Advanced Phishing Protection クラウドサービスに登録するための有効なプロビジョニングキーがあること。詳細については、Cisco Advanced Phishing Protection クラウドサービスからのプロビジョニングキーの取得 （934 ページ）を参照してください。
- Cisco Advanced Phishing Protection クラウドサービスで電子メールゲートウェイを登録するために必要なファイアウォールの HTTPS（In および Out）443 ポートが、FQDN に対して開放されていること。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [セキュリティサービス（Security Services）] > [高度なフィッシング防御（Advanced Phishing Protection）] に移動します。

ステップ 3 [Register] をクリックします。

ステップ 4 [URL] ドロップダウンから、Cisco Advanced Phishing Protection クラウドサービスのリージョンを選択します。

ステップ 5 Advanced Phishing Protection クラウドサービスから取得した 6 文字のプロビジョニングキーを入力します。

ステップ 6 [登録（Register）] をクリックして変更を送信します。

電子メールゲートウェイをセンサーに登録すると、Cisco Advanced Phishing Protection クラウドサービスで、汎用一意 ID（UUID）が生成されます。

（注） 登録に成功すると、Cisco Advanced Phishing Protection クラウドサービスでは、電子メールゲートウェイのクラウドサービスでのホスト名が識別されます。

次のタスク

電子メールゲートウェイで Cisco Advanced Phishing Protection エンジンを有効にします。詳細については、電子メールゲートウェイでの Advanced Phishing Protection の有効化 （936 ページ）を参照してください。

電子メールゲートウェイでの Advanced Phishing Protection の有効化

始める前に

Cisco Advanced Phishing Protection クラウドサービスで電子メールゲートウェイがセンサーとして登録されていることを確認します。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （935 ページ）を参照してください。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [セキュリティサービス（Security Services）] > [高度なフィッシング防御（Advanced Phishing Protection）] に移動します。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 変更を保存します。

次のタスク

Cisco Advanced Phishing Protection クラウドサービスへのメッセージメタデータの転送を有効にします。詳細については、メッセージメタデータの転送を有効にするための受信メールポリシーの設定 （938 ページ）を参照してください。

Cisco Advanced Phishing Protection クラウドサービスからの API アクセスキーの取得

API アクセスキーを使用して、E メールゲートウェイで次のタスクを実行できます。

- APP ライセンスの有効期限の詳細に関する電子メール通知アラートをユーザに送信します。
- 組織レベルですべての電子メールゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの合計数をダッシュボードウィジェットに表示します。ダッシュボードウィジェットは、新しい Web インターフェイスの [高度なフィッシング防御（Advanced Phishing Protection）] レポートページで使用できます。

始める前に

次の内容について確認してください。

- 電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスのセンサーとして登録されていること。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （935 ページ）を参照してください。
- 電子メールゲートウェイで Advanced Phishing Protection が有効になっていること。詳細については、電子メールゲートウェイでの Advanced Phishing Protection の有効化 （936 ページ）を参照してください。

手順

ステップ 1 Cisco Advanced Phishing Protection クラウドサービスにログインします。

ステップ 2 [管理（Manage）] > [ユーザー（Users）] を選択します。

ステップ 3 該当するユーザ名をクリックします。

ステップ 4 [APIシークレットの生成（Generate API Secret）] リンクをクリックして、API アクセスキーを生成します。

ステップ 5 **API アクセス UID** と **API アクセス秘密鍵**をシステムにローカルコピーします。

（注） API アクセスキーをコピーせずに Cisco Advanced Phishing Protection クラウドサービスを閉じる場合は、手順の **1～3** に従い、[APIシークレットの再生成（Regenerate API Secret）] リンクをクリックして新しい API アクセスキーを取得します。

ステップ 6 電子メールゲートウェイのレガシー Web インターフェイスにログインします。

ステップ 7 [セキュリティサービス（Security Services）] > [高度なフィッシング防御（Advanced Phishing Protection）] に移動します。

ステップ 8 [高度なフィッシング防御APIアクセス（Advanced Phishing Protection API Access）] セクションで [設定の編集（Edit Settings）] をクリックします。

ステップ 9 [APIアクセスUID（API Access UID）] フィールドに **API アクセス UID** キーを入力します。

ステップ 10 [APIアクセスキー（API Access key）] フィールドに **API アクセス秘密**鍵を入力します。

ステップ 11 [送信（Submit）] をクリックします。

次のタスク

Cisco Advanced Phishing Protection クラウドサービスへのメッセージメタデータの転送を有効にします。詳細については、メッセージメタデータの転送を有効にするための受信メールポリシーの設定 （938 ページ）を参照してください。

メッセージメタデータの転送を有効にするための受信メールポリシーの設定

メッセージのメタデータが Cisco Advanced Phishing Protection クラウドサービスに転送されるようにメールポリシーを設定できます。

電子メールゲートウェイで Cisco Advanced Phishing Protection クラウドサービスを有効にすると、次のメッセージヘッダーが Cisco Advanced Phishing Protection クラウドサービスと共有されます。

- Authentication-Results
- Authentication-Results-original
- DMARC-result
- DKIM-domain
- DKIM-result
- DKIM-selector
- DKIM-signatures
- From-header
- Full-Header-From
- HELO_domain
- Last-Hop-IP-Address
- List-ID
- Mail-From
- Mailing-list
- Message-ID
- Rcpt-To
- Received-Header
- Received-SPF

- Received-Timestamps
- Reply-To
- SPF-result
- Subject-header
- To-header
- Originator-Return-Address
- X-Mailer
- X-Original-Authentication-Results
- X-Original-From
- X-Original-To
- X-Original-Sender
- X-Originating-IP
- X-OriginatorOrg
- X-Received

始める前に

次の内容について確認してください。

- 電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスのセンサーとして登録されていること。詳細については、電子メールゲートウェイでの Cisco Advanced Phishing Protection センサーの登録 （935 ページ）を参照してください。
- 電子メールゲートウェイで Advanced Phishing Protection が有効になっていること。詳細については、電子メールゲートウェイでの Advanced Phishing Protection の有効化 （936 ページ）を参照してください。

手順

ステップ 1 E メール セキュリティ ゲートウェイにログインします。

ステップ 2 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] に移動します。

ステップ 3 APP フィルタの下にあるリンクをクリックします。

ステップ 4 ドロップダウンリストから [Advanced Phishing Protectionの有効化（設定のカスタマイズ）（Enable Advanced Phishing Protection (Customize Settings)）] を選択します。

ステップ 5 [転送の有効化（Enable Forwarding）] チェックボックスをオンにします。

ステップ 6 [送信（Submit）] をクリックし、変更をコミットします。

Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング

E メール セキュリティ ゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに転送されたメッセージのメタデータをモニタできます。クラウドサービスの[分析（Analyze）] > [メッセージ（Messages）] ページには、メッセージの送信元、およびメッセージと送信者に関連するリスク情報が表示されます。

Cisco Advanced Phishing Protection クラウドサービスのメッセージメタデータは、以下に基づいてレピュテーションスコアが付けられます。

- メッセージの信頼性
- ドメインのレピュテーション
- 送信者の正当性

Advanced Phishing Protection およびクラスタ

中央管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで Advanced Phishing Protection を有効にできます。Cisco Advanced Phishing Protection クラウドサービスに電子メールゲートウェイをスタンドアロンモードで登録している場合は、Cisco Advanced Phishing Protection クラウドサービスに登録されているクラスタへの参加を選択できます。

（注） マシンレベルで Advanced Phishing Protection を無効にすると、グループレベルとクラスタレベルでも無効になります。

[高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ

[モニタ（Monitor）] > [高度なフィッシング防御（Advanced Phishing Protection] レポートページには、次の情報が表示されます。

- Cisco Advanced Phishing Protection クラウドサービスに正常に転送されたメッセージの合計数。
- Cisco Advanced Phishing Protection クラウドサービスに転送されなかったメッセージの合計数。

（注） メッセージメタデータの転送に失敗した場合は、高度なフィッシング防御機能の設定を検証する必要があります。詳細については、電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法 （933 ページ）を参照してください。

[高度なフィッシングからの保護（Advanced Phishing Protection）] レポートページを使用すると、次の情報を確認できます。

- Cisco Advanced Phishing Protection クラウドサービスへの転送を試行したメッセージの総数（グラフィック形式）
- Cisco Advanced Phishing Protection クラウドサービスへ転送されたメッセージの概要（グラフィック形式）

Cisco Advanced Phishing Protection クラウドサービスに転送されるメッセージのメタデータの詳細情報を表示するには、リンクをクリックして Cisco Advanced Phishing Protection クラウドサービスにログインします。詳細については、Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング （940 ページ）を参照してください。

Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング

E メール セキュリティ ゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに転送されたメッセージのメタデータをモニタできます。クラウドサービスの[分析（Analyze）] > [メッセージ（Messages）] ページには、メッセージの送信元、およびメッセージと送信者に関連するリスク情報が表示されます。

Cisco Advanced Phishing Protection クラウドサービスのメッセージメタデータは、以下に基づいてレピュテーションスコアが付けられます。

- メッセージの信頼性
- ドメインのレピュテーション
- 送信者の正当性

Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの表示

Cisco Advanced Phishing Protection クラウドサービスに転送するメッセージのメタデータを成功と失敗に応じて表示できます。

始める前に

E メール ゲートウェイでメッセージ トラッキング機能が有効にされていることを確認します。メッセージ トラッキングを有効にするには、Web インターフェイスで [セキュリティサービス（Security Services）] > [集中管理サービス（Centralized Services）] > [メッセージトラッキング（Message Tracking）] ページに移動します。

手順

ステップ 1 E メール セキュリティ ゲートウェイにログインします。

ステップ 2 [モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] に移動します。

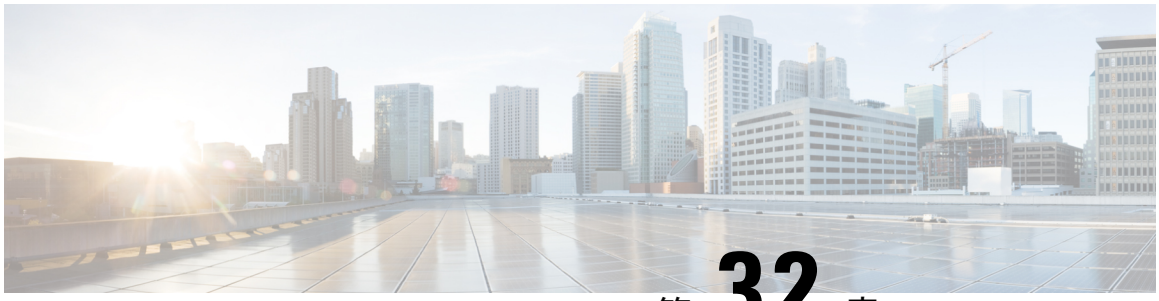
ステップ 3 [詳細設定（Advanced）] をクリックします。

ステップ 4 [メッセージイベント（Message Event）] の [Advanced Phishing Protectionに転送（Advanced Phishing Protection Forwarding）] チェックボックスをオンにします。

ステップ 5 （オプション）Cisco Advanced Phishing Protection クラウドサービスに正常に転送されたメッセージを表示するには、[成功（Successful）] を選択します。

ステップ 6 （オプション）Cisco Advanced Phishing Protection クラウドサービスへの転送に失敗したメッセージを表示するには、[失敗（Failed）] を選択します。

ステップ 7 **[検索（Search）]** をクリックします。



第 32 章

LDAP クエリ

この章は、次の項で構成されています。

- LDAP クエリの概要 （943 ページ）
- LDAP クエリに関する作業 （955 ページ）
- 受信者検証で受け入れクエリを使用する （963 ページ）
- 複数ターゲットアドレスへのメール送信にルーティング クエリを使用する （965 ページ）
- エンベロープ送信者を書き換えるためのマスカレード クエリの使用 （966 ページ）
- 受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （968 ページ）
- 特定のドメインへルーティングするためのドメイン ベース クエリの使用 （972 ページ）
- 一連の LDAP クエリを実行するためのチェーン クエリの使用 （974 ページ）
- LDAP によるディレクトリ ハーベスト攻撃防止 （976 ページ）
- SMTP 認証を行うための AsyncOS の設定 （979 ページ）
- ユーザの外部 LDAP 認証の設定 （988 ページ）
- スパム隔離機能へのエンド ユーザ認証 （991 ページ）
- スパム隔離のエイリアス統合クエリ （993 ページ）
- ユーザ識別名の設定の例 （995 ページ）
- AsyncOS を複数の LDAP サーバと連携させるための設定 （995 ページ）
- サーバとクエリのテスト （996 ページ）

LDAP クエリの概要

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリ（Microsoft Active Directory、SunONE Directory Server、OpenLDAP などのディレクトリ）に格納されている場合は、メッセージの受け入れ、ルーティング、および認証のために LDAP サーバに対してクエリを実行するように電子メールゲートウェイを設定できます。 電子メールゲートウェイは、1 つまたは複数の LDAP サーバと連携させるように設定できます。

ここでは、実行できる LDAP クエリのタイプと、LDAP と電子メールゲートウェイとが連携してメッセージの認証、受け入れ、ルーティングを行う仕組み、および LDAP と連携するように電子メールゲートウェイを設定する方法について概説します。

関連項目

- LDAP クエリについて （944 ページ）
- LDAP と AsyncOS との連携の仕組み （945 ページ）
- 電子メールゲートウェイを LDAP サーバと連携させるための設定 （946 ページ）
- LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （947 ページ）
- LDAP サーバのテスト （950 ページ）
- 特定のリスナーで実行する LDAP クエリの有効化 （950 ページ）
- Microsoft Exchange 5.5 に対する拡張サポート （953 ページ）

LDAP クエリについて

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリに格納されている場合は、次の目的で LDAP サーバに対してクエリを実行するように 電子メールゲートウェイを設定できます。

- **受け入れクエリ**。既存のLDAPインフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メール アドレスの扱い方を定義できます。詳細については、受信者検証で受け入れクエリを使用する （963 ページ）を参照してください。
- **ルーティング（エイリアシング）**。ネットワーク内のLDAPディレクトリに格納されている情報に基づいてメッセージを適切なアドレスやメールホストへルーティングするように、 電子メールゲートウェイを設定できます。詳細については、複数ターゲット アドレスへのメール送信にルーティング クエリを使用する （965 ページ）を参照してください。
- **証明書認証**。ユーザのメールクライアントと電子メールゲートウェイ間のSMTPセッションを認証するためのクライアント証明書の有効性を確認するクエリを作成できます。詳細については、クライアント証明書の有効性の確認 （1001 ページ）を参照してください。
- **マスカレード**。発信メールの場合はエンベロープ送信者、着信メールの場合はメッセージ ヘッダー（To:、Reply To:、From:、CC:など）をマスカレードできます。マスカレードの詳細については、エンベロープ送信者を書き換えるためのマスカレード クエリの使用 （966 ページ）を参照してください。
- **グループ クエリ**。LDAP ディレクトリ内のグループに基づいてメッセージに対するアクションを実行するように電子メールゲートウェイを設定できます。このように設定するには、グループ クエリとメッセージ フィルタとを関連付けます。定義済みの LDAP グループに一致するメッセージに対しては、メッセージ フィルタに使用できる任意のメッセージ アクションを実行できます。詳細については、受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （968 ページ）を参照してください。
- **ドメインベース クエリ**。ドメインベースクエリを作成すると、 電子メールゲートウェイは同じリスナー上でドメインごとに異なるクエリを実行できます。電子メールゲートウェイがドメインベースクエリを実行するときは、どのクエリを使用するかをドメインに基づいて決定し、そのドメインに関連付けられているLDAPサーバに対してクエリを実行します。
- **チェーン クエリ**。チェーンクエリを作成すると、 電子メールゲートウェイに一連のクエリを順番に実行させることができます。チェーンクエリが設定済みのときは、電子メールゲートウェイでシーケンス内のクエリを 1 つずつ実行し、LDAP アプライアンスから肯定的な結果が返されると実行を停止します。チェーンルーティング クエリーでは、電子メー

ルゲートウェイが書き換えられた電子メールアドレスごとに、同じ設定の一連のチェーンクエリーを再実行します。

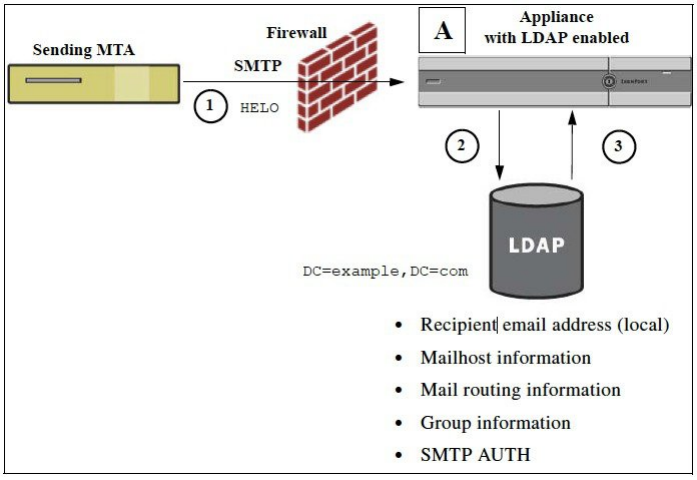
- **ディレクトリ ハーベスト防止**。LDAPディレクトリを使用したディレクトリハーベスト攻撃を防ぐように 電子メールゲートウェイを設定できます。ディレクトリ ハーベスト防止は、SMTPカンバセーション中に行うことも、ワークキューの中で行うこともできます。受信者がLDAPディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。その結果、スパム送信者はメールアドレスが有効なものかどうかを区別できなくなります。LDAPによるディレクトリ ハーベスト攻撃防止 （976 ページ）を参照してください。
- **SMTP 認証**。AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。この機能を利用すると、ユーザはリモート接続するとき（たとえば自宅や出張先にいる場合）でも、メール サーバを使用してメールを送信できるようになります。詳細については、SMTP 認証を行うための AsyncOS の設定 （979 ページ）を参照してください。
- **外部認証**。 電子メールゲートウェイにログインするユーザの認証を LDAP ディレクトリを使用して行うように電子メールゲートウェイを設定できます。詳細については、ユーザの外部 LDAP 認証の設定 （988 ページ）を参照してください。
- **スパム検疫エンドユーザ認証**。エンドユーザ隔離画面にログインするユーザを検証するように、電子メールゲートウェイを設定できます。詳細については、スパム隔離機能へのエンド ユーザ認証 （991 ページ）を参照してください。
- **スパム検疫エイリアス統合**。スパムに関する電子メール通知を使用する場合、このクエリを使用してエンドユーザのエイリアスを統合すると、エンドユーザがエイリアスのメールアドレスごとに隔離通知を受け取ることはなくなります。詳細については、スパム隔離のエイリアス統合クエリ （993 ページ）を参照してください。

LDAP と AsyncOS との連携の仕組み

LDAPディレクトリと電子メールゲートウェイとを連携させると、受信者受け入れ、メッセージルーティング、およびヘッダーマスカレードにLDAPディレクトリサーバを使用できます。LDAP グループクエリをメッセージフィルタと併用すると、メッセージが 電子メールゲートウェイで受信されたときの取り扱いに関するルールを作成できます。

次の図は、 電子メールゲートウェイが LDAP とどのように連携するかを示しています。

図 *58 : LDAP* 設定



1. 送信側 MTA からパブリック リスナー「A」に SMTP 経由でメッセージが送信されます。
2. 電子メールゲートウェイは、LDAP サーバに対してクエリを実行します。この LDAP サーバは [システム管理（System Administration）] > [LDAP] ページ（またはグローバル **ldapconfig** コマンド）で定義されます。
3. データが LDAP ディレクトリから受信されます。リスナーで使用するように [システム管理（System Administration）] > [LDAP] ページ（または **ldapconfig** コマンド）で定義されたクエリに応じて、次の処理が実行されます。
   - メッセージを新しい受信者アドレスにルーティングするか、ドロップまたはバウンスする
   - メッセージを新しい受信者のメールホストにルーティングする
   - メッセージ ヘッダー From:、To:、CC: をクエリに基づいて書き換える
   - メッセージ フィルタ ルール **rcpt-to-group** または **mail-from-group** で定義された、それ以降のアクション（グループ クエリと組み合わせて使用）。

（注） 複数の LDAP サーバに接続するように 電子メールゲートウェイを設定できます。その場合、複数の LDAP サーバを使用して、ロード バランシングやフェールオーバーを行うように LDAP プロファイルを設定できます。複数の LDAP サーバと連携させる方法の詳細については、AsyncOS を複数の LDAP サーバと連携させるための設定（995 ページ）を参照してください。

電子メールゲートウェイを LDAP サーバと連携させるための設定

受け入れ、ルーティング、エイリアシング、およびマスカレードのために 電子メールゲートウェイを LDAP ディレクトリと連携させるには、以下の手順に従って AsyncOS 電子メールゲートウェイを設定する必要があります。

手順

ステップ 1 **LDAP サーバ プロファイルを設定します。**サーバ プロファイルに、AsyncOS から LDAP サーバに接続するための次の情報を設定します。

- クエリ送信先となるサーバの名前とポート
- ベース DN
- サーバとのバインドのための認証要件

サーバプロファイルの設定方法の詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （947 ページ） を参照してください。

LDAP サーバ プロファイルを設定するときに、AsyncOS からの接続先となる LDAP サーバを 1 つまたは複数設定できます。

AsyncOS から複数のサーバに接続するように設定する方法については、AsyncOS を複数の LDAP サーバと連携させるための設定 （995 ページ）を参照してください。

ステップ 2 **LDAP クエリを設定します。**LDAP クエリは、LDAP サーバ プロファイルで設定します。ここで設定するクエリは、実際に使用する LDAP の実装とスキーマに合わせて調整してください。

作成できる LDAP クエリのタイプについては、LDAP クエリについて （944 ページ）を参照してください。

クエリの記述方法については、LDAP クエリに関する作業 （955 ページ）を参照してください。

ステップ 3 **LDAP サーバ プロファイルをパブリック リスナーまたはプライベート リスナーに対してイネーブルにします。**LDAP サーバプロファイルをリスナーに対してイネーブルにすると、そのリスナーによって、メッセージの受け入れ、ルーティング、または送信の際に LDAP クエリが実行されるようになります。

詳細については、特定のリスナーで実行する LDAP クエリの有効化 （950 ページ）を参照してください。

（注） グループ クエリを設定するときは、AsyncOS と LDAP サーバとを連携させるためにさらに設定作業が必要です。グループ クエリの設定方法については、受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （968 ページ）を参照してください。エンドユーザ認証またはスパム通知統合のクエリを設定するときは、スパム隔離機能への LDAP エンドユーザ アクセスをイネーブルにする必要があります。スパム隔離の詳細については、「スパム隔離」の章を参照してください。

LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定するには、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルを作成します。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページの [LDAPサーバプロファイルを追加（Add LDAP Server Profile）] をクリックします。

ステップ 2 サーバ プロファイルの名前を入力します。

ステップ 3 LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロードバランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、AsyncOS を複数の LDAP サーバと連携させるための設定（995 ページ）を参照してください。

ステップ 4 認証方法を選択します。匿名認証を使用することも、ユーザ名とパスフレーズを指定することもできます。

ステップ 5 LDAP サーバのタイプを、[Active Directory]、[OpenLDAP]、[不明またはそれ以外（Unknown or Other）] から選択します。

ステップ 6 ポート番号を入力します。

Active Directory または不明/その他のサーバ タイプの場合、デフォルトのポートは、SSL なしが 3268、SSL ありが 3269 です。

Open LDAP サーバ タイプの場合、デフォルトのポートは、SSL なしが 389、SSL ありが 636 です。

ステップ 7 LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスフレーズを使用して認証する場合は、パスフレーズが格納されているエントリへの完全DNがユーザ名に含まれている必要があります。たとえば、マーケティング グループに属しているユーザの電子メール アドレスが joe@example.com であるとします。このユーザのエントリは、次のようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```

ステップ 8 LDAP サーバとの通信に SSL を使用するかどうかを選択します。

（注） （オプション - [LDAPグローバル設定（LDAP Global Settings）] ページで [LDAPサーバ証明書の検証（Validate LDAP Server Certificate）] オプションが選択され、[SSL構成時の設定（SSL Configuration settings）] ページで FQDN 検証が有効になっている場合のみ）：サーバ証明書にある [共通名（Common Name）]、[SAN：DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式かどうかを確認します。

（注） （オプション - [LDAPグローバル設定（LDAP Global Settings）] ページで [LDAPサーバ証明書の検証（Validate LDAP Server Certificate）] オプションが選択され、[SSL構成時の設定（SSL Configuration settings）] ページで X 509 検証が有効になっている場合のみ）：サーバ証明書の署名アルゴリズムを確認します。

ステップ 9 [詳細（Advanced）] で、キャッシュの存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。

ステップ 10 保持するキャッシュ エントリの最大数を入力します。

（注） このキャッシュは、LDAP サーバごとに保持されます。複数の LDAP サーバを設定する場合は、パフォーマンスを向上させるために、LDAP キャッシュの値を小さく設定する必要があります。また、電子メールゲートウェイでのさまざまなプロセスのメモリ使用率が高い場合、この値を大きくすると、システムのパフォーマンスが低下する可能性があります。

ステップ 11 同時接続の数を入力します。

- ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロードバランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。

  （注） 同時接続の最大数には、LDAP クエリーに使用される LDAP 接続も含まれます。ただし、スパム隔離機能に対して LDAP 認証を使用する場合は、これよりも多くの接続が開かれることがあります。

- 接続がリセットされる前に LDAP サーバへの接続を維持する必要がある最大時間（秒単位）を設定できます。60 ～ 86400 の間の値を選択します。

ステップ 12 サーバへの接続をテストするために、[テストサーバ（Test Server(s)）] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。詳細については、LDAP サーバのテスト （950 ページ）を参照してください。

ステップ 13 クエリを作成します。該当するチェックボックスをオンにして、フィールドに入力します。選択できるのは、[承認（Accept）]、[ルーティング（Routing）]、[マスカレード（Masquerade）]、[グループ（Group）]、[SMTP認証（SMTP Authentication）]、[外部認証（External Authentication）]、[スパム隔離エンドユーザ認証（Spam Quarantine End-User Authentication）]、[スパム隔離エイリアス統合（Spam Quarantine Alias Consolidation）] です。

（注） メッセージを受信または送信するときに 電子メールゲートウェイが LDAP クエリを実行できるようにするには、該当するリスナーに対して LDAP クエリをイネーブルにする必要があります。詳細については、特定のリスナーで実行する LDAP クエリの有効化 （950 ページ）を参照してください。

ステップ 14 クエリをテストするために、[クエリのテスト（Test Query）] ボタンをクリックします。

テスト パラメータを入力して [テストの実行（Run Test）] をクリックします。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新（Update）] をクリックします。詳細については、LDAP サーバのテスト （950 ページ）を参照してください。

（注） 空パスフレーズでのバインドを許可するように LDAP サーバが設定されている場合は、パスフレーズ フィールドが空でもクエリのテストは合格となります。

ステップ 15 変更を送信し、保存します。

（注） サーバ設定の数に制限はありませんが、設定できるクエリは、サーバ1台につき受信者受け入れ1つ、ルーティング1つ、マスカレード1つ、グループ クエリ1つのみです。

LDAP サーバのテスト

[LDAP サーバプロファイルの追加/編集（Add/Edit LDAP Server Profile）] ページの [テストサーバ（Test Server(s)）] ボタン（または CLI の ldapconfig コマンドの test サブコマンド）を使用して、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバが設定されている場合は、各サーバのテストが実行されて、結果が個別に表示されます。

特定のリスナーで実行する LDAP クエリの有効化

メッセージを受信または送信するときに 電子メールゲートウェイが LDAP クエリを実行できるようにするには、該当するリスナーに対して LDAP クエリをイネーブルにする必要があります。

関連項目

- LDAP クエリのグローバル設定の構成 （950 ページ）
- LDAP サーバ プロファイル作成の例 （951 ページ）
- パブリック リスナー上の LDAP クエリの有効化 （952 ページ）
- プライベート リスナーでの LDAP クエリのイネーブル化 （952 ページ）

LDAP クエリのグローバル設定の構成

LDAP グローバル設定では、すべての LDAP トラフィックを電子メールゲートウェイでどのように処理するかを定義します。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページの [設定を編集（Edit Settings）] をクリックします。

ステップ 2 LDAP トラフィックに使用する IP インターフェイスを選択します。 電子メールゲートウェイでインターフェイスの 1 つが自動的にデフォルトとして選択されます。

ステップ 3 LDAP インターフェイスに使用する TLS 証明書を選択します（[ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の **certconfig** コマンドを使用して追加された TLS 証明書。他の MTA との暗号化通信の概要 （829 ページ）を参照してください）。

ステップ 4 LDAP サーバ証明書を検証する場合は、適切なオプションを選択します。

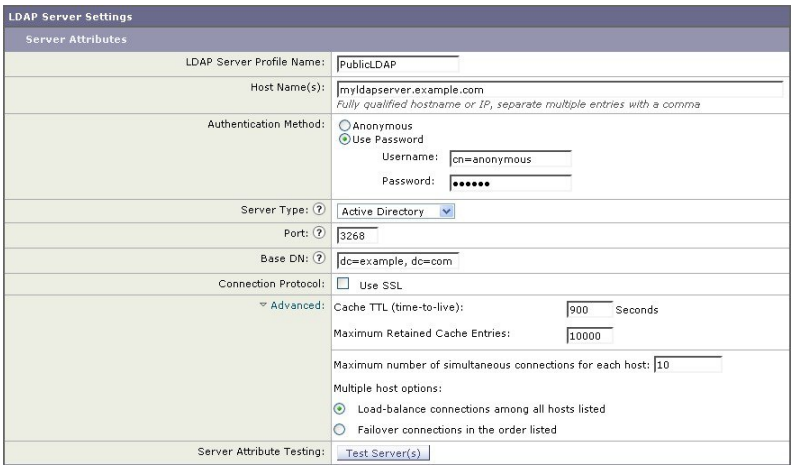
ステップ 5 変更を送信し、保存します。

LDAP サーバ プロファイル作成の例

次に示す例では、[システム管理（System Administration）]>[LDAP] ページを使用して電子メールゲートウェイのバインド先となる LDAP サーバを定義し、受信者を受け入れ、ルーティング、およびマスカレードのクエリを設定します。

（注） LDAP 接続試行のタイムアウトは 60 秒です。この時間には、DNS ルックアップと接続そのものに加えて、 電子メールゲートウェイ自体の認証バインド（該当する場合）も含まれます。初回の失敗後は、同じサーバ内の別のホストに対する試行がただちに行われます（2 つ以上のホストをカンマ区切りリストで指定した場合）。サーバ内にホストが 1 つしかない場合は、そのホストへの接続が繰り返し試行されます。

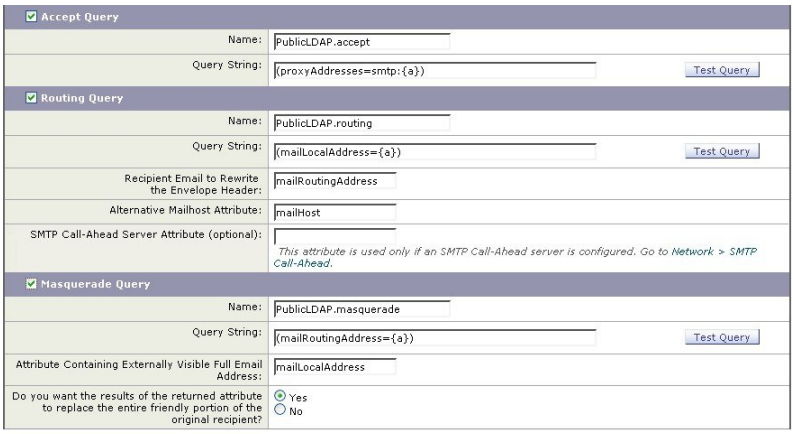
図 *59 : LDAP* サーバ プロファイルの設定（*1/2*）



初めに、「PublicLDAP」というニックネームを myldapserver.example.com LDAP サーバに与えます。接続数は 10（デフォルト値）に設定されており、複数 LDAP サーバ（ホスト）のロード バランス オプションはデフォルトのままとなっています。ここで複数のホストの名前を、カンマ区切りのリストとして指定できます。クエリの送信先は、ポート 3268（デフォルト値）です。SSL は、このホストの接続プロトコルとしてはイネーブルになっていません。example.com のベース DN が定義されています（dc=example,dc=com）。キャッシュの存続可能時間は 900 秒、キャッシュ エントリの最大数は 10000 に設定されています。認証方式は、パスフレーズ認証に設定されています。

受信者受け入れ、メール ルーティング、およびマスカレードのクエリが定義されています。クエリー名では、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一致している必要があります。

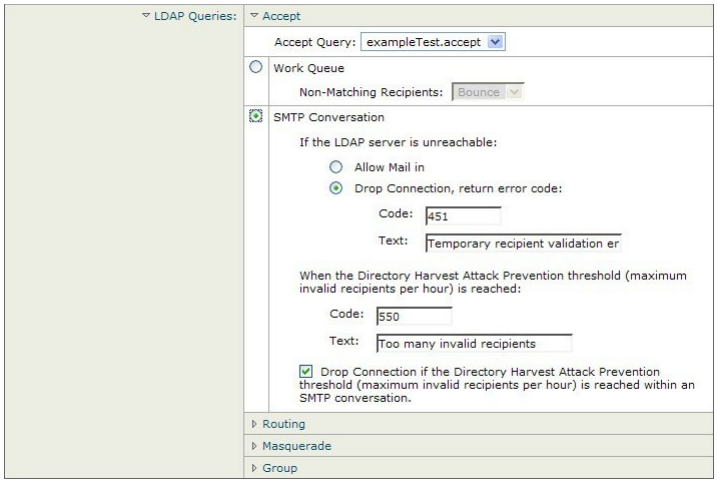
図 *60 : LDAP* サーバ プロファイルの設定（*2/2*）



パブリック リスナー上の LDAP クエリの有効化

この例では、受信者受け入れに対して LDAP クエリを使用するように、パブリック リスナー「InboundMail」を更新します。さらに、受信者受け入れの判定を SMTP カンバセーション中に行うように設定します（詳細については、受信者検証で受け入れクエリを使用する （963 ページ）を参照してください）。

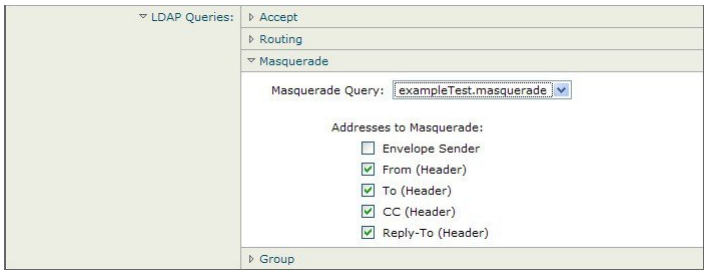
図 *61 :* リスナーでの受け入れとルーティングのクエリのイネーブル化



プライベート リスナーでの LDAP クエリのイネーブル化

この例では、LDAP クエリを使用してマスカレードを行うように、プライベート リスナー「OutboundMail」を更新します。マスカレード対象のフィールドには、From、To、CC、Reply-To があります。

図 *62 :* リスナーでのマスカレード クエリのイネーブル化



Microsoft Exchange 5.5 に対する拡張サポート

AsyncOS には、Microsoft Exchange 5.5 をサポートするための設定オプションがあります。これよりも新しいバージョンの Microsoft Exchange を使用する場合は、このオプションをイネーブルにする必要はありません。LDAP サーバを設定するときに、Microsoft Exchange 5.5 サポートをイネーブルにするかどうかを選択できます。選択するには、CLI を使用する必要があります。次に示すように、`ldapconfig -> edit -> server -> compatibility` サブコマンドを実行して、質問に「y」と答えます。

```
mail3.example.com> ldapconfig

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.

- DELETE - Remove a server configuration.


[]> edit

Enter the name or number of the server configuration you wish to edit.

[]> 1

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Choose the operation you want to perform:

- SERVER - Change the server for the query.

- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
```

```
- LDAPROUTING - Configure message routing.

- MASQUERADE - Configure domain masquerading.

- LDAPGROUP - Configure whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure SMTP authentication.

[]> server

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com


Microsoft Exchange 5.5 Compatibility Mode: Disabled

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)


[N]> y

Do you want to configure advanced LDAP compatibility settings? (Typically not required)

[N]>

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.
```

```
- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

LDAP クエリに関する作業

LDAP サーバ プロファイル内に、実行したい LDAP クエリのタイプごとに 1 つのエントリを作成します。LDAP クエリを作成するときは、実際に使用する LDAP サーバのクエリ構文で入力する必要があります。作成するクエリーは、実際に使用する LDAP ディレクトリ サービスの実装に合わせて調整が必要であることに注意してください。特に、組織固有のニーズを満たすように新しいオブジェクト クラスや属性がディレクトリに追加されている場合です。

関連項目

- LDAP クエリのタイプ （955 ページ）
- ベース識別名（DN） （956 ページ）
- LDAP クエリの構文 （956 ページ）
- セキュア LDAP（SSL） （957 ページ）
- ルーティング クエリー （957 ページ）
- LDAP サーバへの匿名のバインドをクライアントに許可する （957 ページ）
- LDAP クエリのテスト （961 ページ）
- LDAP サーバへの接続のトラブルシューティング （963 ページ）

LDAP クエリのタイプ

- **受け入れクエリ**。詳細については、受信者検証で受け入れクエリを使用する （963ページ）を参照してください。
- **ルーティング クエリ**。詳細については、複数ターゲット アドレスへのメール送信にルーティング クエリを使用する （965 ページ）を参照してください。
- **証明書認証クエリ**。詳細については、クライアント証明書の有効性の確認 （1001ページ）を参照してください。
- **マスカレード クエリ**。詳細については、エンベロープ送信者を書き換えるためのマスカレード クエリの使用 （966 ページ）を参照してください。
- **グループ クエリ**。詳細については、受信者がグループ メンバーであるかどうかを判別するグループ LDAP クエリの使用 （968 ページ）を参照してください。
- **ドメインベース クエリ**。詳細については、特定のドメインへルーティングするためのドメイン ベース クエリの使用 （972 ページ）を参照してください。
- **チェーン クエリ**。詳細については、一連の LDAP クエリを実行するためのチェーン クエリの使用 （974 ページ）を参照してください。

次の目的のためにクエリを設定することもできます。

- **ディレクトリ ハーベスト防止**。詳細については、LDAP クエリについて （944 ページ）を参照してください。
- **SMTP 認証**。詳細については、SMTP 認証を行うための AsyncOS の設定 （979 ページ）を参照してください。
- **外部認証**。詳細については、ユーザの外部 LDAP 認証の設定 （988 ページ）を参照してください。
- **スパム隔離エンドユーザ認証クエリー**。詳細については、スパム隔離機能へのエンドユーザ認証 （991 ページ）を参照してください。
- **スパム隔離エイリアス統合クエリー**。詳細については、スパム隔離のエイリアス統合クエリ （993 ページ）を参照してください。

指定した検索クエリは、システム上で設定済みのすべてのリスナーに使用できます。

ベース識別名（DN）

ディレクトリのルート レベルを「ベース」と呼びます。ベースの名前は DN（Distinguishing Name）です。Active Directory（および RFC 2247 に基づく標準）のベース DN のフォーマットでは、DNS ドメインがドメイン コンポーネント（dc=）に変換されます。たとえば、example.com のベース DN は「dc=example, dc=com」です。DNS 名の各部分が順番に表現されることに注意してください。これには、実際の LDAP 設定が反映されることも、されないこともあります。

実際に使用するディレクトリに複数のドメインが含まれている場合は、クエリの対象のベースを 1 つだけ入力するのでは不都合であることもあります。そのような場合は、LDAP サーバ設定を指定するときに、ベースを「NONE」に設定します。ただし、このように設定すると検索の効率が低下します。

LDAP クエリの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

Cn=First Last,oU=user,dc=domain,DC=COM

クエリに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリは、**maillocaladdress** と入力したときとは異なります。

関連項目

- トークン: （956 ページ）

トークン:

次のトークンを LDAP クエリ内で使用できます。

- {a} ユーザ名@ドメイン名
- {d} ドメイン名

- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAIL FROM: アドレス

（注） {f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリは、次のようになります。

(|(mail={a})(proxyAddresses=smtp:{a}))

（注） 作成したクエリは、[LDAP] ページの [テスト（Test）] 機能（または **ldapconfig** コマンドの **test** サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、LDAP クエリのテスト （961 ページ）を参照してください。

セキュア LDAP（SSL）

AsyncOS と LDAP サーバとの通信に SSL を使用するように設定できます。SSL を使用するように LDAP サーバ プロファイルを設定した場合の動作は次のようになります。

- AsyncOS は、CLI の certconfig で設定された LDAPS 証明書を使用します（自己署名証明書の作成 （833 ページ）を参照）。

  LDAP サーバによっては、LDAPS 証明書の使用をサポートするように設定する作業が必要になります。

- 設定済みの LDAPS 証明書がない場合は、デモ証明書が使用されます。

ルーティング クエリー

LDAP ルーティング クエリの再帰の制限はありません。ルーティングは完全にデータ ドリブンで行われます。ただし、AsyncOS には、ルーティングの永久ループを防止するために循環参照の有無を調べる機能があります。

LDAP サーバへの匿名のバインドをクライアントに許可する

匿名クエリを許可するように LDAP ディレクトリ サーバを設定することが必要になる場合があります。（匿名クエリを許可すると、クライアントが匿名でサーバにバインドしてクエリを実行できるようになります。）匿名クエリを許可するように Active Directory を設定する具体的

な手順については、Microsoft サポート技術情報 320528 を参照してください。URL は次のとおりです。

```
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528
```

または、認証とクエリ実行専用のユーザを 1 つ用意します。このようにすれば、任意のクライアントから匿名クエリを受け付けるように LDAP ディレクトリ サーバを開放する必要はありません。

ここでは、次の手順について説明します。

- 「匿名」認証を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- 「匿名バインド」を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- AsyncOS が LDAP データを Microsoft Exchange 2000 サーバから「匿名バインド」と「匿名」認証の両方を使用して取得するようにセットアップする方法。

ユーザ電子メールアドレスを問い合わせるという目的で「匿名」または「匿名バインド」認証を許可するには、Microsoft Exchange 2000 サーバに対して特定のアクセス許可を設定する必要があります。このような設定が非常に役立つのは、SMTP ゲートウェイに対する着信メール メッセージの有効性を検証するために LDAP クエリを使用する場合です。

関連項目

- 匿名認証のセットアップ （958 ページ）
- Active Directory の匿名バインドのセットアップ （959 ページ）
- Active Directory の実装に関する注意 （961 ページ）

匿名認証のセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する未認証のクエリで特定のデータを使用できるようになります。Active Directory への「匿名バインド」を許可する手順については、Active Directory の匿名バインドのセットアップ （959 ページ）を参照してください。

手順

ステップ 1 必要となる Active Directory アクセス許可を確認します。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリの対象であるユーザが属している OU および CN オブジェクトのすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザー オブジェクト	権限	継承	アクセス許可のタイプ
全員	内容の一覧表示	コンテナ オブジェクト	オブジェクト
全員	内容の一覧表示	組織単位オブジェクト	オブジェクト
全員	パブリック インフォメーション読み取り	ユーザー オブジェクト	プロパティ
全員	電話とメールのオプションの読み取り	ユーザー オブジェクト	プロパティ

ステップ 2 Active Directory のアクセス許可を設定します。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを右クリックして [プロパティ（Properties）] をクリックします。
- [セキュリティ（Security）] をクリックします。
- [詳細設定（Advanced）] をクリックします。
- [追加（Add）] をクリックします。
- ユーザー オブジェクト [全員（Everyone）] をクリックして [OK] をクリックします。
- [権限の種類（Permission Type）] タブをクリックします。
- [適用（Apply onto）] ボックスの [継承（Inheritance）] をクリックします。
- [権限（Permission）] アクセス許可の [許可（Allow）] チェックボックスをオンにします。

ステップ 3 Cisco メッセージング ゲートウェイの設定

コマンドライン インターフェイス（CLI）の **`ldapconfig`** を使用して、次の情報を指定した LDAP サーバ エントリを作成します。

- Active Directory または Exchange サーバのホスト名
- ポート 3268（Port 2）
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ：匿名

Active Directory の匿名バインドのセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する匿名バインド クエリで特定のデータを使用できるようになります。Active Directory サーバの匿名バインドにより、ユーザ名 anonymous とブランクのパスフレーズが送信されます。

（注） 匿名バインドを試行するときに何らかのパスフレーズが Active Directory サーバに送信されると、認証に失敗することがあります。

手順

ステップ 1 必要となる Active Directory アクセス許可を確認します。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリの対象であるユーザが属している OU および CN オブジェクトのすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザーオブジェクト	権限	継承	アクセス許可のタイプ
匿名ログオン	内容の一覧表示	コンテナオブジェクト	オブジェクト
匿名ログオン	内容の一覧表示	組織単位オブジェクト	オブジェクト
匿名ログオン	パブリックインフォメーション読み取り	ユーザーオブジェクト	プロパティ
匿名ログオン	電話とメールのオプションの読み取り	ユーザーオブジェクト	プロパティ

ステップ 2 Active Directory のアクセス許可を設定します。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを右クリックして [プロパティ（Properties）] をクリックします。
- [セキュリティ（Security）] をクリックします。
- [詳細設定（Advanced）] をクリックします。
- [追加（Add）] をクリックします。
- ユーザー オブジェクト [匿名ログオン（ANONYMOUS LOGON）] をクリックして [OK] をクリックします。
- [権限の種類（Permission Type）] タブをクリックします。
- [適用（Apply onto）] ボックスの [継承（Inheritance）] をクリックします。
- [権限（Permission）] アクセス許可の [許可（Allow）] チェックボックスをオンにします。

ステップ 3 Cisco メッセージング ゲートウェイの設定

[システム管理（System Administration）] > [LDAP] ページ（または CLI の **ldapconfig**）を使用して、次の情報を設定した LDAP サーバ エントリを作成します。

- Active Directory または Exchange サーバのホスト名
- ポート 3268（Port 2）
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ：パスフレーズ ベース（cn=anonymous をユーザとして使用し、パスフレーズはブランク）

Active Directory の実装に関する注意

- Active Directory サーバが LDAP 接続を受け付けるポートは、3268 と 389 です。グローバル カタログへのアクセス用のデフォルト ポートは 3268 です。
- Active Directory サーバが LDAPS 接続を受け付けるポートは、636 と 3269 です。Microsoft 製品で LDAPS がサポートされるのは、Windows Server 2003 以上です。
- 電子メールゲートウェイは、グローバルカタログでもあるドメインコントローラに接続してください。これは、複数のベースに対するクエリを同じサーバを使用して実行できるようにするためです。
- クエリを正常に実行するには、Active Directory の中で、ディレクトリ オブジェクトに対する読み取り許可をグループ「Everyone」に付与する必要があります。これには、ドメイン名前付けコンテキストのルートも含まれます。
- 一般的に、多くの Active Directory 実装では、mail 属性エントリに一致する値の「ProxyAddresses」属性エントリが存在します。
- Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

LDAP クエリのテスト

[LDAPサーバプロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [クエリのテスト（Test Query）] ボタン（または CLI の `test` サブコマンド）を使用して、クエリタイプごとに設定した LDAP サーバに対するクエリをテストします。結果が表示されるだけでなく、クエリ接続テストの各ステージの詳細も表示されます。テストは、クエリ タイプのそれぞれに対して行うことができます。

`ldaptest` コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

LDAP サーバ属性の [ホスト名（Host Name）] フィールドに複数のホストを入力した場合は、各 LDAP サーバに対して 電子メールゲートウェイのテストが行われます。

表 *67 : LDAP* クエリのテスト

クエリのタイプ	受信者が一致する場合（PASS）	受信者が一致しない場合（FAIL）
受信者受け入れ（[承認（Accept）]、ldapaccept）	メッセージを受け入れます。	受信者が無効：カンバセーションまたは遅延バウンスまたはメッセージをドロップ（リスナー設定による）。DHAP：ドロップ。
ルーティング（[ルーティング（Routing）]、ldaprouting）	クエリの設定に基づいてルーティングします。	このメッセージの処理を続行します。
マスカレード（[マスカレード（Masquerade）]、masquerade）	クエリ内で定義された変数マッピングに従ってヘッダーを変更します。	このメッセージの処理を続行します。
グループ メンバーシップ（[グループ（Group）]、ldapgroup）	メッセージ フィルタ ルールに対して「true」を返します。	メッセージ フィルタ ルールに対して「false」を返します。
SMTP Auth（[SMTP認証（SMTP Authentication）]、smtpauth）	LDAP サーバから返されたパスフレーズを使用して認証を行います。つまり、SMTP 認証が行われます。	一致するパスフレーズなし：SMTP 認証の試行は失敗します。
外部認証（externalauth）	バインド、ユーザー レコード、およびユーザーのグループ メンバーシップに対して個別に「match positive」が返されます。	バインド、ユーザー レコード、およびユーザーのグループ メンバーシップに対して個別に「match negative」が返されます。
スパム隔離へのエンドユーザ認証（isqauth）	エンドユーザ アカウントに対して「match positive」が返されます。	一致するパスフレーズなし：エンドユーザ認証の試行は失敗します。
スパム隔離のエイリアス統合（isqalias）	統合されたスパム通知の送信先である電子メール アドレスが返されます。	スパム通知を統合できません。

（注） クエリに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリは、**maillocaladdress** と入力したときとは異なります。シスコは、作成したすべてのクエリについて ldapconfig コマンドの test サブコマンドを使用してテストし、正しい結果が返されることを確認するよう強く推奨します。

LDAP サーバへの接続のトラブルシューティング

LDAP サーバが電子メールゲートウェイから到達不能である場合は、次のエラーのいずれかが表示されます。

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

サーバが到達不能になる原因としては、サーバ設定で入力されたポートの誤りや、ファイアウォールでポートが開いていないことが考えられます。LDAP サーバの通信には一般に、ポート 3268 または 389 が使用されます。Active Directory は、ポート 3268 を使用して、マルチサーバ環境で使用されるグローバルカタログにアクセスします（詳細については、付録の「ファイアウォール情報」を参照してください）。AsyncOS 4.0 では、SSL を使用して（通常はポート 636 で） LDAP サーバと通信する機能が追加されました。詳細については、セキュア LDAP（SSL） （957 ページ）を参照してください。

サーバが到達不能になる原因としてはその他に、入力されたホスト名が解決不可能であることが考えられます。

[LDAP サーバプロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [テストサーバ（Test Server(s)）]（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストできます。詳細については、LDAP サーバのテスト （950 ページ）を参照してください。

LDAP サーバが到達不能である場合：

- LDAP 受け入れまたはマスカレードまたはルーティングがワーク キューに対してイネーブルになっている場合は、メールはワーク キュー内に留まります。
- LDAP 受け入れはイネーブルになっておらず、他のクエリ（グローバル ポリシー チェックなど）がフィルタ内で使用されている場合は、そのフィルタの評価結果が false になります。

受信者検証で受け入れクエリを使用する

既存の LDAP インフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メールアドレスの扱い方を定義できます。ディレクトリ内のユーザデータに対する変更は、次回電子メールゲートウェイがディレクトリサーバに対してクエリを実行したときに更

新されます。キャッシュのサイズと、電子メールゲートウェイが取得したデータを保持する時間の長さは設定可能です。

（注） 特別な受信者（たとえばadministrator@example.com）に対してLDAP受け入れクエリをバイパスすることもできます。このように設定するには、受信者アクセステーブル（RAT）を使用します。この設定の方法については、「Configuring the Gateway to Receive Email」の章を参照してください。

関連項目

- 受け入れクエリの例 （964 ページ）
- Lotus Notes の場合の受け入れクエリの設定 （965 ページ）

受け入れクエリの例

次の表に、受け入れクエリの例を示します。

表 *68*：一般的な *LDAP* 実装での *LDAP* クエリ文字列の例：受け入れ

クエリの対象	受信者検証

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory Address Book **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

Sun ONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus Notes/Lotus Domino	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

ユーザ名（左側）の検証を行うこともできます。このことが役に立つのは、ディレクトリに格納されていないドメインのメールも受け入れるようにしたい場合です。受け入れクエリを (uid={u}) に設定してください。

Lotus Notes の場合の受け入れクエリの設定

LDAPACCEPT と Lotus Notes とを組み合わせる場合は、注意が必要です。Notes LDAP に格納されているユーザの属性が次のように設定されているとします。

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

LDAP ディレクトリに存在しないユーザであるにもかかわらず、Lotus はこのユーザへの電子メールを、指定されたアドレス以外の形式（たとえばJoe_User@example.com）であっても受け入れます。したがって、AsyncOS は、このユーザの有効なユーザ メール アドレスをすべて見つけることはできません。

この解決策の 1 つは、他の形式のアドレスのパブリッシュを試みるというものです。詳細については、Lotus Notes 管理者に問い合わせてください。

複数ターゲットアドレスへのメール送信にルーティング クエリを使用する

AsyncOS では、エイリアス拡張（複数ターゲットアドレスへの LDAP ルーティング）がサポートされます。AsyncOS によって、元のメール メッセージはエイリアス ターゲットごとに別の新しいメッセージで置き換えられます（たとえば、recipient@yoursite.com へのメッセージは、newrecipient1@hotmail.com や recipient2@internal.yourcompany.com などへの、それぞれ独立したメッセージで置き換えられます）。ルーティング クエリは、他の電子メール処理システムではエイリアシング クエリと呼ばれることもあります。

関連項目

- ルーティング クエリの例 （965 ページ）

ルーティング クエリの例

表 *69 :* 一般的な *LDAP* 実装での *LDAP* クエリー文字列の例：ルーティング

クエリの対象	別のメールホストへのルーティング
OpenLDAP	`(mailLocalAddress={a})`

クエリの対象	別のメールホストへのルーティング
Microsoft Active Directory Address Book **Microsoft Exchange**	該当しない可能性あり

Sun ONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

Active Directory の実装によっては、`proxyAddresses` 属性のエントリが複数存在することがありますが、この属性の値は Active Directory によって `smtp:user@domain.com` という形式で格納されるため、このデータは LDAP ルーティング/エイリアス拡張には使用できません。ターゲットアドレスはそれぞれ別の `attribute:value` ペアに存在する必要があります。Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

関連項目

- ルーティング：MAILHOST と MAILROUTINGADDRESS （966 ページ）

ルーティング：MAILHOST と MAILROUTINGADDRESS

ルーティング クエリの場合は、MAILHOST の値は IP アドレスではなく、解決可能なホスト名であることが必要です。これには、内部的な DNSconfig が必要になるのが一般的です。

MAILHOST は、ルーティング クエリでは省略可能です。MAILROUTINGADDRESS は、MAILHOST が設定されていない場合は必須です。

エンベロープ送信者を書き換えるためのマスカレードクエリの使用

マスカレードとは、電子メールのエンベロープ送信者（「送信者」または「MAIL FROM」と呼ばれることもあります）および To:、From:、CC: の各ヘッダーを、定義済みのクエリに基づいて書き換える機能です。この機能の一般的な実装例の 1 つが「仮想ドメイン」であり、これによって複数のドメインを 1 つのサイトからホスティングできるようになります。他の一般的な実装としては、ネットワーク インフラストラクチャを「隠す」ために、電子メールヘッダーの文字列からサブドメインを取り除く（「ストリッピング」）というものがあります。

関連項目

- マスカレード クエリの例 （967 ページ）
- 「フレンドリ名」のマスカレード （967 ページ）

マスカレード クエリの例

表 *70:* 一般的な *LDAP* 実装での *LDAP* クエリー文字列の例：マスカレード

クエリの対象	マスカレード
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory Address Book	`(proxyaddresses=smtp:{a})`

Sun ONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

「フレンドリ名」のマスカレード

ユーザ環境によっては、LDAP ディレクトリ サーバ スキーマの中に、メール ルーティング アドレスやローカル メール アドレス以外に「フレンドリ名」が含まれていることがあります。AsyncOS では、エンベロープ送信者（発信メールの場合）やメッセージ ヘッダー（受信メールの場合、To:、Reply To:、From:、CC: など）を、この「フレンドリ名」でマスカレードできます。フレンドリ アドレスには、有効な電子メール アドレスでは通常は許可されない特殊文字（引用符、スペース、カンマなど）が含まれていてもかまいません。

LDAPクエリ経由でヘッダーをマスカレードするときに、フレンドリ メール文字列全体をLDAPサーバからの結果で置き換えるかどうかを設定時に選択できます。この動作がイネーブルになっていても、エンベロープ送信者にはuser@domain部分のみが使用されることに注意してください（フレンドリ名はルールに反するため）。

標準的なLDAPマスカレードのときと同様に、LDAPクエリの結果が空（長さが0またはすべてホワイト スペース）の場合は、マスカレードは行われません。

この機能をイネーブルにするには、LDAPベースのマスカレードクエリをリスナーに対して設定するときに（[LDAP] ページまたは `ldapconfig` コマンド）、次の質問に対して「y」と回答します。

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

たとえば、次のようなLDAPエントリがあるとします。

属性	値
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	“Administrator for example.com,” <joe.smith\@example.com>

この機能がイネーブルになっている場合に、LDAP クエリが (mailRoutingAddress={a}) で、マスカレード属性が (mailLocalAddress) ならば、次のように置き換えられます。

元のアドレス（From、To、CC、Reply-to）	マスカレードされたヘッダー	マスカレードされたエンベロープ送信者
admin@example.com	From: “Administrator for example.com,” <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

受信者がグループメンバーであるかどうかを判別するグループ LDAP クエリの使用

LDAP ディレクトリ内で定義されたグループに受信者が属しているかどうかを、LDAP サーバに対するクエリを使用して判別できます。

手順

ステップ 1 メッセージに rcpt-to-group または mail-from-group ルールを適用するメッセージ フィルタを作成します。

ステップ 2 次に、[システム管理（System Administration）] > [LDAP] ページ（または **ldapconfig** コマンド）を使用して、電子メールゲートウェイのバインド先となる LDAP サーバを定義し、グループメンバーシップを調べるクエリを設定します。

ステップ 3 [ネットワーク（Network）] > [リスナー（Listeners）] ページ（または **listenerconfig -> edit -> ldapgroup** サブコマンド）を使用して、このグループ クエリーをリスナーに対して有効にします。

次のタスク

関連項目

- グループ クエリの例 （969 ページ）
- グループ クエリの設定 （969 ページ）

グループ クエリの例

表 *71 :* 一般的な *LDAP* 実装での *LDAP* クエリ文字列の例：グループ

クエリの対象	グループ
OpenLDAP	OpenLDAP では、memberOf 属性はデフォルトではサポートされません。LDAP 管理者によって、この属性または類似の属性がスキーマに追加されていることがあります。
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
Sun ONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

たとえば、LDAP ディレクトリで「マーケティング」グループのメンバーが ou=Marketing と分類されているとします。この分類を使用して、このグループが送受信するメールを特別な方法で取り扱うことができます。ステップ 1 で、メッセージに作用するメッセージ フィルタを作成し、ステップ 2 と 3 で LDAP ルックアップ メカニズムをイネーブルにします。

グループ クエリの設定

次に示す例では、マーケティング グループ（LDAP グループ「Marketing」として定義）のメンバーからのメールを代替メール配信ホスト `marketingfolks.example.com` に配信します。

手順

ステップ 1 初めに、グループ メンバーシップに関して肯定的に一致するメッセージに作用する、メッセージ フィルタを作成します。この例では、作成するフィルタの中で `mail-from-group` ルールを使用します。メッセージのうち、エンベロープ送信者が LDAP グループ「marketing-group1」に属していることが判明したものはすべて、代替配信ホストに送信されます（フィルタの `alt-mailhost` アクション）。

グループ メンバーシップ フィールド変数（groupName）は、ステップ 2 で定義します。グループ属性「groupName」の値は、`marketing-group1` と定義されます。

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

MarketingGroupfilter:
```

```
if (mail-from-group == "marketing-group1") {

alt-mailhost ('marketingfolks.example.com');}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

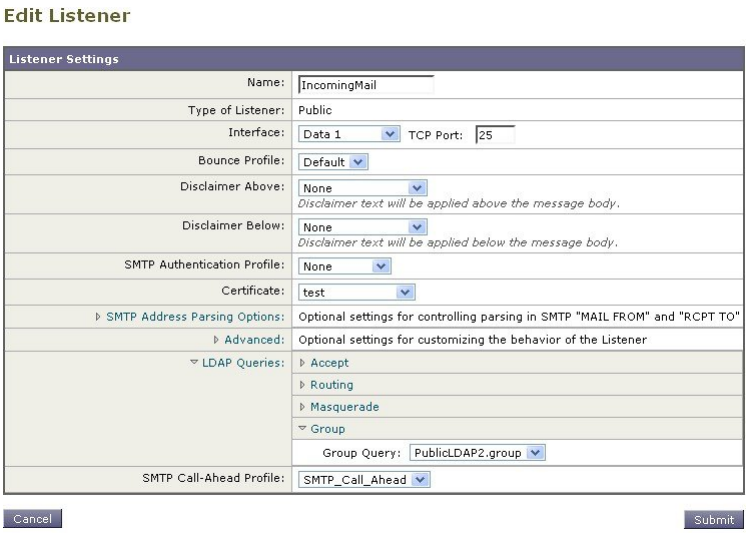
メッセージ フィルタ ルール `mail-from-group` と `rcpt-to-group` の詳細については、メッセージ フィルタ ルール （157 ページ）を参照してください。

ステップ 2 次に、[LDAPサーバプロファイルを追加（Add LDAP Server Profile）]ページを使用して、電子メールゲートウェイのバインド先となるLDAPサーバを定義し、グループメンバーシップを調べる最初のクエリを定義します。

ステップ 3 次に、パブリック リスナー「InboundMail」で LDAP クエリを使用してグループ ルーティングを行うように更新します。[リスナーを編集（Edit Listener）]ページを使用して、前のステップで指定した LDAP クエリをイネーブルにします。

このクエリが実行されると、リスナーが受け入れたメッセージによってLDAPサーバに対するクエリがトリガーされて、グループ メンバーシップが特定されます。PublicLDAP2.group クエリはすでに、[システム管理（System Administration）] > [LDAP] ページで定義されています。

図 *63 :* リスナーでのグループ クエリの指定



ステップ 4 変更を送信し、保存します。

例：グループクエリを使用してスパムとウイルスのチェックをスキップする

メッセージ フィルタはパイプラインの初めの方で実行されるので、グループ クエリを使用すると、特定のグループについてウイルスとスパムのチェックをスキップできます。たとえば、社内の IT グループへのメッセージについては、スパムとウイルスのチェックをスキップしてすべて受信したいという要望があるとします。LDAP レコードの中に、DN をグループ名として使用するグループエントリを作成します。このグループ名は、次の DN エントリで構成されます。

cn=IT, ou=groups, o=sample.com

LDAP サーバ プロファイルを作成し、次のグループ クエリを指定します。

(&(memberOf={g})(proxyAddresses=smtp:{a}))

次に、このクエリをリスナーに対してイネーブルにします。これで、メッセージがそのリスナーで受信されたときに、このグループ クエリがトリガーされます。

IT グループのメンバーについてはウイルスとスパムのチェックをスキップするために、次のメッセージ フィルタを作成して、着信メッセージを LDAP グループと比較して検査します。

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.
```

```
IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){

skip-spamcheck();

skip-viruscheck();

deliver();

}

.
1 filters added.
```

（注） このメッセージフィルタ内の rcpt-to-group には、グループ名として入力された DN（cn=IT, ou=groups, o=sample.com）が反映されています。メッセージフィルタ内で使用しているグループ名が正しいことを確認してください。フィルタの実行時に、LDAP ディレクトリ内でその名前との比較が確実に行われるようにするためです。

リスナーが受け入れたメッセージによって LDAP サーバに対するクエリがトリガーされて、グループ メンバーシップが特定されます。メッセージ受信者が IT グループのメンバーの場合は、メッセージフィルタの定義に従ってウイルスとスパムのチェックがいずれもスキップされて、メッセージが受信者に配信されます。フィルタで LDAP クエリの結果をチェックするには、LDAP サーバに対する LDAP クエリを作成し、その LDAP クエリをリスナーに対してイネーブルにする必要があります。

特定のドメインヘルーティングするためのドメインベース クエリの使用

ドメインベース クエリとは、LDAP クエリをタイプ別にグループ化し、特定のドメインに関連付けたうえで、特定のリスナーに割り当てたものです。ドメインベース クエリが使用されるのは、複数の LDAP サーバがそれぞれ異なるドメインに関連付けられているが、すべての LDAP サーバに対するクエリを同じリスナー上で実行する場合です。たとえば、「MyCompany」という会社が「HisCompany」と「HerCompany」の 2 社を買収するとします。MyCompany は自社のドメイン MyCompany.example.com に加えて HisCompany.example.com および HerCompany.example.com のドメインを運用すると共に、ドメインごとに別の LDAP サーバを運用して、各ドメインに関連付けられた従業員の情報を格納しています。この 3 つのドメインのメールをすべて受け入れるために、MyCompany はドメインベース クエリを作成します。これで、MyCompany.example.com は Mycompany.example.com、HisCompany.example.com、および HerCompany.example.com のメールを同じリスナー上で受け入れることができます。

手順

ステップ 1 ドメインベース クエリで使用するドメインごとに 1 つずつ、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれに対して、ドメインベース クエリに使用するクエリを設定します（受け入れ、ルーティングなど）。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （947 ページ）を参照してください。

ステップ 2 ドメインベース クエリを作成します。ドメインベースクエリを作成するときは、各サーバプロファイルからクエリを選択します。また、どのクエリを実行するかを Envelope To フィールドに基づいて決定するように、電子メールゲートウェイをイネーブルにします。クエリーの作成方法の詳細については、ドメインベース クエリの作成 （973 ページ） を参照してください。

ステップ 3 ドメインベース クエリをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。

（注） ドメインベース クエリは他にも、スパム隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、「スパム隔離」の章を参照してください。

次のタスク

関連項目

- ドメインベース クエリの作成 （973 ページ）

ドメインベース クエリの作成

ドメインベース クエリは、[システム管理（System Administration）] > [LDAP] > [LDAPサーバプロファイル（LDAP Server Profiles）] ページで作成します。

手順

ステップ 1 [LDAPサーバプロファイル（LDAP Server Profiles）] ページの [詳細設定（Advanced）] をクリックします。

ステップ 2 [ドメイン割り当ての追加（Add Domain Assignments）] をクリックします。

ステップ 3 ドメインベース クエリーの名前を入力します。

ステップ 4 クエリー タイプを選択します。

（注） ドメインベースクエリを作成するときに選択するクエリのタイプは、すべて同じでなければなりません。クエリタイプを選択すると、電子メールゲートウェイはそのタイプのクエリを利用可能なサーバプロファイルから取得し、クエリフィールドを生成します。

ステップ 5 [ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

ステップ 6 このドメインに関連付けるクエリーを選択します。

ステップ 7 クエリのドメインがすべて追加されるまで、行を追加します。

ステップ 8 どのクエリにも一致しないときに実行する、デフォルトのクエリを入力できます。デフォルトクエリーを入力しない場合は、[なし（None）] を選択します。

ステップ 9 クエリをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスフレーズまたはメール アドレスを [テスト パラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 10 （省略可能）{f} トークンを受け入れクエリ内で使用する場合は、エンベロープ送信者アドレスをテスト クエリに追加できます。

（注） ドメインベース クエリの作成が終了したら、このクエリをパブリックまたはプライベートのリスナーに関連付ける必要があります。

ステップ 11 変更を送信し、保存します。

一連の LDAP クエリを実行するためのチェーン クエリの使用

チェーンクエリは、 電子メールゲートウェイによって順番に実行が試行される一連の LDAP クエリで構成されます。電子メールゲートウェイは、この「チェーン」の中の各クエリの実行を試行し、LDAP サーバから肯定的なレスポンスが返されると（または「チェーン」の最後のクエリで否定的なレスポンスが返されるか失敗すると）実行を停止します。チェーン ルーティング クエリでは、 電子メールゲートウェイが書き換えられた電子メールアドレスごとに、同じ設定の一連のチェーンクエリを再実行します。チェーン クエリが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、属性 maillocaladdress と mail がユーザ電子メール アドレスを格納するために使用されているとします。この両方の属性に対して確実にクエリを実行するには、チェーン クエリを使用します。

手順

ステップ 1 チェーン クエリ内で使用するクエリごとに、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれについて、チェーン クエリーに使用するクエリーを設定します。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （947 ページ）を参照してください。

ステップ 2 チェーン クエリを作成します。詳細については、チェーン クエリの作成 （975 ページ）を参照してください。

ステップ 3 チェーン クエリをパブリック またはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、「Configuring the Gateway to Receive Mail」の章を参照してください。

（注） ドメインベース クエリは他にも、スパム隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、「スパム隔離」の章を参照してください。

次のタスク

関連項目

- チェーン クエリの作成 （975 ページ）

チェーン クエリの作成

チェーン クエリーは、[システム管理（System Administration）] > [LDAP] > [LDAPサーバプロファイル（LDAP Server Profiles）] ページで作成します。

手順

ステップ 1 [LDAPサーバプロファイル（LDAP Server Profiles）] ページの [詳細設定（Advanced）] をクリックします。

ステップ 2 [チェーン クエリを追加（Add Chain Query）] をクリックします。

ステップ 3 チェーン クエリの名前を入力します。

ステップ 4 クエリー タイプを選択します。

チェーンクエリを作成するときに選択するクエリのタイプは、すべて同じでなければなりません。クエリタイプを選択すると、電子メールゲートウェイはそのタイプのクエリを利用可能なサーバプロファイルから取得し、クエリフィールドを生成します。

ステップ 5 チェーン クエリに追加するクエリを選択します。

電子メールゲートウェイによって、ここで設定した順にクエリが実行されます。したがって、複数のクエリをチェーンクエリに追加する場合は、より限定的なクエリの後でより汎用のクエリが実行されるような順序にすることを推奨します。

ステップ 6 クエリをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスフレーズまたはメール アドレスを [テスト パラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 7 （省略可能）{f} トークンを受け入れクエリ内で使用する場合は、エンベロープ送信者アドレスをテスト クエリに追加できます。

（注） チェーンクエリの作成が終了したら、このクエリをパブリックまたはプライベートのリスナーに関連付ける必要があります。

ステップ 8 変更を送信し、保存します。

LDAP によるディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃は、悪意のある送信者が、よくある名前を持つ受信者宛にメッセージを送信することによって開始します。電子メール ゲートウェイは、受信者がその場所に有効なメールボックスを持っているかどうかを調べて応答を返します。これを大量に実行すると、悪意のある送信者は、どのアドレスにスパムを送信すればよいかを、有効なアドレスの「収穫（ハーベスト）」によって特定できるようになります。

電子メールゲートウェイでは、LDAP受け入れ検証クエリを使用すると、ディレクトリハーベスト攻撃（DHA）を検出して防止できます。LDAP受け入れを設定するときに、ディレクトリハーベスト攻撃防止を SMTP カンバセーション中に行うか、ワーク キューの中で行うかを選択できます。

関連項目

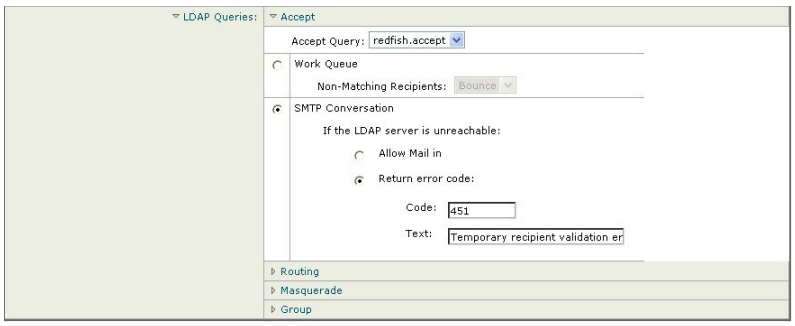
- SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止 （976 ページ）
- 作業キュー内でのディレクトリ ハーベスト攻撃防止 （978 ページ）

SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止

DHA を防止するには、ドメインだけを Recipient Access Table（RAT; 受信者アクセス テーブル）に入力しておき、LDAP 受け入れ検証を SMTP カンバセーション内で実行します。

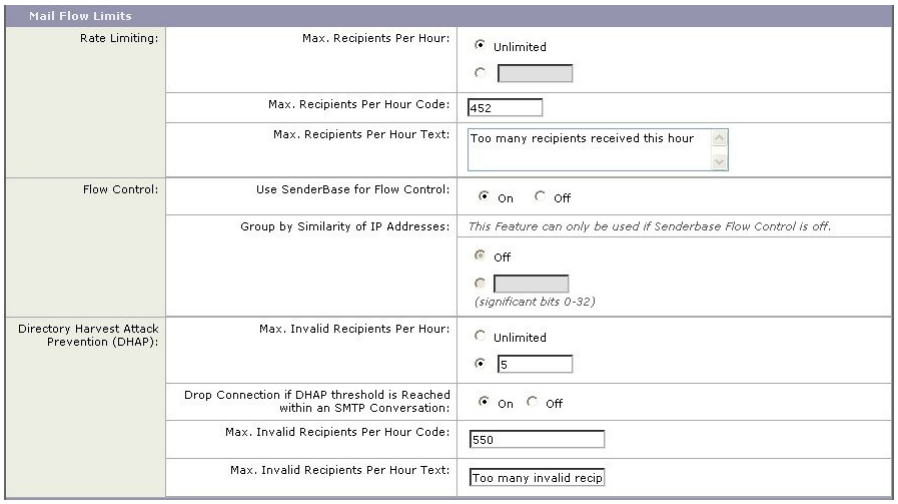
SMTP カンバセーション中にメッセージをドロップするには、LDAP 受け入れのための LDAP サーバプロファイルを設定します。次に、LDAP受け入れクエリをSMTPカンバセーション中に実行するようにリスナーを設定します。

図 *64*：受け入れクエリを *SMTP* カンバセーション中に実行するように設定



リスナーで実行するLDAP受け入れクエリを設定したら、そのリスナーに関連付けられたメール フロー ポリシーの中の DHAP（ディレクトリ ハーベスト攻撃防止）設定を指定する必要があります。

図 *65 : SMTP* カンバセーション中に接続をドロップするようにメール フロー ポリシーを設定する



リスナーに関連付けられたメール フロー ポリシーの中で、ディレクトリ ハーベスト攻撃防止のための次の項目を設定します。

- [1時間あたりの無効な受信者の最大数（Max. Invalid Recipients Per hour）]。このリスナーがリモート ホストから受け取る無効な受信者の 1 時間あたりの最大数です。このしきい値は、RAT 拒否の総数を表します。これは、無効な LDAP 受信者宛てのため SMTP カンバセーション中にドロップされたメッセージの総数と、ワーク キュー内でバウンスされたメッセージの合計です。たとえば、しきい値を 5 と設定した場合に、検出された RAT 拒否が 2 件で、無効な LDAP 受信者宛てのためドロップされたメッセージが 3 件であるとします。この時点で、電子メールゲートウェイはしきい値に到達したと判断して、接続をドロップさせます。デフォルトでは、パブリック リスナーでの 1 時間あたりの受信者の最大数は 25 です。プライベート リスナーの場合は、1 時間あたりの受信者の最大数はデフォルトでは無制限です。この最大数を [無制限（Unlimited）] に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。
- [SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ（Drop Connection if DHAP Threshold is reached within an SMTP conversation）]。ディレクトリハーベスト攻撃防止のしきい値に達したときに電子メールゲートウェイによって接続をドロップさせるように設定します。
- [時間コードあたりの最大受信者数（Max. Recipients Per Hour Code）]。接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。
- [時間テキストあたりの最大受信者数（Max. Recipients Per Hour Text）]。ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。

しきい値に達した場合は、受信者が無効であってもメッセージのエンベロープ送信者にバウンス メッセージが送信されることはありません。

作業キュー内でのディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃（DHA）のほとんどは、ドメインだけを受信者アクセス テーブル（RAT）に入力しておき、LDAP受け入れ検証をワーク キュー内で実行することによって防止できます。この方法を使用すると、悪意のある送信者が、受信者が有効かどうかをSMTPカンバセーション中に知ることはできなくなります。（受け入れクエリが設定されているときは、システムはメッセージを受け入れて、LDAP 受け入れ検証をワーク キュー内で実行します。）ただし、メッセージのエンベロープ送信者には、受信者が無効である場合にバウンスメッセージが送信されます。

関連項目

- ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定 （978 ページ）

ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定

ディレクトリ ハーベスト攻撃を防止するには、初めに LDAP サーバ プロファイルを設定して LDAP 受け入れをイネーブルにします。LDAP 受け入れクエリをイネーブルにしたら、次のように、その受け入れクエリを使用するようにリスナーを設定すると共に、受信者が一致しない場合はメールをバウンスするように指定します。

次に、メール フロー ポリシーを設定します。このポリシーでは、所定の時間内に送信 IP アドレスあたりどれだけの無効な受信者アドレスをシステムが受け入れるかを定義します。この数を超えると、システムはこの状態が DHA（ディレクトリ ハーベスト攻撃）であると判断してアラート メッセージを送信します。このアラート メッセージに含まれる情報は次のとおりです。

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name
'), dhap_limit=n, sender_group=sender_group,


listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name
', 1), sender=envelope_sender, rcpt=envelope_recipients
```

メール フロー ポリシーで指定されたしきい値に達するまでは、システムによってメッセージがバウンスされますが、それ以降は応答を返すことなく受け入れられてドロップされます。したがって、正当な送信者にはアドレスの誤りが通知されますが、悪意のある送信者は、どの受信者が受け入れられたかを判断できません。

この無効受信者カウンタの働きは、現在 AsyncOS に実装されているレート制限機能に似ています。つまり、管理者がこの機能をイネーブルにして、上限値をパブリック リスナーの HAT 内のメール フロー ポリシーの中で設定します（HAT のデフォルトのメール フロー ポリシーを含む）。

また、コマンドライン インターフェイスで `listenerconfig` コマンドを使用して、これを設定することもできます。

この機能は、メール フロー ポリシーを GUI で編集するときにも表示されます（対応するリスナーに対して LDAP クエリが作成済みの場合）。

1 時間あたりの無効受信者数を入力すると、そのメール フロー ポリシーに対して DHAP（ディレクトリ ハーベスト攻撃防止）がイネーブルになります。デフォルトで、パブリック リスナーでは 1 時間あたり最大 25 件の無効受信者が受け入れられます。プライベート リスナーの場合は、1 時間あたりの無効受信者数はデフォルトでは無制限です。この最大数を [無制限（Unlimited）] に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。

SMTP 認証を行うための AsyncOS の設定

AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。

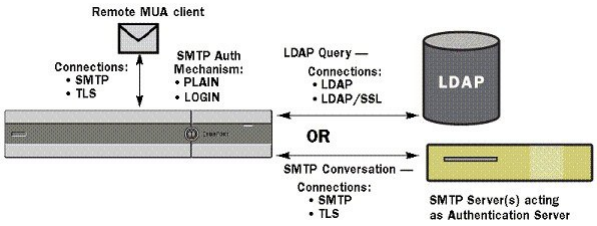
このメカニズムを利用すると、特定の組織に所属するユーザが、その組織のメール サーバにリモートで接続している（自宅や出張先などから）ときもメール サーバを使用してメールを送信できるようになります。メール ユーザー エージェント（MUA）は、メールの送信を試行するときに認証要求（チャレンジ/レスポンス）を発行できます。

SMTP 認証は、発信メール リレーに対しても使用できます。これを利用すると、 電子メール ゲートウェイがネットワークのエッジではない場合に、電子メールゲートウェイからリレー サーバへのセキュア接続を確立できます。

AsyncOS では、ユーザー クレデンシャルの認証方式として次の 2 つがサポートされています。

- LDAP ディレクトリを使用する。
- 別の SMTP サーバを使用する（SMTP Auth 転送と SMTP Auth 発信）。

図 *66 : SMTP Auth* のサポート：*LDAP* ディレクトリ ストアまたは *SMTP* サーバ



SMTP 認証方式を設定したら、HAT メール フロー ポリシー内で使用される SMTP Auth プロファイルを、smtpauthconfig コマンドを使用して作成します（リスナーでの SMTP 認証の有効化 （983 ページ）を参照）。

関連項目

- SMTP 認証の設定 （980 ページ）
- SMTP 認証クエリの設定 （981 ページ）
- 第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth） （982 ページ）
- LDAP を使用する SMTP 認証 （983 ページ）
- クライアント証明書を使用した SMTP セッションの認証 （986 ページ）
- 発信 SMTP 認証 （987 ページ）

- ロギングと SMTP 認証 （987 ページ）

SMTP 認証の設定

LDAP サーバを使用して認証を行う場合は、[LDAPサーバプロファイルを追加（Add LDAP Server Profile）] または [LDAPサーバプロファイルを編集（Edit LDAP Server Profile）] ページ（または **ldapconfig** コマンド）でクエリ タイプとして SMTPAUTH を選択して SMTP 認証クエリを作成します。設定する LDAP サーバのそれぞれについて、SMTP 認証プロファイルとして使用する SMTPAUTH クエリを 1 つ設定できます。

SMTP 認証クエリには、「LDAP バインド」と「属性としてのパスフレーズ」の 2 種類があります。「属性としてのパスフレーズ」を使用するときは、電子メールゲートウェイによって LDAP ディレクトリ内のパスフレーズフィールドが取得されます。パスフレーズは、プレーンテキスト、暗号化、またはハッシュされて格納されている可能性があります。LDAP バインドを使用すると、電子メールゲートウェイは、クライアントによって提供されたクレデンシャルを使用して LDAP サーバへのログインを試行します。

関連項目

- 属性としてのパスフレーズの指定 （980 ページ）

属性としてのパスフレーズの指定

OpenLDAP の規定（RFC 2307 に基づく）では、コーディングのタイプを中カッコで囲み、その後にエンコードされたパスフレーズを続けることになっています（たとえば「{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=」）。この例では、パスフレーズ部分はプレーンテキストのパスフレーズに SHA を適用してから base64 エンコーディングしたものです。

電子メールゲートウェイでは、パスフレーズを取得する前に SASL メカニズムと MUA との間でのネゴシエートが行われ、電子メールゲートウェイと MUA でどの方法を使用するかを決定します（サポートされているメカニズムは LOGIN、PLAIN、MD5、SHA、SSHA、CRYPT SASL です）。その後で、アプライアンスは LDAP データベースに対するクエリを実行してパスフレーズを取得します。LDAP 内では、中カッコで囲まれたプレフィックスがパスフレーズに付いていることがあります。

- プレフィックスが付いていない場合は、LDAP 内に格納されているパスフレーズがプレーンテキストであると見なされます。
- プレフィックスが付いている場合は、アプライアンスはそのハッシュ化パスフレーズを取得し、MUA によって指定されたユーザ名とパスフレーズの両方あるいはどちらかのハッシュを実行して、ハッシュ後のパスフレーズと比較します。電子メールゲートウェイでサポートされるハッシュタイプは SHA1 と MD5 であり、パスフレーズフィールド内では RFC 2307 の規定に基づいて、ハッシュ化パスフレーズの前にハッシュメカニズムのタイプが付加されます。
- LDAP サーバの中には、OpenWave LDAP サーバのように、暗号化されたパスフレーズの前に暗号化タイプを付加しないものもあり、代わりに暗号化タイプが別の LDAP 属性として格納されています。このような場合は、管理者が指定したデフォルトの SMTP AUTH 暗

号化方式であると見なされて、そのパスフレーズとSMTPカンバセーションで取得されたパスフレーズとが比較されます。

電子メールゲートウェイは、SMTP Auth交換から任意のユーザ名を受け取ってLDAPクエリに変換し、このクエリを使用してクリアテキストまたはハッシュ化されたパスフレーズフィールドを取得します。次に、SMTP Auth クレデンシャルで指定されたパスフレーズに対してハッシュが必要な場合は実行し、その結果を LDAP からのパスフレーズと比較します（ハッシュタイプのタグがある場合は取り除く）。一致した場合は、SMTP Authカンバセーションが続行されます。一致しない場合は、エラー コードが返されます。

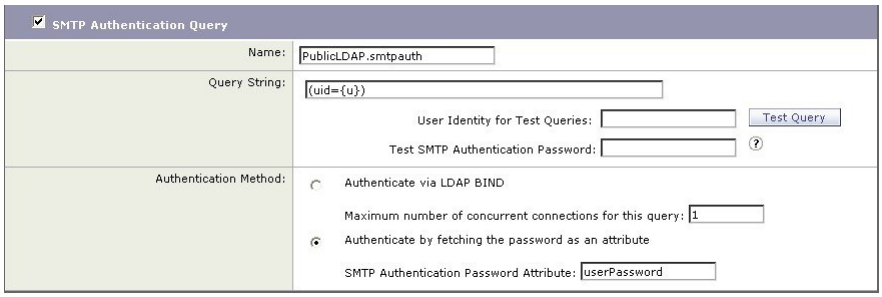
SMTP 認証クエリの設定

表 *72 : SMTP Auth LDAP* クエリのフィールド

名前	クエリの名前
クエリー文字列（Query String）	認証を LDAP バインド経由で行うか、パスフレーズを属性として取得して行うかを選択できます。 [バインド（Bind）] : LDAPサーバへのログイン試行には、クライアントによって指定されたクレデンシャルを使用します（これを「LDAP バインド」と呼びます）。 SMTP Auth クエリで使用される同時接続の最大数を指定します。この数は、上の LDAP サーバ属性で指定した数を超えてはなりません。バインド認証時に大量のセッション タイムアウトが発生するのを防ぐには、ここで指定する同時接続の最大数を大きくします（一般的には、接続のほぼすべてを SMTP Auth に割り当てることができます）。バインド認証ごとに、新しい接続が 1 つ使用されます。残りの接続は、他のタイプの LDAP クエリで共有されます。 [属性としてのパスフレーズ（Passphrase as Attribute）] : パスフレーズを取得して認証を行うには、下の [SMTP認証のパスフレーズの属性（SMTP Auth Passphrase Attribute）] フィールドでパスフレーズを指定します。 いずれかの種類の認証に使用する LDAP クエリを指定します。アクティブ ディレクトリのクエリの例：(&(samaccountname={u})(objectCategory=person)(objectClass=user))
SMTP認証のパスフレーズの属性（SMTP Auth Passphrase Attribute）	[属性としてパスフレーズを取得した認証（Authenticate by fetching the passphrase as an attribute）] を選択した場合は、パスフレーズ属性をここで指定します。

次の例では、[システム管理（System Administration）] > [LDAP] ページを使用して LDAP 設定「PublicLDAP」を編集し、SMTPAUTH クエリを追加しています。クエリ文字列（uid={u}）は、userPassword 属性と比較するように作成されています。

図 *67 : SMTP* 認証クエリ



SMTPAUTH プロファイルの設定が完了すると、そのクエリを SMTP 認証に使用するようにリスナーを設定できます。

第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth）

SMTP 認証カンバセーションのために指定されたユーザ名とパスフレーズを、別の SMTP サーバを使用して検証するように 電子メールゲートウェイを設定できます。

認証を行うサーバは、メールを転送するサーバとは別のものであり、SMTP 認証要求への応答だけを行います。認証に成功したときは、専用メール サーバによるメールの SMTP 転送を続行できます。この機能は、「転送を使用する SMTP Auth」と呼ばれることもあります。クレデンシャルのみが別の SMTP サーバに転送（プロキシ）されて認証が行われるからです。

手順

ステップ 1 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] を選択します。

ステップ 2 [プロファイルを追加...（Add Profile...）] をクリックします。

ステップ 3 SMTP 認証プロファイルの一意の名前を入力します。

ステップ 4 [プロファイルタイプ（Profile Type）] で [転送（Forward）] を選択します。

ステップ 5 **[Next]** をクリックします。

ステップ 6 転送サーバのホスト名/IP アドレスとポートを入力します。認証要求の転送に使用する転送インターフェイスを選択します。同時接続の最大数を指定します。次に、電子メールゲートウェイから転送サーバへの接続に対して TLS を必須とするかどうかを設定します。使用する SASL メカニズムも、[プレーン（PLAIN）] と [ログイン（LOGIN）]から選択できます（使用できる場合）。この選択は、転送サーバごとに設定されます。

ステップ 7 変更を送信し、保存します。

ステップ 8 認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、リスナーでの SMTP 認証の有効化 （983 ページ）を参照してください。

LDAP を使用する SMTP 認証

LDAP ベースの SMTP 認証プロファイルを作成するには、SMTP 認証クエリを LDAP サーバ プロファイルと共に [システム管理（System Administration）] > [LDAP] ページであらかじめ作成しておく必要があります。このプロファイルを使用して SMTP 認証プロファイルを作成します。LDAP プロファイルの作成方法の詳細については、LDAP クエリについて （944 ページ）を参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] を選択します。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 SMTP 認証プロファイルの一意の名前を入力します。

ステップ 4 [プロファイルタイプ（Profile Type）] で [LDAP] を選択します。

ステップ 5 **[Next]** をクリックします。

ステップ 6 この認証プロファイルに使用する LDAP クエリを選択します。

ステップ 7 デフォルトの暗号化方式をドロップダウン メニューから選択します。選択肢には、[SHA]、[Salted SHA]、[Crypt]、[Plain]、[MD5] があります。LDAP サーバによって暗号化後のパスフレーズの前に暗号化タイプが付加される場合は、[なし（None）] を選択してください。LDAP サーバによって暗号化タイプが別エンティティとして保存される場合は（たとえば OpenWave LDAP サーバ）、暗号化方式をメニューから選択してください。デフォルトの暗号化設定は、LDAP クエリにバインドが使用される場合は使用されません。

ステップ 8 [終了（Finish）] をクリックします。

ステップ 9 変更を送信し、保存します。

ステップ 10 認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、リスナーでの SMTP 認証の有効化 （983 ページ）を参照してください。

次のタスク

関連項目

- リスナーでの SMTP 認証の有効化 （983 ページ）

リスナーでの SMTP 認証の有効化

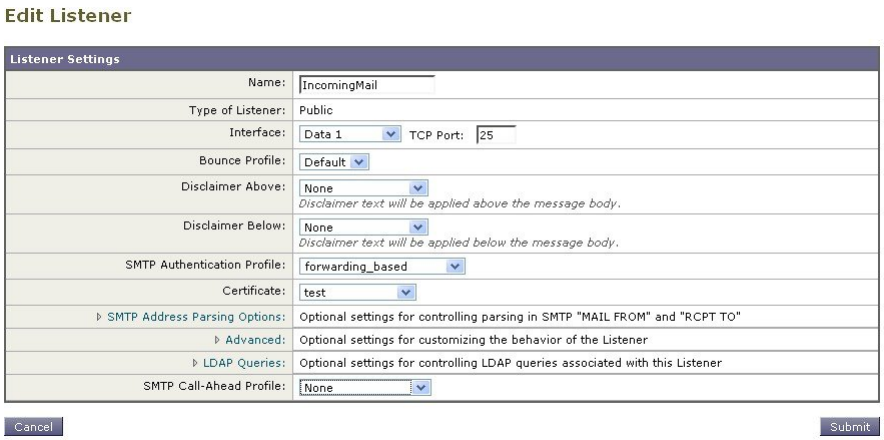
[ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] ページで、実行する認証のタイプ（LDAP ベースまたは SMTP 転送ベース）を指定して SMTP 認証「プロファイル」を作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページ（または **`listenerconfig`** コマンド）を使用して、このプロファイルをリスナーに関連付ける必要があります。

（注） 認証済みのユーザには、ユーザのその時点のメール フロー ポリシーの中で RELAY 接続動作が許可されます。

1 つのプロファイル内で複数の転送サーバを指定することもできます。SASL メカニズム CRAM-MD5 と DIGEST-MD5 は、 電子メールゲートウェイと転送サーバの間ではサポートされません。

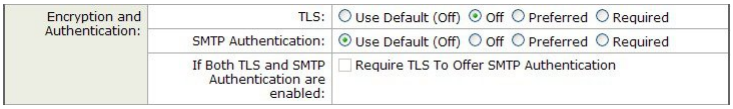
次の例では、リスナー「InboundMail」で SMTPAUTH プロファイルが使用されるように、[リスナーを編集（Edit Listener）] ページで設定しています。

図 *68 : SMTP* 認証プロファイルを *[*リスナーを編集（*Edit Listener*）*]* ページで選択する



プロファイルを使用するようにリスナーを設定したら、そのリスナーでの SMTP 認証を許可、禁止、または必須とするようにホスト アクセス テーブルのデフォルト設定を変更できます。

図 *69 :* メール フロー ポリシーでの *SMTP* 認証のイネーブル化



ケース	説明
1.	[SMTP認証（SMTP Authentication）] フィールドでは、リスナー レベルで SMTP 認証を制御します。[いいえ（No）] を選択した場合は、SMTP 認証に関する他の設定にかかわらず、このリスナーでは認証はイネーブルになりません。
2.	2 番めのプロンプト（[SMTP認証（SMTP Authentication）]）で [必須（Required）] を選択した場合は、AUTH キーワードが発行されるのは TLS がネゴシエートされた（クライアントが別の EHLO コマンドを発行した）後となります。

関連項目

- SMTP 認証と HAT ポリシーの設定 （985 ページ）

• HAT 遅延拒否 （985 ページ）

SMTP 認証と HAT ポリシーの設定

送信者は送信者グループとしてまとめられ、その後でSMTP認証ネゴシエーションが開始するので、ホスト アクセス テーブル（HAT）の設定には影響は及びません。リモートメールホストが接続するときに、電子メールゲートウェイは初めにどの送信者グループが該当するかを特定して、その送信者グループのメールポリシーを適用します。たとえば、リモート MTA「suspicious.com」が SUSPECTLIST という送信者グループに属している場合は、「suspicious.com」の SMTPAUTH ネゴシエーションの結果とは無関係に THROTTLE ポリシーが適用されます。

ただし、SMTPAUTH を使用して認証を受ける送信者の扱いは、「通常の」送信者とは異なります。SMTPAUTH セッションに成功した場合の接続動作は「RELAY」に変更されるので、実質的に受信者アクセス テーブル（RAT）と LDAPACCEPT はバイパスされます。その結果、送信者はメッセージを電子メールゲートウェイ経由でリレーできます。したがって、適用されるレート制限やスロットリングがある場合は、引き続き有効になります。

HAT 遅延拒否

HAT 遅延拒否が設定済みのときは、HAT 送信者グループとメール フロー ポリシーの設定に基づいて本来ならばドロップされる接続も、認証に成功し、RELAY メール フロー ポリシーが許可されます。

メッセージ受信者レベルでHAT拒否を実行するかどうかを設定します。デフォルトでは、HATによって拒否された接続は SMTP カンバセーションの開始時にバナー メッセージをともなって終了されます。

HAT「拒否」設定で電子メールが拒否されると、AsyncOS ではSMTPカンバセーションの開始時ではなく、メッセージ受信者レベル（RCPT TO）で拒否を実行できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。たとえば、ブロックされたメッセージのアドレスおよび各受信者のアドレスからメールを表示できます。また、HAT 拒否の遅延によって、送信側 MTA が何度も再試行される可能性も小さくなります。

HAT 遅延拒否をイネーブルにすると、次の動作が発生します。

- MAIL FROM コマンドが許可されるが、メッセージ オブジェクトは作成されない。
- 電子メールの送信のためのアクセスが拒否されたというメッセージが表示され、すべての RCPT TO コマンドが拒否される。
- SMTP AUTH を使用して送信側 MTA が認証される場合、RELAY ポリシーが許可され、メールを通常どおりに送信できる。

遅延拒否を設定するには、CLI の `listenerconfig --> setup` コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

次の表に、HAT の遅延拒否を設定する方法を説明します。

```
example.com> listenerconfig

Currently configured listeners:
```

```
1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private

2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.


[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>


[...]


By default HAT rejected connections will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?

[N]> y

Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

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

Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

クライアント証明書を使用した SMTP セッションの認証

電子メールゲートウェイは、 電子メールゲートウェイとユーザのメールクライアント間の SMTP セッションを認証するためにクライアント証明書の使用をサポートします。

SMTP認証プロファイルを作成する場合は、証明書を確認するときに使用する証明書認証LDAP クエリを選択します。また、クライアント証明書が使用できなかった場合、電子メールゲートウェイがユーザを認証するためのSMTP AUTH コマンドにフォールバックするかどうかを指定できます。

組織でユーザを認証するためにクライアント証明書を使用する場合、クライアント証明書を持たないユーザがユーザのデータが許可するように指定されている限りメールを送信できるかどうか判断するために、SMTP 認証クエリを使用できます。

発信 SMTP 認証

SMTP 認証は、発信メール リレーをユーザ名とパスフレーズを使用して検証するときにも使用できます。「発信」SMTP 認証プロファイルを作成してから、このプロファイルを全ドメインの SMTP ルートに関連付けます。メール配信試行のたびに、 電子メールゲートウェイは必要なクレデンシャルを使用してアップストリーム メール リレーにログインします。SMTP 認証は、認証プロトコルの PLAIN と LOGIN をサポートします。

手順

ステップ 1 送信 SMTP 認証プロファイルを作成します。

1. [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] を選択します。
2. [プロファイルを追加（Add Profile）] をクリックします。
3. SMTP 認証プロファイルの一意の名前を入力します。
4. [プロファイルタイプ（Profile Type）] で [送信（Outgoing）] を選択します。
5. [次へ（Next）] をクリックします。
6. 認証プロファイルの認証用ユーザ名とパスフレーズを入力します。
7. [終了（Finish）] をクリックします。

ステップ 2 ステップ 1 で作成した送信 SMTP 認証プロファイルを使用するように、SMTP ルートを設定します。

1. [ネットワーク（Network）] > [SMTPルート（SMTP Routes）] を選択します。
2. テーブルの [受信ドメイン（Receiving Domain）] カラムで、[その他のすべてのドメイン（All Other Domains）] リンクをクリックします。
3. SMTP ルートの宛先ホストの名前を [宛先ホスト（Destination Host）] に入力します。これは、発信メールの配信に使用される外部メール リレーのホスト名です。
4. 発信 SMTP 認証プロファイルをドロップダウン メニューから選択します。
5. 変更を送信し、保存します。

ロギングと SMTP 認証

SMTP 認証メカニズム（LDAP ベース、SMTP 転送サーバベース、または SMTP 発信）が 電子メールゲートウェイ上で設定されている場合は、以下のイベントがメールログに記録されます。

- （情報）SMTP 認証成功：認証されたユーザと、使用されたメカニズムも記録されます。（プレーン テキストのパスフレーズが記録されることはありません）。

- （情報）SMTP 認証失敗：認証されたユーザと、使用されたメカニズムも記録されます。
- （警告）認証サーバに接続不可能：サーバ名とメカニズムも記録されます。
- （警告）タイムアウトイベント：転送サーバ（アップストリームの、インジェクションを行う 電子メールゲートウェイと通信）が認証要求を待つ間にタイムアウトした場合。

ユーザの外部 LDAP 認証の設定

ネットワーク上の LDAP ディレクトリを使用してユーザを認証するように 電子メールゲートウェイを設定できます。このように設定すると、ユーザが各自の LDAP ユーザ名とパスフレーズを使用してログインできるようになります。LDAP サーバに対する認証クエリを設定したら、 電子メールゲートウェイによる外部認証の使用をイネーブルにします（GUI の [システム管理（System Administration）] > [ユーザー（Users）] ページ、または CLI の **userconfig** コマンドを使用します）。

手順

ステップ 1 **ユーザー アカウントを検索するためのクエリーを作成します。** LDAP サーバプロファイルで、LDAP ディレクトリ内のユーザ アカウントを検索するためのクエリを作成します。

ステップ 2 **グループ メンバーシップ クエリーを作成します。** ユーザが特定のディレクトリ グループのメンバーかどうかを判断するためのクエリを作成します。

ステップ 3 **LDAP サーバを使用するように外部認証をセットアップします。** この LDAP サーバをユーザ認証に使用するように 電子メールゲートウェイをイネーブルにし、ユーザロールを LDAP ディレクトリ内のグループに割り当てます。詳細については、「Distributing Administrative Tasks」の章の「Adding Users」を参照してください。

（注） [LDAP] ページの [クエリのテスト（Test Query）] ボタン（または **ldaptest** コマンド）を使用して、クエリから返される結果が期待したとおりであることを確認します。詳細については、LDAP クエリのテスト （961 ページ）を参照してください。

次のタスク

関連項目

- ユーザー アカウント クエリ （988 ページ）
- グループ メンバーシップ クエリ （989 ページ）

ユーザー アカウント クエリ

外部ユーザを認証するために、AsyncOS はクエリを使用してそのユーザのレコードを LDAP ディレクトリ内で検索し、ユーザのフル ネームが格納されている属性を見つけます。選択したサーバ タイプに応じて、AsyncOS によってデフォルト クエリーとデフォルト属性が入力されます。アカウントが失効しているユーザは拒否するように電子メールゲートウェイを設定する

こともできます。それには、RFC 2307 で規定されている属性が LDAP ユーザレコード内で定義されている必要があります（shadowLastChange、shadowMax、および shadowExpire）。ユーザー レコードが存在するドメイン レベルのベース DN が必須です。

次の表に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するときに使用されるデフォルトのクエリ文字列とユーザのフル ネーム属性を示します。

表 *73*：デフォルトのユーザ アカウント クエリ文字列と属性：*Active Directory*

サーバー タイプ	アクティブディレクトリ
ベース DN	（ブランク）（ユーザー レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリ文字列	(&(objectClass=user)(sAMAccountName={u}))
ユーザのフル ネームが格納されている属性	displayName

次の表に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するときに使用されるデフォルトのクエリ文字列とユーザのフル ネーム属性を示します。

表 *74*：デフォルトのユーザ アカウント クエリ文字列と属性：*OpenLDAP*

サーバー タイプ	**OpenLDAP**
ベース DN	（ブランク）（ユーザー レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリ文字列	(&(objectClass=posixAccount)(uid={u}))
ユーザのフル ネームが格納されている属性	gecos

グループ メンバーシップ クエリ

AsyncOS は、ユーザが特定のディレクトリ グループのメンバーかどうかを判断するという目的でもクエリを使用します。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [システム管理（System Administration）]>[ユーザー（Users）] ページ（または CLI の userconfig）で外部認証をイネーブルにするときに、ユーザー ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザー ロールによって、そのユーザーがシステム内で持つアクセス許可が決まります。外部認証されたユーザーの場合は、ロールは個々のユーザーではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに Administrator ロールを割り当て、Support というディレクトリ グループのユーザに Help Desk User ロールを割り当てます。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリ文字列が AsyncOS によって入力されます。

（注） Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリ文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

次の表に、AsyncOS が Active Directory サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリ文字列と属性を示します。

表 *75 :* デフォルトのグループ メンバーシップ クエリ文字列と属性：*Active Directory*

サーバー タイプ	アクティブディレクトリ
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	(&(objectClass=group)(member={u})) （注） 使用する LDAP スキーマにおいて memberOf リストの中でユーザ名ではなく識別名が使用されている場合は、{u} の代わりに {dn} を使用できます。
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	member
グループ名が格納されている属性	cn

次の表に、AsyncOS が OpenLDAP サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリ文字列と属性を示します。

表 *76 :* デフォルトのグループ メンバーシップ クエリ文字列と属性：***OpenLDAP***

サーバー タイプ	**OpenLDAP**
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	(&(objectClass=posixGroup)(memberUid={u}))
各メンバーのユーザ名（またはそのユーザのレコードのDN）が格納されている属性	memberUid
グループ名が格納されている属性	cn

スパム隔離機能へのエンド ユーザ認証

スパム隔離へのエンドユーザ認証のクエリとは、ユーザがスパム隔離機能にログインするときにユーザを検証するためのクエリです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリによって「SMTP:」が電子メールアドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

スパム隔離機能のエンドユーザ アクセス検証に LDAP クエリを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにしてください。すでにアクティブなクエリがある場合、そのクエリはディセーブルになります。[システム管理（System Administration）]>[LDAP] ページを開いたときに、アクティブなクエリの横にアスタリスク（*）が表示されます。

サーバ タイプに基づいて、次のデフォルト クエリ文字列がエンドユーザ認証クエリに使用されます。

- **Active Directory**：(sAMAccountName={u})
- **OpenLDAP**：(uid={u})
- **不明またはそれ以外（Unknown or Other）**：（ブランク）

デフォルトでは、プライマリ メール属性は Active Directory サーバの場合は proxyAddresses、OpenLDAP サーバの場合は mail です。独自のクエリとメール属性を入力できます。クエリを CLI で作成するには、ldapconfig コマンドの isqauth サブコマンドを使用します。

（注） ユーザのログイン時に各自のメール アドレス全体を入力させる場合は、(mail=smtp:{a}) というクエリ文字列を使用します。

関連項目

- Active Directory エンドユーザ認証の設定例 （992 ページ）
- OpenLDAP エイリアス統合の設定例 （994 ページ）
- スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）

Active Directory エンドユーザ認証の設定例

ここでは、Active Directory サーバとエンドユーザ認証クエリの設定の例を示します。この例では、Active Directory サーバに対してパスフレーズ認証を使用し、メール属性は mail と proxyAddresses を使用し、Active Directory サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列を使用します。

表 *77 : LDAP* サーバとスパム隔離へのエンドユーザ認証の設定例：*Active Directory*

認証方式	パスフレーズを使用（検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）
サーバー タイプ	アクティブディレクトリ
ポート	3268
ベース DN	（ブランク）
接続プロトコル	（ブランク）
クエリ文字列	(sAMAccountName={u})
メール属性	mail,proxyAddresses

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、メール属性は mail と mailLocalAddress を使用し、OpenLDAP サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列を使用します。

表 *78 : LDAP* サーバとスパム隔離へのエンドユーザ認証の設定例：*OpenLDAP*

認証方式	匿名
サーバー タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）

認証方式	匿名
接続プロトコル	（ブランク）
クエリ文字列	(uid={u})
メール属性	mail,mailLocalAddress

スパム隔離のエイリアス統合クエリ

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリを使用して電子メールエイリアスを1つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメール アドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は1通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ電子メールアドレスとして選択されたアドレスです。

メッセージを統合してプライマリ電子メールアドレスに送信するには、受信者の代替電子メールエイリアスを検索するためのクエリを作成してから、受信者のプライマリ電子メールアドレスの属性を [メール属性（Email Attribute）] フィールドに入力します。

スパム隔離機能のスパム通知に LDAP クエリを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにしてください。すでにアクティブなクエリがある場合、そのクエリはディセーブルになります。[システム管理（System Administration）] > [LDAP] ページを開いたときに、アクティブなクエリの横にアスタリスク（*）が表示されます。

Active Directory サーバの場合は、デフォルトのクエリ文字列は (|(proxyAddresses={a})(proxyAddresses=smtp:{a})) で、デフォルトのメール属性は mail です。OpenLDAP サーバの場合は、デフォルトのクエリ文字列は (mail={a}) で、デフォルトのメール属性は mail です。独自のクエリとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。入力する電子メール属性が複数ある場合は、最初の電子メール属性として、変動する可能性のある値を複数持つ属性（たとえば proxyAddresses）ではなく、値を1つだけ使用する一意の属性（たとえば mail）を入力することを推奨します。

クエリを CLI で作成するには、ldapconfig コマンドの isqalias サブコマンドを使用します。

関連項目

- Active Directory エイリアス統合の設定例 （993 ページ）
- OpenLDAP エイリアス統合の設定例 （994 ページ）

Active Directory エイリアス統合の設定例

ここでは、Active Directory サーバとエイリアス統合クエリの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリ文字列を指定し、メール属性は mail を使用します。

表 *79 : LDAP* サーバとスパム隔離エイリアス統合の設定例：*Active Directory*

認証方式	匿名
サーバー タイプ	アクティブディレクトリ
ポート	3268
ベース DN	（ブランク）
接続プロトコル	SSL を使用する（Use SSL）

クエリ文字列	`(`
	`|(mail={a})(mail=smtp:{a})`
	`)`

メール属性	メール アドレス

（注） この例は、説明のみを目的としています。クエリおよびOU、またはツリー設定は、環境と設定によって異なる場合があります。

OpenLDAP エイリアス統合の設定例

ここでは、OpenLDAP サーバとエイリアス統合クエリの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリ文字列を指定し、メール属性は mail を使用します。

表 *80 : LDAP* サーバとスパム隔離エイリアス統合の設定例：*OpenLDAP*

認証方式	匿名
サーバー タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	SSL を使用する（Use SSL）
クエリ文字列	(mail={a})
メール属性	メール アドレス

（注） この例は、説明のみを目的としています。クエリおよびOU、またはツリー設定は、環境と設定によって異なる場合があります。

ユーザ識別名の設定の例

ここでは、Active Directory サーバとエンドユーザ識別名クエリの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するユーザの識別名検索用のクエリ文字列を指定ます。

表 *81 : LDAP* サーバとスパム隔離エイリアス統合の設定例：*Active Directory*

認証方式	匿名
サーバー タイプ	アクティブディレクトリ
ポート	3268
ベース DN	（ブランク）
接続プロトコル	SSL を使用する（Use SSL）
クエリ文字列	`(proxyAddresses=smtp:{a})`

（注） この例は、説明のみを目的としています。クエリおよびOU、またはツリー設定は、環境と設定によって異なる場合があります。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP プロファイルを設定するときに、 電子メールゲートウェイからの接続先となる複数の LDAP サーバのリストを接続するように設定できます。複数の LDAP サーバを使用するには、LDAP サーバに格納されている情報が同一になるように設定する必要があります。また、構造も同一で、使用する認証情報も同一でなければなりません（レコードを統合できる製品がサードパーティから提供されています）。

冗長化した複数のLDAPサーバに接続するように電子メールゲートウェイを設定すると、LDAPのフェールオーバーまたはロードバランシングを設定できます。

複数の LDAP サーバを使用すると、次のことが可能になります。

- **フェールオーバー**。フェールオーバーのための LDAP プロファイルを設定しておくと、電子メールゲートウェイが最初のLDAPサーバに接続できなくなったときに、リスト内の次の LDAP サーバへのフェールオーバーが行われます。

- **ロード バランシング**。ロードバランシングのための LDAP プロファイルを設定しておくと、電子メールゲートウェイが LDAP クエリを実行するときに、接続がリスト内の LDAP サーバに分散されます。

冗長 LDAP サーバを設定するには、[システム管理（System Administration）] > [LDAP] ページまたは CLI の ldapconfig コマンドを使用します。

サーバとクエリのテスト

[Add（または Edit）LDAP Server Profile] ページの [テストサーバ（Test Server(s)）] ボタン（または CLI の **test** サブコマンド）を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリのテストも実行されて、結果が個別に表示されます。

関連項目

- フェールオーバー （996 ページ）
- ロード バランシング （997 ページ）

フェールオーバー

LDAP クエリが確実に解決されるようにするには、フェールオーバーのための LDAP プロファイルを設定します。LDAP サーバへの接続に失敗した場合、または問い合わせで特定のエラーコード（利用不可やビジーなど）が返される場合、電子メールゲートウェイはリストで指定されている次の LDAP サーバへの問い合わせを試行します。

電子メールゲートウェイは、LDAP サーバリスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。電子メールゲートウェイがリストの最初の LDAP サーバに接続できない場合、または問い合わせで特定のエラーコード（利用不可やビジーなど）が返される場合、電子メールゲートウェイはリストの次の LDAP サーバへの接続を試行します。デフォルトでは、電子メールゲートウェイは常にリスト内の最初のサーバへの接続を試行し、それ以降の各サーバへの接続を、リスト内で指定されている順に試行します。電子メールゲートウェイが確実にプライマリの LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバリストの先頭に入力されていることを確認してください。

電子メールゲートウェイが 2 番目以降の LDAP サーバに接続した場合は、タイムアウトの時間に達するまで、そのサーバに接続したままになります。タイムアウトの時間に達すると、リスト内の最初のサーバへの再接続が試行されます。

（注） 指定された LDAP サーバを問い合わせる試行のみがフェールオーバーします。指定された LDAP サーバに関連付けられた参照サーバまたは継続サーバを問い合わせる試行はフェールオーバーしません。

関連項目

- LDAP フェールオーバーのための電子メールゲートウェイの設定 （997 ページ）

LDAP フェールオーバーのための電子メールゲートウェイの設定

LDAP フェールオーバーを行うように電子メールゲートウェイを設定するには、GUI で以下の手順を実行します。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2 LDAP サーバ プロファイルから、次の項目を設定します。

ケース	説明
1	LDAP サーバの一覧を表示します。
2	最大接続数を設定します。

ステップ 3 他の LDAP 設定を指定して変更を確定します。

ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロードバランシングのための LDAP プロファイルを設定しておくと、電子メールゲートウェイからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、電子メールゲートウェイは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。電子メールゲートウェイは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、電子メールゲートウェイからの接続の負荷は残りの LDAP サーバに分散されます。

関連項目

- ロードバランシングのための電子メールゲートウェイの設定 （998 ページ）

ロードバランシングのための電子メールゲートウェイの設定

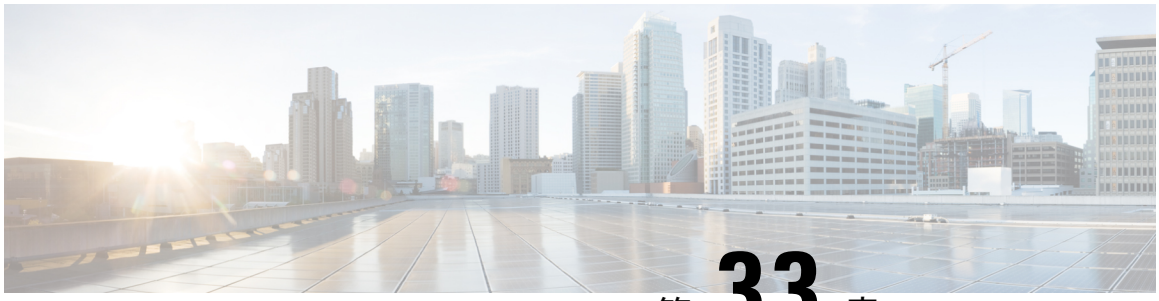
手順

ステップ 1 [システム管理（System Administration）] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2 LDAP サーバ プロファイルから、次の項目を設定します。

ケース	説明
1	LDAP サーバの一覧を表示します。
2	最大接続数を設定します。

ステップ 3 他の LDAP 設定を指定して変更を確定します。



第 33 章

クライアント証明書を使用したSMTPセッションの認証

この章は、次の項で構成されています。

- 証明書と SMTP 認証の概要 （999 ページ）
- クライアント証明書の有効性の確認 （1001 ページ）
- LDAP ディレクトリを使用したユーザの認証 （1002 ページ）
- クライアント証明書を使用した TLS 経由の SMTP 接続の認証 （1003 ページ）
- 電子メールゲートウェイからの TLS 接続の確立 （1003 ページ）
- 無効にされた証明書のリストの更新 （1004 ページ）

証明書と SMTP 認証の概要

電子メールゲートウェイは、電子メールゲートウェイとユーザのメールクライアント間のSMTPセッションを認証するためにクライアント証明書の使用をサポートします。電子メールゲートウェイは、アプリケーションがメッセージを送信するために電子メールゲートウェイに接続しようとするときに、ユーザのメールクライアントからのクライアント証明書を要求することができます。電子メールゲートウェイがクライアント証明書を受け取ったとき、証明書が有効である、有効期限が切れていない、無効になっていないことを確認します。証明書が有効であれば、電子メールゲートウェイは TLS 経由でメールアプリケーションからの SMTP 接続を許可します。

ユーザがメールクライアントにCommon Access Card（CAC）を使用する必要がある組織では、CAC および ActivClient のミドルウェア アプリケーションが電子メールゲートウェイに提供する証明書を要求するために、この機能を使用して電子メールゲートウェイを設定できます。

メールの送信時にユーザに証明書を提供することを要求するように電子メールゲートウェイを設定できますが、ここでは特定のユーザに対する例外を許可します。これらのユーザには、ユーザの認証にSMTP認証LDAPクエリーを使用するように電子メールゲートウェイを設定できます。

ユーザはセキュア接続（TLS）経由でメッセージを送信するために自分のメールクライアントを設定し、電子メールゲートウェイからサーバ証明書を受け入れる必要があります。

関連項目

- クライアント証明書でのユーザの認証方法 （1000 ページ）
- SMTP 認証 LDAP クエリでのユーザの認証方法 （1000 ページ）
- クライアント認証が無効な場合の LDAP SMTP 認証クエリでのユーザの認証方法 （1001 ページ）

クライアント証明書でのユーザの認証方法

表 *82* : クライアント証明書でのユーザの認証方法

	操作内容	詳細
ステップ 1	LDAP サーバの認証クエリを定義します。	クライアント証明書の有効性の確認 （1001 ページ）
ステップ 2	証明書ベースの SMTP 認証プロファイルを作成します。	クライアント証明書を使用した TLS 経由の SMTP 接続の認証 （1003 ページ）
ステップ 3	証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。	Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング （88 ページ）
ステップ 4	TLS、クライアント認証および SMTP 認証を要求するように RELAYED メール フロー ポリシーを変更します。	電子メールゲートウェイからの TLS 接続の確立 （1003 ページ）

SMTP 認証 LDAP クエリでのユーザの認証方法

表 *83* : *SMTP* 認証 *LDAP* クエリでのユーザの認証方法

	操作内容	詳細
ステップ 1	許可クエリー文字列と認証方式のバインドを使用する、サーバの SMTP 認証クエリーを定義します。	LDAP ディレクトリを使用したユーザの認証 （1002 ページ）
ステップ 2	LDAP ベースの SMTP 認証プロファイルを作成します。	SMTP 認証を行うための AsyncOS の設定 （979 ページ）
ステップ 3	LDAP の SMTP 認証プロファイルを使用するようにリスナーを設定します。	ユーザが接続で LDAP ベースの SMTP 認証の使用を許可されていない場合は、電子メールゲートウェイが接続拒否するか、すべてのアクティビティを記録する間一時的に許可するかを選択します。
ステップ 4	TLS および SMTP 認証を要求するように RELAYED メール フロー ポリシーを変更します。	電子メールゲートウェイからの TLS 接続の確立 （1003 ページ）

クライアント認証が無効な場合のLDAP SMTP認証クエリでのユーザの認証方法

表 *84 :* クライアント認証または *LDAP SMTP* 認証クエリーでのユーザの認証方法

	操作内容	詳細
ステップ 1	許可クエリー文字列と認証方式のバインドを使用する、サーバの SMTP 認証クエリーを定義します。	LDAPディレクトリを使用したユーザの認証（1002ページ）
ステップ 2	LDAPサーバの認証ベースのクエリーを定義します。	クライアント証明書の有効性の確認（1001ページ）
ステップ 3	証明書ベースの SMTP 認証プロファイルを作成します。	クライアント証明書を使用した TLS 経由の SMTP 接続の認証（1003 ページ）
ステップ 4	LDAP の SMTP 認証プロファイルを作成します。	SMTP認証を行うためのAsyncOSの設定（979ページ）
ステップ 5	証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。	Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング（88 ページ）
ステップ 6	1. 次の設定を使用するように RELAYED メール フロー ポリシーを変更します。 2. TLS 推奨 3. SMTP 認証必須 4. SMTP 認証のために TLS が必要	電子メールゲートウェイからの TLS 接続の確立（1003 ページ）

クライアント証明書の有効性の確認

ユーザのメールクライアントと 電子メールゲートウェイ間の SMTP セッションを認証するために、証明書認証LDAPクエリがクライアント証明書の有効性をチェックします。このクエリを作成する際に、認証のための証明書フィールドのリストを選択して、ユーザー ID 属性（デフォルトは uid）を指定して、クエリ文字列を入力します。

たとえば、証明書の共通名とシリアル番号を検索するクエリー文字列は、**`(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`** のようになります。クエリーを作成した後で、証明書SMTP認証プロファイルで使用できます。このLDAPクエリーは、OpenLDAP、Active Directory および Oracle Directory をサポートします。

LDAP サーバの設定の詳細については、LDAP クエリ（943 ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2 新しい LDAP プロファイルを作成します。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （947 ページ）を参照してください。

ステップ 3 [認証クエリーを証明（Certificate Authentication Query）] チェックボックスをオンにします。

ステップ 4 クエリー名を入力します。

ステップ 5 ユーザの証明書を認証するためのクエリー文字列を入力します。たとえば、**(&(objectClass=user)(cn={cn}))** と入力します。

ステップ 6 **sAMAccountName** などのユーザ ID 属性を入力します。

ステップ 7 変更を送信し、保存します。

LDAP ディレクトリを使用したユーザの認証

SMTP 認証 LDAP クエリーには、電子メールゲートウェイがユーザのメールクライアントが LDAP ディレクトリのユーザのレコードに基づいて電子メールゲートウェイを介してメール送信できるかを判断する、許可クエリー文字列が含まれています。これは、レコードに許可することが指定してされていれば、クライアントの証明書のないユーザがメールを送信することが可能です。

その他の属性に基づいた結果のフィルタリングもできます。たとえば、`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` というクエリー文字列は、次の条件のいずれかがユーザに当てはまるかどうかチェックします。

- CAC がユーザに発行されていない（`caccn=*`）
- CAC が免除される（`cacexempt=*`）
- CAC なしで一時的にユーザがメールを送信できる期間が将来切れる（`cacemergency>={t}`）

SMTP 認証クエリーの使用の詳細については、SMTP 認証を行うための AsyncOS の設定 （979 ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2 LDAP プロファイルを定義します。詳細については、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルの作成 （947 ページ）を参照してください。

ステップ 3 LDAP プロファイルの SMTP 認証クエリーを定義します。

ステップ 4 [SMTP 認証クエリー（SMTP Authentication Query）] チェックボックスをオンにします。

ステップ 5 クエリー名を入力します。

ステップ 6 ユーザの ID を問い合わせる文字列を入力します。たとえば、`(uid={u})`。

ステップ 7 認証方式に [LDAP BIND] を選択します。

ステップ 8 許可クエリー文字列を入力します。たとえば、`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`。

ステップ 9 変更を送信し、保存します。

クライアント証明書を使用した TLS 経由の SMTP 接続の認証

証明書ベースの SMTP 認証プロファイルでは、電子メールゲートウェイがクライアント証明書を使用して TLS 経由の SMTP 接続を認証できます。プロファイルを作成する場合、証明書を確認するために使用する証明書認証 LDAP クエリーを選択します。また、クライアント証明書が使用できなかった場合、電子メールゲートウェイがユーザを認証するための **SMTP AUTH** コマンドにフォールバックするかどうかを指定できます。

LDAP を使用した SMTP 接続の認証の詳細については、SMTP 認証を行うための AsyncOS の設定 （979 ページ）を参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [SMTP 認証（SMTP Authentication）] を選択します。
ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。
ステップ 3 SMTP 認証プロファイルの名前を入力します。
ステップ 4 [プロファイルタイプ（Profile Type）] で [証明書（Certificate）] を選択します。
ステップ 5 [Next] をクリックします。
ステップ 6 プロファイル名を入力します。
ステップ 7 この SMTP 認証プロファイルに使用する証明書 LDAP クエリーを選択します。

（注） クライアント証明書が使用可能でない場合、SMTP AUTH コマンドを許可するオプションを選択しないでください。

ステップ 8 [終了（Finish）] をクリックします。
ステップ 9 変更を送信し、保存します。

電子メールゲートウェイからの TLS 接続の確立

RELAYED メールフローポリシーの [クライアント証明書の検証（Verify Client Certificate）] オプションは、クライアント証明書が有効な場合ユーザのメールアプリケーションへの TLS 接続を確立するように 電子メールゲートウェイに指示します。TLS 推奨設定にこのオプションを選択した場合、ユーザが証明書を持たない場合にも 電子メールゲートウェイは非 TLS 接続を許可しますが、ユーザが無効な証明書を持っている場合は、接続を拒否します。TLS 必須設定の場合、このオプションを選択すると、電子メールゲートウェイが接続を許可するために有効な証明書が必要になります。

クライアント証明書を持つユーザの SMTP セッションを認証するには、次の設定を選択します。

- TLS 必須（TLS - Required）
- クライアント証明書の検証（Verify Client Certificate）
- SMTP 認証が必要（Require SMTP Authentication）

（注） SMTP 認証は必須ですが、 電子メールゲートウェイは証明書認証を使用しているため、SMTP 認証 LDAP クエリを使用しません。

クライアント証明書の代わりにSMTP認証クエリーを使用して、ユーザのSMTPセッションを認証するには、次の RELAYED メール フロー ポリシーの設定を選択します。

- TLS 必須（TLS - Required）
- SMTP 認証が必要（Require SMTP Authentication）

他のユーザからのLDAPベースのSMTP認証を許可する一方で、特定のユーザからのクライアント証明書の認証を要求するように電子メールゲートウェイに要求するには、次のRELAYEDメールフローポリシーの設定を選択します。

- TLS 推奨（TLS - Preferred）
- SMTP 認証が必要（Require SMTP Authentication）
- TLS に SMTP 認証を提供するよう義務付けます。

無効にされた証明書のリストの更新

E メール セキュリティ アプライアンスは、ユーザの証明書が失効していないことを確認するために、証明書検証の一環として（証明書失効リストと呼ばれる）失効した証明書のリストを確認します。サーバ上でこのリストを最新のバージョンに保ち、電子メールゲートウェイはユーザが作成したスケジュールでこれをダウンロードします。

手順

ステップ 1 [ネットワーク（Network）] > [CRL ソース（CRL Sources）] に移動します。

ステップ 2 SMTP TLS 接続のため CRL チェックをイネーブルにします。

a) [グローバル設定（Global Settings）] で [設定を編集（Edit Settings）] をクリックします。

b) （省略可能）すべてのオプションを選択する場合、[グローバル設定（Global Settings）] チェック ボックスを選択します。

- インバウンドSMTP TLSのCRLチェック（CRL check for inbound SMTP TLS）。
- アウトバウンドSMTP TLSのCRLチェック（CRL check for outbound SMTP TLS）
- WebインターフェイスのCRLチェック（CRL Check for Web Interface）

c) [インバウンドSMTP TLSのCRLチェック（CRL check for inbound SMTP TLS）]、[アウトバウンドSMTP TLSのCRLチェック（CRL check for outbound SMTP TLS）] または [Webインターフェイスの CRL チェック（CRL Check for Web Interface）] オプションのいずれかのチェック ボックスを選択します。
d) 変更を送信します。

ステップ 3 [CRL ソースの追加（Add CRL Source）] をクリックします。

ステップ 4 CRL ソースの名前を入力します。

ステップ 5 ファイル タイプを選択します。ASN.1 または PEM を指定できます。

ステップ 6 ファイル名を含むファイルのプライマリ ソースの URL を入力します。たとえば、**`https://crl.example.com/certs.crl`**

ステップ 7 電子メールゲートウェイがプライマリ ソースに接続できない場合は、必要に応じて 2 番目のソースの URL を入力します。

ステップ 8 CRL ソースをダウンロードするスケジュールを指定します。

ステップ 9 CRL ソースをイネーブルにします。

ステップ 10 変更を送信し、保存します。

クライアント証明書を使用したユーザの SMTP セッションの認証

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] に移動して、LDAP サーバ プロファイルを設定します

ステップ 2 LDAP プロファイルの証明書クエリーを定義します。

a) クエリー名を入力します。
b) 認証する証明書フィールド（シリアル番号、共通名など）を選択します。
c) クエリー文字列を入力します。たとえば、**`(&(caccn={cn})(cacserial={sn}))`**。
d) uid などのユーザ ID フィールドを入力します。
e) 変更を送信します。

ステップ 3 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] に移動し、証明書 SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する証明書 LDAP クエリーを選択します。
c) クライアント証明書が使用可能でない場合、**`SMTP AUTH`** コマンドを許可するオプションを選択しないでください。
d) 変更を送信します。

ステップ 4 [ネットワーク（Network）] > [リスナー（Listener）] に移動して、作成した証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。

ステップ 5 TLS、クライアント認証およびSMTP認証を要求するようにRELAYEDメールフローポリシーを変更します。

（注） SMTP 認証は必須ですが、 電子メールゲートウェイは証明書認証を使用しているため、SMTP AUTH コマンドを使用しません。電子メールゲートウェイは、ユーザを認証するためにメールアプリケーションからのクライアント証明書を要求します。

ステップ 6 変更を送信し、保存します。

SMTP AUTH コマンドを使用したユーザの SMTP セッションの認証

電子メールゲートウェイでは、クライアント証明書の代わりにSMTP AUTHコマンドを使用してユーザのSMTPセッションを認証することができます。ユーザが接続でSMTP AUTHの使用を許可されていない場合は、電子メールゲートウェイが接続拒否するか、すべてのアクティビティを記録する間一時的に許可するかを選択できます。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] に移動して、LDAP サーバ プロファイルを設定します。

ステップ 2 LDAP プロファイルの SMTP 認証クエリーを定義します。

a) クエリー名を入力します。
b) クエリー文字列を入力します。たとえば、**(uid={u})**。
c) 認証方式として [LDAP BIND] を選択します。
d) 許可クエリー文字列を入力します。たとえば、**(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))**。
e) 変更を送信します。

ステップ 3 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] に移動し、LDAP SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する SMTP 認証 LDAP クエリーを選択します。
c) [ユーザがSMTP AUTHコマンドを使用できるかどうかをLDAPで確認する （Check with LDAP if user is allowed to use SMTP AUTH Command）] を選択し、ユーザのアクティビティをモニタして報告することを選択します。
d) 変更を送信します。

ステップ 4 [ネットワーク（Network）] > [リスナー（Listener）] に移動して、作成した LDAP SMTP 認証プロファイルを使用するようにリスナーを設定します。

ステップ 5 TLS および SMTP 認証を要求するように RELAYED メール フロー ポリシーを変更します。

ステップ 6 変更を送信し、保存します。

クライアント証明書または SMTP AUTH を使用したユーザの SMTP セッションの認証

この設定では、電子メールゲートウェイが、クライアント証明書を持つユーザに対してはクライアント認証を要求し、クライアント認証を持たないユーザまたは電子メールの送信にクライアント認証を使用できないユーザに対しては SMTP AUTH を許可する必要があります。

許可されていないユーザによる SMTP AUTH コマンドの使用は禁止されます。

手順

ステップ 1 [システム管理（System Administration）] > [LDAP] に移動して、LDAP サーバ プロファイルを設定します。

ステップ 2 プロファイルの SMTP 認証クエリーを定義します。

a) クエリー名を入力します。
b) クエリー文字列を入力します。たとえば、**(uid={u})**。
c) 認証方式として [LDAP BIND] を選択します。
d) 許可クエリー文字列を入力します。たとえば、**(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))**。

ステップ 3 LDAP プロファイルの証明書クエリーを定義します。

a) クエリー名を入力します。
b) 認証するクライアント証明書フィールド（シリアル番号、共通名など）を選択します。
c) クエリー文字列を入力します。たとえば、**(&(caccn={cn})(cacserial={sn}))**。
d) uid などのユーザ ID フィールドを入力します。
e) 変更を送信します。

ステップ 4 [ネットワーク（Network）] > [SMTP認証（SMTP Authentication）] に移動し、LDAP SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する SMTP 認証 LDAP クエリーを選択します。
c) [ユーザがSMTP AUTHコマンドを使用できるかどうかをLDAPで確認する（Check with LDAP if user is allowed to use SMTP AUTH Command）] を選択し、接続を拒否することを選択します。
d) カスタム SMTP AUTH 応答を入力します。たとえば 525, “Dear user, please use your CAC to send email.” と入力します。
e) 変更を送信します。

ステップ 5 証明書 SMTP 認証プロファイルを設定します。

a) プロファイル名を入力します。
b) 使用する証明書 LDAP クエリーを選択します。
c) クライアント証明書が使用可能でない場合、SMTP AUTH コマンドを許可するオプションを選択します。

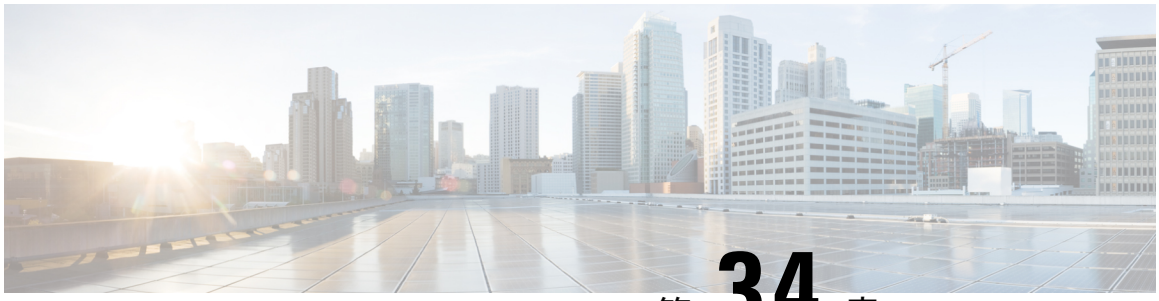
d) ユーザにクライアント証明書がない場合に電子メールゲートウェイが使用する LDAP SMTP 認証プロファイルを選択します。
e) 変更を送信します。

ステップ 6 [ネットワーク（Network）] > [リスナー（Listener）] に移動して、作成した証明書 SMTP 認証プロファイルを使用するようにリスナーを設定します。

ステップ 7 RELAYED メール フロー ポリシーを変更して次のオプションを選択します。

- TLS 推奨
- SMTP 認証必須
- SMTP 認証のために TLS が必要

ステップ 8 変更を送信し、保存します。



第 34 章

電子メール セキュリティ モニタの使用方法

この章は、次の項で構成されています。

- 電子メール セキュリティ モニタの概要 （1009 ページ）
- 電子メール セキュリティ モニタ ページ （1011 ページ）
- 新しい Web インターフェイスの電子メール セキュリティ モニタ ページ （1053 ページ）
- レポート作成の概要 （1106 ページ）
- レポートの管理 （1108 ページ）
- メール レポートのトラブルシューティング （1112 ページ）

電子メール セキュリティ モニタの概要

電子メールセキュリティモニタ機能は、電子メール配信プロセスのすべてのステップからデータを収集します。データベースは、IPアドレスに基づいて各電子メールの送信者を識別して記録します。また、IP レピュテーションサービスと連携してリアルタイムのアイデンティティ情報を収集します。ユーザは、すべての電子メール送信者のローカル メール フロー履歴をただちに報告し、インターネット上の送信者のグローバル情報を含むプロファイルを表示できます。電子メール セキュリティ モニタ機能では、セキュリティ チームが、ユーザへのメール送信者、ユーザによって送受信されるメールの量、およびセキュリティ ポリシーの有効性の「ループを閉じる」ことができます。

この章では、次の方法について説明します。

- 発着するメッセージ フローをモニタするための電子メール セキュリティ モニタ機能へのアクセス。
- 送信者の IP レピュテーションスコアを照会したメールフローポリシーの決定（許可リスト、ブロックリスト、およびグレーリストの更新）。ネットワーク オーナー、ドメイン、さらには個別の IP アドレスについてもクエリーを実行できます。
- メール フロー、メール ステータスおよびシステムに送受信されたメールに関する報告。

電子メール セキュリティ モニタ データベースでは、着信メールの所定の電子メール送信者について、次の重要パラメータを取得します。

- メッセージの量
- 接続履歴
- 受け入れられた接続と拒否された接続の比率
- 受け入れ率と調整上限値
- 送信者レピュテーション フィルタの一致率
- スパムの疑いのある、および明白にスパムと識別されるアンチスパム メッセージの数
- アンチ ウイルス スキャンによって検出されたウイルス陽性メッセージの数

アンチスパム スキャンの詳細については、スパムおよびグレイメールの管理（461 ページ）を参照してください。アンチウイルス スキャンについては、アンチウイルス（439 ページ）を参照してください。

電子メール セキュリティ モニタ機能は、内部ユーザ（電子メール受信者）またはメッセージの送信者を含む、特定のメッセージによってトリガーされたコンテンツ フィルタに関する情報も取得します。

電子メールセキュリティモニタ機能は GUI だけで使用でき、電子メールトラフィックおよび電子メールゲートウェイ（隔離、ワークキュー、感染など）のステータスへのビューを提供します。電子メールゲートウェイは、送信者が標準のトラフィックプロファイルの範囲に該当しない場合に識別します。識別された送信者はインターフェイスで強調表示されるので、送信者を送信者グループに割り当てるか、送信者のアクセスプロファイルを変更することによって是正措置を取ることができます。または、引き続き AsyncOS のセキュリティ サービスに対応させることができます。送信メールにも同様のモニタリング機能があり、メールキューの上位ドメインおよび受信ホストのステータスにビューを提供します（[送信処理ステータス詳細（Delivery Status Details）] ページ （1030 ページ）を参照）。

（注） 電子メールセキュリティモニタ機能では、電子メールゲートウェイの再起動時にワークキューに存在したメッセージの情報は報告されません。

関連項目

- 電子メール セキュリティ モニタと集中管理 （1010 ページ）

電子メール セキュリティ モニタと集中管理

集約レポートデータを表示するには、 Cisco Secure Email and Web Manager を導入します。

クラスタ化されたアプライアンスの電子メール セキュリティ モニタ レポートは集約できません。すべてのレポートは、マシン レベルに制限されます。つまりレポートは、グループ レベルまたはクラスタ レベルでは実行できません。個別のマシンのみで実行できます。

[アーカイブ レポート（Archived Reports）]ページについても同様です。設定されている各マシンは、独自のアーカイブを備えています。したがって、「レポート生成」機能は、選択したマシンのみで実行されます。

[定期レポート（Scheduled Reports）]ページは、マシン レベルに制限されません。したがって、複数のマシンで設定を共有できます。マシン レベルで実行された、個別のスケジュール設定されたレポートは、インタラクティブ レポートとまったく同様なので、クラスタ レベルでスケジュール設定されたレポートを設定する場合、クラスタ内の各マシンが独自のレポートを送信します。

[このレポートをプレビュー（Preview This Report）]ボタンは、ログインホストに対して常に実行できます。

電子メール セキュリティ モニタ ページ

電子メール セキュリティ モニタ機能は、[モニタ（Monitor）] メニューで使用可能なすべてのページ（ただし [隔離（Quarantines）] ページは除く）で構成されます。

GUI でこれらのページを使用して、アプライアンスのリスナーに接続しているドメインをモニタできます。お使いの電子メールゲートウェイの「メールフロー」のモニタ、ソート、分析、および分類を実行し、正規メールの大量送信者と「スパマー」（未承諾の商業用メールの大量送信者）またはウイルス送信者の疑いのあるユーザとを区別できます。これらのページは、システムへの着信接続のトラブルシューティングにも役立ちます（IP レピュテーションスコア、ドメインに対する直近の送信グループの一致など重要情報を含みます）。

これらのページは、電子メールゲートウェイに関連するメール、さらにゲートウェイの範囲を超えて存在するサービス（IP レピュテーションサービス、アンチスパム スキャン サービス、アンチウイルス スキャン セキュリティ サービス、コンテンツフィルタ、およびアウトブレイクフィルタ）に関連するメールの分類に役立ちます。

ページ右上の [印刷用 PDF（Printable PDF）] リンクをクリックすると、すべての電子メール セキュリティ モニタ ページを読みやすい印刷形式の PDF 版で生成できます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

[エクスポート（Export）] リンクでは、グラフおよび他のデータを Comma Separated Value（CSV; カンマ区切り値）形式にエクスポートできます。

エクスポートされた CSV データは、電子メールゲートウェイでの設定にかかわらず、すべてのメッセージトラッキングおよびレポーティングデータを GMT で示します。GMT 時間への変換の目的は、電子メールゲートウェイに依存せずにデータを使用したり、複数の時間帯にあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

（注） ローカライズされた CSV データをエクスポートする場合、一部のブラウザでは見出しが正しく表示されないことがあります。これは、ローカライズされたテキストに対して、一部のブラウザが適切な文字セットを使用していないためです。この問題を回避するには、ファイルをディスクに保存し、[ファイル（File）] > [開く（Open）] を使用してファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

レポートデータのエクスポートの自動化の詳細については、CSVデータの取得（1050ページ）を参照してください。

電子メール セキュリティ モニタ ページのリスト

- [マイ ダッシュボード（My Dashboard）] ページ （1014 ページ）
- [概要（Overview）] ページ （1015 ページ）
- [受信メール（Incoming Mail）] ページ （1020 ページ）
- 送信先 （1027 ページ）
- 送信者 （1028 ページ）
- [送信処理ステータス（Delivery Status）] ページ （1029 ページ）
- [内部ユーザ（Internal Users）] ページ （1030 ページ）
- [DLP インシデント（DLP Incidents）] ページ （1032 ページ）
- [コンテンツフィルタ（Content Filters）] ページ （1033 ページ）
- [DMARC検証（DMARC Verification）] ページ （1034 ページ）
- [アウトブレイク フィルタ（Outbreak Filters）] ページ （1035 ページ）
- [ウイルス タイプ（Virus Types）] ページ （1037 ページ）
- [URL フィルタリング（URL Filtering）] ページ （1038 ページ）
- [Webインタラクショントラッキング（Web Interaction Tracking）] ページ （1039 ページ）
- ファイル レピュテーションおよびファイル分析レポート （1040 ページ）
- [TLS 接続（TLS Connections）] ページ （1041 ページ）
- [受信 SMTP 認証（Inbound SMTP Authentication）] ページ （1042 ページ）
- [レート制限（Rate Limits）] ページ （1043 ページ）
- [システム容量（System Capacity）] ページ （1043 ページ）
- [システムステータス（System Status）] ページ （1047 ページ）
- [大容量のメール（High Volume Mail）] ページ （1049 ページ）
- [メッセージフィルタ（Message Filters）] ページ （1050 ページ）
- 地理的分散ページ （1028 ページ）
- [Safe Print] ページ （1050 ページ）

検索と電子メール セキュリティ モニタ

電子メール セキュリティ モニタ ページの多くには、検索フォームが含まれています。次の各種項目を検索できます。

- IP アドレス（IPv4 および IPv6）
- ドメイン
- ネットワーク オーナー
- 内部ユーザ
- 宛先ドメイン
- 内部送信者のドメイン
- 内部送信者の IP アドレス
- 発信ドメインの配信ステータス

ドメイン、ネットワーク オーナー、および内部ユーザの検索では、検索テキストに完全に一致させるか、入力したテキストで始まる項目（たとえば、「ex」で始まる場合は「example.com」に一致します）を検索するかを選択します。

IPv4 アドレス検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば「17」と入力すると、17.0.0.0 ～ 17.255.255.255 の範囲が検索されます。17.0.0.1 には一致しますが、172.0.0.1 には一致しません。完全一致検索の場合は、4 オクテットすべてを入力するだけです。IP アドレス検索は、CIDR 形式（17.16.0.0/12）もサポートしています。

IPv6 アドレス検索では、AsyncOS は次の形式をサポートします。

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

すべての検索は、ページで現在選択されている時間範囲に限定されます。

レポートに含まれるメッセージの詳細の表示

この機能は、レポートとトラッキングが両方ともローカルの場合（Cisco Secure Email and Web Managerで中央管理されていない場合）にのみ、機能します。

手順

ステップ 1 レポート ページのテーブルにある青色の番号をクリックします

（一部のテーブルにのみ、これらのリンクはあります）。

この番号に関連するメッセージがメッセージ トラッキングで表示されます。

ステップ 2 下にスクロールして、リストを表示します。

次のタスク

関連項目

- メッセージ トラッキングの検索結果の使用 （1121 ページ）

[マイ ダッシュボード（My Dashboard）] ページ

既存のレポートのページからチャート（グラフ）とテーブルを組み合わせてカスタム電子メール セキュリティ レポートのページを作成できます。

目的	操作手順
カスタム レポート ページにモジュールを追加	1. **[モニタ（Monitor）]** > [マイダッシュボード（My Dashboard）] に移動し、モジュールの右上にある [X] をクリックして不要なサンプル モジュールを削除します。 2. 次のいずれかを実行します。 • カスタム レポートにモジュールを追加するには、[モニタ（Monitor）] メニューの下のレポート ページ内のモジュール上の [+] ボタンをクリックします。 • **[モニタ（Monitor）]** > [マイダッシュボード（My Dashboard）] に移動し、いずれかのセクションの [+] ボタンをクリックし、追加するレポート モジュールを選択します。必要なレポートを見つけるために、各セクションの [+レポートモジュール（+ Report Module）] を確認する必要がある場合があります。 3. モジュールがデフォルト設定に追加されます。カスタマイズした（たとえば、列を追加、削除、または並べ替えしたり、）モジュールを追加する場合は、これらのモジュールを追加した後、再度カスタマイズします。元のモジュールの時間範囲は保持されません。 4. 別に凡例を持つチャート（たとえば、[概要（Overview）]ページからのグラフ）を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。 （注） • 特定のレポート ページの特定のモジュールは、上記の方法のいずれかを使用した場合のみ使用できます。ある方式を使用してモジュールを追加できない場合は、他の方法を試してください。 • 各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

目的	操作手順
カスタム レポート ページの表示	1. **[モニタ（Monitor）] >** [マイダッシュボード（My Dashboard）] を選択します。 2. [時間範囲（Time Range）] セクションのレポートの場合：すべてのレポートのページ用に選定された時間範囲は [マイ ダッシュボード（My Dashboard）] ページのすべてのモジュールに適用されます。表示する時間範囲を選択します。 新しく追加されたモジュールは関連するセクションの上部に表示されます。
カスタム レポート ページでのモジュールの再配置	目的の場所にモジュールをドラッグ アンド ドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。

[概要（Overview）] ページ

[概要（Overview）] ページには、隔離および（このページの [システム概要（System Overview）] セクションの）アウトブレイクフィルタのステータスの概要など、お使いの電子メールゲートウェイのメッセージアクティビティの概要が示されます。[概要（Overview）] ページには、グラフや、送受信メッセージの詳細なメッセージ数も表示されます。このページを使用して、ゲートウェイから出入りするすべてのメールのフローをモニタできます。

[概要（Overview）] ページには、受信メール（レピュテーション フィルタリングによって停止されたメッセージなど）に関して、 電子メールゲートウェイと IP レピュテーションサービスの連携方法が分かりやすく示されています。[概要（Overview）] ページでは、次の操作を実行できます。

- ゲートウェイを「出入り」するすべてのメールのメール トレンド グラフを表示する。
- 試行されたメッセージ、IP レピュテーション フィルタリングによって停止されたメッセージ、受信者が無効なメッセージ、スパムとしてマークされたメッセージ、ウイルス検出としてマークされたメッセージ、およびクリーンメッセージの数を経時的に表示する。
- システム ステータスおよびローカル隔離のサマリーを表示する。
- Threat Operations Center（TOC）で入手可能な情報に基づいて、現在のウイルスの発生情報やウイルス以外の発生情報を確認する。

[概要（Overview）] ページは、[システム概要（System Overview）] セクションおよび送受信メールのグラフとサマリーのセクションの 2 つに分かれています。

関連項目

- システム概要 （1016 ページ）
- 送受信のサマリーとグラフ （1017 ページ）

- 電子メールの分類 （1018 ページ）
- メッセージの分類方法 （1019 ページ）

システム概要

[概要（Overview）]ページの[システム概要（System Overview）]セクションは、システムダッシュボードとして機能し、システムおよびワークキューステータス、隔離ステータス、発生アクティビティなどの 電子メールゲートウェイに関する詳細を示します。

