



## **AsyncOS 12.5 for Cisco Content Security Management Appliances ユーザガイド（一般導入）**

初版：2019年7月22日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスココンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

© 2019 Cisco Systems, Inc. All rights reserved.



## 目次

---

### 第 1 章

#### はじめに 1

今回のリリースでの新機能 1

Cisco コンテンツ セキュリティ管理の概要 3

---

### 第 2 章

#### セットアップ、インストール、および基本設定 5

ソリューション導入の概要 5

インストール計画 6

ネットワーク プランニング 6

セキュリティ管理アプライアンスと E メール セキュリティ アプライアンスの統合について 7

クラスタ化された E メール セキュリティ アプライアンスを使用した展開 7

セットアップの準備 8

アプライアンスの物理的なセットアップと接続 8

ネットワーク アドレスと IP アドレスの割り当ての決定 8

セットアップ情報の収集 9

セキュリティ管理アプライアンスへのアクセス 10

ブラウザ要件 10

Web インターフェイスへのアクセスについて 12

Web インターフェイスへのアクセス 12

レガシー Web インターフェイスへのアクセス 13

コマンドライン インターフェイスへのアクセス 14

サポートされる言語 14

SwaggerUI を使用したセキュリティ管理アプライアンス API インターフェイスへのアクセス  
15

システム セットアップ ウィザードの実行	15
はじめる前に	16
システム セットアップ ウィザードの概要	16
システム セットアップ ウィザードの起動	17
エンドユーザ ライセンス契約書の確認	17
システムの設定	17
ネットワークの設定	18
設定の確認	19
次の手順	19
管理対象アプライアンスの追加について	19
管理対象アプライアンス設定の編集	20
管理対象アプライアンスのリストからのアプライアンスの削除	21
セキュリティ管理アプライアンスでのサービスの設定	21
設定変更のコミットおよび破棄	22

---

**第 3 章**

<b>レガシー Web インターフェイスでのレポートの使用</b>	<b>23</b>
レポート データの表示方法	23
セキュリティ管理アプライアンスによるレポート用データの収集方法	24
レポート データの保存方法	25
レポーティングおよびアップグレードについて	25
レポート データのビューのカスタマイズ	25
アプライアンスまたはレポーティング グループのレポート データの表示	26
レポートの時間範囲の選択	27
(Web レポートのみ) チャート化するデータの選択	27
レポート ページのテーブルのカスタマイズ	28
カスタム レポート	28
カスタム レポートに追加できないモジュール	29
カスタム レポート ページの作成	30
レポートに含まれるメッセージやトランザクションの詳細の表示	31
電子メール レポートのパフォーマンスの向上	31
レポーティング データおよびトラッキング データのエクスポート	33

カンマ区切り (CSV) ファイルとしてのレポート データのエクスポート	35
レポートおよびトラッキングにおけるサブドメインとセカンドレベルドメインの比較	36
すべてのレポートのトラブルシューティング	36
バックアップセキュリティ管理アプライアンスのレポート データを表示できない	36
レポーティングがディセーブルになっている	37
電子メール レポートおよび Web レポート	37

## 第 4 章

## 新しい Web インターフェイスでのレポートの使用 39

レポート データの表示方法	39
セキュリティ管理アプライアンスによるレポート用データの収集方法	40
レポート データの保存方法	41
レポーティングおよびアップグレードについて	41
インタラクティブ レポート ページの使用	41
レポート データのビューのカスタマイズ	42
アプライアンスまたはレポーティング グループのレポート データの表示	43
レポートの時間範囲の選択	44
(Web レポートのみ) チャート化するデータの選択	44
(電子メール レポートのみ) レポート ページでのビューのカスタマイズ	45
レポート ページのテーブルのカスタマイズ	45
カウンタを使用しての、トレンドグラフ上のデータのフィルタリング	46
[マイ レポート (My Reports) ] ページ	46
[マイレポート (My Reports) ] ページに追加できないモジュール	47
[マイレポート (My Reports) ] ページでのレポートの追加	48
レポートに含まれるメッセージやトランザクションの詳細の表示	49
電子メール レポートのパフォーマンスの向上	49
レポーティング データおよびトラッキング データのエクスポート	51
カンマ区切り (CSV) ファイルとしてのレポート データのエクスポート	53
すべてのレポートのトラブルシューティング	54
バックアップセキュリティ管理アプライアンスのレポート データを表示できない	54
レポーティングがディセーブルになっている	54

<b>中央集中型の電子メール セキュリティ レポートの作成</b>	<b>55</b>
中央集中型の電子メール レポートの概要	55
中央集中型の電子メール レポートの設定	56
セキュリティ管理アプライアンスでの中央集中型電子メール レポートの有効化	57
管理対象の各 E メール セキュリティ アプライアンスへの中央集中型電子メール レポート サービスの追加	57
電子メール レポート グループの作成	58
E メール セキュリティ アプライアンスでの中央集中型の電子メール レポートの有効化	59
電子メール レポート データの操作	59
新しい Web インターフェイスでの電子メール レポート データの使用	60
検索およびインタラクティブ電子メール レポート ページ	61
[電子メール レポート (Email Reporting) ] ページの概要	62
電子メール レポート ページのテーブルの列の説明	68
[電子メール レポートの概要 (Email Reporting Overview) ] ページ	71
受信メール メッセージのカウント方法	72
アプライアンスによる電子メール メッセージの分類方法	72
[概要 (Overview) ] ページでの電子メール メッセージの分類	73
[受信メール (Incoming Mail) ] ページ	76
[受信メール (Incoming Mail) ] ページ内のビュー	76
[受信メールの詳細 (Incoming Mail Details) ] テーブル	78
[送信者プロフィール (Sender Profile) ] ページ	79
[送信者グループ (Sender Groups) ] レポート ページ	81
[送信者ドメインのレピュテーション (Sender Domain Reputation) ] ページ	81
[送信先 (Outgoing Destinations) ] ページ	82
[送信メッセージ送信者 (Outgoing Senders) ] ページ	83
[内部ユーザ (Internal Users) ] ページ	84
[内部ユーザの詳細 (Internal User Details) ] ページ	85
特定の内部ユーザの検索	86
DLP インシデント	86

[DLPインシデントの詳細 (DLP Incidents Details) ] テーブル	87
[DLP ポリシー詳細 (DLP Policy Detail) ] ページ	88
メッセージフィルタ	88
地理的分散	88
大容量のメール	88
[コンテンツフィルタ (Content Filters) ] ページ	89
[コンテンツフィルタの詳細 (Content Filter Details) ] ページ	90
DMARC 検証	90
マクロ検出	90
[外部脅威フィード (External Threat Feeds) ] ページ	91
[ウイルス タイプ (Virus Types) ] ページ	91
[URL フィルタリング (URL Filtering) ] ページ	93
[Webインタラクショントラッキング (Web Interaction Tracking) ] ページ	93
[偽装メールの検出 (Forged Email Detection) ] ページ	95
[高度なマルウェア防御 (ファイルレピュテーションとファイル分析) (Advanced Malware Protection (File Reputation and File Analysis)) ] レポート ページ	95
ファイル分析レポートの詳細の要件	95
SHA-256 ハッシュによるファイルの識別	97
ファイルレピュテーションとファイル分析レポートのページ	98
その他のレポートでのファイルレピュテーションフィルタ データの表示	101
クラウドで詳細なファイル分析結果が表示されるファイル	101
メールボックスの自動修復	102
[TLS 接続 (TLS Connections) ] ページ	103
[受信 SMTP 認証 (Inbound SMTP Authentication) ] ページ	104
[レート制限 (Rate Limits) ] ページ	105
[アウトブレイク フィルタ (Outbreak Filters) ] ページ	105
グレイメールのレポート	107
AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート	108
[システム容量 (System Capacity) ] ページ	109
[システム容量 (System Capacity) ] ページに表示されるデータの解釈方法	109
[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ]	110

[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ]	111
[システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ]	111
[システム容量 (System Capacity) ] : [システムの負荷 (System Load) ]	111
[システム容量 (System Capacity) ] : [すべて (All) ]	112
[システム容量 (System Capacity) ] グラフのしきい値インジケータ	113
[有効なレポートデータ (Reporting Data Availability) ] ページ	113
新しい Web インターフェイスの電子メール レポート ページの概要	113
[メールフロー概要 (Mail Flow Summary) ] ページ	118
受信メール メッセージのカウント方法	121
アプライアンスによる電子メール メッセージの分類方法	121
[メールフロー概要 (Mail Flow Summary) ] ページでの電子メール メッセージの分類	122
[システム容量 (System Capacity) ] ページ	125
[システム容量 (System Capacity) ] ページに表示されるデータの解釈方法	126
[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ]	127
[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ]	127
[システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ]	128
[システム容量 (System Capacity) ] : [システムの負荷 (System Load) ]	128
[システム容量 (System Capacity) ] : [すべて (All) ]	129
[システム容量 (System Capacity) ] グラフのしきい値インジケータ	129
[高度なマルウェア防御 (Advanced Malware Protection) ] ページ	129
[高度なマルウェア防御 (Advanced Malware Protection) ] : [概要 (Summary) ]	131
[高度なマルウェア防御 (Advanced Malware Protection) ] - [AMP レピュテーション (AMP Reputation) ]	131
[高度なマルウェア防御 (Advanced Malware Protection) ] - [ファイル分析 (File Analysis) ]	133
[高度なマルウェア防御 (Advanced Malware Protection) ] - [ファイル レトロスペクション (File Retrospection) ]	133
[高度なマルウェア防御 (Advanced Malware Protection) ] - [メールボックスの自動修復 (Mailbox Auto Remediation) ]	134
ファイル分析レポートの詳細の要件	134
SHA-256 ハッシュによるファイルの識別	136



その他のレポートでのファイルレピュテーションフィルタデータの表示	137
クラウドで詳細なファイル分析結果が表示されるファイル	137
[ウイルスフィルタリング (Virus Filtering) ] ページ	137
[ウイルスタイプ詳細 (Virus Types Detail) ] テーブル	139
[マクロ検出 (Macro Detection) ] ページ	139
[DMARC検証 (DMARC Verification) ] ページ	140
[DMARC検証の詳細別のドメイン (Domains by DMARC Verification Details) ] テーブル	141
[アウトブレイク フィルタリング (Outbreak Filtering) ] ページ	141
[URL フィルタリング (URL Filtering) ] ページ	144
[偽装メールの検出 (Forged Email Detection) ] ページ	146
[外部脅威フィード (External Threat Feeds) ] ページ	146
[送信者ドメインのレピュテーション (Sender Domain Reputation) ] ページ	147
[メールフローの詳細 (Mail Flow Details) ] ページ	147
メールフローの詳細ページ内のビュー	149
[受信メール (Incoming Mails) ] テーブル	150
[送信者プロファイル (Sender Profile) ] ページ	154
[送信者の詳細 (Sender Details) ] テーブル	156
送信者グループ レポート	157
[送信先 (Outgoing Destinations) ] ページ	157
送信先の詳細の表	159
[TLS暗号化 (TLS Encryption) ] ページ	160
TLS 接続数詳細テーブル	160
[受信 SMTP 認証 (Inbound SMTP Authentication) ] ページ	161
[レート制限 (Rate Limits) ] ページ	163
[国別の接続 (Connections by Country) ] ページ	164
[ユーザ メール サマリー (User Mail Summary) ] ページ	165
[ユーザメールフローの詳細 (User Mail Flow Details) ] テーブル	166
特定の内部ユーザの検索	167
[DLP インシデント サマリー (DLP Incident Summary) ] ページ	168
[Web インタラクション (Web Interaction) ] ページ	169

Webインタラクショントラッキングの詳細 (Web Interaction Tracking Details)	171
[メッセージフィルタ (Message Filters)] ページ	172
[大容量のメール (High Volume Mail)] ページ	172
[コンテンツフィルタ (Content Filters)] ページ	173
[コンテンツフィルタの詳細 (Content Filter Details)] ページ	174
[有効なレポートデータ (Reporting Data Availability)] ページ	174
グレイメールのレポート	174
AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート	175
スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて	175
その他のレポート タイプ	177
[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポート	177
[エグゼクティブサマリー (Executive Summary)] レポート	181
[スケジュールされたレポート (Scheduled Reports)] ページ	181
メール レポートのスケジュール設定	181
スケジュール設定されたレポートの追加	181
スケジュール設定されたレポートの編集	183
スケジュール設定されたレポートの中止	183
オンデマンドでのメール レポートの生成	183
[アーカイブ メール レポート (Archived Email Reports)] ページ	185
[アーカイブ メール レポート (Archived Email Reports)] の表示と管理	185
アーカイブ レポートへのアクセス	186
アーカイブ済みのレポートの削除	186
メール レポートのトラブルシューティング	186
アウトブレイク フィルタ レポートに情報が正しく表示されない	187
レポートのリンクをクリックした後のメッセージ トラッキング結果がレポート結果と一致しない	187
[高度なマルウェア保護判定のアップデート (Advanced Malware Protection Verdict Updates)]	
レポートの結果が異なる	187
ファイル分析レポートの詳細の表示に関する問題	188
ファイル分析レポートの詳細を使用できない	188

ファイル分析レポートの詳細を表示する際のエラー	188
ファイル分析レポートの詳細をプライベートクラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー	188
ファイル分析関連エラーのロギング	188
不正なグレイメールメッセージまたはマーケティングメッセージの総数	189

## 第 6 章

中央集中型 Web レポートリングおよびトラッキングの使用	191
中央集中型 Web レポートリングおよびトラッキングの概要	191
中央集中型 Web レポートリングおよびトラッキングの設定	193
セキュリティ管理アプライアンスでの中央集中型 Web レポートリングのイネーブル化	194
Web セキュリティアプライアンスでの中央集中型レポートリングのイネーブル化	194
管理対象の各 Web セキュリティアプライアンスへの中央集中型 Web レポートリングサー ビスの追加	195
Web レポートでのユーザ名の匿名化	196
Web セキュリティ レポートの使用	196
新しい Web インターフェイスでの Web セキュリティ レポートの使用	197
[Web レポート (Web Reporting) ] ページの説明	197
[ 滞留時間 (Time Spent) ] について	202
Web レポートの概要	202
[ ユーザ (Users) ] レポート (Web)	204
[ ユーザの詳細 (User Details) ] (Web レポートリング)	206
[ ユーザ数レポート (User Count Report) ] (Web)	208
[ Web サイト (Web Sites) ] レポート	208
[ URL カテゴリ (URL Categories) ] レポート	209
未分類の URL の削減	210
URL カテゴリ セットの更新とレポート	211
[ URL カテゴリ (URL Categories) ] ページとその他のレポートリング ページの併用	211
誤って分類された URL と未分類の URL のレポート	212
[ アプリケーションの表示 (Application Visibility) ] レポート	212
アプリケーションとアプリケーションタイプの違いについて	213
[ マルウェア対策 (Anti-Malware) ] レポート	214

[マルウェアのカテゴリ (Malware Category) ] レポート	216
[マルウェアの脅威 (Malware Threat) ] レポート	216
マルウェアのカテゴリについて	216
[高度なマルウェア防御 (ファイルレピュテーション) (Advanced Malware Protection (File Reputation)) ] および [高度なマルウェア防御 (ファイル分析) (Advanced Malware Protection (File Analysis)) ] レポート	218
ファイル分析レポートの詳細の要件	219
SHA-256 ハッシュによるファイルの識別	221
[高度なマルウェア防御 (ファイルレピュテーション) (Advanced Malware Protection (File Reputation)) ] および [高度なマルウェア防御 (ファイル分析) (Advanced Malware Protection (File Analysis)) ] レポート ページ	222
その他のレポートでのファイル レピュテーション フィルタ データの表示	224
クラウドで詳細なファイル分析結果が表示されるファイル	224
[クライアント マルウェア リスク (Client Malware Risk) ] レポート	224
[Web レピュテーション フィルタ (Web Reputation Filters) ] レポート	226
Web レピュテーション フィルタとは	226
Web レピュテーション 設定の調整	228
[L4 トラフィック モニタ (L4 Traffic Monitor) ] レポート	228
[SOCKS プロキシ (SOCKS Proxy) ] レポート	231
ユーザの場所別レポート (Reports by User Location)	232
[システム容量 (System Capacity) ] ページ	233
[システム容量 (System Capacity) ] レポートの表示	233
[システム容量 (System Capacity) ] ページに表示されるデータの解釈方法	234
[システム容量 (System Capacity) ] : [システムの負荷 (System Load) ]	234
[システム容量 (System Capacity) ] : [ネットワーク負荷 (Network Load) ]	235
プロキシ バッファ メモリ スワッピングに関する注意事項	235
[使用可能なデータ (Data Availability) ] ページ	235
新しい Web インターフェイスの Web レポート ページの概要	236
[滞留時間 (Time Spent) ] について	239
[概要 (Overview) ] ページ	240
[アプリケーションの表示 (Application Visibility) ] ページ	242
[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] ページ	244

[SOCKS プロキシ (SOCKS Proxy) ] ページ	247
[URLカテゴリ (URL Categories) ] ページ	249
未分類の URL の削減	250
URL カテゴリ セットの更新とレポート	250
[URL カテゴリ (URL Categories) ] ページとその他のレポート ページの併用	251
誤って分類された URL と未分類の URL のレポート	252
[ユーザ (Users) ] ページ	252
[ユーザの詳細 (User Details) ] ページ (Web レポート)	254
[Webサイト (Web Sites) ] ページ	257
[HTTPSレポート (HTTPS Reports) ] ページ	258
[マルウェア対策 (Anti-Malware) ] ページ	260
[マルウェアのカテゴリ (Malware Category) ] レポート	262
[マルウェアの脅威 (Malware Threat) ] レポート	262
マルウェアのカテゴリについて	262
[高度なマルウェア防御 (Advanced Malware Protection) ] ページ	264
[高度なマルウェア防御 (Advanced Malware Protection) ] : [AMPサマリー (AMP Summary) ]	265
[高度なマルウェア防御 (Advanced Malware Protection) ] : [ファイル分析 (File Analysis) ]	266
[クライアント マルウェア リスク (Client Malware Risk) ] レポート	267
[Web レピュテーションフィルタ (Web Reputation Filters) ] ページ	269
スケジュール設定されたレポートとオンデマンド Web レポートについて	272
Web レポートのスケジュール設定	273
スケジュール設定された Web レポートの保存	273
スケジュール設定された Web レポートの追加	274
スケジュール設定された Web レポートの編集	274
スケジュール設定された Web レポートの削除	275
追加の拡張 Web レポート	275
上位URLカテゴリ - 拡張 (Top URL Categories — Extended)	275
上位アプリケーションタイプ - 拡張 (Top Application Types — Extended)	276
オンデマンドでの Web レポートの生成	277

[アーカイブ Web レポート (Archived Web Reports) ] ページ	278
アーカイブ済みの Web レポートの表示と管理	278
Web トラッキング	279
Web プロキシ サービスによって処理されたトランザクションの検索	279
マルウェアのカテゴリについて	283
L4 トラフィック モニタによって処理されたトランザクションの検索	284
SOCKS プロキシによって処理されるトランザクションの検索	285
新しい Web インターフェイスでの Web トラッキング	285
Web プロキシ サービスによって処理されたトランザクションの検索	286
マルウェアのカテゴリについて	289
レイヤ 4 トラフィック モニタによって処理されたトランザクションの検索	290
SOCKS プロキシによって処理されるトランザクションの検索	291
Web トラッキングの検索結果の使用	291
詳細な Web トラッキング検索結果の表示	292
Web トラッキング検索結果について	292
Web トラッキング検索結果のトランザクションの詳細の表示	292
Web トラッキング機能および高度なマルウェア防御機能について	293
Web トラッキングおよびアップグレードについて	294
Web レポーティングおよびトラッキングのトラブルシューティング	294
中央集中型レポーティングが適切に有効化されているのに機能しない	294
[高度なマルウェア保護判定のアップデート (Advanced Malware Protection Verdict Updates) ] レポートの結果が異なる	295
ファイル分析レポートの詳細の表示に関する問題	295
ファイル分析レポートの詳細を使用できない	295
ファイル分析レポートの詳細を表示する際のエラー	295
ファイル分析レポートの詳細をプライベートクラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー	296
予想されるデータがレポーティングまたはトラッキングの結果に表示されない	296
PDF に Web トラッキング データのサブセットのみが表示される	297
L4 トラフィック モニタ レポートのトラブルシューティング	297
エクスポートされた .CSV ファイルが Web インターフェイスのデータと異なる	297

## Web トラッキング検索結果のエクスポートの問題 297

## 第 7 章

## メッセージのトラッキング 299

トラッキング サービスの概要 299

中央集中型メッセージ トラッキングの設定 300

セキュリティ管理アプライアンスでの中央集中型電子メール トラッキングのイネーブル化 301

E メールセキュリティ アプライアンスでの中央集中型メッセージ トラッキングの設定 301

管理対象の各 E メールセキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加 302

機密情報へのアクセスの管理 303

メッセージ トラッキング データの有効性の検査 303

電子メール メッセージの検索 303

新しい Web インターフェイスでの電子メール メッセージの検索 303

レガシー Web インターフェイスでの電子メール メッセージの検索 306

結果セットの絞り込み 309

メッセージ トラッキングおよび高度なマルウェア防御機能について 310

トラッキング クエリ結果について 311

メッセージの詳細 312

判定チャートと最後の状態の判定 312

エンベロープとヘッダーのサマリー 314

ホスト サマリーの送信 315

処理詳細 315

メッセージ トラッキングのトラブルシューティング 316

予想されるメッセージが検索結果に表示されない 316

添付ファイルが検索結果に表示されない 316

## 第 8 章

## スパム隔離 319

スパム隔離の概要 319

ローカルのスパム隔離と外部のスパム隔離 320

中央集中型スパム隔離の設定 320

スパム隔離の有効化と設定	321
管理対象の各 E メールセキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加	323
セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定	324
スパム隔離へのブラウザ アクセス用 IP インターフェイスの設定	325
スパム隔離への管理ユーザ アクセスの設定	326
隔離対象のメールの受信者の制限	327
スパム隔離の言語	327
[スパム隔離の編集 (Edit Spam Quarantine)] ページ	327
セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御	328
セーフリストとブロックリストのメッセージ処理	328
セーフリストとブロックリストの有効化	329
外部スパム隔離およびセーフリスト/ブロックリスト	330
セーフリストおよびブロックリストへの送信者とドメインの追加 (管理者)	330
セーフリスト エントリとブロックリスト エントリの構文	335
すべてのセーフリストおよびブロックリストのクリア	336
セーフリストおよびブロックリストへのエンドユーザ アクセスについて	336
セーフリストへのエントリの追加 (エンドユーザ)	336
ブロックリストへの送信者の追加 (エンドユーザ)	337
セーフリスト/ブロックリストのバックアップと復元	338
セーフリストとブロックリストのトラブルシューティング	339
セーフリストに登録されている送信者からのメッセージが配信されない	339
エンドユーザのためのスパム管理機能の設定	340
スパム管理機能にアクセスするエンドユーザの認証オプション	340
LDAP 認証プロセス	341
IMAP/POP 認証プロセス	342
SAML 2.0 認証プロセス	343
Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定	343
スパム隔離へのエンドユーザ アクセスの設定	343
スパム隔離へのエンドユーザ アクセス用 URL の決定	345
エンドユーザに表示されるメッセージ	346



エンドユーザへの隔離されたメッセージに関する通知	346
受信者の電子メールのメーリングリストエイリアスおよびスパム通知	348
通知のテスト	349
スパム通知のトラブルシューティング	349
スパム隔離内のメッセージの管理	350
スパム隔離へのアクセス（管理ユーザ）	350
スパム隔離へのアクセス（管理ユーザ）	351
スパム隔離内でのメッセージの検索	351
大量メッセージの検索	351
スパム隔離内のメッセージの表示	352
スパム隔離内のメッセージの配信	352
スパム隔離からのメッセージの削除	353
スパム隔離のディスク領域	353
外部スパム隔離の無効化について	353
スパム隔離機能のトラブルシューティング	354
第 9 章	集約されたポリシー、ウイルス、およびアウトブレイク隔離 355
	集約隔離の概要 355
	隔離の種類 357
	ポリシー、ウイルス、およびアウトブレイク隔離の集約 359
	セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離の有効化 361
	管理対象の各 E メールセキュリティアプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加 362
	ポリシー、ウイルス、アウトブレイク隔離の移行の設定 363
	リリースされたメッセージを処理する代替アプライアンスの指定 365
	カスタム ユーザ ロールの集約隔離アクセスの設定 366
	中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化 366
	E メールセキュリティアプライアンスを使用できないときのメッセージのリリース 366
	ポリシー、ウイルス、およびアウトブレイク隔離の管理 367
	ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て 367

隔離内のメッセージの保持期間	368
隔離メッセージに自動的に適用されるデフォルトアクション	369
システム作成の隔離の設定を確認	369
ポリシー、ウイルス、およびアウトブレイク隔離の設定	370
ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について	372
ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定	372
ポリシー隔離の削除について	373
隔離のステータス、容量、およびアクティビティのモニタリング	373
隔離用のディスク容量の使用率に関するアラート	376
ポリシー隔離とロギング	376
メッセージ処理タスクの他のユーザへの割り当てについて	377
ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザグループの指定	377
ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作	378
隔離内のメッセージの表示	378
隔離されたメッセージおよび国際文字セット	379
ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの検索条件の変更	381
隔離内のメッセージの手動処理	381
メッセージのコピーの送信	382
ポリシー隔離間のメッセージの移動について	382
複数の隔離内にあるメッセージ	382
メッセージの詳細およびメッセージ内容の表示	383
一致した内容の表示	384
添付ファイルのダウンロード	385
隔離されたメッセージの再スキャンについて	385
アウトブレイク隔離	386
アウトブレイク隔離のメッセージの再スキャン	387
ルールサマリービュー	387
[ルールサマリー管理 (Manage by Rule Summary)] リンク	387
シスコへの偽陽性または不審なメッセージの報告	387

集約されたポリシー隔離のトラブルシューティング	388
管理ユーザがフィルタおよび DLP メッセージアクションの隔離を選択できない	388
集約アウトブレイク隔離から解放されたメッセージが再スキャンされない	388

## 第 10 章

**Web セキュリティ アプライアンスの管理 389**

中央集中型コンフィギュレーション管理について	389
適切な設定公開方式の決定	390
Configuration Master を使用して中央集中型で Web セキュリティ アプライアンスを管理する	390
Configuration Master を使用するための重要な注意事項	393
使用する Configuration Master のバージョンの確認	394
セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理の有効化	394
Configuration Master の初期化と設定	395
Configuration Master の初期化	395
Web Security Appliances と Configuration Master の関連付けについて	395
Web Security Appliances の追加と Configuration Master のバージョンとの関連付け	396
Configuration Master と Web セキュリティ アプライアンスとの関連付け	397
サブ Configuration Master の設定	397
アプライアンス リストでの関連する Configuration Master の表示	398
サブ Configuration Master の削除	399
サブ Configuration Master をアクティブ設定として選択	399
公開のための設定	399
既存の Configuration Master からのインポート	400
Web セキュリティ アプライアンスからの設定のインポート	401
Configuration Master での Web セキュリティ機能の直接設定	401
機能が常に有効化されていることの確認	404
イネーブルにされている機能の比較	404
公開する機能の有効化	405
使用しない Configuration Master のディセーブル化	406
拡張ファイル公開を使用するための設定	407
Web セキュリティ アプライアンスへの設定の公開	407

Configuration Master の公開	407
Configuration Master を公開する前に	408
Configuration Master の公開	409
Configuration Master を後日公開	410
コマンドライン インターフェイスによる Configuration Master の公開	411
拡張ファイル公開による設定の公開	412
拡張ファイル公開 : [今すぐ設定を公開する (Publish Configuration Now) ]	412
拡張ファイル公開 : [後日公開 (Publish Later) ]	413
公開ジョブのステータスと履歴の表示	413
公開履歴の表示	414
中央管理型アップグレード管理	414
Web セキュリティ アプライアンスのアップグレードの一元管理を設定	415
一元管理アップグレード マネージャの有効化	415
管理対象の各 Web セキュリティ アプライアンスへの一元管理アップグレード サービスの追加	416
WSA アップグレードの選択とダウンロード	417
インストール ウィザードの使用	418
Web セキュリティ アプライアンスのステータスの表示	420
Web アプライアンス ステータスの概要の表示	420
個々の Web セキュリティ アプライアンスのステータスの表示	420
Web アプライアンス ステータスの詳細	421
URL カテゴリ セットの更新の準備および管理	421
URL カテゴリ セットの更新による影響の理解	422
URL カテゴリ セットの更新に関する通知およびアラートの受信	422
新規または変更されたカテゴリのデフォルト設定の指定	422
URL カテゴリ セットの更新時にポリシーと ID/識別プロファイルの設定を確認	422
Application Visibility and Control (AVC) の更新	423
コンフィギュレーション管理上の問題のトラブルシューティング	423
[設定マスター (Configuration Master) ]>[ID (Identities) ]/[識別プロファイル (Identification Profiles) ]に [グループ (Groups) ]が表示されない	423

[設定マスター (Configuration Master) ]>[アクセス ポリシー (Access Policies) ]>[Web レ ピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings) ] ページの設定が想定とは異なる	424
設定公開失敗のトラブルシューティング	424

---

 第 11 章

**システム ステータスのモニタリング 425**

セキュリティ管理アプライアンスのステータスについて	425
セキュリティ管理アプライアンス 容量のモニタリング	426
キューの処理のモニタリング	426
CPU 使用率のモニタリング	427
管理アプライアンスからのデータ転送のステータスのモニタリング	427
管理対象アプライアンスの設定ステータスの表示	429
Web セキュリティ アプライアンスの追加ステータス情報	430
レポーティング データ アベイラビリティ ステータスのモニタリング	430
電子メール セキュリティ レポート データのアベイラビリティのモニタリング	430
Web セキュリティ レポート データのアベイラビリティのモニタリング	430
電子メール トラッキング データ ステータスのモニタリング	431
管理対象アプライアンスのキャパシティのモニタリング	431
アクティブな TCP/IP サービスの識別	432
ハードウェア障害発生時の管理対象アプライアンスの交換	432

---

 第 12 章

**LDAP との統合 433**

概要	433
スパム隔離と連携させるための LDAP の設定	434
LDAP サーバ プロファイルの作成	434
LDAP サーバのテスト	436
LDAP クエリの設定	436
LDAP クエリの構文	437
置換可能なトークン	437
スパム隔離へのエンドユーザ認証のクエリ	438
Active Directory エンドユーザ認証の設定例	438

OpenLDAP エンドユーザ認証の設定の例	439
スパム隔離のエイリアス統合クエリ	439
Active Directory エイリアス統合の設定例	440
OpenLDAP エイリアス統合の設定例	440
LDAP クエリのテスト	441
ドメインベース クエリ	441
ドメインベース クエリの作成	442
チェーンクエリ	443
チェーンクエリの作成	444
AsyncOS を複数の LDAP サーバと連携させるための設定	445
サーバとクエリのテスト	445
フェールオーバー	445
LDAP フェールオーバーのための Cisco コンテンツ セキュリティ アプライアンスの設定	446
ロード バランシング	447
ロード バランシングのための Cisco コンテンツ セキュリティ アプライアンスの設定	447
LDAP を使用した管理ユーザの外部認証の設定	448
管理ユーザの認証のためのユーザ アカウント クエリ	448
管理ユーザの認証のためのグループ メンバーシップ クエリ	449
管理ユーザの外部認証のイネーブル化	451

## 第 13 章

<b>SMTP ルーティングの設定</b>	<b>453</b>
SMTP ルートの概要	453
SMTP ルート、メール配信、およびメッセージ分裂	454
SMTP ルートと発信 SMTP 認証	454
ローカル ドメインの電子メールのルーティング	454
デフォルトの SMTP ルート	455
SMTP ルートの管理	455
SMTP ルートの定義	455
SMTP ルートの制限	456
SMTP ルートの追加	456

SMTP ルートのエクスポート 456

SMTP ルートのインポート 457

SMTP ルートと DNS 458

## 第 14 章

### Cisco Threat Response ポータルとの統合 459

Cisco Threat Response ポータルへのアプライアンスの統合 459

CLI を使用した Cisco Threat Response ポータルへのアプライアンスの統合 461

threatresponseconfig 462

cloudserviceconfig 463

ケースブックを使用した脅威分析の実行 464

クライアント ID およびクライアント パスワード クレデンシャルの取得 465

攻撃分析のケースブックへ観測対象を追加 467

## 第 15 章

### 管理タスクの分散 469

管理タスクの分散について 469

ユーザ ロールの割り当て 469

事前定義済みユーザ ロール 470

カスタムユーザロール 473

Custom Email User ロールについて 474

Custom Web User ロールについて 478

カスタム ユーザ ロールの削除 480

CLI へのアクセス権を持つユーザ ロール 480

LDAP の使用 480

隔離へのアクセス 480

[ユーザ (Users) ] ページ 480

管理ユーザの認証について 481

admin ユーザのパスワードの変更 481

有効期限後のユーザ パスワードの変更 482

ローカルに定義された管理ユーザの管理 482

ローカルに定義されたユーザの追加 482

ローカルに定義されたユーザの編集 483

ローカルに定義されたユーザの削除	483
ローカルに定義されたユーザのリストの表示	484
パスフレーズの設定と変更	484
パスフレーズの設定およびログインの要件	484
ユーザに対するオンデマンドでのパスフレーズ変更の要求	488
ローカルユーザアカウントのロックおよびロック解除	489
外部ユーザ認証	490
LDAP 認証の設定	491
RADIUS 認証の有効化	491
セキュリティ管理アプライアンスへのアクセスに対する追加の制御	494
IP ベースのネットワーク アクセスの設定	494
直接接続	494
プロキシ経由の接続	494
アクセス リストの作成	495
Web UI セッション タイムアウトの設定	497
CLI セッション タイムアウトの設定	498
メッセージ トラッキングでの機密情報へのアクセスの制御	498
管理ユーザ向けメッセージの表示	499
管理ユーザ アクティビティの表示	499
Web を使用したアクティブなセッションの表示	499
最近のログイン試行の表示	500
コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示	500
管理ユーザ アクセスのトラブルシューティング	501
エラー：ユーザにアクセス権限が割り当てられていません (User Has No Access Privileges Assigned)	501
アクティブメニューがありません (User Has No Active Menus)	502
外部認証されたユーザに設定オプションが表示されます (Externally-Authenticated Users See Preferences Option)	502
第 16 章	
一般的な管理タスク	503
管理タスクの実行	504



Cisco コンテンツ セキュリティ管理アプライアンスのライセンス	504
機能キーの使用	504
仮想アプライアンスのライセンスおよび機能キー	505
CLI コマンドを使用したメンテナンス作業の実行	506
セキュリティ管理アプライアンスのシャットダウン	506
セキュリティ管理アプライアンスのリポート	506
セキュリティ管理アプライアンスの停止	507
CLI の例 : suspend および suspendtransfers コマンド	508
一時停止状態からの再開	508
CLI の例 : resume および resumetransfers コマンド	508
工場出荷時の初期状態への設定のリセット	508
resetconfig コマンド	509
AsyncOS のバージョン情報の表示	509
リモート電源再投入の有効化	510
SNMP を使用したシステムの状態のモニタリング	511
例 : snmpconfig コマンド	511
セキュリティ管理アプライアンスのデータのバックアップ	513
バックアップされるデータ	514
バックアップの制約事項および要件	514
バックアップ期間	516
バックアップ中のサービスのアベイラビリティ	516
バックアッププロセスの中断	517
ターゲットアプライアンスによる管理対象アプライアンスからのデータの直接取得の防 止	517
バックアップステータスに関するアラートの受信	518
単一または定期バックアップのスケジュール設定	518
即時バックアップの開始	519
バックアップステータスの確認	519
ログファイルのバックアップ情報	520
その他の重要なバックアップタスク	520
バックアップアプライアンスのプライマリアプライアンスとしての使用	520

セキュリティ管理アプライアンスでのディザスタ リカバリ	522
アプライアンス ハードウェアのアップグレード	524
AsyncOS のアップグレード	524
アップグレード用のバッチ コマンド	524
アップグレードとアップデートのネットワーク要件の決定	524
アップグレード方式の選択：リモートまたはストリーミング	525
ストリーミング アップグレードの概要	525
リモート アップグレードの概要	525
リモート アップグレードのハードウェア要件およびソフトウェア要件	527
リモート アップグレード イメージのホスティング	527
リモート アップグレード方式における重要な違い	528
アップグレードおよびサービス アップデートの設定	528
アップグレードとアップデートの設定	528
厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレード およびアップデート サーバ設定	530
GUI からのアップデートおよびアップグレード設定値の設定	532
アップグレードの通知	533
アップグレードする前に：重要な手順	534
AsyncOS のアップグレード	534
バックグラウンド ダウンロードのキャンセルまたは削除ステータスの表示	537
アップグレード後	537
AsyncOS の以前のバージョンへの復元について	538
復元の影響に関する重要な注意事項	538
AsyncOS の復元	538
アップデートについて	540
Web 使用率制御の URL カテゴリ セット アップデートについて	540
生成されたメッセージの返信アドレスの設定	540
アラートの管理	541
アラート タイプおよび重大度	542
アラートの配信	542
最新アラートの表示	543

重複したアラートについて	543
Cisco AutoSupport	543
ハードウェア アラートの説明	544
システム アラートの説明	544
ネットワーク設定値の変更	550
システム ホスト名の変更	550
sethostname コマンド	550
ドメイン ネーム システムの設定	551
DNS サーバの指定	551
複数エントリとプライオリティ	551
インターネットルート サーバの使用	552
逆引き DNS ルックアップのタイムアウト	552
DNS アラート	553
DNS キャッシュのクリア	553
グラフィカルユーザ インターフェイスを使用した DNS 設定値の設定	553
TCP/IP トラフィック ルートの設定	554
GUI でのスタティック ルートの管理	554
デフォルト ゲートウェイの変更 (GUI)	554
デフォルト ゲートウェイの設定	554
セキュア通信プロトコルの指定	555
システム時刻の設定	556
ネットワーク タイム プロトコル (NTP) サーバの使用	556
(推奨) ネットワーク タイム プロトコル (NTP) を使用したアプライアンスのシステム時刻の設定	557
GMT オフセットの選択	557
時間帯ファイルの更新	558
時間帯ファイルの自動更新	558
時間帯ファイルの手動更新	558
[設定ファイル (Configuration File) ] ページ	558
設定の保存とインポート	559
コンフィギュレーション ファイルの管理	560

現在の設定ファイルの保存およびエクスポート	560
コンフィギュレーションファイルのロード	561
現在の設定のリセット	563
以前コミットしたコンフィギュレーションへのロールバック	563
設定ファイル用の CLI コマンド	563
showconfig、mailconfig、および saveconfig コマンド	564
loadconfig コマンド	565
rollbackconfig コマンド	565
publishconfig コマンド	565
trailblazerconfig コマンド	566
CLI を使用した設定変更のアップロード	566
ディスク領域の管理	567
(仮想アプライアンスのみ) 使用可能なディスク領域の拡大	568
ディスク領域、クォータ、および使用状況の表示	568
最大ディスク領域と割り当てについて	569
ディスク領域に関するアラートの受信の確認	570
その他のクォータのディスク領域の管理	570
ディスク領域量の再割り当て	571
E メールセキュリティ アプライアンスのシステムの状態グラフの参照のしきい値の調整	571
SAML 2.0 による SSO	572
SSO および SAML 2.0 について	572
SAML 2.0 SSO のワークフロー	572
SAML 2.0 に関する注意事項と制約事項	574
ログアウト	574
一般	574
管理者のスパム隔離へのアクセス	574
スパム隔離用の SSO の設定方法	574
前提条件	575
サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの 設定	575

Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダー の構成	577
Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成	579
スパム隔離のための SSO の有効化	580
ビューのカスタマイズ	581
お気に入りページの使用	581
プリファレンスの設定	582
全般設定	582
Web 使用状況分析のモニタリング	582
Web インターフェイスのレンダリングの改善	583
アプライアンスで有効なサービスの再起動とステータスの表示	583

---

 第 17 章

**ログ 585**

ロギングの概要	585
ロギングとレポートイング	585
ログの取得	586
ファイル名およびディレクトリ構造	587
ログのロールオーバーおよび転送スケジュール	587
ログ ファイル内のタイムスタンプ	588
デフォルトで有効になるログ	588
ログ タイプ	589
ログ タイプの概要	590
ログ タイプの比較	592
コンフィギュレーション履歴ログの使用	594
CLI 監査ログの使用	595
FTP サーバ ログの使用	596
HTTP ログの使用	596
スパム隔離ログの使用	597
スパム隔離 GUI ログの使用	598
テキスト メール ログの使用	598

テキスト メール ログのサンプル	599
テキスト メール ログ エントリの例	601
生成またはリライトされたメッセージ	603
スパム隔離へのメッセージの送信	603
NTP ログの使用	604
レポーティング ログの使用	604
レポーティング クエリー ログの使用	605
セーフリスト/ブロックリスト ログの使用	606
SMA ログの使用	606
ステータス ログの使用	607
システム ログの使用	610
トラッキング ログについて	610
ログ サブスクリプション	611
ログ サブスクリプションの設定	611
ログ レベルの設定	612
GUI でのログ サブスクリプションの作成	613
ログ サブスクリプションの編集	614
ロギングのグローバル設定	614
メッセージ ヘッダーのロギング	615
GUI を使用したロギングのグローバル設定	616
ログ サブスクリプションのロールオーバー	616
ログ サブスクリプション内のログのロールオーバー	616
GUI を使用したログの即時ロールオーバー	617
CLI を介したログの即時ロールオーバー	617
グラフィカル ユーザ インターフェイスでの最近のログ エントリの表示	617
最新のログ エントリの表示 (tail コマンド)	617
ホスト キーの設定	618

トラブルシューティング	621
システム情報の収集	621
ハードウェア問題のトラブルシューティング	621

機能の設定に関する問題のトラブルシューティング	622
一般的なトラブルシューティング リソース	622
特定の機能で発生する問題のトラブルシューティング	622
アラートへの応答	623
アラート：380 または 680 ハードウェアでバッテリー再学習タイムアウト (RAID イベント) (Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware)	623
追加のアラートの説明	624
テクニカル サポートの使用	624
アプライアンスからのサポート ケースのオープンおよび更新	624
仮想アプライアンスのサポートの取得	625
シスコのテクニカル サポート担当者のリモートアクセスの有効化	625
インターネット接続されたアプライアンスへのリモートアクセスの有効化	625
インターネットに直接接続されていないアプライアンスへのリモートアクセスの有効化	626
テクニカル サポートのトンネルの無効化	626
リモートアクセスの無効化	627
サポートの接続状態の確認	627
パケット キャプチャの実行	627
アプライアンスの電源のリモート リセット	629

## 付録 A :

<b>IP インターフェイスおよびアプライアンスへのアクセス</b>	<b>631</b>
IP インターフェイスおよびアプライアンスへのアクセス	631
IP インターフェイス	632
IP インターフェイスの設定	632
GUI を使用した IP インターフェイスの作成	633
FTP 経由でのアプライアンスへのアクセス	634
セキュア コピー (scp) アクセス	636
シリアル接続によるアクセス	636
80 および 90 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細	637
70 シリーズ ハードウェアでのシリアル ポートのピン割り当ての詳細	637

## 付録 B :

<b>ネットワークと IP アドレスの割り当て</b>	<b>639</b>
-----------------------------	------------

イーサネット インターフェイス	639
IP アドレスとネットマスクの選択	639
インターフェイス設定のサンプル	640
IP アドレス、インターフェイス、およびルーティング	641
要約	641
コンテンツ セキュリティ アプライアンスを接続するための戦略	642

---

付録 C :	<b>ファイアウォール情報</b>	643
	ファイアウォール情報	643

---

付録 D :	<b>Web セキュリティ管理の例</b>	649
	Web セキュリティ管理の例	649
	Web セキュリティ アプライアンスの例	649
	例 1 : ユーザの調査	649
	例 2 : URL のトラッキング	651
	例 3 : アクセス数の多い URL カテゴリの調査	652

---

付録 E :	<b>関連リソース</b>	655
	Cisco Notification Service	655
	資料	655
	サードパーティ コントリビュータ	656
	トレーニング	657
	ナレッジ ベースの記事	657
	シスコ サポート コミュニティ	657
	カスタマー サポート	657
	シスコ アカウントの登録	658
	マニュアルに関するフィードバック	658

---

付録 F :	<b>エンド ユーザ ライセンス契約書</b>	659
	Cisco Systems エンド ユーザ ライセンス契約書	659
	Cisco コンテンツ セキュリティ ソフトウェア用エンド ユーザ ライセンス契約補則	666





# 第 1 章

## はじめに

この章は、次の項で構成されています。

- [今回のリリースでの新機能 \(1 ページ\)](#)
- [Cisco コンテンツ セキュリティ管理の概要 \(3 ページ\)](#)

## 今回のリリースでの新機能

ここでは、AsyncOS for Cisco Content Security Management のこのリリースにおける新機能と拡張機能について説明します。リリースの詳細については、次の URL にある製品リリース ノート を参照してください。

<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html>。

アップグレードする場合、以前のリリースとこのリリースの間の他のリリースのリリース ノート も確認する必要があります。これは、これらのリリースで追加された機能および拡張機能を確認するためです。

表 1: AsyncOS 12.5 の新機能

機能	説明
新しいハードウェア モデルのサポート	シスコのコンテンツセキュリティ管理アプライアンス向け AsyncOS 12.5.0 リリースでは、次のハードウェア モデルをサポートしています。 <ul style="list-style-type: none"><li>• M195</li><li>• M395</li><li>• M695</li><li>• M695F</li></ul> 詳細については、 <a href="https://www.cisco.com/c/en/us/products/collateral/security/content-security-m%20anagement-appliance/datasheet_C78-721194.html">https://www.cisco.com/c/en/us/products/collateral/security/content-security-m%20anagement-appliance/datasheet_C78-721194.html</a> を参照してください。

機能	説明
設定マスターの複数のサブセットの管理	<p>特定のバージョンの設定マスターのサブセットを設定して、Web セキュリティアプライアンスのさまざまなポリシー設定を一元的に管理できるようになりました。</p> <p>詳細については、<a href="#">Web セキュリティアプライアンスの管理 (389 ページ)</a> を参照してください。</p>
ケースブックを使用した脅威分析の実行	<p>シスコのコンテンツセキュリティ管理アプライアンスには、ケースブックとピボットメニューのウィジェットが含まれるようになりました。</p> <p>(注) Microsoft Internet Explorer ブラウザを使用してアプライアンスにアクセスしている場合、[ケースブック (Casebook)] ウィジェットを使用することはできません。</p> <p>[ケースブック (Casebook)] ウィジェットと [ピボットメニュー (Pivot Menu)] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。</p> <ul style="list-style-type: none"> <li>観測対象をケースブックに追加し、脅威分析の調査を実行します。</li> <li>新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス (エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など) の監視対象をピボットし、脅威分析のために調査します。</li> </ul> <p>詳細については、<a href="#">Cisco Threat Response ポータルとの統合 (459 ページ)</a> を参照してください。</p>
Cisco Threat Response ポータルでアプライアンスを登録するときに Cisco Threat Response サーバを選択する機能	<p>アプライアンスを Cisco Threat Response ポータルに登録するときに、Cisco Threat Response ポータルにアプライアンスを接続するための Cisco Threat Response サーバを選択できるようになりました。</p> <p>このリリースでサポートされている Cisco Threat Response サーバは次のとおりです。</p> <ul style="list-style-type: none"> <li>米国 (api-sse.cisco.com)</li> <li>欧州 (api.eu.sse.itd.cisco.com)</li> </ul> <p>詳細については、<a href="#">Cisco Threat Response ポータルとの統合 (459 ページ)</a> を参照してください。</p>

機能	説明
新しい Web インターフェイスの[マイレポート (My Reports)] ページ	カスタムレポートページを作成するには、アプライアンスの新しい Web インターフェイスにある既存のすべての電子メールセキュリティ レポートからチャート (グラフ) とテーブルを構成します。 詳細については、 <a href="#">新しい Web インターフェイスでのレポートの使用 (39 ページ)</a> を参照してください。
新しい Web インターフェイスでのポリシー、ウイルス、およびアウトブレイク隔離の設定	アプライアンスの新しい Web インターフェイスから、ポリシー、ウイルス、またはアウトブレイク隔離を設定できるようになりました。 詳細については、 <a href="#">集約されたポリシー、ウイルス、およびアウトブレイク隔離 (355 ページ)</a> を参照してください。
Swagger UI を使用した API の管理	Swagger は、OpenAPI 仕様に基づいて構築された一連のオープンソースのツールです。 Swagger UI を使用すると、Web インターフェイスでの AsyncOS API リソースの設計と管理が容易になります。 詳細については、 <a href="#">セットアップ、インストール、および基本設定 (5 ページ)</a> を参照してください。
Web 使用状況分析のモニタリング	統計分析のために Web サイトの使用状況またはアクティビティの送信を有効または無効にすることができます。 詳細については、 <a href="#">一般的な管理タスク (503 ページ)</a> を参照してください。

## Cisco コンテンツ セキュリティ管理の概要

AsyncOS for Cisco Content Security Management には次の機能が統合されています。

- **外部スパム隔離**：エンドユーザ向けのスパム メッセージおよび疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- **集約ポリシー (Centralized Policy)、ウイルス (Virus)、アウトブレイク隔離 (Outbreak Quarantines)**：これらの隔離および隔離内に隔離されたメッセージを複数の E メールセキュリティアプライアンスから管理するための単一のインターフェイスを提供します。隔離されたメッセージをファイアウォールの背後に保存できます。
- **中央集中型レポート (Centralized reporting)**：複数の E メールおよび Web セキュリティアプライアンスからの集約データに関するレポートを実行します。個別アプライアンスで使用できる同じレポート機能を、セキュリティ管理アプライアンスでも使用できます。

- **中央集中型トラッキング (Centralized tracking)** : 単一のインターフェイスを使用して、メールメッセージを追跡すること、および複数の E メールおよび Web セキュリティ アプライアンスにより処理された Web トランザクションを追跡することができます。
- **Web セキュリティ アプライアンスの中央集中型構成管理 (Centralized Configuration Management for Web Security appliances)** : 簡易性および一貫性のため、複数の Web セキュリティ アプライアンスを対象にポリシー定義とポリシー導入を管理します。



---

(注) 中央集中型の電子メール管理、または E メールセキュリティ アプライアンスの「クラスタリング」にセキュリティ管理アプライアンスは含まれません。

---

- **中央集中型アップグレード管理 (Centralized Upgrade Management)** : 単一のセキュリティ管理アプライアンス (SMA) を使用して、複数の Web セキュリティ アプライアンス (WSA) を同時にアップグレードできます。
- **データのバックアップ (Backup of data)** : レポートリングデータ、トラッキングデータ、隔離されたメッセージ、安全な送信者とブロックされた送信者のリストなど、セキュリティ管理アプライアンスのデータをバックアップします。

1 台のセキュリティ管理アプライアンスからのセキュリティ操作を調整することも、複数のアプライアンス間に負荷を分散させることもできます。



## 第 2 章

# セットアップ、インストール、および基本設定

この章は、次の項で構成されています。

- [ソリューション導入の概要 \(5 ページ\)](#)
- [インストール計画 \(6 ページ\)](#)
- [セットアップの準備 \(8 ページ\)](#)
- [セキュリティ管理アプライアンスへのアクセス \(10 ページ\)](#)
- [Swagger UI を使用したセキュリティ管理アプライアンス API インターフェイスへのアクセス \(15 ページ\)](#)
- [システム セットアップ ウィザードの実行 \(15 ページ\)](#)
- [管理対象アプライアンスの追加について \(19 ページ\)](#)
- [セキュリティ管理アプライアンスでのサービスの設定 \(21 ページ\)](#)
- [設定変更のコミットおよび破棄 \(22 ページ\)](#)

## ソリューション導入の概要

Cisco コンテンツ セキュリティ ソリューションにサービスを提供する Cisco コンテンツ セキュリティ管理アプライアンスを設定するには、次の手順に従います。

	対象アプライアンス	操作手順	詳細情報
ステップ 1	すべてのアプライアンス	お使いのアプライアンスが、使用する機能のシステム要件を満たしていることを確認してください。必要に応じて、アプライアンスをアップグレードします。	

	対象アプライアンス	操作手順	詳細情報
ステップ 2	Eメールセキュリティアプライアンス	中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるようにすべてのEメールセキュリティアプライアンスを設定し、各アプライアンスですべての機能が予期したとおりに動作することを確認します。	Cisco Email Securityのご使用のリリースのマニュアルを参照してください。
ステップ 3 :	Webセキュリティアプライアンス	中央集中型サービスを環境に取り入れる前に、必要なセキュリティ機能が提供されるように少なくとも1つのWebセキュリティアプライアンスを設定し、すべての機能が予期したとおりに動作することを確認します。	『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。
ステップ 4	セキュリティ管理アプライアンス	アプライアンスを設定し、システムセットアップウィザードを実行します。	インストール計画 (6 ページ)、セットアップの準備 (8 ページ)、およびシステムセットアップウィザードの実行 (15 ページ) を参照してください。
ステップ 5	すべてのアプライアンス	導入する各中央集中型サービスを設定します。	セキュリティ管理アプライアンスでのサービスの設定 (21 ページ) から開始します。

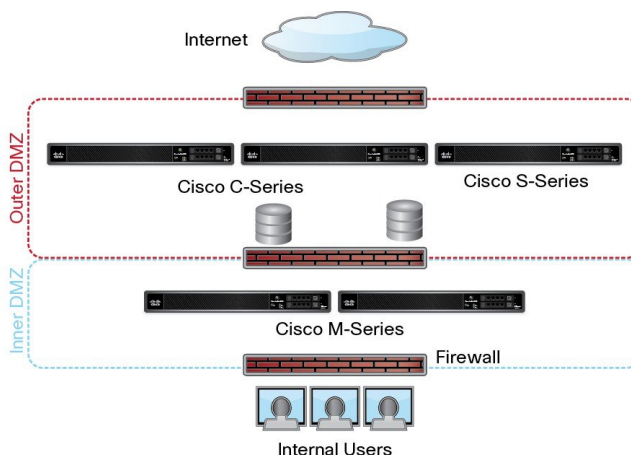
## インストール計画

- [ネットワーク プランニング \(6 ページ\)](#)
- [セキュリティ管理アプライアンスと Eメールセキュリティアプライアンスの統合について \(7 ページ\)](#)
- [クラスタ化された Eメールセキュリティアプライアンスを使用した展開 \(7 ページ\)](#)

## ネットワーク プランニング

セキュリティ管理アプライアンスの利用により、エンドユーザのアプリケーションと、非武装地帯 (DMZ) に存在するより安全なゲートウェイシステムを切り離すことができます。2 層ファイアウォールの使用によって、ネットワークプランニングの柔軟性が高まり、エンドユーザが外部 DMZ に直接接続することを防止できます。

図 1: セキュリティ管理アプライアンスを組み込んだ一般的なネットワーク設定



次の図は、セキュリティ管理アプライアンスと複数の DMZ を組み込んだ一般的なネットワーク設定を示しています。内部ネットワークで、DMZ の外側にセキュリティ管理アプライアンスを導入します。セキュリティ管理アプライアンス (M シリーズ) によって管理対象の E メールセキュリティアプライアンス (C シリーズ) と管理対象の Web セキュリティアプライアンス (S シリーズ) へのすべての接続が開始されます。

企業データセンターはセキュリティ管理アプライアンスを共有し、複数の Web セキュリティアプライアンスおよび E メールセキュリティアプライアンスの中央集中型レポートとメッセージトラッキング、および複数の Web セキュリティアプライアンスの集約ポリシー設定を実行できます。また、セキュリティ管理アプライアンスは外部スパム隔離として使用されます。

E メールセキュリティアプライアンスおよび Web セキュリティアプライアンスをセキュリティ管理アプライアンスに接続してすべてのアプライアンスを適切に設定した後、AsyncOS は管理対象アプライアンスからデータを収集して集約します。集約されたデータからレポートを作成できます。また、電子メールの全体像と Web の使用状況を判断できます。