関連項目

- ステータス（Status） （1016 ページ）
- システム隔離（System Quarantines） （1016 ページ）
- ウイルス脅威レベル （1016 ページ）

ステータス（Status）

このセクションでは、電子メールゲートウェイおよび着信メール処理の現在の状態の概要が示されます。

[システム ステータス（System Status）]：次のいずれかの状態です。

- オンライン（Online）
- リソース節約（Resource Conservation）
- 配信停止（Delivery Suspended）
- 受信停止（Receiving Suspended）
- ワーク キュー一時停止（Work Queue Paused）
- オフライン

詳細については、CLI による管理およびモニタリング （1333 ページ） を参照してください。

[受信メッセージ（Incoming Messages）]：1 時間あたりの着信メールの平均レート。

[ワーク キュー（Work Queue）]：ワーク キュー内の処理待ちメッセージの数。

[システム ステータス（System Status）] ページに移動するには、[システム ステータス詳細（System Status Details）] リンクをクリックします。

システム隔離（System Quarantines）

このセクションには、電子メールゲートウェイでのディスク使用量別の上位 3 つの隔離に関する情報（隔離の名前、隔離の使用度（ディスク領域）、現在の隔離エリア内のメッセージ数など）が表示されます。

[内部隔離（Local Quarantines）] ページに移動するには、[内部隔離（Local Quarantines）] リンクをクリックします。

ウイルス脅威レベル

ここでは、Threat Operations Center（TOC）から報告される、Outbreak のステータスを示します。また、隔離の使用度（ディスク領域）、隔離内のメッセージ数など、アウトブレイク隔離

のステータスを示します。アウトブレイク隔離は、電子メールゲートウェイでアウトブレイクフィルタ機能をイネーブルに設定した場合のみ表示されます。

（注） 脅威レベル インジケータを機能させるためには、ファイアウォールで「**downloads.ironport.com**」に対してポート 80 を開く必要があります。あるいは、ローカル更新サーバを指定した場合は、脅威レベル インジケータがそのアドレスを使用します。また、[サービスのアップデート（Service Updates）]ページを使用してダウンロード用のプロキシを設定済みの場合、脅威レベル インジケータは、正しくアップデートされます。詳細については、サービス アップデート （1253 ページ）を参照してください。

外部 Threat Operations Center ウェブ サイトを表示するには、[アウトブレイクの詳細（Outbreak Details）] をクリックします。このリンクを機能させるには、お使いの 電子メールゲートウェイでインターネットに接続できる必要があります。[個別のウィンドウ（Separate Window）]アイコンは、クリックすると別個のウィンドウにリンクが開かれることを示します。これらのウィンドウを表示できるようにするには、ブラウザのポップアップブロッカを設定する必要があります。

送受信のサマリーとグラフ

送受信のサマリーのセクションでは、システム上のすべてのメールアクティビティのリアルタイム アクティビティへのアクセスが提供され、送受信メールのグラフとメール サマリーで構成されています。ユーザは、[時間範囲（Time Range）] メニューを使用して報告対象となるタイムフレームを選択できます。選択したタイムフレームは、すべての電子メール セキュリティ モニタ ページで使用されます。メッセージの各タイプまたはカテゴリに関する説明は以下のとおりです（電子メールの分類 （1018 ページ）を参照）。

メール トレンド グラフでは、メール フローが視覚的に表示されますが、サマリー テーブルでは、同じ情報の数値的な内訳が示されます。サマリー テーブルには、各メッセージ タイプの割合と実数（試行されたメッセージ、脅威メッセージ、クリーン メッセージの総数を含む）が含まれています。

送信グラフおよびサマリーでも、送信メールに関する同様の情報が示されます。

関連項目

- 電子メール セキュリティ モニタでのメッセージ集計に関する注意事項 （1017 ページ）

電子メール セキュリティ モニタでのメッセージ集計に関する注意事項

電子メール セキュリティ モニタが着信メールの集計に使用する方法は、メッセージあたりの受信者の数によって異なります。たとえば、example.com から 3 人の受信者に送信された着信メッセージは、この送信者からの 3 通として集計されます。

送信者レピュテーションフィルタによってブロックされたメッセージは実際にはワークキューに入らないので、電子メールゲートウェイは着信メッセージの受信者のリストにはアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数はシスコによって算出されたもので、既存の顧客データの大規模なサンプリング研究に基づいています。

電子メールの分類

[概要（Overview）]ページおよび[受信メール（Incoming Mail）]ページで報告されるメッセージは、次のように分類されます。

- [IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）]：HAT ポリシーによってブロックされたすべての接続数に固定乗数（電子メール セキュリティ モニタでのメッセージ集計に関する注意事項（1017ページ）を参照）を乗じた値に受信調整によってブロックされたすべての受信者数を加えた値。
- [ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）]：送信者ドメインのレピュテーション判定に基づいてブロックされたメッセージの総数。
- [無効な受信者（Invalid Recipients）]：従来の LDAP 拒否によって拒否されたすべての受信者数にすべての RAT 拒否数を加えた値。
- [スパムメッセージ検出（Spam Messages Detected）]：アンチスパム スキャン エンジンで陽性、または疑いありとして検出されたメッセージ、およびスパムとウイルスの両方で陽性と検出されたメッセージの総数。
- [ウイルスメッセージ検出（Virus Messages Detected）]：ウイルスとしては陽性だがスパムではないと検出されたメッセージの総数および割合。

（注） スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーンメッセージとして集計されます。それ以外の場合は、メッセージはウイルス陽性として集計されます。

- [高度なマルウェア防御による検出（Detected by Advanced Malware Protection）]：ファイルレピュテーションフィルタリングにより、メッセージの添付ファイルが悪意のあるファイルとして検出されました。この値には、ファイル分析により悪意があると検出された判定のアップデートまたはファイルは含まれません。
- [悪意のあるURLを含むメッセージ（Messages with Malicious URLs）]：メッセージに含まれる 1 つ以上の URL が、URL フィルタリングにより悪意のある URL として検出されました。
- [コンテンツフィルタによる停止（Stopped by Content Filter）]：コンテンツ フィルタによって阻止されたメッセージの総数。
- [DMARC によるサポート（Stopped by DMARC）]：DMARC 検証後に阻止されたメッセージの総数。

（注） 電子メールゲートウェイは、「失敗 - 拒否」、「失敗 - 隔離」、および「失敗 - アクションなし」の結果に基づいて、「DMARC による停止」メッセージの総数を表示します。

- [S/MIME 検証または復号に失敗しました（S/MIME Verification/Decryption）]：S/MIME 検証または復号、あるいはその両方に失敗したメッセージの総数。
- [S/MIME 検証/復号が成功しました（S/MIME Verification/Decryption Successful）]：S/MIME を使用した検証または復号、あるいは復号と検証が成功したメッセージの総数。
- [正常なメッセージ（Clean Messages）]：受け入れられ、ウイルスでもスパムでもないと見なされたメール。受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信された正常なメッセージを最も正確に表したものです。ただし、ウイルス陽性またはスパム陽性としてマークされたにもかかわらず配信されたメッセージは集計されないので、実際のメッセージの配信数と、このクリーン メッセージの数は異なる可能性があります。
- グレイメール メッセージ
  - [マーケティングメッセージ（Marketing Messages）]：たとえば、Amazon.com のような、プロフェッショナルなマーケティング グループによって送信されたアドバタイジング メッセージの総数。
  - [ソーシャル ネットワーキング メッセージ（Social Networking Messages）]：ソーシャル ネットワーク、出会い/結婚 Web サイト、フォーラムなどからの通知メッセージの総数。たとえば、LinkedIn フォーラム、CNET フォーラムなどがあります。
  - [バルク メッセージ（Bulk Messages）]：テクノロジー メディア企業の TechTarget など、認識されていないマーケティング グループによって送信された広告メッセージの総数。

メッセージ トラッキングを使用して、そのカテゴリに所属するメッセージのリストを表示するには、上記の任意のグレイメール カテゴリに対応する番号をクリックします。

（注） メッセージ フィルタに一致し、フィルタによってドロップされたり、バウンスされたりしないメッセージは、クリーンとして処理されます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

メッセージの分類方法

メッセージは電子メール パイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、スパム陽性、ウイルス陽性、またはマルウェア陽性とマークされたメッセージが、コンテンツ フィルタにも一致することがありますこれらの優先ルールに続いて、アウトブレイク フィルタによる隔離（この場合、メッセージが隔離から解放されるまで集計されず、ワーク キューによる処理が再び行われます）の次にスパム陽性、ウイルス陽性、マルウェア陽性、およびコンテンツ フィルタとの一致などさまざまな判定が行われます。

たとえば、メッセージがスパム陽性とマークされると、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されている場合には、このメッセージがドロップされ、スパム カウンタが増分します。さらに、スパム陽性のメッセージを引き続きパイプラインで処理し、以降のコンテンツ フィルタがこのメッセージをドロップ、バウンス、または隔離するよう

にアンチスパム設定が設定されている場合にも、スパム カウンタは増分します。メッセージがスパム陽性、ウイルス陽性、またはマルウェア陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

[受信メール（Incoming Mail）] ページ

[受信メール（Incoming Mail）]ページでは、お使いの電子メールゲートウェイに接続するすべてのリモートホストの電子メールセキュリティモニタ機能によって収集されたリアルタイム情報に関して報告を行うメカニズムが提供されます。これにより、メール送信者のIPアドレス、ドメイン、および組織（ネットワーク オーナー）に関する詳細を収集できます。メール送信者の IP アドレス、ドメイン、組織については、送信者プロファイル検索を実行できます。

[受信メール（Incoming Mail）] ページには、[ドメイン（Domain）]、[IP アドレス（IP Addressl）]、および [ネットワーク所有者（Network Owner）] の 3 種類のビューが用意されており、システムに接続するリモートホストのスナップショットが選択したビューで提供されます。

電子メールゲートウェイで設定済みのすべてのパブリックリスナーにメールを送信した上位ドメイン（またはビューに応じて、IP アドレスまたはネットワークオーナー）の表（[受信メールの詳細（Incoming Mail Details）]）が表示されます。ゲートウェイに入ったすべてのメールのフローをモニタできます。任意のドメイン/IP/ネットワーク オーナーをクリックしてドリルダウンし、送信者プロファイルページ（クリックしたドメイン/IP/ネットワーク オーナーに固有の[受信メール（Incoming Mail）]ページ）のこの送信者に関する詳細にアクセスできます。

使用可能なすべての列がデフォルトで表示されるわけではありません。テーブルの下の [列（Columns)] リンクをクリックすると、異なる情報セットが表示されます。たとえば、デフォルトでは非表示になっている [高度なマルウェア防御による検出（Detected by Advanced Malware Protection）] 列を表示できます。

[受信メール（Incoming Mail）] は、一連のページ（[受信メール（Incoming Mail）]、送信者プロファイル、および送信者グループ レポート）を含むように拡張することもできます。[受信メール（Incoming Mail）] ページでは、次の操作を実行できます。

- メール送信者の IP アドレス、ドメイン、または組織（ネットワーク オーナー）に関する検索を実行する。
- 送信者グループ レポートを表示して、特定の送信者グループおよびメールフローポリシーアクションによる接続を確認する。詳細については、送信者グループ レポート （1026 ページ）を参照してください。
- 試行されたものの、セキュリティ サービス（送信者レピュテーション フィルタリング、アンチスパム、アンチウイルス、グレイメール他）によってブロックされたメッセージの数など、メール送信者に関する詳細な統計情報を確認する。
- アンチスパムまたはアンチウイルスセキュリティサービスによって測定される、大量のスパムまたはウイルス電子メールを送信した送信者別にソートする。
- IP レピュテーションサービスを使用して特定の IP アドレス、ドメイン、および組織の間の関係のドリルダウンと分析を行い、送信者に関する詳細を取得する。

- 特定の送信者をドリルダウンして、送信者の IP レピュテーションスコア、ドメインが直近に一致した送信者グループなど、IP レピュテーションサービスから送信者に関する詳細を取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者をドリルダウンする。
- ドメインに関する情報を収集したら、（必要に応じて）ドメイン、IP アドレス、またはネットワーク オーナーのプロファイル ページから [送信者グループに追加（Add to Sender Group）] をクリックして、既存の送信者グループに IP アドレス、ドメイン、または組織を追加できます。電子メールを受信するためのゲートウェイの設定 （81 ページ） を参照してください。

関連項目

- 受信メール （1021 ページ）
- [受信メールの詳細（Incoming Mail Details）] リスト （1022 ページ）
- データが読み込まれる報告ページ：送信者プロファイル ページ （1024 ページ）
- 送信者グループ レポート （1026 ページ）

受信メール

[受信メール（Incoming Mail）] ページでは、システムで設定済みのすべてのパブリック リスナーのリアルタイムアクティビティへのアクセスが提供され、受信数の上位送信者のドメイン（脅威メッセージの総数別、クリーン メッセージの総数別、グレーメール メッセージの総数別）および [受信メールの詳細（Incoming Mail Details）] リストという 2 つのセクションで構成されます。

[受信メールの詳細（Incoming Mail Details）] リストに含まれるデータの説明については、[受信メールの詳細（Incoming Mail Details）] リスト （1022 ページ）を参照してください。

関連項目

メール トレンド グラフにおける時間範囲に関する注意事項 （1021 ページ）

メール トレンド グラフにおける時間範囲に関する注意事項

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

時間範囲は、次の表に記載のオプションから選択します。

表 *85*：電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時間（Hour）	直近の 60 分 + 最大 5 分

GUI で選択した時間範囲	定義
日（Day）	直近の 24 時間と直近の 60 分
週（Week）	直近の 7 日 + 当日の経過した時間
30 日（30 days）	直近の 30 日 + 当日の経過した時間
90 日（90 days）	直近の 90 日 + 当日の経過した時間
昨日（Yesterday）	00:00 ～ 23:59（午前 0 時～午後 11:59）
先月（Previous Calendar Month）	その月の最初の日の 00:00 ～その月の最後の日の 23:59
カスタム範囲（Custom Range）	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

集中化レポーティングをイネーブルにしていると、表示される時間範囲オプションが異なります。集中管理レポート モードの詳細については、Cisco Secure Email and Web Manager（M シリーズ）の集中型サービス （1559 ページ）を参照してください。

[受信メールの詳細（Incoming Mail Details）] リスト

電子メールゲートウェイのパブリックリスナーに接続した上位送信者が、[受信メール（Incoming Mail）] ページの下部にある受信された外部ドメインリストの表に選択したビューで表示されます。データをソートするには、カラム見出しをクリックします。各種のカテゴリの説明については、電子メールの分類 （1018 ページ）を参照してください。

ダブル DNS ルックアップの実行によって、リモート ホストの IP アドレス（つまり、ドメイン）が取得され、有効性が検証されます。ダブル DNS ルックアップおよび送信者検証の詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

送信者の詳細のリストには、[サマリー（Summary）] と [すべて（All）] の 2 つのビューがあります。

デフォルトの [送信者の詳細（Sender Detail）] ビューでは、各送信者が試行したメッセージの総数が示され、カテゴリ別の内訳が含まれます。カテゴリは、[概要（Overview）] ページの [受信メールサマリー（Incoming Mail Summary）] グラフと同じです。

[IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。

- この送信者からの「調整された」メッセージの数。
- 拒否された、または TCP 拒否の接続数（部分的に集計されます）。
- 接続ごとのメッセージ数に対する控えめな乗数。

電子メールゲートウェイに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。

（注） [概要（Overview）] ページの [IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけが、負荷のために常に限定的です。

表示できる追加のカラムは次のとおりです。

[接続拒否（Connections Rejected）]：HAT ポリシーによってブロックされたすべての接続。 電子メールゲートウェイに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。

[接続承認（Connections Accepted）]：受け入れられたすべての接続。

[ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）]：送信者ドメインのレピュテーション判定に基づいてブロックされたメッセージの総数。

[受信者スロットルによる停止（Stopped by Recipient Throttling）]：[レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] のコンポーネントです。HAT 上限値（1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数）のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] が算出されます。

[高度なマルウェア防御による検出（Detected by Advanced Malware Protection）]：ファイル レピュテーションフィルタリングにより、添付ファイルが悪意のあるファイルとして検出されたメッセージ。この値には、ファイル分析により悪意があると検出された判定のアップデートまたはファイルは含まれません。

[合計脅威件数（Total Threat）]：（送信者レピュテーションにより阻止された、無効な受信者、スパム、およびウイルスとして阻止された）脅威メッセージの総数

テーブルの下部にある [列（Column）] リンクをクリックすると、カラムの表示/非表示が切り替わります。

このリストは、カラム見出しリンクをクリックするとソートされます。カラム見出しの横にある小さな三角形は、データの現在のソートに使用されているカラムを示します。

関連項目

- [ドメイン情報がありません（No Domain Information）]（1023 ページ）
- 詳細の問い合わせ （1024 ページ）

[ドメイン情報がありません（No Domain Information）]

電子メールゲートウェイに接続したものの、ダブル DNS ルックアップで検証できなかったドメインは、専用ドメイン [ドメイン情報がありません（No Domain Information）] に自動的に分類されます。これらの種類の検証されないホストは、送信者の検証によって管理できます。電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

リストに表示される送信者の数は、[表示された項目（Items Displayed）] メニューから選択できます。

詳細の問い合わせ

電子メール セキュリティ モニタのテーブルに表示された送信者については、その送信者（または [ドメイン情報がありません（No Domain Information）] リンク）をクリックして特定の送信者に関する詳細をドリルダウンします。結果は送信者プロファイルページに表示され、IP レピュテーションサービスからのリアルタイム情報が含まれます。送信者プロファイルページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細をドリルダウンできます（データが読み込まれる報告ページ：送信者プロファイル ページ （1024 ページ）を参照）。

[受信メール（Incoming Mail）] ページの下部にある [送信者グループのレポート（Sender Groups Report）] リンクをクリックして、別のレポート（送信者グループ レポート）を表示することもできます。送信者グループ レポートの詳細については、送信者グループ レポート （1026 ページ）を参照してください。

データが読み込まれる報告ページ：送信者プロファイル ページ

[受信メール（Incoming Mail）] ページにある [受信メールの詳細（Incoming Mail Details）] テーブルをクリックすると、その結果として送信者プロファイルページが表示されます。このページには、特定の IP アドレス、ドメイン、または組織（ネットワーク オーナー）のデータが含まれています。送信者プロファイルページには、送信者の詳細情報が示されます。任意のネットワーク オーナーまたは IP アドレスの送信者プロファイル ページは、[受信メール（Incoming Mail）] ページまたは他の送信者プロファイル ページで特定の項目をクリックしてアクセスできます。ネットワーク オーナーは、ドメインを含むエンティティであり、ドメインは、IP アドレスを含むエンティティです。この関係および IP レピュテーションサービスとの関係の詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

IP アドレス、ネットワーク オーナーおよびドメインに関して表示される送信者プロファイル ページは、多少異なります。それぞれのページには、この送信者からの着信メールに関するグラフおよびサマリーテーブルが含まれます。グラフの下には、この送信者に関連するドメインまたは IP アドレスを表示する表（個々の IP アドレスの送信者プロファイル ページには、詳細なリストは含まれません）、およびこの送信者の現在の SenderBase 情報、送信者グループ情報、およびネットワーク情報を含む情報セクションがあります。

- ネットワーク オーナー プロファイル ページには、ネットワーク オーナー、およびこのネットワーク オーナーに関連するドメインや IP アドレスに関する情報が含まれます。
- ドメイン プロファイル ページには、このドメインおよびこのドメインに関連する IP アドレスに関する情報が含まれます。
- IP アドレス プロファイル ページには、IP アドレスのみに関する情報が含まれます。

  各送信者プロファイルページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

- IP レピュテーションサービスからの**グローバル**情報。たとえば、次の情報です。
  - IP アドレス、ドメイン名、またはネットワーク オーナー

- ネットワーク オーナーのカテゴリ（ネットワーク オーナーのみ）
- CIDR 範囲（IP アドレスのみ）
- IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
- この送信者から最初のメッセージを受信してからの日数
- 最後の送信者グループと DNS が検証されたかどうか（IP アドレス送信者プロファイル ページのみ）

日単位マグニチュードは、直近24時間にドメインが送信したメッセージの数の基準です。地震の測定に使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10 を基数とする対数目盛を使用して算出されるメッセージの量の基準です。目盛の最大理論値は 10 に設定されます。これは、世界の電子メール メッセージの量（約 100 億メッセージ/日）に相当します。対数目盛を使用した場合、1 ポイントのマグニチュードの増加は、実際の量の 10 倍の増加に相当します。

月単位マグニチュードは、直近 30 日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。

- 平均マグニチュード（IP アドレスのみ）
- 総累積量/30 日の量（IP アドレス プロファイル ページのみ）
- Bonded Sender ステータス（IP アドレス プロファイル ページのみ）
- IP レピュテーションスコア（IP アドレスプロファイルページのみ）
- 最初のメッセージからの日数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
- このネットワーク オーナーに関連するドメインの数（ネットワーク オーナープロファイル ページおよびドメイン プロファイル ページのみ）
- このネットワーク オーナーの IP アドレスの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
- 電子メールの送信に使用された IP アドレスの数（ネットワーク オーナー ページのみ）

IP レピュテーションサービスによって提供されるすべての情報が記載されたページを表示するには、[SenderBaseからの詳細情報（More from SenderBase）] リンクをクリックします。

- **メール フロー統計**情報。送信者について収集された、指定した時間範囲にわたる電子メール セキュリティ モニタ情報を含みます。
- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する**詳細**は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

  ドメイン プロファイル ページから特定の IP アドレスをドリルダウンするか、ドリルアップして組織プロファイル ページを表示できます。また、テーブルの下部にある [列（Columns）] リンクをクリックして、[IPアドレス（IP Addresses）] テーブル内の送信者アドレスごとに。[DNS検証（DNS Verified）] ステータス、[IPレピュテーションスコア（IP Reputation Score）]、および [最新の送信者グループ（Last Sender Group）] を表示することもできます。そのテーブル内の任意のカラムを非表示にすることもできます。

ネットワーク オーナー プロファイル ページから、そのテーブルの下部にある [列（Columns）] リンクをクリックすることにより、[ドメイン（Domains）] テーブル内のドメインごとの [接続拒否（Connections Rejected）]、[接続承認（Connections Accepted）]、[受信者スロットルによる停止（Stopped by Recipient Throttling）]、および [高度なマルウェア防御による検出（Detected by Advanced Malware Protection）] などの情報を表示できます。そのテーブル内の任意のカラムを非表示にすることもできます。

システムの管理者の場合は、これらの各ページで（必要に応じて）エンティティのチェックボックスをクリックしてから [送信者グループに追加（Add to Sender Group）] をクリックし、送信者グループにネットワーク オーナー、ドメイン、または IP アドレスを追加することもできます。

また、送信者の現在の情報テーブルの送信者グループ情報の下にある [送信者グループに追加（Add to Sender Group）] リンクをクリックして、送信者グループに送信者を追加することもできます。送信者を送信者グループに追加する方法の詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。当然ながら、必ずしも変更を行う必要はありません。セキュリティ サービスに着信メールを処理させることもできます。

関連項目

- 送信者プロファイルの検索 （1026 ページ）

送信者プロファイルの検索

特定の送信者を検索するには、[クイック検索（Quick Search）] ボックスに IP アドレス、ドメイン、または組織名を入力します。

送信者プロファイル ページが送信者の情報と共に表示されます。データが読み込まれる報告ページ：送信者プロファイル ページ （1024 ページ） を参照してください。

送信者グループ レポート

送信者グループ レポートは、送信者グループ別およびメール フロー ポリシー アクション別の接続のサマリーを提供し、SMTP 接続およびメール フロー ポリシーのトレンドを確認できるようにします。[送信者グループによるメール フロー（Mail Flow by Sender Group）] リストには、各送信者グループの割合および接続数が示されます。[メールフローポリシーアクションによる接続（Connections by Mail Flow Policy Action）] グラフは、各メール フローポリシー アクションの接続の割合を示します。このページには、ホスト アクセス テーブル（HAT）ポリシーの有効性の概要が示されます。HAT の詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

[送信者ドメインのレピュテーション（SenderDomainReputation）]ページ

[送信者ドメインのレピュテーション（Sender Domain Reputation）] レポート ページでは、次を表示できます。

- SDR サービスで受信した判定に基づく着信メッセージ（グラフ形式）。
- SDR サービスで受信した脅威カテゴリおよび判定に基づく着信メッセージの概要（表形式）。
- SDR サービスで受信した脅威カテゴリに基づく着信メッセージ（グラフ形式）。

（注） SDR 判定が「Untrusted」または「Questionable」メッセージのみが、「Spam」や「Malicious」などの SDR 脅威カテゴリに分類されます。

- SDR サービスで受信した脅威カテゴリに基づく着信メッセージの概要（表形式）。

[SDRによって処理された着信メッセージの概要（Summary of Incoming Messages handled by SDR）] セクションで特定の判定に対応するメッセージの数をクリックすると、関連するメッセージを [メッセージトラッキング（Message Tracking）] に表示できます。

送信先

[送信先（Outgoing Destinations）] ページには、メールの送信先ドメインに関する情報が示されます。このページは、2 つのセクションで構成されます。ページの上部は、発信脅威メッセージ別の上位宛先および発信クリーンメッセージの上位宛先を示すグラフで構成されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）全カラムを示す表が表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。

[送信先（Outgoing Destinations）] ページを使用すると、次の情報を入手できます。

- 電子メールゲートウェイのメール送信先
- 各ドメインに送信されるメールの量
- クリーン、スパム陽性、ウイルス陽性、マルウェア、またはコンテンツ フィルタによる阻止のメールの割合。
- 配信されたメッセージおよび宛先サーバによってハードバウンスされたメッセージの数

送信者

[送信メッセージ送信者（Outgoing Senders）] ページには、ネットワーク内の IP アドレスおよびドメインから送信された電子メールの数と種類についての情報が表示されます。このページを表示すると、ドメイン別または IP アドレス別に結果を表示できます。各ドメインによって送信されたメールの量を確認する場合にはドメイン別の結果、最も多いウイルス メッセージを送信している、または最も多くコンテンツ フィルタをトリガーしている IP アドレスを表示する場合には IP アドレス別の結果を表示することが推奨されます。

このページは、2 つのセクションで構成されます。ページの左側は、総脅威メッセージ別の上位送信者を示すグラフです。合計脅威メッセージには、スパム陽性、ウイルス陽性、マルウェアのメッセージ、またはコンテンツ フィルタをトリガーしたメッセージが含まれます。ページの上部の右側は、クリーン メッセージ別の上位送信者を表示するグラフです。ページの下部には、総メッセージ数別にソートされた（デフォルト設定）全カラムを示す表が表示されます。

（注） このページには、メッセージ配信に関する情報は表示されません。特定のドメインからのバウンスされたメッセージの数などの配信情報は、[送信処理ステータス（Delivery Status）] ページを使用して追跡できます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。

[送信メッセージ送信者（Outgoing Senders）] ページを使用すると、次の情報を入手できます。

- 最も多くのウイルスに感染、スパム陽性、またはマルウェアと判断された電子メールを送信している IP アドレス。
- 最も頻繁にコンテンツ フィルタをトリガーした IP アドレス
- 最も多くのメールを送信するドメイン

地理的分散ページ

[地理的分散（Geo Distribution）] レポート ページを使用して次の項目を表示できます。

- 発信国別の受信メール接続数の上位（グラフィカルな形式）。
- 発信国別の受信メール接続の合計数（表形式）。

特定の位置情報の受信メールの接続の数をクリックすると、メッセージ トラッキングに関連メッセージを表示できます。

[合計メッセージ数（Total Messages）] 列には、SMTP 接続レベルで受け入れられるメッセージのみ表示されます。

（注） レポート生成中に次の処理が発生します。

- プライベートIPアドレスとして1つ以上の受信メール接続が検出されると、受信メール接続がレポートの「プライベート IP アドレス」として分類されます。
- 有効ではない IP レピュテーションスコアとして 1 つ以上の受信メール接続が検出されると、受信メール接続がレポートで「国情報なし」に分類されます。

[送信処理ステータス（Delivery Status）] ページ

特定の受信者ドメインに対する配信の問題を疑ったり、仮想ゲートウェイ アドレスに関する情報収集を行ったりする場合には、[モニター（Monitor）]>[送信処理ステータス ページ（Delivery Status Page）] をクリックすると、特定の受信者ドメインに関連する電子メール操作に関するモニタリング情報が提供されます。

[送信処理ステータス（Delivery Status）] ページには、CLI で tophosts コマンドを使用した場合と同じ情報が表示されます（詳細については、CLIによる管理およびモニタリング （1333ページ）の「電子メール キューの構成の確認」を参照してください）。

このページには、直近3時間以内にシステムによって配信されたメッセージの上位20、50、または100の受信者ドメインのリストが表示されます。各統計情報のカラム見出しのリンクをクリックすることによって、最新のホストステータス、アクティブな受信者（デフォルト）、切断した接続、配信された受信者、ソフト バウンス イベント、およびハード バウンス受信者別にソートできます。

- 特定のドメインを検索するには、[ドメイン名：（Domain Name:）] フィールドにドメイン名を入力し、[検索（Search）] をクリックします。
- 表示されているドメインをドリルダウンするには、ドメイン名のリンクをクリックします。

[送信処理ステータス詳細（Delivery Status Details）] ページに結果が表示されます。

（注） 受信者ドメインで任意のアクティビティが発生すると、このドメインが「アクティブ」となり、[概要（Overview）] ページに表示されます。たとえば、配信の問題があるためにメールが発信キューにとどまると、この受信者ドメインは、引き続き発信メールの概要に表示されます。

関連項目

- 配信の再試行 （1030 ページ）
- [送信処理ステータス詳細（Delivery Status Details）] ページ （1030 ページ）

配信の再試行

後で配信されるようにスケジュール設定されているメッセージは、[すべての送信を再試行（Retry All Delivery）] をクリックすると、ただちに再試行できます。[すべての送信を再試行（Retry All Delivery）] では、キューに含まれるメッセージがただちに配信されるようにスケジュールを変更できます。down のマークが付いたすべてのドメインと、スケジュールされたメッセージまたはソフト バウンスされたメッセージが、即時配信のキューに入れられます。

特定の宛先ドメインに向けての配信を再施行するには、ドメイン名のリンクをクリックします。[送信処理ステータス詳細（Delivery Status Details）] ページで、[送信を再試行（Retry Delivery）] をクリックします。

CLI で delivernow コマンドを使用して、ただちに配信するようにメッセージのスケジュールを変更することもできます。詳細については、電子メールの即時配信スケジュール（1357ページ）を参照してください。

[送信処理ステータス詳細（Delivery Status Details）] ページ

特定の受信者ドメインに関する統計情報を検索するには、[送信処理ステータス詳細（Delivery Status Details）] ページを使用します。このページには、CLI 内で **hoststatus** コマンドを使用した場合と同じ情報（メール ステータス、カウンタ、およびゲージ）が表示されます。（詳細については、CLIによる管理およびモニタリング（1333ページ）を参照してください）特定のドメインを検索するには、[ドメイン名：（Domain Name:）] フィールドにドメイン名を入力し、[検索（Search）] をクリックします。**altsrchost** 機能を使用している場合、仮想ゲートウェイのアドレス情報が表示されます。

[内部ユーザ（Internal Users）] ページ

[内部ユーザ（Internal Users）] ページでは、内部ユーザによって送受信されたメールに関する情報が、電子メール アドレスごとに表示されます（単一ユーザの複数の電子メール アドレスが、リストに表示される場合があります。レポートでは、電子メールアドレスはまとめられません）。

このページは、2 つのセクションで構成されます。

- 正常な着信メッセージ別および正常な発信メッセージ別の上位ユーザと、グレイメールを受信する上位ユーザを示すグラフ。
- ユーザー メール フローの詳細

レポート対象の時間範囲（時間、日、週、または月）を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。非表示のテーブル カラムを表示するか、またはデフォルト カラムを非表示にするには、テーブルの下の [列（Columns)] リンクをクリックします。

[ユーザー メール フローの詳細（User Mail Flow Details）] リストでは、送受信メールが電子メール アドレス別に正常、スパム、（着信のみ）、ウイルス、マルウェア、コンテンツ フィルタの一致、グレイメール（着信のみ）に分類されます。このリストは、カラム見出しをクリックしてソートできます。

内部ユーザ レポートを使用すると、次の情報を入手できます。

- 最も多くの外部メールを送信したユーザ
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのグレイメール メッセージを受信したユーザ
- 最も多くのスパムを受信したユーザ
- コンテンツ フィルタをトリガーしたユーザとそのコンテンツ フィルタの種類
- 電子メールをコンテンツ フィルタで捕捉されたユーザ

着信内部ユーザとは、Rcpt To: アドレスに基づいてシステムで電子メールを受信する対象ユーザのことです。発信内部ユーザはMail From: アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

一部の送信メール（バウンスなど）の送信者は、null です。これらの送信者は、送信および「不明」に集計されます。

内部ユーザの [内部ユーザの詳細（Internal User Details）] ページを表示するには、この内部ユーザをクリックします。

デフォルトで非表示のカラム（[高度なマルウェア防御で検出された受信メール（Incoming Detected by Advanced Malware Protection）] カラムまたは [高度なマルウェア防御で検出された送信メール（Outgoing Detected by Advanced Malware Protection）] など）を表示するには、テーブルの下の [列（Column）] リンクをクリックします。

関連項目

- 内部ユーザの詳細 （1031 ページ）
- 特定の内部ユーザの検索 （1032 ページ）

内部ユーザの詳細

[内部ユーザの詳細（Internal User Details）] ページでは、各カテゴリ（[スパム検出（Spam Detected）]、[ウイルス検出（Virus Detected）]、[高度なマルウェア防御で検出（Detected by Advanced Malware Protection）]、[コンテンツ フィルタによる受信停止（Stopped By Content Filter）]、[グレーメール検出（Graymail Detected）]、および [正常（Clean）]）のメッセージ数を示す送受信メッセージの内訳など指定したユーザに関する詳細情報が示されます。受信メッセージの場合は任意で、テーブルの下の [列（Column）] リンクをクリックすると、[高度なマルウェア防御で検出された受信メール（Incoming Detected by Advanced Malware Protection）] カラムが表示されます。この値は、ファイル レピュテーション フィルタリングにより悪意のあるファイルと判断された添付ファイルを含むメッセージの数を表します。この値には、判定のアップデートまたはファイル分析により悪意があるファイルとして検出されたファイルは含まれません。送受信コンテンツ フィルタおよび DLP ポリシーの一致も示されます。

コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（[コンテンツフィルタ（Content Filters）] ページ（1033 ページ）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したユーザのリストも取得できます。

特定の内部ユーザの検索

特定の内部ユーザ（電子メール アドレス）は、[内部ユーザ（Internal Users）] ページおよび [内部ユーザの詳細（Internal User Details）] ページの下部にある検索フォームから検索できます。検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example.com」が一致します）を選択します。

[DLP インシデント（DLP Incidents）] ページ

[DLP インシデント（DLP Incidents）] ページには、送信メールで発生した Data Loss Prevention（DLP）ポリシー違反インシデントに関する情報が示されます。電子メールゲートウェイでは、[送信メールポリシー（Outgoing Mail Policies）] テーブルでイネーブルにした DLP 電子メールポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

DLP インシデント レポートを使用すると、次のような情報を取得できます。

- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP インシデント（DLP Incidents）] ページは、次の 2 つの主なセクションで構成されます。

- 重大度（[低（Low）]、[中（Medium）]、[高（High）]、[クリティカル（Critical）]）別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンド グラフ
- [DLP インシデントの詳細（DLP Incidents Details）] リスト

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートするか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

ポリシーによって検出された DLP インシデントに関する詳細情報を表示するには、DLP ポリシーの名前をクリックします。この方法を使用すると、ポリシーによって検出された、機密データを含むメールを送信したユーザのリストを取得できます。

関連項目

- DLP インシデントの詳細（DLP Incidents Details） （1033 ページ）
- [DLP ポリシー詳細（DLP Policy Detail）] ページ （1033 ページ）

DLP インシデントの詳細（DLP Incidents Details）

電子メールゲートウェイの送信メールポリシーで現在イネーブルの DLP ポリシーは、[DLPインシデント（DLP Incidents）] ページの下部にある [DLPインシデントの詳細（DLP Incidents Details）] テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。

[DLP インシデントの詳細（DLP Incidents Details）] テーブルは、ポリシーごとの DLP インシデントの合計数と、重大度レベル別の内訳を示します。重大度レベルには、バウンスされたメッセージの数と、クリアで配信、暗号化で配信、または削除されたメッセージの数も含まれます。データをソートするには、カラム見出しをクリックします。

[DLP ポリシー詳細（DLP Policy Detail）] ページ

[DLP インシデントの詳細（DLP Incidents Details）] テーブルで DLP ポリシーの名前をクリックした場合、その結果として表示される [DLP ポリシー詳細（DLP Policy Detail）] ページにそのポリシーに関する DLP インシデント データが表示されます。このページには、重大度に基づいた DLP インシデントのグラフが表示されます。

このページには、DLP ポリシーに違反したメッセージを送信した各内部ユーザを表示する、ページ下部にある [送信者別インシデント（Incidents by Sender）] リストも含まれます。このリストには、このポリシーに関するユーザごとの DLP インシデントの総数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。[送信者別インシデント（Incidents by Sender）] リストを使用すると、組織の機密データをネットワーク外のユーザに送信した可能性のあるユーザを検索できます。

送信者名をクリックすると、[内部ユーザ（Internal Users）] ページが開きます。詳細については、[内部ユーザ（Internal Users）] ページ （1030 ページ）を参照してください。

[コンテンツフィルタ（Content Filters）] ページ

[コンテンツフィルタ（Content Filters）] ページには、送受信コンテンツ フィルタの上位一致（最も多くのメッセージに一致したコンテンツ フィルタ）に関する情報が 2 種類の形式（棒グラフとリスト）で表示されます。[コンテンツフィルタ（Content Filters）] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認し、次の情報を取得できます。

- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ

リストのコンテンツ フィルタ名をクリックすると、[コンテンツフィルタの詳細（Content Filter Details）] ページにこのフィルタに関する詳細を表示できます。

関連項目

- コンテンツ フィルタの詳細 （1034 ページ）

コンテンツ フィルタの詳細

[コンテンツフィルタの詳細（Content Filter Details）] には、このフィルタの経時的な一致および内部ユーザ別の一致が表示されます。

[内部ユーザ別の一致（Matches by Internal User）] セクションでは、ユーザ名をクリックして内部ユーザ（電子メール アドレス）の [内部ユーザの詳細（Internal User Details）] ページを表示できます（内部ユーザの詳細 （1031 ページ）を参照）。

[DMARC検証（DMARC Verification）] ページ

[DMARC検証（DMARC Verification）] ページには、DMARC 検証が失敗した上位のドメインと、DMARC 検証に失敗したメッセージに対して AsyncOS が実行したアクションの詳細情報が表示されます。このレポートを使用して DMARC 設定を最適化し、次のような情報を取得できます。

- 最も多く DMARC 準拠ではないメッセージを送信したドメインはどれか。
- 各ドメインで、DMARC 検証に失敗したメッセージに対して AsyncOS がどのようなアクションを実行したか。

[DMARC検証（DMARC Verification）] ページの内容は次のとおりです。

- DMARC 検証の失敗数に基づく上位ドメインを示す横棒グラフ。
- ドメイン別に次の情報を示す表。
  - アクションなしで承認、隔離、または拒否されたメッセージの数。数値をクリックすると、選択されているカテゴリのメッセージのリストが表示されます。
  - DMARC 検証に合格したメッセージの数。
  - DMARC 検証試行回数の合計。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートするか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。

[マクロ検出（Macro Detection）] ページ

[マクロ検出（Macro Detection）] レポート ページを使用して、次の項目を表示できます。

- ファイル タイプ別のマクロが有効になった受信添付ファイル数の上位（グラフ形式および表形式）。
- ファイル タイプ別のマクロが有効になった送信添付ファイル数の上位（グラフ形式および表形式）。

マクロが有効になった添付ファイルの数をクリックすると、[メッセージ トラッキング（Message Tracking）] に関連メッセージを表示できます。

（注） レポート生成中に次の処理が発生します。

- アーカイブ ファイル内に 1 つ以上のマクロが検出されると、アーカイブ ファイル タイプが 1 増えます。アーカイブ ファイル内のマクロが有効になった添付ファイルの数はカウントされません。
- 埋め込みファイル内に 1 つ以上のマクロが検出されると、親ファイル タイプが 1 増えます。埋め込みファイル内のマクロが有効になった添付ファイルの数はカウントされません。

[外部脅威フィード（External Threat Feeds）] ページ

[外部脅威フィード（External Threat Feeds）] レポート ページでは、以下を表示できます。

- メッセージで脅威を検出するために使用される上位 ETF ソース（グラフ形式）。
- メッセージで脅威を検出するために使用される ETF ソースの概要（表形式）。
- メッセージで検出された脅威に一致する上位 IOC（グラフ形式）。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソース（グラフ形式）。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソースの概要（表形式）。

[外部脅威フィードソースの概要（Summary of External Threat Feed Sources）] セクションでは、以下を実行できます。

- 特定の ETF ソースでメッセージ数をクリックすると、[メッセージトラッキング（Message Tracking）] に関連メッセージを表示できます。
- 特定の脅威フィード ソースをクリックすると、IOC に基づいた ETF ソースの分布を表示できます。

[侵害の兆候（IOC）の一致の概要（Summary of Indicator of Compromise (IOC) Matches）] セクションでは、以下を実行できます。

- 特定の ETF ソースで IOC の数をクリックすると、[メッセージトラッキング（Message Tracking）] に関連メッセージを表示できます。
- 特定の IOC をクリックすると、ETF ソースに基づいた IOC の分布を表示できます。

[アウトブレイク フィルタ（Outbreak Filters）] ページ

[アウトブレイクフィルタ（Outbreak Filters）] ページには、お使いの電子メールゲートウェイのアウトブレイクフィルタの現在のステータスおよび設定に加えて、最近の発生状況やアウト

ブレイクフィルタによって隔離されたメッセージに関する情報が示されます。このページを使用して、対象を絞ったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできます。

[タイプ別脅威（Threats By Type）] セクションには、電子メールゲートウェイによって受信された脅威メッセージのさまざまなタイプが示されます。

[脅威サマリー（Threat Summary）] セクションには、[マルウェア（Malware）]、[フィッシング（Phish）]、[詐欺（Scam）]、および [ウィルス（Virus）] による脅威メッセージの内訳が示されます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

[過去1年間のアウトブレイクサマリー（Past Year Outbreak Summary）] には、この 1 年間にわたるグローバル発生およびローカル発生が表示されるので、ローカルネットワークのトレンドとグローバルなトレンドを比較できます。グローバル発生リストは、すべての発生（ウイルスとウイルス以外の両方）の上位集合です。これに対して、ローカル発生は、お使いの電子メールゲートウェイに影響を与えたウイルス発生に限定されています。ローカル感染発生データには、ウイルス以外の脅威は含まれません。グローバル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、Threat Operations Center によって検出されたすべての発生を表します。ローカル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、このアプライアンスで検出されたすべてのウイルス感染を表します。[ローカル保護の合計時間（Total Local Protection Time）] は、Threat Operations Center による各ウイルス発生の検出と、主要ベンダーによるアンチウイルス シグニチャの公開との時間差に常に基づいています。必ずしもすべてのグローバル発生が、お使いの電子メールゲートウェイに影響を与えるわけではありません。「--」値は、保護時間が存在しないか、アンチウイルス ベンダーからシグニチャ時間を入手できないことを示します（一部のベンダーは、シグニチャ時間を報告しません）。これは、保護時間がゼロであることを示すのではなく、保護時間の算出に必要な情報を入手できないことを示します。

[隔離されたメッセージ（Quarantined Messages）] セクションでは、感染フィルタの隔離状況の概要が示されます。これは、感染フィルタが捕捉した潜在的な脅威メッセージの数を把握するのに役立つ尺度です。隔離されたメッセージは、解放時に集計されます。通常、メッセージはアンチウイルスおよびアンチスパム ルールが使用可能になる前に隔離されます。メッセージが解放されると、アンチウイルスおよびアンチスパム ソフトウェアによってスキャンされ、陽性か、クリーンかを判定されます。感染トラッキングの動的性質により、メッセージが隔離領域内にあるときでも、メッセージの隔離ルール（および関連付けられる発生）が変更される場合があります。（隔離領域に入った時点ではなく）解放時にメッセージを集計することにより、件数の変動による混乱を防ぎます。

[脅威の詳細（Threat Details）] リストには、脅威のカテゴリ（ウイルス、詐欺、またはフィッシング）、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する情報が表示されます。ウイルス発生の場合は [過去 1 年間のウイルス アウトブレイク（Past Year Virus Outbreaks）] に、発生の名前と ID、ウイルス発生が初めてグローバルに検出された日時、アウトブレイク フィルタによって提供される保護時間、および隔離されたメッセージの数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。このリストは、カラム見出しをクリックしてソートできます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

[最初にグローバルで確認した日時（First Seen Globally）] の時間は、世界最大の電子メールおよびWebモニタリング ネットワークであるSenderBaseのデータに基づいて、Threat Operations Centerによって決定されます。[保護時間（Protection Time）] は、Threat Operations Centerによる各脅威の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に基づいています。

「--」値は、保護時間が存在しないか、アンチウイルスベンダーからシグニチャ時間を入手できないことを示します（一部のベンダーは、シグニチャ時間を報告しません）。保護時間がゼロであることを示しているわけではありません。むしろ、保護時間の算出に必要な情報を入手できないことを意味します。

[受信メッセージからのヒットメッセージ（Hit Messages from Incoming Messages）] セクションには、ウィルス性添付ファイル、その他の脅威（非ウィルス性）、正常な受信メッセージの割合と数が示されます。

[脅威レベル別のヒットメッセージ（Hit Messages by Threat Level）] セクションには、脅威レベル（レベル 1 ～ 5）に基づいて受信脅威メッセージ（ウィルス性および非ウィルス性）の割合と数が示されます。

[アウトブレイク隔離されているメッセージ（Messages resided in Outbreak Quarantine）] セクションには、アウトブレイク隔離エリアに入っていた脅威メッセージの数が、その期間に基づいて示されます。

[書き換えられた上位URL（Top URL's Rewritten）] セクションには、発生回数に基づいて、書き換えられた上位 10 件の URL がリストで示されます。書き換えられた URL をさらに表示するには、[表示されたアイテム（Items Displayed）] ドロップダウンを使用します。数値をクリックすると、[メッセージトラッキング（Message Tracking）] ページで選択した書き換えられた URL を含むすべてのメッセージのリストが表示されます。

[アウトブレイク フィルタ（Outbreak Filters）]ページを使用すると、次の情報を取得できます。

- 隔離されているメッセージの数と、それらの脅威のタイプ
- ウイルス発生に対するアウトブレイク フィルタ機能のリード タイム
- グローバル ウイルス発生と比較したローカル ウイルスの発生状況

[ウイルス タイプ（Virus Types）] ページ

[ウイルス タイプ（Virus Types）] ページでは、ネットワークに浸入したウイルスおよびネットワークから送信されたウイルスの概要が示されます。[ウイルスタイプ（Virus Types）] ページには、お使いの電子メールゲートウェイで稼働するウイルススキャンエンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して特定のアクションを実行することが推奨されます。たとえば、PDFファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDFが添付されているメッセージを隔離するフィルタ アクションを作成することが推奨されます。

複数のウイルス スキャン エンジンを実行している場合、[ウイルスタイプ（Virus Types）]ページには、イネーブルになっているすべてのウイルス スキャン エンジンの結果が含まれます。ページに表示されるウイルスの名前は、ウイルス スキャン エンジンによって判定された名前

です。複数のスキャンエンジンが 1 つのウイルスを検出した場合、同じウイルスに対して複数のエントリが存在する可能性があります。

[ウイルス タイプ（Virus Types）] ページには、ネットワークに浸入したウイルスおよびネットワークで送受信されたウイルスの概要が示されます。[検出した受信ウイルスの上位（Top Incoming Virus Detected）] セクションには、ネットワークに送信されたウイルスのチャートビューが降順で表示されます。[検出した送信ウイルスの上位（Top Outgoing Virus Detected）] セクションには、ネットワークから送信されたウイルスのチャートビューが降順で表示されます。

（注） ウイルスに感染したメッセージをネットワークに送信したホストを表示するには、[受信メール（Incoming Mail）] ページに移動し、同じ報告期間を指定して、ウイルス陽性別にソートします。同様に、ネットワーク内でウイルス陽性の電子メールを送信した IP アドレスを表示するには、[送信メッセージ送信者（Outgoing Senders）] ページを表示し、ウイルス陽性メッセージ別にソートします。

[ウイルス タイプの詳細（Virus Types Details）] リストには、感染した送受信メッセージ、および感染メッセージの総数など特定のウイルスに関する情報が表示されます。感染した受信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した受信メッセージの総数が表示されます。同様に、送信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した送信メッセージの総数が表示されます。ウイルスの種類の詳細は、[受信メッセージ（Incoming Messages）]、[送信メッセージ（Outgoing Messages）]、または [感染したメッセージの合計数（Total Infected Messages）] 別にソートできます。

[URL フィルタリング（URL Filtering）] ページ

- URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。
- URL フィルタリング レポートは、送受信メッセージに対して使用できます。
- URL フィルタリングエンジンによって（アンチスパム/アウトブレイク フィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して）スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではできません。
- [上位URLカテゴリ（Top URL Categories）] モジュールには、コンテンツ フィルタまたはメッセージフィルタに一致するかどうかにかかわらず、スキャンされたメッセージで検出されたすべてのカテゴリが含まれます。
- 各メッセージに関連付けることができる URL レピュテーション レベルは 1 つだけです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。
- [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] で設定したグローバル許可リストの URL は、レポートに含まれません。

  個別のフィルタで使用される許可リストの URL はレポートに含まれます。

- 悪意のある URL とは、アウトブレイク フィルタによってレピュテーションが低いと判定された URL です。ニュートラル URL とは、アウトブレイク フィルタによってクリック時の保護が必要と判定された URL です。このため、ニュートラル URL は、Cisco Web セキュリティ プロキシにリダイレクトするために書き換えられます。
- URL カテゴリ ベースのフィルタの結果はコンテンツおよびメッセージ フィルタ レポートに反映されます。
- Cisco Web セキュリティ プロキシによるクリック時の URL 評価の結果は、レポートに反映されません。

[Webインタラクショントラッキング（Web Interaction Tracking）] ページ

- Web インタラクション トラッキング レポート モジュールには、Web インタラクションのトラッキング機能がイネーブルの場合にのみデータが取り込まれます。
- Web インタラクション トラッキング レポート モジュールは、リアルタイムでは更新されず、30 分おきに更新されます。また、書き換えられた URL をクリックした後で、Web インタラクション トラッキング レポートにこのイベントがレポートされるまでには最大 2 時間かかることがあります。
- Web インタラクション トラッキング レポートは、リアルタイムで更新されません。クラウドにリダイレクトされる書き換えられた URL をクリックした後、Web インタラクション トラッキング レポートにこのイベントがレポートされるまでには最大 2 時間かかることがあります。
- Web インタラクション トラッキング レポートは、送受信メッセージに対して使用できます。
- エンドユーザがクリックした、クラウドにリダイレクトされる書き換えられた URL（ポリシーまたはアウトブレイク フィルタによって）のみが、これらのモジュールに含まれます。
- [Webインタラクショントラッキング（Web Interaction Tracking）] ページには、次のレポートが含まれます。

エンドユーザがクリックした、書き換えられた悪意のある上位 URL（Top Rewritten Malicious URLs clicked by End Users）。次の情報を含む詳細レポートを表示するには、URL をクリックします。

- 書き換えられた悪意のある URL をクリックしたエンドユーザのリスト。
- URL がクリックされた日付と時刻。
- URL がポリシーまたはアウトブレイク フィルタによって書き換えられたかどうか。
- 書き換えられた URL がクリックされたときに実行されたアクション（許可、ブロック、または不明）。URL がアウトブレイク フィルタによって書き換えられており、最終的な判定が使用できない場合、ステータスは不明として表示されます。

書き換えられた悪意のあるURLをクリックした上位エンドユーザ（Top End Users who clicked on Rewritten Malicious URLs）

Webインタラクショントラッキングの詳細（Web Interaction Tracking Details）。次の情報が含まれています。

- クラウドにリダイレクトされる書き換えられたすべての URL のリスト（悪意のあるものとないもの）。詳細レポートを表示するには、URL をクリックします。
- クラウドにリダイレクトされる書き換えられた URL がクリックされた場合に実行されたアクション（許可、ブロック、または不明）。

データを表示するには、次の操作を実行します。

- [受信メールポリシー（Incoming Mail Policies）] > [アウトブレイクフィルタ（Outbreak Filters）] を選択してアウトブレイク フィルタを設定し、メッセージの変更および URL の書き換えを有効にします。
- 「**Cisco Security Proxy にリダイレクト**」アクションを使用して、コンテンツ フィルタを構成します。

エンドユーザが URL をクリックしたときにその URL の判定（正常または悪意のある）が不明である場合、ステータスは不明として表示されます。これは、ユーザのクリック時に、URL がさらに調査されていたか、Web サーバがダウンしていたか、到達不可能であったためである可能性があります。

- 書き換えられた URL をエンドユーザがクリックした回数。クリックされた URL を含むすべてのメッセージのリストを表示するには、番号をクリックします。
- Web インタラクション トラッキング レポートを使用している場合は、次の制限事項に注意してください。
  - 悪意のある URL を書き換えた後に、メッセージを送信して別のユーザ（管理者など）に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックした場合でも、元の受信者の Web インタラクション トラッキング データが増分します。
  - 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用してユーザ（管理者など）に送信する場合、そのユーザ（メッセージのコピーが送信されたユーザ）がその書き換えられた URL をクリックした場合でも、元の受信者の Web インタラクション トラッキング データが増分します。
  - どの時点であっても、電子メールゲートウェイの時刻を変更する予定がある場合は、システム時刻を協定世界時（UTC）と同期するようにしてください。

偽造メールの一致レポート

偽装メールの検出結果の監視 （788 ページ） を参照してください。

ファイル レピュテーションおよびファイル分析レポート

次に示すレポートについては、ファイル レピュテーションおよびファイル分析のレポートとトラッキング （616 ページ）を参照してください。

- 高度なマルウェア防御（Advanced Malware Protection）
- ファイル分析（File Analysis）
- AMP判定のアップデート（AMP Verdict Updates）

[メールボックスの自動修復（Mailbox Auto Remediation）] レポート

[メールボックスの自動修復レポート（Mailbox Auto Remediation report）] ページを使用して（[モニタ（Monitor）] > [メールボックスの自動修復（Mailbox Auto Remediation）]）、メールボックス修復結果の詳細を表示できます。このレポートを使用して次の詳細を表示します。

- メッセージに対してとられる修復のアクション
- SHA-256 ハッシュに関連付けられているファイル名
- メールボックス修復が成功または失敗した受信者について定義されているプロファイル名の一覧
- 修復が失敗した理由
- ドメインにマッピングされたプロファイルがない

メッセージ トラッキングに関連メッセージを表示するには、SHA-256 ハッシュをクリックします。

詳細については、メールボックスでのメッセージの修復 （709 ページ）を参照してください。

[TLS 接続（TLS Connections）] ページ

[TLS 接続（TLS Connections）] ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。

[TLS 接続（TLS Connections）] ページを使用すると、次の情報を測定できます。

- 送受信接続による、全体的な TLS の使用割合
- TLS 接続に成功したパートナー
- TLS 接続に成功しなかったパートナー
- DANE がサポートされている TLS 接続に成功したパートナー
- DANE がサポートされている TLS 接続に失敗したパートナー
- TLS 認証に問題のあるパートナー
- パートナーが TLS を使用したメールの全体的な割合
- DANE がサポートされている送信 TLS 接続に成功した割合
- DANE がサポートされている送信接続に失敗した割合

[TLS 接続（TLS Connections）] ページは、着信接続に関するセクションと、発信接続に関するセクションに分かれています。各セクションには、詳細情報が含まれたグラフ、サマリー、および表が含まれています。

グラフには、指定した時間範囲にわたる、送受信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。グラフには、メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した TLS 暗号化メッセージの量、成功/失敗した DANE 接続の量が表示されます。グラフでは、TLS が必須であった接続と、TLS が単に優先された接続が区別されます。

表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。ドメインごとに、成功/失敗した必須の TLS 接続と優先された TLS 接続の数、試行された TLS 接続の総数（成功したか失敗したかにかかわらず）、暗号化されていない接続の総数、DANE 接続の総数（成功したか失敗したかに応じて）を表示できます。また、TLS が試行されたすべての接続の割合、および正常に送信された暗号化メッセージの総数（TLS が優先か必須かにかかわらず）も表示できます。この表の下部にある [列（Columns）] リンクをクリックすることにより、カラムの表示/非表示を切り替えることができます。

[受信 SMTP 認証（Inbound SMTP Authentication）] ページ

[受信SMTP認証（Inbound SMTP Authentication）] ページには、クライアント証明書の使用情報、および電子メールゲートウェイとユーザのメールクライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。電子メールゲートウェイは、証明書または SMTP AUTH コマンドを受け入れると、メールクライアントへの TLS 接続を確立します。クライアントはこの接続を使用してメッセージを送信します。電子メールゲートウェイは、これらの試行をユーザ単位で追跡できないため、レポートには、ドメイン名とドメイン IP アドレスに基づいて SMTP 認証の詳細が表示されます。

次の情報を確認するには、このレポートを使用します。

- SMTP 認証を使用している着信接続の総数
- クライアント証明書を使用している接続の数
- SMTP AUTH を使用している接続の数
- SMTP 認証を使用しようとして、接続が失敗したドメイン
- SMTP 認証が失敗した一方で、フォールバックを正常に使用している接続の数

[受信SMTP認証（Inbound SMTP Authentication）] ページには、受信した接続のグラフ、SMTP 認証接続を試行したメール受信者のグラフ、および接続の認証試行の詳細を含むテーブルが表示されます。

[受信した接続（Received Connections）] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメールクライアントの着信接続が示されます。このグラフには、電子メールゲートウェイが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。

[受信した受信者（Received Recipients）] グラフには、SMTP 認証を使用して、メッセージを送信するために電子メールゲートウェイへの接続を認証しようとしたメールクライアントを所有

する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。

[SMTP認証の詳細（SMTP Authentication details）] テーブルには、メッセージを送信するために電子メールゲートウェイへの接続を認証しようとしたユーザを含むドメインの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行（成功または失敗）の数、SMTP AUTH コマンドを使用した接続試行（成功または失敗）の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。ページ上部のリンクを使用して、ドメイン名またはドメイン IP アドレス別にこの情報を表示できます。

[レート制限（Rate Limits）] ページ

エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メール メッセージ受信者数を制限できます。[レート制限（Rate Limits）] レポートには、この制限を最も上回った送信者が表示されます。

このレポートは、以下を特定する場合に役立ちます。

- 大量のスパムを送信するために使用される可能性のある信用できないユーザ アカウント
- 通知、アラート、自動報告などに電子メールを使用する組織内の制御不能アプリケーション
- 内部請求やリソース管理のために、組織内で電子メールを過剰に送信している送信元
- スパムとは見なされないが、大量の着信電子メール トラフィックを送信している送信元

内部送信者に関する統計情報を含む他のレポート（[内部ユーザ（Internal Users）]、[送信メッセージ送信者（Outgoing Senders）] など）では、送信されたメッセージの数のみ計測されます。これらのレポートでは、少数のメッセージを多数の受信者に送信した送信者は識別されません。

[上位攻撃者(インシデント別)（Top Offenders by Incident）] チャートには、設定済み制限よりも多くの受信者にメッセージを最も頻繁に送信しようとしたエンベロープ送信者が表示されます。各試行が 1 インシデントに相当します。このチャートでは、すべてのリスナーからのインシデント数が集計されます。

[上位攻撃者(拒否した受信者数)（Top Offenders by Rejected Recipients）] チャートには、設定済みの制限を上回る、最も多くの受信者にメッセージを送信したエンベロープ送信者が表示されます。このチャートでは、すべてのリスナーからの受信者数が集計されます。

エンベロープ送信者によるレート制限の設定、または既存のレート制限の変更については、メール フロー ポリシーを使用した着信メッセージのルールの定義（124 ページ）を参照してください。

[システム容量（System Capacity）] ページ

[システム容量（System Capacity）] ページでは、ワーク キュー内のメッセージ数、ワーク キューで費やした平均時間、送受信メッセージ（量、サイズ、件数）、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページ スワップ情報などシステム負荷の詳細が示されます。

[システム容量（System Capacity）] ページを使用すると、次の情報を確認できます。

- 電子メールゲートウェイが推奨キャパシティを超えて、設定の最適化または追加電子メールゲートウェイが必要になった時間
- キャパシティの問題が今後発生する可能性を示すシステム挙動の過去のトレンド
- 最も多くのリソースを使用したシステムの部分（トラブルシューティングを支援するため）

お使いの電子メールゲートウェイをモニタして、メッセージの量に対してキャパシティが適切であることを確認することが重要です。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。システム キャパシティをモニタする最も効果的な方法は、全体的な量、ワーク キュー内のメッセージ、およびリソース節約モードのインシデントを追跡することです。

- **量**：「通常」のメッセージ量と環境内での「異常」な増加を把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール（Incoming Mail）] ページおよび[送信メール（Outgoing Mail）]ページを使用すると、経時的に量を追跡できます。詳細については、[システム容量（System Capacity）] : [受信メール（Incoming Mail）]（1045 ページ）および[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]（1046 ページ）を参照してください。
- **ワーク キュー**：ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、有害メッセージの異常な増加を処理する、「緩衝装置」として設計されています。しかしワーク キューは、負荷のかかっているシステムを示す最良の指標であり、長く、頻繁なワーク キューのバックアップは、キャパシティの問題を示している可能性があります。[ワーク キュー（WorkQueue）] ページを使用すると、ワーク キュー内でメッセージが費やした平均時間およびワーク キュー内のアクティビティを追跡できます。詳細については、[システム容量（System Capacity）] : [ワークキュー（Workqueue）]（1045 ページ）を参照してください。
- **リソース節約モード**：電子メールゲートウェイがオーバーロードになると、「リソース節約モード」（RCM）になり、CRITICAL システムアラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いの電子メールゲートウェイは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。[システム容量（System Capacity）] : [システムの負荷（System Load）]（1046 ページ）を参照してください。

関連項目

- [システム容量（System Capacity）] : [ワークキュー（Workqueue）]（1045 ページ）
- [システム容量（System Capacity）] : [受信メール（Incoming Mail）]（1045 ページ）
- [システム容量（System Capacity）] : [送信メール（Outgoing Mail）]（1046 ページ）
- [システム容量（System Capacity）] : [システムの負荷（System Load）]（1046 ページ）
- メモリ ページ スワッピングに関する注意事項（1047 ページ）
- [システム容量（System Capacity）] : [すべて（All）]（1047 ページ）

[システム容量（System Capacity）]：[ワークキュー（Workqueue）]

[ワークキュー（Workqueue）] ページには、ワーク キュー内でメッセージが費やした平均時間（スパム隔離またはポリシー、ウイルス、およびアウトブレイク隔離で費やした時間は除く）が表示されます。1 時間から 1 月までの時間範囲を表示できます。平均は、メール配信を遅延させた短期間のイベントおよびシステム上の負荷の長期トレンドの両方を識別するのに役立ちます。

（注） 隔離からワーク キューにメッセージが解放される場合、「ワーク キュー内の平均時間」メトリックではこの時間が無視されます。これにより、重複集計と検疫で費やされた延長時間による統計の歪みを回避できます。

このレポートでは、指定期間のワーク キュー内のメッセージの量および同期間のワーク キュー内の最大メッセージ数も示されます。ワーク キューの最大メッセージのグラフ表示でも、ワーク キューのしきい値レベルが示されます。

[ワークキュー（Workqueue）] グラフにおける不定期のスパイクは、正常であり、発生する可能性があります。ワーク キュー内のメッセージが長期間、設定済みしきい値よりも大きい場合は、キャパシティの問題を示している可能性があります。このシナリオでは、しきい値レベルを調整することを検討するか、またはシステム設定を確認します。

ワーク キューのしきい値レベルを変更する手順については、システム状態パラメータのしきい値の設定 （1273 ページ）を参照してください。

ヒント [ワークキュー（Workqueue）]ページを確認するときは、作業キューバックアップの頻度を測定し、10,000 メッセージを超える作業キュー バックアップに注意することが推奨されます。

[システム容量（System Capacity）]：[受信メール（Incoming Mail）]

[受信メール（Incoming Mail）] ページには、着信接続、着信メッセージの総数、平均メッセージサイズ、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[受信メール（Incoming Mail）] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。着信メール データと送信者プロファイルデータを比較して、特定のドメインからネットワークに送信される電子メールの量のトレンドを表示することも推奨されます。

（注） 着信接続数の増加は、必ずしもシステム負荷に影響を与えるわけではありません。

[システム容量（System Capacity）]：[送信メール（Outgoing Mail）]

[送信メール（Outgoing Mail）] ページには、発信接続、発信メッセージの総数、平均メッセージサイズ、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[送信メール（Outgoing Mail）] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。発信メールデータと発信宛先データを比較して、特定のドメインまたは IP アドレスから送信される電子メールの量のトレンドを表示することも推奨されます。

[システム容量（System Capacity）]：[システムの負荷（System Load）]

システムの負荷レポートに、次が表示されます。

- 全体のCPU使用率（Overall CPU Usage）
- メモリページスワップ（Memory Page Swapping）
- リソース節約アクティビティ

全体のCPU使用率（Overall CPU Usage）

電子メールゲートウェイは、アイドル状態の CPU リソースを使用してメッセージスループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステム キャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリ ページ スワッピングが発生する場合、キャパシティの問題の可能性があります。

（注） このグラフには、CPU 使用率のしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定 （1273 ページ）を参照してください。

このページでは、メール処理、スパムおよびウイルスエンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す良い指標です。電子メールゲートウェイの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

メモリページスワップ（Memory Page Swapping）

メモリ ページ スワッピングのグラフは、システムによるディスクへのページングが必要な頻度を示します。このグラフには、メモリ ページ スワッピングのしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定 （1273 ページ）を参照してください。

リソース節約アクティビティ

リソース節約アクティビティグラフは、電子メールゲートウェイがリソース節約モード（RCM）になった回数を示します。たとえば、グラフにn回と示されている場合は、電子メールゲートウェイが n 回 RCM になり、少なくとも n-1 回終了していることを意味します。

お使いの電子メールゲートウェイは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。リソース節約アクティビティグラフに電子メールゲートウェイが頻繁にRCSになっていることが示されている場合は、システムが過負荷になっていることを示している可能性があります。

メモリ ページ スワッピングに関する注意事項

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリスワッピングは起こり得るものであり、電子メールゲートウェイの問題を示すものではありません。システムが常に高ボリュームのメモリ スワッピングを行っている場合を除き、メモリ スワッピングは予想される正常な動作です（特に C170 および C190 アプライアンスの場合）。パフォーマンスを向上させるには、ネットワークに電子メールゲートウェイを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。

[システム容量（System Capacity）]：[すべて（All）]

[すべて（All）]ページでは、これまでのすべてのシステム キャパシティ レポートを単一のページに統合し、さまざまなレポート同士の関係を表示することができます。たとえば、過剰なメモリ スワッピングの発生と同時期にメッセージ キューが高いことを確認できます。これは、キャパシティの問題の兆候である可能性があります。このページを PDF として保存し、後で参照するために（またはサポート スタッフと共有するために）システム パフォーマンスのスナップショットを保存することが推奨されます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

[システムステータス（System Status）] ページ

[システムステータス（System Status）] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。表示される情報は、CLI で status detail コマンドおよび **dnsstatus** コマンドを使用して入手できる情報と同じです。status detail コマンドの詳細については、CLIによる管理およびモニタリング （1333ページ）の「詳細な電子メール ステータスのモニタリング」を参照してください。**dnsstatus** コマンドの詳細については、同章の「DNS ステータスの確認」を参照してください。

[システム ステータス（System Status）] ページは、[システム ステータス（System Status）]、[ゲージ（Gauges）]、[レート（Rates）]、および [カウンタ（Counters）] の 4 つのセクションで構成されます。

関連項目

- システム ステータス （1048 ページ）
- ゲージ （1048 ページ）

- レート （1049 ページ）
- カウンタ （1049 ページ）

システム ステータス

[システム ステータス（System Status）] セクションには、[メール システムのステータス（Mail System Status）] および [バージョン情報（Version Information）] が示されます。

関連項目

- メール システムのステータス（Mail System Status） （1048 ページ）
- バージョン情報 （1048 ページ）

メール システムのステータス（Mail System Status）

[メール システムのステータス（Mail System Status）] セクションには、次の情報が含まれます。

- システム ステータス（システム ステータスの詳細については、ステータス（Status） （1016 ページ）を参照してください）。
- ステータスが報告された最終時刻。
- 電子メールゲートウェイのアップタイム。
- システム内の最も古いメッセージ（配信用にまだキューに入っていないメッセージも含む）。

バージョン情報

[バージョン情報（Version Information）] セクションには、次の情報が含まれます。

- 電子メールゲートウェイのモデル名。
- インストールされている AsyncOS オペレーティング システムのバージョンとビルド日。
- AsyncOS オペレーティング システムのインストール日。
- 接続先のシステムのシリアル番号。

この情報は、シスコ カスタマー サポートに問い合わせる場合に役立ちます。（テクニカル サポートの使用 （1539 ページ） を参照。）

ゲージ

[ゲージ（Gauges）] には、次のようにキューおよびリソース使用率について示されます。

- メール処理キュー（Mail Processing Queue）
- キュー内のアクティブ受信者（Active Recipients in Queue）
- キュー スペース（Queue Space）
- CPU 使用率

メール ゲートウェイ アプライアンスは、AsyncOS プロセスが消費している CPU 率を参照します。CASE は、アンチスパム スキャン エンジンおよびアウトブレイク フィルタ プロセスなど複数のアイテムを参照します。

- 一般的なリソース使用率（General Resource Utilization）
- ログに使用されているディスク容量（Logging Disk Utilization）

レート

[レート（Rates）] セクションには、次の受信者に関する処理率が示されます。

- メール処理レート（Mail Handling Rates）
- 処理済みの割合（Completion Rates）

カウンタ

システム統計情報用の累積電子メール モニタリング カウンタをリセットし、カウンタの最終リセット日時を表示することができます。リセットは、システム カウンタおよびドメインごとのカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。

（注） 管理者グループまたはオペレータ グループに属するユーザ アカウントのみが、カウンタをリセットできます。ゲスト グループ内で作成したユーザ アカウントでは、カウンタをリセットできません。詳細については、ユーザー アカウントを使用する作業（1191 ページ）を参照してください。

カウンタをリセットするには、[カウンタをリセット（Reset Counters）] をクリックします。このボタンは、CLI の **resetcounters** コマンドと同様の機能を提供します。詳細については、電子メール モニタリング カウンタのリセット（1350 ページ）を参照してください。

- メール処理イベント（Mail Handling Events）
- 処理済みイベント（Completion Events）
- ドメイン キー イベント（Domain Key Events）
- DNS ステータス（DNS Status）

[大容量のメール（High Volume Mail）] ページ

（注） [大容量のメール（High Volume Mail）] ページには、Header Repeats ルールを使用するメッセージ フィルタのデータだけが表示されます。

[大容量のメール（High Volume Mail）] ページには、次のレポートが横棒グラフの形式で表示されます。

- [上位件名（Top Subjects）]。このグラフから、AsyncOS が受信したメッセージの上位件名を確認できます。
- [上位エンベロープ送信者（Top Envelope Senders）]。このグラフから、AsyncOS が受信したメッセージの上位エンベロープ送信者を確認できます。

- [一致数別上位メッセージフィルタ（Top Message Filters by Number of Matches）]。このグラフから、一致数に基づく（Header Repeats ルールを使用する）上位メッセージ フィルタを確認できます。

[大容量のメール（High Volume Mail）] ページには、上位メッセージ フィルタと、該当するメッセージフィルタに一致したメッセージの数を示す表も表示されます。数値をクリックすると、メッセージ トラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートするか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。

[メッセージフィルタ（Message Filters）] ページ

[メッセージフィルタ（Message Filters）] ページには、一致数の上位メッセージ フィルタ（最も多くのメッセージに一致したメッセージフィルタ）に関する情報が 2 種類の形式（棒グラフと表）で表示されます。

棒グラフでは、送受信メッセージによって最も多くトリガーされるメッセージフィルタを確認できます。表には、上位メッセージフィルタと、該当するメッセージフィルタに一致したメッセージの数が示されます。数値をクリックすると、メッセージ トラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートするか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。

[Safe Print] ページ

[Safe Print] レポート ページを使用して、次の内容を表示できます。

- ファイル タイプ別の、Safe Print で出力された添付ファイルの数（グラフ形式）。
- ファイル タイプ別の、Safe Print で出力された添付ファイルの概要（表形式）。

[Safe Printで出力されたファイル種類の概要（Summary of Safe Print File Types）] セクションで Safe Print で出力された添付ファイルの合計数をクリックすると、[メッセージトラッキング（Message Tracking）] にメッセージの詳細が表示されます。

CSV データの取得

電子メール セキュリティ モニタで図やグラフの作成に使用されたデータは、CSV 形式で取得できます。CSV データにアクセスする方法は、次の 2 つです。

- **電子メールによる CSV レポートの配信**。電子メールで配信される、またはアーカイブされる CSV レポートを生成できます。この配信方法は、[レポート（Reports）] ページに表示される各表に関する個別レポートを必要とする場合、または内部ネットワークにアクセスできないユーザに CSV データを送信する場合に便利です。

  Comma-Separated Value（CSV; カンマ区切り）レポート タイプは、スケジュール設定されたレポートの表形式データを含む ASCII テキスト ファイルです。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。単一のレポートの複数の CSV ファイルは、単一の .zip ファイルに圧縮されて、アーカイブ ファイルの保存オプションを提供するか、個別の電子メール メッセージに添付されて電子メールで配信されます。

- **HTTP による CSV ファイルの取得**。電子メール セキュリティ モニタ機能で図やグラフの作成に使用されたデータは、HTTP を使用して取得できます。この配信方法は、他のツールを使用してデータの詳細分析を実行する予定の場合に役立ちます。たとえば、未加工データのダウンロード、処理、および他のシステムでの結果表示を行う自動スクリプトによって、データの取得を自動化できます。

関連項目

- 自動プロセスによる CSV データの取得 （1051 ページ）

自動プロセスによる CSV データの取得

必要とする HTTP クエリーを最も容易に取得する方法は、必要な種類のデータを表示するように電子メール セキュリティ モニタ ページの 1 つを設定することです。次に、[エクスポート（Export）] リンクをコピーできます。これがダウンロード URL です。このようにデータ取得を自動化した場合、ダウンロード URL 内のパラメータを固定し、変更しないことが重要です（下記を参照）。

ダウンロード URL はコード化されるので、（適切な HTTP 認証を使用して）同じクエリーを実行し、同様のデータ セットを取得できる外部スクリプトにコピーできます。このスクリプトでは、Basic HTTP 認証またはクッキー認証を使用できます。自動プロセスで CSV データを取得する場合は、次の事項に注意する必要があります。

- URL の再利用時に関する時間範囲の選択（過去 1 時間、1 日、1 週間など）。URL をコピーして「過去 1 日」の CSV データ セットを取得する場合、この URL を次に使用するときには、URL の再送信時から「過去 1 日」を対象とする新しいデータ セットを取得します。時間範囲の選択は保持され、CSV クエリ文字列（たとえば date_range=current_day）に表示されます。
- データ セットのフィルタリングおよび分類の優先順位。フィルタは保持され、クエリー文字列に表示されます。レポートでは、フィルタはほとんど使用されません。1 つの例としては、発生レポートにおける「グローバル/ローカル」発生セレクタが挙げられます。
- CVS ダウンロードでは、選択した時間範囲について表内のデータのすべての行が返されます。

- CSV では、タイムスタンプおよびキーで指示された表内のデータの行が返されます。スプレッドシートアプリケーションを使用するなどして、別個のステップで更にソートできます。
- 最初の行には、レポートに示される表示名に一致するカラム見出しが含まれています。タイムスタンプ（タイムスタンプ （1052 ページ）を参照）およびキー（オプション キー（Keys） （1053 ページ）を参照）も表示されます。

関連項目

- URL のサンプル （1052 ページ）
- Basic HTTP 認証クレデンシャルの追加 （1052 ページ）
- ファイル形式（File Format） （1052 ページ）
- タイムスタンプ （1052 ページ）
- オプション キー（Keys） （1053 ページ）
- ストリーミング （1053 ページ）

URL のサンプル

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=
MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0
&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

Basic HTTP 認証クレデンシャルの追加

URL に Basic HTTP 認証クレデンシャルを指定する例を次に示します。

`http://example.com/monitor/`

次のようになります。

`http://username:password@example.com/monitor/`

ファイル形式（File Format）

ダウンロードされるファイルは CSV 形式であり、ファイル拡張子は .csv です。ファイル見出しは、デフォルトのファイル名であり、レポートの名前に始まり、レポートのセクションが続きます。

タイムスタンプ

データのストリーミングを行うエクスポートには、各行の時間「間隔」について開始タイムスタンプおよび終了タイムスタンプが示されます。2 種類の開始タイムスタンプおよび終了タイムスタンプ（数値形式および人間が読み取れる文字列形式）が提供されます。タイムスタンプは GMT 時間です。これにより、電子メールゲートウェイが複数の時間帯にある場合、ログの集約が容易になります。

あまりないことですが、データが他のソースのデータとマージされる場合には、エクスポートファイルにタイムスタンプは含まれません。たとえば、発生の詳細のエクスポートでは、レポートのデータと Threat Operations Center（TOC）データがマージされ、タイムスタンプが不適切になります。これは、間隔が存在しないためです。

オプション キー（Keys）

レポートにキーが表示されない場合であっても、エクスポートには、レポート テーブル キーが含まれます。キーが表示される場合、レポートに表示される表示名がカラム見出しとして使用されます。それ以外の場合は、「key0」、「key1」などのカラム見出しが表示されます。

ストリーミング

大部分のエクスポートでは、データをクライアントにストリーミングで戻します。これは、データ量が非常に大きい可能性があるからです。しかし、一部のエクスポートでは、ストリーミング データではなく結果セット全体を返します。通常、レポート データが非レポート データ（発生の詳細など）と集約される場合が該当します。

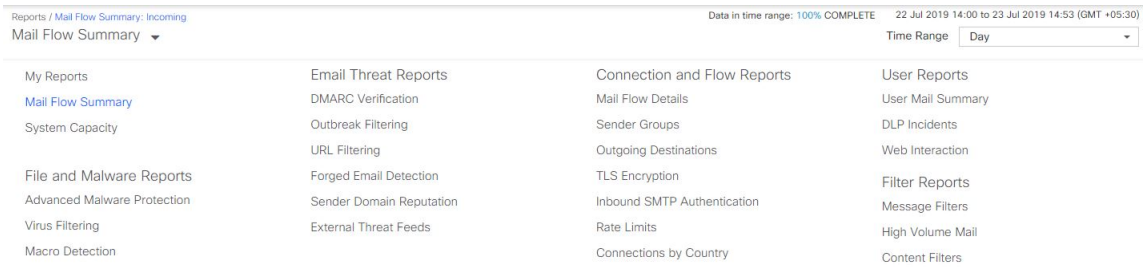
新しいWebインターフェイスの電子メールセキュリティモニタ ページ

新しい Web インターフェイスにログインするには、レガシー Web インターフェイスの [Secure Email Gatewayの外観が新しくなりました。お試しください（Secure Email Gateway is getting a new look. Try it!!）] リンクをクリックします。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセス （37 ページ）を参照してください。

次の図に示す [レポート（Reports）] ドロップダウンを使用すると、電子メールゲートウェイのレポートを表示することができます。

（注） [メールフロー概要（Mail Flow Summary）] レポート ページは、ランディング ページ（ログイン後に表示されるページ）です。

図 *70 : [レポート（Reports）] ドロップダウン*



GUI でこれらのページを使用して、電子メールゲートウェイのリスナーに接続しているドメインをモニタできます。お使いの電子メールゲートウェイの「メールフロー」のモニタ、ソート、分析、および分類を実行し、正規メールの大量送信者と「スパマー」（未承諾の商業用メールの大量送信者）またはウイルス送信者の疑いのあるユーザとを区別できます。これらのページは、システムへの着信接続のトラブルシューティングにも役立ちます（IP レピュテーションスコア、ドメインに対する直近の送信グループの一致など重要情報を含みます）。

これらのページは、電子メールゲートウェイに関連するメール、さらにゲートウェイの範囲を超えて存在するサービス（IP レピュテーションサービス、アンチスパム スキャン サービス、アンチウイルス スキャン セキュリティ サービス、コンテンツフィルタ、およびアウトブレイクフィルタ）に関連するメールの分類に役立ちます。

[エクスポート（Export）] リンクでは、グラフおよび他のデータを Comma Separated Value（CSV; カンマ区切り値）形式にエクスポートできます。

エクスポートされた CSV データは、電子メールゲートウェイでの設定にかかわらず、すべてのメッセージトラッキングおよびレポーティングデータを GMT で示します。GMT 時間への変換の目的は、電子メールゲートウェイに依存せずにデータを使用したり、複数の時間帯にある電子メールゲートウェイからのデータを参照する際にデータを使用したりできるようにするためです。

（注） ローカライズされた CSV データをエクスポートする場合、一部のブラウザでは見出しが正しく表示されないことがあります。これは、ローカライズされたテキストに対して、一部のブラウザが適切な文字セットを使用していないためです。この問題を回避するには、ファイルをディスクに保存し、[ファイル（File）] > [開く（Open）] を使用してファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

レポートデータのエクスポートの自動化の詳細については、CSV データの取得 （1050 ページ）を参照してください。

電子メール セキュリティ モニタ ページのリスト

- [お気に入りレポート（My Favorite Reports）] ページ （1057 ページ）
- [メール フロー概要（Mail Flow Summary）] ページ （1060 ページ）
- [システム容量（System Capacity）] ページ （1043 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] ページ （1070 ページ）
- [ウイルス フィルタリング（Virus Filtering）] ページ （1076 ページ）
- [マクロ検出（Macro Detection）] ページ （1077 ページ）
- [DMARC検証（DMARC Verification）] ページ （1078 ページ）
- [アウトブレイク フィルタリング（Outbreak Filtering）] ページ （1079 ページ）
- [URL フィルタリング（URL Filtering）] ページ （1078 ページ）
- [偽装メールの検出（Forged Email Detection）] ページ （1081 ページ）
- [送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ （1082 ページ）
- [外部脅威フィード（External Threat Feeds）] ページ （1082 ページ）
- [メール フローの詳細（Mail Flow Details）] ページ （1083 ページ）

- 送信者グループ レポート （1093 ページ）
- 送信先 （1093 ページ）
- [TLS暗号化（TLS Encryption）] ページ （1094 ページ）
- [受信 SMTP 認証（Inbound SMTP Authentication）] ページ （1094 ページ）
- [レート制限（Rate Limits）] ページ （1095 ページ）
- [国別の接続（Connections by Country）] ページ （1096 ページ）
- [ユーザー メール サマリー（User Mail Summary）] ページ （1096 ページ）
- [DLP インシデント サマリー（DLP Incident Summary）] ページ （1098 ページ）
- [Web インタラクション（Web Interaction）] ページ （1100 ページ）
- [メッセージフィルタ（Message Filters）] ページ （1103 ページ）
- [大容量のメール（High Volume Mail）] ページ （1104 ページ）
- [コンテンツフィルタ（Content Filters）] ページ （1104 ページ）
- [高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ （1105 ページ）
- [メールポリシーの詳細（Mail Policy Details）] レポートページ （1106 ページ）

検索およびインタラクティブ電子メール レポート ページ

インタラクティブ電子メール レポート ページの多くでは、ページの下部に**[検索対象：（Search For:）]** ドロップダウン メニューがあります。

ドロップダウン メニューから、次のような数種類の条件で検索できます。

- IP アドレス
- ドメイン
- ネットワーク オーナー
- 内部ユーザ
- 宛先ドメイン
- 内部送信者のドメイン
- 内部送信者の IP アドレス
- 着信 TLS ドメイン
- 発信 TLS ドメイン
- SHA-256

多くの検索では、検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example.com」が一致します）を選択します。

IPv4 検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば、「17.*」は 17.0.0.0 ～ 17.255.255.255 の範囲で検索されるので、17.0.0.1 は一致しますが、172.0.0.1 は一致しません。完全一致検索の場合は、4 つすべてのオクテットを入力します。IP アドレス検索は、クラスレス ドメイン間ルーティング（CIDR）形式（17.16.0.0/12）もサポートします。

IPv6 検索の場合、次の例の形式を使用して、アドレスを入力できます。

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

レポートに含まれるメッセージの詳細の表示

この機能は、レポートとトラッキングが両方ともローカルの場合（Cisco Secure Email and Web Managerで中央管理されていない場合）にのみ、機能します。

手順

ステップ 1 レポート ページのテーブルにある青色の番号をクリックします

（一部のテーブルにのみ、これらのリンクはあります）。

この番号に関連するメッセージがメッセージ トラッキングで表示されます。

ステップ 2 下にスクロールして、リストを表示します。

次のタスク

関連項目

- メッセージ トラッキングの検索結果の使用 （1121 ページ）

レポートの時間範囲

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

時間範囲は、次の表に記載のオプションから選択します。

表 *86*：電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時間（Hour）	直近の 60 分 + 最大 5 分
日（Day）	直近の 24 時間と直近の 60 分
週（Week）	直近の 7 日 + 当日の経過した時間
30 日（30 days）	直近の 30 日 + 当日の経過した時間
90 日（90 days）	直近の 90 日 + 当日の経過した時間
昨日（Yesterday）	00:00 ～ 23:59（午前 0 時～午後 11:59）
先月（Previous Calendar Month）	その月の最初の日の 00:00 ～その月の最後の日の 23:59
カスタム範囲（Custom Range）	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

[お気に入りレポート（My Favorite Reports）] ページ

[マイレポート（My Reports）] ページで、既存のすべての電子メール セキュリティ レポートからチャート（グラフ）とテーブルを組み合わせてカスタム レポート ページを作成できます。

目的	操作手順
[お気に入りレポート（My Favorite Reports）] ページへのモジュールの追加	参照先： • [マイレポート（My Reports）] ページに追加できないモジュール （1058 ページ） • [お気に入りレポート（My Favorite Reports）] ページでのレポートの追加 （1059 ページ）

目的	操作手順
[お気に入りレポート（My Favorite Reports）] ページの表示	1. [レポート（Reports）] ドロップダウンから [お気に入りレポート（My Favorite Reports）] を選択します。 2. 表示する時間範囲を選択します。選択した時間範囲は、[お気に入りレポート（My Favorite Reports）] ページのすべてのモジュールを含めて、すべてのレポートに適用されます。 新しく追加されたモジュールはカスタム レポートの上部に表示されます。 （注） 新しい Web インターフェイスの [お気に入りレポート（My Favorite Reports）] ページに追加するレポートモジュールは、レガシー Web インターフェイスに追加されたレポートモジュールとは異なります。割り当てたユーザロールによって異なる場合もあります。
[お気に入りレポート（My Favorite Reports）] ページでのモジュールの再配置	[お気に入りレポート（My Favorite Reports）] ページで、モジュールを目的の場所にドラッグアンドドロップします。
[お気に入りレポート（My Favorite Reports）] ページからのモジュールの削除	次のいずれかの方法で、[お気に入りレポート（My Favorite Reports）] ページからレポートモジュールを削除できます。 • 目的のレポート モジュールの右上にある ★ をクリックします。 • [お気に入りレポート（My Favorite Reports）] ページに移動し、[お気に入りの管理（Manage Favorites）] を選択して該当するレポートモジュールを削除します。

[マイレポート（My Reports）] ページに追加できないモジュール

- [システムステータス（System Status）] ページのすべてのモジュール。
- [有効なレポートデータ（Reporting Data Availability）] ページのすべてのモジュール。
- [有効なメッセージトラッキングデータ（Message Tracking Data Availability）] ページのすべてのモジュール。

- [送信者プロファイル（Sender Profile）] 詳細レポート ページのドメイン単位のモジュール（[SenderBaseからの最新情報（Current Information from SenderBase）]、[送信者グループ情報（Sender Group Information）]、および [ネットワーク情報（Network Information）]）。
- [アウトブレイクフィルタ（Outbreak Filters）] レポート ページの [過去1年間のウイルスアウトブレイクサマリー（Past Year Virus Outbreak Summary）] チャートおよび [過去1年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] テーブル。

[お気に入りレポート（My Favorite Reports）] ページでのレポートの追加

始める前に

- 追加するモジュールが追加可能であることを確認します。[マイレポート（My Reports）] ページに追加できないモジュール （1058 ページ）を参照してください。
- 不要なデフォルト モジュールを削除するには、そのモジュールの右上にある ★ をクリックします。

手順

ステップ 1 [お気に入り レポート（My Favorite Reports）] ページには、次のいずれかの方法でレポートモジュールを追加できます。

（注） 一部のモジュールは、以下のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- [レポート（Reports）] ドロップダウンのレポート ページに移動し、レポート モジュールの上部にある ★ をクリックします。
- [レポート（Reports）] ドロップダウンから [マイレポート（My Reports）] を選択し、[お気に入りの管理（Manage Favorites）] をクリックします。

  レポート モジュールは、電子メール レポート ページのテーブルとチャートに従ってリストされます。必要なレポートモジュールを選択し、**[追加（Add）]** をクリックして [お気に入りレポート（My Favorite Reports）] ページに追加します。[お気に入り レポート（My Favorites Report）] ページにレポートが表示されないようにするには、レポートモジュールを選択して **[削除（Remove）]** をクリックします。

  各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

  （注） [お気に入り レポート（My Favorite Reports）] ページには、最大 10 個のレポートモジュールを追加できます。

ステップ 2 カスタマイズしたレポートモジュール（列を追加、削除、または順序変更したり、チャートにデフォルト以外のデータを表示するなど）を追加する場合は、[お気に入りレポート（My Favorite Reports）] ページでモジュールをカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

ステップ 3 別個の凡例（たとえば、[メールフロー概要（Mail Flow Summary）] ページのグラフ）を含むチャートを追加する場合は、凡例を個別に追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。

[メール フロー概要（Mail Flow Summary）] ページ

[メールフロー概要（Mail Flow Summary）] レポートページは、電子メールゲートウェイ上の電子メール メッセージ アクティビティの概要を示します。[メール フロー概要（Mail Flow Summary）] レポート ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

[メールフロー概要：着信（Mail Flow Summary：Incoming）] レポートページは、電子メールゲートウェイで処理およびブロックされたメッセージの合計数についての着信メールグラフと、着信メールの概要を示します。

このページのメールトレンドグラフを使用して、選択した時間範囲に基づいて電子メールゲートウェイで処理およびブロックされたすべての着信メールのフローをモニタできます。詳細については、レポートの時間範囲 （1056 ページ）を参照してください。

データ内の特定の情報を検索するには、次を参照してください。検索およびインタラクティブ電子メール レポート ページ （1055 ページ）

次のメール トレンド グラフは、着信メール フローを視覚的に表したものです。

- 脅威検出の概要
- コンテンツの概要

それぞれのカテゴリの必須カウンタに基づいて、着信メッセージのメール トレンドを表示できます。詳細については、カウンタを使用しての、トレンドグラフ上のデータのフィルタリング（1066 ページ）を参照してください。

[メールフロー概要：発信（Mail Flow Summary：Outgoing）] レポートページは、電子メールゲートウェイによって処理および配信されたメッセージの合計数についての発信メールグラフと、発信メールの概要を示します。

このページのメールトレンドグラフを使用して、選択した時間範囲に基づいて電子メールゲートウェイによって処理および配信されたすべての送信メールのフローをモニタできます。詳細については、レポートの時間範囲 （1056 ページ）を参照してください。

次のメール トレンド グラフは、送信メールのメール フローを視覚的に表したものです。

処理されたメッセージの必須カウンタに基づいて、発信メッセージのメール トレンドを表示できます。詳細については、カウンタを使用しての、トレンド グラフ上のデータのフィルタリング （1066 ページ）を参照してください。

次のリストでは、[メール フロー概要（Mail Flow Summary）] レポート ページのさまざまなセクションについて説明します。

表 *87 : [メール フロー概要（Mail Flow Summary）] ページの詳細*

セクション	説明
メール フロー概要：着信	
メッセージ数（Number of Messages）	[メッセージ数（Number of Messages）] のグラフは、処理されたメッセージの合計数（脅威メッセージとして処理されたメッセージを含む）を視覚的に表現します。
脅威メッセージ（Threat Messages）	[脅威メッセージ（Threat Messages）] グラフは、電子メール ゲートウェイによってブロックされたメッセージの合計数を視覚的に表現します。
脅威検出のサマリー（Threat Detection Summary）	[脅威検出のサマリー（Threat Detection Summary）] メール トレンド グラフは、次のカテゴリに基づく視覚的な表現です。 • [接続およびIPレピュテーションのフィルタリング（Connection and IP Reputation Filtering）]：IP レピュテーション フィルタリングと無効な受信者によって脅威として分類されるメッセージ。 • [スパム検出（Spam Detection）]：スパム対策スキャン エンジンによって脅威として分類されるメッセージ。 • [電子メール スプーフィング（Email Spoofing）]：DMARC 検証エラーのために脅威として分類されるメッセージ。 • [アウトブレイク脅威サマリー（Outbreak Threat Summary）]：アウトブレイク フィルタリング エンジンによってフィッシング、詐欺、ウイルス、またはマルウェアとして分類されるメッセージ。 • [添付ファイルとマルウェアの検出（Attachment and Malware Detection）]：アンチウイルスおよび AMP エンジンによって脅威として分類されるメッセージ。 • [すべてのカテゴリ（All Categories）]：脅威として分類されるすべてのメッセージ。

セクション	説明
コンテンツ サマリー（Content Summary）	[コンテンツ サマリー（Content Summary）] メール トレンド グラフは、次のカテゴリに基づく視覚的な表現です。 • [グレイメール（Graymail）]：マーケティング、バルク、またはソーシャル ネットワーキングとして分類されるメッセージ。 • [コンテンツ フィルタ（Content Filters）]：コンテンツ フィルタにより分類されるメッセージ。 • [すべてのカテゴリ（All Categories）]：graymail エンジンおよびコンテンツ フィルタによって分類されるすべてのメッセージ。
メール フロー概要：発信	
メッセージ数（Number of Messages）	[メッセージ数（Number of Messages）] のグラフは、処理されたメッセージの合計数（クリーンであるとして処理されたメッセージを含む）を視覚的に表現します。
メッセージ配信（Message Delivery）	[メッセージ配信（Message Delivery）] のグラフは、ハード バウンスを含む、配信されるメッセージの合計数を視覚的に表現します。
送信メール（Outgoing Mails）	[送信メール（Outgoing Mails）] トレンド グラフは、次のカテゴリに基づく視覚的な表現です。 • スパム検出（Spam Detected） • ウイルス検出（Virus Detected） • AMP で検出（Detected by AMP） • コンテンツ フィルタによる停止（Stopped by Content Filters） • DLP による停止（Stopped by DLP）

関連項目

- 電子メールゲートウェイによる電子メールメッセージの分類方法 （1063 ページ）
- 送受信のサマリーとグラフ （1017 ページ）
- [メールフロー概要（Mail Flow Summary）] ページでの電子メール メッセージの分類 （1064 ページ）
- カウンタを使用しての、トレンド グラフ上のデータのフィルタリング （1066 ページ）

電子メールゲートウェイによる電子メールメッセージの分類方法

メッセージは電子メール パイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、メッセージにスパム陽性またはウイルス陽性というマークを付けることができます。コンテンツ フィルタに一致させることもできます。各種フィルタとスキャン アクティビティの優先順位は、メッセージ処理の結果に大きく影響します。

上記の例では、各種判定は次の優先ルールに従います。

- スパム陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

これらのルールに従って、メッセージがスパム陽性とマークされた場合、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されていれば、このメッセージがドロップされてスパム カウンタが増分します。

さらに、スパム陽性のメッセージを引き続き電子メール パイプラインで処理するようにアンチスパム設定が設定されている場合、以降のコンテンツ フィルタがこのメッセージをドロップ、バウンス、または隔離しても、スパム カウンタは増分します。メッセージがスパム陽性またはウイルス陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

また、メッセージがアウトブレイク フィルタによって隔離された場合、隔離からリリースされてワーク キューで再度処理されるまで集計されません。

メッセージ処理の優先順位の詳細については、お使いの電子メールゲートウェイのオンライン ヘルプまたはユーザーガイドで、電子メール パイプラインに関する章を参照してください。

送受信のサマリーとグラフ

送受信のサマリーのセクションでは、システム上のすべてのメール アクティビティのリアルタイム アクティビティへのアクセスが提供され、送受信メールのグラフとメール サマリーで構成されています。ユーザは、[時間範囲（Time Range）] メニューを使用して報告対象となるタイムフレームを選択できます。選択したタイムフレームは、すべての電子メール セキュリティ モニタ ページで使用されます。メッセージの各タイプまたはカテゴリに関する説明は以下のとおりです（電子メールの分類 （1018 ページ）を参照）。

メール トレンド グラフでは、メール フローが視覚的に表示されますが、サマリー テーブルでは、同じ情報の数値的な内訳が示されます。サマリー テーブルには、各メッセージ タイプの割合と実数（試行されたメッセージ、脅威メッセージ、クリーン メッセージの総数を含む）が含まれています。

送信グラフおよびサマリーでも、送信メールに関する同様の情報が示されます。

関連項目

- 電子メール セキュリティ モニタでのメッセージ集計に関する注意事項 （1017 ページ）

電子メール セキュリティ モニタでのメッセージ集計に関する注意事項

電子メール セキュリティ モニタが着信メールの集計に使用する方法は、メッセージあたりの受信者の数によって異なります。たとえば、example.com から 3 人の受信者に送信された着信メッセージは、この送信者からの 3 通として集計されます。

送信者レピュテーションフィルタによってブロックされたメッセージは実際にはワークキューに入らないので、電子メールゲートウェイは着信メッセージの受信者のリストにはアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数はシスコによって算出されたもので、既存の顧客データの大規模なサンプリング研究に基づいています。

[メールフロー概要（Mail Flow Summary）] ページでの電子メール メッセージの分類

脅威とみなされる受信メッセージおよび [メールフロー概要（Mail Flow Summary）] レポートページで配信される送信メッセージは、次のとおり分類されます。

表 *88 : [メールフロー概要（Mail Flow Summary）] ページ上のメールのカテゴリ*

カテゴリ	説明
メール フロー概要：着信	
IP レピュテーション フィルタリング	HAT ポリシーによってブロックされたすべての接続数に、固定乗数を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [IP レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の値は、次の要素に基づいて算出されます。 • この送信者からの「調整された」メッセージの数。 • 拒否された、または TCP 拒否の接続数（部分的に集計されます）。 • 接続ごとのメッセージ数に対する控えめな乗数。 電子メールゲートウェイに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。このような状況で表示される値は、停止されたメッセージの最小数を示す値として解釈されます。 [メールフロー概要（Mail Flow Summary）] レポートページ上の IP レピュテーション フィルタリングの総数および割合は、すべての拒否された接続の数に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
送信者ドメイン レピュテーション フィルタリング	送信者ドメインのレピュテーション判定に基づいてブロックされたメッセージの総数。

カテゴリ	説明
無効な受信者	従来のLDAP拒否によって拒否されたすべてのメール受信者数にすべての RAT 拒否数を加えた総数および割合。
スパム対策	アンチスパム スキャン エンジンで陽性、または疑いありとして検出された受信メッセージの総数および割合。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。
ウイルス対策	ウイルスとしては陽性だがスパムではないと検出された受信メッセージの総数および割合。 次のメッセージは、[ウイルス検出（Virus Detected）] カテゴリに集計されます。 • ウイルス スキャン結果が [修復（Repaired）] または [感染している（Infectious）] であるメッセージ • 暗号化されたメッセージを、ウイルスを含むメッセージとして集計するオプションが選択されている場合に、ウイルス スキャン結果が [暗号化（Encrypted）] であるメッセージ • スキャンできないメッセージに対するアクションが[「配信」なし（NOT "Deliver"）] の場合に、ウイルス スキャン結果が [スキャン不可（Unscannable）] であるメッセージ • 代替メールホストまたは代替受信者へ送信するオプションが選択されている場合に、ウイルス スキャン結果が [スキャン不可（Unscannable）] または [暗号化（Encrypted）] であるメッセージ • アウトブレイク隔離から手動またはタイムアウトにより削除されたメッセージ
高度なマルウェア防御	合計数とファイル分析サービスによりブロックされた受信メッセージの総数および割合。 メッセージ添付ファイルは、レピュテーションフィルタリングによって悪意のある添付ファイルとして検出されました。この値には、ファイル分析により悪意があると検出された判定のアップデートまたはファイルは含まれません。
コンテンツ フィルタ	メッセージやコンテンツ フィルタにより停止された受信メッセージの総数および割合。
DMARC ポリシー	DMARC 検証ポリシーを失敗した受信メッセージの総数および割合。
S/MIME 検証/復号に失敗	S/MIME 検証、復号またはその両方に失敗したメッセージの総数および割合。

カテゴリ	説明
メール フロー概要：発信	
ハード バウンス	永久に配信不能な送信メッセージの総数および割合。
配信済み	配信される送信メッセージの総数および割合。

（注） スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーン メッセージとして集計されます。それ以外の場合は、メッセージはウイルス陽性として集計されます。

さらに、メッセージがメッセージ フィルタと一致し、フィルタによってドロップされたり、バウンスされたりしていない場合、クリーンなメッセージとして扱われます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

関連項目

[メール フローの詳細（Mail Flow Details）] ページ （1083 ページ）

カウンタを使用しての、トレンド グラフ上のデータのフィルタリング

トレンドグラフでは、必要な時間範囲および使用可能なカウンタに基づいてデータをフィルタリングすることができます。

[時間範囲（Time Range）] ドロップダウンで選択した時間範囲は、別の値を選択するまで、トレンド グラフ用に使用されます。

[メール フローの概要（Mail Flow Summary）] レポート ページのトレンド グラフ上のカウンタを使用して、異なるフィルタに固有のデータを表示できます。使用可能なカウンタをクリックすると、データがフィルタリングされます。

[システム容量（System Capacity）] ページ

[システム容量（System Capacity）] ページでは、ワーク キュー内のメッセージ数、ワーク キューで費やした平均時間、送受信メッセージ（量、サイズ、件数）、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページ スワップ情報などシステム負荷の詳細が示されます。

[システム容量（System Capacity）] ページを使用すると、次の情報を確認できます。

- 電子メールゲートウェイが推奨キャパシティを超えて、設定の最適化または追加電子メールゲートウェイが必要になった時間
- キャパシティの問題が今後発生する可能性を示すシステム挙動の過去のトレンド
- 最も多くのリソースを使用したシステムの部分（トラブルシューティングを支援するため）

お使いの電子メールゲートウェイをモニタして、メッセージの量に対してキャパシティが適切であることを確認することが重要です。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。システム キャパシティをモニタする最も効果的な方法は、全体的な量、ワーク キュー内のメッセージ、およびリソース節約モードのインシデントを追跡することです。

- **量**：「通常」のメッセージ量と環境内での「異常」な増加を把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール（Incoming Mail）]ページおよび[送信メール（Outgoing Mail）]ページを使用すると、経時的に量を追跡できます。詳細については、[システム容量（System Capacity）]：[受信メール（Incoming Mail）]（1045 ページ）および[システム容量（System Capacity）]：[送信メール（Outgoing Mail）]（1046 ページ）を参照してください。
- **ワーク キュー**：ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、有害メッセージの異常な増加を処理する、「緩衝装置」として設計されています。しかしワーク キューは、負荷のかかっているシステムを示す最良の指標であり、長く、頻繁なワーク キューのバックアップは、キャパシティの問題を示している可能性があります。[ワーク キュー（WorkQueue）]ページを使用すると、ワーク キュー内でメッセージが費やした平均時間およびワーク キュー内のアクティビティを追跡できます。詳細については、[システム容量（System Capacity）]：[ワークキュー（Workqueue）]（1045 ページ）を参照してください。
- **リソース節約モード**：電子メールゲートウェイがオーバーロードになると、「リソース節約モード」（RCM）になり、CRITICAL システムアラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いの電子メールゲートウェイは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。[システム容量（System Capacity）]：[システムの負荷（System Load）]（1046 ページ）を参照してください。

関連項目

- [システム容量（System Capacity）]：[ワークキュー（Workqueue）]（1045 ページ）
- [システム容量（System Capacity）]：[受信メール（Incoming Mail）]（1045 ページ）
- [システム容量（System Capacity）]：[送信メール（Outgoing Mail）]（1046 ページ）
- [システム容量（System Capacity）]：[システムの負荷（System Load）]（1046 ページ）
- メモリ ページ スワッピングに関する注意事項（1047 ページ）
- [システム容量（System Capacity）]：[すべて（All）]（1047 ページ）

[システム容量（System Capacity）]：[ワークキュー（Workqueue）]

[ワークキュー（Workqueue）]ページには、ワーク キュー内でメッセージが費やした平均時間（スパム隔離またはポリシー、ウイルス、およびアウトブレイク隔離で費やした時間は除く）が表示されます。1 時間から 1 月までの時間範囲を表示できます。平均は、メール配信を遅延させた短期間のイベントおよびシステム上の負荷の長期トレンドの両方を識別するのに役立ちます。

（注） 隔離からワーク キューにメッセージが解放される場合、「ワーク キュー内の平均時間」メトリックではこの時間が無視されます。これにより、重複集計と検疫で費やされた延長時間による統計の歪みを回避できます。

このレポートでは、指定期間のワーク キュー内のメッセージの量および同期間のワーク キュー内の最大メッセージ数も示されます。ワーク キューの最大メッセージのグラフ表示でも、ワーク キューのしきい値レベルが示されます。

[ワークキュー（Workqueue）] グラフにおける不定期のスパイクは、正常であり、発生する可能性があります。ワーク キュー内のメッセージが長期間、設定済みしきい値よりも大きい場合は、キャパシティの問題を示している可能性があります。このシナリオでは、しきい値レベルを調整することを検討するか、またはシステム設定を確認します。

ワーク キューのしきい値レベルを変更する手順については、システム状態パラメータのしきい値の設定 （1273 ページ）を参照してください。

ヒント [ワークキュー（Workqueue）]ページを確認するときは、作業キュー バックアップの頻度を測定し、10,000 メッセージを超える作業キュー バックアップに注意することが推奨されます。

[システム容量（System Capacity）]：[受信メール（Incoming Mail）]

[受信メール（Incoming Mail）] ページには、着信接続、着信メッセージの総数、平均メッセージサイズ、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[受信メール（Incoming Mail）] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。着信メール データと送信者プロファイル データを比較して、特定のドメインからネットワークに送信される電子メールの量のトレンドを表示することも推奨されます。

（注） 着信接続数の増加は、必ずしもシステム負荷に影響を与えるわけではありません。

[システム容量（System Capacity）]：[送信メール（Outgoing Mail）]

[送信メール（Outgoing Mail）] ページには、発信接続、発信メッセージの総数、平均メッセージサイズ、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[送信メール（Outgoing Mail）] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。発信メール データと発信宛先データを比較して、特定のドメインまたは IP アドレスから送信される電子メールの量のトレンドを表示することも推奨されます。

[システム容量（System Capacity）]：[システムの負荷（System Load）]

システムの負荷レポートに、次が表示されます。

- 全体のCPU使用率（Overall CPU Usage）
- メモリページスワップ（Memory Page Swapping）
- リソース節約アクティビティ

全体のCPU使用率（Overall CPU Usage）

電子メールゲートウェイは、アイドル状態の CPU リソースを使用してメッセージスループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステム キャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリ ページ スワッピングが発生する場合、キャパシティの問題の可能性があります。

（注） このグラフには、CPU 使用率のしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定 （1273 ページ）を参照してください。

このページでは、メール処理、スパムおよびウイルスエンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す良い指標です。電子メールゲートウェイの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

メモリページスワップ（Memory Page Swapping）

メモリ ページ スワッピングのグラフは、システムによるディスクへのページングが必要な頻度を示します。このグラフには、メモリ ページ スワッピングのしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定 （1273 ページ）を参照してください。

リソース節約アクティビティ

リソース節約アクティビティグラフは、電子メールゲートウェイがリソース節約モード（RCM）になった回数を示します。たとえば、グラフにn回と示されている場合は、電子メールゲートウェイが n 回 RCM になり、少なくとも n-1 回終了していることを意味します。

お使いの電子メールゲートウェイは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。リソース節約アクティビティグラフに電子メールゲートウェイが頻繁にRCSになっていることが示されている場合は、システムが過負荷になっていることを示している可能性があります。

メモリ ページ スワッピングに関する注意事項

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリスワッピングは起こり得るものであり、電子メールゲートウェイの問題を示すものではありません。システムが常に高ボリュームのメモリ スワッピングを行っている場合を除き、メモリ スワッピングは予想される正常な動作です（特に C170 および C190 アプライアンスの場合）。パフォーマンスを向上させるには、ネットワークに電子メールゲートウェイを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。

[システム容量（System Capacity）]：[すべて（All）]

[すべて（All）]ページでは、これまでのすべてのシステム キャパシティ レポートを単一のページに統合し、さまざまなレポート同士の関係を表示することができます。たとえば、過剰なメモリ スワッピングの発生と同時期にメッセージ キューが高いことを確認できます。これは、キャパシティの問題の兆候である可能性があります。このページを PDF として保存し、後で参照するために（またはサポート スタッフと共有するために）システム パフォーマンスのスナップショットを保存することが推奨されます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

レポート データの有効性

[レポートデータの有効性（Reporting Data Availability）] ページでは、リソース使用率や電子メールトラフィックの障害発生場所をリアルタイムに確認できるようにデータを表示できます。

このページから、Cisco Secure Email and Web Manager によって管理される電子メールゲートウェイ全体のデータアベイラビリティを含めて、すべてのデータリソース使用率および電子メールトラフィックに障害のある場所が表示されます。

このレポートページから、特定の電子メールゲートウェイおよび時間範囲のデータアベイラビリティを表示することもできます。

[高度なマルウェア防御（Advanced Malware Protection）] ページ

高度なマルウェア防御は、次によりゼロデイや電子メールの添付ファイル内のファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

この機能は着信メッセージと発信メッセージに使用できます。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザーガイドまたは Cisco Secure Email Gateway の AsyncOS オンラインヘルプを参照してください。

レポート ページを表示するには、[レポート（Reports）] ドロップダウンの [ファイルおよびマルウェアのレポート（File and Malware Reports）] セクションから [高度なマルウェア防御（Advanced Malware Protection）] を選択します。

[高度なマルウェア防御（Advanced Malware Protection）] レポート ページには、次のレポート ビューが表示されます。

- [高度なマルウェア防御（Advanced Malware Protection）]：[概要（Summary）]（1071 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] - [AMP レピュテーション（AMP Reputation）]（1072 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] – [ファイル分析（File Analysis）]（1073 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] – [ファイル レトロスペクション（File Retrospection）]（1074 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] - [メールボックスの自動修復（Mailbox Auto Remediation）]（1074 ページ）

[高度なマルウェア防御（Advanced Malware Protection）] レポートページには、Cisco Threat Grid アプライアンスに接続された電子メールゲートウェイのリアルタイムデータを提供するメトリックバーが表示されます。

（注）
- メトリック バーでデータを設定するには、CLI で `trailblazerconfig > enable` コマンドを使用する必要があります。詳細については、『*Cisco Email Security Command Reference Guide*』を参照してください。
- Cisco Threat Grid アプライアンスのデータを表示できるのは、日別、週別、および月別のみです。

関連項目

- SHA-256 ハッシュによるファイルの識別 （1076 ページ）
- その他のレポートでのファイル レピュテーション フィルタ データの表示 （1076 ページ）

[高度なマルウェア防御（Advanced Malware Protection）]：[概要（Summary）]

[高度なマルウェア防御（Advanced Malware Protection）]：[概要（Summary）]ページには、ファイル レピュテーションおよびファイル分析サービスで識別される受信および送信ファイルベースの脅威の概要の全体が表示されます。

詳細については、「[高度なマルウェア防御（Advanced Malware Protection）] - [AMP レピュテーション（AMP Reputation）]（1072 ページ）」および「[高度なマルウェア防御（Advanced Malware Protection）] – [ファイル分析（File Analysis）]（1073 ページ）」を参照してください。

[高度なマルウェア防御（Advanced Malware Protection）] - [AMP レピュテーション（AMP Reputation）]

[高度なマルウェア防御（Advanced Malware Protection）] - [AMP レピュテーション（AMP Reputation）] ページには、ファイル レピュテーション サービスによって識別された、受信および送信されたファイル ベースの脅威が表示されます。

判定が変更されたファイルについては、[AMP判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。

圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。

[AMPにより処理された受信ファイル（Incoming files handled by AMP）] セクションには、受信したマルウェア ファイルが [悪意のある（Malicious）]、[正常（Clean）]、[不明（Unknown）]、[スキャン不可能（Unscanable）]、[低リスク（Low Risk）] などのさまざまなカテゴリ別に表示されます。

悪意のある受信ファイルは、次のように分類されます。

- [マルウェア（Malware）] に分類される AMP レピュテーションサーバで受信したブロックリストに登録されているファイル SHA の割合。
- [カスタム検出（Custom Detection）] に分類される AMP for Endpoints コンソールで受信したブロックリストに登録されているファイル SHA の割合。AMP for Endpoints コンソールから取得されたブロックリストに登録されるファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで [シンプルカスタム検出（Simple Custom Detection）] として表示されます。
- [カスタムしきい値（Custom Threshold）] に分類されるしきい値設定に基づいてブロックリストに登録されているファイル SHA の割合。

レポートの [詳細（More Details）] セクションのリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリの詳細を表示できます。

[リスク低（Low Risk）] 判定の詳細をレポートの [AMPにより渡された受信ファイル（Incoming Files Handed by AMP）] セクションに表示できます。

[高度なマルウェア防御：受信（Advanced Malware Protection: Incoming）] レポート ページの [AMP レピュテーション（AMP Reputation）] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル レピュテーション サービスによって識別された受信ファイルの概要（グラフ形式）。
- 選択した時間範囲に受信されたすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位の受信マルウェア脅威ファイル。

- 上位の受信マルウェア脅威ファイル（ファイル タイプ別）。
- 上位の受信マルウェア脅威ファイルを一覧表示する [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] インタラクティブ テーブル。

  ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

  アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の青い番号のリンクをクリックします。

[高度なマルウェア防御：送信（Advanced Malware Protection: Outgoing）] レポート ページの [AMP レピュテーション（AMP Reputation）] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル レピュテーション サービスによって識別された送信ファイルの概要（グラフ形式）。
- 選択した時間範囲に送信されたすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位の送信マルウェア脅威ファイル。
- 上位の送信マルウェア脅威ファイル（ファイル タイプ別）。
- 上位の送信マルウェア脅威ファイルを一覧表示する [送信したマルウェア脅威ファイル（Outgoing Malware Threat Files）] インタラクティブ テーブル。

  ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

  アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の青い番号のリンクをクリックします。

[高度なマルウェア防御（Advanced Malware Protection）]–[ファイル分析（File Analysis）]

[高度なマルウェア防御（Advanced Malware Protection）]–[ファイル分析（File Analysis）] ページには、分析のために送信された各ファイルについて、時刻と判定（または中間判定）が表示されます。電子メールゲートウェイは 30 分ごとに分析結果をチェックします。

1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。

オンプレミスの Cisco AMP Threat Grid アプライアンスでの展開の場合：AMP Threat Grid アプライアンスで許可リストに登録されているファイルは、「クリーン」として表示されます。許可リストについては、AMP Threat Grid のドキュメントまたはオンラインヘルプを参照してください。

ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。詳細については、SHA-256 ハッシュによるファイルの識別 （1076 ページ）を参照してください。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の [詳細（Details）] リンクをクリックします。

圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルのSHA値のみが[ファイル分析（File Analysis）]レポートに含まれます。

[高度なマルウェア防御（Advanced Malware Protection）]レポートページの[ファイル分析（File Analysis）]ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル分析サービスによってファイル分析のためにアップロードされた受信ファイルおよび送信ファイルの数。
- ファイル分析要求が完了している受信ファイルおよび送信ファイルのリスト。
- ファイル分析要求の処理待ちとなっている受信ファイルおよび送信ファイルのリスト。

[高度なマルウェア防御（Advanced Malware Protection）]–[ファイル レトロスペクション（File Retrospection）]

[高度なマルウェア防御（Advanced Malware Protection）]の[ファイルレトロスペクション（File Retrospection）]ページには、この電子メールゲートウェイで処理され、メッセージ受信後に判定が変わったファイルが表示されます。このシナリオの詳細については、お使いの電子メールゲートウェイのマニュアルを参照してください。

高度なマルウェア防御は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が明らかになると、脅威の判定が変わる可能性があります。

1000を超える判定アップデートを表示するには、データを.csvファイルとしてエクスポートします。

1つのSHA-256に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。

使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定のSHA-256の影響を受けるすべてのメッセージを表示するには、SHA-256リンクをクリックします。

[高度なマルウェア防御（Advanced Malware Protection）]レポートページの[ファイル レトロスペクション（File Retrospection）]ビューを使用できます。

- レトロスペクティブな判定変更がある着信ファイルおよび発信ファイルのリスト。

[高度なマルウェア防御（Advanced Malware Protection）]-[メールボックスの自動修復（Mailbox Auto Remediation）]

[高度なマルウェア防御（Advanced Malware Protection）]-[メールボックスの自動修復（Mailbox Auto Remediation）]レポートページには、受信ファイルに対するメールボックス修復の結果の詳細が表示されます。

[高度なマルウェア防御（Advanced Malware Protection）]-[メールボックスの自動修復（Mailbox Auto Remediation）]ページを使用すると、次などのレトロスペクティブセキュリティ情報を表示することができます。

- 受信者のメールボックス修復の成功または失敗を示す一覧

- メッセージに対してとられる修復のアクション
- SHA-256 ハッシュに関連付けられているファイル名
- メールボックス修復が成功または失敗した受信者について定義されているプロファイル名の一覧
- 修復が失敗した理由
- ドメインにマッピングされたプロファイルがない

[修復が失敗した受信者（Recipients for whom remediation was unsuccessful）] フィールドは、次のシナリオで更新されます。

- 無効なメールボックス：受信者が有効な Microsoft Exchange Online ユーザまたは Microsoft Exchange オンプレミスユーザではないか、電子メールゲートウェイに設定された Microsoft Exchange Online または Microsoft Exchange オンプレミスのドメインアカウントに属していない。
- 添付ファイルを含むメッセージをメールボックスで使用できない。たとえば、エンドユーザがメッセージを削除した。
- 認証エラー：Microsoft Exchange オンプレミスのメールボックスに接続するために電子メールゲートウェイで指定されたユーザアカウントが正しくない。
- 接続エラー：電子メールゲートウェイが修復アクションを実行しようとしたときに、電子メールゲートウェイと Microsoft Exchange Online または Microsoft Exchange オンプレミス サービスとの間に接続の問題が発生した。
- 権限に関するエラー：
  - Microsoft Exchange オンプレミスアカウントの場合、Microsoft Exchange オンプレミスのメールボックスに接続するために電子メールゲートウェイで指定されたユーザアカウントに偽装ロールが割り当てられていない。
  - Microsoft Exchange Online アカウントの場合、Office 365 アプリケーションに、受信者のメールボックスにアクセスするために必要な権限がない。
- ドメインにプロファイルがマッピングされていない：受信者ドメインにマッピングされたプロファイルがない。
- メールボックスがアクセス不能または無効：
  - メールボックスへのアクセスに使用されるアカウント プロファイルのプロファイル タイプが正しくない。
  - 受信者が有効な Microsoft Exchange Online ユーザまたは Microsoft Exchange オンプレミス ユーザではない。
  - 受信者が、電子メールゲートウェイに設定された Microsoft Exchange Online または Microsoft Exchange オンプレミスのドメインアカウントに属していない。

メッセージ トラッキングに関連メッセージを表示するには、SHA-256 ハッシュをクリックします。

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイルを処理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルがその SHA-256 値（短縮形式）別に表示されます。

その他のレポートでのファイル レピュテーション フィルタ データの表示

該当する場合は、ファイル レピュテーションおよびファイル分析のデータを他のレポートでも使用できます。レポートによっては、[高度なマルウェア防御で検出（Detected by Advanced Malware Protection）] 列がデフォルトで非表示になっている場合があります。追加の列を表示するには、テーブルの右上にある [列をカスタマイズ（Customize Columns）] アイコンをクリックします。

[ウイルス フィルタリング（Virus Filtering）] ページ

[ウイルスフィルタリング（Virus Filtering）] ページでは、ネットワークに浸入したウイルスおよびネットワークから送信されたウイルスの概要が示されます。[ウイルスフィルタリング（Virus Filtering）] ページには、お使いの電子メールゲートウェイで稼働するウイルススキャンエンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して特定のアクションを実行することが推奨されます。たとえば、PDF ファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDF が添付されているメッセージを隔離するフィルタ アクションを作成することが推奨されます。

複数のウイルス スキャン エンジンを実行している場合、[ウイルスフィルタリング（Virus Filtering）] ページには、イネーブルになっているすべてのウイルス スキャン エンジンの結果が含まれます。ページに表示されるウイルスの名前は、ウイルス スキャン エンジンによって判定された名前です。複数のスキャンエンジンが 1 つのウイルスを検出した場合、同じウイルスに対して複数のエントリが存在する可能性があります。

[ウイルスフィルタリング（Virus Filtering）] ページには、ネットワークに侵入したウイルスおよびネットワークで送受信されたウイルスの概要が示されます。[検出した受信ウイルスの上位（Top Incoming Virus Detected）] セクションには、ネットワークに送信されたウイルスのチャート ビューが降順で表示されます。[検出した送信ウイルスの上位（Top Outgoing Virus Detected）] セクションには、ネットワークから送信されたウイルスのチャート ビューが降順で表示されます。

（注） ウイルスに感染したメッセージをネットワークに送信したホストを表示するには、[受信メール（Incoming Mail）] ページに移動し、同じ報告期間を指定して、ウイルス陽性別にソートします。同様に、ネットワーク内でウイルス陽性の電子メールを送信した IP アドレスを表示するには、[送信メッセージ送信者（Outgoing Senders）] ページを表示し、ウイルス陽性メッセージ別にソートします。

[ウイルス タイプの詳細（Virus Types Details）] リストには、感染した送受信メッセージ、および感染メッセージの総数など特定のウイルスに関する情報が表示されます。感染した受信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した受信メッセージの総数が表示されます。同様に、送信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した送信メッセージの総数が表示されます。ウイルスの種類の詳細は、[受信メッセージ（Incoming Messages）]、[送信メッセージ（Outgoing Messages）]、または [感染したメッセージの合計数（Total Infected Messages）] 別にソートできます。

[マクロ検出（Macro Detection）] ページ

[マクロ検出（Macro Detection）] レポート ページを使用して、次の項目を表示できます。

- ファイル タイプ別のマクロが有効になった受信添付ファイル数の上位および概要（グラフ形式および表形式）。
- ファイル タイプ別のマクロが有効になった送信添付ファイル数の上位および概要（グラフ形式および表形式）。

マクロが有効になった添付ファイルの数をクリックすると、[メッセージ トラッキング（Message Tracking）] に関連メッセージを表示できます。

電子メールゲートウェイ で [マクロ検出（Macro Detection）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから **[マクロ検出（Macro Detection）]** を選択します。

（注） レポート生成中に次の処理が発生します。

- アーカイブ ファイル内に 1 つ以上のマクロが検出されると、アーカイブ ファイル タイプが 1 増えます。アーカイブ ファイル内のマクロが有効になった添付ファイルの数はカウントされません。
- 埋め込みファイル内に 1 つ以上のマクロが検出されると、親ファイル タイプが 1 増えます。埋め込みファイル内のマクロが有効になった添付ファイルの数はカウントされません。

[DMARC検証（DMARC Verification）] ページ

[DMARC検証（DMARC Verification）] ページには、DMARC 検証が失敗した上位のドメインと、DMARC 検証に失敗したメッセージに対して AsyncOS が実行したアクションの詳細情報が表示されます。このレポートを使用して DMARC 設定を最適化し、次のような情報を取得できます。

- 最も多く DMARC 準拠ではないメッセージを送信したドメインはどれか。
- 各ドメインで、DMARC 検証に失敗したメッセージに対して AsyncOS がどのようなアクションを実行したか。

[DMARC検証（DMARC Verification）] ページの内容は次のとおりです。

- DMARC 検証の失敗数に基づく上位ドメインを示すグラフ表示。
- ドメイン別に次の情報を示す表。
  - アクションなしで承認、隔離、または拒否されたメッセージの数。数値をクリックすると、選択されているカテゴリのメッセージのリストが表示されます。
  - DMARC 検証に合格したメッセージの数。
  - DMARC 検証試行回数の合計。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。

[URL フィルタリング（URL Filtering）] ページ

- URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。
- URL フィルタリング レポートは、送受信メッセージに対して使用できます。
- URL フィルタリングエンジンによって（アンチスパム/アウトブレイク フィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して）スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではできません。
- [上位URLカテゴリ（Top URL Categories）] モジュールには、コンテンツ フィルタまたはメッセージフィルタに一致するかどうかにかかわらず、スキャンされたメッセージで検出されたすべてのカテゴリが含まれます。
- 各メッセージに関連付けることができる URL レピュテーション レベルは 1 つだけです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。
- [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] で設定したグローバル許可リストの URL は、レポートに含まれません。

  個別のフィルタで使用される許可リストの URL はレポートに含まれます。

- 悪意のある URL とは、アウトブレイク フィルタによってレピュテーションが低いと判定された URL です。ニュートラル URL とは、アウトブレイク フィルタによってクリック時の保護が必要と判定された URL です。このため、ニュートラル URL は、Cisco Web セキュリティ プロキシにリダイレクトするために書き換えられます。
- URL カテゴリ ベースのフィルタの結果はコンテンツおよびメッセージ フィルタ レポートに反映されます。
- Cisco Web セキュリティ プロキシによるクリック時の URL 評価の結果は、レポートに反映されません。

[アウトブレイク フィルタリング（Outbreak Filtering）] ページ

[アウトブレイクフィルタ（Outbreak Filters）] ページには、最近のアウトブレイクやアウトブレイク フィルタによって隔離されたメッセージに関する情報が表示されます。このページを使用して、対象を絞ったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできます。

[アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページを使用して、次の情報を入手できます。

- ウイルス感染フィルタ ルールによって隔離されたメッセージの数と使用されたルール。
- メッセージがアウトブレイク隔離にとどまる期間
- 最も頻繁に表示される悪意のある可能性がある URL

[アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページを表示するには、[レポート（Reports）] ドロップダウンから [アウトブレイクフィルタリング（Outbreak Filtering）] を選択します。

次の表では、[アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページのさまざまなセクションについて説明します。

表 *89 : [アウトブレイクフィルタリング（Outbreak Filtering）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。
タイプ別脅威	[タイプ別脅威（Threats By Type）] セクションには、電子メールゲートウェイによって受信された脅威メッセージのさまざまなタイプが示されます。

セクション	説明
脅威サマリー	[脅威サマリー（Threat Summary）] セクションには、[マルウェア（Malware）]、[フィッシング（Phish）]、[詐欺（Scam）]、および [ウイルス（Virus）] によるメッセージの内訳が示されます。 このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
脅威の詳細	[脅威の詳細（Threat Details）] インタラクティブ テーブルには、脅威のカテゴリ（ウイルス、詐欺、またはフィッシング）、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する詳細が表示されます。 このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
着信メッセージからのヒット メッセージ	[着信メッセージからのヒットメッセージ（Hit Messages from Incoming Messages）] セクションは、選択した時間帯にアウトブレイク フィルタによって処理された受信メッセージの数のグラフと概要を示しています。 ウイルス以外の脅威には、外部 Web サイトへのリンクを使用したフィッシング電子メール、詐欺、およびマルウェア配布が含まれます。
脅威レベル別のヒット メッセージ	[脅威レベル別のヒットメッセージ（Hit Messages by Threat Level）] セクションは、アウトブレイク フィルタによって検出された脅威の重大度の概要を示しています。 レベル 5 の脅威が範囲または影響において重大であるのに対し、レベル 1 は脅威のリスクが低いことを示します。脅威レベルの説明については、お使いの電子メールゲートウェイのオンラインヘルプまたはユーザーガイドを参照してください。
アウトブレイク検疫内のメッセージ	[アウトブレイク隔離内のメッセージ（Messages resided in Outbreak Quarantine）] は、メッセージがアウトブレイク隔離にとどまっていた時間の長さを示します。 この期間は、潜在的な脅威の安全性の判定に必要なデータを収集するためにかかる時間によって決まります。通常、ウイルス脅威を含むメッセージはアンチウイルス プログラムの更新を待機する必要があるため、ウイルス以外の脅威を含む場合よりも隔離に長くとどまります。各メール ポリシーで指定した最大保持期間も反映されます。

セクション	説明
書き換えられた上位 URL	[書き換えられた上位URL（Top URL's Rewritten）] セクションは、サイトのクリック時評価（受信者がメッセージ内の悪意のある可能性があるリンクをクリックした場合）用に、メッセージ受信者を Cisco Web セキュリティ プロキシにリダイレクトするために最も頻繁に書き換えられた URL を示します。 いずれかの URL が悪意のある URL と見なされると、そのメッセージ内のすべての URL が書き換えられるため、このリストには悪質でない URL が含まれる場合があります。 このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

（注） [アウトブレイクフィルタリング（Outbreak Filtering）] レポートページにテーブルが正しく表示されるためには、電子メールゲートウェイが、Ciscoアップデート サーバと通信できる必要があります。

[偽装メールの検出（Forged Email Detection）] ページ

[偽装メールの検出（Forged Email Detection）] ページには、次のレポートが含まれています。

- **偽装メールの検出数の上位。**受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。
- **偽装メールの検出：詳細。**受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。

セキュリティ管理アプライアンスで [偽装メールの検出（Forged Email Detection）] レポート ページを表示するには、[レポート（Reports）] ドロップダウンから [偽装メールの検出（Forged Email Detection）] を選択します。

[偽装メールの検出（Forged Email Detection）] レポートは、[偽装メールの検出（Forged Email Detection）] コンテンツ フィルタまたは `forged-email-detection` メッセージ フィルタを使用している場合にのみ自動入力されます。

[偽装メールの検出（Forged Email Detection）] レポート ページから、raw データを CSV ファイルにエクスポートできます。レポート ページの上部にある [エクスポート（Export）] リンクをクリックします。エクスポートする必要があるレポート モジュールを選択し、[ダウンロード（Download）] をクリックします。

[送信者ドメインのレピュテーション（SenderDomainReputation）]ページ

[送信者ドメインのレピュテーション（Sender Domain Reputation）] レポート ページでは、次を表示できます。

- SDR サービスで受信した判定に基づく着信メッセージ（グラフ形式）。
- SDR サービスで受信した脅威カテゴリに基づく着信メッセージ（グラフ形式）。

（注） SDR 判定が「Untrusted」または「Questionable」メッセージのみが、「Spam」や「Malicious」などの SDR 脅威カテゴリに分類されます。

- SDR サービスで受信した脅威カテゴリに基づく着信メッセージの概要（表形式）。

セキュリティ管理アプライアンスで [送信者ドメインのレピュテーション（Sender Domain Reputation）] レポート ページを表示するには、[レポート（Reports）] ドロップダウンから [送信者ドメインのレピュテーション（Sender Domain Reputation）] を選択します。

[外部脅威フィード（External Threat Feeds）] ページ

[外部脅威フィード（External Threat Feeds）] レポート ページでは、以下を表示できます。

- メッセージで脅威を検出するために使用される上位 ETF ソース（グラフ形式）。
- メッセージで脅威を検出するために使用される ETF ソースの概要（表形式）。
- メッセージで検出された脅威に一致する上位 IOC（グラフ形式）。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソース（グラフ形式）。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソースの概要（表形式）。

[外部脅威フィードソースの概要（Summary of External Threat Feed Sources）] セクションでは、以下を実行できます。

- 特定の ETF ソースでメッセージ数をクリックすると、[メッセージトラッキング（Message Tracking）] に関連メッセージを表示できます。
- 特定の脅威フィード ソースをクリックすると、IOC に基づいた ETF ソースの分布を表示できます。

[侵害の兆候（IOC）の一致の概要（Summary of Indicator of Compromise (IOC) Matches）] セクションでは、以下を実行できます。

- 特定の ETF ソースで IOC の数をクリックすると、[メッセージトラッキング（Message Tracking）] に関連メッセージを表示できます。
- 特定の IOC をクリックすると、ETF ソースに基づいた IOC の分布を表示できます。

[外部脅威フィード（External Threat Feeds）] レポート ページを表示するには、[レポート（Reports）] ドロップダウンから [外部脅威フィード（External Threat Feeds）] を選択します。

[メール フローの詳細（Mail Flow Details）] ページ

[メールフローの詳細（Mail Flow Details）] レポートページには、管理対象のCisco Secure Manager Email and Web Gateway に接続するすべてのリモートホストのリアルタイム情報に関するインタラクティブレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。送信メッセージ送信者の IP アドレスおよびドメインに関する情報も収集できます。

[メールフローの詳細（Mail Flow Details）] レポート ページを表示するには、[レポート（Reports）] ドロップダウンから [メールフローの詳細（Mail Flow Details）] を選択します。

[メールフローの詳細（Mail Flow Details）] レポート ページには、次のタブがあります。

- 受信メール（Incoming Mails）
- 送信者

データ内の特定の情報を検索するには、検索およびインタラクティブ電子メール レポート ページ （1055 ページ）を参照してください。

[受信メール（Incoming Mails）] タブでは、次の操作を実行できます。

- グラフ形式で、合計脅威メッセージ数での上位送信者を表示します。
- グラフ形式で、クリーン メッセージ数での上位送信者を表示します。
- グレイメール メッセージの上位の送信者をグラフ形式で表示する。
- Cisco Secure Email and Web Manager にメールを送信した送信者の IP アドレス、ドメイン、またはネットワークオーナー（組織）を表示する。
- 電子メールを電子メールゲートウェイに送信した送信者の詳細な統計情報を表示する。統計情報には、接続（承認または拒否）の数、試行されたもののセキュリティ サービス（送信者レピュテーション フィルタリング、アンチスパム、アンチウイルスなど）によってブロックされたメッセージの数、脅威メッセージの総数、グレイメール メッセージおよび正常なメッセージの総数が含まれます。
- [受信メール（Incoming Mails）] インタラクティブ テーブルで、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）についての詳細情報を表示する。詳細については、[受信メール（Incoming Mails）] テーブル （1086 ページ）を参照してください。

  アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の番号付きハイパーリンクをクリックします。

[送信メッセージ送信者（Outgoing Senders）] タブでは、次の操作を実行できます。

- グラフ形式で、合計脅威メッセージ数での上位送信者を表示します。
- グラフ形式で、クリーン メッセージ数での上位送信者を表示します。
- 組織内で送信された脅威メッセージ（スパム、アンチウイルスなど）の上位送信者（IP アドレス別またはドメイン別）を表示する。
- 電子メールを電子メールゲートウェイから送信した送信者の詳細な統計情報を表示する。統計情報には、セキュリティ サービス（送信者レピュテーション フィルタリング、アンチスパム、アンチウイルスなど）によってブロックされた脅威メッセージおよび正常なメッセージの総数が含まれます。
- [送信者の詳細（Sender Details）] インタラクティブ テーブルで、特定の IP アドレスまたはドメインの詳細情報を表示する。詳細については、[送信者の詳細（Sender Details）] テーブル （1092 ページ）を参照してください。

  アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の番号付きハイパーリンクをクリックします。

関連項目

- [受信メール（Incoming Mails）] テーブル （1086 ページ）
- [ドメイン情報がありません（No Domain Information）] （1085 ページ）
- レポートの時間範囲 （1056 ページ）
- メール フローの詳細ページ内のビュー （1084 ページ）

メール フローの詳細ページ内のビュー

[メールフローの詳細（Mail Flow Details）] : [受信（Incoming）] レポート ページには次の 3 種類のビューがあります。

- IP アドレス
- ドメイン（Domains）
- ネットワーク オーナー

これらのビューでは、システムに接続されたリモート ホストのスナップショットが、選択したビューのコンテキストで提供されます。

さらに、[メールフローの詳細（Mail Flow Details）] ページの [受信メール（Incoming Mail）] テーブルでは、送信者の IP アドレス、ドメイン名、またはネットワーク オーナー情報をクリックすると、特定の送信者プロファイル情報を取得できます。[送信者プロファイル（Sender Profile）] の情報の詳細については、[送信者プロファイル（Sender Profile）] ページ （1090 ページ）を参照してください。

（注） ネットワーク オーナーは、ドメインを含むエンティティです。ドメインは、IP アドレスを含むエンティティです。

選択したビューに応じて、[受信メールの詳細（Incoming Mail Details）] インタラクティブテーブルに、電子メールゲートウェイで設定されたすべてのパブリックリスナーに電子メールを送信した上位 IP アドレス、ドメイン、またはネットワークオーナーが表示されます。電子メールゲートウェイに入ったすべてのメールのフローをモニタできます。

IP アドレス、ドメイン、またはネットワーク オーナーをクリックすると、[送信者プロファイル（Sender Profile）] ページの送信者の詳細にアクセスできます。[送信者プロファイル（Sender Profile）] ページは、特定の IP アドレス、ドメインまたはネットワーク オーナーに固有の [メールフローの詳細（Mail Flow Details）] ページです。

[受信メール（Incoming Mails）] インタラクティブ テーブルに含まれるデータの説明については、[受信メール（Incoming Mails）] テーブル （1086 ページ）を参照してください。

[メールフローの詳細（Mail Flow Details）] ページから、raw データを CSV ファイルにエクスポートできます。

（注） [メールフローの詳細（Mail Flow Details）] レポート ページのスケジュール設定されたレポートを生成できます。スケジュール設定されたレポート （1108 ページ）を参照してください。

[メールフローの詳細（Mail Flow Details）] : [送信（Outgoing）] レポート ページには次の 2 種類のビューがあります。

- IP アドレス
- ドメイン（Domains）

これらのビューでは、システムに接続されたリモートホストのスナップショットが、選択したビューのコンテキストで提供されます。

選択したビューに応じて、[送信者の詳細（Sender Details）] インタラクティブ テーブルに、E メール セキュリティ アプライアンスで設定されたパブリック リスナーから電子メールを送信した上位 IP アドレス、ドメイン、または送信者が表示されます。電子メールゲートウェイから出たすべてのメールのフローをモニタできます。

[送信者の詳細（Sender Details）] インタラクティブ テーブルに含まれるデータの説明については、[送信者の詳細（Sender Details）] テーブル （1092 ページ）を参照してください。

[ドメイン情報がありません（No Domain Information）]

電子メールゲートウェイに接続したものの、ダブル DNS ルックアップで検証できなかったドメインは、専用ドメイン [ドメイン情報がありません（No Domain Information）] に自動的に分

類されます。これらの種類の検証されないホストは、送信者の検証によって管理できます。電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

リストに表示される送信者の数は、[表示された項目（Items Displayed）] メニューから選択できます。

レポートの時間範囲

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

時間範囲は、次の表に記載のオプションから選択します。

表 *90*：電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時間（Hour）	直近の 60 分 + 最大 5 分
日（Day）	直近の 24 時間と直近の 60 分
週（Week）	直近の 7 日 + 当日の経過した時間
30 日（30 days）	直近の 30 日 + 当日の経過した時間
90 日（90 days）	直近の 90 日 + 当日の経過した時間
昨日（Yesterday）	00:00 ～ 23:59（午前 0 時～午後 11:59）
先月（Previous Calendar Month）	その月の最初の日の 00:00 ～その月の最後の日の 23:59
カスタム範囲（Custom Range）	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

[受信メール（Incoming Mails）] テーブル

[メールフローの詳細：受信メール（Mail Flow Details: Incoming Mails）] ページの下部にあるインタラクティブな [受信メール（Incoming Mails）] テーブルには、電子メールゲートウェイ上のパブリックリスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメイン、IP アドレス、またはネットワーク オーナーが表示されます。

ダブル DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスを取得してその有効性を検証します。ダブル DNS ルックアップおよび送信者検証の詳細については、電子メールゲートウェイのユーザーガイドまたはオンラインヘルプを参照してください

[受信メール（Incoming Mails）] テーブルの最初の列、または [脅威メッセージの送信者上位（Top Senders by Total Threat Messages）] に表示される送信者、つまりネットワーク オーナー、IP アドレスまたはドメインについては、[送信者（Sender）] または [ドメイン情報がありませ

ん（No Domain Information）] リンクをクリックすると、送信者の詳細情報が表示されます。結果は、[送信者プロファイル（Sender Profile）] ページに表示され、IP レピュテーションサービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、[送信者プロファイル（Sender Profile）] ページ （1090 ページ）を参照してください。

[メールフローの詳細（Mail Flow Details）]ページの下部にある [送信者グループレポート（Sender Groups Report）] をクリックして、[送信者グループ（Sender Groups）] レポートを表示することもできます。[送信者グループ（Sender Groups）] レポート ページの詳細については、送信者グループ レポート （1093 ページ）を参照してください。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表に、[受信メール（Incoming Mails）] テーブル内の列の詳細を示します。

表 *91 : [*受信メール（*Incoming Mail***）*]* テーブル内の列の詳細**

列名	説明
送信者ドメイン（ドメイン）（Sender Domain (Domains)）	送信者のドメイン名。
送信者 IP アドレス（IP アドレス）（Sender IP Address (IP Addresses)）	送信者の IP アドレス。
ホスト名（IP アドレス）（Hostname (IP Addresses)）	送信者のホスト名。
DNS検証（IPアドレス）（DNS Verified (IP Addresses)）	DNS によって検証された IP アドレス。
IP レピュテーションスコア（IP アドレス）	送信者の IP レピュテーションスコア
最後の送信者グループ（IP アドレス）（Last Sender Group (IP Addresses)）	最後の送信者グループの詳細。
最後の送信者グループ（IP アドレス）（Last Sender Group (IP Addresses)）	最後の送信者グループの詳細。

列名	説明
ネットワークオーナー（Network Owner (Network Owners)）	送信者のネットワーク オーナー。
接続拒否（ドメインおよびネットワークオーナー）（Connections Rejected (Domains and Network Owners)）	HAT ポリシーによってブロックされたすべての接続。電子メールゲートウェイに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。
接続承認（ドメインおよびネットワークオーナー）（Connections Accepted (Domains and Network Owners)）	受け入れられたすべての接続。
[試行回数の合計（Total Attempted）]	すべての受け入れられた接続試行と、拒否された接続試行。
受信者スロットルによる停止（ドメインおよびネットワークオーナー）（Stopped by Recipient Throttling (Domains and Network Owners)）	これは、レピュテーション フィルタリングによる阻止の 1 要素です。HAT 上限値（1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数）のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] が算出されます。

列名	説明
[IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）]	[IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • この送信者からの「数が絞り込まれた」メッセージの数 • 拒否された、または TCP 拒否の接続数（部分的に集計されます） • 接続ごとのメッセージ数に対する控えめな乗数。 電子メールゲートウェイに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。 （注） [メールフロー概要（Mail Flow Summary）] ページの [IPレピュテーションフィルタリング（IP Reputation Filtering）] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
[ドメインレピュテーションフィルタによる停止（Stopped by Domain Reputation Filtering）]	送信者ドメインのレピュテーション判定に基づいてブロックされたメッセージの総数。
[無効な受信者の場合に停止（Stopped as Invalid Recipients）]	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
[スパム検出（Spam Detected）]	検出されたすべてのスパム。
[ウイルス検出（Virus Detected）]	検出されたすべてのウイルス。
高度なマルウェア防御で検出（Detected by Advanced Malware Protection）	高度なマルウェア防御エンジンによって検出されたメッセージの総数。
コンテンツフィルタによる阻止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。

列名	説明
DMARCによる停止（Stopped by DMARC）	Domain-based Message Authentication, Reporting and Conformance（DMARC）に失敗したメッセージの総数。 （注） 電子メールゲートウェイは、「失敗 - 拒否」、「失敗 - 隔離」、および「失敗 - アクションなし」の結果に基づいて、「DMARC による停止」メッセージの総数を表示します。
合計脅威件数（Total Threat）	脅威メッセージ（評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの）の総数
マーケティング（Marketing）	不要なマーケティング メッセージとして検出されたメッセージの数。
ソーシャル（Social）	ソーシャル メッセージとして検出されたメッセージの数。
バルク（Bulk）	バルクとして検出されたメッセージの数。
合計グレイメール数（Total Graymails）	グレイメールとして検出されたメッセージの数。
クリーン（Clean）	すべてのクリーン メッセージ。 グレイメール機能が有効になっていない電子メールゲートウェイで処理されるメッセージは、クリーンとして集計されます。

[送信者プロファイル（Sender Profile）] ページ

[受信メール（Incoming Mail Details] インタラクティブ テーブル（ [メールフローの詳細（**Mail Flow Details**）]（新しい Web インターフェイス）または [受信メール（**Incoming Mail**）] ページ）の送信者をクリックすると、[送信者プロファイル（Sender Profile）] ページが表示されます。ここには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）の詳細情報が表示されます。[受信メール（Incoming Mail）] ページまたは他の [送信者プロファイル（Sender Profile）] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロファイル（Sender Profile）] ページにアクセスできます。

ネットワーク オーナーは、ドメインを含むエンティティです。ドメインは、IP アドレスを含むエンティティです。

IP アドレス、ドメインおよびネットワーク オーナーに関して表示される送信者プロファイル ページは、多少異なります。それぞれのページには、特定の送信者からの着信メールに関するグラフおよびサマリーテーブルが含まれます。グラフの下の表に、送信者に関連付けられたドメインまたはIPアドレスが表示されます。（個々のIPアドレスの [送信者プロファイル（Sender Profile）] ページには、詳細なリストが含まれません。）[送信者プロファイル（Sender Profile）] ページには、送信者の現在の SenderBase、送信者グループ、およびネットワーク情報を含む情報セクションも表示されます。

- ネットワーク オーナー プロファイル ページには、ネットワーク オーナー、およびこのネットワーク オーナーに関連するドメインや IP アドレスに関する情報が含まれます。
- ドメイン プロファイル ページには、このドメインおよびこのドメインに関連する IP アドレスに関する情報が含まれます。
- IP アドレス プロファイル ページには、IP アドレスのみに関する情報が含まれます。

各 [送信者プロファイル（Sender Profile）] ページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