## セキュリティ管理アプライアンスとEメールセキュリティアプライアンスの統合について

セキュリティ管理アプライアンスと E メールセキュリティアプライアンスの統合の詳細については、お使いの E メールセキュリティアプライアンスのユーザマニュアルまたはオンラインヘルプで、「Centralizing Services on a Cisco Content Security Management Appliance」の章を参照してください。

## クラスタ化されたEメールセキュリティアプライアンスを使用した展開

E メールアプライアンスの中央集中型管理機能を使用する E メールセキュリティアプライアンスのクラスタに、セキュリティ管理アプライアンスを配置することはできません。ただし、

クラスタ化された E メール セキュリティ アプライアンスは、中央集中型レポートイングとトラッキングのためにセキュリティ管理アプライアンスにメッセージを配信して隔離できます。

## セットアップの準備

システムセットアップ ウィザードを実行する前に、次の手順を実行してください。

- 
- ステップ 1 製品の最新リリース ノートを確認します。[ネットワーク プランニング \(6 ページ\)](#) を参照してください。
  - ステップ 2 セキュリティソリューションのコンポーネントに互換性があることを確認します。を参照してください。
  - ステップ 3 この導入に対応できるネットワークと物理的空間の準備があることを確認します。[インストール計画 \(6 ページ\)](#) を参照してください。
  - ステップ 4 セキュリティ管理アプライアンスを物理的にセットアップし、接続します。[アプライアンスの物理的なセットアップと接続 \(8 ページ\)](#) を参照してください。
  - ステップ 5 ネットワークアドレスと IP アドレスの割り当てを決定します。[ネットワークアドレスと IP アドレスの割り当ての決定 \(8 ページ\)](#) を参照してください。
  - ステップ 6 システムセットアップに関する情報を収集します。「[セットアップ情報の収集 \(9 ページ\)](#)」を参照してください。
- 

## アプライアンスの物理的なセットアップと接続

この章の手順を続行する前に、アプライアンスに付属するクイック スタートガイドに記載された手順を実行してください。このガイドでは、アプライアンスを梱包箱から取り出し、物理的にラックに取り付けて電源を投入済みであることを前提としています。

GUI にログインするには、PC とセキュリティ管理アプライアンスの間にプライベート接続を設定する必要があります。たとえば、付属するクロスケーブルを使用して、アプライアンスの管理ポートからラップトップに直接接続できます。任意で、PC とネットワーク間、およびネットワークとセキュリティ管理アプライアンスの管理ポート間をイーサネット接続（イーサネット ハブなど）で接続できます。

## ネットワーク アドレスと IP アドレスの割り当ての決定



- 
- (注) すでにアプライアンスをネットワークに配線済みの場合は、コンテンツ セキュリティ アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。各アプライアンスの管理ポートに事前に設定されている IP アドレスは、192.168.42.42 です。
-



設定後に、メインセキュリティ管理アプライアンスの [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページに移動し、セキュリティ管理アプライアンスが使用するインターフェイスを変更します。

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

- IP アドレス
- ネットマスク

さらに、ネットワーク全体に関する次の情報も必要になります。

- ネットワーク上のデフォルトのルータ (ゲートウェイ) の IP アドレス
- DNS サーバの IP アドレスおよびホスト名 (インターネットルートサーバを使用する場合は不要)
- NTP サーバのホスト名または IP アドレス (システム時刻を手動で設定する場合は不要)

詳細については、[ネットワークと IP アドレスの割り当て \(639 ページ\)](#) を参照してください。



(注) インターネットとコンテンツセキュリティアプライアンスの間でファイアウォールが稼働しているネットワークの場合は、アプライアンスを正常に機能させるために、特定のポートを開ける必要がある場合があります。ファイアウォールの詳細については、[ファイアウォール情報 \(643 ページ\)](#) を参照してください。

E メールセキュリティアプライアンスとの電子メールメッセージの送受信には、常にセキュリティ管理アプライアンスの同じ IP アドレスを使用します。説明については、使用している E メールセキュリティアプライアンスのマニュアルにあるメールフローに関する情報を参照してください。

Cisco コンテンツセキュリティ管理アプライアンスとその管理対象アプライアンス間の通信では、IPv6 はサポートされていません。

## セットアップ情報の収集

次の表を使用して、システムセットアップの情報を収集してください。システムセットアップウィザードを実行するときに、この情報を手元に用意する必要があります。



(注) ネットワークおよび IP アドレスの詳細については、[ネットワークと IP アドレスの割り当て \(639 ページ\)](#) を参照してください。

次の表は、システムセットアップワークシートを示しています

1	通知	システムアラートが送信される電子メールアドレス:
---	----	--------------------------

2	システム タイム		NTP サーバ (IP アドレスまたはホスト名) :
3	管理者パスワード		「admin」アカウントの新しいパスワードを選択します。
4	AutoSupport		AutoSupport を有効にする __ はい __ いいえ
5	ホストネーム		セキュリティ管理アプライアンスの完全修飾ホスト名 :
6	インターフェイス/IP アドレス		IPアドレス:
			ネットマスク :
7	ネットワーク	ゲートウェイ	デフォルト ゲートウェイ (ルータ) の IP アドレス :
		DNS	__ インターネットのルート DNS サーバを使用
			__ これらの DNS サーバを使用

## セキュリティ管理アプライアンスへのアクセス

セキュリティ管理アプライアンスには、標準の Web ベース グラフィカルユーザインターフェイス、スパム隔離を管理するための別個の Web ベース インターフェイス、コマンドライン インターフェイス、および特定の機能へのアクセス権が付与された管理ユーザ用の特別な、または制限付きの Web ベース インターフェイスがあります。

- [ブラウザ要件 \(10 ページ\)](#)
- [Web インターフェイスへのアクセスについて \(12 ページ\)](#)
- [Web インターフェイスへのアクセス \(12 ページ\)](#)
- [コマンドライン インターフェイスへのアクセス \(14 ページ\)](#)
- [サポートされる言語 \(14 ページ\)](#)

### ブラウザ要件

GUIにアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れるよう設定されている必要があります。さらに、Cascading Style Sheet (CSS) を含む HTML ページを描画できる必要があります。

表 2: サポートされるブラウザおよびリリース

ブラウザ	Windows 7	MacOS 10.6
Safari	—	7.0 以降
Google Chrome	最新の安定バージョン	最新の安定バージョン
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	最新の安定バージョン	最新の安定バージョン

- Internet Explorer 11.0 (Windows 7 のみ)
- Safari 7 以降
- Firefox (最新の安定バージョン)
- Google Chrome (最新の安定バージョン)

ブラウザは、そのブラウザの公式なサポート対象オペレーティング システムに対してのみサポートされます。

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

HTML ページのシームレスなナビゲーションとレンダリングのために、次のブラウザを使用してアプライアンスの新しい Web インターフェイス (AsyncOS 12.0 以降) にアクセスすることをお勧めします。

- Google Chrome (最新の安定バージョン)
- Mozilla Firefox (最新の安定バージョン)

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス (AsyncOS 12.0 以降) でサポートされている解像度は、1280x800 ~ 1680x1050 です。すべてのブラウザに対して最適に表示される解像度は 1440x900 です。



(注) シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

## Web インターフェイスへのアクセスについて

セキュリティ管理アプライアンスには、デフォルトではポート 80 で使用可能な標準管理者インターフェイスと、デフォルトではポート 82 で使用可能なスパム隔離エンドユーザインターフェイスの、2つの Web インターフェイスがあります。スパム隔離 HTTPS インターフェイスを有効にすると、デフォルトでポート 83 に設定されます。

各 Web インターフェイスを設定する際に HTTP または HTTPS を指定できるため（セキュリティ管理アプライアンス上で [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] に移動）、セッション中にそれらを切り替える場合は、再認証を要求される場合があります。たとえば、ポート 80 の HTTP を介して管理者 Web インターフェイスにアクセスし、次に同じブラウザでポート 83 の HTTPS を介してスパム隔離エンドユーザ Web インターフェイスにアクセスした場合、管理者 Web インターフェイスに戻るときに再認証を要求されます。



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

- デフォルトでは、30 分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。この場合、ユーザ名とパスワードを再入力する必要があります。タイムアウト制限を変更するには、[Web UI セッション タイムアウトの設定 \(497 ページ\)](#) を参照してください。

## Web インターフェイスへのアクセス

**ステップ 1** ブラウザを開き、アプライアンスの IP アドレスまたはホスト名を入力します。

**ステップ 2** (新しい Web インターフェイスのみ) 新しい Web インターフェイスには次のいずれかの方法でアクセスできます。

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

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

ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている先駆者の HTTPS ポートです。

`trailblazerconfig` CLI コマンドの詳細については、[trailblazerconfig コマンド \(566 ページ\)](#) を参照してください。

- `trailblazerconfig` CLI コマンドが無効になっているときは、URL (`https://example.com:<https-port>/ng-login`) を使用します  
ここで `example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。
- レガシー Web インターフェイスにログインし、**[クラウドEメールセキュリティ (Cloud Email Security) ]** をクリックして新しい外観を取得します。お試しください! リンクで新しい Web インターフェイスにアクセスできます。

- 重要**
- アプライアンスで AsyncOS API が有効になっていることを確認してください。
  - アプライアンスのレガシー Web インターフェイスにログインする必要があります。
  - `trailblazerconfig` が有効になっている場合は、設定済み HTTPS ポートがファイアウォールで開いている必要があります。デフォルトの HTTPS ポートは 4431 です。  
また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。
  - `trailblazerconfig` が無効になっている場合は、**[管理アプライアンス (Management Appliance) ]>[ネットワーク (Network) ]>[IP インターフェイス (IP Interfaces) ]** で設定された AsyncOS API ポートがファイアウォールで開きます。デフォルトの AsyncOS API HTTP/HTTPS ポートは 6080/6443 です。

**ステップ 3** 次のデフォルト値を入力します。

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

(注) Web インターフェイスまたはコマンドラインインターフェイスのいずれを使用した場合も、システム セットアップ ウィザードの完了後は、このパスフレーズが無効になります。

---

## レガシー Web インターフェイスへのアクセス



- (注) レガシー Web インターフェイスにアクセスするには、セキュリティ管理アプライアンスにログインする必要があります。詳細については、[Web インターフェイスへのアクセス \(12 ページ\)](#) を参照してください。

レポート、メッセージトラッキング、隔離、ネットワーク アクセス、およびシステム ステータスのモニタを有効にして設定するには、レガシー Web インターフェイスにアクセスする必要があります。

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

図 2: レガシー Web インターフェイスへのアクセス



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

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

## コマンドラインインターフェイスへのアクセス

上のコマンドラインインターフェイス (CLI) には、セキュリティ管理アプライアンスで、すべての Cisco コンテンツセキュリティ アプライアンス上での CLI アクセスと同じ方法でアクセスします。ただし、次のような違いがあります。

- システム セットアップは、GUI を使用して実行する必要があります。
- セキュリティ管理アプライアンスでは、一部の CLI コマンドを使用できません。サポートされていないコマンドのリストについては、『IronPort AsyncOS CLI Reference Guide for Cisco Content Security Appliances』を参照してください。

実動環境では、CLI にアクセスするために、SSH を使用する必要があります。ポート 22 でアプライアンスにアクセスするために、標準 SSH クライアントを使用します。ラボ展開の場合、Telnet も使用できますが、このプロトコルは暗号化されません。

## サポートされる言語

該当するライセンス キーを使用すると、AsyncOS では、次の言語で GUI および CLI を表示できます。

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

GUI とデフォルトのレポート言語を選択するには、次のいずれかを実行してください。

- 言語を設定します。 [プリファレンスの設定 \(582 ページ\)](#) を参照してください。

- GUI ウィンドウの右上にある [オプション (Options) ] メニューを使用して、セッションの言語を選択します。

(有効な方法は、ログイン資格情報の認証に使用する方法によって異なります)。

## Swagger UI を使用したセキュリティ管理アプライアンス API インターフェイスへのアクセス

Swagger UI を使用すると、アプライアンスの API リソースを視覚化して操作できます。これは API 仕様から自動的に生成されます。詳細については、<https://swagger.io/tools/swagger-ui/> を参照してください。

セキュリティ管理アプライアンスの新しい Web インターフェイスで Swagger UI にログインする場合、次のいずれかの方法を使用します。

- URL (<https://example.com:<trailblazer-https-port>/swagger>) を使用します

ここで、example.com はアプライアンスのホスト名で、<trailblazer-https-port> はアプライアンスで設定されている先駆者の HTTPS ポートです。



(注) Swagger UI にアクセスするには、アプライアンスで trailblazer の HTTPS ポートを有効にする必要があります。trailblazerconfig CLI コマンドの詳細については、[trailblazerconfig コマンド \(566 ページ\)](#) を参照してください。

- アプライアンスの新しい Web インターフェイスにログインします。右上隅の [?] ボタンをクリックして、ドロップダウンから [APIヘルプ: Swagger (API Help: Swagger) ] を選択します。Swagger UI が新しいブラウザ ウィンドウに開きます。

## システム セットアップ ウィザードの実行

AsyncOS には、システム設定を実行するための、ブラウザベースのシステムセットアップ ウィザードが用意されています。後で、ウィザードでは使用できないカスタム設定オプションを利用する場合があります。ただし、初期セットアップではウィザードを使用して、設定に漏れがないようにする必要があります。

セキュリティ管理アプライアンスでは、GUI を使用する場合のみ、このウィザードがサポートされます。コマンドラインインターフェイス (CLI) によるシステムセットアップはサポートされません。

- [はじめる前に \(16 ページ\)](#)
- [システム セットアップ ウィザードの概要 \(16 ページ\)](#)

## はじめる前に

[セットアップの準備 \(8 ページ\)](#) のすべてのタスクを実行します。



**注意** システム セットアップ ウィザードを使用すると、アプライアンスが完全に再設定されます。アプライアンスを最初にインストールする場合、または既存の設定を完全に上書きする場合にのみ、このウィザードを使用してください。

セキュリティ管理アプライアンスが、管理ポートからネットワークに接続されていることを確認します。



**注意** セキュリティ管理アプライアンスには、管理ポートに IP アドレス 192.168.42.42 がデフォルトで設定済みです。セキュリティ管理アプライアンスをネットワークに接続する前に、他の装置の IP アドレスが、この工場出荷時のデフォルト設定と競合していないことを確認してください。



(注) デフォルトでは、30分以上アイドル状態になっている場合、またはログアウトせずにブラウザを閉じた場合は、セッションがタイムアウトします。この場合、ユーザ名とパスワードを再入力する必要があります。システム セットアップ ウィザードを実行中にセッションがタイムアウトした場合は、最初からやり直す必要があります。タイムアウト制限を変更するには、[Web UI セッション タイムアウトの設定 \(497 ページ\)](#) を参照してください。

## システム セットアップ ウィザードの概要

**ステップ 1** [システム セットアップ ウィザードの起動 \(17 ページ\)](#)

**ステップ 2** [エンドユーザ ライセンス契約書の確認 \(17 ページ\)](#)

**ステップ 3** [システムの設定 \(17 ページ\)](#)

- 通知設定と AutoSupport
- システム時刻設定
- 管理者パスワード

**ステップ 4** [ネットワークの設定 \(18 ページ\)](#)

- アプライアンスのホスト名
- アプライアンスの IP アドレス、ネットワーク マスク、およびゲートウェイ
- デフォルト ルータと DNS 設定



## ステップ5 設定の確認 (19 ページ)

ウィザードの各ページを実行し、ステップ4で設定を慎重に確認します。[前へ (Previous)] をクリックすると、前の手順に戻ることができます。プロセスの最後に、変更を確定するようウィザードのプロンプトが表示されます。確定するまで、大部分の変更は有効になりません。

## ステップ6 次の手順 (19 ページ)

# システムセットアップウィザードの起動

ウィザードを起動するには、[Web インターフェイスへのアクセス \(12 ページ\)](#) の説明に従って GUI にログインします。GUI に初めてログインすると、デフォルトでは、システムセットアップウィザードの最初のページが表示されます。また、[システム管理 (System Administration)] メニューからシステムセットアップウィザードにアクセスすることもできます ([管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [システムセットアップウィザード (System Setup Wizard)] )。

## エンドユーザライセンス契約書の確認

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

## システムの設定

### システムアラート用の電子メールアドレスの入力

ユーザの介入を必要とするシステムエラーが発生した場合、AsyncOS では、電子メールでアラートメッセージが送信されます。アラートの送信先となる電子メールアドレス (複数可) を入力します。

システムアラート用の電子メールアドレスを1つ以上追加する必要があります。複数のアドレスを指定する場合は、カンマで区切ります。入力した電子メールアドレスでは、当初、すべてのレベルのすべてのタイプのアラートが受信されます。アラート設定は、後からカスタマイズできます。詳細については、[アラートの管理 \(541 ページ\)](#) を参照してください。

### 時間の設定

セキュリティ管理アプライアンス上のタイムゾーンを設定して、レポート、メッセージヘッダーおよびログファイルのタイムスタンプが正確になるようにします。ドロップダウンメニューを使用して時間帯を見つけるか、GMT オフセットによって時間帯を定義します。

システムクロック時刻は手動で設定することができますが、ネットワークタイムプロトコル (NTP) サーバを使用してネットワーク上またはインターネット上の他のサーバと時刻を同期することを推奨します。デフォルトでは、Cisco NTP サーバ ([time.sco.cisco.com](http://time.sco.cisco.com)) がコンテンツセキュリティアプライアンスで時刻を同期するためにエントリとして追加されました。NTP

サーバのホスト名を入力し、[エントリの追加 (Add Entry)] をクリックして追加の NTP サーバを設定します。詳細については、[システム時刻の設定 \(556 ページ\)](#) を参照してください。

## パスワードの設定

AsyncOS の admin アカウントのパスワード：adminpassphrase を変更する必要があります。パスワードは安全な場所に保管してください。パスワードの変更はすぐに有効になります。



- (注) パスワードの再設定後にシステム設定を取り消しても、パスワードの変更は元に戻りません。

## AutoSupport のイネーブル化

AutoSupport 機能 (デフォルトで有効) で、セキュリティ管理アプライアンスに関する問題をカスタマーサポートに通知することにより、最適なサポートを提供できます。詳細については、[Cisco AutoSupport \(543 ページ\)](#) を参照してください。

## ネットワークの設定

マシンのホスト名を定義し、ゲートウェイと DNS 設定値を設定します。



- (注) セキュリティ管理アプライアンスが、管理ポートを通してネットワークに接続されていることを確認します。

## ネットワーク設定 (Network Settings)

セキュリティ管理アプライアンスの完全修飾ホスト名を入力します。この名前は、ネットワーク管理者が割り当てる必要があります。

セキュリティ管理アプライアンスの IP アドレスを入力します。

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

次に、Domain Name Service (DNS) 設定値を設定します。AsyncOS には、インターネットのルートサーバに直接問い合わせできる、高性能な内部 DNS リゾルバ/キャッシュが組み込まれていますが、指定した DNS サーバを使用することもできます。独自のサーバを使用する場合は、各 DNS サーバの IP アドレスを指定する必要があります。システムセットアップウィザードを使用して入力できる DNS サーバは、4 台までです。



- (注) 指定した DNS サーバの初期プライオリティは 0 です。詳細については、[ドメインネームシステムの設定 \(551 ページ\)](#) を参照してください。



- (注) アプライアンスでは、着信接続に対して DNS ルックアップを実行するために、稼働中の DNS サーバへのアクセスが必要です。アプライアンスをセットアップするときに、アプライアンスからアクセス可能な稼働中の DNS サーバを指定できない場合は、[インターネットのルート DNSサーバを使用 (Use Internet Root DNS Servers)] を選択するか、管理インターフェイスの IP アドレスを一時的に指定することによってシステム セットアップ ウィザードを完了できます。

## 設定の確認

これで、入力した設定情報の要約がシステム セットアップ ウィザードに表示されます。変更する必要がある場合は、ページの下部にある [前へ (Previous)] をクリックし、情報を編集します。

情報を確認した後、[この設定をインストール (Install This Configuration)] をクリックします。次に、表示される確認ダイアログ ボックスで [インストール (Install)] をクリックします。

[この設定をインストール (Install This Configuration)] をクリックしてもページが反応しないように見える場合、その原因はウィザードで指定した新しい IP アドレスをアプライアンスが使用していることにあります。引き続きこのアプライアンスを使用するには、新しい IP アドレスを使用します。『Quick Start Guide』の手順に従い、新しいハードウェア アプライアンスにアクセスするために使用したコンピュータの IP アドレスを一時的に変更した場合は、まずコンピュータの IP アドレスを元の設定に戻します。

## 次の手順

セキュリティ管理アプライアンスをインストールし、システム セットアップ ウィザードを実行した後、アプライアンス上の他の設定を修正して、モニタリングサービスを設定できます。

システム セットアップ ウィザードを実行するためにアプライアンスにアクセスするときに使用したプロセスに基づき、[システムセットアップの次のステップ (System Setup Next Steps)] ページが表示されます。このページが自動的に表示されない場合、このページを表示するには [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [次のステップ (Next Steps)] を選択します。

[システムセットアップの次のステップ (System Setup Next Steps)] ページのいずれかのリンクをクリックして、Cisco コンテンツ セキュリティ アプライアンスの設定を続行します。

## 管理対象アプライアンスの追加について

各アプライアンスに対して最初の中央集中型サービスを設定するときに、管理対象の電子メールおよび Web セキュリティアプライアンスをセキュリティ管理アプライアンスに追加します。

リモートアプライアンスを追加すると、セキュリティ管理アプライアンスによって、リモートアプライアンスの製品名と追加するアプライアンスのタイプが比較されます。たとえば、[Web セキュリティアプライアンスの追加 (Add Web Security appliance)] ページを使用してア

アプライアンスを追加すると、そのアプライアンスは Web セキュリティ アプライアンスであって E メール セキュリティ アプライアンスではないことを確認するために、セキュリティ管理アプライアンスによってリモートアプライアンスの製品名がチェックされます。また、セキュリティ管理アプライアンスは、リモートアプライアンス上のモニタリングサービスをチェックして、それらが正しく設定され、互換性があることを確認します。

[セキュリティアプライアンス (Security Appliances)] ページには、追加した管理対象アプライアンスが表示されます。[接続が確立されていますか? (Connection Established?)] 列は、モニタリングサービスの接続が適切に設定されているかどうかを示します。

管理対象アプライアンスの追加方法は、次の手順に含まれています。

- [管理対象の各 E メール セキュリティ アプライアンスへの中央集中型電子メール レポート サービスの追加 \(57 ページ\)](#)
- [管理対象の各 E メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加 \(302 ページ\)](#)
- [管理対象の各 E メール セキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加 \(323 ページ\)](#)
- [管理対象の各 E メール セキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加 \(362 ページ\)](#)
- [管理対象の各 Web セキュリティ アプライアンスへの中央集中型 Web レポート サービスの追加 \(195 ページ\)](#)
- [Web Security Appliances の追加と Configuration Master のバージョンとの関連付け \(396 ページ\)](#)

## 管理対象アプライアンス設定の編集

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。

**ステップ 3** [セキュリティアプライアンス (Security Appliance)] セクションで、編集するアプライアンスの名前をクリックします。

**ステップ 4** アプライアンスの設定に必要な変更を行います。

たとえば、モニタリングサービスのチェックボックスをオンまたはオフにする、ファイル転送アクセスを再設定する、または IP アドレスを変更する、などの変更を行います。

(注) 管理対象アプライアンスの IP アドレスを変更すると、さまざまな問題が発生する可能性があります。Web セキュリティ アプライアンスの IP アドレスを変更すると、アプライアンスの公開履歴が失われ、スケジュールされた公開ジョブに対して Web セキュリティ アプライアンスが現在選択されていると、公開エラーが発生します。(割り当てられたすべてのアプライアンスを使用するように設定されたスケジュール済み公開ジョブは、影響を受けません)。E メールセキュリティ アプライアンスの IP アドレスを変更すると、アプライアンスのトラッキングアベイラビリティデータが失われます。

**ステップ 5** [送信 (Submit)] をクリックして、ページ上の変更を送信し、[変更を確定 (Commit Changes)] をクリックして変更を保存します。

## 管理対象アプライアンスのリストからのアプライアンスの削除

### 始める前に

リモートアプライアンスをセキュリティ管理アプライアンスから削除する前にそのアプライアンスで有効なすべての集約管理サービスを無効にする必要があります。たとえば、集約されたポリシー、ウイルス、アウトブレイク隔離サービスが有効な場合、E メールセキュリティアプライアンスでまずそのサービスを無効にする必要があります。電子メールまたはネットワークのセキュリティアプライアンスのマニュアルを参照してください。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。
- ステップ 3** [セキュリティアプライアンス (Security Appliances)] セクションで、削除する管理対象アプライアンスの行にあるゴミ箱アイコンをクリックします。
- ステップ 4** 確認のダイアログボックスで [削除 (Delete)] をクリックします。
- ステップ 5** 変更を送信し、保存します。

## セキュリティ管理アプライアンスでのサービスの設定

電子メールセキュリティサービス :

- [中央集中型の電子メールセキュリティ レポートの使用 \(55 ページ\)](#)
- [メッセージのトラッキング \(299 ページ\)](#)
- [スパム隔離 \(319 ページ\)](#)
- [集約されたポリシー、ウイルス、およびアウトブレイク隔離 \(355 ページ\)](#)

Web セキュリティ サービス :

- [集約されたポリシー、ウイルス、およびアウトブレイク隔離 \(355 ページ\)](#)
- [Web セキュリティ アプライアンスの管理 \(389 ページ\)](#)

## 設定変更のコミットおよび破棄

Cisco コンテンツセキュリティ管理アプライアンスの GUI で設定を変更した後、ほとんどの場合、変更を明示的にコミットする必要があります。

図 3: [変更を確定 (Commit Changes) ] ボタン

Commit Changes »

目的	操作手順
すべての保留中の変更をコミットする	ウィンドウの右上にあるオレンジ色の [変更を確定 (Commit Changes) ] ボタンをクリックします。変更内容の説明を追加し、[確定する (Commit) ] をクリックします。コミットが必要な変更を実行していない場合、[変更を確定 (Commit Changes) ] の代わりにグレーの [保留中の変更なし (No Changes Pending) ] ボタンが表示されます。
すべての保留中の変更を破棄する	ウィンドウの右上にあるオレンジ色の [変更を確定 (Commit Changes) ] ボタンをクリックし、[変更を破棄 (Abandon Changes) ] をクリックします。



(注) 古い Web インターフェイスでの構成変更は、ログアウトし、新しい Cisco コンテンツセキュリティ管理 Web インターフェイスにログインした後に、新しい Web インターフェイスで更新されます。

### 関連項目

- [以前コミットしたコンフィギュレーションへのロールバック \(563 ページ\)](#)



## 第 3 章

# レガシーWebインターフェイスでのレポートの使用

この章は、次の項で構成されています。

- [レポートデータの表示方法](#) (23 ページ)
- [セキュリティ管理アプライアンスによるレポート用データの収集方法](#) (24 ページ)
- [レポートデータのビューのカスタマイズ](#) (25 ページ)
- [レポートに含まれるメッセージやトランザクションの詳細の表示](#) (31 ページ)
- [電子メールレポートのパフォーマンスの向上](#) (31 ページ)
- [レポーティングデータおよびトラッキングデータのエクスポート](#) (33 ページ)
- [レポートおよびトラッキングにおけるサブドメインとセカンドレベルドメインの比較](#) (36 ページ)
- [すべてのレポートのトラブルシューティング](#) (36 ページ)
- [電子メールレポートおよび Web レポート](#) (37 ページ)

## レポートデータの表示方法

表 3: レポートデータの表示方法

目的	参照先
Web ベースのインタラクティブレポートページを表示およびカスタマイズする	<ul style="list-style-type: none"><li>• <a href="#">レポートデータのビューのカスタマイズ</a> (25 ページ)</li><li>• <a href="#">中央集中型の電子メールセキュリティレポーティングの使用</a> (55 ページ)</li><li>• <a href="#">集約されたポリシー、ウイルス、およびアウトブレイク隔離</a> (355 ページ)</li></ul>
PDF レポートまたは CSV レポートを自動的に繰り返し生成する	<ul style="list-style-type: none"><li>• <a href="#">メールレポートのスケジュール設定</a> (181 ページ)</li><li>• <a href="#">Web レポートのスケジュール設定</a> (273 ページ)</li></ul>

目的	参照先
PDF レポートまたは CSV レポートをオンデマンドで生成する	<ul style="list-style-type: none"> <li>• <a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a></li> <li>• <a href="#">オンデマンドでの Web レポートの生成 (277 ページ)</a></li> </ul>
raw データを CSV (カンマ区切り) ファイルとしてエクスポートする	<ul style="list-style-type: none"> <li>• <a href="#">レポーティング データおよびトラッキング データのエクスポート (33 ページ)</a></li> <li>• <a href="#">カンマ区切り (CSV) ファイルとしてのレポート データのエクスポート (35 ページ)</a></li> </ul>
レポート データの PDF を生成する	<a href="#">レポーティング データおよびトラッキング データのエクスポート (33 ページ)</a>
レポート情報を自分自身や他のユーザに電子メールで送信する	<ul style="list-style-type: none"> <li>• <a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a></li> <li>• <a href="#">メールレポートのスケジュール設定 (181 ページ)</a></li> <li>• <a href="#">オンデマンドでの Web レポートの生成 (277 ページ)</a></li> <li>• <a href="#">Web レポートのスケジュール設定 (273 ページ)</a></li> </ul>
特定のトランザクションに関する情報を検索する	<a href="#">レポートに含まれるメッセージやトランザクションの詳細の表示 (31 ページ)</a>



(注) ログイングとレポーティングの違いについては、[ログイングとレポーティング \(585 ページ\)](#) を参照してください。

## セキュリティ管理アプライアンスによるレポート用データの収集方法

セキュリティ管理アプライアンスは、約 15 分ごとにすべての管理対象アプライアンスからすべてのレポートのデータを取得し、これらのアプライアンスからのデータを集約します。アプライアンスによっては、個々のメッセージにセキュリティ管理アプライアンス上のレポーティング データを含める際に多少時間がかかる場合があります。データの詳細については、[システムステータス (System Status)] ページを確認してください。

レポーティング データには、IPv4 と IPv6 の両方に関するトランザクションが含まれます。





- (注) セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイムスタンプを適用します。セキュリティ管理アプライアンス上の時間設定の詳細については、[システム時刻の設定 \(556ページ\)](#) を参照してください。

## レポートデータの保存方法

すべてのアプライアンスでレポートのデータを格納します。次の表に、各アプライアンスがデータを格納する周期を示します。

表 4: Eメールセキュリティアプライアンスと Web セキュリティアプライアンスでのレポートデータの保存

	毎分	毎時	[毎日 (Daily)]	週1回	[月1回 (Monthly)]	年次
Eメールセキュリティアプライアンスまたは Web セキュリティアプライアンスでのローカルレポート	•	•	•	•	•	
Eメールセキュリティアプライアンスまたは Web セキュリティアプライアンスでの中央集中型レポート	•	•	•	•		
セキュリティ管理アプライアンス		•	•	•	•	•

## レポートングおよびアップグレードについて

新しいレポートング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。レポートングデータおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートをご参照ください。

## レポートデータのビューのカスタマイズ

Web インターフェイスでレポートデータを表示する場合、ビューをカスタマイズできます。

目的	操作手順
アプライアンスまたはレポートグループごとにデータを表示する	<a href="#">アプライアンスまたはレポートンググループのレポートデータの表示 (26 ページ)</a>
時間範囲を指定する	<a href="#">レポートの時間範囲の選択 (27 ページ)</a>
(Web レポートの場合) チャート化するデータを選択する	<a href="#">(Web レポートのみ) チャート化するデータの選択 (27 ページ)</a>

目的	操作手順
テーブルをカスタマイズする	<a href="#">レポート ページのテーブルのカスタマイズ (28 ページ)</a> を参照してください
表示する特定の情報またはデータのサブセットを検索する	<ul style="list-style-type: none"> <li>電子メールレポートについては、<a href="#">検索およびインタラクティブ電子メール レポート ページ (61 ページ)</a> です。</li> <li>Web レポートについては、ほとんどのテーブルの下方にある [検索 (Find) ] オプションまたは [フィルタ (Filter) ] オプションを探してください。</li> <li>一部のテーブルには、集約したデータの詳細へのリンク (青色のテキスト) が含まれます。</li> </ul>
レポート関連の設定を指定する	<a href="#">プリファレンスの設定 (582 ページ)</a> を参照してください
使用したいチャートと表だけを使ったカスタム レポートを作成する	<a href="#">カスタム レポート (28 ページ)</a> を参照してください。




(注) すべてのレポートにすべてのカスタマイズ機能を使用できるわけではありません。

## アプライアンスまたはレポーティンググループのレポートデータの表示

電子メールに関するメール フロー サマリーとシステム キャパシティのレポートについては、すべてのアプライアンスから、または中央で管理されている1台のアプライアンスからデータを表示できます。

電子メール レポートでは、[電子メール レポーティンググループの作成 \(58 ページ\)](#) の説明に従い E メール セキュリティ アプライアンスのグループを作成した場合、各レポーティンググループのデータを表示できます

ビューを指定するには、サポートされるページの [次のデータを参照 (View Data For) ] リストからアプライアンスまたはグループを選択します。

最近、別のセキュリティ管理アプライアンスからバックアップしたクラウド メール セキュリティ管理コンソールでレポートデータを表示している場合は、最初に、 > [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] で各アプライアンスを追加する必要があります (ただし、各アプライアンスとの接続は確立しないでください) 。

## レポートの時間範囲の選択

ほとんどの事前定義レポートページでは、含まれるデータの時間範囲を選択できます。選択した時間範囲は、[時間範囲 (Time Range)] メニューで異なる値を選択するまで、すべてのレポート ページに対して使用されます。

使用可能な時間範囲オプションは、アプライアンスごとに異なり、またセキュリティ管理アプライアンス上の電子メール レポーティングおよび Web レポーティングによって異なります。



(注) レポート ページの時間範囲は、グリニッジ標準時 (GMT) オフセットで表示されます。たとえば、太平洋標準時は、GMT + 7 時間 (GMT + 07:00) です。



(注) すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時 (GMT) オフセットで日付および時刻情報が表示されます。ただし、データエクスポートでは、世界の複数のタイムゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。



ヒント ログインするたびに常に表示する、デフォルトの時間範囲を指定できます。詳細については、[プリファレンスの設定 \(582 ページ\)](#) を参照してください。

## (Web レポートのみ) チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できない列もあります。

チャートには、関連付けられたテーブルに表示するように選択した項目 (行) 数に関係なく、テーブルの列の使用可能なすべてのデータが反映されます。

**ステップ 1** チャートの下の [チャートオプション (Chart Options)] をクリックします。

**ステップ 2** 表示するデータを選択します。

**ステップ 3** [完了 (Done)] をクリックします。

## レポート ページのテーブルのカスタマイズ

表 5: Web レポート ページのテーブルのカスタマイズ

目的	操作手順	詳細情報
<ul style="list-style-type: none"> <li>追加の列を表示する</li> <li>表示可能な列を非表示にする</li> <li>テーブルに使用可能な列を判断する</li> </ul>	<p>テーブルの下の [列 (Columns) ] リンクをクリックし、表示する列を選択して、[完了 (Done) ] をクリックします。</p>	<p>ほとんどのテーブルでは、デフォルトで一部の列が非表示になります。</p> <p>レポートページごとに、異なる列が提供されます。</p> <p><a href="#">電子メールレポートページ</a>の <a href="#">テーブルの列の説明 (68 ページ)</a> も参照してください。</p>
<p>テーブルの列の順序を変える</p>	<p>列の見出しを目的の位置までドラッグします。</p>	—
<p>選択した見出しでテーブルをソートする</p>	<p>列の見出しをクリックします。</p>	—
<p>表示するデータの行数を加減する</p>	<p>テーブルの右上にある [表示された項目 (Items Displayed) ] ドロップダウンリストから、表示する行数を選択します。</p>	<p>Web レポートの場合、デフォルトの表示行数を設定することもできます。 <a href="#">プリファレンスの設定 (582 ページ)</a> を参照してください。</p>
<p>可能な場合は、テーブルエントリの詳細を表示する</p>	<p>テーブル内の青色のエントリをクリックします。</p>	<p><a href="#">レポートに含まれるメッセージやトランザクションの詳細の表示 (31 ページ)</a> も参照してください。</p>
<p>データのプールを特定のサブセットに絞り込む</p>	<p>可能な場合は、テーブルの下のフィルタ設定で値を選択するか、入力します。</p>	<p>Web レポートの使用可能なフィルタについては、各レポートページの説明に記載されています。「<a href="#">[Web レポート (Web Reporting) ] ページの説明 (197 ページ)</a>」を参照してください。</p>

## カスタム レポート

既存のレポートページのチャート (グラフ) とテーブルを組み合わせ、カスタムの電子メールセキュリティ レポート ページを作成できます。



(注) Email Security Appliances のリリース 9.6 以降では、[マイレポート (My Reports) ] は [マイダッシュボード (My Dashboard) ] と呼ばれます。

目的	操作手順
カスタム レポート ページにモジュールを追加	<p>参照先：</p> <ul style="list-style-type: none"> <li>• <a href="#">カスタム レポートに追加できないモジュール (29 ページ)</a></li> <li>• <a href="#">カスタム レポート ページの作成 (30 ページ)</a></li> </ul>
カスタム レポート ページの表示	<ol style="list-style-type: none"> <li>1. [メール (Email)] &gt; [レポート (Reporting)] &gt; [マイレポート (My Reports)] を選択します。</li> <li>2. 表示する時間範囲を選択します。選択した時間範囲は [マイレポート (My Reports)] ページのすべてのモジュールを含むすべてのレポートに適用されます。</li> </ol> <p>新しく追加されたモジュールはカスタム レポートの上部に表示されます。</p>
カスタム レポート ページでのモジュールの再配置	目的の場所にモジュールをドラッグアンドドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。
カスタム レポートの CSV バージョンの生成	<p>参照先：</p> <ul style="list-style-type: none"> <li>• <a href="#">オンデマンドでのメール レポートの生成 (183 ページ)</a></li> <li>• <a href="#">オンデマンドでの Web レポートの生成 (277 ページ)</a></li> </ul>
カスタム レポートの CSV バージョンの定期的な生成	<p>参照先：</p> <ul style="list-style-type: none"> <li>• <a href="#">メール レポートのスケジュール設定 (181 ページ)</a></li> <li>• <a href="#">Web レポートのスケジュール設定 (273 ページ)</a></li> </ul>

## カスタム レポートに追加できないモジュール

- [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [システムステータス (System Status)] ページのすべてのモジュール
- [メール (Email)] > [レポート (Reporting)] > [有効なレポートデータ (Reporting Data Availability)] ページのすべてのモジュール
- [メール (Email)] > [メッセージ トラッキング (Message Tracking)] > [有効なメッセージ トラッキング データ (Message Tracking Data Availability)] ページのすべてのモジュール

- 送信者プロファイル詳細レポートのページからの、[SenderBase からの最新情報 (Current Information from SenderBase) ]、[送信者グループ情報 (Sender Group Information) ]、および [ネットワーク情報 (Network Information) ] といったドメイン単位のモジュール
- アウトブレイク フィルタ レポート ページの [過去 1 年間のウイルス アウトブレイク サマリー (Past Year Virus Outbreak Summary) ] チャートおよび [過去 1 年間のウイルス アウトブレイク (Past Year Virus Outbreaks) ] テーブル

## カスタム レポート ページの作成

### 始める前に

- 追加するモジュールが追加可能であることを確認します。 [カスタム レポートに追加できないモジュール \(29 ページ\)](#) を参照してください。
- モジュールの右上の [X] をクリックして、不要なデフォルト モジュールを削除します。

**ステップ 1** 以下のいずれかの方法でカスタム レポート ページにモジュールを追加します。

(注) 一部のモジュールは、以下のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- 追加するモジュールがある [メール (Email) ] タブまたはのレポート ページに移動し、モジュールの上部にある [+] ボタンをクリックします。
- [メール (Email) ] > [レポート (Reporting) ] > [マイレポート (My Reports) ] に移動し、いずれかのセクションの上部にある [+] [レポートモジュール (Report Module) ] ボタンをクリックしてから、追加するレポートモジュールを選択します。検索しているモジュールを表示するには、[マイレポート (My Reports) ] ページの各セクションの+[+] [レポートモジュール (Report Module) ] ボタンをクリックする必要があります。

各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

**ステップ 2** カスタマイズした (たとえば、カラムの追加、削除、または順序変更をした、あるいはチャートにデフォルト以外のデータを表示した) モジュールを追加する場合は、これらのモジュールを [マイレポート (My Reports) ] ページでカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

**ステップ 3** 別に凡例を持つチャート (たとえば、[概要 (Overview) ] ページからのグラフ) を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグアンドドロップします。

# レポートに含まれるメッセージやトランザクションの詳細の表示

**ステップ 1** レポート ページのテーブルにある青色の番号をクリックします

(一部のテーブルにのみ、これらのリンクはあります)。

この数に含まれるメッセージまたはトランザクションは[メッセージトラッキング (Message Tracking)] または [Webトラッキング (Web Tracking)] にそれぞれ表示されます。

**ステップ 2** メッセージまたはトランザクションのリストを表示するには、スクロール ダウンします。

## 次のタスク

- [メッセージのトラッキング \(299 ページ\)](#)

## 電子メール レポートのパフォーマンスの向上

月に固有のエントリが多数発生したことで、集約レポートのパフォーマンスが低下する場合は、レポートフィルタを使用して前年を対象としたレポート ([前年 (Last Year)] レポート) でのデータの集約を制限します。これらのフィルタにより、レポート内の詳細、個々の IP、ドメイン、またはユーザ データを制限できます。概要レポートおよびサマリー情報は、引き続きすべてのレポートで利用できます。

CLI で **reportingconfig > filters** のメニューを使用すると、1 つ以上のレポート フィルタを有効にできます。変更を有効にするには、変更をコミットする必要があります。

- [IP接続レベルの詳細 (IP Connection Level Detail)]。このフィルタを有効にすると、セキュリティ管理アプライアンスは、個々の IP アドレスに関する情報を記録しません。このフィルタは、攻撃による大量の着信 IP アドレスを処理するシステムに適しています。

このフィルタは、次の [前年 (Last Year)] レポートに影響を与えます。

- 受信メールの送信者プロファイル
- 受信メールの IP アドレス
- 送信メッセージ送信者の IP アドレス

- [ユーザの詳細 (User Detail)]。このフィルタを有効にすると、セキュリティ管理アプライアンスは、電子メールを送受信する個々のユーザ、およびユーザの電子メールに適用されるコンテンツ フィルタに関する情報を記録しません。このフィルタは、何百万もの内部ユーザの電子メールを処理するアプライアンス、またはシステムが受信者のアドレスを検証しない場合に適しています。

このフィルタは、次の [前年 (Last Year)] レポートに影響を与えます。

- 内部ユーザ
  - 内部ユーザの詳細
  - 送信メッセージ送信者の IP アドレス
  - コンテンツ フィルタ
- [メールトラフィックの詳細 (Mail Traffic Detail) ]。このフィルタを有効にすると、セキュリティ管理アプライアンスは、アプライアンスがモニタする個々のドメインおよびネットワークに関する情報を記録しません。このフィルタは、有効な着信または発信ドメインの数が数千万の単位で測定される場合に適しています。

このフィルタは、次の [前年 (Last Year) ] レポートに影響を与えます。

- 受信メールのドメイン
- 受信メールの送信者プロファイル
- 内部ユーザの詳細
- 送信メッセージ送信者のドメイン



---

(注) 過去1時間の最新のレポートデータを表示するには、個々のアプライアンスにログインして、そこでデータを表示する必要があります。

---



# レポートデータおよびトラッキングデータのエクスポート

表 6:新しい Web インターフェイスでのレポートデータおよびトラッキングデータのエクスポート

取得対象	CSV	操作手順	注記 (Notes)
raw データ  カンマ区切り (CSV) ファイルとしてのレポートデータのエクスポート (35 ページ) も参照してください。	•	<ol style="list-style-type: none"> <li>1. レポートページの上部にある [エクスポート (Export) ] リンクをクリックします。</li> <li>2. エクスポートする必要があるレポートモジュールを選択し、[ダウンロード (Download) ] をクリックします。</li> </ol>	CSV ファイルには、チャートや表で見ることのできるデータを含む、すべての適用可能なデータが含まれます。
	•	<p>スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。参照先：</p> <ul style="list-style-type: none"> <li>• <a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a></li> <li>• <a href="#">メールレポートのスケジュール設定 (181 ページ)</a></li> </ul>	<p>各 CSV ファイルには、最大 100 行を含めることができます。</p> <p>レポートに複数の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。</p> <p>一部の拡張レポートは、CSV 形式で使用できません。</p>

取得対象	CSV	操作手順	注記 (Notes)
<p>(Webセキュリティ) レポートデータのカスタムサブセット (特定のユーザ用のデータなど)。</p>	<ul style="list-style-type: none"> <li>•</li> </ul>	<ol style="list-style-type: none"> <li>1. [製品 (Product) ] ドロップダウンから [Web] を選択し、[トラッキング (Tracking) ] &gt; [Webトラッキング (Web Tracking) ] を選択します。</li> <li>2. 検索を実行し、検索結果の上にある [エクスポート (Export) ] リンクまたは [すべてをエクスポート (Export All) ] リンクをクリックします。</li> </ol>	<p>CSV ファイルには、検索条件に一致するすべての raw データが含まれます。</p>
<p>(電子メールセキュリティ) データのカスタムサブセット (特定のユーザ用のデータなど)。</p>	<ul style="list-style-type: none"> <li>•</li> </ul>	<ol style="list-style-type: none"> <li>1. [製品 (Product) ] ドロップダウンから [メール (Email) ] を選択し、[トラッキング (Tracking) ] &gt; [メッセージトラッキング (Message Tracking) ] を選択します。</li> <li>2. 検索を実行し、検索結果の上にある [エクスポート (Export) ] リンクまたは [すべてをエクスポート (Export All) ] リンクをクリックします。</li> </ol>	<p>[エクスポート (Export) ] リンクでは、表示された検索結果を使用して検索基準で指定された制限まで CSV ファイルをダウンロードします。</p> <p>[すべてをエクスポート (Export All) ] リンクでは、検索条件に一致する最大 50,000 件のメッセージを含む CSV ファイルをダウンロードします。</p> <p>ヒント : 50,000 件を超えるメッセージをエクスポートする必要がある場合は、短い時間範囲のエクスポートのセットを実行します。</p>

## カンマ区切り (CSV) ファイルとしてのレポート データのエクスポート

raw データをカンマ区切り (CSV) ファイルにエクスポートし、Microsoft Excel などのデータベースアプリケーションを使用してアクセスおよび処理できます。データをエクスポートするその他の方法については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

CSV エクスポートには raw データのみ含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります (そのデータが Web ベースのレポートで表示された場合でも、含まれていない場合があります)。

電子メール メッセージ トラッキングおよびレポート データについては、セキュリティ管理 アプライアンスに設定されている内容に関係なく、エクスポートした CSV データはすべて GMT で表示されます。これにより、特に複数のタイムゾーンのアプライアンスからデータを参照する場合に、アプライアンスとは関係なくデータを使用することが容易になります。

次の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間 (PDT) が GMT - 7 時間で表示されています。

Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100, 2625

表 7: raw データ エントリの表示

カテゴリ ヘッダー	値	説明
タイムスタンプ開始 (Begin Timestamp)	1159772400.0	エポックからの秒数で表されたクエリ開始時刻。
タイムスタンプ終了 (End Timestamp)	1159858799.0	エポックからの秒数で表されたクエリ終了時刻。
開始日 (Begin Date)	2006-10-02 07:00 GMT	クエリの開始日。
End Date	2006-10-03 06:59 GMT	クエリの終了日。
Name	Adware	マルウェア カテゴリの名前。
モニタリングされたトランザクション (Transactions Monitored)	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。

カテゴリ ヘッダー	値	説明
検出されたトランザクション (Transactions Detected)	2625	トランザクションの合計数： 検出されたトランザクション数 + ブロックされたトランザクション数。



- (注) カテゴリ ヘッダーは、レポートの種類ごとに異なります。ローカライズされた CSV データをエクスポートすると、ブラウザによってはヘッダーが正しくレンダリングされない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策としては、ローカルマシンにファイルを保存し、[ファイル (File)] > [開く (Open)] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

## レポートおよびトラッキングにおけるサブドメインとセカンドレベルドメインの比較

レポートおよびトラッキングの検索では、セカンドレベルのドメイン (<http://george.surbl.org/two-level-tlds> に表示されている地域ドメイン) は、ドメインタイプがサブドメインと同じように見えますが、サブドメインとは別の方法で処理されます。次に例を示します。

- レポートには、co.uk などの 2 レベルのドメインの結果は含まれませんが、foo.co.uk の結果は含まれます。レポートには、cisco.com などの主要な企業ドメインの下にサブドメインが含まれます。
- 地域ドメイン co.uk に対するトラッキング検索結果には、foo.co.uk などのドメインは含まれませんが、cisco.com に対する検索結果には subdomain.cisco.com などのサブドメインが含まれます。

## すべてのレポートのトラブルシューティング

- バックアップセキュリティ管理アプライアンスのレポート データを表示できない (36 ページ)
- レポートがディセーブルになっている (37 ページ)

## バックアップセキュリティ管理アプライアンスのレポート データを表示できない

問題

レポートデータを表示するのに、単一の E メールセキュリティ アプライアンスを選択できません。[次のデータを参照 (View Data For) ] オプションはレポート ページには表示されません。

#### ソリューション

「[バックアップ中のサービスのアベイラビリティ \(516 ページ\)](#)」も参照してください。

## レポーティングがディセーブルになっている

#### 問題

進行中のバックアップをキャンセルすると、レポーティングがディセーブルになる場合があります。

#### ソリューション

レポーティング機能は、バックアップが完了すると回復します。

## 電子メール レポートおよび Web レポート

電子メール レポートに固有の情報については、[中央集中型の電子メール セキュリティ レポーティングの使用 \(55 ページ\)](#) を参照してください。

Web レポートに固有の情報については、[中央集中型 Web レポーティングおよびトラッキングの使用 \(191 ページ\)](#) を参照してください。





## 第 4 章

# 新しい Web インターフェイスでのレポートの使用

この章は、次の項で構成されています。

- [レポートデータの表示方法 \(39 ページ\)](#)
- [セキュリティ管理アプライアンスによるレポート用データの収集方法 \(40 ページ\)](#)
- [インタラクティブ レポート ページの使用 \(41 ページ\)](#)
- [レポートデータのビューのカスタマイズ \(42 ページ\)](#)
- [\[マイ レポート \(My Reports\) \] ページ \(46 ページ\)](#)
- [レポートに含まれるメッセージやトランザクションの詳細の表示 \(49 ページ\)](#)
- [電子メール レポートのパフォーマンスの向上 \(49 ページ\)](#)
- [レポートングデータおよびトラッキングデータのエクスポート \(51 ページ\)](#)
- [すべてのレポートのトラブルシューティング \(54 ページ\)](#)

## レポート データの表示方法

次の表に、レポート データを表示するさまざまな方法を示します。

表 8: レポート データの表示方法

目的	参照先
Web ベースのインタラクティブ レポート ページを表示およびカスタマイズする	<ul style="list-style-type: none"><li>• <a href="#">インタラクティブ レポート ページの使用 (41 ページ)</a></li><li>• <a href="#">レポートデータのビューのカスタマイズ (42 ページ)</a></li><li>• <a href="#">中央集中型の電子メールセキュリティ レポートングの使用 (55 ページ)</a></li></ul>
反復する CSV レポートを自動的に生成する	<a href="#">メールレポートのスケジュール設定 (181 ページ)</a>

目的	参照先
CSV レポートをオンデマンドで生成する	<a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a>
raw データを CSV (カンマ区切り) ファイルとしてエクスポートする	<a href="#">レポーティング データおよびトラッキング データのエクスポート (33 ページ)</a> <a href="#">カンマ区切り (CSV) ファイルとしてのレポート データのエクスポート (35 ページ)</a>
レポート情報を自分自身や他のユーザに電子メールで送信する	<a href="#">メールレポートのスケジュール設定 (181 ページ)</a> <a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a>
特定のトランザクションに関する情報を検索する	<a href="#">レポートに含まれるメッセージやトランザクションの詳細の表示 (31 ページ)</a>



(注) ログイングとレポーティングの違いについては、[ログイングとレポーティング \(585 ページ\)](#) を参照してください。

## セキュリティ管理アプライアンスによるレポート用データの収集方法

セキュリティ管理アプライアンスは、約 15 分ごとにすべての管理対象アプライアンスからすべてのレポートのデータを取得し、これらのアプライアンスからのデータを集約します。アプライアンスによっては、個々のメッセージにセキュリティ管理アプライアンス上のレポーティング データを含める際に多少時間がかかる場合があります。データの詳細については、[システムステータス (System Status) ] ページを確認してください。

レポーティング データには、IPv4 と IPv6 の両方に関するトランザクションが含まれます。



(注) セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイムスタンプを適用します。セキュリティ管理アプライアンス上の時間設定の詳細については、[システム時刻の設定 \(556 ページ\)](#) を参照してください。



## レポートデータの保存方法

すべてのアプライアンスでレポートのデータを格納します。次の表に、各アプライアンスがデータを格納する周期を示します。

表 9: Eメールセキュリティアプライアンスでのレポートデータの保存

	毎分	毎時	【毎日 (Daily)】	週1回	【月1回 (Monthly)】	年次
Eメールセキュリティアプライアンスでのローカルレポート	•	•	•	•	•	
Eメールセキュリティアプライアンスで一元化されたレポート	•	•	•	•		
セキュリティ管理アプライアンス		•	•	•	•	•

## レポーティングおよびアップグレードについて

新しいレポーティング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。レポーティングデータおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

## インタラクティブレポートページの使用

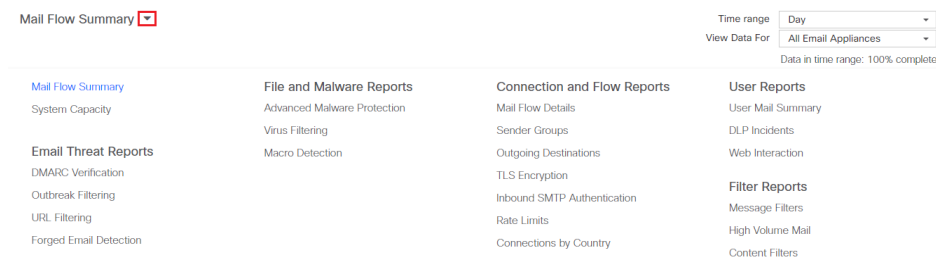
Web インターフェイス上部の [製品 (Product)] ドロップダウンを使用すると、Eメールセキュリティアプライアンスと Web セキュリティアプライアンスを切り替えることができます。

次の図に示す [レポート (Reports)] ドロップダウンを使用すると、Eメールおよび Web セキュリティアプライアンスのレポートを表示することができます。



(注) [メールフロー概要 (Mail Flow Summary)] レポート ページは、ランディング ページ (ログイン後に表示されるページ) です。

図 4: [レポート (Reports)] ドロップダウン



[レポート (Reports) ] ドロップダウンを使用すると、次の表に示すように分類された電子メール レポートおよび Web レポートを表示できます。

E メール セキュリティ アプライアンス	Web セキュリティ アプライアンス
<ul style="list-style-type: none"> <li>• 電子メール脅威のレポート</li> <li>• ファイルおよびマルウェアのレポート</li> <li>• 接続およびフローのレポート</li> <li>• ユーザ レポート</li> <li>• フィルタのレポート</li> </ul>	<ul style="list-style-type: none"> <li>• 一般的なレポート</li> <li>• 脅威レポート</li> </ul>

#### 関連項目

- [レポート データのビューのカスタマイズ \(42 ページ\)](#)
- [レポート ページのテーブルのカスタマイズ \(45 ページ\)](#)
- [\(Web レポートのみ\) チャート化するデータの選択 \(44 ページ\)](#)

## レポート データのビューのカスタマイズ

Web インターフェイスでのレポート データの表示中に、ビューをカスタマイズできます。

目的	操作手順
時間範囲を指定する	<a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
アプライアンスまたはレポートグループごとにデータを表示する	<a href="#">アプライアンスまたはレポートグループのレポートデータの表示 (26 ページ)</a> を参照してください
(Web レポートの場合) チャート化するデータを選択する	<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください
テーブルをカスタマイズする	<a href="#">レポート ページのテーブルのカスタマイズ (45 ページ)</a> を参照してください
(電子メールレポートの場合のみ) ビューをカスタマイズする	<a href="#">(電子メール レポートのみ) レポート ページでのビューのカスタマイズ (45 ページ)</a> を参照してください
カウンタを使用しての、トレンドグラフ上のデータのフィルタリング	<a href="#">カウンタを使用しての、トレンドグラフ上のデータのフィルタリング (46 ページ)</a> を参照してください

目的	操作手順
レポート関連の設定を指定する	<a href="#">プリファレンスの設定 (582 ページ)</a> を参照してください
表示する特定の情報またはデータのサブセットを検索する	<ul style="list-style-type: none"> <li>電子メールレポートについては、<a href="#">検索およびインタラクティブ電子メール レポート ページ (61 ページ)</a> を参照してください。</li> <li>Web レポートについては、ほとんどのテーブルの下方にある [検索 (Find) ] オプションまたは [フィルタ (Filter) ] オプションを探してください。</li> <li>一部のテーブルには、集約したデータの詳細へのリンク (青色のテキスト) が含まれます。詳細については、<a href="#">レポートに含まれるメッセージやトランザクションの詳細の表示 (31 ページ)</a> を参照してください。</li> </ul>
使用したいチャートと表だけを使ったカスタムレポートを作成する	<a href="#">[マイ レポート (My Reports) ] ページ (46 ページ)</a> を参照してください。




(注) すべてのレポートにすべてのカスタマイズ機能を使用できるわけではありません。

## アプライアンスまたはレポートグループのレポート データの表示

電子メールに関するメール フロー サマリーとシステム キャパシティのレポートについては、すべてのアプライアンスから、または中央で管理されている 1 台のアプライアンスからデータを表示できます。

電子メール レポートでは、[電子メール レポートグループの作成 \(58 ページ\)](#) の説明に従い E メール セキュリティ アプライアンスのグループを作成した場合、各レポートグループのデータを表示できます

ビューを指定するには、サポートされるページの [次のデータを参照 (View Data For) ] リストからアプライアンスまたはグループを選択します。

最近、別のセキュリティ管理アプライアンスからバックアップしたクラウド メール セキュリティ管理コンソールでレポート データを表示している場合は、最初に、 > [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] で各アプライアンスを追加する必要があります (ただし、各アプライアンスとの接続は確立しないでください) 。

## レポートの時間範囲の選択

ほとんどの事前定義レポートページでは、含まれるデータの時間範囲を選択できます。選択した時間範囲は、[時間範囲 (Time Range)] メニューで異なる値を選択するまで、すべてのレポートページに対して使用されます。

使用可能な時間範囲オプションは、アプライアンスごとに異なり、またセキュリティ管理アプライアンス上の電子メール レポーティングおよび Web レポーティングによって異なります。



(注) レポート ページの時間範囲は、グリニッジ標準時 (GMT) オフセットで表示されます。たとえば、太平洋標準時は、GMT + 7 時間 (GMT + 07:00) です。



(注) すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時 (GMT) オフセットで日付および時刻情報が表示されます。ただし、データエクスポートでは、世界の複数のタイムゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。



ヒント ログインするたびに常に表示する、デフォルトの時間範囲を指定できます。詳細については、[プリファレンスの設定 \(582 ページ\)](#) を参照してください。

## (Web レポートのみ) チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できない列もあります。

チャートには、関連付けられたテーブルに表示するように選択した項目 (行) 数に関係なく、テーブルの列の使用可能なすべてのデータが反映されます。

**ステップ 1** 特定のチャートで  をクリックします。




**ステップ 2** 表示する必要があるデータを選択します。チャートのプレビューは、選択したオプションに従って表示されます。

**ステップ 3** [Apply] をクリックします。

## (電子メール レポートのみ) レポート ページでのビューのカスタマイズ

ほとんどのレポート ページでは、グラフ ビュー、表ビュー、または統合ビューを選択できます。選択したビューは、レポート ページにデータを表示するために使用されます。


表 10: 電子メール レポート ページでのビューのカスタマイズ

目的	操作手順
データをグラフ ビューで表示する。	データをグラフ形式で表示するには、  をクリックします。
データを表ビューで表示する。	データを表形式で表示するには、  をクリックします。
可能な場合は、テーブルエントリの詳細を表示する	テーブル内の青色のエントリをクリックします。
統合ビューでデータを表示する。	データをグラフおよび表の形式で表示するには、  をクリックします。

## レポート ページのテーブルのカスタマイズ

レポート ページ内のインタラクティブ テーブルの情報を表示、カスタマイズ、ソートできます。選択したビューは、レポート ページにデータを表示するために使用されます。

表 11: レポート ページのテーブルのカスタマイズ

目的	操作手順	詳細情報
<ul style="list-style-type: none"> <li>追加の列を表示する</li> <li>表示可能な列を非表示にする</li> <li>テーブルに使用可能な列を判断する</li> </ul>	<ol style="list-style-type: none"> <li> をクリックします。</li> <li>表示する列を選択し、[閉じる (Close)] をクリックします。</li> </ol>	<p>ほとんどのテーブルでは、デフォルトで一部の列が非表示になります。</p> <p>レポート ページごとに、異なる列が提供されます。</p> <p>それぞれのテーブルのテーブル列の説明を参照してください。</p>
選択した見出しでテーブルをソートする	列の見出しをクリックします。	-
テーブルの列の順序を変える	列の見出しを目的の位置までドラッグします。	-

目的	操作手順	詳細情報
可能な場合は、テーブル エントリの詳細を表示する	テーブル内の青色のエントリをクリックします。	レポートに含まれるメッセージやトランザクションの詳細の表示 (31 ページ) も参照してください。
追加する行の詳細を表示します。	追加する行の詳細を表示するには、テーブルを下方向にスクロールします。	-
特定のサブセットにデータをフィルタリングする	可能な場合は、特定のテーブルの下にあるフィルタ設定で値を入力します。	Web レポートの使用可能なフィルタについては、各レポート ページの説明に記載されています。新しい Web インターフェイスの Web レポート ページの概要 (236 ページ) を参照してください。

## カウンタを使用する、トレンドグラフ上のデータのフィルタリング

トレンドグラフでは、必要な時間範囲および使用可能なカウンタに基づいてデータをフィルタリングすることができます。


[時間範囲 (Time Range) ] ドロップダウンで選択した時間範囲は、別の値を選択するまで、トレンドグラフ用に使用されます。

[メールフローの概要 (Mail Flow Summary) ] レポート ページのトレンドグラフ上のカウンタを使用して、異なるフィルタに固有のデータを表示できます。使用可能なカウンタをクリックすると、データがフィルタリングされます。

## [マイ レポート (My Reports) ] ページ

[マイレポート (My Reports) ] ページで、既存のすべての電子メールセキュリティ レポートからチャート (グラフ) とテーブルを組み合わせることでカスタム レポート ページを作成できます。

目的	操作手順
[マイレポート (My Reports) ] ページへのモジュールの追加	参照先 : <ul style="list-style-type: none"> <li>• [マイレポート (My Reports) ] ページに追加できないモジュール (47 ページ)</li> <li>• [マイレポート (My Reports) ] ページでのレポートの追加 (48 ページ)</li> </ul>

目的	操作手順
<p>[マイレポート (My Reports) ] ページの表示</p>	<ol style="list-style-type: none"> <li>[製品 (Product) ] ドロップダウンから [メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] &gt; [マイレポート (My Reports) ] を選択します。詳細については、<a href="#">インタラクティブレポートページの使用 (41 ページ)</a> を参照してください。</li> <li>表示する時間範囲を選択します。選択した時間範囲は、[マイレポート (My Reports) ] ページのすべてのモジュールを含め、すべてのレポートに適用されます。</li> </ol> <p>新しく追加されたモジュールはカスタムレポートの上部に表示されます。</p> <p>(注) 新しい Web インターフェイスの [マイレポート (My Reports) ] ページに追加するレポートモジュールは、レガシー Web インターフェイスで追加したレポートモジュールとは異なります。割り当てたユーザーロールによって異なる場合もあります。</p>
<p>[マイレポート (My Reports) ] ページでのモジュールの並べ替え</p>	<p>[マイレポート (My Reports) ] ページで、目的の場所にモジュールをドラッグ アンド ドロップします。</p>
<p>[マイレポート (My Reports) ] ページからのモジュールの削除</p>	<p>次のいずれかの方法で、[マイレポート (My Reports) ] ページからレポートモジュールを削除できます。</p> <ul style="list-style-type: none"> <li>目的のレポートモジュールの右上にある  をクリックします。</li> <li>[モニタリング (Monitoring) ] &gt; [マイレポート (My Reports) ] ページに移動し、[お気に入りの管理 (Manage Favorites) ] を選択して目的のレポートモジュールを削除します。</li> </ul>


## [マイレポート (My Reports) ] ページに追加できないモジュール

- [システムステータス (System Status) ] ページのすべてのモジュール。
- [有効なレポートデータ (Reporting Data Availability) ] ページのすべてのモジュール。
- [有効なメッセージトラッキングデータ (Message Tracking Data Availability) ] ページのすべてのモジュール。

- [送信者プロファイル (Sender Profile)] 詳細レポート ページのドメイン単位のモジュール ([SenderBaseからの最新情報 (Current Information from SenderBase)]、[送信者グループ情報 (Sender Group Information)]、および [ネットワーク情報 (Network Information)] )。
- [アウトブレイクフィルタ (Outbreak Filters)] レポート ページの [過去1年間のウイルスアウトブレイクサマリー (Past Year Virus Outbreak Summary)] チャートおよび [過去1年間のウイルスアウトブレイク (Past Year Virus Outbreaks)] テーブル。


## [マイレポート (My Reports)] ページでのレポートの追加

### 始める前に

- 追加するモジュールが追加可能であることを確認します。[[マイレポート \(My Reports\)\] ページに追加できないモジュール \(47 ページ\)](#) を参照してください。
- 不要なデフォルト モジュールを削除するには、そのモジュールの右上にある  をクリックします。

**ステップ 1** 次のいずれかの方法で、[マイレポート (My Reports)] ページにレポート モジュールを追加できます。

(注) 一部のモジュールは、以下のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- [レポート (Reports)] ドロップダウンのレポート ページに移動し、レポートモジュールの上部にある  をクリックします。
- レポート ページ上部の [レポート (Reports)] ドロップダウンから [お気に入りの管理 (Manage Favorites)] を選択します。

レポートモジュールは、電子メールレポートページのテーブルとチャートに従ってリストされます。必要なレポート モジュールを選択し、[追加 (Add)] をクリックして [マイレポート (My Reports)] ページに追加します。[マイレポート (My Report)] ページにレポートが表示されないようにするには、レポート モジュールを選択して [削除 (Remove)] をクリックします。

各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

(注) [マイレポート (My Reports)] ページには、最大 10 個のレポート モジュールを追加できません。

**ステップ 2** カスタマイズ (たとえば、カラムを追加、削除、並べ替えたり、チャートにデフォルト以外のデータを表示したり) したレポートモジュールを追加する場合は、これらのモジュールを [マイレポート (My Reports)] ページでカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。



**ステップ 3** 別個の凡例（たとえば、[メールフロー概要（Mail Flow Summary）] ページのグラフ）を含むチャートを追加する場合は、凡例を個別に追加します。必要に応じて、説明するデータの隣にドラッグアンドドロップします。

---

## レポートに含まれるメッセージやトランザクションの詳細の表示

---

**ステップ 1** レポート ページのテーブルにある青色の番号をクリックします

（一部のテーブルにのみ、これらのリンクはあります）。

この数に含まれるメッセージまたはトランザクションは[メッセージトラッキング（Message Tracking）]または[Webトラッキング（Web Tracking）]にそれぞれ表示されます。

**ステップ 2** メッセージまたはトランザクションのリストを表示するには、スクロール ダウンします。

---

### 次のタスク

- [メッセージのトラッキング（299 ページ）](#)

## 電子メール レポートのパフォーマンスの向上

月内に固有のエントリが多数発生したことで、集約レポートのパフォーマンスが低下する場合は、レポートフィルタを使用して前年を対象としたレポート（[前年（Last Year）] レポート）でのデータの集約を制限します。これらのフィルタにより、レポート内の詳細、個々の IP、ドメイン、またはユーザ データを制限できます。概要レポートおよびサマリー情報は、引き続きすべてのレポートで利用できます。

CLI で **reportingconfig > filters** のメニューを使用すると、1 つ以上のレポート フィルタを有効にできます。変更を有効にするには、変更をコミットする必要があります。

- [IP接続レベルの詳細（IP Connection Level Detail）]。このフィルタを有効にすると、セキュリティ管理アプライアンスは、個々の IP アドレスに関する情報を記録しません。このフィルタは、攻撃による大量の着信 IP アドレスを処理するシステムに適しています。

このフィルタは、次の [前年（Last Year）] レポートに影響を与えます。

- 受信メールの送信者プロファイル
  - 受信メールの IP アドレス
  - 送信メッセージ送信者の IP アドレス
- [ユーザの詳細（User Detail）]。このフィルタを有効にすると、セキュリティ管理アプライアンスは、電子メールを送受信する個々のユーザ、およびユーザの電子メールに適用され

るコンテンツ フィルタに関する情報を記録しません。このフィルタは、何百万もの内部ユーザの電子メールを処理するアプライアンス、またはシステムが受信者のアドレスを検証しない場合に適しています。

このフィルタは、次の [前年 (Last Year) ] レポートに影響を与えます。

- 内部ユーザ
  - 内部ユーザの詳細
  - 送信メッセージ送信者の IP アドレス
  - コンテンツ フィルタ
- [メールトラフィックの詳細 (Mail Traffic Detail) ]。このフィルタを有効にすると、セキュリティ管理アプライアンスは、アプライアンスがモニタする個々のドメインおよびネットワークに関する情報を記録しません。このフィルタは、有効な着信または発信ドメインの数が数千万の単位で測定される場合に適しています。

このフィルタは、次の [前年 (Last Year) ] レポートに影響を与えます。

- 受信メールのドメイン
- 受信メールの送信者プロファイル
- 内部ユーザの詳細
- 送信メッセージ送信者のドメイン



---

(注) 過去1時間の最新のレポートデータを表示するには、個々のアプライアンスにログインして、そこでデータを表示する必要があります。

---

# レポートデータおよびトラッキングデータのエキスポート

表 12: 新しい Web インターフェイスでのレポートデータおよびトラッキングデータのエキスポート

取得対象	CSV	操作手順	注記 (Notes)
raw データ  カンマ区切り (CSV) ファイルとしてのレポートデータのエキスポート (35 ページ) も参照してください。	•	<ol style="list-style-type: none"> <li>1. レポートページの上部にある [エキスポート (Export) ] リンクをクリックします。</li> <li>2. エクスポートする必要があるレポートモジュールを選択し、[ダウンロード (Download) ] をクリックします。</li> </ol>	CSV ファイルには、チャートや表で見ることのできるデータを含む、すべての適用可能なデータが含まれます。
	•	<p>スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。参照先：</p> <ul style="list-style-type: none"> <li>• <a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a></li> <li>• <a href="#">メールレポートのスケジュール設定 (181 ページ)</a></li> </ul>	<p>各 CSV ファイルには、最大 100 行を含めることができます。</p> <p>レポートに複数の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。</p> <p>一部の拡張レポートは、CSV 形式で使用できません。</p>

取得対象	CSV	操作手順	注記 (Notes)
(Webセキュリティ) レポートデータのカスタムサブセット (特定のユーザ用のデータなど)。	•	<ol style="list-style-type: none"> <li>1. [製品 (Product) ] ドロップダウンから [Web] を選択し、[トラッキング (Tracking) ] &gt; [Webトラッキング (Web Tracking) ] を選択します。</li> <li>2. 検索を実行し、検索結果の上にある [エクスポート (Export) ] リンクまたは [すべてをエクスポート (Export All) ] リンクをクリックします。</li> </ol>	CSV ファイルには、検索条件に一致するすべての raw データが含まれます。
(電子メールセキュリティ) データのカスタムサブセット (特定のユーザ用のデータなど)。	•	<ol style="list-style-type: none"> <li>1. [製品 (Product) ] ドロップダウンから [メール (Email) ] を選択し、[トラッキング (Tracking) ] &gt; [メッセージトラッキング (Message Tracking) ] を選択します。</li> <li>2. 検索を実行し、検索結果の上にある [エクスポート (Export) ] リンクまたは [すべてをエクスポート (Export All) ] リンクをクリックします。</li> </ol>	<p>[エクスポート (Export) ] リンクでは、表示された検索結果を使用して検索基準で指定された制限まで CSV ファイルをダウンロードします。</p> <p>[すべてをエクスポート (Export All) ] リンクでは、検索条件に一致する最大 50,000 件のメッセージを含む CSV ファイルをダウンロードします。</p> <p>ヒント : 50,000 件を超えるメッセージをエクスポートする必要がある場合は、短い時間範囲のエクスポートのセットを実行します。</p>

## カンマ区切り (CSV) ファイルとしてのレポート データのエクスポート

raw データをカンマ区切り (CSV) ファイルにエクスポートし、Microsoft Excel などのデータベースアプリケーションを使用してアクセスおよび処理できます。データをエクスポートするその他の方法については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

CSV エクスポートには raw データのみ含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります (そのデータが Web ベースのレポートで表示された場合でも、含まれていない場合があります)。

電子メール メッセージ トラッキングおよびレポート データについては、セキュリティ管理 アプライアンスに設定されている内容に関係なく、エクスポートした CSV データはすべて GMT で表示されます。これにより、特に複数のタイムゾーンのアプライアンスからデータを参照する場合に、アプライアンスとは関係なくデータを使用することが容易になります。

次の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間 (PDT) が GMT - 7 時間で表示されています。

Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100, 2625

表 13: raw データ エントリの表示

カテゴリ ヘッダー	値	説明
タイムスタンプ開始 (Begin Timestamp)	1159772400.0	エポックからの秒数で表されたクエリ開始時刻。
タイムスタンプ終了 (End Timestamp)	1159858799.0	エポックからの秒数で表されたクエリ終了時刻。
開始日 (Begin Date)	2006-10-02 07:00 GMT	クエリの開始日。
End Date	2006-10-03 06:59 GMT	クエリの終了日。
Name	Adware	マルウェア カテゴリの名前。
モニタリングされたトランザクション (Transactions Monitored)	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。

カテゴリ ヘッダー	値	説明
検出されたトランザクション (Transactions Detected)	2625	トランザクションの合計数： 検出されたトランザクション数 + ブロックされたトランザクション数。



- (注) カテゴリ ヘッダーは、レポートの種類ごとに異なります。ローカライズされた CSV データをエクスポートすると、ブラウザによってはヘッダーが正しくレンダリングされない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策としては、ローカルマシンにファイルを保存し、[ファイル (File)] > [開く (Open)] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

## すべてのレポートのトラブルシューティング

- [バックアップセキュリティ管理アプライアンスのレポートデータを表示できない \(36 ページ\)](#)
- [レポートがディセーブルになっている \(37 ページ\)](#)

### バックアップセキュリティ管理アプライアンスのレポート データを表示できない

#### 問題

レポートデータを表示するのに、単一の E メールセキュリティ アプライアンスを選択できません。[次のデータを参照 (View Data For)] オプションはレポート ページには表示されません。

#### ソリューション

「[バックアップ中のサービスのアベイラビリティ \(516 ページ\)](#)」も参照してください。

### レポートがディセーブルになっている

#### 問題

進行中のバックアップをキャンセルすると、レポートがディセーブルになる場合があります。

#### ソリューション

レポート機能は、バックアップが完了すると回復します。



## 第 5 章

# 中央集中型の電子メール セキュリティ レポートिंगの使用

この章は、次の項で構成されています。

- [中央集中型の電子メール レポートिंगの概要 \(55 ページ\)](#)
- [中央集中型の電子メール レポートिंगの設定 \(56 ページ\)](#)
- [電子メール レポート データの操作 \(59 ページ\)](#)
- [新しい Web インターフェイスでの電子メール レポート データの使用 \(60 ページ\)](#)
- [検索およびインタラクティブ電子メール レポート ページ \(61 ページ\)](#)
- [\[電子メール レポート \(Email Reporting\) \] ページの概要 \(62 ページ\)](#)
- [新しい Web インターフェイスの電子メール レポート ページの概要 \(113 ページ\)](#)
- [スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて \(175 ページ\)](#)
- [\[スケジュールされたレポート \(Scheduled Reports\) \] ページ \(181 ページ\)](#)
- [メール レポートのスケジュール設定 \(181 ページ\)](#)
- [オンデマンドでのメール レポートの生成 \(183 ページ\)](#)
- [\[アーカイブ メール レポート \(Archived Email Reports\) \] ページ \(185 ページ\)](#)
- [\[アーカイブ メール レポート \(Archived Email Reports\) \] の表示と管理 \(185 ページ\)](#)
- [メール レポートのトラブルシューティング \(186 ページ\)](#)

## 中央集中型の電子メール レポートिंगの概要

Cisco コンテンツセキュリティ管理アプライアンスは、電子メールのトラフィックパターンおよびセキュリティ リスクをモニタできるように、個別または複数の Email Security Appliances からの集計情報を示します。リアルタイムでレポートを実行して、特定の期間のシステムアクティビティをインタラクティブに表示することも、レポートをスケジュール設定して、定期的に行うこともできます。また、レポートング機能を使用して、raw データをファイルにエクスポートすることもできます。

この機能により、E メールセキュリティ アプライアンスの [モニタ (Monitor) ] メニューの下にリストされるレポートが集約されます。

中央集中型電子メールレポート機能は、概要レポートを生成してネットワークで起きていることを把握できるだけでなく、特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を、ドリルダウンして確認できます。

中央集中型トラッキング機能は、複数の Email Security Appliances を通過する電子メールメッセージの追跡を可能にします。



- (注) E メールセキュリティアプライアンスでデータが保存されるのは、ローカルレポート機能が使用される場合だけです。中央集中型レポートを E メールセキュリティアプライアンスに対してイネーブルにした場合、E メールセキュリティアプライアンスでは、システムキャパシティおよびシステムステータス以外のレポートデータは保持されません。中央集中型電子メールレポートがイネーブルでない場合、生成されるレポートはシステムステータスとシステムキャパシティだけです。

中央集中型レポートへの移行中および移行後のレポートデータのアベイラビリティの詳細については、お使いの E メールセキュリティアプライアンスのマニュアルまたはオンラインヘルプの「Centralized Reporting Mode」の項を参照してください。

## 中央集中型の電子メールレポートの設定

中央集中型電子メールレポートを設定するには、次の手順を順序どおりに実行します。

- [セキュリティ管理アプライアンスでの中央集中型電子メールレポートの有効化](#) (57 ページ)
- [管理対象の各 E メールセキュリティアプライアンスへの中央集中型電子メールレポートサービスの追加](#) (57 ページ)
- [E メールセキュリティアプライアンスでの中央集中型の電子メールレポートの有効化](#) (59 ページ)



- (注) レポート機能とトラッキングを常に同時にイネーブルにせず、レポート機能とトラッキングが適切に機能しない場合、または、レポート機能とトラッキングが各 E メールセキュリティアプライアンスで常に同時に集中管理またはローカル保存されない場合、レポートからドリルダウンしたときのメッセージトラッキングの結果は、予想した結果には一致しません。これは、各機能（レポート機能、トラッキング）のデータが、その機能が有効になっている間にもみキャプチャされるためです。



## セキュリティ管理アプライアンスでの中央集中型電子メールレポートの有効化

### 始める前に

- 中央集中型レポートを有効にする前に、すべての E メールセキュリティアプライアンスが設定され、想定どおりに動作している必要があります。
- 中央集中型電子メールレポートをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。[ディスク領域の管理 \(567 ページ\)](#) を参照してください。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [メール (Email)] > [集約管理レポート (Centralized Reporting)] を選択します。
- ステップ 3** [有効化 (Enable)] をクリックします。
- ステップ 4** システム セットアップ ウィザードを実行してから初めて中央集中型電子メールレポートをイネーブルにする場合は、エンドユーザー ライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 5** 変更を送信し、保存します。

(注) アプライアンスで電子メールレポートがイネーブルになっていて、この処理にディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型電子メールレポートが機能しません。電子メールレポートおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、レポートおよびトラッキングのデータは失われません。詳細については、[ディスク領域の管理 \(567 ページ\)](#) セクションを参照してください。

---

## 管理対象の各 E メールセキュリティアプライアンスへの中央集中型電子メールレポートサービスの追加

他の中央集中型管理機能を設定する際、すでにアプライアンスを追加したかどうかによって、ここでの手順は異なります。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。
- ステップ 3** このページのリストに、すでに E メールセキュリティアプライアンスを追加している場合は、次の手順を実行します。

- a) Eメールセキュリティアプライアンスの名前をクリックします。
- b) [集約管理レポート (Centralized Reporting)] サービスを選択します。

**ステップ4** Eメールセキュリティアプライアンスをまだ追加していない場合は、次の手順を実行します。

- a) [メールアプライアンスの追加 (Add Email Appliance)] をクリックします。
- b) [アプライアンス名 (Appliance Name)] および [IPアドレス (IP Address)] テキストフィールドに、セキュリティ管理アプライアンスの管理インターフェイスのアプライアンス名とIPアドレスを入力します。

(注) [IPアドレス (IP Address)] フィールドにDNS名を入力した場合でも、[送信 (Submit)] をクリックすると、IPアドレスに変換されます。

- c) [集約管理レポート (Centralized Reporting)] サービスがすでに選択されています。
- d) [接続の確立 (Establish Connection)] をクリックします。
- e) 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection)] をクリックします。

(注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開SSHキーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。

- f) 「Success」メッセージがページのテーブルの上に表示されるまで待機します。
- g) [テスト接続 (Test Connection)] をクリックします。
- h) テーブルの上のテスト結果を確認します。

**ステップ5** [送信 (Submit)] をクリックします。

**ステップ6** 中央集中型レポーティングを有効にする各Eメールセキュリティアプライアンスに対してこの手順を繰り返します。

**ステップ7** 変更を保存します。

## 電子メールレポーティンググループの作成

セキュリティ管理アプライアンスからのレポートデータを表示するための、Eメールセキュリティアプライアンスのグループを作成できます。

グループには1つ以上のアプライアンスを含めることができ、アプライアンスは複数のグループに所属できます。

### 始める前に

各アプライアンスで中央集中型レポーティングがイネーブルになっていることを確認します。[管理対象の各Eメールセキュリティアプライアンスへの中央集中型電子メールレポーティングサービスの追加 \(57ページ\)](#) を参照してください。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ]>[集約管理レポート (Centralized Reporting) ] を選択します。
- ステップ 3** [グループの追加 (Add Group) ] をクリックします。
- ステップ 4** グループの一意の名前を入力します。
- Eメールセキュリティアプライアンスのリストには、セキュリティ管理アプライアンスに追加した E メールセキュリティアプライアンスが表示されます。グループに追加するアプライアンスを選択します。
- 追加できるグループの最大数は、接続可能な電子メールアプライアンスの最大数以下です。
- (注) Eメールセキュリティアプライアンスをセキュリティ管理アプライアンスに追加したものの、それがリストに表示されない場合は、セキュリティ管理アプライアンスが Eメールセキュリティアプライアンスからレポートングデータを収集するように、その Eメールセキュリティアプライアンスの設定を編集します。
- ステップ 5** [追加 (Add) ] をクリックして、[グループメンバー (Group Members) ] リストにアプライアンスを追加します。
- ステップ 6** 変更を送信し、保存します。

## Eメールセキュリティアプライアンスでの中央集中型の電子メールレポートの有効化

管理対象の各 Eメールセキュリティアプライアンスで、中央集中型電子メールレポートングを有効にする必要があります。

手順については、お使いの Eメールセキュリティアプライアンスのマニュアルまたはオンラインヘルプで、「[Configuring an Email Security Appliance to Use Centralized Reporting](#)」のセクションを参照してください。

## 電子メールレポートデータの操作

- レポートデータのアクセスおよび表示に関するオプションについては、[レポートデータの表示方法 \(23 ページ\)](#) を参照してください。
- レポートデータのビューをカスタマイズするには、[レポートデータのビューのカスタマイズ \(25 ページ\)](#) を参照してください。
- データ内の特定の情報を検索するには、[検索およびインタラクティブ電子メールレポートページ \(61 ページ\)](#) を参照してください。

- レポート情報を印刷またはエクスポートするには、[レポーティングデータおよびトラッキングデータのエクスポート \(33 ページ\)](#) を参照してください。
- さまざまなインタラクティブレポートページを理解するには、[\[電子メールレポート \(Email Reporting\)\] ページの概要 \(62 ページ\)](#) を参照してください。
- レポートをオンデマンドで生成するには、[オンデマンドでのメールレポートの生成 \(183 ページ\)](#) を参照してください。
- 指定した間隔および時刻に自動的に実行されるようにレポートをスケジュール設定するには、[メールレポートのスケジュール設定 \(181 ページ\)](#) を参照してください。
- アーカイブしたオンデマンドのレポートおよびスケジュール設定したレポートを表示するには、[\[アーカイブ メール レポート \(Archived Email Reports\)\] の表示と管理 \(185 ページ\)](#) を参照してください。
- バックグラウンド情報については、[セキュリティ管理アプライアンスによるレポート用データの収集方法 \(24 ページ\)](#) を参照してください。
- 大量のデータを処理するときにパフォーマンスを向上させるには、[電子メールレポートのパフォーマンスの向上 \(31 ページ\)](#) を参照してください。
- チャートまたはテーブル内に青色のリンクとして表示されるエンティティまたは番号に関する詳細を取得するには、エンティティまたは番号をクリックします。

たとえば、この機能を使用してコンテンツフィルタリング、データ漏洩防止ポリシーに違反したメッセージの詳細を表示することができます（許可されている場合）。この場合、メッセージトラッキングで関連する検索が実行されます。下にスクロールして結果を表示します。

## 新しい Web インターフェイスでの電子メール レポート データの使用

- レポートデータのアクセスおよび表示に関するオプションについては、[レポートデータの表示方法 \(39 ページ\)](#) を参照してください。
- レポートデータのビューをカスタマイズするには、[レポートデータのビューのカスタマイズ \(42 ページ\)](#) を参照してください。
- レポート情報を印刷またはエクスポートするには、[レポーティングデータおよびトラッキングデータのエクスポート \(33 ページ\)](#) を参照してください。
- さまざまなインタラクティブレポートページを理解するには、[インタラクティブレポートページの使用 \(41 ページ\)](#) を参照してください。
- レポートをオンデマンドで生成するには、[オンデマンドでのメールレポートの生成 \(183 ページ\)](#) を参照してください。

- 指定した間隔および時刻に自動的に実行されるようにレポートをスケジュール設定するには、[メールレポートのスケジュール設定（181 ページ）](#)を参照してください。
- アーカイブしたオンデマンドのレポートおよびスケジュール設定したレポートを表示するには、[\[アーカイブ メール レポート \(Archived Email Reports\)\] の表示と管理（185 ページ）](#)を参照してください。
- バックグラウンド情報については、[セキュリティ管理アプライアンスによるレポート用データの収集方法（24 ページ）](#)を参照してください。
- 大量のデータを処理するときにパフォーマンスを向上させるには、[電子メールレポートのパフォーマンスの向上（31 ページ）](#)を参照してください。
- チャートまたはテーブル内に青色のリンクとして表示されるエンティティまたは番号に関する詳細を取得するには、エンティティまたは番号をクリックします。

たとえば、この機能を使用してコンテンツフィルタリング、データ漏洩防止ポリシーに違反したメッセージの詳細を表示することができます（許可されている場合）。この場合、メッセージトラッキングで関連する検索が実行されます。下にスクロールして結果を表示します。

## 検索およびインタラクティブ電子メールレポートページ

インタラクティブ電子メールレポートページの多くでは、ページの下部に[検索対象： (Search For:)] ドロップダウンメニューがあります。

ドロップダウンメニューから、次のような数種類の条件で検索できます。

- IP アドレス
- ドメイン
- ネットワーク オーナー
- 内部ユーザ
- 宛先ドメイン
- 内部送信者のドメイン
- 内部送信者の IP アドレス
- 着信 TLS ドメイン
- 発信 TLS ドメイン
- SHA-256

多くの検索では、検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか（たとえば、「ex」で始まる項目を検索する場合、「example.com」が一致します）を選択します。

IPv4 検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば、「17.\*」は 17.0.0.0～17.255.255.255 の範囲で検索されるので、17.0.0.1 は一致しますが、172.0.0.1 は一致しません。完全一致検索の場合は、4 つすべて

のオクテットを入力します。IPアドレス検索は、クラスレスドメイン間ルーティング (CIDR) 形式 (17.16.0.0/12) もサポートします。

IPv6 検索の場合、次の例の形式を使用して、アドレスを入力できます。

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

## [電子メール レポート (Email Reporting) ] ページの概要



- (注) このリストは、Eメールセキュリティ アプライアンス用 AsyncOS のサポートされている最新リリースで利用できるレポートを示します。Eメールセキュリティ アプライアンスで、これ以前のリリースの AsyncOS を実行している場合、これらのすべてのレポートは利用できません。

表 14: [電子メールレポート (Email Reporting) ] タブのオプション

[電子メールレポート (Email Reporting) ] メニュー	操作
[電子メール レポーティングの概要 (Email Reporting Overview) ] ページ	[概要 (Overview) ] ページには、お使いの Eメールセキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信メッセージに関するグラフやサマリーテーブルが含まれます。  詳細については、 <a href="#">[電子メール レポーティングの概要 (Email Reporting Overview) ] ページ (71 ページ)</a> を参照してください。
[受信メール (Incoming Mail) ] ページ	[受信メール (Incoming Mail) ] ページには、管理対象の Eメールセキュリティ アプライアンスに接続されているすべてのリモートホストのリアルタイム情報に関するインタラクティブなレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー (組織) の情報を収集できます。  詳細については、 <a href="#">[受信メール (Incoming Mail) ] ページ (76 ページ)</a> を参照してください。

[電子メールレポート (Email Reporting)] メニュー	操作
[送信者グループ (Sender Groups)] レポート ページ	<p>[送信者グループ (Sender Groups)] レポート ページには、送信者グループ別およびメールフローポリシーアクション別に接続の要約が表示され、SMTP 接続およびメールフローポリシーのトレンドを確認できます。</p> <p>詳細については、<a href="#">[送信者グループ (Sender Groups)] レポート ページ (81 ページ)</a> を参照してください。</p>
[送信者ドメインのレピュテーション (Sender Domain Reputation)] ページ	<p>このレポート ページでは、SDR サービスで受信した判定や脅威カテゴリに基づいて着信メッセージを表示できます。</p> <p>詳細については、<a href="#">[送信者ドメインのレピュテーション (Sender Domain Reputation)] ページ (81 ページ)</a> を参照してください。</p>
[送信先 (Outgoing Destinations)] ページ	<p>[送信先 (Outgoing Destinations)] ページには、組織がメールを送信する宛先ドメインについての情報が表示されます。ページの上部には、発信脅威メッセージごとの上位の宛先、および発信クリーンメッセージ別の上位の宛先を示すグラフが表示されます。ページの下部には、総受信者数別にソートされた (デフォルト設定) 列を示す表が表示されます。</p> <p>詳細については、<a href="#">[送信先 (Outgoing Destinations)] ページ (82 ページ)</a> を参照してください。</p>
[送信メッセージ送信者 (Outgoing Senders)] ページ	<p>[送信メッセージ送信者 (Outgoing Senders)] ページには、ネットワーク内の IP アドレスおよびドメインから送信された電子メールの数と種類についての情報が表示されます。</p> <p>詳細については、<a href="#">[送信メッセージ送信者 (Outgoing Senders)] ページ (83 ページ)</a> を参照してください。</p>
[内部ユーザ (Internal Users)] ページ	<p>[内部ユーザ (Internal Users)] には、電子メールアドレスごとに内部ユーザによって送受信された電子メールについての情報が表示されます。1人のユーザが複数の電子メールアドレスを持っている場合があります。レポートでは、電子メールアドレスがまとめられません。</p> <p>詳細については、<a href="#">[内部ユーザ (Internal Users)] ページ (84 ページ)</a> を参照してください。</p>
DLP インシデント	<p>[DLPインシデントサマリー (DLP Incident Summary)] ページには、送信メールで発生した Data Loss Prevention (DLP) ポリシー違反インシデントに関する情報が示されます。</p> <p>詳細については、<a href="#">DLP インシデント (86 ページ)</a> を参照してください。</p>

[電子メールレポート (Email Reporting) ] メニュー	操作
メッセージ フィルタ	<p>[メッセージフィルタ (Message Filters) ] ページには、送受信メッセージのメッセージフィルタの上位一致 (最も多くのメッセージに一致したメッセージ フィルタ) に関する情報が表示されます。</p> <p>詳細については、<a href="#">メッセージ フィルタ (88 ページ)</a> を参照してください。</p>
地理的分散	<p>[地理的分散 (Geo Distribution) ] ページには、次の情報が表示されます。</p> <ul style="list-style-type: none"> <li>• 発信国別の受信メール接続数の上位 (グラフィカルな形式)。</li> <li>• 発信国別の受信メール接続の合計数 (表形式)。</li> </ul> <p>詳細については、<a href="#">地理的分散 (88 ページ)</a> を参照してください。</p>
大容量のメール	<p>[大容量のメール (High Volume Mail) ] ページでは、1 人の送信者から送られていたり、件名が同じであったりする、特定の1時間の間に送られた多数のメッセージに関する攻撃が特定されます。</p> <p>詳細については、<a href="#">大容量のメール (88 ページ)</a> を参照してください。</p>
[コンテンツフィルタ (Content Filters) ] ページ	<p>[コンテンツフィルタ (Content Filters) ] ページには、送受信コンテンツ フィルタの上位一致 (最も多くのメッセージに一致したコンテンツ フィルタ) に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツフィルタ (Content Filters) ] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認できます。</p> <p>詳細については、<a href="#">[コンテンツフィルタ (Content Filters) ] ページ (89 ページ)</a> を参照してください。</p>
DMARC 検証	<p>[DMARC検証 (DMARC Verification) ] ページには、Domain-based Message Authentication, Reporting and Conformance (DMARC) 検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。</p> <p>詳細については、<a href="#">DMARC 検証 (90 ページ)</a> を参照してください。</p>



[電子メールレポート (Email Reporting)] メニュー	操作
マクロ検出	<p>[マクロ検出 (Macro Detection)] レポートページには、コンテンツフィルタまたはメッセージフィルタによって最も多く検出された、マクロが有効化された受信/発信添付ファイルがファイルタイプごとに表示されます。</p> <p>詳細については、<a href="#">マクロ検出 (90 ページ)</a> を参照してください。</p>
[外部脅威フィード (External Threat Feeds)] ページ	<p>[外部脅威フィード (External Threat Feeds)] ページには、次のレポートが表示されます。</p> <ul style="list-style-type: none"> <li>• メッセージで脅威を検出するために使用される上位 ETF ソース。</li> <li>• メッセージで検出された脅威に一致する上位 IOC。</li> <li>• 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソース。</li> </ul> <p>詳細については、<a href="#">[外部脅威フィード (External Threat Feeds)] ページ (91 ページ)</a> を参照してください。</p>
[ウイルス タイプ (Virus Types)] ページ	<p>[ウイルスタイプ (Virus Types)] ページでは、ネットワークで送受信されたウイルスの概要が示されます。[ウイルス タイプ (Virus Types)] ページには、Eメールセキュリティ アプライアンスで動作するウイルス スキャンエンジンによって検出され、セキュリティ管理アプライアンスに表示されるウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。</p> <p>詳細については、<a href="#">[ウイルス タイプ (Virus Types)] ページ (91 ページ)</a> を参照してください。</p>
[URL フィルタリング (URL Filtering)] ページ	<p>このページでは、メッセージ内で最も頻繁に生じる URL カテゴリ、スパム メッセージ内の最も一般的な URL、メッセージに表示される悪意のある URL およびニュートラル URL の数を確認します。</p> <p>詳細については、<a href="#">[URL フィルタリング (URL Filtering)] ページ (93 ページ)</a> を参照してください。</p>

[電子メールレポート (Email Reporting)] メニュー	操作
[Web インタラクション トラッキング (Web Interaction Tracking)] ページ	<p>ポリシーまたはアウトブレイク フィルタによって書き換えられた URL をクリックしたエンドユーザと、各ユーザクリックに関連付けられたアクションを識別します。</p> <p>詳細については、<a href="#">[Webインタラクショントラッキング (Web Interaction Tracking)] ページ (93 ページ)</a> を参照してください。</p>
[偽装メールの検出 (Forged Email Detection)] ページ	<p>[偽装メールの検出 (Forged Email Detection)] ページには、次のレポートが含まれています。</p> <ul style="list-style-type: none"> <li>偽装メールの検出数の上位。受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。</li> <li>偽装メールの検出：詳細。受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。</li> </ul> <p><a href="#">[偽装メールの検出 (Forged Email Detection)] ページ (95 ページ)</a> を参照してください。</p>
[高度なマルウェア防御 (ファイルレピュテーションとファイル分析) (Advanced Malware Protection (File Reputation and File Analysis))] レポート ページ	<p>ファイル レピュテーションおよび分析データは 3 つのレポート ページに表示されます。</p> <p>詳細については、<a href="#">[高度なマルウェア防御 (ファイルレピュテーションとファイル分析) (Advanced Malware Protection (File Reputation and File Analysis))] レポート ページ (95 ページ)</a> を参照してください。</p>
メールボックスの自動修復	<p>メールボックスの修復結果の詳細を表示するには、このページを使用します。</p> <p><a href="#">メールボックスの自動修復 (102 ページ)</a> を参照してください。</p>
[TLS 接続 (TLS Connections)] ページ	<p>[TLS接続 (TLS Connections)] ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。</p> <p>詳細については、<a href="#">[TLS 接続 (TLS Connections)] ページ (103 ページ)</a> を参照してください。</p>

[電子メールレポート (Email Reporting)] メニュー	操作
[受信 SMTP 認証 (Inbound SMTP Authentication)] ページ	[受信SMTP認証 (Inbound SMTP Authentication)] ページには、クライアント証明書の使用情報、および Email Security Appliance とユーザのメールクライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。  詳細については、 <a href="#">[受信 SMTP 認証 (Inbound SMTP Authentication)] ページ (104 ページ)</a> を参照してください。
[アウトブレイク フィルタ (Outbreak Filters)] ページ	[アウトブレイクフィルタ (Outbreak Filters)] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する防御をモニタします。  詳細については、 <a href="#">[アウトブレイクフィルタ (Outbreak Filters)] ページ (105 ページ)</a> を参照してください。
[レート制限 (Rate Limits)] ページ	[レート制限 (Rate Limits)] ページには、送信者あたりのメッセージ受信者数に対して設定したしきい値を超える電子メール送信者 (MAIL-FROM アドレスに基づく) が表示されます。  詳細については、 <a href="#">[レート制限 (Rate Limits)] ページ (105 ページ)</a> を参照してください。
[システム容量 (System Capacity)] ページ	レポートデータを送信するセキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。  詳細については、 <a href="#">[システム容量 (System Capacity)] ページ (109 ページ)</a> を参照してください。
[有効なレポートデータ (Reporting Data Availability)] ページ	各アプライアンスのセキュリティ管理アプライアンス上のレポートデータの影響を把握できます。詳細については、 <a href="#">[有効なレポートデータ (Reporting Data Availability)] ページ (113 ページ)</a> を参照してください。
メールレポートのスケジュール設定	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、 <a href="#">メールレポートのスケジュール設定 (181 ページ)</a> を参照してください。
[アーカイブ メール レポート (Archived Email Reports)] の表示と管理	アーカイブ済みのレポートを表示および管理できます。詳細については、 <a href="#">[アーカイブ メール レポート (Archived Email Reports)] の表示と管理 (185 ページ)</a> を参照してください。  また、オンデマンドレポートを生成することもできます。「 <a href="#">オンデマンドでのメールレポートの生成 (183 ページ)</a> 」を参照してください。

## 電子メール レポートの生成 ページのテーブルの列の説明

表 15: 電子メール レポートの生成 ページのテーブルの列の説明

列名	
受信メールの詳細	
[拒否された接続 (Connections Rejected) ]	HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。
[承認された接続 (Connections Accepted) ]	受け入れられたすべての接続。
[試行回数の合計 (Total Attempted) ]	すべての受け入れられた接続試行と、拒否された接続試行。
[受信者スロットルによる停止 (Stopped by Recipient Throttling) ]	これは、レピュテーションフィルタリングによる阻止の 1 要素です。HAT 上限値 (1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数) のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ] が算出されます。

列名	
[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ]	<p>[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ]の値は、次の複数の要素に基づいて算出されます。</p> <ul style="list-style-type: none"> <li>• この送信者からの「数が絞り込まれた」メッセージの数</li> <li>• 拒否された、または TCP 拒否の接続数 (部分的に集計されます)</li> <li>• 接続ごとのメッセージ数に対する控えめな乗数</li> </ul> <p>アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。</p> <p>(注) [概要 (Overview) ]ページの[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ]の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。</p>
[無効な受信者の場合に停止 (Stopped as Invalid Recipients) ]	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
[スパム検出 (Spam Detected) ]	検出されたすべてのスパム。
[ウイルス検出 (Virus Detected) ]	検出されたすべてのウイルス。
コンテンツフィルタによる阻止	コンテンツ フィルタによって阻止されたメッセージの総数。
合計脅威件数 (Total Threat)	脅威メッセージ (評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの) の総数
Marketing	不要なマーケティングメッセージとして検出されたメッセージの数。

列名	
クリーン (Clean)	すべてのクリーン メッセージ。 グレイメール機能が有効になっていないアプリケーションで処理されるメッセージは、クリーンとして集計されます。
<b>ユーザメールフローの詳細 ([内部ユーザ (Internal Users) ] ページ)</b>	
[受信スパム検出 (Incoming Spam Detected) ]	検出されたすべての着信スパム。
[受信ウイルス検出 (Incoming Virus Detected) ]	検出された着信ウイルス。
[受信コンテンツフィルタの一致数 (Incoming Content Filter Matches) ]	検出された着信コンテンツ フィルタの一致。
[コンテンツフィルタによる受信停止 (Incoming Stopped by Content Filter) ]	設定されていたコンテンツ フィルタのために阻止された着信メッセージ。
[正常な受信 (Incoming Clean) ]	すべての着信クリーン メッセージ。
[送信スパム検出 (Outgoing Spam Detected) ]	検出された発信スパム。
[送信ウイルス検出 (Outgoing Virus Detected) ]	検出された発信ウイルス。
[送信コンテンツフィルタの一致数 (Outgoing Content Filter Matches) ]	検出された発信コンテンツ フィルタの一致。
[コンテンツフィルタによる送信停止 (Outgoing Stopped by Content Filter) ]	設定されていたコンテンツ フィルタのため阻止された発信メッセージ。
[正常な送信 (Outgoing Clean) ]	すべての発信クリーン メッセージ。
<b>受信および送信TLS接続 ([TLS接続 (TLS Connections) ] ページ)</b>	
[必要なTLS : 失敗 (Required TLS: Failed) ]	失敗した、必要なすべての TLS 接続。
[必要なTLS : 成功 (Required TLS: Successful) ]	成功した、必要なすべての TLS 接続。
[優先するTLS : 失敗 (Preferred TLS: Failed) ]	失敗した、優先するすべての TLS 接続。
[優先するTLS : 成功 (Preferred TLS: Successful) ]	成功した、優先するすべての TLS 接続。
[総接続数 (Total Connections) ]	TLS 接続の合計数。
[合計メッセージ数 (Total Messages) ]	TLS メッセージの総数。
<b>アウトブレイク フィルタ</b>	
[アウトブレイク名 (Outbreak Name) ]	アウトブレイクの名前。

列名	
[アウトブレイクID (Outbreak ID)]	アウトブレイク ID。
[最初にグローバルで確認した日時 (First Seen Globally)]	ウイルスが最初にグローバルに発見された時刻。
[保護時間 (Protection Time)]	ウイルスから保護されていた時間。
[隔離されたメッセージ (Quarantined Messages)]	隔離に関するメッセージ。

## [電子メールレポートの概要 (Email Reporting Overview)] ページ

セキュリティ管理アプライアンスの [メール (Email)] > [レポート (Reporting)] > [概要 (Overview)] ページには、お使いの E メールセキュリティアプライアンスからの電子メールメッセージアクティビティの概要が表示されます。[概要 (Overview)] ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

概要レベルの [概要 (Overview)] ページに、送受信メールのグラフと送受信メールのサマリーが表示されます。

メールトレンドグラフは、メールフローを視覚的に表したものです。このページのメールトレンドグラフを使用して、アプライアンスを行き来するすべてのメールの流れをモニタできます。



- (注) [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートおよび [エグゼクティブサマリー (Executive Summary)] レポートは、[\[電子メールレポートの概要 \(Email Reporting Overview\)\] ページ \(71 ページ\)](#) に基づきます。詳細については、[\[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\)\] レポート \(177 ページ\)](#) および [\[エグゼクティブサマリー \(Executive Summary\)\] レポート \(181 ページ\)](#) を参照してください。

表 16: [メール (Email)] > [レポート (Reporting)] > [概要 (Overview)] ページの詳細

セクション	説明
時間範囲	表示する時間範囲を選択するためのオプションを伴うドロップダウンリスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。

セクション	説明
[次のデータを参照 (View Data for)]	[概要 (Overview)] のデータを表示する E メールセキュリティ アプライアンスを選択するか、[全Eメールアプライアンス (All Email Appliances)] を選択します。  「アプライアンスまたはレポート グループのレポート データの表示 (26 ページ)」も参照してください。

## 受信メール メッセージのカウント方法

受信メッセージの数は、メッセージごとの受信者数に応じて異なります。たとえば、example.com から 3 人の受信者に送信された着信メッセージは、その送信者からの 3 通のメッセージとしてカウントされます。

送信者レピュテーションフィルタリングによってブロックされたメッセージは、実際にはワークキューに入らないので、アプライアンスは、受信メッセージの受信者のリストにアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数は既存の顧客データの大規模なサンプリング調査に基づいています。

## アプライアンスによる電子メール メッセージの分類方法

メッセージは電子メールパイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、メッセージにスパム陽性またはウイルス陽性というマークを付けることができます。コンテンツフィルタに一致させることもできます。各種フィルタとスキャンアクティビティの優先順位は、メッセージ処理の結果に大きく影響します。

上記の例では、各種判定は次の優先ルールに従います。

- スパム陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

これらのルールに従って、メッセージがスパム陽性とマークされた場合、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されていれば、このメッセージがドロップされてスパム カウンタが増分します。

さらに、スパム陽性のメッセージを引き続き電子メールパイプラインで処理するようにアンチスパム設定が設定されている場合、以降のコンテンツフィルタがこのメッセージをドロップ、バウンス、または隔離しても、スパム カウンタは増分します。メッセージがスパム陽性またはウイルス陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

また、メッセージがアウトブレイクフィルタによって隔離された場合、隔離からリリースされてワーク キューで再度処理されるまで集計されません。

メッセージ処理の優先順位の詳細については、お使いの E メールセキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドで、電子メールパイプラインに関する章を参照してください。



## [概要 (Overview)] ページでの電子メールメッセージの分類

[概要 (Overview)] レポート ページの [受信メールサマリー (Incoming Mail Summary)] でレポートされるメッセージは、次のように分類されています。

表 17: [概要 (Overview)] ページの電子メールのカテゴリ

カテゴリ (Category)	説明
レピュテーションフィルタによる停止	<p>HAT ポリシーによってブロックされたすべての接続数に、固定乗数 (<a href="#">受信メールメッセージのカウント方法 (72 ページ)</a>) を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。</p> <p>[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering)] の値は、次の複数の要素に基づいて算出されます。</p> <ul style="list-style-type: none"> <li>この送信者からの「数が絞り込まれた」メッセージの数</li> <li>拒否された、または TCP 拒否の接続数 (部分的に集計されます)</li> <li>接続ごとのメッセージ数に対する控えめな乗数</li> </ul> <p>アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。</p> <p>[概要 (Overview)] ページの [レピュテーションフィルタによる停止 (Stopped by Reputation Filtering)] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。</p>
無効な受信者数	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
検出されたスパムメッセージ数	スパム対策スキャンエンジンで陽性、または疑いありとして検出されたメッセージの総数。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。

カテゴリ (Category)	説明
検出されたウイルス メッセージ数	<p>ウイルス陽性だがスパムではないと検出されたメッセージの総数および割合。</p> <p>次のメッセージは、[ウイルス検出 (Virus Detected)] カテゴリに集計されます。</p> <ul style="list-style-type: none"> <li>ウイルス スキャン結果が [修復 (Repaired)] または [感染している (Infectious)] であるメッセージ</li> <li>暗号化されたメッセージを、ウイルスを含むメッセージとして集計するオプションが選択されている場合に、ウイルス スキャン結果が [暗号化 (Encrypted)] であるメッセージ</li> <li>スキャンできないメッセージに対するアクションが [「配信」なし (NOT "Deliver")] の場合に、ウイルス スキャン結果が [スキャン不可 (Unscannable)] であるメッセージ</li> <li>代替メールホストまたは代替受信者へ送信するオプションが選択されている場合に、ウイルス スキャン結果が [スキャン不可 (Unscannable)] または [暗号化 (Encrypted)] であるメッセージ</li> <li>アウトブレイク隔離から手動またはタイムアウトにより削除されたメッセージ</li> </ul>
高度なマルウェア防御で検出	<p>メッセージ添付ファイルは、レピュテーション フィルタリングによって悪意のある添付ファイルとして検出されました。この値には、ファイル分析により悪意があると検出された判定のアップデートまたはファイルは含まれません。</p>
悪意のある URL を含むメッセージ	<p>メッセージに含まれる 1 つ以上の URL が、URL フィルタリングにより悪意のある URL として検出されました。</p>
コンテンツフィルタによる阻止	<p>コンテンツ フィルタによって阻止されたメッセージの総数。</p> <p>アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。</p>
DMARCによる停止 (	<p>DMARC 検証に失敗したメッセージの総数。</p>
S/Mime 検証/復号化の失敗	<p>S/MIME 検証または復号化、あるいはその両方に失敗したメッセージの総数。</p>
マーケティングメッセージ	<p>Amazon.com など、認識されているプロフェッショナル マーケティング グループからのアドバタイジング メッセージの総数。</p> <p>このページのこのリスト項目は、システムにマーケティングデータが存在している場合にだけ表示されます。</p> <p>この数には、グレイメール機能が有効になっている E メールセキュリティ アプライアンスと、スパム対策設定でマーケティング電子メール スキャンが有効になっているアプライアンスの両方によって識別されたマーケティング メッセージが含まれています。</p>
ソーシャルネットワーキングメッセージ	<p>ソーシャル ネットワーク、出会い/結婚 Web サイト、フォーラムなどからの通知メッセージの総数。たとえば、LinkedIn フォーラム、CNET フォーラムなどがあります。この情報は、グレイメール機能によって判別されます。</p>

カテゴリ (Category)	説明
バルクメッセージ	テクノロジーメディア企業の TechTarget など、認識されていないマーケティンググループによって送信されたアドバイジングメッセージの総数。  この情報は、グレイメール機能によって判別されます。
グレイメールメッセージ	この数には、グレイメール機能によって検出されたマーケティングメッセージと、ソーシャルネットワークメッセージおよびバルクメールが含まれます。これらの総数がマーケティングメッセージ値に含まれる場合でも、グレイメール機能が有効になっていないアプライアンスで識別されたマーケティングメッセージは含まれません。  メッセージトラッキングを使用して、そのカテゴリに所属するメッセージのリストを表示するには、任意のグレイメールカテゴリに対応する番号をクリックします。  <a href="#">グレイメールのレポート (107 ページ)</a> も参照してください。
S/MIME 検証/復号化の成功	正常に検証、復号化されたか、S/MIME を使用して復号化および検証されたメッセージの総数。
承認されたクリーンメッセージ数	このカテゴリは、受け入れられ、ウイルスでもスパムでもないと思なされたメールです。  受信者単位のスキャンアクション（個々のメールポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーンメッセージを最も正確に表したものです。  ただし、ウイルス陽性またはスパム陽性としてマークされたにもかかわらず配信されたメッセージは集計されないため、実際のメッセージの配信数と、このクリーンメッセージの数は異なる可能性があります。  メッセージがメッセージフィルタと一致し、フィルタによってドロップされたり、バウンスされたりしていない場合は、クリーンなメッセージとして扱われます。メッセージフィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。  グレイメール機能が有効になっていないアプライアンスで処理されるメッセージは、クリーンとして集計されます。
試行されたメッセージの合計数	この数には、スパム、マーケティングメッセージ（グレイメール機能またはスパム対策機能の電子メールスキャン機能によって検出）、ソーシャルネットワーキングメッセージ、バルクメール、およびクリーンメッセージが含まれます。