- IP レピュテーションサービスからのグローバル情報。たとえば、次の情報です。
  - IP アドレス、ドメイン名、またはネットワーク オーナー
  - ネットワーク オーナーのカテゴリ（ネットワーク オーナーのみ）
  - CIDR 範囲（IP アドレスのみ）
  - IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
  - この送信者から最初のメッセージを受信してからの日数
  - 最後の送信者グループと DNS が検証されたかどうか（IP アドレス送信者プロファイル ページのみ）

  日単位マグニチュードは、直近24時間にドメインが送信したメッセージの数の基準です。地震の測定に使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10 を基数とする対数目盛を使用して算出されるメッセージの量の基準です。目盛の最大理論値は 10 に設定されます。これは、世界の電子メール メッセージの量に相当します。対数目盛を使用した場合、1 ポイントのマグニチュードの増加は、実際の量の 10 倍の増加に相当します。

  月単位マグニチュードは、直近 30 日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。

  - 平均マグニチュード（IP アドレスのみ）
  - 総累積量/30 日の量（IP アドレス プロファイル ページのみ）
  - Bonded Sender ステータス（IP アドレス プロファイル ページのみ）
  - IP レピュテーションスコア（IP アドレスプロファイルページのみ）
  - 最初のメッセージからの日数（ネットワーク オーナーとドメイン プロファイル ページのみ）
  - このネットワーク オーナーに関連するドメインの数（ネットワーク オーナープロファイル ページおよびドメイン プロファイル ページのみ）
  - このネットワーク オーナーの IP アドレスの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）

- 電子メールの送信に使用された IP アドレスの数（ネットワーク オーナー ページのみ）

IP レピュテーションサービスによって提供されるすべての情報が記載されたページを表示するには、[SenderBaseからの詳細情報（More from SenderBase）] をクリックします。

- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する詳細は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

ドメイン プロファイルのページから、特定の IP アドレスをクリックして特定の情報を表示することも、組織プロファイルのページを表示することもできます。

[送信者の詳細（Sender Details）] テーブル

[メールフローの詳細（Mail Flow Details）] : [送信（Outgoing）] ページの下部にあるインタラクティブな [送信者の詳細（Sender Details）] テーブルには、電子メールゲートウェイ上のパブリックリスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメインまたは IP アドレスが表示されます。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表に、[送信者の詳細（Sender Details）] テーブル内の列の詳細を示します。

表 *92 : [*送信者の詳細（*Sender Details***）*]* テーブル内の列の詳細**

列名	説明
送信者ドメイン（ドメイン）（Sender Domain (Domains)）	送信者のドメイン名。
送信者 IP アドレス（IP アドレス）（Sender IP Address (IP Addresses)）	送信者の IP アドレス。
ホスト名（IP アドレス）（Hostname (IP Addresses)）	送信者のホスト名。
[スパム検出（Spam Detected）]	検出されたすべてのスパム。
[ウイルス検出（Virus Detected）]	検出されたすべてのウイルス。
高度なマルウェア防御で検出（Detected by Advanced Malware Protection）	高度なマルウェア防御エンジンによって検出されたメッセージの総数。
コンテンツフィルタによる阻止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。

列名	説明
DLP による停止（Stopped by DLP）	DLP エンジンによって阻止されたメッセージの総数。
合計脅威件数（Total Threat）	脅威メッセージ（スパム、ウイルス）の総数
クリーン（Clean）	すべてのクリーン メッセージ。 グレイメール機能が有効になっていない電子メールゲートウェイで処理されるメッセージは、クリーンとして集計されます。
合計メッセージ数（Total Messages）	すべてのメッセージの合計数。

送信者グループ レポート

送信者グループ レポートは、送信者グループ別およびメール フロー ポリシー アクション別の接続のサマリーを提供し、SMTP 接続およびメール フロー ポリシーのトレンドを確認できるようにします。[送信者グループによるメール フロー（Mail Flow by Sender Group）] リストには、各送信者グループの割合および接続数が示されます。[メールフローポリシーアクションによる接続（Connections by Mail Flow Policy Action）] グラフは、各メール フローポリシー アクションの接続の割合を示します。このページには、ホスト アクセス テーブル（HAT）ポリシーの有効性の概要が示されます。HAT の詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

送信先

[送信先（Outgoing Destinations）] ページには、メールの送信先ドメインに関する情報が示されます。このページは、2 つのセクションで構成されます。ページの上部は、発信脅威メッセージ別の上位宛先および発信クリーン メッセージの上位宛先を示すグラフで構成されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）全カラムを示す表が表示されます。

レポート対象の時間範囲（日、週、またはカスタムの範囲など）を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。

[送信先（Outgoing Destinations）] ページを使用すると、次の情報を入手できます。

- 電子メールゲートウェイのメール送信先
- 各ドメインに送信されるメールの量
- クリーン、スパム陽性、ウイルス陽性、マルウェア、またはコンテンツ フィルタによる阻止のメールの割合。
- 配信されたメッセージおよび宛先サーバによってハードバウンスされたメッセージの数

[TLS暗号化（TLS Encryption）] ページ

[TLS暗号化（TLS Encryption）] ページには、メールの送受信に使用される TLS 暗号化の全体的な使用状況が表示されます。このレポートでは、TLS接続を使用してメールを送信する各ドメインの詳細についても示されます。

[TLS暗号化（TLS Encryption）] ページを使用すると、次の情報を確認できます。

- 送受信接続による、全体的な TLS の使用割合
- TLS 接続に成功したパートナー
- TLS 接続に成功しなかったパートナー
- DANE がサポートされている TLS 接続に成功したパートナー
- DANE がサポートされている TLS 接続に失敗したパートナー
- TLS 認証に問題のあるパートナー
- パートナーが TLS を使用したメールの全体的な割合
- DANE がサポートされている送信 TLS 接続に成功した割合
- DANE がサポートされている送信接続に失敗した割合

[TLS暗号化（TLS Encryption）] ページは、着信接続に関するセクションと、発信接続に関するセクションに分かれています。各セクションには、詳細情報が含まれたグラフ、サマリー、および表が含まれています。

グラフには、指定した時間範囲にわたる、送受信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。グラフには、メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した TLS 暗号化メッセージの量、成功/失敗した DANE 接続の量が表示されます。グラフでは、TLS が必須であった接続と、TLS が単に優先された接続が区別されます。

表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。ドメインごとに、成功/失敗した必須の TLS 接続と優先された TLS 接続の数、試行された TLS 接続の総数（成功したか失敗したかにかかわらず）、暗号化されていない接続の総数、DANE 接続の総数（成功したか失敗したかに応じて）を表示できます。また、TLS が試行されたすべての接続の割合、および正常に送信された暗号化メッセージの総数（TLS が優先か必須かにかかわらず）も表示できます。テーブルの右上にある [列をカスタマイズ（Customize Columns）] アイコンを使用して、列を表示または非表示にできます。

[受信 SMTP 認証（Inbound SMTP Authentication）] ページ

[受信SMTP認証（Inbound SMTP Authentication）] ページには、クライアント証明書の使用情報、および電子メールゲートウェイとユーザのメールクライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。電子メールゲートウェイは、証明書または SMTP AUTH コマンドを受け入れると、メールクライアントへの TLS 接続を確立します。クライアントはこの接続を使用してメッセージを送信します。電子メールゲートウェイは、こ

れらの試行をユーザ単位で追跡できないため、レポートには、ドメイン名とドメイン IP アドレスに基づいて SMTP 認証の詳細が表示されます。

次の情報を確認するには、このレポートを使用します。

- SMTP 認証を使用している着信接続の総数
- クライアント証明書を使用している接続の数
- SMTP AUTH を使用している接続の数
- SMTP 認証を使用しようとして、接続が失敗したドメイン
- SMTP 認証が失敗した一方で、フォールバックを正常に使用している接続の数

[受信SMTP認証（Inbound SMTP Authentication）] ページには、受信した接続のグラフ、SMTP 認証接続を試行したメール受信者のグラフ、および接続の認証試行の詳細を含むテーブルが表示されます。

[受信した接続（Received Connections）] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメールクライアントの着信接続が示されます。このグラフには、電子メールゲートウェイが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。

[受信した受信者（Received Recipients）] グラフには、SMTP 認証を使用して、メッセージを送信するために電子メールゲートウェイへの接続を認証しようとしたメールクライアントを所有する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。

[SMTP認証の詳細（SMTP Authentication details）] テーブルには、メッセージを送信するために電子メールゲートウェイへの接続を認証しようとしたユーザを含むドメインの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行（成功または失敗）の数、SMTP AUTH コマンドを使用した接続試行（成功または失敗）の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。ページ上部のタブを使用して、ドメイン名またはドメイン IP アドレス別にこの情報を表示できます。

[レート制限（Rate Limits）] ページ

エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メール メッセージ受信者数を制限できます。[レート制限（Rate Limits）] レポートには、この制限を最も上回った送信者が表示されます。

このレポートは、以下を特定する場合に役立ちます。

- 大量のスパムを送信するために使用される可能性のある信用できないユーザ アカウント
- 通知、アラート、自動報告などに電子メールを使用する組織内の制御不能アプリケーション
- 内部請求やリソース管理のために、組織内で電子メールを過剰に送信している送信元
- スパムとは見なされないが、大量の着信電子メール トラフィックを送信している送信元

内部送信者に関する統計情報を含む他のレポート（[内部ユーザ（Internal Users）]、[送信メッセージ送信者（Outgoing Senders）] など）では、送信されたメッセージの数のみ計測されます。これらのレポートでは、少数のメッセージを多数の受信者に送信した送信者は識別されません。

[上位攻撃者(インシデント別)（Top Offenders by Incident）] チャートには、設定済み制限よりも多くの受信者にメッセージを最も頻繁に送信しようとしたエンベロープ送信者が表示されます。各試行が 1 インシデントに相当します。このチャートでは、すべてのリスナーからのインシデント数が集計されます。

[上位攻撃者(拒否した受信者数)（Top Offenders by Rejected Recipients）] チャートには、設定済みの制限を上回る、最も多くの受信者にメッセージを送信したエンベロープ送信者が表示されます。このチャートでは、すべてのリスナーからの受信者数が集計されます。

エンベロープ送信者によるレート制限の設定、または既存のレート制限の変更については、メール フロー ポリシーを使用した着信メッセージのルールの定義（124 ページ）を参照してください。

[国別の接続（Connections by Country）] ページ

[国別の接続（Connections by Country）] レポート ページを使用すると、次の情報を表示できます。

- 発信国別の受信メール接続数の上位（グラフィカルな形式）。
- 発信国別の受信メール接続の合計数（表形式）。

特定の位置情報の受信メールの接続の数をクリックすると、メッセージ トラッキングに関連メッセージを表示できます。

[合計メッセージ数（Total Messages）] 列には、SMTP 接続レベルで受け入れられるメッセージのみ表示されます。

（注） レポート生成中に次の処理が発生します。

- プライベート IP アドレスとして 1 つ以上の受信メール接続が検出されると、受信メール接続がレポートの「プライベート IP アドレス」として分類されます。
- 有効ではない IP レピュテーションスコアとして 1 つ以上の受信メール接続が検出されると、その受信メール接続はレポートで「国情報なし」に分類されます。

[ユーザー メール サマリー（User Mail Summary）] ページ

[ユーザメール概要（User Mail Summary）] ページでは、内部ユーザによって送受信されたメールに関する情報が、電子メールアドレスごとに表示されます（単一ユーザの複数の電子メール

アドレスが、リストに表示される場合があります。レポートでは、電子メールアドレスはまとめられません）。

このページは、2 つのセクションで構成されます。

- 正常な着信メッセージ別および正常な発信メッセージ別の上位ユーザと、グレイメールを受信する上位ユーザを示すグラフ。
- ユーザー メール フローの詳細

レポート対象の時間範囲（時間、日、週、または月）を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。また、テーブルの右上にある [列をカスタマイズ（Customize Column）] アイコンをクリックすると、非表示のテーブル列を表示したり、デフォルトの列を非表示にしたりできます。

[ユーザー メール フローの詳細（User Mail Flow Details）] リストでは、送受信メールが電子メール アドレス別に正常、スパム、（着信のみ）、ウイルス、マルウェア、コンテンツ フィルタの一致、グレイメール（着信のみ）に分類されます。このリストは、カラム見出しをクリックしてソートできます。

内部ユーザ レポートを使用すると、次の情報を入手できます。

- 最も多くの外部メールを送信したユーザ
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのグレイメール メッセージを受信したユーザ
- 最も多くのスパムを受信したユーザ
- コンテンツ フィルタをトリガーしたユーザとそのコンテンツ フィルタの種類
- 電子メールをコンテンツ フィルタで捕捉されたユーザ

着信内部ユーザとは、Rcpt To: アドレスに基づいてシステムで電子メールを受信する対象ユーザのことです。発信内部ユーザは Mail From: アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

一部の送信メール（バウンスなど）の送信者は、null です。これらの送信者は、送信および「不明」に集計されます。

内部ユーザの [内部ユーザの詳細（Internal User Details）] ページを表示するには、この内部ユーザをクリックします。

表の右上にある [列をカスタマイズ（Customize Columns）] アイコンをクリックすると、[Intelligent Multi-Scanで検出された着信スパム（Incoming Spam Detected by Intelligent Multi-Scan）] 列や [Intelligent Multi-Scanで検出された発信スパム（Outgoing Spam Detected by Intelligent Multi-Scan）] 列など、デフォルトでは非表示の列が表示されます。

関連項目

- [ユーザメールフローの詳細（User Mail Flow Details）] （1098 ページ）

- 特定の内部ユーザの検索 （1032 ページ）

[ユーザメールフローの詳細（User Mail Flow Details）]

[ユーザメールフローの詳細（User Mail Flow Details）] セクションでは、各カテゴリ（[スパム検出（Spam Detected）]、[ウイルス検出（Virus Detected）]、[高度なマルウェア防御で検出（Detected by Advanced Malware Protection）]、[コンテンツフィルタによる受信停止（Stopped By Content Filter）]、[グレイメール検出（Graymail Detected）]、および [正常（Clean）]）のメッセージ数を示す送受信メッセージの内訳など指定したユーザに関する詳細情報が示されます。着信メッセージの場合は、必要に応じて、テーブルの右上にある [列をカスタマイズ（Customize Columns）] アイコンをクリックすると、[Intelligent Multi-Scanで検出された着信スパム（Incoming Spam Detected by Intelligent Multi-Scan）] 列を表示できます。この値は、ファイル レピュテーション フィルタリングにより悪意のあるファイルと判断された添付ファイルを含むメッセージの数を表します。この値には、判定のアップデートまたはファイル分析により悪意があるファイルとして検出されたファイルは含まれません。送受信コンテンツ フィルタおよび DLP ポリシーの一致も示されます。

コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（[コンテンツフィルタ（Content Filters）]ページ（1033 ページ）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したユーザのリストも取得できます。

特定の内部ユーザの検索

特定の内部ユーザ（電子メール アドレス）は、[ユーザメール概要（User Mail Summary）] ページの下部にある検索フォームから検索できます。検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example.com」が一致します）を選択します。

[DLP インシデント サマリー（DLP Incident Summary）] ページ

[DLPインシデントサマリー（DLP Incident Summary）] ページには、送信メールで発生した Data Loss Prevention（DLP）ポリシー違反インシデントに関する情報が示されます。電子メールゲートウェイでは、[送信メールポリシー（Outgoing Mail Policies）] テーブルでイネーブルにした DLP 電子メールポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

DLP インシデント レポートを使用すると、次のような情報を取得できます。

- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLPインシデントサマリー（DLP Incident Summary）] ページは、次の 2 つの主なセクションで構成されます。

- 重大度（[低（Low）]、[中（Medium）]、[高（High）]、[クリティカル（Critical）]）別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンドグラフ
- [DLP インシデントの詳細（DLP Incidents Details）] リスト

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

ポリシーによって検出された DLP インシデントに関する詳細情報を表示するには、DLP ポリシーの名前をクリックします。この方法を使用すると、ポリシーによって検出された、機密データを含むメールを送信したユーザのリストを取得できます。

関連項目

- [DLPインシデントの詳細（DLP Incident Details）] （1099 ページ）
- [DLP ポリシー詳細（DLP Policy Detail）] ページ （1099 ページ）

[DLPインシデントの詳細（DLP Incident Details）]

電子メールゲートウェイの送信メールポリシーで現在イネーブルの DLP ポリシーは、[DLPインシデントの詳細（DLP Incident Details）] テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。

[DLPインシデントの詳細（DLP Incident Details）] テーブルは、ポリシーごとの DLP インシデントの合計数と、重大度レベル別の内訳を示します。重大度レベルには、バウンスされたメッセージの数と、クリアで配信、暗号化で配信、または削除されたメッセージの数も含まれます。データをソートするには、列見出しをクリックします。

[DLP ポリシー詳細（DLP Policy Detail）] ページ

[DLPインシデントの詳細（DLP Incident Details）] テーブルで DLP ポリシーの名前をクリックした場合、その結果として表示される [DLPポリシー詳細（DLP Policy Detail）] ページにそのポリシーに関する DLP インシデント データが表示されます。このページには、重大度に基づいた DLP インシデントのグラフが表示されます。

このページには、DLP ポリシーに違反したメッセージを送信した各内部ユーザを表示する、ページ下部にある [送信者別インシデント（Incidents by Sender）] リストも含まれます。このリストには、このポリシーに関するユーザごとの DLP インシデントの総数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。[送信者別インシデント（Incidents by Sender）] リストを使用すると、組織の機密データをネットワーク外のユーザに送信した可能性のあるユーザを検索できます。

送信者名をクリックすると、[内部ユーザ（Internal Users）] ページが開きます。詳細については、#unique_1506を参照してください。

[Web インタラクション（Web Interaction）] ページ

- Web インタラクション トラッキング レポート モジュールには、Web インタラクションのトラッキング機能がイネーブルの場合にのみデータが取り込まれます。
- Web インタラクション トラッキング レポート モジュールは、リアルタイムでは更新されず、30 分おきに更新されます。また、書き換えられた URL をクリックした後で、Web インタラクション トラッキング レポートにこのイベントがレポートされるまでには最大 2 時間かかることがあります。
- Web インタラクション トラッキング レポートは、リアルタイムで更新されません。クラウドにリダイレクトされる書き換えられた URL をクリックした後、Web インタラクション トラッキング レポートにこのイベントがレポートされるまでには最大 2 時間かかることがあります。
- Web インタラクション トラッキング レポートは、送受信メッセージに対して使用できます。
- エンドユーザがクリックした、クラウドにリダイレクトされる書き換えられたURL（ポリシーまたはアウトブレイク フィルタによって）のみが、これらのモジュールに含まれます。
- [Webインタラクショントラッキング（Web Interaction Tracking）] ページには、次のレポートが含まれます。

エンドユーザがクリックした、悪意のある上位URL（Top Malicious URLs clicked by End Users）。次の情報を含む詳細レポートを表示するには、URL をクリックします。

- 書き換えられた悪意のある URL をクリックしたエンドユーザのリスト。
- URL がクリックされた日付と時刻。
- URL がポリシーまたはアウトブレイク フィルタによって書き換えられたかどうか。
- 書き換えられた URL がクリックされたときに実行されたアクション（許可、ブロック、または不明）。URL がアウトブレイク フィルタによって書き換えられており、最終的な判定が使用できない場合、ステータスは不明として表示されます。

悪意のあるURLをクリックした上位エンドユーザ（Top End Users who clicked on Malicious URLs）

このセクションには、受信メッセージおよび送信メッセージについて、書き換えられた悪意のある URL を最も多くクリックしたユーザの概要が表示されます。

Webインタラクショントラッキングの詳細（Web Interaction Tracking Details）。次の情報が含まれています。

- クラウドにリダイレクトされる書き換えられたすべての URL のリスト（悪意のあるものとないもの）。詳細レポートを表示するには、URL をクリックします。
- クラウドにリダイレクトされる書き換えられた URL がクリックされた場合に実行されたアクション（許可、ブロック、または不明）。

データを表示するには、次の操作を実行します。

- [受信メールポリシー（Incoming Mail Policies）] > [アウトブレイクフィルタ（Outbreak Filters）] を選択してアウトブレイク フィルタを設定し、メッセージの変更および URL の書き換えを有効にします。
- 「**Cisco Security Proxy にリダイレクト**」アクションを使用して、コンテンツ フィルタを構成します。

エンドユーザが URL をクリックしたときにその URL の判定（正常または悪意のある）が不明である場合、ステータスは不明として表示されます。これは、ユーザのクリック時に、URL がさらに調査されていたか、Web サーバがダウンしていたか、到達不可能であったためである可能性があります。

- 書き換えられた URL をエンドユーザがクリックした回数。クリックされた URL を含むすべてのメッセージのリストを表示するには、番号をクリックします。
- Web インタラクション トラッキング レポートを使用している場合は、次の制限事項に注意してください。
  - 悪意のある URL を書き換えた後に、メッセージを送信して別のユーザ（管理者など）に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックした場合でも、元の受信者の Web インタラクション トラッキング データが増分します。
  - 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用してユーザ（管理者など）に送信する場合、そのユーザ（メッセージのコピーが送信されたユーザ）がその書き換えられた URL をクリックした場合でも、元の受信者の Web インタラクション トラッキング データが増分します。
  - どの時点であっても、電子メールゲートウェイの時刻を変更する予定がある場合は、システム時刻を協定世界時（UTC）と同期するようにしてください。

[修復レポート（Remediation Report）] ページ

[修復レポート（Remediation Report）] を使用して、[メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] の修復結果をモニタできます。

このレポートを使用して、以下のことを行います。

- [メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] で試行されたメッセージの一覧を表示する。

• 修復失敗の理由を把握する。たとえば、接続エラー、認証エラーなどです。

次のリストでは、[レート期限（Rate Limit）] レポートのさまざまなセクションについて説明します。

セクション	説明
要約	[概要（Summary）] セクションには、次の情報が表示されます。 • [メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] を使用して修復が試行されたメッセージの合計数。 • 設定された修正アクションに対して正常に修復されたメッセージの数。 • 修復が失敗したメッセージの数。
[メールボックスの自動修復（Mailbox Auto Remediation）]	[メールボックス自動修復（Mailbox Auto Remediation）] レポートセクションには、次の情報が表示されます。 • メールボックス自動修復が成功または失敗した受信者の一覧。 • メッセージに対して行われた自動修復アクション。 • SHA-256 ハッシュに関連付けられているファイル名。SHA-256 ハッシュをクリックして、[メッセージトラッキング（Message Tracking ）] ページ内の関連メッセージを表示します。 • メールボックスの自動修復が成功または失敗した受信者に定義されたプロファイル名の一覧。 • 自動修復に失敗した理由。

セクション	説明

[メールボックスの検索と修復（Mailbox Search and Remediate）]	[メールボックスの検索と修復（Mailbox Search and Remediate）] セクションには、次の詳細情報が表示されます。
	• 進行中または完了した修復バッチの一覧。
	• バッチ内のメッセージの修復ステータス。
	• バッチ名とバッチ ID。バッチの詳細を表示するには、バッチ名をクリックします。
	  • メールボックスの検索と修復が開始された日時。
	  • メールボックスの検索と修復が開始された送信元。
	  • メールボックスの検索と修復を開始したホスト。
	  • メッセージに対して実行された修復アクション。
	  • メッセージの Cisco IronPort メッセージ ID。
	  • メッセージが正常に修復される前に、メッセージが受信者によって読み取られたかどうかを示す開封確認アイコン。
	  • 特定のバッチ内のメッセージの修復ステータス（[成功（Success）]、[失敗（Failed）]、または [進行中（In Progress）]）。
	  • メッセージを送信した送信者の電子メールアドレス。
	  • メッセージが配信され、その後で修復が試行された受信者の電子メールアドレス。
	  • メッセージが受信者に送信された日付と時刻。

[メッセージフィルタ（Message Filters）] ページ

[メッセージフィルタ（Message Filters）] ページには、一致数の上位メッセージ フィルタ（最も多くのメッセージに一致したメッセージ フィルタ）に関する情報が 2 種類の形式（棒グラフと表）で表示されます。

棒グラフでは、送受信メッセージによって最も多くトリガーされるメッセージフィルタを確認できます。表には、上位メッセージフィルタと、該当するメッセージフィルタに一致したメッセージの数が示されます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。

[大容量のメール（High Volume Mail）] ページ

（注） [大容量のメール（High Volume Mail）] ページには、Header Repeats ルールを使用するメッセージ フィルタのデータだけが表示されます。

[大容量のメール（High Volume Mail）] ページには、次のレポートが横棒グラフの形式で表示されます。

- [上位件名（Top Subjects）]。このグラフから、AsyncOS が受信したメッセージの上位件名を確認できます。
- [上位エンベロープ送信者（Top Envelope Senders）]。このグラフから、AsyncOS が受信したメッセージの上位エンベロープ送信者を確認できます。
- [一致数別上位メッセージフィルタ（Top Message Filters by Number of Matches）]。このグラフから、一致数に基づく（Header Repeats ルールを使用する）上位メッセージ フィルタを確認できます。

[大容量のメール（High Volume Mail）] ページには、上位メッセージ フィルタと、該当するメッセージフィルタに一致したメッセージの数を示す表も表示されます。数値をクリックすると、メッセージ トラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート（Export）] リンクを使用して CSV 形式にエクスポートできます。

[コンテンツフィルタ（Content Filters）] ページ

[コンテンツフィルタ（Content Filters）] ページには、送受信コンテンツ フィルタの上位一致（最も多くのメッセージに一致したコンテンツ フィルタ）に関する情報が 2 種類の形式（棒グラフとリスト）で表示されます。[コンテンツフィルタ（Content Filters）] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認し、次の情報を取得できます。

- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ

リストのコンテンツ フィルタ名をクリックすると、[コンテンツフィルタの詳細（Content Filter Details）] ページにこのフィルタに関する詳細を表示できます。

関連項目

- コンテンツ フィルタの詳細 （1105 ページ）

コンテンツ フィルタの詳細

コンテンツ フィルタ名リンクをクリックすると、コンテンツ フィルタの詳細が表示されます。[コンテンツ フィルタの詳細（Content Filter Details）] には、このフィルタの経時的な一致および内部ユーザ別の一致が表示されます。

[内部ユーザ別の一致（Matches by Internal Users）] セクションでは、ユーザ名をクリックして内部ユーザ（電子メール アドレス）の [内部ユーザの詳細（Internal User Details）] ページを表示できます（#unique_1506を参照）。

[Safe Print] ページ

[Safe Print] レポート ページを使用して、次の内容を表示できます。

- ファイル タイプ別の、Safe Print で出力された添付ファイルの数（グラフ形式）。
- ファイル タイプ別の、Safe Print で出力された添付ファイルの概要（表形式）。

[Safe Printで出力されたファイル種類の概要（Summary of Safe Print File Types）] セクションで Safe Print で出力された添付ファイルの合計数をクリックすると、[メッセージトラッキング（Message Tracking）] にメッセージの詳細が表示されます。

[高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ

[レポート（Reports）]>[メールフロー概要（Mail Flow Summary）]>[高度なフィッシング防御（Advanced Phishing Protection] レポートページには、次の情報が表示されます。

- Cisco Advanced Phishing Protection クラウドサービスに正常に転送されたメッセージの合計数。
- Cisco Advanced Phishing Protection クラウドサービスに転送されなかったメッセージの合計数。

（注） メッセージメタデータの転送に失敗した場合は、高度なフィッシング防御機能の設定を検証する必要があります。詳細については、電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法 （933 ページ）を参照してください。

[高度なフィッシングからの保護（Advanced Phishing Protection）] レポートページを使用すると、次の情報を確認できます。

- ダッシュボードで組織レベルのすべての電子メールゲートウェイから Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの合計数。

- Cisco Advanced Phishing Protection クラウドサービスへの転送を試行したメッセージの総数（グラフィック形式）

Cisco Advanced Phishing Protection クラウドサービスに転送されるメッセージのメタデータの詳細情報を表示するには、リンクをクリックして Cisco Advanced Phishing Protection クラウドサービスにログインします。詳細については、Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリング （940 ページ）を参照してください。

[メールポリシーの詳細（Mail Policy Details）] レポートページ

[メールポリシーの詳細（Mail Policy Details）] レポートページを使用して、次を表示できます。

- 設定されたメールポリシーに一致した上位の受信メッセージ（グラフおよび表形式）。
- 設定されたメールポリシーに一致した上位の発信メッセージ（グラフおよび表形式）。

[受信ポリシー（Incoming Policies）] セクションで、特定のメールポリシーに一致した受信メッセージの合計数をクリックして、[メッセージトラッキング（Message Tracking）] でメッセージの詳細を表示します。

[送信ポリシー（Outgoing Policies）] セクションで、特定のメールポリシーに一致した着信メッセージの合計数をクリックして、[メッセージトラッキング（Message Tracking）] でメッセージの詳細を表示します。

レポート作成の概要

AsyncOS におけるレポーティングには、次の 3 つの基本動作が含まれます。

- 日単位、週単位、または月単位で実行されるスケジュール設定されたレポートを作成できます。
- ただちにレポートを生成できます（「オンデマンド」レポート）。
- 以前実行したレポートのアーカイブ版を表示できます（スケジュール設定されたレポートおよびオンデマンド レポートの両方）。

スケジュール設定されたレポートおよびオンデマンド レポートは、[モニタ（Monitor）] > [定期レポート（Scheduled Reports）] ページから設定できます。アーカイブ済みレポートは、[モニタ（Monitor）] > [アーカイブ レポート（Archived Reports）] ページから表示できます。

電子メールゲートウェイは、生成した最新のレポートを保持します（すべてのレポートに対して、最大で合計 1000 バージョン）。必要に応じた数（ゼロも含む）のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリングリストを作成する方が容易です。

デフォルトでは、スケジュール設定された各レポートのうち、直近の 12 のレポートが電子メールゲートウェイにアーカイブされます。レポートは、電子メールゲートウェイの /saved_reports ディレクトリに保管されます。（詳細については、FTP、SSH、および SCP アクセス（1573 ページ）を参照してください。）

関連項目

- スケジュール設定されたレポートまたはアーカイブ レポートのタイプ （1107 ページ）
- レポート用返信アドレスの設定 （1108 ページ）

スケジュール設定されたレポートまたはアーカイブレポートのタイプ

次のレポートの種類から選択できます。

- AMP レピュテーション
- [高度なマルウェア防御（Advanced Malware Protection）] におけるファイル分析
- [高度なマルウェア防御（Advanced Malware Protection）] におけるファイルレトロスペクション
- 国別の接続
- コンテンツ フィルタ
- DLP インシデント サマリー
- DMARC 検証レポート
- 成功もしくは失敗（Delivery Status）
- 要約
- 外部脅威フィード
- 偽装メールの検出
- 大容量のメール
- 受信 SMTP 認証
- マクロ検出
- メール フローの概要：着信
- メールボックスの自動修復
- メールフローの詳細（発信送信者：ドメイン）
- メール フロー概要：発信
- メッセージ フィルタ
- 電子メール レポート
- 発信先
- レート制限
- 送信者ドメインのレピュテーション
- 送信者グループ
- システム容量
- TLS 暗号化
- ユーザメール概要（User Mail Summary）
- URL フィルタリング
- アウトブレイク フィルタ
- ウイルス フィルタリング
- Web インタラクション

各レポートは、対応する電子メール セキュリティ モニタ ページのサマリーで構成されます。

関連項目

- レポートに関する注意事項 （1108 ページ）

レポートに関する注意事項

PDF 形式のコンテンツ フィルタ レポートは、最大 40 のコンテンツ フィルタに制限されます。完全なリストは、CSV 形式のレポートで入手できます。

（注） Windows コンピュータ上で中国語、日本語、または韓国語の PDF を生成するには、Adobe.com から該当するフォント パックをダウンロードしてローカル コンピュータにインストールすることも必要です。

レポート用返信アドレスの設定

レポートに返信アドレスを設定するには、電子メールゲートウェイに生成されるメッセージの返信アドレスの設定 （1272 ページ）を参照してください。CLI から、**addressconfig** コマンドを使用します。

レポートの管理

アーカイブ済みのスケジュール設定されたレポートは、作成、編集、削除、および表示を行うことができます。ただちにレポートを実行することもできます（オンデマンド レポート）。これらのレポートの管理および表示については、後述します。

（注） クラスタ モードでは、レポートを表示できません。マシン モードの場合、レポートを表示できます。

[モニタ（Monitor）]>[定期レポート（Scheduled Reports）]ページには、電子メールゲートウェイで生成済みのスケジュール設定されたレポートのリストが示されます。

関連項目

- スケジュール設定されたレポート （1108 ページ）
- アーカイブ レポート （1110 ページ）

スケジュール設定されたレポート

スケジュール設定されたレポートは、日単位、週単位、または月単位で実行するようにスケジュール設定できます。レポートを実行する時間を選択できます。レポートを実行する時間には関係なく、指定した期間（たとえば、過去 3 日または前の 1 か月）のデータのみが含まれま

す。午前 1 時に実行するようにスケジュール設定されている日単位のレポートには、前の日（午前 0 時～午前 0 時）のデータが含まれることに注意してください。

お使いの電子メールゲートウェイは、デフォルトのレポートセットがスケジュール設定された状態で出荷されています。このレポートセットのいずれかを使用したり、変更や削除を行ったりすることができます。

関連項目

- 自動的に生成するレポートのスケジュール （1109 ページ）
- スケジュール設定されたレポートの編集 （1110 ページ）
- スケジュール設定されたレポートの削除 （1110 ページ）

自動的に生成するレポートのスケジュール

手順

ステップ 1 [モニタ（Monitor）] > [定期レポート（Scheduled Reports）] ページで、[定期レポートを追加（Add Scheduled Report）] をクリックします。

ステップ 2 レポートの種類を選択します。選択したレポートの種類に応じて、異なるオプションを使用できます。

使用可能なスケジュール設定されたレポートの種類の詳細については、スケジュール設定されたレポートまたはアーカイブ レポートのタイプ （1107 ページ）を参照してください。

ステップ 3 レポートのわかりやすいタイトルを入力します。AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

ステップ 4 レポート データの時間範囲を選択します（アウトブレイク フィルタ レポートでは、このオプションを使用できません）。

ステップ 5 レポートの形式を選択します。

- PDF. 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。

  英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

- CSV。カンマ区切りの表データを含む ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 6 使用可能な場合は、レポート オプションを指定します。レポートによっては、レポート オプションはありません。

ステップ 7 スケジュールおよび配信オプションを指定します。電子メール アドレスを指定しない場合、レポートはアーカイブされますが、いずれの受信者にも送信されません。

（注） 外部アカウント（Yahoo や Gmail など）にレポートを送信する場合、外部アカウントの許可リストにレポーティング返信アドレスを追加して、レポートの電子メールが誤ってスパムに分類されないようにしてください。

ステップ 8 [送信（Submit）] をクリックします。変更を保存します。

スケジュール設定されたレポートの編集

手順

ステップ 1 [サービス（Services）] > [集約管理レポート（Centralized Reporting）] ページでリストのレポート タイトルをクリックします。

ステップ 2 変更を行います。

ステップ 3 変更を送信し、保存します。

スケジュール設定されたレポートの削除

手順

ステップ 1 [サービス（Services）] > [集約管理レポート（Centralized Reporting）] ページで、削除するレポートに対応するチェックボックスをオンにします。

（注） スケジュール設定されたレポートをすべて削除するには、[すべて（All）] チェックボックスをオンにします。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 削除を確認し、変更内容を確定させます。

削除されたレポートのアーカイブ版は、自動的に削除されるわけではありません。

アーカイブ レポート

[モニタ（Monitor）] > [アーカイブレポート（Archived Reports）] ページでは、使用可能なアーカイブ済みのレポートのリストが表示されます。[レポートのタイトル（Report Title）] カラムの名前をクリックすると、レポートを表示できます。[今すぐレポートを生成（Generate Report Now）] をクリックすると、ただちにレポートを生成できます。

リストに表示されるレポートの種類をフィルタリングするには、[表示（Show）] メニューを使用します。リストをソートするには、カラム見出しをクリックします。

アーカイブ済みのレポートは、自動的に削除されます。スケジュール設定された各レポートの最大 30 インスタンス（最大 1000 レポート）が保存され、新たなレポートが追加されると、古いレポートが削除されてレポートの数は 1000 に維持されます。30 インスタンスという制限は、レポートの種類に対してではなく、個別のスケジュール設定された各レポートに対して適用されます。

関連項目

- オンデマンド レポートの生成 （1111 ページ）

オンデマンド レポートの生成

レポートは、スケジュールを設定しなくても生成できます。これらのオンデマンド レポートも指定したタイム フレームに基づいていますが、ただちに生成できます。

手順

ステップ 1 [アーカイブ レポート（Archived Reports）] ページで [今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 2 レポートの種類を選択し、必要に応じてタイトルを編集します。AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

使用可能なスケジュール設定されたレポートの種類の詳細については、スケジュール設定されたレポートまたはアーカイブ レポートのタイプ （1107 ページ）を参照してください。

ステップ 3 レポート データの時間範囲を選択します（ウイルス発生レポートでは、このオプションを使用できません）。

カスタムの範囲を作成した場合は、その範囲がリンクとして表示されます。範囲を変更するには、そのリンクをクリックします。

ステップ 4 レポートの形式を選択します。

- PDF. 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。

  英語以外の言語での PDF の生成については、レポートに関する注意事項 （1108 ページ）を参照してください。

- CSV。カンマ区切りの表データを含む ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。任意のレポート オプションを指定します。

ステップ 5 レポートをアーカイブするかどうかを選択します（アーカイブする場合には、レポートが [アーカイブ レポート（Archived Reports）] ページに表示されます）。

ステップ 6 レポートを電子メールで送信するかどうか、レポートの送信先の電子メールアドレスを指定します。

ステップ 7 [このレポートを配信（Deliver this Report）] をクリックしてレポートを生成し、受信者に配信するか、このレポートをアーカイブします。

ステップ 8 変更を保存します。

メール レポートのトラブルシューティング

- メッセージ トラッキングへのリンクが予期しない結果になる （1112 ページ）
- クラウド内のファイル分析の詳細が完全でない （1112 ページ）

メッセージ トラッキングへのリンクが予期しない結果になる

問題

メッセージ トラッキングで詳細情報を表示するためにドリル ダウンすると、予期しない結果が表示されます。

解決方法

これはレポーティングおよびメッセージトラッキングが同時にイネーブルにされていない、正常に動作していない、そして（Cisco Secure Email and Web Manager 上に集中的に保存するのではなく）データをローカルに保存している場合に発生する可能性があります。各機能のデータ（レポートおよびメッセージトラッキング）は、他の機能（レポートまたはメッセージトラッキング）がイネーブルおよび動作しているかどうかに関係なく、機能がイネーブルにされて電子メールゲートウェイ上で動作している間のみ保存されます。そのため、レポートにはメッセージトラッキングで使用できないデータが含まれることがあり、その反対も起こり得ます。

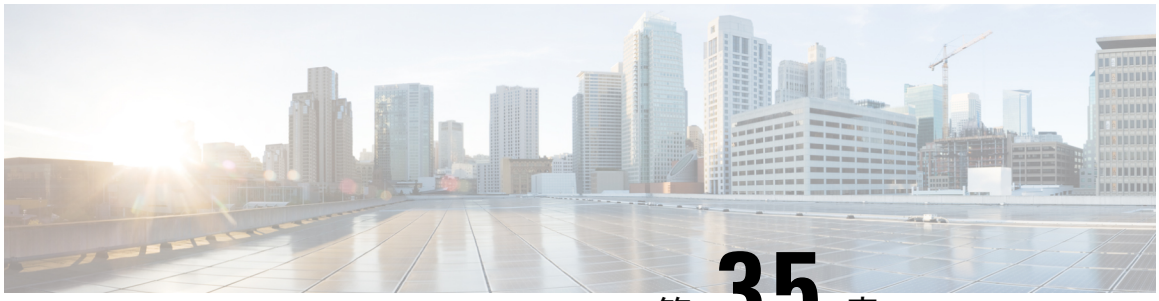
クラウド内のファイル分析の詳細が完全でない

問題

パブリッククラウド内の完全なファイル分析結果は、組織のその他の電子メールゲートウェイからアップロードされたファイルでは取得できません。

解決方法

ファイルの分析結果データを共有するすべての電子メールゲートウェイをグループ化してください。（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定（605 ページ）を参照してください。この設定は、グループの各アプライアンスで実行する必要があります。



第 35 章

メッセージ トラッキング

この章は、次の項で構成されています。

- メッセージ トラッキングの概要 （1113 ページ）
- メッセージ トラッキングの有効化 （1113 ページ）
- レガシー インターフェイスでのメッセージの検索 （1115 ページ）
- 新しい Web インターフェイスでの電子メール メッセージの検索 （1118 ページ）
- メッセージ トラッキングの検索結果の使用 （1121 ページ）
- メッセージ トラッキング データの有効性の検査 （1125 ページ）
- メッセージ トラッキングのトラブルシューティング （1126 ページ）

メッセージ トラッキングの概要

メッセージ トラッキングにより、メッセージ フローの詳細なビューを表示することでヘルプデスク コールを解決に役立ちます。たとえば、メッセージが想定どおりに配信されない場合、ウイルス感染が検出されたか、スパム隔離に入れられたか、あるいはメール ストリーム以外の場所にあるのかを判断できます。

ユーザが指定した基準に一致する特定の電子メール メッセージまたはメッセージのグループを検索できます。

（注） メッセージの内容を読み取るためにメッセージ トラッキングは使用できません。

メッセージ トラッキングの有効化

（注） メッセージ トラッキングのデータは、この機能をイネーブルにした後で処理されたメッセージに対してのみ保持されます。

はじめる前に

- メッセージ トラッキングで添付ファイル名を検索して表示したり、ログ ファイル内の添付ファイル名を表示したりするには、メッセージ フィルタやコンテンツ フィルタなどの本文スキャン プロセスを少なくとも 1 つ設定してイネーブルにする必要があります。
- 件名での検索をサポートするには、ログファイルで件名ヘッダーを記録するように設定する必要があります。詳細については、ログ （1391 ページ）を参照してください。
- 中央集中型トラッキングを設定する場合：該当する電子メールゲートウェイの中央集中型メッセージトラッキングをサポートするように、 Cisco Secure Manager Email and Web Gateway を設定します。『 Cisco Secure Manager Email and Web Gateway User Guide』を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）]>[メッセージ トラッキング（Message Tracking）] をクリックします。

このサービスを一元管理する予定ではない場合でも、このパスを使用します。

ステップ 2 [メッセージトラッキングサービスを有効にする（Enable Message Tracking Service）] を選択します。

ステップ 3 システム設定ウィザードを実行してから初めてメッセージトラッキングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 4 メッセージ トラッキングサービスを選択します。

オプション	説明
ローカル トラッキング（Local Tracking）	この電子メールゲートウェイでメッセージトラッキングを使用します。
中央集中型トラッキング（Centralized Tracking）	これを含め複数の電子メールゲートウェイのメッセージをトレースするために Cisco Secure Manager Email and Web Gateway を使用します。

ステップ 5 （任意）拒否された接続に関する情報を保存するチェックボックスをオンにします。

最適なパフォーマンスを得るために、この設定を無効にしたままにします。

ステップ 6 変更を送信し、保存します。

次のタスク

ローカル トラッキングを選択した場合、次を実行します。

- 誰がDLP違反に関連したコンテンツにアクセスできるかを選択します。メッセージトラッキングでの機密情報へのアクセスの制御 （1197 ページ）を参照してください。
- （任意）メッセージを保存するためのディスク領域の割り当てを調整します。ディスク領域の管理 （1249 ページ） を参照してください。

レガシー インターフェイスでのメッセージの検索

手順

ステップ 1 [メール（Email）] > [メッセージトラッキング（Message Tracking）] > [メッセージトラッキング（Message Tracking）]を選択します。**[モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）]**

ステップ 2 検索条件を入力します。

- すべてのオプションを表示するには、[詳細（Advanced）] リンクをクリックします。
- トラッキングでは、ワイルドカード文字や正規表現はサポートされません。
- トラッキング検索では大文字と小文字は区別されません。
- 特に指定のない限り、クエリーは「AND」検索です。クエリーは、検索フィールドに指定されたすべての条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行のパラメータにテキストストリングを指定すると、クエリーは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。
- 検索条件は、次のとおりです。

オプション	説明
エンベロープ送信者（Envelope Sender）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、そしてメッセージ送信者を検索するための電子メールアドレス、ユーザ名、ドメインを入力します。 文字を入力できます。入力した内容は実行されません。
エンベロープ受信者（Envelope Recipient）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、そしてメッセージ受信者を検索するための電子メールアドレス、ユーザ名、ドメインを入力します。 文字を入力できます。入力した内容は実行されません。

オプション	説明
件名（**Subject**）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、そしてメッセージの件名行で検索するテキスト文字列を入力します。 **警告**：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
受信したメッセージ数（**Message Received**）	日時の範囲を指定します。 日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。 メッセージが電子メールゲートウェイによって受信された現地日時を使用します。
詳細オプション	
送信者IPアドレス/ドメイン/ネットワーク所有者（**Sender IP Address/ Domain / Network Owner**）	リモートホストのIPアドレス、ドメイン、またはネットワーク所有者を指定します。 拒否された接続のみまたはすべてのメッセージを検索の範囲で検索できます。

オプション	説明
添付ファイル（Attachment）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。 添付ファイル名でメッセージを検索できるのは、以下の操作を実行している場合だけです。 • メッセージ フィルタを使用した本文スキャン • コンテンツ フィルタを使用した本文スキャン • 高度なマルウェア防御（AMP）スキャン SHA-256 ハッシュに基づいたファイルの識別方法については、SHA-256ハッシュによるファイルの識別 （616ページ）を参照してください。 Advanced Malware Protection エンジンによって悪意があるとして検出されたメッセージを、脅威名で検索することができます。[カスタム検知（Custom Detection）] および [カスタムしきい値（Custom Threshold）] カテゴリに基づいて悪意があるとして検出されたメッセージを検索するには、[脅威名（Threat Name）] フィールドに *Simple_Custom_ Detection* または *Custom_Threshold* と入力します。また、特定のファイルが Advanced Malware Protection エンジンによってウイルス陽性として検出された場合は、メッセージをウイルス名で検索することもできます。
メッセージ イベント（Message Event）	1つ以上のメッセージ処理イベントを選択します。たとえば、配信メッセージ、隔離メッセージ、ハードバウンス メッセージを検索できます。 メッセージ イベントは「OR」演算子を使用して追加されます。複数のイベントを選択して、指定した条件の任意のものと一致するメッセージを検索します。
メッセージ ID ヘッダー（Message ID Header）	SMTP メッセージ ID ヘッダーのテキスト文字列を入力します。 この RFC 822 メッセージヘッダーは、各電子メール メッセージを識別します。これは最初にメッセージが作成されるときに挿入されます。
Cisco IronPort MID	検索するメッセージ番号を入力します。IronPort MID は、 電子メールゲートウェイ上の各電子メールメッセージを一意に識別します。

オプション	説明
Cisco IronPortホスト（Cisco IronPort Host）	E メール セキュリティ アプライアンスを選択してその 電子メールゲートウェイで処理されたメッセージだけに検索対象を限定するか、またはすべての電子メールゲートウェイを選択します。

ステップ 3 [検索（Search）] をクリックして、クエリーを送信します。

クエリー結果がページの下部に表示されます。

次のタスク

関連項目

- メッセージ トラッキングの検索結果の使用 （1121 ページ）

新しい Web インターフェイスでの電子メール メッセージの検索

電子メールゲートウェイのトラッキングサービスを使用して、メッセージ件名行、日時の範囲、エンベロープ送信者または受信者、処理イベント（たとえば、メッセージがウイルス陽性またはスパム陽性かどうかや、ハードバウンスまたは配信されたかどうか）など、指定した条件に一致する特定の電子メールメッセージまたはメッセージのグループを検索できます。メッセージ トラッキングでは、メッセージ フローの詳細なビューが表示されます。また、特定の電子メール メッセージをドリルダウンし、処理イベント、添付ファイル名、エンベロープおよびヘッダー情報など、メッセージの詳細情報を確認することもできます。

（注） このトラッキング コンポーネントにより個々の電子メール メッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

手順

ステップ 1 [トラッキング（Tracking）] タブをクリックします。

ステップ 2 [メッセージ（Messages）] タブまたは [拒否された接続（Connections Rejected）] タブを選択し、検索結果を絞り込みます。

（注） 送信者 IP アドレス、ドメイン、またはネットワーク所有者に基づいて拒否された接続を検索することができます。

ステップ 3 （任意）[詳細検索（Advanced Search）] をクリックし、その他の検索オプションを表示します。

ステップ 4 次の検索条件を入力します。

（注） トラッキング検索では、ワイルドカード文字や正規表現はサポートされません。トラッキング検索では大文字と小文字は区別されません。

- （メッセージと拒否された接続の場合）[受信したメッセージ数（Message Received）] : [前日（Last Day）]、[最近1週間（Last 7 Days）]、または [カスタム範囲（Custom Range）] を使用してクエリの日時の範囲を指定します。過去 24 時間以内のメッセージを検索するには [前日（Last Day）] オプションを使用し、過去 7 日間のメッセージを検索するには [最近1週間（Last 7 Days）] オプションと当日の経過時間を使用します。

  日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。終了日と終了時刻に現在の日付と 23:59 を指定すると、クエリは現在の日付に関するすべてのデータを返します。

  日付と時間は、データベースに保管される際に GMT 形式に変換されます。 電子メールゲートウェイ上で日付と時刻を表示する場合は、その電子メールゲートウェイの現地時間で表示されます。

  電子メールゲートウェイのログに記録され、 Cisco Secure Email and Web Gateway が取得済みのメッセージのみが検索結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間と、それがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。

- [エンベロープ送信者（Envelope Sender）] : [次で始まる（Begins With）]、[次に合致する（IS）]、または [次を含む（Contains）] を選択し、テキスト文字列を入力してエンベロープ送信者を検索します。電子メール アドレス、ユーザ名、またはドメインを入力できます。次の形式を使用します。
  - E メール ドメインの場合：*example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]*
  - 完全 E メール アドレスの場合：*user@example.com, user@[203.0.113.15] or user@[ipv6:2001:db8:80:1::5]*。
  - 文字を入力できます。入力した内容は実行されません。

- [件名（Subject）] : [次で始まる（Begins With）]、[次に合致する（IS）]、[次を含む（Contains）]、または [空である（Is Empty）] を選択し、テキスト文字列を入力してメッセージ件名行を検索します。

- [エンベロープ受信者（Envelope Recipient）] : [次で始まる（Begins With）]、[次に合致する（IS）]、または [次を含む（Contains）] を選択し、テキストを入力してエンベロープ受信者を検索します。電子メール アドレス、ユーザ名、またはドメインを入力できます。

  電子メールゲートウェイでエイリアス拡張にエイリアステーブルを使用している場合は、本来のエンベロープアドレスではなく、拡張された受信者アドレスが検索されます。それ

以外のあらゆる場合においては、メッセージ トラッキング クエリによって本来のエンベロープ受信者アドレスが検索されます。

この点を除けば、エンベロープ受信者の有効な検索条件はエンベロープ送信者の場合と同じです。

文字を入力できます。入力した内容は実行されません。

- [添付ファイル名（Attachment Name）]：[次で始まる（Begins With）]、[次に合致する（IS）]、または [次を含む（Contains）] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。
- Reply-To：[次で始まる（Begins With）]、[次に合致する（Is）]、または [含む（Contains）] を選択して、メッセージの「`Reply-To`」ヘッダーに基づいてメッセージを検索する文字列を入力します。
- [ファイルSHA256（File SHA256）]：メッセージのファイルの SHA-256 値を入力します。

  SHA-256 ハッシュに基づいたファイルの識別方法については、SHA-256 ハッシュによるファイルの識別 （1076 ページ）を参照してください。
- [シスコのホスト（Cisco Host）]：[すべてのホスト（All Host）] を選択してすべての 電子メールゲートウェイ間で検索するか、ドロップダウンメニューから必要な電子メールゲートウェイを選択します。
- [メッセージIDヘッダーおよびCisco MID（Message ID Header and Cisco MID）]：メッセージ ID ヘッダーのテキスト文字列、Cisco IronPort メッセージ ID（MID）、またはその両方を入力します。
- （メッセージと拒否された接続の場合）[送信者IPアドレス/ドメイン/ネットワーク所有者（Sender IP Address/ Domain / Network Owner）]：送信元 IP アドレス、ドメインまたはネットワーク所有者の詳細を入力します。
  - IPv4 アドレスは、ピリオドで区切られた 4 つの数値であり、それぞれの数値は 0 ～ 255 でなければなりません（例：203.0.113.15）。
  - IPv6 アドレスでは、8 つの 16 ビットの 16 進数値がコロンで区切られて構成されます。

    いずれか 1 箇所で、2001:db8:80:1::5 のようにゼロ圧縮を使用できます。
  - [メッセージイベント（Message Event）]：追跡対象のイベントを選択します。たとえば、配信メッセージ、隔離メッセージ、ハードバウンス メッセージを検索できます。メッセージ イベントは「OR」演算子を使用して追加されます。複数のイベントを選択して、指定した条件の任意のものと一致するメッセージを検索します。

すべてのフィールドに入力する必要はありません。[メッセージイベント（Message Event）]オプションを除き、クエリは「AND」検索になります。このクエリは、検索フィールドで指定された「AND」条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行

のパラメータにテキスト ストリングを指定すると、クエリは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。

ステップ 5 **[検索（Search）]** をクリックします。

各行が 1 つの電子メール メッセージに対応します。ビューでメッセージをさらにロードするにはスクロールダウンします。

必要に応じて、新しい検索基準を入力することにより検索を精密化し、クエリを再実行します。あるいは、次の項で説明するように、結果セットを絞り込んで検索精度を高めることもできます。

次のタスク

- メッセージ トラッキングの検索結果の使用 （1121 ページ）

メッセージ トラッキングの検索結果の使用

次の点に留意してください。

- 電子メールゲートウェイのログに記録され、 Cisco Secure Manager Email and Web Gateway で取得済みのメッセージのみが検索結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間と、それがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。
- 高度なマルウェア防御（ファイル レピュテーション スキャンおよびファイル分析）を使用する検索については、メッセージ トラッキング機能と Advanced Malware Protection 機能について （619 ページ）を参照してください。

検索結果を使用する場合に実行できる操作：

- 検索条件に戻って、クエリー設定の[詳細（Advanced）]をクリックし、[クエリ設定（Query Settings）]までスクロールし、結果の最大数を 1000 に設定すると、250 件以上の検索結果を表示できます。
- 検索結果セクションの右上でオプションを選択すると、各ページに表示される結果を増やすことができます。
- 検索結果セクションの右上から、複数のページの検索結果内を移動できます。
- 条件として追加する検索結果の値の上でカーソルを移動すると、検索結果を限定できます。オレンジ色で強調表示されている場合は、その値をクリックすると、その条件で検索を絞り込むことができます。これで、検索条件が追加されます。たとえば、特定の受信者に送信されたメッセージを検索した場合は、検索結果で送信者の名前をクリックすると、最初に指定した時間範囲内の（および、その他の条件を満たす）、その送信者からその受信者へのすべてのメッセージを見つけることができます。
- 検索条件に 1000 件以上のメッセージが一致する場合、（検索結果セクションの右上にあるリンク）[すべてエクスポート（Export All）] をクリックし、最大 50,000 件の検索結果

をカンマ区切り形式ファイルとしてエクスポートし、他のアプリケーションでデータを使用できます。

- メッセージの行の [詳細の表示（Show Details）] をクリックすると、メッセージの詳細情報を表示できます。メッセージの詳細を表示した新しいブラウザ ウィンドウが開きます。
- 隔離されたメッセージの場合、メッセージが隔離された理由などの詳細情報を表示するにはメッセージ トラッキングの検索結果のリンクをクリックします。
- [メールボックスの検索と修復（Mailbox Search and Remediate）] アクションを使用して、ユーザメールボックスにある悪意のあるメッセージを修復します。詳細については、メールボックス内のメッセージの検索と修復 （733 ページ）を参照してください。

（注） レポート ページのリンクをクリックして、メッセージ トラッキングのメッセージ詳細を表示したが、その結果が予期したものでない場合があります。これは、確認している期間中に、レポーティングとトラッキングを同時に継続してイネーブルにしていない場合に発生する可能性があります。

関連項目

- メッセージ トラッキングの詳細 （1122 ページ）

メッセージ トラッキングの詳細

項目	説明
[エンベロープとヘッダーのサマリー（Envelope and Header Summary）] セクション	
受信時間（Received Time）	電子メールゲートウェイがメッセージを受信した時間。 日時は、 電子メールゲートウェイで設定される現地時間を使用して表示されます。
MID	一義的な IronPort メッセージ ID。
メッセージ サイズ（Message Size）	メッセージ サイズ。
件名（Subject）	メッセージの件名リスト。 トラッキング結果の件名行は、メッセージの件名がないか、ログ ファイルで件名ヘッダーを記録するよう設定されていない場合、[（件名なし）（(No Subject)）] という値になる場合があります。詳細については、ログ （1391 ページ）を参照してください。

項目	説明
エンベロープ送信者（Envelope Sender）	SMTP エンベロープ内の送信者のアドレス。
エンベロープ受信者（Envelope Recipients）	導入でエイリアス拡張のためのエイリアス テーブルを使用する場合、検索では元のエンベロープ アドレスではなく拡張された受信者アドレスを見つけます。エイリアステーブルの詳細については、「ルーティングおよび配信機能の設定」の章にある「エイリアステーブルの作成」を参照してください。 それ以外のあらゆる場合においては、メッセージ トラッキング クエリーによって本来のエンベロープ受信者アドレスが検索されます。
メッセージ ID ヘッダー（Message ID Header）	RFC 822 のメッセージ ヘッダー。
SMTP 認証ユーザ ID（SMTP Auth User ID）	送信者が SMTP 認証を使用してメッセージを送信した場合は、SMTP で認証された送信者のユーザ名。それ以外の場合、この値は「なし（N/A）」となります。
添付ファイル	メッセージに添付されたファイルの名前。 名前に対してクエリーが実行された少なくとも 1 つの添付ファイルを含むメッセージが検索結果に表示されます。 トラッキングできない添付ファイルもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは他のスキャン動作の一環としてのみ実行されます。たとえば、メッセージまたはコンテンツ フィルタリング、DLP、免責事項スタンプなどです。添付ファイル名は、添付ファイルがまだ添付されている間に本文スキャンを通過するメッセージに対してのみ使用できます。添付ファイルの名前が検索結果に表示されない状況を含みます（ただし限定はされません）。 • システムがコンテンツフィルタのみを使用しているときに、メッセージがドロップされるか、またはその添付ファイルがアンチスパムまたはアンチウイルスフィルタによって削除された場合 • 本文スキャンが実行される前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが削除された場合 パフォーマンス上の理由から、添付ファイル内のファイルの名前（たとえば、OLE オブジェクトや、.ZIP ファイルなどのアーカイブ）は検索されません。

項目	説明
（新しいWebインターフェイスのみ）[メッセージイベント（Message Event）]	各イベント タイプに一致するメッセージが含まれている複数のイベントを選択します。
[ホスト サマリーの送信（Sending Host Summary）] セクション	
逆引き DNS ホスト名（Reverse DNS Hostname）	逆引き DNS（PTR）ルックアップによって検証される送信ホストの名前。
IP Address	送信元ホストの IP アドレス。
IP レピュテーション**スコア**	IP レピュテーションスコア。範囲は、10（最も信頼できる送信者）～-10（明らかなスパム送信者）です。スコアが「なし（None）」の場合、そのメッセージが処理された時点で、このホストに関する情報が存在しなかったことを意味します。 IP レピュテーションサービスの詳細については、IP レピュテーション フィルタリング （99 ページ）
[処理詳細（Processing Details）] セクション	
要約情報 （以下のタブのいずれかが表示されている場合、この情報はタブに表示されます。常にサマリー情報を表示します）。	[サマリー（Summary）] タブでは、メッセージ処理中に記録されるステータス イベントを表示します。 エントリには、メールポリシーの処理（アンチスパム スキャンやアンチウイルス スキャンなど）とメッセージ分割などの他のイベントに関する情報、およびコンテンツまたはメッセージ フィルタによって追加されるカスタム ログ エントリが含まれます。 メッセージが配信された場合、配信の詳細がここに表示されます。 記録された最新のイベントは、処理の詳細内で強調表示されます。

項目	説明
DLP に一致した内容（DLP Matched Content）タブ	このタブは、DLP ポリシーによって検出されたメッセージに対してのみ表示されます。 このタブには、DLP ポリシーの一致をトリガーした機密のコンテンツに加え、一致に関する情報が含まれます。 この情報を表示するには 電子メールゲートウェイを設定する必要があります。「メッセージ トラッキングでの機密性の高い DLP データの表示 （657 ページ）」を参照してください。 このタブへのアクセスを制御するには、メッセージ トラッキングでの機密情報へのアクセスの制御（1197ページ）を参照してください。
[URL の詳細（URL Details）] タブ	このタブは、URL レピュテーション コンテンツ フィルタと URL カテゴリ コンテンツ フィルタ、およびアウトブレイク フィルタによって捕捉されたメッセージに対してのみ表示されます。 このタブには、次の情報が表示されます。 • URL に関連付けられているレピュテーション スコアまたはカテゴリ • URL に対して実行されたアクション（書き換え、危険の除去、またはリダイレクト） • メッセージに複数の URL が含まれる場合、フィルタ アクションをトリガーした URL この情報を表示するには 電子メールゲートウェイを設定する必要があります。「メッセージ トラッキングの URL 詳細の表示 （562 ページ）」を参照してください。 このタブへのアクセスを制御するには、メッセージ トラッキングでの機密情報へのアクセスの制御（1197ページ）を参照してください。

関連項目

• レガシー インターフェイスでのメッセージの検索 （1115 ページ）

メッセージ トラッキング データの有効性の検査

メッセージ トラッキング データに含まれる日付範囲を確認すること、およびそのデータの欠落インターバルを識別することができます。

手順

ステップ 1 （新しい Web インターフェイスのみ）ページの右上隅にある歯車アイコンをクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [モニタ（Monitor）] > [メッセージトラッキング（Message Tracking）] を選択します。

ステップ 3 右上隅にある [検索（Search）] ボックスに表示される [時間範囲内のデータ:（Data in time range:）] を確認します。

ステップ 4 [時間範囲内のデータ:（Data in time range:）] で示される値をクリックします。

次のタスク

関連項目

- メッセージ トラッキングおよびアップグレードについて （1126 ページ）

メッセージ トラッキングおよびアップグレードについて

新しいメッセージトラッキング機能は、アップグレードの前に処理されたメッセージには適用できない場合があります。これは、これらのメッセージについては、必須データが保持されていない場合があるためです。メッセージ トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

メッセージ トラッキングのトラブルシューティング

関連項目

- 添付ファイルが検索結果に表示されない （1126 ページ）
- 予想されるメッセージが検索結果に表示されない （1126 ページ）

添付ファイルが検索結果に表示されない

問題

添付ファイル名が検出されず、検索結果に表示されません。

ソリューション

メッセージトラッキングの有効化（1113ページ）を参照してください。メッセージトラッキングの詳細 （1122 ページ）の添付ファイル名の検索の制約についても参照してください。

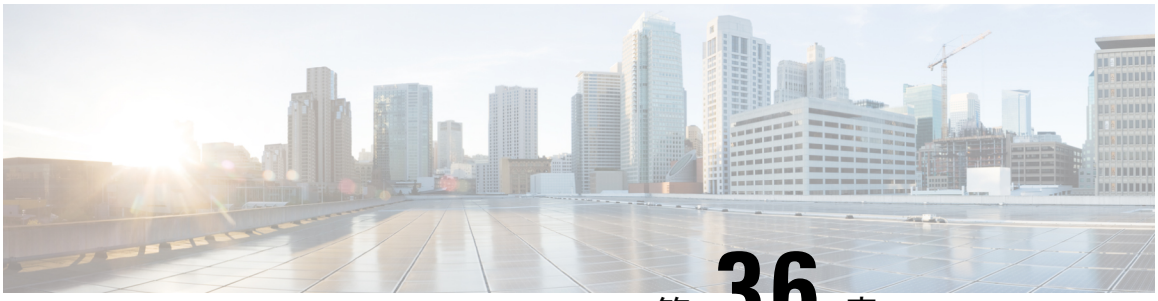
予想されるメッセージが検索結果に表示されない

問題

条件に一致するメッセージが検索結果に含まれていません。

ソリューション

- さまざまな検索、特にメッセージイベントに関連する検索の結果は、電子メールゲートウェイの設定によって異なります。たとえばフィルタ処理していない URL カテゴリを検索すると、メッセージにそのカテゴリの URL が含まれていても、結果には表示されません。意図した動作を実現するように電子メールゲートウェイが正しく設定されていることを確認します。メール ポリシー、コンテンツ フィルタおよびメッセージ フィルタ、隔離の設定などを確認してください。
- レポートのリンクをクリックしても予想される情報が表示されない場合は、メール レポートのトラブルシューティング （1112 ページ）を参照してください。



第 36 章

ポリシー、ウイルス、およびアウトブレイク隔離

この章は、次の項で構成されています。

- ポリシー、ウイルス、およびアウトブレイク隔離の概要 （1129 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離の管理 （1133 ページ）
- ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作 （1143 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離の概要

「ポリシー、ウイルス、およびアウトブレイク隔離」には、ファイル分析の隔離を含むすべての非スパム隔離が含まれます。

電子メールゲートウェイは危険性のあるマルウェア、または組織で許可されていないコンテンツを送受信メッセージで検出した場合、すぐに削除せずに隔離エリアに送信します。隔離エリアはこれらのメッセージを 電子メールゲートウェイまたは Cisco Secure Email and Web Manager で一定期間安全に保持し、ユーザがそれらを評価するまで、またはメッセージの安全性を適切に評価できるアップデートまで待ちます。

組織での非スパム隔離の使用例：

- **ポリシーの実施。**人事担当部門または法務部門が、それらに不快な情報や秘密情報などの許可されない情報が含まれていないか確認します。
- **ウイルス隔離。**ユーザへのウイルスの拡散を防ぐためのアンチウイルス スキャン エンジンによって、暗号化メッセージや感染メッセージまたはスキャン不可能とマークされたメッセージを保管します。
- **アウトブレイクの防止。**アウトブレイク フィルタによってウイルスのアウトブレイクの一部または小規模なマルウェア攻撃としてフラグ付けされたメッセージを、アンチ ウイルスまたはアンチ スパム アップデートがリリースされるまで保管します。
- **ファイル分析の隔離。**判定に到達するまで、分析用に送信されたマルウェアを含む可能性がある添付ファイルを含むメッセージを保存します。

関連項目

- スパム隔離 （1153 ページ）

隔離の種類

隔離タイプ	隔離名	デフォルトで作成される	説明	詳細情報
高度なマルウェア防御（Advanced Malware Protection）	ファイル分析（File Analysis）	○	判定が返されるまで、ファイル分析のために送信されたメッセージを保持します。	• ポリシー、ウイルス、およびアウトブレイク隔離の管理 • ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作
ウイルス	ウイルス	○	アンチウイルスエンジンによる判定に従って、マルウェアを送信する可能性のあるメッセージを保持します。	
アウトブレイク	アウトブレイク	○	アウトブレイクフィルタでスパムまたはマルウェアの可能性があると検出されたメッセージを保持します。	
ポリシー	ポリシー	○	メッセージフィルタ、コンテンツフィルタ、およびDLPメッセージアクションによって検出されたメッセージを保留します。 デフォルトのポリシー隔離が用意されています。	
	Unclassified	○		

隔離タイプ	隔離名	デフォルトで作成される	説明	詳細情報
			メッセージ フィルタ、コンテンツ フィルタ、または DLP メッセージ アクションで指定した隔離が削除された場合にのみ、メッセージを保持します。 この隔離をフィルタやメッセージ アクションに割り当てることはできません。	
	（自分で作成する「ポリシー隔離」）	×	メッセージ フィルタ、コンテンツ フィルタおよび DLP メッセージ アクションで使用するために作成する「ポリシー隔離」。	
スパム	スパム	○	スパムおよびその疑いのあるメッセージを保持して、メッセージの受信者や管理者が確認できるようにします。 スパム隔離は、ポリシー、ウイルス、およびアウトブレイクの隔離グループに含まれておらず、これらの隔離とは別に管理します。	スパム隔離 （1153 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離の管理

- ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て （1133 ページ）
- 隔離内のメッセージの保持期間 （1134 ページ）
- 隔離メッセージに自動的に適用されるデフォルト アクション （1135 ページ）
- システム作成の隔離の設定を確認 （1135 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離の設定 （1135 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について （1138 ページ）
- ポリシー隔離を割り当てるフィルタおよびメッセージ アクションの決定 （1138 ページ）
- ポリシー隔離の削除について （1138 ページ）
- 隔離のステータス、容量、およびアクティビティのモニタリング （1139 ページ）
- ポリシー隔離のパフォーマンス （1141 ページ）
- 隔離用のディスク容量の使用率に関するアラート （1141 ページ）
- ポリシー隔離とロギング （1141 ページ）
- メッセージ処理タスクの他のユーザへの割り当てについて （1142 ページ）
- クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について （1143 ページ）
- ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法 （1143 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て

ポリシー、ウイルス、およびアウトブレイク隔離のディスク領域の詳細については、ディスク領域の管理 （1249 ページ）を参照してください。

隔離を集約しても、ポリシー、ウイルス、およびアウトブレイク隔離は、 電子メールゲートウェイのディスク領域を消費します。

複数の隔離のメッセージは、1つの隔離のメッセージと同じ容量のディスク領域を消費します。

アウトブレイク フィルタと集約隔離の両方が有効な場合、以下のようになります。

- ローカルのポリシー隔離、ウイルス隔離、およびアウトブレイク隔離に割り当てられるべき 電子メールゲートウェイ上のすべてのディスク領域が、アウトブレイク隔離内のメッセージのコピーを保持するために使用されます。これらのメッセージは、アウトブレイク ルールが更新されるたびにスキャンされます。
- 特定の管理対象

関連項目

- 隔離のステータス、容量、およびアクティビティのモニタリング （1139 ページ）
- 隔離用のディスク容量の使用率に関するアラート （1141 ページ）

• 隔離内のメッセージの保持期間 （1134 ページ）

隔離内のメッセージの保持期間

メッセージは次のタイミングで隔離から自動的に削除されます。

- 通常の期限切れ：隔離エリア内のメッセージが設定された保存期間を満了した場合です。各隔離エリアのメッセージの保存期間を指定します。各メッセージには一定の保持期間があり、その期間のみ隔離のリストに表示されます。このトピックで説明する別の状況が発生しない限り、メッセージは指定された期間が経過するまで保持されます。

（注） アウトブレイク フィルタ隔離でのメッセージの通常の保持期間は、アウトブレイク隔離ではなく各メールのアウトブレイク フィルタ セクションで設定します。

- 早期の期限切れ：設定した保持期間が経過する前にメッセージが隔離から強制的に削除された場合です。これは次の場合に発生します。
  - ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て （1133 ページ）で定義した、すべての隔離に対するサイズ制限に達した場合。

    サイズ制限に達すると、隔離に関係なく、古いメッセージからデフォルト アクションが適用されます。すべての隔離のサイズが制限値未満に戻るまで、各メッセージに対してデフォルト アクションが実行されます。このポリシーは、First In First Out（FIFO; 先入れ先出し）です。複数の隔離内に保持されたメッセージの場合は、最新の保持期間に基づいて期限切れになります。

    （任意）ディスク容量が不足したときのリリースまたは削除の対象から、特定の隔離を除外することができます。除外するようにすべての隔離を設定して、ディスク領域が満杯になった場合、新しいメッセージの領域を確保するために隔離内にあるメッセージが配信されます。

    ディスク領域の容量が一定の値に達すると、アラートが送信されます。隔離用のディスク容量の使用率に関するアラート （1141 ページ）を参照してください。

- メッセージを保持している隔離を削除した場合。

メッセージが隔離から自動的に削除されるときに、そのメッセージに対してデフォルト アクションが実行されます。隔離メッセージに自動的に適用されるデフォルト アクション （1135 ページ） を参照してください。

（注） これらのシナリオに加えて、スキャン操作の結果に基づいて、メッセージを隔離から自動的に削除できます（アウトブレイク フィルタまたはファイル分析）。

保存期間への時間調整の影響

- サマータイムと 電子メールゲートウェイのタイムゾーンの変更は保持期間に影響しません。
- 隔離の保持期間を変更すると、その保持期間は新しいメッセージにのみ適用され、既存のメッセージには適用されません。
- システム クロックを変更してメッセージの保持期間が過ぎた場合は、次の最も適切な時間に期限切れになります。
- システム クロックの変更は期限切れの処理中のメッセージには適用されません。

隔離メッセージに自動的に適用されるデフォルト アクション

隔離内のメッセージの保持期間 （1134 ページ）に記述されるいずれかの状況が発生した場合、ポリシー、ウイルス、またはアウトブレイク隔離内のメッセージに対してデフォルトアクションが実行されます。

デフォルト アクションには、以下の 2 つがあります。

- 削除：メッセージを削除します。
- リリース：メッセージが解放されて配信されます。

メッセージのリリース時に、脅威に対する再スキャンが実行される場合があります。詳細については、隔離されたメッセージの再スキャンについて （1151 ページ）を参照してください。

また、指定した保持期間よりも前にリリースされるメッセージには、X-Header の追加などの操作が行われる場合があります。詳細については、ポリシー、ウイルス、およびアウトブレイク隔離の設定 （1135 ページ）を参照してください。

システム作成の隔離の設定を確認

隔離を使用する前に、デフォルトの隔離設定（未分類隔離など）をカスタマイズします。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離の設定 （1135 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離の設定

始める前に

- 既存の隔離を編集する場合は、ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について （1138 ページ）を参照してください。
- 保持期間やデフォルトアクションなど、隔離内のメッセージを自動的に管理する方法を確認します。隔離内のメッセージの保持期間 （1134 ページ）および隔離メッセージに自動的に適用されるデフォルト アクション （1135 ページ）を参照してください。

- 各隔離にアクセスできるユーザーを決め、ユーザーおよびカスタム ユーザー ロールを作成します。詳細は、ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定 （1142 ページ）を参照してください。

手順

ステップ 1 ポリシー、ウイルス、およびアウトブレイク隔離は、次のいずれかの方法で設定できます。

- （新しい Web インターフェイスのみ）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] > [+] を選択します。
- [モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、次のいずれかを実行します。
  - [ポリシー隔離の追加（Add Policy Quarantine）] をクリックします。
  - 編集する隔離をクリックします。

ステップ 2 次の情報を入力します。

次の点を考慮してください。

- ファイル分析隔離の保持期間をデフォルトの 1 時間から変更することは推奨されません。
- 隔離ディスク領域が一杯になった場合でも、指定した保存期間の終了前にこの隔離メッセージを処理されたくない場合、[メッセージに対してデフォルトのアクションを適用して空き容量を増やす（Free up space by applying default action on messages upon space overflow）] の選択を解除します。

  このオプションはすべての隔離では選択しないでください。システムは、少なくとも 1 つの隔離エリアからメッセージを削除して、領域を確保する必要があります。
- デフォルト アクションとして [リリース（Release）] を選択すると、保持期間前にリリースされるメッセージに適用する追加のアクションを指定できます。

オプション	情報
件名の変更（Modify Subject）	追加するテキストを入力し、そのテキストを元の件名の前と後ろのどちらに追加するかを選択します。 たとえば、受信者に不適切なコンテンツを含む可能性があるメッセージであることを警告するテキストを追加します。 （注） 非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。

オプション	情報
[X-Header の追加（Add X-Header）]	X-Headerにはメッセージに対して実行されたアクションを記録できます。この情報は、特定のメッセージが配信された理由についての照会を処理するときなどに役立ちます。 名前と値を入力します。 例： Name = Inappropriate-release-early Value = True
添付ファイルを除去（Strip Attachments）	添付ファイルを除去すると、そのファイルに存在する潜在的なウイルスから保護できます。

ステップ 3 この隔離へのアクセスを付与するユーザを指定します。

ユーザー	情報
ローカル ユーザー（Local Users）	ローカルユーザのリストには、隔離にアクセスできるロールを持つユーザだけが含まれます。 すべての管理者は隔離に完全なアクセス権限を持つため、リストでは管理者が除外されます。
外部認証されたユーザ（Externally Authenticated Users）	外部認証を設定しておく必要があります。
カスタムユーザロール（Custom User Roles）	このオプションは、隔離へのアクセス権限を持つ少なくとも 1 つのカスタムユーザー ロールを作成している場合にのみ表示されます。

ステップ 4 変更を送信し、保存します。

次のタスク

メッセージおよびコンテンツ フィルタ、メッセージを隔離エリアに移動する DLP メッセージアクションを作成します。を参照してください。

ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について

（注）
- 隔離の名前は変更できません。
- 隔離内のメッセージの保持期間 （1134 ページ）も参照してください。

隔離の設定を変更するには、**[モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]** を選択し、隔離の名前をクリックします。

新しい Web インターフェイスで隔離の設定を変更するには、[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] に移動し、必要な隔離で をクリックします。

ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定

ポリシー隔離に関連付けられているメッセージ フィルタ、コンテンツ フィルタ、データ損失の防止（DLP）メッセージ アクション、DMARC 検証プロファイルを表示できます。

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで、[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] をクリックします。

ステップ 2 （新しい Web インターフェイスのみ）必要な隔離を選択して ボタンをクリックします。

ステップ 3 [モニタ（Monitor）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 4 ポリシー隔離の名前をクリックします。

ステップ 5 ページの下部までスクロールし、[関連付けられたメッセージフィルタ/コンテンツ フィルタ/DLP メッセージアクション（Associated Message Filters/Content Filters/DLP Message Actions）] を確認します。

ポリシー隔離の削除について

- ポリシー隔離を削除する前に、アクティブなフィルタやメッセージアクションに関連付けられているかどうかを確認します。ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定 （1138 ページ）を参照してください。
- フィルタやメッセージアクションが割り当てられている場合でも、ポリシー隔離を削除できます。

- 空でない隔離を削除する場合、ディスクがいっぱいになった際にメッセージを削除しないオプションを選択した場合でも、隔離で定義されたデフォルトアクションはすべてのメッセージに適用されます。隔離メッセージに自動的に適用されるデフォルト アクション（1135 ページ）を参照してください。
- フィルタまたはメッセージアクションに関連付けられた隔離を削除した後でそのフィルタまたはメッセージ アクションにより隔離されたメッセージは、未分類隔離に格納されます。隔離を削除する前に、未分類隔離のデフォルト設定をカスタマイズしておく必要があります。
- 未分類隔離は削除できません。

隔離のステータス、容量、およびアクティビティのモニタリング

目的	操作手順
すべての非スパム隔離に割り当てられている領域の合計	（新しいWebインターフェイスのみ）電子メールゲートウェイで ⚙ をクリックして、レガシーWebインターフェイスをロードします。 **[モニタ（Monitor）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]**を選択し、そのページの最初のセクションを確認します。 割り当ての変更方法については、ディスク領域の管理（1249 ページ）を参照してください。
スパム隔離以外のすべての隔離で使用可能な領域を確認する	（新しい Web インターフェイスのみ）[隔離（Quarnatine）]>[その他の隔離（Other Quarantine）]を選択します。 **[モニタ（Monitor）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]** を選択し、テーブルのすぐ下で確認します。
現在すべての隔離が使用している合計容量を確認する	（新しいWebインターフェイスのみ）電子メールゲートウェイで ⚙ をクリックして、レガシーWebインターフェイスをロードします。 [モニタ（Monitor）]>[システムステータス（System Status）]を選択し、[隔離に使用されるキュースペース（Queue Space Used by Quarantine）]を探します。

目的	操作手順
現在各隔離に使用されている容量を確認する	（新しい Web インターフェイスのみ）[隔離（Quarantines Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 **[モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]** を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します。
現在すべての隔離にあるメッセージの総数を確認する	（新しいWebインターフェイスのみ）電子メールゲートウェイで ⚙ をクリックして、レガシーWebインターフェイスをロードします。 [モニタ（Monitor）] > [システムステータス（System Status）] を選択し、[隔離内のアクティブメッセージ（Active Messages in Quarantine）] を探します。
現在各隔離にあるメッセージ数を確認する	（新しい Web インターフェイスのみ）[隔離（Quarantines Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 [モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブル行でその隔離を確認します。
すべての隔離による総 CPU 使用率を確認する	（新しいWebインターフェイスのみ）電子メールゲートウェイで ⚙ をクリックして、レガシーWebインターフェイスをロードします。 [モニタ（Monitor）] > [システムステータス（System Status）] を選択し、[CPU使用率（CPU Utilization）] セクションを確認します。
最後のメッセージが各隔離に送信された日時（ポリシー隔離間の移動を除く）を確認する	（新しい Web インターフェイスのみ）**[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）]** を選択します。 [モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択し、テーブル行でその隔離を確認します。

目的	操作手順
ポリシー隔離が作成された日時を確認する	（新しいWebインターフェイスのみ）電子メールゲートウェイで ⚙ をクリックして、レガシーWebインターフェイスをロードします。 **[モニタ（Monitor）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]**を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します。 作成日および作成者の名前はシステムが作成した隔離では使用されません。
ポリシー隔離の作成者の名前	
ポリシー隔離に関連付けられたフィルタおよびメッセージ アクションを確認する	ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定 （1138 ページ） を参照してください。

ポリシー隔離のパフォーマンス

ポリシー隔離エリアに保存されたメッセージは、ハード ドライブ容量に加えて、システム メモリを使用します。1つの電子メールゲートウェイのポリシー隔離エリア内で数十万件のメッセージを保存すると、過剰なメモリ使用により電子メールゲートウェイのパフォーマンスが低下することがあります。電子メールゲートウェイでのメッセージの隔離、削除、および解放により多くの時間が必要になるため、メッセージ処理の速度が低下し、電子メールパイプラインが渋滞します。

電子メールゲートウェイが通常の速度で電子メールを処理できるように、ポリシー隔離には平均で 2 万件よりも少ないメッセージを保存することを推奨します。

隔離のメッセージ数を調べるには、隔離のステータス、容量、およびアクティビティのモニタリング （1139 ページ）を参照してください。

隔離用のディスク容量の使用率に関するアラート

ポリシー、ウイルス、およびアウトブレイク隔離の合計容量が75%、85%、および95%になると、アラートが送信されます。使用率は、メッセージが隔離内に格納されたときにチェックされます。たとえば、メッセージが隔離に追加されたときに隔離エリアの合計サイズが指定容量の 75% 以上に増加すると、アラートが送信されます。

ポリシー隔離とロギング

AsyncOS により、隔離されるすべてのメッセージが個別にロギングされます。

Info: MID 482 quarantined to "Policy" (message filter:policy_violation)

そのメッセージを隔離したメッセージ フィルタまたはアウトブレイク フィルタ機能のルールがかっこ内に出力されます。メッセージを格納する隔離ごとに個別のログエントリが生成されます。

また、隔離から削除されるメッセージも個別にロギングされます。

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

すべての隔離から削除されたメッセージが完全に削除されたり配信がスケジュールされたりすると、次のように個別にロギングされます。

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

メッセージが再注入されると、新しいメッセージID（MID）を持つ新しいメッセージオブジェクトが作成されます。これは、次のように新しい MID「by 行」がある既存のログ メッセージを使用してロギングされます。

Info: MID 483 rewritten to 513 by Policy Quarantine

メッセージ処理タスクの他のユーザへの割り当てについて

メッセージの処理および確認タスクを、他の管理者ユーザに割り当てることができます。次に例を示します。

- 人事部門ではポリシー隔離の確認と管理を行います。
- 法務部門では Confidential Material 隔離を管理します。

隔離の設定を指定するときに、これらの部門のユーザにアクセス権限を割り当てます。隔離のアクセス権限は、既存のユーザのみに割り当てることができます。

すべてまたは一部の隔離へのアクセスを付与したり、すべての隔離にアクセスできないようにしたりできます。隔離を閲覧するための権限が付与されていないユーザには、GUI または CLI の隔離リストにその隔離が表示されません。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定（1142 ページ）
- 管理タスクの分散 （1191 ページ）

ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザグループの指定

管理ユーザに隔離へのアクセスを許可した場合、実行できるアクションはそのユーザ グループにより異なります。

- 管理者グループのユーザは、隔離の作成、設定、削除、および集約ができ、隔離メッセージを管理できます。

- オペレータ、ゲスト、読み込み専用オペレータ、およびヘルプ デスク ユーザー グループに属するユーザーに加え、隔離管理権限を持つカスタム ユーザー ロールのユーザーは、隔離エリア内のメッセージの検索、閲覧および処理が可能ですが、隔離の設定変更、作成、削除、または集約はできません。各隔離にどのユーザがアクセスできるかを指定できます。
- Technicians グループに属するユーザは隔離にアクセスできません。

また、メッセージ トラッキングおよびデータ消失防止など、関連機能のアクセス権限により、[隔離（Quarantine）]ページに表示されるオプションおよび情報が異なります。たとえば、メッセージ トラッキングにアクセスできないユーザの場合、そのユーザにはメッセージ トラッキング リンクおよび、隔離されたメッセージに関する情報が表示されません。

エンドユーザは、ポリシー、ウイルス、およびアウトブレイク隔離を閲覧したりアクセスしたりすることはできません。

クラスタ設定におけるポリシー、ウイルス、およびアウトブレイク隔離について

ポリシー、ウイルス、およびアウトブレイク隔離は、中央集中型管理を使用した展開でマシンレベルでのみ設定できます。

ポリシー、ウイルス、アウトブレイク隔離の設定の集約方法

Cisco Secure Email and Web Manager 上でポリシー、ウイルス、およびアウトブレイク隔離を集約できます。詳細については、集約されたポリシー、ウイルス、およびアウトブレイク隔離（1564 ページ）を参照してください。

ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作

関連項目

- 隔離内のメッセージの表示 （1144 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの索 （1145 ページ）
- 隔離内のメッセージの手動処理 （1146 ページ）
- 複数の隔離内にあるメッセージ （1147 ページ）
- メッセージの詳細およびメッセージ内容の表示 （1148 ページ）
- 隔離されたメッセージの再スキャンについて （1151 ページ）
- アウトブレイク隔離 （1151 ページ）

隔離内のメッセージの表示

目的	操作手順
隔離のすべてのメッセージを表示する	（新しい Web インターフェイスのみ）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 [モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。 テーブル内の隔離の行で、[メッセージ（Messages）] 列の青い番号をクリックします。
アウトブレイク隔離エリアのメッセージを表示する	（新しい Web インターフェイス）[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）] を選択します。 [モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。 テーブル内の隔離の行で、[メッセージ（Messages）] 列の青い番号をクリックします。 [ルールサマリー管理（Manage by Rule Summary）] リンク （1152 ページ）。
隔離のメッセージのリスト表示を移動する	[前へ（Previous）]、[次へ（Next）]、ページ番号、または二重矢印のリンクをクリックします。二重矢印を使用すると、リストの先頭（[<<]）または最後（[>>]）のページに移動します。
隔離エリアのメッセージのリストをソートする	列見出しをクリックします（列に複数の項目が含まれる場合と [その他の隔離（In other quarantines）] 列を除く）。
テーブルの列サイズを変更する	列見出し間の境界線をドラッグします。
メッセージの隔離の原因となったコンテンツを表示する	一致した内容の表示 （1149 ページ） を参照してください。

関連項目

- 隔離されたメッセージおよび国際文字セット （1145 ページ）

隔離されたメッセージおよび国際文字セット

メッセージの件名に国際文字セット（2 バイト、可変長、および非 ASCII エンコーディング）の文字が含まれる場合、[ポリシー隔離（Policy Quarantine）] ページでは、非 ASCII 文字の件名行が復号されて表示されます。

ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの索

（注）
- ユーザは、アクセス権限が付与された隔離内のメッセージだけを検索および表示できます。
- ポリシー、ウイルスおよびアウトブレイク隔離の検索では、スパム隔離内のメッセージは見つかりません。

手順

ステップ 1 （新しい Web インターフェイスのみ）該当する隔離の青い番号のリンクをクリックします。

ヒント （新しい Web インターフェイスのみ）アウトブレイク隔離では、各アウトブレイクルールにより隔離されたすべてのメッセージを検索することもできます。アウトブレイク隔離で [ルールサマリー（Rule Summary）] タブをクリックして、関連するルールをクリックします。

ステップ 2 （新しい Web インターフェイスのみ）**[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [検索（Search）]** を選択します。

ステップ 3 （新しい Web インターフェイスのみ）該当する隔離の青い番号のリンクをクリックします。

ヒント （新しい Web インターフェイスのみ）アウトブレイク隔離では、各アウトブレイクルールにより隔離されたすべてのメッセージを検索することもできます。アウトブレイク隔離で [ルールサマリー（Rule Summary）] タブをクリックして、関連するルールをクリックします。

ステップ 4 **[モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]** を選択します。

ステップ 5 [隔離全体を検索（Search Across Quarantines）] ボタンをクリックします。

ヒント アウトブレイク隔離では、各アウトブレイク ルールにより隔離されたすべてのメッセージを検索することもできます。アウトブレイク テーブル行で [ルールサマリー管理（Manage by Rule Summary）] リンクをクリックします

ステップ 6 （任意）他の検索条件を入力します。

- [エンベロープ送信者（Envelope Sender）]および[エンベロープ受信者（Envelope Recipient）]には任意の文字を入力できます。エントリの検証は実行されません。
- 検索結果には、指定した条件のすべてに一致するメッセージだけが含まれます。たとえば、[エンベロープ受信者（Envelope Recipient）]および[件名（Subject）]を指定した場合は、[エンベロープ受信者（Envelope Recipient）]および[件名（Subject）]に指定した条件の両方に一致するメッセージだけが検索結果として表示されます。

次のタスク

これらの検索結果は、隔離のリストと同じように操作できます。詳細については、隔離内のメッセージの手動処理 （1146 ページ）を参照してください。

隔離内のメッセージの手動処理

手動でメッセージを処理する場合は、[メッセージアクション（Message Actions）]ページからメッセージ アクションを選択します。

メッセージに対し、次の処理を実行できます。

- 削除
- リリース
- 隔離からの予定していた終了の遅延
- 指定した電子メール アドレスへのメッセージのコピーの送信
- 別の隔離へのメッセージの移動

通常、以下の状況でリストのメッセージを処理できます。ただし、すべての状況ですべてのアクションが使用できるわけではありません。

- **[モニタ（Monitor）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）]**または（新しいWebインターフェイスのみ）**[隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [表示（View）]** ページの隔離のリストから、隔離内のメッセージ数をクリックします。
- [隔離全体を検索（Search Across Quarantines）]をクリックするとき。
- 隔離の名前をクリックし、隔離内を検索するとき。

複数のメッセージに同時にアクションを実行するには、次の操作を行います。

- メッセージ リストの上部の選択リストからオプションを選択する。
- ページの各メッセージの横のチェックボックスを選択する。

- メッセージリストの上部のテーブル見出しでチェックボックスを選択する。これにより、画面に表示されているすべてのメッセージにアクションが適用されます。他のページのメッセージは影響を受けません。

アウトブレイク隔離のメッセージのみに実行できるオプションもあります。を参照してください。

関連項目

- メッセージのコピーの送信 （1147 ページ）
- ポリシー隔離間のメッセージの移動について （1147 ページ）
- 複数の隔離内にあるメッセージ （1147 ページ）
- 隔離メッセージに自動的に適用されるデフォルト アクション （1135 ページ）

メッセージのコピーの送信

メッセージのコピーは、Administrators グループに属しているユーザだけが送信できます。

メッセージのコピーを送信するには、[コピーの送信先（Send Copy To）] フィールドに電子メール アドレスを入力し、[送信（Submit）] をクリックします。メッセージのコピーを送信しても、そのメッセージに対してその他のアクションが実行されることはありません。

ポリシー隔離間のメッセージの移動について

1 つの 電子メールゲートウェイ上で、1 つのポリシー隔離から別のポリシー隔離へ手動でメッセージを移動できます。

別の隔離にメッセージを移動する場合次のようになります。

- 有効期限は変更されません。メッセージには、元の隔離での保持期限が適用されます。
- 一致したコンテンツおよび他の関連情報を含め、メッセージの隔離理由は変更されません。
- あるメッセージが複数の隔離にあり、すでにメッセージのコピーを保持している場所にメッセージを移動した場合、移動したメッセージのコピーの有効期限および隔離の理由は、移動先の隔離エリアに元からあるメッセージのコピーを上書きします。

複数の隔離内にあるメッセージ

同じメッセージが複数の隔離内に格納されている場合、これらの隔離へのアクセス権限があるかどうかにかかわらず、隔離メッセージ リストの [その他の隔離（In other quarantines）] 列に [はい（Yes）] が表示されます。

複数の隔離内にメッセージが格納されている場合、以下の点に注意してください。

- すべての隔離からリリースされるまで、そのメッセージは配信されません。いずれかの隔離から削除されたメッセージは配信されなくなります。

- すべての隔離から削除またはリリースされるまで、そのメッセージはいずれの隔離からも削除されません。

複数の隔離内に格納されているメッセージをリリースする場合、それらのすべての隔離に対するアクセス権限が付与されていない場合があるため、次のルールが適用されます。

- すべての隔離からリリースされるまで、そのメッセージはリリースされません。
- いずれかの隔離内で削除済みとしてマークされると、他の隔離からも配信できなくなります（ただしリリースは可能です）。

メッセージが複数の隔離内にキューイングされ、ユーザがそのうちの1つまたは複数の隔離にアクセスできない場合は、次の処理が行われます。

- ユーザは、ユーザがアクセスできる各隔離についてそのメッセージが存在するかどうか通知されます。
- ユーザがアクセスできる隔離での保持期間の情報のみが GUI に表示されます（同じメッセージに対して、隔離ごとに別々の終了日時が存在します）。
- ユーザは、そのメッセージを保管している他の隔離の名前を知らされません。
- メッセージの隔離先にユーザがアクセスできない場合、その隔離理由は表示されません。
- ユーザがアクセスできるキューのメッセージのみリリースできます。
- ユーザがアクセスできない他の隔離にもメッセージがキューイングされている場合、それらの隔離にアクセスできるユーザによって処理されるまで（あるいは早期または通常の期限切れによって「正常に」メッセージがリリースされるまで）、そのメッセージは変更されずに隔離内に残ります。

メッセージの詳細およびメッセージ内容の表示

メッセージの内容を表示したり、[隔離されたメッセージ（Quarantined Message）] ページにアクセスしたりするには、メッセージの件名行をクリックします。

[隔離されたメッセージ（Quarantined Message）]ページには、[隔離の詳細（Quarantine Details）] と [メッセージの詳細（Message Details）] の 2 つのセクションがあります。

[隔離されたメッセージ（Quarantined Message）]ページから、メッセージを読んだり、メッセージアクションを選択したり、メッセージのコピーを送信したりウイルス検査を実行したりできます。また、メッセージが隔離エリアから解放されるときに Encrypt on Delivery フィルタ アクションによって暗号化されるかどうかを確認することもできます。

[メッセージの詳細（Message Details）] セクションには、メッセージ本文、メッセージ ヘッダー、および添付ファイルが表示されます。メッセージ本文は最初の 100 K だけが表示されます。メッセージがそれよりも長い場合は、最初の 100 K が表示され、その後に省略記号（...）が続きます。実際のメッセージが切り捨てられることはありません。この処置は表示目的のためだけに行われます。[メッセージの詳細（Message Details）] の下部にある [メッセージ部分（Message Parts）] セクション内の [message body] をクリックすることにより、メッセージ本文をダウンロードできます。また、添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードすることもできます。

ウイルスの含まれるメッセージを表示する場合、ご使用のコンピュータにデスクトップアンチウイルス ソフトウェアがインストールされていると、そのアンチウイルス ソフトウェアから、

ウイルスが検出されたと警告される場合があります。これは、ご使用のコンピュータに対して脅威ではないため、無視しても問題ありません。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング（Message Tracking）] リンクをクリックします。

（注） 特別な Outbreak 検疫の場合、追加の機能を利用できます。アウトブレイク隔離 （1151 ページ） を参照してください。

関連項目

- 一致した内容の表示 （1149 ページ）
- 添付ファイルのダウンロード （1150 ページ）
- ウイルス テスト （1150 ページ）

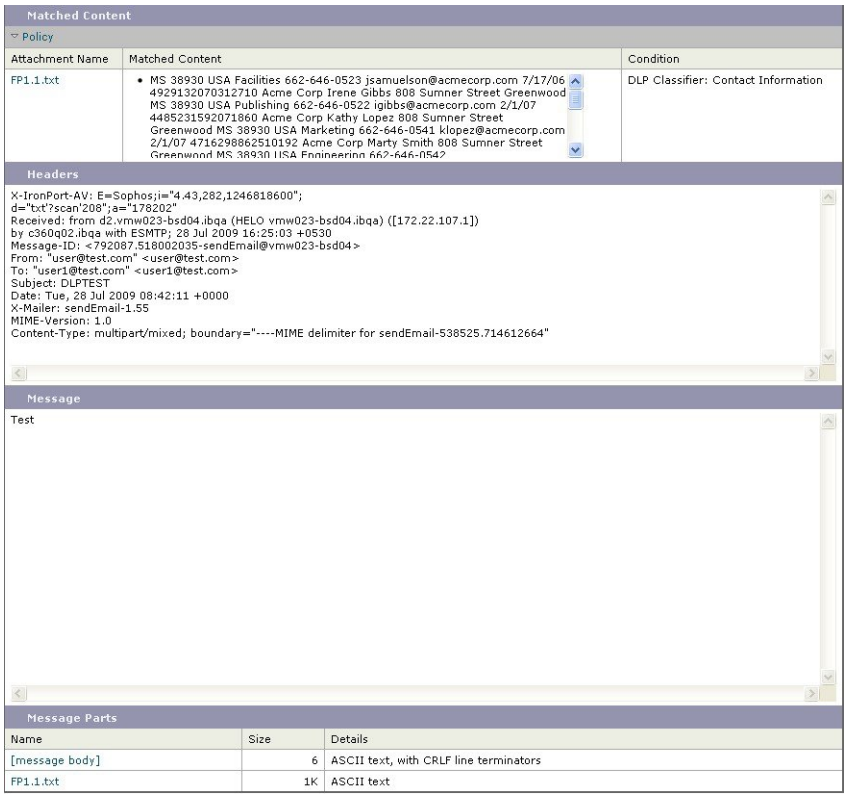
一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して検疫アクションを設定した場合、検疫されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致を除き、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、メッセージの一致した内容やコンテンツ フィルタの一致をメッセージの件名に含めることもできます。

一致した内容が添付ファイルに含まれる場合は、その判定結果が DLP ポリシー違反、コンテンツ フィルタ条件、メッセージ フィルタ条件、または画像解析のいずれによるものかに関係なく、添付ファイルの内容がその隔離理由と共に表示されます。

メッセージフィルタまたはコンテンツ フィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタ アクションをトリガーした内容と共に）GUI で表示されることがあります。GUI の表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。これは、GUI で使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールと共に一覧表示するテーブルは正しく表示されます。

図 *71 : Policy* 検疫エリア内で表示された一致内容



添付ファイルのダウンロード

[メッセージ部分（Message Parts）] または [一致した内容（Matched Content）] セクション内の添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードできます。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。ウイルスが含まれる可能性がある添付ファイルは、ユーザ自身の自己責任においてダウンロードしてください。[メッセージ部分（Message Parts）] セクション内の [メッセージ本文（message body）] をクリックすることにより、メッセージ本文をダウンロードすることもできます。

ウイルス テスト

メッセージがウイルスに感染していないかどうかを検査するには、[テスト開始（Start Test）] をクリックします。アンチウイルス シグニチャが最新のものであることを確認できるまで、メッセージの保管に隔離を使用します。

ウイルスの検査では、オリジナルのメッセージではなく、メッセージのコピーがアンチウイルス エンジンに送信されます。アンチウイルス エンジンの判定結果は、[隔離（Quarantines）] エリアの上に表示されます。

隔離されたメッセージの再スキャンについて

隔離されたすべてのキューからメッセージが解放されるとき、電子メールゲートウェイおよび最初にメッセージを隔離したメールポリシーで有効化されている機能によって、次の再スキャンが発生します。

- ポリシーおよびウイルス隔離から解放されるメッセージはアンチウイルス、高度なマルウェア防御、グレイメール エンジンによって再スキャンされます。
- アウトブレイク隔離から解放されたメッセージは、アンチスパム、AMP、およびアンチウイルスエンジンによって再スキャンされます。（アウトブレイク隔離中のメッセージの再スキャンの詳細については、を参照してください。）
- ファイル分析隔離から解放されるメッセージは、脅威に対する再スキャンが実行されます。
- 添付ファイルを含むメッセージは、ポリシー、ウイルス、およびアウトブレイク隔離から解放されるときにファイル レピュテーション サービスによって再スキャンされます。

再スキャン時に、判定結果が前回そのメッセージを処理したときの判定結果と一致する場合、そのメッセージは再隔離されません。逆に、判定が異なると、そのメッセージは別の隔離に送信される可能性があります。

原理的に、メッセージの検疫が無限に繰り返されることはないようになっています。たとえば、メッセージが暗号化されていて、その結果、Virus 検疫に送信されるとします。管理者がそのメッセージを解放しても、アンチウイルスエンジンはまだそのメッセージを復号化できません。しかし、そのメッセージは再隔離されない必要があります。再隔離されるとループ状態となり、そのメッセージは隔離からまったく解放されなくなります。2 回とも判定は同じ結果になるので、システムは 2 回めには Virus 検疫を無視します。

アウトブレイク隔離

Outbreak 検疫は、Outbreak フィルタ機能の有効なライセンス キーが入力されている場合に存在します。Outbreak フィルタ機能では、しきい値セットに従ってメッセージが Outbreak 検疫に送信されます。詳細については、を参照してください。

アウトブレイク隔離は、他の隔離と同様の機能を持ち、メッセージを検索したり、メッセージを解放または削除したりなどできます。

- 標準（Standard）
- ルールのサマリー

アウトブレイク隔離には、他の隔離では使用できない追加の機能があります（[ルールサマリーによる管理（Manage by Rule Summary）] リンク、メッセージの詳細を表示しているときのシスコへの送信機能、およびスケジュールされた保存期間の終了日時で検索結果内のメッセージを並べ替えるオプション）。

アウトブレイク フィルタ機能のライセンスの有効期限が切れると、メッセージをアウトブレイク隔離にそれ以上追加できなくなります。隔離エリア内に現在存在するメッセージの保存期間

が終了してアウトブレイク隔離が空になると、GUI の隔離リストに アウトブレイク隔離は表示されなくなります。

関連項目

- アウトブレイク隔離のメッセージの再スキャン （1152 ページ）
- [ルール サマリー管理（Manage by Rule Summary）] リンク （1152 ページ）
- シスコへの偽陽性または不審なメッセージの報告 （1152 ページ）

アウトブレイク隔離のメッセージの再スキャン

アウトブレイク隔離に入れられたメッセージは、新しく公開されたルールによってもう脅威ではないと見なされると、自動的に解放されます。

電子メールゲートウェイ上でアンチスパムおよびアンチウイルスがイネーブルになっている場合、スキャンエンジンは、メッセージに適用されるメールフローポリシーに基づいて、アウトブレイク隔離から解放されたすべてのメッセージをスキャンします。

[ルール サマリー管理（Manage by Rule Summary）] リンク

検疫リストで Outbreak 検疫の横にある [ルール概要による管理（Manage by Rule Summary）] リンクをクリックして、[ルール概要による管理（Manage by Rule Summary）] ページを表示します。検疫エリア内のすべてのメッセージに対し、それらのメッセージを検疫させた感染防止ルールに基づいてメッセージアクション（Release、Delete、Delay Exit）を実行できます。これは、アウトブレイク隔離から多数のメッセージを片付ける場合に適しています。詳細については、「[アウトブレイク隔離（Outbreak Quarantine）]および[ルールサマリーによる管理（Manage by Rule Summary）] ビュー」に記載のトピック を参照してください。

シスコへの偽陽性または不審なメッセージの報告

アウトブレイク隔離内のメッセージについてメッセージの詳細を表示しているとき、偽陽性または不審なメッセージを報告するためにそのメッセージをシスコへ送信できます。

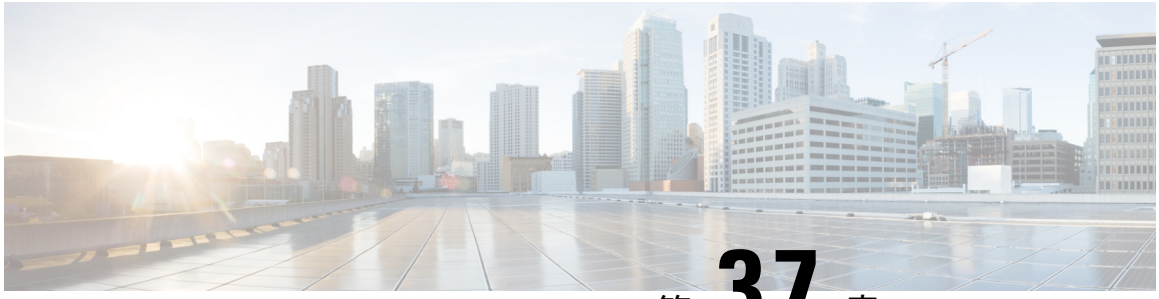
手順

ステップ 1 アウトブレイク隔離内のメッセージの移動

ステップ 2 [メッセージの詳細（Message Details）] セクションで、[シスコにコピーを送信する（Send a Copy to Cisco Systems）] チェックボックスを選択します。

ステップ 3 新しい Web インターフェイスで、テーブルのアウトブレイク フィルタ エントリの [メッセージ（Message）] 列にある青色の番号をクリックし、メッセージのチェック ボックスをオンにして、[コピーの送信（Send a Copy）] を選択します。

ステップ 4 受信者のアドレスを入力し、**[送信（Send）]** をクリックします。



第 37 章

スパム隔離

この章は、次の項で構成されています。

- スパム隔離の概要 （1153 ページ）
- ローカルのスパム隔離と外部のスパム隔離 （1154 ページ）
- ローカルのスパム隔離の設定 （1154 ページ）
- セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御 （1161 ページ）
- エンドユーザのためのスパム管理機能の設定 （1174 ページ）
- スパム隔離内のメッセージの管理 （1185 ページ）
- スパム隔離のディスク領域 （1188 ページ）
- 外部スパム隔離の無効化について （1188 ページ）
- スパム隔離機能のトラブルシューティング （1189 ページ）

スパム隔離の概要

スパム隔離（別名 ISQ）およびエンドユーザ隔離（別名 EUQ）は、「誤検出」（電子メールゲートウェイが正規の電子メールメッセージをスパムと見なすこと）が問題とされる組織でのセーフガードメカニズムとなります。メッセージがスパムである、またはスパムの疑いがあると電子メールゲートウェイが判断した場合、メッセージを配信または削除する前に、受信者または管理者にそのメッセージを確認してもらうことができます。スパム隔離はこのためにメッセージを保存します。

電子メールゲートウェイの管理ユーザは、スパム隔離内のすべてのメッセージを閲覧できます。エンドユーザー（通常はメッセージの受信者）は、そのユーザー宛の隔離されたメッセージを、若干異なる Web インターフェイスで表示できます。

スパム隔離は、ポリシー、ウイルス、アウトブレイク隔離とは異なります。

関連項目

- スパムおよびグレイメールの管理 （461 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離 （1129 ページ）

ローカルのスパム隔離と外部のスパム隔離

ローカルのスパム隔離では、電子メールゲートウェイでスパムおよびスパムの疑いがあるメッセージなどを保存します。外部のスパム隔離は、別の Cisco Secure Email and Web Manager でこれらのメッセージを保存できます。

次の場合は外部のスパム隔離の使用を検討してください。

- 複数の電子メールゲートウェイからのスパムを集約して保存および管理する必要がある。
- 電子メールゲートウェイで保持可能な量より多くのスパムを保存する必要がある。
- スパム隔離とそのメッセージを定期的にバックアップする必要がある。

関連項目

- スパム隔離のディスク領域 （1188 ページ）
- 外部スパム隔離の操作 （1560 ページ）

ローカルのスパム隔離の設定

次の表 は、メッセージをスパム隔離に送信する方法を示しています

手順

	コマンドまたはアクション	目的
ステップ 1	まだ実行していない場合はアンチスパム機能を有効にします。	詳細については、スパムおよびグレイメールの管理 （461 ページ）を参照してください。
ステップ 2	隔離設定を有効にし、設定を行います。	詳細については、レガシー Web インターフェイスでのスパム隔離の有効化と設定 （1155 ページ）を参照してください。
ステップ 3	スパム隔離に割り当てられたディスク領域を調整します。	詳細については、ディスク領域の管理 （1249 ページ）を参照してください。
ステップ 4	隔離へのブラウザ アクセスを有効にします。	詳細については、スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定 （1157ページ）を参照してください。
ステップ 5	スパムを隔離に送信するように電子メールゲートウェイを設定します。	詳細については、次を参照してください。 • スパムを隔離するためのメール ポリシーの設定 （1159 ページ） • 隔離対象のメールの受信者の制限 （1159 ページ）

	コマンドまたはアクション	目的
ステップ 6	見出しに文字エンコーディングの情報がないメッセージのデフォルトの文字エンコーディングを指定します。	詳細については、メッセージ テキストが正しく表示されることの確認 （1160 ページ）を参照してください。

次のタスク

関連項目

- スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定 （1157 ページ）
- スパム隔離への管理ユーザ アクセスの設定 （1158 ページ）
- スパムを隔離するためのメール ポリシーの設定 （1159 ページ）
- 隔離対象のメールの受信者の制限 （1159 ページ）
- メッセージ テキストが正しく表示されることの確認 （1160 ページ）
- スパム隔離の言語 （1161 ページ）

レガシー Web インターフェイスでのスパム隔離の有効化と設定

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] >[スパム隔離（Spam Quarantine）] を選択します。

ステップ 3 事前にスパム隔離を有効にしていない場合は、[スパム隔離を有効にする（Enable Spam Quarantine）] を選択します。

スパム隔離の設定を編集する場合は、 [スパム隔離（Spam Quarantine）] セクションの [隔離名（Quarantine Name）] カラムにある [スパム隔離（Spam Quarantine）] リンクをクリックします。

ステップ 4 次のオプションを指定します。

オプション	説明
[次を使用してメッセージを配信（Deliver Messages Via）]	隔離関係のすべての送信電子メール（スパム通知やスパム隔離からリリースされたメッセージなど）は、メッセージ送信が設定されている他の 電子メールゲートウェイまたはサーバを経由して配信する必要があります。 これらのメッセージは、SMTP またはグループウェアサーバを使用してルーティングできます。また、 電子メールゲートウェイの発信リスナーインターフェイス（通常は Data 2 インターフェイス）を指定することもできます。 代替用アドレスは、ロードバランシングとフェールオーバーに使用します。 電子メールゲートウェイが複数台ある場合は、管理対象となる任意の電子メールゲートウェイの発信リスナーインターフェイスをプライマリアドレスまたは代替用アドレスとして使用できます。これらはいずれも同じインターフェイス（Data 1 または Data 2）を発信リスナーとして使用する必要があります。 これらのアドレスについての他の注意事項を画面で確認してください。
次の日数の経過後に削除（Schedule Delete After）	メッセージを削除する前に保持する日数を指定します。 隔離エリアの容量が満杯になるのを防ぐために、古いメッセージから削除するように隔離を設定することを推奨します。自動削除をスケジュールしないという選択も可能です。
[メッセージのリリース時にCiscoに通知（Notify Cisco Upon Message Release）]	メッセージのリリース時にシスコに通知する場合は、[**Send a copy of released messages To cisco for analysis (推奨)**] チェックボックスをオンにします。

オプション	説明
[スパム隔離のアピアランス（Spam Quarantine Appearance）]	**ロゴ（Logo）** デフォルトでは、ユーザがログインして隔離されたメッセージを確認するときに、スパム隔離のページの最上部にシスコ ロゴが表示されます。 代わりにカスタム ロゴを使用するには、そのロゴをアップロードします。ロゴは、高さ 50 ピクセル、幅 500 ピクセルまでの .jpg、.gif、または .png ファイルにする必要があります。
	ログイン ページ メッセージ（Login page message） （任意）ログイン ページ メッセージを指定します。このメッセージは、隔離を閲覧するためにエンド ユーザおよび管理者がログインするときに表示されます。 メッセージを指定しない場合、次のメッセージが表示されます。 ログイン情報を入力してください。入力する情報がわからない場合は、管理者に問い合わせてください。（Enter your login information below. If you are unsure what to enter, please contact your administrator.）
管理ユーザ（Administrative Users）	スパム隔離への管理ユーザアクセスの設定 （1158ページ）を参照してください。

ステップ 5 変更を送信し、保存します。

次のタスク

- ローカルのスパム隔離の設定 （1154 ページ）に戻ります。

スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定

管理者およびエンド ユーザがスパム隔離にアクセスするときには、別のブラウザ ウィンドウが開きます。

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] を選択します。

ステップ 3 インターフェイス名をクリックします（この例では、管理インターフェイスを使用します）。

ステップ 4 [スパム隔離（Spam Quarantine）] セクションで、スパム隔離にアクセスするための設定を行います。

- デフォルトでは、HTTP がポート 82 を使用し、HTTPS がポート 83 を使用します。
- 通知とスパム隔離のブラウザ ウィンドウに記載される URL を指定します。

  使用している Cisco Secure Email and Web Manager のホスト名をエンドユーザに表示したくない場合は、代わりのホスト名を指定できます。

ステップ 5 変更を送信し、保存します。

次のタスク

スパム隔離アクセス用に指定したホスト名を DNS サーバが解決できることを確認します。

スパム隔離への管理ユーザ アクセスの設定

管理者権限を持つすべてのユーザは、スパム隔離設定を変更したり、スパム隔離内のメッセージを表示および管理したりすることができます。管理者ユーザに対してスパム隔離アクセスを設定する必要はありません。

次のロールのユーザに対してスパム隔離へのアクセスを設定すると、これらのユーザはスパム隔離内のメッセージを表示、リリース、削除できます。

- 演算子
- Read-Only Operator
- Help desk user
- ゲスト
- スパム隔離権限を持つカスタム ユーザー ロール

これらのユーザはスパム隔離設定にアクセスできません。

始める前に

スパム隔離にアクセスできるユーザーまたはカスタム ユーザー ロールを作成します。詳細については、管理タスクの分散 （1191 ページ） を参照してください。

手順

ステップ 1 Cisco Secure Email and Web Manager で、[サービスステータス（Service Status）] をクリックし、[スパム隔離（Spam Quarantine）] に対応する にカーソルを合わせて、[スパム隔離設定の編集（Edit Spam Quarantine Settings）] をクリックします。

ステップ 2 トグルスイッチをクリックしてスパム隔離を有効にします。

ステップ 3 追加するユーザ タイプ（ローカル、外部認証、またはカスタム ロール）のリンクをクリックします。

ユーザまたはロールを追加済みの場合は、ユーザ名かロールをクリックすると、すべての対象ユーザまたはロールが表示されます。

ステップ 4 追加するユーザまたはロールを選択します。

管理者権限を持つユーザは、スパム隔離へのフルアクセスが自動的に与えられるため、表示されません。

ステップ 5 [OK] をクリックします。

ステップ 6 **[送信（Submit）]** をクリックします。

次のタスク

関連項目

スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）

スパムを隔離するためのメール ポリシーの設定

スパム隔離を有効にした後、スパムまたはスパムの疑いのあるメッセージをその隔離に送信するように、メールポリシーを設定できます。メールがスパム隔離に送信されるように、メールポリシーでアンチスパム スキャンを有効にする必要があります。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policies）] ページで、対応するメール ポリシーの [スパム対策（Anti-Spam）] カラムにあるリンクをクリックします。

ステップ 2 [スパム対策設定（Anti-Spam Settings）] セクションで、[IronPortスパム対策サービスを使用（Use IronPort Anti-Spam service）] を選択します。

ステップ 3 [ポジティブスパムの設定（Positively-Identified Spam Settings）] セクションで、[このアクションをメッセージに適用する（Apply This Action to Message）] オプションに [スパム隔離（Spam Quarantine）] を選択します。

ステップ 4 スパムの疑いのあるメッセージおよびマーケティング電子メールに対しても設定します。

ステップ 5 変更を送信し、保存します。

隔離対象のメールの受信者の制限

電子メールゲートウェイで複数のメールポリシーを使用して（[メールポリシー（Mail Policies）]>[受信メールポリシー（Incoming Mail Policy）]）、メールの隔離対象から除外する受信者アド

レスのリストを指定できます。そのメールポリシーにアンチスパムを設定する際、隔離の代わりに [配信（Deliver）] または [ドロップ（Drop）] を選択します。

メッセージ テキストが正しく表示されることの確認

AsyncOS では、メッセージ ヘッダーに指定されたエンコーディングに基づいてメッセージの文字セットが決定されます。しかし、ヘッダーに指定されたエンコーディングが実際のテキストと一致していないと、そのメッセージは、スパム隔離内で閲覧される際に正しく表示されません。このような状況は、スパム メッセージの場合に発生することがよくあります。

これらのメッセージに対してメッセージのテキストが正しく表示されることを確認するには、を参照してください。

関連項目

- デフォルト エンコーディングの指定 （1160 ページ）

デフォルト エンコーディングの指定

着信メッセージのヘッダーに文字セットのエンコーディングが指定されていない場合に、デフォルトエンコーディングを指定するように電子メールゲートウェイを設定できます。

そうすることにより、そのようなメッセージをスパム隔離内で正しく表示するのに役立ちます。ただし、デフォルトエンコーディングを指定すると、他の文字セットのメッセージが正しく表示されなくなる可能性があります。この設定は、メッセージヘッダーにエンコーディングが指定されていないメッセージに対してのみ適用されます。一般に、このカテゴリに入るメールの多くが 1 つの特定のエンコーディングになると予測される場合にだけ、デフォルト エンコーディングを設定します。

たとえば、隔離されるメッセージのうち、メッセージヘッダーに文字セットのエンコーディングが指定されていないものの多くが日本語（ISO-2022-JP）である場合は、[スキャン動作（Scan Behavior）] ページのエンコーディングを [日本語（ISO-2022-JP）（Japanese (ISO-2022-JP)）] として設定できます。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [スキャン動作（Scan Behavior）] をクリックします。

ステップ 2 [グローバル設定（Global Settings）] で [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [何も指定されていないときに使用する符号化（Encoding to use when none is specified）] ドロップダウン リストから目的のエンコーディング タイプを選択します。

ステップ 4 **[送信（Submit）]** をクリックします。

ステップ 5 [変更を確定（Commit Changes）] をクリックします。

スパム隔離の言語

各ユーザは、ウィンドウの右上にある [オプション（Options）] メニューからスパム隔離の言語を選択します。

セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御

管理者およびエンドユーザは、メッセージがスパムであるかどうかを判断するためにセーフリストとブロックリストを使用できます。セーフリストでは、スパムとして処理しない送信者およびドメインが指定されます。ブロックリストでは、常にスパムとして処理する送信者およびドメインが指定されます。

エンド ユーザー（電子メール ユーザー）に各自の電子メール アカウントのセーフリストとブロックリストの管理を許可することができます。たとえば、エンドユーザは、もう興味のないメーリングリストから電子メールを受信している場合があります。そのようなユーザは、このメーリングリストからの電子メールが自分の受信箱に送信されないように、その送信者を自分のブロックリストに追加できます。また、エンドユーザは、スパムではない特定の送信者からの電子メールが自分のスパム隔離に送信されていることに気づくこともあります。これらの送信者からのメッセージが隔離されないようにするために、エンドユーザはそれらの送信者を自分のセーフリストに追加できます。

エンド ユーザおよび管理者が行った変更はお互いに表示され、両者が変更できます。

関連項目

- セーフリストとブロックリストのメッセージ処理 （1161 ページ）
- レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 （1162 ページ）
- 外部スパム隔離およびセーフリスト/ブロックリスト （1163 ページ）
- セーフリストおよびブロックリストへの送信者とドメインの追加（管理者） （1164 ページ）
- セーフリストおよびブロックリストへのエンドユーザ アクセスについて （1170 ページ）
- 複数の 電子メールゲートウェイ（ Cisco Secure Email and Web Manager を使用しない展開）でのセーフリストまたはブロックリストの同期 （1172 ページ）
- セーフリスト/ブロックリストのバックアップと復元 （1173 ページ）
- セーフリストとブロックリストのトラブルシューティング （1174 ページ）

セーフリストとブロックリストのメッセージ処理

セーフリストまたはブロックリストに送信者を追加しても、電子メールゲートウェイではメッセージに対するウイルスのスキャンや、内容に関連したメールポリシーの基準をメッセージが満たすかどうかの判定が行われます。受信者のセーフリストにメッセージの送信者が含まれていても、他のスキャン設定と結果によってはメッセージが配信されない場合があります。

セーフリストとブロックリストを有効にすると、電子メールゲートウェイは、アンチスパムスキャンの直前にセーフリスト/ブロックリスト データベースと照合してメッセージをスキャンします。電子メールゲートウェイがセーフリストまたはブロックリストのエントリに一致する送信者またはドメインを検出した場合、受信者が複数存在すると（かつ各受信者のセーフリスト/ブロックリスト設定が異なると）、そのメッセージは分裂します。たとえば、受信者 A と受信者 B の両方に送信されるメッセージがあるとします。受信者 A のセーフリストにはこの送信者のエントリがありますが、受信者 B のセーフリストおよびブロックリストにはエントリがありません。この場合、メッセージは 2 つのメッセージ ID で 2 つのメッセージに分割されます。受信者 A に送信されるメッセージは、セーフリストに一致していることが X-SLBL-Result-セーフリスト ヘッダーによってマークされ、アンチスパム スキャンをスキップします。一方、受信者 B 宛のメッセージは、アンチスパム スキャン エンジンによってスキャンされます。その後、どちらのメッセージもパイプライン（アンチウイルス スキャン、コンテンツ ポリシーなど）を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合の配信の動作は、セーフリスト/ブロックリスト機能を有効にするときに指定したブロックリスト アクションによって決まります。セーフリストの配信の場合と同様に、セーフリスト/ブロックリスト設定の異なる複数の受信者が存在すると、そのメッセージは分裂します。分裂したメッセージのうちブロックリストに含まれるものは、ブロックリストアクション設定に応じて隔離されるかドロップされます。隔離を実行するようにブロックリスト アクションが設定されている場合、そのメッセージはスキャンされ、最終的に隔離されます。削除するようにブロックリストアクションが設定されている場合、そのメッセージは、セーフリスト/ブロックリスト スキャンの直後にドロップされます。

セーフリストとブロックリストはスパム隔離内に保持されているため、配信の動作は、他のアンチスパム設定にも左右されます。たとえば、アンチスパム スキャンをスキップするようにホスト アクセス テーブル（HAT）で「承認（Accept）」メール フロー ポリシーを設定すると、そのリスナー上でメールを受信するユーザは、自分のセーフリストとブロックリストの設定がそのリスナー上で受信されたメールに適用されなくなります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメール フロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

関連項目

- レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 （1162 ページ）
- 外部スパム隔離およびセーフリスト/ブロックリスト （1163 ページ）

レガシーWebインターフェイスでのセーフリストとブロックリストの有効化

始める前に

- スパム隔離を有効にする必要があります。「ローカルのスパム隔離の設定 （1154ページ）」を参照してください。

- 外部セーフリスト/ブロックリストを使用するように 電子メールゲートウェイを設定します。お使いの電子メールゲートウェイのマニュアルで外部スパム隔離を設定する手順を参照してください。

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] >[スパム隔離（Spam Quarantine）] に移動します。

ステップ 3 [エンドユーザセーフリスト/ブロックリスト（End-User Safelist/Blocklist）] の下にある [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [エンドユーザセーフリスト/ブロックリスト機能を有効にする（Enable End User Safelist/Blocklist Feature）] を選択します。

ステップ 5 [ブロックリストアクション（Blocklist Action）] に [隔離（Quarantine）] または [削除（Delete）] を選択します。

ステップ 6 [ユーザごとの最大リスト項目数（Maximum List Items Per User）] を指定します。

これは、各受信者のリストごとのアドレスまたはドメインの最大数です。ユーザごとのリストエントリ数を大きくすると、システムのパフォーマンスに悪影響を与えることがあります。

ステップ 7 [更新頻度（Update Frequency）] を選択します。

この値によって、外部スパム隔離を使用する電子メールゲートウェイのセーフリスト/ブロックリストを AsyncOS が更新する頻度が決まります。この設定の意味については、外部スパム隔離およびセーフリスト/ブロックリスト （1163 ページ）で説明します。

ステップ 8 更新頻度を選択します。この値によって、外部スパム隔離を使用する電子メールゲートウェイのセーフリスト/ブロックリストを AsyncOS が更新する頻度が決まります。この設定の意味については、外部スパム隔離およびセーフリスト/ブロックリスト （1163 ページ）で説明します。

ステップ 9 変更を送信し、保存します。

外部スパム隔離およびセーフリスト/ブロックリスト

Cisco Secure Email and Web Manager で外部スパム隔離を使用する場合、セーフリスト/ブロックリストはその管理アプライアンスに保存されます。これにより、すべてのアプライアンスを対象に安全な送信者とブロックされた送信者を一か所で管理できます。

電子メールゲートウェイは受信メールの処理時にセーフリストとブロックリスト内の送信者を評価するため、Cisco Secure Email and Web Manager に保存されているセーフリストおよびブロックリストが受信メールに適用されるように、これらを電子メールゲートウェイに送信する必要があります。 Cisco Secure Email and Web Manager でセーフリスト/ブロックリスト機能を設定する際に、その更新頻度を設定します。

Cisco Secure Email and Web Manager での外部セーフリストおよびブロックリストの操作の詳細については、『*Cisco Secure Email and Web Manager User Guide*』のトピックを参照してください

セーフリストおよびブロックリストへの送信者とドメインの追加（管理者）

スパム隔離のインターフェイスでセーフリストとブロックリストを管理します。

多数の受信者（組織のエンドユーザー）が特定の送信者またはドメインを許可リストまたはブロックリストに含めているかどうかも確認できます。

管理者は、各エンドユーザが表示および操作する同じエントリのスーパーセットを表示して操作します。

始める前に

- スパム隔離にアクセスできることを確認します。スパム隔離へのアクセス（管理ユーザ）（1186 ページ）を参照してください。
- セーフリスト/ブロックリストへのアクセスを有効にします。レガシー Web インターフェイスでのセーフリストとブロックリストの有効化 （1162 ページ）を参照してください。
- （任意）このセクションの手順を使用してこれらのリストを作成する代わりに、セーフリスト/ブロックリストをインポートするには、セーフリスト/ブロックリストのバックアップと復元 （1173 ページ）で説明する手順を使用します。
- セーフリストとブロックリストのエントリの必須形式を把握します。セーフリストエントリとブロックリスト エントリの構文 （1169 ページ）を参照してください。

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで、[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）] をクリックします。

または

[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] を選択し、ページの右上隅にある **[オプション（Options）]** ドロップダウン メニューを選択します。

ステップ 2 [セーフリスト（Safelist）] または [ブロックリスト（Blocklist）] を選択します。

ステップ 3 （任意）送信者または受信者を検索します。

ステップ 4 次の 1 つまたは複数の操作を実行します。

目的	操作手順
1 人の受信者に対して複数の送信者を追加する	新しい Web インターフェイスで 1 人の受信者に複数の送信者を追加する場合 **1.** [受信者（Recipients）] タブを選択します。 **2.** +アイコンをクリックして、受信者のアドレスと送信者リストを追加します。 **3.** 受信者の電子メール アドレスを入力します。 **4.** 送信者の電子メール アドレスとドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 **5.** ✓ をクリックしてエントリを保存します。 既存の送信者アドレスを変更するには、必要な受信者アドレスの横にあるチェックボックスをオンにして編集アイコンをクリックし、送信者のアドレスを変更してから ✓ をクリックしてエントリを保存します。 レガシー Web インターフェイスで 1 人の受信者に複数の送信者を追加する場合 **1.** [表示方法：受信者（View by: Recipient）] を選択します。 **2.** [追加（Add）] をクリックするか、受信者の [編集（Edit）] をクリックします。 **3.** 受信者の電子メール アドレスを入力または編集します。 **4.** 送信者の電子メール アドレスおよびドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 **5.** **[送信（Submit）]** をクリックします。

目的	操作手順
1 人の送信者に対して複数の受信者を追加する	新しい Web インターフェイスで 1 人の送信者に複数の受信者を追加する場合 **1.** [送信者（Sender）] タブを選択します。 **2.** +をクリックして、送信者のアドレスと受信者リストを追加します。 **3.** 送信者のアドレスまたはドメインを入力します。 **4.** 受信者の電子メール アドレスを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 **5.** ✓ をクリックしてエントリを保存します。 既存の受信者アドレスを変更するには、必要な送信者アドレスの横にあるチェックボックスをオンにして編集アイコンをクリックし、送信者のアドレスを変更してから ✓ をクリックしてエントリを保存します。 レガシー Web インターフェイスで 1 人の送信者に複数の受信者を追加する場合 **1.** [表示方法：送信者（View by: Sender）] を選択します。 **2.** [追加（Add）] をクリックするか、または送信者の [編集（Edit）] をクリックします。 **3.** 送信者アドレスまたはドメインを入力または編集します。 **4.** 受信者の電子メール アドレスを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。 **5.** **[送信（Submit）]** をクリックします。

目的	操作手順
受信者に関連付けられたすべての送信者を削除する	新しい Web インターフェイスで 1 人の受信者に関連付けられたすべての送信者を削除する場合 **1.** 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 すべてのエントリを選択し、削除することができます。 **2.** ごみ箱アイコンをクリックしてテーブル行全体を削除できます。 レガシー Web インターフェイスで 1 人の受信者に関連付けられたすべての送信者を削除する場合 **1.** [表示方法（View by）] オプションを選択します。 **2.** ゴミ箱アイコンをクリックしてテーブル行全体を削除します。
送信者に関連付けられたすべての受信者を削除する	新しい Web インターフェイスで 1 人の送信者に関連付けられたすべての受信者を削除する場合 **1.** 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 すべてのエントリを選択し、削除することができます。 **2.** ごみ箱アイコンをクリックしてテーブル行全体を削除できます。 レガシー Web インターフェイスで 1 人の送信者に関連付けられたすべての受信者を削除する場合 **1.** [表示方法（View by）] オプションを選択します。 **2.** ゴミ箱アイコンをクリックしてテーブル行全体を削除します。

目的	操作手順
受信者の個々の送信者を削除する	新しい Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合 **1.** 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 複数のエントリを選択、削除することができます。 **2.** 編集アイコンをクリックして、個々の受信者または送信者を変更します。 **3.** テキスト ボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 **4.** ✓ をクリックしてエントリを保存します。 レガシー Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合 **1.** [表示方法（View by）] オプションを選択します。 **2.** 個々の受信者または送信者の [編集（Edit）] をクリックします。 **3.** テキスト ボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 **4.** **[送信（Submit）]** をクリックします。

目的	操作手順
送信者の個々の受信者を削除する	新しい Web インターフェイスで 1 人の送信者の個々の受信者を削除する場合 1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 複数のエントリを選択、削除することができます。 2. 編集アイコンをクリックして、個々の受信者または送信者を変更します。 3. テキスト ボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. ✓ をクリックしてエントリを保存します。 レガシー Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合 1. [表示方法（View by）] オプションを選択します。 2. 個々の受信者または送信者の [編集（Edit）] をクリックします。 3. テキスト ボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。 4. **[送信（Submit）]** をクリックします。

次のタスク

関連項目

- セーフリスト エントリとブロックリスト エントリの構文 （1169 ページ）
- すべてのセーフリストおよびブロックリストのクリア （1170 ページ）

セーフリスト エントリとブロックリスト エントリの構文

送信者を次の形式でセーフリストとブロックリストに追加できます。

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]

- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

送信者アドレスやドメインなどの同一エントリを、セーフリストとブロックリストの両方に同時に追加することはできません。ただし、ドメインをセーフリストに追加し、そのドメインに所属する送信者の電子メールアドレスをブロックリストに追加すること(またはその逆)は可能です。両方のルールが適用されます。たとえば *example.com* がセーフリストに含まれている場合、*george@example.com* をブロックリストに追加することができます。この場合、電子メールゲートウェイは、スパムとして処理される *george@example.com* からのメールを除いて、*example.com* からのすべてのメールをスパムのスキャンなしで配信します。

.domain.com のような構文を使用して、サブドメインの範囲を許可したり、ブロックしたりすることはできません。ただし、構文 *server.domain.com* を使用して特定のドメインをブロックすることは可能です。

すべてのセーフリストおよびブロックリストのクリア

すべての送信者と受信者を含む、セーフリストおよびブロックリストのすべてのエントリを削除する必要がある場合は、セーフリスト/ブロックリストのバックアップと復元 （1173ページ）の手順を使用してエントリなしでファイルをインポートします。

セーフリストおよびブロックリストへのエンドユーザアクセスについて

エンドユーザはスパム隔離から各自のセーフリストとブロックリストにアクセスします。スパムの隔離へのエンドユーザアクセスを設定するには、「Webブラウザからのスパム隔離へのエンドユーザ アクセスの設定」を参照してください。

必要に応じて、スパム隔離の URL と下記の手順をエンド ユーザに提供してください。

関連項目

- セーフリストへのエントリの追加（エンド ユーザー）
- ブロックリストへの送信者の追加（エンド ユーザー）

セーフリストへのエントリの追加（エンド ユーザー）

（注） セーフリストに登録されている送信者からのメッセージの配信は、システムの他の設定によって異なります。セーフリストとブロックリストのメッセージ処理 （1161ページ）を参照してください。

エンド ユーザは、次の 2 つの方法で送信者をセーフリストに追加できます。

- 隔離されたメッセージの送信者のセーフリストへの追加 （1171 ページ）

• 隔離されたメッセージのない送信者のセーフリストへの追加 （1171 ページ）

隔離されたメッセージの送信者のセーフリストへの追加

エンド ユーザは、スパム隔離に送信されたメッセージの送信者をセーフリストに追加できます。

手順

ステップ 1 （新しい Web インターフェイスのみ）[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [セーフリスト（Safelist）] を選択します。

または

[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] > [セーフリスト（Safelist）] を選択します。

ステップ 2 （新しい Web インターフェイスのみ）[リリースしてセーフリストに追加（Release and Add to Safelist）] アイコンをクリックしてメッセージをリリースし、セーフリストに追加します。

または

ドロップダウン メニューから [リリースしてセーフリストに追加（Release and Add to Safelist）] を選択します。

指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メール パイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

隔離されたメッセージのない送信者のセーフリストへの追加

手順

ステップ 1 （新しい Web インターフェイスのみ）**[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [セーフリスト（Safelist）]** を選択し、ページの右上にあるプラス アイコンをクリックします。

ステップ 2 （新しい Web インターフェイスのみ）電子メール アドレスまたはドメインを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。

ステップ 3 （新しい Web インターフェイスのみ） をクリックしてエントリを保存します。

ステップ 4 必要に応じて、レガシー インターフェイスから次のタスクを実行できます。

a) **[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）]** を選択します。

b) ページの右上隅にある **[オプション（Options）]** ドロップダウン メニューを選択します。

c) **[セーフリスト（Safelist）]** を選択します。

d) [セーフリスト（Safelist）] ダイアログボックスから、電子メールアドレスまたはドメインを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
e) **[一覧に追加（Add to List）]** をクリックします。

ブロックリストへの送信者の追加（エンド ユーザー）

ブロックリストに登録されている送信者からのメッセージは、管理者が定義したセーフリスト/ブロックリスト アクション設定に応じて、拒否または隔離されます。

（注） この手順でのみブロックリスト エントリを追加できます。

手順

ステップ 1 （新しい Web インターフェイスのみ）[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2 （新しい Web インターフェイスのみ）[ブロックリスト（Blocklist）] を選択し、[+] アイコンをクリックして、ブロックリストに追加するドメインまたは電子メール アドレスを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。

ステップ 3 （新しい Web インターフェイスのみ） をクリックしてエントリを保存します。

ステップ 4 必要に応じて、レガシー インターフェイスから次のタスクを実行できます。

a) **[モニタ（Monitor）] > [スパム隔離（Spam Quarantine）]** を選択します。
b) ページの右上にある **[オプション（Options）]** ドロップダウン メニューから **[ブロックリスト（Blocklist）]** を選択します。
c) ブロックリストに追加するドメインまたは電子メールアドレスを入力します。ドメインと電子メール アドレスは、コンマで区切って複数入力できます。
d) **[一覧に追加（Add to List）]** をクリックします。

複数の 電子メールゲートウェイ（ Cisco Secure Email and Web Manager を使用しない展開）でのセーフリストまたはブロックリストの同期

複数の電子メールゲートウェイを Cisco Secure Email and Web Manager なしで使用する場合、セーフリスト/ブロックリストおよびその構成設定を、複数の電子メールゲートウェイ間で手動で同期することが必要になる場合があります。

セーフリスト/ブロックリストのバックアップと復元 （1173ページ）で説明されている手順を使用して .csv ファイルをエクスポートおよびインポートしてから、FTP を使用してファイルをアップロードおよびダウンロードできます。

セーフリスト/ブロックリストのバックアップと復元

電子メールゲートウェイをアップグレードする場合、またはインストールウィザードを実行する場合は、事前にセーフリスト/ブロックリストデータベースをバックアップしておく必要があります。セーフリスト/ブロックリストの情報は、アプライアンスの設定が格納されるメインの XML コンフィギュレーション ファイルには含まれていません。

セーフリスト/ブロックリストのコピーを保存して複数の 電子メールゲートウェイを同期する場合も、この手順を使用できます。

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[設定ファイル（Configuration File）] を選択します。

ステップ 3 [エンドユーザセーフリスト/ブロックリストデータベース(スパム隔離)（End-User Safelist/Blocklist Database (Spam Quarantine)）] セクションまでスクロールします。

目的	操作手順
セーフリスト/ブロックリストをエクスポートする	.csv ファイルのパスおよびファイル名をメモし、必要に応じて変更します。 [すぐにバックアップ（Backup Now）] をクリックします。 電子メールゲートウェイは次の命名規則を使用して、電子メールゲートウェイの /configuration ディレクトリに .csv ファイルを保存します。 *slbl-<serial number>-<timestamp>.csv*
セーフリスト/ブロックリストをインポートする	**注意** このプロセスによって、すべてのユーザのセーフリストおよびブロックリストの既存のエントリがすべて上書きされます。 [リストアするファイルを選択（Select File to Restore）] をクリックします。 configuration ディレクトリ内のファイル リストから目的のファイルを選択します。 復元するセーフリスト/ブロックリストバックアップ ファイルを選択します。 [復元（Restore）] をクリックします。

セーフリストとブロックリストのトラブルシューティング

セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログ ファイルまたはシステム アラートを表示できます。

電子メールがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが ISQ_log ファイルまたはアンチスパム ログ ファイルに記録されます。セーフリストに含まれる電子メールは、セーフリストに一致していることが *X-SLBL-Result*-セーフリスト ヘッダーによってマークされます。ブロックリストに含まれる電子メールは、ブロックリストに一致していることが *X-SLBL-Result*-ブロックリスト ヘッダーによってマークされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリスト プロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、アラート （1275 ページ）を参照してください。

ログ ファイルの詳細については、ログ （1391 ページ）を参照してください。

関連項目

- セーフリストに登録されている送信者からのメッセージが配信されない （1174 ページ）

セーフリストに登録されている送信者からのメッセージが配信されない

問題

セーフリストに登録されている送信者からのメッセージが配信されませんでした。

ソリューション

考えられる原因：

- マルウェアまたはコンテンツ違反のためメッセージがドロップされました。セーフリストとブロックリストのメッセージ処理 （1161 ページ）を参照してください。
- 電子メールゲートウェイが複数あり、その送信者をセーフリストに最近追加した場合、メッセージが処理された時点ではセーフリスト/ブロックリストが同期されていなかった可能性があります。外部スパム隔離およびセーフリスト/ブロックリスト （1163 ページ）および複数の 電子メールゲートウェイ（Cisco Secure Email and Web Manager を使用しない展開）でのセーフリストまたはブロックリストの同期 （1172 ページ）を参照してください。

エンド ユーザのためのスパム管理機能の設定

目的	参照先
スパム管理機能へのエンドユーザ アクセスのさまざまな認証方式について、利点と制限事項を把握します。	スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）およびサブセクション

目的	参照先
エンド ユーザがブラウザから直接スパム隔離にアクセスすることを許可します。	スパム管理機能にアクセスするエンド ユーザの認証オプション （1175ページ）
メッセージがスパム隔離にルーティングされたときに、その宛先のユーザに通知を送信します。 通知にはスパム隔離へのリンクを含めることができます。	エンドユーザへの隔離されたメッセージに関する通知 （1180 ページ）
ユーザが、安全であると判断した送信者、およびスパムまたはその他の無用なメールを送信すると判断した送信者の電子メール アドレスとドメインを指定できるようにします。	セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御 （1161 ページ）

関連項目

- スパム管理機能にアクセスするエンド ユーザの認証オプション （1175 ページ）
- Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定 （1177 ページ）
- エンド ユーザへの隔離されたメッセージに関する通知 （1180 ページ）

スパム管理機能にアクセスするエンド ユーザの認証オプション

（注） メールボックス認証では、ユーザが電子メール エイリアス宛てのメッセージを表示することはできません。

エンドユーザによるスパム隔離へのアクセスの場合	操作手順
Webブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証必須	1. [エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、[LDAP]、[SAML 2.0] または [メールボックス（IMAP/POP）（Mailbox (IMAP/POP)）]を選択します。 2. [スパム通知（Spam Notifications）] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする（Enable login without credentials for quarantine access）] の選択を解除します。

エンドユーザによるスパム隔離へのアクセスの場合	操作手順
Webブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証不要	1. [エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、[LDAP]、[SAML 2.0] または [メールボックス（IMAP/POP）（Mailbox (IMAP/POP)）]を選択します。 2. [スパム通知（Spam Notifications）] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする（Enable login without credentials for quarantine access）] をオンにします。
通知内のリンク経由でのみアクセス、認証不要	[エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、認証方式として [なし（None）] を選択します。
アクセスなし	[エンドユーザ隔離アクセス（End User Quarantine Access）] 設定で、[エンドユーザの隔離へのアクセスを有効にする（Enable End-User Quarantine Access）] の選択を解除します。

関連項目

- LDAP 認証プロセス （1176 ページ）
- スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）
- エンド ユーザへの隔離されたメッセージに関する通知 （1180 ページ）
- スパム管理機能にアクセスするエンド ユーザの認証オプション （1175 ページ）
- セーフリストおよびブロックリストへのエンドユーザ アクセスについて （1170 ページ）

LDAP 認証プロセス

1. ユーザは、自分のユーザ名とパスフレーズを Web UI ログイン ページに入力します。
2. スパム隔離は、匿名検索を実行するように、または指定された「サーバ ログイン」DN とパスフレーズによる認証ユーザとして、指定された LDAP サーバに接続します。Active Directory の場合、一般に「グローバル カタログ ポート」（6000 番台）上でサーバ接続を確立する必要があり、検索を実行するために、スパム隔離がバインドできる低い特権LDAP ユーザを作成する必要があります。
3. 次に、スパム隔離は、指定された BaseDN とクエリ ストリングを使用してユーザを検索します。ユーザーの LDAP レコードが見つかると、スパム隔離は、そのレコードの DN を抽出し、ユーザー レコードの DN と最初にユーザーが入力したパスフレーズを使用してディレクトリへのバインドを試みます。このパスフレーズ チェックに成功すると、ユーザは正しく認証されます。しかしまだ、スパム隔離は、そのユーザに対してどのメールボックスの内容を表示するのか決定する必要があります。
4. メッセージは、受信者のエンベロープ アドレスを使用してスパム隔離に保管されます。ユーザのパスフレーズが LDAP に対して検証された後、スパム隔離は、「プライマリ電子メール属性」を LDAP レコードから取得して、どのエンベロープ アドレスの隔離された

メッセージを表示する必要があるのか決定します。「プライマリ電子メール属性」には、電子メールアドレスが複数格納されている場合があり、これらのアドレスを使用して、隔離からどのエンベロープアドレスが認証ユーザに対して表示される必要があるのかが決定されます。

関連項目

- スパム管理機能にアクセスするエンドユーザの認証オプション （1175 ページ）

IMAP/POP 認証プロセス

1. メール サーバ設定に応じて、ユーザは、自分のユーザ名（joe）または電子メール アドレス（joe@example.com）と、パスフレーズを Web UI ログイン ページに入力します。ユーザに電子メールアドレスをフルに入力する必要があるのか、ユーザ名だけを入力すればよいのか知らせるために、ログイン ページ メッセージを変更できます（スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）を参照）。
2. スパム隔離は、IMAP サーバまたは POP サーバに接続し、入力されたログイン名（ユーザ名または電子メールアドレス）とパスフレーズを使用して IMAP/POP サーバへのログインを試みます。パスフレーズが受け入れられると、そのユーザは認証されたと見なされ、スパム隔離はただちに IMAP/POP サーバからログアウトします。
3. ユーザが認証された後、スパム隔離は、ユーザの電子メール アドレスに基づいて、そのユーザ宛の電子メールのリストを作成します。
   - スパム隔離の設定において、修飾のないユーザ名（joe など）に追加するドメインを指定している場合は、このドメインを後ろに追加してできる完全修飾電子メールアドレスを使用して、隔離エリア内の一致するエンベロープが検索されます。
   - それ以外の場合、スパム隔離は、入力された電子メールアドレスを使用して、一致するエンベロープを検索します。

IMAP の詳細については、ワシントン大学の Web サイトを参照してください。

http://www.washington.edu/imap/

Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定

手順

ステップ 1 スパム管理機能へのエンドユーザアクセスのさまざまな認証方式について、利点と制限事項を把握します。

ステップ 2 LDAP を使用してエンドユーザを認証する場合は、[システム管理（System Administration）] > [LDAP] > [LDAPサーバプロファイル（LDAP Server Profile）] ページの [スパム隔離エンドユーザ認証クエリー（Spam Quarantine End-User Authentication Query）] 設定などで、LDAP サーバプロファイルを設定します。

例：

If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the **System Administration** > **SAML** page.