- (注) スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーンメッセージとして集計されます。そうでない場合は、ウイルス陽性メッセージにカウントされます。さらに、メッセージがメッセージフィルタと一致し、フィルタによってドロップされたり、バウンスされたりしていない場合、クリーンなメッセージとして扱われます。メッセージフィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

## [受信メール (Incoming Mail)] ページ

セキュリティ管理アプライアンスの [受信メール (Incoming Mail)] > [レポート (Reporting)] > [受信メール (Incoming Mail)] ページには、管理対象のセキュリティ管理アプライアンスに接続されているすべてのリモートホストのリアルタイム情報のインタラクティブなレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー (組織) の情報を収集できます。また、メール送信者の IP アドレス、ドメイン、組織については、送信者プロファイル検索を実行することもできます。

[受信メールの詳細 (Incoming Mail Details)] インタラクティブ テーブルには、特定の IP アドレス、ドメイン、またはネットワーク オーナー (組織) についての詳細情報が表示されます。いずれかの IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロファイル (Sender Profile)] ページにアクセスするには、[受信メール (Incoming Mail)] ページの上部、または他の [送信者プロファイル (Sender Profile)] ページにある対応するリンクをクリックします。

[受信メール (Incoming Mail)] ページでは、次の操作を実行できます。

- セキュリティ管理アプライアンスにメールを送信した送信者の IP アドレス、ドメイン、またはネットワーク オーナー (組織) に関する検索を実行する。 [検索およびインタラクティブ電子メール レポート ページ \(61 ページ\)](#) を参照してください。
- 送信者グループレポートを表示して、特定の送信者グループおよびメールフローポリシーアクションに従って接続をモニタする。詳細については、[\[送信者グループ \(Sender Groups\)\] レポート ページ \(81 ページ\)](#) を参照してください。
- 電子メールをアプライアンスに送信した送信者の詳細な統計情報を表示する。統計情報には、セキュリティ サービス (送信者レピュテーションフィルタリング、アンチスパム、アンチウイルスなど) によってブロックされたメッセージの数が含まれます。
- アンチスパムまたはアンチウイルスセキュリティサービスによって測定される、大量のスパムまたはウイルス電子メールを送信した送信者別にソートする。
- SenderBase レピュテーション サービスを使用して特定の IP アドレス、ドメイン、および組織の間の関係を分析し、送信者に関する情報を取得する。
- 送信者の SenderBase レピュテーション スコア (SBRs)、ドメインが直近に一致した送信者グループなど、送信者に関する詳細を SenderBase レピュテーション サービスから取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルスセキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者についての詳細情報を取得する。

## [受信メール (Incoming Mail)] ページ内のビュー

[受信メール (Incoming Mail)] ページには、次の 3 つのビューがあります。

- IP アドレス
- ドメイン (Domains)
- ネットワーク オーナー

これらのビューでは、システムに接続されたリモートホストのスナップショットが、選択したビューのコンテキストで提供されます。

さらに、[受信メール (Incoming Mail)] ページの [受信メールの詳細 (Incoming Mail Details)] セクションでは、送信者の IP アドレス、ドメイン名、またはネットワーク オーナー情報をクリックすると、特定の送信者プロファイル情報を取得できます。[送信者プロファイル (Sender Profile)] の情報の詳細については、[送信者プロファイル (Sender Profile)] ページ (79 ページ) を参照してください。



(注) ネットワーク オーナーは、ドメインを含むエンティティです。ドメインは、IP アドレスを含むエンティティです。

選択したビューに応じて、[受信メールの詳細 (Incoming Mail Details)] インタラクティブテーブルに、E メールセキュリティ アプライアンスで設定されたすべてのパブリック リスナーに電子メールを送信した上位 IP アドレス、ドメイン、またはネットワーク オーナーが表示されます。アプライアンスに入ったすべてのメールのフローをモニタできます。

IP アドレス、ドメイン、またはネットワーク オーナーをクリックすると、[送信者プロファイル (Sender Profile)] ページの送信者の詳細にアクセスできます。[送信者プロファイル (Sender Profile)] ページは特定の IP アドレス、ドメインまたはネットワーク オーナーに固有の [受信メール (Incoming Mail)] ページです。

送信者グループ別のメール フロー情報にアクセスするには、[受信メール (Incoming Mail)] ページの下部にある [送信者グループレポート (Sender Groups Report)] リンクをクリックします。[送信者プロファイル (Sender Profile)] ページ (79 ページ) を参照してください。

場合によっては、いくつかのレポートページに、トップレベルのページからアクセスできる独自のサブレポートが複数含まれることがあります。たとえば、セキュリティ管理アプライアンスの [受信メール (Incoming Mail)] レポート ページでは、個々の IP アドレス、ドメイン、およびネットワーク オーナーの情報を表示できます。これらは [受信メール (Incoming Mail)] レポート ページからアクセスできるサブページです。

トップレベル ページ (この場合には [受信メール (Incoming Mail)] レポート ページ) の右上にある [印刷可能な PDF (Printable PDF)] リンクをクリックすると、これらの各サブレポート ページの結果を、1つの統合レポートに生成できます。[電子メールレポート (Email Reporting)] ページの概要 (62 ページ) の重要な情報を参照してください。

[メール (Email)] > [レポート (Reporting)] > [受信メール (Incoming Mail)] ページには次のビューがあります。[IP アドレス (IP Addresses)]、[ドメイン (Domains)]、または [ネットワーク所有者 (Network Owners)]

[受信メールの詳細 (Incoming Mail Details)] インタラクティブテーブルに含まれるデータの説明については、[受信メールの詳細 (Incoming Mail Details)] テーブル (78 ページ) を参照してください。

[受信メール (Incoming Mail)] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細

## [ドメイン情報がありません (No Domain Information)] リンク

については、[\[電子メール レポート \(Email Reporting\)\] ページの概要 \(62 ページ\)](#) を参照してください。



(注) [\[受信メール \(Incoming Mail\)\] レポート ページのスケジュール設定されたレポートを生成できません。](#) [メール レポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [ドメイン情報がありません (No Domain Information)] リンク

セキュリティ管理アプライアンスに接続したものの、ダブル DNS ルックアップで検証できなかったドメインは、専用ドメイン [ドメイン情報がありません (No Domain Information)] に自動的に分類されます。これらの種類の検証外ホストを管理する方法は、送信者の検証によって制御できます。送信者の検証の詳細については、ご使用の E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[表示された項目 (Items Displayed)] メニューを使用して、リストに表示する送信者の数を選択できます。

## メールトレンドグラフにおける時間範囲

メールのグラフは、さまざまなきめ細かさを選択して表示できます。同じデータの日、週、月、および年のビューを選択できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

時間範囲の詳細については、[レポートの時間範囲の選択 \(27 ページ\)](#) を参照してください。

## [受信メールの詳細 (Incoming Mail Details)] テーブル

[受信メール (Incoming Mail)] ページの下部にあるインタラクティブな [受信メールの詳細 (Incoming Mail Details)] テーブルには、E メールセキュリティ アプライアンス上のパブリックリスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメイン、IP アドレス、またはネットワーク オーナーが表示されます。データをソートするには、列見出しをクリックします。

ダブル DNS ルックアップを実行することで、システムはリモートホストの IP アドレスの正当性を確保および検証します。ダブル DNS ルックアップおよび送信者検証の詳細については、E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[受信メールの詳細 (Incoming Mail Details)] テーブルの最初の列、または [脅威メッセージの送信者上位 (Top Senders by Total Threat Messages)] に表示される送信者、つまりネットワーク オーナー、IP アドレスまたはドメインについては、[送信者 (Sender)] または [ドメイン情報がありません (No Domain Information)] リンクをクリックすると、送信者の詳細情報が表示されます。結果は、[送信者プロファイル (Sender Profile)] ページに表示され、SenderBase レピュテーション サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、[\[送信者プロファイル \(Sender Profile\)\] ページ \(79 ページ\)](#) を参照してください。

[受信メール (Incoming Mail)] ページの下部にある [送信者グループレポート (Sender Groups Report)] をクリックして、[送信者グループ (Sender Groups)] レポートを表示することもできます。[送信者グループ (Sender Groups)] レポート ページの詳細については、[\[送信者グループ \(Sender Groups\)\] レポート ページ \(81 ページ\)](#) を参照してください。

アクセス権限でメッセージトラッキングデータを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## [送信者プロフィール (Sender Profile)] ページ

[受信メール (Incoming Mail)] インタラクティブ テーブル ([メールフローの詳細 (Mail Flow Details)] (新しい Web インターフェイス) または [受信メール (Incoming Mail)] ページ) の送信者をクリックすると、[送信者プロフィール (Sender Profile)] ページが表示されます。ここでは、特定の IP アドレス、ドメイン、またはネットワーク オーナー (組織) の詳細情報が表示されます。[メールフローの詳細 (Mail Flow Details)] ページまたは他の [送信者プロフィール (Sender Profile)] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロフィール (Sender Profile)] ページにアクセスできます。

ネットワーク オーナーは、ドメインを含むエンティティです。ドメインは、IP アドレスを含むエンティティです。

IP アドレス、ドメインおよびネットワーク オーナーに関して表示される送信者プロフィール ページは、多少異なります。それぞれのページには、特定の送信者からの着信メールに関するグラフおよびサマリーテーブルが含まれます。グラフの下の表に、送信者に関連付けられたドメインまたは IP アドレスが表示されます。(個々の IP アドレスの [送信者プロフィール (Sender Profile)] ページには、詳細なリストが含まれません)。[送信者プロフィール (Sender Profile)] ページには、送信者の現在の SenderBase、送信者グループ、およびネットワーク 情報を含む情報 セクションも表示されます。

- ネットワーク オーナー プロファイル ページには、ネットワーク オーナー、およびこのネットワーク オーナーに関連するドメインや IP アドレスに関する情報が含まれます。
- ドメイン プロファイル ページには、このドメインおよびこのドメインに関連する IP アドレスに関する情報が含まれます。
- IP アドレス プロファイル ページには、IP アドレスのみにに関する情報が含まれます。

各 [送信者プロフィール (Sender Profile)] ページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

- SenderBase レピュテーション サービスからのグローバル情報。たとえば、次の情報です。
  - IP アドレス、ドメイン名、またはネットワーク オーナー
  - ネットワーク オーナーのカテゴリ (ネットワーク オーナーのみ)
  - CIDR 範囲 (IP アドレスのみ)

- IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
- この送信者から最初のメッセージを受信してからの日数
- 最後の送信者グループと DNS が検証されたかどうか (IP アドレス送信者プロフィール ページのみ)

日単位マグニチュードは、直近24時間にドメインが送信したメッセージの数の基準です。地震の測定に使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10を基数とする対数目盛を使用して算出されるメッセージの量の基準です。目盛の最大理論値は10に設定されます。これは、世界の電子メールメッセージの量に相当します。対数目盛を使用した場合、1ポイントのマグニチュードの増加は、実際の量の10倍の増加に相当します。

月単位マグニチュードは、直近30日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。

- 平均マグニチュード (IP アドレスのみ)
- 総累積量/30日の量 (IP アドレス プロファイル ページのみ)
- Bonded Sender ステータス (IP アドレス プロファイル ページのみ)
- SenderBase 評価スコア (IP アドレス プロファイル ページのみ)
- 最初のメッセージからの日数 (ネットワーク オーナーとドメイン プロファイル ページのみ)
- このネットワーク オーナーに関連するドメインの数 (ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ)
- このネットワーク オーナーの IP アドレスの数 (ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ)
- 電子メールの送信に使用された IP アドレスの数 (ネットワーク オーナー ページのみ)

SenderBase 評価サービスによって提供されるすべての情報を示すページを表示するには、[SenderBaseからの詳細情報 (More from SenderBase) ] をクリックします。

- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する詳細は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

ドメイン プロファイルのページから、特定の IP アドレスをクリックして特定の情報を表示することも、組織プロフィールのページを表示することもできます。



## [送信者グループ (Sender Groups) ] レポート ページ

[送信者グループ (Sender Groups) ] レポート ページには、送信者グループ別およびメールフローポリシーアクション別に接続の要約が表示され、SMTP 接続およびメールフローポリシーのトレンドを確認できます。[送信者グループによるメールフロー (Mail Flow by Sender Group) ] リストには、各送信者グループの割合および接続数が示されます。[メールフローポリシーアクションによる接続 (Connections by Mail Flow Policy Action) ] グラフは、各メールフローポリシーアクションの接続の割合を示します。このページには、ホストアクセステーブル (HAT) ポリシーの有効性の概要が示されます。HAT に関する詳細については、お使いの E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[送信者グループ (Sender Groups) ] レポート ページを表示するには、[メール (Email) ] > [レポート (Reporting) ] > [送信者グループ (Sender Groups) ] を選択します。

[送信者グループ (Sender Group) ] レポート ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[\[電子メールレポート \(Email Reporting\) \] ページの概要 \(62 ページ\)](#) を参照してください。



(注) [送信者グループ (Sender Group) ] レポート ページのスケジュール設定されたレポートを生成できます。[メールレポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [送信者ドメインのレピュテーション (Sender Domain Reputation) ] ページ

[送信者ドメインのレピュテーション (Sender Domain Reputation) ] レポート ページでは、次を表示できます。

- SDR サービスで受信した判定に基づく着信メッセージ (グラフ形式)。
- SDR サービスで受信した脅威カテゴリおよび判定に基づく着信メッセージの概要 (表形式)。
- SDR サービスで受信した脅威カテゴリに基づく着信メッセージ (グラフ形式)。



(注) SDR 判定が「非常に問題がある」または「悪い」メッセージのみが、「スパム」や「悪意あり」などの SDR 脅威カテゴリに分類されます。

- SDR サービスで受信した脅威カテゴリに基づく着信メッセージの概要 (表形式)。

[SDRによって処理された着信メッセージの概要 (Summary of Incoming Messages handled by SDR) ] セクションで特定の判定に対応するメッセージの数をクリックすると、関連するメッセージを [メッセージトラッキング (Message Tracking) ] に表示できます。

## [送信先 (Outgoing Destinations) ] ページ

[メール (Email) ] > [レポート (Reporting) ] > [送信先 (Outgoing Destinations) ] ページには、組織がメールを送信する宛先のドメインについての情報が表示されます。

[送信先 (Outgoing Destinations) ] ページを使用して、次の情報を入手できます。

- Eメールセキュリティ アプライアンスが送信するメールの宛先のドメイン
- 各ドメインに送信されるメールの量
- クリーン、スパム陽性、ウイルス陽性、マルウェア、またはコンテンツフィルタによる阻止のメールの割合。
- 配信されたメッセージおよび宛先サーバによってハードバウンズされたメッセージの数。

次のリストでは、[送信先 (Outgoing Destinations) ] ページのさまざまなセクションについて説明します。

表 18: [メール (Email) ] > [レポート (Reporting) ] > [送信先 (Outgoing Destinations) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[脅威総数別の上位宛先 (Top Destination by Total Threat) ]	組織によって送信された発信脅威メッセージ (スパム、アンチウイルスなど) の上位の宛先ドメイン。コンテンツ フィルタをトリガーしたスパム陽性またはウイルス陽性の脅威メッセージを含む、脅威メッセージの総数。
[正常なメッセージの上位宛先 (Top Destination by Clean Messages) ]	組織によって送信されたクリーンな発信脅威メッセージの上位の宛先ドメイン。
[送信先の詳細 (Outgoing Destination Details) ]	組織によって送信されたすべての発信メッセージの宛先ドメインに関する、総受信者数別にソートされたすべての詳細情報。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。  アクセス権限でメッセージトラッキングデータを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[送信先 (Outgoing Destinations) ] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート \(Email Reporting\) \] ページの概要 \(62 ページ\)](#) を参照してください。



(注) [送信先 (Outgoing Destinations) ] ページのスケジュール設定されたレポートを生成できます。  
メールレポートのスケジュール設定 (181 ページ) を参照してください。

## [送信メッセージ送信者 (Outgoing Senders) ] ページ

[メール (Email) ] > [レポート (Reporting) ] > [送信メッセージ送信者 (Outgoing Senders) ] ページには、ネットワーク内の IP アドレスおよびドメインから送信された電子メールの数と種類についての情報が表示されます。

[送信メッセージ送信者 (Outgoing Senders) ] ページを使用して、次の情報を入手できます。

- 最も多くのウイルスに感染したまたはスパムあるいはマルウェアと判断された電子メールを送信している IP アドレス
- 最も頻繁にコンテンツ フィルタをトリガーした IP アドレス
- 最も多くのメールを送信するドメイン
- 配信が試行された場所で処理された受信者の総数。

[送信メッセージ送信者 (Outgoing Sender) ] ページを表示するには、次の手順を実行します。

[送信メッセージ送信者 (Outgoing Senders) ] の結果は次の 2 種類のビューで表示できます。

- [ドメイン (Domain) ] : このビューでは、各ドメインから送信された電子メールの量を表示できます。
- [IP アドレス (IP Address) ] : このビューでは、最も多くのウイルスメッセージを送信したか、または最も多くのコンテンツ フィルタをトリガーした IP アドレスを表示できます。

次のリストでは、[送信先 (Outgoing Destinations) ] ページの両方のビューのさまざまなセクションについて説明します。

表 19: [メール (Email) ] > [レポート (Reporting) ] > [送信メッセージ送信者 (Outgoing Sender) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[脅威メッセージ総数の上位送信者 (Top Senders by Total Threat Messages) ]	組織内の発信脅威メッセージ (スパム、アンチウイルスなど) の上位送信者 (IP アドレス別またはドメイン別)。
[正常なメッセージの上位送信者 (Top Sender by Clean Messages) ]	組織内で送信されたクリーンな発信メッセージの上位送信者 (IP アドレス別またはドメイン別)。

セクション	説明
[送信者の詳細 (Sender Details)]	<p>組織内によって送信されたすべての発信メッセージの送信者のすべての詳細情報 (IP アドレス別またはドメイン別)。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。</p> <p>アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートの DLP およびコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。</p>



(注) このページには、メッセージ配信に関する情報は表示されません。特定のドメインからのバウンズされたメッセージの数などの配信情報を追跡するには、適切な E メールセキュリティ アプライアンスにログインし、[モニタ (Monitor)] > [送信処理ステータス (Delivery Status)] を選択します。

[送信メッセージ送信者 (Outgoing Senders)] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メールレポート (Email Reporting)] ページの概要 (62 ページ) を参照してください。



(注) [送信メッセージ送信者 (Outgoing Senders)] レポート ページのスケジュール設定されたレポートを生成できます。メールレポートのスケジュール設定 (181 ページ) を参照してください。

## [内部ユーザ (Internal Users)] ページ

[メール (Email)] > [レポート (Reporting)] > [内部ユーザ (Internal Users)] ページには、電子メールアドレスごとに内部ユーザによって送受信された電子メールについての情報が表示されます。1人のユーザが複数の電子メールアドレスを持っている場合があります。レポートでは、電子メールアドレスがまとめられません。

[内部ユーザ (Internal Users)] インタラクティブ レポート ページを使用すると、次のような情報を取得できます。

- 最も多くの外部メールを送信したユーザ
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのグレイメール メッセージを受信したユーザ
- 最も多くのスパムを受信したユーザ
- コンテンツ フィルタをトリガーしたユーザとそのコンテンツ フィルタの種類
- 電子メールをコンテンツ フィルタで捕捉されたユーザ

表 20: [メール (Email)] &gt; [レポート (Reporting)] &gt; [内部ユーザ (Internal Users)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	1～90日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[正常な受信メッセージ数の上位ユーザ (Top Users by Clean Incoming Messages)]	組織内で送信されたクリーンな着信メッセージの上位ユーザ (IP アドレス別またはドメイン別)。
[正常な送信メッセージ数の上位ユーザ (Top Users by Clean Outgoing Messages)]	組織内で送信されたクリーンな発信メッセージの上位ユーザ (IP アドレス別またはドメイン別)。
[ユーザメールフローの詳細 (User Mail Flow Details)]	<p>[ユーザメールフローの詳細 (User Mail Flow Details)] インタラクティブセクションでは、電子メールアドレスごとに送受信メールが分類されます。列ヘッダーをクリックすることにより、表示をソートできます。</p> <p>ユーザの詳細を参照するには、[内部ユーザ (Internal User)] 列でユーザ名をクリックします。詳細については、<a href="#">[内部ユーザの詳細 (Internal User Details)] ページ (85 ページ)</a> を参照してください。</p> <p>アクセス権限でメッセージトラッキングデータを表示できる場合、このレポートのコンテンツフィルタ違反に対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。</p>

[内部ユーザ (Internal Users)] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[\[電子メールレポート \(Email Reporting\)\] ページの概要 \(62 ページ\)](#) を参照してください。



(注) [内部ユーザ (Internal Users)] ページのスケジュール設定されたレポートを生成できます。[メールレポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [内部ユーザの詳細 (Internal User Details)] ページ

[内部ユーザの詳細 (Internal User Details)] ページでは、各カテゴリ ([スパム検出 (Spam Detected)]、[ウイルス検出 (Virus Detected)]、[高度なマルウェア防御で検出 (Detected By Advanced Malware Protection)]、[コンテンツフィルタによる停止 (Stopped By Content Filter)] など) のメッセージ数を示す受信および送信メッセージの内訳など、ユーザに関する詳細情報が示されます。送受信コンテンツフィルタの一致も示されます。

着信内部ユーザとは、**Rept To:** アドレスに基づいてシステムで電子メールを受信する対象ユーザのことで、発信内部ユーザは**Mail From:** アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします ([[コンテンツフィルタ \(Content Filters\)](#)] ページ (89 ページ) を参照)。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したすべてのユーザのリストも表示できます。



(注) 送信メールの中には (バウンスなど)、送信者が null になっているものがあります。これらの送信者は、送信「不明」として集計されます。

## 特定の内部ユーザの検索

[ユーザメール概要 (User Mail Summary)] ページおよび [ユーザメールフローの詳細 (User Mail Flow Details)] ページの下部にある検索フォームで、特定の内部ユーザ (電子メールアドレス) を検索できます。検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか (たとえば、「ex」で始まる項目を検索する場合、「example@example.com」が一致します) を選択します。

## DLP インシデント

[メール (Email)] > [レポート (Reporting)] > [DLP インシデント (DLP Incidents)] ([DLP インシデントサマリー (DLP Incident Summary)] ページには、送信メールで発生した、データ漏洩防止 (DLP) ポリシーに違反するインシデントの情報が示されます。E メールセキュリティ アプライアンスでは、[送信メールポリシー (Outgoing Mail Policies)] テーブルで有効にした DLP 電子メール ポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

[DLP インシデントサマリー (DLP Incident Summary)] レポートを使用すると、次のような情報を取得できます。

- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP インシデントサマリー (DLP Incident Summary)] ページには次の 2 つのメインセクションがあります。

- 重大度 ([低 (Low)], [中 (Medium)], [高 (High)], [重大 (Critical)]) 別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンド グラフ
- [DLP インシデントの詳細 (DLP Incident Details)] リスト

表 21: [メール (Email) ]&gt;[レポート (Reporting) ]&gt;[DLPインシデントサマリー (DLP Incident Summary) ]ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[重大度別上位インシデント (Top Incidents by Severity) ]	重大度別の上位 DLP インシデント。
[インシデントサマリー (Incident Summary) ]	各電子メールアプライアンスの送信メールポリシーで現在有効になっている DLP ポリシーは、[DLPインシデントサマリー (DLP Incident Summary) ]ページの下部にある [DLPインシデントの詳細 (DLP Incident Details) ]インタラクティブテーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。
[上位DLPポリシー一致数 (Top DLP Policy Matches) ]	一致している上位 DLP ポリシー。
[DLPインシデントの詳細 (DLP Incident Details) ]	[DLPインシデントの詳細 (DLP Incident Details) ]テーブルには、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。  [DLPインシデントの詳細 (DLP Incidents Details) ]テーブルの詳細については、 <a href="#">[DLPインシデントの詳細 (DLP Incidents Details) ]テーブル (87 ページ)</a> を参照してください。

ポリシーによって検出された DLP インシデントに関する詳細情報を表示するには、DLP ポリシーの名前をクリックします。この方法を使用すると、ポリシーによって検出された、機密データを含むメールを送信したユーザのリストを取得できます。

## [DLPインシデントの詳細 (DLP Incidents Details) ]テーブル

[DLPインシデントの詳細 (DLP Incident Details) ]テーブルは、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが表示されるインタラクティブテーブルです。データをソートするには、列見出しをクリックします。

このテーブルに表示される DLP ポリシーの詳細情報を検索するには、DLP ポリシー名をクリックして、その DLP ポリシーのページを表示します。詳細については、[\[DLPポリシー詳細 \(DLP Policy Detail\) \]ページ \(88 ページ\)](#) を参照してください。

アクセス権限でメッセージトラッキングデータを表示できる場合、このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## [DLP ポリシー詳細 (DLP Policy Detail)] ページ

[DLPインシデントの詳細 (DLP Incident Details)] テーブルで DLP ポリシーの名前をクリックした場合、その結果として表示される [DLPポリシー詳細 (DLP Policy Detail)] ページにそのポリシーに関する DLP インシデント データが表示されます。このページには、重大度に基づいた DLP インシデントのグラフが表示されます。

このページには、DLP ポリシーに違反したメッセージを送信した各内部ユーザを表示する、ページ下部にある [送信者別インシデント (Incidents by Sender)] テーブルも含まれます。このテーブルには、このポリシーに関するユーザごとの DLP インシデントの総数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。[送信者別インシデント (Incidents by Sender)] テーブルを使用すると、組織の機密データをネットワーク外のユーザに送信した可能性のあるユーザを特定できます。

インシデント詳細ページの送信者名をクリックすると [内部ユーザ (Internal Users)] ページが開きます。詳細については、[内部ユーザ (Internal Users)] ページ (84 ページ) を参照してください。

## メッセージフィルタ

[メッセージフィルタ (Message Filters)] ページには、送受信メッセージのメッセージフィルタの上位一致 (最も多くのメッセージに一致したメッセージフィルタ) に関する情報が表示されます。

## 地理的分散

[地理的分散 (Geo Distribution)] レポート ページを使用して次の項目を表示できます。

- 発信国別の受信メール接続数の上位 (グラフィカルな形式)。
- 発信国別の受信メール接続の合計数 (表形式)。

国情報を表示しない受信メール接続の上位と合計数の例を次に示します。

- プライベート IP アドレスに属する送信者 IP アドレス
- 送信者の IP アドレスは、有効な SBRS を取得していません。

## 大容量のメール

このページのレポートは、次の目的で使用します。

- 1人の送信者から送られていたり、件名が同じであったり、1時間の間に送られたりした、多数のメッセージが関係する攻撃を特定します。
- このような攻撃が独自のドメイン内で発生しないように上位ドメインをモニタします。この状況が生じると、組織の1つ以上のアカウントが侵害される可能性があります。



- フィルタを適宜調整できるように、誤検出を特定します。

このページのレポートには、ヘッダー反復ルールを使用し、そのルールで設定されたメッセージ数のしきい値を超えるメッセージフィルタからのデータのみが表示されます。他のルールと組み合わせた場合、ヘッダー反復ルールの評価は最後になります。また、先行する条件によってメッセージの処理が決定されると評価は行われません。同様に、レート制限で検出されたメッセージはヘッダー反復メッセージフィルタに達しません。したがって、別の状況では大容量のメールと見なされるメッセージが、これらのレポートに含まれない場合があります。特定のメッセージをホワイトリストに追加するようにフィルタを設定している場合は、それらのメッセージもレポートから除外されます。

メッセージフィルタおよびヘッダー反復ルールの詳細については、お使いの E メールセキュリティ アプライアンスのオンラインヘルプまたはユーザガイドを参照してください。

#### 関連項目

- [\[レート制限 \(Rate Limits\) \] ページ \(105 ページ\)](#)

## [コンテンツフィルタ (Content Filters) ] ページ

[メール (Email) ] > [レポート (Reporting) ] > [コンテンツフィルタ (Content Filters) ] ページには、送受信コンテンツ フィルタの上位一致 (最も多くのメッセージに一致したコンテンツ フィルタ) に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツフィルタ (Content Filters) ] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認し、次の情報を取得できます。

- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ。
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ。

特定のフィルタの詳細情報を表示するには、フィルタ名をクリックします。[コンテンツフィルタの詳細 (Content Filter Details) ] ページが表示されます。[コンテンツフィルタの詳細 (Content Filter Details) ] ページの詳細については、[\[コンテンツフィルタの詳細 \(Content Filter Details\) \] ページ \(90 ページ\)](#) を参照してください。

アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[コンテンツフィルタ (Content Filters) ] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[\[電子メールレポート \(Email Reporting\) \] ページの概要 \(62 ページ\)](#) を参照してください。



- (注) [\[コンテンツフィルタ \(Content Filter\) \] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [コンテンツフィルタの詳細 (Content Filter Details)] ページ

[コンテンツフィルタの詳細 (Content Filter Detail)] ページには、このフィルタの経時的な一致および内部ユーザ別の一致が表示されます。

[内部ユーザ別の一致 (Matches by Internal User)] セクションで、内部ユーザ (電子メールアドレス) の詳細ページを表示するユーザ名をクリックします。詳細については、[\[内部ユーザの詳細 \(Internal User Details\)\] ページ \(85 ページ\)](#) を参照してください。

アクセス権限でメッセージトラッキングデータを表示できる場合、このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## DMARC 検証

[DMARC検証 (DMARC Verification)] ページには、Domain-based Message Authentication, Reporting and Conformance (DMARC) 検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。このレポートを使用して DMARC 設定を最適化し、次のような情報を取得できます。

- DMARC 検証に失敗したメッセージを最も多く送信したドメイン
- 各ドメインで、DMARC 検証に失敗したメッセージに対して実行されたアクション

DMARC 検証の詳細については、お使いの E メールセキュリティアプライアンスのオンラインヘルプまたはユーザガイドで「Email Authentication」の章を参照してください。

## マクロ検出

[マクロ検出 (Macro Detection)] レポート ページを使用して、次の項目を表示できます。

- ファイルタイプ別のマクロが有効になった受信添付ファイル数の上位 (グラフ形式および表形式)。
- ファイルタイプ別のマクロが有効になった送信添付ファイル数の上位 (グラフ形式および表形式)。

マクロが有効になった添付ファイルの数をクリックすると、[メッセージトラッキング (Message Tracking)] に関連メッセージを表示できます。



(注) レポート生成中に次の処理が発生します。

- アーカイブ ファイル内に 1 つ以上のマクロが検出されると、アーカイブ ファイル タイプが 1 増えます。アーカイブ ファイル内のマクロが有効になった添付ファイルの数はカウントされません。
- 埋め込みファイル内に 1 つ以上のマクロが検出されると、親ファイル タイプが 1 増えます。埋め込みファイル内のマクロが有効になった添付ファイルの数はカウントされません。

## [外部脅威フィード (External Threat Feeds) ] ページ

[外部脅威フィード (External Threat Feeds) ] レポート ページでは、以下を表示できます。

- メッセージで脅威を検出するために使用される上位 ETF ソース (グラフ形式)。
- メッセージで脅威を検出するために使用される ETF ソースの概要 (表形式)。
- メッセージで検出された脅威に一致する上位 IOC (グラフ形式)。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソース (グラフ形式)。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソースの概要 (表形式)。

[外部脅威フィードソースの概要 (Summary of External Threat Feed Sources) ] セクションでは、以下を実行できます。

- 特定の ETF ソースでメッセージ数をクリックすると、[メッセージトラッキング (Message Tracking) ] に関連メッセージを表示できます。
- 特定の脅威フィード ソースをクリックすると、IOC に基づいた ETF ソースの分布を表示できます。

[侵害の兆候 (IOC) の一致の概要 (Summary of Indicator of Compromise (IOC) Matches) ] セクションでは、以下を実行できます。

- 特定の ETF ソースで IOC の数をクリックすると、[メッセージトラッキング (Message Tracking) ] に関連メッセージを表示できます。
- 特定の IOC をクリックすると、ETF ソースに基づいた IOC の分布を表示できます。

## [ウイルス タイプ (Virus Types) ] ページ

[メール (Email) ] > [レポート (Reporting) ] > [ウイルスタイプ (Virus Types) ] ページでは、ネットワークで送受信されたウイルスの概要が示されます。[ウイルス タイプ (Virus Types) ]

ページには、E メールセキュリティ アプライアンスで動作するウイルス スキャン エンジンによって検出され、セキュリティ管理アプライアンスに表示されるウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。たとえば、PDF ファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDF が添付されているメッセージを隔離するフィルタ アクションを作成することが推奨されます。



(注) ウイルス感染フィルタでは、ユーザが介入することなく、これらの種類のウイルスに感染したメッセージを隔離することができます。

複数のウイルス スキャン エンジンを実行している場合、[ウイルス タイプ (Virus Types) ] ページには、イネーブルになっているすべてのウイルス スキャン エンジンの結果が含まれます。ページに表示されるウイルスの名前は、ウイルス スキャン エンジンによって判定された名前です。複数のスキャン エンジンが1つのウイルスを検出した場合、同じウイルスに対して複数のエントリが存在する可能性があります。

表 22: [メール (Email) ] > [レポート (Reporting) ] > [ウイルス タイプ (Virus Types) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[検出した受信ウイルス タイプの上位 (Top Incoming Virus Types Detected) ]	このセクションでは、ネットワークに送信されたウイルスのチャート ビューが表示されます。
[検出した送信ウイルス タイプの上位 (Top Outgoing Virus Types Detected) ]	このセクションでは、ネットワークから送信されたウイルスのチャート ビューが表示されます。
[ウイルス タイプ 詳細 (Virus Types Detail) ]	各ウイルス タイプの詳細が表示されるインタラクティブ テーブル。



(注) ウイルスに感染したメッセージをネットワークに送信したホストを表示するには、[受信メール (Incoming Mail) ] ページに移動し、同じ報告期間を指定して、ウイルス陽性別にソートします。同様に、ネットワーク内でウイルス陽性の電子メールを送信した IP アドレスを表示するには、[送信メッセージ送信者 (Outgoing Senders) ] ページを表示し、ウイルス陽性メッセージ別にソートします。

[ウイルス タイプ (Virus Types) ] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート \(Email Reporting\) \] ページの概要 \(62 ページ\)](#) を参照してください。



- (注) [ウイルスタイプ (Virus Types)] ページのスケジュール設定されたレポートを生成できます。[メールレポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [URL フィルタリング (URL Filtering)] ページ

- URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。
- URL フィルタリング レポートは、送受信メッセージに対して使用できます。
- URL フィルタリング エンジンによって (アンチスパム/アウトブレイクフィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して) スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではありません。
- [上位URLカテゴリ (Top URL Categories)] モジュールには、コンテンツ フィルタまたはメッセージフィルタに一致するかどうかにかかわらず、スキャンされたメッセージで検出されたすべてのカテゴリが含まれます。
- 各メッセージを関連付けることができるレピュテーション レベルは1つのみです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。
- [セキュリティサービス (Security Services)] > [URL フィルタリング (URL Filtering)] で設定したグローバル ホワイトリストの URL は、レポートに含まれません。

個別のフィルタで使用されるホワイトリストの URL はレポートに含まれます。

- 悪意のある URL とは、アウトブレイク フィルタによってレピュテーションが低いと判定された URL です。ニュートラル URL とは、アウトブレイク フィルタによってクリック時の保護が必要であると判定された URL です。したがって、ニュートラル URL は Cisco Web セキュリティ プロキシにリダイレクトするために書き換えられています。
- URL カテゴリ ベースのフィルタの結果はコンテンツおよびメッセージフィルタ レポートに反映されます。
- Cisco Web セキュリティ プロキシによるクリック時の URL 評価の結果は、レポートに反映されません。

## [Web インタラクション トラッキング (Web Interaction Tracking)] ページ

- Web インタラクション トラッキング レポート モジュールは、Web インタラクション トラッキング機能が管理対象の E メール セキュリティ アプライアンスで有効になっている場合にのみ入力されます。
- Web インタラクション トラッキング レポートは、送受信メッセージに対して使用できます。

- エンドユーザがクリックした、書き換えられた URL (ポリシーまたはアウトブレイクフィルタによって) のみが、これらのモジュールに含まれます。
- [Webインタラクショントラッキング (Web Interaction Tracking)] ページには、次のレポートが含まれます。

エンドユーザがクリックした、書き換えられた悪意のある上位 URL (Top Rewritten Malicious URLs clicked by End Users)。次の情報を含む詳細レポートを表示するには、URL をクリックします。

- 書き換えられた悪意のある URL をクリックしたエンドユーザのリスト。
- URL がクリックされた日付と時刻。
- URL がポリシーまたはアウトブレイク フィルタによって書き換えられたかどうか。
- 書き換えられた URL がクリックされたときに実行されたアクション (許可、ブロック、または不明)。URL がアウトブレイク フィルタによって書き換えられており、最終的な判定が使用できない場合、ステータスは不明として表示されます。



(注) 制限があるため、アウトブレイクによって書き換えられたすべての URL のステータスが不明として表示されます。

### 書き換えられた悪意のある URL をクリックした上位エンドユーザ (Top End Users who clicked on Rewritten Malicious URLs)

Web インタラクショントラッキングの詳細。次の情報が含まれています。

- 書き換えられたすべての URL のリスト (悪意のあるものとないもの)。詳細レポートを表示するには、URL をクリックします。
- 書き換えられた URL がクリックされた場合に実行されたアクション (許可、ブロック、または不明)。

エンドユーザが URL をクリックしたときにその URL の判定 (クリーンまたは悪意のある) が不明である場合、ステータスは不明として表示されます。これは、ユーザのクリック時に、URL がさらに調査されていたか、Web サーバがダウンしていたか、到達不可能であったためである可能性があります。

- 書き換えられた URL をエンドユーザがクリックした回数。クリックされた URL を含むすべてのメッセージのリストを表示するには、番号をクリックします。
- 次の点に注意してください。
  - 悪意のある URL を書き換えた後に、メッセージを送信して別のユーザ (管理者など) に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクショントラッキングデータが増分します。
  - 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用して元の受信者以外のユーザ (管理者など) に送信する場合、その他のユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクショントラッキングデータが増分します。

## [偽装メールの検出 (Forged Email Detection)] ページ

- [偽装メールの検出 (Forged Email Detection)] ページには、次のレポートが含まれています。
  - 偽装メールの検出数の上位。受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。
  - 偽装電子メール検出詳細 (Forged Email Detection Details)。受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。
- [偽装メールの検出 (Forged Email Detection)] レポートは、[偽装メールの検出 (Forged Email Detection)] コンテンツ フィルタまたは forged-email-detection メッセージ フィルタを使用している場合にのみ自動入力されます。

## [高度なマルウェア防御 (ファイルレピュテーションとファイル分析) (Advanced Malware Protection (File Reputation and File Analysis))] レポート ページ

- [ファイル分析レポートの詳細の要件 \(95 ページ\)](#)
- [SHA-256 ハッシュによるファイルの識別 \(97 ページ\)](#)
- [ファイルレピュテーションとファイル分析レポートのページ \(98 ページ\)](#)
- [その他のレポートでのファイルレピュテーションフィルタ データの表示 \(101 ページ\)](#)

### ファイル分析レポートの詳細の要件

- [\(クラウドファイル分析\) 管理アプライアンスがファイル分析サーバに到達できることを確認する \(95 ページ\)](#)
- [\(クラウドファイル分析\) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する \(95 ページ\)](#)
- [\(オンプレミスのファイル分析\) ファイル分析アカウントをアクティブ化する \(96 ページ\)](#)
- [追加の要件 \(97 ページ\)](#)

#### (クラウドファイル分析) 管理アプライアンスがファイル分析サーバに到達できることを確認する

ファイル分析レポートの詳細を取得するには、アプライアンスがポート 443 経由でファイル分析サーバに接続できる必要があります。詳細については、[ファイアウォール情報 \(643 ページ\)](#) を参照してください。

#### (クラウドファイル分析) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する

組織のすべてのコンテンツセキュリティアプライアンスで、組織内の Cisco E メールセキュリティアプライアンスまたは Cisco Web セキュリティアプライアンスから分析用に送信され

**(オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する**

るファイルに関するクラウド内の詳細な結果が表示されるようにするには、すべてのアプライアンスを同じアプライアンス グループに結合する必要があります。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] を選択します。

**ステップ 3** [ファイル分析 (File Analysis) ] セクションにスクロールします。

**ステップ 4** 管理対象アプライアンスが別のファイル分析クラウドサーバを指している場合は、結果の詳細の表示元となるサーバを選択します。

結果の詳細は、その他のクラウドサーバによって処理されたファイルでは使用できません。

**ステップ 5** 分析グループ ID を入力します。

- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- この値に CCOID を使用することを推奨します。
- この値は大文字と小文字が区別されます。
- この値は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。
- アプライアンスは 1 つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

**ステップ 6** [今すぐグループ化 (Group Now) ] をクリックします。

**ステップ 7** このアプライアンスとデータを共有する各 E メール セキュリティアプライアンスで、同じグループを設定します。

**次のタスク****関連項目**

[クラウドで詳細なファイル分析結果が表示されるファイル \(101 ページ\)](#)

**(オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する**

オンプレミス (プライベートクラウド) の Cisco AMP Threat Grid Appliance を導入した場合、Threat Grid Appliance で使用可能なレポート詳細を表示するために、Cisco コンテンツセキュリティ管理アプライアンスのファイル分析アカウントをアクティブ化する必要があります。通常、これは 1 回のみ必要です。



### 始める前に

重大レベルでシステム アラートを受信していることを確認します。

**ステップ 1** Threat Grid Appliance からファイル分析レポート詳細に最初にアクセスしようとするときに、数分待ってから、リンクを含むアラートを受信します。

このアラートを受信しなかった場合は、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アラート (Alerts)] に移動し、[上位アラートを表示 (View Top Alerts)] をクリックします。

**ステップ 2** アラート メッセージ内のリンクをクリックします。

**ステップ 3** 管理アプライアンスのアカウントをアクティブ化します。

### 追加の要件

追加の要件については、お使いのセキュリティ管理アプライアンス リリースのリリース ノート (次の場所で入手可能) を参照してください <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

## SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム (SHA-256) を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイル进行处理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイル进行处理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルがその SHA-256 値 (短縮形式) 別に表示されます。

## ファイルレピュテーションとファイル分析レポートのページ

レポート	説明
高度なマルウェア対策 (Advanced Malware Protection)	

レポート	説明
	<p>ファイルレピュテーションサービスによって特定されたファイルベースの脅威を示します。</p> <p>判定が変更されたファイルについては、[AMP判定のアップデート (AMP Verdict Updates)] レポートを参照してください。これらの判定は、[高度なマルウェア防御 (Advanced Malware Protection)] レポートに反映されません。</p> <p>圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御 (Advanced Malware Protection)] レポートに含まれます。</p> <p>(注) AsyncOS 9.6.5 以降、高度なマルウェア防御レポートが、追加フィールド、グラフなどを表示するように強化されました。アップグレード後に表示されるレポートには、アップグレード前のレポートのデータは含まれません。AsyncOS 9.6.5 アップグレード前の高度なマルウェア防御レポートを表示するには、ページの下部にあるハイパーリンクをクリックします。</p> <p>[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category)] セクションには次の内容が表示されます。</p> <ul style="list-style-type: none"> <li>• [マルウェア (Malware)] に分類される AMP レピュテーションサーバで受信したブラックリストファイル SHA の割合。</li> <li>• [カスタム検出 (Custom Detection)] に分類される AMP for Endpoints コンソールで受信したブラックリストファイル SHA の割合。</li> </ul> <p>AMP for Endpoints コンソールから取得されるブラックリストに追加されたファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル (Incoming Malware Threat Files)] セクションで [シンプルカスタム検出 (Simple Custom Detection)] として表示されます。</p> <ul style="list-style-type: none"> <li>• [カスタムしきい値 (Custom Threshold)] に分類される AMP for Endpoints コンソールで受信したブラックリストファイル SHA の割合。</li> </ul> <p>レポートの [詳細の表示 (More Details)] セクション内のリンクをクリックすると、エンドポイントコンソールの AMP のブラックリストファイル SHA のファイルトラジェクトリの詳細を表示することができます。</p>

レポート	説明
	<p>[リスク低 (Low Risk) ]判定の詳細をレポートの [AMPにより渡された受信ファイル (Incoming Files Handed by AMP) ]セクションに表示できます。</p>
<p>[高度なマルウェア防御 (Advanced Malware Protection) ]におけるファイル分析</p>	<p>分析用に送信された各ファイルの時間と判定 (または中間判定) を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。</p> <p>1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>オンプレミスの Cisco AMP Threat Grid Appliance での導入の場合 : AMP Threat Grid Appliance でホワイトリストに登録されているファイルは、「クリーン」として表示されます。ホワイトリストについては、AMP Threat Grid のマニュアルまたはオンライン ヘルプを参照してください。</p> <p>ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。</p> <p>SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。</p> <p>ファイルを分析したサーバに関する詳細を表示するには、<a href="#">ファイル分析レポートの詳細の要件 (95 ページ)</a> を参照してください。</p> <p>圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析 (File Analysis) ] レポートに含まれます。</p> <p>(注) AsyncOS 9.6.5 以降、ファイル分析レポートが、追加フィールド、グラフなどを表示するように強化されました。アップグレード後に表示されるレポートには、アップグレード前のレポートのデータは含まれません。AsyncOS 9.6.5 アップグレード前のファイル分析レポートを表示するには、ページの下部にあるハイパーリンクをクリックします。</p>

レポート	説明
[高度なマルウェア防御判定の更新 (Advanced Malware Protection Verdict Updates) ]	<p>高度なマルウェア防御は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。</p> <p>[AMP判定のアップデート (AMP Verdict Updates) ] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、お使いのEメールセキュリティアプライアンスのマニュアルを参照してください。</p> <p>1000を超える判定アップデートを表示するには、データを.csv ファイルとしてエクスポートします。</p> <p>1つのSHA-256に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。</p> <p>使用可能な最大時間範囲内 (レポートに選択された時間範囲に関係なく) に特定のSHA-256の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。</p>

## その他のレポートでのファイルレピュテーションフィルタデータの表示

該当する場合は、ファイルレピュテーションおよびファイル分析のデータを他のレポートでも使用できます。レポートによっては、[高度なマルウェア防御で検出 (Detected by Advanced Malware Protection) ] 列がデフォルトで非表示になっている場合があります。追加列を表示するには、テーブル下部の [列 (Columns) ] リンクをクリックします。

## クラウドで詳細なファイル分析結果が表示されるファイル

パブリッククラウドのファイル分析を導入した場合は、ファイル分析のためにアプライアンスグループに追加された、任意の管理対象アプライアンスからアップロードされたすべてのファイルの詳細な結果を表示できます。

グループに管理アプライアンスを追加した場合は、[管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] ページにあるボタンをクリックして、グループの管理対象アプライアンスのリストを表示できます。

分析グループのアプライアンスはファイル分析クライアント ID で識別されます。特定のアプライアンスのこの ID を判別するには、次の場所を参照してください。

アプライアンス	ファイル分析クライアント ID の場所
E メールセキュリティアプライアンス	[セキュリティ サービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション
Web セキュリティアプライアンス	[セキュリティ サービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション
Cisco コンテンツセキュリティ管理アプライアンス	[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] ページの下部

#### 関連項目

- [\(クラウドファイル分析\) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する \(95 ページ\)](#)

## メールボックスの自動修復

[メールボックス自動修復 (Mailbox Auto Remediation)] レポートページを使用してメールボックスの修復結果の詳細を表示できます。このレポートを使用して次の詳細を表示します。

- 受信者のメールボックス修復の成功または失敗を示す一覧
- メッセージに対してとられる修復のアクション
- SHA-256 ハッシュに関連付けられているファイル名

[修復が失敗した受信者 (Recipients for whom remediation was unsuccessful)] フィールドは、次のシナリオで更新されます。

- 受信者が有効な Office 365 ユーザではない、または受信者がアプライアンスで構成されている Office 365 ドメインアカウントに属していない。
- 添付ファイルを含むメッセージをメールボックスで使用できない。たとえば、エンドユーザがメッセージを削除した。
- アプライアンスが設定済みの修復のアクションを実行しようとしたときにアプライアンスと Office 365 サービス間の接続に問題があった。

メッセージ トラッキングに関連メッセージを表示するには、SHA-256 ハッシュをクリックします。

## [TLS 接続 (TLS Connections)] ページ

[メール (Email)] > [レポート (Reporting)] > [TLS 接続 (TLS Connections)] ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。

[TLS 接続 (TLS Connections)] ページを使用すると、次の情報を測定できます。

- 送受信接続による、全体的な TLS の使用割合。
- TLS 接続に成功したパートナー。
- TLS 接続に成功しなかったパートナー。
- TLS 認証に問題のあるパートナー。
- パートナーが TLS を使用したメールの全体的な割合。

表 23: [メール (Email)] > [レポート (Reporting)] > [TLS 接続 (TLS Connections)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[受信TLS接続数グラフ (Incoming TLS Connections Graph)]	グラフには、選択したタイムフレームに応じて、直近の 1 時間、1 日、または 1 週間における、受信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。
[受信TLS接続数サマリー (Incoming TLS Connections Summary)]	この表には、着信メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した受信 TLS 暗号化メッセージの量が表示されます。
[受信TLSメッセージサマリー (Incoming TLS Message Summary)]	この表には、着信メッセージの総量の概要が表示されます。
[受信TLS接続数詳細 (Incoming TLS Connections Details)]	表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。各ドメインについて、接続の総数、送信されたメッセージ、および成功/失敗した TLS 接続の数を表示できます。各ドメインについて、成功/失敗した接続の割合を表示することもできます。
[送信TLS接続数グラフ (Outgoing TLS Connections Graph)]	グラフには、選択したタイムフレームに応じて、直近の 1 時間、1 日、または 1 週間における、送信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。
[送信TLS接続数サマリー (Outgoing TLS Connections Summary)]	この表には、発信メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した送信 TLS 暗号化メッセージの量が表示されます。
[送信TLSメッセージサマリー (Outgoing TLS Message Summary)]	この表には、発信メッセージの総量が表示されます。

セクション	説明
[送信TLS接続数詳細 (Outgoing TLS Connections Details)]	表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。各ドメインについて、接続の総数、送信されたメッセージ、成功/失敗した TLS 接続の数、および最後の TLS ステータスを表示できます。各ドメインについて、成功/失敗した接続の割合を表示することもできます。

## [受信 SMTP 認証 (Inbound SMTP Authentication)] ページ

[受信SMTP認証 (Inbound SMTP Authentication)] ページには、クライアント証明書の使用情報、および Email Security Appliance とユーザのメールクライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。アプライアンスは、証明書または SMTP AUTH コマンドを受け入れると、メールクライアントへの TLS 接続を確立します。クライアントはこの接続を使用してメッセージを送信します。アプライアンスは、これらの試行をユーザ単位で追跡できないため、レポートには、ドメイン名とドメイン IP アドレスに基づいて SMTP 認証の詳細が表示されます。

次の情報を確認するには、このレポートを使用します。

- SMTP 認証を使用している着信接続の総数
- クライアント証明書を使用している接続の数
- SMTP AUTH を使用している接続の数
- SMTP 認証を使用しようとして、接続が失敗したドメイン
- SMTP 認証が失敗した一方で、フォールバックを正常に使用している接続の数

[受信SMTP認証 (Inbound SMTP Authentication)] ページには、受信した接続のグラフ、SMTP 認証接続を試行したメール受信者のグラフ、および接続の認証試行の詳細を含むテーブルが表示されます。

[受信した接続 (Received Connections)] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメールクライアントの着信接続が示されます。このグラフには、アプライアンスが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。

[受信した受信者 (Received Recipients)] グラフには、SMTP 認証を使用して、メッセージを送信するために Email Security Appliances への接続を認証しようとしたメールクライアントを所有する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。

[SMTP認証の詳細 (SMTP Authentication details)] テーブルには、メッセージを送信するために Email Security Appliance への接続を認証しようとしたユーザを含むドメインの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行 (成功または失敗) の数、SMTP AUTH コマンドを使用した接続試行 (成功または失敗) の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。ペー



ジ上部のリンクを使用して、ドメイン名またはドメイン IP アドレス別にこの情報を表示できます。

## [レート制限 (Rate Limits) ] ページ

エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メール メッセージ受信者数を制限できます。[レート制限 (Rate Limits) ] レポートには、この制限を最も上回った送信者が表示されます。

このレポートは、以下を特定する場合に役立ちます。

- 大量のスパムを送信するために使用される可能性のある信用できないユーザ アカウント
- 通知、アラート、自動報告などに電子メールを使用する組織内の制御不能アプリケーション
- 内部請求やリソース管理のために、組織内で電子メールを過剰に送信している送信元
- スパムとは見なされないが、大量の着信電子メールトラフィックを送信している送信元

内部送信者に関する統計情報を含む他のレポート ([内部ユーザ (Internal Users) ]、[送信メッセージ送信者 (Outgoing Senders) ] など) では、送信されたメッセージの数のみ計測されます。これらのレポートでは、少数のメッセージを多数の受信者に送信した送信者は識別されません。

[上位攻撃者(インシデント別) (Top Offenders by Incident) ] チャートには、設定済み制限よりも多くの受信者にメッセージを最も頻繁に送信しようとしたエンベロープ送信者が表示されます。各試行が1インシデントに相当します。このチャートでは、すべてのリスナーからのインシデント数が集計されます。

[上位攻撃者(拒否した受信者数) (Top Offenders by Rejected Recipients) ] チャートには、設定済みの制限を上回る、最も多くの受信者にメッセージを送信したエンベロープ送信者が表示されます。このチャートでは、すべてのリスナーからの受信者数が集計されます。

[エンベロープ送信者のレート制限 (Rate Limit for Envelope Senders) ] 設定を含む [レート制限 (Rate Limiting) ] 設定は、E メールセキュリティ アプライアンスの [メールポリシー (Mail Policies) ] > [メールフローポリシー (Mail Flow Policies) ] で設定します。レート制限の詳細については、ご使用の E メールセキュリティ アプライアンスのマニュアルまたはオンラインヘルプを参照してください。

### 関連項目

- [大容量のメール \(88 ページ\)](#)

## [アウトブレイク フィルタ (Outbreak Filters) ] ページ

[メール (Email) ] > [レポート (Reporting) ] > [アウトブレイクフィルタ (Outbreak Filters) ] ページには、最近の発生状況やウイルス感染フィルタによって隔離されたメッセージに関する情報が表示されます。このページを使用して、対象を絞ったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできます。

[アウトブレイクフィルタ (Outbreak Filters) ] ページを使用して、次の情報を入手できます。

- ウイルス感染フィルタ ルールによって隔離されたメッセージの数と使用されたルール。
- ウイルスの発生に対する、ウイルス感染機能のリードタイム。
- グローバル ウイルス感染発生と比較したローカル ウイルスの発生状況。
- メッセージがアウトブレイク隔離にとどまる期間
- 最も頻繁に表示される悪意のある可能性がある URL

[タイプ別脅威 (Threats By Type) ] セクションには、アプライアンスによって受信された脅威メッセージのさまざまなタイプが示されます。[脅威サマリー (Threat Summary) ] セクションには、[ウイルス (Virus) ]、[フィッシュ (Phish) ]、および[詐欺 (Scam) ] によるメッセージの内訳が示されます。

[過去1年間のアウトブレイクサマリー (Past Year Outbreak Summary) ] には、この1年間にわたるグローバル発生およびローカル発生が表示されるので、ローカルネットワークのトレンドとグローバルなトレンドを比較できます。グローバル発生リストは、すべての発生（ウイルスとウイルス以外の両方）の上位集合です。これに対して、ローカル発生は、お使いのアプライアンスに影響を与えたウイルス発生に限定されています。ローカル感染発生データには、ウイルス以外の脅威は含まれません。グローバル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、Threat Operations Center によって検出されたすべての発生を表します。ローカル感染発生データは、アウトブレイク隔離で現在設定されているしきい値を超えた、このアプライアンスで検出されたすべてのウイルス感染を表します。[ローカル保護の合計時間 (Total Local Protection Time) ] は、Threat Operations Center による各ウイルス発生の検出と、主要ベンダーによるアンチウイルスシグニチャの公開との時間差に常に基づいています。必ずしもすべてのグローバル発生が、お使いのアプライアンスに影響を与えるわけではありません。「--」値は、保護時間が存在しないか、アンチウイルスベンダーからシグニチャ時間を入手できないことを示します（一部のベンダーは、シグニチャ時間を報告しません）。これは、保護時間がゼロであることを示すのではなく、保護時間の算出に必要な情報を入手できないことを示します。

[隔離されたメッセージ (Quarantined Messages) ] セクションでは、感染フィルタの隔離状況の概要が示されます。これは、感染フィルタが捕捉した潜在的な脅威メッセージの数を把握するのに役立つ尺度です。隔離されたメッセージは、解放時に集計されます。通常、メッセージはアンチウイルスおよびアンチスパムルールが使用可能になる前に隔離されます。メッセージが解放されると、アンチウイルスおよびアンチスパムソフトウェアによってスキャンされ、陽性か、クリーンかを判定されます。感染トラッキングの動的性質により、メッセージが隔離領域内にあるときでも、メッセージの隔離ルール（および関連付けられる発生）が変更される場合があります。（隔離領域に入った時点ではなく）解放時にメッセージを集計することにより、件数の変動による混乱を防ぎます。

[脅威の詳細 (Threat Details) ] リストには、脅威のカテゴリ（ウイルス、詐欺、またはフィッシング）、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する情報が表示されます。ウイルス発生の場合は[過去1年間のウイルスアウトブレイク (Past Year Virus Outbreaks) ] に、発生の名前と ID、ウイルス発生が初めてグローバルに検出された日時、アウトブレイクフィルタによって提供される保護時間、および隔離されたメッセージの数が含まれます。グローバル発生またはローカル発生のどちらを表示するかを選択できます。

[最初にグローバルで確認した日時 (First Seen Globally)] の時間は、世界最大の電子メールおよび Web トラフィック モニタリング ネットワークである SenderBase のデータに基づいて、Threat Operations Center によって決定されます。[保護時間 (Protection Time)] は、Threat Operations Center による各脅威の検出と、主要ベンダーによるアンチウイルス シグニチャの解放との時間差に基づいています。

「--」値は、保護時間が存在しないか、アンチウイルスベンダーからシグニチャ時間を入手できないことを示します (一部のベンダーは、シグニチャ時間を報告しません)。保護時間がゼロであることを示しているわけではありません。むしろ、保護時間の算出に必要な情報を入手できないことを意味します。

このページの他のモジュールには次の情報が表示されます。

- 選択した期間にアウトブレイク フィルタによって処理された受信メッセージの数。

ウイルス以外の脅威には、外部 Web サイトへのリンクを使用したフィッシング電子メール、詐欺、およびマルウェア配布が含まれます。

- アウトブレイク フィルタで検出された脅威の重大度。

レベル5の脅威が範囲または影響において重大であるのに対し、レベル1は脅威のリスクが低いことを示します。脅威レベルの説明については、お使いの E メールセキュリティ アプライアンスのオンラインヘルプまたはユーザ ガイドを参照してください。

- メッセージがアウトブレイク隔離にとどまっていた時間。

この期間は、潜在的な脅威の安全性の判定に必要なデータを収集するためにかかる時間によって決まります。通常、ウイルス脅威を含むメッセージはアンチウイルスプログラムの更新を待機する必要があるため、ウイルス以外の脅威を含む場合よりも隔離に長くとどまります。各メールポリシーで指定した最大保持期間も反映されます。

- サイトのクリック時評価 (受信者がメッセージ内の悪意のある可能性があるリンクをクリックした場合) 用に、メッセージ受信者を Cisco Web セキュリティ プロキシにリダイレクトするために最も頻繁に書き換えられた URL。

いずれかの URL が悪意のある URL と見なされると、そのメッセージ内のすべての URL が書き換えられるため、このリストには悪質でない URL が含まれる場合があります。



- (注) [アウトブレイクフィルタ (Outbreak Filters)] レポート ページにテーブルが正しく表示されるためには、アプライアンスが、[セキュリティサービス (Security Services)] > [サービスのアップデート (Service Updates)] で指定した Cisco アップデート サーバと通信できる必要があります。[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アップデート設定 (Update Settings)]

詳細については、「Outbreak Filters」の章を参照してください。

## グレイメールのレポート

グレイメールの統計情報は、次のレポートに反映されます。

レポート	含まれるグレイメール データ
[メールフロー概要 (Mail Flow Summary) ] ページ > [着信 (Incoming) ] タブ	グレイメール カテゴリ (マーケティング、ソーシャル、およびバルク) ごとの着信グレイメール メッセージの数と、グレイメール メッセージの総数。
[メールフローの詳細 (Mail Flow Details) ] ページ > [送信者 (Outgoing Senders) ] タブ	グレイメールの上位送信者。
[メールフローの詳細 (Mail Flow Details) ] ページ > [着信メール (Incoming Mails) ] タブ	グレイメール カテゴリ (マーケティング、ソーシャル、およびバルク) ごとの着信グレイメール メッセージの数と、すべての IP アドレス、ドメイン名、またはネットワーク オーナーのグレイメール メッセージの総数。
[ユーザメールの概要 (User Mail Summary) ] ページ > [グレイメールの上位ユーザ (Top Users by Graymail) ]	グレイメールを受信する上位エンドユーザ。
[ユーザメールの概要 (User Mail Summary) ] ページ > [ユーザメールの詳細 (User Mail Details) ]	グレイメール カテゴリ (マーケティング、ソーシャル、およびバルク) ごとの着信グレイメール メッセージの数と、すべてのユーザのグレイメール メッセージの総数。

#### 関連項目

- [AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート \(108 ページ\)](#)

## AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート

AsyncOS 9.5 へのアップグレード後 :

- マーケティング メッセージの数は、アップグレードの前後に検出されたマーケティング メッセージの合計です。
- グレイメール メッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数は含まれません。
- 試行されたメッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数も含まれます。
- 管理対象の E メールセキュリティ アプライアンスでグレイメール機能が有効になっていない場合、マーケティング メッセージはクリーン メッセージとしてカウントされます。

## [システム容量 (System Capacity) ] ページ

[メール (Email) ]>[レポート (Reporting) ]>[システム容量 (System Capacity) ] ページでは、作業キュー内のメッセージ数、着信および発信メッセージ (量、サイズ、件数)、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページスワップ情報などシステム負荷の詳細が示されます。

[システム容量 (System Capacity) ] ページを使用すると、次の情報を確認できます。

- E メールセキュリティ アプライアンスが推奨されるキャパシティをいつ超えたかを特定します。これによって、設定の最適化や追加アプライアンスがいつ必要になったかがわかります。
- キャパシティの問題が今後発生する可能性を示すシステム挙動の過去のトレンド。
- トラブルシューティングのために、システムが最もリソースを使用している部分を識別します。

E メールセキュリティ アプライアンスをモニタして、キャパシティがメッセージ量に適したものになっているかを確認します。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。システムキャパシティをモニタする最も効果的な方法は、全体的な量、作業キュー内のメッセージ、およびリソース節約モードのインシデントを追跡することです。

- **量** : 「正常」なメッセージ量と環境内での「通常」のスパイクを把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール (Incoming Mail) ] ページおよび [送信メール (Outgoing Mail) ] ページを使用すると、経時的に量を追跡できます。詳細については、[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ] (111 ページ) および [システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ] (111 ページ) を参照してください。
- **ワーク キュー** : ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、非スパムメッセージの異常な増加を処理する、「緩衝装置」として設計されています。ただし、作業キューは負荷のかかっているシステムを示す指標でもあります。長く、頻繁な作業キューのバックアップは、キャパシティの問題を示している可能性があります。[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ] ページを使用すると、作業キュー内のアクティビティを追跡できます。詳細については、[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ] (110 ページ) を参照してください。
- **リソース節約モード** : アプライアンスがオーバーロードになると、リソース節約モード (RCM) になり、CRITICAL システム アラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。「リソース節約アクティビティ (112 ページ)」を参照してください。

## [システム容量 (System Capacity) ] ページに表示されるデータの解釈方法

[システム容量 (System Capacity) ] ページにデータを表示する時間範囲を選択する場合、次のことに留意することが重要です。

**[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ]**

- **Day レポート** : Day レポートでは、時間テーブルを照会し、24 時間の間に 1 時間ごとにアプライアンスが受信したクエリの正確な数を表示します。この情報は時間テーブルから収集されます。これは正確な数値です。
- **Month レポート** : Month レポートでは、30 日間または 31 日間（その月の日数に応じる）の日テーブルを照会し、30 日間または 31 日間の正確なクエリ数を表示します。これも正確な数値です。

[システム容量 (System Capacity) ] ページの [最大 (Maximum) ] 値インジケータは、指定された期間内の最大値を示します。[平均 (Average) ] 値は指定された期間内のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [平均 (Average) ] 値と [最大 (Maximum) ] 値を表示することができます。

特定のグラフの [詳細の表示 (View Details) ] リンクをクリックすると、個々の E メールセキュリティアプライアンスのデータおよびセキュリティ管理アプライアンスに接続されたアプライアンスのデータ全体が表示されます。

**[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ]**

[ワークキュー (Workqueue) ] ページには、ワーク キュー内でメッセージが費やした平均時間（スパム隔離またはポリシー、ウイルス、およびアウトブレイク隔離で費やした時間は除く）が表示されます。1 時間から 1 月までの時間範囲を表示できます。平均は、メール配信を遅延させた短期間のイベントおよびシステム上の負荷の長期トレンドの両方を識別するのに役立ちます。



**(注)** 隔離からワーク キューにメッセージが解放される場合、「ワーク キュー内の平均時間」メトリックではこの時間が無視されます。これにより、重複集計と検疫で費やされた延長時間による統計の歪みを回避できます。

このレポートでは、指定期間のワーク キュー内のメッセージの量および同期間のワーク キュー内の最大メッセージ数も示されます。ワーク キューの最大メッセージのグラフ表示でも、ワーク キューのしきい値レベルが示されます。

[ワークキュー (Workqueue) ] グラフにおける不定期のスパイクは、正常であり、発生する可能性があります。ワーク キュー内のメッセージが長期間、設定済みしきい値よりも大きい場合は、キャパシティの問題を示している可能性があります。このシナリオでは、しきい値レベルを調整することを検討するか、またはシステム設定を確認します。

ワーク キューのしきい値レベルを変更するには、[E メールセキュリティアプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。



**ヒント** [ワークキュー (Workqueue) ] ページを確認するときは、作業キューバックアップの頻度を測定し、10,000 メッセージを超える作業キューバックアップに注意することが推奨されます。

## [システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ]

[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ] ページには、着信接続、着信メッセージの総数、平均メッセージサイズ、着信メッセージの総サイズが示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。着信メール データと送信者プロフィール データを比較して、特定のドメインからネットワークに送信される電子メールメッセージの量のトレンドを表示することも推奨されます。



(注) 着信接続数の増加は、必ずしもシステム負荷に影響を与えるわけではありません。

## [システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ]

[システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ] ページには、発信接続、発信メッセージの総数、平均メッセージサイズ、発信メッセージの総サイズが示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。発信メール データと送信先データを比較して、特定のドメインまたは IP アドレスから送信される電子メールメッセージの量のトレンドを表示することも推奨されます。

## [システム容量 (System Capacity) ] : [システムの負荷 (System Load) ]

システムの負荷レポートに、次が表示されます。

- [全体のCPU使用率 \(Overall CPU Usage\)](#) (111 ページ)
- [メモリページスワップ \(Memory Page Swapping\)](#) (112 ページ)
- [リソース節約アクティビティ](#) (112 ページ)

### 全体のCPU使用率 (Overall CPU Usage)

Email Security Appliances は、アイドル状態の CPU リソースを使用してメッセージスループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステム キャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリページスワッピングが発生する場合、キャパシティの問題の可能性があります。



(注) このグラフには、目視基準である CPU 使用率のしきい値も示されます。この線の位置を調整するには、[E メールセキュリティ アプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。キャパシティの問題に対応するために実行できるアクションを提案するアラートを送信するように、E メールセキュリティ アプライアンスを設定できます。

## メモリページスワップ (Memory Page Swapping)

このページでは、メール処理、スパムおよびウイルスエンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す良い指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

### メモリページスワップ (Memory Page Swapping)

メモリ ページスワッピングのグラフは、システムによるディスクへのページングが必要な頻度を示します (KB/秒単位)。

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが常に高ボリュームのメモリ スワッピングを行う場合以外は、メモリ スワッピングは予想される正常な動作です (特に C170 アプライアンスの場合)。パフォーマンスを向上させるには、ネットワークに E メールセキュリティ アプライアンスを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。



(注) このグラフには、目視基準であるメモリ ページスワッピングのしきい値も示されます。この線の位置を調整するには、[E メールセキュリティ アプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。キャパシティの問題に対応するために実行できるアクションを提案するアラートを送信するように、E メールセキュリティ アプライアンスを設定できます。

### リソース節約アクティビティ

リソース節約アクティビティ グラフは、E メールセキュリティ アプライアンスがリソース節約モード (RCM) になった回数を示します。たとえば、グラフに  $n$  回と示されている場合は、アプライアンスが  $n$  回 RCM になり、少なくとも  $n-1$  回終了していることを意味します。

お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。リソース節約アクティビティ グラフにアプライアンスが頻繁に RCM になっていることが示されている場合は、システムが過負荷になっていることを示している可能性があります。

## [システム容量 (System Capacity) ] : [すべて (All) ]

[すべて (All) ] ページでは、これまでのすべてのシステムキャパシティ レポートを単一のページに統合し、さまざまなレポート同士の関係を表示することができます。たとえば、過剰なメモリ スワッピングの発生と同時期にメッセージ キューが高いことを確認できます。これは、キャパシティの問題の兆候である可能性があります。このページを PDF ファイルとして保存し、後で参照するために (またはサポート スタッフと共有するために) システム パフォーマンスのスナップショットを保存することが推奨されます。



## [システム容量 (System Capacity) ]グラフのしきい値インジケータ

一部のグラフでは、線は、これを頻繁または継続的に超える場合は問題を示している可能性があるデフォルト値です。このビジュアルインジケータを調整するには、[Eメールセキュリティアプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。

## [有効なレポートデータ (Reporting Data Availability) ] ページ

[メール (Email) ]>[レポート (Reporting) ]>[有効なレポートデータ (Reporting Data Availability) ] ページでは、リソース使用率および電子メールトラフィックの障害のある場所がリアルタイムに表示されるようにデータを表示、更新およびソートできます。

このページから、セキュリティ管理アプライアンスによって管理されるアプライアンス全体のデータアベイラビリティを含めて、すべてのデータリソース使用率および電子メールトラフィックに障害のある場所が表示されます。

このレポート ページから、特定のアプライアンスおよび時間範囲のデータアベイラビリティを表示することもできます。

# 新しいWebインターフェイスの電子メールレポートページの概要



- (注) このリストは、Eメールセキュリティアプライアンス用 AsyncOS のサポートされている最新リリースで、Web インターフェイスの [レポート (Reports) ] ドロップダウンから利用できるレポートを示します。詳細については、[インタラクティブレポート ページの使用 \(41 ページ\)](#) を参照してください。Eメールセキュリティアプライアンスで、これ以前のリリースの AsyncOS を実行している場合、これらのすべてのレポートは利用できません。

表 24: [電子メールレポート (Email Reports) ] ドロップダウンのオプション

[レポート (Reports) ] ドロップダウンのオプション	操作
[メールフロー概要 (Mail Flow Summary) ] ページ	[メールフロー概要 (Mail Flow Summary) ] レポート ページは、Eメールセキュリティアプライアンス上のアクティビティの概要を示します。これには、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。  詳細については、 <a href="#">[メールフロー概要 (Mail Flow Summary) ] ページ (118 ページ)</a> を参照してください。

[レポート (Reports) ] ドロップダウンのオプション	操作
[システム容量 (System Capacity) ] ページ	[システム容量 (System Capacity) ] レポートページには、セキュリティ管理アプライアンスに送信された、レポートデータの全体的なワークロードに関する詳細情報が表示されます。  詳細については、 <a href="#">[システム容量 (System Capacity) ] ページ (125 ページ)</a> を参照してください。
ファイルおよびマルウェアのレポート	
[高度なマルウェア防御 (Advanced Malware Protection) ] ページ (ファイルレピュテーションおよびファイル分析)	[高度なマルウェア防御 (Advanced Malware Protection) ] レポートページには、着信および送信ファイルベースの脅威についての、サマリー、ファイルレピュテーション、ファイル分析、ファイルレトロスペクション、およびメールボックス自動修復の詳細を表示するレポート ビューが表示されます。  詳細については、 <a href="#">[高度なマルウェア防御 (Advanced Malware Protection) ] ページ (129 ページ)</a> を参照してください。
[ウイルスフィルタリング (Virus Filtering) ] ページ	[ウイルスフィルタリング (Virus Filtering) ] レポートページでは、ネットワークで送受信されたウイルスの概要が示されます。このページには、Eメールセキュリティアプライアンスで動作するウイルススキャンエンジンによって検出され、セキュリティ管理アプライアンスに表示されるウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。  詳細については、 <a href="#">[ウイルスフィルタリング (Virus Filtering) ] ページ (137 ページ)</a> を参照してください。
[マクロ検出 (Macro Detection) ] ページ	[マクロ検出 (Macro Detection) ] レポート ページには、コンテンツフィルタとメッセージフィルタによって最も多く検出された、マクロが有効化された受信/発信添付ファイルがファイルタイプごとに表示されます。  詳細については、 <a href="#">[マクロ検出 (Macro Detection) ] ページ (139 ページ)</a> を参照してください。
電子メール脅威のレポート	
[DMARC検証 (DMARC Verification) ] ページ	[DMARC 検証 (DMARC Verification) ] レポート ページには、Domain-based Message Authentication, Reporting and Conformance (DMARC) 検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。  詳細については、 <a href="#">[DMARC検証 (DMARC Verification) ] ページ (140 ページ)</a> を参照してください。

[レポート (Reports) ] ドロップダウンのオプション	操作
[アウトブレイク フィルタリング (Outbreak Filtering) ] ページ	<p>[アウトブレイクフィルタ (Outbreak Filters) ] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、フィッシング、詐欺、ウイルス、およびマルウェア攻撃に対する防御をモニタします。</p> <p>詳細については、<a href="#">[アウトブレイク フィルタリング (Outbreak Filtering) ] ページ (141 ページ)</a> を参照してください。</p>
[URL フィルタリング (URL Filtering) ] ページ	<p>メッセージ内で最も頻繁に使用される URL カテゴリ、スパムメッセージ内の最も一般的な URL、メッセージに表示される悪意のある URL およびニュートラル URL の数を確認するには、このページを使用します。</p> <p>詳細については、<a href="#">[URL フィルタリング (URL Filtering) ] ページ (144 ページ)</a> を参照してください。</p>
[偽装メールの検出 (Forged Email Detection) ] ページ	<p>[偽造メールの検出 (Forged Email Detection) ] レポート ページには、次のレポートが含まれています。</p> <ul style="list-style-type: none"> <li>偽装メールの検出数の上位。受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。</li> <li>偽装メールの検出：詳細。受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。</li> </ul> <p>詳細については、<a href="#">[偽装メールの検出 (Forged Email Detection) ] ページ (146 ページ)</a> を参照してください。</p>
[送信者ドメインのレピュテーション (Sender Domain Reputation) ] ページ	<p>このレポートページでは、SDR サービスで受信した判定や脅威カテゴリに基づいて着信メッセージを表示できます。</p> <p>詳細については、<a href="#">[送信者ドメインのレピュテーション (Sender Domain Reputation) ] ページ (147 ページ)</a> を参照してください。</p>

[レポート (Reports) ] ドロップダウンのオプション	操作
[外部脅威フィード (External Threat Feeds) ] ページ	<p>[外部脅威フィード (External Threat Feeds) ] ページには、次のレポートが表示されます。</p> <ul style="list-style-type: none"> <li>• メッセージで脅威を検出するために使用される上位 ETF ソース。</li> <li>• メッセージで検出された脅威に一致する上位 IOC。</li> <li>• 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソース。</li> </ul> <p>詳細については、<a href="#">[外部脅威フィード (External Threat Feeds) ] ページ (146 ページ)</a> を参照してください。</p>
接続およびフローのレポート	
[メール フローの詳細 (Mail Flow Details) ] ページ	<p>[メール フローの詳細 (Mail Flow Details) ] レポート ページには、管理対象の E メールセキュリティ アプライアンスに接続するすべてのリモートホストのリアルタイム情報に関するインタラクティブレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー (組織) の情報を収集できます。</p> <p>詳細については、<a href="#">[メール フローの詳細 (Mail Flow Details) ] ページ (147 ページ)</a> を参照してください。</p>
[送信者グループ (Sender Groups) ] レポート ページ	<p>[送信者グループ (Sender Groups) ] レポート ページには、送信者グループ別およびメール フロー ポリシー アクション別に接続の要約が表示され、SMTP 接続およびメール フロー ポリシーのトレンドを確認できます。</p> <p>詳細については、<a href="#">#unique_197</a>を参照してください。</p>
[送信先 (Outgoing Destinations) ] ページ	<p>[送信先 (Outgoing Destinations) ] レポート ページには、組織がメールを送信するドメインについての情報が表示されます。ページの上部には、発信脅威メッセージごとの上位の宛先、および発信クリーンメッセージ別の上位の宛先を示すグラフが表示されます。ページの下部には、総受信者数別にソートされた (デフォルト設定) 列を示す表が表示されます。</p> <p>詳細については、<a href="#">[送信先 (Outgoing Destinations) ] ページ (157 ページ)</a> を参照してください。</p>

[レポート (Reports) ] ドロップダウンのオプション	操作
[TLS 接続 (TLS Connections) ] ページ	<p>[TLS 暗号化 (TLS Encryption) ] レポート ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。</p> <p>詳細については、<a href="#">#unique_199</a>を参照してください。</p>
[受信 SMTP 認証 (Inbound SMTP Authentication) ] ページ	<p>[受信 SMTP 認証 (Inbound SMTP Authentication) ] レポート ページには、クライアント証明書の使用情報、および E メールセキュリティ アプライアンスとユーザのメールクライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。</p> <p>詳細については、<a href="#">[受信 SMTP 認証 (Inbound SMTP Authentication) ] ページ (161 ページ)</a> を参照してください。</p>
[レート制限 (Rate Limits) ] ページ	<p>[レート制限 (Rate Limits) ] レポート ページには、送信者あたりのメッセージ受信者数に対して設定したしきい値を超える電子メール送信者 (MAIL-FROM アドレスに基づく) が表示されます。</p> <p>詳細については、<a href="#">[レート制限 (Rate Limits) ] ページ (163 ページ)</a> を参照してください。</p>
[国別の接続 (Connections by Country) ] ページ	<p>[国別の接続 (Connections by Country) ] レポート ページには以下が表示されます。</p> <ul style="list-style-type: none"> <li>• 発信国別の受信メール接続数の上位 (グラフィカルな形式)。</li> <li>• 発信国別の受信メール接続およびメッセージの合計数 (表形式)。</li> </ul> <p>詳細については、<a href="#">[国別の接続 (Connections by Country) ] ページ (164 ページ)</a> を参照してください。</p>
ユーザ レポート	
[ユーザ メール サマリー (User Mail Summary) ] ページ	<p>[ユーザ メール サマリー (User Mail Summary) ] レポートには、電子メールアドレスごとに内部ユーザによって送受信された電子メールについての情報が表示されます。1 人のユーザが複数の電子メールアドレスを持っている場合があります。レポートでは、電子メールアドレスがまとめられません。</p> <p>詳細については、<a href="#">#unique_203</a>を参照してください。</p>

[レポート (Reports) ] ドロップダウンのオプション	操作
[DLP インシデント サマリー (DLP Incident Summary) ] ページ	[DLP インシデント サマリー (DLP Incident Summary) ] ページには、送信メールで発生したデータ漏洩防止 (DLP) ポリシー違反のインシデントに関する情報が表示されます。  詳細については、 <a href="#">[DLP インシデント サマリー (DLP Incident Summary) ] ページ (168 ページ)</a> を参照してください。
[Web インタラクション (Web Interaction) ] ページ	[Web インタラクション (Web Interaction) ] レポート ページは、ポリシーまたはアウトブレイク フィルタによって書き換えられた URL をクリックしたエンドユーザと、各ユーザクリックに関連付けられたアクションを示します。  詳細については、 <a href="#">#unique_205</a> を参照してください。
フィルタのレポート	
[メッセージフィルタ (Message Filters) ] ページ	[メッセージフィルタ (Message Filters) ] レポート ページには、送受信メッセージのメッセージフィルタの上位一致 (最も多くのメッセージに一致したメッセージフィルタ) に関する情報が表示されます。  詳細については、 <a href="#">[メッセージフィルタ (Message Filters) ] ページ (172 ページ)</a> を参照してください。
[大容量のメール (High Volume Mail) ] ページ	[大容量のメール (High Volume Mail) ] レポート ページでは、1人の送信者から送られていたり、件名が同じであったりする、特定の1時間の間に送られた多数のメッセージに関する攻撃が特定されます。  詳細については、 <a href="#">[大容量のメール (High Volume Mail) ] ページ (172 ページ)</a> を参照してください。
[コンテンツフィルタ (Content Filters) ] ページ	[コンテンツフィルタ (Content Filters) ] レポート ページには、送受信コンテンツフィルタの上位一致 (最も多くのメッセージに一致したコンテンツ フィルタ) に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。  詳細については、 <a href="#">[コンテンツフィルタ (Content Filters) ] ページ (173 ページ)</a> を参照してください。

## [メールフロー概要 (Mail Flow Summary) ] ページ

セキュリティ管理アプライアンスの [メールフロー概要 (Mail Flow Summary) ] レポート ページは、Eメールセキュリティ アプライアンスからの Eメールメッセージアクティビティの概

要を示します。[メールフロー概要 (Mail Flow Summary)] レポート ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

[メールフロー概要：着信 (Mail Flow Summary : Incoming)] レポート ページは、アプライアンスで処理およびブロックされたメッセージの合計数についての着信メール グラフと、着信メールの概要を示します。

このページのメール トレンド グラフを使用して、選択した時間範囲に基づいてアプライアンスで処理およびブロックされたすべての着信メールのフローをモニタできます。詳細については、[レポートの時間範囲の選択 \(27 ページ\)](#) を参照してください。

データ内の特定の情報を検索するには、次を参照してください。[検索およびインタラクティブ電子メール レポート ページ \(61 ページ\)](#)

次のメール トレンド グラフは、着信メール フローを視覚的に表したものです。

- 脅威検出の概要
- コンテンツの概要

それぞれのカテゴリの必須カウンタに基づいて、着信メッセージのメールトレンドを表示できます。詳細については、[カウンタを使用するの、トレンドグラフ上のデータのフィルタリング \(46 ページ\)](#) を参照してください。

[メールフロー概要：発信 (Mail Flow Summary : Outgoing)] レポート ページは、アプライアンスによって処理および配信されたメッセージの合計数についての発信メール グラフと、発信メールの概要を示します。

このページのメール トレンド グラフを使用して、選択した時間範囲に基づいてアプライアンスによって処理および配信されたすべての送信メールのフローをモニタできます。詳細については、[レポートの時間範囲の選択 \(27 ページ\)](#) を参照してください。

次のメール トレンド グラフは、送信メールのメール フローを視覚的に表したものです。

処理されたメッセージの必須カウンタに基づいて、発信メッセージのメールトレンドを表示できます。詳細については、[カウンタを使用するの、トレンドグラフ上のデータのフィルタリング \(46 ページ\)](#) を参照してください。

次のリストでは、[メールフロー概要 (Mail Flow Summary)] レポート ページのさまざまなセクションについて説明します。

表 25: [メールフロー概要 (Mail Flow Summary)] ページの詳細

セクション	説明
メール フロー概要：着信	
メッセージ数 (Number of Messages)	[メッセージ数 (Number of Messages)] のグラフは、処理されたメッセージの合計数 (脅威メッセージとして処理されたメッセージを含む) を視覚的に表現します。

セクション	説明
脅威メッセージ (Threat Messages)	[脅威メッセージ (Threat Messages) ] グラフは、E メールセキュリティ アプライアンスによってブロックされたメッセージの合計数を視覚的に表現します。
脅威検出のサマリー (Threat Detection Summary)	<p>[脅威検出のサマリー (Threat Detection Summary) ] メールトレンドグラフは、次のカテゴリに基づく視覚的な表現です。</p> <ul style="list-style-type: none"> <li>• [接続およびレピュテーションのフィルタリング (Connection and Reputation Filtering) ] : レピュテーションフィルタリングと無効な受信者によって脅威として分類されるメッセージ。</li> <li>• [スパム検出 (Spam Detection) ] : スпам対策スキャンエンジンによって脅威として分類されるメッセージ。</li> <li>• [電子メールスプーフィング (Email Spoofing) ] : DMARC 検証エラーのために脅威として分類されるメッセージ。</li> <li>• [アウトブレイク脅威サマリー (Outbreak Threat Summary) ] : アウトブレイク フィルタリング エンジンによってフィッシング、詐欺、ウイルス、またはマルウェアとして分類されるメッセージ。</li> <li>• [添付ファイルとマルウェアの検出 (Attachment and Malware Detection) ] : アンチウイルスおよび AMP エンジンによって脅威として分類されるメッセージ。</li> <li>• [すべてのカテゴリ (All Categories) ] : 脅威として分類されるすべてのメッセージ。</li> </ul>
コンテンツ サマリー (Content Summary)	<p>[コンテンツ サマリー (Content Summary) ] メールトレンドグラフは、次のカテゴリに基づく視覚的な表現です。</p> <ul style="list-style-type: none"> <li>• [グレイメール (Graymail) ] : マーケティング、バルク、またはソーシャル ネットワーキングとして分類されるメッセージ。</li> <li>• [コンテンツ フィルタ (Content Filters) ] : コンテンツ フィルタにより分類されるメッセージ。</li> <li>• [すべてのカテゴリ (All Categories) ] : graymail エンジンおよびコンテンツ フィルタによって分類されるすべてのメッセージ。</li> </ul>
メール フロー概要 : 発信	



セクション	説明
メッセージ数 (Number of Messages)	[メッセージ数 (Number of Messages)] のグラフは、処理されたメッセージの合計数 (クリーンであるとして処理されたメッセージを含む) を視覚的に表現します。
メッセージ配信 (Message Delivery)	[メッセージ配信 (Message Delivery)] のグラフは、ハードバウンスを含む、配信されるメッセージの合計数を視覚的に表現します。
送信メール (Outgoing Mails)	[送信メール (Outgoing Mails)] トレンド グラフは、次のカテゴリに基づく視覚的な表現です。 <ul style="list-style-type: none"> <li>• スпам検出 (Spam Detected)</li> <li>• ウイルス検出 (Virus Detected)</li> <li>• AMP で検出 (Detected by AMP)</li> <li>• コンテンツ フィルタによる停止 (Stopped by Content Filters)</li> <li>• DLP による停止 (Stopped by DLP)</li> </ul>

#### 関連項目

- [アプライアンスによる電子メール メッセージの分類方法 \(72 ページ\)](#)
- [受信メール メッセージのカウント方法 \(72 ページ\)](#)
- [\[メールフロー概要 \(Mail Flow Summary\)\] ページでの電子メール メッセージの分類 \(122 ページ\)](#)

## 受信メール メッセージのカウント方法

受信メッセージの数は、メッセージごとの受信者数に応じて異なります。たとえば、example.com から 3 人の受信者に送信された着信メッセージは、その送信者からの 3 通のメッセージとしてカウントされます。

送信者レピュテーションフィルタリングによってブロックされたメッセージは、実際にはワークキューに入らないので、アプライアンスは、受信メッセージの受信者のリストにアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数は既存の顧客データの大規模なサンプリング調査に基づいています。

## アプライアンスによる電子メール メッセージの分類方法

メッセージは電子メールパイプラインを通過するので、複数のカテゴリに該当する場合があります。たとえば、メッセージにスパム陽性またはウイルス陽性というマークを付けることがで

きます。コンテンツフィルタに一致させることもできます。各種フィルタとスキャンアクティビティの優先順位は、メッセージ処理の結果に大きく影響します。

上記の例では、各種判定は次の優先ルールに従います。

- スпам陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

これらのルールに従って、メッセージがスパム陽性とマークされた場合、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されていれば、このメッセージがドロップされてスパム カウンタが増分します。

さらに、スパム陽性のメッセージを引き続き電子メールパイプラインで処理するようにアンチスパム設定が設定されている場合、以降のコンテンツフィルタがこのメッセージをドロップ、バウンス、または隔離しても、スパムカウンタは増分します。メッセージがスパム陽性またはウイルス陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

また、メッセージがアウトブレイクフィルタによって隔離された場合、隔離からリリースされてワーク キューで再度処理されるまで集計されません。

メッセージ処理の優先順位の詳細については、お使いの E メールセキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドで、電子メールパイプラインに関する章を参照してください。

## [メールフロー概要 (Mail Flow Summary) ] ページでの電子メール メッセージの分類

脅威とみなされる受信メッセージおよび [メールフロー概要 (Mail Flow Summary) ] レポート ページで配信される送信メッセージは、次のとおり分類されます。

表 26: [メールフロー概要 (Mail Flow Summary) ] ページ上のメールのカテゴリ

カテゴリ (Category)	説明
メール フロー概要 : 着信	

カテゴリ (Category)	説明
評価フィルタリング	<p>HAT ポリシーによってブロックされたすべての接続数に、固定乗数 (受信メールメッセージのカウント方法 (72 ページ) を参照) を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。</p> <p>[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering)] の値は、次の要素に基づいて算出されます。</p> <ul style="list-style-type: none"> <li>• この送信者からの「調整された」メッセージの数。</li> <li>• 拒否された、またはTCP拒否の接続数 (部分的に集計されます)。</li> <li>• 接続ごとのメッセージ数に対する控えめな乗数。</li> </ul> <p>アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。このような状況で表示される値は、停止されたメッセージの最小数を示す値として解釈されます。</p> <p>[メールフロー概要 (Mail Flow Summary)] レポート ページ上の評価フィルタリングの総数および割合は、すべての拒否された接続の数に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。</p>
無効な受信者	従来のLDAP拒否によって拒否されたすべてのメール受信者数にすべてのRAT拒否数を加えた総数および割合。
スパム対策	アンチスパム スキャン エンジンで陽性、または疑いありとして検出された受信メッセージの総数および割合。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。

カテゴリ (Category)	説明
ウイルス対策	<p>ウイルスとしては陽性だがスパムではないと検出された受信メッセージの総数および割合。</p> <p>次のメッセージは、[ウイルス検出 (Virus Detected) ] カテゴリに集計されます。</p> <ul style="list-style-type: none"> <li>• ウイルス スキャン結果が [修復 (Repaired) ] または [感染している (Infectious) ] であるメッセージ</li> <li>• 暗号化されたメッセージを、ウイルスを含むメッセージとして集計するオプションが選択されている場合に、ウイルス スキャン結果が [暗号化 (Encrypted) ] であるメッセージ</li> <li>• スキャンできないメッセージに対するアクションが [「配信」なし (NOT "Deliver") ] の場合に、ウイルス スキャン結果が [スキャン不可 (Unscannable) ] であるメッセージ</li> <li>• 代替メールホストまたは代替受信者へ送信するオプションが選択されている場合に、ウイルス スキャン結果が [スキャン不可 (Unscannable) ] または [暗号化 (Encrypted) ] であるメッセージ</li> <li>• アウトブレイク隔離から手動またはタイムアウトにより削除されたメッセージ</li> </ul>
高度なマルウェア防御	<p>合計数とファイル分析サービスによりブロックされた受信メッセージの総数および割合。</p> <p>メッセージ添付ファイルは、レピュテーションフィルタリングによって悪意のある添付ファイルとして検出されました。この値には、ファイル分析により悪意があると検出された判定のアップデートまたはファイルは含まれません。</p>
コンテンツ フィルタ	メッセージやコンテンツフィルタにより停止された受信メッセージの総数および割合。
DMARC ポリシー	DMARC 検証ポリシーを失敗した受信メッセージの総数および割合。
S/MIME 検証/復号に失敗	S/MIME 検証、復号またはその両方に失敗したメッセージの総数および割合。
<b>メール フロー概要 : 発信</b>	
ハード バウンス	永久に配信不能な送信メッセージの総数および割合。
配信済み	配信される送信メッセージの総数および割合。



(注) スキャンできないメッセージまたは暗号化されたメッセージを配信するようにアンチウイルス設定を行った場合、これらのメッセージは、ウイルス陽性としてではなく、クリーンメッセージとして集計されます。それ以外の場合は、メッセージはウイルス陽性として集計されます。

さらに、メッセージがメッセージフィルタと一致し、フィルタによってドロップされたり、バウンスされたりしていない場合、クリーンなメッセージとして扱われます。メッセージフィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

#### 関連項目

[\[メールフローの詳細 \(Mail Flow Details\)\] ページ \(147 ページ\)](#)

## [システム容量 (System Capacity)] ページ

[システム容量 (System Capacity)] レポート ページでは、作業キュー内のメッセージ数、着信および発信メッセージ (量、サイズ、件数)、全体的な CPU 使用率、機能別の CPU 使用率、メモリ ページスワップ情報などシステム負荷の詳細が示されます。

[システム容量 (System Capacity)] レポート ページを使用すると、次の情報を確認できます。

- E メールセキュリティ アプライアンスが推奨されるキャパシティをいつ超えたかを特定します。これによって、設定の最適化や追加アプライアンスがいつ必要になったかがわかります。
- キャパシティの問題が今後発生する可能性を示すシステム挙動の過去のトレンド。
- トラブルシューティングのために、システムが最もリソースを使用している部分を識別します。

セキュリティ管理アプライアンスで [システム容量 (System Capacity)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [システム容量 (System Capacity)] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

E メールセキュリティ アプライアンスをモニタして、キャパシティがメッセージ量に適したものになっているか確認することができます。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。システム キャパシティをモニタする最も効果的な方法は、全体的な量、作業キュー内のメッセージ、およびリソース節約モードのインシデントを追跡することです。

- **量** : 「正常」なメッセージ量と環境内での「通常」のスパイクを把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール (Incoming Mail)] ページおよび [送信メール (Outgoing Mail)] ページを使用すると、経時的に量を追跡できます。詳細については、[\[システム容量 \(System Capacity\)\] : \[受信メール \(Incoming Mail\)\] \(111 ページ\)](#) および [\[システム容量 \(System Capacity\)\] : \[送信メール \(Outgoing Mail\)\] \(111 ページ\)](#) を参照してください。

- **ワーク キュー** : ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、非スパムメッセージの異常な増加を処理する、「緩衝装置」として設計されています。ただし、作業キューは負荷のかかっているシステムを示す指標でもあります。長く、頻繁な作業キューのバックアップは、キャパシティの問題を示している可能性があります。[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ] ページを使用すると、作業キュー内のアクティビティを追跡できます。詳細については、[システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ] (110 ページ) を参照してください。
- **リソース節約モード** : アプライアンスがオーバーロードになると、リソース節約モード (RCM) になり、CRITICAL システム アラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。リソース節約アクティビティ (112 ページ) を参照してください。

#### 関連項目

- [システム容量 (System Capacity) ] ページに表示されるデータの解釈方法 (109 ページ)
- [システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ] (110 ページ)
- [システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ] (111 ページ)
- [システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ] (111 ページ)
- [システム容量 (System Capacity) ] : [すべて (All) ] (112 ページ)
- [システム容量 (System Capacity) ] グラフのしきい値インジケータ (113 ページ)

## [システム容量 (System Capacity) ] ページに表示されるデータの解釈方法

[システム容量 (System Capacity) ] ページにデータを表示する時間範囲を選択する場合、次のことに留意することが重要です。

- **Day レポート** : Day レポートでは、時間テーブルを照会し、24 時間の間に 1 時間ごとにアプライアンスが受信したクエリの正確な数を表示します。この情報は時間テーブルから収集されます。これは正確な数値です。
- **Month レポート** : Month レポートでは、30 日間または 31 日間 (その月の日数に応じる) の日テーブルを照会し、30 日間または 31 日間の正確なクエリ数を表示します。これも正確な数値です。

[システム容量 (System Capacity) ] ページの [最大 (Maximum) ] 値インジケータは、指定された期間内の最大値を示します。[平均 (Average) ] 値は指定された期間内のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [平均 (Average) ] 値と [最大 (Maximum) ] 値を表示することができます。

特定のグラフの [詳細の表示 (View Details) ] リンクをクリックすると、個々の E メールセキュリティアプライアンスのデータおよびセキュリティ管理アプライアンスに接続されたアプライアンスのデータ全体が表示されます。

## [システム容量 (System Capacity) ] : [ワークキュー (Workqueue) ]

[ワークキュー (Workqueue) ] ページには、ワーク キュー内でメッセージが費やした平均時間 (スパム隔離またはポリシー、ウイルス、およびアウトブレイク隔離で費やした時間は除く) が表示されます。1 時間から 1 月までの時間範囲を表示できます。平均は、メール配信を遅延させた短期間のイベントおよびシステム上の負荷の長期トレンドの両方を識別するのに役立ちます。



- (注) 隔離からワーク キューにメッセージが解放される場合、「ワーク キュー内の平均時間」メトリックではこの時間が無視されます。これにより、重複集計と検疫で費やされた延長時間による統計の歪みを回避できます。

このレポートでは、指定期間のワーク キュー内のメッセージの量および同期間のワーク キュー内の最大メッセージ数も示されます。ワーク キューの最大メッセージのグラフ表示でも、ワーク キューのしきい値レベルが示されます。

[ワークキュー (Workqueue) ] グラフにおける不定期のスパイクは、正常であり、発生する可能性があります。ワーク キュー内のメッセージが長期間、設定済みしきい値よりも大きい場合は、キャパシティの問題を示している可能性があります。このシナリオでは、しきい値レベルを調整することを検討するか、またはシステム設定を確認します。

ワーク キューのしきい値レベルを変更するには、[E メールセキュリティアプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。



- ヒント [ワークキュー (Workqueue) ] ページを確認するときは、作業キューバックアップの頻度を測定し、10,000 メッセージを超える作業キューバックアップに注意することが推奨されます。

## [システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ]

[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ] ページには、着信接続、着信メッセージの総数、平均メッセージサイズ、着信メッセージの総サイズが示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[システム容量 (System Capacity) ] : [受信メール (Incoming Mail) ] ページを使用すると、経時的にメール量の増加を追跡し、システム キャパシティの計画を立てることができます。着信メール データと送信者プロフィール データを比較して、特定のドメインからネットワークに送信される電子メールメッセージの量のトレンドを表示することも推奨されます。



(注) 着信接続数の増加は、必ずしもシステム負荷に影響を与えるわけではありません。

## [システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ]

[システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ] ページには、発信接続、発信メッセージの総数、平均メッセージサイズ、発信メッセージの総サイズが示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常のメッセージ量とスパイクのトレンドを理解しておくことが重要です。[システム容量 (System Capacity) ] : [送信メール (Outgoing Mail) ] ページを使用すると、経時的にメール量の増加を追跡し、システムキャパシティの計画を立てることができます。発信メールデータと送信先データを比較して、特定のドメインまたは IP アドレスから送信される電子メールメッセージの量のトレンドを表示することも推奨されます。

## [システム容量 (System Capacity) ] : [システムの負荷 (System Load) ]

システムの負荷レポートに、次が表示されます。

- 全体のCPU使用率 (Overall CPU Usage) (111 ページ)
- メモリページスワップ (Memory Page Swapping) (112 ページ)
- リソース節約アクティビティ (112 ページ)

### 全体のCPU使用率 (Overall CPU Usage)

Email Security Appliances は、アイドル状態の CPU リソースを使用してメッセージスループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステムキャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリページスワッピングが発生する場合、キャパシティの問題の可能性がります。



(注) このグラフには、目視基準である CPU 使用率のしきい値も示されます。この線の位置を調整するには、[E メールセキュリティアプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。キャパシティの問題に対応するために実行できるアクションを提案するアラートを送信するように、E メールセキュリティアプライアンスを設定できます。

このページでは、メール処理、スパムおよびウイルスエンジン、レポート、および隔離などさまざまな機能によって使用される CPU の量を表示するグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使用する製品の領域を示す良い指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

### メモリページスワップ (Memory Page Swapping)

メモリページスワッピングのグラフは、システムによるディスクへのページングが必要な頻度を示します (KB/秒単位)。



システムは、定期的にメモリをスワップするように設計されているので、一部のメモリスワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが常に高ボリュームのメモリスワッピングを行う場合以外は、メモリスワッピングは予想される正常な動作です（特にC170アプライアンスの場合）。パフォーマンスを向上させるには、ネットワークにEメールセキュリティアプライアンスを追加するか、設定を調整して、最大のスループットを確保することが必要な場合もあります。



(注) このグラフには、目視基準であるメモリ ページスワッピングのしきい値も示されます。この線の位置を調整するには、[Eメールセキュリティアプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。キャパシティの問題に対応するために実行できるアクションを提案するアラートを送信するように、Eメールセキュリティアプライアンスを設定できます。

## リソース節約アクティビティ

リソース節約アクティビティ グラフは、Eメールセキュリティアプライアンスがリソース節約モード (RCM) になった回数を示します。たとえば、グラフにn回と示されている場合は、アプライアンスがn回 RCM になり、少なくとも n-1 回終了していることを意味します。

お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。リソース節約アクティビティ グラフにアプライアンスが頻繁に RCM になっていることが示されている場合は、システムが過負荷になっていることを示している可能性があります。

## [システム容量 (System Capacity) ] : [すべて (All) ]

[すべて (All) ] ページでは、これまでのすべてのシステムキャパシティ レポートを単一のページに統合し、さまざまなレポート同士の関係を表示することができます。たとえば、過剰なメモリスワッピングの発生と同時期にメッセージキューが高いことを確認できます。これは、キャパシティの問題の兆候である可能性があります。このページを PDF ファイルとして保存し、後で参照するために（またはサポート スタッフと共有するために）システム パフォーマンスのスナップショットを保存することが推奨されます。

## [システム容量 (System Capacity) ] グラフのしきい値インジケータ

一部のグラフでは、線は、これを頻繁または継続的に超える場合は問題を示している可能性があるデフォルト値です。このビジュアルインジケータを調整するには、[Eメールセキュリティアプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#) を参照してください。

## [高度なマルウェア防御 (Advanced Malware Protection) ] ページ

高度なマルウェア防御は、次によりゼロデイや電子メールの添付ファイル内のファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザーに通知する。

この機能は着信メッセージと発信メッセージに使用できます。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザ ガイドまたはEメールセキュリティ アプライアンスの AsyncOS のオンラインヘルプを参照してください。

レポート ページを表示するには、[レポート (Reports) ] ドロップダウンの [フィルタおよびマルウェアのレポート (Filter and Malware Reports) ] セクションから [高度なマルウェア防御 (Advanced Malware Protection) ] を選択します。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページには、次のレポート ビューが表示されます。

- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] : \[概要 \(Summary\) \] \(131 ページ\)](#)
- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] - \[AMP レピュテーション \(AMP Reputation\) \] \(131 ページ\)](#)
- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] - \[ファイル分析 \(File Analysis\) \] \(133 ページ\)](#)
- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] - \[ファイル レトロスペクション \(File Retrospection\) \] \(133 ページ\)](#)
- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] - \[メールボックスの自動修復 \(Mailbox Auto Remediation\) \] \(134 ページ\)](#)

セキュリティ管理アプライアンスで [高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [高度なマルウェア防御 (Advanced Malware Protection) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページには、Cisco Threat Grid アプライアンスに接続されたすべての管理対象のアプライアンスのリアルタイム データを提供するメトリック バーが表示されます。



- (注)
- メトリック バーでデータを設定するには、CLI で `trailblazerconfig > enable` コマンドを使用する必要があります。詳細については、[trailblazerconfig コマンド \(566 ページ\)](#) を参照してください。
  - Cisco Threat Grid アプライアンスのデータを表示できるのは、日別、週別、および月別のみです。

#### 関連項目

- [SHA-256 ハッシュによるファイルの識別 \(97 ページ\)](#)
- [ファイル分析レポートの詳細の要件 \(95 ページ\)](#)
- [その他のレポートでのファイルレピュテーションフィルタ データの表示 \(101 ページ\)](#)

## [高度なマルウェア防御 (Advanced Malware Protection) ] : [概要 (Summary) ]

[高度なマルウェア防御 (Advanced Malware Protection) ] : [概要 (Summary) ] ページには、ファイルレピュテーションおよびファイル分析サービスで識別される受信および送信ファイルベースの脅威の概要の全体が表示されます。

詳細については、「[\[高度なマルウェア防御 \(Advanced Malware Protection\) \]-\[AMP レピュテーション \(AMP Reputation\) \] \(131 ページ\)](#)」および「[\[高度なマルウェア防御 \(Advanced Malware Protection\) \]-\[ファイル分析 \(File Analysis\) \] \(133 ページ\)](#)」を参照してください。

## [高度なマルウェア防御 (Advanced Malware Protection) ]-[AMP レピュテーション (AMP Reputation) ]

[高度なマルウェア防御 (Advanced Malware Protection) ]-[AMP レピュテーション (AMP Reputation) ] ページには、ファイルレピュテーションサービスによって識別された、受信および送信されたファイルベースの脅威が表示されます。

判定が変更されたファイルについては、[\[AMP判定のアップデート \(AMP Verdict Updates\) \]](#) レポートを参照してください。これらの判定は、[\[高度なマルウェア防御 \(Advanced Malware Protection\) \]](#) レポートに反映されません。

圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [\[高度なマルウェア防御 \(Advanced Malware Protection\) \]](#) レポートに含まれます。

[AMPにより処理された受信ファイル (Incoming files handled by AMP) ] セクションには、受信したマルウェアファイルが [\[悪意のある \(Malicious\) \]](#)、[\[正常 \(Clean\) \]](#)、[\[不明 \(Unknown\) \]](#)、[\[スキャン不可能 \(Unscannable\) \]](#)、[\[低リスク \(Low Risk\) \]](#) などのさまざまなカテゴリ別に表示されます。

悪意のある受信ファイルは、次のように分類されます。

- [マルウェア (Malware) ] に分類される AMP レピュテーション サーバで受信したブラックリストファイル SHA の割合。
- [カスタム検出 (Custom Detection) ] に分類される AMP for Endpoints コンソールで受信したブラックリストファイル SHA の割合。AMP for Endpoints コンソールから取得されるブラックリストに追加されたファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル (Incoming Malware Threat Files) ] セクションで [シンプルカスタム検出 (Simple Custom Detection) ] として表示されます。
- [カスタムしきい値 (Custom Threshold) ] に分類されるしきい値設定に基づくブラックリストファイル SHA の割合。

レポートの [詳細 (More Details) ] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブラックリスト追加ファイル SHA のファイル トラジェクトリ詳細を表示できます。

[リスク低 (Low Risk) ] 判定の詳細をレポートの [AMPにより渡された受信ファイル (Incoming Files Handed by AMP) ] セクションに表示できます。

[高度なマルウェア防御 : 受信 (Advanced Malware Protection: Incoming) ] レポート ページの [AMP レピュテーション (AMP Reputation) ] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル レピュテーション サービスによって識別された受信ファイルの概要 (グラフ形式) 。
- 選択した時間範囲に受信されたすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位の受信マルウェア脅威ファイル。
- 上位の受信マルウェア脅威ファイル (ファイル タイプ別) 。
- 上位の受信マルウェア脅威ファイルを一覧表示する [受信したマルウェア脅威ファイル (Incoming Malware Threat Files) ] インタラクティブ テーブル。

ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の青い番号のリンクをクリックします。

[高度なマルウェア防御 : 送信 (Advanced Malware Protection: Outgoing) ] レポート ページの [AMP レピュテーション (AMP Reputation) ] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル レピュテーション サービスによって識別された送信ファイルの概要 (グラフ形式) 。
- 選択した時間範囲に送信されたすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位の送信マルウェア脅威ファイル。
- 上位の送信マルウェア脅威ファイル (ファイル タイプ別) 。

- 上位の送信マルウェア脅威ファイルを一覧表示する [送信したマルウェア脅威ファイル (Outgoing Malware Threat Files)] インタラクティブ テーブル。  
ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。  
アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の青い番号のリンクをクリックします。

## [高度なマルウェア防御 (Advanced Malware Protection)]-[ファイル分析 (File Analysis)]

[高度なマルウェア防御 (Advanced Malware Protection)]-[ファイル分析 (File Analysis)] ページには、分析のために送信された各ファイルについて、時刻と判定 (または中間判定) が表示されます。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。

1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。

オンプレミスの Cisco AMP Threat Grid アプライアンスでの導入の場合：AMP Threat Grid アプライアンスでホワイトリストに登録されているファイルは、「クリーン」として表示されません。ホワイトリストについては、AMP Threat Grid のマニュアルまたはオンライン ヘルプを参照してください。

ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。詳細については、[SHA-256 ハッシュによるファイルの識別 \(97 ページ\)](#) を参照してください。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の [詳細 (Details)] リンクをクリックします。

ファイルを分析したサーバに関する詳細を表示するには、[ファイル分析レポートの詳細の要件 \(95 ページ\)](#) を参照してください。

圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析 (File Analysis)] レポートに含まれます。

[高度なマルウェア防御 (Advanced Malware Protection)] レポートページの [ファイル分析 (File Analysis)] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル分析サービスによってファイル分析のためにアップロードされた受信ファイルおよび送信ファイルの数。
- ファイル分析要求が完了している受信ファイルおよび送信ファイルのリスト。
- ファイル分析要求の処理待ちとなっている受信ファイルおよび送信ファイルのリスト。

## [高度なマルウェア防御 (Advanced Malware Protection)]-[ファイル レトロスペクション (File Retrospection)]

[高度なマルウェア防御 (Advanced Malware Protection)] の [ファイル レトロスペクション (File Retrospection)] ページには、このアプライアンスで処理され、メッセージ受信後に判定が変

わったファイルが表示されます。このシナリオの詳細については、お使いの E メールセキュリティ アプライアンスのマニュアルを参照してください。

高度なマルウェア防御は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が明らかになると、脅威の判定が変わる可能性があります。

1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。

1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。

使用可能な最大時間範囲内 (レポートに選択された時間範囲に関係なく) に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページの [ファイルレトロスペクション (File Retrospection) ] ビューを使用できます。

- レトロスペクティブな判定変更がある着信ファイルおよび発信ファイルのリスト。

## [高度なマルウェア防御 (Advanced Malware Protection) ]-[メールボックスの自動修復 (Mailbox Auto Remediation) ]

[高度なマルウェア防御 (Advanced Malware Protection) ]-[メールボックスの自動修復 (Mailbox Auto Remediation) ] レポート ページには、受信ファイルに対するメールボックス修復の結果の詳細が表示されます。

[高度なマルウェア防御 (Advanced Malware Protection) ]-[メールボックスの自動修復 (Mailbox Auto Remediation) ] ページを使用すると、次などのレトロスペクティブセキュリティ情報を表示することができます。

- SHA-256 ハッシュに関連付けられているファイル名。
- メッセージに対して行われた修復処理。
- メールボックス修復が成功または失敗した受信者の一覧。

[修復が失敗した受信者 (Recipients for whom remediation was unsuccessful) ] フィールドは、次のシナリオで更新されます。