ステップ 3 スパム隔離へのエンドユーザ アクセスを設定します。

スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）

ステップ 4 スパム隔離へのエンドユーザ アクセスの URL を決定します。

スパム隔離へのエンドユーザ アクセス用 URL の決定 （1179 ページ）

次のタスク

関連項目

- スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）
- スパム隔離へのエンドユーザ アクセス用 URL の決定 （1179 ページ）
- エンド ユーザに表示されるメッセージ （1180 ページ）

スパム隔離へのエンドユーザ アクセスの設定

管理ユーザは、エンドユーザアクセスがイネーブルにされているかどうかに関わらず、スパム隔離にアクセスできます。

始める前に

スパム管理機能にアクセスするエンドユーザの認証オプション （1175 ページ）で要件を参照してください。

手順

ステップ 1 レガシーインターフェイスを使用している場合は、**[管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] > [モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] > [設定の編集（Edit Settings）]** に移動し、[エンドユーザの隔離アクセス（End-User Quarantine Access）] へと下にスクロールします。新しい Web インターフェイスを使用している場合は、 [Cisco Secure Email and Web Manager] に移動し、[サービスステータス（Service Status）] をクリックして アイコンにマウスのカーソルを合わせて [エンドユーザの隔離設定の編集（Edit End-User Quarantine Settings）] をクリックします。レガシー インターフェイスにリダイレクトされます。

ステップ 2 [エンドユーザの隔離へのアクセスを有効にする（Enable End-User Quarantine Access）] を選択します。

ステップ 3 エンド ユーザが隔離されたメッセージを表示しようとしたときに、エンド ユーザの認証に使用する方式を指定します。

選択オプション	追加情報
なし	このオプションを選択すると、追加の認証なしでスパム通知内のリンクを介してエンドユーザが隔離されたメッセージにアクセスできるようになります。
メールボックス（IMAP/POP）	認証に LDAP ディレクトリを使用しないサイトの場合、隔離は、ユーザの電子メールアドレスとパスフレーズの正当性を、それらのユーザのメールボックスが保持されている標準ベースの IMAP または POP サーバに対して検証することもできます。 スパム隔離にログインするとき、エンドユーザは自身の完全な電子メールアドレスとメールボックスのパスフレーズを入力します。 POP サーバがバナー内で APOP サポートをアドバタイズしている場合、セキュリティ上の理由から（つまり、パスフレーズが平文で送信されるのを回避するために）、Cisco アプライアンスは APOP のみを使用します。一部またはすべてのユーザに対して APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを設定する必要があります。 サーバで SSL を使用するように設定している場合は、SSL を選択します。ユーザがユーザ名だけを入力した場合に、電子メールアドレスを自動入力するために追加するドメインを指定できます。「権限のないユーザ名にドメインを追加（Append Domain to Unqualified Usernames）」するには、ログインするユーザ用のエンベロープのドメインを入力します。
LDAP	このトピックの「はじめる前に」で触れたセクションの説明に従って、LDAP を設定します。

ステップ 4 メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。

このチェックボックスをオンにすると、ユーザは、スパム隔離ページからメッセージ本文を表示できなくなります。この場合、隔離されたメッセージの本文を表示するには、そのメッセージを解放してから、ユーザのメール アプリケーション（Microsoft Outlook など）で表示する必要があります。この機能は、ポリシーおよび規制（表示したすべての電子メールをアーカイブすることが要求されている場合など）へのコンプライアンスの目的で使用できます。

ステップ 5 変更を送信し、保存します。

スパム隔離へのエンドユーザ アクセス用 URL の決定

エンド ユーザがスパム隔離に直接アクセスするために使用できる URL は、マシンのホスト名と、隔離が有効になっている IP インターフェイス上の設定（HTTP/S とポート番号）から作成されます。たとえば、`HTTP://mail3.example.com:82` となります。

エンドユーザは、以下のいずれかの方法で、新しい Web インターフェイスのスパム検疫にアクセスできます。

- `trailblazerconfig` CLI コマンドが有効になっているときに、`https://example.com:<trailblazer-https-port>/euq-login` の URL を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている先駆者の HTTPS ポートです。

- `trailblazerconfig` CLI コマンドが無効になっているときに、`https://example.com:<https-port>/euq-login` の URL を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。

（注） ローカルおよび外部認証のユーザは、エンドユーザのスパム隔離ポータルにログインできません。

エンド ユーザに表示されるメッセージ

通常、エンド ユーザにはスパム隔離内にある自身のメッセージだけが表示されます。

アクセス方法（通知経由または Web ブラウザから直接）と認証方式（LDAP または IMAP/POP）によっては、スパム隔離内にある複数の電子メール アドレス宛のメールが表示される場合があります。

LDAP 認証を使用する場合、LDAP ディレクトリ内でプライマリ電子メール属性に複数の値が設定されていると、それらの値（アドレス）のすべてがユーザに関連付けられます。したがって、検疫エリア内には、LDAP ディレクトリでエンド ユーザに関連付けられたすべての電子メール アドレス宛の検疫されたメッセージが存在します。

認証方式が IMAP/POP の場合、またはユーザが通知から直接隔離にアクセスした場合は、そのユーザの電子メール アドレス（または通知の送信先アドレス）宛のメッセージのみが隔離に表示されます。

メンバーになっているエイリアスに送信されたメッセージについては、受信者の電子メールのメーリング リスト エイリアスおよびスパム通知 （1183 ページ）を参照してください。

関連項目

- スパム隔離へのエンドユーザ アクセスの設定 （1178 ページ）
- 受信者の電子メールのメーリング リスト エイリアスおよびスパム通知 （1183 ページ）

エンド ユーザへの隔離されたメッセージに関する通知

特定またはすべてのユーザに、スパム隔離内にスパムまたはその疑いのあるメッセージがあることを通知する電子メールを送信するように、システムを設定できます。

デフォルトでは、エンドユーザの隔離されたメッセージがスパム通知に表示されます。通知には、ユーザがスパム隔離内に隔離されたメッセージを表示できるリンクが含まれます。隔離されたメッセージを受信トレイに送るか、削除するかを決定できます。

（注） クラスタ設定では、マシン レベルでのみ通知を受信するユーザを選択できます。

始める前に

- エンドユーザが通知に表示されるメッセージを管理するには、スパム隔離にアクセスできる必要があります。スパム隔離へのエンドユーザアクセスの設定 （1178ページ）を参照してください。
- 通知を使用してスパムを管理するための認証オプションを把握して実装します。スパム管理機能にアクセスするエンドユーザの認証オプション （1175ページ）を参照してください。
- エンドユーザが複数のエイリアスで電子メールを受信する場合については、受信者の電子メールのメーリング リスト エイリアスおよびスパム通知 （1183ページ）を参照してください。

手順

ステップ 1 （新しい Web インターフェイスのみ） 電子メールゲートウェイで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 レガシーインターフェイスを使用している場合は、**[管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] > [設定の編集（Edit Settings）]** に移動し、**[スパム通知（Spam Notifications）]** へと下にスクロールします。ただし、新しい Web インターフェイスを使用している場合は、[Cisco Secure Email and Web Manager] に移動し、[サービスステータス（Service Status）] をクリックして ⚙ アイコンの上にカーソルを合わせ、[スパム通知設定の編集（Edit Spam Notification Settings）] をクリックします。レガシー インターフェイスにリダイレクトされます。

ステップ 3 [スパム通知を有効にする（Enable Spam Notification）] を選択します。

ステップ 4 通知の差出人アドレスを入力します。

ステップ 5 通知するエンドユーザを指定します。

ステップ 6 （任意）通知の件名をカスタマイズします。

ステップ 7 （任意）通知のタイトルをカスタマイズします。

ステップ 8 通知のデフォルト言語を選択します。

ステップ 9 エンドユーザ向けに隔離アクセスを設定します。

a) ユーザが通知に記載されたリンクをクリックしてスパム隔離にアクセスしたときにそのユーザが自動的にログインされるようにするには、[クレデンシャルを使用せずにログインする（Login without credentials）] チェックボックスをオンにします。エンドユーザは、通

知の [リリース（Release）] リンクをクリックするだけでメッセージをリリースできます。このオプションをオフにすると、エンドユーザは通知の [リリース（Release）] リンクをクリックしてメッセージをリリースすることはできなくなります。

このオプションは、メールボックス（IMAP / POP）、LDAP、または SAML 2.0 のいずれかのエンドユーザ認証方式を選択した場合にのみ表示されます。認証方式として [なし（None）] を選択した場合、エンドユーザはスパム通知内のリンクをクリックすると、自動的にスパム隔離にログインします。

b) 通知内のリンクの有効期限（日数）を設定します。0 ～ 365 の範囲内の数を入力してください。これらのリンクは、指定された期間後に自動的に期限切れになります。リンクを期限切れにしない場合は、0 を入力します。

（メールボックス（IMAP / POP）、LDAP、および SAML 2.0 の場合）このオプションは、[クレデンシャルを使用せずにログインする（Login without credentials）] チェックボックスをオンにした場合にのみ設定できます。

CLI で **spamdigestconfig** コマンドを使用して有効期限を設定することもできます。

ステップ 10 メッセージ本文をカスタマイズします。

a) （任意）デフォルトのテキストおよび変数をカスタマイズします。

変数を挿入するには、挿入する位置にカーソルを置いて、右側のメッセージ変数リストで変数の名前をクリックします。または変数を入力します。

次のメッセージ変数は、特定のエンド ユーザに対応した実際の値に展開されます。

- [新規メッセージ数（New Message Count）]（%new_message_count%）：ユーザの最後のログイン以後の新しいメッセージの数。
- [総メッセージ数（Total Message Count）]（%total_message_count%）：スパム隔離内にあるこのユーザ宛のメッセージの数。
- [メッセージ保存期間（Days Until Message Expires）]（%days_until_expire%）
- [隔離URL（Quarantine URL）]（%quarantine_url%）：隔離にログインし、メッセージを表示するための URL。
- [ユーザ名（Username）]（%username%）
- [新しいメッセージテーブル（New Message Table）]（%new_quarantine_messages%）：ユーザの新しい隔離メッセージのリスト。送信者、メッセージ件名、日付、およびメッセージをリリースするリンクを示します。ユーザは、メッセージ件名をクリックしてスパム隔離のメッセージを表示します。
- [新しいメッセージテーブル（件名なし）]（%new_quarantine_messages_no_subject%）：[新しいメッセージテーブル（New Message Table）] と似ていますが、各メッセージの件名の場所には [メッセージの表示（View Message）] リンクのみが表示されています。

b) スパム通知内のすべての隔離メッセージを表示するためにリンクを表示するか非表示にするかを選択します。[通知メールのすべての隔離メッセージを表示するリンクを表示する（Show link to show all Quaranted messages in Notification Mails）] で、要件に応じて [はい（Yes）] または [いいえ（No）] を選択します

（メールボックス（IMAP / POP）、LDAP、および SAML 2.0 の場合）。このオプションは、[クレデンシャルを使用せずにログインする（Login without credentials）] チェックボックス（[隔離へのアクセス（Quarantine Access）]の下）をオンにした場合にのみ表示されます。

[はい（Yes）] を選択した場合は、スパム隔離にアクセスする前にエンドユーザを強制的に認証できます。[チャレンジアクセス（Challenge Access）] をオンにします。このオプションは、エンドユーザ認証方式として [なし（None）] を選択した場合は使用できません。

CLIで **spamdigestconfig** コマンドを使用して、リンクを表示または非表示にすることもできます。

c) [メッセージのプレビュー（Preview Message）] をクリックして、メッセージの内容を確認します。

ステップ 11 メッセージ形式（HTML、テキスト、または HTML/テキスト）を選択します。

ステップ 12 バウンスされた通知の送信先のアドレスを指定します。

ステップ 13 （任意）[統合されたメッセージは同じLDAPユーザの違うアドレスに送信されます（Consolidate messages sent to the same LDAP user at different addresses）] を選択します。

ステップ 14 通知スケジュールを設定します。

ステップ 15 変更を送信し、保存します。

次のタスク

これらの通知を確実に受信できるように、エンドユーザにスパム隔離からの通知電子メールの差出人アドレスを各自のメールアプリケーション（Microsoft Outlook、Mozilla Thunderbird など）の迷惑メール設定にある「許可リスト」に追加することを推奨してください。

関連項目

- 受信者の電子メールのメーリング リスト エイリアスおよびスパム通知 （1183 ページ）
- 通知のテスト （1184 ページ）
- スパム通知のトラブルシューティング （1185 ページ）

受信者の電子メールのメーリング リスト エイリアスおよびスパム通知

電子メールが隔離されている各エンベロープ受信者（メーリングリストおよびその他のエイリアスを含む）に通知を送信できます。メーリングリストごとに1つの要約を受信します。メーリングリストに通知を送信すると、リストの購読者全員に通知が届きます。複数の電子メールエイリアスに属するユーザ、通知を受信するLDAPグループに属するユーザ、または複数の電

子メールアドレスを使用するユーザは、複数のスパム通知を受信する場合があります。次の表に、ユーザが複数の通知を受け取る状況の例を示します。

表 *93*：アドレス/エイリアスに応じた通知数

ユーザー	電子メール アドレス	エイリアス	通知
Sam	sam@example.com	—	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com、admin@example.com	hr@example.com	3

LDAP 認証を使用する場合、メーリング リスト エイリアスに通知を送信しないように選択することができます。または、メーリング リスト エイリアスにスパム通知を送信することを選択した場合、複数の通知が送信されないようにすることができます。スパム隔離のエイリアス統合クエリ （993 ページ）を参照してください。

アプライアンスが電子メール通知にスパム隔離のエイリアス統合クエリを使用していない限り、通知内のリンクをクリックしてスパム隔離にアクセスしたユーザに、そのエンドユーザが所有する他のエイリアス宛の隔離対象メッセージは表示されません。アプライアンスで処理した後に展開される配布リストに通知が送信された場合、複数の受信者がそのリストの同じ隔離にアクセスできます。

つまり、各メーリングリストの購読者は、全員が同じ通知を受信することになり、その検疫にログインしてメッセージを解放したり、削除したりできます。この場合、エンドユーザが隔離にアクセスして、通知に示されたメッセージを表示しようとしても、それらのメッセージは他のユーザによってすでに削除されている可能性もあります。

（注） LDAP を使用していない場合で、エンド ユーザが複数の電子メール通知を受信することがないようにする必要がある場合は、通知をディセーブルにすることを検討します。この場合、代わりとして、エンド ユーザが検疫に直接アクセスできるようにし、LDAP または POP/IMAP で認証します。

通知のテスト

テスト用のメールポリシーを設定し、単一のユーザに対してのみスパムを隔離することで通知をテストできます。その後、スパム隔離の通知設定で、[スパム通知を有効にする（Enable Spam Notification）] チェックボックスをオンにし、[エンドユーザの隔離へのアクセスを有効にする（Enable End-User Quarantine Access）] チェックボックスをオフにします。これにより、[バウンスされたメッセージの送信先（Deliver Bounced Messages To）] フィールドに設定された管理者だけが、隔離内の新しいスパムについて通知されます。

スパム通知のトラブルシューティング

関連項目

- ユーザが複数の通知を受信する （1185 ページ）
- 受信者が通知を受信しない （1185 ページ）
- ユーザが複数の通知を受信する （1185 ページ）
- 受信者が通知を受信しない （1185 ページ）

ユーザが複数の通知を受信する

問題

ユーザが 1 つのメッセージに対して複数のスパム通知を受信します。

ソリューション

考えられる原因：

- ユーザが複数の電子メール アドレスを所有し、スパム メッセージがその内の 2 つ以上のアドレスに送信されました。
- ユーザが、スパム メッセージを受信した 1 つ以上の電子メール エイリアスのメンバーです。重複を最小限にするための詳細については、受信者の電子メールのメーリング リスト エイリアスおよびスパム通知 （1183 ページ） を参照してください。

受信者が通知を受信しない

問題

受信者にスパム通知が届きません。

ソリューション

- スパム受信者ではなく [バウンスメッセージの送信先：（Deliver Bounce Messages To:）] のアドレスに通知が送信される場合は、スパム通知が有効になっていても、スパム隔離へのアクセスが有効になっていないことを意味します。スパム管理機能にアクセスするエンドユーザの認証オプション （1175 ページ）を参照してください。
- ユーザに各自の電子メール クライアントの迷惑メール設定を確認してもらいます。

スパム隔離内のメッセージの管理

ここでは、ローカルまたは外部のスパム隔離内にあるメッセージの操作方法について説明します。

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

関連項目

- スパム隔離へのアクセス（管理ユーザ） （1186 ページ）
- スパム隔離内でのメッセージの検索 （1186 ページ）

- スパム隔離内のメッセージの表示 （1187 ページ）
- スパム隔離内のメッセージの配信 （1187 ページ）
- スパム隔離からのメッセージの削除 （1188 ページ）

スパム隔離へのアクセス（管理ユーザ）

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

手順

ステップ 1 （新しい Web インターフェイスのみ）[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）] を選択します。

ステップ 2 [モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] を選択し、[メッセージ（Messages）] カラムの数字をクリックします。

スパム隔離内でのメッセージの検索

手順

ステップ 1 エンベロープ受信者を指定します。

（注） アドレスの一部を入力できます。

ステップ 2 入力した受信者に検索結果が厳密に一致する必要があるか、あるいは入力した値が検索結果のアドレスの一部、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 3 検索の対象期間を入力します。カレンダー アイコンをクリックして、日付を選択します。

ステップ 4 差出人アドレスを指定し、入力した値が検索結果のアドレスの一部、全体、先頭、または末尾のいずれと一致する必要があるかを選択します。

ステップ 5 **[検索（Search）]**をクリックします。検索基準に一致するメッセージがページの [検索（Search）] セクションの下に表示されます。

次のタスク

関連項目

大量メッセージの検索 （1187 ページ）

大量メッセージの検索

スパム隔離内に大量のメッセージが収集されている場合、および検索条件が絞り込まれていない場合、クエリーの結果が返されるまでに非常に長い時間がかかる可能性があり、場合によってはタイムアウトします。

その場合、検索を再実行するかどうか確認されます。大量の検索が同時に複数実行されると、パフォーマンスに悪影響を与える可能性があることに注意してください。

スパム隔離内のメッセージの表示

メッセージのリストにより、スパム隔離内のメッセージが表示されます。一度に表示されるメッセージの件数を選択できます。列見出しをクリックすることにより、表示をソートできます。同じ列を再びクリックすると、逆順にソートされます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。メッセージは、[メッセージの詳細（Message Details）] ページに表示されます。メッセージの最初の 20 KB が表示されます。メッセージがそれよりも長い場合、表示は 20 KB で打ち切られ、メッセージの最後にあるリンクからメッセージをダウンロードできます。

[メッセージの詳細（Message Details）]ページから、メッセージを削除したり（**[削除（Delete）]** を選択）、**[リリース（Release）]** を選択してメッセージを解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング（Message Tracking）] リンクをクリックします。

次の点に注意してください。

- **添付ファイルを含むメッセージの表示**

  添付ファイルを含むメッセージを表示すると、メッセージの本文が表示された後、添付ファイルのリストが続いて表示されます。

- **HTML メッセージの表示**

  スパム隔離では、HTML ベースのメッセージは近似で表示されます。画像は表示されません。

- **エンコーディングされたメッセージの表示**

  Base64 でエンコーディングされたメッセージは、復号されてから表示されます。

スパム隔離内のメッセージの配信

メッセージをリリースして配信するには、リリースする 1 つまたは複数のメッセージの隣にあるチェックボックスをクリックし、ドロップダウン メニューから [リリース（Release）] を選択します。その後、[送信（Submit）] をクリックします。

ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

リリースされたメッセージは、それ以降の電子メールパイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

スパム隔離からのメッセージの削除

スパム隔離では、メッセージが一定時間後に自動で削除されるように設定できます。また、スパム隔離が最大サイズに達したら、古いものから順にメッセージが自動で削除されるように設定することもできます。スパム隔離からメッセージを手動で削除することも可能です。

個別のメッセージを削除するには、削除するメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから[削除（Delete）]を選択します。その後、[送信（Submit）]をクリックします。ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

スパム隔離内のすべてのメッセージを削除するには、その隔離を無効にし（外部スパム隔離の無効化について （1188 ページ）を参照）、[すべてのメッセージを削除（Delete All Messages）]リンクをクリックします。リンクの末尾にある括弧内の数字は、スパム隔離内のメッセージの件数です。

スパム隔離のディスク領域

デフォルトでは、スパム隔離内のメッセージは一定期間後に自動的に削除されます。検疫エリアが満杯になった場合は、古いスパムから削除されます。

関連項目

- ディスク領域の管理 （1249 ページ）

外部スパム隔離の無効化について

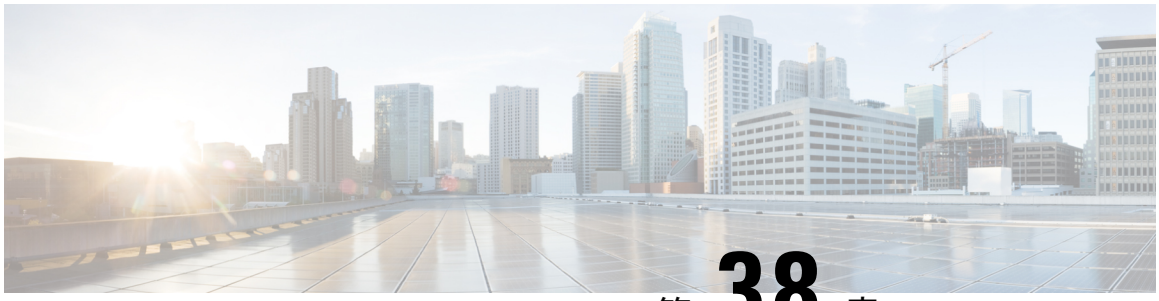
スパム隔離をディセーブルにする場合は、次を参照してください。

- ディセーブルになっているスパム隔離内にメッセージが存在する場合は、すべてのメッセージの削除を選択できます。
- スパムまたはその疑いのあるメッセージを隔離するように設定されたメールポリシーは、メッセージを配信するように設定が変更されます。メールポリシーの調整が必要になる場合があります。
- 外部スパム隔離を完全にディセーブルにするには、 電子メールゲートウェイおよび Cisco Secure Email and Web Manager の両方でディセーブルにします。

電子メールゲートウェイのみで外部スパム隔離をディセーブルにしても、外部隔離またはそのメッセージとデータは削除されません。

スパム隔離機能のトラブルシューティング

- セーフリストとブロックリストのトラブルシューティング （1174 ページ）
- スパム通知のトラブルシューティング （1185 ページ）
- メッセージ テキストが正しく表示されることの確認 （1160 ページ）



第 38 章

管理タスクの分散

この章は、次の項で構成されています。

- ユーザー アカウントを使用する作業 （1191 ページ）
- 委任管理のためのカスタム ユーザー ロールの管理 （1198 ページ）
- パスフレーズ （1208 ページ）
- 電子メールゲートウェイへのアクセスの設定 （1216 ページ）
- 管理ユーザへのメッセージの表示 （1221 ページ）
- セキュア シェル（SSH）キーの管理 （1222 ページ）
- 管理ユーザー アクセスのモニタリング （1224 ページ）

ユーザー アカウントを使用する作業

電子メールゲートウェイには、ユーザアカウントを追加する方法が2つあります。電子メールゲートウェイ自体でユーザアカウントを作成する方法と、LDAPまたはRADIUSディレクトリなどの独自の中央認証システムを使用してユーザ認証を有効にする方法です。ユーザーと外部認証ソースへの接続を管理するには、GUIで[システム管理（System Administration）]>[ユーザー（Users）]ページを使用します（または、CLIで**userconfig**コマンドを使用します）。ユーザを認証するために外部ディレクトリを使用することについては、外部認証（1210ページ）を参照してください。

必要に応じて、次を使用して、特定のユーザ ロールに二要素認証を有効にできます。

- Web インターフェイスの [システム管理（System Administration）] > [ユーザー（Users）] ページ。二要素認証 （1215 ページ）を参照してください。
- CLI での `userconfig > twofactorauth` コマンド。『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

システムのデフォルトのユーザアカウントであるadminはすべての管理権限を持っています。adminユーザーアカウントは削除できませんが、パスフレーズを変更してアカウントをロックすることはできます。

新しいユーザー アカウントを作成する場合は、そのユーザーを定義済みのユーザー ロールまたはカスタム ユーザー ロールに割り当てます。各ロールには、システム内での異なるレベルの権限が含まれます。

電子メールゲートウェイで作成できる各ユーザアカウントの数に制限はありませんが、システムで予約されている名前でユーザアカウントを作成することはできません。たとえば、「operator」や「root」という名前のユーザ アカウントは作成できません。

ユーザの役割

表 *94 :* ユーザー ロールの一覧

ユーザー ロール	説明
admin	admin ユーザーはシステムのデフォルト ユーザー アカウントであり、すべての管理権限を持っています。便宜上、admin ユーザー アカウントをここに記載しましたが、これはユーザー ロールを使用して割り当てることはできず、パスワードの変更以外、編集や削除もできません。 **`resetconfig`** コマンドと revert コマンドを発行できるのは、admin ユーザだけです。
管理者	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。ただし、**`resetconfig`** コマンドと **`revert`** コマンドにアクセスできるのは admin ユーザだけです。 （注） AsyncOS は、GUI から 電子メールゲートウェイを同時に設定する複数の管理者をサポートしません。
専門技術者	Technician ロールを持つユーザアカウントは、システムのアップグレード、 電子メールゲートウェイの再起動、ライセンスキーの管理を実行できます。また、専門技術者は、 電子メールゲートウェイをアップグレードするために以下の処理も実行できます。 • 電子メールの配信および受信の一時停止。 • ワークキューとリスナーのステータスの表示。 • 設定ファイルの保存および電子メール送信。 • セーフリストとブロックリストのバックアップ。専門技術者はこれらのリストを復元できません。 • クラスタからの 電子メールゲートウェイの接続解除。 • Cisco テクニカル サポートへのリモート サービス アクセスの有効化または無効化。 • サポート要求の申請。

ユーザー ロール	説明
オペレータ	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザー アカウントの作成または編集。 • **resetconfig** コマンドの発行。 • 電子メールゲートウェイのアップグレード。 • **systemsetup** コマンドの発行またはシステム設定ウィザードの実行。 • **adminaccessconfig** コマンドの発行。 • 隔離機能の実行（作成、編集、削除、および隔離の中央集中を含む）。 • ユーザ名とパスフレーズ以外の LDAP サーバ プロファイル設定の変更（LDAP が外部認証に対して有効になっている場合）。 これら以外は、Administrator ロールと同じ権限を持ちます。
ゲスト	Guest ロールを持つユーザ アカウントはステータス情報とレポートだけを参照できます。Guest ロールを持つユーザは、アクセスが隔離でイネーブルの場合、隔離エリア内のメッセージを管理できます。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。
オペレータ（読み取り専用）	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために変更を行って送信できますが、保存できません。このロールのユーザは、アクセスが隔離でイネーブルの場合、隔離エリア内のメッセージを管理できます。 このロールのユーザは、以下にはアクセスできません。 • ファイル システム、FTP、SCP。 • 作成、編集、削除、または隔離の中央集中の設定。
ヘルプ デスク ユーザー	ヘルプ デスク ユーザー ロールを持つユーザーがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング。 • 隔離エリア内のメッセージの管理。 このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。このロールのユーザがそのデバイスを管理する前に、各隔離アクセスをイネーブルにする必要があります。

ユーザー ロール	説明
カスタム ユーザー ロール	カスタム ユーザー ロールを持つユーザー アカウントはそのロールに割り当てられている電子メール セキュリティ機能にのみアクセスできます。アクセスできる機能は、DLP ポリシー、電子メール ポリシー、レポート、検疫、ローカル メッセージ トラッキング、暗号化プロファイル、トレースデバッグツール、アクセス ログ サブスクリプション、ロギング API、およびログファイルの任意の組み合わせになります。ユーザは、機能のグローバルなイネーブル化を含むシステム設定機能にアクセスできません。カスタム ユーザー ロールを定義できるのは管理者だけです。詳細については、委任管理のためのカスタム ユーザー ロールの管理（1198 ページ）を参照してください。 （注） カスタム ユーザー ロールに割り当てられているユーザーは、CLI にアクセスできません。

上記の表に定義されているロールはすべて GUI と CLI の両方にアクセスできます。ただし、Help Desk User ロールとカスタム ユーザー ロールは GUI にのみアクセスできます。

ユーザーを認証するために LDAP ディレクトリを使用する場合は、ユーザー ロールに個々のユーザーではなくディレクトリ グループを割り当てます。ユーザー ロールにディレクトリ グループを割り当てると、そのグループの各ユーザーはそのユーザー ロールで定義された権限を受け取ります。詳細については、外部認証 （1210 ページ）を参照してください。

関連項目

- ユーザの管理 （1194 ページ）

ユーザの管理

[ユーザー（Users）]ページには、システムの既存のユーザーが一覧（ユーザー名、氏名、およびユーザー タイプまたはグループを含む）で表示されます。

[ユーザー（Users）] ページからは、次の操作が行えます。

- 新しいユーザの追加。詳細については、ユーザの追加 （1195 ページ）を参照してください。
- ユーザの削除。詳細については、ユーザの削除 （1196 ページ）を参照してください。
- ユーザの編集。ユーザのパスフレーズの変更、ユーザのアカウントのロックおよびロック解除など。詳細については、ユーザの編集 （1196 ページ）を参照してください。
- ユーザにパスフレーズの変更を強制します。ユーザにパスフレーズの変更を強制（1196 ページ）を参照してください。

- ローカル アカウント用のユーザ アカウントとパスフレーズ設定値の設定。詳細については、制限的なユーザアカウントとパスフレーズの設定値の構成（1209ページ）を参照してください。
- ユーザを認証するために LDAP または RADIUS ディレクトリを使用するよう 電子メール ゲートウェイをイネーブルにする。詳細については、外部認証（1210ページ）を参照してください。
- 特定のユーザ ロールに二要素認証を有効にします。詳細については、二要素認証 （1215ページ）を参照してください。
- メッセージ トラッキング内の DLP Matched Content への管理者以外のアクセスをイネーブルにする。詳細については、メッセージ トラッキングでの機密情報へのアクセスの制御（1197 ページ）を参照してください。

ユーザの追加

はじめる前に

- ユーザが使用するユーザ ロールを設定します。
  - 定義済みのユーザ ロールについては、ユーザの役割 （1192ページ）を参照してください。
  - カスタム ロールを作成するには、委任管理のためのカスタム ユーザー ロールの管理（1198 ページ）を参照してください。
- パスフレーズの要件を指定します。制限的なユーザアカウントとパスフレーズの設定値の構成 （1209 ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 [ユーザを追加（Add User）] をクリックします。

ステップ 3 ユーザのログイン名を入力します。一部の単語（「operator」や「root」など）が予約されています。

ステップ 4 ユーザの氏名を入力します。

ステップ 5 定義済みのユーザー ロールまたはカスタム ユーザー ロール（Custom user role）を選択します。

ステップ 6 パスフレーズを入力します。

（注） ログインパスフレーズを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスフレーズも作成できます。

ステップ 7 変更を送信し、保存します。

ユーザの編集

パスフレーズなどを変更するには、この手順を使用します。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。
ステップ 2 [ユーザー（Users）] 一覧でユーザーの名前をクリックします。
ステップ 3 ユーザに対して変更を行います。
ステップ 4 変更を送信し、保存します。

ユーザにパスフレーズの変更を強制

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。
ステップ 2 [ユーザー（Users）] 一覧からユーザーを選択します。
ステップ 3 [パスフレーズ変更を適用（Enforce Passphrase Change）] をクリックします。
ステップ 4 次回のログイン時または指定した期間（日数）が経過した後にユーザがパスフレーズを変更する必要があるかどうかを選択します。
ステップ 5 （任意）指定した期間が経過した後にパスフレーズの変更を適用する場合は、パスフレーズの期限切れ後にパスフレーズをリセットするまでの猶予期間（日数）を設定します。
ステップ 6 [OK] をクリックします。
ステップ 7 変更を送信し、保存します。

ユーザの削除

手順

ステップ 1 [ユーザー（Users）] 一覧でユーザーの名前に対応するゴミ箱アイコンをクリックします。
ステップ 2 表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。
ステップ 3 変更を保存します。

メッセージ トラッキングでの機密情報へのアクセスの制御

機密情報が含まれている可能性のあるメッセージの詳細に対し、管理アクセスを制限することが必要になる場合があります。

- データ損失防止（DLP）ポリシーに違反するメッセージには、企業の秘密情報、またはクレジットカード番号や医療記録を含む個人情報などの情報が含まれている可能性があります。デフォルトでは、この内容は、電子メールゲートウェイへのアクセスを持つすべてのユーザが閲覧可能です。
- アウトブレイク フィルタ、またはURL レピュテーションもしくはカテゴリに基づくコンテンツ フィルタによって捕捉されるURLも、機密性が高いと見なされる場合があります。デフォルトでは、この内容を閲覧できるのは、管理者特権を持つユーザのみです。

この機密性の高い内容は、メッセージ トラッキング結果に表示されたメッセージの [メッセージの詳細（Message Details）] ページにある専用のタブに表示されます。

これらのタブとその内容は、管理ユーザに対し、そのユーザ ロールに基づいて非表示にできます。ただし、管理者ロールを持つユーザに対してこの機密性の高い内容を非表示にするオプションはありますが、管理者ロールを持つユーザは、これらの権限を変更できるため、機密性の高い情報をいつでも閲覧することができます。

はじめる前に

これらの機能の前提条件を満たしていることを確認します。メッセージ トラッキングの URL 詳細の表示 （562 ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] ページに移動します。

ステップ 2 [メッセージトラッキング内の機密情報へのアクセス（Access to Sensitive Information in Message Tracking）] で、[設定の編集（Edit Settings）] をクリックします。

ステップ 3 機密情報のタイプごとに、データへのアクセス権を付与するロールを選択します。

メッセージ トラッキングにアクセスできないカスタム ロールはこの情報を見ることができないため、表示されません。

ステップ 4 変更を送信し、保存します。

次のタスク

関連項目

- メッセージ トラッキングの詳細 （1122 ページ）
- メッセージ トラッキングでの機密性の高い DLP データの表示 （657 ページ）
- メッセージ トラッキングの URL 詳細の表示 （562 ページ）

委任管理のためのカスタム ユーザー ロールの管理

カスタムユーザーロールを設計し、組織内でのそれぞれのロールに一致した特定の責任をユーザーに委任することができます。委任管理者は、それぞれが責任を負う電子メール セキュリティ機能にのみアクセスでき、それぞれのロールに関連しないシステム設定機能にはアクセスできません。委任管理を行うことで、電子メールゲートウェイの電子メールセキュリティ機能に対するユーザのアクセスを、定義済みのAdministrator、Operator、およびHelp Desk Userロールより柔軟に制御できるようになります。

たとえば、電子メールゲートウェイの特定ドメインの電子メールポリシーの管理に関与しているユーザがいる場合に、それらのユーザに、定義済みのAdministratorおよびOperatorロールで付与されるシステム管理やセキュリティサービスの設定機能にはアクセスさせたくないことがあります。それぞれのユーザーに管理するメールポリシーへのアクセス権限、およびそれらのポリシーで処理されるメッセージを管理するために使用できる他の電子メールセキュリティ機能（メッセージ トラッキングやポリシー隔離など）を付与できるメール ポリシー管理者用のカスタム ユーザー ロールを作成できます。

GUI で [システム管理（System Administration）] > [ユーザーの役割（User Roles）] ページを使用して（または、CLI で userconfig -> role コマンドを使用して）、カスタム ユーザー ロールを定義し、それぞれが責任を負う電子メール セキュリティ機能（メール ポリシー、DLP ポリシー、電子メール レポート、および隔離など）を管理します。委任管理者が管理できる電子メールセキュリティ機能の一覧については、アクセス権限の割り当て（1199ページ）を参照してください。カスタムロールは、[システム管理（System Administration）]>[ユーザー（Users）] ページを使用して、ローカル ユーザー アカウントを追加または編集するときにも作成できます。詳細については、ユーザーアカウント追加時のカスタムユーザーロールの定義（1205ページ）を参照してください。

カスタム ユーザー ロールを作成する際には、そのロールの責任が他の委任管理者の責任と重複しすぎないようにする必要があります。たとえば、複数の委任管理者が同じコンテンツ フィルタに対する責任を持ち、そのコンテンツ フィルタを異なるメールポリシーで使用する場合、1 人の委任管理者がそのフィルタに加えた変更により、他の委任管理者が管理しているメールポリシーに意図せぬ悪影響を及ぼすことがあります。

カスタム ユーザー ロールを作成すると、他のユーザー ロールと同様にローカル ユーザーと外部認証グループをそのカスタム ユーザー ロールに割り当てることができます。詳細については、ユーザーアカウントを使用する作業（1191ページ）を参照してください。カスタムロールに割り当てられているユーザはCLIにアクセスできないことに注意してください。

関連項目

- [アカウント権限（Account Privileges）] ページ （1199 ページ）
- アクセス権限の割り当て （1199 ページ）
- カスタム ユーザー ロールの定義 （1205 ページ）
- ユーザー アカウント追加時のカスタム ユーザー ロールの定義 （1205 ページ）
- カスタム ユーザー ロールの責任のアップデート （1206 ページ）
- カスタム ユーザー ロールの編集 （1207 ページ）

- カスタム ユーザー ロールの複製 （1207 ページ）
- カスタム ユーザー ロールの削除 （1207 ページ）

[アカウント権限（Account Privileges）] ページ

委任管理者が電子メールゲートウェイにログインすると、[アカウント権限（Account Privileges）] ページに委任管理者が責任を持つセキュリティ機能へのリンク、およびそれぞれのアクセス権限についての簡単な説明が表示されます。委任管理者は、[オプション（Options）] メニューで [アカウント権限（Account Privileges）] を選択することでこのページに戻ることができます。委任管理者は、Web ページの上部にあるメニューを使用して、管理する機能にアクセスすることもできます。

次の図は、メール ポリシー、電子メール レポーティング、メッセージ トラッキング、および隔離にアクセスできる委任管理者の [アカウント権限（Account Privileges）] ページを示しています。

図 *72 :* 委任管理者の *[アカウント権限（Account Privileges）]* ページ

アクセス権限の割り当て

カスタム ユーザー ロールを作成する場合、委任管理者が責任を負うセキュリティ機能へのアクセス レベルを定義します。

委任管理者が管理できるセキュリティ機能は以下のとおりです。

- 送受信のメールポリシーとコンテンツフィルタ。
- データ損失防止（DLP）ポリシー
- 電子メールレポーティング
- メッセージ トラッキング
- トレースデバッグツール
- スパム、ポリシー、ウイルス、およびアウトブレイク隔離

- Cisco Email Encryption プロファイル
- ログ サブスクリプション（Log Subscription）

カスタム ユーザー ロールのアクセス レベルを定義したら、委任管理者が責任を負うことになる具体的なメール ポリシー、コンテンツ フィルタ、DLP ポリシー、隔離、または暗号化プロファイルを割り当てる必要があります。

たとえば、異なる DLP ポリシーに対して責任を負う 2 つの異なる DLP ポリシー管理者ロールを作成できます。1 つのロールは企業の秘密保持や許容範囲での使用に関する DLP 違反にのみ責任を負い、他のロールはプライバシー保護に関する DLP 違反に責任を負うようにできます。DLP ポリシーへのアクセスに加えて、これらのカスタム ユーザー ロールにはメッセージ データのトラッキング、隔離とレポートの表示に対する権限を割り当てることもできます。それらのロールは、メッセージ トラッキングの使用において責任を負うポリシーに関連する DLP 違反を検索できます。

カスタム ユーザー ロールに割り当てることができる責任については、[ユーザーの役割（User Roles）] ページの [代表管理者用のカスタムのユーザー役割（Custom User Roles for Delegated Administration）] テーブル内の割り当て済み権限のリンクをクリックして確認できます。カスタム ユーザー ロールの責任のアップデート （1206 ページ） を参照してください。

関連項目

- メール ポリシーとコンテンツ フィルタ （1200 ページ）
- DLP ポリシー （1202 ページ）
- 電子メール レポーティング （1203 ページ）
- メッセージ トラッキング （1204 ページ）
- トレース （1204 ページ）
- 隔離 （1204 ページ）
- 暗号化プロファイル （1205 ページ）
- ログ サブスクリプション （1205 ページ）

メール ポリシーとコンテンツ フィルタ

メールポリシーとコンテンツフィルタのアクセス権限では、電子メールゲートウェイ上の送受信メールポリシーとコンテンツフィルタへの委任管理者のアクセスレベルを定義します。特定のメール ポリシーとコンテンツ フィルタをカスタム ユーザー ロールに割り当て、そのロールに属する委任管理者、およびOperator と Administrator だけがメール ポリシーとコンテンツ フィルタを管理できるようにすることができます。

このアクセス権限を持つすべての委任管理者は、デフォルトの送受信メール ポリシーを表示できますが、すべてのアクセス権限を持っている場合のみそれらのポリシーを編集できます。

アクセス権限を持つすべての委任管理者は、それぞれのメール ポリシーで使用する新しいコンテンツ フィルタを作成できます。委任管理者が作成したコンテンツ フィルタは、そのカスタム ユーザー ロールに割り当てられているの他の委任管理者が使用できます。いずれのカスタム ユーザー ロールにも割り当てられていないコンテンツ フィルタはパブリックであり、メー

ル ポリシーのアクセス権限を持つすべての委任管理者が表示できます。OperatorやAdministratorが作成したコンテンツ フィルタは、デフォルトでパブリックです。委任管理者は、それぞれのカスタム ユーザー ロールに割り当てられているメール ポリシーの既存のコンテンツ フィルタはすべてイネーブルまたはディセーブルにできますが、パブリック コンテンツ フィルタは変更も削除もできません。

委任管理者が自分のポリシー以外のメール ポリシーで使用されているコンテンツ フィルタを削除した場合、またはそのコンテンツ フィルタが他のカスタム ユーザー ロールに割り当てられている場合、AsyncOSはそのコンテンツ フィルタをシステムから削除しません。代わりに、AsyncOS はそのカスタム ユーザー ロールからコンテンツ フィルタのリンクを解除し、委任管理者のメール ポリシーから削除します。そのコンテンツ フィルタは、他のカスタム ユーザー ロールとメール ポリシーでは引き続き使用可能です。

委任管理者は、それぞれのコンテンツ フィルタで任意のテキスト リソースやディクショナリを使用できますが、GUI で [テキスト リソース（Text Resources）] ページや [ディクショナリ（Dictionaries）] ページにアクセスして、それらを表示または変更することはできません。委任管理者は、新しいテキスト リソースやディクショナリを作成することもできません。

送信メール ポリシーの場合、委任管理者は DLP ポリシーをイネーブルまたはディセーブルできますが、DLP ポリシーの権限も持っている場合を除き、DLP の設定をカスタマイズすることはできません。

メール ポリシーとコンテンツ フィルタ用の以下のアクセス レベルのいずれかをカスタム ユーザー ロールに割り当てることができます。

- **アクセスなし（No access）**：委任管理者は、 電子メールゲートウェイのメールポリシーとコンテンツフィルタを表示も編集もできません。
- **割り当てられた隔離を表示、割り当てられた隔離を編集（View assigned, edit assigned）**：委任管理者はカスタム ユーザー ロールに割り当てられているメール ポリシーとコンテンツ フィルタを表示および編集でき、新しいコンテンツ フィルタを作成できます。委任管理者は、ポリシーのスパム対策、ウイルス対策、およびアウトブレイク フィルタの設定を編集できます。委任管理者はポリシーに対してそれぞれのコンテンツ フィルタをイネーブルにでき、責任があるものかどうかに関係なく、そのポリシーに割り当てられている既存のコンテンツ フィルタをディセーブルにできます。委任管理者はメール ポリシーの名前、その送信者、受信者、またはグループを変更することはできません。委任管理者は、それぞれのカスタム ユーザー ロールに割り当てられているメール ポリシーのコンテンツ フィルタの順序を変更できます。
- **すべてを表示、割り当てられた隔離を編集（View all, edit assigned）**：委任管理者は、 電子メールゲートウェイのすべてのメールポリシーとコンテンツフィルタを表示できますが、そのカスタムユーザロールに割り当てられているもののみ編集できます。

すべてを表示、すべてを編集（フルアクセス）（View all, edit all (full access)）：委任管理者は、電子メールゲートウェイのすべてのメールポリシーとコンテンツフィルタ（デフォルトのメールポリシーを含む）に対するすべてのアクセス権限を持ち、新しいメールポリシーを作成できます。委任管理者は、すべてのメール ポリシーの送信者、受信者、およびグループを変更できます。メール ポリシーの順序を変更することもできます。

[ユーザーの役割（User Roles）] ページの [電子メールセキュリティ マネージャ（Email Security Manager）] または [代表管理者用のカスタムのユーザー役割（Custom User Roles for Delegated

Administration）]テーブルを使用して、個々のメールポリシーとコンテンツ フィルタをカスタム ユーザー ロールに割り当てることができます。

[代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] テーブルを使用したメール ポリシーとコンテンツ フィルタの割り当ての詳細については、カスタム ユーザー ロールの責任のアップデート （1206 ページ）を参照してください。

DLP ポリシー

DLP ポリシーのアクセス権限では、 電子メールゲートウェイの DLP Policy Manager を介した DLP ポリシーへの委任管理者のアクセスレベルを定義します。DLP ポリシーを特定のカスタムユーザー ロールに割り当て、オペレータと管理者に加えて、委任管理者にそれらのポリシーを管理させることができます。DLP アクセス権を持つ委任管理者は、データ消失防止の Global Settings ページから DLP 設定ファイルをエクスポートできます。

委任管理者がメール ポリシー権限も保持している場合は、 DLP ポリシーをカスタマイズできます。委任管理者は、それぞれの DLP ポリシーの任意のカスタム DLP ディクショナリを使用できますが、カスタム DLP ディクショナリは表示も変更もできません。

DLP ポリシー用の以下のアクセス レベルのいずれかをカスタム ユーザー ロールに割り当てることができます。

- **アクセスなし（No access）**：委任管理者は 電子メールゲートウェイの DLP ポリシーを表示も編集もできません。
- **割り当てられた隔離を表示（View assigned）、割り当てられた隔離を編集（edit assigned）**：委任管理者は DLP Policy Manager を使用して、カスタム ユーザー ロールに割り当てられている DLP ポリシーを表示および編集できます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの名前変更も順序変更もできません。委任管理者は DLP 設定をエクスポートできます。
- **すべてを表示（View all）、割り当てられた隔離を編集（edit assigned）**：委任管理者はカスタム ユーザー ロールに割り当てられている DLP ポリシーを表示および編集できます。委任管理者は DLP 設定をエクスポートできます。委任管理者は、そのカスタム ユーザー ロールに割り当てられていない DLP ポリシーをすべて表示できますが、編集することはできません。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序変更やポリシー名の変更はできません。
- **すべてを表示、すべてを編集（フルアクセス）（View all, edit all (full access)）**：委任管理者は、 電子メールゲートウェイのすべての DLP ポリシーに対するすべてのフルアクセス権限を持ち、新しいポリシーを作成することもできます。委任管理者は、DLP Policy Manager 内の DLP ポリシーの順序を変更できます。 電子メールゲートウェイで使用する DLP モードは変更できません。

[ユーザーの役割（User Roles）] ページの [DLPポリシーマネージャ（DLP Policy Manager）] または [代表管理者用のカスタムのユーザー役割（Custom User Roles for Delegated Administration）] テーブルを使用して、個々の DLP ポリシーをカスタム ユーザー ロールに割り当てることができます。

DLP ポリシーや DLP Policy Manager の詳細については、データ損失の防止 （625 ページ）を参照してください。

[代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] の一覧を使用して DLP ポリシーを割り当てる方法の詳細については、カスタム ユーザー ロールの責任のアップデート （1206 ページ）を参照してください。

電子メール レポーティング

電子メール レポーティングのアクセス権限では、カスタムユーザー ロールのメール ポリシー、コンテンツ フィルタ、および DLP ポリシーへのアクセス権限に従い、委任管理者が表示できるレポートと [電子メール セキュリティ モニタ（Email Security Monitor）] ページを定義します。それらのレポートは割り当てられているポリシーに対してフィルタリングされていません。委任管理者は、自分が責任を負っていないメールと DLP ポリシーのレポートを表示できます。

電子メール レポーティング用の以下のアクセス レベルのいずれかをカスタム ユーザー ロールに割り当てることができます。

- **アクセスなし（No access）**：委任管理者は、 電子メールゲートウェイのレポートを表示できません。
- **関連するレポートを表示（View relevant reports）**：委任管理者は、[電子メール セキュリティ モニタ（Email Security Monitor）] ページにあるそれぞれのメール ポリシー、コンテンツ フィルタ、およびDLPポリシーのアクセス権限に関連するレポートを表示できます。メール ポリシーとコンテンツ フィルタのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。
  - 概要
  - 受信メール
  - [送信先（Outgoing Destinations）]
  - [送信者（Outgoing Senders）]
  - [内部ユーザ（Internal Users）]
  - コンテンツ フィルタ
  - ウイルス アウトブレイク（Virus Outbreaks）
  - ウイルスの種類
  - アーカイブ レポート（Archived Reports）

  DLP ポリシーのアクセス権限がある委任管理者は、以下の [電子メール セキュリティ モニタ（Email Security Monitor）] ページを表示できます。
  - 概要
  - DLP インシデント（DLP Incidents）
  - アーカイブ レポート（Archived Reports）
- **すべてのレポートを表示（View all reports）**：委任管理者は、 電子メールゲートウェイのすべてのレポートと [電子メールセキュリティモニタ（Email Security Monitor）] ページを表示できます。

電子メール レポーティングと [電子メール セキュリティ モニタ（Email Security Monitor）] の詳細については、電子メールセキュリティ モニタの使用方法 （1009ページ）の章を参照してください。

メッセージ トラッキング

メッセージ トラッキングのアクセス権限では、カスタム ユーザー ロールに割り当てられている委任管理者がメッセージ トラッキングへのアクセス権限を持つかどうかを定義します。メッセージ トラッキングには、[システム管理（System Administration）]>[ユーザー（Users）]ページで [DLP トラッキング ポリシー（DLP Tracking Policies）] オプションがイネーブルになっていて、カスタム ユーザー ロールに DLP ポリシーのアクセス権限もある場合に、組織の DLP ポリシー違反となる可能性があるメッセージの内容も含まれます。

委任管理者はそれぞれに割り当てられている DLP ポリシーに対する DLP 違反のみ検索できます。

メッセージ トラッキングの詳細については、メッセージ トラッキング （1113 ページ）を参照してください。

委任管理者に、メッセージ トラッキング内の一致した DLP の内容を表示するためのアクセスを許可する方法の詳細については、メッセージ トラッキングでの機密情報へのアクセスの制御（1197 ページ）を参照してください。

トレース

トレースのアクセス権限では、カスタム ユーザー ロールに割り当てられている委任管理者がトレースを使用して、システムを介したメッセージ フローをデバッグできるかどうかを定義します。アクセス権限がある委任管理者は、トレースを実行して、生成されるすべての出力を表示できます。トレース結果は、委任管理者のメールまたは DLP ポリシー権限に基づきフィルタリングはされません。

トレースの使用方法の詳細については、テスト メッセージを使用したメール フローのデバッグ：トレース （1515 ページ）を参照してください。

隔離

隔離のアクセス権限では、委任管理者が割り当てられた隔離を管理できるかどうかを定義します。委任管理者は、割り当てられた隔離内の任意のメッセージを表示して、メッセージの解放や削除などのアクションを実行できますが、隔離の設定（サイズ、保存期間など）の変更、検疫の作成または削除はできません。

[モニタ（Monitor）]>[隔離（Quarantines）]ページまたは [ユーザーの役割（User Roles）]ページの [代表管理者用のカスタムのユーザー役割（Custom User Roles for Delegated Administration）] テーブルを使用して、任意の隔離をカスタム ユーザー ロールに割り当てることができます。

管理ユーザに隔離管理タスクを割り当てる方法については、メッセージ処理タスクの他のユーザへの割り当てについて （1142 ページ）とスパム隔離への管理ユーザ アクセスの設定 （1158 ページ）を参照してください。

[代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧を使用して隔離を割り当てる方法の詳細については、カスタム ユーザー ロールの責任のアップデート （1206 ページ）を参照してください。

暗号化プロファイル

暗号化プロファイルのアクセス権限では、委任管理者がコンテンツ フィルタまたは DLP ポリシーの編集時に、それぞれのカスタム ユーザー ロールに割り当てられている暗号化プロファイルを使用できるかどうかを定義します。暗号化プロファイルは、メールまたはDLPポリシーのアクセス権限があるカスタム ユーザー ロールにのみ割り当てることができます。カスタム ロールに割り当てられない暗号化プロファイルは、メールまたは DLP ポリシー権限を持つすべての委任管理者が使用できます。委任管理者はいずれの暗号化プロファイルも表示または変更できません。

暗号化プロファイルは、[セキュリティ サービス（Security Services）] > [IronPort メール暗号化（IronPort Email Encryption）] ページを使用して暗号化プロファイルを作成または編集するときに割り当てることができます。

ログ サブスクリプション

ログ サブスクリプション アクセス権限は、カスタムユーザロールに割り当てられた委任管理者がログサブスクリプションまたはロギング API にアクセスしてログファイルを表示またはダウンロードできるかどうかを定義します。

カスタム ユーザー ロールの定義

GUI で [ユーザの役割（User Roles）] ページを使用して（または CLI で userconfig -> role コマンドを使用して）、新しいユーザ ロールを定義し、そのロールのアクセス権限を割り当てます。[ユーザの役割（User Roles）] ページには、 電子メールゲートウェイの既存のすべてのカスタムユーザロールと各ロールのアクセス権限が表示されます。

手順

ステップ 1 [システム管理（System Administration）] > [User Roles（ユーザの役割）] を選択します。

ステップ 2 [ユーザ役割の追加（Add User Role）] をクリックします。

ステップ 3 ユーザー ロールの名前を入力します。

ステップ 4 ユーザー ロールの説明とその権限を入力します。

ステップ 5 ユーザーロールのアクセス権限を選択します。（各タイプのアクセス権限の詳細については、アクセス権限の割り当て （1199 ページ）を参照してください）。

ステップ 6 変更を送信し、保存します。

ユーザー アカウント追加時のカスタム ユーザー ロールの定義

電子メールゲートウェイに対してローカルユーザアカウントの追加または編集を行う際に、新しいカスタムユーザロールを作成できます。

ユーザーアカウントの追加の詳細については、ユーザの管理（1194ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] ページに移動します。

ステップ 2 [ユーザの追加（Add User）] をクリックします。

ステップ 3 ユーザー アカウント作成時には、[カスタム役割（Custom Roles）] を選択します。

ステップ 4 [役割を追加（Add Role）] を選択します。

ステップ 5 新しいロールの名前を入力します。

ステップ 6 新しいユーザ アカウントを送信します。

AsyncOS により、新しいユーザー アカウントとカスタム ユーザー ロールが追加されたという通知が表示されます。

ステップ 7 [システム管理（System Administration）] > [ユーザの役割（User Roles）] ページに移動します。

ステップ 8 [代表管理者用のカスタムのユーザー役割（Custom User Roles for Delegated Administration）] テーブルでカスタム ユーザー ロールの名前をクリックします。

ステップ 9 ユーザー ロールの説明とその権限を入力します。

ステップ 10 ユーザー ロールのアクセス権限を選択します。（各タイプのアクセス権限の詳細については、アクセス権限の割り当て（1199 ページ）を参照してください）。

ステップ 11 変更を送信し、保存します。

カスタム ユーザー ロールの責任のアップデート

手順

ステップ 1 [システム管理（System Administration）] > [ユーザの役割（User Roles）] ページに移動します。

ステップ 2 アップデートするカスタム ユーザー ロールのアクセス権限の名前をクリックします。

AsyncOS により、 電子メールゲートウェイで使用可能なすべてのメールポリシー、コンテンツフィルタ、DLP ポリシー、または隔離の一覧、およびその他すべての割り当て済みカスタムユーザロールの名前が表示されます。

ステップ 3 委任管理者に責任を割り当てるメール ポリシー、コンテンツ フィルタ、DLP ポリシー、または隔離を選択します。

ステップ 4 変更を送信し、保存します。

カスタム ユーザー ロールの編集

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）] ページに移動します。

ステップ 2 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧でユーザ ロールの名前をクリックします。

ステップ 3 ユーザー ロールに変更を加えます。

ステップ 4 変更を送信し、保存します。

カスタム ユーザー ロールの複製

同様のアクセス権限がある複数のカスタム ユーザー ロールを作成し、異なるユーザーのセットに異なる責任を割り当てたいことがあります。たとえば、電子メールゲートウェイが複数ドメインのメッセージを処理する場合、同様のアクセス権限だが、ドメインに基づく異なるメールポリシーに対する権限であるカスタムユーザロールを作成することができます。こうすることで、委任管理者は、他の委任管理者の責任を妨げることなくそれぞれのドメインのメールポリシーを管理できます。

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）] ページに移動します。

ステップ 2 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧で、複製するユーザ ロールに対応する複製アイコンをクリックします。

ステップ 3 カスタム ユーザー ロールの名前を変更します。

ステップ 4 新しいカスタム ユーザー ロールに必要なすべてのアクセス権限の変更を行います。

ステップ 5 変更を送信し、保存します。

カスタム ユーザー ロールの削除

カスタムロールが削除されると、ユーザは未割り当て状態になり、電子メールゲートウェイにアクセスできなくなります。複数の個人に割り当てられたカスタム ユーザー ロールを削除すると、警告メッセージを受信しません。削除したカスタム ユーザー ロールに割り当てられていたすべてのユーザーを再割り当てする必要があります。

手順

ステップ 1 [システム管理（System Administration）]>[ユーザの役割（User Roles）]ページに移動します。

ステップ 2 [代表管理者用のカスタムのユーザ役割（Custom User Roles for Delegated Administration）] 一覧で、削除するユーザ ロールに対応するゴミ箱のアイコンをクリックします。

ステップ 3 表示される警告ダイアログで [削除（Delete）] をクリックして削除を確認します。

ステップ 4 変更を保存します。

パスフレーズ

- パスフレーズの変更 （1208 ページ）
- ユーザー アカウントのロックおよびロック解除 （1209 ページ）
- 制限的なユーザ アカウントとパスフレーズの設定値の構成 （1209 ページ）
- 外部認証 （1210 ページ）
- 二要素認証 （1215 ページ）

パスフレーズの変更

管理ユーザは GUI の最上部にある [オプション（Options）]>[パスフレーズの変更（Change Passphrase）] リンクを使用して自分のパスフレーズを変更できます。

新しいパスフレーズを送信するとすぐにログアウトされ、ログイン画面が表示されます。

CLI で、passphrase コマンドまたは passwd コマンドを使用してパスフレーズを変更します。「admin」ユーザー アカウントのパスフレーズを忘れた場合は、パスフレーズをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

（注） ログインパスフレーズを手動で作成することに加えて、電子メールゲートウェイにログインするためのシステム生成パスフレーズも作成できます。

passphrase コマンドでは、セキュリティのために古いパスフレーズの入力が必要です。

（注） パスフレーズの変更はすぐに有効になり、変更の確定は必要ではありません。

ユーザー アカウントのロックおよびロック解除

ユーザアカウントのロックは、ローカルユーザが電子メールゲートウェイにログインするのを防止します。ユーザー アカウントは、次のいずれかの場合にロックされることがあります。

- AsyncOS は、ユーザが [ローカルユーザアカウントとパスフレーズの設定（Local User Account & Passphrase Settings）] セクションで定義されている失敗ログイン試行の最大回数を超えた場合にユーザ アカウントをロックします。
- 管理者は、[システム管理（System Administration）]>[ユーザー（Users）] ページを使用して、セキュリティ目的でユーザー アカウントを手動でロックできます。

[ユーザ役割の編集（Edit User）] ページでユーザ アカウントを表示すると、AsyncOS によりユーザ アカウントがロックされた理由が表示されます。

ユーザー アカウントをロック解除するには、[ユーザー（Users）] 一覧でユーザー名をクリックしてユーザー アカウントを開き、[アカウントのロック解除（Unlock Account）] をクリックします。

ローカル ユーザー アカウントを手動でロックするには、[ユーザー（Users）] 一覧でユーザー名をクリックしてユーザー アカウントを開き、[アカウントのロック（Lock Account）] をクリックします。AsyncOS は、ユーザが電子メールゲートウェイにログインできなくなるというメッセージを表示し、継続するかどうかを問い合わせてきます。

ユーザーが設定した試行回数を超えた後でログインに失敗した場合、すべてのローカル ユーザーアカウントをロックするように設定することもできます。詳細については、制限的なユーザ アカウントとパスフレーズの設定値の構成 （1209 ページ）を参照してください。

（注） admin アカウントをロックした場合は、シリアル コンソール ポートへのシリアル通信接続経由で admin としてログインしてロック解除するしかありません。admin ユーザは、admin アカウントがロックされた場合でも、シリアルコンソールポートを使用して常に電子メールゲートウェイにアクセスできます。シリアルコンソールポートを使用して電子メールゲートウェイにアクセスする方法の詳細については、電子メールゲートウェイへの接続 （28 ページ）を参照してください。

制限的なユーザ アカウントとパスフレーズの設定値の構成

ユーザー アカウントとパスフレーズの制限を定義して、組織全体にパスフレーズ ポリシーを強制的に適用することができます。ユーザアカウントとパスフレーズの制限は、 電子メールゲートウェイに定義されたローカルユーザに適用されます。次の設定値を設定できます。

- **ユーザーアカウントのロック。**ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。
- **パスフレーズ存続期間のルール。**ログイン後にユーザがパスフレーズの変更を要求されるまでの、パスフレーズの存続期間を定義できます。
- **パスフレーズのルール。**任意指定の文字や必須の文字など、ユーザが選択できるパスフレーズの種類を定義できます。

ユーザーアカウントとパスフレーズの制限は、[システム管理（System Administration）]>[ユーザー（Users）]ページの[ローカル ユーザー アカウントとパスフレーズの設定（Local User Account & Passphrase Settings）]セクションで定義します。

外部認証

ネットワークのLDAPまたはRADIUSディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用して 電子メールゲートウェイにログインするユーザを認証するよう 電子メールゲートウェイを設定できます。認証のために外部ディレクトリを使用するよう 電子メールゲートウェイを設定するには、GUI で[システム管理（System Administration）]>[ユーザー（Users）]ページを使用するか、CLI で userconfig コマンドと external サブコマンドを使用します。

外部認証がイネーブルの状態でユーザが電子メールゲートウェイにログインすると、電子メールゲートウェイは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、 電子メールゲートウェイは最初に設定された外部サーバをチェックして、ユーザがそこで定義されたかどうかを確認します。 電子メールゲートウェイが最初の外部サーバに接続できなければ、 電子メールゲートウェイは一覧の次の外部サーバをチェックします。

LDAPサーバの場合は、ユーザが外部サーバで認証に失敗すると、電子メールゲートウェイはここで定義されたローカルユーザとしてユーザを認証しようとします。そのユーザが外部サーバまたは電子メールゲートウェイに存在しない場合、またはユーザが間違ったパスフレーズを入力した場合は、 電子メールゲートウェイへのアクセスが拒否されます。

外部RADIUSサーバに接続できなければ、一覧の次のサーバが試行されます。すべてのサーバに接続できない場合、電子メールゲートウェイはここで定義されたローカルユーザとしてユーザを認証しようとします。ただし、外部RADIUSサーバが何らかの理由（パスフレーズ間違いやユーザ未登録など）でユーザを拒否すると、電子メールゲートウェイへのアクセスは拒否されます。

関連項目

- LDAP 認証のイネーブル化 （1210 ページ）
- RADIUS 認証の有効化 （1211 ページ）
- SAML 認証の有効化 （1214 ページ）

LDAP 認証のイネーブル化

ユーザーを認証するためにLDAPディレクトリを使用する以外に、LDAPグループをCiscoユーザー ロールに割り当てることができます。たとえば、ITグループのユーザーを管理者ユーザー ロールに割り当てたり、Supportグループのユーザーをヘルプデスク ユーザー ロールに割り当てたりできます。1人のユーザが複数のLDAPグループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可がAsyncOSによってそのユーザに付与されます。たとえば、ユーザがOperator権限を持つグループとHelp Desk User権限を持つグループに属する場合、AsyncOSはユーザにHelp Desk User ロールの権限を割り当てます。

（注） 外部ユーザが自分の LDAP グループのユーザロールを変更する場合は、 電子メールゲートウェイからログアウトして再度ログインする必要があります。これにより、そのユーザに新しいロールの権限が付与されます。

はじめる前に

LDAP サーバの LDAP サーバプロファイルおよび外部認証クエリーを定義します。詳細については、LDAP クエリ （943 ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 **[Web 認証（Web Authentication）]** セクションまでスクロールします。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 **[外部認証を有効にする（Enable External Authentication）]** チェックボックスをオンにします。

ステップ 5 認証タイプとして **[LDAP]** を選択します。

ステップ 6 Web ユーザー インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

ステップ 7 ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 8 タイムアウトするまで電子メールゲートウェイがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 9 電子メールゲートウェイで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 10 また、[行の追加（Add Row）] をクリックして別のディレクトリ グループを追加することもできます。 電子メールゲートウェイが認証する各ディレクトリグループに対してステップ 9 とステップ 10 を繰り返します。

ステップ 11 変更を送信し、保存します。

RADIUS 認証の有効化

ユーザの認証に RADIUS ディレクトリを使用し、ユーザのグループを Cisco ロールに割り当てることもできます。RADIUS サーバは CLASS 属性をサポートする必要があります（AsyncOS は RADIUS ディレクトリのユーザーを Cisco ユーザー ロールに割り当てるために CLASS 属性を使用します）。AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の 2 つの認証プロトコルをサポートします。

RADIUS ユーザーを Cisco ユーザー ロールに割り当てるには、最初に RADIUS サーバで <radius-group> という文字列値を使用して CLASS 属性を設定します（これは Cisco ユーザー ロールにマップされます）。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用することはできません。AsyncOS は CLASS 属性で複数の値

をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザは、 電子メールゲートウェイにログインできません。

電子メールゲートウェイが RADIUS サーバと通信できない場合、ユーザは 電子メールゲートウェイのローカルユーザアカウントでログインできます。

（注） 外部ユーザが RADIUS グループのユーザ ロールを変更する場合は、アプライアンスからログアウトして再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] ページで、[有効（Enable）] をクリックします。

ステップ 2 すでに有効になっていない場合は、[外部認証を有効にする（Enable External Authentication）] オプションをオンにします。

ステップ 3 RADIUS サーバのホスト名を入力します。

ステップ 4 RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。

ステップ 5 RADIUS サーバの共有秘密パスワードを入力します。

ステップ 6 タイムアウトするまで電子メールゲートウェイがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7 （任意）[行を追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS サーバについて、3 ～ 6 のステップを繰り返します。

（注） 最大 10 個の RADIUS サーバを追加できます。

ステップ 8 RADIUS サーバに再度問い合わせ、「External Authentication Cache Timeout」フィールドで再認証するまで、AsyncOS が外部認証クレデンシャルを保存する秒数を入力します。デフォルトはゼロ（0）です。

（注） RADIUS サーバがワンタイム パスワード（たとえば、トークンから作成されるパスワード）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

ステップ 9 グループ マッピングの設定

設定	説明
外部認証されたユーザを複数のローカル ロールにマッピング。	AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザを電子メールゲートウェイ ロールに割り当てます。CLASS 属性の要件： • 3 文字以上 • 253 文字以下 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。 複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。 次の 電子メールゲートウェイ ロールは、制限の少ないものから順番に並べられています。 • admin • 管理者（Administrator） • 専門技術者 • Operator cloudadmin • Read-only Operator • ヘルプ デスク ユーザー • ゲスト
外部認証されたすべてのユーザを管理ロールにマップします。	AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。

ステップ 10 Administrator ロールまたは異なる 電子メール ゲートウェイ ユーザー ロール タイプにすべての外部認証されたユーザーをマッピングするかを選択します。

ステップ 11 異なるロールタイプにユーザをマッピングする場合、[グループ名（Group Name）]または[ディレクトリ（Directory）] フィールドの RADIUS CLASS 属性に定義されているようにグループ名を入力し、[ロール（Role）] フィールドから 電子メール ゲートウェイ ロール タイプを選択します。[行を追加（Add Row）] をクリックして、さらにロール マッピングを追加できます。

ユーザー ロール タイプの詳細については、ユーザーアカウントを使用する作業（1191 ページ）を参照してください。

ステップ 12 変更を送信し、保存します。

SAML 認証の有効化

SAML を使用したシングル サインオンを有効化し、ユーザを認証してユーザのグループをシスコのルールに割り当てることができます。

始める前に

サービス プロバイダーおよび ID プロバイダーの設定を含む SAML プロファイルが設定済みである必要があります。「電子メールゲートウェイでの SSO の設定方法 （1311 ページ）」を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] に移動します。

ステップ 2 **[Web 認証（Web Authentication）]** セクションまでスクロールします。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 **[外部認証を有効にする（Enable External Authentication）]** チェックボックスをオンにします。

ステップ 5 ドロップダウンリストから、認証タイプとして [SAML] を選択します。

ステップ 6 **（任意）**[外部認証属性名マップ（External Authentication Attribute Name Map）] フィールドに、グループ マッピングから検索する属性名を入力します。

属性名は、SAML 応答をリレーするために ID プロバイダーに対して設定する属性によって異なります。 電子メールゲートウェイは、[グループマッピング（Group Mapping）] フィールドに設定した属性に照らし、SAML 応答からの属性名の一致するエントリを検索します。これは省略可能であり、設定しない場合、 電子メールゲートウェイは、SAML 応答内に存在するすべての属性の一致するエントリを、[グループマッピング（Group Mapping）] フィールドに設定された値と照らして検索します。

ステップ 7 [グループマッピング（Group Mapping）] フィールドに、事前定義済みまたはカスタムのユーザ ロールに基づいて SAML ディレクトリで定義されているグループ名属性を入力します。[行の追加（Add Row）] をクリックして複数のロール マッピングを追加できます。

グループ マッピングには、グループ属性を含める必要があります。「未指定のグループ（Unspecified Groups）」属性を追加して、SAML アサーションまたは応答を認証できます。

ユーザー ロール タイプの詳細については、ユーザーアカウントを使用する作業 （1191 ページ）を参照してください。

（注） [グループマッピング（Group Mapping）] の属性は、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一致している必要があります。

ステップ 8 変更を送信し、保存します。

次のタスク

SAML 外部認証を有効にした後は、 電子メールゲートウェイのログインページにある [シングルサインオンを使用（Use Single Sign On）] リンクを使用し、ユーザ名を入力して 電子メールゲートウェイにログインできます。

二要素認証

RADIUS ディレクトリを使用して、特定のユーザ ロールの二要素認証を設定できます。 電子メールゲートウェイは、RADIUS サーバとの通信に使用する次の認証プロトコルをサポートします。

- Password Authentication Protocol（PAP）
- Challenge Handshake Authentication Protocol（CHAP）

次のユーザ ロールに対して二要素認証を有効にできます。

- 定義済み
- カスタム

機能は次によりテストされています。

- RSA 認証マネージャ v8.2
- FreeRADIUS v1.1.7 以上
- ISE v1.4 以降

関連項目

- 二要素認証の有効化 （1215 ページ）
- 二要素認証の無効化 （1216 ページ）

二要素認証の有効化

はじめる前に

IT 管理者から二要素認証に必要な RADIUS サーバの詳細を入手していることを確認します。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] ページで、[二要素認証（Two-Factor Authentication）] の下の [有効にする（Enable）] をクリックします。

ステップ 2 RADIUS サーバのホスト名または IP アドレスを入力します。

ステップ 3 RADIUS サーバのポート番号を入力します。

ステップ 4 RADIUS サーバの共有秘密パスワードを入力します。

ステップ 5 タイムアウトまでにサーバからの応答を待つ時間を秒単位で入力します。

ステップ 6 適切な認証プロトコルを選択します。

ステップ 7 （任意）[行の追加（Add Row）] をクリックして別の RADIUS サーバを追加します。各 RADIUS サーバについて、2 ～ 6 のステップを繰り返します。

（注） 最大 10 個の RADIUS サーバを追加できます。

ステップ 8 二要素認証を有効にする必須ユーザ ロールを選択します。

ステップ 9 変更を送信し、保存します。

二要素認証を有効にすると、ユーザは電子メールゲートウェイにログインするために、ユーザ名とパスフレーズを入力した後にパスコードを入力することが求められます。

二要素認証の無効化

はじめる前に

お使いの 電子メールゲートウェイで二要素認証を有効にしていることを確認します。

手順

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] ページで、[二要素認証（Two-Factor Authentication）] の下の [グローバル設定を編集（Edit Global Settings）] クリックします

ステップ 2 [二要素認証を有効にする（Enable Two-Factor Authentication）] の選択を解除します。

ステップ 3 変更を送信し、保存します。

電子メールゲートウェイへのアクセスの設定

AsyncOS では、電子メールゲートウェイへのユーザのアクセス権管理を、管理者が制御できます。これを使用して、Web UI セッションのタイムアウトや、ユーザと組織のプロキシサーバから電子メールゲートウェイへのアクセス元となる IP アドレスを指定する、アクセスリストなどを管理できます。

関連項目

- IP ベースのネットワーク アクセスの設定 （1217 ページ）
- セッション タイムアウトの設定 （1219 ページ）

IP ベースのネットワーク アクセスの設定

アプライアンスに直接接続するユーザおよび逆プロキシで接続するユーザ（リモートユーザに逆プロキシを使用する組織の場合）のアクセスリストを作成して、電子メールゲートウェイにアクセスするユーザの IP アドレスを制御できます。

関連項目

- 直接接続 （1217 ページ）
- プロキシ経由の接続 （1217 ページ）
- ネットワーク アクセスを制限する際の重要な注意事項 （1217 ページ）
- アクセス リストの作成 （1218 ページ）

直接接続

電子メールゲートウェイに接続可能なマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセスリストの IP アドレスを持つすべてのマシンから、電子メールゲートウェイにアクセスできます。リストに含まれていないアドレスから電子メールゲートウェイに接続しようとするユーザのアクセスは拒否されます。

プロキシ経由の接続

リモートユーザのマシンと電子メールゲートウェイの間で逆プロキシサーバが使用される組織のネットワークの場合、AsyncOS では電子メールゲートウェイに接続可能なプロキシの IP アドレスを含むアクセスリストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモートユーザの IP アドレスを電子メールゲートウェイに送信するには、プロキシで x-forwarded-for HTTP ヘッダーを電子メールゲートウェイへの接続要求に含める必要があります。

x-forwarded-for ヘッダーは RFC 非準拠の HTTP ヘッダーであり、次の形式になります。

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF .

このヘッダーの値はカンマ区切りの IP アドレスのリストです。左端のアドレスがリモートユーザーマシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます（ヘッダー名は設定可能です）。電子メールゲートウェイは、ヘッダーのリモートユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセスリストで許可されたユーザ IP アドレスやプロキシ IP アドレスと照合します。

（注） AsyncOS は x-forwarded-for ヘッダーでは IPv4 アドレスだけをサポートします。

ネットワーク アクセスを制限する際の重要な注意事項

注意：次のいずれかの条件が true の場合、ネットワークアクセスの変更を送信して確定した後、電子メールゲートウェイにアクセスできなくなることがあります。

- **[特定の接続のみを許可（Only Allow Specific Connections）]** を選択し、現在のマシン（クラスタ化環境内の PC、電子メールゲートウェイ、または Cisco Secure Manager Email and Web Gateway など）の IP アドレスがリストに含まれない場合。
- **[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）]** を選択し、現在電子メールゲートウェイに接続されているプロキシの IP アドレスがプロキシリストに存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。
- [特定の直接接続またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）] を選択し、
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合

    または

  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、電子メールゲートウェイに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

アクセス リストの作成

ネットワーク アクセス リストは、GUI または **adminaccessconfig > ipaccess** CLI コマンドを使用して作成できます。

はじめる前に

ネットワークアクセスの設定を変更後、電子メールゲートウェイからロックアウトされないようにします。ネットワークアクセスを制限する際の重要な注意事項 （1217ページ）を参照してください。

手順

ステップ 1 [システム管理（System Administration）] > [Network Access（ネットワーク アクセス）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 アクセス リストの制御モードを選択します。

オプション	説明
すべてを許可（Allow All）	このモードでは、電子メールゲートウェイへのすべての接続が許可されます。 これが操作のデフォルト モードです。
特定の接続のみを許可（Only Allow Specific Connections）	このモードは、ユーザの IP アドレスが、アクセスリストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザの電子メールゲートウェイへの接続を許可します。

オプション	説明
特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）	このモードは、次の条件を満たせば、逆プロキシ経由で電子メールゲートウェイへの接続を許可します。 • 接続プロキシの IP アドレスが、アクセス リストの [プロキシサーバのIPアドレス（IP Address of Proxy Server）] フィールドに含まれている。 • プロキシの接続要求に **`x-forwarded-header`** HTTP ヘッダーが記載されている。 • **`x-forwarded-header`** の値が空ではない。 • リモート ユーザの IP アドレスが x-forwarded-header に含まれ、それがアクセス リスト内のユーザに対して定義された IP アドレス、IP 範囲、または CIDR 範囲と一致する。
特定の直接またはプロキシ経由接続のみを許可（Only Allow Specific Connections Directly or Through Proxy）	このモードは、アクセスリストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザの IP アドレスが一致すれば、電子メールゲートウェイへの逆プロキシ経由接続または直接接続を許可します。プロキシ経由接続の条件は、[特定のプロキシ経由接続のみを許可（Only Allow Specific Connections Through Proxy）] モードと同じです。

ステップ 4 電子メールゲートウェイへの接続を許可するユーザの IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを指定する場合は、カンマで区切ります。

ステップ 5 プロキシ経由接続が許可されている場合は、次の情報を入力します。

1. 電子メールゲートウェイへの接続を許可するプロキシの IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。
2. プロキシが電子メールゲートウェイに送信する発信元の IP ヘッダーの名前。これには、リモートユーザマシンの IP アドレスと、要求を転送したプロキシサーバの IP アドレスが含まれます。デフォルトのヘッダー名は x-forwarded-for です。

ステップ 6 変更を送信および確定後に電子メールゲートウェイからロックアウトされる変更が構成されていないことを確認します。

ステップ 7 変更を送信し、保存します。

セッション タイムアウトの設定

• Web UI セッション タイムアウトの設定 （1220 ページ）

• CLI セッション タイムアウトの設定 （1220 ページ）

Web UI セッション タイムアウトの設定

AsyncOS が、電子メールゲートウェイの Web UI から非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッション タイムアウトは以下に適用されます。

- すべてのユーザ（管理者を含む）
- HTTP セッションおよび HTTPS セッション
- Cisco スパム隔離

AsyncOS によってユーザがログアウトされると、電子メールゲートウェイはユーザの Web ブラウザをログインページにリダイレクトします。

手順

ステップ 1 [システム管理（System Administration）] > [Network Access（ネットワーク アクセス）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 ログアウトまでにユーザを非アクティブにできる分数を [Web UI 非アクティブ タイムアウト（Web UI Inactivity Timeout）] フィールドに入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 4 変更を送信し、保存します。

次のタスク

また、CLI で adminaccessconfig コマンドを使用して Web UI セッション タイムアウトを設定することもできます。『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

CLI セッション タイムアウトの設定

AsyncOS が、電子メールゲートウェイの CLI から非アクティブなユーザをログアウトするまでの時間を指定できます。以下に CLI セッション タイムアウトが適用されます。

- すべてのユーザ（管理者を含む）
- セキュア シェル（SSH）、SCP、および直接シリアル接続を使用している接続のみ

（注） CLI セッション タイムアウト時に未確定の設定変更は失われます。設定を変更したらすぐに確定してください。

手順

ステップ 1 [システム管理（System Administration）] > [Network Access（ネットワーク アクセス）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [CLI 非アクティブ タイムアウト（CLI Inactivity Timeout）] フィールドに、ログアウトされるまでにユーザを非アクティブにできる分数を入力します。5 ～ 1440 分のタイムアウト期間を定義できます。

ステップ 4 変更を送信し、保存します。

次のタスク

また、CLI で adminaccessconfig コマンドを使用して CLI セッション タイムアウトを設定することもできます。『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

管理ユーザへのメッセージの表示

- ログイン前のメッセージの表示 （1221 ページ）
- ログイン後のメッセージの表示 （1221 ページ）

ログイン前のメッセージの表示

ユーザが SSH、FTP、または Web UI から電子メールゲートウェイにログインしようとする前にメッセージを表示するように電子メールゲートウェイを設定できます。ログインバナーは、ログインプロンプトの上に表示されるカスタマイズ可能なテキストです。ログインバナーを使用して、内部のセキュリティ情報または電子メールゲートウェイのベストプラクティスに関する説明を表示できます。たとえば、許可しない電子メールゲートウェイの使用を禁止する簡単な注意文言を作成したり、ユーザが電子メールゲートウェイに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

CLI の adminaccessconfig > banner コマンドを使用して、ログイン バナーを作成します。ログイン バナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログインバナーは、電子メールゲートウェイの /data/pub/configuration ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

ログイン後のメッセージの表示

ユーザが SSH、FTP、または Web UI を使用して電子メールゲートウェイに正常にログインした後に、ウェルカムバナーを表示するように AsyncOS を設定できます。ウェルカムバナーを使用して、内部のセキュリティ情報または電子メールゲートウェイのベストプラクティスに関する説明を表示できます。

CLI で adminaccessconfig > welcome コマンドを使用して、ウェルカム バナーを作成します。ウェルカム バナーの最大長は 1600 文字です。

ウェルカムバナーは、電子メールゲートウェイの /data/pub/configuration ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

詳細については、『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

セキュア シェル（SSH）キーの管理

sshconfig コマンドを使用して、次の操作を実行します。

- システムで設定されたユーザ アカウント（admin アカウントを含む）の authorized_keys ファイルにセキュア シェル（SSH）公開ユーザ キーを追加したり、それらのキーを削除したりできます。これにより、パスフレーズチャレンジではなく SSH キーを使用してユーザ アカウントを認証できるようになります。
- 次の SSH サーバの設定を編集できます。
  - 公開キー認証アルゴリズム
  - 暗号アルゴリズム
  - KEX アルゴリズム
  - MAC メソッド
  - 最小サーバ キー サイズ

（注） 電子メールゲートウェイから他のホストマシンへのログファイルの SCP プッシュを実行する場合に使用されるホストキーを設定するには、**logconfig -> hostkeyconfig** を使用します。詳細については、ログ （1391 ページ）を参照してください。

hostkeyconfig を使用すると、リモートホストのキーをスキャンし、電子メールゲートウェイに追加できます。

関連項目

- 例：新しい公開キーのインストール （1222 ページ）
- 例：SSH サーバ設定の編集 （1223 ページ）

例：新しい公開キーのインストール

次の例では、管理者アカウントの新規公開キーをインストールします。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
```

```
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

例：SSH サーバ設定の編集

次に、SSH サーバ設定を編集する方法の例を示します。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup
Enter the Public Key Authentication Algorithms do you want to use
```

```
[rsa1,ssh-dss,ssh-rsa]> rsa1
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,
cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]> aes192-ctr
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96]> hmac-sha1
Enter the Minimum Server Key Size do you want to use
[1024]> 2048
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1]> diffie-hellman-group-exchange-sha1
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
Cipher Algorithms:
        aes192-ctr
MAC Methods:
        hmac-sha1
Minimum Server Key Size:
        2048
KEX Algorithms:
        diffie-hellman-group-exchange-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

リモート SSH コマンド実行

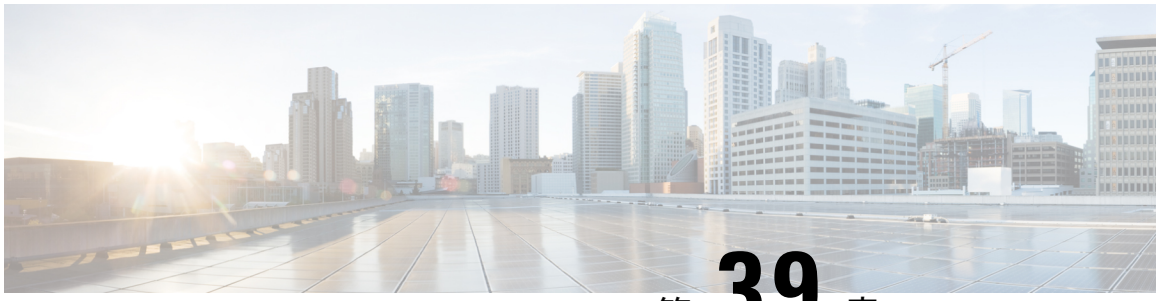
CLI では、リモート SSH コマンド実行を使用してコマンドを実行できます。たとえば、電子メールゲートウェイで admin アカウントに対して SSH 公開キーが設定されている場合は、チャレンジされないリモートホストから次のコマンドを実行できます。

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

管理ユーザー アクセスのモニタリング

目的	操作手順
電子メールゲートウェイについて、アクティブユーザすべてのセッション詳細を表示する	ページ右上で [オプション（Options）]>[アクティブなセッション（Active Sessions）] をクリックします コマンドライン インターフェイスで、w、whoami および who コマンドを使用します。

目的	操作手順
電子メールゲートウェイに最近ログインしたユーザを表示します。 また、リモートホストのIPアドレス、ログイン時間、ログアウト時間、および合計時間も表示する	コマンドライン インターフェイスで last コマンドを使用します。



第 39 章

システム管理

この章は、次の項で構成されています。

（注） このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、付録B「IPアドレスのインターフェイスおよびルーティング」を参照してください。

- 電子メールゲートウェイの管理 （1228 ページ）
- 電子メールゲートウェイのライセンス （1231 ページ）
- 仮想電子メールゲートウェイのライセンス （1242 ページ）
- 設定ファイルの管理 （1243 ページ）
- [設定ファイル（Configuration File）] ページ （1249 ページ）
- ディスク領域の管理 （1249 ページ）
- セキュリティ サービスの管理 （1251 ページ）
- サービス アップデート （1253 ページ）
- アップグレードおよびアップデートを取得するための設定 （1254 ページ）
- AsyncOS のアップグレード （1264 ページ）
- リモート電源再投入の有効化 （1269 ページ）
- AsyncOS の以前のバージョンへの復元 （1271 ページ）
- 電子メールゲートウェイに生成されるメッセージの返信アドレスの設定 （1272 ページ）
- システム状態パラメータのしきい値の設定 （1273 ページ）
- 電子メールゲートウェイの状況の確認 （1274 ページ）
- アラート （1275 ページ）
- ネットワーク設定値の変更 （1303 ページ）
- SAML 2.0 を使用したシングル サインオン（SSO） （1309 ページ）
- AsyncOS API 向けの電子メールゲートウェイでの OpenID Connect 1.0 の設定 （1320 ページ）
- システム タイム （1323 ページ）
- ビューのカスタマイズ （1325 ページ）
- 全般設定 （1327 ページ）
- 最大 HTTP ヘッダー サイズの構成 （1328 ページ）

- サービス エンジンの再起動とステータスの表示 （1328 ページ）
- 国際化ドメイン名（IDN）を含むメッセージの受信と配信 （1329 ページ）

電子メールゲートウェイの管理

以下のタスクでは、電子メールゲートウェイ内の一般的な機能を簡単に管理できます。

- 電子メールゲートウェイのシャットダウンおよび再起動 （1228 ページ）
- 電子メールの受信と配信の一時停止 （1228 ページ）
- 一時停止している電子メールの受信と配信の再開 （1229 ページ）

電子メールゲートウェイのシャットダウンおよび再起動

電子メールゲートウェイは、シャットダウンまたは再起動した後で、配信キュー内のメッセージを失わずに後で再起動できます。

CLI で shutdown または reboot コマンドを使用するか、Web インターフェイスを使用できます。

手順

ステップ 1 [システム管理（System Administration）] > [シャットダウン/サスペンド（Shutdown/Suspend）] を選択します。

ステップ 2 [システム オペレーション（System Operations）] セクションで、[操作（Operation）] ドロップダウン リストから [シャットダウン（Shutdown）] または [再起動（Reboot）] を選択します。

ステップ 3 開いている接続が、強制的に閉じられることなく完了できるまでの許容時間を秒数の単位で入力します。

デフォルトの遅延値は 30 秒です。

ステップ 4 [確定する（Commit）] をクリックします。

電子メールの受信と配信の一時停止

AsyncOS では、電子メールの受信と配信を一時停止できます。次の動作を停止できます。

- 特定のリスナーまたは複数リスナーでの電子メールの受信。
- 特定のドメインまたは複数ドメインへの電子メールの配信。

CLI で suspend コマンドを使用するか、Web インターフェイスを使用します。

手順

ステップ 1 [システム管理（System Administration）] > [シャットダウン/サスペンド（Shutdown/Suspend）] を選択します。

ステップ 2 特定のリスナーまたは複数リスナーでの電子メールの受信を一時停止します。

[メールの操作（Mail Operations）] セクションで、一時停止する機能またはリスナーを選択します。電子メールゲートウェイに複数のリスナーが存在する場合は、リスナー単位で電子メールの受信を停止することもできます。

ステップ 3 特定のドメインまたは複数ドメインへの電子メールの配信を一時停止します。要件に応じて、次のいずれかを実行します。

1. すべての電子メールの配信を停止するには、[ドメイン/サブドメインの指定（Specify Domain(s)/Subdomain(s)）] フィールドに ALL と入力し、[Enter] を押します。
2. 特定のドメインまたはサブドメインへの電子メールの配信を停止するには、[ドメイン/サブドメインの指定（Specify Domain(s)/Subdomain(s)）] フィールドにドメインまたはサブドメインの名前または IP アドレスを入力し、[Enter] を押します。複数のエントリを追加する場合は、カンマ区切りのテキストを使用します。

ステップ 4 開いている接続が、強制的に閉じられることなく完了できるまでの許容時間を秒数の単位で入力します。

開いている接続が存在しない場合、システムはただちにオフラインになります。

デフォルト遅延値は 30 秒です。

ステップ 5 [確定する（Commit）] をクリックします。

次のタスク

一時停止したサービスを再開する準備が整っている場合は、一時停止している電子メールの受信と配信の再開 （1229 ページ）を参照してください。

一時停止している電子メールの受信と配信の再開

一時停止している電子メールの受信と配信を再開するには、[シャットダウン/サスペンド（Shutdown/Suspend）] ページまたは resume コマンドを使用します。

手順

ステップ 1 [システム管理（System Administration）] > [シャットダウン/サスペンド（Shutdown/Suspend）] を選択します。

ステップ 2 [メールの操作（Mail Operations）] セクションで、再開する機能またはリスナーを選択します。

電子メールゲートウェイに複数のリスナーが存在する場合は、リスナー単位で電子メールの受信を再開できます。

ステップ 3 すべての電子メール、または特定の 1 つ以上のドメインへの電子メールの配信を再開します。

[ドメイン/サブドメインの指定（Specify Domain(s)/Subdomain(s)）] フィールドで、該当するエントリを閉じるアイコンをクリックします。

ステップ 4 [確定する（Commit）] をクリックします。

出荷時の初期状態へのリセット

注意 シリアル インターフェイスを使用して、またはデフォルトの Admin ユーザー アカウントで管理ポート上のデフォルト設定を使用して Web インターフェイスまたは CLI に再接続できない場合は、出荷時の初期状態にリセットしないでください。

電子メールゲートウェイを物理的に移動する際、出荷時の初期状態で始めなければならない場合があります。出荷時の設定にリセットすると元に戻せないため、ユニットを移動する場合や、設定の問題を解決する最後の手段としてのみ使用してください。出荷時の初期状態にリセットすると、Web インターフェイスまたは CLI から切断され、 電子メールゲートウェイへの接続に使用したサービス（FTP、SSH、HTTP、HTTPS）がディセーブルにされ、作成した追加のユーザアカウントが削除されます。次の方法で、出荷時の初期状態にリセットできます。

- Web インターフェイスで、[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページの [リセット（Reset）] ボタンをクリックするか、[システム管理（System Administration）]>[システム セットアップ ウィザード（System Setup Wizard）] の [設定情報のリセット（Reset Configuration）] ボタンをクリックします。
- CLI で、**resetconfig** コマンドを使用します。

（注） **resetconfig** コマンドは、 電子メールゲートウェイがオフライン状態にあるときにのみ動作します。出荷時の設定にリセットした後、 電子メールゲートウェイはオンライン状態に戻ります。

次のステップ

- システム セットアップ ウィザードを実行します。詳細については、システム セットアップ ウィザードの使用 （35 ページ）を参照してください。
- メール配信をオンにして、メール配信を再開します。

AsyncOS のバージョン情報の表示

電子メールゲートウェイに現在インストールされている AsyncOS のバージョンを確認するには、Web インターフェイスの [モニタ（Monitor）] メニューから [システム概要（System Overview）] ページを使用するか（システム ステータス （1048 ページ）を参照）、CLI で version コマンドを使用します。

電子メールゲートウェイのライセンス

- ライセンス キー （1231 ページ）
- スマート ソフトウェア ライセンシング （1233 ページ）

ライセンス キー

- ライセンス キーの追加および管理 （1231 ページ）
- ライセンス キーのダウンロードとアクティベーションの自動化 （1232 ページ）
- 期限切れ機能キー （1233 ページ）

ライセンス キーの追加および管理

物理 電子メールゲートウェイの場合、ライセンスキーは 電子メールゲートウェイのシリアル番号と有効化されている機能に固有です（他のシステム上の 1 つのシステムでキーを再利用することはできません）。

CLI のライセンス キーを使用するには、**featurekey** コマンドを使用します。

手順

ステップ 1 [システム管理（System Administration）] > [ライセンス キー（Feature Keys）] を選択します。

ステップ 2 アクションの実行：

目的	操作手順
実行中のライセンス キーのステータスを表示します	[シリアル番号 <serial number> のライセンス キー（Feature Keys for <serial number>）] セクションを確認します。
電子メールゲートウェイに対して発行されていて、まだアクティベーションされていないライセンスキーを表示します	[保留中のライセンス（Pending Activation）] セクションを確認します。 自動ダウンロードおよびアクティベーションを有効にしている場合は、ライセンス キーはこのリストには表示されません。

目的	操作手順
最近発行されたライセンスキーを確認する	[保留中のライセンス（Pending Activation）] セクションで、[新しいキーをチェック（Check for New Keys）] ボタンをクリックします。 これはライセンス キーの自動ダウンロードおよびアクティベーションを有効にしていない場合、または次の自動チェックの前にライセンス キーをダウンロードする必要がある場合に役立ちます。
発行されたライセンス キーをアクティブ化します	[保留中のライセンス（Pending Activation）] リストで、[選択したキーを有効化（Activate Selected Keys）] をクリックします。
新しいライセンス キーを追加します	**[機能の有効化（Feature Activation）]** セクションを使用します。

次のタスク

関連項目

- ライセンス キーのダウンロードとアクティベーションの自動化 （1232 ページ）
- [設定ファイル（Configuration File）] ページ （1249 ページ）

ライセンス キーのダウンロードとアクティベーションの自動化

電子メールゲートウェイに対して発行されたライセンスキーを自動的にチェック、ダウンロードおよびアクティブ化するように、この 電子メールゲートウェイを設定できます。

手順

ステップ 1 [システム管理（System Administration）] > [ライセンス キーの設定（Feature Key Settings）] を選択します。

ステップ 2 [ライセンス キー設定の編集（Edit Feature Key Settings）] をクリックします。

ステップ 3 新しいライセンス キーのチェック頻度を確認するには、（?）ヘルプ ボタンをクリックしてください。

ステップ 4 設定事項を指定します。

ステップ 5 変更を送信し、保存します。

次のタスク

関連項目

• ライセンス キーの追加および管理 （1231 ページ）

期限切れ機能キー

ライセンスキーの有効期限が切れる場合、キー失効の 90 日前、60 日前、30 日前、15 日前、5 日前、1 日前、およびキー失効時に電子メールゲートウェイからアラートが送信されます。これらのアラートを受信するには、システム アラートに登録されていることを確認してください。詳細については、アラート （1275 ページ）を参照してください。

（Webインターフェイスを使用して）アクセスしようとしている機能の機能キーの有効期限が切れている場合は、シスコの担当者またはサポート組織までご連絡ください。

スマート ソフトウェア ライセンシング

• 概要 （1233 ページ）
• スマート ソフトウェア ライセンシングのイネーブル化 （1235 ページ）
• Cisco Smart Software Manager での電子メールゲートウェイの登録 （1236 ページ）
• ライセンスの要求 （1238 ページ）
• Cisco Smart Software Manager からの電子メールゲートウェイの登録解除 （1238 ページ）
• Cisco Smart Software Manager での電子メールゲートウェイの再登録 （1239 ページ）
• 転送設定の変更 （1239 ページ）
• 認証と証明書の更新 （1239 ページ）
• スマート エージェントの更新 （1240 ページ）
• アラート （1240 ページ）
• クラスタ モードでのスマート ライセンス （1241 ページ）

概要

スマート ソフトウェア ライセンシングを使用すると、電子メールゲートウェイのライセンスをシームレスに管理およびモニタできます。スマート ソフトウェア ライセンスをアクティブ化するには、Cisco Smart Software Manager（CSSM）で電子メールゲートウェイを登録する必要があります。CSSMは、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。スマート ライセンスを使用すると、製品認証キー（PAK）を使用して Web サイトで個別に登録するのではなく、単一のトークンで登録することができます。

電子メールゲートウェイを登録すると、電子メールゲートウェイのライセンスを追跡し、CSSMポータル経由でライセンスの使用状況を監視できます。電子メールゲートウェイにインストールされているスマートエージェントは、アプライアンスとCSSMを接続し、ライセンスの使用状況に関する情報を CSSM を渡して、CSSM が使用状況を追跡できるようにします。

Cisco Smart Software Manager については https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

始める前に

- ご利用の電子メールゲートウェイからインターネットに接続できることを確認します。
- シスコ セールス チームに問い合わせて Cisco Smart Software Manager ポータル（https://software.cisco.com/#module/SmartLicensing）でスマート アカウントを作成するか、Cisco Smart Software Manager サテライトをネットワークにインストールしてください。

  Cisco Smart Software Manager の対象ユーザーアカウントの作成または Cisco Smart Software Manager サテライトのインストールの詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

（注） 対象ユーザーとは、インターネットに接続している従業員、再委託先、および電子メールゲートウェイの展開（オンプレミスまたはクラウドのいずれか該当する方）の対象となるその他の承認された個人の総数です。

ライセンスの使用状況に関する情報を直接インターネットに送信したくない対象ユーザーの場合、CSSM 機能のサブセットを提供する Smart Software Manager サテライトをオンプレミスにインストールすることもできます。サテライトアプリケーションをダウンロードして導入した後は、インターネットを使用して CSSM にデータを送信せずに、ライセンスをローカルで安全に管理できます。CSSM サテライトは、情報をクラウドに定期的に送信します。

（注） Smart Software Manager サテライトを使用する場合、Smart Software Manager サテライト Enhanced Edition 6.1.0 を使用してください。

- （従来の）クラシックライセンスの既存ユーザーは、クラシックライセンスをスマートライセンスに移行する必要があります。

  https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic を参照してください。
- 電子メールゲートウェイのシステムクロックを CSSM のシステムクロックと同期させる必要があります。電子メールゲートウェイのシステムクロックと CSSM のシステムクロックのずれは、スマートライセンス操作の失敗の原因となります。

（注） インターネットに接続してプロキシ経由で CSSM に接続する場合、[セキュリティサービス（Security Services）] > [サービスのアップデート（Service updates）] を使用して、電子メールゲートウェイに設定されているプロキシと同じプロキシを使用する必要があります

（注） 仮想対象ユーザーの場合、新しい PAK ファイル（新規または更新）を受信するたびに、ライセンスファイルを生成し、電子メールゲートウェイのファイルをロードします。ファイルをロードした後は、PAK をスマート ライセンスに変換する必要があります。スマート ライセンス モードでは、ファイルのロード中、ライセンス ファイルの機能キー セクションは無視され、証明書情報のみが使用されます。

（注） すでに Cisco SecureX アカウントを持っている場合は、まず電子メールゲートウェイを Cisco SecureX に登録してから、電子メールゲートウェイでスマートライセンスモードを有効にしてください。

電子メールゲートウェイに対してスマート ソフトウェア ライセンシングを有効にするには、次の手順を実行する必要があります。

	操作内容	詳細情報
ステップ 1	スマート ソフトウェア ライセンシングの有効化	スマート ソフトウェア ライセンシングのイネーブル化（1235 ページ）
ステップ 2	Cisco Smart Software Manager での電子メールゲートウェイの登録	Cisco Smart Software Manager での電子メールゲートウェイの登録 （1236 ページ）
ステップ 3	ライセンス（機能キー）の要求	ライセンスの要求 （1238 ページ）

スマート ソフトウェア ライセンシングのイネーブル化

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 [スマート ソフトウェア ライセンシングの有効化（Enable Smart Software Licensing）] をクリックします。

スマート ソフトウェア ライセンシングの詳細については、スマート ソフトウェア ライセンシングの詳細のリンクをクリックします。

ステップ 3 スマート ソフトウェア ライセンシングについての情報を読んだ後、**[OK]** をクリックします。

ステップ 4 変更を保存します。

次のタスク

スマート ソフトウェア ライセンシングを有効すると、クラシック ライセンス モードのすべての機能がスマート ライセンス モードでも自動的に使用可能になります。クラシックライセンスモードの既存対象ユーザーの場合、CSSMで電子メールゲートウェイを登録せずに、スマート ソフトウェア ライセンシング機能を使用できる 90 日間の評価期間があります。

有効期限および評価期間の期限の前に、一定の間隔（90 日前、60 日前、30 日前、15 日前、5 日前、および最終日）で通知が表示されます。評価期間の間または終了後に、CSSM で電子メールゲートウェイを登録できます。

（注） クラシックライセンスモードにおけるアクティブなライセンスを持たない仮想電子メールゲートウェイの対象ユーザーの場合、スマート ソフトウェア ライセンシング機能を有効にしても、評価期間は提供されません。クラシックライセンスモードにおけるアクティブなライセンスを持つ仮想電子メールゲートウェイの対象ユーザーのみに、評価期間が提供されます。新規仮想電子メールゲートウェイ対象ユーザーがスマートライセンス機能の評価を希望する場合には、シスコセールスチームに連絡し、スマートアカウントに評価ライセンスを追加してください。評価ライセンスは、登録後に評価目的で使用されます。

（注） 電子メールゲートウェイでスマートライセンシング機能を有効にすると、スマートライセンシングからクラシック ラインセンシング モードにロールバックすることができなくなります。

Cisco Smart Software Manager での電子メールゲートウェイの登録

電子メールゲートウェイを Cisco Smart Software Manager に登録するには、[システム管理（System Administration）] メニューでスマート ソフトウェア ライセンシング機能を有効にする必要があります。

手順

ステップ 1 E メールゲートウェイで [システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 2 [スマートライセンスの登録（Smart License Registration）] オプションを選択します。

ステップ 3 [トランスポート設定（Transport Settings）] を変更する場合には、[編集（Edit）] をクリックします。次のオプションを使用できます。

- [直接（Direct）]：電子メールゲートウェイを HTTPS 経由で Cisco Smart Software Manager に直接接続します。このオプションは、デフォルトで選択されます。
- [トランスポートゲートウェイ（Transport Gateway）]：電子メールゲートウェイをトランスポートゲートウェイまたは Smart Software Manager サテライト経由で Cisco Smart Software Manager に接続します。このオプションを選択した場合、トランスポート ゲートウェイまたは Smart Software Manager サテライトの URL を入力してから [OK] をクリックする必要があります。このオプションは HTTP および HTTPS をサポートします。FIPS モードの場合、トランスポート ゲートウェイは HTTPS のみをサポートします。トランスポート ゲートウェイについては、Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

  ログイン クレデンシャルを使用して、Cisco Smart Software Manager ポータル

  （https://software.cisco.com/#module/SmartLicensing）にアクセスします。新しいトークンを作成するには、このポータルの [仮想アカウント（Virtual Account）] ページに移動して [全般（General）] タブにアクセスします。電子メールゲートウェイ用の製品インスタンス登録トークンをコピーします。

  製品インスタンス登録トークンの作成については、https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

ステップ 4 電子メールゲートウェイに戻り、製品インスタンス登録トークンを貼り付けます。

ステップ 5 [登録（Register）] をクリックします。

ステップ 6 [スマートソフトウェアライセンシング（Smart Software Licensing）] ページで、[すでに登録されている場合は、この製品インスタンスを再登録します（Reregister this product instance if it is already registered）] チェックボックスをオンにして、電子メールゲートウェイを再登録することもできます。Cisco Smart Software Manager での電子メールゲートウェイの再登録 （1239 ページ）を参照してください。

次のタスク

製品登録プロセスには数分かかります。[スマートソフトウェアライセンシング（Smart Software Licensing）] ページで登録ステータスを表示できます。

（注） スマート ソフトウェア ライセンシングを有効にし、電子メールゲートウェイを Cisco Smart Software Manager に登録すると、Cisco Cloud Services ポータルが自動的に有効になり、電子メールゲートウェイに登録されます。

ライセンスの要求

登録プロセスが正常に完了した後、電子メールゲートウェイの機能のライセンスを要求しなければならない場合があります。

手順

ステップ 1 **[システム管理（System Administration）] > [ライセンス（Licenses）]** を選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 要求するライセンスに対応する [ライセンスの要求/リリース（License Request/Release）] 列のチェック ボックスをオンにします。

ステップ 4 **[送信（Submit）]** をクリックします。

（注） デフォルトでは、メール処理と Cisco Secure Email Gateway のバウンス検証のライセンスを利用できます。これらのライセンスは、有効化、無効化、またはリリースすることができません。

メール処理と Cisco Secure Email Gateway のバウンス検証のライセンスに評価期間やコンプライアンス違反はありません。これは、仮想電子メールゲートウェイには適用されません。

次のタスク

ライセンスは、期限超過また期限切れになるとコンプライアンス違反（OOC）モードになり、各ライセンスに 30 日間の猶予期間が提供されます。有効期限および OOC 猶予期間の期限の前に、一定の間隔（30 日前、15 日前、5 日前、および最終日）で通知が表示されます。

OOC 猶予期間の有効期限が過ぎると、ライセンスは使用できず、機能を利用できなくなります。機能にもう一度アクセスするには、CSSM ポータルでライセンスをアップデートして、認証を更新する必要があります。

Cisco Smart Software Manager からの電子メールゲートウェイの登録解除

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウン リストから、**[登録解除（Deregister）]** を選択し、**[実行（Go）]** をクリックします。

ステップ 3 **[送信（Submit）]** をクリックします。

Cisco Smart Software Manager での電子メールゲートウェイの再登録

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウンリストから、**[登録（Register）]** を選択し、**[実行（Go）]** をクリックします。

次のタスク

登録プロセスについては、Cisco Smart Software Manager での電子メールゲートウェイの登録（1236 ページ） を参照してください。

回避できないシナリオにおいては、電子メールゲートウェイの設定をリセットした後に電子メールゲートウェイを登録することができます。

転送設定の変更

CSSM で電子メールゲートウェイを登録する前にのみ、トランスポート設定を変更できます。

（注） スマートライセンス機能が有効になっている場合にのみ、トランスポート設定を変更できます。電子メールゲートウェイがすでに登録されている場合、トランスポート設定を変更するには、電子メールゲートウェイの登録を解除する必要があります。トランスポート設定を変更した後に、電子メールゲートウェイを再登録する必要があります。

トランスポート設定を変更する方法は、Cisco Smart Software Manager での電子メールゲートウェイの登録を参照してください。

認証と証明書の更新

Cisco Smart Software Manager で電子メールゲートウェイを登録した後に、証明書を更新できます。

（注） 電子メールゲートウェイが正常に登録された後にのみ、認証を更新できます。

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウン リストから、適切なオプションを選択します。

- 認証を今すぐ更新
- 証明書を今すぐ更新

ステップ 3 **[移動（Go）]** をクリックします。

アラート

次のシナリオで通知が送信されます。

- スマート ソフトウェア ライセンシングが正常に有効化された
- スマート ソフトウェア ライセンシングの有効化に失敗した
- 評価期間が開始された
- 評価期間が終了した（評価期間中および期間終了時に一定の間隔で送信）
- 正常に登録された
- 登録に失敗した
- 正常に認証された
- 認証に失敗した
- 正常に登録解除された
- 登録解除に失敗した
- ID 証明書が正常に更新された
- ID 証明書の更新に失敗した
- 認証の有効期限が切れた
- ID 証明書の有効期限が切れた
- コンプライアンス違反猶予期間の期限が切れた（コンプライアンス違反猶予期間中および期間終了時に一定の間隔で送信）
- 機能の有効期限に関する最初のインスタンスが発生した

スマート エージェントの更新

電子メールゲートウェイにインストールされているスマートエージェントのバージョンを更新するには、次の手順を実行します。

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 **[スマートエージェントの更新ステータス（Smart Agent Update Status）]** セクションで、**[今すぐ更新（Update Now）]** をクリックし、プロセスに従います。

（注） CLI コマンド `saveconfig` を使用して、または **[システム管理（System Administration）] > [設定サマリー（Configuration Summary）]** を使用して Web インターフェイス経由で設定変更を保存しようとすると、スマート ライセンス関連の設定は保存されません。

クラスタ モードでのスマート ライセンス

クラスタ構成では、スマート ソフトウェア ライセンシングを有効にして、すべてのマシンを同時に Cisco Smart Software Manager に登録できます。

手順：

1. ログインしている電子メールゲートウェイでクラスタモードからマシンモードに切り替えます。
2. [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] ページに移動します。
3. [有効（Enable）] をクリックします。
4. [クラスタ内のすべてのマシンでスマートソフトウェアライセンシングを有効にする（Enable Smart Software Licensing on all machines in the cluster）] チェックボックスをオンにします。
5. [OK] をクリックします。
6. [クラスタ内のマシン全体でスマートソフトウェアライセンシングを登録する（Register Smart Software Licensing across machines in cluster）] チェックボックスをオンにします。
7. [登録（Register）] をクリックします。

（注） CLI で `license_smart` コマンドを使用して、スマート ソフトウェア ライセンシングを有効にしてすべてのマシンを同時に Cisco Smart Software Manager に登録できます。

（注） クラスタ構成では、スマート ソフトウェア ライセンシングを有効にして、すべてのマシンを個別に Cisco Smart Software Manager に登録することもできます。クラスタモードでのスマートライセンスでは、任意の電子メールゲートウェイにログインしてスマートライセンスを設定できます。電子メールゲートウェイにログインし、クラスタの他の電子メールゲートウェイに 1 つずつアクセスして、最初の電子メールゲートウェイからログオフすることなくスマートライセンス機能を設定できます。

詳細については、クラスタを使用した中央集中型管理 （1481 ページ）を参照してください。

仮想電子メールゲートウェイのライセンス

仮想電子メールゲートウェイのセットアップとライセンス付与については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このマニュアルは、資料 に記載されている場所から入手できます。

（注） 仮想電子メールゲートウェイのライセンスをインストールする前に、テクニカルサポートのトンネルを開くこと、またはシステム セットアップ ウィザードを実行することはできません。

仮想電子メールゲートウェイのライセンスの有効期限

仮想電子メールゲートウェイのライセンスの有効期限が切れてから 180 日間、この電子メールゲートウェイはセキュリティサービスなしでメールの配信を続行します。この期間中、セキュリティ サービスは更新されません。

ライセンスの有効期限が切れる時点から 180 日前、150 日前、120 日前、90 日前、60 日前、30 日前、15 日前、5 日前、1 日前、および 0 秒前にアラートが送信されます。また、猶予期間の終了についても、同じ間隔でアラートが送信されます。これらは、[システム（System）] タイプ、[重大（Critical）] 重大度レベルのアラートです。確実にアラートが届くようにするには、アラート受信者の追加 （1277 ページ）を参照してください。

これらのアラートはシステム ログにも記録されます。

個々のライセンスキーが、仮想電子メールゲートウェイのライセンスよりも先に期限切れになることがあります。これらの有効期限が近づいてきた場合にも、アラートが送信されます。

関連項目

- 仮想電子メールゲートウェイでの AsyncOS の復元がライセンスに影響を及ぼす可能性（1271 ページ）

設定ファイルの管理

電子メールゲートウェイ内のすべての設定は、1 つの設定ファイルで管理できます。このファイルは Extensible Markup Language（XML）形式で保持されます。

このファイルは次の複数の方法で使用できます。

- 設定ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。電子メールゲートウェイの設定を間違えた場合、保存した最新のコンフィギュレーション ファイルに「ロールバック」できます。
- 既存のコンフィギュレーション ファイルをダウンロードし、電子メールゲートウェイの設定全体を素早く確認できます。（新しいブラウザの多くに、XML ファイルを直接レンダリングする機能が含まれています）。現在の設定にマイナー エラー（誤入力など）があった場合、この機能がトラブルシューティングに役立つことがあります。
- 既存のコンフィギュレーション ファイルをダウンロードし、変更を加えて同じ 電子メールゲートウェイにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と Web インターフェイスの両方が「バイパス」されます。
- FTP アクセスを使用して設定ファイル全体をアップロードしたり、設定ファイルの一部または全体を CLI に直接貼り付けたりできます。
- ファイルは XML 形式であるため、設定ファイルのすべての XML エンティティを定義する、関連付けられた Document Type Definition（DTD）も提供されます。XML 設定ファイルをアップロードする前にこの DTD をダウンロードして XML 設定ファイルを検証できます（XML 検証ツールはインターネットで簡単に入手できます）。

XML 設定ファイルを使用した複数の電子メールゲートウェイの管理

- ある電子メールゲートウェイから既存の設定ファイルをダウンロードし、変更を行い、別の電子メールゲートウェイにアップロードできます。これにより、複数の電子メールゲートウェイのインストールを簡単に管理できるようになります。現時点では、設定ファイルを C/X シリーズ 電子メールゲートウェイから M シリーズ Cisco Secure Manager Email and Web Gateway にロードできません。
- ある電子メールゲートウェイからダウンロードされた既存の設定ファイルを、複数のサブセクションに分割できます。（複数の電子メールゲートウェイ環境の）すべての電子メールゲートウェイで共通するこれらのセクションを変更し、サブセクションの更新時にこれらのセクションを他の電子メールゲートウェイにロードできます。

たとえば、Global Unsubscribe コマンドをテストするためにテスト環境で電子メールゲートウェイを使用できます。グローバル配信停止リストを適切に設定した場合は、テスト電子メールゲートウェイのグローバル配信停止設定セクションをすべての実稼働電子メールゲートウェイにロードできます。

コンフィギュレーション ファイルの管理

電子メールゲートウェイで設定ファイルを管理するには、[システム管理（System Administration）] > [設定ファイル（Configuration File）] をクリックします。

[設定ファイル（Configuration File）] ページには、次のセクションが含まれています。

- [現在の設定（Current Configuration）]：現在の設定ファイルを保存およびエクスポートするために使用します。
- [設定をロード（Load Configuration）]：設定ファイル全体または一部をロードするために使用します。
- [エンドユーザセーフリスト/ブロックリストデータベース（スパム隔離）（End-User Safelist/Blocklist Database (Spam Quarantine)）]：詳細については、セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御 （1161 ページ）およびセーフリスト/ブロックリストのバックアップと復元 （1173 ページ）を参照してください。
- [設定情報のリセット（Reset Configuration）]：現在の設定を出荷時デフォルト値にリセットするために使用します（リセット前に設定を保存する必要があります）。

（注） 秘密キーと証明書は設定ファイルと暗号化パスフレーズと共に、暗号化されない PEM 形式で含められます。

関連項目

- 現在の設定ファイルの保存およびエクスポート （1244 ページ）
- コンフィギュレーション ファイルのロード （1245 ページ）
- 設定ファイルのメール送信 （1245 ページ）
- 現在の設定のリセット （1248 ページ）

現在の設定ファイルの保存およびエクスポート

[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページの **[現在の設定（Current Configuration）]** のセクションを使用すると、現在の設定ファイルを、ローカルマシンに保存したり、電子メールゲートウェイで保存したり（FTP/SCP ルートの configuration ディレクトリに保存されます）、指定されたアドレスに電子メールで送信したりできます。

次の情報は、設定ファイルには保存されません。

- URL フィルタリング機能で使用されるサービスとのセキュアな通信に使用される証明書。
- [テクニカルサポートに問い合わせる（Contact Technical Support）] ページに保存されている CCO ユーザー ID と契約 ID。

[設定ファイル内のパスフレーズを隠す（Mask passphrases in the Configuration Files）] チェックボックスをクリックして、ユーザのパスフレーズをマスクできます。パスフレーズをマスクすると、元の暗号化されたパスフレーズが、エクスポートまたは保存されたファイルで「*****」に置き換えられます。ただし、パスフレーズがマスクされた設定ファイルを AsyncOS に再びロードすることはできないことに注意してください。

[設定ファイル内のパスフレーズを隠す（Encrypt passphrases in the Configuration Files）] チェックボックスをクリックして、ユーザのパスフレーズをマスクできます。次に、暗号化される、設定ファイル内の重要なセキュリティ パラメータを示します。

- 証明書の秘密キー
- RADIUS パスワード
- LDAP バインドのパスワード
- ローカル ユーザのパスワードのハッシュ
- SNMP パスワード
- DK/DKIM 署名キー
- 発信 SMTP 認証パスワード
- PostX 暗号化キー
- PostX 暗号化プロキシ パスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード
- アップデータ サーバの URL

これは、saveconfig コマンドを使用してコマンドライン インターフェイスでも構成できます。

設定ファイルのメール送信

[システム管理（System Administration）] > [設定ファイル（Configuration File）] の [ファイルをメールで送信（Email file to）] フィールドを使用するか、mailconfig コマンドを使用して、現在の設定を添付ファイルとしてユーザにメール送信できます。

コンフィギュレーション ファイルのロード

[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページの [設定をロード（Load Configuration）] セクションを使用して、新しい設定情報を電子メールゲートウェイにロードします。これは、`loadconfig` コマンドを使用してコマンドラインインターフェイスでも構成できます。

情報は次の 3 つのいずれかの方法でロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする。
- 設定ファイルをローカル マシンから直接アップロードする。
- 設定情報を直接貼り付ける。

（注） パスフレーズがマスクされた設定ファイルはロードできません。

クラスタモードでは、クラスタまたは電子メールゲートウェイのいずれの設定をロードするかを選択できます。クラスタ設定をロードする手順については、クラスタ化された電子メールゲートウェイの設定のロード （1505 ページ）を参照してください。

どの方法の場合でも、設定の上部に次のタグを含める必要があります。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

... your configuration information in valid XML

</config>
```

</config>閉じタグは設定情報の後に指定する必要があります。XML構文の値は、電子メールゲートウェイの configuration ディレクトリにある DTD（Document Type Definition）を使用して解析および検証されます。DTD ファイルの名前は config.dtd です。loadconfig コマンドを使用したときにコマンドラインで検証エラーが報告された場合、変更はロードされません。設定ファイルをアップロードする前に、電子メールゲートウェイの外部で DTD をダウンロードし、設定ファイルを検証できます。

いずれの方法の場合でも、設定ファイル全体（最上位のタグである <config></config> 間で定義された情報）または設定ファイルの *complete* および *unique* サブセクション（上記の宣言タグが含まれ、<config></config> タグ内に存在する場合）をインポートできます。

「complete（完全）」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次の内容をアップロードまたは解析します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosu

</config>
```

この場合は、アップロード中に検証エラーが発生します。ただし、

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosupport_enabled>

</config>
```

この場合は、検証エラーが発生しません。

「unique（一意）」とは、アップロードまたは貼り付けられる設定ファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは1つのホスト名しか持

つことができないため、次の内容（宣言と <config></config> タグを含む）をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

上記の内容は許容されます。ただし、システムでは複数のリスナーを定義できるため（リスナーごとに異なる受信者アクセス テーブルが定義されます）、

```
<rat>
       <rat_entry>
             <rat_address>ALL</rat_address>
         <access>RELAY</access>
     </rat_entry>
</rat>
```

上記の内容だけをアップロードすることは多義的と見なされ、「完全」な構文であっても許可されません。

注意 設定ファイルまたは設定ファイルのサブセクションをアップロードまたは解析する場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

設定ファイルのディスク領域の割り当てが、現在電子メールゲートウェイに保存されているデータの量よりも小さい場合、設定ファイルで指定されたクォータを満たすために、最も古いデータが削除されます。

空白タグと省略されたタグ

設定ファイルのセクションをアップロードまたは解析する場合は注意が必要です。タグを含めないと、コンフィギュレーションファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、

```
<listeners></listeners>
```

上記の内容をアップロードすると、システムからすべてのリスナーが削除されます。

注意 設定ファイルのサブセクションをアップロードしたり、貼り付けたりした場合、Web インターフェイスまたは CLI から切断され、大量の設定データが破壊されることがあります。別のプロトコル、シリアルインターフェイス、または管理ポートのデフォルト設定を使用して電子メールゲートウェイに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しい設定ファイルをアップロードする前に、必ず設定データをバックアップしてください。

ログ サブスクリプションのパスフレーズのロードについての注意事項

パスフレーズが必要なログサブスクリプションを含むコンフィギュレーションファイルをロードしようとしても（たとえば、FTPプッシュを使用）、loadconfigコマンドは不明なパスフレーズについて警告しません。FTPプッシュが失敗し、logconfigコマンドを使用して正しいパスフレーズを設定するまで警告が生成されます。

文字セット エンコーディングについての注意事項

XML コンフィギュレーション ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「`ISO-8859-1`」である必要があります。`showconfig` コマンド、`saveconfig` コマンド、または `mailconfig` コマンドを発行するたびにエンコーディング属性がファイルで指定されることに注意してください。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つ設定ファイルだけをロードできます。

関連項目

- クラスタ化された電子メールゲートウェイの設定のロード （1505 ページ）

現在の設定のリセット

現在の設定をリセットすると、電子メールゲートウェイが元の出荷時デフォルト値に戻ります。リセットする前に設定を保存する必要があります。GUIでこのボタンを使用して設定をリセットすることは、クラスタリング環境ではサポートされていません。

出荷時の初期状態へのリセット （1230 ページ） を参照してください。

設定ファイルの表示

設定ファイルの詳細は、`showconfig` コマンドを使用してのみ表示できます。`showconfig` コマンドは、現在の設定を画面に出力します。

```
mail3.example.com> showconfig


Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
Product: IronPort model number Messaging Gateway Appliance(tm)
Model Number: model number
Version: version of AsyncOS installed
Serial Number: serial number

Current Time: current time and date

[The remainder of the configuration file is printed to the screen.]
```

[設定ファイル（Configuration File）] ページ

- 設定ファイルの管理 （1243 ページ）
- 出荷時の初期状態へのリセット （1230 ページ）
- セーフリスト/ブロックリストのバックアップと復元 （1173 ページ）

ディスク領域の管理

- （仮想 E メール ゲートウェイのみ）使用可能なディスク領域の増加 （1249 ページ）
- ディスク領域の使用率の表示および割り当て （1250 ページ）
- その他のクォータのディスク領域の管理 （1250 ページ）
- ディスク領域に関するアラートの受信の確認 （1251 ページ）

（仮想 E メール ゲートウェイのみ）使用可能なディスク領域の増加

ESXi 5.5 および VMFS 5 を実行する仮想 E メール ゲートウェイの場合、2 TB を超えるディスク領域を割り当てることができます。ESXi 5.1 を実行する E メール ゲートウェイの場合は 2 TB に制限されます。

仮想 E メール ゲートウェイ インスタンスにディスク領域を追加するには、次の手順を実行します。

（注） ディスク領域の削減はサポートされていません。詳細については、VMware のマニュアルを参照してください。

はじめる前に

必要な追加ディスク領域を慎重に検討します。

手順

ステップ 1 E メール ゲートウェイのインスタンスをダウンさせます。

ステップ 2 VMware が提供するユーティリティまたは管理ツールを使用してディスク領域を増やします。

VMware のマニュアルで仮想ディスク設定の変更に関する情報を参照してください。ESXi 5.5 に関するこの情報は、リリースの時点では、http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html で参照可能でした。

ステップ 3 [システム管理（System Administration）]>[ディスク管理（Disk Management）]に移動して、変更内容が反映されたことを確認します。

ディスク領域の使用率の表示および割り当て

Eメール ゲートウェイで、展開で使用される各機能にディスク領域を割り当てることで、ディスク使用率を最適化できます。

目的	操作手順
• 各サービスのディスク領域クォータと現在の使用率を表示します • いつでもEメールゲートウェイでディスク領域を再割り当てできます	[システム管理（System Administration）]>[ディスク管理（Disk Management）] に移動します。
データ ボリュームの管理	• サービスの報告と追跡およびスパム隔離の場合、最も古いデータが自動的に削除されます。 • ポリシー、ウイルス、アウトブレイク隔離の場合、隔離に設定されたデフォルトアクションが実行されます。隔離メッセージに自動的に適用されるデフォルトアクション （1135 ページ）を参照してください。 • その他のクォータの場合、まず手動でデータを削除して、設定する新しいクォータを下回るように使用量を減らします。その他のクォータのディスク領域の管理 （1250ページ） を参照してください。

その他のクォータのディスク領域の管理

その他のクォータにはシステム データとユーザ データが含まれます。システム データは削除できません。管理できるユーザ データには次のファイル タイプがあります。

管理対象	手順
ログ ファイル	[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] に移動して、 • どのログ ディレクトリが最もディスク領域を消費しているかを確認します。 • 生成されるすべてのログ サブスクリプションが必要であることを確認します。 • 必要以上に詳細なログ レベルになっていないかを確認します。 • 可能な場合は、ロールオーバー ファイル サイズを小さくします。
パケット キャプチャ	[ヘルプとサポート（Help and Support）]（画面上部の右側付近）> [パケットキャプチャ（Packet Capture）] に移動します。
コンフィギュレーション ファイル （これらのファイルが多くのディスク領域を消費する可能性は低いと考えられます）。	E メール ゲートウェイの /data/pub ディレクトリに FTP でアクセスします。 E メール ゲートウェイへの FTP アクセスを構成するには、FTP、SSH、および SCP アクセス （1573 ページ）を参照してください。
クオータ サイズ	[システム管理（System Administration）] > [ディスク管理（Disk Management）] に移動します。

ディスク領域に関するアラートの受信の確認

その他のディスク使用量がクォータの 75% に達すると、警告レベルのシステム アラートを受信します。これらのアラートを受信した場合は、対処する必要があります。

確実にアラートが届くようにするには、アラート （1275 ページ）を参照してください。

ディスク領域と集中管理

ディスク領域管理はマシン モードでのみ使用可能で、グループまたはクラスタ モードでは使用できません。

セキュリティ サービスの管理

[サービスの概要（Services Overview）] ページには次のエンジンの現在のサービスとルールのバージョンがリストされます。

- Graymail

- McAfee
- Sophos

[サービスの概要（Services Overview）] ページでは、次のタスクを実行できます。

- エンジンを手動で更新します。詳細については、エンジンの手動アップデート （1252 ページ）を参照してください。
- エンジンの以前のバージョンにロールバックします。詳細については、エンジンの以前のバージョンへのロールバック （1253 ページ）を参照してください。

[自動更新（Automatic Updates）] 列は特定のエンジンの自動更新の状態を示します。自動更新を有効または無効にする場合、特定のエンジンの [グローバル設定（Global Settings）] ページに移動します。

特定のサービスエンジンの自動更新を無効にすると、警告が定期的に表示されます。警告の間隔を変更する場合、[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページの [無効な自動エンジン更新のアラート間隔（Alert Interval for Disabled Automatic Engine Updates）] オプションを使用します。

（注） ロールバックが適用されているエンジンの場合、自動更新は自動的に無効になります。

関連項目

- エンジンの手動アップデート （1252 ページ）
- エンジンの以前のバージョンへのロールバック （1253 ページ）
- ログの表示 （1253 ページ）
- システム アラート （1285 ページ）

エンジンの手動アップデート

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [サービスの概要（Services Overview）] ページに進みます。

ステップ 2 サービス エンジンの最新サービスまたはルール バージョンを参照するには、[入手可能な更新（Available Updates）] 列の [更新（Update）] をクリックします。

（注） [更新（Update）] オプションは、特定のエンジンの新しい更新が入手可能である場合にのみ使用できます。

エンジンの以前のバージョンへのロールバック

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [サービスの概要（Services Overview）] ページに進みます。

ステップ 2 [バージョンの変更（Modify Versions）] カラムで [変更（Change）] をクリックします。

ステップ 3 必要なルールおよびサービス バージョンのアップデートを選択し、[適用（Apply）] クリックします。

電子メールゲートウェイにより、エンジンが以前のバージョンにロールバックされます。

（注） サービス アップデートには、サービス バージョンとルール バージョンがパッケージとして一緒に含まれています。

[適用（Apply）] をクリックすると、そのエンジンの自動更新が自動的に無効になります。自動更新を有効にするには、そのエンジンの [グローバル設定（Global Settings）] ページに移動します。

ログの表示

エンジンのロールバックおよび自動更新の無効化に関する情報は、次のログに記載されます。

- アップデータ ログ：エンジンのロールバックおよびエンジンの自動更新に関する情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

  詳細については、アップデータ ログの例 （1449 ページ）を参照してください。

サービス アップデート

次のサービスは最大の効果得るために更新する必要があります。

- ライセンス キー（Feature Keys）
- McAfee Anti-Virus の定義
- PXE エンジン
- Sophos Anti-Virus の定義
- IronPort アンチ スパム ルール
- アウトブレイク フィルタ ルール
- タイム ゾーンルール
- URL カテゴリ（URL フィルタリング機能に使用します。詳細は、将来の URL カテゴリ セットの変更 （584 ページ） を参照してください。

- 登録クライアント（URL フィルタリング機能で使用されるクラウドベース サービスとの通信に必要な証明書を更新するために使用されます。詳細については、Talosインテリジェンスサービスへの接続について （548 ページ）を参照してください。）
- グレイメール ルール

（注） DLP エンジンとコンテンツ照合分類子の設定は、[セキュリティサービス（Security Services）] > [データ損失防止（Data Loss Prevention）] ページで扱われます。詳細については、DLPエンジンおよびコンテンツ照合分類子の更新について （657ページ）を参照してください。

サービス アップデートの設定は、DLP アップデートを除いてアップデートを受け取るすべてのサービスに使用されます。DLPアップデートを除いて、任意のサービスにそれぞれ設定を指定できません。

これらの重要なアップデートを取得するようにネットワークと電子メールゲートウェイを設定するには、「アップグレードおよびアップデートを取得するための設定 （1254ページ）」を参照してください。

アップグレードおよびアップデートを取得するための設定

- アップグレードおよびアップデートの配信オプション （1254 ページ）
- Ciscoサーバからアップグレードおよびアップデートをダウンロードするためのネットワークの設定 （1255 ページ）
- 厳密なファイアウォール環境でのアップグレードとアップデートのための電子メールゲートウェイの設定 （1255 ページ）
- ローカル サーバからのアップグレードおよびアップデート （1256 ページ）
- ローカル サーバからアップグレードおよびアップデートするためのハードウェアおよびソフトウェア要件 （1257 ページ）
- ローカル サーバでのアップグレード イメージのホスト （1258 ページ）
- アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259ページ）
- 自動アップデートの設定 （1262 ページ）
- アップデータサーバ証明書の有効性を検証するための電子メールゲートウェイの設定（1262 ページ）
- プロキシサーバとの通信を信頼するためのアプライアンスの設定 （1263 ページ）

アップグレードおよびアップデートの配信オプション

電子メールゲートウェイに AsyncOS アップグレードファイルおよびアップデートファイルを配信する方法は複数あります。

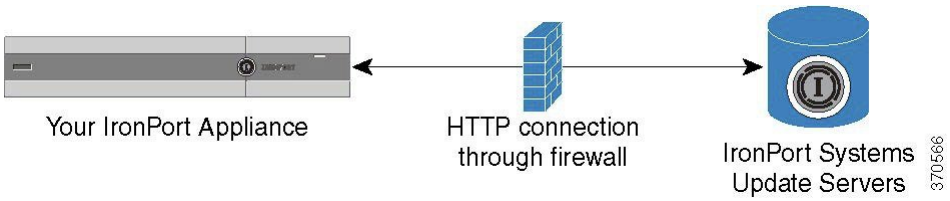
- 各電子メールゲートウェイでは、シスコのアップデートサーバからファイルを直接ダウンロードできます。これがデフォルトの方法です。
- シスコからファイルを1回ダウンロードし、ネットワーク内のサーバから電子メールゲートウェイにファイルを配信できます。ローカルサーバからのアップグレードおよびアップデート （1256 ページ）を参照してください。

方法の選択と設定については、アップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）を参照してください。

Cisco サーバからアップグレードおよびアップデートをダウンロードするためのネットワークの設定

電子メールゲートウェイは、アップグレードおよびアップデートを検索してダウンロードするために、Cisco アップデートサーバに直接接続できます。

図 *73*：ストリーミング アップデートの方法



Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。厳密なファイアウォールポリシーがある場合は、代わりに静的な場所の設定が必要になることがあります。詳細については、厳密なファイアウォール環境でのアップグレードとアップデートのための 電子メールゲートウェイの設定 （1255 ページ）を参照してください。

ポート 80 および 443 による Cisco アップデート サーバからのアップグレードのダウンロードを許可する、ファイアウォールのルールを作成します。

厳密なファイアウォール環境でのアップグレードとアップデートのための 電子メールゲートウェイの設定

Cisco IronPort アップグレードおよびアップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォールポリシーを厳しく設定している場合、アップデートおよびAsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

手順

ステップ 1 シスコ カスタマー サポートに問い合わせて、スタティック URL アドレスを取得します。

ステップ 2 ポート 80 によるスタティック IP アドレスからのアップグレードおよびアップデートのダウンロードを許可する、ファイアウォールのルールを作成します。

ステップ 3 [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] を選択します。

ステップ 4 [アップデート設定を編集（Edit Update Settings）] をクリックします。

ステップ 5 [アップデート設定を編集（Edit Update Settings）] ページの [アップデートサーバ（イメージ）（Update Servers (images)）] セクションで、[ローカルアップデートサーバ（Local Update Servers）] を選択し、ステップ 1 で受け取った AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルのスタティック URL を [ベースURL（Base URL）] フィールドに入力します。

ステップ 6 IronPort アップデート サーバが [アップデートサーバ（リスト）（Update Servers (list)）] セクションで選択されていることを確認します。

ステップ 7 変更を送信し、保存します。

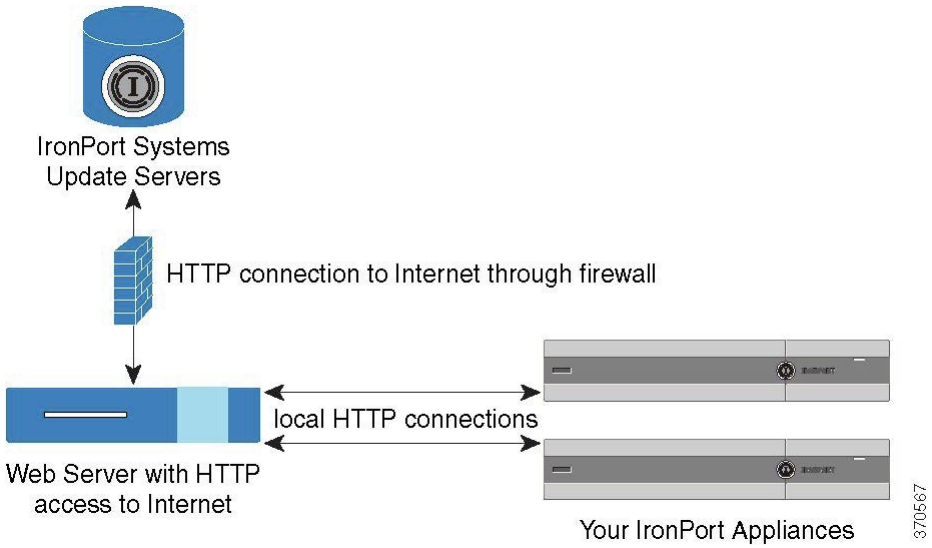
ローカル サーバからのアップグレードおよびアップデート

直接 Cisco アップデート サーバからアップグレードを取得するのではなく、AsyncOS アップグレード イメージをローカル サーバにダウンロードし、所有するネットワーク内からアップグレードをホスティングできます。この機能を使用して、インターネットにアクセスできるネットワーク上のすべてのサーバに HTTP でアップグレードイメージをダウンロードします。アップデートイメージをダウンロードする場合は、内部 HTTP サーバ（アップデート マネージャ）を設定し、アプライアンスで AsyncOS イメージをホスティングすることができます。

電子メールゲートウェイがインターネットにアクセスできない場合や、ダウンロードに使用するミラーサイトへのアクセスが組織で制限される場合はローカルサーバを使用します。ローカルサーバから各 電子メールゲートウェイへの AsyncOS アップグレードのダウンロードは、通常 Cisco IronPort サーバからのダウンロードよりも高速です。

（注） AsyncOS アップグレードに限りローカル サーバを使用することを推奨します。セキュリティ アップデート イメージにローカル アップデート サーバを使用する場合、ローカル サーバは Cisco IronPort から自動的にセキュリティアップデートを受信しないため、ネットワーク上の 電子メールゲートウェイは常に最新のセキュリティサービスではない可能性があります。

図 *74* : リモート アップデートの方法



手順

ステップ 1 アップグレード ファイルを取得および供給するようにローカル サーバを設定します。

ステップ 2 アップグレード ファイルをダウンロードします。

ステップ 3 GUI の [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] ページまたは CLI の **updateconfig** コマンドのいずれかを使用して、ローカル サーバを使用するようにアプライアンスを設定します。

ステップ 4 [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] ページまたは CLI の upgrade コマンドのいずれかを使用して、アプライアンスをアップグレードします。

ローカル サーバからアップグレードおよびアップデートするためのハードウェアおよびソフトウェア要件

AsyncOS アップグレード ファイルおよびアップデート ファイルのダウンロードでは、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- Cisco Systems アップデート サーバへのインターネット アクセス。
- Web ブラウザ（ブラウザ要件 （13 ページ）を参照）。

（注） 今回のリリースでアップデートサーバのアドレスへのHTTPアクセスを許可するファイアウォール設定値を設定する必要がある場合、特定のIPアドレスではなくDNS名を使用する必要があります。

AsyncOS アップデート ファイルのホスティングでは、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- Web サーバ：たとえば、Microsoft Internet Information Services（IIS; インターネット インフォメーション サービス）または Apache オープン ソース サーバでは、次の要件を満たしている必要があります。
  - 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
  - ディレクトリの参照ができること
  - 匿名認証（認証不要）または基本（「シンプル」）認証用に設定されていること
  - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

ローカル サーバでのアップグレード イメージのホスト

ローカル サーバの設定が完了したら、http://updates.ironport.com/fetch_manifest.html にアクセスしてアップグレードイメージのZIPファイルをダウンロードします。イメージをダウンロードするには、（物理 電子メールゲートウェイの）シリアル番号または（仮想 電子メールゲートウェイの）VLN および 電子メールゲートウェイのバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレードのバージョンをクリックし、ディレクトリ構造を変更せずにローカル サーバのルート ディレクトリにある ZIP ファイルを解凍します。アップグレードイメージを使用するには、[アップデート設定を編集（Edit Update Settings）] ページで（または CLI の updateconfig を使用して）ローカルサーバを使用するように 電子メールゲートウェイを設定します。

ローカルサーバは、ネットワーク上の 電子メールゲートウェイで利用可能な AsyncOS アップグレードをダウンロード済みのアップグレードイメージに限定する XML ファイルもホスティングします。このファイルは「マニフェスト」と呼ばれます。マニフェストはアップグレードイメージの ZIP ファイルの asyncos ディレクトリにあります。ローカル サーバのルート ディレクトリにある ZIP ファイルを解凍したら、[アップデート設定を編集（Edit Update Settings）] ページで（または CLI の updateconfig を使用して）、XML ファイルの完全な URL（ファイル名を含む）を入力します。

リモート アップグレードの詳細については、ナレッジ ベースを参照するか、シスコ サポート プロバイダーにお問い合わせください。

プロキシ サーバを経由したアップデート

電子メールゲートウェイは、（デフォルトで）シスコのアップデートサーバに直接接続して、アップデートを受け取るように設定されます。この接続は、ポート 80 の HTTP によって確立され、コンテンツは暗号化されます。ファイアウォールでこのポートを開かないようにする場合は、アップデートされたルールを電子メールゲートウェイで受け取ることができる、プロキシサーバおよび具体的なポートを定義できます。

プロキシ サーバを使用する場合は、任意で認証およびポートを指定できます。

（注） プロキシ サーバを定義すると、プロキシ サーバを使用するように設定されているすべてのサービス アップデートで、そのプロキシ サーバが自動的に使用されます。任意のサービスのアップデートのために、プロキシ サーバをオフにはできません。

アップグレードおよびアップデートをダウンロードするためのサーバ設定

電子メールゲートウェイにアップグレードおよびアップデートをダウンロードするために必要なサーバ情報および接続情報を指定します。

AsyncOS のアップグレードとサービスのアップデートに同じまたは異なる設定を使用できます。

はじめる前に

電子メールゲートウェイがシスコから直接アップグレードおよびアップデートをダウンロードするか、または代わりにネットワーク上のローカルサーバでこれらのイメージをホスティングするかを設定します。次に、選択した方式をサポートするようにネットワークをセットアップします。アップグレードおよびアップデートを取得するための設定 （1254 ページ）のすべての内容を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] を選択します。

ステップ 2 **[更新設定を編集（Edit Update Settings）]** をクリックします。

ステップ 3 オプションを入力します。

設定	説明
アップデート サーバ（イメージ）（Update Servers (images)）	Cisco IronPort AsyncOS アップグレード イメージを、Cisco IronPort アップデート サーバまたはネットワーク上のローカル サーバのどちらからダウンロードするかを選択します。デフォルトは、アップグレードおよびアップデートの両方で Cisco IronPort アップデート サーバです。 アップグレードとアップデートに同じ設定を使用するには、表示されるフィールドに情報を入力します。 ローカル アップデート サーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスフレーズも入力します。 AsyncOS アップグレードおよび McAfee Anti-Virus 定義ファイルにそれぞれ別の設定を入力するには、[クリックして AsyncOS の異なる設定を使用する（Click to use different settings for AsyncOS）] リンクをクリックします。 （注） Cisco Intelligent Multi-Scan でサードパーティのアンチスパム ルールのアップデートをダウンロードするには、別のローカル サーバが必要です。
アップデートサーバ（リスト）（Update Servers (lists)）	導入に適したアップグレードおよびアップデートのみ各電子メールゲートウェイで利用できることを確認するために、Cisco IronPort は関連するファイルのマニフェストリストを生成します。 利用可能なアップグレードおよびサービス アップデートのリスト（マニフェスト XML ファイル）を、Cisco IronPort アップデート サーバまたはネットワーク上のローカル サーバのどちらからダウンロードするかを選択します。 アップデートおよび AsyncOS アップグレードのためのサーバの指定は、別のセクションに分かれています。デフォルトのアップグレードおよびアップデートは Cisco IronPort アップデート サーバです。 ローカル アップデート サーバを選択した場合、サーバのファイル名および HTTP ポート番号を含む、各リストのマニフェスト XML ファイルのフルパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスフレーズを入力します。

設定	説明
自動更新（**Automatic Updates**）	Sophos および McAfee Anti-Virus 定義ファイル、Cisco Anti-Spam ルール、Cisco Intelligent Multi-Scan ルール、PXE Engine アップデート、アウトブレイク フィルタ ルール、時間帯ルールに対する自動アップデートとアップデート間隔（電子メールゲートウェイがアップデートを確認する頻度）をイネーブルにします。 数字の後に秒、分、時間を表すs（秒）、m（分）およびh（時）を含めます。自動更新をディセーブルにするには、0（ゼロ）を入力します。 （注） [セキュリティ サービス（Security Services）] > [データ消失防止（Data Loss Prevention）] ページからのみ、DLP の自動アップデートを有効にできます。ただし、最初にすべてのサービスの自動アップデートをイネーブルにする必要があります。詳細については、DLP エンジンおよびコンテンツ照合分類子の更新について （657 ページ）を参照してください。
無効な自動エンジン更新のアラート間隔（**Alert Interval for Disabled Automatic Engine Updates**）	「自動更新」機能が特定のエンジンで無効になっている場合、送信されるアラートの特定の頻度を入力します。 末尾に m、h、または d が含まれ、月、時間、または日を示します。デフォルト値は 30 日です。
インターフェイス（**Interface**）	表示されているセキュリティ コンポーネントのアップデートをアップデート サーバに問い合わせる際に使用するネットワーク インターフェイスを選択します。利用可能なプロキシ データ インターフェイスが表示されます。デフォルトでは、 電子メール ゲートウェイで使用するインターフェイスを選択します。
HTTP プロキシ サーバ（HTTP Proxy Server）	GUI に表示されているサービスで使用されるオプションのプロキシ サーバ。 プロキシ サーバを指定すると、すべてのサービスのアップデートのために使用できます。
HTTPS プロキシ サーバ（HTTPS Proxy Server）	HTTPS を使用したオプションのプロキシ サーバ。HTTPS プロキシ サーバを定義すると、GUI に表示されているサービスのアップデートで使用されます。

ステップ 4 変更を送信し、保存します。

自動アップデートの設定

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] ページに移動して、[更新設定を編集（Edit Update Settings）] をクリックします。

ステップ 2 チェックボックスをオンにして、自動アップデートをイネーブルにします。

ステップ 3 アップデート間隔（次のアップデートの確認までに待機する時間）を入力します。数字の後に **m**（分）および**h**（時）を追加します。最大アップデート間隔は 1 時間です。

アップデータサーバ証明書の有効性を検証するための電子メールゲートウェイの設定

電子メールゲートウェイでは、電子メールゲートウェイがアップデータサーバと通信するたびに、シスコのアップデータサーバの証明書の有効性を確認できます。このオプションが設定されている場合、検証に失敗すると、更新はダウンロードされず、詳細がアップデータ ログに記録されます。

このオプションを構成するには、updateconfig コマンドを使用します。次の例は、このオプションを構成する方法を示しています。

```
mail.example.com> updateconfig
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------
Feature Key updates                               http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                   Update URL:
-------------------------------------------------------------------------------------
Feature Key updates                               http://downloads.ironport.com/asyncos
```

```
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates          Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

プロキシサーバとの通信を信頼するためのアプライアンスの設定

透過的でないプロキシサーバを使用している場合、プロキシ証明書の署名に使用するCA証明書を電子メールゲートウェイに追加できます。これにより、電子メールゲートウェイはプロキシサーバ通信を信頼します。