- アプライアンスが設定済みの修復のアクションを実行しようとしたときにアプライアンスと Office 365 サービス間の接続に問題があった。

メッセージ トラッキングに関連メッセージを表示するには、SHA-256 ハッシュをクリックします。

## ファイル分析レポートの詳細の要件

- (クラウドファイル分析) 管理アプライアンスがファイル分析サーバに到達できることを確認する (95 ページ)

- (クラウドファイル分析) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する (95 ページ)
- (オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する (96 ページ)
- 追加の要件 (97 ページ)

#### (クラウドファイル分析) 管理アプライアンスがファイル分析サーバに到達できることを確認する

ファイル分析レポートの詳細を取得するには、アプライアンスがポート 443 経由でファイル分析サーバに接続できる必要があります。詳細については、[ファイアウォール情報 \(643 ページ\)](#) を参照してください。

#### (クラウドファイル分析) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する

組織のすべてのコンテンツセキュリティアプライアンスで、組織内の Cisco E メールセキュリティアプライアンスまたは Cisco Web セキュリティアプライアンスから分析用に送信されるファイルに関するクラウド内の詳細な結果が表示されるようにするには、すべてのアプライアンスを同じアプライアンスグループに結合する必要があります。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] を選択します。
- ステップ 3** [ファイル分析 (File Analysis) ] セクションにスクロールします。
- ステップ 4** 管理対象アプライアンスが別のファイル分析クラウドサーバを指している場合は、結果の詳細の表示元となるサーバを選択します。
- 結果の詳細は、その他のクラウドサーバによって処理されたファイルでは使用できません。
- ステップ 5** 分析グループ ID を入力します。
- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
  - この変更はすぐに反映されます。コミットする必要はありません。
  - この値に CCOID を使用することを推奨します。
  - この値は大文字と小文字が区別されます。
  - この値は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。
  - アプライアンスは 1 つのグループだけに属することができます。
  - いつでもグループにマシンを追加できますが、追加できるのは一度のみです。
- ステップ 6** [今すぐグループ化 (Group Now) ] をクリックします。

**ステップ 7** このアプライアンスとデータを共有する各 Eメールセキュリティアプライアンスで、同じグループを設定します。

---

### 次のタスク

#### 関連項目

[クラウドで詳細なファイル分析結果が表示されるファイル](#) (101 ページ)

### (オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する

オンプレミス (プライベートクラウド) の Cisco AMP Threat Grid Appliance を導入した場合、Threat Grid Appliance で使用可能なレポート詳細を表示するために、Cisco コンテンツセキュリティ管理アプライアンスのファイル分析アカウントをアクティブ化する必要があります。通常、これは 1 回のみ必要です。

#### 始める前に

重大レベルでシステム アラートを受信していることを確認します。

---

**ステップ 1** Threat Grid Appliance からファイル分析レポート詳細に最初にアクセスしようとするときに、数分待ってから、リンクを含むアラートを受信します。

このアラートを受信しなかった場合は、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アラート (Alerts)] に移動し、[上位アラートを表示 (View Top Alerts)] をクリックします。

**ステップ 2** アラートメッセージ内のリンクをクリックします。

**ステップ 3** 管理アプライアンスのアカウントをアクティブ化します。

---

#### 追加の要件

追加の要件については、お使いのセキュリティ管理アプライアンス リリースのリリース ノート (次の場所で入手可能) を参照してください <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

## SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム (SHA-256) を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイル进行处理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイル进行处理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルがその SHA-256 値 (短縮形式) 別に表示されます。



## その他のレポートでのファイルレピュテーションフィルタデータの表示

該当する場合は、ファイルレピュテーションおよびファイル分析のデータを他のレポートでも使用できます。レポートによっては、[高度なマルウェア防御で検出 (Detected by Advanced Malware Protection)] 列がデフォルトで非表示になっている場合があります。追加列を表示するには、テーブル下部の [列 (Columns)] リンクをクリックします。

## クラウドで詳細なファイル分析結果が表示されるファイル

パブリッククラウドのファイル分析を導入した場合は、ファイル分析のためにアプライアンスグループに追加された、任意の管理対象アプライアンスからアップロードされたすべてのファイルの詳細な結果を表示できます。

グループに管理アプライアンスを追加した場合は、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] ページにあるボタンをクリックして、グループの管理対象アプライアンスのリストを表示できます。

分析グループのアプライアンスはファイル分析クライアント ID で識別されます。特定のアプライアンスのこの ID を判別するには、次の場所を参照してください。

アプライアンス	ファイル分析クライアント ID の場所
Eメールセキュリティアプライアンス	[セキュリティサービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション
Webセキュリティアプライアンス	[セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション
Cisco コンテンツセキュリティ管理アプライアンス	[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] ページの下部

### 関連項目

- (クラウドファイル分析) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する (95 ページ)

## [ウイルスフィルタリング (Virus Filtering)] ページ

[ウイルスフィルタリング (Virus Filtering)] レポート ページでは、ネットワークで送受信されたウイルスの概要が示されます。[ウイルスタイプ (Virus Types)] ページには、Eメールセキュリティアプライアンスで動作するウイルススキャンエンジンによって検出され、セキュリティ管理アプライアンスに表示されるウイルスが表示されます。このレポートを使用して、

特定のウイルスに対して処置を行います。たとえば、PDF ファイルに組み込まれることが判明しているウイルスを大量に受信している場合、PDF が添付されているメッセージを隔離するフィルタアクションを作成することが推奨されます。

セキュリティ管理アプライアンスで[ウイルスフィルタリング (Virus Filtering) ] レポートページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [ウイルスフィルタリング (Virus Filtering) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

複数のウイルス スキャン エンジンを実行している場合、[ウイルスフィルタリング (Virus Filtering) ] レポート ページには、イネーブルになっているすべてのウイルス スキャン エンジンの結果が含まれます。ページに表示されるウイルスの名前は、ウイルス スキャン エンジンによって判定された名前です。複数のスキャンエンジンが1つのウイルスを検出した場合、同じウイルスに対して複数のエントリが存在する可能性があります。

次のリストでは、[ウイルスフィルタリング (Virus Filtering) ] レポート ページのさまざまなセクションについて説明します。

表 27: [ウイルスフィルタリング (Virus Filtering) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data For) ] (ドロップダウン リスト)	データを表示する E メール セキュリティ アプライアンスを選択するか、[全 E メール アプライアンス (All Email Appliances) ] を選択します。  <a href="#">アプライアンスまたはレポート グループのレポート データの表示 (26 ページ)</a> も参照してください。
[検出した受信ウイルス タイプの上位 (Top Incoming Virus Types Detected) ]	このセクションでは、ネットワークに送信されたメッセージ内で検出されたウイルスのチャート ビューが表示されます。
[検出した送信ウイルス タイプの上位 (Top Outgoing Virus Types Detected) ]	このセクションでは、ネットワークから送信されたメッセージ内で検出されたウイルスのチャート ビューが表示されます。
[ウイルス タイプ 詳細 (Virus Types Detail) ]	各ウイルス タイプの詳細が表示されるインタラクティブ テーブル。  詳細については、 <a href="#">[ウイルス タイプ 詳細 (Virus Types Detail) ] テーブル (139 ページ)</a> を参照してください。



(注) ウイルスに感染したメッセージをネットワークに送信したホストを表示するには、[受信メール (Incoming Mail)] ページに移動し、同じ報告期間を指定して、ウイルス陽性メッセージ別にソートします。同様に、ネットワーク内でウイルス陽性の電子メールを送信した IP アドレスを表示するには、[送信メッセージ送信者 (Outgoing Senders)] ページに進み、ウイルス陽性メッセージ別にソートします。

[ウイルスフィルタリング (Virus Filtering)] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

[ウイルスフィルタリング (Virus Filtering)] レポート ページのスケジュール設定されたレポートを生成できます。[メールレポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [ウイルス タイプ詳細 (Virus Types Detail)] テーブル

[ウイルス タイプ詳細 (Virus Types Detail)] テーブルは、ウイルスに感染したメッセージの合計数と、着信および発信メッセージ別の内訳を示すインタラクティブテーブルです。データをソートするには、列見出しをクリックします。

次の表は、[ウイルス タイプ詳細 (Virus Types Detail)] テーブルのテーブル列の説明を示しています。

表 28: [ウイルス タイプ詳細 (Virus Types Detail)] テーブルのテーブル列の説明

列名	説明
ウイルス タイプ	ウイルス タイプの名前。
着信メッセージ (Incoming Messages)	ウイルスとして検出された着信メッセージの数。
発信メッセージ (Outgoing Messages)	ウイルスとして検出された送信メッセージの数。
感染したメッセージの合計数	感染したメッセージ (受信および送信) の合計数。

## [マクロ検出 (Macro Detection)] ページ

[マクロ検出 (Macro Detection)] レポート ページを使用して、次の項目を表示できます。

- ファイルタイプ別のマクロが有効になった受信添付ファイル数の上位 (グラフ形式および表形式)。
- マクロが有効な受信添付ファイルの総数 (ファイルタイプ別、表形式)。

- ファイルタイプ別のマクロが有効になった送信添付ファイル数の上位（グラフ形式および表形式）。
- マクロが有効な送信添付ファイルの総数（ファイルタイプ別、表形式）。

セキュリティ管理アプリケーションで[マクロ検出 (Macro Detection)] レポートページを表示するには、[製品 (Product)] ドロップダウンから[電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)] > [マクロ検出 (Macro Detection)]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[マクロ検出 (Macro Detection)] レポート ページから、raw データを CSV ファイルにエクスポートすることができます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

マクロが有効になった添付ファイルの数をクリックすると、[メッセージトラッキング (Message Tracking)] に関連メッセージを表示できます。



(注) レポート生成中に次の処理が発生します。

- アーカイブ ファイル内に 1 つ以上のマクロが検出されると、アーカイブ ファイル タイプが 1 増えます。アーカイブ ファイル内のマクロが有効になった添付ファイルの数はカウントされません。
- 埋め込みファイル内に 1 つ以上のマクロが検出されると、親ファイル タイプが 1 増えます。埋め込みファイル内のマクロが有効になった添付ファイルの数はカウントされません。

## [DMARC検証 (DMARC Verification)] ページ

[DMARC 検証 (DMARC Verification)] レポートページには、Domain-based Message Authentication, Reporting and Conformance (DMARC) 検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。このレポートを使用して DMARC 設定を最適化し、次のような情報を取得できます。

- DMARC 検証に失敗したメッセージを最も多く送信したドメイン
- 各ドメインで、DMARC 検証に失敗したメッセージに対して実行されたアクション

[DMARC検証 (DMARC Verification)] レポート ページを使用すると、次の情報を表示できます。

- 上位ドメイン (DMARC 検証の失敗別、グラフ形式)。

- ドメインの合計 (DMARC 検証の詳細別、表形式)。詳細については、[\[DMARC検証の詳細別のドメイン \(Domains by DMARC Verification Details\) \]テーブル \(141 ページ\)](#) を参照してください。

セキュリティ管理アプライアンスで [DMARC検証 (DMARC Verification) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [DMARC検証 (DMARC Verification) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の青い番号のリンクをクリックします。

[DMARC 検証 (DMARC Verification) ] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

DMARC 検証の詳細については、お使いの E メールセキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドで「Email Authentication」の章を参照してください。

## [DMARC検証の詳細別のドメイン (Domains by DMARC Verification Details) ] テーブル

[DMARC検証の詳細別のドメイン (Domains by DMARC Verification Details) ] テーブルは、Domain-based Message Authentication, Reporting and Conformance (DMARC) の失敗 (拒否、隔離、またはアクションなし)、試行、および成功があった送信者ドメインの詳細を表示するインタラクティブ テーブルです。

テーブルの情報をカスタマイズしてソートするには、[レポート ページのテーブルのカスタマイズ \(45 ページ\)](#) を参照してください。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## [アウトブレイク フィルタリング (Outbreak Filtering) ] ページ

[アウトブレイクフィルタ (Outbreak Filters) ] ページには、最近のアウトブレイクやアウトブレイクフィルタによって隔離されたメッセージに関する情報が表示されます。このページを使用して、対象を絞ったウイルス、詐欺、およびフィッシング攻撃に対する防御をモニタできません。

[アウトブレイクフィルタリング (Outbreak Filtering) ] レポート ページを使用して、次の情報を入手できます。

- ウイルス感染フィルタ ルールによって隔離されたメッセージの数と使用されたルール。
- メッセージがアウトブレイク隔離にとどまる期間
- 最も頻繁に表示される悪意のある可能性がある URL

セキュリティ管理アプライアンスで [アウトブレイクフィルタリング (Outbreak Filtering) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [アウトブレイクフィルタリング (Outbreak Filtering) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

次の表では、[アウトブレイクフィルタリング (Outbreak Filtering) ] レポート ページのさまざまなセクションについて説明します。

表 29: [アウトブレイクフィルタリング (Outbreak Filtering) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data For) ] (ドロップダウン リスト)	データを表示する E メールセキュリティ アプライアンスを選択するか、[全 E メールアプライアンス (All Email Appliances) ] を選択します。  <a href="#">アプライアンスまたはレポーティング グループのレポートデータの表示 (26 ページ)</a> も参照してください。
タイプ別脅威	[タイプ別脅威 (Threats By Type) ] セクションには、アプライアンスによって受信された脅威メッセージのさまざまなタイプが示されます。
脅威サマリー	[脅威サマリー (Threat Summary) ] セクションには、[マルウェア (Malware) ]、[フィッシング (Phish) ]、[詐欺 (Scam) ]、および [ウイルス (Virus) ] によるメッセージの内訳が示されます。  このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
脅威の詳細	[脅威の詳細 (Threat Details) ] インタラクティブ テーブルには、脅威のカテゴリ (ウイルス、詐欺、またはフィッシング)、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する詳細が表示されます。  このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

セクション	説明
着信メッセージからのヒットメッセージ	<p>[着信メッセージからのヒットメッセージ (Hit Messages from Incoming Messages) ]セクションは、選択した時間帯にアウトブレイク フィルタによって処理された受信メッセージの数のグラフと概要を示しています。</p> <p>ウイルス以外の脅威には、外部 Web サイトへのリンクを使用したフィッシング電子メール、詐欺、およびマルウェア配布が含まれます。</p>
脅威レベル別のヒットメッセージ	<p>[脅威レベル別のヒットメッセージ (Hit Messages by Threat Level) ]セクションは、アウトブレイク フィルタによって検出された脅威の重大度の概要を示しています。</p> <p>レベル 5 の脅威が範囲または影響において重大であるのに対し、レベル 1 は脅威のリスクが低いことを示します。脅威レベルの説明については、お使いの E メールセキュリティアプライアンスのオンラインヘルプまたはユーザガイドを参照してください。</p>
アウトブレイク 検疫内のメッセージ	<p>[アウトブレイク 隔離内のメッセージ (Messages resided in Outbreak Quarantine) ]は、メッセージがアウトブレイク 隔離にとどまっていた時間の長さを示します。</p> <p>この期間は、潜在的な脅威の安全性の判定に必要なデータを収集するためにかかる時間によって決まります。通常、ウイルス脅威を含むメッセージはアンチウイルス プログラムの更新を待機する必要があるため、ウイルス以外の脅威を含む場合よりも隔離に長くとどまります。各メール ポリシーで指定した最大保持期間も反映されます。</p>
書き換えられた上位 URL	<p>[書き換えられた上位 URL (Top URL's Rewritten) ]セクションは、サイトのクリック時評価 (受信者がメッセージ内の悪意のある可能性があるリンクをクリックした場合) 用に、メッセージ受信者を Cisco Web セキュリティ プロキシにリダイレクトするために最も頻繁に書き換えられた URL を示します。</p> <p>いずれかの URL が悪意のある URL と見なされると、そのメッセージ内のすべての URL が書き換えられるため、このリストには悪質でない URL が含まれる場合があります。</p> <p>このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。</p>



- (注) [アウトブレイクフィルタリング (Outbreak Filtering) ] レポート ページにテーブルが正しく表示されるためには、アプライアンスが、Cisco アップデート サーバと通信できる必要があります。

詳細については、お使いの E メールセキュリティ アプライアンスのオンラインヘルプまたは ユーザ ガイドの「Outbreak Filters」の章を参照してください。

## [URL フィルタリング (URL Filtering) ] ページ

URL フィルタリング レポートは、送受信メッセージに対して使用できます。

URL フィルタリング エンジンによって (アンチスパム/アウトブレイク フィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して) スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではありません。



- (注) URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。

[URL フィルタリング (URL Filtering) ] レポート ページでは、次の情報を表示できます。

- [上位URLカテゴリ (Top URL Categories) ] モジュールには、コンテンツ フィルタまたはメッセージフィルタに一致するかどうかにかかわらず、スキャンされたメッセージで検出されたすべてのカテゴリが含まれます。

各メッセージを関連付けることができるレピュテーション レベルは1つのみです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。

- 上位URLスパムメッセージ (Top URL Spam Messages)

E メールセキュリティ アプライアンスの [セキュリティサービス (Security Services) ] > [URL フィルタリング (URL Filtering) ] ページで設定したグローバル ホワイトリストの URL は、レポートに含まれません。

個別のフィルタで使用されるホワイトリストの URL はレポートに含まれます。

- 悪意のある URL とは、アウトブレイク フィルタによってレピュテーションが低いと判定された URL です。ニュートラルURL とは、アウトブレイク フィルタによってクリック時の保護が必要と判定された URL です。このため、ニュートラルURL は、Cisco Web セキュリティ プロキシにリダイレクトするために書き換えられます。

URL カテゴリ ベースのフィルタの結果はコンテンツおよびメッセージ フィルタ レポートに反映されます。



Cisco Web セキュリティ プロキシによるクリック時の URL 評価の結果は、レポートに反映されません。

セキュリティ管理アプライアンスで [URLフィルタリング (URL Filtering)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [URLフィルタリング (URL Filtering)] を選択します。詳細については、[インタラクティブレポート ページの使用 \(41 ページ\)](#) を参照してください。

次の表では、[URLフィルタリング (URL Filtering)] レポート ページのさまざまなセクションについて説明します。

表 30: [URLフィルタリング (URL Filtering)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data For)] (ドロップダウン リスト)	データを表示する E メールセキュリティ アプライアンスを選択するか、[全 E メール アプライアンス (All Email Appliances)] を選択します。 <a href="#">アプライアンスまたはレポートグループのレポートデータの表示 (26 ページ)</a> も参照してください。
上位 URL カテゴリ (Top URL Categories)	このセクションには、着信および発信メッセージの上位 URL カテゴリの概要とグラフィカル ビューが表示されます。  このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
上位 URL スпамメッセージ (Top URL Spam Messages)	このセクションには、着信および発信の上位 URL スпамメッセージの概要とグラフィカル ビューが表示されます。
悪意のある URL およびニュートラルな URL (Malicious and Neutral URLs)	このセクションには、着信および発信メッセージの悪意のある URL とニュートラル URL のチャートビューおよび概要が表示されます。  このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[URLフィルタリング (URL Filtering)] レポート ページから raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポートデータおよびトラッキングデータのエクスポート \(33 ページ\)](#) を参照してください。

## [偽装メールの検出 (Forged Email Detection)] ページ

[偽装メールの検出 (Forged Email Detection)] ページには、次のレポートが含まれています。

- **偽装メールの検出数の上位。**受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。
- **偽装メールの検出：詳細。**受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。

セキュリティ管理アプライアンスで [偽装メールの検出 (Forged Email Detection)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)] > [偽装メールの検出 (Forged Email Detection)]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[偽装メールの検出 (Forged Email Detection)] レポートは、[偽装メールの検出 (Forged Email Detection)] コンテンツ フィルタまたは forged-email-detection メッセージ フィルタを使用している場合にのみ自動入力されます。

[偽装メールの検出 (Forged Email Detection)] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポーティング データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

## [外部脅威フィード (External Threat Feeds)] ページ

[外部脅威フィード (External Threat Feeds)] レポート ページでは、以下を表示できます。

- メッセージで脅威を検出するために使用される上位 ETF ソース (グラフ形式)。
- メッセージで脅威を検出するために使用される ETF ソースの概要 (表形式)。
- メッセージで検出された脅威に一致する上位 IOC (グラフ形式)。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソース (グラフ形式)。
- 悪意のある着信メール接続をフィルタするために使用される上位 ETF ソースの概要 (表形式)。

[外部脅威フィードソースの概要 (Summary of External Threat Feed Sources)] セクションでは、以下を実行できます。

- 特定の ETF ソースでメッセージ数をクリックすると、[メッセージトラッキング (Message Tracking)] に関連メッセージを表示できます。
- 特定の脅威フィード ソースをクリックすると、IOC に基づいた ETF ソースの分布を表示できます。

[侵害の兆候 (IOC) の一致の概要 (Summary of Indicator of Compromise (IOC) Matches)] セクションでは、以下を実行できます。

- 特定の ETF ソースで IOC の数をクリックすると、[メッセージトラッキング (Message Tracking)] に関連メッセージを表示できます。
- 特定の IOC をクリックすると、ETF ソースに基づいた IOC の分布を表示できます。

セキュリティ管理アプライアンスで [外部脅威フィード (External Threat Feeds)] レポートページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [外部脅威フィード (External Threat Feeds)] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

## [送信者ドメインのレピュテーション (Sender Domain Reputation)] ページ

[送信者ドメインのレピュテーション (Sender Domain Reputation)] レポートページでは、次を表示できます。

- SDR サービスで受信した判定に基づく着信メッセージ (グラフ形式)。
- SDR サービスで受信した脅威カテゴリおよび判定に基づく着信メッセージの概要 (表形式)。
- SDR サービスで受信した脅威カテゴリに基づく着信メッセージ (グラフ形式)。



(注) SDR 判定が「非常に問題がある」または「悪い」メッセージのみが、「スパム」や「悪意あり」などの SDR 脅威カテゴリに分類されます。

- SDR サービスで受信した脅威カテゴリに基づく着信メッセージの概要 (表形式)。

セキュリティ管理アプライアンスで [送信者ドメインのレピュテーション (Sender Domain Reputation)] レポートページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [送信者ドメインのレピュテーション (Sender Domain Reputation)] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

## [メール フローの詳細 (Mail Flow Details)] ページ

セキュリティ管理アプライアンスの [メールフローの詳細 (Mail Flow Details)] レポートページでは、お使いの管理対象のセキュリティ管理アプライアンスに接続するすべてのリモートホストのリアルタイム情報がインタラクティブに報告されます。システムに電子メールを送信し

ている IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。送信メッセージ送信者の IP アドレスおよびドメインに関する情報も収集できます。

セキュリティ管理アプライアンスで [メールフローの詳細 (Mail Flow Details)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [メールフローの詳細 (Mail Flow Details)] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[メールフローの詳細 (Mail Flow Details)] レポート ページには、次のタブがあります。

- 受信メール (Incoming Mails)
- 送信者

データ内の特定の情報を検索するには、[検索およびインタラクティブ電子メールレポート ページ \(61 ページ\)](#) を参照してください。

[受信メール (Incoming Mails)] タブでは、次の操作を実行できます。

- グラフ形式で、合計脅威メッセージ数での上位送信者を表示します。
- グラフ形式で、クリーンメッセージ数での上位送信者を表示します。
- グレイメールメッセージの上位の送信者をグラフ形式で表示する。
- セキュリティ管理アプライアンスにメールを送信した送信者の IP アドレス、ドメイン、またはネットワーク オーナー（組織）を表示する。
- 電子メールをアプライアンスに送信した送信者の詳細な統計情報を表示する。統計情報には、接続（承認または拒否）の数、試行されたもののセキュリティ サービス（送信者レピュテーションフィルタリング、アンチスパム、アンチウイルスなど）によってブロックされたメッセージの数、脅威メッセージの総数、グレイメールメッセージおよび正常なメッセージの総数が含まれます。
- [受信メール (Incoming Mails)] インタラクティブテーブルで、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）についての詳細情報を表示する。詳細については、[\[受信メール \(Incoming Mails\)\] テーブル \(150 ページ\)](#) を参照してください。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の番号付きハイパーリンクをクリックします。

[送信メッセージ送信者 (Outgoing Senders)] タブでは、次の操作を実行できます。

- グラフ形式で、合計脅威メッセージ数での上位送信者を表示します。
- グラフ形式で、クリーンメッセージ数での上位送信者を表示します。
- 組織内で送信された脅威メッセージ（スパム、アンチウイルスなど）の上位送信者（IP アドレス別またはドメイン別）を表示する。
- 電子メールをアプライアンスから送信した送信者の詳細な統計情報を表示する。統計情報には、セキュリティ サービス（送信者レピュテーションフィルタリング、アンチスパム、

アンチウイルスなど) によってブロックされた脅威メッセージおよび正常なメッセージの総数が含まれます。

- [送信者の詳細 (Sender Details)] インタラクティブ テーブルで、特定の IP アドレスまたはドメインの詳細情報を表示する。詳細については、[送信者の詳細 (Sender Details)] テーブル (156 ページ) を参照してください。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の番号付きハイパーリンクをクリックします。

#### 関連項目

- [ドメイン情報がありません (No Domain Information)] リンク (78 ページ)
- メールトレンド グラフにおける時間範囲 (78 ページ)
- メールフローの詳細ページ内のビュー (149 ページ)
- [受信メール (Incoming Mails)] テーブル (150 ページ)
- [送信者の詳細 (Sender Details)] テーブル (156 ページ)

## メール フローの詳細ページ内のビュー

[メールフローの詳細 (Mail Flow Details)] : [受信 (Incoming)] レポート ページには次の 3 種類のビューがあります。

- IP アドレス
- ドメイン (Domains)
- ネットワーク オーナー

これらのビューでは、システムに接続されたリモートホストのスナップショットが、選択したビューのコンテキストで提供されます。

さらに、[メールフローの詳細 (Mail Flow Details)] ページの [受信メール (Incoming Mail)] テーブルでは、送信者の IP アドレス、ドメイン名、またはネットワーク オーナー情報をクリックすると、特定の送信者プロファイル情報を取得できます。[送信者プロファイル (Sender Profile)] の情報の詳細については、[送信者プロファイル (Sender Profile)] ページ (79 ページ) を参照してください。



- (注) ネットワーク オーナーは、ドメインを含むエンティティです。ドメインは、IP アドレスを含むエンティティです。

選択したビューに応じて、[受信メールの詳細 (Incoming Mail Details)] インタラクティブ テーブルに、E メールセキュリティ アプライアンスで設定されたすべてのパブリック リスナーに電子メールを送信した上位 IP アドレス、ドメイン、またはネットワーク オーナーが表示されます。アプライアンスに入ったすべてのメールのフローをモニタできます。

## [ドメイン情報がありません (No Domain Information)] リンク

IP アドレス、ドメイン、またはネットワーク オーナーをクリックすると、[送信者プロファイル (Sender Profile)] ページの送信者の詳細にアクセスできます。[送信者プロファイル (Sender Profile)] ページは、特定の IP アドレス、ドメインまたはネットワーク オーナーに固有の [メールフローの詳細 (Mail Flow Details)] ページです。

[受信メール (Incoming Mails)] インタラクティブ テーブルに含まれるデータの説明については、[受信メール (Incoming Mails)] テーブル (150 ページ) を参照してください。

[メールフローの詳細 (Mail Flow Details)] ページから、raw データを CSV ファイルにエクスポートできます。

[メールフローの詳細 (Mail Flow Details)] : [送信 (Outgoing)] レポート ページには次の 2 種類のビューがあります。

- IP アドレス
- ドメイン (Domains)

これらのビューでは、システムに接続されたリモートホストのスナップショットが、選択したビューのコンテキストで提供されます。

選択したビューに応じて、[送信者の詳細 (Sender Details)] インタラクティブ テーブルに、E メールセキュリティ アプライアンスで設定されたパブリック リスナーから電子メールを送信した上位 IP アドレス、ドメイン、または送信者が表示されます。アプライアンスから出たすべてのメールのフローをモニタできます。

[送信者の詳細 (Sender Details)] インタラクティブ テーブルに含まれるデータの説明については、[送信者の詳細 (Sender Details)] テーブル (156 ページ) を参照してください。

## [ドメイン情報がありません (No Domain Information)] リンク

セキュリティ管理アプライアンスに接続したものの、ダブル DNS ルックアップで検証できなかったドメインは、専用ドメイン [ドメイン情報がありません (No Domain Information)] に自動的に分類されます。これらの種類の検証外ホストを管理する方法は、送信者の検証によって制御できます。送信者の検証の詳細については、ご使用の E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

[表示された項目 (Items Displayed)] メニューを使用して、リストに表示する送信者の数を選択できます。

## メールトレンドグラフにおける時間範囲

メールのグラフは、さまざまなきめ細かさを選択して表示できます。同じデータの日、週、月、および年のビューを選択できます。データはリアルタイムでモニタリングされているので、情報は定期的に更新され、データベースで集計されます。

時間範囲の詳細については、[レポートの時間範囲の選択 \(27 ページ\)](#) を参照してください。

## [受信メール (Incoming Mails)] テーブル

[メールフローの詳細 : 受信メール (Mail Flow Details: Incoming Mails)] ページの下部にあるインタラクティブな [受信メール (Incoming Mails)] テーブルには、E メールセキュリティ ア

ライセンス上のパブリックリスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメイン、IP アドレス、またはネットワーク オーナーが表示されます。

ダブル DNS ルックアップを実行することで、システムはリモートホストの IP アドレスを取得してその有効性を検証します。ダブル DNS ルックアップおよび送信者検証の詳細については、AsyncOS E メールセキュリティ アプライアンスのユーザガイドまたはオンラインヘルプを参照してください。

【受信メール (Incoming Mails)】テーブルの最初の列、または【脅威メッセージの送信者上位 (Top Senders by Total Threat Messages)】に表示される送信者、つまりネットワーク オーナー、IP アドレスまたはドメインについては、【送信者 (Sender)】または【ドメイン情報がありません (No Domain Information)】リンクをクリックすると、送信者の詳細情報が表示されます。結果は、【送信者プロファイル (Sender Profile)】ページに表示され、SenderBase レピュテーション サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、[【送信者プロファイル \(Sender Profile\)】ページ \(79 ページ\)](#) を参照してください。

【メールフローの詳細 (MailFlowDetails)】ページの下部にある【送信者グループレポート (Sender Groups Report)】をクリックして、【送信者グループ (Sender Groups)】レポートを表示することもできます。【送信者グループ (Sender Groups)】レポートページの詳細については、[#unique\\_197](#)を参照してください。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表に、【受信メール (Incoming Mails)】テーブル内の列の詳細を示します。

表 31:【受信メール (Incoming Mail)】テーブル内の列の詳細

列名	説明
送信者ドメイン (ドメイン) (Sender Domain (Domains))	送信者のドメイン名。
送信者 IP アドレス (IP アドレス) (Sender IP Address (IP Addresses))	送信者の IP アドレス。
ホスト名 (IP アドレス) (Hostname (IP Addresses))	送信者のホスト名。
DNS 検証 (IP アドレス) (DNS Verified (IP Addresses))	DNS によって検証された IP アドレス。
SBRS (IP アドレス) (SBRS (IP Addresses))	送信者の SenderBase レピュテーション スコア。

## [受信メール (Incoming Mails)] テーブル

列名	説明
最後の送信者グループ (IP アドレス) (Last Sender Group (IP Addresses))	最後の送信者グループの詳細。
最後の送信者グループ (IP アドレス) (Last Sender Group (IP Addresses))	最後の送信者グループの詳細。
ネットワークオーナー (Network Owner (Network Owners))	送信者のネットワーク オーナー。
接続拒否 (ドメインおよびネットワークオーナー) (Connections Rejected (Domains and Network Owners))	HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。
接続承認 (ドメインおよびネットワークオーナー) (Connections Accepted (Domains and Network Owners))	受け入れられたすべての接続。
[試行回数の合計 (Total Attempted) ]	すべての受け入れられた接続試行と、拒否された接続試行。
受信者スロットルによる停止 (ドメインおよびネットワークオーナー) (Stopped by Recipient Throttling (Domains and Network Owners))	これは、レピュテーションフィルタリングによる阻止の 1 要素です。HAT 上限値 (1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数) のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ] が算出されます。



列名	説明
[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ]	<p>[レピュテーションフィルタによる停止 (Stopped by Reputation Filtering) ] の値は、次の複数の要素に基づいて算出されます。</p> <ul style="list-style-type: none"> <li>• この送信者からの「数が絞り込まれた」メッセージの数</li> <li>• 拒否された、または TCP 拒否の接続数 (部分的に集計されず)</li> <li>• 接続ごとのメッセージ数に対する控えめな乗数。</li> </ul> <p>アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。その代わりに、拒否された接続の数は、各時間間隔で最も顕著だった送信者についてのみ維持されます。この場合、表示される値は「下限」、つまり少なくともこの数のメッセージが阻止されたと解釈できます。</p> <p>(注) [メールフロー概要 (Mail Flow Summary) ] ページの [レピュテーションフィルタリング (Reputation Filtering) ] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。</p>
[無効な受信者の場合に停止 (Stopped as Invalid Recipients) ]	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
[スパム検出 (Spam Detected) ]	検出されたすべてのスパム。
[ウイルス検出 (Virus Detected) ]	検出されたすべてのウイルス。
高度なマルウェア防御で検出 (Detected by Advanced Malware Protection)	高度なマルウェア防御エンジンによって検出されたメッセージの総数。
コンテンツフィルタによる阻止 (Stopped by Content Filter)	コンテンツ フィルタによって阻止されたメッセージの総数。
DMARCによる停止 (Stopped by DMARC)	Domain-based Message Authentication, Reporting and Conformance (DMARC) に失敗したメッセージの総数。
合計脅威件数 (Total Threat)	脅威メッセージ (評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの) の総数

列名	説明
Marketing	不要なマーケティング メッセージとして検出されたメッセージの数。
ソーシャル (Social)	ソーシャル メッセージとして検出されたメッセージの数。
バルク (Bulk)	バルクとして検出されたメッセージの数。
合計グレイメール数 (Total Graymails)	グレイメールとして検出されたメッセージの数。
クリーン (Clean)	すべてのクリーン メッセージ。  グレイメール機能が有効になっていないアプライアンスで処理されるメッセージは、クリーンとして集計されます。

## [送信者プロフィール (Sender Profile) ] ページ

[受信メール (Incoming Mail) ] インタラクティブ テーブル ([メールフローの詳細 (Mail Flow Details) ] (新しい Web インターフェイス) または [受信メール (Incoming Mail) ] ページ) の送信者をクリックすると、[送信者プロフィール (Sender Profile) ] ページが表示されます。ここでは、特定の IP アドレス、ドメイン、またはネットワーク オーナー (組織) の詳細情報が表示されます。[メールフローの詳細 (Mail Flow Details) ] ページまたは他の [送信者プロフィール (Sender Profile) ] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロフィール (Sender Profile) ] ページにアクセスできます。

ネットワーク オーナーは、ドメインを含むエンティティです。ドメインは、IP アドレスを含むエンティティです。

IP アドレス、ドメインおよびネットワーク オーナーに関して表示される送信者プロフィール ページは、多少異なります。それぞれのページには、特定の送信者からの着信メールに関するグラフおよびサマリーテーブルが含まれます。グラフの下の表に、送信者に関連付けられたドメインまたは IP アドレスが表示されます。(個々の IP アドレスの [送信者プロフィール (Sender Profile) ] ページには、詳細なリストが含まれません)。[送信者プロフィール (Sender Profile) ] ページには、送信者の現在の SenderBase、送信者グループ、およびネットワーク 情報を含む情報セクションも表示されます。

- ネットワーク オーナー プロファイル ページには、ネットワーク オーナー、およびこのネットワーク オーナーに関連するドメインや IP アドレスに関する情報が含まれます。
- ドメイン プロファイル ページには、このドメインおよびこのドメインに関連する IP アドレスに関する情報が含まれます。
- IP アドレス プロファイル ページには、IP アドレスのみにに関する情報が含まれます。

各 [送信者プロフィール (Sender Profile) ] ページには、ページの下部の現在の情報テーブルに次のデータが含まれます。

- SenderBase レピュテーションサービスからのグローバル情報。たとえば、次の情報です。
  - IP アドレス、ドメイン名、またはネットワーク オーナー
  - ネットワーク オーナーのカテゴリ (ネットワーク オーナーのみ)
  - CIDR 範囲 (IP アドレスのみ)
  - IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
  - この送信者から最初のメッセージを受信してからの日数
  - 最後の送信者グループと DNS が検証されたかどうか (IP アドレス送信者プロフィール ページのみ)

日単位マグニチュードは、直近24時間にドメインが送信したメッセージの数の基準です。地震の測定に使用されるリヒター スケールと同様に、SenderBase マグニチュードは、10を基数とする対数目盛を使用して算出されるメッセージの量の基準です。目盛の最大理論値は10に設定されます。これは、世界の電子メールメッセージの量に相当します。対数目盛を使用した場合、1ポイントのマグニチュードの増加は、実際の量の10倍の増加に相当します。

月単位マグニチュードは、直近30日間に送信された電子メールの量に基づいて割合が算出される点を除いて、日単位マグニチュードと同じ方法を使用して算出されます。

- 平均マグニチュード (IP アドレスのみ)
- 総累積量/30日の量 (IP アドレス プロファイル ページのみ)
- Bonded Sender ステータス (IP アドレス プロファイル ページのみ)
- SenderBase 評価スコア (IP アドレス プロファイル ページのみ)
- 最初のメッセージからの日数 (ネットワーク オーナーとドメイン プロファイル ページのみ)
- このネットワーク オーナーに関連するドメインの数 (ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ)
- このネットワーク オーナーの IP アドレスの数 (ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ)
- 電子メールの送信に使用された IP アドレスの数 (ネットワーク オーナー ページのみ)

SenderBase 評価サービスによって提供されるすべての情報を示すページを表示するには、[SenderBaseからの詳細情報 (More from SenderBase)] をクリックします。

- このネットワーク オーナーによって管理されるドメインおよび IP アドレスに関する詳細は、ネットワーク オーナー プロファイル ページに表示されます。ドメイン内の IP アドレスに関する詳細は、ドメイン ページに表示されます。

## [送信者の詳細 (Sender Details) ]テーブル

ドメイン プロファイルのページから、特定の IP アドレスをクリックして特定の情報を表示することも、組織プロフィールのページを表示することもできます。

## [送信者の詳細 (Sender Details) ]テーブル

[メールフローの詳細 (Mail Flow Details) ] : [送信 (Outgoing) ] ページの下部にあるインタラクティブな [送信者の詳細 (Sender Details) ] テーブルには、E メールセキュリティ アプライアンス上のパブリックリスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメインまたは IP アドレスが表示されます。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表に、[送信者の詳細 (Sender Details) ] テーブル内の列の詳細を示します。

表 32: [送信者の詳細 (Sender Details) ] テーブル内の列の詳細

列名	説明
送信者ドメイン (ドメイン) (Sender Domain (Domains))	送信者のドメイン名。
送信者 IP アドレス (IP アドレス) (Sender IP Address (IP Addresses))	送信者の IP アドレス。
ホスト名 (IP アドレス) (Hostname (IP Addresses))	送信者のホスト名。
[スパム検出 (Spam Detected) ]	検出されたすべてのスパム。
[ウイルス検出 (Virus Detected) ]	検出されたすべてのウイルス。
高度なマルウェア防御で検出 (Detected by Advanced Malware Protection)	高度なマルウェア防御エンジンによって検出されたメッセージの総数。
コンテンツフィルタによる阻止 (Stopped by Content Filter)	コンテンツ フィルタによって阻止されたメッセージの総数。
DLP による停止 (Stopped by DLP)	DLP エンジンによって阻止されたメッセージの総数。
合計脅威件数 (Total Threat)	脅威メッセージ (スパム、ウイルス) の総数
クリーン (Clean)	すべてのクリーン メッセージ。  グレイメール機能が有効になっていないアプライアンスで処理されるメッセージは、クリーンとして集計されます。

列名	説明
合計メッセージ数 (Total Messages)	すべてのメッセージの合計数。

## 送信者グループレポート

送信者グループレポートは、送信者グループ別およびメールフローポリシーアクション別の接続のサマリーを提供し、SMTP 接続およびメールフローポリシーのトレンドを確認できるようにします。[送信者グループによるメールフロー (Mail Flow by Sender Group)] リストには、各送信者グループの割合および接続数が示されます。[メールフローポリシーアクションによる接続 (Connections by Mail Flow Policy Action)] グラフは、各メールフローポリシーアクションの接続の割合を示します。このページには、ホストアクセステーブル (HAT) ポリシーの有効性の概要が示されます。HATの詳細については、[電子メールを受信するためのゲートウェイの設定](#)を参照してください。

## [送信先 (Outgoing Destinations)] ページ

[送信先 (Outgoing Destinations)] レポートページには、組織がメールを送信するドメインについての情報が表示されます。

[送信先 (Outgoing Destinations)] ページを使用すると、次の情報を表示できます。

- Eメールセキュリティアプライアンスが送信するメッセージの宛先のドメイン
- 各ドメインに送信されるメッセージの量
- クリーン、スパム陽性、ウイルス陽性、マルウェア、またはコンテンツフィルタによる阻止のメッセージの割合。
- 配信されたメッセージおよび宛先サーバによってハードバウンズされたメッセージの数。

セキュリティ管理アプライアンスで [送信先 (Outgoing Destinations)] レポートページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [\[モニタリング \(Monitoring\)\] > \[送信先 \(Outgoing Destinations\)\]](#) を選択します。詳細については、[インタラクティブレポートページの使用 \(41 ページ\)](#) を参照してください。

データ内の特定の情報を検索するには、[検索およびインタラクティブ電子メールレポートページ \(61 ページ\)](#) を参照してください。

次のリストでは、[送信先 (Outgoing Destinations)] レポートページのさまざまなセクションについて説明します。

表 33: [送信先 (Outgoing Destinations) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data For) ] (ドロップダウン リスト)	データを表示する E メールセキュリティ アプライアンスを選択するか、[全Eメールアプライアンス (All Email Appliances) ] を選択します。  <a href="#">アプライアンスまたはレポートグループのレポートデータの表示 (26 ページ)</a> も参照してください。
脅威メッセージの配信先上位 (Top Destinations by Total Threat Messages)	組織によって送信された発信脅威メッセージ (スパム、アンチウイルスなど) の上位の宛先ドメイン。合計脅威メッセージには、スパムやウイルス検出、またはコンテンツフィルタによってトリガーされたメッセージが含まれます。
正常なメッセージの配信先上位 (Top Destinations by Clean Messages)	組織によって送信されたクリーンな発信脅威メッセージの上位の宛先ドメイン。
送信先の詳細 (Outgoing Destinations Details)	組織によって送信されたすべての発信メッセージの宛先ドメインに関する、総受信者数別にソートされたすべての詳細情報。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。  詳細については、 <a href="#">送信先の詳細の表 (159 ページ)</a> を参照してください。  このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[送信先 (Outgoing Destinations) ] レポート ページから raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

[送信先 (Outgoing Destinations) ] ページのスケジュール設定されたレポートを生成できます。[メール レポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

#### 関連項目

[送信先の詳細の表 \(159 ページ\)](#)

## 送信先の詳細の表

[送信先の詳細 (Outgoing Destinations Detail)] テーブルは、処理されて配信されたメッセージの合計数、脅威 (スパム、ウイルス等) またはクリーンであるとして処理されたメッセージの内訳、ハードバウンス済みまたは配信済みメッセージを示すインタラクティブテーブルです。データをソートするには、列見出しをクリックします。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

次の表は、[送信先の詳細 (Outgoing Destinations Detail)] テーブルのテーブル列の説明を示しています。

表 34: [送信先の詳細 (Outgoing Destinations Detail)] テーブルのテーブル列の説明

列名	説明
宛先ドメイン	宛先ドメインの名前。
スパム検出 (Spam Detected)	スパムとして検出されたメッセージ数。
ウイルス検出 (Virus Detected)	スパムとして検出されたメッセージ数。
コンテンツフィルタによる阻止 (Stopped by Content Filter)	コンテンツ フィルタによって阻止されたメッセージの数。
合計脅威件数 (Total Threat)	脅威 (スパム、ウイルス等) として検出されたメッセージの合計数。
クリーン (Clean)	クリーンであると検出されたメッセージの数
処理済みメッセージの合計 (Total Proceed)	脅威またはクリーンであるとして処理されたメッセージの合計数。
ハードバウンス (Hard Bounces)	永続的に配信不能としてマークされたメッセージの数。
配信済み (Delivered)	配信されるメッセージの数。
送信済みメッセージの合計 (Total Messages Delivered)	配信されるメッセージの合計数 (ハードバウンスを含む)。

## [TLS暗号化 (TLS Encryption)] ページ

[TLS暗号化 (TLS Encryption)] ページには、メールの送受信に使用される TLS 暗号化の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。

[TLS暗号化 (TLS Encryption)] ページを使用すると、次の情報を確認できます。

- 送受信接続による、全体的な TLS の使用割合
- TLS 接続に成功したパートナー
- TLS 接続に成功しなかったパートナー
- TLS 認証に問題のあるパートナー
- パートナーが TLS を使用したメールの全体的な割合

[TLS暗号化 (TLS Encryption)] ページは、着信接続に関するセクションと、発信接続に関するセクションに分かれています。各セクションには、詳細情報が含まれたグラフ、サマリー、および表が含まれています。

グラフには、指定した時間範囲にわたる、送受信 TLS の暗号化された接続および暗号化されない接続のビューが表示されます。グラフには、メッセージの総量、暗号化された/暗号化されないメッセージの量、成功/失敗した TLS 暗号化メッセージの量、。グラフでは、TLS が必須であった接続と、TLS が単に優先された接続が区別されます。

表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。ドメインごとに、成功/失敗した必須の TLS 接続と優先された TLS 接続の数、試行された TLS 接続の総数（成功したか失敗したかにかかわらず）、また、TLS が試行されたすべての接続の割合、および正常に送信された暗号化メッセージの総数（TLS が優先か必須かにかかわらず）も表示できます。テーブルの右上にある [列をカスタマイズ (Customize Columns)] アイコンを使用して、列を表示または非表示にできます。

### TLS 接続数詳細テーブル

TLS 接続数詳細テーブルは、接続、送信したメッセージ、および成功または失敗した TLS 接続の数の合計数、着信および発信メッセージの最終 TLS ステータスを表示する、対話型のテーブルです。各ドメインについて、成功/失敗した接続の割合を表示することもできます。

次の表は、TLS 接続数詳細テーブルの列の説明を示しています。

表 35: TLS 接続数詳細テーブルの列の説明

列名	説明
ドメイン	送信者のドメイン名。
成功した TLS 必須失敗しました (Failed)	失敗した、必要なすべての TLS 接続。



列名	説明
成功した TLS 必須Success	成功した、必要なすべての TLS 接続。
失敗したTLS推奨 (TLS Pref. Failed)	失敗した、優先するすべての TLS 接続。
成功したTLS推奨 (TLS Pref. Success)	成功した、優先するすべての TLS 接続。
最終 TLS ステータス	次の条件に基づいて割り当てられた TLS 接続のステータス : <ul style="list-style-type: none"> <li>• 0 : なし</li> <li>• 1 : 必須 - 失敗</li> <li>• 2 : 推奨 - 失敗</li> <li>• 3 : 必須 - 成功</li> <li>• 4 : 推奨 - 成功</li> </ul>
DANE失敗 (DANE Failure)	DANE がサポートされている送信 TLS 接続の失敗の合計数。
DANE成功 (DANE Success)	DANE がサポートされている送信 TLS 接続の成功の合計数。
合計TLS接続数 (Total TLS Connections)	TLS 接続の合計数。
暗号化されていない接続 (Unencrypted Connections)	暗号化されていない TLS 接続の合計数。
TLSの割合(%%) (% TLS of all Connections)	すべての TLS 接続に対する TLS 暗号化の割合。
TLS経由のメッセージ (Messages by TLS)	TLS メッセージの総数。

## [受信 SMTP 認証 (Inbound SMTP Authentication)] ページ

[受信SMTP認証 (Inbound SMTP Authentication)] レポートページには、クライアント証明書の使用情報、およびEメールセキュリティアプライアンスとユーザのメールクライアント間でSMTPセッションを認証するためのSMTP AUTH コマンドが表示されます。アプライアンスは、証明書またはSMTP AUTH コマンドを受け入れると、メールクライアントへのTLS接続を確立します。クライアントはこの接続を使用してメッセージを送信します。アプライアンスは、これらの試行をユーザ単位で追跡できないため、レポートには、ドメイン名とドメインIPアドレスに基づいてSMTP認証の詳細が表示されます。

次の情報を確認するには、このレポートを使用します。

- SMTP 認証を使用している着信接続の総数
- クライアント証明書を使用している接続の数
- SMTP AUTH を使用している接続の数
- SMTP 認証を使用しようとして、接続が失敗したドメイン
- SMTP 認証が失敗した一方で、フォールバックを正常に使用している接続の数

セキュリティ管理アプライアンスで [受信SMTP認証 (Inbound SMTP Authentication)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)] > [受信SMTP認証 (Inbound SMTP Authentication)]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[受信SMTP認証 (Inbound SMTP Authentication)] には 2 つのビューがあります。

- ドメイン (Domains)
- IP アドレス

これらのビューでは、SMTP 認証のスナップショットが、選択したビューのコンテキストで提供されます。

[受信SMTP認証 (Inbound SMTP Authentication)] レポート ページには、受信した接続のグラフ、SMTP 認証接続を試行した受信した受信者のグラフ、および接続の認証試行の詳細を含むテーブルが表示されます。

次のリストでは、[受信SMTP認証 (Inbound SMTP Authentication)] レポート ページのさまざまなセクションについて説明します。

表 36: [受信SMTP認証 (Inbound SMTP Authentication)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	表示する時間範囲を選択するためのオプションを伴うドロップダウンリスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data For)] (ドロップダウンリスト)	データを表示する E メールセキュリティアプライアンスを選択するか、[全 E メールアプライアンス (All Email Appliances)] を選択します。 <a href="#">アプライアンスまたはレポートグループのレポートデータの表示 (26 ページ)</a> も参照してください。

セクション	説明
[受信した接続 (Received Connections) ] グラフ	[受信した接続 (Received Connections) ] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメールクライアントの着信接続が示されます。このグラフには、アプライアンスが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。
[受信した受信者 (Received Recipients) ] グラフ	[受信した受信者 (Received Recipients) ] グラフには、SMTP 認証を使用して、メッセージを送信するために Email Security Appliances への接続を認証しようとしたメールクライアントを所有する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。
(ドメイン名または IP アドレスによる) SMTP 認証の詳細。	(ドメイン名または IP アドレスによる) SMTP 認証の詳細テーブルには、メッセージを送信するために E メールセキュリティアプライアンスへの接続を認証しようとするユーザの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行 (成功または失敗) の数、SMTP AUTH コマンドを使用した接続試行 (成功または失敗) の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。

## [レート制限 (Rate Limits) ] ページ

エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メールメッセージ受信者数を制限できます。[レート制限 (Rate Limits) ] レポートには、この制限を最も上回った送信者が表示されます。

このレポートは、以下を特定する場合に役立ちます。

- 大量のスパムを送信するために使用される可能性のある信用できないユーザアカウント
- 通知、アラート、自動報告などに電子メールを使用する組織内の制御不能アプリケーション
- 内部請求やリソース管理のために、組織内で電子メールを過剰に送信している送信元
- スпамとは見なされないが、大量の着信電子メールトラフィックを送信している送信元

セキュリティ管理アプライアンスで [レート制限 (Rate Limits) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [レート制限 (Rate Limits) ]

を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

内部送信者に関する統計情報を含む他のレポート ([内部ユーザ (Internal Users)]、[送信メッセージ送信者 (Outgoing Senders)] など) では、送信されたメッセージの数のみ計測されません。これらのレポートでは、少数のメッセージを多数の受信者に送信した送信者は識別されません。

[上位攻撃者(インシデント別) (Top Offenders by Incident)] チャートには、設定済み制限よりも多くの受信者にメッセージを最も頻繁に送信しようとしたエンベロープ送信者が表示されます。各試行が1インシデントに相当します。このチャートでは、すべてのリスナーからのインシデント数が集計されます。

[上位攻撃者(拒否した受信者数) (Top Offenders by Rejected Recipients)] チャートには、設定済みの制限を上回る、最も多くの受信者にメッセージを送信したエンベロープ送信者が表示されます。このチャートでは、すべてのリスナーからの受信者数が集計されます。

[エンベロープ送信者のレート制限 (Rate Limit for Envelope Senders)] 設定を含む [レート制限 (Rate Limiting)] 設定は、E メールセキュリティ アプライアンスの [メール ポリシー (Mail Policies)] > [メール フロー ポリシー (Mail Flow Policies)] で設定します。レート制限の詳細については、ご使用の E メールセキュリティ アプライアンスのマニュアルまたはオンラインヘルプを参照してください。

#### 関連項目

[\[大容量のメール \(High Volume Mail\)\] ページ \(172 ページ\)](#)

## [国別の接続 (Connections by Country)] ページ

[国別の接続 (Connections by Country)] レポート ページを使用すると、次の情報を表示できます。

- 発信国別の受信メール接続数の上位 (グラフィカルな形式)。
- 発信国別の受信メール接続およびメッセージの合計数 (表形式)。

セキュリティ管理アプライアンスで [国別の接続 (Connections by Country)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [電子メール (Email)] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [国別の接続 (Connections by Country)] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

国情報を表示しない受信メール接続の上位と合計数の例を次に示します。

- 送信者 IP アドレスがプライベート IP アドレスに属している。
- 送信者の IP アドレスは、有効な SBRS を取得していません。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の青い番号のリンクをクリックします。

[国別の接続 (Connections by Country) ] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

## [ユーザーメールサマリー (User Mail Summary) ] ページ

[ユーザーメール概要 (User Mail Summary) ] ページでは、内部ユーザによって送受信されたメールに関する情報が、電子メールアドレスごとに表示されます (単一ユーザの複数の電子メールアドレスが、リストに表示される場合があります。レポートでは、電子メールアドレスはまとめられません)。

このページは、2つのセクションで構成されます。

- 正常な着信メッセージ別および正常な発信メッセージ別の上位ユーザと、グレイメールを受信する上位ユーザを示すグラフ。
- ユーザメールフローの詳細

レポート対象の時間範囲 (時間、日、週、または月) を選択できます。グラフまたは詳細リストのデータは、すべてのレポートと同様に [エクスポート (Export) ] リンクを使用して CSV 形式にエクスポートできます。また、テーブルの右上にある [列をカスタマイズ (Customize Column) ] アイコンをクリックすると、非表示のテーブル列を表示したり、デフォルトの列を非表示にしたりできます。

[ユーザーメールフローの詳細 (User Mail Flow Details) ] リストでは、送受信メールが電子メールアドレス別に正常、スパム、(着信のみ)、ウイルス、マルウェア、コンテンツ フィルタの一致、グレイメール (着信のみ) に分類されます。このリストは、カラム見出しをクリックしてソートできます。

内部ユーザ レポートを使用すると、次の情報を入手できます。

- 最も多くの外部メールを送信したユーザ
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのグレイメール メッセージを受信したユーザ
- 最も多くのスパムを受信したユーザ
- コンテンツ フィルタをトリガーしたユーザとそのコンテンツ フィルタの種類
- 電子メールをコンテンツ フィルタで捕捉されたユーザ

着信内部ユーザとは、**Rcpt To:** アドレスに基づいてシステムで電子メールを受信する対象ユーザのことです。発信内部ユーザは**Mail From:** アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

一部の送信メール (バウンスなど) の送信者は、null です。これらの送信者は、送信および「不明」に集計されます。

内部ユーザの [内部ユーザの詳細 (Internal User Details) ] ページを表示するには、この内部ユーザをクリックします。

表の右上にある [列をカスタマイズ (Customize Columns) ] アイコンをクリックすると、[Intelligent Multi-Scanで検出された着信スパム (Incoming Spam Detected by Intelligent Multi-Scan) ] 列や

## [ユーザメールフローの詳細 (User Mail Flow Details) ] テーブル

[Intelligent Multi-Scanで検出された発信スパム (Outgoing Spam Detected by Intelligent Multi-Scan) ] 列など、デフォルトでは非表示の列が表示されます。

## 関連項目

- [\[ユーザメールフローの詳細 \(User Mail Flow Details\) \]](#)
- [特定の内部ユーザの検索](#)