このオプションを構成するには、updateconfigコマンドを使用します。次の例は、このオプションを構成する方法を示しています。

```
mail.example.com> updateconfig
...
...
...
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
[]> add
Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
Paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAgTA0tBUjENM.....................................
-----END CERTIFICATE-----
.
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

AsyncOS のアップグレード

手順

	コマンドまたはアクション	目的
ステップ 1	まだ実行していない場合は、すべてのアップデートとアップグレードのダウンロードに適用される設定を行い、これらのダウンロードをサポートして任意で配信できるようにネットワークをセットアップします。	アップグレードおよびアップデートを取得するための設定 （1254 ページ）
ステップ 2	アップグレードが使用可能になる時期を確認し、インストールするかどうかを決定します。	使用可能なアップグレードの通知 （1264 ページ）
ステップ 3	各アップグレードの実行前に、必須タスクと推奨タスクを実行します。	AsyncOS のアップグレードの準備 （1266 ページ） クラスタ内のマシンのアップグレード （1494 ページ）
ステップ 4	アップグレードを実行します。	アップグレードのダウンロードとインストール （1266 ページ）

クラスタ化されたシステムのアップグレードについて

クラスタ化されたマシンをアップグレードする場合は、クラスタ内のマシンのアップグレード （1494 ページ）を参照してください。

アップグレード手順用のバッチ コマンドについて

アップグレード手順用のバッチ コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』（http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html）を参照してください。

使用可能なアップグレードの通知

デフォルトでは、AsyncOS アップグレードが電子メールゲートウェイで使用可能な場合、管理者および技術者の権限を持つユーザには、Web インターフェイスの上部に通知が表示されます。

クラスタ マシンでは、現在ユーザがログインしているマシンだけにアクションが適用されます。

目的	操作手順
最新のアップグレードの詳細情報を表示する	アップグレード通知にカーソルを合わせます。
使用できるすべてのアップグレードのリストを表示する	通知の下向き矢印をクリックします。
現在の通知を閉じる 新しいアップグレードが入手可能になるまで、電子メールゲートウェイは別の通知を表示しません。	下向き矢印をクリックして [通知を消去（Clear the notification）] を選択してから、[閉じる（Close）] をクリックします。
今後の通知を中止する（管理者権限を持つユーザのみ）	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] に移動します。

使用可能なアップグレードの通知

デフォルトでは、AsyncOS アップグレードが電子メールゲートウェイで使用可能な場合、管理者および技術者の権限を持つユーザには、Web インターフェイスの上部に通知が表示されます。

クラスタ マシンでは、現在ユーザがログインしているマシンだけにアクションが適用されます。

目的	操作手順
最新のアップグレードの詳細情報を表示する	アップグレード通知にカーソルを合わせます。
使用できるすべてのアップグレードのリストを表示する	通知の下向き矢印をクリックします。
現在の通知を閉じる 新しいアップグレードが入手可能になるまで、電子メールゲートウェイは別の通知を表示しません。	下向き矢印をクリックして [通知を消去（Clear the notification）] を選択してから、[閉じる（Close）] をクリックします。
今後の通知を中止する（管理者権限を持つユーザのみ）	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] に移動します。

AsyncOS のアップグレードの準備

ベスト プラクティスとして、次の手順を実行したアップグレードの準備を推奨します。

始める前に

ワークキュー内のすべてのメッセージをクリアします。ワークキューをクリアせずにアップグレードを実行することはできません。

手順

ステップ 1 XML 設定ファイルのオフボックスを保存します。何らかの理由でアップグレード前のリリースに戻す場合は、このファイルが必要です。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合、リストのオフボックスをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。CLI からのアップグレードを実行する場合は、suspendlistener コマンドを使用します。GUI からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。

ステップ 4 キューが空になるまで待ちます。CLI の workqueue コマンドでワークキュー内のメッセージ数を表示するか、rate コマンドで電子メールゲートウェイのメッセージスループットをモニタすることができます。

（注） アップグレード後、再びリスナーをイネーブルにします。

アップグレードのダウンロードとインストール

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードし後でインストールできます。

（注） AsyncOS を Cisco IronPort サーバからではなくローカル サーバから 1 回の操作でダウンロードとアップグレードする場合は、アップグレードはダウンロード中に即座に実行されます。アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

はじめる前に

- Cisco から直接アップグレードをダウンロードするか、またはネットワーク上のサーバからアップグレードイメージをホストするかを選択します。次に、選択した方式をサポートするようにネットワークをセットアップします。そして、選択した入手先からアップグレードを入手するために電子メールゲートウェイを設定します。アップグレードおよび

アップデートを取得するための設定 （1254 ページ）およびアップグレードおよびアップデートをダウンロードするためのサーバ設定 （1259 ページ）を参照してください。

- ここで、アップグレードをインストールする場合は、AsyncOS のアップグレードの準備（1266 ページ）の手順を実行します。
- クラスタ化されたシステムのアップグレードをインストールする場合は、クラスタ内のマシンのアップグレード （1494 ページ）を参照してください。
- アップグレードをダウンロードするだけの場合、インストールの準備が完了するまでの前提条件はありません。
- アップグレード後は、FIPS モードでは TLS v1.0 を使用できなくなります。ただし、必要に応じて、電子メールゲートウェイで TLS v1.0 を再び有効にすることができます。

手順

ステップ 1 [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 2 [アップグレードオプション（Upgrade Options）] をクリックします。

ステップ 3 [アップグレード（Upgrade）] をクリックしてアップグレードプロセスに進みます。

ステップ 4 次のオプションを選択します。

目的	操作手順
1 回の操作でアップグレードのダウンロードとインストールを実行する	[ダウンロードしてインストール（Download and Install）] をクリックします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。
アップグレードインストーラをダウンロードする	[ダウンロードのみ（Download only）] をクリックします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。 インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。
ダウンロードしたアップグレードインストーラをインストールする	[Install（インストール）] をクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。 インストールする AsyncOS のバージョンは、[インストール（Install）] オプションの下に表示されます。

ステップ 5 以前にダウンロードしたインストーラでインストールする場合を除き、利用可能なアップグレードのリストから AsyncOS のバージョンを選択します。

ステップ 6 インストール中の場合、次に従います。

a) 現在の設定を電子メールゲートウェイ上の configuration ディレクトリに保存するかどうかを選択します。
b) コンフィギュレーション ファイルでパスフレーズをマスクするかどうかを選択します。

（注） マスクされたパスフレーズが記載されたコンフィギュレーション ファイルは、GUI の [設定ファイル（Configuration File）] ページや CLI の loadconfig コマンドからロードできません。

c) コンフィギュレーションファイルのコピーを電子メールで送信する場合は、ファイルを送信する電子メールアドレスを入力します。複数の電子メールアドレスを指定する場合は、カンマで区切ります。

ステップ 7 [続行（Proceed）] をクリックします。

ステップ 8 インストール中の場合、次に従います。

a) プロセス中のプロンプトに応答できるようにしてください。

応答するまでプロセスは中断されます。

ページの上部の近くに、経過表示バーが表示されます。

b) プロンプトで、[今すぐ再起動（Reboot Now）] をクリックします。
c) 約 10 分後、電子メールゲートウェイにアクセスしてログインします。

アップグレードの問題を修正するために電子メールゲートウェイの電源を再投入する必要があると思われる場合は、再起動後 20 分以上が経過してから再投入してください。

次のタスク

- プロセスが中断された場合、プロセスを再開する必要があります。
- アップグレードをダウンロードしてインストールしなかった場合は次のとおりです。

  アップグレードをインストールする準備ができたら、「始める前に」の項の前提条件も含め次の手順を最初から実行しますが、[インストール（Install）] オプションを選択します。

- アップグレードをインストールした場合、次のとおりです。
  - リスナーを再びイネーブル（再開）にします。
  - 新しいシステムの設定ファイルを保存します。詳細については、設定ファイルの管理（1243 ページ）を参照してください。
- アップグレードが完了したら、再びリスナーをイネーブルにします。

バックグラウンド ダウンロードのキャンセルまたは削除ステータスの表示

手順

ステップ 1 [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 2 [アップグレードオプション（Upgrade Options）] をクリックします。

ステップ 3 次のオプションを選択します。

目的	操作手順
ダウンロードステータスの表示	ページの中央を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。
ダウンロードのキャンセル	ページの中央にある、[ダウンロードをキャンセル（Cancel Download）] ボタンをクリックします。 このオプションは、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除（Delete File）] ボタンをクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。

ステップ 4 （任意）アップグレード ログを確認します。

リモート電源再投入の有効化

電子メールゲートウェイシャーシの電源をリモートでリセットする機能は、80および90シリーズ ハードウェアでのみ使用できます。

電子メールゲートウェイの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

はじめる前に

- 専用のリモート電源再投入（RPC）ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、ハードウェア インストレーション ガイドを参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、電子メールゲートウェイがリモートアクセス可能であることを確認します。

- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。**ipconfig** コマンドを使用して設定することはできません。
- 電子メールゲートウェイの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスへのアクセスに関する詳細については、CLI のリファレンス ガイドを参照してください。

手順

ステップ 1 SSH またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

ステップ 2 管理者権限を持つアカウントを使用してログインします。

ステップ 3 以下のコマンドを入力します。

```
remotepower
setup
```

ステップ 4 プロンプトに従って、以下の情報を指定します。

1. この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
2. 電源の再投入コマンドを実行するために必要なユーザ名とパスフレーズ。

   これらのクレデンシャルは、電子メールゲートウェイへのアクセスに使用する他のクレデンシャルに依存しません。

ステップ 5 commit を入力して変更を保存します。

ステップ 6 設定をテストして、電子メールゲートウェイの電源をリモートで管理できることを確認します。

ステップ 7 入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

次のタスク

関連項目

- 電子メールゲートウェイの電源のリモートリセット （1538 ページ）

AsyncOS の以前のバージョンへの復元

AsyncOS には、緊急時に AsyncOS オペレーティング システムを以前の認定済みのビルドに戻す機能があります。

復元の影響

電子メールゲートウェイにおける revert コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての設定ログおよびデータベースを破壊します。管理インターフェイスのネットワーク情報のみが保存されます。他のすべてのネットワーク設定は削除されます。さらに、復元は電子メールゲートウェイが再設定されるまでメール処理を中断します。このコマンドはネットワーク設定を破壊するため、revert コマンドを発行する場合は電子メールゲートウェイへの物理的なローカルアクセスが必要になります。

注意 戻し先のバージョンのコンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルに下位互換性はありません。

仮想電子メールゲートウェイでの AsyncOS の復元がライセンスに影響を及ぼす可能性

AsyncOS 9.0 for Email から AsyncOS 8.5 for Email に復元した場合、ライセンスは変更されません。

AsyncOS 9.0 for Email から AsyncOS 8.0 for Email に復元した場合、電子メールゲートウェイがセキュリティ機能なしでメールを配信する 180 日間の猶予期間はなくなります。

どちらの場合も、ライセンス キーの有効期限は変更されません。

関連項目

- 仮想電子メールゲートウェイのライセンスの有効期限 （1242 ページ）

AsyncOS の復元

手順

ステップ 1 戻し先のバージョンの設定ファイルがあることを確認してください。設定ファイルに下位互換性はありません。設定ファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。詳細については、設定ファイルのメール送信 （1245 ページ）を参照してください。

ステップ 2 電子メールゲートウェイの現在の設定のバックアップコピーを、（パスフレーズをマスクしない状態で）別のマシンに保存します。

（注） このコピーは、バージョンを戻した後にロードする設定ファイルではありません。

ステップ 3 セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。

ステップ 4 メール キューが空になるまで待ちます。

ステップ 5 バージョンを戻す電子メールゲートウェイの CLI にログインします。

revert コマンドの実行時には、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないてください。

ステップ 6 CLI から **revert** コマンドを発行します。

（注） 復元プロセスは時間のかかる処理です。復元が完了して、電子メールゲートウェイへのコンソールアクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

ステップ 7 電子メールゲートウェイが 2 回リブートするまで待ちます。

ステップ 8 マシンが 2 回再起動したら、シリアル コンソールで **interfaceconfig** コマンドを使用して、アクセス可能な IP アドレスをインターフェイスに設定します。

ステップ 9 設定したインターフェイスの 1 つで FTP または HTTP をイネーブルにします。

ステップ 10 作成した XML 設定ファイルを FTP で取得するか、または GUI インターフェイスに貼り付けます。

ステップ 11 戻し先のバージョンの XML 設定ファイルをロードします。

ステップ 12 セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースをインポートして復元します。

ステップ 13 変更を保存します。

復元が完了した電子メールゲートウェイは、選択された AsyncOS バージョンを使用して稼働します。

電子メールゲートウェイに生成されるメッセージの返信アドレスの設定

AsyncOS によって、次のタイミングで生成されるメールのエンベロープ送信者を設定できます。

- Anti-Virus 通知
- バウンス
- DMARC フィードバック
- 通知（notify() および notify-copy() フィルタの動作）
- 隔離通知（および隔離管理機能における「コピー送信」）
- レポート
- その他のすべてのメッセージ

返信アドレスの表示、ユーザー、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

システムで生成された電子メール メッセージの返信アドレスを GUI または addressconfig コマンドを使用して CLI で変更できます。

手順

ステップ 1 [システム管理（System Administration）] > [返信先アドレス（Return Addresses）] ページの順に進みます。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 1 つまたは複数のアドレスへの変更

ステップ 4 変更を送信し、保存します。

システム状態パラメータのしきい値の設定

組織の要件に応じて、CPU 使用率や作業キューの最大メッセージ数など、電子メールゲートウェイのさまざまな状態パラメータのしきい値を設定できます。指定されたしきい値を超えた場合にアラートを送信するように、電子メールゲートウェイを設定することもできます。

（注） CLI を使用してシステムのヘルス パラメータのしきい値を設定するには、healthconfig コマンドを使用します。詳細については、CLIのインライン ヘルプ、または『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

はじめる前に

しきい値を注意深く決定します。

手順

ステップ 1 [システム管理（System Administration）] > [システムの状態（System Health）] をクリックします。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 次のオプションを設定します。

- CPU 使用率のしきい値レベルを指定します（パーセント）。

  現在の CPU 使用率が設定済みのしきい値を超えた場合に、アラートを受信するかどうかを指定します。最初のアラートが送信された後、最初のアラートがトリガーされてから 15 分以内に、CPU 使用率が移動平均を 5% 超えた場合、追加のアラートが送信されます。

（注） メール処理プロセスのCPU使用率だけに基づいて、これらのアラートがトリガーされます。

- メモリ ページ スワッピングのしきい値レベルを指定します（割合）。

  全体的なメモリ スワップ使用率が設定済みのしきい値を超えた場合に、アラートを受信するかどうかを指定します。最初のアラートが送信された後、メモリページスワッピングが最初のアラートをトリガーした値を150%超えた場合、または15分のアラート間隔の後、追加のアラートが送信されます。例えば、しきい値が 10 に設定されている場合、

  - メモリ スワップ使用率が 10.1% に達すると、最初のアラートが送信されます。
  - メモリ スワップ使用率が 15.1% に達すると、もう一度アラートが送信されます。

- 作業キューの最大メッセージ数のしきい値レベルを指定します（メッセージ数）。

  また、作業キューのメッセージ数が設定済みのしきい値を超えた場合に、アラートを受信するかどうかを指定します。最初のアラートが送信された後、15分以内に作業キューの最大メッセージ数が最初のアラートをトリガーした値を 150% 超えた場合、追加のアラートが送信されます。たとえば、しきい値が 1000 に設定されている場合、

  - 作業キューの最大メッセージ数が 1002 に達したときに、最初のアラートが送信されました。
  - 15 分以内に作業キューの最大メッセージ数が 1510 に達すると、アラートがもう 1 つ送信されます。

（注） この機能のアラートはすべて、システム アラート カテゴリに属します。

ステップ 4 変更を送信し、保存します。

次のタスク

この機能のアラートを設定した場合は、システムアラートに登録されていることを確認してください。この説明については、アラート受信者の追加 （1277 ページ） を参照してください。

電子メールゲートウェイの状況の確認

ヘルスチェック機能を使用して、電子メールゲートウェイの状態を確認できます。ヘルスチェックを実行すると、現在のステータスログの履歴データ（最大3カ月）が分析され、電子メールゲートウェイの状態が判断されます。

（注） システムでこの分析を実行するには、ステータス ログに 1 カ月以上のログ データが含まれている必要があります。

ヘルス チェックを実行するには、

- Web インターフェイスで、[システム管理（System Administration）] > [システムの状態（System Health）] ページに移動して、[ヘルスチェックを実行（Run Health Check）] をクリックします。
- CLI で、コマンド **healthcheck** を実行します。

分析結果により、過去数カ月にシステムで次の問題が 1 つ以上発生したかどうかが示されます。

- リソース節約モード
- メール処理の遅延
- High CPU usage
- 高いメモリ使用量
- 高いメモリ ページ スワッピング

ヘルスチェックにおいて、電子メールゲートウェイで上記の問題が 1 つ以上発生していることが示された場合、システム設定を確認して最適化することを検討してください。詳細については、
http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html
を参照してください。

アラート

アラートメッセージは自動生成される標準電子メールメッセージであり、E メール ゲートウェイで発生するイベントに関する情報が含まれています。これらのイベントにはマイナーからメジャーまでの重要度（または重大度）レベルがあり、一般的に E メール ゲートウェイの特定のコンポーネントまたは機能に関連しています。アラートは、E メール ゲートウェイで生成されます。送信するアラートメッセージの種類、重大度、および送信するユーザを非常に詳細なレベルで指定できます。アラートは、GUI の [システム管理（System Administration）] > [アラート（Alerts）] ページ（または CLI の alertconfig コマンド）で管理します。

アラートの重大度

アラートは、次の重大度に従って送信されます。

- クリティカル：すぐに対処が必要です。
- 警告：今後モニタリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります。
- 情報：デバイスのルーティン機能で生成される情報。

AutoSupport

十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラートメッセージをシスコに送信するように電子メールゲートウェイを設定できます。この機能は AutoSupport と呼ばれ、シスコによるお客様のニーズへのプロアクティブな対応に役

立ちます。また、AutoSupport はシステムの稼働時間、**status** コマンドの出力、および使用されている AsyncOS バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラート タイプが System で重大度レベルが Information のアラートを受信するように設定されているアラート受信者は、シスコに送信される各メッセージのコピーを受信します。内部にアラート メッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能をイネーブルまたはディセーブルにするには、アラート設定値の設定（1278ページ）を参照してください。

アラートの配信

電子メールゲートウェイから [アラート受信者（Alert Recipient）] で指定されたアドレスに送信されるアラートは、該当の送信先に対して定義された SMTP ルートに従います

アラートメッセージは電子メールゲートウェイ内の問題の通知に使用されるため、送信にAsyncOSの標準メール配信システムを使用しません。代わりに、アラートメッセージはAsyncOSで重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メール システムで処理されます。

アラート メール システムは、AsyncOS と同一の設定を共有しません。このため、アラート メッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラート メッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - アラート メッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- アラート メッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージ フィルタまたはコンテンツ フィルタの処理対象にも含まれません。
- アラートメッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

（注） （オプション - TLS サポートが `alertconfig` CLI コマンドを使用して有効化され、FQDN 検証が [SSL構成時の設定（SSL Configuration Settings）] ページで有効な場合のみ）：サーバ証明書にある [共通名（Common Name）]、[SAN: DNS名（SAN: DNS Name）] フィールド、またはその両方が FQDN 形式かどうかを確認します

（注） （オプション - TLS サポートが `alertconfig` CLI コマンドを使用して有効化され、X 509 検証が [SSL構成時の設定（SSL Configuration Settings）] ページで有効な場合のみ）：サーバ証明書の署名アルゴリズムを確認します。

アラート メッセージの例

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see
http://support.ironport.com

If you desire further information, please contact your support provider.
```

アラート受信者の追加

アラートエンジンでは、送信するアラートの種類とアラート受信者を詳細に制御できます。たとえば、アラート受信者が System（アラートの種類）に関する Critical（重大度）の情報が送信されたときのみ通知を受信するように設定することで、アラート受信者に特定のアラートのみを送信するように設定できます。

（注） システムのセットアップ時に AutoSupport をイネーブルにした場合、指定した電子メールアドレスにすべての重大度およびクラスのアラートを受信します（デフォルト）。この設定はいつでも変更できます。

手順

ステップ 1 [システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ 2 [受信者を追加（Add Recipient）] をクリックします。

ステップ 3 受信者の電子メールアドレスを入力します。複数のアドレスをカンマで区切って入力することもできます。

ステップ 4 （任意）シスコ サポートからソフトウェア リリースおよび重大なサポート通知のアラートを受信するには、[リリースおよびサポート通知（Release and Support Notifications）] をオンにします。

ステップ 5 この受信者が受信するアラートのタイプと重大度を選択します。

ステップ 6 変更を送信し、保存します。

アラート設定値の設定

次の設定は、すべてのアラートに適用されます。

（注） 後から確認するために 電子メールゲートウェイに保存するアラートの数を定義するには alertconfig CLI コマンドを使用します。

手順

ステップ 1 [アラート（Alerts）] ページで [設定を編集（Edit Settings）] をクリックします。

ステップ 2 アラートの送信に使用する Header From: アドレスを入力するか、[自動生成（Automatically Generated）]（「alert@<hostname>」を自動生成）を選択します。

ステップ 3 重複したアラートを送信するまでに待機する秒数を指定する場合は、チェックボックスをオンにします。詳細については、重複したアラートの送信 （1279 ページ）を参照してください。

- 重複したアラートを送信するまでに待機する秒数の初期値を指定します。
- 重複したアラートを送信するまでに待機する秒数の最大値を指定します。

ステップ 4 [IronPort AutoSupport] オプションをオンにすることで、AutoSupport をイネーブルにできます。AutoSupport の詳細については、AutoSupport （1275 ページ）を参照してください。

- AutoSupport がイネーブルの場合、Information レベルの System アラートを受信するように設定されたアラート受信者に、毎週 AutoSupport レポートが送信されます。チェックボックスを外すことでディセーブルにできます。

ステップ 5 変更を送信し、保存します。

アラート設定

アラート設定では、アラートの全般的な動作と設定を制御します。設定には次のような項目があります。

- RFC 2822 Header From：アラートを送信するタイミング（アドレスを入力するか、デフォルトの「alert@<hostname>」を使用します）。また、alertconfig -> from コマンドを使用して、この値を CLI で設定することもできます。
- 重複したアラートを送信するまでに待機する秒数の初期値。
- 重複したアラートを送信するまでに待機する秒数の最大値。
- AutoSupport のステータス（イネーブルまたはディセーブル）。

- Information レベルの System アラートを受信するように設定されたアラート受信者への、AutoSupport の毎週のステータス レポートの送信。

重複したアラートの送信

AsyncOSが重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を0に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、アラートは5秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に大きな秒数になります。[重複するアラート メッセージを送信する前に待機する最大の秒数（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

最新アラートの表示

電子メールゲートウェイは最新のアラートを保存するので、アラートメッセージを消失または削除した場合にGUIおよびCLIの両方で表示できます。これらのアラートは、電子メールゲートウェイからダウンロードできません。

最新のアラートのリストを表示するには、[アラート（Alerts）]ページにある[トップアラートを表示（View Top Alerts）] ボタンをクリックするか、CLI で displayalerts コマンドを使用します。GUI でアラートを、日付、レベル、クラス、テキスト、受信者によって調整します。

デフォルトでは、電子メールゲートウェイは **[トップアラート（Top Alerts）]** ウィンドウに表示するために最大 50 個のアラートを保存します電子メールゲートウェイが保存するアラートの数を編集するには、CLI で alertconfig -> setup コマンドを使用します。この機能を無効にするにはアラートの数を 0 に変更します。

アラートの説明

次の表に、分類したアラートのリストを示します。表には、アラート名（Cisco で使用される内部記述子）、アラートの実際のテキスト、説明、重大度（critical、information、または warning）およびメッセージのテキストに含まれるパラメータ（存在する場合）が含まれています。アラートの実際のテキストでは、パラメータ値は置き換えられます。たとえば、次のアラート メッセージではメッセージのテキストに「$ip」が記述されています。アラート生成時に「$ip」は実際の IP アドレスに置き換えられます。

- アンチスパム アラート （1280 ページ）
- アンチウイルス アラート （1280 ページ）
- ディレクトリ獲得攻撃（DHAP）アラート （1281 ページ）

- ハードウェア アラート （1282 ページ）
- スパム隔離アラート （1283 ページ）
- セーフリスト/ブロックリスト アラート （1284 ページ）
- システム アラート （1285 ページ）
- アップデータ アラート （1298 ページ）
- アウトブレイク フィルタ アラート （1299 ページ）
- クラスタリング アラート （1300 ページ）

アンチスパム アラート

次の表は、AsyncOS で生成されるさまざまなアンチスパム アラートのリストです。アラートの説明と重大度が記載されています。

表 *95*：発生する可能性があるアンチスパム アラートのリスト

アラート名	メッセージと説明	パラメータ
AS.SERVER.ALERT	$engine anti-spam - $message $tb クリティカル。アンチスパム エンジンに障害が発生した場合に送信されます。	「**engine**」：アンチスパム エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
AS.TOOL.INFO_ALERT	Update - $engine - $message 情報。アンチスパム エンジンに問題が発生した場合に送信されます。	「**engine**」：アンチスパム エンジンの名前 「**message**」：メッセージ。
AS.TOOL.ALERT	Update - $engine - $message クリティカル。アンチスパム エンジンの管理に使用されるツールの 1 つに問題があり、アップデートが中止される場合に送信されます。	「**engine**」：アンチスパム エンジンの名前 「**message**」：メッセージ。

アンチウイルス アラート

次の表は、AsyncOS で生成されるさまざまなアンチウイルス アラートのリストです。アラートの説明と重大度が記載されています。

表 *96 :* 発生する可能性があるアンチウイルス アラートのリスト

アラート名	メッセージと説明	パラメータ
AV.SERVER.ALERT /AV.SERVER.CRITICAL	$engine antivirus - $message $tb クリティカル。アンチウイルス スキャン エンジンに重大な問題が発生した場合に送信されます。	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb 情報。アンチウイルス スキャン エンジンに情報イベントが発生した場合に送信されます。	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb 警告。アンチウイルス スキャン エンジンに問題が発生した場合に送信されます。	「**engine**」：アンチウイルス エンジンのタイプ。 「**message**」：ログ メッセージ。 「**tb**」：イベントのトレースバック。
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID $mid antivirus $what error $tag クリティカル。メッセージのスキャン中に、アンチウイルス スキャンがエラーを生成した場合に送信されます。	「**mid**」：MID 「**what**」：発生したエラー。 「**tag**」：ウイルス アウトブレイク名（設定されている場合）。
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid is malformed and cannot be scanned by $engine. クリティカル。メッセージが不正なため、スキャン エンジンはメッセージのスキャンに失敗しました。再試行の最大回数を超過したため、メッセージはエンジンにスキャンされずに処理されます。	「**mid**」：MID 「**engine**」：使用されているエンジン。

ディレクトリ獲得攻撃（DHAP）アラート

以下の表は、AsyncOS で生成されるさまざまな DHAP アラートのリストです。アラートの説明と重大度が記載されています。

表 *97 :* 発生する可能性があるディレクトリ獲得攻撃アラートのリスト

アラート名	メッセージと説明	パラメータ
LDAP.DHAP_ALERT	LDAP: Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack.	
	警告。ディレクトリ獲得攻撃の可能性を検出した場合に送信されます。	

ハードウェア アラート

以下の表は、AsyncOS で生成されるさまざまなハードウェア アラートのリストです。アラートの説明と重大度が記載されています。

表 *98 :* 発生する可能性があるハードウェア アラートのリスト

アラート名	メッセージと説明	パラメータ
INTERFACE.ERRORS	Port $port: has detected $in_err input errors, $out_err output errors, $col collisions please check your media settings.	「**port**」：インターフェイス名。 「**in_err**」：最後のメッセージ以降の入力エラー数。 「**out_err**」：最後のメッセージ以降の出力エラー数。 「**col**」：最後のメッセージ以降のパケット衝突数。
	警告。インターフェイス エラーを検出した場合に送信されます。	
MAIL.MEASUREMENTS_FILESYSTEM	The $file_system partition is at $capacity% capacity	「**file_system**」：ファイルシステムの名前 「**capacity**」：ファイル システムの使用率（%）。
	警告。ディスク パーティションが 75 % の使用率に近づいた場合に送信されます。	
MAIL.MEASUREMENTS_FILESYSTEM。CRITICAL	The $file_system partition is at $capacity% capacity	「**file_system**」：ファイルシステムの名前 「**capacity**」：ファイル システムの使用率（%）。
	クリティカル。ディスク パーティションが 90 % の使用率に達した場合（95 %、96 %、97 % など）に送信されます。	
SYSTEM.RAID_EVENT_ALERT	A RAID-event has occurred: $error	「**error**」：RAID エラーのテキスト。
	警告。重大な RAID-event が発生した場合に送信されます。	

アラート名	メッセージと説明	パラメータ
SYSTEM.RAID_EVENT_ALERT_INFO	A RAID-event has occurred: $error 情報。RAID-event が発生した場合に送信されます。	「**error**」：RAID エラーのテキスト。

スパム隔離アラート

以下の表は、AsyncOS で生成されるさまざまなスパム隔離アラートのリストです。アラートの説明と重大度が記載されています。

表 *99*：発生する可能性があるスパム隔離アラートのリスト

アラート名	メッセージと説明	パラメータ
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at $host:$port 情報。AsyncOS が（オフボックス）IP アドレスに接続できない場合に送信されます。	「**host**」：オフボックス隔離のアドレス。 「**port**」：オフボックス隔離に接続するポート。
ISQ.CRITICAL	ISQ: $msg クリティカル。スパム隔離に重大なエラーが発生した場合に送信されます。	「**msg**」：表示されるメッセージ
ISQ.DB_APPROACHING_FULL	ISQ: Database over $threshold% full 警告。スパム隔離データベースがフルに近い場合に送信されます。	「**threshold**」：アラートを開始する使用率のしきい値
ISQ.DB_FULL	ISQ: database is full クリティカル。スパム隔離データベースがフルになった場合に送信されます。	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID $mid for $rcpt: $reason 警告。スパム隔離からの電子メールの削除に失敗した場合に送信されます。	「**mid**」：MID 「**rcpt**」：受信者または「all」 「**reason**」：メッセージが削除されない理由
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: $reason 警告。通知メッセージの送信に失敗した場合に送信されます。	「**reason**」：通知が送信されない理由

アラート名	メッセージと説明	パラメータ
ISQ.MSG_QUAR_FAILED	警告。メッセージの隔離に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID $mid to $rcpt: $reason	「**mid**」：MID 「**rcpt**」：受信者または「all」 「**reason**」：メッセージが解放されない理由
	警告。メッセージの開放に失敗した場合に送信されます。	
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID $mid: $reason	「**mid**」：MID 「**reason**」：メッセージが解放されない理由
	警告。受信者が不明のため、メッセージの開放に失敗した場合に送信されます。	
ISQ.NO_EU_PROPS	ISQ: Could not retrieve $user's properties. Setting defaults	「**user**」：エンドユーザ名
	情報。AsyncOS がユーザの情報を取得できない場合に送信されます。	
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host	
	情報。AsyncOS が外部隔離を参照するように設定されているものの、外部隔離が定義されていない場合に送信されます。	

セーフリスト/ブロックリスト アラート

次の表は、AsyncOS で生成されるさまざまなセーフリスト/ブロックリスト アラートのリストです。アラートの説明と重大度が記載されています。

表 *100*：発生する可能性があるセーフリスト/ブロックリスト アラートのリスト

アラート名	メッセージと説明	パラメータ
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '$error'.	「**error**」：エラーの原因
	クリティカル。セーフリスト/ブロックリストデータベースの復旧に失敗しました。	
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: $current of $limit.	「**current**」：データベース使用量（MB） 「**limit**」：設定された制限使用量（MB）
	クリティカル。セーフリスト/ブロックリストデータベースが許容されたディスク領域を超過しました。	

システム アラート

次の表は、AsyncOS で生成されるさまざまなシステム アラートのリストです。アラートの説明と重大度が記載されています。

表 *101* : 発生する可能性があるシステム アラートのリスト

コンポーネント/アラート名	メッセージと説明	パラメータ
AMP.ENGINE.ALERT	Advanced Malware Protection の問題に関するアラートの確実な受信 （615 ページ）を参照してください	-
AMP.ENGINE.ALERT.WARN	アラートテキスト：ファイル分析グループ名を Cisco Threat Grid サーバーに登録できませんでした。Cisco TAC に連絡して、サポートを受けてください。 アラートレベル：警告（WARNING）。 説明：電子メールゲートウェイが、スマートアカウント ID を使用したアプライアンスグループ名の Cisco Thread Grid サーバーへの登録に失敗すると、アラートが送信されます。	パラメータ：失敗の理由
AsyncOS API アラート	『AsyncOS API for Cisco Secure Email Gateway - Getting Started Guide』の「Alerts」セクションを参照してください。	-
メールボックス自動修復アラート	の「アラート」セクションを参照してください。 メールボックスでのメッセージの修復（709 ページ）	-
COMMON.APP_FAILURE	An application fault occurred: $error 警告。不明なアプリケーション障害が発生した場合に送信されます。	「**error**」：エラーのテキスト（通常はトレースバック）
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<$level>: <$class> 情報：自動更新が特定のエンジン <$engine> に対して有効になっています。これでこのエンジンの自動エンジン更新を受け取ることになります。	'**$engine**'：サービス エンジンの名前。値は次のとおりです。 • Sophos • McAfee • グレイメール

コンポーネント/アラート名	メッセージと説明	パラメータ
COMMON.ENGINE_AUTO_UPDATE_DISABLED	<$level>: <$class> 情報：自動更新が特定のエンジン <$engine> に対して無効になっています。特定のエンジンのグローバル設定ページで自動更新を有効にしない限り、このエンジンの自動更新を受け取ることはありません。	'**$engine**'：サービス エンジンの名前。値は次のとおりです。 • Sophos • McAfee • グレイメール
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired. Please contact your authorized Cisco sales representative. 警告。ライセンス キーの有効期限が切れた場合に送信されます。	「**feature**」：有効期限が切れる機能の名前。
COMMON.KEY_EXPIRING_ALERT	Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative. 警告。ライセンス キーの有効期限が切れる場合に送信されます。	「**feature**」：有効期限が切れる機能の名前。 「**days**」：有効期限が切れるまでの日数。
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice. Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative. 警告。ライセンス キーの有効期限が切れる場合の最後の通知として送信されます。	「**feature**」：有効期限が切れる機能の名前。 「**days**」：有効期限が切れるまでの日数。
KEYS.GRACE_EXPIRING_ALERT	この電子メールゲートウェイのすべてのセキュリティ サービス ライセンスが期限切れになりました。The email gateway will continue to deliver mail without security services for $days days. To renew security services licenses, Please contact your authorized Cisco sales representative. クリティカル。仮想電子メールゲートウェイのライセンス有効期限について、猶予期間の開始時点から定期的に送信されます。	「**days**」：アラート送信時点での猶予期間の残り日数。 猶予期間の詳細については、仮想電子メールゲートウェイのライセンスの有効期限 （1242 ページ）を参照してください。

コンポーネント/アラート名	メッセージと説明	パラメータ
KEYS.GRACE_FINAL_EXPIRING_ALERT	This is the final notice. All security services licenses for this email gateway have expired. The email gateway will continue to deliver mail without security services for 1 day. To renew security services licenses, Please contact your authorized Cisco sales representative. クリティカル。仮想電子メールゲートウェイライセンスの有効期限の 1 日前に送信されます。	猶予期間の詳細については、仮想電子メールゲートウェイのライセンスの有効期限 （1242 ページ）を参照してください。
KEYS.GRACE_EXPIRED_ALERT	Your grace period has expired. All security sevice have expired, and your email gateway is non-functional. The email gateway will no longer deliver mail until a new license is applied. To renew security services licenses, Please contact your authorized Cisco sales representative. クリティカル。仮想電子メールゲートウェイの猶予期間を過ぎると送信されます。	猶予期間の詳細については、仮想電子メールゲートウェイのライセンスの有効期限 （1242 ページ）を参照してください。
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver. Unable to contact root servers. 警告。電子メールゲートウェイがルート DNS サーバに問い合わせることができない場合に送信されます。	
COMMON.INVALID_FILTER	Invalid $class: $error 警告。無効なフィルタが存在する場合に送信されます。	「**class**」：「Filter」、「SimpleFilter」などのいずれか。 「**error**」：フィルタが無効な理由に関する追加の情報。

コンポーネント/アラート名	メッセージと説明	パラメータ
IPBLOCKD.HOST_ADDED_TO_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	The host at $ip has been added to the blocked list because of an SSH DOS attack. The host at $ip has been permanently added to the ssh allowed list. The host at $ip has been removed from the blocked list.	「**ip**」：ログインを試行したIPアドレス。
	警告。 SSHを介して電子メールゲートウェイへの接続を試みているが、有効なクレデンシャルを提示しないIPアドレスは、2分以内に11回以上試行に失敗した場合、SSHのブロックリストに追加されます。 同じIPアドレスからユーザが正常にログインすると、そのIPアドレスは許可リストに追加されます。 許可リスト上のアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。 エントリは約1日後にブロックリストから自動的に削除されます。	
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false	「**name**」：クエリーの名前。
	クリティカル。LDAPグループクエリーに失敗した場合に送信されます。	
LDAP.HARD_ERROR	LDAP: work queue processing error in $name reason $why	「**name**」：クエリーの名前。 「**why**」：エラーが発生した理由。
	クリティカル。LDAPクエリーが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。	
LOG.ERROR.*	クリティカル。さまざまなロギングエラー。	
MAIL.FILTER.RULE_MATCH_ALERT	MID $mid matched the $rule_name rule. \n Details: $details	「**mid**」：メッセージの一意の識別番号。 「**rule_name**」：一致したルールの名前。 「**details**」：メッセージまたはルールに関する詳細情報。
	情報。Header Repeatsルールがtrueと評価されるたびに送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server. クリティカル。各受信者のスキャン時にLDAP グループ クエリーに失敗した場合に送信されます。	
MAIL.QUEUE.ERROR.*	クリティカル。メール キューのさまざまなハード エラー。	
MAIL.OMH.DELIVERY_RETRY	Subject - 'Alert: Message Delivery failed for $hostname. DANE verification failed for one or more Domain(s).' メッセージ - The message delivery failed due to DANE verification failure for all mail exchange (MX) hosts in $hostname.電子メールゲートウェイはメッセージの配信を再度試行するか、メッセージをバウンスします。	' host' - DANE 検証が失敗したホスト。
MAIL.RES_CON_START_ALERT. MEMORY	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. RAM utilization for this system has exceeded the resource conservation threshold of $memory_threshold_start%. The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches $memory_threshold_halt%. クリティカル。メモリ使用率がシステム リソース節約しきい値を超過した場合に送信されます。	「**hostname**」： ホストの名前。 「**memory_threshold_start**」：メモリのターピットを開始するパーセントしきい値。 「**memory_threshold_halt**」：メモリがフルのためにシステムが停止するパーセントしきい値。
MAIL.RES_CON_START_ALERT. QUEUE_SLOW	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. The queue is overloaded and is unable to maintain the current throughput. クリティカル。メール キューが過負荷となり、システム リソース節約がイネーブルになった場合に送信されます。	「**hostname**」： ホストの名前。

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.RES_CON_START_ ALERT. QUEUE	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Queue utilization for this system has exceeded the resource conservation threshold of $queue_threshold_start%. The allowed receiving rate for this system will be gradually decreased as queue utilization approaches $queue_threshold_halt%.	「**hostname**」：ホストの名前。 「**queue_threshold_start**」：キューのターピットを開始するパーセントしきい値。 「**queue_threshold_halt**」：キューがフルのためにシステムが停止するパーセントしきい値。
	クリティカル。キュー使用率がシステム リソース節約しきい値を超過した場合に送信されます。	
MAIL.RES_CON_START_ ALERT. WORKQ	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Listeners have been suspended because the current work queue size has exceeded the threshold of $suspend_threshold. Listeners will be resumed once the work queue size has dropped to $resume_threshold. These thresholds may be altered via use of the 'tarpit' command on the system CLI.	「**hostname**」：ホストの名前。 「**suspend_threshold**」：リスナーが一時停止されるワーク キューの下限サイズ。 「**resume_threshold**」：リスナーが再開されるワーク キューの上限サイズ。
	情報。ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。	
MAIL.RES_CON_START_ ALERT	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.	「**hostname**」：ホストの名前。
	クリティカル。電子メールゲートウェイが「リソース節約」モードになった場合に送信されます。	
MAIL.RES_CON_STOP_ALERT	This system (hostname: $hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.	「**hostname**」：ホストの名前。
	情報。電子メールゲートウェイの「リソース節約」モードが解除された場合に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.URL_REP_CLIENT.CATEGORY_CHANGE	将来の URL カテゴリ セットの変更 （584 ページ）を参照してください。	—
MAIL.BEAKER_CONNECTOR.CERTIFICATE_INVALID	URL フィルタリングのトラブルシューティング （562 ページ）を参照してください。	
MAIL.BEAKER_CONNECTOR.ERROR_FETCHING_CERTIFICATE		
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, $num msgs, $reason クリティカル。ワーク キューが中断された場合に送信されます。	「**num**」：ワーク キューに存在するメッセージ数。 「**reason**」：ワーク キューが中断された理由。
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, $num msgs クリティカル。ワーク キューが再開された場合に送信されます。	「**num**」：ワーク キューに存在するメッセージ数。
NTP.NOT_ROOT	Not running as root, unable to adjust system time 警告。root として NTP が実行されていないために電子メールゲートウェイが時刻を調整できない場合に送信されます。	
QUARANTINE.ADD_DB_ERROR	Unable to quarantine MID $mid - quarantine system unavailable クリティカル。メッセージを隔離エリアに送ることができない場合に送信されます。	「**mid**」：MID
QUARANTINE.DB_UPDATE_FAILED	Unable to update quarantine database (current version: $version; target $target_version) クリティカル。隔離データベースがアップデートできない場合に送信されます。	「**version**」：検出されたスキーマ バージョン。 「**target_version**」：対象のスキーマ バージョン。
QUARANTINE.DISK_SPACE_LOW	The quarantine system is unavailable due to a lack of space on the $file_system partition. クリティカル。隔離用のディスク領域がフルになった場合に送信されます。	「**file_system**」：ファイルシステムの名前
QUARANTINE.THRESHOLD_ALERT	Quarantine "$quarantine" is $full% full 警告。隔離エリアの容量使用率が 5 %、50 %、または 75 % に達した場合に送信されます。	「**quarantine**」：隔離の名前。 「**full**」：隔離エリアの容量使用率。

コンポーネント/アラート名	メッセージと説明	パラメータ
QUARANTINE.THRESHOLD_ALERT.SERIOUS	Quarantine "$quarantine" is $full% full クリティカル。隔離エリアの容量使用率が 95 % に達した場合に送信されます。	「**quarantine**」：隔離の名前。 「**full**」：隔離エリアの容量使用率。
REPORTD.DATABASE_OPEN_FAILED_ALERT	The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg クリティカル。レポート エンジンがデータベースを開けない場合に送信されます。	「**err_msg**」：発生したエラー メッセージ
REPORTD.AGGREGATION_DISABLED_ALERT	Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc.). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically. 警告。システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportdは集約をディセーブルにし、アラートを送信します。	「**threshold**」：しきい値
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration). 警告。レポート エンジンがレポート データを保存できなかった場合に送信されます。	「**duration**」：クライアントがレポートデーモンへの問い合わせを試行する時間。この値は、人間が読み取れる形式の文字列です（「1h 3m 27s」）。
REPORTING.CLIENT.JOURNAL.FULL	Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost. クリティカル。レポートエンジンが新規データを保存できない場合に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
REPORTING.CLIENT.JOURNAL.FREE	Reporting Client: The reporting system is now able to handle new data. 情報。レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE	A failure occurred while building periodic report '$report_title'. This subscription has been removed from the scheduler. クリティカル。レポート エンジンがレポートを作成できない場合に送信されます。	「**report_title**」：レポートのタイトル
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE	A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler. クリティカル。レポートを電子メールで送信できなかった場合に送信されます。	「**report_title**」：レポートのタイトル
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report '$report_title'. This subscription has been removed from the scheduler. クリティカル。レポートをアーカイブできなかった場合に送信されます。	「**report_title**」：レポートのタイトル
SENDERBASE.ERROR	Error processing response to query $query: response was $response 情報。SenderBase からの応答を処理中にエラーが発生した場合に送信されます。	「**query**」：クエリーするアドレス。 「**response**」：受信した応答の raw データ。
SMTPAUTH.FWD_SERVER_FAILED_ ALERT	SMTP Auth: could not reach forwarding server $ip with reason: $why 警告。SMTP 認証転送サーバが到達不能である場合に送信されます。	「**ip**」：リモート サーバの IP。 「**why**」：エラーが発生した理由。
SMTPAUTH.LDAP_QUERY_FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details. 警告。LDAP クエリーが失敗した場合に送信されます。	

コンポーネント/アラート名	メッセージと説明	パラメータ
SYSTEM.HERMES_SHUTDOWN_FAILURE. REBOOT	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=reboot 警告。再起動中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	「**error**」：発生したエラー。
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=shut down 警告。システムをシャットダウンしている際に問題が発生した場合に送信されます。	「**error**」：発生したエラー。
SYSTEM.LOGIN_FAILURES_LOCK_ALERT	User "$user" is locked after $numlogins consecutive login failures. Last login attempt was from $rhost 情報：失敗したログイン試行が最大数になったためにユーザ アカウントがロックされると送信されます。	'user'：ユーザの名前 'numlogins'：構成済みのアラートしきい値 ' rhost'：リモート ホストのアドレス
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Error updating recipient validation data: $why クリティカル。受信者検証のアップデートに失敗した場合に送信されます。	「why」：エラー メッセージ。
SYSTEM.SERVICE_TUNNEL.DISABLED	Tech support: Service tunnel has been disabled 情報。シスコ サポート サービス用に作成されたトンネルが無効の場合に送信されます。	
SYSTEM.SERVICE_TUNNEL.ENABLED	Tech support: Service tunnel has been enabled, port $port 情報。シスコ サポート サービス用に作成されたトンネルが有効の場合に送信されます。	「**port**」：サービス トンネルに使用されるポート。

コンポーネント/アラート名	メッセージと説明	パラメータ
IPBLOCKD.HOST_ADDED_TO_ALLOWED_LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED_LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED_LIST	The host at $ip has been added to the blocked list because of an SSH DOS attack. The host at $ip has been permanently added to the ssh allowed list. The host at $ip has been removed from the blocked list.	「**ip**」：ログインを試行したIPアドレス。
	警告。 SSHを介して電子メールゲートウェイへの接続を試みているが、有効なクレデンシャルを提示しないIPアドレスは、2分以内に11回以上試行に失敗した場合、SSHのブロックリストに追加されます。 同じIPアドレスからユーザが正常にログインすると、そのIPアドレスは許可リストに追加されます。 許可リスト上のアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。 エントリは約1日後にブロックリストから自動的に削除されます。	
WATCHDOG_RESTART_ALERT_MSG	<$level>: <$class>, <$hostname>: $subject $text 警告。 電子メールゲートウェイは、次のエンジンのヘルス条件をモニタするウォッチドッグサービスを使用します。 • スパム対策 • ウイルス対策 • アンチ マルウェア防御 • グレイメール 上記のエンジンのいずれかが特定期間のウォッチドッグサービスに応答しない場合、ウォッチドッグ サービスはエンジンを再起動し、管理者にアラートを送信します。	[「件名」（'subject'）]：エンジンに固有のウォッチドッグ アラートの件名 [「テキスト」（'text'）]：エンジンに固有のウォッチドッグアラートのテキスト

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.IMH.GEODB_UPDATE_COUNTRIES'	警告。[位置情報の更新（Geolocation Update）]：サポート対象の国のリストが変更されています。 追加された国：<$added> 削除された国：<$deleted> これに応じてHAT送信者グループ、メッセージ フィルタ、およびコンテンツ フィルタの設定を確認します。	'added'：次の国が追加されます。<iso_code1>:<country_name1>,<iso_code2>:<country_name2>, 'deleted'：次の国が削除されます。<iso_code1>:<country_name1>:<iso_code2>:<country_name2>,
MAIL.UPDATED_SHORT_URL_DOMAIN_LIST	情報（Info）。短縮URLドメインのリストが更新されています。 追加されたドメイン：<$added_domains> 削除されたドメイン：<$deleted_domains>	'added_domains'：次のドメインが追加されます。<domains_1>, <domain_2> 'deleted_domains'：次のドメインが削除されます。<domain_3>, <domain_4>
MAIL.DOMAINS_NOT_REACHABLE	警告。以下のドメインは短縮されたURLサポートの電子メールゲートウェイではアクセスできません。<$domains> 電子メールゲートウェイがこれらのドメインに接続できるようにするために、ファイアウォールのルールを確認します。	<$domains>：ドメインのカンマ区切りリスト。
MAIL.UPGRADE_CONFIG_CHANGE.ALERT	情報（Info）。アップグレード中にユーザ設定値がシステムによって変更された場合に送信されます。	**'text'**：インテリジェントマルチスキャンおよびグレイメールグローバル設定がアップグレード中に変更されました。インテリジェントマルチスキャンおよびグレイメール設定のグローバル設定を確認してください。
CERTIFICATE.CERT_EXPIRING_ALERT	証明書「$certificate」は$days日後に期限切れになります。 アラートレベル：警告（WARNING）	「**certificate**」：期限が近づいている証明書の名前。 「**days**」：有効期限が切れるまでの日数。
CERTIFICATE.CERT_CRITICAL_EXPIRING_ALERT	証明書「$certificate」は$days時間後に期限切れになります。 アラートレベル：クリティカル（CRITICAL） 「クリティカル」証明書の有効期間は、5日未満です。	「**certificate**」：期限が近づいている証明書の名前。 「**days**」：日数と残り時間（HH：MM：SS）。たとえば、4日10:12:20時間（4 days 10:12:20 hour(s)）です。

コンポーネント/アラート名	メッセージと説明	パラメータ
CERTIFICATE.CERT_EXPIRED_ALER	証明書「$certificate」の有効期限が切れています。 アラートレベル：クリティカル（CRITICAL）	「**certificate**」：期限が切れている証明書の名前。
MAIL.APP.NO_ACCESS_KEY	アラートテキスト：「Cisco Advanced Phishing Protection クラウドサービスの有効期限のポーリングに失敗しました。API AccessUID と API アクセス秘密鍵を追加してください。（Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date, add API AccessUID and API Access secret key.）」 説明：API アクセスキーと秘密鍵が入力されなかったため、APP の有効期限についてのクエリに失敗して、アラートが送信されました。	該当なし
MAIL.APP.INVALID_KEY	アラートテキスト：API アクセスキーが無効なため、Cisco Advanced Phishing Protection クラウドサービスの有効期限についてのポーリングに失敗しました。（Failed to poll for the Cisco Advanced Phishing Protection Cloud Service expiry date because the API Access Key is invalid.）API アクセス UID と秘密鍵を再設定する必要があります。（You need to re-configure the API Access UID and secret key.） 説明：API アクセスキーと秘密鍵が入力されなかったため、APP の有効期限についてのクエリに失敗して、アラートが送信されました。	該当なし
MAIL.APP.EXPIRED	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスの有効期限が切れ、無効になっています。（The Cisco Advanced Phishing Protection Cloud Service has expired and is disabled.）シスコアカウントマネージャに連絡して、サービスを更新および有効化してください。（Contact your Cisco Account Manager to renew the service and enable it.） 説明：Cisco Advanced Phishing Protection クラウドサービスの有効期限が切れて無効になっています。APP ライセンスを更新して、APP サービスを有効にする必要があります。	該当なし

コンポーネント/アラート名	メッセージと説明	パラメータ
MAIL.APP.EXPIRY_REMINDER	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスは $eaas_expiry_date に期限切れになります。（Cisco Advanced Phishing Protection Cloud Service expires on $eaas_expiry_date.）シスコアカウントマネージャに連絡して、サービスを更新してください。（You need to contact your Cisco Account Manager to renew the service.） 説明：有効期限の 3 日前からアラートが毎日送信されます。	パラメータ：eaas_expiry_date eaas_expiry_date（Cisco Advanced Phishing Protection クラウドサービスの有効期限）
MAIL.APP.SERVICE_ UNAVAILABLE	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスの更新。（Cisco Advanced Phishing Protection Cloud Service update.）クラウドサービスとの通信を確立できません。（Unable to establish communication with the cloud service.） 説明：10 回連続してメールを APP に転送できなかったため、APP クラウドサービスを利用できません。	該当なし
MAIL.APP.SERVICE_ AVAILABLE	アラートテキスト：Cisco Advanced Phishing Protection クラウドサービスの更新。（Cisco Advanced Phishing Protection Cloud Service update.）クラウドサービスとの通信が確立されました。（Communication with the cloud service has been established.） 説明：APP クラウドサービスは利用可能です。	該当なし

アップデータ アラート

次の表に、AsyncOS で生成される可能性があるさまざまなアップデータ アラートのリストを示します。

表 *102* : 発生する可能性があるアップデータ アラートのリスト

アラート名	メッセージと説明	パラメータ
UPDATER.APP.UPDATE_ABANDONED	$app abandoning updates until a new version is published. The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage 警告。アプリケーションはアップデートを中止しています。	「**app**」：アプリケーション名。 「**attempts**」：試行した回数。
UPDATER.UPDATERD.ANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least $threshold. 警告。サーバのマニフェストの取得に失敗しました。	「**threshold**」：人間が読み取れるしきい値の文字列。
UPDATER.UPDATERD.RELEASE_NOTIFICATION	$mail_text 警告。リリースの通知です。	「**mail_text**」：通知するテキスト。 「**notification_subject**」：通知するテキスト。
UPDATER.UPDATERD.UPDATE_FAILED	Unknown error occured: $traceback クリティカル。アップデートの実行に失敗しました。	「**traceback**」：トレースバック。

アウトブレイク フィルタ アラート

次の表は、AsyncOS で生成されるさまざまなアウトブレイク フィルタ アラートのリストです。アラートの説明と重大度が記載されています。アウトブレイク フィルタは、隔離（具体的にはアウトブレイク隔離）で使用されるシステム アラートでも参照される場合があることに注意してください。

表 *103* : 発生する可能性があるアウトブレイク フィルタ アラートのリスト

アラート名	メッセージと説明	パラメータ
VOF.GTL_THRESHOLD_ALERT	Outbreak Filters Rule Update Alert:$text All rules last updated at: $time on $date. 情報。アウトブレイク フィルタのしきい値が変更された場合に送信されます。	「**text**」：アップデート アラートのテキスト。 「**time**」：最終アップデートの時刻。 「**date**」：最終アップデートの日付。

アラート名	メッセージと説明	パラメータ
AS.UPDATE_FAILURE	$engine update unsuccessful. This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com. The specific error on the email gateway for this failure is: $error	「**engine**」：アップデートに失敗したエンジン。 「**error**」：発生したエラー。
	警告。アンチスパム エンジンまたはCASE ルールのアップデートに失敗した場合に送信されます。	

クラスタリング アラート

次の表は、AsyncOS で生成されるさまざまなクラスタリング アラートのリストです。アラートの説明と重大度が記載されています。

表 *104 :* 発生する可能性があるクラスタリング アラートのリスト

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.AUTH_ERROR	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Machine does not appear to be in the cluster	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	クリティカル。認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Existing connection dropped	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	警告。クラスタへの接続がドロップされた場合に送信されます。	
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Connection failure	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	警告。クラスタへの接続に失敗した場合に送信されます。	
CLUSTER.CC_ERROR.FORWARD_FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Message forward failed, no upstream connection	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
	クリティカル。電子メールゲートウェイがクラスタのマシンにデータを転送できなかった場合に送信されます。	

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=No route found クリティカル。マシンがクラスタの別のマシンへのルートを取得できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Invalid host key クリティカル。無効な SSH ホスト キーがあった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Operation timed out 警告。指定された操作がタイムアウトした場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**ip**」：リモート ホストの IP。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine $name - $error - $why クリティカル。電子メールゲートウェイがクラスタの別のマシンの有効なIPアドレスを取得できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	Error connecting to cluster machine $name - $error - whyerror:=Machine does not appear to be in the cluster クリティカル。クラスタのマシンに接続する際に認証エラーが発生した場合に送信されます。マシンがクラスタのメンバでない場合に起きる可能性があります。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.DROPPED	Error connecting to cluster machine $name - $error - whyerror:=Existing connection dropped 警告。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、クラスタへの接続がドロップした場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。

アラート名	メッセージと説明	パラメータ
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine $name - $error - whyerror:=Connection failure 警告。不明な接続エラーが発生し、マシンがクラスタの別のマシンの有効なIPアドレスを取得できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	Error connecting to cluster machine $name - $error - whyerror:=Message forward failed, no upstream connection クリティカル。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、電子メールゲートウェイがマシンにデータを転送できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found クリティカル。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、別のマシンへのルートを取得できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.SSH_KEY	Error connecting to cluster machine $name - $error - whyerror:=Invalid host key クリティカル。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、有効な SSH ホスト キーを取得できなかった場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.CC_ERROR_NOIP.TIMEOUT	Error connecting to cluster machine $name - $error - whyerror:=Operation timed out 警告。マシンがクラスタの別のマシンの有効なIPアドレスを取得できず、指定された操作がタイムアウトした場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**why**」：エラーに関する詳細なテキスト。
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name クリティカル。設定データが同期から外れ、リモートホストに送信された場合に送信されます。	「**name**」：マシンのホスト名およびシリアル番号（またはいずれか）。 「**sections**」：送信中のクラスタ セクションのリスト。

ネットワーク設定値の変更

このセクションでは、電子メールゲートウェイのネットワーク操作の設定に使用する機能について説明します。これらの機能では、システム セットアップ ウィザードの使用 （35 ページ）でシステム セットアップ ウィザード（または **systemsetup** コマンド）を利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- **sethostname**
- DNS 設定（GUI および **dnsconfig** コマンドを利用）
- ルーティング設定（GUI、**routeconfig** コマンドおよび **setgateway** コマンドを利用）
- **dnsflush**
- パスフレーズ（Passphrase）
- ネットワーク アクセス
- ログイン バナー

システム ホスト名の変更

システムの識別には、ホスト名が使用されます。完全修飾ホスト名を入力する必要があります。ホスト名を変更するには：

- Web インターフェイスで、[ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] をクリックし、[管理（Management）] をクリックして [ホスト名（Hostname）] でホスト名を変更します。
- CLI で sethostname コマンドを使用します。

（注） 変更を確定するまで、新しいホスト名は有効になりません。

ドメイン ネーム システム（DNS）設定値の構成

GUI の [ネットワーク（Network）] メニューの [DNS] ページまたは dnsconfig コマンドで、 電子メールゲートウェイの DNS 設定値を設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバを利用するか、および使用する具体的なサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数
- DNS キャッシュのクリア

DNS サーバの指定

AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、またはインターネットのルート DNS サーバおよび指定した権威 DNS サーバを使用できます。インターネットのルートサーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、当該ドメインに対する権威サーバ（最終的な DNS レコードを提供）である必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット DNS」を設定する場合は、in-addr.arpa（PTR）エントリも同様に設定する必要があります。このため、たとえば「.eng」クエリーをネームサーバ 1.2.3.4 にリダイレクトする際に、すべての .eng エントリが 172.16 ネットワークにある場合、スプリット DNS 設定に「eng,16.172.in-addr.arpa」を指定する必要があります。

複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリーを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。システムは最初のクエリの有効期限が切れるか「タイムアウト」するまで短時間待機し、その後次のクエリに対しては前回よりも少し長い時間待機します。その後も同様です。待機時間は、DNS サーバの正確な合計数と設定されているプライオリティに依存します。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 *105 : DNS* サーバ、プライオリティ、およびタイムアウト間隔の例

プライオリティ	サーバ	タイムアウト（秒）
0	1.2.3.4、1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバが 1 つダウンしている場合、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ（1.2.3.6）が使用され、最終的にプライオリティ 2（1.2.3.7）のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

インターネット ルート サーバの使用

AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。

（注） デフォルト DNS サーバにインターネット ルート サーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリを再帰的に解決できる必要があります。

逆引き DNS ルックアップのタイムアウト

電子メールゲートウェイは電子メールの送受信の際、リスナーに接続しているすべてのリモートホストに対して「二重 DNS ルックアップ」の実行を試みます。（二重 DNS ルックアップを実行することで、システムはリモートホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS（PTR）ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS（A）ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しないか、A レコードが存在しない場合ログファイルには、一致する受信者がドロ、システムはホスト アクセス テーブル（HAT）内のエントリと一致する IP アドレスのみを使用します）。この特別なタイムアウト時間はこのルックアップにのみ適用され、複数エントリとプライオリティ（1304 ページ）で説明されている一般的な DNS タイムアウトには適用されません。

各 DNS サーバのデフォルト値は 20 秒です。DNS サーバに複数のエントリが存在する場合、合計タイムアウト値は（DNS サーバの数 x 逆引き DNS ルックアップのタイムアウトの値）秒です。たとえば、DNS サーバの数が 8 で、逆引き DNS ルックアップのタイムアウトの値が 20 秒の場合、合計タイムアウト値は（8 x 20）= 160 秒です。

秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトを無効にできます。値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。また、受信ホストの証明書にホストの IP ルックアップにマッピングされた一般名（CN）がある場合、TLS 認証接続を求めるドメインに電子メールゲートウェイがメールを送信するのを防止します。

DNS アラート

電子メールゲートウェイの再起動時に、まれにメッセージ「DNS キャッシュのブートストラップに失敗しました（Failed to bootstrap the DNS cache）」が付与されたアラートが生成される場合があります。メッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

DNS キャッシュのクリア

GUI の [キャッシュを消去（Clear Cache）] ボタン、または dnsflush コマンドを使用して、DNS キャッシュのすべての情報をクリアします（dnsflush コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください）。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

グラフィカル ユーザー インターフェイスを使用した DNS 設定値の設定

手順

ステップ 1 [ネットワーク（Network）] > **[DNS]** を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 インターネットのルート DNS サーバまたはユーザ独自の DNS サーバを使用するか、またはインターネットのルート DNS サーバを使用して代替 DNS サーバを指定するかを選択します。

ステップ 4 ユーザ独自の DNS サーバを使用する場合は、サーバ ID を入力し [行を追加（Add Row）] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、DNS サーバの指定 （1304 ページ）を参照してください。

ステップ 5 あるドメインに対して代替 DNS サーバを指定する場合は、ドメインと代替 DNS サーバの IP アドレスを入力します。[行を追加（Add Row）] をクリックし、ドメインを追加します。

（注） ドメイン名をカンマで区切ることで、1 つの DNS サーバに対して複数のドメインを入力できます。IP アドレスをカンマで区切ることで、複数の DNS サーバを入力することもできます。

ステップ 6 DNS トラフィック用のインターフェイスを選択します。

ステップ 7 逆引き DNS ルックアップを中止するまでに待機する秒数を入力します。

ステップ 8 [キャッシュをクリア（Clear Cache）] をクリックして、DNS キャッシュをクリアすることもできます。

ステップ 9 変更を送信し、保存します。

TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。

電子メールゲートウェイはインターネット プロトコル バージョン 4（IPv4）およびインターネット プロトコル バージョン 6（IPv6）の両方のスタティックルートを使用します。

スタティック ルートは CLI で routeconfig コマンドを使用して管理するか、または次の手順に従います。

手順

ステップ 1 [ネットワーク（Network）] > [ルーティング（Routing）] を選択します。

ステップ 2 作成するスタティック ルートのタイプ（IPv4 または IPv6）のために、[ルートを追加（Add Route）] をクリックします。

ステップ 3 ルートの名前を入力します。

ステップ 4 宛先 IP アドレスを入力します。

ステップ 5 ゲートウェイの IP アドレスを入力します。

ステップ 6 変更を送信し、保存します。

デフォルト ゲートウェイの設定

デフォルト ゲートウェイを設定するには、CLI で setgateway コマンドを使用するか、または次の手順に従います。

手順

ステップ 1 [ネットワーク（Network）] > [ルーティング（Routing）] を選択します。

ステップ 2 変更するインターネット プロトコル バージョンのために、ルート リストで [デフォルトルート（Default Route）] をクリックします。

ステップ 3 ゲートウェイの IP アドレスを変更します。

ステップ 4 変更を送信し、保存します。

SSL 設定の指定

[SSL構成時の設定（SSL Configuration Settings）] ページまたは sslconfig コマンドを使用して、電子メールゲートウェイの SSL 設定を構成できます。

手順

ステップ 1 [システム管理（System Administration）] > [SSL 構成時の設定（SSL Configuration Settings）] をクリックします。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

重要 下位の AsyncOS バージョン（12.0 や 12.1 など）からアップグレードした場合、デフォルトの SSL 暗号は AsyncOS 14.x 以降で次のように変更されます。

- **GUI HTTPS の場合**：

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA
```

- **インバウンド SMTP の場合**：

```
AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:
!aNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA
```

- **アウトバウンド SMTP の場合**：

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:
!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:!kRSA:@STRENGTH:-aNULL:-EXPORT
:-IDEA:!DHE-RSA-AES256-SHA
```

ステップ 3 要件に応じて、次を実行します。

- GUI HTTPS SSL を設定します。[GUI HTTPS] で、使用する SSL 方式と暗号方式を指定します。
- 受信 SMTP SSL を設定します。[受信SMTP（Inbound SMTP）] で、使用する SSL 方式と暗号化方式を指定します。
- 送信 SMTP SSL を設定します。[送信SMTP（Outbound SMTP）] で、使用する SSL 方式と暗号化方式を指定します。
- その他の TLS クライアントサービスを設定します。電子メールゲートウェイが非 FIPS モードの場合、[その他のTLSクライアントサービス（Other TLS Client Services）] では、TLS v1.0 方式がデフォルトで無効になります。「LDAP」および「Updater」の TLS クライアントサービスに対しては、電子メールゲートウェイで TLS v1.0 方式を有効にできます。

次の点を考慮してください。

- （非 FIPS モードの場合）TLS v1.0 方式と v1.1 方式を同時には有効にできません。ただし、これらの方式は TLS v1.2 方式と共に有効にできます。
- 非 FIPS モードで TLS v1.0 が有効になっている下位の AsyncOS バージョン（例：12.x または 13.0）から AsyncOS 13.5.1 以降にアップグレードすると、TLS v1.0 がデフォルトで無効になります。アップグレード後に電子メールゲートウェイで TLS v1.0 方式を有効にする必要があります。
- AsyncOS 13.5.1 以降では、SSLv2 および SSLv3 方式はサポートされません。

- 電子メールゲートウェイが FIPS モードの場合、TLS v1.0 方式はサポートされません。
- 電子メールゲートウェイが非 FIPS モードの場合、TLS v1.0 方式はデフォルトで無効になります。

ステップ 4 （オプション）[TLSを介したアラート（Alerts over TLS）]、[アウトバウンドSMTP（Outbound SMTP）]、[アップデータ（Updater）]、および [LDAP] サーバサービスについて、電子メールゲートウェイがピア証明書でFQDN検証を実行できるようにするには、[有効にする（Enable）] チェックボックスをオンにします。

ステップ 5 （オプション）[TLSを介したアラート（Alerts over TLS）]、[アウトバウンドSMTP（Outbound SMTP）]、[アップデータ（Updater）]、および [LDAP] サーバサービスについて、電子メールゲートウェイがピア証明書でX.509検証を実行できるようにするには、[有効にする（Enable）] チェックボックスをオンにします。

ステップ 6 **[送信（Submit）]** をクリックします。

ステップ 7 [変更を確定（Commit Changes）] をクリックします。

SAML 2.0 を使用したシングル サインオン（SSO）

- シングル サインオン（SSO）と SAML 2.0 について （1309 ページ）
- SAML 2.0 SSO のワークフロー （1309 ページ）
- SAML 2.0 に関する注意事項と制約事項 （1310 ページ）
- 電子メールゲートウェイでの SSO の設定方法 （1311 ページ）

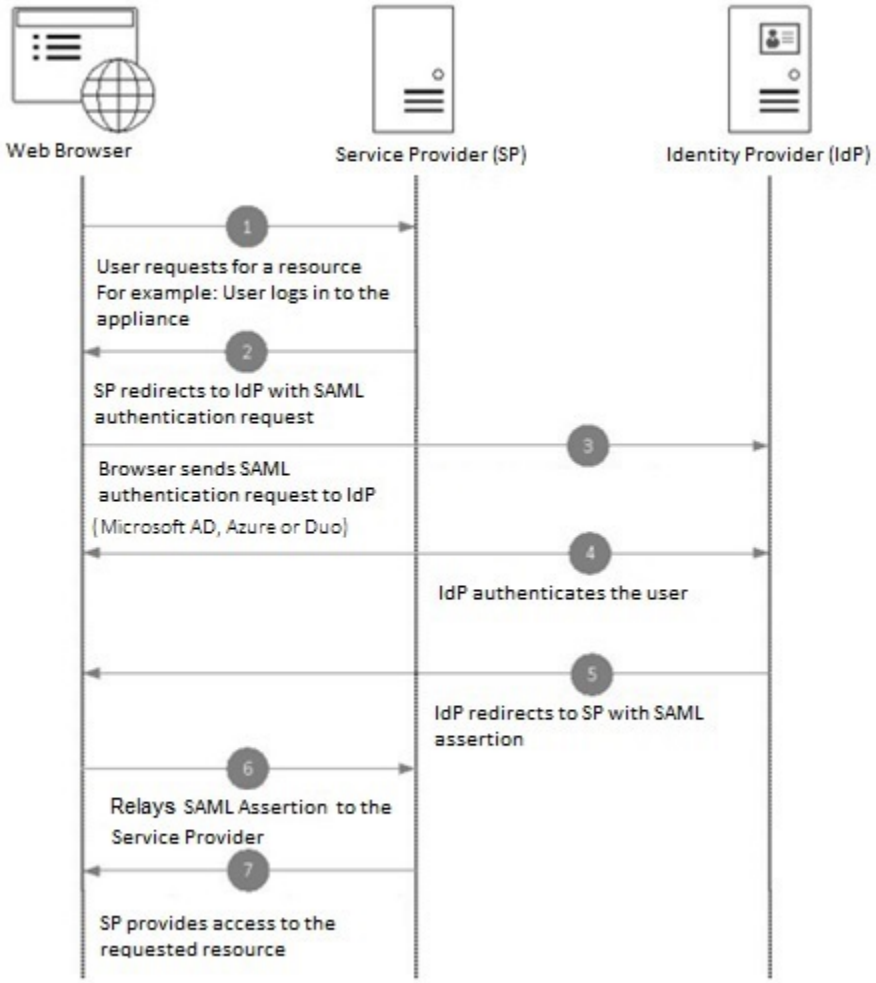
シングル サインオン（SSO）と SAML 2.0 について

電子メールゲートウェイは SAML 2.0 SSO をサポートするようになりました。これにより、管理ユーザは組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用している同じクレデンシャルで電子メールゲートウェイのWebインターフェイスにログインできます。たとえば、SAML IDプロバイダー（IdP）としてDuo、Microsoft AD FS、またはAzureを有効にした場合、SAML 2.0 SSO をサポートするサービスプロバイダー（SP）として電子メールゲートウェイを設定できます。ユーザは一度サインインすれば、すべての SAML 2.0 SSO 対応サービスにアクセスできます。

SAML 2.0 SSO のワークフロー

SAML 2.0 SSO ワークフローを、次の図に表示します。

図 *75 : SAML* のワークフロー



SAML 2.0 に関する注意事項と制約事項

- 一般 （1310 ページ）
- ログアウト （1311 ページ）
- 制限事項 （1311 ページ）

一般

SAML によるシングルサインオンは、グラフィカル ユーザー インターフェイス（GUI）でのみ使用できます。SAML プロファイルの設定には、GUI とコマンド ライン インターフェイス（CLI）を使用できます。

電子メールゲートウェイでは、サービスプロバイダーと ID プロバイダーのインスタンスを 1 つのみ設定できます。

ログアウト

ユーザは電子メールゲートウェイからログアウトしても、他の SAML 2.0 SSO 対応アプリケーションからログアウトされることはありません。

制限事項

クラスタ レベルで SAML プロファイルを設定することはできません。すべての SAML 設定は、マシン レベルに制限されます。

電子メールゲートウェイでの SSO の設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	前提条件を確認します。	前提条件 （1311 ページ）
ステップ 2	電子メールゲートウェイをサービスプロバイダーとして設定します。	電子メールゲートウェイをサービスプロバイダーとして設定する （1312ページ）
ステップ 3	（IDP で） 電子メールゲートウェイを操作するように ID プロバイダーを設定します。	電子メールゲートウェイと通信するようにIDプロバイダーを設定する （1315ページ）
ステップ 4	電子メールゲートウェイで ID プロバイダーを設定します。	電子メールゲートウェイでの ID プロバイダーの設定 （1319 ページ）
ステップ 5	電子メールゲートウェイで SAML を使用した外部認証を有効にします。	SAML 認証の有効化 （1214 ページ）

前提条件

- サポートされるアイデンティティ プロバイダー （1311 ページ）
- セキュアな通信の証明書 （1312 ページ）

サポートされるアイデンティティ プロバイダー

組織で使用する ID プロバイダーが 電子メールゲートウェイでサポートされているかどうかを確認します。事前認定済みの ID プロバイダーは次のとおりです。

- Microsoft Active Directory Federation Services（AD FS）2.0 以降
- Duo Access Gateway

- Azure AD

（注） 任意の標準 SAML 2.0 ID プロバイダーを使用して、E メールゲートウェイで SAML を使用して SSO を設定できます。

セキュアな通信の証明書

電子メールゲートウェイと ID プロバイダーの間の通信をセキュリティで保護するために必要な次の証明書を取得します。

- 電子メールゲートウェイで SAML 認証要求に署名する、または ID プロバイダーで SAML アサーションを暗号化する場合、自己署名証明書または信頼できる CA の証明書、および関連付けられている秘密キーを取得します。
- ID プロバイダーで SAML アサーションに署名する場合は、ID プロバイダーの証明書を取得して 電子メールゲートウェイにインポートします。 電子メールゲートウェイはこの証明書を使用して、署名済み SAML アサーションを確認します。

証明書の変換

電子メールゲートウェイから証明書を作成およびエクスポートするには、証明書の使用 （830 ページ）を参照してください。通常、 電子メールゲートウェイから取得した証明書は .pfx 形式であり、 電子メールゲートウェイをサービスプロバイダーとして設定するときには .pem 形式に変換する必要があります。

証明書を .pfx 形式から .pem 形式に変換するには、次の操作を行います。

- OpenSSL ツールをダウンロードしてインストールし、 電子メールゲートウェイから取得した証明書ファイル（.pfx）をインポートします。
- 次のコマンドを実行して、証明書を .pem 形式でエクスポートします。`openssl pkcs12 -in <certname>.pfx -nokeys -out cert.pem`
- 次のコマンドを実行して、秘密キーを .pem 形式でエクスポートします。`openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
- 次のコマンドを実行して、秘密キーからパスフレーズを削除します。`openssl rsa -in key.pem -out server.key`

電子メールゲートウェイをサービスプロバイダーとして設定する

（注） ID プロバイダーでのサービスプロバイダーの設定値は、 電子メールゲートウェイでのサービスプロバイダー設定に基づいて設定されます。

始める前に

前提条件 （1311 ページ）を確認してください。

手順

ステップ 1 Web インターフェイスを使用して 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [SAML] に移動します。

ステップ 3 [サービスプロバイダーの追加（Add Service Provider）] をクリックします。

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	サービス プロバイダー プロファイルの名前を入力します。
コンフィギュレーション設定	
エンティティ ID	サービスプロバイダー（この場合、ご使用の電子メールゲートウェイ）のグローバルな固有の名前を入力します。通常、サービス プロバイダー エンティティ ID の形式は URI です。
名前 ID の形式	ID プロバイダーが SAML アサーションでユーザを指定するのに使用する形式。 このフィールドは設定できません。IDプロバイダーでサービスプロバイダーを設定するときに、この値が必要になります。
アサーション コンシューマ URL	認証が正常に完了した後で、ID プロバイダーが SAML アサーションを送信する URL を入力します。 アサーションコンシューマ URL は、 電子メールゲートウェイへのアクセスに使用される URL です。ID プロバイダーでサービス プロバイダーを設定するときに、この値が必要になります。

フィールド	説明
SP 証明書	サービスプロバイダーの証明書は、次のいずれかの方法でインポートできます。 • 電子メールゲートウェイで使用可能な署名付き証明書をドロップダウンリストから選択します。 • 証明書をインポートして秘密キーと関連付けます。証明書は（.cert）形式にし、秘密キーは（.key）形式にする必要があります。 • PKCS #12 ファイル形式で証明書をインポートします。PKCS # 12 形式の証明書ではパスワードが必須です。 （任意）認証要求の署名（Signing Authentication Requests） アプライアンスで SAML 認証要求に署名する場合、 1. 電子メールゲートウェイから取得された証明書と、関連付けられている秘密キーをアップロードします。 証明書は **.cert** 形式でアップロードする必要があります。詳細については、セキュアな通信の証明書（1312 ページ）を参照してください。 2. 秘密キーのパスフレーズを入力します。 3. [署名要求（Sign Requests）] を選択します。 （任意）**暗号化されたアサーションの復号（Decrypt Encrypted Assertions）** SAML アサーションを暗号化するように ID プロバイダーを設定する場合、 1. 電子メールゲートウェイから取得された証明書と、関連付けられている秘密キーをアップロードします。 2. 秘密キーのパスフレーズを入力します。 （注） 秘密キーは **.key** 形式である必要があります。証明書の使用方法については、セキュアな通信の証明書（1312 ページ）を参照してください。

フィールド	説明
署名アサーション	SAML アサーションに署名するように ID プロバイダーを設定する場合、[署名アサーション（Sign Assertions）] を選択します。 このオプションを選択すると、 電子メールゲートウェイに ID プロバイダーの証明書を追加する必要があります。 電子メールゲートウェイでの ID プロバイダーの設定 （1319 ページ）を参照してください。
組織詳細	組織の詳細を入力します。ID プロバイダーは、エラー ログでこの情報を使用します。
技術的な問い合わせ先	技術的な問い合わせ先の電子メール アドレスを入力します。ID プロバイダーは、エラー ログでこの情報を使用します。

ステップ 5 [送信（Submit）] をクリックし、変更をコミットします。

ステップ 6 [SSOの設定（SSO Settings）] ページに表示されるサービス プロバイダーのメタデータ（エンティティ ID とアサーション顧客 URL）と、[サービスプロバイダー設定（Service Provider Settings）] ページに表示される名前 ID の形式を書き留めます。ID プロバイダーでサービス プロバイダーを設定するときに、これらの詳細が必要になります。

必要に応じて、メタデータをファイルとしてエクスポートできます。設定が完了したら、[メタデータのエクスポート（Export Metadata）] をクリックしてメタデータ ファイルを保存します。一部の ID プロバイダーでは、メタデータ ファイルからサービス プロバイダーの詳細をロードできます。

次のタスク

電子メールゲートウェイと通信するように ID プロバイダーを設定します。 電子メールゲートウェイと通信するように ID プロバイダーを設定する （1315 ページ） を参照してください。

電子メールゲートウェイと通信するように ID プロバイダーを設定する

始める前に

次の内容について確認してください。

- 電子メールゲートウェイをサービスプロバイダーとして設定します。 電子メールゲートウェイをサービスプロバイダーとして設定する （1312 ページ）を参照してください。
- サービスプロバイダーのメタデータの詳細がコピーされているか、またはメタデータ ファイルがエクスポートされている。 電子メールゲートウェイをサービスプロバイダーとして設定する （1312 ページ）を参照してください。

手順

ステップ 1 ID プロバイダーで、次のいずれかを実行します。

- サービスプロバイダー（お使いの電子メールゲートウェイ）の詳細を手動で構成します。
- ID プロバイダーがメタデータ ファイルからサービス プロバイダーの詳細をロードすることを許可している場合は、メタデータ ファイルをインポートします。

電子メールゲートウェイが SAML 認証要求に署名するように構成済みの場合、または SAML アサーションを暗号化する予定の場合は、必ず関連する証明書を ID プロバイダーに追加します。

ID プロバイダー固有の手順については、以下を参照してください。

- 電子メールゲートウェイと通信するように AD FS を設定する （1316 ページ）。
- 電子メールゲートウェイと通信するように Duo Access Gateway を設定する （1317 ページ）。
- 電子メールゲートウェイと通信するように Azure AD を設定する （1318 ページ）。

ステップ 2 ID プロバイダーのメタデータを書き留めるかまたはメタデータをファイルとしてエクスポートします。

次のタスク

電子メールゲートウェイ上で ID プロバイダーの設定を構成します。 電子メールゲートウェイでの ID プロバイダーの設定 （1319 ページ） を参照してください。

電子メールゲートウェイと通信するように AD FS を設定する

以下は、お使いの 電子メールゲートウェイと通信するように AD FS（2.0 以降）を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、Microsoft のマニュアルを参照してください。

- リレーパーティとしてサービスプロバイダー（電子メールゲートウェイ）のアサーション コンシューマ URL を追加します。
- [リレーパーティトラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [ID（Identifiers）] > [リレーパーティID（Relaying Party Identifier）] で、サービスプロバイダー（電子メールゲートウェイ）のエンティティ ID を入力します。この値が、 電子メールゲートウェイのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を構成済みの場合は、サービス プロバイダーの証明書（認証要求を署名するために使用される）を [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [署名（Signature）] の下で .cer 形式でアップロードします。

- 暗号化された SAML アサーションを送信するように AD FS を構成する場合は、サービスプロバイダー（電子メールゲートウェイ）の証明書を[リレーパーティトラスト（Relaying Party Trusts）]>[プロパティ（Properties）]>[暗号化（Encryption）]の下で .cer 形式でアップロードします。
- [リレー パーティ トラスト（Relaying Party Trusts）]>[プロパティ（Properties）]>[詳細（Advanced）]の下で、セキュアハッシュ アルゴリズムを SHA-1 に設定します。
- 応答に SPNameQualifier を含めるためのカスタム ルールを追加します。次のファイルは、サンプルのカスタム ルールです。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>

issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer=
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

- 要求ルールを編集し、電子メール アドレスの LDAP 属性を発信要求タイプ（電子メールアドレス）として送信する発行変換規則を追加します。また、発行変換規則を追加して、グループ属性の LDAP 属性を送信要求タイプ（未指定のグループ）として送信するようにします。

電子メールゲートウェイと通信するように Duo Access Gateway を設定する

以下は、お使いの 電子メールゲートウェイと通信するように Duo Access Gateway を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、Duo Security のマニュアルを参照してください。

- SAMLアサーションを受信および処理するサービスプロバイダーエンドポイントとして、サービスプロバイダーの（ 電子メールゲートウェイの）アサーションコンシューマ URL を追加します。
- [Duo管理パネル（Duo Admin Panel）]>[アプリケーション（Applications）]>[アプリケーションの保護（Protect an Application）]>[SAMLサービスプロバイダー（SAML Service Provider）]で、サービスプロバイダー（ 電子メールゲートウェイ）のエンティティ ID を入力します。この値が、電子メールゲートウェイのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービスプロバイダー（ 電子メールゲートウェイ）を構成済みの場合は、Duo Access Gateway に認証ソースを設定する際に、サービスプロバイダーの証明書（認証要求を署名するために使用される）を .cer 形式でアップロードします。
- 暗号化された SAML アサーションを送信するように Duo を構成する計画の場合は、Duo Access Gateway に認証ソースを設定する際に、サービスプロバイダーの（電子メールゲートウェイの）証明書を .cer 形式でアップロードします。

- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、NameID 形式として [未指定（unspecified）] を選択します。
- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、セキュア ハッシュ アルゴリズムを SHA-256 に設定します。
- [Duo管理パネル（Duo Admin Panel）] で [SAML-サービスプロバイダー設定（SAML - Service Provider Setting）] を設定ファイルとして保存し、Duo Access Gateway でその設定ファイルを SAML アプリケーションとしてインポートします。

電子メールゲートウェイと通信するように Azure AD を設定する

以下は、お使いの 電子メールゲートウェイと通信するように Azure AD を実行する必要があるタスクの概要です。完全かつ詳細な手順については、Microsoft Azure AD のマニュアルを参照してください。

- SAML アサーションを受信および処理するサービスプロバイダー識別子として、サービスプロバイダーの（ 電子メールゲートウェイの）アサーションコンシューマ URL を追加します。
- [エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [基本SAML設定（Basic SAML Configuration）] にある Azure ポータルにサービスプロバイダーの（電子メールゲートウェイの）エンティティ ID を入力します。この値が、 電子メールゲートウェイのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービスプロバイダー（ 電子メールゲートウェイ）を構成済みの場合は、[SAML署名証明書（SAML Signing Certificate section）] セクション（[エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [SAML署名証明書（SAML Signing Certificate）]）で、サービスプロバイダーの証明書（認証要求を署名するために使用される）をアップロードします。
- [ユーザ属性とクレーム（User Attributes and Claims）] セクション（[エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [ユーザ属性とクレーム（User Attributes and Claims）]）でグループクレームを設定し、グループ属性を追加します。
- [SAML] > [ユーザとグループ（Users & Groups）] のために作成された Azure アプリケーションでユーザまたはグループを追加して、この Azure SAML アプリケーションにログインできるユーザを制御します。

電子メールゲートウェイでの ID プロバイダーの設定

始める前に

次の内容について確認してください。

- 電子メールゲートウェイとの通信のための ID プロバイダーが構成されている。 電子メールゲートウェイと通信するようにIDプロバイダーを設定する（1315ページ）を参照してください。
- ID プロバイダーのメタデータの詳細がコピーされている、または ID プロバイダーのメタデータがファイルとしてエクスポートされている。

手順

ステップ 1 Web インターフェイスで 電子メールゲートウェイにログインします。

ステップ 2 [システム管理（System Administration）] > [SAML] に移動します。

ステップ 3 [IDプロバイダーの追加（Add Identity Provider）] をクリックします

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	ID プロバイダー プロファイルの名前を入力します。
構成設定（ID プロバイダー設定の手動構成）	
エンティティ ID	ID プロバイダーのグローバルに一意の名前を入力します。通常、ID プロバイダー エンティティ ID の形式は URI です。
SSO URL	サービス プロバイダーが SAML 認証要求を送信する必要がある URL を指定します。
証明書	ID プロバイダーが SAML アサーションに署名する場合、ID プロバイダーの署名証明書をアップロードする必要があります。
構成設定（ID プロバイダー メタデータのインポート）	
IDP メタデータのインポート	[メタデータのインポート（Import Metadata）] をクリックして、メタデータ ファイルを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

SAML 認証の有効化 （1214 ページ）。

AsyncOS API 向けの電子メールゲートウェイでの OpenID Connect 1.0 の設定

- 概要 （1320 ページ）
- ワークフロー （1320 ページ）
- サンプルアクセストークン （1321 ページ）
- 前提条件 （1321 ページ）
- 電子メールゲートウェイでの OpenID Connect の設定 （1321 ページ）

概要

Cisco Secure Email Gateway は、OpenID Connect 1.0 認証で ID プロバイダー（IDP）を使用するアプリケーションまたはクライアントとの統合をサポートし、電子メールゲートウェイで使用可能な AsyncOS API とシームレスに接続します。現在、お使いの E メールゲートウェイは、Microsoft AD FS のみを使用して OpenID Connectで認定されています。

ワークフロー

次のワークフローでは、AD FS を ID プロバイダー、外部アプリケーションをクライアント、電子メールゲートウェイをリソースプロバイダーとして使用しています。

手順：

1. （1 回限りのアクティビティ）アクセストークンを検証するように電子メールゲートウェイを設定します。詳細については、電子メールゲートウェイでの OpenID Connect の設定（1321 ページ）を参照してください。
2. （1 回限りのアクティビティ）電子メールゲートウェイは、OpenID Connect の設定メタデータと必要なキーを取得して、ステップ 1 で行った設定に基づいてアクセストークンを検証します。
3. AD FS で外部アプリケーションを認証した後、アクセストークンを取得します。アクセストークンを認証および受信する方法の詳細については、認証プロバイダーまたは ID プロバイダーのマニュアルを参照してください。
4. API 要求をアクセストークンとともに電子メールゲートウェイに送信します。
5. 電子メールゲートウェイは、ステップ 2 で取得したキーセットを使用して API 要求のアクセストークンを検証します。
6. 電子メールゲートウェイは、アクセストークン内の必要な要求（発行者、対象者）を検証します。

7. 電子メールゲートウェイは、ロール要求値を使用して、AsyncOS API にアクセスするためのユーザロール権限を許可し、割り当てます。
8. 電子メールゲートウェイは、AsyncOS API 要求に適切な応答を提供します。

サンプルアクセストークン

次に、サンプルアクセストークンの形式を示します。

```
Header
alg:RSA256
typ:JWT
[...]
Payload
claim: aud: CiscoEmailAPICaller
claim: iss: http://adfsserver/adfs/services/trust
claim: iat: 1594712147
claim: exp: 1594712807
claim: CustomOrgIdentifier: MyCustomOrgId
claim: LastName: Fernandes
claim: FirstName: Erik
claim: Email: erik.fernandes@customorg.com
claim: Role: LogCollector
claim: Role: ReadOnly
[...]
```

電子メールゲートウェイは、次のアルゴリズムによってのみ署名されたアクセストークンの検証をサポートします。

- RSA256
- RSA384
- RSA512

前提条件

OpenID Connect で電子メールゲートウェイを設定する前に、次の前提条件を満たしていることを確認します。

- 組織で使用される認証プロバイダーは電子メールゲートウェイでサポートされている。
- アプリケーションは認証プロバイダーで認証し、アクセストークンを取得できる。
- 電子メールゲートウェイは、HTTP 経由で認証プロバイダーに接続して、OpenID Connect メタデータ設定を取得できる。

電子メールゲートウェイでの OpenID Connect の設定

始める前に

次の情報について確認してください。

- （認証プロバイダーの設定に基づいて）認証プロバイダーによって発行された有効なアクセストークン。
- アクセストークンには、電子メールゲートウェイが必要な許可チェックを実行できるようにするためのロール情報が含まれている必要があります。

手順

ステップ 1 [システム管理（System Administration）] > [OpenID Connect] をクリックします。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 以下の表に記載される必須パラメータを入力して、OpenID Connect を設定します。

OpenID Connect パラメータ	説明
[IDプロバイダーのメタデータのURL（Identity Provider Metadata URL）]	Open ID Connect の設定メタデータを取得するために使用する ID プロバイダーの URL を入力します。メタデータは、アクセストークンの検証に使用されます。 ID プロバイダーの URL は、https://example.com/adfs/.well-known/openid-configuration のようになります。
発行元（Issuer）	アクセストークンの発行者の値を入力します。 （注） この値は、アクセストークンの検証時にアクセストークンの発行者要求値と一致する必要があります。 発行者は http://example.com/adfs/services/trust のようになります。
対象読者	アクセストークンの対象者要求値と一致する必要がある対象者の値を入力します。 （注） 複数の対象者値を追加する場合は、[行を追加（Add Row）] をクリックします。
[要求名（Claim Name）]	ユーザロール情報を含むアクセストークンの要求の名前を入力します。要求名は、アクセストークンからロール情報を取得するために使用されます。

OpenID Connect パラメータ	説明
ID プロバイダーとアプライアンスロールのマッピング	ID プロバイダーサーバで定義されたユーザグループロールを入力し、電子メールゲートウェイで設定された対応するローカルユーザロールを選択して、両方のロールをマッピングします。 （注） 複数のロールマッピングレコードを追加する場合は、[行を追加（Add Row）] をクリックします。

ステップ 4 変更を送信し、保存します。

次のタスク

AsyncOS API コールの Authorization Bearer ヘッダーにアクセストークンを含め、API 要求を送信します。

次に、API の Authorization Bearer ヘッダーにアクセストークンを含めた AsynOS API を呼び出す例を示します。

```
curl --location --request
GET 'https://esa.com/esa/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'

--header 'Authorization: Bearer <add access_token here>’
```

システム タイム

電子メールゲートウェイのシステム時刻の設定、使用する時間帯の設定、または NTP サーバとクエリーインターフェイスの選択を行うには、GUI の [システム管理（System Administration）] メニューから [タイムゾーン（Time Zone）] ページまたは [時刻設定（Time Settings）] ページを使用するか、CLI の ntpconfig コマンド、settime コマンドおよび settz コマンドを使用します。

AsyncOS で使用される時間帯ファイルは、[システム管理（System Administration）] > [時刻設定（Time Settings）] ページ、または tzupdate CLI コマンドで確認することもできます。

タイム ゾーンの選択

[タイムゾーン（Time Zone）] ページ（GUI の [システム管理（System Administration）] メニューから利用可能）では、電子メールゲートウェイの時間帯を表示します。特定の時間帯または GMT オフセットを選択できます。

手順

ステップ 1 [システム管理（System Administration）] > [タイム ゾーン（Time Zone）] ページで、[設定を編集（Edit Settings）] をクリックします。

ステップ 2 地域、国、および時間帯をプルダウン メニューから選択します。

ステップ 3 変更を送信し、保存します。

GMT オフセットの選択

手順

ステップ 1 [システム管理（System Administration）] > [タイム ゾーン（Time Zone）] ページで、[設定を編集（Edit Settings）] をクリックします。

ステップ 2 地域のリストから [GMT オフセット（GMT Offset）] を選択します。

ステップ 3 [タイム ゾーン（Time Zone）] リストでオフセットを選択します。オフセットとは、GMT（グリニッジ子午線）に達するために足し引きする必要がある時間のことです。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の東側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の西側にあたります。

ステップ 4 変更を送信し、保存します。

時刻設定の編集

次の方法の 1 つを使用して、電子メールゲートウェイの時間設定を編集できます。

- （推奨）Network Time Protocol（NTP）を使用した電子メールゲートウェイのシステム時刻の設定 （1324 ページ）
- 電子メールゲートウェイのシステム時刻の手動設定 （1325 ページ）

（推奨）Network Time Protocol（NTP）を使用した電子メールゲートウェイのシステム時刻の設定

これは、特に電子メールゲートウェイが他のデバイスに統合されている場合に推奨される、時刻の設定方法です。統合されたデバイスはすべて、同じの NTP サーバを使用する必要があります。

手順

ステップ 1 [システム管理（System Administration）] > [時刻設定（Time Settings）] ページに移動します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 [時刻の設定方法（Time Keeping Method）] セクションで、[NTP（Network Time Protocol）を使用（Use Network Time Protocol）] を選択します。

ステップ 4 NTP サーバのアドレスを入力し、[行を追加（Add Row）] をクリックします。複数の NTP サーバを追加できます。

ステップ 5 NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。

ステップ 6 NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。

ステップ 7 変更を送信し、保存します。

電子メールゲートウェイのシステム時刻の手動設定

通常、この時刻の設定方法は推奨されません。代わりにネットワーク タイム プロトコル サーバを使用します。

手順

ステップ 1 [システム管理（System Administration）] > [時刻設定（Time Settings）] ページに移動します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 [時刻の設定方法（Time Keeping Method）] セクションで、[時刻を手動で設定（Set Time Manually）] を選択します。

ステップ 4 月、日、年、時、分、および秒を入力します。

ステップ 5 [A.M.] または [P.M.] を選択します。

ステップ 6 変更を送信し、保存します。

ビューのカスタマイズ

• お気に入りページの使用 （1325 ページ）
• ユーザ設定値の設定 （1326 ページ）

お気に入りページの使用

（ローカル認証された管理ユーザ限定）よく利用するページのクイック アクセス リストを作成できます。

目的	操作手順
お気に入りリストにページを追加する	追加するページに移動し、ウィンドウの右上隅付近にある [お気に入り（My Favorites）] メニューから [このページをお気に入りに追加（Add This Page To My Favorites）] を選択します。 お気に入りへの変更では確定操作は必要ありません。
お気に入りの順序を変更する	[お気に入り（My Favorites）]>[お気に入りをすべて表示（View All My Favorites）] を選択し、適切な順序にお気に入りをドラッグします。
お気に入りを削除する	[お気に入り（My Favorites）]>[お気に入りをすべて表示（View All My Favorites）] を選択し、お気に入りを削除します。
お気に入りページに移動する	ウィンドウの右上隅付近にある [お気に入り（My Favorites）] からページを選択します。
カスタム レポート ページを表示または作成する	[マイ ダッシュボード（My Dashboard）] ページ （1014 ページ） を参照してください。

ユーザ設定値の設定

ローカルユーザは、各アカウントに固有な言語などのプリファレンス設定を定義できます。これらの設定は、ユーザが電子メールゲートウェイに最初にログインするときにデフォルトで適用されます。各ユーザにプリファレンス設定が保存され、ユーザが電子メールゲートウェイにログインするクライアントマシンに関係なく同じです。

ユーザがこれらの設定を変更し、変更をコミットしないと、再びログインするときに設定がデフォルト値に戻ります。

（注） この機能は、外部認証されたユーザは使用できません。これらのユーザは、[オプション（Options）] メニューから直接言語を選択できます。

手順

ステップ 1 プリファレンス設定を定義するユーザ アカウントでアプライアンスにログインします。

ステップ 2 [オプション（Options）]> [環境設定（Preferences）] を選択します。[オプション（Options）] メニューは、ウィンドウの上部右側にあります。

ステップ 3 [設定を編集（Edit Preferences）] をクリックします。

ステップ 4 設定を行います。

プリファレンス設定	説明
言語の表示（Language Display）	Web インターフェイスおよび CLI で使用する言語の Web 用 AsyncOS。
ランディング ページ（Landing Page）	ユーザが電子メールゲートウェイにログインするときに表示されるページ。
表示されるレポート時間範囲（Reporting Time Range Displayed）（デフォルト）	[レポート（Reporting）] タブでレポートに対して表示するデフォルトの時間範囲。
表示するレポート行の数（Number of Reporting Rows Displayed）	デフォルトで各レポートに表示されるデータの行数。

ステップ 5 変更を送信し、保存します。

ステップ 6 ページ下部の [前のページに戻る（Return to previous page）] リンクをクリックします。

全般設定

電子メールゲートウェイの次の一般設定を編集できます。

- Internet Explorer の互換モードの上書き （1327 ページ）
- 新しい Web インターフェイスを使用した電子メールゲートウェイの使用状況統計の収集（1328 ページ）

Internet Explorer の互換モードの上書き

優れた Web インターフェイスのレンダリングのために、Internet Explorer 互換モードのオーバーライドを有効にすることを推奨します。

（注） この機能を有効にすることが組織のポリシーに違反する場合は、この機能を無効にすることができます。

手順

ステップ 1 [システム管理（System Administration）] > [一般設定（General Settings）] をクリックします。

ステップ 2 [IE 互換モードの上書き（Override IE Compatibility Mode）] チェックボックスをオンにします。

ステップ 3 変更を送信し、保存します。

新しいWebインターフェイスを使用した電子メールゲートウェイの使用状況統計の収集

[使用状況分析（Usage Analytics）] は、分析統計情報のためにサイトアクティビティデータへのインサイトを得るために使用します。[使用状況分析（Usage Analytics）] が有効になっている場合、電子メールゲートウェイは新しい Web インターフェイスで電子メールゲートウェイの機能の使用状況データを収集します。使用状況の統計情報は、分析して、電子メールゲートウェイのユーザエクスペリエンスを向上させるためのインサイトを得るために使用します。

デフォルトで、使用状況の分析機能は電子メールゲートウェイで有効になっています。使用状況の分析機能を無効にするには、次の手順を実行します。

手順

ステップ 1 [システム管理（System Administration）] > [一般設定（General Settings）] をクリックします。
ステップ 2 [使用状況分析（Usage Analytics）] チェックボックスをオフにします。
ステップ 3 変更を送信し、保存します。

最大 HTTP ヘッダー サイズの構成

電子メールゲートウェイに送信される HTTP 要求の HTTP ヘッダーの最大サイズを設定するため、CLI で `adminaccessconfig > maxhttpheaderfieldsize` コマンドを使用できるようになりました。

HTTP ヘッダー フィールドのサイズの既定値は 4096（4 KB）、最大値は 33554432（32 MB）です。

サービス エンジンの再起動とステータスの表示

CLI で `diagnostic > services` サブコマンドを使用して、以下を実行できます。

- 電子メールゲートウェイで有効になっているサービスエンジンを再起動します。電子メールゲートウェイを再起動する必要はありません。
- 電子メールゲートウェイで有効になっているサービスエンジンのステータスを表示します。

詳細については、Cisco Secure Email Gateway の『CLI リファレンスガイド』を参照してください。

国際化ドメイン名（IDN）を含むメッセージの受信と配信

電子メールゲートウェイは、IDN ドメインを含む電子メールアドレスを持つメッセージを受信および配信できます。

現在、電子メールゲートウェイは次の言語の IDN ドメインのみをサポートしています。

インドの地域言語：ヒンディー語、タミル語、テルグ語、カンナダ語、マラーティ語、パンジャブ語、マラヤラム語、ベンガル語、グジャラート語、ウルドゥー語、アッサム語、ネパール語、バングラ語、ボド語、ドグリ語、カシミール語、コンカニ語、マイティリ語、マニプリ語、オリヤ語、サンスクリット語、サンタル語、シンド語、トゥル語。

ヨーロッパおよびアジアの言語：フランス語、ロシア語、日本語、ドイツ語、ウクライナ語、韓国語、スペイン語、イタリア語、中国語、オランダ語、タイ語、アラビア語、カザフ語。

関連トピック：

- 前提条件 （1329 ページ）
- 電子メールゲートウェイで IDN ドメインを使用して設定可能な機能 （1330 ページ）

前提条件

国際化ドメイン名（IDN）機能を使用する前に、次の前提条件を満たしていることを確認してください。

- すべての着信メッセージには UTF-8 でエンコードされた IDN が必要です。

  たとえば、電子メールゲートウェイにメッセージを送信する MTA は IDN をサポートし、メッセージ内のドメインが UTF-8 形式であることを確認する必要があります。

- すべての発信メッセージには UTF-8 でエンコードされた IDN が必要であり、宛先サーバはそれに応じて IDN を受け入れ、サポートする必要があります。

  たとえば、電子メールゲートウェイからのメッセージを受け入れる MTA は UTF-8 形式でエンコードされた IDN とドメインをサポートする必要があります。

- 該当するすべての DNS レコードで、Punycode 形式を使用して IDN を設定する必要があります。

  たとえば、IDN に MX レコードを設定する場合、DNS レコードのドメインは Punycode 形式である必要があります。

電子メールゲートウェイで IDN ドメインを使用して設定可能な機能

このリリースでは、電子メールゲートウェイ内で IDN ドメインを使用して設定できるのは次の機能**のみ**です。

- **SMTP ルートの設定**：
  - IDN ドメインを追加または編集します。
  - IDN ドメインを使用して SMTP ルートをエクスポートまたはインポートします。
- **DNS の設定**：IDN ドメインを使用して DNS サーバを追加または編集します。
- **リスナーの設定**：
  - インバウンドリスナーまたはアウトバウンドリスナーのデフォルトドメインの IDN ドメインを追加または編集します。
  - HAT テーブルまたは RAT テーブルで IDN ドメインを追加または編集します。
  - IDN ドメインを使用して HAT テーブルまたは RAT テーブルをエクスポートまたはインポートします。
- **メールポリシーの設定**
  - [着信メールポリシー（Incoming Mail Policies）] の送信者（[送信者を追跡する（Following Senders）] オプションまたは [送信者を追跡しない（Following Senders are）] オプション）と受信者（[受信者を追跡する（Following Recipients）]または[受信者を受信しない（Recipients are not）]オプション）の IDN ドメインを使用してドメインを追加または編集します。
  - [発信メールポリシー（Outgoing Mail Policies）] の送信者（[送信者を追跡する（Following Senders）] オプションまたは [送信者を追跡しない（Following Senders are）] オプション）と受信者（[受信者を追跡する（Following Recipients）]または[受信者を受信しない（Recipients are not）]オプション）の IDN ドメインを使用してドメインを追加または編集します。
  - [着信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] で IDN ドメインを使用した送信者または受信者を検索します。
  - IDN ドメインを使用して送信者判定の例外を定義します。
  - IDN ドメインを使用してアドレスリストを作成します。
  - 宛先の制御に IDN ドメインを使用して宛先ドメインを追加または編集します。
- **バウンスプロファイルの設定**：IDN ドメインを使用して代替電子メールアドレスを追加または編集します。
- **送信者ドメインレピュテーションの設定**：IDN ドメインの送信者ドメイン レピュテーション スコアを定義します。

- **IP レピュテーションの設定**：IDN ドメインの IP レピュテーションスコアを定義します。
- **LDAP の設定**：IDN ドメインを使用して、LDAP グループクエリを作成し、クエリを受け入れ、クエリをルーティングし、クエリをマスカレードします。
- **レポートの設定**：IDNデータ（ユーザ名、電子メールアドレス、ドメイン）をレポートに表示します。
- **メッセージトラッキングの設定**：メッセージトラッキングに IDN データ（ユーザ名、電子メールアドレス、およびドメイン）を表示します。
- **ポリシー、ウイルス、およびアウトブレイク隔離の設定**：
  - ウイルス対策エンジンによる判定に従って、マルウェアを送信する可能性のある IDN ドメインを含むメッセージを表示します。
  - スパムまたはマルウェアの可能性があるとアウトブレイクフィルタによって検出された IDN ドメインを含むメッセージを表示します。
  - メッセージフィルタ、コンテンツフィルタ、およびDLPメッセージアクションによって検出された IDN ドメインを含むメッセージを表示します。
- **スパムの隔離の設定**：
  - スパム、または疑いのあるスパムとして検出されたIDNドメインを含むメッセージを表示します。
  - IDNドメインを含む電子メールアドレスをセーフリストとブロックリストのカテゴリに追加します。

（注） 現在、IDN ドメインを持つ受信者は、[スパムの管理（Spam Quarantine）] 設定ページの [エンドユーザの隔離アクセス（End-User Quarantine Access] セクションでエンドユーザ認証方式が [なし（None）] に設定されている場合にのみ、エンドユーザの隔離にアクセスできます。

- [SPF構成設定（SPF Configuration Settings）]：IDN ドメインを使用してメッセージの SPF 検証を実行します。
- [DKIM構成設定（DKIM Configuration Settings）]：IDN ドメインを使用して DKIM 署名とメッセージの検証を実行します
- [DMARC構成設定（DMARC Configuration Settings）]：IDNドメインを使用してメッセージの DMARC 検証を実行します。

第 40 章

CLI による管理およびモニタリング

この章は、次の項で構成されています。

- CLI を使用した管理およびモニタリングの概要 （1333 ページ）
- 使用可能なモニタリング コンポーネントの読み取り （1334 ページ）
- CLI を使用したモニタリング （1340 ページ）
- 電子メール キューの管理 （1351 ページ）
- SNMP を使用したシステムの状態のモニタリング （1361 ページ）

CLI を使用した管理およびモニタリングの概要

CLI を使用した電子メールゲートウェイの管理およびモニタリングには次のようなタスクがあります。

- メッセージ アクティビティのモニタリング。
  - 電子メールゲートウェイが電子メールパイプラインで処理している未処理メッセージ、受信者、バウンス受信者の数
  - 最後の 1 分、5 分、または 15 分の間隔に基づくメッセージ配信またはバウンス メッセージの時間レート
- システム リソースのモニタリング。次に、例を示します。
  - メモリ使用量
  - ディスク容量
  - 接続数
- 簡易ネットワーク管理プロトコル（SNMP）を使用する、システムの機能障害のモニタリング。次に、例を示します。
  - ファン障害
  - 更新の失敗
  - 異常に高い電子メールゲートウェイの温度
- パイプライン内の電子メールの管理。次に、例を示します。

- キュー内の受信者の削除
- 別のホストへのメッセージのリダイレクト
- 受信者の削除またはメッセージのリダイレクトによるキューのクリア
- 電子メールの受信、送信、またはワーク キュー処理の一時停止または再開
- 特定のメッセージの検索

使用可能なモニタリング コンポーネントの読み取り

- イベント カウンタの読み取り （1334 ページ）
- システム ゲージの読み取り （1336 ページ）
- 配信およびバウンスされたメッセージのレートの読み取り （1339 ページ）

イベント カウンタの読み取り

カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。

カウンタは、イベントが発生するごとに増加し、次の 3 つのバージョンで表示されます。

リセット	**resetcounters コマンドによる最後のカウンタ リセット以降**
Uptime	最後のシステム再起動以降
保存期間（Lifetime）	電子メールゲートウェイの存続期間中の合計

次の表に、電子メールゲートウェイをモニタするときに使用できるカウンタとその説明を示します。

（注） これは、全体的なリストです。表示されるカウンタは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 *106* : カウンタ

統計	説明
Receiving	
Messages Received	配信キューに受信されたメッセージ。
Recipients Received	受信されたすべてのメッセージの受信者。

統計	説明
Generated Bounce Recipients	システムによってバウンスが生成され、配信キューに挿入された対象の受信者。
Rejection 拒否した受信者	受信者アクセス テーブル（RAT）によって、または早期接続終了などの予期しないプロトコル ネゴシエーションによって配信キューへの受信を拒否された受信者。
ドロップされたメッセージ	フィルタ ドロップ アクションの一致によって配信キューへの受信を拒否されたメッセージ、またはシンクホール キューイング リスナーによって受信されたメッセージ。エイリアス テーブル内の /dev/null エントリ宛てのメッセージは、ドロップされたメッセージと見なされます。アンチスパム フィルタリング（システムでイネーブルになっている場合）によってドロップされたメッセージも、このカウンタに計上されます。
キュー（Queue） ソフトバウンスしたイベント数	ソフトバウンス イベントの数。複数回ソフトバウンスしたメッセージには、複数のソフトバウンス イベントが設定されます。
Completion 完了した受信者	ハード バウンスされた受信者、配信された受信者、および削除された受信者の総合計。配信キューから削除されたすべての受信者。
ハード バウンスされた受信者	DNS ハード バウンス、5XX ハード バウンス、フィルタ ハードバウンス、期限切れハードバウンス、およびその他のハードバウンスの総合計。受信者へのメッセージの配信に失敗し、配信がただちに終了となったものを表します。
DNS ハード バウンス	受信者へのメッセージの配信試行中に検出された DNS エラー。
5XX ハード バウンス	受信者へのメッセージの配信試行中に、宛先メールサーバから「5XX」応答コードが返されたものを表します。
期限切れハード バウンス	配信キューに許容されている最大時間、または最大接続試行回数を超えているメッセージ受信者。

統計	説明
フィルタ ハード バウンス	一致フィルタの bounce アクションによってプリエンプトされた受信者の配信。アンチスパム フィルタリング（システムでイネーブルになっている場合）によってドロップされたメッセージも、このカウンタに計上されます。
その他のハード バウンス	メッセージ配信中の予期しないエラー。または、メッセージ受信者が bouncerecipients コマンドによって明示的にバウンスされたものを表します。
配信された受信者	メッセージが正常に配信された受信者。
削除された受信者	deleterecipients コマンドによって明示的に削除されたメッセージ受信者、またはグローバル配信停止リストに合致するメッセージ受信者の合計。
Global Unsubscribe Hits	グローバル配信停止設定との一致により削除されたメッセージ受信者。
現在の ID	配信キューに挿入されたメッセージに割り当てられた最後のメッセージID。MIDは、電子メールゲートウェイによって受信されたすべてのメッセージに関連付けられており、メールログで追跡できます。MIDは、231でゼロにリセットされます。
Message ID（MID）	
Injection Connection ID (ICID)	リスナー インターフェイスへの接続に割り当てられた最後のインジェクション接続ID。ICIDは231でロールオーバー（ゼロにリセット）されます。
Delivery Connection ID (DCID)	宛先メール サーバへの接続に割り当てられた最後の配信接続 ID。DCID は 231 でロール オーバー（ゼロにリセット）されます。

システム ゲージの読み取り

ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

次の表に、電子メールゲートウェイをモニタするときに使用できるゲージとその説明を示します。

（注） これは、全体的なリストです。表示されるゲージは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 *107 :* ゲージ

統計	説明
System Gauges	
RAM Utilization	システムによる物理 Random Access Memory（RAM; ランダム アクセス メモリ）の使用率。
CPU Utilization	CPU の使用状況のパーセンテージ。
Disk I/O Utilization	ディスク I/O の使用率。 （注） Disk I/O Utilization ゲージには、既知の値の測定は表示されません。このゲージには、これまでにシステムで確認され、最後の再起動以降の最大値に対して測定された I/O 使用率が表示されます。したがって、ゲージに 100 % と表示されている場合、システムでは起動後最も高いレベルの I/O 使用率が発生しています（必ずしも、システム全体の 100 % の物理ディスク I/O を表すものではありません）。
Resource Conservation	0 ～ 60 または 999 の値。0 ～ 60 の数値は、重要なシステム リソースの急速な消耗を防止するために、システムがメッセージの受け入れを減らしている度合いを表しています。数値が大きいほど、受け入れを減らす度合いが大きくなります。ゼロは、受け入れの減少がないことを示します。このゲージに 999 と表示されている場合、システムは「リソース節約モード」になっており、メッセージは受け入れられません。システムがリソース節約モードかどうかに関係なく、アラート メッセージは送信されます。
Disk Utilization: Logs	ログに使用されているディスクの割合。ステータス ログには LogUsd、XML ステータスには log_used として表示されます。
Connections Gauges	
現在のインバウンド接続	リスナー インターフェイスへの現在の着信接続。
現在のアウトバウンド接続	宛先メール サーバへの現在の発信接続。
Queue Gauges	

統計	説明
アクティブ受信者	配信キュー内のメッセージ受信者。Unattempted Recipients と Attempted Recipients の合計。
Unattempted Recipients	Active Recipients のサブカテゴリ。配信がまだ試行されていない、キュー内のメッセージ受信者。
Attempted Recipients	Active Recipients のサブカテゴリ。試行されたものの、ソフトバウンスイベントによって失敗した配信の対象となっている、キュー内のメッセージ受信者。
Messages in Work Queue	キューに入る前に、エイリアス テーブル拡張、マスカレード、アンチスパム、アンチウイルス スキャン、メッセージフィルタ、およびLDAPクエリーによる処理を待つメッセージの数。
Messages in Quarantine	隔離エリア内にあるメッセージに、解放または削除されたが実際の処理がまだ行われていないメッセージを足した一意の数。たとえば、Outbreakからすべての隔離対象メッセージを解放すると、Outbreak の合計メッセージ数はただちにゼロになりますが、このフィールドでは、完全に配信されるまでの隔離対象メッセージが反映されます。
Destinations in Memory	メモリ内の宛先ドメインの数。メッセージの配信先となる各ドメインに対して、宛先オブジェクトがメモリ内に作成されます。そのドメインに対するすべてのメールが配信された後、宛先オブジェクトは3時間保持されます。3時間のうちに、そのドメインに対して新しいメッセージがバインドされなければ、オブジェクトは期限切れとなり、宛先は（tophosts コマンドなどで）報告されなくなります。1 つのドメインにだけメールを配信している場合は、このカウンタが「1」になります。メッセージを送信したことがない（または、長い時間電子メールゲートウェイによってメッセージが処理されていない）場合、カウンタは「0」になります。 仮想ゲートウェイを使用している場合、各仮想ゲートウェイの宛先ドメインには別個の宛先オブジェクトが作成されます（たとえば、3 つの異なる仮想ゲートウェイから yahoo.com に配信している場合、yahoo.com が 3 つの宛先オブジェクトとしてカウントされます）。
Kilobytes Used	使用されるキュー ストレージ（キロバイト単位）。

統計	説明
Kilobytes in Quarantine	隔離対象メッセージに使用されるキュー ストレージ。メッセージ サイズと、上記の "Messages in Quarantine" にカウントされている受信者ごとに 30 バイトを足した値になります。この計算では通常、使用されるスペースが過大に見積もられます。
Kilobytes Free	残りのキュー ストレージ（キロバイト単位）。

配信およびバウンスされたメッセージのレートの読み取り

すべてのレートは、クエリーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。

たとえば、電子メールゲートウェイが 1 分間に 100 受信者を受信すると、1 分間隔に対するレートは、1 時間あたり 6,000 となります。5 分間隔に対するレートは 1 時間あたり 1,200 となり、15 分間隔に対するレートは 1 時間あたり 400 となります。レートは、1 分間のレートが継続した場合の 1 時間あたりの平均レートを示すように計算されます。したがって、1 分で 100 件のメッセージの方が 15 分で 100 件のメッセージよりもレートは高くなります。

次の表に、電子メールゲートウェイをモニタするときに使用できるレートとその説明を示します。

（注） これは、全体的なリストです。表示されるレートは、選択した表示オプションまたはコマンドによって異なります。このリストは参照用として使用してください。

表 *108 :* レート

統計	説明
Messages Received	1 時間あたりに配信キューに挿入されるメッセージのレート。
Recipients Received	1 時間あたりに配信キューに挿入されるすべてのメッセージに対する受信者数のレート。
Soft Bounced Events	1 時間あたりのソフト バウンス イベント数のレート（複数回ソフト バウンスしたメッセージには、複数のソフト バウンス イベントが設定されます）。
Completed Recipients	ハードバウンスされた受信者、配信された受信者、および削除された受信者の総合計のレート。配信キューから削除された受信者は、完了済みと見なされます。

統計	説明
Hard Bounced Recipients	1 時間あたりの DNS ハード バウンス、5XX ハード バウンス、フィルタ ハード バウンス、期限切れハード バウンス、およびその他のハード バウンスの総合計のレート。ハード バウンスとは、受信者へのメッセージの配信試行に失敗し、その配信がただちに終了されることをいいます。
Delivered Recipients	受信者に正常に配信された 1 時間あたりのメッセージ数のレート。

CLI を使用したモニタリング

- 電子メール ステータスのモニタリング （1340 ページ）
- 詳細な電子メール ステータスのモニタリング （1341 ページ）
- メール ホストのステータスのモニタリング （1343 ページ）
- 電子メール キューの構成の確認 （1346 ページ）
- リアルタイム アクティビティの表示 （1346 ページ）
- 着信電子メール接続のモニタリング （1348 ページ）
- DNS ステータスの確認 （1349 ページ）
- 電子メール モニタリング カウンタのリセット （1350 ページ）
- アクティブな TCP/IP サービスの識別 （1351 ページ）

電子メール ステータスのモニタリング

電子メールゲートウェイにおける電子メール動作のステータスをモニタすることが必要になることがあります。status コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返された統計情報は、カウンタとゲージのいずれかの形式で表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。

各項目の説明については、CLI を使用した管理およびモニタリングの概要（1333 ページ）を参照してください。

表 *109 :* メール ステータス

統計	説明
Status as of	現在のシステム日時を表示します。
Last counter reset	カウンタが最後にリセットされた時刻を表示します。

統計	説明
System status	online、offline、receiving suspended、または delivery suspended。ステータスが "receiving suspended" になるのは、すべてのリスナーが一時停止した場合のみです。すべてのリスナーに対する受信と配信が一時停止されると、ステータスは "offline" になります。
Oldest Message	システムによる配信を待つ、最も古いメッセージを表示します。
Features	featurekey コマンドによってシステムにインストールされた特別な機能を表示します。

例

```
mail3.example.com> status

Status as of:               Thu Oct 21 14:33:27 2004 PDT
Up since:                     Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:         Never
System status:              Online
Oldest Message:              4 weeks 46 mins 53 secs
Counters:                      Reset          Uptime        Lifetime
  Receiving
    Messages Received      62,049,822         290,920      62,049,822
    Recipients Received    62,049,823         290,920      62,049,823
  Rejection
    Rejected Recipients     3,949,663          11,921       3,949,663
    Dropped Messages       11,606,037             219      11,606,037
  Queue
    Soft Bounced Events     2,334,552          13,598       2,334,552
  Completion
    Completed Recipients   50,441,741         332,625      50,441,741
  Current IDs
    Message ID (MID)                                      99524480
    Injection Conn. ID (ICID)                             51180368
    Delivery Conn. ID (DCID)                              17550674
Gauges:                                 Current
  Connections
    Current Inbound Conn.                     0
    Current Outbound Conn.                   14
  Queue
    Active Recipients                     7,166
    Messages In Work Queue                    0
    Messages In Quarantine               16,248
    Kilobytes Used                      387,143
      Kilobytes In Quarantine           338,206
    Kilobytes Free                   39,458,745
mail3.example.com>
```

詳細な電子メール ステータスのモニタリング

status detail コマンドは、電子メール動作についてモニタされた詳細な情報を返します。返された統計情報は、カウンタ、レート、およびゲージのいずれかのカテゴリで表示されます。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベ

ントの合計数を表示できます。ゲージは、メモリ、ディスク スペース、またはアクティブ接続などのシステム リソースの現在の使用率を示します。すべてのレートは、クエリーが作成された特定の時点における、1 時間あたりの平均イベント発生レートを示します。レートには、過去 1 分間、5 分間、および 15 分間という 3 つの間隔で 1 時間あたりの平均レートが計算されます。各項目の説明については、CLI を使用した管理およびモニタリングの概要 （1333 ページ）を参照してください。

例

```
mail3.example.com> status detail
Status as of:           Thu Jun 30 13:09:18 2005 PDT
Up since:               Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)
Last counter reset:            Tue Jun 29 19:30:42 2004 PDT
System status:                 Online
Oldest Message:                No Messages
Feature - IronPort Anti-Spam:  17 days
Feature - Sophos:              Dormant/Perpetual
Feature - Outbreak Filters: Dormant/Perpetual
Feature - Central Mgmt:        Dormant/Perpetual
Counters:                       Reset          Uptime        Lifetime
  Receiving
    Messages Received       2,571,967          24,760       3,113,176
    Recipients Received     2,914,875          25,450       3,468,024
    Gen. Bounce Recipients      2,165               0           7,451
  Rejection
    Rejected Recipients     1,019,453             792       1,740,603
    Dropped Messages        1,209,001              66       1,209,028
  Queue
    Soft Bounced Events        11,236               0          11,405
  Completion
    Completed Recipients    2,591,740          49,095       3,145,002
      Hard Bounced Recipients   2,469               0           7,875
        DNS Hard Bounces          199               0           3,235
        5XX Hard Bounces        2,151               0           4,520
        Expired Hard Bounces      119               0             120
        Filter Hard Bounces         0               0               0
        Other Hard Bounces          0               0               0
      Delivered Recipients  2,589,270          49,095       3,137,126
      Deleted Recipients            1               0               1
        Global Unsub. Hits          0               0               0
    DomainKeys Signed Msgs         10               9              10
  Current IDs
    Message ID (MID)                                          7615199
    Injection Conn. ID (ICID)                                 3263654
    Delivery Conn. ID (DCID)                                  1988479
Rates (Events Per Hour):      1-Minute       5-Minutes      15-Minutes
  Receiving
    Messages Received             180             300             188
    Recipients Received           180             300             188
  Queue
    Soft Bounced Events             0               0               0
  Completion
    Completed Recipients          360             600             368
      Hard Bounced Recipients       0               0               0
      Delivered Recipients        360             600             368
Gauges:                              Current
  System
    RAM Utilization                      1%
    CPU Utilization
      MGA                                0%
```

```
    AntiSpam                              0%
    AntiVirus                             0%
  Disk I/O Utilization                    0%
  Resource Conservation                    0
Connections
  Current Inbound Conn.                    0
  Current Outbound Conn.                   0
Queue
  Active Recipients                        0
    Unattempted Recipients                 0
    Attempted Recipients                   0
  Messages In Work Queue                   0
  Messages In Quarantine                  19
  Destinations In Memory                   3
  Kilobytes Used                         473
    Kilobytes In Quarantine              473
  Kilobytes Free                39,845,415
```

（注） 新たにインストールされた電子メールゲートウェイでは、最も古いメッセージカウンタにメッセージが示される場合がありますが、実際にはカウンタに示される受信者はありません。リモート ホストが接続されており、メッセージの受信が非常に遅い（つまり、メッセージを受信するまでに数分かかる）場合には、受信された受信者カウンタに「0」と表示され、最も古いメッセージ カウンタに「1」と表示されることがあります。これは、最も古いメッセージ カウンタに処理中のメッセージが表示されるためです。接続が最終的にドロップされると、カウンタはリセットされます。

メール ホストのステータスのモニタリング

特定の受信者ホストへの配信に問題があると思われる場合や、仮想ゲートウェイ アドレスに関する情報を収集する場合には、hoststatus コマンドを実行するとそれらの情報を表示できます。hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。コマンドには、取得するホスト情報のドメインを入力する必要があります。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です。返される統計情報は、カウンタとゲージの 2 つのカテゴリに表示されます。各項目の説明については、CLI を使用した管理およびモニタリングの概要 （1333 ページ）を参照してください。

また、hoststatus コマンドに固有のその他のデータも返されます。

表 *110 : hoststatus* コマンドのその他のデータ

統計	説明
Pending Outbound Connections	開いている接続や作業中の接続とは対照的な、宛先メール ホストへの保留中、または「初期」接続。Pending Outbound Connections は、プロトコルのグリーティングの段階にまだ達していない接続です。

統計	説明
Oldest Message	このドメインに対する配信キュー内で最も古いアクティブ受信者の経過時間。このカウンタは、ソフトバウンスイベントやホストの停止によって配信できない、キュー内のメッセージの経過時間を判断するのに役立ちます。
Last Activity	このフィールドは、そのホストにメッセージ配信が試みられるたびに更新されます。
Ordered IP Addresses	このフィールドには、IP アドレスの Time To Live（TTL; 存続可能時間）、MX レコードに応じた IP アドレスの優先順位、および実際のアドレスが表示されます。MX レコードは、ドメインに対するメールサーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。
Last 5XX error	このフィールドには、ホストから返された最新の 5XX ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。
MX Records	MX レコードは、ドメインに対するメール サーバの IP アドレスを指定します。1 つのドメインが複数の MX レコードを持つことができます。各 MX レコードのメール サーバには優先順位が割り当てられます。優先順位の数値が最も小さい MX レコードが優先されます。
SMTP Routes for this host	このドメインに対して SMTP ルートが定義されている場合は、ここに表示されます。
Last TLS Error	このフィールドには、最新の発信 TLS 接続エラーの説明と、電子メールゲートウェイが確立を試みた TLS 接続のタイプが表示されます。このフィールドが表示されるのは、TLS エラーが存在する場合のみです。

仮想ゲートウェイ

次の仮想ゲートウェイ情報は、仮想ゲートウェイアドレスを設定している場合のみ表示されます（電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください）。

表 *111 : hoststatus* コマンドのその他の仮想ゲートウェイ データ

統計	説明
Host up/down	同じ名前のグローバル hoststatus フィールドと同じ定義。Virtual Gateway アドレスごとに追跡されます。
最後のアクティビティ（Last Activity）	同じ名前のグローバル hoststatus フィールドと同じ定義。Virtual Gateway アドレスごとに追跡されます。

統計	説明
Recipients	このフィールドも、グローバル hoststatus コマンドの定義に対応します。Active Recipients フィールド：仮想ゲートウェイ アドレスごとに追跡されます。
Last 5XX error	このフィールドには、ホストから返された最新の 5XX ステータス コードと説明が表示されます。このフィールドが表示されるのは、5XX エラーが存在する場合のみです。

例

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com
Host mail status for: 'aol.com'
Status as of:          Tue Mar 02 15:17:32 2010
Host up/down:          up
Counters:
  Queue
    Soft Bounced Events                         0
  Completion
    Completed Recipients                        1
      Hard Bounced Recipients                   1
        DNS Hard Bounces                        0
        5XX Hard Bounces                        1
        Filter Hard Bounces                     0
        Expired Hard Bounces                    0
        Other Hard Bounces                      0
      Delivered Recipients                      0
      Deleted Recipients                        0
Gauges:
  Queue
    Active Recipients                           0
      Unattempted Recipients                    0
      Attempted Recipients                      0
    Connections
      Current Outbound Connections              0
      Pending Outbound Connections              0
Oldest Message         No Messages
Last Activity          Tue Mar 02 15:17:32 2010
Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)
    Preference   IPs
    15           64.12.137.121    64.12.138.89     64.12.138.120
    15           64.12.137.89     64.12.138.152    152.163.224.122
    15           64.12.137.184    64.12.137.89     64.12.136.57
    15           64.12.138.57     64.12.136.153    205.188.156.122
    15           64.12.138.57     64.12.137.152    64.12.136.89
    15           64.12.138.89     205.188.156.154  64.12.138.152
    15           64.12.136.121    152.163.224.26   64.12.137.184
    15           64.12.138.120    64.12.137.152    64.12.137.121
MX Records:
    Preference   TTL        Hostname
    15           52m24s     mailin-01.mx.aol.com
    15           52m24s     mailin-02.mx.aol.com
    15           52m24s     mailin-03.mx.aol.com
    15           52m24s     mailin-04.mx.aol.com
    Last 5XX Error:
```

```
    ----------
    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
 (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
    ----------
Last TLS Error:             Required - Verify
    ----------
    TLS required, STARTTLS unavailable
    (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
Virtual gateway information:
===============================================================
example.com (PublicNet_017):
    Host up/down:         up
    Last Activity         Wed June 22 13:47:02 2005
    Recipients            0
```

（注） 仮想ゲートウェイ アドレス情報は、altsrchost機能を使用している場合のみ表示されます。

電子メール キューの構成の確認

電子メールキューに関する現在の情報を取得し、特定の受信者ホストに配信の問題（キューの増大など）があるかどうかを判断するには、tophosts コマンドを使用します。tophosts コマンドは、キュー内の上位 20 の受信者のリストを返します。リストは、アクティブ受信者、発信接続、配信済み受信者、ソフト バウンス イベント、およびハード バウンスされた受信者など、さまざまな統計情報別にソートできます。CLI を使用した管理およびモニタリングの概要 （1333 ページ）を参照してください。

例

```
mail3.example.com> tophosts

Sort results by:
1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
5. Hard Bounced Recipients
[1]> 1
Status as of:         Mon Nov 18 22:22:23 2003
                    Active     Conn.    Deliv.    Soft      Hard
#  Recipient Host   Recip      Out      Recip.    Bounced   Bounced
1  aol.com          365        10       255       21         8
2  hotmail.com      290         7       198       28        13
3  yahoo.com        134         6       123       11        19
4  excite.com        98         3        84        9         4
5  msn.com           84         2        76       33        29
mail3.example.com>
```

リアルタイム アクティビティの表示

電子メールゲートウェイではリアルタイムモニタリングが可能であり、システムにおける電子メールアクティビティの進捗状況を確認できます。rate コマンドは、電子メール動作に関する

リアルタイムモニタリング情報を返します。この情報は、ユーザが指定した間隔で定期的に更新されます。**rate** コマンドを停止するには、Ctrl+C を使用します。

次の表に、表示されるデータを示します。

表 *112 : rate* コマンドのデータ

統計	説明
Connections In	着信接続の数。
Connections Out	発信接続の数。
Recipients Received	システムに受信された受信者の合計数。
Recipients Completed	完了した受信者の合計数。
Delta	最後のデータ アップデート以降変化した、Received 受信者数および Completed 受信者数の差異。
Queue Used	メッセージ キューのサイズ（キロバイト単位）。

例

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1
Hit Ctrl-C to return to the main prompt.
Time     Connections Recipients          Recipients               Queue
             In    Out   Received    Delta  Completed    Delta     K-Used
23:37:13     10      2   41708833        0   40842686        0         64
23:37:14      8      2   41708841        8   40842692        6        105
23:37:15      9      2   41708848        7   40842700        8         76
23:37:16      7      3   41708852        4   40842705        5         64
23:37:17      5      3   41708858        6   40842711        6         64
23:37:18      9      3   41708871       13   40842722       11         67
23:37:19      7      3   41708881       10   40842734       12         64
23:37:21     11      3   41708893       12   40842744       10         79
^C
```

hostrate コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。この情報は、status detail コマンドのサブセットです（詳細な電子メール ステータスのモニタリング （1341 ページ） を参照。）

表 *113 : hostrate* コマンドのデータ

統計	説明
Host Status	特定のホストの現在のステータス（up、down、または unknown）。
Current Connections Out	ホストに対する現在の発信接続数。

統計	説明
Active Recipients in Queue	キュー内の特定のホストに対するアクティブ受信者の合計数。
Active Recipients in Queue Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するアクティブ受信者の合計数の差異。
Delivered Recipients Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対する配信済み受信者の合計数の差異。
Hard Bounced Recipients Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するハード バウンスされた受信者の合計数の差異。
Soft Bounce Events Delta	最後の既知のホスト ステータス以降変化した、キュー内の特定のホストに対するソフト バウンスされた受信者の合計数の差異。

hostrate コマンドを停止するには、Ctrl+C を使用します。

例

```
mail3.example.com> hostrate
Recipient host:
[]> aol.com
Enter the number of seconds between displays.
[10]> 1
    Time   Host  CrtCncOut  ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt
           Status                      Delta   Delta     Delta     Delta
23:38:23       up          1         0       0       4         0         0
23:38:24       up          1         0       0       4         0         0
23:38:25       up          1         0       0      12         0         0
^C
```

着信電子メール接続のモニタリング

大量の送信者を識別するため、またはシステムへの着信接続をトラブルシューティングするために、電子メールゲートウェイに接続しているホストのモニタが必要になる場合があります。topin コマンドは、システムに接続しているリモート ホストのスナップショットを示します。このスナップショットには、特定のリスナーに接続しているリモート IP アドレスごとに 1 つの行を持つテーブルが表示されます。同じ IP アドレスから異なるリスナーへの 2 つの接続は、topin コマンドを使用して表示されるフィールドについて説明する、次の表の 2 行になります。

表 *114 : topin* コマンドのデータ

統計	説明
Remote Hostname	リモート ホストのホスト名。リバース DNS ルックアップによって取得されます。

統計	説明
Remote IP Address	リモート ホストの IP アドレス。
listener	接続を受信している、電子メールゲートウェイ上のリスナーのニックネーム。
Connections In	コマンドが実行されたときに開いていた、指定のIPアドレスを持つリモート ホストからの同時接続数。

システムは、リバースDNSルックアップによってリモートホスト名を検索してから、フォワードDNSルックアップによってその名前を検証します。フォワードルックアップで元のIPアドレスにならない場合、またはリバース DNS ルックアップに失敗した場合、テーブルのホスト名カラムにはIPアドレスが表示されます。送信者検証プロセスの詳細については、送信者の検証 （137 ページ）を参照してください。

例

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003
#  Remote hostname             Remote IP addr.   listener        Conn. In
1  mail.remotedomain01.com     172.16.0.2        Incoming01            10
2  mail.remotedomain01.com     172.16.0.2        Incoming02            10
3  mail.remotedomain03.com     172.16.0.4        Incoming01             5
4  mail.remotedomain04.com     172.16.0.5        Incoming02             4
5  mail.remotedomain05.com     172.16.0.6        Incoming01             3
6  mail.remotedomain06.com     172.16.0.7        Incoming02             3
7  mail.remotedomain07.com     172.16.0.8        Incoming01             3
8  mail.remotedomain08.com     172.16.0.9        Incoming01             3
9  mail.remotedomain09.com     172.16.0.10       Incoming01             3
10 mail.remotedomain10.com     172.16.0.11       Incoming01             2
11 mail.remotedomain11.com     172.16.0.12       Incoming01             2
12 mail.remotedomain12.com     172.16.0.13       Incoming02             2
13 mail.remotedomain13.com     172.16.0.14       Incoming01             2
14 mail.remotedomain14.com     172.16.0.15       Incoming01             2
15 mail.remotedomain15.com     172.16.0.16       Incoming01             2
16 mail.remotedomain16.com     172.16.0.17       Incoming01             2
17 mail.remotedomain17.com     172.16.0.18       Incoming01             1
18 mail.remotedomain18.com     172.16.0.19       Incoming02             1
19 mail.remotedomain19.com     172.16.0.20       Incoming01             1
20 mail.remotedomain20.com     172.16.0.21       Incoming01             1
```

DNS ステータスの確認

dnsstatus コマンドは、DNSルックアップおよびキャッシュ情報の統計を表示するカウンタを返します。カウンタごとに、そのカウンタの最後のリセット以降、最後のシステム再起動以降、およびシステムの存続期間中に発生したイベントの合計数を表示できます。

次の表に、使用可能なカウンタを示します。

表 *115 : dnsstatus* コマンドのデータ

統計	説明
DNS 要求	ドメイン名を解決するためのシステム DNS キャッシュに対する上位レベルの非反復要求。
ネットワーク要求	DNS情報を取得するためのネットワーク（非ローカル）への要求。
Cache Hits	レコードが検出されて返された、DNS キャッシュへの要求。
Cache Misses	レコードが検出されなかった、DNS キャッシュへの要求。
Cache Exceptions	レコードが検出されたものの、ドメインが不明である、DNSキャッシュへの要求。
Cache Expired	レコードが検出された、DNS キャッシュへの要求。 キャッシュでは、使用状況が考慮され、古すぎるレコードは破棄されます。 Time To Live（TTL; 存続可能時間）を超えていても、多くのエントリがキャッシュに存在する場合があります。これらのエントリは使用されない限り、期限切れカウンタには含まれません。キャッシュがフラッシュされると、有効なエントリと無効（古すぎる）エントリの両方が削除されます。フラッシュ動作によって、期限切れカウンタが変更されることはありません。

例

```
mail3.example.com> dnsstatus
Status as of: Sat Aug 23 21:57:28 2003
Counters:                    Reset          Uptime        Lifetime
  DNS Requests         211,735,710       8,269,306     252,177,342
  Network Requests     182,026,818       6,858,332     206,963,542
  Cache Hits           474,675,247      17,934,227     541,605,545
  Cache Misses         624,023,089      24,072,819     704,767,877
  Cache Exceptions      35,246,211       1,568,005      51,445,744
  Cache Expired            418,369           7,800         429,015
mail3.example.com>
```

電子メール モニタリング カウンタのリセット

resetcounters コマンドは、累積する電子メール モニタリング カウンタをリセットします。リセットは、グローバルカウンタとホスト単位のカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。

（注） GUI で、カウンタをリセットすることもできます。[システムステータス（System Status）] ページ （1047 ページ） を参照してください。

例

```
mail3.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

アクティブな TCP/IP サービスの識別

電子メールゲートウェイで使用されるアクティブな TCP/IP サービスを識別するには、コマンドライン インターフェイスで tcpservices コマンドを使用します。

電子メール キューの管理

Cisco AsyncOS では、電子メール キュー内のメッセージに対する動作を実行できます。電子メールキュー内のメッセージは、削除、バウンス、一時停止、またはリダイレクトすることができます。また、キュー内の古いメッセージを検索、削除、およびアーカイブすることもできます。

キュー内の受信者の削除

特定の受信者が配信されていない場合や、電子メール キューをクリアする場合には、deleterecipients コマンドを使用します。deleterecipients コマンドでは、配信を待つ特定の受信者を削除することによって、電子メール配信キューを管理できます。削除される受信者は、受信者の宛先である受信者ホストによって、または、メッセージ エンベロープの Envelope From 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージ（すべてのアクティブ受信者）を一度に削除することもできます。

（注） deleterecipients 機能を実行するには、電子メールゲートウェイをオフラインまたは配信一時停止の状態にすることを推奨します（電子メールの受信と配信の一時停止 （1228 ページ）を参照）。

（注） この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルドカードは使用できません。deleterecipients コマンドは、削除されるメッセージの合計数を返します。また、メール ログ サブスクリプション（IronPort テキスト形式のみ）が設定されている場合、メッセージの削除は別個の行としてログに記録されます。

例

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

電子メールゲートウェイには、必要に応じて受信者を削除するための各種のオプションが用意されています。次に、受信者ホスト別の受信者の削除、Envelope From アドレスによる削除、およびキュー内のすべての受信者の削除の例を示します。

受信者ドメインによる削除

```
Please enter the hostname for the messages you wish to delete.
[]> example.com
Are you sure you want to delete all messages being delivered to "example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

Envelope From アドレスによる削除

```
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com
Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

すべて削除

```
Are you sure you want to delete all messages in the delivery queue (all active recipients)?
 [N]> Y
Deleting messages, please wait.
1000 messages deleted.
```

キュー内の受信者のバウンス

deleterecipients コマンドと同様に、bouncerecipients コマンドでは、配信を待つ特定の受信者をハードバウンスすることによって、電子メール配信キューを管理できます。メッセージのバウンスは、bounceconfig コマンドに指定された通常のバウンス メッセージ設定に従います。

（注） bouncerecipients 機能を実行するには、電子メールゲートウェイをオフラインまたは配信一時停止の状態にすることを推奨します（電子メールの受信と配信の一時停止 （1228ページ）を参照）。

（注） この機能はどの状態でも使用できますが、機能の実行中に一部のメッセージが配信される可能性があります。

受信者ホストおよび送信者の一致は、同一文字列の一致である必要があります。ワイルドカードは使用できません。bouncerecipients コマンドは、バウンスされたメッセージの合計数を返します。

（注） bouncerecipients 機能ではリソースが集中的に使用され、完了までに数分かかる場合があります。オフラインまたは配信一時停止の状態の場合は、バウンス メッセージの実際の送信（ハードバウンス生成がオンの場合）は、resume コマンドを使用して Cisco AsyncOS をオンライン状態にした後でのみ開始されます。

例

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

バウンスされる受信者は、宛先受信者ホストによって、またはメッセージ エンベロープの Envelope From 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージを一度にバウンスすることもできます。

受信者ホストによるバウンス

```
Please enter the hostname for the messages you wish to bounce.
[]> example.com
Are you sure you want to bounce all messages being delivered to "example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

Envelope From アドレスによるバウンス

```
Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com
Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

すべてバウンス

```
Are you sure you want to bounce all messages in the queue? [N]> Y
Bouncing messages, please wait.
1000 messages bounced.
```

キュー内のメッセージのリダイレクト

redirectrecipients コマンドを使用すると、電子メール配信キュー内のすべてのメッセージを別のリレー ホストにリダイレクトできます。受信者を、このホストから大量の SMTP メールを受け入れる準備ができていないホストまたは IP アドレスにリダイレクトすると、メッセージがバウンスするだけでなく、メールが失われる可能性もあることに注意してください。

⚠

注意 メッセージを、/dev/null を宛先とする受信側ドメインにリダイレクトすると、メッセージが失われます。メールをこのようなドメインにリダイレクトしても、CLI に警告は表示されません。メッセージをリダイレクトする前に、受信側ドメインがあるかどうか SMTP ルートを確認してください。

例

次に、すべてのメールを example2.com ホストにリダイレクトする例を示します。

```
mail3.example.com> redirectrecipients
Please enter the hostname or IP address of the machine you want to send all mail to.
[]> example2.com
WARNING: redirecting recipients to a host or IP address that is not prepared to accept
large volumes of SMTP mail from this host will cause messages to bounce and possibly
result in the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
Redirecting messages, please wait.
246 recipients redirected.
```

キュー内の受信者に基づいたメッセージの表示

showrecipients コマンドを使用すると、電子メール配信キューからのメッセージが受信者ホストまたは Envelope From アドレスごとに表示されます。また、キュー内のすべてのメッセージを表示することもできます。

例

```
mail3.example.com> showrecipients
Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
Showing messages, please wait.
MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
1527     1230      user123456@ironport.com Testing
[0]      [0]       9554@example.com
1522     1230      user123456@ironport.com Testing
[0]      [0]       3059@example.com
1529     1230      user123456@ironport.com Testing
[0]      [0]       7284@example.com
1530     1230      user123456@ironport.com Testing
```

```
[0]      [0]       8243@example.com
1532     1230      user123456@ironport.com Testing
[0]      [0]       1820@example.com
1531     1230      user123456@ironport.com Testing
[0]      [0]       9595@example.com
1518     1230      user123456@ironport.com Testing
[0]      [0]       8778@example.com
1535     1230      user123456@ironport.com Testing
[0]      [0]       1703@example.com
1533     1230      user123456@ironport.com Testing
[0]      [0]       3052@example.com
1536     1230      user123456@ironport.com Testing
[0]      [0]       511@example.com
```

次に、すべての受信者ホストへのキュー内のメッセージの例を示します。

電子メール配信の一時停止

メンテナンスやトラブルシューティングのために電子メールの配信を一時的に停止するには、suspenddel コマンドを使用します。suspenddel コマンドは、Cisco AsyncOS を配信一時停止の状態にします。この状態には、次のような特徴があります。

- 発信電子メール配信は停止されます。
- 着信電子メール接続は受け入れられます。
- ログ転送は続行します。
- CLI はアクセス可能のままになります。

suspenddel コマンドを実行すると、開いていた発信接続が閉じられ、新規の接続は開かれません。suspenddel コマンドはただちに開始され、確立しているすべての接続を正常に閉じることができます。配信一時停止の状態から通常の動作に戻すには、resumedel コマンドを使用します。

（注） 「delivery suspend」状態は、システムを再起動しても保持されます。suspenddel コマンドを使用してから電子メールゲートウェイを再起動する場合は、resumedel コマンドを使用して再起動してから配信を再開する必要があります。

例

```
mail3.example.com> suspenddel
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

電子メール配信の再開

resumedel コマンドは、suspenddel コマンドの使用後に Cisco AsyncOS を通常の動作状態に戻します。

構文

resumedel

```
mail3.example.com> resumedel
Mail delivery resumed.
```

電子メールの受信の一時停止

すべてのリスナーに対して 電子メールの受信を一時停止するには、suspendlistener コマンドを使用します。受信が一時停止されている間、システムはリスナーの特定のポートへの接続を受け入れません。

これは、このリリースの AsyncOS で変更された動作です。以前のリリースでは、システムは接続を受け入れ、次のように応答してから接続解除していました。

- SMTP: 421 *hostname* Service not available, closing transaction channel
- QMQP: ZService not available

（注） 「receiving suspend」状態は、システムを再起動しても保持されます。suspendlistener コマンドを使用してから電子メールゲートウェイを再起動する場合、リスナーでメッセージの受信を再開するには、resumelistener コマンドを使用する必要があります。

構文

```
suspendlistener mail3.example.com> suspendlistener
Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

電子メールの受信の再開

resumelistener コマンドは、suspendlistener コマンドの使用後に Cisco AsyncOS を通常の動作状態に戻します。

構文

```
resumelistener

mail3.example.com> resumelistener
```

```
Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Receiving resumed.
mail3.example.com>
```

電子メールの配信と受信の再開

resume コマンドは、配信と受信の両方を再開します。

構文

```
resume
```

```
mail3.example.com> resume
Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

電子メールの即時配信スケジュール

delivernow コマンドを使用すると、後で配信するようにスケジュールされた受信とホストをただちに再試行できます。delivernow コマンドでは、キュー内の電子メールに即時配信を再スケジュールすることができます。down のマークが付いたすべてのドメインと、スケジュールされたメッセージまたはソフト バウンスされたメッセージが、即時配信のキューに入れられます。

delivernow コマンドは、キュー内の（スケジュールされた、およびアクティブな）すべての受信者または特定の受信者に対して呼び出すことができます。特定の受信を選択する際は、即時配信をスケジュールする受信者のドメイン名を入力する必要があります。システムは、文字列全体の文字と長さを照合します。

構文

```
delivernow
```

```
mail3.example.com> delivernow
Please choose an option for scheduling immediate delivery.
1. By recipient host
2. All messages
[1]> 1
Please enter the domain to schedule for immediate delivery.
[]> recipient.example.com
Rescheduling all messages to recipient.example.com for immediate delivery.
mail3.example.com>
```

ワーク キューの休止

LDAP 受信者アクセス、マスカレード、LDAP 再ルーティング、メッセージ フィルタ、スパム対策、およびウイルス対策スキャン エンジンの処理は、すべて「ワーク キュー」で実行されます。処理フローについてはルーティングおよび配信機能の設定（853 ページ）を、「ワーク キュー内のメッセージ」ゲージの説明についてはシステム ゲージの読み取り（1336 ページ）を参照してください。workqueue コマンドを使用して、ワークキュー部分のメッセージ処理を手動で休止することができます。

たとえば、多くのメッセージがワーク キュー内にあるときに、LDAP サーバの設定を変更する必要があるとします。おそらく、LDAP 受信者アクセス クエリーに基づいて、メッセージをバウンスからドロップに切り替えようとします。または、キューを休止して、最新のアンチウイルス スキャン エンジンの定義ファイルを手動で確認（antivirusupdate コマンドを使用）する可能性もあります。workqueue コマンドを使用すると、ワークキューを休止してから再開することで、処理を停止した状態で他の設定変更を行うことができます。

ワーク キューを休止してから再開すると、そのイベントがログに記録されます。次に例を示します。

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S
Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

次の例では、ワーク キューが中止されます。

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:02:30 2003 GMT
Status:   Operational
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- PAUSE - Pause the work queue
- RATE - Display work queue statistics over time
[]> pause
Manually pause work queue?  This will only affect unprocessed messages.  [N]> y
Reason for pausing work queue:
[]> checking LDAP server
Status as of:  Sun Aug 17 20:04:21 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
```

（注） 理由の入力は任意です。理由を入力しないと、その理由は「Manually paused by user」としてログに記録されます。

次の例では、ワーク キューが再開されます。

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:42:10 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- RESUME - Resume the work queue
```

```
- RATE - Display work queue statistics over time
[]> resume
Status:   Operational
Messages: 1243
```

古いメッセージの検索およびアーカイブ

時折、古くなったメッセージが配信できずに、キューに留まっていることがあります。これらのメッセージは削除したり、アーカイブしたりすることができます。これを行うには、showmessage CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージを表示します。oldmessage CLI コマンドを使用すると、システム上の最も古い非隔離メッセージが表示されます。その後は、任意で removemessage を使用して、所定のメッセージ ID に対応するメッセージを安全に削除できます。このコマンドでは、ワーク キュー、再試行キュー、または宛先キュー内のメッセージのみを削除できます。メッセージがこれらのキューのいずれにもない場合は、削除できません。

また、archivemessage[mid] CLI コマンドを使用して、所定のメッセージ ID に対応するメッセージを configuration ディレクトリ内の mbox ファイルにアーカイブすることもできます。

oldmessage コマンドを使用して、隔離エリア内のメッセージのメッセージ ID を取得することはできません。ただし、メッセージ ID がわかっている場合は、指定のメッセージを表示したり、アーカイブしたりすることができます。メッセージがワーク キュー、再試行キュー、または宛先キューにないと、removemessage コマンドでメッセージを削除することはできません。

（注） シスコのスパム検疫内のメッセージに対しては、これらのキュー管理コマンドを実行できません。

構文

```
archivemessage
```

```
example.com> archivemessage
Enter the MID to archive and remove.
[0]> 47
 MID 47 has been saved in file oldmessage_47.mbox in the configuration directory
example.com>
```

構文

```
oldmessage
```

```
example.com> oldmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from example.com ([172.16.0.102])
  by example.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@example.com
To: 4031@test.example2.com
```

```
Subject: Testing
Message-Id: <20070215061136.68297.16346@example.com>
```

システム内のメッセージのトラッキング

findevent CLI コマンドは、オンボックスのメール ログ ファイルを使用して、システム内のメッセージのトラッキング（追跡）プロセスを容易にします。findevent CLI コマンドを使用すると、メッセージ ID の検索、またはサブジェクト ヘッダー、エンベロープ送信者、またはエンベロープ受信者に対する正規表現の一致検索によって、メール ログから特定のメッセージを検索できます。現在のログ ファイルやすべてのログ ファイルの結果を表示することも、ログ ファイルを日付別で表示することもできます。ログ ファイルを日付別で表示する場合は、特定の日付か、日付の範囲を指定できます。

ログを表示するメッセージを識別した後は、findevent コマンドによって、分裂情報（分裂したログ メッセージ、バウンス、およびシステム生成メッセージ）を含む、そのメッセージ ID に対するログ情報を表示できます。次に、findevent CLI コマンドで、サブジェクト ヘッダーに「confidential」とあるメッセージの受信と配信を追跡する例を示します。

```
example.com>
findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 3
Enter the regular expression to search for.
[]> confidential
Currently configured logs:
1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to use for message tracking.
[]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
The following matching message IDs were found. Please choose one to
show additional log information:
1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential
[1]> 1
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1 (172.19.1.86) address
10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To: <ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
```

```
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

SNMP を使用したシステムの状態のモニタリング

AsyncOS オペレーティング システムは、SNMP（シンプル ネットワーク管理プロトコル）を使用したシステム ステータスのモニタリングをサポートしています。このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています。（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。以下の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP が有効の場合、使用されるデフォルトバージョンは SNMPv3 です。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。
- 認証のパスフレーズと暗号は異なっていなければなりません。暗号化アルゴリズムは AES のみにする必要があります。認証アルゴリズムは SHA-1 のみにする必要があります。次に snmpconfig コマンドを実行するときは、コマンドにこのパスフレーズが「記憶」されています。
- SNMPv3 ユーザ名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a SHA -A ironport mail.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ ストリングを設定する必要があります。コミュニティ ストリングは、public にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- SNMPv3 を使用する場合は、次の表に示すサポートされるセキュリティレベルのいずれかを選択する必要があります。

セキュリティ レベル	認証	プライバシー
noAuthNoPriv	○ 認証は、SNMPv3 ユーザ名を使用して行われます。	×
authNoPriv	○ 認証は、SNMPv3 認証パスフレーズを使用して行われます。	×

セキュリティ レベル	認証	プライバシー
authPriv	○ 認証は、SNMPv3 認証パスフレーズを使用して行われます。	○ プライバシーは、SNMPv3 プライバシーパスフレーズを使用してアクティブ化されます。

- SNMPv2 と SNMPv3 の両方を有効にする場合は、トラップに必要なバージョンを選択する必要があります。
- トラップを使用するには、SNMP マネージャ（AsyncOS には含まれていません）が実行中であり、その IP アドレスがトラップ ターゲットとして入力されている必要があります（ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します）。

電子メールゲートウェイに対して SNMP モニタリングをイネーブルにして設定するには、snmpconfig コマンドを使用します。インターフェイスの値を選択し、設定し終えると、電子メールゲートウェイは SNMPv3 GET 要求に応答します。これらのバージョン 3 要求には、一致するパスフレーズが含まれている必要があります。デフォルトでは、バージョン 1 および 2 要求は拒否されます。イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ ストリングが含まれている必要があります。

MIB ファイル

電子メールゲートウェイ用の次の MIB ファイルは、http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html から入手できます。使用可能な最新の MIB ファイルを使用します。

- ASYNCOS-MAIL-MIB.txt：電子メールゲートウェイ用のエンタープライズ MIB の SNMPv2 互換の説明。
- AsyncOS SMI.txt（IRONPORT-SMI.txt）：Cisco コンテンツ セキュリティ製品で ASYNCOS-MAIL-MIB の役割を定義する「管理情報構造」（SMI）ファイル。

ハードウェア オブジェクト

Intelligent Platform Management Interface Specification（IPMI）準拠のハードウェア センサーによって、温度、ファン スピード、電源モジュール ステータスなどの情報が報告されます。

ハードウェア ステータスをポーリングして、致命的な状況になる前に潜在的なハードウェア障害を識別することを推奨します。重大値の 10 % 以内の温度を不安原因と考えることができます。

電子メールゲートウェイの電源モジュールの数や動作温度の範囲などの情報については、モデルのハードウェアガイドを参照してください。ハードウェア ガイドの場所については、資料（7 ページ）を参照してください。

ハードウェア トラップ

ステータス変更トラップは、ステータスが変更されると送信されます。ファン障害および高温トラップは、5 秒ごとに送信されます。その他のトラップは、障害条件アラーム トラップです。これらのトラップは、ステータスが（良好から障害へ）変更されたときに一度だけ送信されます。

たとえば、C170 電子メールゲートウェイで次のしきい値に達すると、トラップが送信されます。

表 *116 : C170* 電子メールゲートウェイのハードウェア トラップ：温度およびハードウェアの条件

モデル	高温（CPU）	高温（周囲）	高温（バックプレーン）	高温（ライザー）	ファン障害	電源モジュール	RAID	リンク
C170	90C	47C	NA	NA	0 RPM	ステータスの変化	ステータスの変化	ステータスの変化

電子メールゲートウェイで使用可能なトラップおよびしきい値を表示するには、コマンドライン インターフェイスで snmpconfig コマンドを実行します。

障害条件アラーム トラップは、個々のコンポーネントの致命的な障害を示しますが、システム全体の障害の原因になるとは限りません。たとえば、複数のファンまたは電源モジュールを持つ電子メールゲートウェイで 1 つのファンまたは電源モジュールに障害が発生しても、電子メールゲートウェイは動作し続けます。

関連項目

- 例：snmpconfig コマンド （1364 ページ）

SNMP トラップ

SNMP には、1 つまたは複数の条件が満たされたときに管理アプリケーション（通常は、SNMP 管理コンソール）に知らせるためのトラップ（または通知）を送信する機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は電子メールゲートウェイ）で、ある条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、SNMP 管理コンソール ソフトウェアが稼働するホストに送信します。

SNMP トラップを有効にして設定するには、snmpconfig コマンドを使用します。

複数のトラップ ターゲットの指定方法：トラップ ターゲットの入力を求められたときに、カンマで区切った IP アドレスを 10 個まで入力できます。

例：snmpconfig コマンド

次の例では、C690 ハードウェア電子メールゲートウェイで snmpconfig コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 1 および 2 からの GET 要求に対してコミュニティ ストリング public が入力されています。

```
mail1.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> setup

Do you want to enable SNMP? [Y]>
SNMP default version is V3

Choose an IP interface for SNMP requests.
1. Management (10.10.4.5/27: mail1.example.com) [1]>

Which port shall the SNMP daemon listen on?
[161]>

Select SNMPv3 security level:
1. noAuthNoPriv - Authentication is done using the SNMPv3 username, and no privacy is
activated.
2. authNoPriv - Authentication is done using the SNMPv3 authentication passphrase, and
no privacy is activated.
3. authPriv - Authentication is done using the SNMPv3 authentication passphrase, and
privacy is activated using the SNMPv3 privacy passphrase.
[3]>

Select SNMPv3 authentication type:
1. SHA
[1]>

Select SNMPv3 privacy protocol:
1. AES
[1]>

Enter the SNMPv3 authentication passphrase.
[]>

The SNMPv3 passphrase must be at least 8 characters.

Enter the SNMPv3 authentication passphrase.
[]>

Enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Enter the SNMPv3 privacy passphrase again to confirm.
[]>
Warning: The same authentication and privacy passwords reduce the security of the system.

Do you want to set other passwords? [Y]> n

Service SNMP V1/V2c requests? [N]> Y
```

```
Enter the SNMP V1/V2c community string.
[ironport]>

Shall SNMP V2c requests be serviced from IPv4 addresses? [Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate multiple networks
 with commas.
[127.0.0.1/32]>

Select the version for SNMP traps:
1. 2c
2. 3
[2]>

Enter the Trap target as a host name, IP address or list of IP addresses separated by
commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 10.10.0.28

Enterprise Trap Status
1. CPUUtilizationExceeded Disabled
2. FIPSModeDisableFailure Enabled
3. FIPSModeEnableFailure Enabled
4. FailoverHealthy Enabled
5. FailoverUnhealthy Enabled
6. connectivityFailure Disabled
7. keyExpiration Enabled
8. linkUpDown Enabled
9. memoryUtilizationExceeded Disabled
10. resourceConservationMode Enabled
11. updateFailure Enabled

Do you want to change any of these settings? [N]>

Enter the System Location string.
[Unknown: Not Yet Configured]>

Enter the System Contact string.
[snmp@localhost]>

Current SNMP settings:
Listening on interface "Management" 10.10.4.5/27 port 161.
SNMP v3: Enabled.
Security level: authPriv
Authentication Protocol: SHA
Encryption Protocol: AES
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32,fe::1/64.
SNMP v1/v2 Community String: ironport
Trap version: V3
Trap target: 10.10.0.28
Location: Unknown: Not Yet Configured
System Contact: snmp@localhost

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
mail1.example.com > commit
```

第 41 章

サービスログを使用したフィッシング検知機能の有効性の向上

この章は、次の項で構成されています。

- 概要 （1367 ページ）
- 電子メールゲートウェイでのサービスログの有効化 （1368 ページ）
- 電子メールゲートウェイでのサービスログの無効化 （1368 ページ）
- FAQ （1368 ページ）

概要

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

サービスログは、フィッシング検出を改善するためにCisco Talosクラウドサービスに送信されます。

（注） AsyncOS 13.5 以降、サービスログでは Cisco Talos クラウドサービスに送信されるテレメトリデータとして、SENDERBASE が置き換えられます。

電子メールゲートウェイは、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

電子メールゲートウェイでのサービスログの有効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [サービスログ（Service Logs）] に移動します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [限られた情報をサービスログ情報サービスと共有する（推奨）（Enable sharing limited data with the Service Logs Information Service (Recommended)）] チェックボックスをオンにします。

このボックスをオンにすると、電子メールゲートウェイの機能がグローバルにイネーブルになります。イネーブルにした場合、（Cisco アンチスパム スキャンがイネーブルになっているかどうかに関係なく）データの収集およびデータの収集にコンテキスト適応スキャン エンジン（CASE）が使用されます。また、CLI の **servicelogsconfig** コマンドを使用して同様の設定を行うこともできます。

ステップ 4 [送信（Submit）] をクリックし、変更をコミットします。

電子メールゲートウェイでのサービスログの無効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [サービスログ（Service Logs）] に移動します。

ステップ 2 [無効化（Disable）] をクリックして変更を確定します。

FAQ

シスコは、プライバシーが重要であると認識しており、プライバシーを考慮してサービスを設計および操作しています。Cisco Talos クラウドサービスに登録した場合は、シスコは組織の電子メールトラフィックに関する集約した統計情報を収集しますが、個人を特定できる情報を収集したり、使用したりすることはありません。シスコが収集した、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます。

どのようなデータを共有するのですか。

データは、メッセージ属性の要約情報および電子メールゲートウェイがどのように各種メッセージを処理したかに関する情報です。メッセージの本文すべてを収集するわけではありません。繰り返しになりますが、シスコに提供された、ユーザまたは組織を特定できる可能性のあ

る情報は、すべて極秘として扱われます（後述のシスコは、共有されたデータがセキュアであることをどのように確認していますか。（1370 ページ）を参照してください）。

次の表では、「人間にわかりやすい」形式でサンプルのログ エントリを説明しています。

表 *117*：電子メールメッセージ情報ごとに共有される統計情報

項目	サンプルデータ
インバウンド SMTP 接続の GUID	0FyIkNX8ThST1 /IdfyNshg==
電子メールメッセージの GUID	1Hss77LIS6u7y5 GDn0QFEQ==
Cisco Secure Email Gateway メッセージ ID	5191655
受信者の数とその有効性	1
シスコ以外の Talos エンジン（アンチウイルスや高度なマルウェア防御など）からのスキャナの判定	4
メッセージの処理	MSG_DISP_DROPPED
メッセージの処理理由	MSG_DISP_FILTER
メッセージはアウトバウンド配信用か。	true
メッセージ サイズ	35100
着信メールリレー	true
メールフローの方向	IP_DIR_OUT
AMP 判定情報	file_sha2_256: "\ 217 \ 263 \ 037 \ 004 \ 374`N \3264\265\016\314\227\005E\337\373q \177A\245 \017\004\204\340\231\260!^
ドロップされたメッセージのサンプリング	true

表 *118*：定期的に共有される統計の設定情報

項目	サンプルデータ
アウトブレイクフィルタ機能の有効化	true
送信者ドメインレピュテーション（SDR）無効フラグ	true
Context Adaptive Scanning Engine（CASE）のバージョン	3.8.5-036

項目	サンプルデータ
Talos エンジン	1.95.0.220
有効化された機能の汎用リスト	Sophos_enabled

シスコは、共有されたデータがセキュアであることをどのように確認していますか。

Cisco Talos クラウドサービスへの登録に同意する場合：

- 電子メールゲートウェイから送信されたデータは、セキュアな gRPC/HTTP2 プロトコルを使用して Cisco Talos クラウドサービスに送信されます。
- お客様のデータはすべて、シスコで慎重に取り扱われます。このデータは、セキュアな場所に保存され、データへのアクセスは、企業の電子メールセキュリティ製品およびサービスの向上またはカスタマーサポートの提供のためにデータにアクセスする必要のあるシスコの従業員および請負業者に限られます。
- データに基づいてレポートまたは統計情報が作成された場合、電子メールの受信者またはお客様の企業を特定する情報が、シスコ以外で共有されることはありません。

データを共有することで Cisco 電子メールゲートウェイのパフォーマンスに影響はありますか。

シスコは、ほとんどのお客様には若干のパフォーマンス上の影響があると認識しています。IronPort は、電子メール配信プロセスの一環として、既存のデータを記録します。顧客データは電子メールゲートウェイで集約され、Cisco Talos クラウドサービスに送信されます。HTTPS を介して転送されるデータの総サイズは、一般的な企業の電子メール トラフィック帯域幅の 1 % 未満と予想しています。

イネーブルにした場合、（Cisco アンチスパム スキャンがイネーブルになっているかどうかに関係なく）データの収集およびデータの収集にコンテキスト適応スキャン エンジン（CASE）が使用されます。

その他ご質問がありましたら、シスコ カスタマー サポートまでお問い合わせください。シスコサポートコミュニティ （8 ページ） を参照してください。

その他の方法でデータを共有できますか。

シスコがより高品質のセキュリティ サービスを提供できるようにするために、ご協力をお考えのお客様のために、追加データの提供を可能にするコマンドを用意しています。このより高レベルのデータ共有では、メッセージに含まれる添付ファイルの明確なファイル名、ハッシュされていないテキスト、および URL のホスト名も提供されます。この機能の詳細について関心をお持ちの場合は、システム エンジニアまたはシスコ カスタマー サポートにお問い合わせください。

第 42 章

GUI での他のタスク

この章は、次の項で構成されています。

- グラフィカル ユーザー インターフェイス（GUI） （1371 ページ）
- GUI のシステム情報 （1372 ページ）
- GUI からの XML ステータスの収集 （1373 ページ）

グラフィカル ユーザー インターフェイス（GUI）

グラフィカル ユーザー インターフェイス（GUI）は、システムのモニタリングおよび設定用の一部のコマンドライン インターフェイス（CLI）コマンドに代わる Web ベースのインターフェイスです。GUI を使用することにより、AsyncOS コマンド構文を知らなくても、単純な Web ベース インターフェイスを使用してシステムをモニタできます。インターフェイスに対して HTTP、HTTPS、またはその両方のサービスをイネーブルにすると、GUI にアクセスし、ログインできるようになります。詳細については、「電子メールゲートウェイへのアクセス」の章を参照してください。

インターフェイスでの GUI のイネーブル化

システムはデフォルトで、管理インターフェイスの HTTP がイネーブルになった状態で出荷されます。

GUI をイネーブルにするには、コマンドライン インターフェイスで interfaceconfig コマンドを実行し、接続先のインターフェイスを編集して、HTTP サービスとセキュア HTTP サービスのいずれか、または両方をイネーブルにします。

（注） また、いずれかのインターフェイスで GUI をイネーブルにした後は、[ネットワーク（Network）] > [IPインターフェイス（IP Interfaces）] ページを使用して、別のインターフェイスに対して GUI をイネーブルまたはディセーブルにすることもできます。詳細については、IP インターフェイス （1573 ページ）を参照してください。

（注） インターフェイスでセキュア HTTP をイネーブルにするには、証明書をインストールする必要があります。詳細については、「HTTPS の証明書のイネーブル化」を参照してください。

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

さらに、このインターフェイス（HTTP または HTTPS 経由）で GUI にアクセスしようとするすべてのユーザは（ユーザーアカウントを使用する作業（1191 ページ）を参照）、標準のユーザ名とパスフレーズのログイン ページで自分自身を認証する必要があります。

（注） GUI にアクセスできるようにするには、commit コマンドを使用して変更内容を保存する必要があります。

次の例では、GUI は Data 1 インターフェイスでイネーブルになります。interfaceconfig コマンドは HTTP はポート 80、HTTPS はポート 443 でイネーブルにするために使用されます（デモ証明書は certconfig コマンドが実行できるようになるまで HTTP 用に一時的に使用されます。詳細については、「電子メールゲートウェイへの証明書のインストール」を参照してください）。ポート 80 への HTTP 要求は、Data 1 インターフェイスではポート 443 に自動的にリダイレクトされるように設定されます。

GUI のシステム情報

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

GUI からの XML ステータスの収集

XML ページを通じてステータスを表示するか、XML ステータス情報にプログラムでアクセスします。

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

GUI のページにあるこの表の情報は、対応する URL にアクセスすることで動的な XML 出力としても使用できます。

GUI のページ名	対応する XML ステータス URL
メール ステータス（Mail Status）	http://*hostname*/xml/status
特定のホストのホスト メール ステータス（Host Mail Status for a Specified Host）	http://*hostname*/xml/hoststatus?hostname=*host*
DNS ステータス（DNS Status）	http://*hostname*/xml/dnsstatus
上位着信ドメイン（Top Incoming Domains）	http://*hostname*/xml/topin
上位送信ドメイン（Top Outgoing Domains）[1]	http://*hostname*/xml/tophosts

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

第 43 章

高度なネットワーク構成

この章は、次の項で構成されています。

- イーサネット インターフェイスのメディア設定 （1375 ページ）
- ネットワーク インターフェイス カードのペアリングおよびチーミング （1377 ページ）
- 仮想ローカル エリア ネットワーク（VLAN） （1379 ページ）
- Direct Server Return （1384 ページ）
- イーサネット インターフェイスの最大伝送単位 （1388 ページ）
- マルチキャスト アドレスでの ARP 応答の受け入れまたは拒否 （1389 ページ）

イーサネット インターフェイスのメディア設定

イーサネットインターフェイスのメディア設定にアクセスするには、etherconfig コマンドを使用します。個々のイーサネットインターフェイスが現在の設定と共に一覧表示されます。インターフェイスを選択すると、可能なメディア設定が表示されます。例については、メディア設定の編集例 （1376 ページ） を参照してください。

etherconfig を使ったイーサネットインターフェイスのメディア設定の編集

etherconfig コマンドを使って、イーサネットインターフェイスのデュプレックス設定（全二重/半二重）や速度（10/100/1000 Mbps）を設定できます。デフォルトでは、インターフェイスが自動的にメディア設定を選択しますが、場合によってはこの設定を上書きする必要があります。

（注） 「セットアップとインストール」の章の説明に従ってGUIのシステム設定ウィザード（またはコマンドライン インターフェイスの systemsetup コマンド）を実行し、変更を確定していれば、電子メールゲートウェイ上でデフォルトのイーサネット インターフェイス設定が構成されているはずです。

一部の電子メールゲートウェイは、光ファイバ ネットワーク インターフェイス オプションを備えています。その場合は、各電子メールゲートウェイ上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス（Data 3 と Data 4）が表示されます。これらのギガビット光ファイバ インターフェイスは、異種混在構成で銅線（Data 1、Data 2、および Management）インターフェイスとペアにすることができます。ネットワーク インターフェイス カードのペアリングおよびチーミング （1377 ページ） を参照してください。

メディア設定の編集例

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> media
Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]> edit
Enter the name or number of the ethernet interface you wish to edit.
[]> 2
Please choose the Ethernet media options for the Data 2 interface.
1. Autoselect
2. 10baseT/UTP half-duplex
3. 10baseT/UTP full-duplex
4. 100baseTX half-duplex

5. 100baseTX full-duplex


6. 1000baseTX half-duplex
7. 1000baseTX full-duplex
[1]> 5
Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (100baseTX full-duplex: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

ネットワーク インターフェイス カードのペアリングおよびチーミング

NIC ペアリングで 2 つの物理データ ポートを組み合わせることにより、NIC からアップストリームのイーサネット ポートへのデータ パスに障害が発生した場合に、バックアップ イーサネット インターフェイスを提供できます。ペアリングでは、基本的に各イーサネット インターフェイスをプライマリ インターフェイスおよびバックアップ インターフェイスとして設定します。プライマリ インターフェイスに障害が発生した場合（つまり、NIC とアップストリーム ノード間のキャリアが途切れた場合）は、バックアップ インターフェイスがアクティブになり、アラートが送信されます。プライマリ インターフェイスは再度起動したときに自動的にアクティブになります。この製品のマニュアルでは、「NIC ペアリング」と「NIC チーミング」は同義語です。

（注） NIC ペアリングは、C170、C190、および C195 電子メールゲートウェイでは使用できません。

十分な数のデータ ポートがあれば、複数の NIC ペアを作成できます。ペアを作成するときは、任意のデータ ポートを組み合わせることができます。次に例を示します。

Data 1 と Data 2

Data 3 と Data 4

Data 2 と Data 3

など

一部の電子メールゲートウェイは、光ファイバ ネットワーク インターフェイス オプションを備えています。その場合は、各電子メールゲートウェイ上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス（Data 3 と Data 4）が表示されます。これらのギガビット光ファイバ インターフェイスは、異種混在構成で銅線（Data 1、Data 2、および Management）インターフェイスとペアにすることができます。

NIC ペアリングと VLAN

VLAN（仮想ローカルエリア ネットワーク（VLAN） （1379 ページ）を参照）は、プライマリ インターフェイスにのみ設定できます。

NIC ペアの名前

NIC ペアを作成するときは、そのペアを参照するときに使用する名前を指定する必要があります。バージョン 4.5 よりも前の AsyncOS で作成した NIC ペアには、アップグレード後、自動的に「Pair 1」というデフォルト名が指定されます。

NIC ペアリングに関して生成されたアラートは、特定の NIC ペアを名前で参照します。

NIC ペアリングと既存のリスナー

リスナーが割り当てられたインターフェイスでNICペアリングをイネーブルにすると、バックアップインターフェイスに割り当てられた全リスナーの削除、再割り当て、ディセーブル化のいずれかを選択するように求められます。

etherconfig コマンドを使った NIC ペアリングのイネーブル化

（注） NICペアリングは、C170、C190、およびC195電子メールゲートウェイでは使用できません。

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> pairing

Paired interfaces:

Choose the operation you want to perform:

- NEW - Create a new pairing.

[]> new

Please enter a name for this pair (Ex: "Pair 1"):

[]> Pair 1

Warning: The backup (Data 2) for the NIC Pair is currently configured with one or more
IP addresses. If you continue, the Data 2 interface will be deleted.

Do you want to continue? [N]> y

The interface you are deleting is currently used by listener "OutgoingMail".

What would you like to do?

1. Delete: Remove the listener and all its settings.

2. Change: Choose a new interface.
```

```
3. Ignore: Leave the listener configured for interface "Data 2" (the listener will be
disabled until you add a new interface named "Data 2" or edit the listener's settings).


[1]>

Listener OutgoingMail deleted for mail3.example.com.

Interface Data 2 deleted.

Paired interfaces:

1. Pair 1:


Primary (Data 1) Active, Link is up

Backup (Data 2) Standby, Link is up

Choose the operation you want to perform:

- DELETE - Delete a pairing.

- STATUS - Refresh status.

[]>
```

仮想ローカル エリア ネットワーク（VLAN）

電子メールゲートウェイの任意の物理ネットワークポートに、複数の仮想ローカルエリアネットワーク（VLAN）を設定できます。

VLAN を使用すると、以下が可能になります。

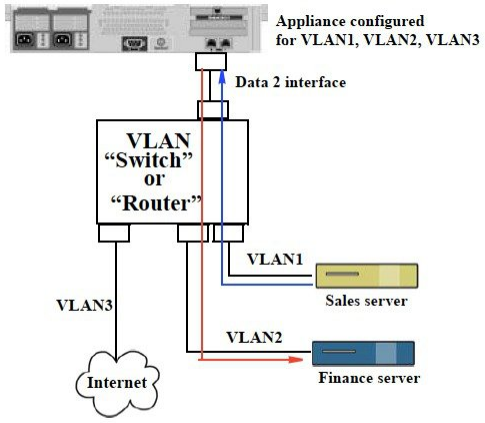
- 電子メールゲートウェイが接続できるネットワークの数を、電子メールゲートウェイ上の物理インターフェイスの数以上に増やすことができます。
- 既存のリスナーの別の「ポート」に、より多くのネットワークを定義できます。
- 管理を容易にするためまたは帯域幅を増やすために、セキュリティ目的でネットワークをセグメント化できます。

使用事例：

VLAN の制限事項のために直接通信できない 2 つのメールサーバが、電子メールゲートウェイを介してメールを送信できます。電子メールゲートウェイの Data 2 インターフェイスは、VLAN1 および VLAN2 で設定されます。青い線は、営業ネットワーク（VLAN1）からアプライアンスに送信されたメールを示しています。電子メールゲートウェイはメールをいつものように処理してから、配信時にパケットを宛先 VLAN2 情報（赤線）でタグ付けします。

VLAN による電子メールゲートウェイ間通信の実現

図 *76 : VLAN* による電子メールゲートウェイ間通信の実現



VLAN の設定について

「データ」および「管理」ポートおよび一部の電子メールゲートウェイモデルで使用可能な光ファイバデータポートなど、電子メールゲートウェイの任意の物理ネットワークポートに、複数の VLAN を設定できます。AsyncOS は、最大 30 の VLAN をサポートします。

物理ポートは、VLAN に配置するために IP アドレスを設定する必要がありません。VLAN を作成した物理ポートに VLAN 以外のトラフィックを受信する IP アドレスを設定できるため、VLAN のトラフィックと VLAN 以外のトラフィックの両方を同じインターフェイスで受信できます。

VLAN は、NIC ペアリング（ペアになっている NIC で使用可能）や Direct Server Return（DSR）と併用できます。

VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データ ポート」として表示されます。「DDDD」は最大 4 桁の ID です（VLAN 2、VLAN 4094 など）。VLAN ID は、電子メールゲートウェイで一意である必要があります。

関連項目

FTP、SSH、および SCP アクセス （1573 ページ）

VLAN の管理

VLAN の作成、編集、および削除を行うには、etherconfig コマンドを使用します。作成後、[ネットワーク（Network）]>[インターフェイス（Interfaces）]ページまたは CLI の interfaceconfig コマンドを使用して VLAN を設定できます。すべての変更を保存することを忘れないでください。

etherconfig コマンドによる新しい VLAN の作成

この例では、Data 1 ポート上に 2 つの VLAN（VLAN 31 と VLAN 34）を作成します。

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
2. Data 2
3. Management
[1]> 1

VLAN interfaces:
1. VLAN 34 (Data 1)
Choose the operation you want to perform:

- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
```

```
2. Data 2

3. Management

[1]> 1

VLAN interfaces:

1. VLAN 31 (Data 1)

2. VLAN 34 (Data 1)

Choose the operation you want to perform:

- NEW - Create a new VLAN.

- EDIT - Edit a VLAN.

- DELETE - Delete a VLAN.

[]>

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]>
```

interfaceconfig コマンドによる VLAN の IP インターフェイスの作成

この例では、VLAN 31 イーサネット インターフェイス上に新しい IP インターフェイスを作成します。

インターフェイスに変更を加えると、電子メールゲートウェイとの接続が閉じることがあります。

```
mail3.example.com> interfaceconfig

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.
```

```
- DELETE - Remove an interface.
[]> new

Please enter a name for this IP interface (Ex: "InternalNet"):

[]> InternalVLAN31
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 10.10.10.10):
[]> 10.10.31.10
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Ethernet interface:
1. Data 1
2. Data 2
3. Management
4. VLAN 31
5. VLAN 34
[1]> 4
Hostname:
[]> mail31.example.com
Do you want to enable SSH on this interface? [N]>
Do you want to enable FTP on this interface? [N]>
Do you want to enable HTTP on this interface? [N]>
Do you want to enable HTTPS on this interface? [N]>
Currently configured interfaces:
1. Data 1 (10.10.1.10/24: example.com)
2. InternalVLAN31 (10.10.31.10/24: mail31.example.com)
3. Management (10.10.0.10/24: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
```

```
- DELETE - Remove an interface.

[]>
```

Web インターフェイスを使用した VLAN の設定

etherconfig コマンドを使用して VLAN を作成した後、[ネットワーク（Network）] > [リスナー（Listeners）] ページを使用して設定できます。

Direct Server Return

Direct Server Return（DSR）は、同じ Virtual IP（VIP; 仮想 IP）を共有する複数の電子メールゲートウェイ間で負荷を分散するための軽量負荷分散メカニズムをサポートする機能です。

DSR は、電子メールゲートウェイの「ループバック」イーサネット インターフェイス上に作成された IP インターフェイスを介して実装されます。

（注） 電子メールゲートウェイの負荷分散の設定は、このマニュアルでは取り上げません

Direct Server Return のイネーブル化

DSR をイネーブルにするには、参加している各電子メールゲートウェイの「ループバック」イーサネット インターフェイスをイネーブルにします。次に、CLI の **interfaceconfig** コマンドまたは GUI の [ネットワーク（Network）] > [インターフェイス（Interfaces）] ページを使用して、ループバック インターフェイス上に仮想 IP（VIP）で IP インターフェイスを作成します。最後に、CLI の **listenerconfig** コマンドまたは GUI の [ネットワーク（Network）] > [リスナー（Listeners）] ページを使用して、新しい IP インターフェイス上にリスナーを作成します。すべての変更を保存することを忘れないでください。

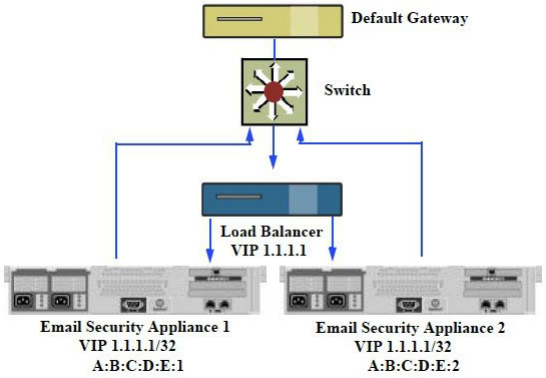
（注） ループバック インターフェイスを使用した場合、電子メールゲートウェイはそのインターフェイスの ARP 応答を発行しません

DSR をイネーブルにするときは、次のルールが適用されます。

すべてのシステムが同じ仮想 IP（VIP）アドレスを使用します。

すべてのシステムがロード バランサと同じスイッチおよびサブネット上にある必要があります。

図 *77 : DSR* を使用したスイッチ上の複数の電子メールゲートウェイ間でのロードバランス



DSR を使用したスイッチ上の複数の電子メールゲートウェイ間でのロードバランス

etherconfig コマンドによるループバック インターフェイスのイネーブル化

イネーブルになったループバック インターフェイスは、他のインターフェイス（Data 1 など）と同じように扱われます。

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.


[]> loopback

Currently configured loopback interface:

Choose the operation you want to perform:


- ENABLE - Enable Loopback Interface.

[]> enable

Currently configured loopback interface:


1. Loopback

Choose the operation you want to perform:

- DISABLE - Disable Loopback Interface.
```

```
[]>

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]>
```

interfaceconfig コマンドによるループバック上の IP インターフェイスの作成

ループバック インターフェイス上に IP インターフェイスを作成します。

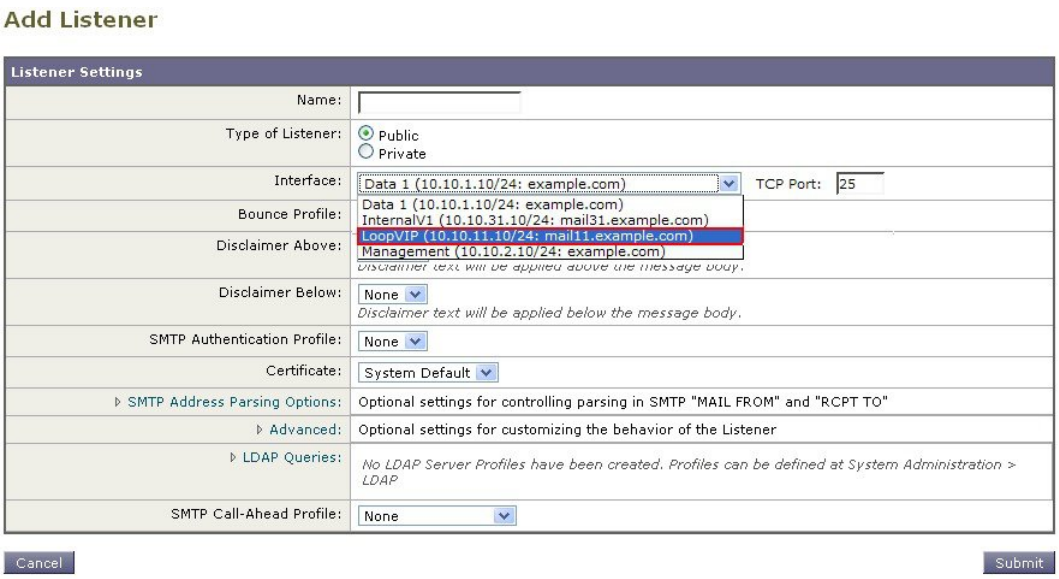
```
mail3.example.com> interfaceconfig

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalV1 (10.10.31.10/24: mail31.example.com)

3. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> new

Please enter a name for this IP interface (Ex: "InternalNet"):

[]> LoopVIP

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 10.10.10.10):

[]> 10.10.1.11

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

[255.255.255.0]> 255.255.255.255

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:
```

```
1. Data 1

2. Data 2

3. Loopback

4. Management

5. VLAN 31

6. VLAN 34

[1]> 3

Hostname:

[]> example.com

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


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


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

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


Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalV1 (10.10.31.10/24: mail31.example.com)

3. LoopVIP (10.10.1.11/24: example.com)

4. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>
```

新しい IP インターフェイス上のリスナーの作成

GUI または CLI を使って新しい IP インターフェイス上にリスナーを作成します。たとえば、次の図に示すように、新たに作成した IP インターフェイスを GUI の [リスナーを追加（Add Listener）] ページで選択できます。

図 *78 :* 新しいループバック *IP* インターフェイス上のリスナーの作成



イーサネット インターフェイスの最大伝送単位

最大伝送単位（MTU）は、イーサネット インターフェイスが受け入れる最大のデータ単位です。etherconfig コマンドを使用してイーサネット インターフェイスの MTU を減らすことができます。イーサネット インターフェイスが受け入れることができる最大 MTU のデフォルト MTU サイズは 1500 バイトです。

インターフェイスの MTU を編集するには：

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> mtu

Ethernet interfaces:

1. Data 1 mtu 1400

2. Data 2 default mtu 1500

3. Management default mtu 1500
```

```
Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]> edit

Enter the name or number of the ethernet interface you wish to edit.

[]> 2

Please enter a non-default (1500) MTU value for the Data 2 interface.

[]> 1200

Ethernet interfaces:

1. Data 1 mtu 1400

2. Data 2 mtu 1200

3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]>
```

マルチキャストアドレスでのARP応答の受け入れまたは拒否

マルチキャスト アドレスで ARP 応答を受け入れるか拒否するかを指定できます。この機能を設定するには、MULTICAST サブコマンドを使用します。

次の例で、マルチキャストアドレスで ARP 応答を受け入れるように電子メールゲートウェイを設定する方法を示します。

```
mail.example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> multicast
ARP replies with a multicast address will be rejected.
Choose the operation you want to perform:
- ACCEPT - Accept ARP replies with a multicast address.
[]> accept
ARP replies with a multicast address will be accepted.
```

第 44 章

ログ

この章は、次の項で構成されています。

- 概要 （1391 ページ）
- ログ タイプ （1405 ページ）
- ログ サブスクリプション （1466 ページ）

概要

- ログ ファイルおよびログ サブスクリプションについて （1391 ページ）
- ログ タイプ （1391 ページ）
- ログ取得方法 （1402 ページ）

ログ ファイルおよびログ サブスクリプションについて

ログは、AsyncOS の電子メール動作に関する重要な情報を収集する、簡潔で効率的な方法です。これらのログには、電子メールゲートウェイでのアクティビティに関する情報が記録されます。情報は、バウンス ログや配信ログなど、表示するログによって異なります。

ほとんどのログは、プレーンテキスト（ASCII）形式で記録されますが、配信ログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキストエディタで読むことができます。

シスコは、複数の電子メールゲートウェイからのログに対応する集中化レポーティングおよびトラッキングツールとして、M シリーズ Cisco Secure Manager Email and Web Gateway を提供しています。詳細については、シスコの担当者にお問い合わせください。

ログ サブスクリプションはログ タイプを名前、ログ レベル、およびサイズや宛先情報などのその他の制約に関連付けます。同じログ タイプで複数のサブスクリプションを使用できます。

ログ タイプ

ログタイプは、メッセージデータ、システム統計情報、バイナリまたはテキストデータなど、生成されたログにどの情報が記録されるかを示します。ログ タイプは、ログ サブスクリプショ

ンを作成するときに選択します。詳細については、ログ サブスクリプション（1466ページ）を参照してください。

AsyncOS では、次のログ タイプが生成されます。

表 *119*：ログ タイプ

ログ	説明
テキスト メール ログ	テキスト メール ログには、電子メール システムの動作に関する情報が記録されます。たとえば、メッセージの受信、メッセージの配信試行、接続のオープンとクローズ、バウンス、TLS 接続などです。
qmail 形式メール ログ	qmail 形式配信ログには、次の配信ログと同じ電子メール システムの動作に関する情報が記録されますが、qmail形式で格納されます。
配信ログ	配信ログには、電子メールゲートウェイの電子メール配信動作に関する重要な情報が記録されます。たとえば、配信試行時の各受信者の配信やバウンスに関する情報などです。ログ メッセージは「ステートレス」です。つまり、関連するすべての情報が各ログ メッセージに記録されるので、ユーザは、現在の配信試行に関する情報について前のログ メッセージを参照する必要がありません。配信ログは、リソースの効率性を保つためにバイナリ形式で記録されます。配信ログ ファイルは、提供されるユーティリティを使用して XML または CSV（カンマ区切り値）形式に変換し、後処理する必要があります。変換ツールは、次の場所にあります。 https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools
バウンス ログ	バウンス ログには、バウンスされた受信者の情報が記録されます。バウンスされた各受信者を記録する情報には、メッセージ ID、受信者 ID、エンベロープ送信元アドレス、エンベロープ宛先アドレス、受信者がバウンスされる理由、および受信者ホストからの応答コードが含まれます。また、バウンスされた各受信者メッセージの一定量を記録するように選択することもできます。この容量はバイト単位で定義され、デフォルトはゼロです。
ステータス ログ	このログ ファイルには、status detail および dnsstatus などの CLI ステータス コマンドで検出されたシステムの統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

ログ	説明
ドメイン デバッグ ログ	ドメインデバッグログには、電子メールゲートウェイと指定の受信者ホスト間のSMTP会話でのクライアントとサーバの通信が記録されます。このログ タイプは、特定の受信者ホストに関する問題のデバッグに使用できます。ログ ファイルに記録するSMTPセッションの総数を指定する必要があります。セッションが記録されるにつれ、この数は減少していきます。ログ サブスクリプションを削除または編集して、すべてのセッションが記録される前にドメインデバッグを停止できます。
インジェクションデバッグ ログ	インジェクションデバッグ ログには、電子メールゲートウェイと、システムに接続している指定のホスト間のSMTP会話が記録されます。インジェクション デバッグ ログは、E メール セキュリティ アプライアンスとインターネット上のホスト間の通信に関する問題をトラブルシューティングするのに役立ちます。
システム ログ	システムログには、ブート情報、仮想電子メールゲートウェイ ライセンスの期限切れアラート、DNSステータス情報、およびcommitコマンドを使用してユーザが入力したコメントが記録されます。システムログは、電子メールゲートウェイの基本的な状態のトラブルシューティングに役立ちます。
CLI 監査ログ	CLI監査ログには、システム上のすべてのCLIアクティビティが記録されます。
FTP サーバ ログ	FTP ログには、インターフェイスで有効になっている FTP サービスの情報が記録されます。接続の詳細とユーザ アクティビティが記録されます。
GUI ログ	HTTP ログを参照してください。
HTTP ログ	HTTPログには、インターフェイスでイネーブルになっているHTTPサービス、セキュアHTTPサービス、またはその両方のサービスに関する情報が記録されます。HTTPを介してグラフィカルユーザーインターフェイス（GUI）にアクセスするため、HTTP ログは基本的に、CLI監査ログのGUI版になっています。GUI でアクセスされるセッションデータ（新しいセッション、セッションの期限切れ）やページが記録されます。 これらのログには、SMTP トランザクションに関する情報（たとえば、電子メールゲートウェイから電子メールで送信されるスケジュール済みレポートに関する情報）も記録されます。

ログ	説明
NTP ログ	NTP ログには、設定されている任意のネットワーク タイム プロトコル（NTP）サーバと電子メールゲートウェイ間の会話が記録されます。詳細については「システム管理」の章の「ネットワーク タイム プロトコル（NTP）設定の編集（Time Keeping Method）」を参照してください。
LDAP デバッグ ログ	LDAP デバッグ ログは、LDAP インストールのデバッグを目的としています(「LDAP クエリー」の章を参照）。電子メールゲートウェイが LDAP サーバに送信しているクエリに関する有用な情報がここに記録されます。詳細については、次を参照してください。
アンチスパム ログ	アンチスパム ログには、最新のアンチスパム ルールのアップデート受信に関するステータスなど、システムのアンチスパム スキャン機能のステータスが記録されます。また、コンテキスト適応スキャンエンジンに関するすべてのログもここに記録されます。
アンチスパム アーカイブ	アンチスパム スキャン機能をイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。アンチスパム エンジンの詳細については、「アンチスパム」の章を参照してください。
グレイメール エンジン ログ	グレイメール エンジン、ステータス、設定などの情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。
グレーメールアーカイブ	アーカイブされたメッセージ（スキャン済みの「アーカイブ メッセージ」アクションに関連付けられているメッセージ）が含まれます。この形式は、mbox 形式のログ ファイルです。
アンチウイルス ログ	アンチウイルス ログには、最新のアンチウイルス アイデンティティ ファイルのアップデート受信に関するステータスなど、システムのアンチウイルス スキャン機能のステータスが記録されます。
アンチウイルス アーカイブ	アンチウイルス エンジンをイネーブルにすると、スキャンされ、「メッセージのアーカイブ」アクションに関連付けられたメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。詳細については、「ウイルス対策」の章を参照してください。
AMP エンジン ログ	AMP エンジンのログは、システムの高度なマルウェア防御機能の状態を記録します。詳細については、ファイル レピュテーション フィルタリングとファイル分析 （585 ページ）を参照してください。

ログ	説明
AMP アーカイブ	高度なマルウェア防御エンジンがスキャン不可能またはマルウェアを含む添付ファイルがあると判断したメッセージをアーカイブするために、メール ポリシーを設定している場合、そのメッセージがここにアーカイブされます。この形式は、mbox 形式のログ ファイルです。
スキャン ログ	スキャン ログには、スキャン エンジンに関するすべての LOG および COMMON メッセージが保持されます（アラート（1275 ページ）を参照してください）。これは一般に、アプリケーションの障害、送信されたアラート、失敗したアラート、およびログ エラー メッセージになります。このログは、システム全体のアラートには適用されません。
スパム隔離ログ	スパム隔離ログには、スパム隔離プロセスに関連付けられたアクションが記録されます。
スパム隔離 GUI ログ	スパム隔離ログには、GUI を介した設定、エンド ユーザー認証、およびエンド ユーザー アクション（電子メールの解放など）を含む、スパム隔離に関連付けられたアクションが記録されます。
SMTP 会話ログ	SMTP 会話ログには、着信および発信 SMTP 会話のすべての部分が記録されます。
セーフリスト/ブロックリスト ログ	セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定およびデータベースに関するデータが記録されます。
レポーティング ログ	レポーティング ログには、中央集中型レポーティング サービスのプロセスに関連付けられたアクションが記録されます。
レポーティング クエリー ログ	レポーティング クエリ ログには、電子メール ゲートウェイで実行されるレポーティング クエリに関連付けられたアクションが記録されます。
アップデータ ログ	アップデータ ログには、McAfee アンチウイルス定義のアップデートなど、システム サービスのアップデートに関するイベントが記録されます。
トラッキング ログ	トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットになっています。
認証ログ	認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

ログ	説明
コンフィギュレーション履歴ログ	コンフィギュレーション履歴ログは、どのような電子メールゲートウェイの変更がいつ行われたかの情報を記録します。ユーザが変更をコミットするたびに、新しいコンフィギュレーション履歴ログが作成されます。
アップグレード ログ	アップグレードのダウンロードとインストールに関するステータス情報。
API ログ	API ログは、電子メールゲートウェイの AsyncOS API に関連するさまざまなイベントを記録します。次に例を示します。 • API が起動したか、または停止したか • API への接続に失敗したか、または閉じたか（応答提供後） • 認証が成功したか、または失敗したか • 要求に含まれるエラー • AsyncOS API とのネットワーク設定変更通信中のエラー
統合イベント ログ	統合イベント ログでは、1 行のログに各メッセージ イベントがまとめられます。このログ タイプを使用すると、分析のためにセキュリティ情報イベント管理（SIEM）ベンダーまたはアプリケーションに送信されるデータ（ログ情報）のバイト数を減らすことができます。このログは、ほとんどの SIEM ベンダーによって幅広く使用されている Common Event Format（CEF）ログ メッセージ形式です。
CSN ログ	CSN ログには、CSN データのアップロードに関する詳細が記録されます。CSN データ（電子メールゲートウェイおよび機能の使用状況の詳細）は、トレースレベルで確認できます。
Advanced Phishing Protection ログ	Advanced Phishing Protection のログには、Cisco Advanced Phishing Protection クラウドサービスに関連する情報が記録されます。ほとんどの情報は [情報（Info）] または [クリティカル（Critical）] レベルです。

ログ	説明
監査ログ	監査ログで認証、許可、アカウンティングのイベント（AAA：Authentication、Authorization、および Accounting）を記録します。 監査ログの詳細の一部を次に示します。 • ユーザー - ログオン • ユーザ - ログオンに失敗しました。パスワードが正しくありません • ユーザ - ログオンに失敗しました。ユーザ名が不明です • ユーザ - ログオンに失敗しました。アカウントの有効期限が切れています • ユーザー - ログオフ • ユーザー - ロックアウト • ユーザー - アクティブ化済み • ユーザー - パスワードの変更 • ユーザー - パスワードのリセット • ユーザー -セキュリティ設定/プロファイルの変更 • ユーザー - 作成済み • ユーザー - 削除または変更 • ユーザ設定 - ユーザが行った設定変更。 • グループ/ロール - 削除/変更済み • グループ/ロール - アクセス許可の変更 • 隔離 - 隔離内のメッセージに対して実行されるアクション。
CSA ログ	CSA ログには、Cisco Secure Awareness クラウドサービスに関連する情報が含まれています。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

ログ タイプの特徴

次の表に、各ログ タイプの特徴をまとめます。

表 *120 :* ログ タイプの比較

						記載内容								
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
メール ログ	•		•			•	•	•	•	•		•		
qmail 形式配信ログ		•			•		•	•	•			•		
配信ログ		•			•		•	•	•			•		
バウンス ログ	•		•						•	•		•		
ステータス ログ		•	•			•								
ドメイン デバッグ ログ	•		•					•	•	•			•	
インジェクション デバッグ ログ	•		•				•				•			
システム ログ	•		•			•								
CLI 監査ログ	•		•			•								

						記載内容								
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
FTP サーバログ	•		•			•								
HTTP ログ	•		•			•								
NTP ログ	•		•			•								
LDAP ログ	•		•											
アンチスパムログ	•		•			•								
Anti-Spam Archive				•										
グレーメールエンジン ログ	•		•			•								
グレーメールアーカイブ				•										
アンチウイルス ログ	•		•			•								

	記載内容													
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
アンチウイルス アーカイブ				•										
AMP エンジン ログ	•		•			•								
AMP アーカイブ				•										
スキャン ログ	•		•			•								•
スパム隔離	•		•			•								
スパム隔離 GUI	•		•			•								
セーフリスト/ブロックリスト ログ	•		•			•								
レポーティング ログ	•		•		•									

						記載内容								
	トランザクション関連	ステートレス	テキストとして記録	mboxファイルとして記録	バイナリとして記録	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンス	個別のソフトバウンス	インジェクション SMTP カンバセーション	ヘッダーのロギング	配信 SMTP カンバセーション	設定情報
レポーティング クエリ ログ	•		•		•									
アップデータ ログ			•											
トラッキング ログ	•				•	•	•	•	•	•		•		
認証ログ	•		•											
設定履歴ログ	•		•											•
API ログ	•		•											
統合イベント ログ	•		•				•	•						
CSN ログ	•		•			•								•
Advanced Phishing Protection ログ	•		•											
監査ログ			•											

ログ取得方法

ログ ファイルは、次のいずれかのファイル転送プロトコルに基づいて取得できます。プロトコルは、グラフィカル ユーザー インターフェイスでサブスクリプションを作成または編集するときに設定するか、ログ サブスクリプションのプロセス中に logconfig コマンドを使用して設定します。

（注） 特定のログで「ログ プッシュ」の方法を使用している場合、そのログは CLI を使用してトラブルシューティングまたは検索目的でローカルで使用することはできません。

表 *121* : ログ転送プロトコル

手動でダウンロード	この方法では、[ログサブスクリプション（Log Subscriptions）] ページにあるログ ディレクトリへのリンクをクリックし、アクセスするログ ファイルをクリックすることによって、いつでもログ ファイルにアクセスできます。ブラウザによっては、ブラウザ ウィンドウでのファイルの表示、またはそれをテキスト ファイルとして開いたり保存することができます。この方法はHTTP（S）プロトコルを使用し、デフォルトの取得方法になっています。 （注） この方法を使用すると、この方法を CLI で指定した場合でも、レベル（マシン、グループ、またはクラスタ）には関係なく、クラスタ内のどのコンピュータのログも取得できません。
FTP プッシュ	この方法では、リモート コンピュータ上の FTP サーバに定期的にログ ファイルをプッシュします。サブスクリプションには、リモート コンピュータ上のユーザ名、パスフレーズ、および宛先ディレクトリが必要です。ログファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。
SCP Push	この方法では、リモート コンピュータ上の SCP サーバに定期的にログ ファイルをプッシュします。この方法には、SSH1 または SSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、リモート コンピュータ上のユーザ名、SSH キー、および宛先ディレクトリが必要です。ログ ファイルは、ユーザが設定したロールオーバー スケジュールに基づいて転送されます。

Syslog Push	この方法では、リモート syslog サーバにログ メッセージを送信します。この方法は、RFC 3164 に準拠しています。 （注） syslog プッシュを使用して転送できるのは、テキストベースのログだけです。 Syslog プッシュ方式を選択した後、以下のフィールドに次の情報を入力します。 • ホスト名（Hostname）：リモート Syslog サーバのホスト名を入力します。 • ポート（Port）：リモート Syslog サーバのポート番号を入力します。デフォルトで使用されるポート番号は 514 です。 • プロトコル（Protocol）：ログ送信に必要なプロトコル（UDP または TCP）を選択します。 • 最大メッセージサイズ（Maximum message size）：リモート Syslog サーバに送信するログメッセージの最大サイズ（バイト単位）を入力します。 （注） （TCP プロトコルの場合）最大メッセージサイズの値は 1024 ー 65535 バイトの整数である必要があります。 （注） （UDP プロトコルの場合）最大メッセージサイズの値は 1024 ー 9216 バイトの整数である必要があります。 • ファシリティ（Facility）：必要に応じて、ログに必要なファシリティを選択します。デフォルトでは、ドロップダウンリストで[認証（Auth）] ファシリティオプションが選択されています。
	• TLS：（TCP プロトコルの場合のみ適用）：TLS 接続を介して電子メールゲートウェイからリモート Syslog サーバにログメッセージを送信するには、このオプションを選択します。 • TLS オプションを選択した場合は、電子メールゲートウェイとリモート Syslog サーバ間の TLS 接続を確立するために、電子メールゲートウェイに有効なクライアント証明書を追加します。 • Syslog プッシュ方式では、電子メールゲートウェイの [SSL 設定（SSL Configuration）] ページの [その他の TLS クライアントサービス（Other TLS Client Services）] オプションで選択したものと同じ TLS バージョンを使用します。 • Syslog プッシュ方式の TLS サポートでは、DEFAULT SSL 暗号リストが使用されます。DEFAULT キーワードは OpenSSL DEFAULT 暗号ストリングで、通常は `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2` です。

	• **Syslog ディスクバッファ（TCP プロトコルのみに適用可能）**：Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定するには、このチェックボックスをオンにします。これにより、リモート Syslog サーバーが使用できないときに、セキュアな電子メールゲートウェイがログイベントをキャッシュできるようになります。Syslog サーバーが使用可能になると、セキュアな電子メールゲートウェイは、そのログサブスクリプションのバッファ内のすべてのデータを Syslog サーバーに送信し始めます。 （注） • ログデータの損失を避けるため、この手順を開始する前に Syslog サーバーが稼働していることを確認してください。 • Syslog サーバーの予想される最大ダウンタイムに対応できる十分なスペースを確保して、ローカルディスクバッファのサイズを決定します。これにより、ログデータの損失を回避できます。 • ローカル保持用のセカンダリ ログサブスクリプションがある場合は、セカンダリ サブスクリプションをキャンセルして、プライマリ サブスクリプション用のローカルディスクバッファ用のスペースを確保することをお勧めします。 • セキュアな電子メールゲートウェイは、Syslog サーバーへの接続が失われた後、最初の数秒間のログデータをキャッシュできない場合があります。これは、TCP 上での Syslog の特性によるものです。 • デフォルトの Syslog バッファサイズは 100 MB です。許可される最大ディスクバッファサイズは 10 GB です。サイズは、バイト（10485760）、メガバイト（10 M）、またはギガバイト（10 G）で入力できます。
（統合イベント ログのみ）AWS S3 プッシュ	この方法では、Amazon Web Services（AWS）パブリック クラウドで使用可能な Amazon Simple Storage Service（S3）バケットに定期的にログファイルをプッシュします。Amazon S3 バケットにアクセスするために、サブスクリプションには S3 バケット名、アクセス キー、および秘密キーが必要です。ログ ファイルを転送するためのロールオーバー スケジュールを設定できます。 （注） この取得方法を使用するには、有効な AWS S3 バケットがあることを確認してください。詳細については、https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html にある AWS のユーザ マニュアルを参照してください。

ログ ファイル名とディレクトリ構造

AsyncOS は、ログ サブスクリプション名に基づいて各ログ サブスクリプションのディレクトリを作成します。ディレクトリ内の実際のログ ファイル名は、ユーザが指定したログ ファイル名、ログ ファイルが開始されたときのタイムスタンプ、および単一文字のステータス コードで構成されます。ログのファイル名は、次の形式で作成されます。

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

ステータス コードは、.current または .s（保存済みを示す）になります。保存済みステータスのログ ファイルだけを転送または削除するようにしてください。

ログのロールオーバーおよび転送スケジュール

ログ ファイルはログ サブスクリプションによって作成され、到達したユーザ指定の最初の条件（最大ファイルサイズまたはスケジュール設定されたロールオーバー）に基づいて、ロールオーバー（および、プッシュ ベースの取得オプションが選択されている場合は転送）されます。最大ファイルサイズとスケジュール設定されたロールオーバーの時間間隔の両方を設定するには、CLI で、または GUI の [ログサブスクリプション（Log Subscriptions）] ページで logconfig コマンドを使用します。また、GUI の [今すぐロールオーバー（Rollover Now）] ボタン、または CLI の rollovernow コマンドを使用して、選択したログ サブスクリプションをロールオーバーすることもできます。ロールオーバーのスケジュール設定の詳細については、ログ サブスクリプションのロールオーバー （1472 ページ）を参照してください。

手動のダウンロードを使用して取得されたログは、指定した最大数（デフォルトは 10 ファイル）に達するか、またはシステムでログ ファイル用にさらにスペースが必要になるまで保存されます。

デフォルトで有効になるログ

電子メールゲートウェイは、多数のログサブスクリプションがデフォルトでイネーブルになった状態で事前に設定されています（適用したライセンスキーによって、その他のログが設定される場合があります）。デフォルトでは、取得方法は「手動でのダウンロード」です。

エラーだけが含まれるように 1 に設定された error_logs を除き、事前に設定されるすべてのログ サブスクリプションのログ レベルは3になります。詳細については、ログ レベル （1468ページ）を参照してください。新規のログ サブスクリプションの作成、または既存のログ サブスクリプションの変更については、ログ サブスクリプション （1466 ページ）を参照してください。

ログ タイプ

- テキスト メール ログの使用 （1407 ページ）
- 配信ログの使用 （1421 ページ）
- バウンス ログの使用 （1424 ページ）
- ステータス ログの使用 （1425 ページ）
- ドメイン デバッグ ログの使用 （1429 ページ）

- インジェクション デバッグ ログの使用 （1429 ページ）
- システム ログの使用 （1431 ページ）
- CLI 監査ログの使用 （1431 ページ）
- FTP サーバ ログの使用 （1432 ページ）
- HTTP ログの使用 （1433 ページ）
- NTP ログの使用 （1434 ページ）
- スキャン ログの使用 （1434 ページ）
- アンチスパム ログの使用 （1435 ページ）
- グレイメール ログの使用 （1435 ページ）
- アンチウイルス ログの使用 （1436 ページ）
- AMP エンジン ログの使用 （1436 ページ）
- スパム隔離ログの使用 （1442 ページ）
- スパム隔離 GUI ログの使用 （1443 ページ）
- LDAP デバッグ ログの使用 （1443 ページ）
- セーフリスト/ブロックリスト ログの使用 （1445 ページ）
- レポーティング ログの使用 （1446 ページ）
- レポーティング クエリー ログの使用 （1447 ページ）
- アップデータ ログの使用 （1448 ページ）
- トラッキング ログについて （1449 ページ）
- 認証ログの使用 （1450 ページ）
- コンフィギュレーション履歴ログの使用 （1451 ページ）
- 外部脅威フィードのエンジン ログの使用 （1452 ページ）
- 統合イベント ログの使用 （1453 ページ）
- CSN ログの使用 （1461 ページ）
- Advanced Phishing Protection ログの使用 （1461 ページ）
- 監査ログの使用 （1462 ページ）
- CSA ログの使用 （1464 ページ）

ログ ファイル内のタイムスタンプ

次のログ ファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、および GMT オフセット（秒単位でログの始まりにのみ表示）が含まれます。

- アンチウイルス ログ
- LDAP ログ
- システム ログ
- メール ログ

テキスト メール ログの使用

これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。これらのログは、特定のメッセージの配信を理解し、システムパフォーマンスを分析するうえで有益な情報源となります。

これらのログに、特別な設定は必要ありません。ただし、添付ファイル名を表示するには、適切なシステムの設定が必要です。添付ファイル名は、常に記録されるわけではありません。詳細については、メッセージ トラッキングの有効化（1113ページ）およびメッセージ トラッキングの概要 （1113 ページ）を参照してください。

次の表に、テキスト メール ログに表示される情報を示します。

表 *122*: テキスト メール ログの統計情報

統計	説明
ICID	インジェクション接続 ID。システムに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが送信されます。
DCID	配信接続 ID。別のサーバに対する個々の SMTP 接続を表す数値 ID であり、この接続で 1 個から数千個のメッセージが配信されます。1 つのメッセージ送信で一部または全部の RID が一緒に配信されます。
RCID	RPC Connection ID（RPC 接続 ID）。スパム隔離に対する個々の RPC 接続を表す数値 ID です。この ID を使用して、スパム隔離との間で送受信されるメッセージを追跡します。
MID	Message ID（メッセージ ID）：この ID を使用して、ログを通過するメッセージを追跡します。
RID	Recipient ID（受信者 ID）：各メッセージ受信者に ID が割り当てられます。
新規作成	新規の接続が開始されました。
開始	新規のメッセージが開始されました。

テキスト メール ログの解釈

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。

（注） ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

表 *123 :* テキスト メール ログの詳細

1	Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes
2	Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
3	Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>
4	Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>
5	Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>
6	Mon Apr 17 19:59:59 2003 Info: ICID 5 close
7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

次の表を、前述のログ ファイルを読み取るためのガイドとして、使用してください。

表 *124 :* テキスト メール ログの例の詳細

行番号	説明
1	システムに対して新しい接続が開始され、インジェクション ID（ICID）「5」が割り当てられました。接続は管理 IP インターフェイスで受信され、10.1.1.209 のリモート ホストで開始されました。
2	クライアントから MAIL FROM コマンドが実行された後、メッセージにメッセージ ID（MID）「6」が割り当てられました。
3	送信者アドレスが識別され、受け入れられます。
4	受信者が識別され、受信者 ID（RID）「0」が割り当てられました。
5	MID 5 が受け入れられ、ディスクに書き込まれ、承認されます。

行番号	説明
6	受信に成功し、受信接続がクローズします。
7	次に、メッセージ配信プロセスが開始されます。192.168.42.42 から 10.5.3.25 への配信に、配信接続 ID（DCID）「8」が割り当てられました。
8	RID「0」へのメッセージ配信が開始されました。
9	RID「0」への MID 6 の配信に成功しました。
10	配信接続がクローズします。

テキスト メール ログ エントリの例

次に、さまざまな状況に基づいたいくつかのサンプル ログ エントリを示します。

メッセージのインジェクションおよび配信

1 人の受信者に対するメッセージが電子メールゲートウェイにインジェクトされます。メッセージは正常に配信されます。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None

Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative

Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

正常なメッセージ配信

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

失敗したメッセージ配信（ハード バウンス）

2 人の受信者が指定されたメッセージが電子メールゲートウェイにインジェクトされます。配信時に、宛先ホストが 5XX エラーを返します。このエラーは、メッセージをいずれの受信者にも配信できないことを示します。電子メールゲートウェイは送信者に通知し、キューから受信者を削除します。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address
64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

ソフト バウンスの後の正常な配信

メッセージが電子メールゲートウェイにインジェクトされます。最初の配信試行で、メッセージはソフト バウンスして、その後の配信キューに入れられます。2回めの試行でメッセージは正常に配信されます。

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23
2003

Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

scanconfig コマンドのメッセージ スキャン結果

scanconfig コマンドを使用して、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）のシステムの動作を決定できます。オプションは、Deliver、Bounce、または Drop です。

次に、scanconfig を Deliver に設定したテキスト メール ログの例を示します。

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line
seen before first header


Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

次に、scanconfig を drop に設定したテキスト メール ログの例を示します。

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

添付ファイルを含むメッセージ

この例では、添付ファイル名の識別を有効にするように、条件「Message Body Contains」を含むコンテンツ フィルタが設定されています。

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes

Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0

Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
```

```
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

3 つの添付ファイルの 2 番目が Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

DANE のサポートによる正常なメッセージ配信

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [必須（Mandatory）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。TLSA レコードの検証に成功した場合、メッセージが受信者に配信されます。

```
Tue Nov 13 12:13:33 2018 Debug: Trying DANE MANDATORY for example.org
Tue Nov 13 12:13:33 2018 Debug: SECURE MX record(mail.example.org) found for example.org
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q('mail.example.org', 'CNAME')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QN('mail.example.org', 'CNAME',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QIP  ('mail.example.org','CNAME','8.8.8.8',60)
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q  ('mail.example.org', 'CNAME', '8.8.8.8')
Tue Nov 13 12:13:34 2018 Debug: DNSSEC Response data([], , 0, 1799)
Tue Nov 13 12:13:34 2018 Debug: Received NODATA for domain mail.example.org type CNAME
Tue Nov 13 12:13:34 2018 Debug: No CNAME record(NoError) found for domain(mail.example.org)
Tue Nov 13 12:13:34 2018 Debug: SECURE A record (4.31.198.44) found for
MX(mail.example.org) in example.org
Tue Nov 13 12:13:34 2018 Info: New SMTP DCID 92 interface 10.10.1.191 address 4.31.198.44
 port 25
Tue Nov 13 12:13:34 2018 Info: ICID 13 lost
Tue Nov 13 12:13:34 2018 Info: ICID 13 close
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q('_25._tcp.mail.example.org', 'TLSA')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QN('_25._tcp.mail.example.org', 'TLSA',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QIP
('_25._tcp.mail.example.org','TLSA','8.8.8.8',60)
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q  ('_25._tcp.mail.example.org', 'TLSA',
'8.8.8.8')
Tue Nov 13 12:13:35 2018 Debug: DNSSEC Response data(['0301010c72ac70b745ac19998811b13
1d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0, 1799)
Tue Nov 13 12:13:35 2018 Debug: DNS encache (_25._tcp.mail.example.org, TLSA,
[(2550119024205761L, 0,
'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
Tue Nov 13 12:13:35 2018 Debug: SECURE TLSA Record found for MX(mail.example.org) in
example.org
Tue Nov 13 12:13:36 2018 Info: DCID 92 Certificate verification successful
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384 for example.org
Tue Nov 13 12:13:36 2018 Info: Delivery start DCID 92 MID 23 to RID [0]
```

証明書の検証失敗によるメッセージ配信の失敗

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [必須（Mandatory）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。証明書の検証に失敗すると、メッセージが後ほど配信されます。安全なTLSA レコードが見つからない場合、メッセージはバウンスされます。

```
Wed Nov 14 05:52:08 2018 Debug: DNS query: QN('server1.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 05:52:08 2018 Debug: DNS query: QIP
('server1.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q  ('server1.example.net', 'CNAME',
'10.10.2.184')
Wed Nov 14 05:52:08 2018 Debug: DNSSEC Response data([], , 0, 284)
Wed Nov 14 05:52:08 2018 Debug: Received NODATA for domain server1.example.net type CNAME
Wed Nov 14 05:52:08 2018 Debug: No CNAME record(NoError) found for
domain(server1.example.net)
Wed Nov 14 05:52:08 2018 Debug: Secure CNAME(server1.example.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: SECURE A record (10.10.1.198) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Info: New SMTP DCID 102 interface 10.10.1.191 address 10.10.1.198
 port 25
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with CNAME(server1.example.net)
for
MX(someone.cs2.example.net) in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.server1.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(server1.example.net) in
 example.net
Wed Nov 14 05:52:08 2018 Debug: DCID 102 All TLSA records failed for certificate not
trusted
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
 in example.net
Wed Nov 14 05:52:08 2018 Info: DCID 102 Certificate verification successful
Wed Nov 14 05:52:08 2018 Info: DCID 102 TLS success protocol TLSv1.2 cipher
DHE-RSA-AES128-SHA256
for example.net
Wed Nov 14 05:52:08 2018 Info: Delivery start DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: Message done DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: MID 26 RID [0] Response 'ok:  Message 31009 accepted'
Wed Nov 14 05:52:08 2018 Info: Message finished MID 26 done

Wed Nov 14 06:36:22 2018 Debug: Trying DANE MANDATORY for example.net
Wed Nov 14 06:36:22 2018 Debug: SECURE MX record(someone.cs2.example.net) found for
example.net
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('someone.cs2.example.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('someone.cs2.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP
('someone.cs2.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('someone.cs2.example.net', 'CNAME',
'10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data(['mail.example2.net.'], secure, 0,
 3525)
```

```
Wed Nov 14 06:36:22 2018 Debug: DNS encache (someone.cs2.example.net, CNAME,
[(2692348132363369L, 0,
'SECURE', 'mail.example2.net')])
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('mail.example2.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('mail.example2.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP
('mail.example2.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('mail.example2.net', 'CNAME', '10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data([], , 0, 225)
Wed Nov 14 06:36:22 2018 Debug: Received NODATA for domain mail.example2.net type CNAME
Wed Nov 14 06:36:22 2018 Debug: No CNAME record(NoError) found for
domain(mail.example2.net)
Wed Nov 14 06:36:22 2018 Debug: Secure CNAME(mail.example2.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: INSECURE A record (10.10.1.197) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net) in example.net
Wed Nov 14 06:36:22 2018 Info: New SMTP DCID 104 interface 10.10.1.191 address 10.10.1.197
 port 25
Wed Nov 14 06:36:36 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 06:36:36 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
 in example.net
Wed Nov 14 06:36:36 2018 Debug: DCID 104 All TLSA records failed for certificate not
trusted
Wed Nov 14 06:36:36 2018 Info: MID 27 DCID 104 DANE failed for the domain example.net:
DANE Certificate verification failed
Wed Nov 14 06:36:36 2018 Info: Failed for all MX hosts in example.net
```

無効な TLSA レコードによるメッセージ配信の失敗

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [必須（Mandatory）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。無効な TLSA レコードが見つかると、後ほどメッセージの配信が試行されるか、メッセージがバウンスされます。

```
Tue Aug 7 05:15:18 2018 Debug: Trying DANE MANDATORY for example-dane.net
Tue Aug 7 05:15:18 2018 Debug: SECURE MX record (someone.example-dane.net) found for
test-tlsabogus.net
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('someone.example-dane.net', 'CNAME',
'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
('someone.example-dane.net','CNAME','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME',
'10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data ([], , 0, 300)
Tue Aug 7 05:15:18 2018 Debug: SECURE A record (10.10.1.198) found for MX
(someone.example-dane.net)
in example-dane.net
Tue Aug 7 05:15:18 2018 Info: ICID 32 close
Tue Aug 7 05:15:18 2018 Info: New SMTP DCID 61 interface 10.10.1.194 address 10.10.1.198
 port 25
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('_25._tcp.someone.example-dane.net', 'TLSA',

'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
```

```
('_25._tcp.someone.example-dane.net','TLSA','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA',
 '10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data
(['03010160b3f16867357cdfef37bb6acd687af54f
225e3bfa945e1d37bfd37bd4eb6020'], bogus, 0, 60)
Tue Aug 7 05:15:18 2018 Debug: DNS encache (_25._tcp.someone.example-dane.net, TLSA,
[(11065394975822091L,
 0, 'BOGUS', '03010160b3f16867357cdfef37bb6acd687af54f225e3bfa945e1d37bfd37bd4eb6020')])
Tue Aug 7 05:15:18 2018 Debug: BOGUS TLSA Record is found for MX (someone.example-dane.net)

in example-dane.net
Tue Aug 7 05:15:18 2018 Debug: Trying next MX record in example-dane.net
Tue Aug 7 05:15:18 2018 Info: MID 44 DCID 61 DANE failed: TLSA record BOGUS
Tue Aug 7 05:15:18 2018 Debug: Failed for all MX hosts in example-dane.net
```

TLSA レコードが見つからない場合に状況対応型 TLS にロールバックする

1 人の受信者に対するメッセージが電子メールゲートウェイに到達します。電子メールゲートウェイは、DNS サーバから安全な DNS MX レコード、DNS A レコード、TLSA レコードをリクエストします。DANE を [状況対応型（Opportunistic）] と選択している場合、TLSA レコードが受信者のドメインの X.509 証明書の値に対して検証されます。受信者のドメインの TLSA レコードが見つからない場合、SMTP カンバセーションの暗号化に状況対応型の TLS が使用されます。

```
Wed Sep 12 06:51:32 2018 Debug: Trying DANE OPPORTUNISTIC for example-dane.com
Wed Sep 12 06:51:32 2018 Debug: SECURE MX record (mx.example-dane.com) found for
digitalhellion.com
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QN ('mx.example-dane.com', 'CNAME',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QIP ('mx.example-dane.com',
'CNAME','8.8.8.8',60)
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME', '8.8.8.8')
Wed Sep 12 06:51:32 2018 Debug: DNSSEC Response data ([], , 0, 1799)
Wed Sep 12 06:51:32 2018 Debug: Received NODATA for domain mx.example-dane.com type CNAME
Wed Sep 12 06:51:32 2018 Debug: No CNAME record (NoError) found for domain
(mx.example-dane.com)
Wed Sep 12 06:51:32 2018 Debug: SECURE A record (162.213.199.115) found for MX
(mx.example-dane.com)
in example-dane.com
Wed Sep 12 06:51:32 2018 Info: ICID 1 lost
Wed Sep 12 06:51:32 2018 Info: ICID 1 close
Wed Sep 12 06:51:33 2018 Info: New SMTP DCID 2 interface 10.10.1.173 address
162.213.199.115 port 25
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QN ('_25._tcp.mx.example-dane.com', 'TLSA',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QIP
('_25._tcp.mx.example-dane.com','TLSA','8.8.8.8', 60)
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA',
'8.8.8.8')
Wed Sep 12 06:51:34 2018 Debug: DNSSEC Response data ([], , 3, 1798)
Wed Sep 12 06:51:34 2018 Debug: Received NXDomain for domain _25._tcp.mx.example-dane.com'
 type TLSA
Wed Sep 12 06:51:34 2018 Debug: No TLSA record (NXDomain) found for MX
(mx.example-dane.com)
Wed Sep 12 06:51:34 2018 Debug: Falling back to conventional TLS for MX
(mx.example-dane.com)
in example-dane.com
Wed Sep 12 06:51:34 2018 Info: MID 1 DCID 2 DANE failed for the domain example-dane.com:
 No TLSA Record
```

```
Wed Sep 12 06:51:34 2018 Info: DCID 2 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384
Wed Sep 12 06:51:35 2018 Info: Delivery start DCID 2 MID 1 to RID [0]
```

送信者の発信国に基づいて受信したメッセージ

この例では、ログには、受信されたメッセージが特定の送信者グループの国に基づいて表示されています。

```
Thu Apr  6 06:50:18 2017 Info: ICID 73 ACCEPT SG ALLOWED_LIST match country[us] SBRS
-10.0 country United States
```

メッセージ添付ファイル内の最大 URL 数が URL スキャン制限を超えている

この例では、ログはURL スキャンの制限を超えた、メッセージの添付ファイル内の URL の数を示しています

```
Wed Nov 8 13:35:48 2017 Info:  MID $mid not completely scanned for URL Filtering. Error:
 $error
```

メッセージ本文内の最大 URL 数が URL スキャン制限を超えている

この例では、ログはURL スキャンの制限を超えた、メッセージの本文内の URL の数を示しています。

```
Wed Nov 8 13:37:42 2017 Info: MID 976 not completely scanned for URL Filtering.
Error: The number of URLs in the message body exceeded the URL scan limit.
```

Cisco プロキシ サーバにリダイレクトされる悪意のある短縮 URL

次の例では、ある短縮 URl が、URL レピュテーション スコアが -3 であるため悪意があるものとしてマークされ、Cisco Security Proxy サーバにリダイレクトされたことがログに表示されています。

```
Tue Nov 7 10:42:41 2017 Info: MID 9 having URL: http://ow.ly/Sb6O30fJvVn has been expanded
 to http://bit.ly/2frAl1x
Tue Nov 7 10:42:42 2017 Info: MID 9 having URL: http://bit.ly/2frAl1x has been expanded
 to http://thebest01.wayisbetter.cn/?cMFN
Tue Nov 7 10:42:42 2017 Info: MID 9 URL http://thebest01.wayisbetter.cn/?cMFN has
reputation -3.854 matched Action: URL redirected to Cisco Security proxy
Tue Nov 7 10:42:42 2017 Info: MID 9 rewritten to MID 10 by
url-reputation-proxy-redirect-action filter 'aa'
```

メッセージ内の短縮 URL を展開できない

この例では、ログは、メッセージに含まれる短縮 URL を実際の URL に展開できなかったことを示します。

```
Mon Oct 30 10:58:59 2017 Info: MID 36 having URL: http://ow.ly/P0Kw30fVst3 has been
expanded to http://bit.ly/2ymYWPR
Mon Oct 30 10:59:00 2017 Info: MID 36 having URL: http://bit.ly/2ymYWPR has been expanded
 to http://ow.ly/cTS730fVssH
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://ow.ly/cTS730fVssH has been
expanded to http://bit.ly/2xK8PD9
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://bit.ly/2xK8PD9 has been expanded
 to http://ow.ly/lWOi30fVssl
Mon Oct 30 10:59:02 2017 Info: MID 36 having URL: http://ow.ly/lWOi30fVssl has been
```

```
expanded to http://bit.ly/2ggHv9e
Mon Oct 30 10:59:03 2017 Info: MID 36 having URL: http://bit.ly/2ggHv9e has been expanded
 to http://ow.ly/4fSO30fVsqx
Mon Oct 30 10:59:04 2017 Info: MID 36 having URL: http://ow.ly/4fSO30fVsqx has been
expanded to http://bit.ly/2hKEFcW
Mon Oct 30 10:59:05 2017 Info: MID 36 having URL: http://bit.ly/2hKEFcW has been expanded
 to http://ow.ly/NyH830fVsq6
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://ow.ly/NyH830fVsq6 has been
expanded to http://bit.ly/2ysnsNi
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://bit.ly/2ysnsNi has been expanded
 to http://ow.ly/JhUN30fVsnL
Mon Oct 30 10:59:07 2017 Info: MID 36 having URL: http://ow.ly/JhUN30fVsnL has been
expanded to http://bit.ly/2hKQmAe
Mon Oct 30 10:59:07 2017 Info: MID 36 URL http://bit.ly/2hKQmAe is marked malicious due
 to : URL depth exceeded
Mon Oct 30 11:04:48 2017 Warning: MID 40 Failed to expand URL http://mail1.example.com/abcd
 Reason: Error while trying to retrieve expanded URL
Mon Oct 30 11:04:48 2017 Info: MID 40 not completely scanned for URL Filtering. Error:
Message has a shortened URL that could not be expanded
```

メッセージ添付ファイルでの悪意のある URL のログ エントリ

この例では、レピュテーション スコアが -9.5 で、悪意のあるメッセージの添付ファイルに含まれる URL がログに表示されています。

```
Mon Nov 6 06:50:18 2017 Info: MID 935 Attachment file_1.txt URL http://jrsjvysq.net has
 reputation -9.5 matched
Condition: URL Reputation Rule
```

抽出エラーが原因でスキャン不可とマークされたメッセージ

この例では、ログは添付ファイル抽出エラーが原因でコンテンツ スキャナによってスキャンされないメッセージを示しています。

```
Tue Oct 24 08:28:58 2017 Info: Start MID 811 ICID 10
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 From: <sender@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 RID 0 To: <recipient@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 Message-ID '<example@cisco.com>'
Tue Oct 24 08:28:58 2017 Info: MID 811 Subject 'Test mail'
Tue Oct 24 08:28:58 2017 Info: MID 811 ready 5242827 bytes from <user2@sender.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Oct 24 08:28:59 2017 Info: MID 811 attachment 'gzip.tar.gz'
Tue Oct 24 08:28:59 2017 Info: MID 811 was marked as unscannable due to extraction
failures. Reason: Error in extraction process - Decoding Errors.
Tue Oct 24 08:28:59 2017 Info: ICID 10 close
Tue Oct 24 08:28:59 2017 Info: MID 811 quarantined to "Policy" (Unscannable: due to
Extraction Failure)
Tue Oct 24 08:28:59 2017 Info: Message finished MID 811 done
```

RFC 違反が原因でスキャン不可とマークされたメッセージ

この例では、ログはRFC違反が原因でコンテンツ スキャナによってスキャンされないメッセージを示しています。

```
Tue Oct 24 08:23:26 2017 Info: Start MID 807 ICID 6
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 From: <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 RID 0 To: <recipient@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 Subject 'Test Mail'
Tue Oct 24 08:23:26 2017 Info: MID 807 ready 427 bytes from <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 matched all recipients for per-recipient policy
```

```
DEFAULT in the inbound table
Tue Oct 24 08:23:26 2017 Info: MID 807 was marked as unscannable due to an RFC violation.
 Reason: A Unix-From header was found in the middle of a header block.
Tue Oct 24 08:23:26 2017 Info: MID 807 queued for delivery
Tue Oct 24 08:23:26 2017 Info: ICID 6 close
```

生成またはリライトされたメッセージに対するログ エントリ

リライト/リダイレクトアクションなどの一部の機能（alt-rcpt-to フィルタ、アンチスパム RCPT リライト、bcc() アクション、アンチウイルス リダイレクションなど）によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

または

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

「rewritten」エントリについては、ログ内で新しい MID の使用を示す行の後に表示される点に注目してください。

スパム隔離エリアに送信されたメッセージ

メッセージを隔離領域に送信すると、メール ログでは、RPC 接続を識別する RPC 接続 ID（RCID）を使用して、隔離領域との間の移動が追跡されます。次のメール ログでは、スパムとしてタグが付けられたメッセージがスパム隔離に送信されています。

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local
IronPort Spam Quarantine


Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877

Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
```

```
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

外部脅威フィードのメール ログの例

メール ログには、受信メッセージで検出された脅威と、そのようなメッセージに対して実行されたアクションに関する情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

```
Thu Jun 7 20:48:10 2018 Info: MID 91 Threat feeds source 'S1' detected malicious URL:
'http://digimobil.mobi/' in attachment(s): malurl.txt. Action: Attachment stripped
```

SDR フィルタリングのログ エントリの例

SDR フィルタリング情報はメール ログに書き込まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

- 送信者ドメイン レピュテーションの認証の失敗 （393 ページ）
- 送信者ドメイン レピュテーションのリクエストのタイムアウト （394 ページ）
- 送信者ドメイン レピュテーションの無効なホスト （394 ページ）
- 送信者ドメインのレピュテーションの一般的なエラー （394 ページ）

送信者ドメイン レピュテーションの認証の失敗

この例のログは、SDR サービスに接続する際の認証失敗のために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Authentication failure.
```

ソリューション

CLI で `sdradvancedconfig` コマンドを使用すると、電子メールゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメイン レピュテーションのリクエストのタイムアウト

この例のログは、SDR サービスと通信する際のリクエスト タイムアウトのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
```

```
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Request timed out.
```

ソリューション

SDRリクエストがタイムアウトになると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。

送信者ドメイン レピュテーションの無効なホスト

この例のログは、電子メールゲートウェイで無効なSDR サービス ホストが設定されたためにSDR に基づいてフィルタ処理されなかったメッセージが表示しています。

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Invalid host configured.
```

ソリューション

CLI で `sdradvancedconfig` コマンドを使用すると、電子メールゲートウェイを SDR サービスに接続する際に必要なパラメータを設定できます。

送信者ドメインのレピュテーションの一般的なエラー

この例のログは、不明なエラーのために SDR に基づいてフィルタ処理されなかったメッセージを表示しています。

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
 224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match ipr[none] ipr not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain
Reputation. Reason: Unknown error.
```

ソリューション

不明なエラーが発生すると、メッセージがスキャン不可としてマークされ、設定したアクションがメッセージに適用されます。

有効期限が切れた Cisco Advanced Phishing Protection クラウドサービス

この例では、Cisco Advanced Phishing Protection クラウドサービスの有効期限が切れていることが、ログ に示されています。

```
Wed May 6 11:47:45 2020 Critical: The Cisco Advanced
Phishing Protection Cloud Service has expired and is disabled. Contact
your Cisco Account Manager to renew the service and enable it.
```

解決策：シスコアカウントマネージャに連絡して、サービスを更新および有効にする必要があります。

Cisco Advanced Phishing Protection クラウドサービスの有効期限に関するリマインダ

この例では、Cisco Advanced Phishing Protection クラウドサービスが特定の日付に期限切れになることが、ログによって示されています。

```
 Fri May 8 04:50:26 2020 Info: Cisco Advanced
Phishing Protection Cloud Service expires on
2020-05-10 07:00:00. You need to contact your Cisco Account
Manager to renew the service
```

解決策：シスコアカウントマネージャに連絡してサービスを更新する必要があります。

API アクセス UID と API アクセス秘密鍵がない

この例では、API アクセス UID と API アクセス秘密鍵がないため、電子メールゲートウェイで Cisco Advanced Phishing Protection クラウドサービスの有効期限をポーリングできなかったことが、ログに示されています。

```
 Wed May 6 17:52:52 2020 Critical: Failed to poll
for the Cisco Advanced Phishing Protection Cloud Service
expiry date. You need to add the API Access UID and API Access
secret key.
```

解決策：API アクセス UID と API アクセス秘密鍵を追加する必要があります。

無効な API アカウント UID または API アクセス秘密鍵

この例では、無効な API アクセス UID や API アクセス秘密鍵が原因で、電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスの有効期限をポーリングできなかったことが、ログで示されています。

```
Wed May 6 17:52:52 2020 Critical: Failed to poll
for the Cisco Advanced Phishing Protection Cloud Service
expiry date because the API Access Key is invalid. You need
to re-configure the API Access UID and secret key
```

解決策：API アクセス UID と秘密鍵を再設定する必要があります。

配信ログの使用

配信ログには、AsyncOS の電子メール配信動作に関する重要な情報が記録されます。ログメッセージは「ステートレス」です。つまり、関連するすべての情報が各ログメッセージに記録さ

れるので、ユーザは、現在の配信試行に関する情報について前のログメッセージを参照する必要がありません。

配信ログには、受信者ごとの電子メール配信動作に関連するすべての情報が記録されます。すべての情報は、論理的にレイアウトされ、シスコが提供するユーティリティを使用して変換した後は、人による読み取りが可能になります。変換ツールは、次の場所にあります。
https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools

配信ログは、リソースの効率性を保つためにバイナリ形式で記録されて転送されます。次の表に、配信ログに記録される情報を示します。

表 *125*：配信ログの統計情報

統計	説明
配信ステータス（Delivery status）	success（メッセージは正常に配信されました）またはbounce（メッセージはハードバウンスされました）
Del_time	配信時間
Inj_time	インジェクション時間。del_time - inj_time = time 受信者メッセージがキューに留まっていた時間
Bytes	メッセージ サイズ
Mid	メッセージ ID
Ip	受信者ホスト IP。受信者メッセージを受信またはバウンスしたホストの IP アドレス
From	Envelope From（Envelope Sender または MAIL FROM としても知られます）
Source_ip	送信元ホスト IP。着信メッセージのホストの IP アドレス
コード	受信者ホストからの SMTP 応答コード
返信（Reply）	受信者ホストからの SMTP 応答メッセージ
Rcpt Rid	受信者 ID。受信者 ID は <0> から始まります。複数の受信者が指定されたメッセージには、複数の受信者 ID が付きます。
受信者（To）	エンベロープ受信者
Attempts	配信試行回数

配信ステータスが bounce であった場合は、次の追加情報が配信ログに表示されます。

表 *126* : 配信ログのバウンス情報

統計	説明
理由	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
コード	受信者ホストからの SMTP 応答コード
エラー（Error）	受信者ホストからの SMTP 応答メッセージ

ログヘッダーを設定している場合（メッセージヘッダーのロギング（1471 ページ）を参照）、ヘッダー情報は配信情報の後に表示されます。

表 *127* : 配信ログのヘッダー情報

統計	説明
顧客データ（Customer_data）	ログに記録されるヘッダーの始まりを示す XML タグ
ヘッダー名（Header Name）	ヘッダーの名前
値	ログに記録されるヘッダーの内容

配信ログ エントリの例

ここでは、さまざまな配信ログ エントリの例を示します。

正常なメッセージ配信

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

配信ステータス バウンス

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05 08:28:32.929 2003"

bytes="4074" mid="94157762" ip="0.0.0.0" from="campaign1@yourdomain.com"

source_ip="192.168.102.1 "reason="5.1.0 - Unknown address error" code="550"

error="["Requested action not taken: mailbox unavailable"]">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

ログヘッダー付きの配信ログ エントリ

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28 15:55:17.696 2003"
 bytes="139" mid="202" ip="10.1.1.13" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" code="250" reply="sent">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

バウンス ログの使用

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。次の表に、バウンス ログに記録される情報を示します。

表 *128* : バウンス ログの統計情報

統計	説明
タイムスタンプ	バウンス イベントの時刻
ログ レベル（Log level）	このバウンス ログの詳細レベル
バウンス タイプ（Bounce type）	Bounced または Delayed（ハードバウンスまたはソフトバウンスなど）
MID/RID	メッセージ ID および受信者 ID
From	エンベロープ送信者
受信者（To）	エンベロープ受信者
理由	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
応答	受信者ホストからの SMTP 応答コードおよびメッセージ

また、ログに記録するメッセージサイズを指定しているか、**ログヘッダー**を設定している（メッセージヘッダーのロギング （1471 ページ）を参照）場合、メッセージおよびヘッダー情報はバウンス情報の後に表示されます。

表 *129 :* バウンス ログのヘッダー情報

ヘッダー	ヘッダー名およびヘッダーのコンテンツ。
メッセージ（Message）	ログに記録されるメッセージのコンテンツ。

バウンス ログ エントリの例

ソフトバウンスされた受信者（バウンス タイプ = **Delayed**）

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>


Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

ハードバウンスされた受信者（バウンス タイプ = **Bounced**）

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0 From:<campaign1@yourdomain.com>
To:<user2@sampledomain.com>


Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no such active
account.'])"
```

メッセージ本文およびログヘッダー付きのバウンス ログ

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0 From:<campaign1@yourdomain.com>
To:<user@sampledomain.com>


Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers: ['xname:
userID2333']' Message: Message-Id:



<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

（注） テキスト文字列 \015\012 は、改行を表します（CRLF など）。

ステータス ログの使用

ステータス ログには、status、status detail、および dnsstatus などの CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

ステータス ログの読み取り

次の表に、ステータス ログ ラベルと、一致するシステム統計情報を示します。

表 *130 :* ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率
DskIO	Disk I/O 使用率
RAMUtil	RAM 使用率
QKUsd	使用されているキュー（キロバイト単位）
QKFre	空いているキュー（キロバイト単位）
CrtMID	メッセージ ID（MID）
CrtICID	インジェクション接続 ID（ICID）
CRTDCID	配信接続 ID（DCID）
InjBytes	インジェクトされたメッセージの合計サイズ（バイト単位）
InjMsg	インジェクトされたメッセージ
InjRcp	インジェクトされた受信者
GenBncRcp	生成されたバウンス受信者
RejRcp	拒否された受信者
DrpMsg	ドロップされたメッセージ
SftBncEvnt	ソフト バウンスされたイベント
CmpRcp	完了した受信者
HrdBncRcp	ハード バウンスされた受信者
DnsHrdBnc	DNS ハード バウンス
5XXHrdBnc	5XX ハード バウンス
FltrHrdBnc	フィルタ ハード バウンス
ExpHrdBnc	期限切れハード バウンス
OtrHrdBnc	その他のハード バウンス
DlvRcp	配信された受信者

統計	説明
DelRcp	削除された受信者
GlbUnsbHt	グローバル配信停止リストとの一致数
ActvRcp	アクティブ受信者
UnatmptRcp	未試行受信者
AtmptRcp	試行受信者
CrtCncIn	現在の着信接続
CrtCncOut	現在の発信接続
DnsReq	DNS 要求
NetReq	ネットワーク要求
CchHit	キャッシュ ヒット
CchMis	キャッシュ ミス
CchEct	キャッシュ例外
CchExp	キャッシュ期限切れ
CPUTTm	アプリケーションが使用した合計 CPU 時間
CPUETm	アプリケーションが開始されてからの経過時間
MaxIO	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作
RamUsd	割り当て済みのメモリ（バイト単位）
SwIn	スワップインされたメモリ。
SwOut	スワップアウトされたメモリ。
SwPgIn	ページインされたメモリ。
SwPgOut	ページアウトされたメモリ。
MMLen	システム内の合計メッセージ数
DstInMem	メモリ内の宛先オブジェクト数
ResCon	リソース保持の tarpit 値（大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します）
WorkQ	ワーク キューにある現在のメッセージ数

統計	説明
QuarMsgs	ポリシー、ウイルス、および Outbreak 隔離にある個々のメッセージ数（複数の隔離エリアに存在するメッセージは一度だけカウントされます）
QuarQKUsd	ポリシー、ウイルス、および Outbreak 隔離メッセージによって使用されるキロバイト
LogUsd	使用されるログ パーティションの割合
SophLd	Sophos アンチウイルススキャンで使用される CPU の割合
McafLd	McAfee アンチウイルス スキャンで使用される CPU の割合
CASELd	CASE スキャンで使用される CPU の割合
TotalLd	CPU の合計消費量
LogAvail	ログ ファイルに使用できるディスク スペース
EuQ	スパム隔離内の推定メッセージ数
EuqRls	スパム隔離解放キュー内の推定メッセージ数
RptLD	レポートの処理中の CPU 負荷
QtnLd	隔離処理中の CPU 負荷
EncrQ	暗号化のキュー内のメッセージ

ステータス ログの例

```
Fri Feb 28 12:11:48 2020 Info: Status: CPULd 45 DskIO 22 RAMUtil 22 QKUsd 6676975
QKFre 1711633 CrtMID 6130195 CrtICID 722770 CrtDCID 54 InjMsg 4572789 InjRcp
4575323 GenBncRcp 255536 RejRcp 20388 DrpMsg 469642 SftBncEvnt 0 CmpRcp 3650806 HrdBncRcp
 255536
DnsHrdBnc 23 5XXHrdBnc 28 FltrHrdBnc 255485 ExpHrdBnc 0
OtrHrdBnc 0 DlvRcp 3394965 DelRcp 305 GlbUnsbHt 0 ActvRcp 65 UnatmptRcp 65 AtmptRcp 0
CrtCncIn 9
CrtCncOut 0 DnsReq 7756744 NetReq 7769130 CchHit 8373490 CchMis
1989637 CchEct 1625236 CchExp 1569329 CPUTTm 37 CPUETm 62 MaxIO 465600 RAMUsd 1473355956
 MMLen 54782
DstInMem 11 ResCon 0 WorkQ 54710 QuarMsgs 375
QuarQKUsd 145096 LogUsd 26 SophLd 15 BMLd 0 CASELd 0 TotalLd 100 LogAvail 116G EuQ 64
EuqRls 0 CmrkLd 0
McafLd 9 SwIn 122 SwOut 5295 SwPgIn 368 SwPg Out 63639
SwapUsage 4% RptLd 0 QtnLd 19 EncrQ 0 InjBytes 516664777890
```

ドメイン デバッグ ログの使用

ドメインデバッグログには、電子メールゲートウェイと指定の受信者ホスト間のSMTP会話でのクライアントとサーバの通信が記録されます。このログタイプは主に、特定の受信者ホストに関する問題のデバッグに使用されます。

表 *131*: ドメイン デバッグ ログの統計情報

統計	説明
タイムスタンプ	バウンス イベントの時刻
ログ レベル（Log level）	このバウンス ログの詳細レベル
From	エンベロープ送信者
受信者（To）	エンベロープ受信者
理由	配信時の SMTP 応答に対する RFC 1893 Enhanced Mail Status Code の解釈
応答	受信者ホストからの SMTP 応答コードおよびメッセージ

ドメイン デバッグ ログの例

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END WITH "." ON A
LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

インジェクション デバッグ ログの使用

インジェクション デバッグ ログには、電子メールゲートウェイと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントと電子メールゲートウェイ間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、接続ホストに「送信」または接続ホストから「受信」に分類されます。

記録するホストの会話を指定するには、IP アドレス、IP 範囲、ホスト名、または部分ホスト名を指定する必要があります。IP 範囲内で接続している IP アドレスがすべて記録されます。部分ドメイン内のホストがすべて記録されます。システムは、接続している IP アドレスに対してリバース DNS ルックアップを実行して、ホスト名に変換します。DNS に対応する PTR レコードがない IP アドレスは、ホスト名に一致しません。

記録するセッション数も指定する必要があります。

インジェクション デバッグ ログ内の各行には、次の表に示す情報が含まれます。

表 *132*：インジェクション デバッグ ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
ICID	インジェクション接続 ID は、別のログ サブスクリプションで同じ接続に関連付けることができる固有識別子です。
Sent/Received	「Sent to」と記された行は、接続ホストに送信された実際のバイトです。「Rcvd from」と記された行は、接続ホストから受信した実際のバイトです。
[IPアドレス（IP Address）]	接続ホストの IP アドレス。

インジェクション デバッグ ログの例

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220 postman.example.com
ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
<recipient@example.com> ok\015\012'
Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go ahead\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject: Test
Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the content of the
message'
Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
```

```
postman.example.com\015\012'
```

システム ログの使用

表 *133 :* システム ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	ログに記録されたイベント。

システム ログの例

次のシステム ログの例は、commit を実行したユーザの名前と入力されたコメントを含む、いくつかの commit エントリを示しています。

```
Wed Sep 8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:02:45 2004 Info: System is coming up

Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password

Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW

Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples

Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

CLI 監査ログの使用

表 *134 : CLI* 監査ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
メッセージ	メッセージは、入力された CLI コマンド、CLI 出力（メニュー、リストなど）、および表示されるプロンプトで構成されます。

CLI 監査ログの例

次の CLI 監査ログの例は、who および textconfig CLI コマンドが入力された PID 16434 の情報を示しています。

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '


Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n======== ========== =========
=========== ====\nadmin Wed 11AM 3m 45s 10.1.3.14 tail\nadmin 02:32PM
0s 10.1.3.14 cli\nmail3.example.com> '


Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]>
'
```

FTP サーバ ログの使用

表 *135 : FTP* サーバ ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
ID	接続 ID。FTP 接続ごとの別個の ID
メッセージ	ログ エントリのメッセージ セクションは、ログファイル ステータス情報、または FTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

FTP サーバ ログの例

次の FTP サーバ ログの例には、接続（ID:1）が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```
Wed Sep 8 18:03:06 2004 Info: Begin Logfile

Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21

Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
```

```
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

HTTP ログの使用

表 *136 : HTTP* ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
ID	セッション ID
申請	接続マシンの IP アドレス
ユーザー	接続ユーザのユーザ名
メッセージ	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

HTTP ログの例

次の HTTP ログの例は、管理者ユーザと GUI の対話（システム設定ウィザードの実行など）を示しています。

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port
443

Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303

Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200

Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=19
0 HTTP/1.1 200

Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

NTP ログの使用

表 *137 : NTP* ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、サーバへの簡易ネットワーク タイムプロトコル（SNTP）クエリーまたは adjust: メッセージで構成されます。

NTP ログの例

次の NTP ログの例は、電子メールゲートウェイから NTP ホストへの 2 度のポーリングを示しています。

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652

Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096

Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152

Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

スキャン ログの使用

スキャンログには、電子メールゲートウェイのスキャンエンジンのすべての LOG および COMMON メッセージが含まれています。使用可能な COMMON および LOG アラート メッセージのリストについては、「システム管理」の章の「アラート」を参照してください。

表 *138 :* スキャン ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、いずれかのスキャン エンジンのアプリケーションの障害、送信されたアラート、失敗したアラート、またはログエラーメッセージで構成されています。

スキャン ログの例

次のログの例は、Sophosアンチウイルスに関する警告アラートを送信している電子メールゲートウェイの履歴を示しています。

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...' (attempt #0).


Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to
```

```
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...'.


Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com
with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
database on this system is...".
```

アンチスパム ログの使用

表 *139* : アンチスパム ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、アンチスパムアップデートの確認と結果（エンジンまたはアンチスパムルールのアップデートが必要であったかどうかなど）で構成されます。

アンチスパム ログの例

次のアンチスパム ログの例は、アンチスパム エンジンによる、スパム定義のアップデートおよび CASE アップデートの確認を示しています。

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) : case-daemon: server
successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) : startup: Region profile:
Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy: Fuzzy plugin v7
successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) : uribllocal: running URI
blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config: Finished loading
configuration
```

グレイメール ログの使用

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージには、グレイメールエンジン、ステータス、設定などの情報が含まれます。

グレイメール ログの例

```
Tue Mar 24 08:56:45 2015 Info: graymail [BASE] Logging at DEBUG level

Tue Mar 24 08:56:45 2015 Info: graymail [HANDLER] Initializing request handler

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Loaded graymail scanner library

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Created graymail scanner instance

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Debug mode disabled on graymail process


Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Starting thread WorkerThread_0
```

アンチウイルス ログの使用

表 *140* : アンチウイルス ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、アンチウイルス アップデートの確認と結果（エンジンまたはウイルス定義のアップデートが必要であったかどうかなど）で構成されます。

アンチウイルス ログの例

次のアンチウイルス ログの例は、Sophosアンチウイルスエンジンによる、ウイルス定義（IDE）とエンジン自体のアップデートの確認を示しています。

```
Thu Sep 9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep 9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine update needed

Thu Sep 9 14:18:04 2004 Info: Current IDE serial=2004090902. No update needed.
```

このログを一時的にDEBUGレベルに設定すると、アンチウイルスエンジンが所定のメッセージについて特定の判定を返した理由を診断するのに役立ちます。DEBUG ロギング情報は冗長です。使用の際は注意してください。

AMP エンジン ログの使用

AMP エンジン ログには、次の詳細が含まれます。

- ファイル レピュテーション サーバに送信されたファイル レピュテーション クエリーと、ファイル レピュテーション サーバから受信された応答。
- ファイル分析（ファイル分析サーバにファイルがアップロードされている場合）。ファイル分析の状態は、ファイル分析サーバから応答が受信されるまで定期的に記録されます。

AMP エンジン ログ エントリの例

次に特定のシナリオに基づく AMP エンジン ログ エントリの例を示します。

- ファイル レピュテーションとファイル分析サーバの初期化 （1437 ページ）
- ファイル レピュテーション サーバが未構成 （1437 ページ）
- ファイル レピュテーション クエリーの初期化 （1437 ページ）
- ファイル レピュテーション サーバからファイル レピュテーション クエリーに対して受信した応答 （1438 ページ）
- 分析のためのファイル アップロードとファイル分析プロセス （1439 ページ）
- ファイルが分析用にアップロードされない （1440 ページ）
- ファイル アップロード制限が原因でファイル分析がスキップされたファイル アップロード （1441 ページ）
- ファイル分析サーバのエラーが原因でファイル分析がスキップされたファイルアップロード （1441 ページ）
- 受信したファイル レトロスペクティブ判定 （1442 ページ）

ファイル レピュテーションとファイル分析サーバの初期化

```
Wed Oct 5 15:17:31 2016 Info: File reputation service initialized successfully
Wed Oct 5 15:17:31 2016 Info: The following file type(s) can be sent for File Analysis:
 Microsoft Windows / DOS Executable, Microsoft Office 97-2004 (OLE), Microsoft Office
2007+ (Open XML), Other potentially malicious file types, Adobe Portable Document Format
 (PDF). To allow analysis of new file type(s), go to Security Services > File Reputation
 and Analysis.
Wed Oct 5 15:17:31 2016 Info: File Analysis service initialized successfully
```

ファイル レピュテーション サーバが未構成

```
Tue Oct 4 23:15:24 2016 Warning: MID 12 reputation query failed for attachment
'Zombies.pdf' with error "Cloud query failed"
```

ファイル レピュテーション クエリーの初期化

```
Fri Oct 7 09:44:04 2016 Info: File reputation query initiating. File Name = 'mod-6.exe',
 MID = 5, File Size = 1673216 bytes,
File Type = application/x-dosexec
```

統計	説明
ファイル名（File Name）	SHA-256 ハッシュ ID がファイル レピュテーション サーバに送信されるファイルの名前。 ファイル名が使用できない場合、ファイル名が不明であると表現します。
MID	電子メールパイプラインを通過するメッセージの追跡に使用されるメッセージ ID。

統計	説明
ファイル サイズ（File size）	SHA-256 ハッシュ識別子がファイル レピュテーション サーバに送信されるファイルのサイズ。
ファイル タイプ（File Type）	SHA-256 ハッシュ識別子がファイル レピュテーション サーバに送信されるファイルのタイプ。 次のファイル タイプがサポートされています。 • Microsoft Windows / DOS Executable • Microsoft Office 97-2004（OLE） • Microsoft Office 2007+（Open XML） • その他の悪意がある可能性のあるファイル タイプ • Adobe Portable Document Format（PDF）

ファイル レピュテーション サーバからファイル レピュテーション クエリーに対して受信した応答

```
Fri Oct 7 09:44:06 2016 Info: Response received for file reputation query from Cloud.
File
Name = 'mod-6.exe', MID = 5, Disposition = MALICIOUS, Malware = W32.061DEF69B5-100.SBX.TG,
Reputation Score = 73, sha256 =
061def69b5c100e9979610fa5675bd19258b19a7ff538b5c2d230b467c312f19, upload_action = 2
```

統計	説明
ファイル名（File Name）	SHA-256 ハッシュ ID がファイル レピュテーション サーバに送信されるファイルの名前。 ファイル名が使用できない場合、ファイル名が不明であると表現します。
MID	電子メール パイプラインを通過するメッセージの追跡に使用されるメッセージ ID。
傾向（Disposition）	ファイル レピュテーション傾向値は次のとおりです。 • MALICIOUS • CLEAN • FILE UNKNOWN：レピュテーション スコアがゼロの場合。 • VERDICT UNKNOWN：傾向が FILE UNKNOWN でありスコアが非ゼロの場合。 • LOW RISK：ファイル分析の後でファイルに動的なコンテンツが見つからない場合、判定は「LOW RISK」です。ファイル分析用にファイルは送信されず、メッセージは電子メール パイプラインを通過します。
マルウェア（Malware）	マルウェア脅威の名前。

統計	説明
レピュテーション スコア（Reputation score）	ファイル レピュテーション サーバによってファイルに割り当てられるレピュテーション スコア。 ファイル傾向が **VERDICT UNKNOWN** の場合、電子メールゲートウェイはファイルレピュテーション判定を、レピュテーションスコアとしきい値に基づいて調整します。
アップロード アクション（Upload Action）	特定のファイルに実行される、ファイル レピュテーション サーバによって推奨されるアップロード アクションの値： • 0：アップロード用に送信する必要はありません。 • 1：アップロード用にファイルを送信します。 （注） 電子メールゲートウェイはアップロードアクションの値が「1」の場合にファイルをアップロードします。 • 2：アップロード用にファイルを送信しません。 • 3：アップロード用にメタデータのみを送信します。

分析のためのファイル アップロードとファイル分析プロセス

```
Wed Sep 28 11:31:58 2016 Info: File uploaded for analysis. SHA256:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b9133001172418 00f0ea

Wed Sep 28 11:36:58 2016 Info: File Analysis is running for SHA:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b9133001172418 00f0ea

Fri Oct 7 07:39:13 2016 Info: File Analysis complete. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Submit Timestamp:
1475825466, Update Timestamp: 1475825953, Disposition: 3 Score: 100, run_id: 194926004
Details: Analysis is completed for the File
SHA256[16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc]
Spyname:[W32.16454AFF50-100.SBX.TG]
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。
送信タイムスタンプ（Submit Timestamp）	電子メールゲートウェイによってファイルがファイル分析サーバにアップロードされた日付と時刻。
更新タイムスタンプ（Update Timestamp）	ファイルに対するファイル分析が完了した日付と時刻
傾向（Disposition）	ファイル レピュテーションの判定結果で、次の値があります。 • 1 - マルウェアの検出なし • 2 - 正常 • 3 - マルウェア

統計	説明
スコア（Score）	ファイル分析サーバによってファイルに割り当てられる分析スコア。
実行 ID（Run ID）	ファイル分析サーバが特定のファイル分析についてファイルに割り当てる数値（ID）。
詳細（Details）	ファイル分析中にエラーが報告された場合は追加情報。そうでない場合は、ファイルに対する最終的な分析が完了していることを示します。
スパイ名（Spy Name）	ファイル分析中にファイル内にマルウェアが見つかった場合は、脅威の名前。

ファイルが分析用にアップロードされない

```
Wed Sep 14 12:27:52 2016 Info: File not uploaded for analysis. MID = 0 File
SHA256[a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82] file
mime[text/plain] Reason: No active/dynamic contents exists
```

統計	説明
MID	電子メール パイプラインを通過するメッセージの追跡に使用されるメッセージ ID。
ファイル MIME（File MIME）	ファイルの MIME タイプ。
理由	以下に示すのは、upload_action が '1' に設定されている場合でも、ファイルがファイル分析サーバにアップロードされない理由の値の 1 つです。 • 別のノードでファイルがすでにアップロードされている：ファイルはすでに別の電子メールゲートウェイを介してファイル分析サーバにアップロードされています。 • ファイル分析が進行中：ファイルは進行中のアップロードのためにすでに選択されています。 • ファイルはファイル分析サーバにすでにアップロード済み • サポート対象のファイル タイプではない • ファイル サイズが範囲外：アップロード ファイルのサイズがファイル分析サーバによって設定されているしきい値を超えています。 • アップロード キューが満杯であった • ファイル分析サーバのエラー • アクティブなコンテンツまたは動的コンテンツが存在していない • 一般または不明エラー

ファイル アップロード制限が原因でファイル分析がスキップされたファイル アップロード

```
Tue Jun 20 13:22:56 2017 Info: File analysis upload skipped. SHA256:
b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef,Timestamp[1454782976]
details[File SHA256[b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef]
file
mime[application/pdf], upload priority[Low] not uploaded, re-tries[3], backoff[986]
discarding ...]
Tue Jun 20 13:22:56 2017 Critical: The attachment could not be uploaded to the
File Analysis server because the appliance exceeded the upload limit
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。
Timestamp	ファイル分析サーバへのファイルのアップロードが失敗した日付と時刻。
詳細（Details）	ファイル分析サーバのエラーの詳細。
ファイル MIME（File MIME）	ファイルの MIME タイプ。
アップロード優先順位（Upload priority）	[アップロード優先順位（Upload priority）] の値は以下のとおりです。 • [高（High）] - PDF ファイル タイプを除くすべての選択されたファイル タイプの場合。 • [低（Low）] - PDF ファイル タイプのみの場合。
再試行回数（Re-tries）	当該のファイルに対して実行されたアップロード試行の回数。 （注） 1ファイルに対し、最大3回までアップロードを試行できます。
バックオフ（x）（Backoff (x)）	電子メールゲートウェイがファイル分析サーバにファイルをアップロードしようとする前に待機する必要がある秒数（x）。これは、電子メールゲートウェイが 1 日あたりのアップロード制限に達したときに発生します。
重要（理由）（Critical (Reason)）	電子メールゲートウェイがアップロード制限を超えたため、ファイル分析サーバに添付ファイルをアップロードできませんでした。

ファイル分析サーバのエラーが原因でファイル分析がスキップされたファイル アップロード

```
Sat Feb 6 13:22:56 2016 Info:SHA256:
69e17e213732da0d0cbc48ae7030a4a18e0c1289f510e8b139945787f67692a5,Timestamp[1454959409]
details[Server Response HTTP code:[502]]
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。

統計	説明
Timestamp	ファイル分析サーバへのファイルのアップロードが試行された日付と時刻。
詳細（Details）	ファイル分析サーバのエラーに関する情報。

受信したファイル レトロスペクティブ判定

```
Fri Oct 7 07:39:13 2016 Info: Retrospective verdict received. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Timestamp: 1475832815.7,
Verdict: MALICIOUS, Reputation Score: 0, Spyname: W32.16454AFF50-100.SBX.
```

統計	説明
SHA256	対応するファイルの SHA-256 ハッシュ ID。
Timestamp	ファイル分析サーバからファイルのレトロスペクティブな判定を受信した日時。
判定	ファイルのレトロスペクティブな判定の値は「悪意のある」または「正常」です。
Reputation Score	ファイル レピュテーション サーバによってファイルに割り当てられるレピュテーション スコア。
Spyname	ファイル分析中にファイル内にマルウェアが見つかった場合は、脅威の名前。

スパム隔離ログの使用

表 *141* : スパム ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、実行されたアクション（メッセージの隔離、隔離エリアからの解放など）で構成されます。

スパム隔離ログの例

次のログの例は、隔離から admin@example.com にメッセージ（MID 8298624）が解放されていることを示しています。

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work
queue)
```

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

スパム隔離 GUI ログの使用

表 *142 :* スパム *GUI* ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	メッセージは、ユーザ認証などの実行されたアクションで構成されます。

スパム隔離 GUI ログの例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82

Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228

Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

LDAP デバッグ ログの使用

表 *143 : LDAP* デバッグ ログの統計情報

統計	説明
タイムスタンプ	バイトが転送された時刻
メッセージ	LDAP デバッグ メッセージ。

LDAP デバッグ ログの例

（注） ログ ファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

1	Thu Sep 9 12:24:56 2004 Begin Logfile
2	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
3	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
4	Thu Sep 9 12:25:02 2004 LDAP: Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa
5	Thu Sep 9 12:28:08 2004 LDAP: Clearing LDAP cache
6	Thu Sep 9 13:00:09 2004 LDAP: Query '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun (sun.qa:389)
7	Thu Sep 9 13:00:09 2004 LDAP: After substitute, query is '(&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa))'
8	Thu Sep 9 13:00:09 2004 LDAP: connecting to server
9	Thu Sep 9 13:00:09 2004 LDAP: connected
10	Thu Sep 9 13:00:09 2004 LDAP: Query (&(ObjectClass=inetLocalMailRecipient) (mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa)) returned 1 results
11	Thu Sep 9 13:00:09 2004 LDAP: returning: [<LDAP:>]

前述のログ ファイルを読み取るためのガイドとして、使用してください。

表 *144 : LDAP* デバッグ ログの例の詳細

行番号	説明
1	ログ ファイルが開始されます。

行番号	説明
2 3 4	リスナーは、明確に「sun.masquerade」というLDAPクエリーによって、マスカレードにLDAPを使用するように設定されています。 アドレスemployee@routing.qaがLDAPサーバで検索され、一致が検出されます。その結果のマスカレードアドレスはemployee@mail.qaであり、マスカレードの設定によってこのアドレスがメッセージヘッダー、エンベロープ送信者、またはその両方に書き込まれます。
5	ユーザは手動でldapflushを実行しています。
6	クエリーは、sun.qa、ポート389に送信されます。クエリーテンプレートは(&(ObjectClass={g})(mailLocalAddress={a}))です。 {g}は、発信側フィルタ（rcpt-to-groupまたはmail-from-groupルール）で指定されたグループ名に置換されます。 {a}は、当該のアドレスに置換されます。
7	ここで代入（前述のとおり）が実行されます。LDAPサーバに送信される前のクエリーはこのようになります。
8	サーバへの接続がまだ確立されていないので、接続します。
9	サーバに送信されるデータです。
10	結果は、確実に空になります。つまり、1つのレコードが返されますが、クエリーはフィールドを要求していないので、データは報告されません。これらは、データベースに一致があるかどうかをクエリーでチェックするときに、グループ クエリーとアクセプト クエリーの両方に使用されます。

セーフリスト/ブロックリスト ログの使用

次の表に、セーフリスト/ブロックリスト ログに記録される統計情報を示します。

表 *145*：セーフリスト/ブロックリスト ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

セーフリスト/ブロックリスト ログの例

次のセーフリスト/ブロックリストログの例は、電子メールゲートウェイによって 2 時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC:
10800 seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.


Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.

.........................

Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

レポーティング ログの使用

次の表は、レポート ログに記録された統計情報を示しています。

表 *146 :* レポーティング ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング ログの例

次のレポーティングログの例は、情報ログレベルに設定された電子メールゲートウェイを示しています。

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
```

```
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692

Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds

Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41

Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692

Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

レポーティング クエリー ログの使用

次の表に、レポーティング クエリー ログに記録される統計情報を示します。

表 *147*: レポーティング クエリー ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

レポーティング クエリー ログの例

次のレポーティングクエリログの例は、電子メールゲートウェイによって、2007 年 8 月 29 日から 10 月 10 日までの期間で毎日の発信メールトラフィッククエリが実行されていることを示しています。

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENT_FILTER',
```

```
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_PROCESSED'] for rollup period "day" with
 interval range 2007-08-29 to 2007-10-01
with key constraints

None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval
 range 2007-08-29 to
2007-10-01 with key constraints None sorting on
['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

アップデータ ログの使用

表 *148 :* アップデータ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、システム サービス アップデート情報のほか、AsyncOS によるアップデートの確認と、スケジュールされている次回アップデートの日時で構成されます。

アップデータ ログの例

次のログの例は、電子メールゲートウェイが新規の McAfee アンチウイルス定義でアップデートされていることを示しています。

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update 11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for mcafee

Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:12:52
2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files
```

```
Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"

Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:17:52
2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:22:52
2008
```

アップデータ ログの例

この例では、ログは、無効にされている自動更新、Sophos Anti-virus 定義に適用されているバックアップを表示します。

```
Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Debug: postx updates disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Trace: command session starting

Fri Mar 10 15:05:55 2017 Info: Automatic updates disabled for engine Sophos engine

Fri Mar 10 15:05:55 2017 Info: Sophos: Backup update applied successfully

Fri Mar 10 15:05:55 2017 Info: Internal SMTP system attempting to send a message to
abshastr@ironport.com
with subject ‘Automatic updates are now disabled for sophos’ attempt #0).

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “amp”

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled
```

トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログ メッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキングログは、メッセージトラッキングデータベースを作成するため、電子メールゲートウェイのメッセージ トラッキング コンポーネントで使用されます。ログ ファイルはデータベースの作成プロセスで消費されるので、トラッキング ログは一過性のものになります。トラッキング ログの情報は、人による読み取りや解析を目的とした設計になっていません。

Cisco Secure Manager Email and Web Gateway を使用することで、複数の電子メールゲートウェイからのトラッキング情報の表示もできます。

認証ログの使用

認証ログには、成功したユーザ ログインと失敗したログイン試行が記録されます。

表 *149 :* 認証ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、電子メールゲートウェイにログインしようとしたユーザのユーザ名、ユーザ権限ロールの詳細（「admin」、「operator」など）、およびそのユーザが正常に認証されたかどうかという情報で構成されます。

認証ログの例

次のログの例は、「admin」、「joe」、および「dan」というユーザによるログイン試行を示しています。

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX

Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

正しくないパスコードが原因の二要素認証ログイン失敗の例

次の例では、入力された不正なパスコードのために2要素認証ログインが失敗したことがログに示されています。

```
Thu Mar 16 05:47:47 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:48:18 2017 Info: Two-Factor RADIUS Authentication failed.
```

```
Thu Mar 16 05:48:48 2017 Info: An authentication attempt by the user **** from
21.101.210.150 failed
```

タイムアウトが原因の二要素認証ログイン失敗の例

この例では、ログはタイムアウトに起因する二要素認証ログインの失敗を示しています。

```
Thu Mar 16 05:46:04 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:46:59 2017 Info: RADIUS server example.cisco.com communication error. No
valid responses from server (timeout).

Thu Mar 16 05:46:59 2017 Info: Two-Factor Authentication RADIUS servers timed out.
Authentication could fail due to this.
```

二要素認証のログインの成功例

次の例では、2 要素認証のログインが成功したことがログに表示されています。

```
Thu Mar 16 05:49:05 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:49:05 2017 Info: Two-Factor RADIUS Authentication was successful.

Thu Mar 16 05:49:05 2017 Info: The user admin successfully logged on from 21.101.210.150

with privilege admin using an HTTPS connection.
```

コンフィギュレーション履歴ログの使用

コンフィギュレーション履歴ログは、ユーザの名前、ユーザが変更を行った設定の場所の説明、および変更を保存するときにユーザが入力したコメントがリストされた追加のセクションを持つコンフィギュレーションファイルで構成されます。ユーザが変更を保存するたびに、変更後のコンフィギュレーション ファイルを含む新しいログが作成されます。

コンフィギュレーション履歴ログの例

次の設定履歴ログの例は、システムへのログインを許可されているローカルユーザを定義するテーブルにユーザ（admin）がゲスト ユーザを追加したことを示しています。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<!--

XML generated by configuration change.

Change comment: added guest user

User: admin

Configuration are described as:

This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160
```

```
Version: 6.7.0-231

Serial Number: 000000000ABC-D000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time
Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"

Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>
```

外部脅威フィードのエンジン ログの使用

ETF ログには、ETF エンジン、ステータス、設定などに関する情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

外部脅威フィードのエンジン ログの例

```
Thu Jun 7 04:54:15 2018 Info: THREAT_FEEDS: Job failed with exception: Invalid URL or
Port Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source:
 S1
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
 domain: s1.co, collection: sss
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: Observables are being fetched from the source:
 S1 between 2018-06-07 04:34:13+00:00 and 2018-06-07 05:04:13.185909+00:00
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: 21 observables were fetched from the source:
 S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source:
S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
 domain: s1.co, collection: sss
```

ETF ソース設定の失敗 - 無効なコレクション名

この例では、無効なコレクション名が原因で、電子メールゲートウェイが外部脅威フィードソースから脅威フィードを取得できなかったことがログに示されています。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com, cause of failure: Invalid Collection name
```

ソリューション

Web インターフェイスの [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページに移動するか、CLI で `threatfeedsconfig > sourceconfig`

サブコマンドを使用して、設定した外部脅威フィードソースの正確なコレクション名を入力します。

ETF ソース設定の失敗 - HTTP エラー

この例では、HTTP エラーが原因で、電子メールゲートウェイが外部脅威フィードソースから脅威フィードを取得できなかったことがログに示されています。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

ソリューション

Web インターフェイスの [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページに移動するか、CLI で `threatfeedsconfig > sourceconfig` サブコマンドを使用して、設定した外部脅威フィード ソースの正確なポーリング パスまたはユーザ認証クレデンシャルを入力します。

ETF ソース設定の失敗 - 無効な URL

この例では、無効な URL が原因で、電子メールゲートウェイが外部脅威フィードソースから脅威フィードを取得できなかったことがログに示されています。

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

ソリューション

Web インターフェイスの [メールポリシー（Mail Policies）] > [外部脅威フィードマネージャ（External Threat Feeds Manager）] ページに移動するか、CLI で `threatfeedsconfig > sourceconfig` サブコマンドを使用して、設定した外部脅威フィードソースの正確なホスト名またはポート番号を入力します。

統合イベント ログの使用

ログ タイプを統合イベント ログとしてログ サブスクリプションを設定する場合、ログ出力の 1 行に特定のメッセージ属性を含めるには、[ログフィールド（Log Fields）] オプションを使用します。

ログタイプが統合イベントログのログサブスクリプションを設定すると、次のログフィールドがデフォルトで選択されます。

- ICID
- DCID
- シリアル番号
- MID

（注） [選択されたログフィールド（Selected Log Fields）] リストからはデフォルトのログフィールドを削除できません。

統合イベント ログの例

この例のログには、ログ タイプが統合イベント ログのログ サブスクリプションを設定するときに選択された使用可能なすべてのフィールドが表示されます。

```
Thu Mar 18 08:04:50 2021: CEF:0|Cisco|C100V Email Security Virtual Appliance|14.0.0-657
|ESA_CONSOLIDATED_LOG_EVENT|Consolidated Log
Event|5|deviceExternalId=42127C7DDEE76852677B-F80CE8074CD3
ESAMID=1053 ESAICID=134 ESAAMPVerdict=UNKNOWN ESAASVerdict=NEGATIVE ESAAVVerdict=NEGATIVE

ESACFVerdict=MATCH endTime=Thu Mar 18 08:04:46 2021 ESADLPVerdict=NOT_EVALUATED
dvc=10.10.193.13 ESAAttachmentDetails={'test.txt': {'AMP': {'Verdict': 'FILE UNKNOWN',
'fileHash': '7f843d263304fb0516d6210e9de4fa7f01f2f623074aab6e3ee7051f7b785cfa'},
'BodyScanner':
{'fsize': 10059}}} ESAFriendlyFrom=test@esa.com ESAGMVerdict=NEGATIVE startTime=Thu Mar
 18 08:04:29 2021
deviceInboundInterface=Incomingmail deviceDirection=0 ESAMailFlowPolicy=ACCEPT
suser=test@esa.com
cs1Label=MailPolicy cs1=DEFAULT ESAMFVerdict=NOT_EVALUATED act=QUARANTINED
ESAFinalActionDetails=To POLICY
cs4Label=ExternalMsgID cs4='<20210318070601.40490.18684@mail1.example.com>'
ESAMsgSize=11873 ESAOFVerdict=POSITIVE
duser=9076@testing.com ESAHeloIP=10.11.1.2 cfp1Label=SBRSScore cfp1=None ESASDRDomainAge=27
 years 2 months 15 days
cs3Label=SDRThreatCategory cs3=N/A cs6Label=SDRRepScore cs6=Weak ESASPFVerdict={'mailfrom':
 {'result': 'None',
'sender': 'test@esa.com'}, 'helo': {'result': 'None', 'sender': 'postmaster'}, 'pra':
{'result': 'None', 'sender':
'test@esa.com'}} sourceHostName=unknown ESASenderGroup=UNKNOWNLIST sourceAddress=10.11.1.2
 msg='Testing'
```

ログ フィールド	CEF フィールド名	CEF フィールド値
プレフィックス フィールド		

ログ フィールド	CEF フィールド名	CEF フィールド値
	CEF形式のバージョン（CEF format version）	例：0
	アプライアンスベンダー（Appliance vendor）	例：Cisco
	アプライアンス製品（Appliance product）	例：C100V Email Security Virtual Appliance
	アプライアンスのバージョン（Appliance version）	例：13.0.0-234
	イベントクラスID（Event Class ID）	例：ESA_CONSOLIDATED_LOG_EVENT
	イベント名（Event Name）	例：Consolidated Log Event
	重大度	例：5
GUI フィールド		
シリアル番号（Serial Number）	deviceExternalId	例：42156AC79142E979C5CD-02DE6639E9C
ICIDタイムスタンプ（ICID Timestamp）	startTime	例：Mon Jul 29 11:22:22 2019
ICID	ESAICID	例：199
リスナー名（Listener Name）	deviceInboundInterface（着信メールの場合） deviceOutboundInterface（送信メールの場合）	例：Inbound 例：Outbound
送信者IP（Sender IP）	sourceAddress	例：10.10.2.75
送信者ドメイン（Sender Domain）	sourceHostName	例：demo.cisco.com
メールの方向（Mail Direction）	deviceDirection	例：0 0：着信 1：発信
メールの言語（Mail Language）	cs5	例： cs5Label=ESAMsgLanguage cs5=English

ログ フィールド	CEF フィールド名	CEF フィールド値
SBRS スコア（SBRS Score）	cfp1	例：cfp1Label=SBRSScore, cfp1=1.1
Data IP	dvc	例：10.10.2.75
メール送信者の地理的位置（Mail Sender Geo Location）	cs2	例：cs2Label=GeoLocation cs2=India
大きすぎる送信者からのメッセージ（Message Too Big from Sender）	ESAMsgTooBigFromSender	例：true 可能な値： true/false
レート制限IP（Rate Limited IP）	ESARateLimitedIP	例：10.10.2.75
メールポリシー名（Mail Policy Name）	cs1	例：cs1Label=MailPolicy cs1=default
メール フローポリシー名（Mail Flow Policy Name）	ESAMailFlowPolicy	例：ACCEPT
送信者グループ名（Sender Group Name）	ESASenderGroup	例：UNKNOWNLIST
DHA IP	ESADHASource	例：10.10.2.75
受信者（Recipients）	duser	例：demo@test.com
リモートIP/Heloドメイン IP（Remote IP/Helo Domain IP）	ESAHeloIP	例：10.10.2.75
リモートホスト/Heloドメイン（Remote Host/ Helo Domain）	ESAHeloDomain	例：test.com
TLS発信接続ステータス（TLS Outgoing Connection Status）	ESATLSOutConnStatus	例：Success 可能な値： Success/Failure
TLS発信プロトコル（TLS Outgoing Protocol）	ESATLSOutProtocol	例：TLSv1.2
TLS発信暗号（TLS Outgoing Cipher）	ESATLSOutCipher	例：ECDHE-RSA-AES128-GCM-SHA256

ログ フィールド	CEF フィールド名	CEF フィールド値
TLS着信接続ステータス（TLS Incoming Connection Status）	ESATLSInConnStatus	例：Success 可能な値： Success/Failure
TLS着信プロトコル（TLS Incoming Protocol）	ESATLSInProtocol	例：TLSv1.2
TLS着信暗号（TLS Incoming Cipher）	ESATLSInCipher	例： ECDHE-RSA-AES128-GCM-SHA256
DMARC判定（DMARC Verdict）	ESADMARCVerdict	例：Success 可能な値： PermFailure/TempFailure/ Reject/Success
DKIM判定（DKIM Verdict）	ESADKIMVerdict	例：Pass 可能な値： Pass/Neutral/TempError/ PermError/HardFail/None
SPF判定（SPF Verdict）	ESASPFVerdict	例：ESASPFVerdict={'mailfrom': {'sender': 'test@cisco.com', 'result': 'SoftFail'}, 'helo': {'sender': 'postmaster', 'result': 'None'}} 可能な値： Pass/Neutral/SoftFail/Fail/ TempError/PermError
危険性のない送信元（Friendly From）	ESAFriendlyFrom	例：demo@test.com
送信者（Mail From）	suser	例：demo@test.com
Reply-To	ESAReplyTo	例：demo@test.com
Subject	msg	例：This is a sample subject
MID	ESAMID	例：101
メッセージID（Message ID）	cs4	例：cs1Label=ExternalMsgID cs1=20190729112221.42958.40626 @vm21esa0075.cs21

ログ フィールド	CEF フィールド名	CEF フィールド値
メッセージ サイズ	ESAMsgSize	例：ESAMsgSize=32199
SDRレピュテーションスコア（SDR Reputation Score）	cs6	例：cs6Label= SDRRepScore cs6=Tainted
SDR統合ドメイン使用年数（SDR Consolidated Domain Age）	ESASDRDomainAge	例：1 year 21 days
SDR統合脅威カテゴリ（SDR Consolidated Threat Category）	cs3	例：cs3Label= SDRThreatCategory cs3=mal
メッセージフィルタ判定（Message Filters Verdict）	メッセージフィルタ判定（Message Filters Verdict）	例：MATCH 可能な値： NOT EVALUATED/MATCH/NO MATCH
AS判定（AS Verdict）	ESAASVerdict	例：POSITIVE 可能な値： Not EVALUATED/NEGATIVE/SUSPECT/ BULK_MAIL/SOCIAL_MAIL/MARKE TING_MAIL/POSITIVE
AV判定（AV Verdict）	ESAAVVerdict	例：POSITIVE 可能な値： NOT EVALUATED/NEGATIVE/REPAIRED /ENCRYPTED/UNSCANNABLE/POSI TIVE
AMP判定（AMP Verdict）	ESAAMPVerdict	例：UNKNOWN 可能な値： NOT EVALUATED/CLEAN/FA_PENDING/ UNKNOWN/SKIPPED/ UNSCANNABLE /LOW_RISK/MALICIOUS

ログ フィールド	CEF フィールド名	CEF フィールド値
グレイメール判定（Graymail Verdict）	ESAGMVerdict	例：POSITIVE 可能な値： NOT EVALUATED/POSITIVE/NEGATIVE
コンテンツフィルタ判定（Content Filters Verdict）	ESACFVerdict	例：MATCH 可能な値： NOT EVALUATED/MATCH/NO MATCH
アウトブレイクフィルタ判定（Outbreak Filters Verdict）	ESAOFVerdict	例：NEGATIVE 可能な値： NOT EVALUATED/POSITIVE/NEGATIVE
DLP判定（DLP Verdict）	ESADLPVerdict	例：VIOLATION 可能な値： NOT EVALUATED/NO TRIGGER/VIOLATION/NO VIOLATION
URLの詳細（URL Details）	ESAURLDetails	例： {url1:{expanded_url:<>, category:<>, wbrs_score:<>, in_attachment:<>, Attachment_with_url:<>,},url2:{…}} （注） 255 文字を超えるURLは切り捨てられます。
ファイルの詳細（File Details）	ESAAttachmentDetails	例： {name1:{source: {<>hash:<>, verdicts:<>}}} （注） 255 文字を超えるファイル名は切り捨てられます。

ログ フィールド	CEF フィールド名	CEF フィールド値
メールボックス自動修復の詳細（Mailbox Auto-Remediation Details）	ESAMARAction	例： {action:<>;succesful_rcpts=<>;failed_recipients=<>;filename=<>}
DCID	ESADCID	例：199
DCIDタイムスタンプ（DCID Timestamp）	EndTime	例：Mon Jul 29 09:55:07 2019
DANEステータス（DANE Status）	ESADaneStatus	例：Success 可能な値： success/failure
DANEホスト（DANE Host）	ESADaneHost	例：testdomain.com
メッセージの最終アクション（Message Final Action）	act	例：act=DELIVERED 可能な値： DROPPED/BOUNCED/DELIVERED：メッセージが検疫されていない場合。 QUARANTINED：メッセージが検疫されている場合。 DQ：メッセージが遅延検疫に送信される場合。これは例外であり、検疫タイプではありません。
メッセージの最終アクションの詳細（Message Final Action Details）	ESAFinalActionDetails	例： act=DROPPED ESAFinalActionDetails= By AMP act=QUARANTINED ESAFinalActionDetails=To SPAM

（注） 選択されたログフィールドに値がない場合（たとえば、DKIMが電子メールゲートウェイで有効になっていないときの「DKIMVerdict」）、そのログフィールドはログメッセージに含まれません。

CSN ログの使用

CSN ログには、CSN データのアップロードに関する詳細が記録されます。CSN データ（電子メールゲートウェイおよび機能の使用状況の詳細）は、トレースレベルで確認できます。

CSN データログエントリの例：

- この例では、電子メールゲートウェイのスマートライセンスが Cisco Smart Software Manager（CSSM）に登録されていないため、CSN データがシスコに送信されなかったことが、ログに示されています。

```
Tue Apr 7 12:52:47 2020 Warning: Device is not
registered with CSSM. Skipping upload of CSN data
```

解決策：Cisco Smart Software Manager（CSSM）に電子メールゲートウェイのスマートライセンスを登録します。

- この例では、Cisco Security Services Exchange（SSE）の接続エラーが原因で、CSN データがシスコに送信されなかったことが、ログに示されています。

```
Thu Apr 9 13:32:46 2020 Warning: The appliance
failed to upload CSN data. reason for failure:
SSE error: HTTP Error 503: Service Unavailable
```

解決策：電子メールゲートウェイで CSN を無効にしてから、もう一度有効にします。

Advanced Phishing Protection ログの使用

Advanced Phishing Protection のログには、Cisco Advanced Phishing Protection クラウドサービスに関連する情報が記録されます。ほとんどの情報は [情報（Info）] または [クリティカル（Critical）] レベルです。

Advanced Phishing Protection のデータログのエント例：

- この例では、サービスが期限切れになったため、電子メールゲートウェイが Cisco Advanced Phishing Protection クラウドサービスにメッセージヘッダーを転送できなかったことが、ログに示されています。

```
Wed May 6 18:21:40 2020 Info: eaas : You cannot
forward the MID [877] Message Headers to Cisco Advanced
Phishing Protection Cloud Service as the service has
expired
```

- この例では、Cisco Advanced Phishing Protection クラウドサービスが期限切れになり、電子メールゲートウェイで無効になっていることが、ログに示されています。

```
Wed May 6 18:21:40 2020 Info: eaas : Cisco
Advanced Phishing Protection Cloud Service has expired
and is disabled. Contact your Cisco Account manager to
renew the service and then enable it.
```

解決策：シスコアカウントマネージャに連絡して、サービスを更新してから有効にします。

- この例では、Cisco Advanced Phishing Protection クラウドサービスが特定の日付に期限切れになることが、ログで示されています。

```
Fri May 8 04:50:26 2020 Info: eaas : Cisco
Advanced Phishing Protection Cloud Service expires on
2020-05-10 07:00:00. You need to contact your Cisco Account
manager to renew the service.
```

解決策：シスコアカウントマネージャに連絡して、サービスを更新します。

監査ログの使用

監査ログで認証、許可、アカウンティングのイベント（AAA：Authentication、Authorization、およびAccounting）を記録します。ほとんどの情報は、デバッグレベルまたはトレースレベルです。

監査ログエントリの例：

- この例では、ユーザー（admin など）が次の場合にログが表示されます。
  - 電子メールゲートウェイの Web インターフェイスにログインする必要があります。
  - 電子メールゲートウェイの Web インターフェイスからログアウトしました。

```
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Event: Successful login
Tue Aug 25 12:33:17 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session established
 successfully
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: User logged out
Tue Aug 25 12:33:58 2020 Info: Appliance: mail1.example.com,
Interaction Mode: GUI, User: admin, Source IP: 192.168.1.1, Event: Session terminated
```

- この例では、ユーザー（admin）が `logconfig` CLI コマンドを入力したことがログに示されています。

```
Thu Oct  8 13:33:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: User input was 'logconfig'
Thu Oct  8 13:33:46 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: User input was 'Enter'
```

- この例では、ユーザー（admin）が電子メールゲートウェイのレガシー Web インターフェイスで GUI ページを表示したことがログに示されています。

```
Thu Oct  8 13:35:07 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /network/dns, Event: User visited the web page.
Thu Oct  8 13:35:13 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /system_administration/sslconfig, Event: User
visited the web page.
Thu Oct  8 13:35:24 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /monitor/mail_reports/threatfeeds_report, Event:
User visited the web page.
```

- この例では、新しいユーザ（admin）が Web インターフェイスを使用して電子メールゲートウェイに追加されても、変更はコミットされていないことがログに示されています。

```
Thu Oct  8 13:36:30 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Added
 user "admin" and changes
will reflect after commit.
Thu Oct  8 13:37:22 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /system_administration/access/users, Event: Deleted
 user "admin" and changes
will reflect after commit.
```

- この例では、電子メールゲートウェイの Web インターフェイスでコミットされなかったすべての変更がユーザ（admin）によって破棄されたことがログに示されています。

```
Thu Oct  8 13:39:44 2020 Info: Appliance: mail1.example.com, Interaction Mode: GUI,
 User: admin,
Source IP: 192.168.1.1, Location: /commit, Event: User discarded all uncommitted
changes.
```

- この例では、ユーザー（adminなど）がCLIを介してコミットされなかったすべての変更を破棄したことがログに示されています。

```
Thu Oct  8 13:41:38 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: User discarded all uncommitted changes.
```

- この例では、ユーザー（adminなど）がWeb UIセッションタイムアウトの設定を変更したことがログに示されています。

（注） 電子メールゲートウェイで行われた設定変更の詳細を表示するには、設定履歴ログを表示するか、監査ログのデバッグモードを有効にします。

```
Thu Oct  8 13:45:46 2020 Info: Appliance: mail1.example.com, User: admin,
Event: The following configuration changes were commited with comment - 'N/A'
Thu Oct  8 13:45:46 2020 Info: * [standalone] Number of seconds before the Web UI
session times out.
```

- この例では、認証に失敗したため、AsyncOS API がログサブスクリプションを取得できなかったことがログに示されています。

```
Thu Oct  8 13:52:28 2020 Debug: 08/Oct/2020 13:52:28 +0000 Error - Code: 401,
Details: Unauthorized (No permission -- see authorization schemes)
Thu Oct  8 13:52:28 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,

User: admin, Role: Role Not Available, Source IP: 192.168.1.1, Destination IP:
192.168.2.2,
Location: GET /esa/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: User is not
 valid.
```

- この例では、認証に成功したため、AsyncOS API がログサブスクリプションを取得できたことがログに示されています。

```
Thu Oct  8 13:52:37 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,

User: admin, Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,

Location: GET /esa/api/v2.0/config/logs/subscriptions/ HTTP/1.0, Event: API Access
Success.
```

- この例では、ログに次の内容が表示されています。
  - CLI を使用して電子メールゲートウェイに新しいユーザ（admin）が追加されましたが、変更はコミットされませんでした。
  - 既存のユーザアカウントの詳細は、CLI を使用して電子メールゲートウェイで更新されましたが、変更はコミットされませんでした。

```
Thu Oct  8 13:42:48 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,

User: admin, Source IP: 192.168.1.1, Event: Added user "hops" and changes will reflect
 after commit
Thu Oct  8 13:43:26 2020 Info: Appliance: mail1.example.com, Interaction Mode: CLI,
 User: admin,
Source IP: 192.168.1.1, Event: Updated user "hops" and changes will reflect after
commit
```

- この例では、ユーザー（admin）が電子メールゲートウェイの新しい Web インターフェイスでメッセージトラッキング検索を実行したことがログに示されています。

```
Mon Oct 12 04:04:47 2020 Info: Appliance: mail1.example.com, Interaction Mode: API,
 User: admin,
Role: Administrator, Source IP: 192.168.1.1, Destination IP: 192.168.2.2,
Location: GET
/esa/api/v2.0/message-tracking/messages?startDate=2020-10-12T00:00:00.000Z
&endDate=2020-10-12T04:13:00.000Z&ciscoHost=All_Hosts&searchOption=messages&offset=0&limit=100
 HTTP/1.0,
Event: API Access Success.
```

（注） 電子メールゲートウェイの新しい Web インターフェイスで実行するアクション（トラッキング、レポート、隔離の検索など）は、これらのアクションに使用される対応する API に基づき、ログとして記録されます。

CSA ログの使用

Cisco Secure Awareness クラウドサービスの情報はメールログに記録されます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

Cisco Secure Awareness ログエントリの例：

- この例では、無効なトークンが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Tue Oct 13 10:12:59 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of an invalid token.
```

解決策：Cisco Secure Awareness クラウドサービスから有効な認証トークンを取得してください。

- この例では、接続エラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of a connection error.
```

解決策：電子メールゲートウェイを Cisco Secure Awareness クラウドサービスに接続するために使用するファイアウォール設定を確認します。

- この例では、内部サーバエラーが原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 10:59:36 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
of an internal server error.
```

解決策：詳細については、シスコ テクニカル サポートにお問い合わせください。

- この例では、SSL 証明書の検証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:02:46 2020 Warning: CSA:
 The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed because
the SSL certificate verification failed.
```

解決策：必要なプロキシサーバの CA 証明書を電子メールゲートウェイのカスタム認証局リストに追加します。

- この例では、プロキシ認証の失敗が原因で Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Wed Oct 14 11:09:48 2020 Warning: CSA:
The download of the Repeat Clickers list from
the Cisco Security Awareness cloud service failed
because the proxy authentication failed.
```

解決策：電子メールゲートウェイでプロキシサーバが正しい認証ログイン情報を使用して設定されているかどうかを確認します。

- この例では、Cisco Secure Awareness クラウドサービスでレポート API が有効になっていなかったことが原因で、Cisco Secure Awareness クラウドサービスへの要求が失敗したことがログに示されています。

```
Mon Aug 17 15:35:42 2020 Warning: CSA:
The download of the Repeat Clickers list failed.
A request to the CSA cloud service failed because
the Report API was not enabled on the CSA cloud service
```

解決策：Cisco Secure Awareness クラウドサービスの [環境（Environment）] > [設定（Settings）] > [レポートAPI（Report API）] タブで [レポートAPIを有効にする（Enable Report API）] チェックボックスをオンにします。

- この例では、Cisco Secure Awareness 機能が特定の日付で期限切れになることがログに示されています。

```
2020-10-15 08:00:11,968 INFO csa The Cisco Security
Awareness feature expires on 2029-12-28T23:59:59Z. You need to
contact your Cisco Account Manager to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、Cisco Secure Awareness 機能のライセンスの有効期限が切れており、電子メールゲートウェイでこの機能が無効になっていることがログに示されています。

```
2020-10-27 13:33:21,714 CRITICAL csa The Cisco Security
Awareness feature license has expired, and the feature is
disabled on your email gateway. Contact your Cisco Account Manager
to renew the license.
```

解決策：シスコアカウントマネージャに連絡して、ライセンスを更新します。

- この例では、ダウンロードされたリピートクリッカーリストが空であることがログに示されています。

```
Tue Oct 13 10:10:18 2020 Info: CSA: The downloaded
Repeat Clickers list is empty.
```

解決策：Cisco Secure Awareness クラウドサービスでシミュレートされたフィッシングメッセージを作成し、組織内の受信者に送信します。

- この例では、ダウンロード試行の最大数に達したため、Cisco Secure Awareness クラウドサービスからのリピートクリッカーリストのダウンロードが失敗したことがログに示されています。

```
Fri Oct 16 05:22:08 2020 Warning: CSA: The download
of the Repeat Clickers list from the Cisco Security Awareness
cloud service failed because you have reached the maximum
number of attempts.
```

解決策：Cisco Secure Awareness クラウドサービスからリピートクリッカーリストをダウンロードする試行回数を増やすには、シスコサポートに連絡してください。

ログ サブスクリプション

- ログ サブスクリプションの設定 （1467 ページ）
- GUI でのログ サブスクリプションの作成 （1469 ページ）
- ロギングのグローバル設定 （1469 ページ）
- ログ サブスクリプションのロールオーバー （1472 ページ）
- ホスト キーの設定 （1476 ページ）

ログ サブスクリプションの設定

[システム管理（System Administration）] の [ログサブスクリプション（Log Subscriptions）] ページ（または CLI の **logconfig** コマンド）を使用して、ログ サブスクリプションを設定します。ログ サブスクリプションによって、エラーを含む AsyncOS アクティビティの情報を保存するログ ファイルが作成されます。ログ サブスクリプションは、取得されるか、または別のコンピュータに配信（プッシュ）されるかのどちらかです。一般に、ログサブスクリプションには次の属性があります。

表 *150* : ログ ファイルの属性

属性	説明
ログタイプ（Log type）	記録される情報のタイプと、ログサブスクリプションの形式を定義します。詳細については、表「ログ タイプ」を参照してください。
ログ名（Log Name）	今後の参照に使用するログ サブスクリプションのニックネーム。
ログ フィールド（Log Fields）	特定のメッセージの統合イベント ログ行に含める必要があるログ フィールドを選択します。 （注） [シリアル番号（Serial Number）] および [MID] ログ フィールドはデフォルトで選択されており、これらの選択を解除することはできません。 （注） このフィールドは、ログ タイプが統合イベント ログのログ サブスクリプションを設定する場合にのみ適用されます。
ファイル名（File Name）	ディスクに書き込むときのファイルの物理名に使用されます。複数の電子メールゲートウェイを使用している場合、ログファイルを生成したシステムを識別するため、ログファイル名を固有にする必要があります。
ファイルサイズ別ロールオーバー（Rollover by File Size）	ファイルの最大サイズ。このサイズに到達すると、ローリング オーバーされます。
時刻によりロールオーバー（Rollover by Time）	ファイルのロールオーバーの時間間隔を設定します。
レート制限（Rate Limit）	指定した時間範囲（秒単位）内での、ログファイルのログ記録されるイベントの最大数を設定します。 デフォルトの時間範囲の値は 10 秒です。
ログ レベル（Log level）	ログ サブスクリプションごとに詳細のレベルを設定します。

属性	説明
取得方法（Retrieval method）	ログサブスクリプションが電子メールゲートウェイから取得される方法を定義します。

ログ レベル

ログ レベルによって、ログに送信される情報量が決定します。ログには、5つの詳細レベルのいずれかを設定できます。詳細レベルを高くするほど大きいログ ファイルが作成され、システムのパフォーマンスが低下します。詳細レベルの高い設定には、詳細レベルの低い設定に保持されるすべてのメッセージと、その他のメッセージも含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。

（注） ログ レベルは、すべてのメール ログ タイプに対して選択できます。

表 *151* : ログ レベル

ログ レベル	説明
クリティカル	詳細レベルの最も低い設定。エラーだけがログに記録されます。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできませんが、ログ ファイルがすぐには最大サイズに達しなくなります。このログ レベルは、syslog レベルの「Alert」と同等です。
警告	システムによって作成されたすべてのエラーと警告。この設定にすると、パフォーマンスやその他の重要なアクティビティをモニタできません。このログ レベルは、syslog レベル「Warning」と同等です。
情報	情報設定では、システムの秒単位の動作がキャプチャされます。たとえば、接続のオープンや配信試行などです。Information レベルは、ログに推奨される設定です。このログ レベルは、syslog レベル「Info」と同等です。
デバッグ（Debug）	エラーの原因を調べるときは、Debug ログ レベルを使用します。この設定は一時的に使用し、後でデフォルト レベルに戻します。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。
トレース（Trace）	Trace ログ レベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログ レベルは、syslog レベルの [デバッグ（Debug）] と同等です。

GUI でのログ サブスクリプションの作成

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 [ログサブスクリプションを追加（Add Log Subscription）] をクリックします。

ステップ 3 ログ タイプを選択し、ログ名（ログ ディレクトリ用）とログ ファイル自体の名前を入力します。

ステップ 4 （統合イベント ログのみ）特定のメッセージのログ行に含める必要があるログ フィールドを選択します。

ステップ 5 AsyncOS がログ ファイルをロールオーバーする前の最大ファイル サイズ、およびロールオーバー間の時間間隔を指定します。ファイルのロールオーバーの詳細については、ログ サブスクリプションのロールオーバー （1472 ページ）を参照してください。

ステップ 6 ログ レベルを選択します。使用可能なオプションは、[クリティカル（Critical）]、[警告（Warning）]、[情報（Information）]、[デバッグ（Debug）]、または [トレース（Trace）] です。

ステップ 7 ログの取得方法を設定します。

ステップ 8 変更を送信し、保存します。

ログ サブスクリプションの編集

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 [ログ設定（Log Settings）] カラムでログの名前をクリックします。

ステップ 3 ログ サブスクリプションを変更します。

ステップ 4 変更を送信し、保存します。

ロギングのグローバル設定

システムは、テキスト メール ログおよびステータス ログ内にシステムの測定を定期的に記録します。[システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）] ページの [グローバル設定（Global Settings）] セクションにある [設定を編集（Edit Settings）] ボタン（または、CLI の `logconfig -> setup` コマンド）を使用して、次の情報を設定します。

- システムの測定頻度。これは、システムが測定を記録するまで待機する時間（秒単位）です。
- メッセージ ID ヘッダーを記録するかどうか。
- リモート応答ステータス コードを記録するかどうか。
- 元のメッセージのサブジェクト ヘッダーを記録するかどうか。
- メッセージごとにログに記録するヘッダーのリスト。

すべてのログには、次の 3 つのデータを任意で記録できます。

1. メッセージ ID

   このオプションを設定すると、可能な場合はすべてのメッセージのメッセージIDヘッダーがログに記録されます。このメッセージ ID は、受信したメッセージから取得される場合と、AsyncOS 自体で生成される場合があります。次に例を示します。

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
   ```

2. リモート応答

   このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次に例を示します。

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
   ```

   リモート応答文字列は、SMTP カンバセーション配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

   ```
   [...]