## [ユーザメールフローの詳細 (User Mail Flow Details) ] テーブル

[ユーザメールフローの詳細 (User Mail Flow Details) ] テーブルでは、受信および送信メッセージの内訳、各カテゴリ ([スパム検出 (Spam Detected) ]、[ウイルス検出 (Virus Detected) ]、[コンテンツフィルタによる停止 (Stopped By Content Filter) ] など) のメッセージ数など、ユーザに関する詳細情報が示されます。送受信コンテンツ フィルタの一致も示されます。

着信内部ユーザとは、Rcpt To: アドレスに基づいてシステムで電子メールを受信する対象ユーザのことです。発信内部ユーザはMail From: アドレスに基づいており、内部ネットワーク内の送信者が送信している電子メールの種類を追跡する場合に役立ちます。

送信メールの中には (バウンスなど) 、送信者がnullになっているものがあります。これらの送信者は、送信「不明」として集計されます。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表は、[ユーザメールフローの詳細 (User Mail Flow Details) ] テーブルの列の説明を示しています。

表 37: [ユーザメールフローの詳細 (User Mail Flow Details) ] テーブルの列の説明

列名	説明
内部ユーザ	内部ユーザのドメイン名。
[受信スパム検出 (Incoming Spam Detected) ]	検出されたすべての受信スパム。
[受信ウイルス検出 (Incoming Virus Detected) ]	検出された受信ウイルス。
高度なマルウェア防御で検出された受信メール (Incoming Detected by Advanced Malware Protection)	高度なマルウェア防御 (ファイル分析とファイル レピュテーション) で検出された受信メッセージ。
[受信コンテンツフィルタの一致数 (Incoming Content Filter Matches) ]	検出された受信コンテンツ フィルタの一致。

列名	説明
[コンテンツフィルタによる受信停止 (Incoming Stopped by Content Filter) ]	設定したコンテンツフィルタによって阻止された受信メッセージ。
受信マーケティング (Incoming Marketing)	マーケティングとして検出された受信メッセージ。
受信ソーシャルネットワーキング (Incoming Social Networking)	ソーシャル ネットワーキングとして検出された受信メッセージ。
受信バルク (Incoming Bulk)	バルクとして検出された受信メッセージ。
受信グレイメール (Incoming Graymails)	グレイメールとして検出された受信メッセージ。
[正常な受信 (Incoming Clean) ]	すべての着信クリーン メッセージ。
[送信スパム検出 (Outgoing Spam Detected) ]	検出された発信スパム。
[送信ウイルス検出 (Outgoing Virus Detected) ]	検出された送信ウイルス。
[送信コンテンツフィルタの一致数 (Outgoing Content Filter Matches) ]	検出された送信コンテンツ フィルタの一致。
[コンテンツフィルタによる送信停止 (Outgoing Stopped by Content Filter) ]	設定されていたコンテンツフィルタのため阻止された発信メッセージ。
[正常な送信 (Outgoing Clean) ]	すべての発信クリーン メッセージ。

## 特定の内部ユーザの検索

[ユーザメール概要 (User Mail Summary) ] ページおよび [ユーザメールフローの詳細 (User Mail Flow Details) ] ページの下部にある検索フォームで、特定の内部ユーザ (電子メールアドレス) を検索できます。検索テキストに完全に一致させるか、入力したテキストで始まる項目を検索するか (たとえば、「ex」で始まる項目を検索する場合、「example@example.com」が一致します) を選択します。

## [DLP インシデント サマリー (DLP Incident Summary) ] ページ

[DLP インシデント (DLP Incidents) ] ([DLP インシデント サマリー (DLP Incident Summary) ]) レポート ページには、送信メールで発生した、データ消失防止 (DLP) ポリシーに違反するインシデントの情報が示されます。E メールセキュリティ アプライアンスでは、[送信メールポリシー (Outgoing Mail Policies) ] テーブルで有効にした DLP 電子メールポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

[DLP インシデント サマリー (DLP Incident Summary) ] レポートを使用すると、次のような情報を取得できます。

- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP インシデント サマリー (DLP Incident Summary) ] ページには次の 2 つのメイン セクションがあります。

- 重大度 ([低 (Low) ]、[中 (Medium) ]、[高 (High) ]、[重大 (Critical) ]) 別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンドグラフ。
- [DLP インシデントの詳細 (DLP Incident Details) ] リスト。

セキュリティ管理 アプライアンスで [DLP インシデント サマリー (DLP Incident Summary) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから **[モニタリング (Monitoring) ] > [DLP インシデント サマリー (DLP Incident Summary) ]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[DLP インシデント (DLP Incidents) ] レポート ページから raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポーティング データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

データ内の特定の情報を検索するには、[検索およびインタラクティブ電子メールレポート ページ \(61 ページ\)](#) を参照してください。

次のリストでは、[DLP インシデント サマリー (DLP Incident Summary) ] レポート ページのさまざまなセクションについて説明します。



表 38: [DLPインシデントサマリー (DLP Incident Summary) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	表示する時間範囲を選択するためのオプションを伴うドロップダウンリスト。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data For) ] (ドロップダウンリスト)	データを表示する E メールセキュリティ アプライアンスを選択するか、[全 E メール アプライアンス (All Email Appliances) ] を選択します。  <a href="#">アプライアンスまたはレポート グループのレポートデータの表示 (26 ページ)</a> も参照してください。
[重大度別上位インシデント (Top Incidents by Severity) ]	重大度別の上位 DLP インシデント。
[インシデントサマリー (Incident Summary) ]	各電子メール アプライアンスの送信メール ポリシーで現在有効になっている DLP ポリシーは、[DLPインシデントサマリー (DLP Incident Summary) ] ページの下部にある [DLPインシデントの詳細 (DLP Incident Details) ] インタラクティブ テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。
[上位 DLP ポリシー一致数 (Top DLP Policy Matches) ]	一致している上位 DLP ポリシー。
[DLPインシデントの詳細 (DLP Incident Details) ]	[DLPインシデントの詳細 (DLP Incidents Details) ] テーブルには、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。  このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## [Web インタラクション (Web Interaction) ] ページ

- Web インタラクション トラッキング レポート モジュールには、Web インタラクションのトラッキング機能がイネーブルの場合のみデータが取り込まれます。
- Web インタラクション トラッキング レポート モジュールは、リアルタイムでは更新されず、30 分おきに更新されます。また、書き換えられた URL をクリックした後で、Web インタラクション トラッキング レポートにこのイベントがレポートされるまでには最大 2 時間かかることがあります。

- Web インタラクション トラッキング レポートは、リアルタイムで更新されません。クラウドにリダイレクトされる書き換えられた URL をクリックした後、Web インタラクション トラッキング レポートにこのイベントがレポートされるまでには最大 2 時間かかることがあります。
- Web インタラクション トラッキング レポートは、送受信メッセージに対して使用できます。
- エンドユーザがクリックした、クラウドにリダイレクトされる書き換えられた URL (ポリシーまたはアウトブレイク フィルタによって) のみが、これらのモジュールに含まれます。
- [Web インタラクション トラッキング (Web Interaction Tracking) ] ページには、次のレポートが含まれます。

エンドユーザがクリックした、悪意のある上位 URL (Top Malicious URLs clicked by End Users) 。次の情報を含む詳細レポートを表示するには、URL をクリックします。

- 書き換えられた悪意のある URL をクリックしたエンドユーザのリスト。
- URL がクリックされた日付と時刻。
- URL がポリシーまたはアウトブレイク フィルタによって書き換えられたかどうか。
- 書き換えられた URL がクリックされたときに実行されたアクション (許可、ブロック、または不明) 。 URL がアウトブレイク フィルタによって書き換えられており、最終的な判定が使用できない場合、ステータスは不明として表示されます。

#### 悪意のある URL をクリックした上位エンドユーザ (Top End Users who clicked on Malicious URLs)

このセクションには、受信メッセージおよび送信メッセージについて、書き換えられた悪意のある URL を最も多くクリックしたユーザの概要が表示されます。

Web インタラクション トラッキングの詳細 (Web Interaction Tracking Details) 。次の情報が含まれています。

- クラウドにリダイレクトされる書き換えられたすべての URL のリスト (悪意のあるものとなないもの) 。詳細レポートを表示するには、URL をクリックします。
- クラウドにリダイレクトされる書き換えられた URL がクリックされた場合に実行されたアクション (許可、ブロック、または不明) 。

データを表示するには、次の操作を実行します。

- [受信メールポリシー (Incoming Mail Policies) ] > [アウトブレイクフィルタ (Outbreak Filters) ] を選択してアウトブレイク フィルタを設定し、メッセージの変更および URL の書き換えを有効にします。
- 「Cisco Security Proxy にリダイレクト」アクションを使用して、コンテンツ フィルタを構成します。

エンドユーザが URL をクリックしたときにその URL の判定 (正常または悪意のある) が不明である場合、ステータスは不明として表示されます。これは、ユーザのクリック時に、URL がさらに調査されていたか、Web サーバがダウンしていたか、到達不可能であったためである可能性があります。

- 書き換えられた URL をエンドユーザがクリックした回数。クリックされた URL を含むすべてのメッセージのリストを表示するには、番号をクリックします。
- Web インタラクショントラッキングレポートを使用している場合は、次の制限事項に注意してください。
  - 悪意のある URL を書き換えた後に、メッセージを送信して別のユーザ（管理者など）に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックした場合でも、元の受信者の Web インタラクショントラッキングデータが増分します。
  - 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用してユーザ（管理者など）に送信する場合、そのユーザ（メッセージのコピーが送信されたユーザ）がその書き換えられた URL をクリックした場合でも、元の受信者の Web インタラクショントラッキングデータが増分します。
  - どの時点であっても、アプライアンスの時刻を変更する予定がある場合は、システム時刻は協定世界時 (UTC) と同期するようにしてください。

## Webインタラクショントラッキングの詳細 (Web Interaction Tracking Details)

[Webインタラクショントラッキングの詳細 (Web Interaction Tracking Details)] テーブルは、次の情報を含むインタラクティブテーブルです。

- 書き換えられたすべての URL のリスト（悪意のあるものとないもの）。
- 書き換えられた URL がクリックされた場合に実行されたアクション（許可、ブロック、または不明）。
- エンドユーザが URL をクリックしたときにその URL の判定（クリーンまたは悪意のある）が不明である場合、ステータスは不明として表示されます。これは、ユーザのクリック時に、URL がさらに調査されていたか、Web サーバがダウンしていたか、到達不可能であったためである可能性があります。
- 書き換えられた URL をエンドユーザがクリックした回数。
- 次の点に注意してください。
  - 悪意のある URL を書き換えた後に、メッセージを送信して別のユーザ（管理者など）に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクショントラッキングデータが増分します。
  - 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用して元の受信者以外のユーザ（管理者など）に送信する場合、その他のユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクショントラッキングデータが増分します。

このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## [メッセージフィルタ (Message Filters) ] ページ

[メッセージフィルタ (Message Filters) ] レポート ページには、送受信メッセージのメッセージフィルタの上位一致 (最も多くのメッセージに一致したメッセージフィルタ) に関する情報が表示されます。

[メッセージフィルタ (Message Filters) ] レポート ページを使用すると、次を表示できます。

- グラフィカル形式での、一致数による上位メッセージ フィルタ。
- 表形式での、一致数による上位メッセージ フィルタ。

セキュリティ管理アプライアンスで [メッセージフィルタ (Message Filters) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [メッセージフィルタ (Message Filters) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[メッセージフィルタ (Message Filters) ] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポーティング データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

## [大容量のメール (High Volume Mail) ] ページ

[大容量のメール (High Volume Mail) ] レポート ページを使用すると、次の操作を実行することができます。

- 1人の送信者から送られていたり、件名が同じであったり、1時間の間に送られたりした、多数のメッセージが関係する攻撃を特定します。
- このような攻撃が独自のドメイン内で発生しないように上位ドメインをモニタします。この状況が生じると、組織の1つ以上のアカウントが侵害される可能性があります。
- フィルタを適宜調整できるように、誤検出を特定します。

[大容量のメール (High Volume Mail) ] レポート ページを使用すると、次の情報を表示することができます。

- 上位の件名を持つメッセージ (グラフ形式) 。
- 上位のエンベロープ送信者を持つメッセージ (グラフ形式) 。
- 上位のメッセージ フィルタ (一致数別、グラフ形式) 。
- メッセージ フィルタの合計 (一致数別、表形式) 。

セキュリティ管理アプライアンスで [大容量のメール (High Volume Mail) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [大容量のメール (High

Volume Mail) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[大容量のメール (High Volume Mail) ] レポート ページから、raw データを CSV ファイルにエクスポートすることができます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。

このページのレポートには、ヘッダー反復ルールを使用し、そのルールで設定されたメッセージ数のしきい値を超えるメッセージフィルタからのデータのみが表示されます。他のルールと組み合わせた場合、ヘッダー反復ルールの評価は最後になります。また、先行する条件によってメッセージの処理が決定されると評価は行われません。同様に、レート制限で検出されたメッセージはヘッダー反復メッセージフィルタに達しません。したがって、別の状況では大容量のメールと見なされるメッセージが、これらのレポートに含まれない場合があります。特定のメッセージをホワイトリストに追加するようにフィルタを設定している場合は、それらのメッセージもレポートから除外されます。

メッセージフィルタおよびヘッダー反復ルールの詳細については、お使いの E メールセキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドを参照してください。

## [コンテンツフィルタ (Content Filters) ] ページ

[コンテンツフィルタ (Content Filters) ] レポート ページには、送受信コンテンツ フィルタの上位一致 (最も多くのメッセージに一致したコンテンツ フィルタ) に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツ フィルタ (Content Filters) ] レポート ページを使用して、次のタイプの質問に答えることができます。

- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ。
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ。

[コンテンツ フィルタ (Content Filters) ] レポート ページを使用すると、次を表示できます。

- グラフィカル形式での、上位の着信および発信コンテンツ フィルタの一致。
- 表形式での、上位の着信および発信コンテンツ フィルタの一致。

セキュリティ管理アプライアンスで [コンテンツフィルタ (Content Filters) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [電子メール (Email) ] を選択し、[レポート (Reports) ] ドロップダウンから **[モニタリング (Monitoring) ] > [コンテンツフィルタ (Content Filters) ]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[コンテンツ フィルタ (Content Filters) ] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) を参照してください。



(注) 注: [コンテンツフィルタ (Content Filter)] ページのスケジュール設定されたレポートを生成できます。 [メールレポートのスケジュール設定 \(181 ページ\)](#) を参照してください。

## [コンテンツフィルタの詳細 (Content Filter Details)] ページ

[コンテンツフィルタの詳細 (Content Filter Detail)] ページには、このフィルタの経時的な一致および内部ユーザ別の一致が表示されます。

[内部ユーザ別の一致 (Matches by Internal User)] セクションで、内部ユーザ (電子メールアドレス) の詳細ページを表示するユーザ名をクリックします。詳細については、[#unique\\_203](#) を参照してください。

アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

## [有効なレポートデータ (Reporting Data Availability)] ページ

[メール (Email)] > [レポート (Reporting)] > [有効なレポートデータ (Reporting Data Availability)] ページでは、リソース使用率および電子メール トラフィックの障害のある場所がリアルタイムに表示されるようにデータを表示、更新およびソートできます。

このページから、セキュリティ管理アプライアンスによって管理されるアプライアンス全体のデータ アベイラビリティを含めて、すべてのデータ リソース使用率および電子メール トラフィックに障害のある場所が表示されます。

このレポート ページから、特定のアプライアンスおよび時間範囲のデータ アベイラビリティを表示することもできます。

## グレイメールのレポート

グレイメールの統計情報は、次のレポートに反映されます。

レポート	含まれるグレイメール データ
[メールフロー概要 (Mail Flow Summary)] ページ > [着信 (Incoming)] タブ	グレイメール カテゴリ (マーケティング、ソーシャル、およびバルク) ごとの着信グレイメールメッセージの数と、グレイメールメッセージの総数。
[メールフローの詳細 (Mail Flow Details)] ページ > [送信者 (Outgoing Senders)] タブ	グレイメールの上位送信者。

レポート	含まれるグレイメールデータ
[メールフローの詳細 (Mail Flow Details)] ページ > [着信メール (Incoming Mails)] タブ	グレイメール カテゴリ (マーケティング、ソーシャル、およびバルク) ごとの着信グレイメールメッセージの数と、すべての IP アドレス、ドメイン名、またはネットワーク オーナーのグレイメールメッセージの総数。
[ユーザメールの概要 (User Mail Summary)] ページ > [グレイメールの上位ユーザ (Top Users by Graymail)]	グレイメールを受信する上位エンドユーザ。
[ユーザメールの概要 (User Mail Summary)] ページ > [ユーザメールの詳細 (User Mail Details)]	グレイメール カテゴリ (マーケティング、ソーシャル、およびバルク) ごとの着信グレイメールメッセージの数と、すべてのユーザのグレイメールメッセージの総数。

#### 関連項目

- [AsyncOS 9.5 へのアップグレード後のマーケティングメッセージのレポート \(108 ページ\)](#)

## AsyncOS 9.5 へのアップグレード後のマーケティングメッセージのレポート

AsyncOS 9.5 へのアップグレード後 :

- マーケティングメッセージの数は、アップグレードの前後に検出されたマーケティングメッセージの合計です。
- グレイメールメッセージの総数には、アップグレードの前に検出されたマーケティングメッセージの数は含まれません。
- 試行されたメッセージの総数には、アップグレードの前に検出されたマーケティングメッセージの数も含まれます。
- 管理対象の E メールセキュリティアプライアンスでグレイメール機能が有効になっていない場合、マーケティングメッセージはクリーンメッセージとしてカウントされます。

## スケジュール設定された電子メールレポートとオンデマンドの電子メールレポートについて

#### 使用可能なレポートの種類

特記のない限り、次のタイプの電子メールセキュリティレポートは、スケジュール設定されたレポートおよびオンデマンドレポートとして使用できます。

- [コンテンツフィルタ (Content Filters)] : このレポートには最大 40 のコンテンツ フィルタが表示されます。このページに表示されるその他の情報については、[\[コンテンツフィルタ \(Content Filters\)\] ページ \(173 ページ\)](#) を参照してください。
- [DLPインシデントサマリー (DLP Incident Summary)] : このページに表示される情報については、[\[DLP インシデント サマリー \(DLP Incident Summary\)\] ページ \(168 ページ\)](#) を参照してください。
- [送信処理ステータス (Delivery Status)] : このレポートページには、特定の受信者ドメインまたは仮想ゲートウェイアドレスへの配信の問題についての情報が表示されます。また、このページには、直近 3 時間以内にシステムによって配信されたメッセージの上位 20、50、または 100 の受信者ドメインのリストが表示されます。各統計情報の列見出しのリンクをクリックすることによって、最新のホストステータス、アクティブな受信者 (デフォルト)、切断した接続、配信された受信者、ソフト バウンス イベント、およびハード バウンス受信者別にソートできます。E メールセキュリティ アプライアンスでの [送信処理ステータス (Delivery Status)] ページの役割の詳細については、お使いの E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。
- [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] : このレポートは [\[メールフロー概要 \(Mail Flow Summary\)\] ページ \(118 ページ\)](#) に基づき、指定されたドメインのグループに制限されます。表示される情報については、[\[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\)\] レポート \(177 ページ\)](#) を参照してください。
- [エグゼクティブサマリー (Executive Summary)] : このレポートは [\[メールフロー概要 \(Mail Flow Summary\)\] ページ \(118 ページ\)](#) の情報に基づきます。表示される情報については、[\[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\)\] レポート \(177 ページ\)](#) を参照してください。
- [メールフローの詳細 (Mail Flow Details)] : このページに表示される情報については、[\[メールフローの詳細 \(Mail Flow Details\)\] ページ \(147 ページ\)](#) を参照してください。
- [ユーザメール概要 (User Mail Summary)] : このページに表示される情報については、[#unique\\_203](#)を参照してください。
- [送信先 (Outgoing Destinations)] : このページに表示される情報については、[\[送信先 \(Outgoing Destinations\)\] ページ \(157 ページ\)](#) を参照してください。
- [送信者グループ (Sender Groups)] : このページに表示される情報については、[#unique\\_197](#)を参照してください。
- [TLS暗号化 (TLS Encryption)] : このページに表示される情報については、[#unique\\_199](#)を参照してください。
- [ウイルスタイプ (Virus Types)] : このページに表示される情報については、[\[ウイルスフィルタリング \(Virus Filtering\)\] ページ \(137 ページ\)](#) を参照してください。

### 時間範囲

各レポートは、前日、過去 7 日間、前月、過去の日 (最大 250 日)、または過去の月 (最大 12 ヶ月) のデータを含めるように設定できます。また、指定した日数 (2 ~ 100 日) または指定した月数 (2 ~ 12 ヶ月) のデータを含めることもできます。



レポートの実行時間にかかわらず、直前の時間間隔（過去1時間、1日、1週間、または1ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前1時に実行するようにスケジュールを設定した場合、レポートには前日の00:00から23:59までのデータが含まれます。

## 言語とロケール



- (注) 個々のレポートに特定のロケールを使用して、PDF レポートをスケジュール設定したり、raw データを CSV ファイルとしてエクスポートしたりすることができます。[スケジュール設定されたレポート (Scheduled Reports)] ページの言語ドロップダウンメニューでは、ユーザが現在選択しているロケールおよび言語で PDF レポートを表示またはスケジュールすることができます。 [レポーティング データおよびトラッキング データのエクスポート \(33 ページ\)](#) の重要な情報を参照してください。

## アーカイブ済みレポートの保存

レポートの保存期間や、アーカイブ済みレポートがいつシステムから削除されるかについては、[\[アーカイブメールレポート \(Archived Email Reports\)\] の表示と管理 \(185 ページ\)](#) を参照してください。

## その他のレポートタイプ

セキュリティ管理アプライアンスの [メール (Email)] > [レポート (Reporting)] セクションでは、次の2種類の特別なレポートを生成できます。

- [\[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\)\] レポート \(177 ページ\)](#)
- [\[エグゼクティブサマリー \(Executive Summary\)\] レポート \(181 ページ\)](#)

### [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポート

[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートには、ネットワーク内の1つまたは複数のドメインの着信および発信メッセージの概要が表示されます。これは [エグゼクティブサマリー (Executive Summary)] レポートと似ていますが、レポートデータが、指定したドメインで送受信されるメッセージに制限されます。[送信メールサマリー (Outgoing Mail Summary)] には、送信サーバの PTR (ポインタ レコード) のドメインが、指定したドメインに一致する場合にのみデータが表示されます。複数のドメインが指定されている場合、このアプライアンスはすべてのドメインのデータを1つのレポートに集約します。

サブドメインのレポートを生成するには、Eメールセキュリティアプライアンスおよびセキュリティ管理アプライアンスのレポーティングシステムで、親ドメインをセカンドレベルドメインとして追加する必要があります。たとえば、`example.com` をセカンドレベルドメインとして追加した場合、`subdomain.example.com` のようなサブドメインをレポーティングに使用できるようになります。セカンドレベルドメインを追加するには、Eメールセキュリティアプライ

[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ] レポートと送信者レピュテーションフィルタリングによってブロックされたメッセージ

アンスの CLI で **reportingconfig -> mailsetup -> tld** を実行し、セキュリティ管理アプライアンスの CLI で **reportingconfig -> domain -> tld** を実行します。

その他のスケジュール設定されたレポートとは異なり、[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ] レポートはアーカイブされません。

### [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ] レポートと送信者レピュテーションフィルタリングによってブロックされたメッセージ

送信者レピュテーションフィルタリングによってブロックされたメッセージはワークキューに入らないため、AsyncOS はこれらのメッセージに対して、宛先ドメインを判定するための処理は行いません。アルゴリズムによって、ドメインごとに拒否されたメッセージ数が推定されます。ドメインごとのブロックされたメッセージの正確な数を知るには、メッセージが受信者レベル (RCPT TO) に達するまでセキュリティ管理アプライアンスでの HAT 拒否を遅らせます。そうすることで、AsyncOS が着信メッセージから受信者データを収集できるようになります。Eメールセキュリティアプライアンスで **listenerconfig -> setup** コマンドを使用して拒否を遅らせることができます。ただし、このオプションはシステムのパフォーマンスに影響を及ぼす可能性があります。遅延した HAT 拒否の詳細については、ご使用の Eメールセキュリティアプライアンスのマニュアルを参照してください。



- (注) セキュリティ管理アプライアンスのドメインごとのエグゼクティブサマリーレポートでレピュテーションフィルタによる停止を表示するには、Eメールセキュリティアプライアンスとセキュリティ管理アプライアンスの両方で **hat\_reject\_info** を有効にする必要があります。セキュリティ管理アプライアンス上で **hat\_reject\_info** を有効にするには、**reportingconfig > domain > hat\_reject\_info** コマンドを実行します。

### [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ] レポートのドメインおよび受信者のリストの管理

コンフィギュレーションファイルを使用して、[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ] レポートのドメインおよび受信者を管理できます。コンフィギュレーションファイルは、アプライアンスのコンフィギュレーションディレクトリに保存されるテキストファイルです。このファイルの行ごとに、個別のレポートが生成されます。これによって、大量のドメインおよび受信者を1つのレポートに含めることができ、複数のドメインレポートを1つのコンフィギュレーションファイルで定義できます。

コンフィギュレーションファイルの各行には、ドメイン名のスペース区切りリストと、レポート受信者の電子メールアドレスのスペース区切りリストが含まれます。ドメイン名のリストと電子メールアドレスのリストはカンマで区切られます。subdomain.example.com のように、親ドメイン名の前にサブドメイン名とピリオドを追加すると、サブドメインを含めることができます。

次に示すファイルは、3つのレポートを生成する1つのレポートコンフィギュレーションファイルです。

```
yourdomain.com sampledomain.com, admin@yourdomain.com
```

```
sampledomain.com, admin@yourdomain.com user@sampledomain.com  
subdomain.example.com mail.example.com, user@example.com
```



- (注) コンフィギュレーションファイルと1つの名前付きレポートに定義された設定を使用して、複数のレポートを同時に生成することができます。たとえば、Bigfishという名前の会社がRedfishとBluefishという名前の会社を買収し、RedfishとBluefishのドメインを引き続き維持するとします。Bigfish社は、個々のドメインレポートに対応する3行が含まれるコンフィギュレーションファイルを使用して1つの[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ]レポートを作成します。アプライアンスで[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ]レポートが生成されると、Bigfish社の管理者はBigfish.com、Redfish.com、およびBluefish.comドメインのレポートを受信し、Redfish社の管理者はRedfish.comドメインのレポートを受信し、Bluefish社の管理者はBluefish.comドメインのレポートを受信します。

名前付きレポートごとに異なるコンフィギュレーションファイルを実験にアップロードできます。また、複数のレポートに対して同じコンフィギュレーションファイルを使用することもできます。たとえば、異なる期間の同じドメインに関するデータが表示される、複数の名前付きレポートを作成できます。アプライアンスにコンフィギュレーションファイルをアップロードする場合は、ファイル名を変更しない限り、GUIでレポート設定を更新する必要がありません。

## [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ]レポートの作成

- ステップ 1** セキュリティ管理アプライアンスでレポートのスケジュールを設定することも、すぐにレポートを生成することもできます。

レポートのスケジュールを設定するには、次の手順を実行します。

- (新しいWebインターフェイスのみ) クラウドEメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- [メール (Email) ]>[レポート (Reporting) ]>[スケジュール設定されたレポート (Scheduled Reports) ]を選択します。
- [定期レポートの追加 (Add Scheduled Report) ]をクリックします。

オンデマンドレポートを作成するには、次の手順を実行します。

- (新しいWebインターフェイスのみ) クラウドEメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- [メール (Email) ]>[レポート (Reporting) ]>[アーカイブレポート (Archived Reports) ]を選択します。
- [今すぐレポートを生成 (Generate Report Now) ]をクリックします。

- ステップ 2** [レポートタイプ (Report Type) ] ドロップダウンリストから、[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ]レポートタイプを選択します。

**ステップ 3** レポートを含めるドメインおよびレポート受信者の電子メールアドレスを指定します。レポートを生成するための、次のいずれかのオプションを選択できます。

- [ドメインを個別に指定してレポートを生成 (Generate report by specifying individual domains) ]。レポートのドメインおよびレポート受信者の電子メールアドレスを入力します。複数のエントリを指定する場合は、カンマで区切ります。また、`subdomain.yourdomain.com` のようなサブドメインを使用することもできます。あまり頻繁には変更されないと予測される少数のドメインのレポートを作成する場合は、ドメインを個別に指定することを推奨します。
- [ファイルをアップロードしてレポートを生成 (Generate reports by uploading file) ]。レポートのドメイン、および受信者の電子メールアドレスのリストが含まれるコンフィギュレーションファイルをインポートします。アプライアンスのコンフィギュレーションディレクトリからコンフィギュレーションファイルを選択することも、ローカルコンピュータからアップロードすることもできます。頻繁に変更される多数のドメインのレポートを作成する場合は、コンフィギュレーションファイルの使用を推奨します。ドメインベースのレポートのコンフィギュレーションファイルの詳細については、[\[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\) \] レポートのドメインおよび受信者のリストの管理 \(178 ページ\)](#) を参照してください。

(注) レポートを外部アカウント (Yahoo! メールや Gmail など) に送信する場合は、レポートメッセージが誤ってスパムに分類されないように外部アカウントのホワイトリストにレポーティング返信アドレスを追加する必要がある場合があります。

**ステップ 4** [タイトル (Title) ] テキストフィールドに、レポートのタイトル名を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

**ステップ 5** [送信ドメイン (Outgoing Domain) ] セクションで、発信メールサマリーのドメインタイプを選択します。選択肢は [サーバ別 (By Server) ] または [電子メールアドレス別 (By Email Address) ] です。

**ステップ 6** [時間範囲 (Time Range to Include) ] ドロップダウンリストから、レポートデータの時間範囲を選択します。

**ステップ 7** [フォーマット (Format) ] セクションで、レポートの形式を選択します。

次のオプションがあります。

- PDF. 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー (Preview PDF Report) ] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- CSV. カンマ区切りの値の raw データが含まれる ASCII テキストファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

**ステップ 8** [スケジュール (Schedule) ] セクションから、レポートを生成するスケジュールを選択します。

選択肢は [日単位 (Daily) ]、[週単位 (Weekly) ] (曜日のドロップダウンリストがあります) または [月単位 (monthly) ] です。

**ステップ 9** (任意) レポートのカスタム ログをアップロードします。ロゴは、レポートの上部に表示されます。

- このロゴは、最大で 550 X 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。
- ログ ファイルをアップロードしなかった場合、デフォルトのシスコ ロゴが使用されます。

**ステップ 10** このレポートの言語を選択します。アジア言語での PDF ファイルの生成については、[レポーティング データおよびトラッキング データのエクスポート \(33 ページ\)](#) の重要な情報を参照してください。

**ステップ 11** [送信 (Submit)] をクリックして、ページ上の変更を送信し、[変更を確定 (Commit Changes)] をクリックして変更を保存します。

## [エグゼクティブサマリー (Executive Summary)] レポート

[エグゼクティブ サマリー (Executive Summary)] レポートは、E メールセキュリティ アプライアンスからの送受信電子メール メッセージ アクティビティの大きな概要です。セキュリティ管理 アプライアンスで表示できます。

このレポート ページには、[\[メールフロー概要 \(Mail Flow Summary\)\] ページ \(118 ページ\)](#) で表示できる情報の概要が表示されます。[電子メールレポーティングの概要 (Email Reporting Overview)] ページの詳細については、[\[メールフロー概要 \(Mail Flow Summary\)\] ページ \(118 ページ\)](#) を参照してください。

## [スケジュールされたレポート (Scheduled Reports)] ページ

- [メールレポートのスケジュール設定 \(181 ページ\)](#)
- [Web レポートのスケジュール設定 \(273 ページ\)](#)

## メールレポートのスケジュール設定

スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて ([175 ページ](#)) に示されているすべてのレポートをスケジュール設定できます。

レポートのスケジュール設定の管理方法については、次を参照してください。

- [スケジュール設定されたレポートの追加 \(181 ページ\)](#)
- [スケジュール設定されたレポートの編集 \(183 ページ\)](#)
- [スケジュール設定されたレポートの中止 \(183 ページ\)](#)

## スケジュール設定されたレポートの追加

スケジュール設定された電子メール レポートを追加するには、次の手順を実行します。

- 
- ステップ 1** [メール (Email) ]>[レポート (Reporting) ]>[スケジュール設定されたレポート (Scheduled Reports) ] を選択します。
- ステップ 2** [定期レポートの追加 (Add Scheduled Report) ] をクリックします。
- ステップ 3** レポート タイプを選択します。
- レポートタイプの説明については、[スケジュール設定された電子メールレポートとオンデマンドの電子メールレポートについて \(175 ページ\)](#) を参照してください。
- (注) - [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary) ] レポートの設定の詳細については、[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\) \] レポート \(177 ページ\)](#) を参照してください。
- スケジュール設定されたレポートに使用できるオプションは、レポート タイプによって異なります。この手順の残りの部分で説明するオプションを、すべてのレポートに適用する必要はありません。
- ステップ 4** [タイトル (Title) ] フィールドに、レポートのタイトルを入力します。
- 同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを推奨します。
- ステップ 5** [含む時間範囲 (Time Range to Include) ] ドロップダウンメニューからレポートの時間範囲を選択します。
- ステップ 6** 生成されるレポートの形式を選択します。
- デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。
- ステップ 7** レポートに応じて、[行数 (Number of Rows) ] で、レポートに含めるデータの量を選択します。
- ステップ 8** レポートに応じて、レポートをソートする基準となる列を選択します。
- ステップ 9** [スケジュール (Schedule) ] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。また、レポートのスケジュール設定に時刻を含めることもできます。時刻は、深夜 0 時を基準とした増分になります (00:00 ~ 23:59 が 1 日) 。
- ステップ 10** [メール (Email) ] テキストフィールドに、生成されたレポートが送信される電子メールアドレスを入力します。
- 電子メール受信者を指定しない場合でも、レポートはアーカイブされます。
- 必要に応じた数 (ゼロも含む) のレポート受信者を追加できます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリングリストを作成するほうが容易です。
- ステップ 11** レポートの言語を選択します。
- アジア言語については、[レポーティング データおよびトラッキング データのエクスポート \(33 ページ\)](#) の重要な情報を参照してください。
- ステップ 12** [送信 (Submit) ] をクリックします。
-

## スケジュール設定されたレポートの編集

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [メール (Email)] > [レポート (Reporting)] > [スケジュール設定されたレポート (Scheduled Reports)] を選択します。
- ステップ 3** [レポートタイトル (Report Title)] 列の、変更するレポート名リンクをクリックします。
- ステップ 4** レポート設定値を変更します。
- ステップ 5** 変更を送信し、保存します。

## スケジュール設定されたレポートの中止

スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、次のステップを実行します。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [メール (Email)] > [レポート (Reporting)] > [スケジュール設定されたレポート (Scheduled Reports)] を選択します。
- ステップ 3** 生成を中止するレポートに対応するチェックボックスを選択します。スケジュール設定されたすべてのレポートを削除するには、[すべて (All)] チェックボックスを選択します。
- ステップ 4** [削除 (Delete)] をクリックします。

(注) 削除されたレポートのアーカイブ版は、自動的に削除されるわけではありません。以前に生成されたレポートを削除するには、[アーカイブ済みのレポートの削除 \(186 ページ\)](#) を参照してください。

## オンデマンドでのメールレポートの生成

および新しい Web インターフェイスの電子メールレポートページの概要 (113 ページ) で説明したインタラクティブレポートページを使用して表示 (および PDF を生成) できるレポートに加えて、[スケジュール設定された電子メールレポートとオンデマンドの電子メールレポートについて \(175 ページ\)](#) に示したレポートの、指定したタイムフレームの PDF ファイルまたは raw データ CSV ファイルをいつでも保存できます。

オンデマンドレポートを生成するには、次の手順を実行します。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [メール (Email)] > [レポート (Reporting)] > [アーカイブレポート (Archived Reports)] を選択します。
- ステップ 3** [今すぐレポートを生成 (Generate Report Now)] をクリックします。
- ステップ 4** レポート タイプを選択します。
- レポートタイプの説明については、[スケジュール設定された電子メールレポートとオンデマンドの電子メールレポートについて \(175 ページ\)](#) を参照してください。
- ステップ 5** [タイトル (Title)] テキスト フィールドに、レポートのタイトル名を入力します。
- AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。
- (注) [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートの設定の詳細については、[\[ドメイン毎のエグゼクティブサマリー \(Domain-Based Executive Summary\)\] レポート \(177 ページ\)](#) を参照してください。
- スケジュール設定されたレポートに使用できるオプションは、レポート タイプによって異なります。この手順の残りの部分で説明するオプションを、すべてのレポートに適用する必要はありません。
- ステップ 6** [含める時間範囲 (Time Range to Include)] ドロップダウンリストから、レポート データの時間範囲を選択します。
- これはカスタム時間範囲オプションです。
- ステップ 7** [フォーマット (Format)] セクションで、レポートの形式を選択します。
- 次のオプションがあります。
- PDF. 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー (Preview PDF Report)] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
  - CSV. カンマ区切りの値の raw データが含まれる ASCII テキストファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。
- ステップ 8** レポートを実行するアプライアンスまたはアプライアンス グループを選択します。アプライアンス グループを作成していない場合、このオプションは表示されません。
- ステップ 9** [配信オプション (Delivery Option)] セクションから、次のオプションを選択します。
- [アーカイブレポート (Archive Report)] チェックボックスをオンにして、レポートをアーカイブします。
- このオプションを選択すると、レポートが [アーカイブレポート (Archived Reports)] ページに表示されます。



(注) [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートはアーカイブできません。

- [今すぐ受信者にメールを送る (Email now to recipients)] チェックボックスをオンにして、レポートを電子メールで送信します。

テキストフィールドに、レポートの受信者の電子メールアドレスを入力します。

**ステップ 10** このレポートの言語を選択します。アジア言語での PDF ファイルの生成については、[レポートデータおよびトラッキングデータのエクスポート \(33 ページ\)](#) の重要な情報を参照してください。

**ステップ 11** [このレポートを配信 (Deliver This Report)] をクリックして、レポートを生成します。

---

## [アーカイブメールレポート (Archived Email Reports)] ページ

- [スケジュール設定された電子メールレポートとオンデマンドの電子メールレポートについて \(175 ページ\)](#)
- [オンデマンドでのメールレポートの生成 \(183 ページ\)](#)
- [\[アーカイブメールレポート \(Archived Email Reports\)\] の表示と管理 \(185 ページ\)](#)

## [アーカイブメールレポート (Archived Email Reports)] の表示と管理

スケジュール設定されたレポートおよびオンデマンドレポートは、一定期間アーカイブされません。

セキュリティ管理アプライアンスでは、スケジュール設定された各レポートの最大 30 のインスタンスで、生成された最新のレポートをすべてのレポートに対して、合計 1000 バージョンまで保持します。30 インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。

アーカイブ済みのレポートは、アプライアンスの /periodic\_reports ディレクトリに保管されます。(詳細については、[IP インターフェイスおよびアプライアンスへのアクセス \(631 ページ\)](#) を参照してください)。

## アーカイブレポートへのアクセス

[メール (Email)] > [レポート (Reporting)] > [アーカイブレポート (Archived Reports)] ページには、生成されたがまだ消去されておらず、アーカイブすることを指定した、スケジュール設定されたレポートとオンデマンドレポートが表示されます。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [メール (Email)] > [レポート (Reporting)] > [アーカイブレポート (Archived Reports)] を選択します。
- ステップ 3** リストが長い場合に特定のレポートを見つけるには、[表示 (Show)] メニューからレポートタイプを選択してリストをフィルタリングするか、または列のヘッダーをクリックし、その列でソートします。
- ステップ 4** [レポートタイトル (Report Title)] をクリックすると、そのレポートが表示されます。
- 

## アーカイブ済みのレポートの削除

[[アーカイブメールレポート \(Archived Email Reports\)](#)] の表示と管理 (185 ページ) で説明したルールに従って、レポートは自動的にシステムから削除されます。ただし、不要なレポートを手動で削除することもできます。

アーカイブ済みのレポートを手動で削除するには、次の手順を実行します。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [メール (Email)] > [レポート (Reporting)] > [アーカイブレポート (Archived Reports)] を選択します。  
選択可能なアーカイブ済みのレポートが表示されます。
- ステップ 3** 削除する 1 つまたは複数のレポートのチェックボックスを選択します。
- ステップ 4** [削除 (Delete)] をクリックします。
- ステップ 5** スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、[スケジュール設定されたレポートの中止 \(183 ページ\)](#) を参照してください。
- 

## メールレポートのトラブルシューティング

- [アウトブレイク フィルタ レポートに情報が正しく表示されない \(187 ページ\)](#)
- [レポートのリンクをクリックした後のメッセージトラッキング結果がレポート結果と一致しない \(187 ページ\)](#)
- [\[高度なマルウェア保護判定のアップデート \(Advanced Malware Protection Verdict Updates\)\] レポートの結果が異なる \(187 ページ\)](#)

- [ファイル分析レポートの詳細の表示に関する問題 \(188 ページ\)](#)

「[すべてのレポートのトラブルシューティング \(36 ページ\)](#)」も参照してください。

## アウトブレイク フィルタ レポートに情報が正しく表示されない

### 問題

アウトブレイク フィルタ レポートに脅威情報が正しく表示されません。

### ソリューション

[管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[アップデート設定 (Update Settings) ]で指定した Cisco アップデート サーバとアプライアンスが通信できることを確認します。

## レポートのリンクをクリックした後のメッセージトラッキング結果がレポート結果と一致しない

### 問題

レポートからドリルダウンしたときのメッセージトラッキング結果が、予期した結果に一致しません。

### ソリューション

これは、レポートとトラッキングが常に同時に有効にならずに適切に機能しない場合、または、レポートとトラッキングが各 E メールセキュリティアプライアンスで常に同時に集中管理またはローカル保存されない場合に発生する可能性があります。各機能 (レポート、トラッキング) のデータは、その機能が有効になっている間だけキャプチャされます。

### 関連項目

- [メッセージトラッキングデータの有効性の検査 \(303 ページ\)](#)

## [高度なマルウェア保護判定のアップデート (Advanced Malware Protection Verdict Updates) ] レポートの結果が異なる

### 問題

Web セキュリティアプライアンスおよび E メールセキュリティアプライアンスが同じファイルを分析用に送信し、Web および電子メールの [AMP 判定のアップデート (AMP Verdict Updates) ] レポートに、そのファイルの異なる判定が表示されます。

### 解決方法

この状況は一時的です。判定アップデートがすべてダウンロードされると、結果が一致します。これには最大で 30 分かかります。

## ファイル分析レポートの詳細の表示に関する問題

- [ファイル分析レポートの詳細を使用できない \(188 ページ\)](#)
- [ファイル分析レポートの詳細を表示する際のエラー \(188 ページ\)](#)
- [ファイル分析レポートの詳細をプライベート クラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー \(188 ページ\)](#)
- [ファイル分析関連エラーのロギング \(188 ページ\)](#)

### ファイル分析レポートの詳細を使用できない

#### 問題

ファイル分析レポートの詳細を使用できません。

#### 解決方法

「[ファイル分析レポートの詳細の要件 \(95 ページ\)](#)」を参照してください。

### ファイル分析レポートの詳細を表示する際のエラー

#### 問題

ファイル分析レポートの詳細を表示しようとする、 「使用可能なクラウドサーバ構成がありません (No cloud server configuration is available) 」 エラーが表示されます。

#### ソリューション

[管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ]>[セキュリティアプライアンス (Security Appliances) ]に移動して、ファイル分析機能が有効になっている E メールセキュリティ アプライアンスを少なくとも 1 つ追加します。

### ファイル分析レポートの詳細をプライベートクラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー

#### 問題

ファイル分析レポートの詳細を表示しようとする、 API キーエラー、登録エラー、またはアクティベーションエラーが表示されます。

#### ソリューション

プライベートクラウド (オンプレミス) の Cisco AMP Threat Grid Appliance を使用している場合は、 [\(オンプレミスのファイル分析\) ファイル分析アカウントをアクティブ化する \(96 ページ\)](#) を参照してください。

Threat Grid Appliance のホスト名が変更される場合は、参照先の手順のプロセスを繰り返す必要があります。

### ファイル分析関連エラーのロギング

登録エラーおよびその他のファイル分析関連のエラーが GUI ログに記録されます。

## 不正なグレイメールメッセージまたはマーケティングメッセージの総数

### 問題

マーケティングメール、ソーシャルメール、およびバルクメールの数が、グレイメールメッセージの総数を超える。

### ソリューション

マーケティングメッセージの総数には、AsyncOS 9.5 へのアップグレードの前後に受信したマーケティングメッセージが含まれますが、グレイメールメッセージの総数にはアップグレード後に受信したメッセージだけが含まれます。「[AsyncOS 9.5 へのアップグレード後のマーケティングメッセージのレポート \(108 ページ\)](#)」を参照してください。





## 第 6 章

# 中央集中型 Web レポートイングおよびトラッキングの使用

この章は、次の項で構成されています。

- [中央集中型 Web レポートイングおよびトラッキングの概要](#) (191 ページ)
- [中央集中型 Web レポートイングおよびトラッキングの設定](#) (193 ページ)
- [Web セキュリティ レポートの使用](#) (196 ページ)
- [新しい Web インターフェイスでの Web セキュリティ レポートの使用](#) (197 ページ)
- [\[Web レポート \(Web Reporting\)\] ページの説明](#) (197 ページ)
- [新しい Web インターフェイスの Web レポート ページの概要](#) (236 ページ)
- [スケジュール設定されたレポートとオンデマンド Web レポートについて](#) (272 ページ)
- [Web レポートのスケジュール設定](#) (273 ページ)
- [オンデマンドでの Web レポートの生成](#) (277 ページ)
- [\[アーカイブ Web レポート \(Archived Web Reports\)\] ページ](#) (278 ページ)
- [アーカイブ済みの Web レポートの表示と管理](#) (278 ページ)
- [Web トラッキング](#) (279 ページ)
- [新しい Web インターフェイスでの Web トラッキング](#) (285 ページ)
- [Web トラッキングの検索結果の使用](#) (291 ページ)
- [Web レポートイングおよびトラッキングのトラブルシューティング](#) (294 ページ)

## 中央集中型 Web レポートイングおよびトラッキングの概要

Cisco コンテンツ セキュリティ管理アプライアンスは、複数の Web セキュリティ アプライアンスのセキュリティ機能から情報を収集し、Web トラフィック パターンとセキュリティ リスクのモニタに使用できるデータを記録します。リアルタイムでレポートを実行して、特定の期間のシステムアクティビティをインタラクティブに表示することも、レポートをスケジュール設定して、定期的に行うこともできます。また、レポートイング機能を使用して、raw データをファイルにエクスポートすることもできます。

中央集中型 Web レポートینگ機能を使用すると、管理者は全体的なレポートを作成してネットワークの現状を把握できるだけでなく、特定のドメイン、ユーザ、または URL カテゴリのトラフィックの詳細をドリルダウンして確認できます。

## ドメイン

ドメインについては、Web レポートینگ機能で以下のデータ要素を生成し、ドメインレポートに含めることができます。たとえば **Facebook.com** ドメインに関するレポートを作成している場合、レポートに次の情報を含めることができます。

- Facebook.com にアクセスした上位ユーザのリスト
- Facebook.com 内でアクセスされた上位 URL のリスト

## [ユーザ (User) ]

ユーザについては、Web レポートینگ機能で以下のデータ要素を生成し、ユーザレポートに含めることができます。たとえば、「**Jamie**」というタイトルのユーザレポートに次の情報を含めることができます。

- ユーザ「**Jamie**」がアクセスした上位ドメインのリスト
- マルウェアまたはウイルスが陽性であった上位 URL のリスト
- ユーザ「**Jamie**」がアクセスした上位カテゴリのリスト

## URL カテゴリ

URL カテゴリについては、カテゴリ レポートに含めるデータを Web レポートینگ機能で生成できます。たとえば、「**Sports**」というカテゴリのレポートに次の情報を含めることができます。

- 「**Sports**」カテゴリに含まれていた上位ドメインのリスト
- 「**Sports**」カテゴリにアクセスした上位ユーザのリスト

上記のどの例のレポートも、ネットワーク上の特定の項目に関する包括的なビューを提供して、管理者が対処できるようにすることを目的としています。

## 一般

ロギングページとレポートページの詳細については、[ロギングとレポート \(585 ページ\)](#) を参照してください。



- 
- (注) アクセスされた特定の URL だけでなく、ユーザが利用するすべてのドメイン情報を取得することができます。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を入手するには、[Web トラッキング (Web Tracking) ] ページの [Web プロキシ サービスによって処理されたトランザクションの検索 \(279 ページ\)](#) を使用します。
-





- (注) Web セキュリティ アプライアンスは、ローカル レポートが使用されている場合にのみデータを保存します。集約管理レポートが Web セキュリティ アプライアンスで有効な場合、Web セキュリティ アプライアンスはシステム容量とシステム ステータス データのみを保持します。中央集中型 Web レポートングがイネーブルになっていない場合、生成されるレポートはシステム キャパシティとシステム ステータスだけです。

セキュリティ管理アプライアンスで Web レポートング データを表示する方法は複数あります。


- インタラクティブ レポート ページを表示する場合は、[\[Web レポート \(Web Reporting\) \] ページの説明 \(197 ページ\)](#) を参照してください。
- レポートをオンデマンドで生成するには、[オンデマンドでの Web レポートの生成 \(277 ページ\)](#) を参照してください。
- レポートが定期的に繰り返し作成されるようにスケジュールを設定する場合は、[スケジュール設定されたレポートとオンデマンド Web レポートについて \(272 ページ\)](#) を参照してください。
- 以前に実行されたレポート (スケジュール設定されたレポートとオンデマンドで生成されたレポートの両方) のアーカイブ版を表示する方法については、[アーカイブ済みの Web レポートの表示と管理 \(278 ページ\)](#) を参照してください。
- 個々のトランザクションに関する情報を表示するには、[Web トラッキング \(279 ページ\)](#) を参照してください。

## 中央集中型 Web レポートングおよびトラッキングの設定

中央集中型 Web レポートングおよびトラッキングを設定するには、次の手順を順序どおりに実行します。

- [セキュリティ管理アプライアンスでの中央集中型 Web レポートングのイネーブル化 \(194 ページ\)](#)
  - [Web レポートでのユーザ名の匿名化 \(196 ページ\)](#)
- [Web セキュリティ アプライアンスでの中央集中型レポートングのイネーブル化 \(194 ページ\)](#)
- [管理対象の各 Web セキュリティ アプライアンスへの中央集中型 Web レポートングサービスの追加 \(195 ページ\)](#)
- [Web レポートでのユーザ名の匿名化 \(196 ページ\)](#)

## セキュリティ管理アプライアンスでの中央集中型 Web レポートングのイネーブル化

- ステップ 1** 中央集中型 Web レポートングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「[ディスク領域の管理 \(567 ページ\)](#)」を参照してください。
- ステップ 2** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 3** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [ウェブ (Web)] > [集約管理レポート (Centralized Reporting)] を選択します。
- ステップ 4** システムセットアップウィザードの実行後初めて中央集中型レポートングをイネーブルにする場合は、次の手順を実行します
- [有効化 (Enable)] をクリックします。
  - エンドユーザ ライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 5** 以前に中央集中型レポートングをディセーブルにし、その後イネーブルにする場合は、次の手順を実行します。
- [設定の編集 (Edit Settings)] をクリックします。
  - [中央集中型 Web レポートングサービスを有効にする (Enable Centralized Web Report Services)] チェックボックスを選択します。
  - [Web レポートでのユーザ名の匿名化 \(196 ページ\)](#) はここで実行することも、後で実行することもできます。
- ステップ 6** 変更を送信し、保存します。

## Webセキュリティアプライアンスでの中央集中型レポートングのイネーブル化


中央集中型レポートングを有効にする前に、すべての Web セキュリティ アプライアンスが設定され、想定どおりに動作している必要があります。

中央集中型レポートングは、それを使用する各 Web セキュリティ アプライアンスごとに有効にする必要があります。

『AsyncOS for Cisco Web Security Appliances User Guide』の「Enabling Centralized Reporting」セクションを参照してください。

## 管理対象の各 Web セキュリティ アプライアンスへの中央集中型 Web レポートング サービスの追加

他の中央集中型管理機能を設定する際、すでにアプライアンスを追加したかどうかによって、ここでの手順は異なります。


- 
- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] を選択します。
- ステップ 3** リストに、すでに Web セキュリティ アプライアンスを追加している場合は、次の手順を実行します。
- Web Security Appliances の名前をクリックします。
  - [集約管理レポート (Centralized Reporting) ] サービスを選択します。
- ステップ 4** Web セキュリティ アプライアンスをまだ追加していない場合は、次の手順を実行します。
- [Webアプライアンスの追加 (Add Web Appliance) ] をクリックします。
  - [アプライアンス名 (Appliance Name) ] および [IP アドレス (IP Address) ] テキスト フィールドに、Web セキュリティアプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。  
(注) [IP アドレス (IP Address) ] フィールドに DNS 名を入力した場合でも、[送信 (Submit) ] をクリックすると、IP アドレスに変換されます。
  - [集約管理レポート (Centralized Reporting) ] サービスがすでに選択されています。
  - [接続の確立 (Establish Connection) ] をクリックします。
  - 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection) ] をクリックします。  
(注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。
  - 「Success」メッセージがページのテーブルの上に表示されるまで待機します。
  - [テスト接続 (Test Connection) ] をクリックします。
  - テーブルの上のテスト結果を確認します。
- ステップ 5** [送信 (Submit) ] をクリックします。
- ステップ 6** 中央集中型レポートングをイネーブルにする各 Web Security Appliances に対してこの手順を繰り返します。
- ステップ 7** 変更を保存します。
-

## Web レポートでのユーザ名の匿名化

デフォルトでは、レポートページと PDF にユーザ名が表示されます。ただし、ユーザのプライバシーを保護するために、Web レポートでユーザ名を識別できないようにすることができます。



(注) このアプライアンスの管理者権限を持つユーザは、インタラクティブレポートを表示する際、常にユーザ名を表示できます。

- ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [ウェブ (Web)] > [集約管理レポート (Centralized Reporting)] を選択します。
- ステップ 3** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 4** [レポートでユーザ名を匿名にする (Anonymize usernames in reports)] チェックボックスをオンにします。
- ステップ 5** 変更を送信し、保存します。

## Web セキュリティ レポートの使用

Web レポートページでは、システム内の 1 つまたはすべての管理対象 Web セキュリティアプライアンスに関する情報をモニタできます。

目的	参照先
レポートデータのアクセスおよび表示オプションを確認する	<a href="#">レポートデータの表示方法 (23 ページ)</a>
インタラクティブ レポート ページのビューをカスタマイズする	<a href="#">レポートデータのビューのカスタマイズ (25 ページ)</a>
データ内の特定のトランザクションに関する情報を検索する	<a href="#">Web トラッキング (279 ページ)</a>
レポート情報を印刷またはエクスポートする	<a href="#">レポートデータおよびトラッキングデータのエクスポート (33 ページ)</a>
さまざまなインタラクティブ レポート ページについて理解する	<a href="#">[Web レポート (Web Reporting)] ページの説明 (197 ページ)</a>
レポートをオンデマンドで生成する	<a href="#">新しい Web インターフェイスの Web レポート ページの概要 (236 ページ)</a>

目的	参照先
レポートが指定した間隔で所定の時刻に自動的に実行されるようスケジュールを設定する	<a href="#">スケジュール設定されたレポートとオンデマンド Web レポートについて (272 ページ)</a>
アーカイブ済みのオンデマンドレポートとスケジュールされたレポートを表示する	<a href="#">アーカイブ済みの Web レポートの表示と管理 (278 ページ)</a>
データの収集方法を理解する	<a href="#">セキュリティ管理アプライアンスによるレポート用データの収集方法 (24 ページ)</a>