   250 ok hostname

   250 Ok: queued as 9C8B425DA7
   ```

   文字列の先頭にある空白や句読点（および、250応答の場合はOK文字）は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、電子メールゲートウェイはデフォルトで、DATA コマンドに対して「250 Ok: Message MID accepted」という文字列で応答します。したがって、リモートホストが別の 電子メールゲートウェイである場合は、文字列「Message MID accepted」がログに記録されます。

3. オリジナルの件名

   このオプションをイネーブルにすると、各メッセージの元のサブジェクト ヘッダーがログに記録されます。

   ```
   Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
   ```

```
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

メッセージ ヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[ログサブスクリプションのグローバル設定（Log Subscriptions Global Settings）] ページ（または、CLI の logconfig -> logheaders サブコマンド）に、記録するヘッダーを指定します。電子メールゲートウェイは、指定されたメッセージヘッダーをテキストメールログ、配信ログ、およびバウンスログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。

（注） システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。

SMTP プロトコルについての RFC は、http://www.faqs.org/rfcs/rfc2821.html にあります。この RFC には、ユーザ定義のヘッダーが規定されています。

logheaders コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 *152 :* ヘッダーのログ（*Log Headers*）

ヘッダー名	ヘッダーの名前
値	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「date, x-subject」を指定すると、メールログに次の行が表示されます。

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

GUI を使用したロギングのグローバル設定の構成

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 [グローバル設定（Global Settings）] セクションまでスクロールします。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 システム測定頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクト ヘッダーを加えるかどうかを含めた情報を指定します。

ステップ 5 ログに加えるその他のヘッダーを入力します。

ステップ 6 変更を送信し、保存します。

ログ サブスクリプションのロールオーバー

電子メールゲートウェイ上のログファイルが大きくなりすぎないようにするために、ログファイルがユーザ指定の最大ファイルサイズまたは時間間隔に達すると、AsyncOS は「ロールオーバー」を実行してログファイルをアーカイブし、着信するログデータ用の新しいファイルを作成します。ログサブスクリプション用に定義された取得方法に基づいて、古いログファイルは取得のために電子メールゲートウェイ上に保管されるか、または外部のコンピュータに配信されます。電子メールゲートウェイからログファイルを取得する方法の詳細については、ログ取得方法 （1402 ページ）を参照してください。

AsyncOS は、ログ ファイルをロールオーバーするときに次のアクションを実行します。

- ロールオーバーのタイムスタンプと、saved（保存済み）を示す文字「**s**」拡張子を使用して、現在のログ ファイルの名前を変更します。
- 新しいログ ファイルを作成し、「**current**」の拡張子を使用して、そのファイルを最新として指定します。
- 新しく保存されたログ ファイルをリモート ホストに転送します（プッシュ ベースの取得方法を使用している場合）。
- 同じサブスクリプションから、以前に失敗したログ ファイルをすべて転送します（プッシュ ベースの取得方法を使用している場合）。
- 保存すべきファイルの総数を超えた場合は、ログ サブスクリプション内の最も古いファイルを削除します（ポーリング ベースの取得方法を使用している場合）。

  ログ サブスクリプションのロールオーバーの設定は、GUI の [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] ページ、または CLI の logconfig コマンドを使用して、サブスクリプションを作成または編集するときに定義します。ログ ファイルのロールオーバーをトリガーするために使用できる 2 つの設定は次のとおりです。

- 最大ファイル サイズ。
- 時間間隔。

ファイル サイズによるロールオーバー

AsyncOS は、ログ ファイルで使用されるディスク領域が多くなりすぎないようにするために、最大ファイル サイズに達したログ ファイルをロールオーバーします。ロールオーバーのための最大ファイル サイズを定義する場合は、メガバイトを示す m とキロバイトを示す k のサフィックスを使用します。たとえば、ログ ファイルが 10 MB に達したら AsyncOS によってロールオーバーされるようにする場合は、「10m」と入力します。

時刻によりロールオーバー

ロールオーバーを定期的に実行されるようにスケジュールする場合は、次のいずれかの時間間隔を選択できます。

- **[なし（None）]**。AsyncOS は、ログ ファイルが最大ファイル サイズに達した場合にのみロールオーバーを実行します。
- **[カスタム時間間隔（Custom Time Interval）]**。AsyncOS は、以前のロールオーバーから指定された時間が経過した後にロールオーバーを実行します。スケジュール設定されたロールオーバーのためのカスタムの時間間隔を作成するには、d、h、および m をサフィックスとして使用して、ロールオーバー間の日数、時間数、および分数を入力します。
- **[日次ロールオーバー（Daily Rollover）]**。AsyncOS は、毎日指定された時刻にロールオーバーを実行します。日単位のロールオーバーを選択した場合は、24 時間形式（HH:MM）を使用して、AsyncOS がロールオーバーを実行する時刻を入力します。

  GUI では、[日次ロールオーバー（Daily Rollover）] オプションのみが提供されます。CLI の logconfig コマンドを使用して日単位のロールオーバーを設定する場合は、[週次ロールオーバー（Weekly Rollover）] オプションを選択し、アスタリスク（*）を使用して AsyncOS がすべての曜日にロールオーバーを実行することを指定します。

- **[週次ロールオーバー（Weekly Rollover）]**。AsyncOS は、1 つ以上の曜日の指定された時刻にロールオーバーを実行します。たとえば、毎週水曜日と金曜日の午前 0：00 にログ ファイルをロールオーバーするように AsyncOS を設定できます。週単位のロールオーバーを設定するには、ロールオーバーを実行する曜日と 24 時間形式（HH:MM）の時刻を選択します。

  CLI を使用している場合は、ダッシュ（-）を使用して日の範囲を指定するか、アスタリスク（*）を使用してすべての曜日を指定するか、またはカンマ（,）を使用して複数の日と時刻を区切ることができます。

  次の表に、CLI を使用して、水曜日と金曜日の午前 0:00（00:00）にログ サブスクリプションのファイルをロールオーバーする方法を示します。

表 *153 : CLI* での週単位のログ ロールオーバーの設定

`Do you want to configure time-based log files rollover? [N]> y`
`Configure log rollover settings:`
`1. Custom time interval.`
`2. Weekly rollover.`
`[1]> 2`
`1. Monday`

```
2. Tuesday
```

```
3. Wednesday
```

```
4. Thursday
```

```
5. Friday
```

```
6. Saturday
```

```
7. Sunday
```

```
Choose the day of week to roll over the log files.  Separate multiple days with comma,

or use "*" to specify every day of a week.
Also you can use dash to specify a range like "1-5":
```

```
[]> 3, 5
```

```
Enter the time of day to rollover log files in 24-hour format (HH:MM).
You can specify hour as "*" to match every hour, the same for minutes.
Separate multiple times of day with comma:
```

```
[]> 00:00
```

オンデマンドでのログ サブスクリプションのロールオーバー

GUI を使用してログ サブスクリプションをただちにロールオーバーするには、次の手順を実行します。

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）]ページで、ロール オーバーするログの右側のチェックボックスをオンにします。

ステップ 2 任意で、[すべて（All）]チェックボックスをオンにして、すべてのログをロールオーバー対象として選択できます。

ステップ 3 ロールオーバー対象として1つまたは複数のログを選択すると、[今すぐロールオーバー（Rollover Now）]ボタンがイネーブルになります。[今すぐロールオーバー（Rollover Now）]ボタンをクリックして、選択したログをロール オーバーします。

GUI での最近のログ エントリの表示

はじめる前に

GUI を介してログを表示するには、管理インターフェイスで HTTP または HTTPS サービスをイネーブルにしておく必要があります。

手順

ステップ 1 [システム管理（System Administration）]>[ログサブスクリプション（Log Subscriptions）] を選択します。

ステップ 2 テーブルの [ログファイル（Log Files）] カラムでログ サブスクリプションを選択します。

ステップ 3 サインインします。

ステップ 4 ログ ファイルのいずれかを選択して、ブラウザに表示するか、またはディスクに保存します。

CLI での最近のログ エントリの表示（tail コマンド）

AsyncOS は、電子メールゲートウェイに設定されたログの最新エントリを表示する tail コマンドをサポートしています。tail コマンドを実行して現在設定されているログの番号を選択すると、そのログが表示されます。Ctrl+ C を押して、tail コマンドを終了します。

例

次の例では、tail コマンドを使用してシステム ログを表示します。（このログは commit コマンドによるユーザのコメントを特に追跡します）。tail コマンドは、tail mail_logs のように、表示するログの名前をパラメータとして指定することもできます。

```
mail3.example.com> tail

Currently configured logs:


1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download

4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download

6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download

7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download

8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download

9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
```

```
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download

11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download

12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download

13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download

14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download

15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download

16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual Download

17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download

18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download

19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download

20. "status" Type: "Status Logs" Retrieval: Manual Download

21. "system_logs" Type: "System Logs" Retrieval: Manual Download

22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download

23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download


Enter the number of the log you wish to tail.

[]> 19

Press Ctrl-C to stop.

Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host

Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:

Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs
config

Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes: Receiving
suspended.

^Cmail3.example.com>
```

ホスト キーの設定

`logconfig -> hostkeyconfig` サブコマンドを使用して、電子メールゲートウェイから他のサーバにログをプッシュするときに、SSH で使用するホストキーを管理します。SSH サーバには、秘密キーと公開キーの 2 つのホスト キーが必要です。秘密ホスト キーは SSH サーバにあり、リモート マシンから読み取ることはできません。公開ホスト キーは、SSH サーバと対話する必要のある任意のクライアント マシンに配信されます。

（注） ユーザー キーを管理するには、セキュア シェル（SSH）キーの管理 （1222 ページ）を参照してください。

`hostkeyconfig` サブコマンドによって、次の機能が実行されます。

表 *154*：ホスト キーの管理：サブコマンドのリスト

コマンド	説明
新規作成	新しいキーを追加します。
編集（Edit）	既存のキーを変更します。
削除（Delete）	既存のキーを削除します。
スキャン（Scan）	ホスト キーを自動的にダウンロードします。
印刷（Print）	キーを表示します。
ホスト（Host）	システム ホスト キーを表示します。これは、リモート システムの「known_hosts」ファイルに配置される値です。
フィンガープリント（Fingerprint）	システム ホスト キーのフィンガープリントを表示します。
ユーザー（User）	リモート マシンにログをプッシュするシステム アカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモート システムの「authorized_keys」ファイルに配置される値です。

次の例では、AsyncOS によってホスト キーがスキャンされ、ホスト用に追加されます。

```
mail3.example.com> logconfig

Currently configured logs:

[ list of logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.
```

```
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> hostkeyconfig
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan
Please enter the host or IP address to lookup.
[]> mail3.example.com
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]
SSH1:rsa
mail3.example.com 1024 35
```

```
[ key displayed ]

Add the preceding host key(s) for mail3.example.com? [Y]>

Currently installed host keys:

1. mail3.example.com ssh-dss [ key displayed ]

2. mail3.example.com ssh-rsa [ key displayed ]

3. mail3.example.com 1024 35 [ key displayed ]

Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.

- DELETE - Remove a key.

- SCAN - Automatically download a host key.

- PRINT - Display a key.

- HOST - Display system host keys.

- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]>

Currently configured logs:

[ list of configured logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]>
```

第 45 章

クラスタを使用した中央集中型管理

この章は、次の項で構成されています。

- クラスタを使用した中央集中型管理の概要 （1481 ページ）
- クラスタの要件 （1482 ページ）
- クラスタの構成 （1483 ページ）
- クラスタの作成とクラスタへの参加 （1484 ページ）
- クラスタの管理 （1492 ページ）
- GUI でのクラスタの管理 （1498 ページ）
- クラスタ通信 （1500 ページ）
- クラスタ化された電子メールゲートウェイの設定のロード （1505 ページ）
- ベスト プラクティスとよく寄せられる質問（FAQ） （1507 ページ）

クラスタを使用した中央集中型管理の概要

シスコの中央集中型管理機能を使用して複数の電子メールゲートウェイを同時に管理、設定することにより、管理に要する時間を短縮し、ネットワーク全体で設定の一貫性を確保することができます。複数の電子メールゲートウェイを管理するためにハードウェアを追加購入する必要はありません。中央集中型管理機能によって、ネットワーク内の信頼性、柔軟性、およびスケーラビリティが向上し、ローカルポリシーを順守しながらグローバルな管理を行うことができます。

クラスタ とは、設定情報を共有する一連のマシンのことです。クラスタの内部では、マシン（電子メールゲートウェイ）がグループに分割されます。どのクラスタにも1つ以上のグループがあります。個々のマシンは、必ずいずれかのグループのメンバになります。管理者ユーザは、システムのさまざまな要素をクラスタ単位、グループ単位、またはマシン単位で設定できます。これにより、電子メールゲートウェイを、ネットワーク、地域、部署、または論理的な関係に基づいて分割できます。

クラスタはピアツーピアアーキテクチャで実装されるため、クラスタ内にプライマリ/セカンダリの関係は存在しません。どのマシンにログインしても、クラスタの制御と管理を行うことができます。（ただし、一部のコンフィギュレーションコマンドは制限されます。制限コマンド （1496 ページ） を参照してください。）

ユーザー データベースはクラスタ内のすべてのマシン間で共有されます。つまり、ユーザのセットと管理者（および対応するパスフレーズ）はクラスタ全体で1つしか存在しません。クラスタに参加するすべてのマシンは1つの管理者パスフレーズを共有します。これをクラスタの管理パスフレーズと呼びます。

（注） 1 つのクラスタに 20 を超える電子メールゲートウェイがあると、クラスタの通信におけるエラーの原因となる可能性があります。

クラスタの要件

- クラスタ内の各マシンには、DNS で解決可能なホスト名が必要です。代わりに IP アドレスを使用することもできますが、両者を混在させることはできません。

  DNS とホスト名の解決 （1501 ページ）を参照してください。クラスタの通信は、通常、マシンの DNS ホスト名を使って開始されます。

- 1 つのクラスタは、全体として同じバージョンの AsyncOS を実行しているマシンで構成されている必要があります。

  クラスタのメンバをアップグレードする方法については、クラスタ内のマシンのアップグレード （1494 ページ）を参照してください。

- 各マシンは、SSH（通常はポート 22）と Cluster Communication Service（CCS）のいずれかを使ってクラスタに参加できます。

  クラスタ通信 （1500 ページ）を参照してください。

- クラスタに参加したマシンは、SSH または CCS 経由で通信できます。使用するポートは設定可能です。SSH は通常ポート 22 上でイネーブルになっており、CCS はデフォルトでポート 2222 上でイネーブルになっていますが、どちらのサービスも別のポートに設定できます。

  電子メールゲートウェイに対して開く必要がある通常のファイアウォールポートに加えて、クラスタ化されたマシンが CCS 経由で通信する場合は、各マシンが CCS ポート経由で相互に接続できる必要があります。クラスタ通信 （1500 ページ）を参照してください。

- マシンのクラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、CLI（コマンド ライン インタフェース）の **clusterconfig** コマンドを使用する必要があります。

  クラスタを作成した後は、クラスタ以外の設定を GUI または CLI から管理できます。

  クラスタの作成とクラスタへの参加 （1484 ページ）およびGUI でのクラスタの管理 （1498 ページ）を参照してください。

- 電子メールゲートウェイで二要素認証を有効にしている場合は、事前共有キーを使用してクラスタマシンに参加させることができます。CLI の `clusterconfig > prepjoin` コマンドを使用して、この設定を構成します。

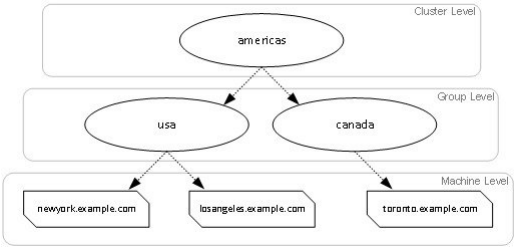
または

クラスタを作成したりそれに参加したりする前に、電子メールゲートウェイで二要素認証を無効にします。詳細については、二要素認証の無効化（1216ページ）を参照してください。

クラスタの構成

クラスタでは、設定情報が3つのグループ（レベル）に分かれています。最上位レベルはクラスタの設定、中位レベルはグループの設定、最下位レベルはマシンごとの設定をそれぞれ表します。

図 *79*：クラスタのレベル階層



各レベルには、設定が可能なメンバが1つ以上存在します。これらをモードと呼びます。モードは特定のレベルに含まれる名前の付いたメンバを表します。たとえば、「usa」グループは図に示した2つのグループ モードの1つです。レベルは一般的な用語ですが、モードは具体的なものを示します。モードは常に名前で参照されます。上の図に示されているクラスタは、6つのモードを持っています。

設定は特定のレベルで設定されますが、それらは常に特定のモードに対して設定されます。すべてのモードに対する設定を1つのレベルで設定する必要はありません。クラスタ モードは特別なケースです。クラスタは1つしか存在しないため、クラスタ モードの設定はすべてクラスタ レベルで設定されると言えます。

通常、ほとんどの設定はクラスタ レベルで設定する必要があります。ただし、下位レベルで個別に設定された設定は上位レベルで設定された設定よりも優先されます。したがって、クラスタ モードの設定をグループ モードやマシン モードの設定で上書きできます。

たとえば、最初にクラスタ モードでグッド ネイバー テーブルを設定し、クラスタ内のすべてのマシンでその設定を使用するとします。次に、このテーブルをマシン モードでマシン newyork 用に設定します。この場合、クラスタ内の他のすべてのマシンは引き続きクラスタ レベルで定義されたグッド ネイバー テーブルを使用しますが、マシン newyork はクラスタの設定をマシン モードの個別の設定で上書きします。

特定のグループやマシン用にクラスタの設定を上書きする機能によって、非常に柔軟な設定が可能になります。ただし、多くの設定をマシン モードで個別に設定すると、クラスタの当初の目的である管理のしやすさが大きく損なわれます。

初期設定

ほとんどの機能については、新しいモードで設定を始めたときのデフォルトの初期設定は空です。設定が空であることとモードの設定が存在しないことは明確に区別されます。例として、1 つのグループと 1 台のマシンからなる非常に簡単なクラスタを考えます。LDAP クエリーがクラスタ レベルで設定されているとします。グループ レベルとマシン レベルでは何も設定されていません。

クラスタ	(ldap queries: a, b, c)
グループ	
マシン	

ここで、グループに対して新しいLDAPクエリーの設定を作成したとします。その結果は次のようになります。

クラスタ	(ldap queries: a, b, c)
グループ	(ldap queries: None)
マシン	

すると、クラスタ レベルの設定がグループ レベルの設定で上書きされますが、新しいグループ設定は初期状態では空です。グループ モードには、独自に設定された LDAP クエリーが実際には存在しません。このグループ内のマシンは、この「空の」LDAPクエリーをグループから継承します。

次に、このグループに次のような LDAP クエリーを追加します。

クラスタ	(ldap queries: a, b, c)
グループ	(ldap queries: d)
マシン	

これで、クラスタ レベルで設定されたクエリーとは別に、グループにもクエリーが設定されました。マシンはグループのクエリーを継承します。

クラスタの作成とクラスタへの参加

クラスタの作成とクラスタへの参加は、グラフィカル ユーザー インターフェイス（GUI）からはできません。クラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、コマンドライン インターフェイス（CLI）を使用する必要があります。クラスタの作成後は、GUI と CLI のどちらからも設定を変更できます。

注意 電子メールゲートウェイで二要素認証を有効にしている場合は、事前共有キーを使用してクラスタマシンに参加させることができます。CLI の `clusterconfig > prepjoin` コマンドを使用して、この設定を構成します。

または

クラスタを作成したりそれに参加したりする前に、電子メールゲートウェイで二要素認証を無効にします。詳細については、二要素認証の無効化（1216ページ）を参照してください。

clusterconfig コマンド

マシン上でクラスタの作成やクラスタへの参加を行うには、`clusterconfig` コマンドを使用します。

- 新しいクラスタを作成すると、そのクラスタのすべての初期設定はそのクラスタを作成したマシンから継承されます。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成したときにそのスタンドアロンの設定が使用されます。
- マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタレベルから継承されます。つまり、そのマシン固有の設定（IP アドレスなど）を除くすべての設定が消失し、そのマシンが参加したクラスタ、グループ、またはその両方の設定に置き換わります。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成するときにそのスタンドアロンの設定が使用され、マシン レベルの設定は保持されません。

現在のマシンがまだクラスタに含まれていない場合は、`clusterconfig` コマンドを実行すると、既存のクラスタに参加するか、新しいクラスタを作成するかのオプションが表示されます。

この時点で、新しいクラスタにマシンを追加できます。これらのマシンは、SSH または CCS を使用して通信できます。

```
newyork.example.com> clusterconfig

Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 2

Enter the name of the new cluster.

[]> americas

New cluster committed: Wed Jun 22 10:02:04 2005 PDT

Creating a cluster takes effect immediately, there is no need to commit.
```

```
Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

既存のクラスタへの参加

既存のクラスタに参加するには、クラスタに追加するホスト上で clusterconfig コマンドを実行します。SSH と CCS のどちらを使用してクラスタに参加するかを選択できます。

既存のクラスタにホストを参加させるには、次の要件を満たす必要があります。

- クラスタ内のマシンの SSH ホスト キーを検証できること
- クラスタ内のマシンの IP アドレスを知っており、そのマシンに（SSH や CCS 経由で）接続できること
- クラスタに属するマシン上の管理ユーザの管理者パスフレーズを知っていること

SSH を使った既存クラスタへの参加

次の表に、SSH オプションを使ってマシン「losangeles.example.com」をクラスタに追加する例を示します。

```
losangeles.example.com> clusterconfig


Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.
```

```
[1]> 3


While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.


WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster
settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on
losangeles.example.com? [N]> n

Enter the IP address of a machine in the cluster.

[]> IP address is entered

Enter the remote port to connect to. The must be the normal admin ssh
port, not the CCS port.

[22]> 22

Enter the admin passphrase for the cluster.
The administrator passphrase for the clustered machine is entered

Please verify the SSH host key for IP address:

Public host key fingerprint: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

Is this a valid key for this host? [Y]> y

Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.
```

```
[]>

(Cluster americas)>
```

CCS を使った既存クラスタへの参加

SSH を使用できない場合は、代わりに CCS を使用します。CCS の唯一の利点は、そのポートではクラスタ通信しか行われない（ユーザー ログインや SCP などは行われない）ことです。CCS を使って既存のクラスタにマシンを追加するには、clusterconfig の `prepjoin` サブコマンドを使ってクラスタに追加するマシンの準備を行います。次の例では、マシン「newyork」上で `prepjoin` コマンドを実行して、クラスタに追加するマシン「losangeles」の準備を行っています。

`prepjoin` コマンドを実行してから、クラスタに追加するホストの CLI で「`clusterconfig prepjoin print`」と入力し、現在クラスタに含まれているホストのコマンドラインにキーをコピーすることにより、クラスタに追加するホストのユーザ キーを取得します。

マシンがクラスタに追加された後は、`clusterconfig` コマンドを使ってクラスタのさまざまな設定が可能です。

```
Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]> prepjoin

Prepare Cluster Join Over CCS

No host entries waiting to be added to the cluster.

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

[]> new

Enter the hostname of the system you want to add.
```

```
[]> losangeles.example.com

Enter the serial number of the host mail3.example.com.

[]> unique serial number is added

Enter the user key of the host losangeles.example.com. This can be obtained by typing
"clusterconfig prepjoin print" in the CLI on mail3.example.com. Press enter on a blank
line to finish.


unique user key from output of prepjoin print is pasted

Host losangeles.example.com added.

Prepare Cluster Join Over CCS

1. losangeles.example.com (serial-number)

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

- DELETE - Remove a host from the pending join list.

[]>


(Cluster Americas)> clusterconfig

Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

事前共有キーによる SSH を使った既存クラスタへの参加

次の表は、事前共有キーを使用して SSH 経由でマシン（testmachine.example.com）を（test_cluster）クラスタに参加させる方法を示しています。

```
testmachine.example.com> clusterconfig


Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 3


While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.


WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster
settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on
testmachine.example.com? [N]>

Enter the IP address of a machine in the cluster.

[]> IP address entered

Enter the remote port to connect to. The must be the normal admin ssh
port, not the CCS port.

[22]>

Would you like to join this appliance to a cluster using pre-shared keys?
Use this option if you have enabled two-factor authentication on the appliance.) [Y]>
yes

To join this appliance to a cluster using pre-shared keys, log in to the cluster machine,

run the clusterconfig > prepjoin > command, enter the
following details, and commit your changes.
Host: pod1226-esa07.ibesa
Serial Number: 42291A18D741EDB4C601-BC14E5579F34
User Key:

ssh-dss
AAAAB3NzaC1kc3MAAACBAJ6Xm+ja4aau9n4DOcJs/gGwEDEUWgERYchhgWApKt6IW+s58I7knGM81rQgQbNdNCO58D
EqaVGmP0Vyb0TTpgvh6f0mr80OuTgWh9bqg4uiOJvbKvlTvDt0o7//mTklm159zr2KT/qFH+9L5i+8iIMX62R5y+a
6E8JV0BrJCNAAAAFQCmK+WOu9HSribsC0f/5dVoADdxEwAAAIA5p7NR74rlSrs0JWWYItNAtE1SamAN+gqCOdUWGPPHT
qdrtBIlPQ9tfFoThZElqY4Tx81ku9laasoRLruQ2Z36R3bQGzIn4jzQqujvvbxTvLK9eLoSr8yFbEE3ZvuUo0+vhDn
LIDX2N65AQSQsTaOrKX+yQZ8yAVt48CsctpsDrgAAAIAVROGlWoSl8g3FFm2eRTa+/oZ+cMjv+pSZiZoiUCoaIlouc
u1ZDpN413QBnf6p/3D8wVD8m5uo8O4N/HXasAMektZvGoP4Sf+shItPuISRv3lrMTEYsD0sqVcMc7vIXUeD2jpOk7MB
```

```
ooVkTZB/rdTbNMfXrhDkNJ2IAPQQiUKVnw==

Before you proceed to the next step, make sure you add the 'Host', Serial Number' and
'User Key'
details to the cluster machine.

Would you like to continue? [Y]> yes

Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster test_cluster

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>

(Cluster test_cluster)>
```

グループの追加

すべてのクラスタには1つ以上のグループが含まれている必要があります。新しいクラスタを作成すると、「**Main_Group**」という名前のデフォルトのグループが自動的に作成されます。しかし、クラスタ内に追加のグループを作成することもできます。次の例は、既存のクラスタ内に追加のグループを作成し、そのグループにマシンを割り当てる方法を示しています。

手順

ステップ1 **clusterconfig** コマンドを実行します。

ステップ2 **addgroup** サブコマンドを選択し、新しいグループの名前を入力します。

ステップ 3 **setgroup** サブコマンドを使用して、新しいグループに割り当てるマシンを選択します。

クラスタの管理

CLI でのクラスタの管理

クラスタに含まれるマシンでは、CLI を異なるモードに切り替えることができます。モードはあるレベルに含まれる特定の（名前の付いた）メンバを表していることを思い出してください。

CLI のモードに応じて、設定が変更される正確な場所が決まります。デフォルトは、ユーザがログインしたマシン（「ログイン ホスト」）を示す「マシン」モードです。

別のモードに切り替えるには、clustermode コマンドを使用します。

表 *155 :* クラスタの管理

コマンドの例	説明
`clustermode`	クラスタ モードへの切り替えを確認するプロンプトが表示されます。
`clustermode group northamerica`	グループ「northamerica」用のグループ モードに切り替わります。
`clustermode machine losangeles.example.com`	マシン「losangeles」用のマシン モードに切り替わります。

CLI プロンプトの表示が現在のモードに変わります。

```
(Cluster Americas)>
```

または

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

マシン モードでは、プロンプトにマシンの完全修飾ドメイン名が表示されます。

設定のコピーと移動

すべての非制限コマンド（制限コマンド （1496 ページ）を参照）に、新しい操作として **CLUSTERSHOW** と **CLUSTERSET** が追加されました。**CLUSTERSHOW** は、コマンド設定のモードを表示するときに使用します（新たに追加された操作 （1496 ページ）を参照）。**CLUSTERSET**

操作は、（現在のコマンドで設定できる）現在の設定をモード間またはレベル間で（たとえば、あるマシンからあるグループへ）移動またはコピーするときに使用します。

コピー すると、現在のモードの設定が保持されます。移動 すると、現在のモードの設定がリセット（クリア）されます。つまり、移動した後は、現在のモードに設定が設定されなくなります。

たとえば、（**destconfig** コマンドで）グループ **northamerica** にグッド ネイバー テーブルを設定し、クラスタ全体にこの設定を適用する場合は、**destconfig** コマンド内で **clusterset** 操作を使って現在の設定をクラスタ モードにコピー（または移動）できます。（新しい設定の実験 （1493 ページ） を参照。）

注意 設定を移動またはコピーするときは、依存関係に矛盾が生じないように注意してください。たとえば、免責事項のスタンプが設定されたリスナーを別のマシンに移動またはコピーしても、その新しいマシンに同じ免責事項が設定されていない場合、新しいマシンでは免責事項のスタンプがイネーブルになりません。

新しい設定の実験

クラスタの最も効果的な使用方法の1つは、新しい設定を実験することです。まず、分離された環境で、マシン モードでの変更を行います。次に、設定に問題がなければ、設定変更を上位のクラスタ モードに移動し、すべてのマシンに適用します。

次の例は、あるマシンでリスナーの設定を変更し、準備ができたらその設定をクラスタの残りのマシンにパブリッシュする手順を示しています。通常、リスナーはクラスタ レベルで設定されるため、この例では最初に設定をあるマシンのマシン モードに格下げしてから、設定の変更を行い、テストしています。このような実験的な変更は、クラスタ内の他のマシンで同じ変更を行う前に、1 つのマシン上でテストする必要があります。

手順

ステップ 1 **clustermode cluster** コマンドを使ってクラスタ モードに変更します。

clustermode コマンドは、モードをクラスタ、グループ、およびマシン レベルに変更するときに使用する CLI コマンドです。

ステップ 2 **listenerconfig** を実行して、クラスタに設定されたリスナーの設定を表示します。

ステップ 3 実験するマシンを選び、clusterset コマンドを使って設定をクラスタから「下位の」マシン モードにコピーします。

ステップ 4 次のように clustermode コマンドを使って実験マシンのマシン モードに移行します。

```
clustermode machine newyork.example.com
```

ステップ 5 実験マシンのマシン モードで listenerconfig コマンドを実行し、実験マシンに固有の変更を行います。

ステップ 6 変更を確定します。

ステップ 7 実験マシン上で設定変更の実験を続行し、必ず変更を確定します。

ステップ 8 新しい設定を他のすべてのマシンに適用する準備ができたら、clustersetコマンドを使って設定を上位のクラスタ モードに移動します。

ステップ 9 変更を確定します。

クラスタからの脱退（削除）

マシンをクラスタから永続的に削除するには、clusterconfig の REMOVEMACHINE 操作を使用します。マシンをクラスタから永続的に削除すると、その設定は「平板化」され、そのマシンはクラスタに含まれていたときと同じように動作します。たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

クラスタ内のマシンのアップグレード

クラスタには、異なるバージョンの AsyncOS を実行しているマシンを接続できません。

AsyncOS のアップグレードをインストールする前に、clusterconfig コマンドを使ってクラスタ内の各マシンを切断する必要があります。すべてのマシンをアップグレードしたら、clusterconfig コマンドを使ってクラスタを再接続します。マシンを同じバージョンにアップグレードする間は、2 つのクラスタを別個に稼働させることができます。また、GUI の [アップグレード（Upgrades）] ページでクラスタ化されたマシンをアップグレードすることもできます。

バックグラウンドでアップグレードをダウンロードできるため、アップグレードをインストールする準備が整うまで、クラスタ内のマシンを切断する必要はありません。

（注） クラスタから個々のマシンを切断する前にアップグレードコマンドを使用すると、AsyncOS によってクラスタ内のすべてのマシンが切断されます。マシンをアップグレードする前に、各マシンをクラスタから切断することを推奨します。各マシンを切断してアップグレードしている間、他のマシンは引き続きクラスタとして動作します。

手順

ステップ 1 クラスタ内のマシン上で、clusterconfig の disconnect 操作を使用します。たとえば、マシン losangeles.example.com を切断するには、clusterconfig disconnect losangeles.example.com と入力します。commit は必要ありません。

ステップ 2 必要に応じて、suspendlistenerコマンドを使ってアップグレード処理中の新しい接続やメッセージの受信を停止します。

ステップ 3 upgrade コマンドを実行して、AsyncOS を新しいバージョンにアップグレードします。

（注） クラスタ内のマシンをすべて切断するように求める警告または確認メッセージは無視してください。マシンがすでに切断されているため、この時点で AsyncOS によってクラスタ内の他のマシンが切断されることはありません。

ステップ 4 マシンの AsyncOS のバージョンを選択します。アップグレードが完了すると、マシンが再起動します。

ステップ 5 アップグレードされたマシン上で resume コマンドを使って新しいメッセージの受信を開始します。

ステップ 6 クラスタ内のマシンごとにステップ 1 ～ 5 を繰り返します。

（注） クラスタからマシンを切断すると、そのマシンを使って他のマシンの設定を変更できなくなります。クラスタの設定を変更することはできますが、設定の同期が取れなくなるため、マシンが切断されている間は設定を変更しないでください。

ステップ 7 すべてのマシンをアップグレードした後で、アップグレードされたマシンごとに clusterconfig の reconnect 操作を実行してマシンを再接続します。たとえば、マシン losangeles.example.com を切断するには、clusterconfig reconnect losangeles.example.com と入力します。クラスタに接続できるのは、同じバージョンの AsyncOS を実行しているマシンだけです。

CLI コマンドのサポート

すべてのコマンドがクラスタに対応

AsyncOS のすべての CLI コマンドがクラスタ対応になりました。一部のコマンドは、クラスタモードで実行したときの動作がやや異なります。たとえば、次のコマンドをクラスタに含まれるマシン上で実行すると、コマンドの動作が変更されます。

commit および clearchanges コマンド

commit

commit コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてで確定します。

commitdetail

commitdetail コマンドは、クラスタ内のすべてのマシンに反映された設定変更の詳細を表示します。

clearchanges

clearchanges（clear）コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてでクリアします。

新たに追加された操作

CLUSTERSHOW

各コマンドに、コマンド設定時のモードを表示する CLUSTERSHOW 操作が追加されました。

下位レベルの既存の設定で上書きされる操作を実行するCLIコマンドを入力すると、通知メッセージが表示されます。たとえば、クラスタモードでコマンドを入力すると、次のような通知メッセージが表示されることがあります。

```
Note: Changes to these settings will not affect the following groups and machines
because they are overriding the cluster-wide settings:

East_Coast, West_Coast

facilities_A, facilities_B, receiving_A
```

グループ モードの設定を編集した場合も、同じようなメッセージが表示されます。

制限コマンド

ほとんどの CLI コマンドとそれに対応する GUI ページは、任意のモード（クラスタ、グループ、マシン）で実行できます。しかし、一部のコマンドとページは1つのモードだけに制限されています。

システム インターフェイスには（GUI と CLI のどちらにも）、コマンドが制限されること、およびどのように制限されるかが必ず明示されます。コマンドを設定するための適切なモードに簡単に切り替えることができます。

- GUI では、[モードを変更（Change Mode）] メニューまたは [この機能の設定は現在、次で定義されています：（Settings for this features are currently defined at:）] リンクを使ってモードを切り替えます。
- CLI では、clustermode コマンドを使ってモードを切り替えます。

表 *156 :* クラスタ モードに制限されるコマンド

clusterconfig	sshconfig
clustercheck	userconfig
passwd	

上記のコマンドをグループ モードまたはマシン モードで実行しようとすると、警告メッセージが表示され、適切なモードに切り替えることができます。

（注） passwd コマンドは、ゲスト ユーザが使用できるようにするための特例です。ゲスト ユーザがクラスタ内のマシン上で passwd コマンドを実行すると、警告メッセージは表示されず、ユーザのモードを変更せずにクラスタ レベルのデータに対して操作が行われます。他のすべてのユーザに対しては、上記の（他の制限されるコンフィギュレーション コマンドと同じ）動作が行われます。

次のコマンドは、マシン モードに制限されます。

antispamstatus	etherconfig	resume	suspenddel
antispamupdate	featurekey	resumedel	suspendlistener
antivirusstatus	hostrate	resumelistener	techsupport
antivirusupdate	hoststatus	rollovernow	tophosts
bouncerecipients	interfaceconfig	routeconfig	topin
deleterecipients	ldapflush	sbstatus	trace
delivernow	ldaptest	setgateway	version
diagnostic	nslookup	sethostname	vofflush
dnsflush	quarantineconfig	settime	vofstatus
dnslistflush	rate	shutdown	workqueue
dnslisttest	reboot	status	
dnsstatus	resetcounters	suspend	

上記のコマンドをクラスタ モードまたはグループ モードで実行しようとすると、警告メッセージが表示され、適切なモードに切り替えることができます。

次のコマンドは、さらにログイン ホスト（ユーザがログインしているマシン）に制限されます。これらのコマンドを使用するには、ローカル ファイル システムにアクセスできる必要があります。

表 *157*：ログイン ホスト モードに制限されるコマンド

last	resetconfig	tail	upgrade
ping	supportrequest	telnet	who

GUI でのクラスタの管理

GUI では、クラスタの作成、クラスタへの参加、およびクラスタ固有の設定の管理（**clusterconfig** コマンドと同等の操作）を行うことはできませんが、クラスタ内のマシンの参照、設定の作成や削除、およびクラスタ間、グループ間、マシン間での設定のコピーや移動（つまり、**clustermode** および **clusterset** と同等の操作）を行うことができます。

[受信メールの概要（Incoming Mail Overview）] ページは、表示しているメール フロー モニタリングのデータがローカル マシンに格納されるため、ログイン ホストに制限されるコマンドの例です。別のマシンの [受信メールの概要（Incoming Mail Overview）] レポートを表示するには、そのマシンの GUI にログインする必要があります。

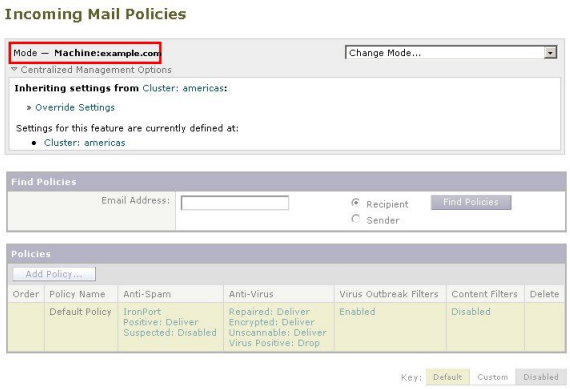
電子メールゲートウェイ上でクラスタリングがイネーブルになっている場合は、ブラウザのアドレスフィールドの URL に注意してください。この URL には、必要に応じて **machine**、**group**、または **cluster** という単語が含まれています。たとえば、最初にログインしたときの [受信メールの概要（Incoming Mail Overview）] ページの URL は次のように表示されます。

https://ホスト名/**machine**/連番**/monitor/incoming_mail_overview**

（注） [モニタ（Monitor）] メニューの [受信メールの概要（Incoming Mail Overview）] ページと [受信メールの詳細（Incoming Mail Details）] ページは、ログイン マシンに制限されます。

[メールポリシー（Mail Policies）]、[セキュリティサービス（Security Services）]、[ネットワーク（Network）]、[システム管理（System Administration）] の各タブには、ローカル マシンに制限されないページが表示されます。[メールポリシー（Mail Policies）] タブをクリックすると、GUI 内の中央集中型管理情報が変更されます。

図 *80 : GUI* の中央集中型管理機能：設定が規定されていない場合



上の図では、このマシンの現在の機能に関する設定がクラスタ モードから継承されています。継承された設定は薄いグレーで表示（プレビュー）されます。これらの設定を保持することも、クラスタ レベルの設定をこのマシン用に上書きして変更することも可能です。

（注） 継承された設定（プレビュー表示）には、常にクラスタから継承した設定が表示されます。グループ レベルとクラスタ レベルの間で依存するサービスをイネーブルまたはディセーブルにするときは注意してください。詳細については、設定のコピーと移動 （1492 ページ）を参照してください。

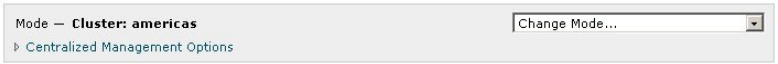
[設定を上書き（Override Settings）] リンクをクリックすると、この機能に対応する新しいページが表示されます。このページでは、マシン モードの新しい設定を作成できます。デフォルト設定をそのまま使用することもできますが、別のモードですでに設定している場合は、それらの設定をこのマシンにコピーすることもできます。

図 *81 : GUI* の中央集中型管理機能：新しい設定の作成

または、図「GUI の中央集中型管理機能：設定が規定されていない場合」に示すように、この設定がすでに定義されているモードに移動することもできます。これらのモードは、中央集中型管理ボックスの下部にある [この機能の設定は現在、次で定義されています：（Settings for this feature are currently defined at:）] に表示されます。ここには、設定が実際に規定されているモードだけが表示されます。別のモードで規定された（別のモードから継承された）設定のページを表示すると、ページ上にそれらの設定が表示されます。

表示されたいずれかのモード（たとえば、図「GUI の中央集中型管理機能：設定が規定されていない場合」に示す [クラスタ：南/北/中央アメリカ（Cluster: Americas）] リンク）をクリックすると、そのモードの設定を表示して管理できる新しいページが表示されます。

図 *82 : GUI* の中央集中型管理機能：定義された設定



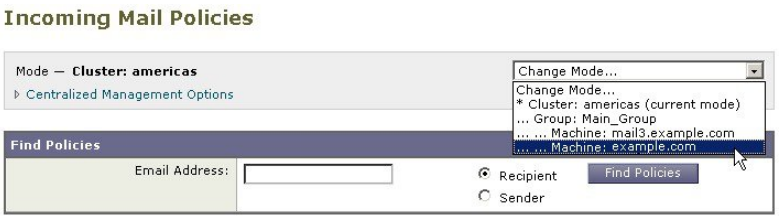
特定のモードで設定を規定すると、中央集中型管理ボックスがすべてのページに最小化された状態で表示されます。[集約管理オプション（Centralized Management Options）] リンクをクリックすると、ボックスが展開され、現在のモードで現在のページに関して設定できるオプションのリストが表示されます。[設定を管理（Manage Settings）] ボタンをクリックすると、現在の設定を別のモードにコピーまたは移動したり、設定を完全に削除したりできます。

たとえば、次の図では、[集約管理オプション（Centralized Management Options）] リンクがクリックされ、設定可能なオプションが表示されています。

図 *83 : GUI* の中央集中型管理機能：設定の管理

ボックスの右側には [モードを変更（Change Mode）] メニューが表示されます。このメニューには現在のモードが表示され、このメニューを使っていつでも他のモード（クラスタ、グループ、またはマシン）に移動できます。

図 *84 : [*モードを変更（*Change Mode*）*]* メニュー



別のモードを表すページに移動すると、中央集中型管理ボックスの左側にある「モード—」というテキストが一時的に黄色で点滅し、モードが変更されたことを知らせます。

特定のタブに含まれる一部のページは、マシンモードに制限されています。ただし、（現在のログイン ホストに制限される）[受信メールの概要（Incoming Mail Overview）] ページとは異なり、これらのページはクラスタ内のどのマシンでも使用できます。

図 *85 :* 中央集中型管理機能：マシンに制限される機能

[モードを変更（Change Mode）] メニューから管理するマシンを選択します。テキストが一時的に点滅し、モードが変更されたことを知らせます。

クラスタ通信

クラスタ内のマシンは、メッシュ ネットワークを使って相互に通信します。デフォルトでは、すべてのマシンが他のすべてのマシンに接続します。1 つのリンクが切断されても、他のマシンが更新を受信できなくなることはありません。

デフォルトでは、クラスタ内のすべての通信が SSH を使って保護されます。各マシンは、ルートテーブルのコピーをメモリ内に保持し、リンクの切断と確立に応じてメモリ内のテーブルを変更します。また、クラスタに含まれる他のすべてのマシンに対して定期的に（1 分間隔で）「ping」を実行します。これにより、リンクの最新状態を確認し、ルータや NAT がタイムアウトした場合でも接続を維持します。

（注） 電子メールゲートウェイがクラスタモードであり、他の電子メールゲートウェイのデータにリモートでアクセスする（設定関連ではなく、たとえば隔離内に存在するメッセージを表示したり、レポートの更新を高速化したりする）計画がある場合、クラスタの再接続が試行され、その結果、アラートやエラーが生成される場合があります。電子メールゲートウェイは自動的に再接続されるため、手動による介入は不要です。

DNS とホスト名の解決

マシンをクラスタに接続するには、DNS が必要です。クラスタの通信は、通常、（マシン上のインターフェイスのホスト名ではなく）マシンの DNS ホスト名を使って開始されます。ホスト名を解決できないマシンは、形式的にはクラスタに含まれていても、実際にはクラスタ内の他のマシンと通信できません。

ホスト名が電子メールゲートウェイ上の SSH または CCS をイネーブルにした正しい IP インターフェイスを指すように、DNS を設定する必要があります。これは非常に重要です。DNS が SSH または CCS をイネーブルにしていない別の IP アドレスを参照すると、ホストが見つかりません。中央集中型管理では、インターフェイスごとのホスト名ではなく、sethostname コマンドで設定した「メイン ホスト名」が使用されます。

IP アドレスを使ってクラスタ内の他のマシンに接続する場合は、接続先のマシンが接続元の IP アドレスの逆ルックアップを実行できる必要があります。DNS 内にその IP アドレスがないために逆ルックアップがタイムアウトすると、そのマシンはクラスタに接続できません。

クラスタリング、完全修飾ドメイン名、およびアップグレード

AsyncOS をアップグレードすると、DNS の変更によって接続が失われることがあります。（クラスタ内のマシン上のインターフェイスのホスト名ではなく）クラスタ内のマシンの完全修飾ドメイン名を変更する必要がある場合は、AsyncOS をアップグレードする前に、sethostname を使ってホスト名の設定を変更し、そのマシンの DNS レコードを更新する必要があることに注意してください。

クラスタ通信のセキュリティ

Cluster Communication Security（CCS）は、標準の SSH サービスに似たセキュア シェル サービスです。シスコが CCS を実装したのは、クラスタ通信に標準の SSH を使用することに対する懸念に応えるためです。マシン間の SSH 通信では、同じポートで（管理者などの）通常のログインを開きます。多くの管理者は、クラスタ化されたマシン上で通常のログインを開くことを好みません。

ヒント：CCS はデフォルトですが、クラスタ化されたマシン間のポート 22 の通信がファイアウォールによってブロックされない場合は、CCS をイネーブルにしないでください。クラスタリングでは、すべてのマシン間でフル メッシュの SSH トンネル（ポート 22 上）が使用されます。いずれかのマシンですでに CCS をイネーブルにした場合は、クラスタからすべてのマシ

ンを削除し、最初からやり直してください。クラスタ内の最後のマシンを削除すると、クラスタが削除されます。

CCSは、管理者がCLIへのログインではなく、クラスタ通信を開始できるように強化されています。デフォルトでは、このサービスはディセーブルです。interfaceconfigコマンドで他のサービスをイネーブルにするためのプロンプトが表示されたときに、CCSをイネーブルにするかどうかの選択を求められます。次に例を示します。

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

Which port do you want to use for SSH?

[22]>

Do you want to enable Cluster Communication Service on this interface?

[N]> y

Which port do you want to use for Cluster Communication Service?

[2222]>
```

CCS のデフォルトのポート番号は 2222 です。必要な場合は、これを別の開いている未使用のポート番号に変更できます。マシンの参加が完了し、参加したマシンにクラスタのすべての設定データが適用されると、次の質問が表示されます。

```
Do you want to enable Cluster Communication Service on this interface? [N]> y


Which port do you want to use for Cluster Communication Service?

[2222]>
```

クラスタの整合性

「クラスタ対応」のマシンは、クラスタ内の他のマシンへのネットワーク接続を継続的に確認します。この確認は、クラスタ内の他のマシンに対する定期的な「ping」によって行われます。

特定のマシンとの通信の試行がすべて失敗すると、通信を試行したマシンはリモートホストが切断されたことを示すメッセージをログに記録します。システムはリモートホストがダウンしたことを示すアラートを管理者に送信します。

マシンがダウンしても、確認用の ping は引き続き送信されます。マシンがクラスタのネットワークに再び参加すると、それまでオフラインだったマシンが更新をダウンロードできるように、同期コマンドが実行されます。この同期コマンドは、一方のマシンに含まれる変更がもう一方のマシンに含まれるかどうかも判定します。含まれない場合は、それまでダウンしていたマシンが更新をサイレントでダウンロードします。

切断/再接続

マシンは、クラスタから切断できます。時折、たとえばマシンをアップグレードするために、マシンを意図的に切断することがあります。切断は、たとえば停電やソフトウェアまたはハー

ドウェアのエラーのために突発的に起きることもあります。1 台の電子メールゲートウェイがセッションで許可されている SSH 接続の最大数を超えて開こうとする場合も、切断が起きることがあります。クラスタから切断されたマシンに直接アクセスしてマシンを設定することはできますが、切断されたマシンを再接続するまでは、クラスタ内の他のマシンに変更が反映されません。

マシンをクラスタに再接続すると、そのマシンはただちにすべてのマシンに再接続しようとします。

理論的には、クラスタから2台のマシンを切断した場合、同じような変更が各マシンのローカルデータベースに同時に確定される可能性があります。これらのマシンをクラスタに再接続すると、これらの変更の同期が試行されます。競合がある場合は、最新の変更が記録されます（他の変更はすべて破棄されます）。

電子メールゲートウェイは、変更されるすべての変数を確定時にチェックします。確定データには、バージョン情報、連番 ID、その他の比較可能な情報が含まれます。変更しようとしているデータが以前の変更と競合することがわかった場合は、変更を破棄するオプションが表示されます。たとえば、次のようなメッセージが表示されます。

```
(Machine mail3.example.com)> clustercheck

This command is restricted to "cluster" mode. Would you like to switch to "cluster"

mode? [Y]> y

Checking Listeners (including HAT, RAT, bounce profiles)...

Inconsistency found!

Listeners (including HAT, RAT, bounce profiles) at Cluster enterprise:

mail3.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

test.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

How do you want to resolve this inconsistency?

1. Force entire cluster to use test.example.com version.


2. Force entire cluster to use mail3.example.com version.

3. Ignore.

[1]>
```

変更を破棄しなかった場合、変更は（確定されませんが）保持されます。変更を現在の設定に照らして確認し、その後の処理方法を決めることができます。

また、いつでも `clustercheck` コマンドを使ってクラスタが正常に動作していることを確認できます。

```
losangeles> clustercheck
```

```
Do you want to check the config consistency across all machines in the cluster? [Y]> y

Checking losangeles...

Checking newyork...

No inconsistencies found.
```

互いに依存する設定

電子メールゲートウェイでは次の設定を行わないことをお勧めします。

中央集中型管理環境では、互いに依存する設定が異なるモードで設定されることがあります。設定モデルの高い柔軟性によって複数のモードで設定できるため、個々のマシンでどの設定が使用されるかは継承の法則に基づいて決まります。しかし、一部の設定は他の設定に依存しており、依存する設定の適用範囲は同じモードの設定に制限されません。したがって、あるレベルで特定のマシン用に設定された設定を参照する設定を別のレベルで設定することも可能です。

互いに依存する設定の最も一般的な例は、ページ上の別のクラスタ セクションからデータを取得する選択フィールドに関するものです。たとえば、次の機能をそれぞれ異なるモードで設定できます。

- LDAP クエリーの使用
- ディクショナリまたはテキスト リソースの使用
- バウンス プロファイルまたは SMTP 認証プロファイルの使用。

中央集中型管理には、制限コマンドと非制限コマンドがあります。（制限コマンド（1496ページ）を参照。）非制限コマンドは、通常、クラスタ全体で共有できるコンフィギュレーション コマンドです。

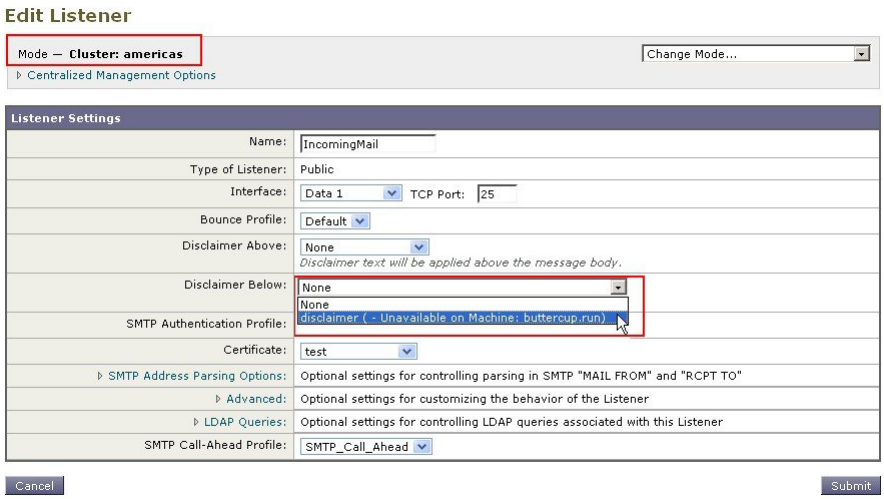
listenerconfig コマンドは、クラスタ内のすべてのマシンに設定できるコマンドの例です。非制限コマンドは、クラスタ内のすべてのマシンに反映できるため、マシンごとにデータを変更する必要がないコマンドです。

一方、制限コマンドは特定のモードだけに適用されるコマンドです。たとえば、ユーザを特定のマシン用に設定することはできません。ユーザはクラスタ全体に1セットしか設定できません（そうしないと、同じログイン名でリモート マシンにログインすることができなくなります）。同じように、メールフローモニタのデータ、システム概要のカウンタ、およびログファイルは、マシン単位でしか保持されないため、これらのコマンドやページはマシンだけに制限する必要があります。

定期レポートはクラスタ全体で同じに設定できますが、レポートの表示はマシン別に行われます。したがって、GUI の [定期レポート（Scheduled Reports）] ページは 1 つでも、設定はクラスタ モードで行い、レポートの表示はマシン モードで行う必要があります。

[システム時刻（System Time）] のページには、**settz**、**ntpconfig**、**settime** の各コマンドが含まれ、制限コマンドと非制限コマンドが混在しています。この場合、settime は（時間の設定がマシンに固有のものであるため）マシン モードだけに制限する必要がありますが、**settz** と **ntpconfig** はクラスタ モードまたはグループ モードで設定できます。

図 *86* : 互いに依存する設定の例



この図では、リスナー「IncomingMail」がマシン レベルでのみ設定された「disclaimer」という名前のフッターを参照しています。使用可能なフッター リソースのドロップダウン リストには、クラスタでは使用できるのにマシン「buttercup.run」では使用できないフッターが表示されています。このジレンマを解消するには、次の 2 つの方法があります。

- フッター「disclaimer」をマシン レベルからクラスタ レベルに格上げする
- リスナーをマシン レベルに格下げして、相互依存を解消する

中央集中型管理されたシステムの特長を最大限に活かすためには、1 つめの方法を推奨します。クラスタ化されたマシンの設定を調整するときは、設定間の相互依存に注意してください。

クラスタ化された電子メールゲートウェイの設定のロード

AsyncOS では、クラスタ化された電子メールゲートウェイにクラスタ設定をロードできます。次のようなシナリオでクラスタ設定をロードできます。

- オンプレミス環境からホスト環境に移行する際に、オンプレミスのクラスタの設定をホスト環境に移行する場合。
- クラスタ内の電子メールゲートウェイがダウンしたまたは廃棄する必要があり、その電子メールゲートウェイから、クラスタに追加する予定の新しい電子メールゲートウェイに設定をロードする場合。
- 電子メールゲートウェイをクラスタに追加するときに、クラスタ内の既存の電子メールゲートウェイの 1 つから新しく追加した電子メールゲートウェイに設定をロードする場合。
- バックアップ設定をクラスタにロードする場合。

必要に応じて、クラスタの設定または電子メールゲートウェイの設定を有効なクラスタ設定ファイルからロードできます。

（注） スタンドアロン電子メールゲートウェイの設定をクラスタ化電子メールゲートウェイにロードすることはできません。

はじめる前に

- 有効で完全な XML コンフィギュレーション ファイルがあることを確認します。コンフィギュレーション ファイルのロード （1245 ページ）を参照してください。
- 設定のロード先とする電子メールゲートウェイの現在の設定のバックアップを作成します。現在の設定ファイルの保存およびエクスポート （1244 ページ）を参照してください。
- セットアップに含める予定のすべての電子メールゲートウェイを使用してクラスタのセットアップを作成します。クラスタの作成とクラスタへの参加 （1484 ページ）を参照してください。

（注） 1 つのグループにすべての電子メールゲートウェイを含めることができます。セットアップのクラスタ通信用インターフェイスの名前と SSH および CCS 設定が、XML コンフィギュレーション ファイルでの設定と同じであることを確認します。

手順

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] をクリックします。

ステップ 2 [モード（Mode）] ドロップダウン メニューからクラスタを選択します。

ステップ 3 クラスタの設定と電子メールゲートウェイの設定のどちらをロードするかに応じて、次のいずれかを実行します。

- **クラスタの設定のロード**

  1. [設定をロード（Load Configuration）] セクションで、ドロップダウン リストから [クラスタ（Cluster）] を選択します。
  2. [ロード（Load）] をクリックしてクラスタの設定をロードします。コンフィギュレーション ファイルのロード （1245 ページ）を参照してください。
  3. ロードされた設定からクラスタの電子メールゲートウェイにグループを割り当て、選択したグループの電子メールゲートウェイから電子メールゲートウェイの設定をそれぞれの電子メールゲートウェイにコピーします。[グループ設定（Group Configuration）] および [アプライアンス設定（Appliance Configuration）] ドロップダウン リストを使用します。

     電子メールゲートウェイの設定をコピーしない場合は、**[アプライアンス設定（Appliance Configuration）]** ドロップダウンリストから **[コピー禁止（Don't Copy）]** を選択します。

     1. 設定の内容を確認します。[レビュー（Review）] をクリックします。

2. [確認（Confirm）] をクリックします。
3. [続行（Continue）] をクリックします。

- 電子メールゲートウェイの設定のロード

1. [設定をロード（Load Configuration）] セクションで、ドロップダウン リストから [クラスタのアプライアンス（Appliance in cluster）] を選択します。
2. [ロード（Load）]をクリックして設定をロードします。コンフィギュレーション ファイルのロード（1245 ページ）を参照してください。スタンドアロン電子メールゲートウェイの設定をクラスタ化電子メールゲートウェイにロードすることはできないことに注意してください。
3. ロードした設定から電子メールゲートウェイの設定を選択し、その設定をロードする、クラスタ内の対象電子メールゲートウェイを選択します。ドロップダウンリストを使用します。
4. [OK] をクリックします。
5. [続行（Continue）] をクリックします。
6. 電子メールゲートウェイの設定を複数の電子メールゲートウェイにコピーするには、ステップ **a** ～ **e** を繰り返します。

ステップ 4 クラスタ化された電子メールゲートウェイのネットワーク設定を確認してから、変更を確定します。

ベスト プラクティスとよく寄せられる質問（FAQ）

ベストプラクティス

クラスタを作成すると、現在ログインしているマシンが自動的に最初のマシンとしてクラスタに追加され、Main_Group にも追加されます。マシン レベルの設定は、できる限りクラスタ レベルに移動されます。グループ レベルの設定は存在せず、マシン レベルに残された設定は、クラスタ レベルでは意味を成さないのでクラスタ化できません。例として、IP アドレスやライセンス キーなどがあります。

設定はできる限りクラスタ レベルに残します。クラスタ内の 1 つのマシンにだけ異なる設定が必要な場合は、そのクラスタ設定をそのマシンのマシン レベルにコピーします。この場合は、設定を移動しないでください。工場出荷時のデフォルト値がない設定（HAT テーブル、SMTPROUTES テーブル、LDAP サーバ プロファイルなど）を移動すると、クラスタ設定を継承するシステムに空のテーブルが作成され、電子メールが処理されなくなるおそれがあります。

マシンにクラスタ設定を再度継承させるには、CM の設定を管理し、マシンの設定を削除します。マシンがクラスタ設定を上書きするかどうかは、次のメッセージが表示されたときにわかります。

Settings are defined:

To inherit settings from a higher level: Delete Settings for this feature at this mode.

You can also Manage Settings.

Settings for this feature are also defined at:

Cluster: xxx

または、次のメッセージが表示されます。

Delete settings from:

Cluster: xxx

Machine: yyyy.domain.com

コピーと移動の違い

コピーする必要がある場合：クラスタに設定を作成し、グループまたはマシンには設定を作成しないか、別の設定を作成する場合。

移動する必要がある場合：クラスタには設定を作成せず、グループまたはマシンに設定を作成する場合。

適切な CM の設計方法

LIST 操作で CM マシンのリストを出力すると、次のように表示されます。

cluster = CompanyName

Group Main_Group:

Machine lab1.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab2.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Paris:

Machine lab3.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab4.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Rome:

Machine lab5.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab6.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

現在変更しているレベルを忘れないように注意してください。たとえば、（RENAMEGROUP を使って）Main_Group の名前を変更した場合は、次のように表示されます。

cluster = CompanyName

Group London:

Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)

...

しかし、最初にグループ レベルで London のシステムを変更すると、クラスタ レベルを基本的な設定を行うための通常の設定レベルとして使用しなくなるため、このような設定は管理者にとって混乱の元です。

ヒント：グループにクラスタと同じ名前を付けること（クラスタ「London」とグループ「London」など）は推奨しません。グループ名としてサイト名を使用する場合、クラスタに場所を表す名前を付けることは推奨しません。

正しい方法は、前述のように、できるだけ多くの設定をクラスタ レベルに残すことです。ほとんどの場合、プライマリ サイトや主要なマシン群を Main_Group に残し、グループを追加のサイト用に使用してください。これは、両方のサイトを「同等」に扱う場合にも当てはまります。CM にはプライマリ/セカンダリのサーバがなく、クラスタ化されたすべてのマシンがピアになることを思い出してください。

ヒント：追加のグループを使用する場合は、マシンをクラスタに追加する前にグループを簡単に準備できます。

クラスタのセットアップでスパム隔離またはポリシー隔離へアクセスするためのベスト プラクティス

ログインしている電子メールゲートウェイからクラスタ内の他のアプライアンスのスパム隔離またはポリシー隔離にアクセスすると、ログインしている電子メールゲートウェイの CPU 使用率を過度に増加させる原因となる場合があります。この状況を回避するには、必要な電子メールゲートウェイにログインして、スパム隔離またはポリシー隔離にアクセスします。

手順：サンプル クラスタの設定

このサンプル クラスタを設定するには、clusterconfig を実行する前に、すべてのマシン上ですべての GUI からログアウトします。プライマリ サイトのいずれかのマシン上で clusterconfig を実行します。次に、他のローカル マシンとリモート マシンのうち、（IP アドレスなどのマシン専用の設定を除いて）できるだけ多くの設定を共有する必要があるマシンだけをこのクラスタに追加します。clusterconfig コマンドを使ってリモート マシンをクラスタに追加することはできません。リモート マシン上の CLI を使って clusterconfig（既存のクラスタへの参加）を実行する必要があります。

前述の例では、lab1 にログインし、clusterconfig を実行して CompanyName という名前のクラスタを作成しています。同じ要件のマシンは 1 つしかないので、lab2 にログインし、saveconfig で既存の設定を保存します（この設定は lab1 の設定のほとんどを継承して大幅に変更されます）。次に、lab2 上で clusterconfig を使って既存のクラスタに参加します。他にも同じようなポリシーと設定を必要とするマシンがこのサイトにある場合は、上記の手順を繰り返します。

CONNSTATUS を実行して、DNS でホスト名が正しく解決されることを確認します。マシンがクラスタに追加されると、新しいマシンのほとんどの設定は lab1 から継承され、古い設定は消失します。追加されたマシンが運用マシンである場合は、これまでの設定の代わりに新しい設定を使ってメールが引き続き処理されるかどうかを予測する必要があります。マシンをクラスタから削除しても、そのマシンが古い専用の設定に戻ることはありません。

次に、例外となるマシンの数を数えます。例外が 1 台しかない場合は、マシン レベルの設定をいくつか追加すればよく、そのマシン用に追加のグループを作成する必要はありません。そのマシンをクラスタに追加し、設定をマシン レベルにコピーする作業を始めます。このマシンが既存の運用マシンである場合は、設定をバックアップし、前述のように電子メール処理の変更を検討する必要があります。

前述の例のように、例外が2台以上ある場合は、それらのマシンがクラスタで共有されない設定を共有するかどうかを判断します。共有する場合は、これらのマシン用のグループを1つ以上作成します。共有しない場合は、各マシンでマシン レベルの設定を作成すればよく、追加のグループを作成する必要はありません。

前述の例では、クラスタにすでに含まれているいずれかのマシン上で CLI の clusterconfig を実行し、ADDGROUP を選択する必要があります。この作業を 2 回行います（Paris に対して 1 回、Rome に対して 1 回）。

これで、GUI と CLI を使ってクラスタ用の設定とすべてのグループ（まだマシンがないグループも含む）用の設定を作成できます。各マシンのマシン固有の設定を作成できるようになるのは、マシンをクラスタに追加した後 です。

上書き（例外）用の設定を作成する最適な方法は、上位レベル（クラスタなど）から下位レベル（グループなど）に設定をコピーすることです。

たとえば、クラスタを作成した後の dnsconfig の初期設定は次のようになりました。

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: No

Group Rome: No

Machine lab2.cable.nu: No

この DNS の設定を「グループにコピー」すると、次のようになります。

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: Yes

Group Rome: No

Machine lab2.cable.nu: No

ここで、Paris グループ レベルの DNS の設定を編集すると、Paris グループの他のマシンはその設定を継承します。Paris グループ以外のマシンは、マシン固有の設定がない限り、クラスタの設定を継承します。DNS の設定に加えて、SMTPROUTES の設定もグループ レベルで作成するのが一般的です。

ヒント CLI のさまざまなメニューで CLUSTERSET 機能を使用するときは、設定をすべてのグループにコピーする特別なオプションを使用できます。このオプションは GUI では使用できません。

完成されたリスナーは、グループまたはクラスタから自動的に継承されるため、通常はクラスタ内の最初のシステム上でのみリスナーを作成します。これによって管理作業が大幅に軽減されます。ただし、そのためにはグループまたはクラスタ全体でインターフェイスに同じ名前を付ける必要があります。

設定をグループ レベルで正しく規定した後は、マシンをクラスタに追加し、このグループに含めることができます。これには次の 2 つの手順が必要です。

まず、残りの 4 つのシステムをクラスタに追加するため、各システム上で clusterconfig を実行します。大きく複雑なクラスタほど、追加処理にかかる時間も長くなり、数分かかることもあります。LIST および CONNSTATUS サブコマンドを使って追加処理の進行状況をモニタできます。追加処理が完了したら、SETGROUP を使ってマシンを Main_Group から Paris および Rome に移動します。クラスタに追加されたすべてのマシンが最初に Paris や Rome の設定ではなく Main_Group の設定を継承することは避けられません。これは、新しいシステムがすでに稼働中である場合、メール フローのトラフィックに影響する可能性があります。

ヒント 試験用マシンを運用マシンと同じクラスタに含めないでください。試験用システムには新しいクラスタ名を使用してください。これによって、予期しない変更（たとえば、誰かが試験用システムを変更し、誤って運用メールを消失するなど）に対する防御層が追加されます。

GUI でクラスタのデフォルト以外の CM 設定を使用する場合のオプションの要約

設定の上書き（デフォルトの設定から開始）。たとえば、SMTPROUTES 設定のデフォルトの設定は空のテーブルであり、テーブルを最初から作成できます。

設定の上書き（ただし、クラスタ「xxx」またはグループ「yyy」から現在継承している設定のコピーから開始）。たとえば、SMTPROUTES テーブルの新しいコピーをグループ レベルで使用できます。このテーブルは、初期状態ではクラスタのテーブルとまったく同じです。（SETGROUP で）同じグループに追加されたすべての電子メールゲートウェイにこのテーブルが適用されます。このグループに含まれないマシンでは、引き続きクラスタ レベルの設定が使用されます。この独立したテーブルで SMTPROUTES を変更しても、他のグループ、クラスタの設定を継承するマシン、および個々のマシン レベルで設定が規定されているマシンには影響しません。これが最も一般的な選択です。

中央集中型管理オプションのサブメニューである [設定を管理（Manage Settings）]。このメニューでは、上記のように設定をコピーできますが、設定を移動または削除することもできます。SMTPROUTES をグループまたはマシン レベルに移動すると、ルート テーブルはクラスタ レベルでは空になり、より具体的なレベルに存在することになります。

[設定を管理（Manage Settings）]。同じ SMTPROUTES の例で削除オプションを使用した場合も、クラスタの SMTPROUTES テーブルが空になります。SMTPROUTES をグループ レベルまたはマシン レベルですでに設定している場合は、これで問題ありません。クラスタ レベルの設定を削除し、グループまたはマシンの設定だけに依存することは推奨しません。クラスタ全体の設定は、新しく追加したマシンに対するデフォルトとして有用であり、これを保持することによって、管理する必要があるグループまたはサイトの設定の数が 1 つ減ります。

セットアップと設定に関する質問

Q. これまでスタンドアロンとして設定されていたマシンがあり、既存のクラスタに参加しました。これまでの設定はどうなりますか。

A. マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。クラスタに参加した時点で、ローカルで設定されたネットワーク以外の設定は消失し、クラスタや関連するグループの設定で上書きされます。（これにはユーザ/パスフレーズのテーブルも含まれ、パスフレーズとユーザはクラスタ内で共有されます）。

Q. クラスタ化されたマシンがあり、それをクラスタから（永続的に）削除しました。これまでの設定はどうなりますか。

A.マシンをクラスタから永続的に削除すると、その設定階層は「平板化」され、そのマシンは引き続きクラスタに含まれていたときと同じように動作します。マシンに継承されたすべての設定が、スタンドアロンとして設定されたマシンに適用されます。

たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

一般的な質問

Q. 中央集中型で管理されるマシンの間でログ ファイルは集約されますか。

A. いいえ。ログ ファイルは引き続き個々のマシンごとに保持されます。Cisco Secure Manager Email and Web Gateway を使って複数のマシンのメールログを集約し、トラッキングやレポート作成に利用できます。

Q. ユーザー アクセスはどうなりますか。

A.電子メールゲートウェイはクラスタ全体で 1 つのデータベースを共有します。特に、admin アカウント（およびパスフレーズ）は、クラスタ全体で 1 つしかありません。

Q. データセンターをクラスタ化するにはどうすればよいですか。

A.データセンターは、それ自体をクラスタにせずに、クラスタ内の「グループ」にするのが理想的です。しかし、データセンター間で共有する設定が多くない場合は、各データセンターを別個のクラスタにした方がうまくいく場合があります。

Q. オフラインのシステムを再接続するとどうなりますか。

A. クラスタにシステムを再接続すると、システム間の同期が試行されます。

ネットワークに関する質問

Q. 中央管理機能は「ピアツーピア」アーキテクチャと「プライマリ/セカンダリ」アーキテクチャのどちらですか。

A：すべてのマシンにすべてのマシン用のあらゆるデータ（使用されないマシン固有の設定を含む）があるため、中央集中型管理機能は「ピアツーピア」アーキテクチャと見なすことができます。

Q. ピアにならないようにアプライアンスをセットアップするにはどうすればよいですか。「セカンダリ」システムが必要です。

A. このアーキテクチャでは、本物の「セカンダリ」マシンは設定できません。しかし、マシンレベルで HTTP（GUI）アクセスと SSH（CLI）アクセスをディセーブルにすることは可能です。このように GUI アクセスや CLI アクセスができないマシンは、clusterconfig コマンドでのみ 設定可能です（つまり、ログイン ホストではなくなります）。これはセカンダリマシンを設定するのに似ていますが、ログインアクセスを再度イネーブルにすると、この設定は無効になります。

Q. 複数のセグメント化されたクラスタを作成できますか。

A. クラスタを「島」のように分離することは可能です。実際、たとえばパフォーマンス上の理由などで、このようなクラスタを作成するのが有益な場合もあります。

Q. クラスタ化された電子メールゲートウェイのうち、1 台の IP アドレスとホスト名を再設定したいのですが、再設定した場合、再起動コマンドを実行できるようになる前に GUI/CLI セッションが終了しませんか。

A. 次の手順に従ってください。

1. 新しい IP アドレスを追加します。
2. リスナーを新しいアドレスに移動します。
3. クラスタを脱退します。
4. ホスト名を変更します。
5. どのマシンから表示した clusterconfig の接続リストにも、古いマシン名が表示されないことを確認します。
6. すべての GUI セッションがログアウトしたことを確認します。
7. （interfaceconfig または [ネットワーク（Network）] > [リスナー（Listeners）] を使って）どのインターフェイスでも CCS がイネーブルになっていないことを確認します。
8. マシンを再びクラスタに追加します。

Q. 送信先コントロール機能をクラスタ レベルで適用できますか。それともこの機能はローカル マシン レベル専用ですか。

A. クラスタ レベルでも設定できますが、制限はマシン単位で適用されます。したがって、接続を 50 個に制限すると、クラスタ内のそれぞれのマシンにその制限が設定されます。

計画と設定

Q：クラスタをセットアップするときに、効率を最大限に高め、問題を最小限に抑えるにはどうすればよいですか。

1. 初期の計画
   - できるだけ多くの項目をクラスタ レベルで設定します。
   - 例外のみをマシン単位で管理します。
   - データセンターが複数ある場合は、たとえば、グループを使ってクラスタ共通でもマシン固有でもない特性を共有します。
   - 各電子メールゲートウェイのインターフェイスとリスナーに同じ名前を使用します。
2. 制限コマンドに注意してください。
3. 設定間の相互依存に注意してください。

   たとえば、listenerconfig コマンドは、（クラスタ レベルでも）マシン レベルにしか存在しないインターフェイスに依存します。クラスタ内のどのマシンにもマシン レベルのインターフェイスが存在しない場合、そのリスナーはイネーブルになります。

   インターフェイスの削除も listenerconfig に影響します。
4. 設定に注意してください。

   すでに設定されているマシンがクラスタに参加すると、そのマシン単独の設定は消失します。前に設定した設定の一部を再び適用する場合は、クラスタに参加する前にすべての設定をメモしてください。

   「切断された」マシンは、まだクラスタに含まれています。マシンを再接続すると、オフライン中に行った変更がクラスタの他のマシンと同期化されます。

   マシンをクラスタから永続的に削除すると、そのマシンはクラスタのメンバとして持っていたすべての設定を保持します。しかし、考えを変えて再びそのマシンをクラスタに追加すると、そのマシンのスタンドアロンの設定はすべて消失します。

   saveconfig コマンドを使って設定の記録を取ってください。

第 46 章

テストとトラブルシューティング

この章は、次の項で構成されています。

- テスト メッセージを使用したメール フローのデバッグ：トレース （1515 ページ）
- 電子メールゲートウェイのテストにリスナーを使用 （1523 ページ）
- ネットワークのトラブルシューティング （1527 ページ）
- リスナーのトラブルシューティング （1532 ページ）
- アプライアンスからの電子メール配信のトラブルシューティング （1534 ページ）
- パフォーマンスのトラブルシューティング （1536 ページ）
- Web インターフェイスの外観およびレンダリングの問題 （1538 ページ）
- アラートへの応答 （1538 ページ）
- ハードウェア問題のトラブルシューティング （1538 ページ）
- 電子メールゲートウェイの電源のリモートリセット （1538 ページ）
- テクニカル サポートの使用 （1539 ページ）

テストメッセージを使用したメールフローのデバッグ：トレース

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

（注） トレースは、ファイル レピュテーション スキャンのテストには効果がありません。

[トレース（Trace）] ページ（および **trace** CLI コマンド）では、次の表に示されている入力パラメータのプロンプトが表示されますテーブル。

表 *158 : [*トレース（*Trace***）*]* ページに対する入力**

値	説明	例
ソース IP アドレス	リモートドメインの送信元を模倣するため、リモート クライアントの IP アドレスを入力します。これは、インターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）アドレスを指定できます。 注：trace コマンドを実行すると、IP アドレスと完全修飾ドメイン名の入力が求められます。完全修飾ドメイン名が一致するかどうかを確認するための IP アドレスの逆引きは行われません。trace コマンドでは、完全修飾ドメイン名フィールドを空白にすることはできないため、DNS が一致を正しく逆引きしないシナリオはテストできません。	**203.45.98.109** **2001:0db8:85a3::8a2e:0370:7334**
ソース IP アドレスの完全修飾ドメイン名	模倣する完全修飾リモートドメイン名を入力します。ヌルのままにすると、送信元 IP アドレスに対してリバース DNS ルックアップが実行されます。	**smtp.example.com**
次の動作をトレースするリスナー	テストメッセージの送信をエミュレートするため、システムに設定されているリスナーのリストから選択します。	**InboundMail**
ネットワークオーナーの組織 ID	ネットワークオーナーに固有の ID 番号を入力するか、送信元 IP アドレスに関連付けられたネットワークオーナー ID の検索を指示します。GUI を介して送信者グループにネットワーク オーナーを追加した場合は、この情報を表示できます。	**34**

値	説明	例
IP レピュテーションスコア	スプーフィングドメインに与える IP レピュテーションスコアを入力するか、送信元 IP アドレスに関連付けられた IP レピュテーションスコアの検索を指示します。このパラメータは、IP レピュテーションスコアを使用するポリシーをテストするときに役立ちます。手動で入力した IP レピュテーションスコアは、コンテキスト適応スキャンエンジン（CASE）に渡されないことに注意してください。詳細については、リスナーの IP レピュテーション フィルタリング スコアのしきい値の編集 （102 ページ）を参照してください。	**-7.5**
エンベロープ送信者（Envelope Sender）	テストメッセージのエンベロープ送信者を入力します。	**admin@example.net**
エンベロープ受信者	テストメッセージの受信者のリストを入力します。複数のエントリを指定する場合は、カンマで区切ります。	**joe** **frank@example.com**
メッセージ本文	ヘッダーを含む、テスト メッセージのメッセージ本文を入力します。メッセージ本文の入力を終了するには、別の行にピリオドを入力します。「ヘッダー」は、メッセージ本文の一部とみなされるため（空白行により分割されます）、ヘッダーを省略したり、不十分な形式が含まれると、予期しないトレース結果となる可能性がある点に注意してください。	**To: 1@example.com** From: ralph Subject: Test **this is a test message** .

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

メッセージ本文は、ローカル ファイル システムからアップロードできます（CLI では、**/configuration** ディレクトリにアップロードしたメッセージ本文を使用してテストできます。 電子メールゲートウェイにインポートするためにファイルを配置する方法の詳細については、FTP、SSH、および SCP アクセス （1573 ページ）を参照してください）。

概要が出力されると、生成されたメッセージの確認とテストメッセージの再実行を求められます。別のテスト メッセージを入力すると、[トレース（Trace）] ページおよび trace コマンドでは、以前に入力した前掲の表の値が使用されます。

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

表 *159*：トレースを実行したときの出力の表示

trace コマンド セクション	**出力**
ホスト アクセス テーブル（HAT）およびメール フロー ポリシーの処理	指定したリスナーに対するホスト アクセス テーブルの設定が処理されます。システムからは、入力したリモート IP アドレスおよびリモート ドメイン名と一致した HAT 内のエントリが報告されます。デフォルトのメール フロー ポリシーと送信者グループ、およびどちらが所定のエントリに一致したかを確認できます。 電子メールゲートウェイが（REJECT または TCPREFUSE アクセスルールを介して）接続を拒否するように設定された場合、処理中の trace コマンドはその時点で終了します。 HAT プロパティの設定の詳細については、定義済みの送信者グループとメール フロー ポリシーの理解 （118 ページ）を参照してください。
エンベロープ送信者アドレスの処理 これらのセクションには、指定したエンベロープ送信者に対して電子メールゲートウェイの設定がどのように影響するかが要約されます（つまり、MAIL FROM コマンドが 電子メールゲートウェイの設定によってどのように解釈されるかがわかります）。**`trace`** コマンドは、このセクションの前に「**`Processing MAIL FROM:`**」と出力します。	
デフォルト ドメイン	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ送信者に対するすべての変更がこのセクションに出力されます。 詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

trace コマンド セクション	**出力**
マスカレード	メッセージのエンベロープ送信者を変換するように指定した場合、ここに変更が表示されます。**listenerconfig -> edit -> masquerade -> config** サブコマンドを使用して、プライベート リスナーに対するエンベロープ送信者のマスカレードをイネーブルにします。 詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。
エンベロープ受信者の処理 これらのセクションでは、指定したエンベロープ受信者に対して電子メールゲートウェイがどのように影響するかの要約を示します（つまり、RCPT TO コマンドが電子メールゲートウェイの設定によってどのように解釈されるかがわかります）。trace コマンドは、このセクションの前に「Processing Recipient List:」と出力します。	
デフォルト ドメイン	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ受信者に対するすべての変更がこのセクションに出力されます。 詳細については、電子メールを受信するためのゲートウェイの設定（81 ページ）を参照してください。
ドメイン マップの変換	ドメイン マップ機能によって、受信者アドレスが代替アドレスに変換されます。ドメイン マップの変更を指定しており、指定した受信者アドレスが一致した場合は、このセクションに変換が出力されます。 詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。
受信者アクセス テーブル（RAT）	ポリシーとパラメータのほか、このセクションには、RAT 内のエントリに一致する各エンベロープ受信者が出力されます（たとえば、リスナーの RAT の制限をバイパスするように受信者が指定された場合など）。 受け入れる受信者の指定の詳細については、電子メールを受信するためのゲートウェイの設定（81 ページ）を参照してください。
エイリアス テーブル	このセクションには、 電子メールゲートウェイで設定されたエイリアステーブル内のエントリに一致する各エンベロープ受信者（および 1 つまたは複数の受信者アドレスへの後続の変換）が出力されます。 詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。

trace コマンド セクション	出力
Pre-Queue メッセージ操作 ここでは、メッセージの内容を受信した後、ワークキュー上でメッセージがキューから出る前に、各メッセージに電子メールゲートウェイがどのように影響するかを示します。この処理は、最後の **250 ok** コマンドがリモート MTA に返される前に実行されます。 **trace** コマンドは、このセクションの前に「Message Processing:」と出力します。	
仮想ゲートウェイ	**altsrchost** コマンドを実行すると、エンベロープ送信者の完全アドレス、ドメイン、または名前、あるいは IP アドレスの一致に基づいて、特定のインターフェイスにメッセージが割り当てられます。エンベロープ送信者が **altsrchost** コマンドのエントリに一致すると、その情報がこのセクションに出力されます。 この時点で割り当てられた仮想ゲートウェイ アドレスは、メッセージ フィルタの処理によって上書きされる可能性があることに注意してください。 詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。
バウンス プロファイル	バウンス プロファイルは、処理中の 3 つの時点で適用されます。ここが最初のポイントです。リスナーにバウンス プロファイルが割り当てられる場合は、プロセス内のこの時点で割り当てられます。その情報がこのセクションに出力されます。 詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。
ワーク キュー操作 次の一連の機能は、ワーク キュー内のメッセージに対して実行されます。機能が実行されるのは、クライアントからのメッセージが受け入れられた後、そのメッセージが配信用として宛先キューに入れられる前です。status コマンドおよび status detail コマンドにより、「Messages in Work Queue」が報告されます。	
マスカレード	メッセージの [宛先:（To:）]、[差出人:（From:）]、および [CC:] ヘッダーが（リスナーから入力されたスタティック テーブルまたは LDAP クエリーを通じて）マスクされるように指定した場合は、ここに変更が表示されます。**listenerconfig -> edit -> masquerade -> config** サブコマンドを使用して、プライベート リスナーに対してメッセージヘッダーのマスカレードをイネーブルにします。 詳細については、ルーティングおよび配信機能の設定（853 ページ）を参照してください。

trace コマンド セクション	出力
LDAP ルーティング	リスナーに対して LDAP クエリーがイネーブルになっている場合は、このセクションにLDAP許可、再ルーティング、マスカレード、およびグループ クエリーの結果が出力されます。 詳細については、LDAP クエリ （943 ページ）を参照してください。
メッセージ フィルタの処理	システムでイネーブルになっているすべてのメッセージフィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最終結果が「true」の場合、そのフィルタ内の各アクションが順番に実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。ルールが「false」と評価され、アクションのリストが else 句と関連付けられている場合、それらのアクションが代わりに評価されます。このセクションには、順番に処理されたメッセージ フィルタの結果が出力されます。 メッセージ フィルタを使用した電子メール ポリシーの適用（155 ページ）を参照してください。
メール ポリシーの処理 メール ポリシーの処理セクションには、アンチスパム、アンチウイルス、アウトブレイク フィルタ機能と、指定されたすべての受信者に対する免責事項スタンプ機能が表示されます。複数の受信者が電子メール セキュリティ マネージャの複数のポリシーに一致する場合は、一致する各ポリシーが次の各セクションに繰り返し表示されます。文字列「Message Going to」は、どの受信者がどのポリシーと一致するかを定義します。	
スパム対策	このセクションには、アンチスパム スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチスパム スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。 電子メールゲートウェイが、その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、**`trace`** コマンドの処理は停止します。 （注）システムでアンチスパム スキャンが使用できない場合、この手順は省略されます。アンチスパム スキャンを使用できても、ライセンス キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 「スパムおよびグレイメールの管理 （461 ページ）」を参照してください。

trace コマンド セクション	出力
アンチウイルス	このセクションには、アンチウイルス スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチウイルス スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。感染したメッセージを「クリーニング」するように 電子メールゲートウェイが設定されている場合は、その情報が表示されます。その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。 （注）システムでアンチウイルス スキャンが使用できない場合、この手順は省略されます。アンチウイルス スキャンを使用できても、ライセンス キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 アンチウイルス （439 ページ）を参照してください。
コンテンツ フィルタの処理	システムでイネーブルになっているすべてのコンテンツ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最終結果が「true」の場合、そのフィルタ内の各アクションが順番に実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。このセクションには、順番に処理されたコンテンツ フィルタの結果が出力されます。 コンテンツ フィルタ （325 ページ）を参照してください。
アウトブレイク フィルタの処理	このセクションには、アウトブレイク フィルタ機能をバイパスする添付ファイルのあるメッセージが示されます。メッセージが受信者に対するアウトブレイク フィルタによって処理されることになっている場合、メッセージは処理され、その評価が出力されます。 電子メールゲートウェイが、判定に基づいてメッセージを隔離、バウンス、またはドロップするように設定されている場合、その情報が出力されて、処理が停止します。 アウトブレイク フィルタ （513 ページ）を参照してください。

trace コマンド セクション	出力
フッター スタンプ	このセクションには、メッセージにフッター テキスト リソースが付加されたかどうかが示されます。テキスト リソースの名前が表示されます。テキスト リソース（791 ページ）のメッセージの免責事項スタンプ（793 ページ）を参照してください。
配信操作 次の各セクションには、メッセージが配信されるときに発生する動作が示されます。trace コマンドは、このセクションの前に「Message Enqueued for Delivery」と出力します。	
ドメインおよびユーザごとのグローバル配信停止	trace コマンドの入力として指定した受信者が、グローバル配信停止機能に示されている受信者、受信者ドメイン、または IP アドレスに一致すると、未登録の受信者アドレスがこのセクションに出力されます。 ルーティングおよび配信機能の設定（853 ページ）を参照してください。
送信者ドメインのレピュテーション	送信者ドメインのレピュテーション判定によってブロックされたメッセージの処理結果を表示します。 次に、処理結果の例を示します。 • レピュテーション：ニュートラル • ドメインの経過時間：33 年 9 ヵ月と 6 日 • カテゴリ：N/A • アクション：メッセージのドロップ
最終結果 すべての処理が出力されると、最終結果が表示されます。CLI では、「Would you like to see the resulting message?」という問いに対して **y** と入力して、結果のメッセージを表示します。	

電子メールゲートウェイのテストにリスナーを使用

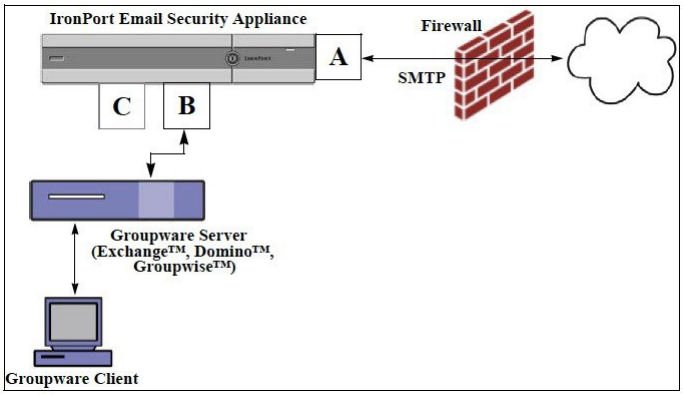
「シンクホール」のリスナーは、メッセージ生成システムをテストし、受信パフォーマンスの簡単な測定ができます。シンクホールリスナーには、キューイングと非キューイングの 2 種類があります。

- キューイング リスナーは、メッセージをキューに保存しますが、その後メッセージをただちに削除します。メッセージ生成システムのインジェクション部分全体のパフォーマンスを測定する場合は、キューイング リスナーを使用します。

- 非キューイング リスナーはメッセージを承認した後、保存しないですぐに削除します。メッセージ生成システムから電子メールゲートウェイまでの接続のトラブルシューティングを行う場合は、非キューイングリスナーを使用します。

たとえば次の図では、シンクホールリスナー「C」を作成して、「B」というプライベートリスナーをミラーリングします。非キューイング版では、グループウェアクライアントからグループウェアサーバを経由して電子メールゲートウェイまでのシステムのパフォーマンスパスをテストします。キューイング版は、同じ方法およびメッセージをキューに入れてSMTP経由で配信するための電子メールゲートウェイの機能をテストします。

図 *87*: エンタープライズ ゲートウェイに対するシンクホールリスナー



次に、listenerconfig コマンドを使用して、管理インターフェイス上で Sinkhole_1 という名前のシンクホール キューイング リスナーを作成します。リスナーのためのこのホスト アクセス テーブル（HAT）は、次のホストからの接続を受け入れるように編集されています。

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

（注） 最後のエントリである .tst により、.tst ドメイン内にあるすべてのホストから Sinkhole_1 という名前のリスナーに電子メールを送信できるようになります。

例

```
mail3.example.com> listenerconfig

Currently configured listeners:

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

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

Choose the operation you want to perform:

- NEW - Create a new listener.
```

```
- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new

Please select the type of listener you want to create.

1. Private

2. Public

3. Sinkhole

[2]> 3

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

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

[]> Sinkhole_1

Please choose an IP interface for this Listener.

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

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

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

[1]> 1

Choose a protocol.

1. SMTP

2. QMQP

[1]> 1

Please enter the IP port for this listener.

[25]> 25

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

Hostnames such as "example.com" are allowed.

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

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

Separate multiple entries with commas.


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

Do you want to enable rate limiting per host? (Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a remote
domain.) [N]> n
```

```
Default Policy Parameters
==========================
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 600
Maximum Number Of Messages Per Connection: 10,000
Maximum Number Of Recipients Per Message: 100,000
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: No
Spam Detection Enabled: No
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Would you like to change the default host access policy? [N]> n
Listener Sinkhole_1 created.
Defaults have been set for a Sinkhole Queuing listener.
Use the listenerconfig->EDIT command to customize the listener.
Currently configured listeners:
1. Sinkhole_1 (on Management, 192.168.42.42) SMTP Port 25 Sinkhole Queuing
2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public
3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
```

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

キューイングタイプのシンクホールリスナーを設定して、HAT でインジェクションシステムからの接続を受け入れるよう変更したら、インジェクションシステムを使用して、電子メールゲートウェイへの電子メールの送信を開始します。status、status detail、および rate コマンドを

使用して、システムのパフォーマンスをモニタします。また、グラフィカルユーザーインターフェイス（GUI）でシステムをモニタすることもできます。詳細については、以下を参照してください。

• CLI を使用したモニタリング （1340 ページ）
• GUI での他のタスク （1371 ページ）

ネットワークのトラブルシューティング

電子メールゲートウェイにネットワーク接続の問題があると思われる場合は、電子メールゲートウェイが適切に動作していることを確認します。

電子メールゲートウェイのネットワーク接続テスト

手順

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

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

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

AsyncOS x.x for Cisco


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

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

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

または

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

status コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返される統計情報は、カウンタとゲージの2つのカテゴリにグループ化されます。レートなどの電子メールの動作についての全般的なモニタリング情報については、status detail コマンドを使用します。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。（詳細については、CLI を使用したモニタリング（1340 ページ）を参照してください。）

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

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

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send the
configuration file.


Separate multiple addresses with commas.

[]> user@example.com

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


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

mail3.example.com>
```

トラブルシューティング

電子メールゲートウェイがネットワーク上でアクティブであることが確認されたら、次のコマンドを使用して、ネットワークの問題をピンポイントで特定します。

- netstat コマンドを使用すると、次のようなネットワーク接続（着信と発信の両方）、ルーティング テーブル、ネットワーク インターフェイスのさまざまな統計情報が表示されます。
  - アクティブなソケットのリスト
  - ネットワーク インターフェイスの状態
  - ルーティング テーブルの内容
  - リッスン キューのサイズ
  - パケット トラフィック情報
- diagnostic -> network -> flush コマンドを使用すると、ネットワークに関連するすべてのキャッシュをフラッシュできます。
- diagnostic -> network -> arpshow コマンドを使用すると、システムの ARP キャッシュを表示できます。
- packetcapture コマンドを使用すると、コンピュータが接続されているネットワーク上で送受信されている TCP/IP や他のパケットを傍受して表示できます。

packetcapture を使用するには、ネットワークインターフェイスとフィルタを設定します。このフィルタでは、UNIX の tcpdump コマンドと同じ形式を使用します。パケットの捕捉を開始するには start を、停止するには stop を使用します。捕捉を停止した後、SCP または FTP を使用して /pub/captures ディレクトリからファイルをダウンロードする必要があります。詳細については、パケットキャプチャの実行（1543 ページ）を参照してください。

- 電子メールゲートウェイでネットワーク上にアクティブな接続があり、ネットワーク上の特定のセグメントに到達できることを確認するには、動作している既知のホストに対して ping コマンドを使用します。

  ping コマンドを使用すると、電子メールゲートウェイからネットワークホストへの接続をテストできます。

```
mail3.example.com> ping

Which interface do you want to send the pings from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1
Please enter the host you wish to ping.
[]> anotherhost.example.com
Press Ctrl-C to stop.
PING anotherhost.example.com (x.x.x.x): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

（注） ping コマンドを終了するには、Ctrl+C を使用する必要があります。

- traceroute コマンドを使用すると、電子メールゲートウェイからネットワークホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

```
mail3.example.com> traceroute

Which interface do you want to trace from?

1. Auto

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

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

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

[1]> 1

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

[]> 10.1.1.1

Press Ctrl-C to stop.

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

1 gateway (192.168.0.1) 0.202 ms 0.173 ms 0.161 ms

2 hostname (10.1.1.1) 0.298 ms 0.302 ms 0.291 ms

mail3.example.com>
```

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

  `nslookup` コマンドでは、電子メールゲートウェイが、動作している DNS（ドメインネームサービス）サーバからホスト名と IP アドレスを解決して到達できることを確認できます。

```
mail3.example.com> nslookup

Please enter the host or IP to resolve.

[]> example.com


Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>
```

```
A=192.0.34.166 TTL=2d
```

表 *160 : DNS* の機能の確認：クエリーのタイプ

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

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

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

```
mail3.example.com> tophosts

Sort results by:

1. Active Recipients

2. Connections Out

3. Delivered Recipients

4. Soft Bounced Events

5. Hard Bounced Recipients

[1]> 1

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

ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1 aol.com36510255218

2 hotmail.com29071982813

3 yahoo.com13461231119

4 excite.com9838494
```

```
5 msn.com8427633 29

^C
```

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

  `hoststatus` コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した `resetcounters` コマンドからの累積です。（詳細については、メール ホストのステータスのモニタリング（1343 ページ）を参照してください。）

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

- ファイアウォールの権限を確認します。

  電子メールゲートウェイが正しく機能するためには、ポート 20、21、22、23、25、53、80、123、443、および 628 を開く必要がある場合があります（ファイアウォール情報（1607 ページ）を参照）。

- ネットワーク上の電子メールゲートウェイから、dnscheck@ironport.com に対して電子メールを送信します

  システムの基本的な DNS チェックを実行するために、ネットワーク内から dnscheck@ironport.com に電子メールを送信します。オートレスポンダによる電子メールによって、次の 4 つのテストについての結果と詳細が返されます。

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

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

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

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

リスナーのトラブルシューティング

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

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

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

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

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

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

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

- インジェクションを行っているマシンから、Telnet または FTP を使用して、電子メールゲートウェイに手動で接続します。次に例を示します。

```
injection_machine% telnet appliance_name
```

電子メールゲートウェイ内で `telnet` コマンドを使用して、リスナーから実際の電子メールゲートウェイに接続することもできます。

```
mail3.example.com> telnet

Please select which interface you want to telnet from.

1. Auto

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

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

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

[1]> 3

Enter the remote hostname or IP.

[]> 193.168.1.1

Enter the remote port.

[25]> 25

Trying 193.168.1.1...

Connected to 193.168.1.1.

Escape character is '^]'.
```

あるインターフェイスから他のインターフェイスに接続できない場合は、電子メールゲートウェイの Management、Data1、Data2 インターフェイスからネットワークに接続している方法に問題がある可能性があります。詳細については、FTP、SSH、および SCP アクセス（1573 ページ）を参照してください。リスナーのポート 25 に対して telnet を実行して、SMTP コマンドを手動で入力できます（このプロトコルを熟知している場合）。

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

  インジェクション デバッグ ログには、電子メールゲートウェイと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントと電子メールゲートウェイ間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、接続ホストに「送信」または接続ホストから「受信」に分類されます。

  詳細については、「テキスト メール ログの使用 （1407 ページ）」および「インジェクション デバッグ ログの使用 （1429 ページ）」を参照してください。

アプライアンスからの電子メール配信のトラブルシューティング

電子メールゲートウェイからの電子メールの配信に問題があると疑われる場合は、次の方法を試してください。

- 問題がドメインに限定されたものであるかどうかを判断します。

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

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

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

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

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

  ```
  destconfig -> list
  ```

- `hoststatus` コマンドを使用します。

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

  ホストが使用可能で、接続を受け入れていますか。

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

  `hoststatus` コマンドでは、特定のホストに対する 5XX エラー（Permanent Negative Completion Reply）がある場合に、ホストから返された直前の「5XX」のステータス コードと説明が

表示されます。このホストに対する直前の発信 TLS 接続が失敗した場合は、`hoststatus` コマンドで失敗した理由が表示されます。

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

  ドメインデバッグログには、電子メールゲートウェイと指定の受信者ホスト間のSMTP会話でのクライアントとサーバの通信が記録されます。このタイプのログファイルは、特定の受信ホストに関する問題のデバッグに使用できます。

  詳細については、ドメイン デバッグ ログの使用 （1429 ページ）を参照してください。

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

  詳細については、バウンス ログの使用 （1424 ページ）を参照してください。

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

  詳細については、テキスト メール ログの使用 （1407 ページ）を参照してください。

- `telnet` コマンドを使用して、電子メールゲートウェイから問題のあるドメインに接続します。

```
mail3.example.com> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enter the remote hostname or IP.
[]> problemdomain.net
Enter the remote port.

[25]> 25
```

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

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:
```

```
[]> example.com

Enter the destination host to connect to. Append the port (example.com:26) if you are

not connecting on port 25:

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

Connecting to 1.1.1.1 on port 25.

Connected to 1.1.1.1 from interface 10.10.10.10.

Checking TLS connection.

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

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.

TLS verification completed.
```

パフォーマンスのトラブルシューティング

電子メールゲートウェイのパフォーマンスに関する問題があると疑われる場合は、次の方法を使用してください。

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

  rate コマンドは、電子メール動作に関するリアルタイムモニタリング情報を返します。詳細については、リアルタイムアクティビティの表示（1346ページ）を参照してください。

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

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

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

（注） メモリの使用率は、常に 45% 未満である必要があります。メモリの使用率が 45% を超えると、電子メールゲートウェイは「リソース節約モード」に入ります。これによって「バックオフ」アルゴリズムが起動され、リソースのオーバーサブスクリプションが防止され、電子メールによる次のアラートが送信されます。

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


RAM utilization for this system has exceeded the resource conservation threshold of
 45%.
The allowed injection rate for this system will be gradually decreased as RAM
utilization approaches 60%.
```

この状況は、配信機能が低下していて、大量のインジェクションが行われているときにのみ発生します。メモリの使用率が 45% を超えたときには、キュー内のメッセージの数を調べて、特定のドメインがダウン状態または配信不可能になっていないかどうかを確認します（`hoststatus` コマンドまたは `hostrate` コマンドを使用します）。また、システムのステータスも確認して、配信が中断されないようにします。インジェクションが停止しても、依然としてメモリの使用率が高い場合は、シスコ カスタマー サポートにご連絡ください。

- 問題が 1 つのドメインに限定されていますか。

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

  キューのサイズを確認します。このサイズを制御したり、問題が生じている特定のドメインの受信者に対処するために、電子メールキューにあるメッセージを削除、バウンス、中断、またはリダイレクトすることができます。詳細については、電子メール キューの管理（1351 ページ）を参照してください。以下のコマンドを使用します。

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

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

Web インターフェイスの外観およびレンダリングの問題

Internet Explorer の互換モードの上書き （1327 ページ） を参照してください。

アラートへの応答

-
- その他のディスク使用量がクォータに近づいているというアラートのトラブルシューティング （1538 ページ）

その他のディスク使用量がクォータに近づいているというアラートのトラブルシューティング

問題

その他のディスク使用量がクォータに近づいているというアラートを受信しました。

解決方法

クォータを増やすか、ファイルを削除できます。その他のクォータのディスク領域の管理 （1250 ページ） を参照してください。

ハードウェア問題のトラブルシューティング

ハードウェア電子メールゲートウェイの前面/背面パネルのライトは、電子メールゲートウェイの状態およびステータスを示します。これらのインジケータの説明については、『*Cisco x90s Series Content Security Appliances Installation and Maintenance Guide*』など、http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手できるハードウェア ガイドを参照してください。

温度範囲など、電子メールゲートウェイの仕様についてもこれらのマニュアルで確認できます。

電子メールゲートウェイの電源のリモートリセット

電子メールゲートウェイのハードリセットが必要な場合は、サードパーティのインテリジェント プラットフォーム管理インターフェイス（IPMI）ツールを使用して電子メールゲートウェイシャーシをリモートからリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。

  詳細については、リモート電源再投入の有効化 （1269 ページ）を参照してください。

- この機能を使用する場合は、使用が必要になる前に、あらかじめ有効にしておく必要があります。

  詳細については、リモート電源再投入の有効化 （1269 ページ）を参照してください。

- 次の IPMI コマンドのみがサポートされています。
  - **status、on、off、cycle、reset、diag、soft**
  - サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

はじめる前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

手順

ステップ 1 IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

ここで **192.0.2.1** は、リモート電源管理ポートに割り当てられた IP アドレスであり、**remoteresetuser** およびパスワードは、この機能を有効にしたときに入力したクレデンシャルです。

ステップ 2 電子メールゲートウェイが再起動されるまで、少なくとも 11 分間待ちます。

テクニカル サポートの使用

- 仮想電子メールゲートウェイのテクニカルサポート （1540 ページ）
- 電子メールゲートウェイからのサポートケースのオープンおよび更新 （1540 ページ）
- シスコのテクニカル サポート担当者のリモート アクセスの有効化 （1541 ページ）
- パケット キャプチャの実行 （1543 ページ）

仮想電子メールゲートウェイのテクニカルサポート

仮想電子メールゲートウェイのテクニカルサポートを受けるための要件は、http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html にある『Cisco Content Security Virtual Appliance Installation Guide』に記載されています。

電子メールゲートウェイからのサポートケースのオープンおよび更新

はじめる前に

- 緊急の問題の場合、この方法は使用しないでください。代わりに、シスコカスタマーサポート （9 ページ）に示されるその他の方法の 1 つを使用してサポートください。

  次の手順は、情報が必要であるまたは回避策があるけれども代替策を使用したいといった問題に限り使用します。

- ヘルプに関しては別の選択肢を検討してみてください。
  - ナレッジ ベース （8 ページ）
  - シスコサポートコミュニティ （8 ページ）
- 電子メールゲートウェイからシスコテクニカルサポートに直接アクセスするには、Cisco.com ユーザー ID がこの電子メールゲートウェイのサービス契約に関連付けられている必要があります。Cisco.com プロファイルに現在関連付けられているサービス契約の一覧を参照するには、Cisco.com Profile Manager（https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do）にアクセスしてください。Cisco.com のユーザ ID がない場合は、登録して ID を取得してください。シスコ アカウントの登録 （9 ページ）を参照してください。

  Cisco.com ユーザー ID とサポート契約 ID は、安全な場所に保存してください。
- この手順を使用してサポートケースを開くと、電子メールゲートウェイの設定ファイルがシスコカスタマーサポートに送信されます。電子メールゲートウェイの設定を送信したくない場合、別の方法を使用してカスタマーサポートにお問い合わせください。
- クラスタ設定では、サポート要求と保存されたそれらの値はマシンに固有のものです。
- 電子メールゲートウェイがインターネットに接続され電子メールを送信できる必要があります。
- 既存の事例に関する情報を送信する場合は、ケース番号を確認してください。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 [ヘルプとサポート（Help and Support）]>[テクニカルサポートに問い合わせる（Contact Technical Support）] を選択します。

ステップ 3 フォームに入力します。

ステップ 4 [送信（Send）] をクリックします。

（注） CCO ユーザー ID と最後に入力された契約 ID は、将来使用できるように電子メールゲートウェイに保存されます。

シスコのテクニカル サポート担当者のリモート アクセスの有効化

シスコのカスタマーアシスタンスのみ、次の方法を使用して電子メールゲートウェイにアクセスできます。

- インターネット接続された電子メールゲートウェイへのリモートアクセスの有効化 （1541 ページ）
- インターネットに直接接続されていない電子メールゲートウェイへのリモートアクセスの有効化 （1542 ページ）
- リモート アクセスの無効化 （1543 ページ）
- テクニカル サポートのトンネルの無効化 （1543 ページ）
- サポートの接続状態の確認 （1543 ページ）

インターネット接続された電子メールゲートウェイへのリモートアクセスの有効化

サポートは、この手順で電子メールゲートウェイと **upgrades.ironport.com** のサーバ間で作成される SSH トンネル経由で電子メールゲートウェイにアクセスします。

はじめる前に

インターネットから到達可能なポートを識別します。デフォルトでは、ポート 25 で、このポートは大部分の環境で機能します。システムは、電子メール メッセージを送信するために、このポートを介して一般的なアクセスを行う必要があるためです。このポート経由の接続は、ほとんどのファイアウォール設定で許可されます。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 GUI ウィンドウの右上にある、[ヘルプとサポート（Help and Support）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 情報を入力します。

オプション	説明
シード文字列（Seed String）	シード文字列は、シスコ カスタマー サポートがこの電子メールゲートウェイにアクセスするための安全な共有秘密を生成するために使用されます。

オプション	説明
セキュア トンネル（Secure Tunnel）	リモート アクセス接続にセキュア トンネルを使用するために、このチェックボックスをオンにします。 接続ポートを入力します。 デフォルトでは、ポート 25 です。このポートはほとんどの環境で機能します。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

サポート担当者のリモート アクセスが必要なくなったときは、テクニカル サポートのトンネルの無効化 （1543 ページ）を参照してください。

インターネットに直接接続されていない電子メールゲートウェイへのリモートアクセスの有効化

インターネットに直接接続されていないアプライアンスの場合、インターネットに接続されている第 2 の電子メールゲートウェイを介してアクセスされます。

はじめる前に

- 電子メールゲートウェイは、インターネットに接続されている第 2 の電子メールゲートウェイにポート 22 で接続する必要があります。
- インターネットに接続されている電子メールゲートウェイで該当電子メールゲートウェイへのサポートトンネルを作成するには、インターネット接続された電子メールゲートウェイへのリモートアクセスの有効化 （1541 ページ）の手順を実行します。

手順

ステップ 1 サポートが必要な電子メールゲートウェイのコマンドライン インターフェイスから、**techsupport** コマンドを入力します。

ステップ 2 **sshaccess** と入力します。

ステップ 3 プロンプトに従います。

次のタスク

サポート担当者のリモートアクセスが必要なくなったときは、次のトピックを参照してください。

- リモート アクセスの無効化 （1543 ページ）
- テクニカル サポートのトンネルの無効化 （1543 ページ）

テクニカル サポートのトンネルの無効化

有効にした techsupport トンネルは、upgrades.ironport.com に 7 日間接続されたままになります。その後、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。

トンネルを手動で無効にします。

手順

ステップ 1 電子メールゲートウェイにログインします。

ステップ 2 GUI ウィンドウの右上にある、[ヘルプとサポート（Help and Support）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 3 [無効（Disable）] をクリックします。

リモート アクセスの無効化

techsupport コマンドを使用して作成したリモート アクセス アカウントは、非アクティブ化されるまでアクティブのままです。

手順

ステップ 1 コマンドライン インターフェイスから、techsupport コマンドを入力します。

ステップ 2 sshaccess と入力します。

ステップ 3 disable と入力します。

サポートの接続状態の確認

手順

ステップ 1 コマンドライン インターフェイスから、techsupport コマンドを入力します。

ステップ 2 status と入力します。

パケット キャプチャの実行

パケットキャプチャは、サポート担当者が TCP/IP データおよびその他に電子メールゲートウェイから出入りするパケットを表示できるようにします。これはネットワーク設定をデバッグし

たり、どのようなネットワークトラフィックが電子メールゲートウェイに到達または送出されているかを検出することができます。

手順

ステップ 1 [ヘルプとサポート（Help and Support）] > [パケットキャプチャ（Packet Capture）] を選択します。

ステップ 2 パケット キャプチャ設定の指定：

a) [パケットキャプチャ設定（Packet Capture Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

b) （任意）パケット キャプチャの期間、制限およびフィルタを入力します。

サポート担当者が、これらの設定の方法を説明する場合があります。

時間の単位を指定しないでキャプチャ期間を入力すると、AsyncOS はデフォルトで秒を使用します。

[フィルタ（Filters）] セクションで次を実行します。

- カスタム フィルタは、UNIX の tcpdump コマンドでサポートされた任意の構文（host 10.10.10.10 && port 80 など）を使用できます。
- クライアント IP は、電子メールゲートウェイを介してメッセージを送信するメールクライアントなどの電子メールゲートウェイに接続しているマシンの IP アドレスです。
- サーバ IP は、電子メールゲートウェイがメッセージを配信する Exchange サーバなどの電子メールゲートウェイが接続しているマシンの IP アドレスです。
- クライアントとサーバの IP アドレスを使用して、中間に電子メールゲートウェイがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。

c) [送信（Submit）] をクリックします。

ステップ 3 [キャプチャを開始（Start Capture）] をクリックします。

- キャプチャは一度に 1 つだけ実行できます。
- パケット キャプチャが実行されている場合、[パケットキャプチャ（Packet Capture）] ページには、実行中のキャプチャのステータス（ファイルサイズや経過時間などの現在の統計情報）が表示されます。
- GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。
- パケット キャプチャ ファイルは 10 個の部分に分割されます。パケット キャプチャが終了する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。

- GUI で開始されたキャプチャはセッション間で維持されます。（CLI で実行したキャプチャは、セッションが終了したときに停止します）。

ステップ 4 キャプチャを指定した期間実行するようにします。またはキャプチャを無期限に実行する場合、[キャプチャを停止（Stop Capture）] をクリックして停止します。

ステップ 5 パケット キャプチャ ファイルへアクセスします。

- [パケットキャプチャファイルの管理（Manage Packet Capture Files）] リストでファイルをクリックして、[ファイルのダウンロード（Download File）] をクリックします。
- 電子メールゲートウェイの captures サブディレクトリ内のファイルにアクセスするには、FTP または SCP を使用します。

次のタスク

サポートでファイルを使用できるようにします。

- 電子メールゲートウェイへのリモートアクセスを許可した場合、技術者がFTPまたはSCPを使用してパケットキャプチャファイルにアクセスできます。シスコのテクニカル サポート担当者のリモート アクセスの有効化 （1541 ページ）を参照してください。
- 電子メールでファイルをサポートに送信します。

第 47 章

D-Mode を使用した発信メール配信電子メールゲートウェイの最適化

この章は、次の項で構成されています。

- 機能の概要：最適化された発信配信の D-Mode （1547 ページ）
- 最適化された発信メール配信の電子メールゲートウェイの設定 （1549 ページ）
- IronPort Mail Merge（IPMM）を使用した大量のメールの送信 （1551 ページ）

機能の概要：最適化された発信配信の D-Mode

D-Mode は、特定の電子メールゲートウェイを発信電子メール配信向けに最適化する、キーでイネーブルにされる機能です。着信メール処理に特有の機能は、D-Mode ではディセーブルになっています。

- D-Mode 対応電子メールゲートウェイ固有の機能 （1547 ページ）
- D-Mode 対応電子メールゲートウェイでディセーブルになっている標準機能 （1548 ページ）
- D-Mode 対応電子メールゲートウェイに適用される標準機能 （1548 ページ）

D-Mode 対応電子メールゲートウェイ固有の機能

- 256 の仮想ゲートウェイアドレス：Cisco Virtual Gateway テクノロジーを使用すると、個別の IP アドレス、ホスト名およびドメインを使用してホストするすべてのドメインのエンタープライズ メール ゲートウェイを設定して、同じ物理電子メールゲートウェイ内でホストしながら、これらのドメインの個別の企業電子メールポリシー拡張およびアンチスパム戦略を作成できます。電子メールを受信するためのゲートウェイの設定 （81 ページ）にある「リスナーのカスタマイズ」に関する情報を参照してください。
- IronPort Mail Merge（IPMM）：IronPort Mail Merge（IPMM）を使用すると、個別の個人向けメッセージをカスタマーシステムから生成する手間を省くことができます。ユーザは、数千の個別メッセージを生成し、メッセージ生成システムと電子メールゲートウェイ間で送信する必要がなくなるため、システムにかかる負荷が軽減され、電子メール配信のスループットが向上します。詳細については、IronPort Mail Merge（IPMM）を使用した大量のメールの送信 （1551 ページ）を参照してください。

- リソースを節約するバウンス設定：D-Mode 対応電子メールゲートウェイを設定して、ブロックされている可能性のある宛先を検出し、その宛先へのすべてのメッセージをバウンスできます。詳細については、リソースを節約するバウンス設定の構成（1550ページ）を参照してください。
- 発信配信のパフォーマンスの向上

D-Mode 対応電子メールゲートウェイでディセーブルになっている標準機能

- IronPort Anti-Spam スキャンおよびオン/オフボックス スパム隔離：アンチスパム スキャンは、通常、着信メールに関係するため、IronPort Anti-Spam スキャン エンジンはディセーブルにされます。したがって、スパム対策の章は適用されません。
- アウトブレイクフィルタ：アウトブレイクフィルタは、着信メールの隔離に使用されるため、D-Mode対応電子メールゲートウェイではディセーブルになっています。したがって、アウトブレイク フィルタの章の情報は適用されません。
- サービスログ：サービスログ機能は、D-Mode対応電子メールゲートウェイでは無効になっています。
- レポーティング：レポーティング機能は限定されます。一部のレポートは使用できません。発生するレポーティングも、パフォーマンス上の理由により、非常に限定的なレベルで実行するように設定されています。

（注） D-Mode対応電子メールゲートウェイの電子メールセキュリティモニタ概要レポートに示される合計には、これらの機能がD-Mode対応電子メールゲートウェイでディセーブルにされている場合でも、スパム、および陽性と疑わしいスパムの数が、誤って含まれる可能性があります。

- データ損失防止：発信メッセージの DLP スキャンは、D-Mode 対応電子メールゲートウェイでディセーブルになっています。

D-Mode 対応電子メールゲートウェイに適用される標準機能

表 *161 : D-Mode* 対応電子メールゲートウェイに含まれる *AsyncOS* 機能

機能	詳細情報
アンチウイルス スキャン	アンチウイルス （439 ページ）を参照してください。
DomainKeys 署名	DKIM/DomainKeys は、送信者により使用される署名キーに基づいて電子メールの信頼性を確認する方式です。電子メール認証（741 ページ）を参照してください。

機能	詳細情報
集中管理	クラスタを使用した中央集中型管理（1481 ページ）を参照してください。
配信スロットリング	各ドメインに対して、一定期間でシステムが超えることができない、接続および受信者の最大数を割り当てることができます。「グッド ネイバー」テーブルは、destconfig コマンドで定義されます。 詳細については、宛先制御による電子メール配信の管理（894 ページ）を参照してください。
バウンス検証	バウンス メッセージの信頼性を検証します。バウンス検証（895 ページ）を参照してください。
委任管理	管理タスクの分散（1191 ページ）を参照してください。
トレース（デバッグ）	テスト メッセージを使用したメール フローのデバッグ：トレース（1515 ページ）を参照してください。
VLAN、NIC ペアリング	高度なネットワーク構成（1375 ページ）を参照してください。
オプションのアンチウイルス エンジン	オプションのアンチウイルス スキャンを追加することで、アウトバウンド メッセージの完全性を保証できます。アンチウイルス スキャンの概要（439 ページ）を参照してください。

最適化された発信メール配信の電子メールゲートウェイの設定

手順

ステップ 1 提供されているライセンス キーを適用します。システム セットアップ ウィザードを実行する前（電子メールゲートウェイを設定する前）に、このキーを電子メールゲートウェイに適用する必要があります。キーの適用は、[システム管理（System Administration）]>[ライセンスキー（Feature Key）] ページを介して、または CLI の featurekey コマンドを入力して行います。

（注） 前述のライセンス キーには、サンプルの Sophos または McAfee Anti-Virus の 30 日間ライセンスが含まれています。これは、アウトバウンド メールでのアンチウイルス スキャンのテストに使用できます。

ステップ 2 電子メールゲートウェイを再起動します。

ステップ 3 システム セットアップ ウィザード（GUI または CLI）を実行して、電子メールゲートウェイを設定します。

発信メール配信用に最適化された電子メールゲートウェイには、アンチスパムスキャンもアウトブレイクフィルタも含まれないことに注意してください。（これらの章は無視してください）。

（注） クラスタ環境では、D-Mode 機能キーで設定された電子メールゲートウェイを、配信パフォーマンスパッケージで設定されていない AsyncOS 電子メールゲートウェイと組み合わせることはできません。

リソースを節約するバウンス設定の構成

最適化された発信メール配信向けに電子メールゲートウェイを設定した後は、潜在的な配信問題を検出し、特定の宛先へのすべてのメッセージをバウンスするようにシステムを設定できます。

（注） この設定を使用すると、配信不能と見なされる宛先ドメインのキューのすべてのメッセージがバウンスされます。メッセージは、配信問題が解決された後で再送信する必要があります。

リソースを節約するバウンス設定をイネーブルにする例

```
mail3.example.com> bounceconfig

Choose the operation you want to perform:

- NEW - Create a new profile.

- EDIT - Modify a profile.

- DELETE - Remove a profile.

- SETUP - Configure global bounce settings.

[]> setup

Do you want to bounce all enqueued messages bound for a domain if the host is down? [N]>

y
```

この機能を使用する場合、最新の接続試行が 10 回連続で失敗すると、ホストは「ダウン」と見なされます。AsyncOS は、ダウン ホストを 15 分ごとにスキャンします。そのため、接続は、キューがクリアされる前に 11 回以上試行されます。

IronPort Mail Merge（IPMM）を使用した大量のメールの送信

（注） IronPort Mail Merge は、D-Mode 対応電子メールゲートウェイでのみ使用可能です。

IronPort Mail Merge の概要

IronPort Mail Merge を使用すると、個別の個人向けメッセージをカスタマー システムから生成する手間を省くことができます。ユーザは、数千の個別メッセージを生成し、メッセージ生成システムと電子メール ゲートウェイ間で送信する必要がなくなるため、システムにかかる負荷が軽減され、電子メール配信のスループットが向上します。

IPMM では、個人向けに置換されるメッセージの場所を表す変数を使用して、各メッセージの本文が作成されます。各メッセージ受信者に対して、受信電子メールアドレスおよび変数置換だけを電子メール ゲートウェイに送信する必要があります。また、IPMM を使用して、受信者に応じて、送信するメッセージの本文の特定の「パーツ」を含めたり、除外したりできます（たとえば、2 つの異なる国の受信者に送信するメッセージの最後に異なる著作権宣言文を含めることができます）。

Mail Merge 機能の利点

- メール管理者にとって使いやすい。IPMM は、変数置換および一般的な多くの言語の抽象化インターフェイスを提供するため、各受信者の個人向けメッセージを簡単に作成できます。
- メッセージ生成システムの負荷を軽減する。メッセージ本文の 1 つのコピーと必須の置換のテーブルだけが必要であるため、ほとんどのメッセージ生成「作業」をメッセージ生成システムから、最適化された発信メール配信向けに設定された電子メールゲートウェイに移行して、負荷を軽減できます。
- 配信スループットが改善される。数千の着信メッセージを受け取り、キューに入れるために必要なリソースを軽減することで、電子メールゲートウェイは、アウトバウンド配信パフォーマンスを大幅に改善できます。
- キュー ストレージの効率性が向上する。各メッセージ受信に保存する情報を減らすことで、ユーザは、D-Mode 対応電子メールゲートウェイのキューストレージの使用効率を大幅に向上できます。

Mail Merge の使用

SMTP インジェクション

IPMM は、SMTP をトランスポートプロトコルとして拡張します。電子メールゲートウェイで行う特別な設定は必要ありません（デフォルトでは、IPMM は、プライベートリスナーでイネーブルにして、D-Mode 対応電子メールゲートウェイのパブリックリスナーでディセーブルにできます）。ただし、現在、SMTP をインジェクションプロトコルとして使用していない場合は、D-Mode 対応電子メールゲートウェイ インターフェイスを介して SMTP を利用する新しいプライベートリスナーを作成する必要があります。

listenerconfig の setipmm サブコマンドを使用して、リスナーで IPMM を有効にします。詳細については、電子メールを受信するためのゲートウェイの設定 （81 ページ）を参照してください。

IPMM は、MAIL FROM と DATA の 2 つのコマンドを変更し、XDFN を追加することで、SMTP を変更します。MAIL FROM コマンドは XMRG FROM に、DATA コマンドは XPRT に置き換えられています。

Mail Merge メッセージを生成するには、メッセージの生成に使用されるコマンドを特定の順序で発行する必要があります。

1. 送信ホストを示す、初期 EHLO ステートメント。
2. 各メッセージは、送信者アドレスを示す、XMRG FROM: ステートメントで始まります。
3. 各受信者は、次のように定義されます。
4. 1つ以上のXDFN変数割り当てステートメントが含まれます。これには、パーツ定義（XDFN *PART=1,2,3...）やその他の任意の受信者固有の変数が含まれます。
5. 受信者電子メール アドレスは、RCPT TO: ステートメントで定義されます。RCPT TO: の前にあり、前述の XMRG FROM または RCPT TO コマンドの後にある任意の変数割り当ては、この受信者電子メール アドレスにマッピングされます。
6. 各パーツは、XPRT n コマンドを使用して定義されます。各パーツは、DATA コマンドと同様にピリオド（.）文字で終端します。最後のパーツは、XPRT n LAST コマンドで定義されます。

変数置換

メッセージヘッダーなど、メッセージ本文の任意のパーツに、置換用の変数を含めることができます。変数は、HTML メッセージにも表示できます。変数は、ユーザが定義し、アンパサンド（&）文字で始まり、セミコロン（;）文字で終端する必要があります。アスタリスク（*）で始まる変数名は、予約されているため使用できません。

予約変数

IPMM には、事前に定義されている 5 つの特殊な「予約」変数が含まれます。

表 *162 : IPMM* : 予約変数

*FROM	予約変数 *FROM は、「Envelope From」パラメータから派生します。「Envelope From」パラメータは、「XMRG FROM:」コマンドにより設定されます。
*TO	予約変数 *TO は、「RCPT TO:」コマンドで設定される、エンベロープ受信者値から派生します。
*PARTS	予約変数 *PARTS は、パーツのカンマ区切りリストを含みます。これは、「RCPT TO:」で受信者を定義する前に設定され、特定のユーザが受信する「XPRT n」メッセージ本文ブロックを決定します。
*DATE	予約変数 *DATE は、現在の日付スタンプに置き換えられます。
*DK	予約変数 *DK は、DomainKeys 署名プロファイルの指定に使用されます（このプロファイルはすでに AsyncOS に存在している必要があります）。DomainKeys 署名プロファイルの作成の詳細については、電子メール認証 （741 ページ）を参照してください。

メッセージの例 1

次の例のメッセージ本文（ヘッダーを含む）には、最後のメッセージで置換される、4 つの異なる変数と 5 つの置換用の場所が含まれます。同じ変数がメッセージ本文で複数回使用されることがあるため注意してください。また、予約変数 &*TO; が使用されます。これは、受信者の電子メールアドレスに置換されます。この予約変数は、個別の変数として渡す必要はありません。次の例の変数は太字で示されています。

```
From: Mr.Spacely <spacely@example.com>

To: &first_name;&last_name;&*TO;


Subject: Thanks for Being an Example.Com Customer

Dear &first_name;,
Thank you for purchasing a &color; sprocket.
```

このメッセージは、電子メールゲートウェイに一度だけインジェクトする必要があります。各受信者に対して、次の追加情報が必要です。

- 受信者の電子メール アドレス
- 変数置換の名前と値のペア

パーツ アセンブリ

SMTP は、各メッセージ本文に単一の DATA コマンドを使用し、IPMM は、1 つ以上の XPRT コマンドを使用してメッセージを作成します。パーツは、受信者ごとに指定される順序に従ってアセンブルされます。各受信者は、任意またはすべてのメッセージパーツを受信できます。パーツは、任意の順序でアセンブルできます。

特殊な変数 *PARTS は、パーツのカンマ区切りリストを含みます。

たとえば、次の例のメッセージでは、2 つのパーツが含まれます。

最初のパーツには、メッセージヘッダーとメッセージ本文の一部が含まれます。2番目のパーツには、特別なカスタマー向けに含めることができる割引価格が含まれます。

メッセージの例 2（パート 1）

```
From: Mr. Spacely <spacely@example.com>


To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer

Dear &first_name;,

Thank you for purchasing a &color; sprocket.
```

メッセージの例 2（パート 2）

```
Please accept our offer for 10% off your next sprocket purchase.
```

メッセージ部分は、電子メールゲートウェイに一度だけインジェクトする必要があります。この場合、各受信者に、次の追加情報が必要です。

- 最後のメッセージに含まれる、パーツの順序付きリスト
- 受信者の電子メール アドレス
- 変数置換の名前と値のペア

IPMM および DomainKeys 署名

IPMM は、DomainKeys 署名をサポートします。DomainKeys プロファイルを指定するには、*DK 予約変数を使用します。次に例を示します。

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2 *DK=mass_mailing_1
```

この例では、「mail_mailing_1」は、前に設定した DomainKeys プロファイルの名前です。

コマンドの説明

クライアントは、IPMM メッセージをリスナーにインジェクトするときに、次のキーコマンドで拡張 SMTP を使用します。

XMRG FROM

構文：

```
XMRG FROM: <sender email address>
```

このコマンドは、SMTP MAIL FROM: コマンドの代わりに使用されます。これは、次に IPMM メッセージがあることを示します。IPMM ジョブは、XMRG FROM: コマンドで開始されます。

XDFN

構文：

```
XDFN <KEY=VALUE> [KEY=VALUE]
```

XDFN コマンドは、受信者別のメタデータを設定します。キーと値のペアは、オプションでかぎカッコまたは角カッコで囲むことができます。

*PARTS は、XPRT コマンド（以下を参照）で定義されているように、インデックス番号を示す特殊な予約変数です。*PARTS 変数は、整数のカンマ区切りリストとして分割されます。整数は、XPRT コマンドにより定義されているように送信される本文パーツと一致します。その他の予約変数には、*FROM、*TO および *DATE があります。

XPRT

構文：

```
XPRT index_number LAST

Message

.
```

XPRT コマンドは、SMTP DATA コマンドの代わりに使用されます。このコマンドは、コマンド入力後にメッセージパーツの送信者を受け取ります。コマンドは、行の末尾に単一のピリオドを付けて完了します（これは、SMTP DATA コマンドを完了する方法と同じです）。

特殊キーワード **LAST** は、Mail Merge ジョブの最後を示します。これは、インジェクトされる最後のパーツを指定するときに使用する必要があります。

LAST キーワードが使用されると、メッセージがキューに入り、配信が始まります。

変数定義に関する注意事項

- XDFN コマンドで変数を定義する場合、実際のコマンドラインは、システムの物理的制限を超えることはできないため注意してください。D-Mode 対応電子メールゲートウェイの場合、この制限は、1 行あたり 4 KB です。ホスト システムによっては、しきい値がこれより低くなることがあります。非常に長いコマンドラインで複数の変数を定義する場合は注意してください。
- 変数キーと値のペアを定義する場合、スラッシュ「/」文字を使用して、特殊文字をエスケープできます。これは、メッセージ本文に、誤って変数定義と置換される可能性がある HTML 文字エンティティが含まれる場合に役に立ちます（たとえば、文字エンティティ™ は、商標文字の HTML 文字エンティティを定義します）。コマンド XDFN trade=foo を作成して、HTML 文字エンティティ「™」を含む IPMM メッセージを作成した場合、アセンブルされるメッセージには、商標文字ではなく、変数置換（「foo」）が含まれます。これは、GET コマンドを含む URL で使用されることがあるアンパサンド文字「&」の場合も同じです。

IPMM カンバセーションの例

次に、メッセージの例 2（前述の例）での IPMM カンバセーションの例を示します。このメッセージは、この例の 2 人の受信者「Jane User」および「Joe User」に送信されます。

この例では、**太字**フォントは、D-Mode 対応電子メールゲートウェイとの手動による SMTP カンバセーションで入力する内容です。また、等幅フォントは、SMTP サーバからの応答を表し、イタリック体フォントは、コメントまたは変数を表します。

接続が確立されます。

```
220 ESMTP


EHLO foo


250 - ehlo responses from the listener enabled for IPMM
```

カンバセーションが開始されます。

```
XMRG FROM:<user@domain.com> [Note: This replaces the MAIL FROM: SMTP command.]

250 OK
```

変数およびパーツが各受信者に設定されます。

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2

[Note: This line defines three variables (first_name, last_name, and color) and then
uses the *PARTS reserved variable to define that the next recipient defined will receive
message parts numbers 1 and 2.]

250 OK

RCPT TO:<jane@company.com>

250 recipient <jane@company.com> ok

XDFN first_name="Joe" last_name="User" color="black" *PARTS=1

[Note: This line defines three variables (first_name, last_name, and color) and then
uses the *PARTS reserved variable to define that the next recipient defined will receive
message parts numbers 1 only.]

RCPT TO:<joe@company1.com>

250 recipient <joe@company1.com> ok
```

次に、パーツ 1 が送信されます。

```
XPRT 1 [Note: This replaces the DATA SMTP command.]

354 OK, send part

From: Mr. Spacely <spacely@example.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer
```

```
&*DATE;

Dear &first_name;,

Thank you for purchasing a &color; sprocket.

.
```

次に、パーツ 2 が送信されます。LAST キーワードは、パーツ 2 がアセンブルする最後のパーツであることを示すときに使用されます。

```
XPRT 2 LAST

Please accept our offer for 10% off your next sprocket purchase.

.

250 Ok, mailmerge message enqueued
```

「250 Ok, mailmerge message queued」は、メッセージが受け取られたことを示します。

この例に基づいて、受信者 Jane User は、このメッセージを受信します。

```
From: Mr. Spacely <spacely@example.com>

To: Jane User <jane@company.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Jane,

Thank you for purchasing a red sprocket.

Please accept our offer for 10% off your next sprocket purchase.
```

受信者 Joe User は、このメッセージを受信します。

```
From: Mr. Spacely <spacely@example.com>

To: Joe User <joe@company1.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Joe,
```

```
Thank you for purchasing a black sprocket.
```

コード例

シスコは、一般的なプログラミング言語でライブラリを作成して、IPMM メッセージを IPMM 対応の電子メールゲートウェイリスナーにインジェクトするタスクを抽象化します。IPMM ライブラリの使用例については、シスコ カスタマー サポートにお問い合わせください。コードは、構文説明のために広範囲にわたってコメント化されています。

第 48 章

Cisco Secure Email and Web Manager（M シリーズ）の集中型サービス

この章は、次の項で構成されています。

- Cisco Secure Email and Web Manager サービスの概要 （1559 ページ）
- ネットワーク プランニング （1560 ページ）
- 外部スパム隔離の操作 （1560 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離について （1564 ページ）
- 中央集中型レポーティングの設定 （1570 ページ）
- 中央集中型メッセージ トラッキングの設定 （1571 ページ）
- 中央集中型サービスの使用 （1572 ページ）

Cisco Secure Email and Web Manager サービスの概要

Cisco Secure Email and Web Manager（M-Series アプライアンス）は、複数の 電子メールゲートウェイ上の特定のサービスに対して一元化されたインターフェイスを提供する外部または「オフボックス」ロケーションです。

Cisco Secure Email and Web Manager には次の機能が含まれています。

- 外部スパム隔離。エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 一元化されたスパム、ポリシー、ウイルス、およびアウトブレイク隔離。アンチ ウイルス スキャン、アウトブレイク フィルタおよびポリシーにより隔離されたメッセージを保存し管理するために、ファイアウォールの内側の 1 つの場所を提供します。
- 中央集中型レポーティング。複数の電子メールゲートウェイからの集計データに関するレポートを実行します。
- 中央集中型トラッキング。複数の電子メールゲートウェイを通過する電子メールメッセージを追跡します。

Cisco Secure Email and Web Manager の設定および使用に関する詳細については、『Cisco Secure Email and Web Manager User Guide』を参照してください。

⚠

注意 電子メールゲートウェイの二要素認証を有効にしている場合は、事前共有キーを使用して Cisco Secure Email and Web Manager に追加できます。この設定を行うには、CLI で `smaconfig > add` コマンドを使用します。

または

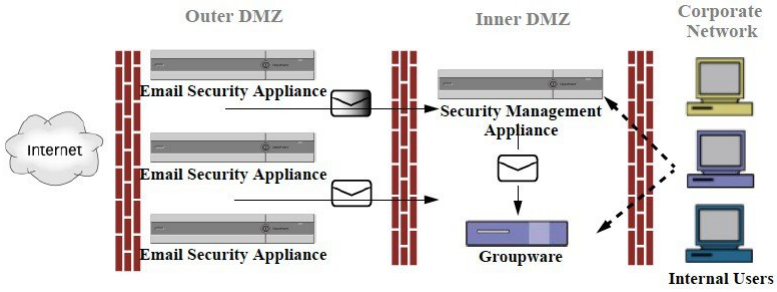
Cisco Secure Email and Web Manager に追加する前に、電子メールゲートウェイの二要素認証を無効にします。詳細については、二要素認証の無効化（1216ページ）を参照してください。

ネットワーク プランニング

Cisco Secure Email and Web Manager を使用すると、エンドユーザ インターフェイス（メールアプリケーションなど）を、さまざまな DMZ 内のよりセキュアなゲートウェイシステムから切り離すことができます。2層ファイアウォールの使用によって、ネットワーク プランニングの柔軟性が高まり、エンドユーザが外部 DMZ に直接接続することを防止できます。

次の図は、Cisco Secure Email and Web Manager と複数の DMZ を組み込んだ一般的なネットワーク設定を示しています。

図 *88 : Cisco Secure Email and Web Manager* による一般的なネットワーク設定



大規模な企業データセンターは、1つまたは複数の電子メールゲートウェイの外部スパム隔離として機能する 1 つの Cisco Secure Email and Web Manager を共有できます。一方、リモートオフィスでは、電子メールゲートウェイのローカル使用のためのローカルスパム隔離を維持できます。

外部スパム隔離の操作

- メールフローおよび外部スパム隔離 （1561 ページ）
- ローカルのスパム隔離から外部の隔離への移行 （1561 ページ）
- 外部スパム隔離と外部セーフリスト/ブロックリストの有効化 （1562 ページ）

• ローカルのスパム隔離を無効化して外部隔離をアクティブ化する （1563 ページ）
• 外部のスパム隔離のトラブルシューティング （1564 ページ）

メールフローおよび外部スパム隔離

ネットワークがネットワーク プランニング（1560ページ）の説明に従って設定される場合、インターネットからの着信メールは外部 DMZ のアプライアンスによって受信されます。正規のメールは、内部 DMZ のメール転送エージェント（MTA）（グループウェア）に従って、最終的に企業ネットワーク内のエンドユーザまで送信されます。

スパムおよび陽性と疑わしいスパム（メールフローポリシー設定値に基づく）は、Cisco Secure Email and Web Manager のスパム隔離エリアに送信されます。次にエンドユーザが隔離エリアにアクセスして、スパムを削除し、自分宛に配信されるメッセージを解放することを選択できます。スパム隔離に残っているメッセージは、設定された期間後に自動的に削除されます。

Cisco Secure Email and Web Manager で外部隔離からリリースされているメッセージは、配信元の 電子メールゲートウェイに返されます。これらのメッセージは通常、配信前に、HAT およびその他のポリシーやスキャンの設定、RAT、ドメイン例外、エイリアシング、着信フィルタ、マスカレード、バウンス検証、およびワーク キューの各プロセスを通過しません。

Cisco Secure Email and Web Manager にメールを送信するように設定された 電子メールゲートウェイは、その Cisco Secure Email and Web Manager からリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。これを機能させるために、 Cisco Secure Email and Web Manager の IP アドレスが変更されないようにしてください。 Cisco Secure Email and Web Manager の IP アドレスが変わると、受信側の 電子メールゲートウェイは、メッセージを他の着信メッセージであるものとして処理します。 Cisco Secure Email and Web Manager の受信と配信では、常に同じ IP アドレスを使用する必要があります。

Cisco Secure Email and Web Manager では、スパム隔離設定で指定されている IP アドレスから隔離対象のメールを受け入れます。セキュリティ管理アプライアンスでスパム隔離を設定するには、『 Cisco Secure Email and Web Manager User Guide』を参照してください。

Cisco Secure Email and Web Manager によってリリースされたメールは、スパム隔離設定で定義されたように、プライマリおよびセカンダリホストに配信されます（『 Cisco Secure Email and Web Manager User Guide』を参照）。したがって、 Cisco Secure Email and Web Manager にメールを配信する 電子メールゲートウェイの数に関係なく、リリースされるすべてのメール、通知、およびアラートが単一のホスト（グループウェアまたはコンテンツ セキュリティ アプライアンス）に送信されます。 Cisco Secure Email and Web Manager からの配信によって、プライマリホストが過負荷にならないように注意してください。

ローカルのスパム隔離から外部の隔離への移行

電子メールゲートウェイ上で現在使用中のローカルのスパム隔離を、そのローカル隔離内のメッセージにアクセスできるようにしたまま、 Cisco Secure Email and Web Manager でホストされる外部スパム隔離に移行する場合は、移行中に新しいメッセージがローカル隔離に入らないようにする必要があります。

次の戦略の使用を検討します。

- スパム対策の設定： Cisco Secure Email and Web Manager を代替ホストとして指定して、メールポリシーにスパム対策を設定します。この処置により、ローカル隔離にアクセス可能なまま、新しいスパムは外部の隔離に送信されます。
- より短い有効期限の設定：ローカル隔離に対して [次の日数の経過後に削除（Schedule Delete After）] 設定をより短い期間に設定します。
- 残っているすべてのメッセージを削除：ローカル隔離内に残っているすべてのメッセージを削除するには、その隔離をディセーブルにし、ローカル隔離のページで [すべて削除（Delete All）] リンクをクリックします（スパム隔離からのメッセージの削除（1188 ページ）を参照）。このリンクは、まだメッセージが残っているローカルのスパム隔離がディセーブルになっているときにだけ使用可能になります。

これで外部隔離をイネーブルにし、ローカル隔離をディセーブルにする準備ができます。

（注） ローカル隔離と外部隔離の両方がイネーブルの場合、ローカル隔離が使用されます。

外部スパム隔離と外部セーフリスト/ブロックリストの有効化

電子メールゲートウェイでは、外部スパム隔離を 1 つだけイネーブルにすることができます。

はじめる前に

- メールフローおよび外部スパム隔離 （1561 ページ）の情報を確認してください。
- ローカルのスパム隔離から外部の隔離への移行（1561 ページ）の情報を確認してから実行してください。
- 中央集中型スパム隔離およびセーフリスト/ブロックリスト機能をサポートするように Cisco Secure Email and Web Manager を設定します。 Cisco Secure Email and Web Manager のマニュアルを参照してください。
- これまで、E メール セキュリティ アプライアンスに別の外部スパム隔離を設定していた場合は、まず、その外部スパム隔離設定をディセーブルにする必要があります。

電子メールゲートウェイごとに次の手順を完了します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2 [構成] をクリックします。

ステップ 3 [スパム外部隔離を有効にする（Enable External Spam Quarantine）] を選択します。

ステップ 4 [名前（Name）] フィールドに、 Cisco Secure Email and Web Manager の名前を入力します。

この名前に意味はありません。参照目的でのみ使用されます。たとえば、 Cisco Secure Email and Web Manager のホスト名を入力します。

ステップ 5 IP アドレスとポート番号を入力します。

これらは [スパム隔離設定（Spam Quarantines Settings）] ページ（[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）]）で Cisco Secure Email and Web Manager に指定した IP アドレスとポート番号に一致する必要があります。

ステップ 6 （任意）**外部のセーフリスト/ブロック リスト**機能をイネーブルにするチェックボックスをオンにして、適切なブロック リスト アクションを指定します。

ステップ 7 変更を送信し、保存します。

ステップ 8 この手順を 電子メールゲートウェイごとに繰り返します。

次のタスク

ローカル隔離を使用していた場合は、ローカルのスパム隔離を無効化して外部隔離をアクティブ化する （1563 ページ）を参照してください。

関連項目

- ローカルのスパム隔離と外部のスパム隔離 （1154 ページ）
- スパム隔離 （1153 ページ）
- スパムおよびグレイメールの管理 （461 ページ）
- メッセージがスパムかどうかスキャンするための電子メールゲートウェイの設定方法 （462 ページ）

ローカルのスパム隔離を無効化して外部隔離をアクティブ化する

外部スパム隔離をイネーブルにする前に、ローカルのスパム隔離を使用していた場合、外部検疫にメッセージを送信するためにはローカル隔離をディセーブルにする必要があります。

はじめる前に

外部スパム隔離と外部セーフリスト/ブロックリストの有効化 （1562 ページ）の「はじめる前に」の項の情報を含む、すべての手順に従ってください。

手順

ステップ 1 [モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2 [スパム検疫（Spam Quarantine）] セクションで、[スパム検疫（Spam Quarantine）] リンクをクリックします。

ステップ 3 [スパム隔離を有効にする（Enable Spam Quarantine）] をオフにします。

この変更によって生じたメールポリシーを調整するための警告は無視します。外部隔離を設定していた場合、メール ポリシーは自動的に外部スパム隔離にメッセージを送信します。

ステップ 4 変更を送信し、保存します。

外部のスパム隔離のトラブルシューティング

問題： Cisco Secure Email and Web Manager からリリースされたメッセージが、 電子メールゲートウェイによって不必要に再処理されます。

解決策：これは、 Cisco Secure Email and Web Manager の IP アドレスが変更された場合に発生することがあります。メールフローおよび外部スパム隔離 （1561 ページ） を参照してください。

一元化されたポリシー、ウイルス、アウトブレイク隔離について

- 集約されたポリシー、ウイルス、およびアウトブレイク隔離 （1564 ページ）
- ポリシー、ウイルス、アウトブレイク隔離の移行について （1565 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離の集約 （1566 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について （1568 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング （1569 ページ）

集約されたポリシー、ウイルス、およびアウトブレイク隔離

Cisco Secure Email and Web Manager 上でポリシー、ウイルス、およびアウトブレイク隔離を集約できます。メッセージは、 電子メールゲートウェイによって処理されますが、 Cisco Secure Email and Web Manager 上の隔離に格納されます。

ポリシー、ウイルス、およびアウトブレイク隔離を一元化する利点としては、次のものがあります。

- 管理者は複数の 電子メールゲートウェイで隔離されたメッセージを 1 ヵ所で管理できます。
- セキュリティ リスクを減らすため、隔離されたメッセージは DMZ 内ではなくファイアウォールの内側に保管されます。
- 集約された隔離は、 Cisco Secure Email and Web Manager の標準のバックアップ機能を使用してバックアップできます。

詳細については、お使いの Cisco Secure Email and Web Manager のユーザマニュアルまたはオンラインヘルプを参照してください。

一元化されたポリシー、ウイルス、アウトブレイク隔離の制限事項

- 各電子メールゲートウェイでは、すべてのポリシー、ウイルス、アウトブレイク隔離を一元化するか、またはすべてローカルに保存する必要があります。
- スキャンエンジンが Cisco Secure Email and Web Manager では使用できないため、ウイルスについてのポリシー、ウイルス、またはアウトブレイク隔離のテストメッセージを手動でテストできません。

クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件

一元化されたポリシー、ウイルス、およびアウトブレイク隔離を、クラスタ化されたアプライアンスの任意のレベルでイネーブルにできます。

要件：

- 電子メールゲートウェイの特定のレベル（マシン、グループ、またはクラスタ）で一元化されたポリシー、ウイルス、アウトブレイク隔離をイネーブルにする前に、同じレベルに属するすべてのアプライアンスを最初に Cisco Secure Email and Web Manager に追加する必要があります。
- コンテンツ、メッセージ フィルタおよび DLP メッセージ アクションは同じレベルで設定され、そのレベル以下のすべてのレベルで上書きされない必要があります。
- 一元化されたポリシー、ウイルス、アウトブレイク隔離は同じレベルで設定され、設定したレベル以下のすべてのレベルで上書きされない必要があります。
- Cisco Secure Email and Web Manager との通信に使用するインターフェイスが、グループまたはクラスタ内のすべてのアプライアンスで同じ名前になっていることを確認します。

次に例を示します。

電子メールゲートウェイで、クラスタまたはグループレベルで一元化されたポリシー、ウイルス、アウトブレイク隔離をイネーブルにしたい一方で、クラスタに接続されているが設定がマシンレベルで定義されている場合、クラスタまたはグループレベルでこの機能をイネーブルにする前に、マシンレベルでの集中型の隔離設定を削除する必要があります。

ポリシー、ウイルス、アウトブレイク隔離の移行について

ポリシー、ウイルス、アウトブレイク隔離を一元化すると、電子メールゲートウェイの既存のポリシー、ウイルス、アウトブレイク隔離は Cisco Secure Email and Web Manager に移行します。

Cisco Secure Email and Web Manager で移行を設定しますが、電子メールゲートウェイで一元化されたポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化の変更を確定したときに移行が発生します。

この変更を確定すると、次が発生します。

- 電子メールゲートウェイのローカルポリシー、ウイルス、アウトブレイク隔離がディセーブルになります。これらの隔離に入る新しいメッセージはすべて、 Cisco Secure Email and Web Manager で隔離されます。
- Cisco Secure Email and Web Manager への既存の非スパム隔離の移行が開始されます。

- すべてのローカルポリシー、ウイルス、アウトブレイク隔離が削除されます。カスタム移行を設定した場合は、移行しないように選択したローカルポリシー隔離もすべて削除されます。ポリシー隔離の削除の影響については、ポリシー隔離の削除について （1138 ページ）を参照してください。
- 移行前に複数の隔離に存在したメッセージは、移行後に該当の集中型隔離に存在します。
- 移行はバックグラウンドで実行されます。かかる時間は、隔離エリアのサイズとネットワークによって異なります。電子メールゲートウェイで中央集中型の隔離をイネーブルにすると、移行が完了したときに通知を受け取るための 1 つまたは複数の電子メールアドレスを入力できます。
- 送信元ローカル隔離ではなく中央集中型の隔離の設定が、それらのメッセージに適用されます。ただし、元の有効期限は各メッセージに適用されたままです。

（注） 移行時に自動的に作成されるすべての中央集中型の隔離は、デフォルトの隔離設定になります。

ポリシー、ウイルス、およびアウトブレイク隔離の集約

始める前に

（注） メンテナンス ウィンドウからまたはピーク時間帯以外に、この手順を実行してください。

- 最初に Cisco Secure Email and Web Manager に、一元化されたポリシー、ウイルス、アウトブレイク隔離の設定をします。オンラインヘルプの「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の章の「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の項にあるテーブル、または Cisco Secure Email and Web Manager のユーザーガイドを参照してください。
- Cisco Secure Email and Web Managerで中央集中型の隔離に割り当てられた容量が既存のローカル隔離が占める総容量よりも小さい場合、メッセージは Cisco Secure Email and Web Manager の隔離の設定に基づいて早期に期限切れとなります。移行の前に、隔離エリアのサイズを減らす手動の操作を行うことを検討してください。早期の期限切れの詳細については、隔離メッセージに自動的に適用されるデフォルトアクション （1135 ページ）を参照してください。
- 自動的な移行を選択する場合、または移行中に中央集中型の隔離を作成するためのカスタム移行を設定する場合は、中央集中型の隔離を設定するためのガイドラインとして使用できるよう、現在の電子メールゲートウェイの隔離設定を書き留めておくようにしてください。
- 電子メールゲートウェイをクラスタ コンフィギュレーションで展開している場合は、クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件 （1565 ページ）を参照してください。

- この手順で確定した変更は、すぐに発生することに注意してください。ポリシー、ウイルス、アウトブレイク隔離の移行について （1565 ページ）を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 Cisco Secure Email and Web Manager との通信に使用するインターフェイスおよびポートを入力します。

Cisco Secure Email and Web Manager からインターフェイスおよびポートに到達可能であることを確認します。

電子メールゲートウェイがクラスタ化されている場合、選択したインターフェイスがクラスタ内のすべてのマシンで使用できる必要があります。

ステップ 4 移行が完了したときに通知を受け取るには、1 つまたは複数の電子メールアドレスを入力します。

ステップ 5 想定どおりであるか確認するために、移行された隔離に関する情報を確認します。

ステップ 6 カスタム移行を完了した場合は、この手順で変更を確定した際に削除される隔離に注意してください。

ステップ 7 コンテンツおよびメッセージ フィルタ、およびアップデートするための DLP メッセージ アクションに関する情報が、想定どおりであることを確認します。

（注） クラスタ設定では、フィルタおよびメッセージ アクションが特定のレベルで定義され、そのレベル以下のすべてのレベルで上書きされていない場合に限り、メッセージ フィルタ アクションは特定のレベルで自動的にアップデートできます。移行後は、中央集中型の隔離名でフィルタおよびメッセージアクションを手動で再設定する必要があります。

ステップ 8 移行のマッピングを再設定する必要がある場合は、次を実行します。

a) Cisco Secure Email and Web Manager に戻ります。

b) 移行のマッピングを再設定します。

Cisco Secure Email and Web Manager で、再マッピングする隔離を選択し、**[集中型隔離から削除（Remove from Centralized Quarantine）]** をクリックします。その後、隔離を再マッピングできます。

c) Cisco Secure Email and Web Manager で新たに移行の設定を確定します。

d) この手順を最初から繰り返します。

重要[セキュリティ サービス（Security Services）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] ページを必ずリロードしてください。

ステップ 9 [送信（Submit）] をクリックします。

ステップ 10 移行のマッピングを再設定する必要がある場合は、ステップ 8 の手順に従います。

ステップ 11 変更を保存します。

（注） 移行の進行中は、電子メールゲートウェイまたは Cisco Secure Email and Web Manager の構成を変更しないでください。

ステップ 12 ページの上部で移行ステータスを確認します。また、移行を設定するときに電子メールアドレスを入力した場合は、移行の完了を通知する電子メールを待ってください。

次のタスク

オンラインヘルプの「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の項目にある表、または Cisco Secure Email and Web Manager のユーザーガイドに記載されているその他の作業を実行します。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定（1142 ページ）

一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について

電子メールゲートウェイで一元化されたポリシー、ウイルス、アウトブレイク隔離を無効にする場合、次が発生します。

- ローカル隔離は、電子メールゲートウェイ上で自動的にイネーブルになります。
- システムに作成された隔離、およびメッセージフィルタ、コンテンツフィルタ、DLP メッセージアクションから参照される隔離は、自動的に電子メールゲートウェイで作成されます。ウイルス、アウトブレイク、および未分類の隔離は、割り当て済みユーザルールを含め、隔離が一元化される前と同じ設定で作成されます。その他すべての隔離は、デフォルト設定で作成されます。
- 新しく隔離されたメッセージは、すぐにローカル隔離に入ります。
- 中央集中型の隔離エリア内のメッセージは、ディセーブルにされたとき、次のいずれかが発生するまでそのままです。
  - 有効期限が切れたとき、メッセージは手動で削除するか自動的に削除されます。
  - メッセージは次のいずれかに該当する場合、手動または自動的にリリースされます。

* Cisco Secure Email and Web Manager で代替のリリースのアプライアンスが設定されている。Cisco Secure Email and Web Manager のオンラインヘルプまたはマニュアルを参照してください。

* 中央集中型の隔離が電子メールゲートウェイ上で再度イネーブルになります。

中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化

始める前に

- 中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化の影響を理解します。
- 次のいずれかを実行します。
  - 現在中央集中型のポリシー、およびウイルス アウトブレイク隔離内にあるすべてのメッセージを処理します。
  - ディセーブルにした後で、中央集中型の隔離エリアから解放されるメッセージを処理する代替のリリースのアプライアンスが指定されていることを確認します。詳細については、お使いの Cisco Secure Email and Web Manager のオンラインヘルプまたはユーザーガイドを参照してください。

手順

ステップ 1 電子メールゲートウェイで、[セキュリティサービス（Security Services）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2 一元化されたスパム、ポリシー、ウイルス、およびアウトブレイク隔離をディセーブルにします。

ステップ 3 変更内容を送信し、確定します。

ステップ 4 新しく作成したローカル隔離の設定をカスタマイズします。

一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング

Cisco Secure Email and Web Manager が使用できない場合

ポリシー、ウイルス、アウトブレイク隔離が使用できなくなった Cisco Secure Email and Web Manager で一元化されている場合、電子メールゲートウェイでこれらの中央集中型の隔離を無効にする必要があります。

交換用 Cisco Secure Email and Web Manager を展開する場合は、Cisco Secure Email and Web Manager と各電子メールゲートウェイで隔離の移行を再設定しなければなりません。オンラインヘルプの「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の章の「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の項にあるテーブル、またはCisco Secure Email and Web Manager のユーザーガイドを参照してください。

中央集中型レポーティングの設定

始める前に

- Cisco Secure Email and Web Manager の中央集中型レポーティングを有効にし、設定します。前提条件と手順について、『 Cisco Secure Email and Web Manager User Guide』を参照してください。
- Cisco Secure Email and Web Manager でレポーティングサービスに十分なディスク領域が割り当てられていることを確認します。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [レポート（Reporting）] をクリックします。

ステップ 2 [レポート サービス（Reporting Service）] セクションで [集約管理レポート（Centralized Reporting）] オプションを選択します。

ステップ 3 変更を送信し、保存します。

高度なマルウェア防御レポートの要件

Cisco Secure Email and Web Manager での高度なマルウェア防御（ファイルレピュテーションとファイル分析）機能に関する完全なレポートに必要な設定については、オンラインヘルプの電子メールレポートの章の高度なマルウェア防御レポートについての情報、またはお使いのバージョンの Cisco Secure Email and Web Manager ソフトウェアのユーザーガイドを参照してください。

中央集中型レポーティングに変更後のレポート情報の可用性

電子メールゲートウェイで中央集中型レポーティングがイネーブルな場合

- 電子メールゲートウェイにある月次レポート用の既存データは、Cisco Secure Email and Web Manager に転送されません。
- 電子メールゲートウェイにあるアーカイブレポートは、使用できなくなります。
- 電子メールゲートウェイは週次データのみ保存します。
- 月次レポートおよび年次レポート用の新規データは、Cisco Secure Email and Web Manager に保存されます。
- 電子メールゲートウェイでスケジュール設定されたレポートは、停止されます。
- 電子メールゲートウェイ上のスケジュール設定されたレポートの設定ページにはアクセスできなくなります。

中央集中型レポーティングのディセーブル化について

電子メールゲートウェイで中央集中型レポーティングをディセーブルにした場合、電子メールゲートウェイで新規月次レポートデータの保存が開始され、スケジュールされたレポートが再開し、アーカイブされたレポートにアクセスできます。中央集中型レポーティングをディセーブルにした場合に、E メール セキュリティ アプライアンスでは、過去の時間および日ごとのデータだけが表示され、過去の週ごとや月ごとのデータは表示されません。これは、一時的な変更です。十分なデータが蓄積されれば、過去の週および月のレポートが表示されます。電子メールゲートウェイを中央集中型レポーティングモードに戻した場合、過去の週のデータはインタラクティブレポートに表示されます。

中央集中型メッセージ トラッキングの設定

始める前に

（注） 電子メールゲートウェイで中央集中型トラッキングおよびローカルトラッキングの両方をイネーブルにすることはできません。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [メッセージ トラッキング（Message Tracking）] をクリックします。

ステップ 2 [メッセージ トラッキング サービス（Message Tracking Service）] セクションで [設定を編集（Edit Settings）] をクリックします。

ステップ 3 [メッセージ トラッキング サービスを有効にする（Enable Message Tracking Service）] チェックボックスを選択します。

ステップ 4 [集約管理トラッキング（Centralized Tracking）] オプションを選択します。

ステップ 5 （任意）拒否された接続に関する情報を保存するチェックボックスをオンにします。

（注） 拒否された接続のトラッキング情報を保存すると、 Cisco Secure Email and Web Manager のパフォーマンスに悪影響を与えるおそれがあります。

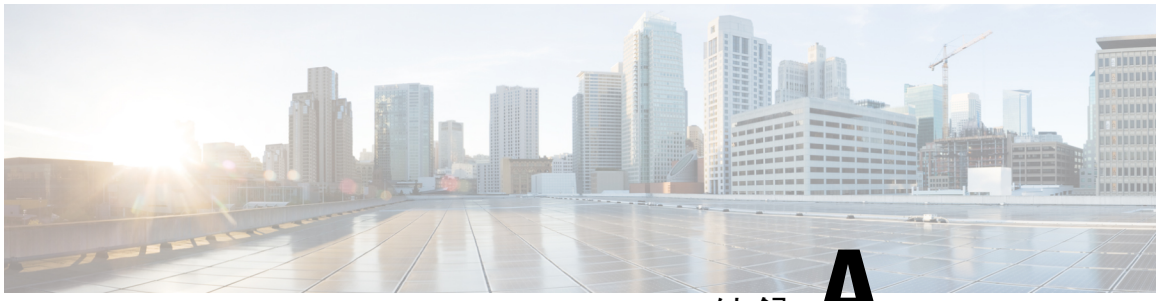
ステップ 6 変更を送信し、保存します。

次のタスク

中央集中型トラッキングを使用するには、電子メールゲートウェイと Cisco Secure Email and Web Manager の両方で監視機能をイネーブルにする必要があります。 Cisco Secure Email and Web Manager の集中型トラッキングを有効にするには、『 Cisco Secure Email and Web Manager User Guide』を参照してください。

中央集中型サービスの使用

中央集中型サービスを使用する手順については、『 Cisco Secure Email and Web Manager User Guide』を参照してください。



付録 A

FTP、SSH、および SCP アクセス

この付録の構成は、次のとおりです。

- IP インターフェイス （1573 ページ）
- 電子メールゲートウェイへの FTP アクセスの設定 （1574 ページ）
- セキュア コピー（scp）アクセス （1576 ページ）
- シリアル接続経由での 電子メールゲートウェイへのアクセス （1577 ページ）

IP インターフェイス

IP インターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1 つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IP インターフェイスまたは両方にインターネット プロトコル バージョン 4（IPv4）または IP Version 6（IPv6）を割り当てることができます。

表 *163*: インターフェイスに対してデフォルトでイネーブルになるサービス

		デフォルトで有効かどうか	
サービス	デフォルト ポート	管理インターフェイス[2]	新規作成されたインターフェイス
FTP	21	×	×
SSH	22	対応	×
HTTP	80	対応	×
HTTPS	443	対応	×

[2] ここに示す「管理インターフェイス」の設定は、Cisco C170 電子メールゲートウェイの Data 1 インターフェイスのデフォルト設定でもあります。

- グラフィカル ユーザー インターフェイス（GUI）を使用して電子メールゲートウェイにアクセスする必要がある場合は、インターフェイスで HTTP、HTTPS、またはその両方をイネーブルにする必要があります。

- 設定ファイルのアップロードまたはダウンロードを目的として電子メールゲートウェイにアクセスする必要がある場合は、インターフェイスでFTPをイネーブルにする必要があります。
- Secure Copy（scp）を使用しても、ファイルをアップロードまたはダウンロードできます。

IP インターフェイス経由のスパム隔離への HTTP または HTTPS アクセスを設定できます。

電子メール配信および仮想ゲートウェイの場合、各 IP インターフェイスは特定の IP アドレスおよびホスト名を持つ1つの仮想ゲートウェイアドレスとして機能します。インターフェイスを独立したグループに（CLI を使用して）「参加」させることもできます。システムは、電子メールの配信時にこれらのグループを順番に使用します。

仮想ゲートウェイの参加またはグループ化は、大規模な電子メールキャンペーンを複数のインターフェイス間でロードバランシングする際に役立ちます。VLAN を作成し、他のインターフェイスと同様に（CLI を使用して）設定することもできます。詳細については、高度なネットワーク構成 （1375 ページ）を参照してください。

関連項目

- AsynOS によるデフォルト IP インターフェイスの選択方法 （1574 ページ）

AsynOS によるデフォルト IP インターフェイスの選択方法

AsyncOS は、[ネットワーク（Network）]>[IPインターフェイス（IP Interfaces）]ページまたは `ifconfig` CLI コマンドで表示された最も小さな番号の IP アドレスに基づいてデフォルト IP インターフェイスを選択します。当該のサブネット上に存在するリストの最初のIPインターフェイスが使用されます。

同一サブネット内で複数のIPアドレスがデフォルトゲートウェイとして設定されている場合、最も小さな番号の IP アドレスが使用されます。たとえば、次の IP アドレスが同一サブネット内で設定されているとします。

- `10.10.10.2/24`
- `10.10.10.30/24`
- `10.10.10.100/24`
- `10.10.10.105/24`

AsyncOS はデフォルトの IP インターフェイスとして `10.10.10.2/24` を選択します。

電子メールゲートウェイへの FTP アクセスの設定

手順

ステップ 1 [ネットワーク（Network）]>[IPインターフェイス（IP Interfaces）]ページまたは `interfaceconfig` コマンドを使用して、インターフェイスに対して FTP アクセスをイネーブルにします。

FTP、SSH、および SCP アクセス

危険 サービスを interfaceconfig コマンドでディセーブルにすると、CLI との接続が解除されることがあります。これは、電子メールゲートウェイにどのように接続しているかによって異なります。別のプロトコル、シリアルインターフェイス、または管理ポートのデフォルト設定を使用して電子メールゲートウェイに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。

ステップ 2 変更を送信し、保存します。

ステップ 3 FTP 経由でインターフェイスにアクセスします。インターフェイスに対して正しい IP アドレスを使用していることを確認します。次に例を示します。

```
$ ftp 192.168.42.42
```

（注） ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。

ステップ 4 実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照し、ファイルをコピーおよび追加（「GET」および「PUT」）できます。次の表を参照してください。

ディレクトリ名	説明
/configuration	以下のコマンドからのデータがこのディレクトリにエクスポートされるか、このディレクトリからデータがインポート（保存）されます。 • Virtual Gateway マッピング（altsrchost） • XML 形式の設定データ（saveconfig、loadconfig） • ホスト アクセス テーブル（HAT）（hostaccess） • 受信者アクセス テーブル（RAT）（rcptaccess） • SMTP ルート エントリ（smtproutes） • エイリアス テーブル（aliasconfig） • マスカレード テーブル（masquerade） • メッセージ フィルタ（filters） • グローバル配信停止データ（unsubscribe） • trace コマンドのテスト メッセージ • セーフリスト/ブロックリスト バックアップ ファイル（*slbl*<タイムスタンプ><シリアル番号>*.csv* 形式で保存）
/antivirus	Anti-Virus エンジンのログ ファイルが保存されるディレクトリです。このディレクトリにあるログ ファイルを検査して、ウイルス定義ファイル（scan.dat）の成功した最終ダウンロードを手動で確認できます。

ディレクトリ名	説明
/configuration /system_logs /cli_logs /status /reportd_logs reportqueryd_logs /ftpd_logs /mail_logs /asarchive /bounces /error_logs /avarchive /gui_logs /sntpd_logs /RAID.output /euq_logs /scanning /antispam /antivirus /euqgui_logs /ipmitool.output	`logconfig` コマンドと `rollovernow` コマンドを使用するロギング用に自動的に作成されます。各ログの詳細については、ログ （1391 ページ）を参照してください。 ログ ファイル タイプの違いについては、「ログ ファイル タイプの比較」を参照してください。

ステップ 5 ご使用のFTPプログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

セキュア コピー（scp）アクセス

クライアント オペレーティング システムで secure copy（`scp`）コマンドをサポートしている場合は、前述の表に示すディレクトリ間でファイルをコピーできます。たとえば、次の例では、ファイル `/tmp/test.txt` は、クライアントマシンからホスト名が `mail3.example.com` の電子メールゲートウェイの configuration ディレクトリにコピーされます。

コマンドを実行すると、ユーザー（admin）のパスフレーズを求めるプロンプトが表示されることに注意してください。この例を参考用としてだけ示します。特殊なオペレーティング システムの secure copy の実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration

The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.

DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.

admin@mail3.example.com's passphrase: (type the passphrase)

test.txt 100% |***************************| 1007 00:00

%
```

この例では、同じファイルが電子メールゲートウェイからクライアントマシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .

admin@mail3.example.com's passphrase: (type the passphrase)

test.txt 100% |***************************| 1007 00:00

%
```

電子メールゲートウェイに対するファイルの転送および取得には、セキュアコピー（scp）を FTP に代わる方法として使用できます。

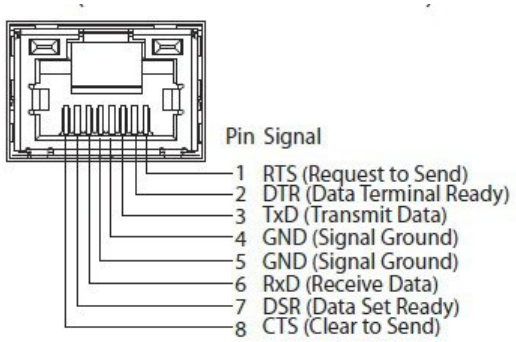
（注） operators グループおよび administrators グループのユーザのみが、電子メールゲートウェイへのアクセスにセキュアコピー（scp）を使用できます。詳細については、ユーザの追加 （1195 ページ）を参照してください。

シリアル接続経由での電子メールゲートウェイへのアクセス

シリアル接続を介して電子メールゲートウェイに接続する場合は、コンソールポートに関する次の情報を使用します。

このポートの詳細については、アプライアンスのハードウェア インストール ガイドを参照してください。

80 および 90 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細



70 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細

次の図に、シリアル ポート コネクタのピン番号を示し、以下の表でシリアル ポート コネクタのピン割り当てとインターフェイス信号を定義します。

図 *89 :* シリアル ポートのピン番号

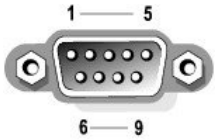
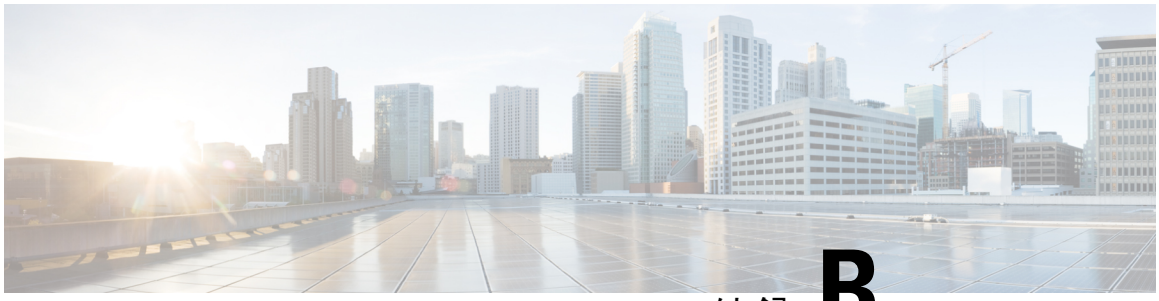


表 *164 :* シリアル ポートのピン割り当て

ピン	信号	I/O	定義
1	DCD		データ キャリア検出
2	SIN		シリアル入力
3	SOUT		シリアル出力
4	DTR		データ ターミナル レディ
5	GND	適用対象外	信号用接地
6	DSR		データ セット レディ
7	RTS		送信要求
8	CTS		送信可

ピン	信号	I/O	定義
9	RI		リング インジケータ
シェル	適用対象外	適用対象外	シャーシ アース

FTP、SSH、および SCP アクセス



付録 B

ネットワークと IP アドレスの割り当て

この付録の構成は、次のとおりです。

- イーサネット インターフェイス （1581 ページ）
- IP アドレスとネットマスクの選択 （1581 ページ）
- 電子メールゲートウェイを接続するための戦略 （1584 ページ）

イーサネット インターフェイス

電子メールゲートウェイには、構成（任意選択の光ネットワークインターフェイスがあるかどうか）に応じて、システムの背面パネルに最大4つのイーサネットインターフェイスがあります。次のラベルが付いています。

- 管理
- Data1
- Data2
- Data3
- Data4

IP アドレスとネットマスクの選択

ネットワークを設定するとき、 電子メールゲートウェイが発信パケットを送信するインターフェイスを一意に選択できる必要があります。この要件によって、イーサネットインターフェイスのIPアドレスとネットマスクの選択に関して、いくつかのことが決まります。単一のネットワークに配置できるインターフェイスは1つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、指定されたネットワークの物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとしていずれか 1 つの IP アドレスを使用して、インターフェイスからパケットを送信できます。このプロパティは、仮想ゲートウェイ テクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは IP アドレスの残りのビットです。4 オクテット アドレス内の有効なビット数は、クラスレス ドメイン間ルーティング（CIDR）形式で表現されることがあります。これは、スラッシュ記号、後にビット数（1～32）が続きます。

この方法では、単純にバイナリ表記で 1 を数えることでネットマスクを表現できます。したがって 255.255.255.0 は「/24」となり、255.255.240.0 は「/20 」となります。

インターフェイス設定のサンプル

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。 電子メールゲートウェイの場合、これらのインターフェイス名は、3 つのインターフェイス（Management、Data1、Data2）の中の 2 つのインターフェイスを示します。

ネットワーク 1：

個別のインターフェイスは別のネットワーク上に存在するように示す必要があります。

インターフェイス	IPアドレス	ネットマスク	ネットアドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.X 宛てのデータ（X は自分のアドレスを除く 1 ～ 255 の任意の数字、この場合は 10）は Int1 に出力されます。192.168.0.X 宛てのすべてのデータは Int2 に出力されます。この形式ではない他のアドレス（最も考えられるのは WAN またはインターネット上）に向かうパケットは、デフォルト ゲートウェイに送信されます。デフォルト ゲートウェイはこれらのネットワークのどちらかの上に存在する必要があります。その後、デフォルト ゲートウェイがパケットを転送します。

ネットワーク 2：

2 つの異なるインターフェイスのネットワーク アドレス（IP アドレスのネットワーク部分）は同じにすることができません。

イーサネットインターフェイス	IPアドレス	ネットマスク	ネットアドレス
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

これは、2 つのイーサネット インターフェイスが同じネットワーク アドレスを持つという、競合した状態を表しています。コンテンツ セキュリティ アプライアンスからのパケットが 192.168.1.11 に送信された場合、パケットの配信にどのイーサネット インターフェイスを使用すべきかは特定できません。2 つのイーサネット インターフェイスが 2 つの物理ネットワーク

に別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。電子メールゲートウェイでは、競合するネットワークを設定できません。

2つのイーサネットインターフェイスを同じ物理ネットワークに接続することはできますが、電子メールゲートウェイが一意の配信インターフェイスを選択できるようにIPアドレスとネットマスクを設定する必要があります。

IP アドレス、インターフェイス、およびルーティング

GUI または CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルト ゲートウェイ）が選択した内容よりも優先されます。

たとえば、3つのネットワーク インターフェイスがそれぞれ別のネットワークセグメントに設定された次のような 電子メールゲートウェイがあるとします（すべて /24 と仮定）。

イーサネット	IP
管理	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

デフォルト ゲートウェイは 192.19.0.1 です。

ここで、AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、Data1 上の IP（192.19.1.100）を選択した場合、すべての TCP トラフィックが Data1 イーサネット インターフェイス経由になると予想されることと思います。しかし、実際には、デフォルト ゲートウェイとして設定されているインターフェイス（ここではManagement）からトラフィックが送出されます。ただし、トラフィックの送信元アドレスには Data1 の IP が設定されています。

要約

コンテンツ セキュリティ アプライアンスは、配信可能なパケットが経由する一意のインターフェイスを常に識別できなければなりません。この決定を行うために、電子メールゲートウェイは、パケットの宛先 IP アドレスと、そのイーサネット インターフェイスのネットワークおよび IP アドレス設定を組み合わせて使用します。次の表に、ここまで説明してきた例をまとめます。

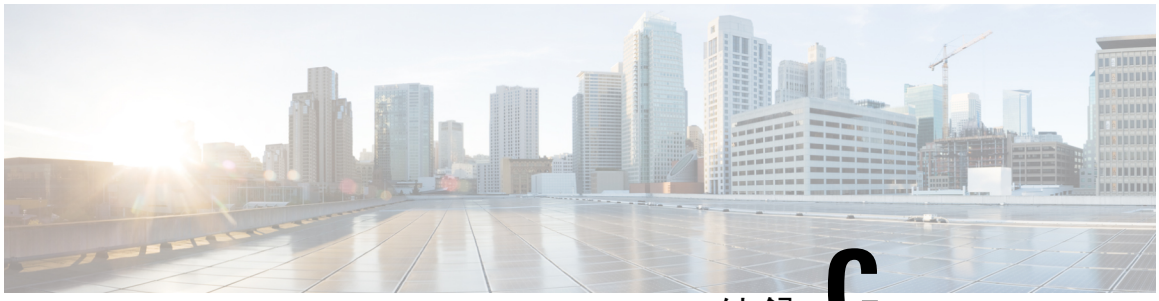
	同じネットワーク	異なるネットワーク
同じ物理インターフェイス	許可	許可
異なる物理インターフェイス	不可	許可

電子メールゲートウェイを接続するための戦略

電子メールゲートウェイを接続する際には、次の点に留意してください。

- 通常、管理トラフィック（CLI、Web インターフェイス、ログ配信）は、電子メール トラフィックよりもはるかに少量です。
- 2 つのイーサネットインターフェイスが同じネットワーク スイッチに接続されているが最終的にダウンストリームの別のホスト上の単一インターフェイスと通信するだけの場合、あるいはすべてのデータがすべてのポートにエコーされるネットワーク ハブにそれらが接続されている場合、2 つのインターフェイスを使用しても得られる利点はありません。
- 1000Base-T で動作しているインターフェイスでの SMTP カンバセーションは、100Base-T で動作している同じインターフェイスでのカンバセーションよりも少し高速ですが、速くなるのは理想的な条件下でのみです。
- 配信ネットワークのその他の部分にボトルネックがある場合、ネットワークへの接続を最適化しても意味がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続に使用するインターフェイスの数とそれらへのアドレス指定の方法は、基礎となるネットワークの複雑性によって決める必要があります。ご使用のネットワーク トポロジやデータのボリュームから判断して不要であれば、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワーク トポロジでの必要に応じて接続を増やすこともできます。



付録 C

メール ポリシーとコンテンツ フィルタの例

この付録の構成は、次のとおりです。

- 受信メール ポリシーの概要 （1585 ページ）

受信メール ポリシーの概要

この例では、次のタスクを示し、メール ポリシーの機能について説明します。

1. デフォルトの着信メールポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタおよびコンテンツ フィルタを編集します。
2. 販売部とエンジニアリング部の異なるユーザのセットに 2 つの新しいポリシーを追加して、それぞれに異なる電子メール セキュリティ設定を指定します。
3. [着信メール ポリシーの概要（Incoming Mail Overview policy）] テーブルで使用する 3 つの新しいコンテンツ フィルタを作成します。
4. ポリシーをもう一度編集して、コンテンツ フィルタをグループによってイネーブルまたはディセーブルにします。

この例では、受信者によって異なるメールポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタおよびコンテンツ フィルタの設定を管理できる、機能と柔軟性を示しています。この例では、メール ポリシーおよびコンテンツ フィルタのアクセス権限を持つ「ポリシー管理者」と呼ばれるカスタム ユーザー ロールを割り当てます。アンチスパム、アンチウイルス、アウトブレイク フィルタ、および委任管理の機能の詳細については、次の章を参照してください。

- スパムおよびグレイメールの管理 （461 ページ）
- アンチウイルス （439 ページ）
- アウトブレイク フィルタ （513 ページ）
- 管理タスクの分散 （1191 ページ）

メール ポリシーへのアクセス

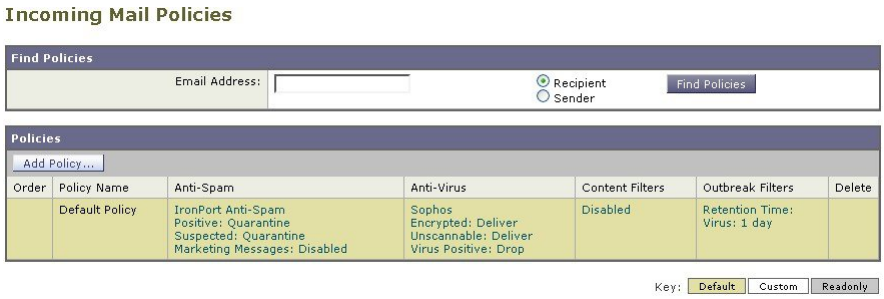
[メールポリシー（Mail Policies）] メニューを使用して、着信および発信メール ポリシーにアクセスできます。

新規システムでは、システムセットアップ ウィザードのすべての手順を完了して、Anti-Spam、Sophos または McAfee Anti-Virus およびアウトブレイク フィルタをイネーブルにするように選択した場合、以下の図のような [着信メールポリシー（Incoming Mail Policies）] ページが表示されます。

デフォルトでは、これらの設定は、デフォルトの着信メール ポリシーでイネーブルにされます。

- アンチスパム（ スパム隔離がイネーブルの場合）：イネーブル
  - 陽性と判定されたスパム：隔離、メッセージの件名が追加
  - 陽性と疑わしいスパム：隔離、メッセージの件名が追加
  - マーケティング電子メール：スキャンはイネーブルにされない
- アンチスパム（スパム隔離がイネーブルではない場合）：イネーブル
  - 陽性と判定されたスパム：配信、メッセージの件名が追加
  - 陽性と疑わしいスパム：配信、メッセージの件名が追加
  - マーケティング電子メール：スキャンはイネーブルにされない
- アンチウイルス：イネーブル、ウイルスのスキャンおよび修復、アンチウイルス スキャン結果が X-Header に追加
  - 修復されたメッセージ：配信、メッセージの件名が追加
  - 暗号化されたメッセージ：配信、メッセージの件名が追加
  - スキャンできないメッセージ：配信、メッセージの件名が追加
  - ウイルスに感染したメッセージ：ドロップ
- アウトブレイク フィルタ：イネーブル
  - ファイル拡張子は予測されない
  - 疑わしいウイルス添付ファイルのあるメッセージの保存期間は 1 日
  - メッセージの変更は有効ではない
- コンテンツ フィルタ：ディセーブル

図 *90 : [*着信メールポリシー（***Incoming Mail Policies***）*]* ページ：新規電子メールゲートウェイのデフォルト



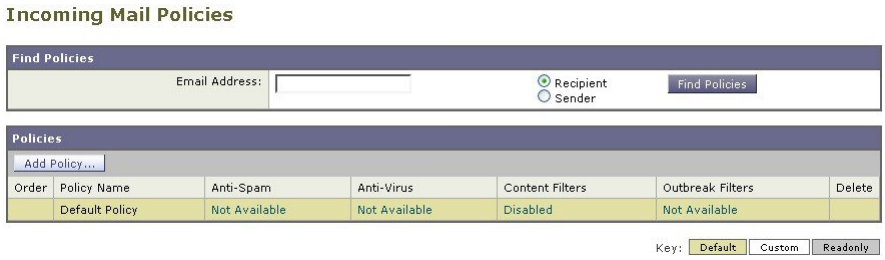
（注） この例では、着信メールポリシーは、スパム隔離がイネーブルにされている場合のデフォルトのアンチスパム設定を使用します。

[有効（Enabled）]、[無効（Disabled）]、[利用不可（Not Available）]

メールポリシーテーブル（着信または発信のいずれか）の列は、各ポリシー名のセキュリティサービスの状態のリンクを表示します。サービスがイネーブルの場合、[有効（Enabled）] という語またはコンフィギュレーションの要約が表示されます。同様に、サービスがディセーブルの場合、[無効（Disabled）] という語が表示されます。

サービスのライセンス契約書に同意していない場合、またはサービスの有効期限が切れている場合、リンクとして [利用不可（Not Available）] が表示されます。この場合、[利用不可（Not Available）] リンクをクリックすると、[セキュリティ サービス（Security Services）] タブ内に、サービスのポリシー単位の設定を指定できるページではなく、グローバルページが表示されます。ページが別のタブに変わったことを示す警告が表示されます。次の図を参照してください。

図 *91 :* 使用できないセキュリティ サービス



着信メッセージのデフォルトのアンチスパム ポリシーの設定

このメールポリシーテーブル内の各行は、異なるポリシーを表します。各列は、異なるセキュリティ サービスを表します。

- デフォルト ポリシーを編集するには、着信または発信メール ポリシー テーブルの下部の行にあるセキュリティ サービスの任意のリンクをクリックします。

メール ポリシーとコンテンツ フィルタの例

この例では、着信メールのデフォルト ポリシーのアンチスパム設定をより積極的に変更します。デフォルト値では、陽性と判定されたスパム メッセージおよび陽性と疑わしいスパム メッセージが隔離され、マーケティング電子メールのスキャンがディセーブルになります。次に、陽性と判定されたスパムがドロップされるように設定を変更する例を示します。陽性と疑わしいスパムは引き続き隔離されます。マーケティング電子メールのスキャンは、イネーブルにされ、マーケティング メッセージは目的の受信者に配信されます。マーケティング メッセージの件名には、テキスト [MARKETING] が前に追加されます。

手順

ステップ 1 アンチスパム セキュリティ サービスのリンクをクリックします。

（注） デフォルトのセキュリティ サービス設定の場合、このページの最初の設定では、ポリシーでサービスがイネーブルになるかどうかを定義します。[無効（Disable）] をクリックしてすべてのサービスをディセーブルにできます。

ステップ 2 [陽性と判定されたスパムの設定（Positively Identified Spam Settings）] セクションでは、[このメッセージに適用されるアクション（Action to apply to this message）] を [ドロップ（Drop）] に変更します。

ステップ 3 [マーケティングメールの設定（Marketing Email Settings）] セクションでは、[はい（Yes）] をクリックして、マーケティング電子メールのスキャンをイネーブルにします。

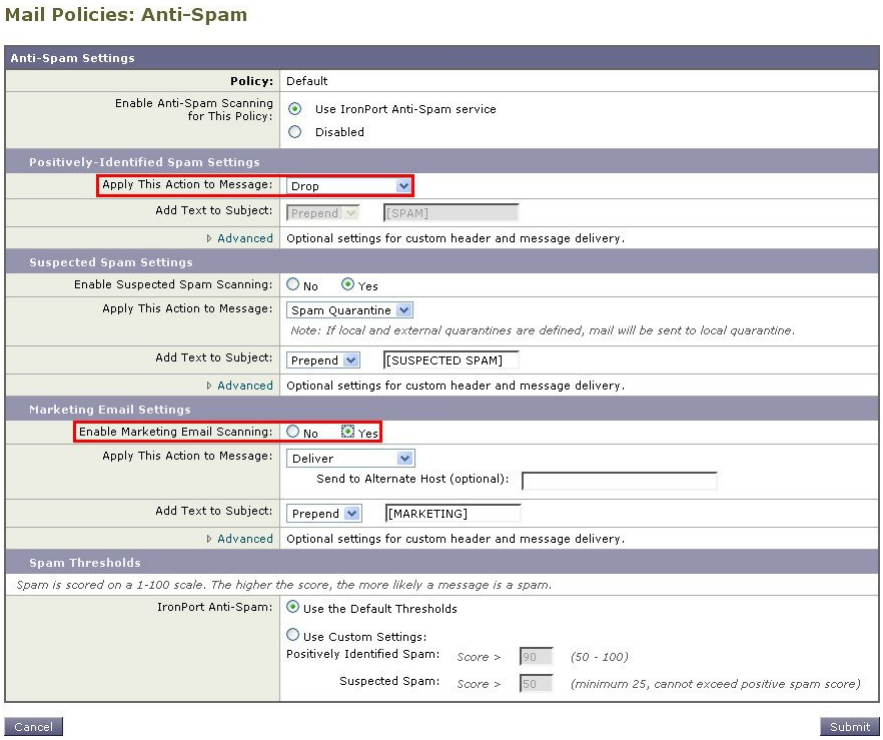
イネーブルにされている場合、デフォルト アクションでは、テキスト [MARKETING] が件名の前に追加され、問題のないマーケティング メッセージが配信されます。

[メッセージにテキストを追加（Add text to message）] フィールドでは、US-ASCII 文字だけを使用できます。

ステップ 4 [送信（Submit）] をクリックします。着信メール ポリシー テーブルのアンチスパム セキュリティ サービスの要約リンクが変更され、新しい値が反映されているため注意してください。

前述の手順と同様、デフォルト ポリシーのデフォルト アンチウイルスおよびウイルス アウトブレイク フィルタ設定を変更できます。

図 *92 : [*スパム対策設定（***Anti-Spam Settings***）*]* ページ



送信者および受信者のグループのメール ポリシーの作成

この例では、販売部（メンバーはLDAP受け入れクエリーにより定義されます）用とエンジニアリング部用の2つの新しいポリシーを作成します。ポリシーは両方とも、これらのポリシーの管理を担当するロールに属す委任管理者を作成するためにポリシー管理者カスタム ユーザ ロールに割り当てられます。次に、それぞれに異なる電子メールセキュリティ設定を設定します。

手順

ステップ 1 [ポリシーを追加（Add Policy）]ボタンをクリックして、新しいポリシーの作成を開始します。

ステップ 2 一意な名前を定義して、（必要な場合）ポリシーの順序を調整します。

ポリシーの名前は、定義されるメール ポリシー テーブル（着信または発信のいずれか）で一意でなければなりません。

各受信者は、適切なテーブル（着信または発信）の各ポリシーに対して上から順に評価されます。

メール ポリシーとコンテンツ フィルタの例

ステップ 3 [編集可能なユーザー（役割）（Editable By (Roles)）] リンクをクリックし、メール ポリシーの管理を担当する委任管理者にカスタム ユーザー ロールを選択します。

リンクをクリックすると、AsyncOS は、メール ポリシーの編集権限がある委任管理者のカスタム ロールを表示します。委任管理者は、ポリシーのアンチスパム、アンチウイルス、アウトブレイク フィルタの設定を編集し、ポリシーのコンテンツ フィルタを有効化または無効化できます。オペレータおよび管理者のみがメール ポリシーの名前または送信者、受信者、またはグループを変更できます。メール ポリシーへのフル アクセス権があるカスタム ユーザー ロールはメール ポリシーに自動的に割り当てられます。

委任管理の詳細については、管理タスクの分散 （1191 ページ）を参照してください。

ステップ 4 ポリシーのユーザを定義します。

ユーザが、送信者または受信者のいずれであるかを定義します（詳細については、ポリシー マッチングの例 （313 ページ）を参照してください）。以下の図では、着信メール ポリシーの受信者および発信メール ポリシーの送信者というデフォルト形式を示しています。

ポリシーのユーザは、次の方法で定義できます。

- 完全な電子メール アドレス：user@example.com
- 電子メール アドレスの一部：user@
- ドメインのすべてのユーザ：@example.com
- 部分ドメインのすべてのユーザ：@.example.com
- LDAP クエリーとのマッチング

（注） ユーザの入力は、AsyncOS の GUI および CLI の両方で、大文字と小文字が区別されます。たとえば、ユーザの受信者 Joe@ を入力すると、joe@example.com に送信されるメッセージが一致します。

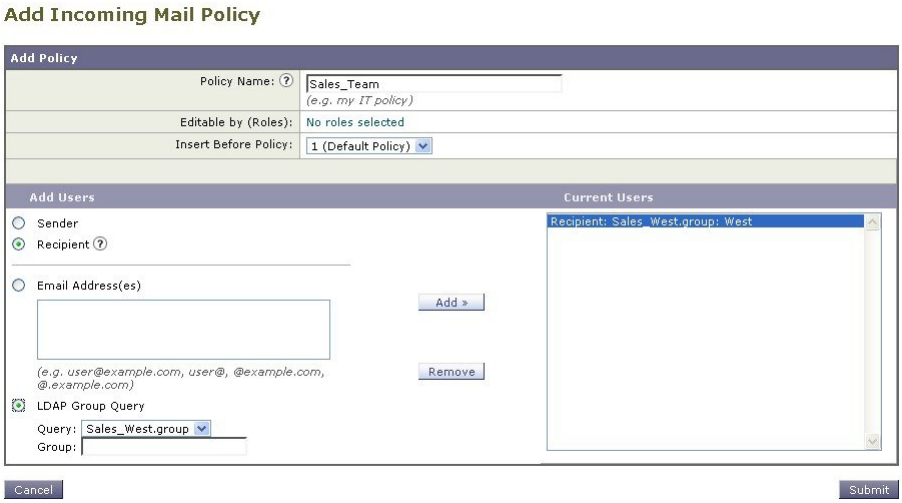
ユーザ情報を、たとえば Microsoft Active Directory、SunONE Directory Server（以前の「iPlanet Directory Server」）または Open LDAP ディレクトリなど、ネットワーク インフラストラクチャの LDAP ディレクトリ内に保存する場合、電子メールゲートウェイを設定して、LDAP サーバをクエリし、受信者アドレスの受け取り、代替アドレスまたはメールホスト、あるいはその両方へのメッセージのリルーティング、ヘッダーのマスカレード、メッセージに特定のグループの受信者または送信者があるかどうかの判別を行うことができます。

電子メールゲートウェイをこのように設定した場合、設定したクエリーを使用してメールポリシーのユーザを定義できます。

詳細については、LDAP クエリ （943 ページ）を参照してください。

メール ポリシーとコンテンツ フィルタの例

図 *93* : ポリシーのユーザの定義



ステップ 5 [追加（Add）]ボタンをクリックして、[現在のユーザ（Current Users）]リストにユーザを追加します。

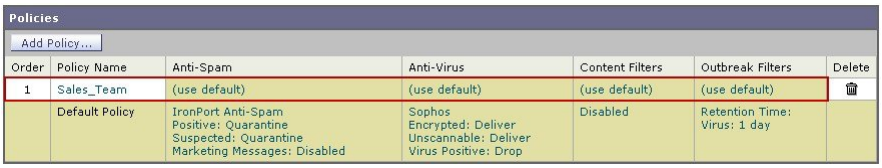
ポリシーには、送信者、受信者およびLDAPクエリーを組み合わせて含めることができます。

[削除（Remove）]ボタンを使用すると、定義されているユーザを現在のユーザのリストから削除できます。

ステップ 6 ユーザの追加が完了したら、[送信（Submit）] をクリックします。

ポリシーを最初に追加する場合、すべてのセキュリティ サービス設定では、デフォルト値が使用されるため注意してください。

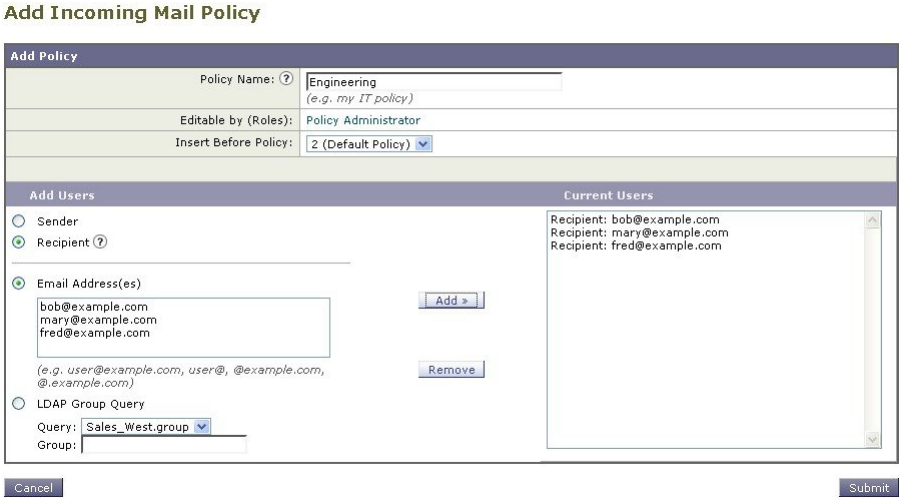
図 *94* : 新しく追加されたポリシー：販売グループ



ステップ 7 [ポリシーを追加（Add Policy）] ボタンをもう一度クリックして、別の新しいポリシーを追加します。

このポリシーでは、エンジニアリング チームのメンバーの各電子メール アドレスが定義されます。

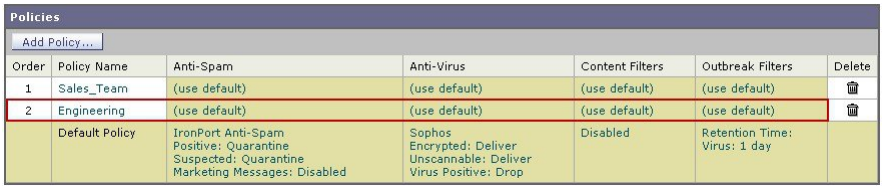
図 *95 :* エンジニアリング チームのポリシーの作成



ステップ 8 エンジニアリング ポリシーのユーザの追加が完了したら、[送信（Submit）] をクリックします。

ステップ 9 変更を保存します。

図 *96 :* 新しく追加されたポリシー：エンジニアリング チーム



（注） この時点では、新しく作成された両方のポリシーに、デフォルト ポリシーで使用される同じ設定が適用されています。いずれかのポリシーのユーザへのメッセージが一致しますが、メール処理設定は、デフォルト ポリシーと同じです。そのため、「Sales_Group」または「Engineering」ポリシーのユーザと一致するメッセージは、デフォルト ポリシーと同様に処理されます。

[デフォルト（Default）]、[カスタム（Custom）]、[無効（Disabled）]

テーブル下部のキーは、特定のポリシーのセルのカラー コーディングが、デフォルト行に定義されているポリシーとどのように関係するかを示しています。

- イエローのシェーディングは、ポリシーがデフォルト ポリシーと同じ設定を使用していることを示します。
- シェーディングなし（ホワイト）は、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。
- グレーのシェーディングは、セキュリティ サービスがポリシーでディセーブルにされていることを示します。

送信者および受信者のグループごとのメール ポリシーの作成

この例では、前述の項で作成した 2 つのポリシーを編集します。

- 販売グループでは、アンチスパム設定をデフォルト ポリシーよりも積極的になるように変更します（着信メッセージのデフォルトのアンチスパム ポリシーの設定（1587ページ）を参照。）陽性と識別されたスパム メッセージをドロップするデフォルト ポリシーが使用されます。ただし、この例では、スパム隔離エリアに送信されるように、マーケティング メッセージの設定を変更します。

  この積極的なポリシーでは、販売チームの受信トレイに送信される不要なメッセージが最小限に押さえられます。

  アンチスパム設定の詳細については、スパムおよびグレイメールの管理（461ページ）を参照してください。

- エンジニアリング チームでは、example.com へのリンクを除く疑わしいメッセージの URL を変更するために、アウトブレイク フィルタ機能の設定をカスタマイズします。拡張子「dwg」の添付ファイルは、アウトブレイク フィルタのスキャンをバイパスします。

  アウトブレイク フィルタの設定の詳細については、アウトブレイク フィルタ（513ページ）を参照してください。

  販売チーム ポリシーのアンチスパム設定を編集するには、次の手順を実行します。

手順

ステップ 1 販売ポリシー行のアンチスパム セキュリティ サービス（[スパム対策（Anti-Spam）]）列のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は[（デフォルトを使用）（use default）] です。

ステップ 2 アンチスパム セキュリティ サービス ページで、[このポリシーのスパム対策スキャンを有効にする（Enable Anti-Spam Scanning for this Policy）] の値を [デフォルト設定を使用（Use Default Settings）] から [スパム対策を使用（Use Cisco Anti-Spam）] に変更します。

[スパム対策サービスを使用（Use Cisco Anti-Spam service）] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

ステップ 3 [スパムと確定された場合の設定（Positively-Identified Spam Settings）] セクションで、[このアクションをメッセージに適用する（Apply This Action to Message）] を [ドロップ（Drop）] に変更します。

ステップ 4 [疑わしいスパムの設定（Suspected Spam Settings）] セクションで、[はい（Yes）] をクリックして、陽性と疑わしいスパムのスキャンをイネーブルにします。

ステップ 5 [疑わしいスパムの設定（Suspected Spam Settings）] セクションで、[このアクションをメッセージに適用する（Apply This Action to Message）] を [スパム隔離（Spam Quarantine）] に変更します。

（注） [スパム隔離（Spam Quarantine）] を選択すると、「スパム隔離」の章で定義されている設定に従って、メールが転送されます。

ステップ 6 [件名へテキストを追加（Add text to subject）] フィールドで、[なし（None）] をクリックします。

スパム隔離エリアに配信されるメッセージには、件名タギングが追加されません。

ステップ 7 [マーケティングメールの設定（Marketing Email Settings）] セクションで、[はい（Yes）] をクリックして、問題のない送信元からのマーケティング メールのスキャンをイネーブルにします。

ステップ 8 [このアクションをメッセージに適用する（Apply This Action to Message）] セクションで、[スパム隔離（Spam Quarantine）] を選択します。

ステップ 9 変更を送信し、保存します。

このシェーディングは、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。

この時点では、スパムの疑いがあり、その受信者が販売チーム ポリシーで定義されている LDAP クエリーと一致するメッセージは、IronPort スパム検疫エリアに配信されます。

送信者および受信者のグループごとのメール ポリシーの作成

エンジニアリング チーム ポリシーのアウトブレイク フィルタ設定を編集するには、次の手順を実行します。

手順

ステップ 1 エンジニアリング ポリシー行のアウトブレイク フィルタ機能セキュリティ サービス（[アウトブレイクフィルタ（Outbreak Filters）] カラム）のリンクをクリックします。

このポリシーは新しく追加されたポリシーであるため、リンクの名前は[（デフォルトを使用）（use default）] です。

ステップ 2 [アウトブレイク フィルタ機能セキュリティ サービス（Outbreak Filters feature security service）] ページで、ポリシーのスキャン設定を [アウトブレイクフィルタを有効にする（設定をカスタマイズ）（Enable Outbreak Filtering (Customize settings)）] に変更します。

[（設定をカスタマイズ）（(Customize settings)）] を選択すると、デフォルト ポリシーで定義されている設定が無効になります。

また、別の設定を選択できるようにページの残りの部分のコンテンツがイネーブルになります。

ステップ 3 ページの [添付ファイルのスキャンのバイパス（Bypass Attachment Scanning）] セクションで、ファイル拡張子フィールドに **dwg** と入力します。

メール ポリシーとコンテンツ フィルタの例

ファイル拡張子「dwg」は、電子メールゲートウェイが添付ファイルのスキャン時にフィンガープリントにより認識できる既知のファイルタイプのリストにはありません。

（注） 3 文字のファイル拡張子の前にピリオド（.）を入力する必要はありません。

ステップ 4 [拡張子を追加（Add Extension）] をクリックして、.dwg ファイルをアウトブレイク フィルタ機能スキャンをバイパスするファイル拡張子のリストに追加します。

ステップ 5 [メッセージの変更を有効にする（Enable Message Modification）] をクリックします。

メッセージの変更を有効にすると、電子メールゲートウェイはフィッシングおよび詐欺など脅威としてターゲットされるものや、疑わしいまたは不正な Web サイトへの URL がスキャンできるようになります。アプライアンスは、ユーザが Web サイトへアクセスしようとすると Cisco セキュリティプロキシを介してリダイレクトするように、メッセージ中のリンクを書き換えます。

（注） アウトブレイク フィルタが非ウイルス性の脅威をスキャンするために、メール ポリシーでアンチスパム スキャンをイネーブルにする必要があります。

ステップ 6 [未署名のメッセージに対して有効にする（Enable for Unsigned Messages）] を選択します。

その結果、電子メールゲートウェイは署名されたメッセージの URL を書き変えることができます。他のメッセージの変更および非ウイルス性の脅威が検出されたメッセージが解放されるまで隔離にとどまる時間が設定ができるように URL の書き換えをイネーブルにする必要があります。この例では、デフォルトの保存期間は 4 時間です。

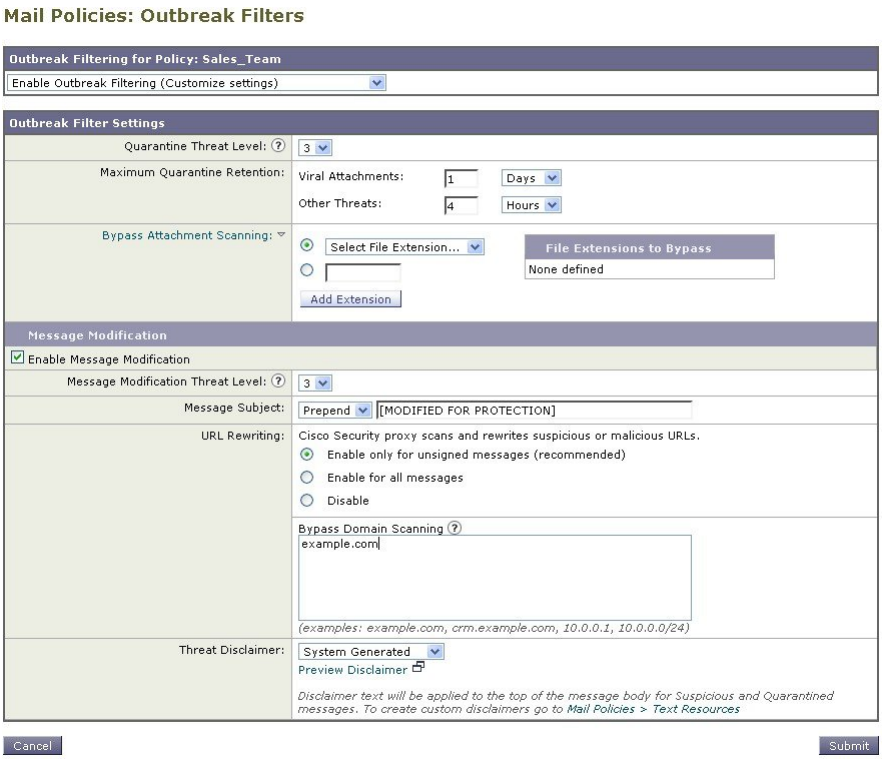
ステップ 7 [ドメインのスキャンをバイパス（Bypass Domain Scanning）] フィールドに example.com と入力します。

電子メールゲートウェイは example.com へのリンクを変更しません。

ステップ 8 [脅威に関する免責事項（Threat Disclaimer）] で [システムが生成（System Generated）] を選択します。

電子メールゲートウェイは、メッセージの内容についてユーザに警告するためにメッセージ本文の上に免責事項を挿入できます。次の例では、システムで生成された脅威に関する免責事項を使用しています。

図 *97:* アウトブレイク フィルタの設定



ステップ 9 変更を送信し、保存します。

このシェーディングは、ポリシーがデフォルト ポリシーとは異なる設定を使用していることを示します。

この時点では、ファイル拡張子が dwg である添付ファイルを含む任意のメッセージ、および受信者がエンジニアリング チーム ポリシーで定義されている受信者とマッチングする任意のメッセージは、アウトブレイク フィルタ スキャンをバイパスし、処理を続行します。example.com ドメインへのリンクを含むメッセージは、Cisco セキュリティ プロキシを介してリダイレクトするようにリンクを修正されることはなく、疑わしいと見なされません。

メール ポリシーでの送信者または受信者の検索

[ポリシー検索（Find Policies）] ボタンを使用して、[受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページで定義されているポリシーですでに定義されているユーザを検索します。

たとえば、joe@example.com と入力して、[ポリシー検索（Find Policies）] ボタンをクリックすると、ポリシーとマッチングする特定の定義済みユーザを含むポリシーを示す結果が表示されます。

ポリシーの名前をクリックして、[ポリシー設定を編集（Edit Policy）] ページに移動してそのポリシーのユーザを編集します。

ユーザを検索する場合、デフォルト ポリシーは常に表示されるため注意してください。これは、定義上、送信者または受信者が設定されているポリシーと一致しない場合、デフォルトのポリシーが必ず一致するためです。

管理例外

前述の2つの例で示されている手順を使用して、管理例外に基づいたポリシーの作成および設定を開始できます。つまり、組織のニーズを評価した後で、メッセージの大部分がデフォルトポリシーで処理されるように、ポリシーを設定できます。また、必要に応じて、異なるポリシーを管理して、特定のユーザまたはユーザ グループの追加「例外」ポリシーを作成できます。このようにすることで、メッセージ分裂が最小化され、ワーク キューの各分裂メッセージの処理により受けるシステム パフォーマンスの影響が少なくなります。

スパム、ウイルスおよびポリシー実行に対する組織またはユーザの許容値に基づいて、ポリシーを定義できます。次の表に、いくつかのポリシーの例の概要を示します。「積極的な」ポリシーでは、エンドユーザのメールボックスに到達するスパムおよびウイルスの量が最小限に抑えられます。「保守的な」ポリシーでは、偽陽性を回避し、ポリシーに関係なく、ユーザによるメッセージの見落としを防ぐことができます。

表 *165*：積極的および保守的なメール ポリシーの設定

	積極的な設定	保守的な設定
スパム対策	陽性と判定されたスパム：ドロップ 陽性と疑わしいスパム：隔離 マーケティング メール：メッセージの件名の前に「[Marketing]」が追加されて配信	陽性と判定されたスパム：隔離 陽性と疑わしいスパム：メッセージの件名の前に「[Suspected Spam]」が追加されて配信 マーケティング メール：ディセーブル
ウイルス対策	修復されたメッセージ：配信 暗号化されたメッセージ：ドロップ スキャンできないメッセージ：ドロップ 感染メッセージ：ドロップ	修復されたメッセージ：配信 暗号化されたメッセージ：隔離 スキャンできないメッセージ：隔離 感染メッセージ：ドロップ
ウイルス フィルタ	イネーブル、バイパスできる特定のファイル名拡張子またはドメインなし すべてのメッセージのメッセージ変更の有効化	バイパスできるファイル名拡張子またはドメインの有効化 未署名のメッセージのメッセージ変更の有効化

コンテンツに基づくメッセージのフィルタリング

この例では、[受信メールポリシー（Incoming Mail Policy）] テーブルで使用される新しいコンテンツ フィルタを 3 つ作成します。これらのコンテンツ フィルタは、ポリシー管理のカスタム ユーザー ロールに属す委任管理者が編集できます。次のフィルタを作成します。

1. 「scan_for_confidential」

   このフィルタは、文字列「confidential」が含まれているかメッセージをスキャンします。文字列が見つかると、メッセージのコピーが電子メール エイリアス hr@example.com に送信され、メッセージがポリシー隔離エリアに送信されます。

2. 「no_mp3s」

   このフィルタは、MP3 添付ファイルを削除し、MP3 ファイルが削除されたことを受信者に通知します。

3. 「ex_employee」

   このコンテンツ フィルタは、特定のエンベロープ受信者アドレス（元受信者）に送信されるメッセージをスキャンします。メッセージが一致した場合、特定の通知メッセージがメッセージ送信者に送信され、メッセージがバウンスされます。

コンテンツ フィルタを作成したら、各ポリシー（デフォルト ポリシーを含む）を設定して、異なる組み合わせで特定のコンテンツ フィルタをイネーブルにします。

件名に「Confidential」とあるメッセージの隔離

最初の例のコンテンツ フィルタには、1 つの条件と 2 つのアクションが含まれます。

手順

ステップ 1 [メールポリシー（Mail Policies）] タブをクリックします。

ステップ 2 [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。

ステップ 3 [フィルタを追加（Add Filter）] ボタンをクリックします。

ステップ 4 [名前（Name）] フィールドに、新しいフィルタの名前として scan_for_confidential と入力します。

フィルタ名には、ASCII 文字、数字、下線またはダッシュを含めることができます。コンテンツ フィルタ名の最初の文字は、文字または下線でなければなりません。

ステップ 5 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、[ポリシー管理者（Policy Administrator）] を選択し、[OK] をクリックします。

ポリシー管理者ユーザ ロールに属する委任管理者はこのコンテンツ フィルタを編集し、自身のメール ポリシーで使用できます。

ステップ 6 [説明（Description）] フィールドに、説明を入力します。たとえば、「scan all incoming mail for the string ‘confidential’」と入力します。

ステップ 7 [条件を追加（Add Condition）] をクリックします。

ステップ 8 [メッセージ本文（Message Body）] を選択します。

ステップ 9 [テキストを含む:（Contains text:）] フィールドに confidential と入力して、[OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filter）] ページに、追加される条件が表示されます。

ステップ 10 [アクションを追加（Add Action）] をクリックします。

ステップ 11 [コピーを送信(Bcc:)（Send Copy To (Bcc:)）] を選択します。

ステップ 12 [メールアドレス（Email Addresses）] フィールドに、hr@example.com と入力します。

ステップ 13 [件名（Subject）] フィールドに、[message matched confidential filter] と入力します。

ステップ 14 [OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filter）] ページに、追加されるアクションが表示されます。

ステップ 15 [アクションを追加（Add Action）] をクリックします。

ステップ 16 [隔離（Quarantine）] を選択します。

ステップ 17 ドロップダウン メニューで、[ポリシー隔離領域（Policy quarantine area）] を選択します。

ステップ 18 [OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filter）] ページに、追加される 2 番目のアクションが表示されます。

ステップ 19 変更を送信し、保存します。

この時点では、コンテンツフィルタは、いずれの着信メールポリシーでも有効になっていません。この例では、新しいコンテンツフィルタをプライマリリストに追加しただけの状態です。このコンテンツフィルタはいずれのポリシーにも適用されていないため、電子メールゲートウェイによる電子メール処理は、このフィルタの影響を受けません。

メッセージから MP3 添付ファイルを除去

2 番目の例のコンテンツ フィルタには、条件はなく、アクションは 1 つ含まれます。

手順

ステップ 1 [フィルタを追加（Add Filter）] ボタンをクリックします。

ステップ 2 [名前（Name）] フィールドに、新しいフィルタの名前として no_mp3s と入力します。

ステップ 3 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、[ポリシー管理者（Policy Administrator）] を選択し、[OK] をクリックします。

ステップ 4 [説明（Description）] フィールドに、説明を入力します。たとえば、strip all MP3 attachments と入力します。

ステップ 5 [アクションを追加（Add Action）] をクリックします。

ステップ 6 [ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] を選択します。

ステップ 7 [ファイルタイプが次の場合（File type is）] を選択します。

ステップ 8 ドロップダウン フィールドで、[-- mp3] を選択します。

ステップ 9 必要な場合、置換メッセージを入力します。

ステップ 10 [OK] をクリックします。

ステップ 11 変更を送信し、保存します。

（注） コンテンツ フィルタを作成するときに条件を指定する必要はありません。条件が定義されていない場合、定義されるアクションは常にルールに適用されます（条件を指定しないことは、true() メッセージ フィルタ ルールを使用すること同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます）。

元従業員に送られたバウンス メッセージ

3 番目の例のコンテンツ フィルタには、1 つの条件と 2 つのアクションを使用します。

手順

ステップ 1 [フィルタを追加（Add Filter）] ボタンをクリックします。

ステップ 2 [名前:（Name:）] フィールドに、新しいフィルタの名前として **ex_employee** と入力します。

ステップ 3 [編集可能なユーザ（役割）（Editable By (Roles)）] リンクをクリックし、[ポリシー管理者（Policy Administrator）] を選択し、[OK] をクリックします。

ステップ 4 [説明：（Description:）] フィールドに、説明を入力します。たとえば、**bounce messages intended for Doug** と入力します。

ステップ 5 [条件を追加（Add Condition）] をクリックします。

ステップ 6 [エンベロープ受信者（Envelope Recipient）] を選択します。

ステップ 7 エンベロープ受信者に対して、[次で始まる（Begins with）] を選択して、**doug@** と入力します。

ステップ 8 [OK] をクリックします。

[コンテンツフィルタ（Content Filters）] ページがリフレッシュされ、追加された条件が表示されます。元従業員の電子メール アドレスを含む LDAP ディレクトリを作成できます。元従業員がそのディレクトリに追加されると、このコンテンツ フィルタは、動的に更新されます。

ステップ 9 [アクションを追加（Add Action）] をクリックします。

ステップ 10 [通知（Notify）] を選択します。

ステップ 11 [送信者（Sender）] チェックボックスを選択して、[件名（Subject）] フィールドに、 message bounced for ex-employee of **example.com** と入力します。

ステップ 12 [テンプレート利用（Use template）] セクションで、通知テンプレートを選択します。

（注） リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、ユーザーインターフェイスに表示されません。たとえば、コンテンツ ディクショナリ、通知テンプレートおよびメッセージ免責事項は、[メールポリシー（Mail Policies）] > [ディクショナリ（Dictionaries）] ページ（または CLI の **dictionaryconfig** コマンド）から事前に設定されていない場合、オプションとして表示されません。ディクショナリの作成の詳細については、コンテンツディクショナリ （791 ページ）を参照してください。

ステップ 13 [OK] をクリックします。

[コンテンツフィルタの追加（Add Content Filters）] ページに、追加されるアクションが表示されます。

ステップ 14 [アクションを追加（Add Action）] をクリックします。

ステップ 15 [バウンスする（最終アクション）（Bounce (Final Action)）] を選択して、[OK] をクリックします。

コンテンツ フィルタに指定できる最終アクションは1つだけです。複数の最終アクションを追加しようとすると、GUI にエラーが表示されます。

このアクションを追加すると、この元従業員へのメッセージの送信者が、通知テンプレートとバウンス通知テンプレートの 2 つのメッセージを受け取る可能性があります。

ステップ 16 変更を送信し、保存します。

各受信者のグループごとのコンテンツ フィルタの適用

前述の例では、[受信メールポリシー（Incoming Mail Policy）] ページを使用して、3 つのコンテンツ フィルタを作成しました。[着信コンテンツフィルタ（Incoming Content Filters）] ページと [発信コンテンツフィルタ（Outgoing Content filters）] ページには、ポリシーに適用できるすべてのコンテンツフィルタの「プライマリリスト」が含まれています。

図 *98 : [*受信コンテンツフィルタ（*Incoming Content Filters***）*]* : 作成された *3* つのフィルタ**

この例では、[受信コンテンツフィルタ（Incoming Content Filters）] テーブルで使用される新しいコンテンツ フィルタを 3 つ適用します。

- デフォルト ポリシーには、3 つすべてのコンテンツ フィルタが適用されます。
- エンジニアリング グループには、no_mp3s フィルタは適用されません。
- 販売グループには、デフォルト着信メール ポリシーとしてコンテンツ フィルタが適用されます。

デフォルトでのすべての受信者のコンテンツ フィルタのイネーブル化

リンクをクリックして、個々のポリシーに対してコンテンツ フィルタをイネーブルにして選択します。

手順

ステップ 1 [受信メールポリシー（Incoming Mail Policies）] をクリックして、[受信メールポリシー（Incoming Mail Policy）] テーブルに戻ります。

ページがリフレッシュされ、デフォルト ポリシーおよび送信者および受信者のグループのメール ポリシーの作成（1589 ページ）で追加した 2 つのポリシーが表示されます。コンテンツ フィルタリングは、デフォルトでは、すべてのポリシーでディセーブルにされているため注意してください。

ステップ 2 デフォルト ポリシー行のコンテンツ フィルタ セキュリティ サービス（[コンテンツフィルタ（Content Filters）] 列）のリンクをクリックします。

ステップ 3 コンテンツ フィルタ セキュリティ サービス ページで、[コンテンツフィルタリング：デフォルトポリシー（Content Filtering for Default Policy）] の値を [コンテンツフィルタを無効にする（Disable Content Filters）] から [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更します。

プライマリリストで定義されているコンテンツフィルタ（[受信コンテンツフィルタ（Incoming Content Filters）] ページを使用してコンテンツ フィルタの概要（325 ページ）で作成されたフィルタ）が、このページに表示されます。値を [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更すると、各フィルタのチェックボックスがディセーブル（グレー表示）からイネーブルに変わります。

ステップ 4 各コンテンツ フィルタの [有効（Enable）] チェックボックスをオンにします。

ステップ 5 [送信（Submit）] をクリックします。

[受信メール ポリシー（Incoming Mail Policies）] ページのテーブルは、デフォルト ポリシーで有効化されているフィルタの名前を示します。

エンジニアリングの受信者への MP3 添付ファイルの許可

「エンジニアリング」ポリシーの「no_mp3s」コンテンツ フィルタをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 エンジニアリング チーム ポリシー行の [コンテンツフィルタセキュリティサービス（Content Filters security service）]（[コンテンツフィルタ（Content Filters）] 列）のリンクをクリックします。

ステップ 2 コンテンツ フィルタ セキュリティ サービス ページで、[ポリシーのコンテンツフィルタリング: エンジニアリング（Content Filtering for Policy: Engineering）] の値を [コンテンツフィルタを有効にする（デフォルトのメールポリシー設定を継承）（Enable Content Filtering (Inherit default policy settings)）] から [コンテンツフィルタを有効にする（設定をカスタマイズ）（Enable Content Filters (Customize settings)）] に変更します。

このポリシーはデフォルト値を使用していたため、値を [デフォルト設定を使用（Use Default Settings）] から [はい（Yes）] に変更すると、各フィルタのチェックボックスがディセーブル（グレー表示）からイネーブルに変わります。

ステップ 3 「no_mp3s」フィルタのチェックボックスの選択を解除します。

ステップ 4 [送信（Submit）] をクリックします。

[受信メールポリシー（Incoming Mail Policies）] ページのテーブルは、エンジニアリング ポリシーでイネーブルにされているフィルタの名前を示します。

ステップ 5 変更を保存します。

次のタスク

この時点では、エンジニアリング ポリシーのユーザ リストと一致する着信メッセージで MP3 添付ファイルは削除されません。ただし、他のすべての着信メッセージでは、MP3 添付ファイルが削除されます。

GUI でのコンテンツ フィルタの設定に関する注意事項

- コンテンツ フィルタを作成するときに条件を指定する必要はありません。アクションが定義されていない場合、定義されるアクションは常にルールに適用されます（アクションを指定しないことは、true() メッセージ フィルタ ルールを使用すること同じで、コンテンツ フィルタがポリシーに適用される場合、すべてのメッセージがマッチングされます）。
- カスタム ユーザー ロールをコンテンツ フィルタに割り当てていない場合、パブリックのコンテンツ フィルタになり、メール ポリシーの任意の委任管理者が使用できます。委任管理者とコンテンツ フィルタの詳細については、管理タスクの分散（1191 ページ）を参照してください。
- 管理者とオペレータは、コンテンツフィルタがカスタムユーザロールに割り当てられていない場合でも、電子メールゲートウェイのすべてのコンテンツフィルタを表示および編集できます。
- フィルタ ルールおよびアクションのテキストを入力する場合、正規表現照合において、次のメタ文字に特殊な意味があります。^ $ * + ? { [ ] \ | ( )

  正規表現を使用しない場合、「\」（バックスラッシュ）を使用して、これらの任意の文字をエスケープする必要があります。たとえば、「*Warning*」と入力します。

- コンテンツ フィルタに複数の条件を定義する場合、コンテンツ フィルタが一致したと見なされるために、定義されるアクションのすべて（論理 AND）、または定義されたいずれかのアクション（論理 OR）の適用が必要かどうかを定義できます。

メール ポリシーとコンテンツ フィルタの例

- 「benign」コンテンツ フィルタを作成して、メッセージ分裂およびコンテンツ フィルタをテストできます。たとえば、唯一のアクションが「配信」であるコンテンツ フィルタを作成できます。このコンテンツ フィルタは、メール処理に影響を与えませんが、このフィルタを使用して、メール ポリシー処理が、システムの他の要素（たとえば、メール ログ）に影響を与えているかテストできます。
- 逆に、着信コンテンツまたは発信コンテンツフィルタの「プライマリリスト」の概念を使用して、電子メールゲートウェイにより処理されるすべてのメールのメッセージ処理に即時に影響を与える、非常に優れた、広範囲に及ぶコンテンツフィルタを作成できます。このコンテンツ フィルタは次のように作成できます。
  - [受信コンテンツフィルタ（Incoming Content Filters）] または [送信コンテンツフィルタ（Outgoing Content filters）] ページを使用して、順序が 1 の新しいコンテンツ フィルタを作成します。
  - [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページを使用して、デフォルト ポリシーの新しいコンテンツ フィルタをイネーブルにします。
  - 残りすべてのポリシーでこのコンテンツ フィルタをイネーブルにします。
- コンテンツ フィルタで使用できる [Bcc:] および [隔離（Quarantine）] アクションは、作成する隔離エリアの保持設定に役に立ちます（詳細については、ポリシー、ウイルス、およびアウトブレイク隔離 （1129ページ）を参照してください）。メッセージがすぐにはシステムからリリースされないようにするため（つまり、隔離エリアの割り当てディスク領域がすぐにいっぱいにならないようにするため）、ポリシー隔離とのメールフローをシミュレートするフィルタを作成できます。
- scanconfig コマンドと同じ設定が使用されるため、「Entire Message」条件は、メッセージのヘッダーをスキャンしません。「Entire Message」を選択すると、メッセージ本文および添付ファイルだけがスキャンされます。特定のヘッダー情報を検索するには、「Subject」または「Header」条件を使用します。
- LDAP クエリによるユーザの設定は、電子メールゲートウェイで LDAP サーバが設定されている場合（つまり、ldapconfig コマンドを使用して特定の文字列を含む特定の LDAP サーバをクエリするように電子メールゲートウェイが設定されている場合）だけ GUI に表示されます。
- リソースが事前に定義されていないため、コンテンツ フィルタ ルール ビルダのいくつかのセクションは、GUI に表示されません。たとえば、通知テンプレートおよびメッセージ免責事項は、[テキストリソース（Text Resources）] ページまたは CLI の textconfig コマンドを使用して事前に設定されていない場合、オプションとして表示されません。
- コンテンツフィルタ機能は、次の文字エンコーディングのテキストを認識し、これらを追加およびスキャンできます。
  - Unicode（UTF-8）
  - Unicode（UTF-16）
  - Western European/Latin-1（ISO 8859-1）
  - Western European/Latin-1（Windows CP1252）
  - 中国語（繁体字）（Big 5）

メール ポリシーとコンテンツ フィルタの例

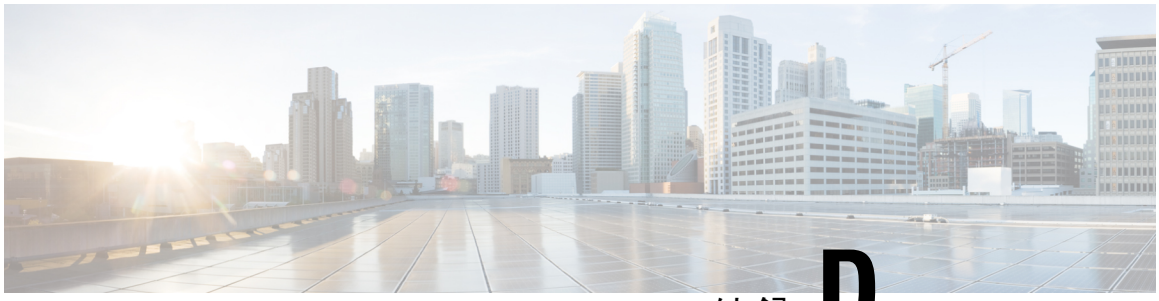
- 中国語（簡体字）（GB 2312）
- 中国語（簡体字）（HZ GB 2312）
- 韓国語（ISO 2022-KR）
- 韓国語（KS-C-5601/EUC-KR）
- 日本語（Shift-JIS（X0123））
- 日本語（ISO-2022-JP）
- 日本語（EUC）

複数の文字セットを1つのコンテンツ フィルタ内で組み合わせてマッチングできます。複数の文字エンコーディングでのテキストの表示および入力については、Webブラウザのマニュアルを参照してください。ほとんどのブラウザでは、複数の文字セットを同時にレンダリングできます。

図 *99*：コンテンツ フィルタでの複数の文字セット

- 着信または発信コンテンツ フィルタの要約ページで、[説明（Description）]、[ルール（Rules）] および [ポリシー（Policies）] のリンクを使用して、コンテンツ フィルタに提供されているビューを変更します。
  - [説明（Description）] ビューには、各コンテンツ フィルタの説明フィールドに入力したテキストが表示されます（これはデフォルト ビューです）。
  - [ルール（Rules）] ビューには、ルール ビルダ ページにより構築されたルールおよび正規表現が表示されます。
  - [ポリシー（Policies）] ビューには、イネーブルにされている各コンテンツ フィルタのポリシーが表示されます。

メール ポリシーとコンテンツ フィルタの例



付録 D

ファイアウォール情報

この章は、次の項で構成されています。

- ファイアウォール情報 （1607 ページ）
- ネットワーク攻撃からの電子メールゲートウェイの保護 （1613 ページ）

ファイアウォール情報

次の表に示すポートは、 Cisco Secure Email Gateway を正常に動作させるために開く必要がある場合があります（デフォルト値を示す）。

表 *166 :* ファイアウォール ポート

デフォルト ポート	プロトコル	入力/出力	ホストネーム	目的
20/21	TCP	入力または出力	AsyncOS IP、FTP サーバ	ログ ファイルのアグリゲーション用 FTP。 データ ポート TCP 1024 以上はすべて開いている必要があります。 詳細については、ナレッジベースの FTP ポート情報を検索してください。ナレッジ ベース （8 ページ）を参照してください。
22	TCP	入力	AsyncOS IP	CLI への SSH アクセス、ログ ファイルのアグリゲーション。
22	TCP	発信	SSH サーバ	ログ ファイルの SSH アグリゲーション。

ファイアウォール情報

22	TCP	発信	SCP サーバ	ログ サーバへの SCP 配信。
25	TCP	発信	任意（Any）	電子メール送信用 SMTP。
25	TCP	入力	AsyncOS IP	バウンスされた電子メールを受信する SMTP または外部のファイアウォールから電子メールをインジェクトする場合。
53	UDP/TCP	発信	DNS サーバ	インターネット ルート サーバまたはファイアウォール外部の DNS サーバを使用するように設定されている場合の DNS。また、SenderBase クエリの場合。
80	HTTP	入力	AsyncOS IP	システム モニタリングのための GUI への HTTP アクセス。
80	HTTP	発信	downloads.ironport.com	McAfee 定義を除くサービス更新。
80	HTTP	発信	updates.ironport.com	AsyncOS アップグレードおよび McAfee の定義。
80	HTTP	発信	TAXII サーバ	E メールゲートウェイで外部脅威フィードを使用できるようにします。
82	HTTP	入力	AsyncOS IP	スパム隔離の表示に使用されます。
83	HTTPS	入力	AsyncOS IP	スパム隔離の表示に使用されます。
110	TCP	発信	POP サーバ	スパム隔離のためのエンドユーザの POP 認証。
123	UDP	入力および出力	NTP サーバ	タイム サーバがファイアウォールの外側にある場合の NTP。
143	TCP	発信	IMAP サーバ	スパム隔離のためのエンドユーザの IMAP 認証。
161	UDP	入力	AsyncOS IP	SNMP クエリ。

162	UDP	発信	管理ステーション	SNMP トラップ。
389 または 3268	LDAP	発信	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォールの外側にある場合の LDAP。Cisco スパム隔離のための LDAP 認証。
636 または 3269	LDAPS	発信	LDAPS	LDAPS — ActiveDirectory のグローバル カタログ サーバ（SSL 使用）
443	TCP	入力	AsyncOS IP	システム モニタリングのための GUI への Secure HTTP（https）アクセス。
443	TCP	発信	res.cisco.com	アップデート サーバの最新のファイルを確認します。
443	TCP	発信	update-manifests.ironport.com	アップデートサーバから最新のファイルのリストを取得します（物理ハードウェア E メール ゲートウェイの場合）。
443	TCP	発信	update-manifests.sco.cisco.com	アップデートサーバから最新のファイルのリストを取得します（仮想 E メール ゲートウェイの場合）。
443	TCP	発信	serviceconfig.talos.cisco.com grpc.talos.cisco.com ~~email-sender-ip-rep-grpc.talos.cisco.com~~ IP ベースのファイア ウォールの場合： 146.112.62.0/24 146.112.63.0/24 146.112.255.0/24 146.112.59.0/24 2a04:e4c7:ffff::/48 2a04: e4c7: fffe::/48	Cisco Talos インテリジェンス サービス：IP の評価、URL の評価およびカテゴリの取得とサービスログの詳細の送信を行います。

ファイアウォール情報

443	TCP	発信	kinesis.us-west-2.amazonaws.com sensor-provisioner.ep.prod .agari.com houston.sensor.prod.agari.com	Cisco Advanced Phishing Protection クラウドサービスに登録し、ヘッダーの詳細を送信します。
443	TCP	発信	[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] の [ファイル レピュテーションの詳細設定（Advanced Settings for File Reputation）] セクションの [クラウドサーバプール（Cloud Server Pool）] で設定されているとおりです。	設定されている場合、これはファイル レピュテーションを取得するためにクラウド サービスにアクセスするためのポートです。デフォルト ポートは 32137 です。ファイル分析サービスの場合はポート 443 を参照してください。
443	TCP	発信	[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] の [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクションで設定されているとおりです。	ファイル分析のためのクラウド サービスへのアクセス。ファイル レピュテーション サービスの場合は、ポート 443 または 32137 を参照してください。

443	TCP	入力および出力	[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] の [ファイル レピュテーションの詳細設定（Advanced Settings for File Reputation）] セクションの AMP for Endpoints コンソールの統合のパラメータで設定されているとおりです。 api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com api.amp.cisco.com api.eu.amp.cisco.com api.apjc.amp.cisco.com	AMP for Endpoints コンソール サーバにアクセスします。
443	TCP	入力および出力	outlook.office365.com login.microsoftonline.com。	メールボックス自動修復のために Office 365 サービスにアクセスします。
443	TCP	入力および出力	オンプレミス Microsoft Exchange Server のホスト名	メールボックスのメッセージを修復するには、オンプレミス Microsoft Exchange Server にアクセスします。
443	TCP	発信	aggregator.cisco.com	Cisco Aggregator サーバにアクセスします。
443	HTTPS	発信	logapi.ces.cisco.com	シスコ TAC によって収集されたデバッグ ログをアップロードするため。
443	HTTPS	発信	TAXII サーバ	E メールゲートウェイで外部脅威フィードを使用できるようにします。
443	HTTPS	入力および出力	api sse.cisco.com	Cisco SecureX または Cisco Threat Response に E メールゲートウェイを登録するために使用します。

ファイアウォール情報

443	HTTPS	入力および出力	api.eu.sse.itd.cisco.com	Cisco SecureX または Cisco Threat Response に E メールゲートウェイを登録するために使用します。
443	HTTPS	入力および出力	api.apj.sse.itd.cisco.com	Cisco SecureX または Cisco Threat Response に E メールゲートウェイを登録するために使用します。
443	HTTPS	入力および出力	est.sco.cisco.com	証明書をダウンロードする場合に使用し、Cisco SecureX または Cisco Threat Response に登録するときに検証済みのサイトに E メールゲートウェイがアクセスしているかどうかを確認します。
443	HTTPS	入力および出力	AsyncOS IP	`trailblazerconfig` CLI コマンドを使用した、GUI への HTTPS アクセス。
514	UDP/TCP	発信	Syslog サーバ	Syslog ロギング。
628	TCP	入力および入力	AsyncOS IP	外部ファイアウォールから電子メールをインジェクトする場合の QMQP。
990	TCP/FTP	発信	support-ftp.cisco.com	シスコ TAC によって収集されたデバッグ ログをアップロードするため。
1024 以降	—	—	—	ポート 21（FTP）に関する上記の情報を参照してください。
2222	CCS	入力および入力	AsyncOS IP	クラスタ通信サービス（中央集中管理用）。
	TCP	発信	AsyncOS IP	Cisco スパム隔離.
7025	TCP	入力および出力	AsyncOS IP	この機能が一元化されている場合、Cisco Secure Email Gateway と Cisco Secure Manager Email and Web Gateway 間でポリシー、ウイルス、およびアウトブレイク隔離データを渡します。

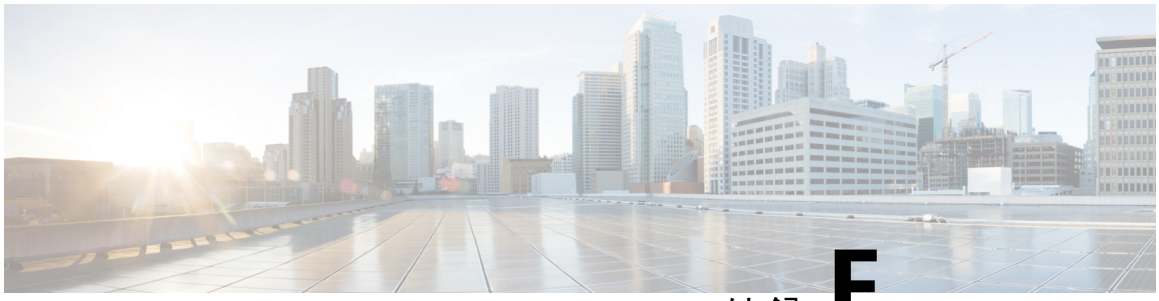
6080	HTTP	入力または出力	AsyncOS IP	HTTP サーバの API ポートへのアクセス
6443	HTTPS	入力または出力	AsyncOS IP	HTTPS サーバの API ポートへのアクセス

ネットワーク攻撃からの電子メールゲートウェイの保護

電子メールゲートウェイをネットワーク攻撃から保護するには、次の前提条件を満たす必要があります。

- ポート 22（SSH）を電子メールゲートウェイの外部 IP アドレスに公開しないこと。
- Web インターフェイスと CLI 構成設定を使用して電子メールゲートウェイを管理する際、特定の IP アドレスのみを有効にすること。
- （必要な場合）`adminaccessconfig` CLI コマンドを使用して Host ヘッダー対策機能を有効にすること。
- `adminaccessconfig` CLI コマンドを使用して、クロスサイトスクリプティング対策機能を有効にすること。
- パブリックリスナーにリレールールを設定しないこと。

（注） 外部リスナーでリレールールが必要な場合は、通常のパブリックリスナーで「SMTP AUTH」を設定します。



付録 E

エンド ユーザー ライセンス契約書

この付録の構成は、次のとおりです。

- Cisco Systems エンド ユーザー ライセンス契約書 （1615 ページ）
- Cisco コンテンツ セキュリティ ソフトウェア用エンドユーザー ライセンス契約補則 （1622 ページ）

Cisco Systems エンド ユーザー ライセンス契約書

重要：本エンド ユーザー ライセンス契約書をよくお読みください。お客様がシスコのソフトウェアまたは機器を認定販売元から購入したかどうか、また、お客様ご自身またはお客様が代表する法人（総称して「お客様」）がこのシスコ エンド ユーザー ライセンス契約におけるエンド ユーザーとして登録済みかどうかを確認することは、非常に重要です。エンド ユーザーとして登録されていないお客様は本ソフトウェアを使用するライセンスを有しておらず、このエンド ユーザー ライセンス契約の限定保証は適用されません。お客様が認定販売元から購入されたことを前提として、シスコのソフトウェア、またはシスコが提供するソフトウェアをダウンロード、インストールまたは使用することにより、お客様はこの契約に同意したものと見なされます。

Cisco Systems, Inc. Cisco Systems, Inc.、または同社に代わり本ソフトウェアのライセンスを許諾する同社の関連会社（以下、「シスコ」）は、お客様が本ソフトウェアを認定販売元から購入し、かつ本エンド ユーザー ライセンス契約書に含まれるすべての条件、および本製品に添付され、お客様の発注時に入手可能になる補遺ライセンス契約書に記載の、ライセンスに関する一切の追加制限条件（以下総称して「本契約」）に同意する場合に限り、お客様に対し本ソフトウェアのライセンスを許諾します。本エンド ユーザー ライセンス契約書内の各規定と補遺ライセンス契約書内の各規定が相反する場合、補遺ライセンス契約書内の各規定が優先します。本ソフトウェアをダウンロード、インストールまたは使用することにより、お客様は本ソフトウェアをご自身が認定販売元から購入したことを表明したこととなり、お客様に本契約の拘束力が及びます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、（A）お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、（B）お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および代金払い戻しの

エンド ユーザー ライセンス契約書

有効期限は、認定販売元から本ソフトウェアを購入後 30 日間であり、お客様が最初の登録済みエンド ユーザ購入者である場合にのみ適用されます。本エンド ユーザー ライセンス契約において、「認定販売元」とは、（A）シスコ、（B）対象地域内でエンド ユーザーにシスコの機器、ソフトウェアおよびサービスを配布および/もしくは販売することについてシスコより認定を受けたディストリビュータもしくはシステムインテグレータ、または（C）シスコの機器、ソフトウェアおよびサービスをお客様の地域内でエンド ユーザーに配布および/もしくは販売することについて、ディストリビュータとシスコとの契約の条件に従い、ディストリビュータもしくはシステム インテグレータにより認定された再販業者を意味します。

本契約の以下の条件は、本ソフトウェア（後に定義）のお客様による使用に適用されます。ただし、（*a*）本ソフトウェアのお客様による使用に適用される、お客様とシスコとの間の別段の署名済み契約が存在する場合、または（*b*）本ソフトウェアに、導入もしくはダウンロードの手続きの一部として、本ソフトウェアのお客様による使用に適用される別段の「クリック同意」ライセンス契約もしくは第三者ライセンス契約が含まれている場合は、この限りではありません。上記各契約書内の各規定が矛盾する場合、その優先順位は、以下のとおりです。（*1*）署名済の契約、（*2*）クリック同意契約または第三者のライセンス契約、（*3*）本契約。本契約において、「本ソフトウェア」とは、認定販売元からお客様に提供されるシスコ機器に組み込まれたファームウェアおよびコンピュータ プログラムを含むコンピュータ プログラム、ならびに一切のアップグレード、更新、バグ修正またはこれらの修正バージョン（総称して「アップグレード」）であって、*Cisco Software Transfer and Re-licensing Policy*（随時シスコによりなされる修正を含む）に基づいて再許諾されたもの、またはこれらのいずれかのバックアップ コピーを意味します。

本件ライセンス。本契約の各契約条件に従うことを条件として、シスコはお客様に対し、お客様が必要なライセンス料を認定販売元に支払った本ソフトウェアおよび本文書を社内業務目的で使用するための、非排他的かつ譲渡不能なライセンスを付与します。「本文書」とは、本ソフトウェアに関する情報を文書化したもの（当該情報がユーザ マニュアル、技術マニュアル、研修資料、仕様書その他のいずれに含まれているか否かは問わない）であって、認定販売元が何らかの形式（CD-ROMやオンラインを含む）により本ソフトウェアとともに提供するものを意味します。本ソフトウェアを使用するには、登録番号または製品認証キーを入力し、シスコの Web サイトにてお手持ちの本ソフトウェアをオンライン登録した上で、必要なライセンス キーまたはライセンス ファイルを入手する必要があります。

お客様が本ソフトウェアを使用するためのライセンスは、単一のハードウェア シャーシもしくはカード、または該当する補遺ライセンス契約書、もしくは認定販売元が同意済みで、お客様が必要なライセンス料を認定販売元に支払済みの該当する発注書（以下、「本発注書」）に記載されているその他の制限に限定され、お客様はこの制限を超えて本ソフトウェアを使用してはなりません。

本文書または該当する補遺ライセンス契約書に別途明記されていない限り、お客様は、以下のいずれかのみを目的として本ソフトウェアを使用する必要があります。お客様が所有または賃借しており、お客様の社内業務目的に使用されるシスコ機器に本ソフトウェアを組み込んで使用すること。当該シスコ機器上で本ソフトウェアを実行すること。（対応する本文書が、シスコ以外の機器に本ソフトウェアをインストールすることを許可している場合に）当該シスコ機器と通信すること。お客様には上記以外のいかなるライセンス（黙示のライセンス、禁反言の法理が適用されるライセンス、またはその他のライセンス）も付与されません。

エンド ユーザー ライセンス契約書

シスコがライセンス料を徴収しない評価版またはベータ版については、上記のライセンス料の支払い要件は適用されません。

一般的な各種制限。本契約は、ソフトウェアおよび資料の使用許諾であり、所有権を譲渡するものではありません。すべてのソフトウェアおよび資料の所有権はシスコが保有しています。お客様は、本件ソフトウェアおよび本件文書に、シスコまたはそのサプライヤもしくはライセンサの営業秘密が含まれていることを認識しているものとします。この営業秘密には、各プログラムの固有の内部設計および構造ならびに関連インターフェイス情報が含まれますが、これらのみには限定されません。本契約に明示的に別段の規定がない限り、お客様は、お客様が認定販売元から購入したシスコ機器の使用に関連する場合にのみ本ソフトウェアを使用するものとし、以下のいずれについてもこれを行う権利を有しておらず、またこれを行わないことについて特に同意するものとします。

（i）他の個人もしくは法人に、ライセンス権を移転もしくは譲渡するか、本ライセンスのサブライセンスを付与すること（その時点で有効な、シスコのライセンスの再許諾および移転に関するポリシーに従って行う場合は除きます）、または、お客様が認定販売元から購入したものではないシスコ機器もしくは中古のシスコ機器上で本ソフトウェアを使用すること。なお、お客様は、計画された移転、譲渡、サブライセンスの付与または使用はいずれも無効となることを了解するものとします。

（ii）以下のいずれかを行うこと。（a）本件ソフトウェアのエラーを修正するか、本件ソフトウェアを変更または改変すること、（b）本件ソフトウェアをもとに派生物を作成するか、第三者による当該行為を許可すること。

（iii）本ソフトウェアを対象とするリバースエンジニアリング、逆コンパイル、復号化、逆アセンブルを行うか、その他の方法で本ソフトウェアを人間の可読形式に変換すること。なお、本制限事項にかかわらず、適用法に基づいて明示的に許可されている場合、または適用されるオープン ソース ライセンスに基づいて当該特定の行為を許容すべきことがシスコに義務づけられている場合は除きます。

（iv）本ソフトウェアで実行したベンチマーク テストの結果を公表すること。

（v）シスコの書面による許可なく、サービス ビューロ、タイム シェアリング、またはその他の方法により、第三者へのサービス提供を目的として本ソフトウェアを使用、または使用を許可すること。

（vi）シスコの書面による事前の同意なしに、本ソフトウェアおよび本文書に含まれる企業秘密を第三者に対して開示、提供、またはその他の何らかの方法により公開すること。お客様は、かかる営業秘密を保護するため、相当のセキュリティ対策を講じる必要があります。

シスコは、準拠法により求められている範囲内で、お客様からの書面による依頼に応じて、本ソフトウェアと独自に開発された他のプログラムとの互換性を実現するために必要なインターフェイス情報を、シスコが妥当とみなす料金が支払われた場合にお客様に提供するものとします。お客様は、上記情報について厳格な秘密保持義務を遵守すると共に、その提供条件としてシスコが提示した準拠規定に従って上記情報を使用する必要があります。

本件ソフトウェア、本件アップグレード版、および追加コピー版。本契約のその他の規定にかかわらず、以下の条件が適用されます。（1）お客様は、追加コピー版またはアップグレード版の作成または取得時に、オリジナルのソフトウェアの有効なライセンスを保有しており、アップグレードまたは追加コピー版の適用料金を認定販売元に支払っている場合を除き、かか

エンド ユーザー ライセンス契約書

る追加コピー版またはアップグレード版を作成または使用するライセンスまたは権利を有しません。（2）アップグレードの使用は、お客様が最初のエンド ユーザ購入者または賃借者であるか、またはアップグレードされるソフトウェアを使用するための有効なライセンスを保持しており、かつ認定販売元から供給されたシスコ機器に限定されます。（3）追加の複製物の作成および使用は、必要なバックアップ用途のみに限定されます。

所有権表示。お客様は、いかなる形式であれ、本ソフトウェアのすべての複製物について、あらゆる著作権、財産権およびその他の表示を、それらの著作権およびその他の所有権の表示が本ソフトウェアに含まれているのと同じ形式かつ方法で保持し、複製することに同意します。本契約に基づき明示的に許可される場合でなければ、お客様は、シスコから書面による事前の許可を得ることなく本件ソフトウェアのコピー版または複製物を作成してはなりません。

契約の期間および終了。本契約および本契約において供与されるライセンスは、終了時まで有効に存続します。お客様は、本件ソフトウェアおよび本件文書のすべてのコピーを破棄することにより、随時、本契約および本件ライセンスを終了させることができます。お客様が本契約のいずれかの規定に従わなかった場合、本契約に基づくお客様の権利は、シスコからの通知なしにただちに終了します。お客様は、上記終了時に、保有または管理している本件ソフトウェアおよび本件文書のすべてのコピーを破棄する必要があります。お客様のあらゆる守秘義務、「一般的な制限」と題する条項に基づいてお客様に課されたあらゆる制約および制限、あらゆる責任制限、および保証の否認と制限はすべて、本契約終了後も存続するものとします。また「米国政府がエンドユーザー購入者の場合」および「限定保証表明およびエンド ユーザー ライセンス契約書に適用される一般規定」と題された各条項の各規定の効力は、本契約の終了後も存続します。

お客様の記録の検査。お客様は、シスコとその独立会計士に対して、お客様の通常の営業時間中にお客様の帳簿、記録、財務諸表を査察し、本契約の条項に従っていることを確認する権利を認めるものとします。上記監査の結果、本契約に反する行為が発覚した場合、お客様は、相当のライセンス料に上記監査の実施に伴う相当の費用を加えた額を、速やかにシスコへ支払う必要があります。

輸出、再輸出、移転、および使用に関する規制。本契約に基づいてシスコによって供給されるソフトウェア、本文書、および技術、またはそれらの直接的な製品（「本製品および技術」）は、アメリカ合衆国（「米国」）の法令およびその他関連国の法令に基づく輸出規制の対象となっています。お客様は、シスコの本件ソフトウェアと付帯技術の輸出、再輸出、移転、および使用に適用される各種法規に従う必要があると共に、必要となる米国および現地の各種許可、認可、または許諾をすべて取得するものとします。シスコとお客様の各々は、上記許認可または許諾の取得に関連して相手方当事者から相当の根拠に基づき請求を受けたその他の情報、裏付け文書、および各種支援を提供することに同意しているものとします。コンプライアンス、輸出、再輸出、移転、および使用についての法律に関する情報は、以下の URL に掲載されています。

https://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html

米国政府機関がエンドユーザ購入者である場合。本ソフトウェアおよび資料は、連邦調達規則（FAR）（以下「FAR」） (48 C.F.R.) 2.101 で定義される「商用品目」に分類されます。これは、「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」で構成されます（当該用語は FAR 12.212 で使用されています）。FAR 12.212 および DoD FAR 補則227.7202-1 から 227.7202-4 で定められているとおり、また、他の FAR 条項、または本契

エンド ユーザー ライセンス契約書

約の組み込み先である契約書内のこれと矛盾する他の契約条項にかかわらず、お客様は、連邦政府機関エンドユーザに対して、本ソフトウェアおよび本文書とともに本契約に定める権利のみを提供することができ、または、本契約が直接契約である場合は、連邦政府機関エンドユーザは、本ソフトウェアおよび本文書とともに本契約に定める権利のみを取得します。ソフトウェアと資料のいずれか、または両方を使用することにより、政府機関は、本ソフトウェアと資料が「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」であることに同意し、この契約書に規定されている権利および制限に同意したことになります。

指定コンポーネントおよび追加条件。本件ソフトウェアは、本書に規定されたものとは異なるライセンス契約条件、保証の否認、制限付き保証又は他の条件（総称して「追加条件」）が適用される、第三者のコンポーネントを含んでいる可能性のある単一又は複数のコンポーネントであって、本件文書、readme.txt ファイル、第三者のクリック同意又はその他（https://www.cisco.com/ 上など）においてシスコにより指定されたもの（「指定コンポーネント」）を含むこと、又は指定コンポーネントと共に提供されることがあります。お客様は、かかる指定コンポーネントについて該当する追加条件に同意するものとします。

限定保証

本契約に規定の各種制限および条件を前提として、シスコは、お客様への出荷日（シスコ以外の認定販売元による再販の場合、シスコの初回出荷より 90 日以内の日）を始期として、（a）90 日間、または（b）本ソフトウェアを組み込んでいる製品（以下、「本製品」）に添付される保証カード（存在する場合）に明記されている、本ソフトウェアに固有の保証期間（設定されている場合）、のいずれか長い方の期間内で、（a）通常の使用において、本ソフトウェアの提供媒体に材質上および製造上の欠陥がないこと、ならびに（b）本ソフトウェアが本文書に実質的に適合していること、を保証します。シスコによる本件製品の出荷日は、本件製品の出荷に用いられる梱包材に記載されています。上記を除き、本ソフトウェアは「現状のまま」で提供されます。この限定保証は、最初の登録済みエンドユーザたるお客様が認定販売元から購入した本ソフトウェアに対してのみ適用されます。この限定保証のもとでは、お客様の唯一の救済、かつシスコおよびそのサプライヤの全責任は、（i）欠陥のある媒体の交換、および/または（ii）シスコの選択により、本ソフトウェアの修理、交換、もしくは代金の返金に限定されます。いずれの場合も、この限定保証に反するようなエラーまたは欠陥が、保証期間内に、お客様に本ソフトウェアを提供した認定販売元に報告されることを条件とします。シスコ、またはお客様に本ソフトウェアを提供した認定販売元は、救済の条件として、自らの判断で、本ソフトウェアおよび/または本文書の返却を請求できます。シスコはいかなる場合でも以下の 2 点について保証しません。（i）本件ソフトウェアにエラーが生じないこと、（ii）お客様が、問題または障害なく本件ソフトウェアを使用できること。また、ネットワークへの侵入やネットワークの攻撃を目的とする新技術が日々開発されているため、シスコは、本件ソフトウェアまたは本件ソフトウェアが使用される各種機器、システムもしくはネットワークが、侵入または攻撃に耐えられることについても保証しません。

制約事項。この保証は、本件ソフトウェア、本件製品、または本件ソフトウェアの使用先として許可されているその他の機器が以下のいずれかに該当するものの場合には適用されません。（a）シスコまたはシスコ認定代理人以外によって改変されたもの、（b）シスコが提示した指示に従ってインストール、運用、メンテナンスされていないもの、（c）異常な物理的もしくは電気的負荷、異常な環境条件、誤使用、過失、事故による影響を受けたもの、（d）ベータ版、評価版、テスト版、実演版としてその使用が許諾されているもの。本ソフトウェアの保証

エンド ユーザー ライセンス契約書

は、以下のいずれかに該当するものには適用されません。（e）一時的に使用される本ソフトウェアの各種モジュール、（f）シスコのソフトウェア センターに掲載されていないあらゆる本ソフトウェア、（g）シスコがシスコのソフトウェア センターにて「現状のまま」で明示的に提供しているあらゆる本ソフトウェア、（h）認定販売元がライセンス料を受領していないあらゆる本ソフトウェア、および（i）認定販売元以外の第三者から供給された本ソフトウェア。

保証の放棄

保証に関する本条項に明記されているものを除き、あらゆる明示または黙示の条件、表明および保証は、適用法により許される範囲で除外され、シスコ、そのサプライヤおよびライセンサによって明示的に放棄されます。上記条件、表明および保証は、以下の（i）または（ii）を含みますが、これらに限定されません。（i）商品性、特定目的への適合性、非侵害、十分な品質、不干渉、情報内容の正確性に関する黙示の保証または条件、（ii）各種取引、法律、利用、または商慣行に起因する黙示の保証または条件。これらのいずれかが排除できない場合はその範囲において、かかる黙示の条件、表明および/または保証の存続期間は、上記の「限定保証」条項で言及されている明示的な保証期間に限定されます。州または司法管轄区域によっては、黙示保証の有効期間を限定することが許可されていないため、お客様に上記の制限が適用されない場合があります。この保証は、お客様に特定の法的権利を付与するものですが、お客様は、法域によってはその他の権利を有する場合もあります。この放棄および除外は、上記の明示保証がその本質的な目的を達成できない場合にも適用されるものとします。

責任の否認–責任の制限。本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カナダ、日本またはカリブ海沿岸諸国の場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為（過失を含む）、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様が認定販売元に支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。(すなわち、複数の請求が行われた場合でも制限が拡大されることはありません)。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為（過失を含む）、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様がシスコに支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該対象外製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。(すなわち、複数の請求が行われた場合でも制限が拡大されることはありません)。本契約のいかなる規定も、（i）シスコ、ならびにその関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが、その過失に起因する身体障害または死亡に関してお客様に対して負う責任、（ii）詐欺的な不実表示に関するシスコの責任、または（iii）適用法のもとで排除できないシスコの責任を限定するものではありません。

責任の否認–結果的損害および他の損失に関する免責。本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カリブ海沿岸諸国またはカナダの場合、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコまたはそのサプライヤは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業

の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコまたはそのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。一部の州または法域では、結果的な損害または偶発的な損害の制限または除外が許可されていないため、上記制限がお客様に適用されない場合があります。

本ソフトウェアの取得地が日本の場合、死亡もしくは人身傷害または詐欺的な不実表示に起因または関連する責任を除き、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコもしくは認定販売元またはそれらのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、その発生原因（契約、不法行為（過失を含む）または本ソフトウェアの使用もしくは使用不能に起因するものを含むが、これらに限定されない）にかかわらず、それぞれの場合において、たとえ当該損害が発生する可能性についてシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が完全には適用されない場合があります。上記の排除は、（i）死亡または人身傷害、（ii）詐欺的な不実表示、または（iii）適用法のもとで排除できない条件に関連するシスコの責任、に起因または関連する責任には適用されません。

お客様は以下の 3 点について認識および同意しているものとします。（i）シスコは、本契約内の保証の放棄および責任の制限に依拠して価格を決定し本契約を結んでいること、（ii）これは、両当事者間のリスク配分（契約上の救済措置が、その本質的な目的を達成できず、結果的に損失を被るというリスクを含む）にも反映されていること、（iii）これは、両当事者間での取引の基幹を成す事項であること。

準拠法、管轄裁判所。本ソフトウェアの取得地が、認定販売元により受諾された発注書上の住所の記載から判断して、米国、ラテンアメリカ諸国またはカリブ海沿岸諸国の場合、本契約および保証（「本保証」）に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がカナダの場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず、カナダのオンタリオ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、オンタリオ州内の各裁判所が専属的に管轄します。本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニア（オーストラリアを除く）の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず英国の各法

に準拠し、同法に従って解釈されます。本契約または本保証に起因する各種申し立てについては、英国内の各裁判所が専属的に管轄します。また、本契約が英国法に準拠する場合、本契約の当事者ではない者は、本契約のいずれの条項についても、Contracts (Rights of Third Parties) Act 1999（1999 年契約（第三者の権利）法）に基づいて権利行使を行ったり、利益を享受したりする権利を有しません。本ソフトウェアの取得地が日本の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず日本国の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、日本国内の東京地方裁判所が専属的に管轄します。本ソフトウェアの取得地がオーストラリアの場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらずオーストラリア連邦ニュー サウス ウェールズ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、ニュー サウス ウェールズ州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がその他の国の場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。

上記のすべての国について、両当事者は、国際物品売買契約に関する国際連合条約の規定の適用を明示的に否定します。上記にかかわらず、いずれの当事者も、当事者の知的所有権または所有権の侵害の申し立てに対して、適切な司法管轄区域の裁判所において暫定的な差し止めによる救済を求めることができます。本契約のいずれかの規定が無効または施行不能なものとなった場合でも、本契約の残りの規定および本件保証書は有効に存続します。本契約内に別段の明示規定がない限り、本契約は、本件ソフトウェアおよび本件文書の使用許諾に関する両当事者の合意事項をまとめた唯一の文書となり、本件注文書またはその他の文書内の抵触規定または追加規定に優先し、これらの規定はすべて除外されます。本契約書は英語で記述されており、両当事者は、英語版が優先することに同意しているものとします。

各種製品保証規定やシスコ製品に関するその他の情報は、以下の URL でご確認ください。

http://www.cisco.com/go/warranty

Cisco コンテンツ セキュリティ ソフトウェア用エンド ユーザー ライセンス契約補則

重要（よくお読みください）

本エンド ユーザー ライセンス契約補則（以下「SEULA」）には、お客様とシスコとの間のエンドユーザーライセンス契約（以下「EULA」）に基づいてライセンスされているソフトウェア製品に対する追加条項（以下、総称して「契約」）が記載されています。この SEULA 内で定義されずに使用されている大文字の用語は、EULA で定義されたとおりの意味となります。この SEULA と EULA の条項に不一致がある場合は、この SEULA の条項が優先して適用されます。

お客様は、EULA により定められたお客様による本ソフトウェアへのアクセスおよび使用における制限事項の他に、本 SEULA に記載されている条項に同意したものと見なされます。

エンド ユーザー ライセンス契約書

本ソフトウェアのダウンロード、インストール、または本ソフトウェアを内蔵する機器の使用により、お客様およびお客様が代表する企業体は本契約に法的に拘束されます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、（A）お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、（B）お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および払い戻しに関するお客様の権利は、シスコまたはシスコ認定リセラーからの購入後 30 日で失効し、お客様が最初のエンド ユーザ購入者である場合にのみ適用されます。

本 SEULA が対象とするお客様の製品の名称および詳細は、次の Cisco Systems E メール セキュリティ アプライアンス（「ESA」）、Cisco Systems Web セキュリティアプライアンス（「WSA」）、および Cisco Systems セキュリティ管理アプリケーション（「SMA」）（まとめて「コンテンツセキュリティ」と呼ぶ）およびそれらの仮想アプライアンスの同等品（「ソフトウェア」）になります。

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

エンド ユーザー ライセンス契約書

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

定義

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the Web セキュリティアプライアンス and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at https://www.cisco.com/c/en/us/about/legal/service-descriptions.html

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, Web セキュリティアプライアンス , and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

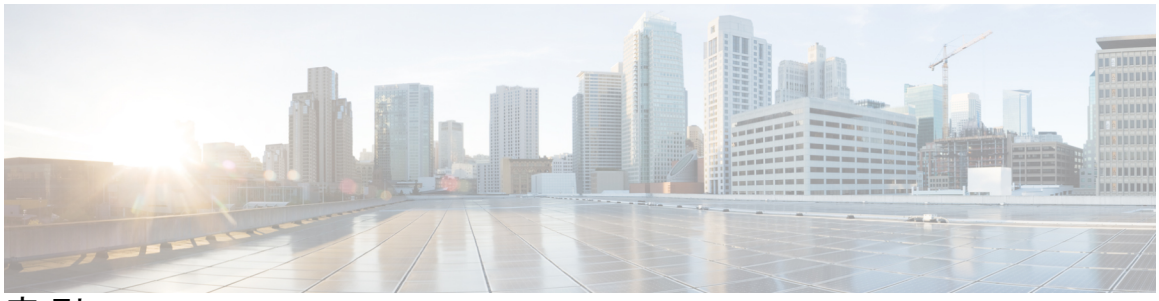
Consent and License to Use Data.

Subject to the Cisco Privacy Statement at https://www.cisco.com/c/en/us/about/legal/privacy.html, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling Service Logs in the Software. Instructions to enable or disable Service Logs are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.

エンド ユーザー ライセンス契約書



索 引

記号

\[Separate Window\] アイコン 1016
< 82, 1341, 1345–1347, 1349–1352, 1355–1357, 1359
$EnvelopeSender 変数 140
$TRUSTED メール フロー ポリシー 453

数字

1 時間あたりの最大受信者数 96

A

Active Directory Wizard 48
Advanced Malware Protection 585
ALL エントリ 108, 110, 148
    HAT 内 108, 110
    RAT での 148
ALLOWED_LIST 送信者グループ 453
AMP アーカイブ 1391
AMP エンジン ログ 1391
AMP。高度なマルウェア防御を参照。 585
Anti-Virus Logs 1391
archivemessage コマンド 1359
AsyncOS のアップグレード 1264
AsyncOS 復元 1271
AutoSupport 機能 42, 64, 1275

B

Bounce Logs 1391
bouncerecipients コマンド 1352

C

certificate 834
charset 1160
CIDR アドレス ブロック 110
Cisco Security Intelligence
        Operations[CiscoSecurityIntelligenceOperations] 516
Cisco Web セキュリティ サービス[CiscoWebせきゅりてぃさーびす] 548
CLI 13
    「コマンドライン インターフェイス」を参照 13
CLI Audit Logs 1391
CPU 使用率 1336
CRAM-MD5 983
CSV データ 1051

D

D-Mode 627
default 35, 41–42, 52, 54, 147
    hostname 41, 52
    IP アドレス 35
    ゲートウェイ 42, 54
    ドメイン 147
    ルータ 42, 54
deleterecipients コマンド 1351
delivernow コマンド 1357
Delivery Connection ID (DCID) 1334
Delivery Logs 1391
Direct Server Return（DSR） 1384
DKIM 検証 764
    Authentication-Results ヘッダー 764
DLP 626, 635–636, 639, 643, 648, 657, 660
    false positive、最小化 626, 635–636, 639, 643
    エンジンと分類子の更新 657
    トラブルシューティング 660
    メッセージ トラッキングに重要なコンテンツを含む 657
    リスク要因スコア 643
    重要度スケール 648
DLP ポリシー 635, 639, 643, 646
    コンテンツ照合分類子 635
    検出ルール 639, 643
    送信者および受信者のフィルタリング 646
    添付ファイルのフィルタリング 646
DNS 42, 54, 1022, 1304–1305
    サーバ 42, 54
    スプリット 1304
    タイムアウト 1304
    プライオリティ 1304
    逆引き DNS ルックアップのタイムアウト 1305

DNS (続き)
逆引き DNS ルックアップのタイムアウトの無効化、逆引き DNS ルックアップ 1305
無効化 1305
権威サーバ 1304
設定 42, 54
二重検索 1022
DNS キャッシュ 1349
DNS サーバ 1304
DNS リスト 201
DNS ルックアップ 1349
DNSBL 201
dnsstatus コマンド 1349
Document Type Definition（DTD） 1245
Domain Debug Logs 1391
Domain Name Service（DNS） 42, 54
設定 42, 54
drop-attachments-where-dictionary-match 271
DSR 1384
ループバック インターフェイス 1384
ロード バランシング 1384
仮想 IP（VIP） 1384

E

E メール セキュリティ仮想アプライアンス 27
ライセンスの読み込み 27
email 859
アドレスの書き換え 859

F

filters 155, 158, 165, 184, 190, 197, 202
コメント文字 158
スキャン可能なアーカイブ ファイルのタイプ 197
ディクショナリ用語の一致 165, 202
解析不可能なメッセージ 190
空白ヘッダーの一致 190
正規表現および Python 184
findevent 1360
FTP 1573
FTP Server Logs 1391
FTP アクセス 1574

G

GUI 13–14, 54, 1371
アクセス 14
ブラウザ要件 13
有効化 54, 1371
GUI セッションのタイムアウト 1220
GUI ログ。HTTP ログを参照してください。 1391

H

HAT 118, 124, 133
HAT 変数のテスト 118
エクスポート 133
HAT Order 123
GUI を使用した編集 123
HAT 内の最終エントリ 108
HAT 変数のテスト 118
hostname 41, 52
セットアップ中のホスト名の指定 41
hostrate コマンド 1347
hoststatus コマンド 1345
HTTP 54, 1371, 1573
GUI 1371
有効化 54
HTTP Logs 1391
HTTP 認証 1052
HTTPS 54, 852, 1371, 1573
GUI 1371
証明書 852
有効化 54
HTTPS ログイン 14

I

IMAP 認証 1178
implementsv 141
Injection Connection ID (ICID) 1334
Injection Debug Logs 1391
IP インターフェイス 43, 54
リスナーの定義 54
割り当て 43
IronPort Anti-Spam 用評価キー 63
IronPort Text Mail Logs 1391
IronPort スパム隔離 75
リリースされたメッセージと電子メールパイプライン 75
IronPort スパム隔離。「スパム隔離」を参照 1131
IronPort スパム対策 47, 63, 462, 509
filters 462
テスト 509
評価キー 47, 63
IronPort スパム対策ルール用プロキシ サーバ 1259
IronPort メール暗号化 663, 667, 672, 696
エンベロープ設定 667
キー サーバ設定 667
フィルタ アクションと使用 672, 696
メッセージ設定 667
設定 663
通知設定 667

L

LDAP 191–192, 950, 953, 955–957, 961, 964–965, 981, 988, 993, 995, 1175, 1177, 1210
- LDAPS 証明書 957
- load-balancing 995
- Microsoft Exchange 5.5 のサポート 953
- OpenLDAP クエリ 964
- SSL 957
- SunONE クエリ 964
- エイリアス拡張 965
- エイリアス統合クエリ 993
- クエリ トークン 956
- クエリのテスト 955, 961
- グループ クエリ 191–192
- テストサーバ 950
- フェールオーバー 995
- ベース DN 956
- 外部認証 988, 1210
- 再帰クエリ 957
- 接続 961
- 接続プーリング 981
- 匿名クエリ 957
- 複数のサーバ 995

LDAP Debug Logs 1391
LDAP エラー 963
LDAP ルーティング クエリー 826
- SMTP コールアヘッド受信者検証 826

LDAPS 証明書 957
listener 95, 806
- 暗号化の有効化 95
- 不正な MAIL FROM およびデフォルト ドメイン 95
- 免責事項の追加 806

listenerconfig コマンド 82

M

M-Series 1559
MAIL FROM 165, 327
mailertable 機能 853
mbox 形式 249
mbox 形式のログ ファイル 451
McAfee 63
- 評価キー 63

McAfee Anti-Virus エンジン 444
memory 1336
MIB ファイル 1362
MTA 66, 97, 829
MX 19

N

netmask 43
NIC チーミング 1377
NIC ペアリング 1377
- アップグレード時に名前を指定 1377
- アラート 1377

not.double.verified 139
NTP サーバ 1324
- 削除 1324

NTP ログ 1391
NXDOMAIN 139, 146

O

oldmessage コマンド 1359
overflow 524

P

passphrase 1209
- 設定 1209

PEM 形式、証明書用 688
POP 認証 1178
POP/IMAP サーバ 97
Possible Delivery 910
PVO。「隔離、ポリシー、ウイルス、およびアウトブレイク」を参照 1131

Q

qmail 形式配信ログ 1391

R

RADIUS 外部認証 1211
RAM 1536
RAM Utilization 1336
RAT 152
- 受信者のバイパス 152
- 受信者のバイパス（CLI） 152
- 受信者のバイパス（GUI） 152

rate command 1347
RBL 165
RCPT TO 165, 327
RCPT TO コマンド 150
Received ヘッダー 502
redirectrecipients 1354
removemessage コマンド 1359
resetcounters コマンド 1350
resume コマンド 1357
resumedel コマンド 1355

resumelistener コマンド 1356
revert 1271
　インストール 1271
RFC 10, 312, 612, 829, 1361
　1065 1361
　1066 1361
　1067 1361
　1213 1361
　1907 1361
　2047 612
　2487 829
　2821 10
　821 312
　822 312

S

SBRS 103, 113, 202
　none 113, 202
　テスト 103
SBRS のメッセージ フィルタ 105
SBRS。Senderbase レピュテーション サービス スコアを参照 113
Scanning Logs 1391
scp コマンド 1576
SDS.「Cisco Webセキュリティ サービス」を参照[CiscoWebせきゅりてぃさーびすをさんしょう] 548
secure copy 1576
Secure LDAP 957
SenderBase 96, 113
　送信者グループの SBO 113
SenderBase Affiliate ネットワーク 99
SenderBase ネットワーク オーナー識別番号 110
SenderBase レピュテーション サービス 99, 1009
SenderBase レピュテーション サービス スコア 113
SenderBase レピュテーション スコア 100, 113, 505
SenderBase レピュテーション スコア、CLI の構文 113
SenderBase、クエリ 113
SERVFAIL 139, 146
showmessage コマンド 1359
showrecipients 1354
SIDF の検証 165, 765, 768, 773, 776
　results 773
　テスト 776
　準拠レベル 768
　設定 765
　有効化 768
SIDF レコード 766–767
　テスト 767
　有効な 766
SMI ファイル 1362
SMTP 97, 150, 509
　IronPort Anti-Spam のテスト 509
SMTP (続き)
　response 150
　メッセージ 97
SMTP コールアヘッド サーバ プロファイル 821, 826
　リスナーでのイネーブル化 826
　作成 821
SMTP コールアヘッド受信者検証 819, 825–826, 828
　LDAP ルーティング クエリーを使用 826
　SMTP サーバ応答 825
　バイパス 828
　通信のワークフロー 819
SMTP デーモン 54
　インジェクタを参照 54
　リスナーを参照 54
SMTP ルート 853, 856
　メール配信と分割 856
　制限 856
SMTP 通信 819
　SMTP コールアヘッド サーバ 819
SMTP 認証（SMTP Auth） 980, 983
　DIGEST-MD5 983
　TLS 983
　サポート対象認証メカニズム 980
SMTP 認証プロファイル 983
SMTP 認証済みユーザの一致するフィルタ ルール 207
SNMP 1361–1363
　MIB ファイル 1362
　SMI ファイル 1362
　traps 1363
　コミュニティ ストリング 1361
　概要 1361
　複数のトラップ ターゲットの指定 1363
SNMP（簡易ネットワーク管理プロトコル） 1361
snmpconfig command 1364
SNMPv1 1361
SNMPv2 1361
Sophos 47, 63, 460
　updates 460
　評価キー 47, 63
Sophos ウイルス スキャン 452
　filters 452
SPF レコード 766–767
　テスト 767
　有効な 766
SPF 検証 165, 765, 768, 772–773, 776
　results 773
　テスト 776
　受信 SPF ヘッダー 772
　準拠レベル 768
　設定 765
　有効化 768

spf-passed フィルタ ルール 165, 775
spf-status フィルタ ルール 165, 774
SSH 16
SSL 957
STARTTLS 829
　定義 829
status detail コマンド 1341
Status Logs 1391
status コマンド 1341
strip-header フィルタ アクション 250
suspenddel コマンド 1355
suspendlistener コマンド 1356

T

Threat Operations Center（TOC） 519
throttling 99
TLS 829, 840
　default 840
　Preferred 840
　証明書 829
　必須 840
tophosts コマンド 1346
topin command 1349
trace コマンド 103
TTL 1343

U

updates 657
　DLP エンジンと分類子 657
URL レピュテーション 543
uuencoded 添付ファイル 160

V

version 1048
Virtual Gateway アドレス 248
Virtual Gateway アドレスのモニタリング 921
Virtual Gateway キュー 913
VLAN 1379–1380
　ラベル 1380
　定義済みの 1379

W

WBRS 543
　「URL レピュテーション」を参照[WBRS:URLれぴゅてーしょんをさんしょう] 543
Web UI セッションのタイムアウト 1220
Web インターフェイス 54
　有効化 54
Web レピュテーション 214, 256
　メッセージ フィルタ 214, 256

X

X-Header、追加 612
X-IronPort-AV ヘッダー 447
XML 1245, 1373, 1391
XML ステータス機能 1373

あ

アウトブレイク フィルタ 48, 64, 338, 513, 515, 517–520, 522–525, 529, 531–533, 540
　messagesOutbreak フィルタの変更 519
　　メッセージ変更 519
　SNMP トラップ 540
　アラート 540
　アラートのイネーブル化 529
　アンチ ウイルス スキャンなしで使用 523
　アンチウイルス隔離 524
　コンテキスト適応スキャン エンジン アウトブレイク フィルタ 517
　　CASE 517
　スキップ 338
　バイパスされたファイル拡張子 532
　メッセージの再評価 524–525
　メッセージの遅延 517
　メッセージ変更レベルのしきい値の設定 533
　リンクのリダイレクト 518
　ルール 520
　ルールの更新 531
　概要 513
　隔離レベルのしきい値の設定 532
　脅威カテゴリのアウトブレイク フィルタ 515
　　ウイルス アウトブレイク 515
　常時ルール 522
　定義済みのアウトブレイク ルール 519
　定義済みのアダプティブ ルール 520
　適応型スキャン（Adaptive Scanning） 529
　非ウイルス性の脅威 515
　評価キー 48, 64
　複数のスコア 523
アウトブレイク フィルタの評価キー 48, 64
アップグレード 1254–1255, 1269
　available 1269
　GUI 経由で取得 1255
　ストリーミング 1254–1255
　ローカル（local） 1254
アップデートの強制 460

アドレス タギング キー 908
消去 908
アドレス タギング キーの削除 908
アドレスの一部 110, 150
HAT 内 110
RAT での 150
アドレスの書き換え 859
アラート 529, 1275
アウトブレイク フィルタでのイネーブル化 529
重大度 1275
アラート メッセージ 41, 64
アラートリスト 1279
アラート設定 41, 64
アンチウイルス 447, 449–453, 813
アクション 450
ウイルスに感染 449
オリジナル メッセージのアーカイブ 451
カスタム アラート通知の送信 453
カスタム ヘッダーの追加 452
スキャンと修復 447
スキャンのみ 447
スキャン不可（Unscannable） 449
デフォルト通知を送信 452
メッセージの件名の変更 451
メッセージ受信者の変更 452
暗号化 449
詳細オプション 450
代替送信ホストに送信 453
添付ファイルをドロップ 447
アンチウイルス アーカイブ ログ 1391
アンチウイルス隔離。「隔離、ウイルス」を参照 1131
アンチスパム アーカイブ ログ 1391
アンチスパム ログ 1391

い

イメージ スキャン 264
イメージのスキャン 264
イメージの判定 264
イメージ分析 264, 327, 338
インジェクション制御のカウンタ リセット 137
インジェクション制御期間 137
インジェクタ 54
リスナーを参照 54
インストール 1271
復帰 1271
インポート 803, 805
HTML テキスト リソース 805
テキスト リソース 803

う

ウィザード 35, 48
アクティブディレクトリ 48
システム セットアップ 35
ウイルス メッセージ 1018
ウイルス隔離。「隔離」を参照 1131
ウイルス。 1131

え

エクスポート 804–805
HTML テキスト リソース 805
テキスト リソース 804
エンコーディング 809
免責事項 809
エンタープライズ ゲートウェイ 66
エンタープライズ ゲートウェイ構成 97
エンド ユーザ隔離 1177
スパム隔離、エンド ユーザー アクセスを参照 1177
エンベロープ受信者 191
エンベロープ受信者、書き換え 859
エンベロープ送信者 192
エンベロープ送信者の DNS 検証 139

お

オープン リレー、定義 148
オフセットの指定 1324

か

カウンタ 1334
カスタム SMTP 応答 140
変数（variable） 140
カスタム ヘッダー 502
カスタム ユーザー ロールのアクセス権限 1199
カテゴリ 568
news 568
SaaS および B2B（SaaS and B2B） 568
Web ページ翻訳（Web Page Translation） 568
Web ホスティング（Web Hosting） 568
Web メール（Web-Based Email） 568
アダルト（Adult） 568
アドバタイズメント（Advertisements） 568
アルコール（Alcohol） 568
インターネット電話（Internet Telephony） 568
インフラストラクチャおよびコンテンツ配信ネットワーク（Infrastructure and Content Delivery Networks） 568
エンターテイメント（Entertainment） 568

カテゴリ (続き)
オークション（Auctions） 568
オンライン コミュニティ（Online Communities） 568
オンライン ストレージおよびバックアップ（Online Storage and Backup） 568
オンライン トレード（Online Trading） 568
ギャンブル（Gambling） 568
ゲーム（Games） 568
コンピュータ セキュリティ（Computer Security） 568
コンピュータおよびインターネット（Computers and Internet） 568
ショッピング（Shopping） 568
ストリーミング オーディオ（Streaming Audio） 568
ストリーミング ビデオ（Streaming Video） 568
スポーツおよびレクリエーション（Sports and Recreation） 568
ソーシャル ネットワーキング（Social Networking） 568
ソフトウェア アップデート 568
ダイナミックおよびレジデンシャル（Dynamic and Residential） 568
タバコ（Tobacco） 568
チャットおよびインスタント メッセージ（Chat and Instant Messaging） 568
デジタル ポストカード（Digital Postcards） 568
パーク ドメイン（Parked Domains） 568
ハッキング（Hacking） 568
ピア ファイル転送（Peer File Transfer） 568
ビジネスおよび産業（Business and Industry） 568
ファイル転送サービス（File Transfer Services） 568
ファッション（Fashion） 568
フィルタリング回避（Filter Avoidance） 568
フリーウェアおよびシェアウェア（Freeware and Shareware） 568
プロフェッショナル ネットワーキング（Professional Networking） 568
ヘイト スピーチ（Hate Speech） 568
ポルノ（Pornography） 568
ユーモア（Humor） 568
違法ダウンロード（Illegal Downloads） 568
違法ドラッグ（Illegal Drugs） 568
違法行為（Illegal Activities） 568
飲食（Dining and Drinking） 568
下着および水着（Lingerie and Swimsuits） 568
科学技術（Science and Technology） 568
過激（Extreme） 568
求職（Job Search） 568
教育（Education） 568
業務用電子メール（Organizational Email） 568
金融（Finance） 568
携帯電話 568

カテゴリ (続き)
芸術（arts） 568
健康および栄養（Health and Nutrition） 568
検索エンジンおよびポータル（Search Engines and Portals） 568
個人サイト（Personal Sites） 568
参照（reference） 568
子供向け（Safe for Kids） 568
児童虐待コンテンツ（Child Abuse Content） 568
自然（Nature） 568
写真検索および画像（Photo Searches and Images） 568
社会および文化（Society and Culture） 568
社会科学（Social Science） 568
宗教（Religion） 568
出会い系（Dating） 568
乗り物（Transportation） 568
性教育（Sex Education） 568
性的でないヌード（Non-Sexual Nudity） 568
政治（Politics） 568
政府および法律（Government and Law） 568
占星術（Astrology） 568
非政府組織（Non-Governmental Organizations） 568
不正および盗用（Cheating and Plagiarism） 568
不動産（Real Estate） 568
武器（Weapons） 568
宝くじ（Lotteries） 568
未分類 568
旅行（Travel） 568

き

キー サイズ 744
キュー 82

く

クエリー 963, 965–966, 968, 980, 988, 993
SMTP 認証 980
グループ 968
スパム隔離エイリアス統合 993
マスカレード 966
ルーティング 965
外部認証 988
受け入れ 963
グッド ネイバー テーブル 840
クラウド内のファイル分析結果の詳細を得るためにアプライアンスをグループ化する 605
クラスタ 550
グラフ 1372

グラフィカル ユーザー インターフェイス 13
「GUI」を参照 13
グローバル カウンタ 1350

け

ゲージ 1336
ケース（コンテキスト適応スキャンエンジン [TM]） 506

こ

コード本体> 82, 1341, 1345–1347, 1349–1352, 1355–1357, 1359
コールアヘッド SMTP サーバ 819, 827
ルーティング 827
このマニュアルに関するフィードバック、送信 9
コミュニティ ストリング 1361
コンテンツ スキャナ 260
コンテンツ フィルタ 327, 338, 346, 352, 1131, 1598–1600, 1603
アクション 338
条件 327
非 ASCII 文字セット 352, 1603
変数 346
例 1598–1600
コンテンツ フィルタによる阻止 1018
コンテンツ照合分類子 635

さ

サードパーティ リレー 148
サブネット 43

し

しきい値、SenderBase レピュテーション スコアの 113
システム クロック 41, 64
システム セットアップ ウィザード 35
システム ログ 1391
システム時刻[しすてむじこく] 41, 64
設定 41, 64
システム隔離。「隔離、ポリシー、ウイルス、およびアウトブレイク」を参照 1131
システム容量 1045–1047, 1067–1070
システムの負荷レポート 1046, 1069
メモリ ページ スワッピング 1047, 1070
ワークキュー ページ 1045, 1067
シリアル接続のピン割り当て 28, 1577

す

スキャン可能なアーカイブ ファイルのタイプ 197
スケジュール設定されたログ ロールオーバー 1473
ステートレス ログ 1421
ストリーミング アップグレード 1255
スパム 509
テスト 509
スパム メッセージ 1018
スパム隔離 1154–1155, 1174, 1176–1177, 1180, 1183–1184, 1187–1188, 1562
IMAP/POP 認証 1177
LDAP 認証 1176
エイリアス統合 1183
エンド ユーザー アクセス 1177
エンドユーザ アクセス 1174
すべてのメッセージの削除 1188
メッセージの詳細 1187
メッセージ変数 1180
リリースされたメッセージと電子メールパイプライン 1187
ローカル（local） 1154
外部 1154, 1562
通知 1180
通知のテスト 1184
複数の通知の受信 1183
満杯時の動作 1155
無効化 1188
スパム隔離内の全メッセージの削除 1188
スパム対策 96, 440, 464, 488, 490–491, 509
HAT パラメータ 96
IronPort スパム対策 464
アプライアンスによって生成されたメッセージのスキャン 490
テスト 509
デフォルトのスキャン エンジンの選択 488
誤検出および検出漏れのレポート 491
複数のスキャン エンジンの使用 440

せ

セーフリスト/ブロックリスト 1161–1164, 1173–1174
workqueue 1161
インポートとエクスポート 1173
トラブルシューティング 1174
バックアップと復元 1173
外部スパム隔離 1163
管理 1164
有効化 1162
セキュア HTTP（https） 829
セキュア ソケット レイヤ（SSL） 829
セキュアでないリレー 148

た

タイム サーバ 41, 64
タイム ゾーン 1324
ダブル DNS で検証済み 1023, 1085
ダミー アカウント 103

ち

チェーン クエリー 975
　作成 975

て

ディレクトリ ハーベスト攻撃（DHA） 976
データ損失防止 1131
テキスト リソース 802–806
　HTML ベース 804
　HTML リソースへのエクスポートおよびインポート 805
　インポート 803
　エクスポート 804
　コード ビュー 804
　ポリシーおよび設定での使用 805
　管理 802
　免責事項 806
テスト 457, 509
　IronPort スパム対策 509
　Sophos ウイルス エンジン 457
デフォルト DNS サーバ 1305
デフォルト ルータ 42
デモ証明書 54
デュアル DKIM および DomainKey 署名 748

と

ドメイン キー 742, 744, 754
　確認 742
　署名キー サイズ 744
　署名キーのインポート 754
　署名の検証 742
ドメイン プロファイル 757
　すべての既存のプロファイルの削除 757
トラブルシューティング 660
　DLP 660
トレース 506

ね

ネットワーク アクセス リスト 1217
ネットワーク タイム プロトコル（NTP） 41, 64
　設定 41, 64

は

ハード電源リセット 1269, 1538
バイパス 152, 253
　throttling 152
　スパム対策 253
パフォーマンス 1536
パブリック リスナー 108
　デフォルト エントリ 108
パブリックブロックリスト 201

ふ

フォワード DNS ルックアップ 1348
プライベート インジェクタ 58
プライベート リスナー 108
　デフォルト エントリ 108
ブラックホール リスナー 82, 1523
プロトコル 82
　「メール プロトコル」を参照 82

へ

ベース DN 956
ヘッダー 859
ヘッダー、メッセージ フィルタでの削除 250
ヘッダー、ロギング 507
ヘッダー、挿入 675
ヘッダーの削除 250
ヘッダーの挿入 675

ほ

ホスト アクセス テーブル（HAT） 123
　GUI での順序の変更 123

ま

マーケティング メッセージ 1018
マルウェア 441
　定義済みの 441
マルチレイヤ アンチウイルス スキャン 440

め

メーリング リスト 1183
　通知 1183

メール プロトコル 82
定義 < 82
メール ポリシー 312
最初に一致したものが有効 312
メール ポリシー、発信 650
DLP 650
メールのループ、検出 296
メールの配信 910
Possible Delivery 910
メッセージのタイムアウト 910
メール転送エージェントMTA を参照。 1561
メッセージ ID（MID） 1334
メッセージ トラッキング 506, 657
および重要なコンテンツ 657
着信リレー 506
メッセージ フィルタ 155, 157–158, 160, 165, 195–198, 202, 223, 235, 275–276, 280, 1131
（非）アクティブ 276
attachment-protected 165
attachment-unprotected 165
body-dictionary-match 202
MIME タイプ 197
SenderBase レピュテーション スコア 202
status 276
エクスポート 280
フィルタ アクション 223
ルール 157
暗号化 198
移動 276
概要 155
結合 158, 165
構文 158
削除 275
時刻と日付 195
順序付け 160
追加 275
変数 235
乱数 196
メッセージ フィルタ アクション変数 807
免責事項での使用 807
メッセージ ヘッダー 195
メッセージ ヘッダー、メッセージ フィルタでの追加 250
メッセージに含まれる URL のリダイレクト 555
メッセージに含まれる URL の書き換え 555
メッセージのエンコード 282
変更 282
メッセージのリレー 54
メッセージのレプリケーション 223, 244
メッセージ配信の再試行 1030
メッセージ分裂 314
定義済みの 314
メッセージ変更レベルのしきい値 533
メッセージ変数 1180
スパム隔離の通知 1180
メッセージ本文のスキャン 198

も

モニタリング 1340

ゆ

ユーザー アカウント 1191, 1209
ロックとロック解除 1209
制限 1191
ユーザー グループ 1191–1192
ユーザー タイプ 1192

り

リアルタイム モニタリング 1346
リスク要因スコア 626, 643
DLP 643
リソース節約モード 1336, 1536
リバース DNS ルックアップ 116, 913, 1348
リモート 1254
リンク集約 1377

る

ルーティング 827
SMTP コールアヘッド サーバ 827
ルート サーバ（DNS） 42, 54
ループバック インターフェイス 1384

れ

レート 1339
レトロスペクティブな判定 620
レピュテーション フィルタの段階的アプローチ 102
レピュテーションフィルタによる停止 1018
レポーティング 506
着信リレー 506

ろ

ロギング、ヘッダー 507
ログ 1391, 1397, 1405, 1451, 1468–1469, 1472, 1532
Anti-Spam Archive 1391
Anti-Virus Archive 1391
Bounce Logs 1391

ログ (続き)
CLI Audit Logs 1391
Delivery Logs 1391
FTP Server Logs 1391
HTTP Logs 1391
Injection Debug Logs 1391
IronPort Text Mail Logs 1391
LDAP Debug Logs 1391
NTP ログ 1391
qmail 形式配信ログ 1391
Scanning 1391
Status Logs 1391
アンチウイルス 1391
グローバル属性 1469
コンフィギュレーション履歴ログ 1451
トラブルシューティング 1532
ファイル名の拡張子 1472
ログ (続き)
レベル 1468
形式 1391
定義 1391
定義されたログ サブスクリプション 1391
登録 1405
比較 1397
ログ サブスクリプション 451, 1391, 1405
Sophos 451
ログ ファイル タイプ 1391
ログ ファイルのロールオーバー 1472

わ

ワーク キュー 1336, 1358
ワーク キュー、一時停止 1358
ワーク キューの一時停止 1358

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。