## 新しい Web インターフェイスでの Web セキュリティ レポートの使用

Web レポーティング ページでは、システム内の 1 つまたはすべての管理対象 Web セキュリティ アプライアンスに関する情報をモニタできます。

目的	参照先
レポートデータのアクセスおよび表示オプションを確認する	<a href="#">レポートデータの表示方法 (39 ページ)</a>
インタラクティブレポートページのビューをカスタマイズする	<a href="#">レポートデータのビューのカスタマイズ (42 ページ)</a>
データ内の特定のトランザクションに関する情報を検索する	<a href="#">新しい Web インターフェイスでの Web トラッキング (285 ページ)</a>
レポート情報を印刷またはエクスポートする	<a href="#">レポーティングデータおよびトラッキングデータのエクスポート (33 ページ)</a>
さまざまなインタラクティブレポート ページについて理解する	<a href="#">新しい Web インターフェイスの Web レポート ページの概要 (236 ページ)</a>

## [Web レポート (Web Reporting)] ページの説明



- (注) [Webレポート (Web Reporting)] タブのどのオプションをオンデマンドまたはスケジュール済みレポートとして使用できるかについては、[スケジュール設定されたレポートとオンデマンド Web レポートについて \(272 ページ\)](#) を参照してください。

表 39: [Web レポート (Web Reporting) ] タブの詳細

[Web レポート (Web Reporting) ] メニュー	操作
Web レポートの概要 (202 ページ)	<p>[概要 (Overview) ] ページには、お使いの Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリーテーブルも含まれます。詳細については、<a href="#">Web レポートの概要 (202 ページ)</a> を参照してください。</p>
[ユーザ (Users) ] レポート (Web) (204 ページ)	<p>[ユーザ (Users) ] ページには複数の Web トラッキングリンクが表示され、各ユーザの Web トラッキング情報を確認できます。</p> <p>[ユーザ (Users) ] ページでは、システム上のユーザ (1 人または複数) がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。</p> <p>[ユーザ (Users) ] ページのインタラクティブな [ユーザ (Users) ] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [ユーザの詳細 (User Details) ] ページに表示されます。</p> <p>[ユーザの詳細 (User Details) ] ページでは、[ウェブ (Web) ] &gt; [レポート (Reporting) ] &gt; [ユーザ (Users) ] ページのインタラクティブな [ユーザ (Users) ] テーブルで指定したユーザについて具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザレベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。</p> <p>詳細については、<a href="#">[ユーザ (Users) ] レポート (Web) (204 ページ)</a> を参照してください。システムにおける各ユーザの情報については、<a href="#">[ユーザの詳細 (User Details) ] (Web レポートリング) (206 ページ)</a> を参照してください。</p>
[ユーザ数レポート (User Count Report) ] (Web)	<p>[ユーザ数 (User Count) ] ページは、中央集中型レポートリングが有効な Web セキュリティ アプライアンスの認証されたユーザと認証されていないユーザの合計数に関する集約情報を提供します。このページには、直近の過去 30 日間、90 日間、および 180 日間のユニーク ユーザ数が表示されます。</p> <p>(注) システムは、1 時間ごとに、認証されたユーザと認証されていないユーザの合計ユーザ数を計算します。</p>

[Web レポート (Web Reporting) ] メニュー	操作
[Web サイト (Web Sites) ] レポート (208 ページ)	<p>[Web サイト (Web Sites) ] ページでは、管理対象アプライアンスで発生しているアクティビティ全体を集約して表示できます。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。詳細については、<a href="#">[Web サイト (Web Sites) ] レポート (208 ページ)</a> を参照してください。</p>
[URL カテゴリ (URL Categories) ] レポート (209 ページ)	<p>[URL カテゴリ (URL Categories) ] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。</p> <ul style="list-style-type: none"> <li>• トランザクションごとに発生するブロックアクションまたは警告アクションをトリガーした上位 URL。</li> <li>• 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブな列見出しのあるインタラクティブテーブルとなっていて、必要に応じてデータをソートできます。</li> </ul> <p>詳細については、<a href="#">[URL カテゴリ (URL Categories) ] レポート (209 ページ)</a> を参照してください。</p>
[アプリケーションの表示 (Application Visibility) ] レポート (212 ページ)	<p>[アプリケーションの表示 (Application Visibility) ] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティアプライアンス内で特定のアプリケーションタイプに適用されているコントロールを適用し、表示できます。詳細については、<a href="#">[アプリケーションの表示 (Application Visibility) ] レポート (212 ページ)</a> を参照してください。</p>
[マルウェア対策 (Anti-Malware) ] レポート (214 ページ)	<p>[マルウェア対策 (Anti-Malware) ] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェアポートとマルウェアサイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、<a href="#">[マルウェア対策 (Anti-Malware) ] レポート (214 ページ)</a> を参照してください。</p>

[Web レポート (Web Reporting) ] メニュー	操作
[高度なマルウェア防御 (ファイルレピュテーション) (Advanced Malware Protection (File Reputation)) ] および [高度なマルウェア防御 (ファイル分析) (Advanced Malware Protection (File Analysis)) ] レポート ( 218 ページ)	<p>ファイルレピュテーションおよび分析データは3つのレポートリング ページに表示されます。</p> <p>詳細については、<a href="#">[高度なマルウェア防御 (ファイルレピュテーション) (Advanced Malware Protection (File Reputation)) ]</a> および <a href="#">[高度なマルウェア防御 (ファイル分析) (Advanced Malware Protection (File Analysis)) ]</a> レポート (218 ページ) を参照してください。</p>
[クライアント マルウェア リスク (Client Malware Risk) ] レポート (224 ページ)	<p><a href="#">[クライアントマルウェアリスク (Client Malware Risk) ]</a> ページは、セキュリティ関連のレポートリングページです。このページを使用して、著しく頻繁にマルウェアサイトに接続している可能性がある個々のクライアント コンピュータを特定できます。</p> <p>詳細については、<a href="#">[クライアントマルウェアリスク (Client Malware Risk) ]</a> レポート (224 ページ) を参照してください。</p>
[Web レピュテーション フィルタ (Web Reputation Filters) ] レポート (226 ページ)	<p>指定した時間範囲内のトランザクションに対する、Web レピュテーションフィルタリングに関するレポートを表示できます。詳細については、<a href="#">[Web レピュテーションフィルタ (Web Reputation Filters) ]</a> レポート (226 ページ) を参照してください。</p>
[L4 トラフィック モニタ (L4 Traffic Monitor) ] レポート (228 ページ)	<p>指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、<a href="#">[L4 トラフィック モニタ (L4 Traffic Monitor) ]</a> レポート (228 ページ) を参照してください。</p>
[SOCKS プロキシ (SOCKS Proxy) ] レポート (231 ページ)	<p>宛先、ユーザなど、SOCKS プロキシ トランザクションのデータを表示できます。</p> <p>詳細については、<a href="#">[SOCKS プロキシ (SOCKS Proxy) ]</a> レポート (231 ページ) を参照してください。</p>
ユーザの場所別レポート (Reports by User Location) (232 ページ)	<p><a href="#">[ユーザの場所別のレポート (Reports by User Location) ]</a> ページでは、モバイルユーザがローカル システムまたはリモート システムから実行しているアクティビティを確認できます。</p> <p>詳細については、<a href="#">ユーザの場所別レポート (Reports by User Location) (232 ページ)</a> を参照してください。</p>



[Web レポート (Web Reporting) ] メニュー	操作
Web トラッキング (279 ページ)	<p>[Web トラッキング (Web Tracking) ] ページでは、次のタイプの情報を検索できます。</p> <ul style="list-style-type: none"> <li>• <a href="#">Web プロキシサービスによって処理されたトランザクションの検索 (279 ページ)</a> では、基本的な Web 関連情報 (アプライアンスで処理されている Web トラフィックのタイプなど) を追跡して表示することができます。</li> </ul> <p>これには、時間範囲、ユーザ ID、クライアント IP アドレスなどの情報が含まれるほか、特定のタイプの URL、各接続が占有している帯域幅の量、特定のユーザの Web 使用状況のトラッキングなどの情報も含まれます。</p> <ul style="list-style-type: none"> <li>• <a href="#">L4 トラフィック モニタによって処理されたトランザクションの検索 (284 ページ)</a> では、マルウェアの転送アクティビティに関与しているサイト、ポート、およびクライアント IP アドレスの L4TM データを検索できます。</li> <li>• <a href="#">SOCKS プロキシによって処理されるトランザクションの検索 (285 ページ)</a> では、SOCKS プロキシによって処理されたトランザクションを検索できます。</li> </ul> <p>詳細については、<a href="#">Web トラッキング (279 ページ)</a> を参照してください。</p>
[システム容量 (System Capacity) ] ページ (233 ページ)	<p>レポートングデータをセキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。</p> <p>詳細については、<a href="#">[システム容量 (System Capacity) ] ページ (233 ページ)</a> を参照してください。</p>
[使用可能なデータ (Data Availability) ] ページ (235 ページ)	<p>各アプライアンスのセキュリティ管理アプライアンス上のレポートングデータの影響を把握できます。詳細については、<a href="#">[使用可能なデータ (Data Availability) ] ページ (235 ページ)</a> を参照してください。</p>
[スケジュール設定されたレポート (Scheduled Reports) ]	<p>指定した時間範囲のレポートのスケジュールを設定できます。詳細については、<a href="#">スケジュール設定されたレポートとオンデマンド Web レポートについて (272 ページ)</a> を参照してください。</p>
[アーカイブレポート (Archived Reports) ]	<p>指定した時間範囲のレポートをアーカイブできます。詳細については、<a href="#">アーカイブ済みの Web レポートの表示と管理 (278 ページ)</a> を参照してください。</p>



- (注) ほとんどの Web レポートングカテゴリでレポートをスケジュール設定できます。これには、拡張された上位 URL カテゴリおよび上位アプリケーションタイプに関する追加のレポートが含まれます。レポートのスケジュール設定の詳細については、[スケジュール設定されたレポートとオンデマンド Web レポートについて \(272 ページ\)](#) を参照してください。

## [ 滞留時間 (Time Spent) ] について

さまざまなテーブルの [ 滞留時間 (Time Spent) ] 列は、Web ページでユーザが費やした時間を表します。各 URL カテゴリでユーザが費やした時間。ユーザを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。

トランザクションイベントに「viewed」のタグが付けられる（ユーザが特定の URL に進む）と、[ 滞留時間 (Time Spent) ] の値の計算が開始され、Web レポートングテーブルのフィールドとして追加されます。

費やされた時間を計算するため、AsyncOS はアクティブ ユーザごとに、1 分間のアクティビティに対して 60 秒という時間を割り当てます。この 1 分間の終わりに、各ユーザが費やした時間は、そのユーザが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザは各ドメインで 15 分ずつ費やしたと見なされます。

経過時間の値に関して、以下の注意事項を考慮してください。

- アクティブ ユーザは、アプライアンスを介して HTTP トラフィックを送信し、Web サイトにアクセスした、すなわち AsyncOS が「ページビュー」と見なす動作を行ったユーザ名または IP アドレスとして定義されています。
- AsyncOS では、クライアントアプリケーションが開始する要求とは逆に、ユーザが開始する HTTP 要求としてページビューを定義します。AsyncOS はヒューリスティックアルゴリズムを使用して、可能な限り効果的にユーザ ページビューを識別します。

単位は時間：分形式で表示されます。

## Web レポートの概要

[ ウェブ (Web) ] > [ レポート (Reporting) ] > [ 概要 (Overview) ] ページでは、お使いの Web セキュリティアプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリーテーブルも含まれます。

[ 概要 (Overview) ] ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシアクティビティ、および各種トランザクションサマリーが表示されます。トランザクションサマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしいトランザクションと、そのグラフの隣にそれらのトランザクションがブロックされた数、およびブロックされた方法が表示されます。

[概要 (Overview)] ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位アプリケーションタイプおよびカテゴリ、これらのブロックまたは警告を生成している上位ユーザが表示されます。

表 40: [ウェブ (Web)] > [レポート (Reporting)] > [概要 (Overview)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[次のデータを参照 (View Data for)]	概要データを表示する Web セキュリティ アプライアンスを選択するか、[すべての Web アプライアンス (All Web Appliances)] を選択します。 <a href="#">アプライアンスまたはレポート グループのレポート データの表示 (26 ページ)</a> も参照してください。
[Web プロキシアクティビティ総数 (Total Web Proxy Activity)]	このセクションでは、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される Web プロキシアクティビティを表示できます。  このセクションには、トランザクションの実際の数 (縦の目盛り)、およびアクティビティが発生したおよその日付 (横の時間軸) が表示されます。
[Web プロキシの概要 (Web Proxy Summary)]	このセクションでは、疑わしい Web プロキシアクティビティまたは正常なプロキシアクティビティの比率を、トランザクションの総数も含めて表示できます。
[L4 トラフィックモニタの概要 (L4 Traffic Monitor Summary)]	このセクションでは、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される L4 トラフィックを報告します。
[疑わしいトランザクション (Suspect Transactions)]	このセクションでは、管理者が疑わしいトランザクションと分類した Web トランザクションを表示できます。  このセクションには、トランザクションの実際の数 (縦の目盛り)、およびアクティビティが発生したおよその日付 (横の時間軸) が表示されます。
[疑わしいトランザクションの概要 (Suspect Transactions Summary)]	このセクションでは、ブロックまたは警告された疑わしいトランザクションの比率を表示できます。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。

## [ ユーザ (Users) ] レポート (Web)

セクション	説明
[総トランザクション数の上位URLカテゴリ (Top URL Categories by Total Transactions) ]	このセクションには、ブロックされている上位 10 の URL カテゴリが表示されます。URL カテゴリのタイプ (縦の目盛り)、特定タイプのカテゴリが実際にブロックされた回数 (横の目盛り) などがあります。  すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、 <a href="#">URL カテゴリ セットの更新とレポート (211 ページ)</a> を参照してください。
[総トランザクション数の上位アプリケーションタイプ (Top Application Types by Total Transactions) ]	このセクションには、ブロックされている上位アプリケーションタイプが表示されます。これには、実際のアプリケーションタイプ名 (縦の目盛り)、特定のアプリケーションがブロックされた回数 (横の目盛り) が含まれます。
[検出された上位マルウェアカテゴリ (Top Malware Categories Detected) ]	このセクションには、検出されたすべてのマルウェアカテゴリが表示されます。
[ブロックまたは警告されたトランザクション数の上位ユーザ (Top Users Blocked or Warned Transactions) ]	このセクションには、ブロックされたトランザクションまたは警告が発行されたトランザクションを生成している実際のユーザが表示されます。ユーザは IP アドレスまたはユーザ名で表示できます。ユーザ名を識別できないようにするには、 <a href="#">Web レポートでのユーザ名の匿名化 (196 ページ)</a> を参照してください。
Web トラフィック タップ ステータス	タップされていないトラフィック トランザクションおよびタップされたトラフィック トランザクションがグラフ形式で表示されます。
Web トラフィック タップ サマリ	タップされたトラフィック トランザクションおよびタップされていないトラフィック トランザクションの概要が、トラフィック トランザクションの合計とともに表示されます。
タップされた HTTP/HTTPS トラフィック	タップされた HTTP および HTTPS トラフィック トランザクションがグラフ形式で表示されます。
タップされたトラフィック サマリ	HTTP および HTTPS トラフィック トランザクションの概要が、HTTP および HTTPS トラフィック トランザクションの合計とともに表示されます。

## [ ユーザ (Users) ] レポート (Web)

[ウェブ (Web) ] > [レポート (Reporting) ] > [ユーザ (Users) ] ページには、各ユーザの Web レポートリング情報を表示できる複数のリンクが表示されます。

[ユーザ (Users) ] ページでは、システム上のユーザ (1 人または複数) がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。

[ユーザ (Users) ] ページには、システム上のユーザに関する次の情報が表示されます。

表 41: [ウェブ (Web) ] &gt; [レポート (Reporting) ] &gt; [ユーザ (Users) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[ブロックされたトランザクション数の上位ユーザ (Top Users by Transactions Blocked) ]	このセクションには、IP アドレスまたはユーザ名で示された上位ユーザ (縦の目盛り)、そのユーザがブロックされたトランザクションの数 (横の目盛り) が表示されます。レポートを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページまたはスケジュール設定されたレポートでユーザ名を認識不可能にする方法の詳細については、 <a href="#">セキュリティ管理アプライアンスでの中央集中型 Web レポートのイネーブル化 (194 ページ)</a> を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。ユーザ名を非表示にするには、 <a href="#">Web レポートでのユーザ名の匿名化 (196 ページ)</a> を参照してください。
[帯域幅使用量の上位ユーザ (Top Users by Bandwidth Used) ]	このセクションには、システム上で最も帯域幅 (ギガバイト単位の使用量を示す横の目盛り) を使用している上位ユーザが、IP アドレスまたはユーザ名 (縦の目盛り) で表示されます。
[ユーザテーブル (Users Table) ]	<p>特定のユーザ ID またはクライアント IP アドレスを検索できます。[ユーザ (User) ] セクション下部のテキスト フィールドに特定のユーザ ID またはクライアント IP アドレスを入力し、[ユーザ ID またはクライアント IP アドレスの検索 (Find User ID or Client IP address) ] をクリックします。IP アドレスが正確に一致していなくても結果は返されます。</p> <p>[ユーザテーブル (Users Table) ] では、特定のユーザをクリックして、さらに具体的な情報を得ることができます。この情報は、[ユーザの詳細 (User Details) ] ページに表示されます。[ユーザの詳細 (User Details) ] ページの詳細については、<a href="#">ユーザの詳細 (User Details) ] (Web レポート) (206 ページ)</a> を参照してください。</p>



(注) クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。詳細は、[LDAP との統合 \(433 ページ\)](#) の章の [LDAP サーバプロファイルの作成 \(434 ページ\)](#) を参照してください。



ヒント このレポートのビューをカスタマイズするには、[Web セキュリティレポートの使用 \(196 ページ\)](#) を参照してください。

[ユーザ (Users) ] ページの使用例については、[例 1 : ユーザの調査 \(649 ページ\)](#) を参照してください。



- (注) [ユーザ (Users)] ページについて、レポートを生成またはスケジュールすることができます。詳細については、[スケジュール設定されたレポートとオンデマンド Web レポートについて \(272 ページ\)](#) を参照してください。

## [ユーザの詳細 (User Details)] (Web レポートिंग)

[ユーザの詳細 (User Details)] ページでは、[ウェブ (Web)] > [レポート (Reporting)] > [ユーザ (Users)] ページのインタラクティブな [ユーザ (Users)] テーブルで指定したユーザに関する具体的な情報を確認できます。

[ユーザの詳細 (User Details)] ページでは、システムでの個々のユーザのアクティビティを調査できます。特に、ユーザレベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。

特定のユーザの [ユーザの詳細 (User Details)] ページを表示するには、[ウェブ (Web)] > [ユーザ (Users)] ページの [ユーザ (User)] テーブルでそのユーザをクリックします。

[ユーザの詳細 (User Details)] ページには、システム上の個々のユーザに関する次の情報が表示されます。

表 42: [ウェブ (Web)] > [レポート (Reporting)] > [ユーザの詳細 (User Details)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	レポートに含めるデータの時間範囲を選択できるメニュー。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[総トランザクション数別の URL カテゴリ (URL Categories by Total Transactions)]	このセクションには、特定のユーザが使用している特定の URL カテゴリのリストが表示されます。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、 <a href="#">URL カテゴリ セットの更新とレポート (211 ページ)</a> を参照してください。
[総トランザクション数別のトレンド (Trend by Total Transactions)]	このグラフには、ユーザが Web にいつアクセスしたかが表示されます。 たとえば、1 日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。 [時間範囲 (Time Range)] ドロップダウンリストを使用すると、このグラフを拡張し、このユーザが Web を閲覧していた時間を表示するきめ細かさを増減できます。

セクション	説明
[一致したURLカテゴリ (URL Categories Matched)]	<p>[一致したURLカテゴリ (URL Categories Matched)] セクションには、完了したトランザクションとブロックされたトランザクションの両方について、一致したカテゴリが表示されます。</p> <p>このセクションでは、特定の URL カテゴリを検索することもできます。セクション下部のテキストフィールドに URL カテゴリを入力し、[URLカテゴリの検索 (Find URL Category)] をクリックします。カテゴリは正確に一致している必要はありません。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URL カテゴリ セットの更新とレポート (211 ページ)</a> を参照してください。</p>
[一致したドメイン (Domains Matched)]	<p>このセクションでは、このユーザがアクセスした特定のドメインまたは IP アドレスを確認できます。また、ユーザがこれらのカテゴリで費やした時間、およびレビューで設定したその他のさまざまな情報も参照できます。セクション下部のテキストフィールドにドメインまたは IP アドレスを入力し、[ドメインまたはIPの検索 (Find Domain or IP)] をクリックします。ドメインまたは IP アドレスは正確に一致している必要はありません。</p>
[一致したアプリケーション (Applications Matched)]	<p>このセクションでは、特定のユーザが使用している特定のアプリケーションを検索できます。たとえば、Flash ビデオを多用するサイトにユーザがアクセスしている場合は、[アプリケーション (Application)] 列にそのアプリケーションタイプが表示されます。</p> <p>セクション下部のテキストフィールドにアプリケーション名を入力し、[アプリケーションの検索 (Find Application)] をクリックします。アプリケーションの名前は正確に一致している必要はありません。</p>
[検出されたマルウェア脅威 (Malware Threats Detected)]	<p>このテーブルでは、特定のユーザがトリガーしている上位のマルウェア脅威を確認できます。</p> <p>特定のマルウェア脅威の名前に関するデータを [マルウェア脅威の検索 (Find Malware Threat)] フィールドで検索できます。マルウェア脅威の名前を入力し、[マルウェア脅威の検索 (Find Malware Threat)] をクリックしてください。マルウェア脅威の名前は正確に一致している必要はありません。</p>
[一致したポリシー (Policies Matched)]	<p>このセクションでは、Web にアクセスする際にこのユーザに適用されるポリシー グループを検索できます。</p> <p>セクション下部のテキストフィールドにポリシー名を入力し、[ポリシーの検索 (Find Policy)] をクリックします。ポリシーの名前は正確に一致している必要はありません。</p>



- (注) [クライアントマルウェアリスクの詳細 (Client Malware Risk Details)] テーブルのクライアントレポートでは、ユーザ名の末尾にアスタリスク (\*) が付いていることがあります。たとえば、クライアントレポートに「jsmith」と「jsmith\*」の両方のエントリが表示される場合があります。アスタリスク (\*) が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

[ユーザの詳細 (Users Details)] ページの使用例については、[例 1 : ユーザの調査 \(649 ページ\)](#) を参照してください。

## [ ユーザ数レポート (User Count Report) ] (Web)

[Web] > [レポート (Reporting)] > [ユーザ数 (User Count)] ページには、中央集中型レポートिंगが有効な Web セキュリティ アプライアンスの認証されたユーザと認証されていないユーザの合計数に関する集約情報が表示されます。このページには、直近の過去 30 日間、90 日間、および 180 日間のユニーク ユーザ数が表示されます。



- (注) システムは、1 時間ごとに、認証されたユーザと認証されていないユーザの合計ユーザ数を計算します。

## [ Web サイト (Web Sites) ] レポート

[ウェブ (Web)] > [レポート (Reporting)] > [Web サイト (Web Sites)] ページでは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。

[Web サイト (Web Sites)] ページには次の情報が表示されます。

表 43: [ウェブ (Web)] > [レポート (Reporting)] > [Web サイト (Web Sites)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[総トランザクション数の上位ドメイン (Top Domains by Total Transactions)]	このセクションには、サイト上でアクセスされた上位ドメインがグラフ形式で表示されます。



セクション	説明
[ブロックされたトランザクション数の上位ドメイン (Top Domains by Transactions Blocked) ]	このセクションには、トランザクションごとに発生するブロック アクションをトリガーした上位ドメインが、グラフ形式で表示されます。たとえば、ユーザがあるドメインにアクセスしたが、特定のポリシーが適用されていたために、ブロック アクションがトリガーされたとします。このドメインはブロックされたトランザクションとしてこのグラフに追加され、ブロック アクションをトリガーしたドメイン サイトが表示されます。
[一致したドメイン (Domains Matched) ]	<p>このセクションでは、サイト上でアクセスされたドメインがインタラクティブなテーブルに表示されます。このテーブルでは、特定のドメインをクリックすることで、そのドメインに関するさらに詳細な情報にアクセスできます。[Webトラッキング (Web Tracking) ] ページに [プロキシサービス (Proxy Services) ] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。</p> <p>特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。</p> <p>Web トラッキングの使用例については、<a href="#">例 2 : URL のトラッキング (651 ページ)</a> を参照してください。</p> <p>(注) このデータを .csv ファイルにエクスポートすると、最初の 300,000 エントリのみがエクスポートされます。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196 ページ\)](#) を参照してください。



(注) [Webサイト (Web Sites) ] ページの情報について、レポートを生成またはスケジュールすることができます。詳細については、[スケジュール設定されたレポートとオンデマンド Web レポートについて \(272 ページ\)](#) を参照してください。

## [URLカテゴリ (URL Categories) ] レポート

[Web]>[レポート (Reporting) ]>[URL カテゴリ (URL Categories) ] ページを使用して、システム上のユーザがアクセスしているサイトの URL カテゴリを表示できます。

[URL カテゴリ (URL Categories) ] ページには次の情報が表示されます。

表 44: [ウェブ (Web)] &gt; [レポート (Reporting)] &gt; [URL カテゴリ (URL Categories)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[総トランザクション数の上位URLカテゴリ (Top URL Categories by Total Transactions)]	このセクションには、サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。
[ブロックまたは警告されたトランザクション数別の上位URLカテゴリ (Top URL Categories by Blocked and Warned Transactions)]	このセクションには、トランザクションごとに発生するブロックアクションまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロックアクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
[一致したURLカテゴリ (URL Categories Matched)]	[一致したURLカテゴリ (URL Categories Matched)] セクションには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。  未分類の URL が多数ある場合は、 <a href="#">未分類の URL の削減 (210 ページ)</a> を参照してください。
[URLフィルタリングのバイパス (URL Filtering Bypassed)]	URL フィルタリングの前に実行されるポリシー、ポートおよび管理ユーザエージェントのブロックングを示します。



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196 ページ\)](#) を参照してください。



(注) このページよりもさらに詳細なレポートを生成するには、[上位URLカテゴリ - 拡張 \(Top URL Categories — Extended\) \(275 ページ\)](#) を参照してください。

- URL カテゴリに関するスケジュール設定されたレポートでデータアベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「この時間範囲の一部のデータは使用不可でした。(Some data in this time range was unavailable.)」というメッセージが表示されます。ギャップが存在しない場合は何も表示されません。

## 未分類の URL の削減

未分類の URL の比率が 15 ~ 20 % を上回る場合は、次のオプションを検討してください。

- 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。これらのトランザクションは、代わりに[URL フィルタリングバイパス (URL Filtering Bypassed) ]統計情報に含まれるようになります。これを行うには、『AsyncOS for Cisco Web Security Appliances User Guide』でカスタム URL カテゴリについて参照してください。
- 既存またはその他のカテゴリに含めるべきサイトについては、[誤って分類された URL と未分類の URL のレポート \(212 ページ\)](#) を参照してください。

## URL カテゴリ セットの更新とレポート

[URL カテゴリ セットの更新の準備および管理 \(421 ページ\)](#) で説明されているように、セキュリティ管理アプライアンスでは一連の定義済み URL カテゴリが定期的に更新される場合があります。

これらの更新が行われた場合、古いカテゴリのデータは、古すぎて価値がなくなるまで、引き続きレポートと Web トラッキング結果に表示されます。カテゴリ セットの更新後に生成されたレポートデータには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

古いカテゴリと新しいカテゴリの間に重複した箇所がある場合、有効な統計情報を得るために、より注意深くレポート結果を検証する必要があることがあります。たとえば、調査対象のタイム フレーム内に「Instant Messaging」カテゴリと「Web-based Chat」カテゴリが「Chat and Instant Messaging」という 1 つのカテゴリにマージされていた場合、「Instant Messaging」および「Web-based Chat」カテゴリに対応するサイトへのマージ前のアクセスは「Chat and Instant Messaging」の合計数にカウントされません。同様に、インスタントメッセージング サイトまたは Web ベースチャットサイトへのマージ後のアクセスは、「Instant Messaging」または「Web-based Chat」カテゴリの合計数には含まれません。

## [URL カテゴリ (URL Categories) ] ページとその他のレポート ページの併用

[URL カテゴリ (URL Categories) ] ページと [\[アプリケーションの表示 \(Application Visibility\) \] ページ \(242 ページ\)](#) および [\[ユーザ \(Users\) \] ページ \(252 ページ\)](#) を併用すると、特定のユーザと、特定のユーザがアクセスしようとしているアプリケーション タイプまたは Web サイトを調査できます。

たとえば、[\[URL カテゴリ \(URL Categories\) \] ページ \(249 ページ\)](#) で、サイトからアクセスされたすべての URL カテゴリの詳細を表示する、人事部門向けの概要レポートを生成できます。同じページの [\[URL カテゴリ \(URL Categories\) \] インタラクティブ テーブル](#) では、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[ストリーミングメディア (Streaming Media) ] カテゴリ リンクをクリックすると、特定の [\[URL カテゴリ \(URL Categories\) \] レポート ページ](#) が表示されます。このページには、ストリーミング メディア サイトにアクセスしている上位ユーザが表示されるだけでなく ([カテゴリ別の総トランザクション上位ユーザ (Top Users by Category for Total Transactions) ] セクション)、YouTube.com や QuickPlay.com などのアクセスされたドメインも表示されます ([一致したドメイン (Domains Matched) ] インタラクティブ テーブル)。

## 誤って分類された URL と未分類の URL のレポート

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているため、そのユーザのアクセス先を正確に確認する必要があります。ここから、[ユーザ (Users)] インタラクティブ テーブルのユーザをクリックすることができます。このアクションにより [ユーザ (Users)] ページ (252 ページ) が表示され、そのユーザのトレンドを確認し、そのユーザの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [完了したトランザクション (Transactions Completed)] リンクをクリックして、Web トラッキングの詳細を表示できます。これにより、[Web トラッキング (Web Tracking)] ページに [Web プロキシサービスによって処理されたトランザクションの検索 \(279 ページ\)](#) が表示され、ユーザがサイトにアクセスした日付、完全な URL、その URL で費やされた時間などについて、実際の詳細情報を確認できます。

[URL カテゴリ (URL Categories)] ページの他の使用例については、[例 3 : アクセス数の多い URL カテゴリの調査 \(652 ページ\)](#) を参照してください。

## 誤って分類された URL と未分類の URL のレポート

誤って分類された URL と未分類の URL について、次の URL で報告できます。

[https://securityhub.cisco.com/web/submit\\_urls](https://securityhub.cisco.com/web/submit_urls)

送信内容は評価され、今後のルール更新への組み込みに活用されます。

送信された URL のステータスを確認するには、このページの [送信した URL のステータス (Status on Submitted URLs)] タブをクリックします。

## [アプリケーションの表示 (Application Visibility)] レポート



(注) [アプリケーションの表示 (Application Visibility)] の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding Application Visibility and Control」の章を参照してください。

[ウェブ (Web)] > [レポート (Reporting)] > [アプリケーションの可視性 (Application Visibility)] ページでは、セキュリティ管理アプライアンスと Web セキュリティ アプライアンス内の特定のアプリケーションタイプに制御を適用することができます。

アプリケーション制御を使用すると、URL フィルタリングのみを使用する場合よりも Web トラフィックをきめ細かく制御できるだけでなく、次のタイプのアプリケーションおよびアプリケーションタイプの制御を強化できます。

- 回避アプリケーション (アノニマイザや暗号化トンネルなど)。
- コラボレーションアプリケーション (Cisco Webex、Facebook、インスタントメッセージングなど)。
- リソースを大量消費するアプリケーション (ストリーミングメディアなど)。

## アプリケーションとアプリケーションタイプの違いについて

レポートに関連するアプリケーションを制御するには、アプリケーションとアプリケーションタイプの違いを理解することが非常に重要です。

- **アプリケーションタイプ**。1つまたは複数のアプリケーションを含むカテゴリです。たとえば**検索エンジン**は、Google Search や Craigslist などの検索エンジンを含むアプリケーションタイプです。インスタントメッセージングは、Yahoo Instant Messenger や Cisco Webex などを含む別のアプリケーションタイプです。Facebook もアプリケーションタイプです。
- **アプリケーション**。アプリケーションタイプに属している特定のアプリケーションです。たとえば、YouTube はメディア アプリケーションタイプに含まれるアプリケーションです。
- **アプリケーション動作**。アプリケーション内でユーザが実行できる特定のアクションまたは動作です。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション動作が含まれているわけではありません。



- (注) Application Visibility and Control (AVC) エンジンを使用して Facebook アクティビティを制御する方法の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding Application Visibility and Control」の章を参照してください。

[アプリケーションの表示 (Application Visibility)] ページには次の情報が表示されます。

表 45: [ウェブ (Web)] > [レポート (Reporting)] > [アプリケーションの表示 (Application Visibility)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[総トランザクション数の上位アプリケーションタイプ (Top Application Types by Total Transactions)]	このセクションには、サイト上でアクセスされた上位アプリケーションタイプがグラフ形式で表示されます。たとえば、Yahoo Instant Messenger などのインスタントメッセージングツール、Facebook、Presentation というアプリケーションタイプが表示されます。
[ブロックされたトランザクション数の上位アプリケーション (Top Applications by Blocked Transactions)]	このセクションには、トランザクションごとに発生するブロックアクションをトリガーした上位アプリケーションタイプがグラフ形式で表示されます。たとえば、ユーザが Google Talk や Yahoo Instant Messenger などの特定のアプリケーションタイプを起動しようとしたが、特定のポリシーが適用されているために、ブロックアクションがトリガーされたとします。このアプリケーションは、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。

セクション	説明
[一致したアプリケーションタイプ (Application Types Matched) ]	[一致したアプリケーションタイプ (Application Types Matched) ]インタラクティブテーブルでは、[総トランザクション数の上位アプリケーションタイプ (Top Applications Type by Total Transactions) ]テーブルに表示されているアプリケーションタイプに関するさらに詳しい情報を表示できます。[アプリケーション (Applications) ]列で、詳細を表示するアプリケーションをクリックできます。
[一致したアプリケーション (Applications Matched) ]	<p>[一致したアプリケーション (Applications Matched) ]セクションには、指定した時間範囲内のすべてのアプリケーションが表示されます。これはインタラクティブな列見出しのあるインタラクティブテーブルとなっていて、必要に応じてデータをソートできます。</p> <p>[一致したアプリケーション (Applications Matched) ]セクションに表示する列を設定することができます。このセクションの列の設定については、<a href="#">Webセキュリティレポートの使用 (196 ページ)</a> を参照してください。</p> <p>[アプリケーション (Applications) ]テーブルに表示する項目を選択後、表示する項目の数を[表示された項目 (Items Displayed) ]ドロップダウンメニューから選択できます。選択肢は[10]、[20]、[50]、[100]です。</p> <p>さらに、[一致したアプリケーション (Application Matched) ]セクション内で特定のアプリケーションを検索できます。このセクション下部のテキストフィールドに特定のアプリケーション名を入力し、[アプリケーションの検索 (Find Application) ]をクリックします。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196 ページ\)](#) を参照してください。



(注) [アプリケーションの表示 (Application Visibility) ]ページの情報に関して、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、[スケジュール設定されたレポートとオンデマンドWebレポートについて \(272 ページ\)](#) を参照してください。

## [マルウェア対策 (Anti-Malware) ]レポート

[ウェブ (Web) ]>[レポート (Reporting) ]>[マルウェア対策 (Anti-Malware) ]ページはセキュリティ関連のレポートニングページであり、イネーブルなスキャンエンジン (Webroot、Sophos、McAfee、または Adaptive Scanning) によるスキャン結果が反映されます。

このページを使用して、Webベースのマルウェアの脅威を特定およびモニタすることができます。



(注) L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、[\[L4 トラフィック モニタ \(L4 Traffic Monitor\) \]レポート \(228 ページ\)](#) を参照してください。

[マルウェア対策 (Anti-Malware) ]ページには次の情報が表示されます。

表 46:[ウェブ (Web) ]>[レポート (Reporting) ]>[マルウェア対策 (Anti-Malware) ]ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[上位マルウェアカテゴリ: モニタまたはブロック済み (Top Malware Categories: Monitored or Blocked) ]	このセクションには、所定のカテゴリ タイプによって検出された上位マルウェア カテゴリが表示されます。この情報はグラフ形式で表示されます。有効なマルウェア カテゴリの詳細については、 <a href="#">マルウェアのカテゴリについて (216 ページ)</a> を参照してください。
[上位マルウェアの脅威: モニタまたはブロック済み (Top Malware Threats: Monitored or Blocked) ]	このセクションには、上位のマルウェアの脅威が表示されます。この情報はグラフ形式で表示されます。
[マルウェアカテゴリ (Malware Categories) ]	<p>[マルウェアカテゴリ (Malware Categories) ] インタラクティブ テーブルには、[上位マルウェアカテゴリ (Top Malware Categories) ] チャートに表示されている個々のマルウェア カテゴリに関する詳細情報が表示されます。</p> <p>[マルウェアカテゴリ (Malware Categories) ] インタラクティブ テーブル内のリンクをクリックすると、個々のマルウェア カテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。</p> <p>例外: このテーブルの [アウトブレイクヒューリスティック (Outbreak Heuristics) ] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。</p> <p>有効なマルウェア カテゴリの詳細については、<a href="#">マルウェアのカテゴリについて (216 ページ)</a> を参照してください。</p>
[マルウェア脅威 (Malware Threats) ]	<p>[マルウェアの脅威 (Malware Threats) ] インタラクティブ テーブルには、[上位マルウェア脅威 (Top Malware Threats) ] セクションに表示されている個々のマルウェアの脅威に関する詳細情報が表示されます。</p> <p>「アウトブレイク (Outbreak) 」のラベルと番号が付いている脅威は、他のスキャンエンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

## [マルウェアのカテゴリ (Malware Category) ]レポート

[マルウェアのカテゴリ (Malware Category) ]レポート ページでは、個々のマルウェア カテゴリとネットワークでのその動作に関する詳細情報を表示できます。

[マルウェアのカテゴリ (Malware Category) ]レポート ページにアクセスするには、次の手順を実行します。

- ステップ 1** セキュリティ管理アプライアンスで、ドロップダウン リストから **[ウェブ (Web) ]** を選択します。
- ステップ 2** **[モニタリング (Monitoring) ] > [マルウェア対策 (Anti-Malware) ]** ページを選択します。
- ステップ 3** [マルウェアカテゴリ (Malware Categories) ] インタラクティブテーブルで、[マルウェアのカテゴリ (Malware Category) ] 列内のカテゴリをクリックします。
- ステップ 4** このレポートのビューをカスタマイズするには、[Webセキュリティ レポートの使用 \(196 ページ\)](#) を参照してください。

## [マルウェアの脅威 (Malware Threat) ]レポート

[マルウェア脅威 (Malware Threats) ]レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[クライアントの詳細 (Client Detail) ] ページへのリンクがあります。レポート上部のトレンドグラフには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

このレポートを表示するには、[マルウェア対策 (Anti-Malware) ] レポート ページの [マルウェアのカテゴリ (Malware Category) ] 列でカテゴリをクリックします。

詳細については、テーブルの下の [サポートポータルマルウェア詳細 (Support Portal Malware Details) ] リンクをクリックしてください。

## マルウェアのカテゴリについて

Web セキュリティ アプライアンスは次のタイプのマルウェアをブロックできます。



マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェアアプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザヘルパーオブジェクト	ブラウザヘルパーオブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザプラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイクヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。

[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）]および[高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）]レポート

マルウェアのタイプ	説明
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。  公然と、または密かに、システムプロセスやユーザアクションを記録する。  これらの記録を後で取得して確認できるようにする。
トロイのダウンロード	トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンロードはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークションサイト、あるいはオンライン支払サイトに関するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

## [高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）]および[高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）]レポート

- [ファイル分析レポートの詳細の要件](#)（219 ページ）
- [SHA-256 ハッシュによるファイルの識別](#)（221 ページ）
- [\[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection \(File Reputation\)）\]および\[高度なマルウェア防御（ファイル分析）（Advanced Malware Protection \(File Analysis\)）\]レポート](#) ページ（222 ページ）
- [その他のレポートでのファイルレピュテーションフィルタデータの表示](#)（224 ページ）
- [Web トラッキング機能および高度なマルウェア防御機能について](#)（293 ページ）

## ファイル分析レポートの詳細の要件

- (クラウドファイル分析) 管理アプライアンスがファイル分析サーバに到達できることを確認する (219 ページ)
- (クラウドファイル分析) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する (219 ページ)
- (オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する (220 ページ)
- 追加の要件 (221 ページ)

### (クラウド ファイル分析) 管理アプライアンスがファイル分析サーバに到達できることを確認する


ファイル分析レポートの詳細を取得するには、アプライアンスがポート 443 経由でファイル分析サーバに接続できる必要があります。詳細については、[ファイアウォール情報 \(643 ページ\)](#) を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスがインターネットに直接接続していない場合は、このトラフィック用にプロキシサーバを設定します ([アップグレードとアップデートの設定 \(528 ページ\)](#) を参照)。プロキシを使用してアップグレードおよびサービスアップデートを入手するようにアプライアンスを設定済みの場合は、既存の設定が使用されます。

HTTPS プロキシを使用する場合は、そのプロキシでトラフィックを復号しません。パススルー機能を使用してファイル分析サーバと通信するようにしてください。プロキシサーバはファイル分析サーバからの証明書を信頼する必要がありますが、ファイル分析サーバに自身の証明書を提供する必要はありません。

### (クラウド ファイル分析) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の Cisco E メール セキュリティ アプライアンスまたは Cisco Web セキュリティ アプライアンスから分析用に送信されるファイルに関するクラウド内の詳細な結果が表示されるようにするには、すべてのアプライアンスを同じアプライアンス グループに結合する必要があります。

**ステップ 1** (新しい Web インターフェイスのみ) セキュリティ管理アプライアンスで  をクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] を選択します。

**ステップ 3** [ファイル分析 (File Analysis) ] セクションにスクロールします。

**ステップ 4** 管理対象アプライアンスが別のファイル分析クラウドサーバを指している場合は、結果の詳細の表示元となるサーバを選択します。

結果の詳細は、その他のクラウドサーバによって処理されたファイルでは使用できません。

**ステップ 5** 分析グループ ID を入力します。

**(オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する**

- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- この値に CCOID を使用することを推奨します。
- この値は大文字と小文字が区別されます。
- この値は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。
- アプライアンスは 1 つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

**ステップ 6** [今すぐグループ化 (Group Now) ] をクリックします。

**ステップ 7** このアプライアンスとデータを共有する各 Web セキュリティアプライアンスで、同じグループを設定します。

---

### 次のタスク

#### 関連項目

[クラウドで詳細なファイル分析結果が表示されるファイル \(224 ページ\)](#)

### (オンプレミスのファイル分析) ファイル分析アカウントをアクティブ化する


オンプレミス (プライベート クラウド) の Cisco AMP Threat Grid Appliance を導入した場合、Threat Grid Appliance で使用可能なレポート詳細を表示するために、Cisco コンテンツセキュリティ管理アプライアンスのファイル分析アカウントをアクティブ化する必要があります。通常、これは 1 回のみ必要です。

#### 始める前に

重大レベルでシステム アラートを受信していることを確認します。

---

**ステップ 1** Threat Grid Appliance からファイル分析レポート詳細に最初にアクセスしようとするときに、数分待ってから、リンクを含むアラートを受信します。

このアラートを受信しなかった場合は、[] アイコンをクリックしてレガシー Web インターフェイスをロードし、[管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [アラート (Alerts) ] を選択して、[上位アラートを表示 (View Top Alerts) ] をクリックします。

**ステップ 2** アラート メッセージ内のリンクをクリックします。

**ステップ 3** 必要に応じて、Cisco AMP Threat Grid Appliance にサインインします。

ステップ 4 管理アプライアンスのアカウントをアクティブ化します。

---

#### 追加の要件

追加の要件については、お使いのセキュリティ管理アプライアンス リリースのリリース ノート（次の場所で入手可能）を参照してください <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

#### SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイル进行处理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイル进行处理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルがその SHA-256 値（短縮形式）別に表示されます。組織のマルウェア インスタンスに関連付けられたファイル名を特定するには、[高度なマルウェア 防御（Advanced Malware Protection）] レポート ページを選択し、テーブルの SHA-256 リンクをクリックします。関連付けられたファイル名が詳細ページに表示されます。

## [高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）]および[高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）]レポート ページ

レポート	説明
高度なマルウェア対策 (Advanced Malware Protection)	<p>ファイルレピュテーションサービスによって特定されたファイルベースの脅威を示します。</p> <p>各 SHA にアクセスしようとしたユーザ、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。</p> <p>[マルウェア脅威ファイルの詳細 (Malware Threat File Details)] レポート ページ下部にあるリンクをクリックすると、レポートに対して選択された時間範囲に関係なく、設定可能な最大時間範囲内で検出されたそのファイルのすべてのインスタンスが [Web トラッキング (Web Tracking)] に表示されます。</p> <p>判定が変更されたファイルについては、[AMP 判定のアップデート (AMP Verdict Updates)] レポートを参照してください。これらの判定は、[高度なマルウェア防御 (Advanced Malware Protection)] レポートに反映されません。</p> <p>圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御 (Advanced Malware Protection)] レポートに含まれます。</p> <p>[カテゴリ別マルウェアファイル (Malware Files by Category)] セクションは、[カスタム検出 (Custom Detection)] に分類される、AMP for Endpoints コンソールから受信したブラックリストファイル SHA の割合を示しています。</p> <p>AMP for Endpoints コンソールから取得されるブラックリストに追加されたファイル SHA の脅威名は、レポートの [マルウェア脅威ファイル (Malware Threat Files)] セクションで [シンプルカスタム検出 (Simple Custom Detection)] として表示されます。</p> <p>AMP for Endpoints コンソールでブラックリストに登録されたファイル SHA のファイル トラジェクトリの詳細を表示するには、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. [レポート (Reporting)] &gt; [高度なマルウェア防御 (Advanced Malware Protection)] を選択します。</li> <li>2. トラジェクトリの詳細を表示するファイル SHA のリンクをクリックします。</li> <li>3. [詳細の表示 (More Details)] セクションで [AMP コンソール (AMP Console)] リンクをクリックします。</li> </ol>

レポート	説明
[ファイル分析 (File Analysis) ]	<p>分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。</p> <p>1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>オンプレミスの Cisco AMP Threat Grid Appliance での導入の場合：Cisco AMP Threat Grid Appliance でホワイトリストに登録されているファイルは、「クリーン」として表示されます。ホワイトリストについては、AMP Threat Grid のオンライン ヘルプを参照してください。</p> <p>ドリル ダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。</p> <p>また、分析を実行したサーバでSHAに関する追加の詳細を直接表示するには、SHA を検索するか、またはファイル分析の詳細ページ下部にある Cisco AMP Threat Grid リンクをクリックします。</p> <p>ファイルを分析したサーバに関する詳細を表示するには、<a href="#">ファイル分析レポートの詳細の要件（219 ページ）</a> を参照してください。</p> <p>圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析 (File Analysis) ] レポートに含まれます。</p>
[AMP判定のアップデート (AMP Verdict Updates) ]	<p>このアプライアンスで処理され、トランザクションの処理後に判定が変わったファイルの一覧を示します。この状況の詳細については、お使いの Web セキュリティ アプライアンスのマニュアルを参照してください。</p> <p>1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。</p> <p>複数の Web Security Appliances で同じファイルの判定アップデートが異なる場合、最新のタイム スタンプが付いた結果が表示されます。</p> <p>SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内にこの SHA-256 が含まれた、すべてのトランザクションの Web トラッキング結果が表示されます。</p> <p>使用可能な最大時間範囲内（レポート用に選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けたすべてのトランザクションを表示するには、<a href="#">[マルウェアの脅威ファイル (Malware Threat Files) ]</a> ページの下部にあるリンクをクリックします。</p>

## その他のレポートでのファイルレピュテーションフィルタ データの表示

該当する場合は、ファイルレピュテーションおよびファイル分析のデータを他のレポートでも使用できます。レポートによっては、[高度なマルウェア防御でブロック (Blocked by Advanced Malware Protection)] 列がデフォルトで非表示になっている場合があります。追加列を表示するには、テーブルの下の [列 (Columns)] リンクをクリックします。

## クラウドで詳細なファイル分析結果が表示されるファイル

パブリッククラウドのファイル分析を導入した場合は、ファイル分析のためにアプライアンスグループに追加された、任意の管理対象アプライアンスからアップロードされたすべてのファイルの詳細な結果を表示できます。

グループに管理アプライアンスを追加した場合は、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] ページにあるボタンをクリックして、グループの管理対象アプライアンスのリストを表示できます。

分析グループのアプライアンスはファイル分析クライアント ID で識別されます。特定のアプライアンスのこの ID を判別するには、次の場所を参照してください。

アプライアンス	ファイル分析クライアント ID の場所
E メールセキュリティアプライアンス	[セキュリティサービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション
Web セキュリティアプライアンス	[セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション。
Cisco コンテンツセキュリティ管理アプライアンス	[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] ページの下部

### 関連項目

[\(クラウドファイル分析\) 詳細なファイル分析結果が表示されるように管理アプライアンスを設定する \(219 ページ\)](#)

## [クライアントマルウェアリスク (Client Malware Risk)] レポート

[ウェブ (Web)] > [レポート (Reporting)] > [クライアントマルウェアリスク (Client Malware Risk)] ページは、クライアントマルウェアリスクアクティビティをモニタするために使用できるセキュリティ関連のレポートニング ページです。



[クライアントマルウェアリスク (Client Malware Risk) ]ページでは、システム管理者が最も多くブロックまたは警告を受けているユーザを確認できます。このページで収集された情報から、管理者はユーザリンクをクリックして、そのユーザが多数のブロックや警告を受けている原因、およびネットワーク上の他のユーザよりも多く検出されている原因となっているユーザの行動を確認できます。

さらに[クライアントマルウェアリスク (Client Malware Risk) ]ページには、L4 トラフィックモニタ (L4TM) によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。マルウェアサイトに頻繁に接続するコンピュータは、マルウェアに感染している可能性があります。これらのマルウェアは中央のコマンド/コントロールサーバに接続しようとするので、除去しなければなりません。

次の表で、[クライアントマルウェアリスク (Client Malware Risk) ]ページの情報について説明します。

表 47:[クライアントマルウェアリスク (Client Malware Risk) ]レポート ページの内容

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	レポートに含めるデータの時間範囲を選択できるメニュー。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[Webプロキシ:モニタまたはブロックされた上位クライアント (Web Proxy: Top Clients Monitored or Blocked) ]	このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。
[L4トラフィックモニタ:検出されたマルウェア接続 (L4 Traffic Monitor: Malware Connections Detected) ]	このチャートには、組織内で最も頻繁にマルウェアサイトに接続している 10 台のコンピュータの IP アドレスが表示されます。  このチャートは <a href="#">[L4 トラフィックモニタ (L4 Traffic Monitor) ]レポート (228 ページ)</a> の <a href="#">[上位クライアントIP (Top Client IPs) ]</a> チャートと同じです。詳細およびチャート オプションについてはこの項を参照してください。

セクション	説明
[Webプロキシ:クライアントマルウェアリスク (Web Proxy: Client Malware Risk) ]	<p>[Webプロキシ: クライアントマルウェアリスク (Web Proxy: Client Malware Risk) ] テーブルには、[Webプロキシ:マルウェアリスクによる上位クライアント (Web Proxy: Top Clients by Malware Risk) ] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。</p> <p>このテーブルで各ユーザをクリックすると、そのクライアントに関連する [ユーザの詳細 (User Details) ] ページが表示されます。このページの詳細については、[ユーザの詳細 (User Details) ] (Web レポーティング) (206 ページ) を参照してください。</p> <p>テーブルで任意のリンクをクリックすると、個々のユーザと、マルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。たとえば [ユーザID/クライアントIPアドレス (User ID/Client IP Address) ] 列のリンクをクリックすると、そのユーザの [ユーザ (User) ] ページに移動します。</p>
[L4トラフィックモニタ:マルウェアリスク別クライアント (L4 Traffic Monitor: Clients by Malware Risk) ]	<p>このテーブルには、組織内でマルウェアサイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。</p> <p>このテーブルは [L4 トラフィック モニタ (L4 Traffic Monitor) ] レポート (228 ページ) の [クライアントソースIP (Client Source IPs) ] テーブルと同じです。テーブルの操作についてはこの項を参照してください。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

## [Web レピュテーションフィルタ (Web Reputation Filters) ] レポート

[ウェブ (Web) ] > [レポート (Reporting) ] > [Web レピュテーションフィルタ (Web Reputation Filters) ] では、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ (ユーザが設定) の結果を確認できます。

### Web レピュテーション フィルタとは

Web レピュテーション フィルタは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーション スコアを URL に割り当てます。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらす URL ベースのマルウェアを防ぐために役立ちます。Web セキュリティ アプライアンスは、URL レピュテーション スコアを使用して、疑わしいアクティビティを特定するとともに、マルウェア攻撃を未然に防ぎ

ます。Web レピュテーション フィルタは、アクセス ポリシーと復号ポリシーの両方と組み合わせ使用できます。

Web レピュテーション フィルタでは、統計データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ~ +10 の Web レピュテーションスコアにマッピングされます (+10 がマルウェアを含む可能性が最も低い)。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書 (EULA) の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

Web レピュテーション フィルタの詳細については、『IronPort AsyncOS for Web User Guide』の「Web Reputation Filters」を参照してください。

[Web レピュテーション フィルタ (Web Reputation Filters)] ページには次の情報が表示されません。

表 48: [ウェブ (Web)] > [レポート (Reporting)] > [Web レピュテーション フィルタ (Web Reputation Filters)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	1 ~ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[Web レピュテーション アクション (トレンド) (Web Reputation Actions (Trend))]	このセクションには、指定した時間 (横方向の時間軸) に対する Web レピュテーション アクションの総数 (縦方向の目盛り) が、グラフ形式で表示されます。このセクションでは、時間の経過に伴う Web レピュテーション アクションの潜在的なトレンドを確認できます。
[Web レピュテーション アクション (ボリューム) (Web Reputation Actions (Volume))]	このセクションには、Web レピュテーション アクションのボリュームがトランザクション数の比率で表示されます。

セクション	説明
[WBRISによってブロックされるWebレピュテーションの脅威タイプ (Web Reputation Threat Types Blocked by WBRIS) ]	このセクションには、Web レピュテーションフィルタリングによってブロックされたトランザクションで発生した脅威タイプが表示されます。 注：WBRIS では、常に、脅威のタイプを識別できるわけではありません。
[他のトランザクションで脅威タイプが検知されました (Threat Types Detected in Other Transactions) ]	このセクションには、Web レピュテーションフィルタリングによってブロックされないトランザクションで発生した脅威タイプが表示されます。 これらの脅威がブロックされなかった理由には、次のようなものがあります。 <ul style="list-style-type: none"> <li>• すべての脅威に、ブロッキングのしきい値を満たすスコアがあるわけではありません。ただし、アプライアンスのその他の機能は、これらの脅威を検出する可能性があります。</li> <li>• ポリシーが、脅威を許可するよう設定されている可能性があります。</li> </ul> 注：WBRIS では、常に、脅威のタイプを識別できるわけではありません。
Web レピュテーションアクション (スコアによる内訳) (Web Reputation Actions (Breakdown by Score))	Adaptive Scanning がイネーブルでない場合、このインタラクティブテーブルには各アクションの Web レピュテーションスコアの内訳が表示されます。



ヒント このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

## Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーション設定の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

## [L4 トラフィック モニタ (L4 Traffic Monitor) ] レポート

[ウェブ (Web) ]>[レポート (Reporting) ]>[L4 トラフィック モニタ (L4 Traffic Monitor) ] ページには、指定した時間範囲内に L4 トラフィック モニタによってお使いの Web セキュリティアプライアンス上で検出されたマルウェアポートとマルウェアサイトに関する情報が表示されます。マルウェアサイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

L4 トラフィック モニタは、Web セキュリティアプライアンスのすべてのポートに着信するネットワークトラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベーステーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

このレポートのデータを使用して、ポートまたはサイトをブロックするかどうかを判断したり、特定のクライアント IP アドレスが著しく頻繁にマルウェアサイトに接続している理由（たとえば、その IP アドレスに関連付けられたコンピュータが、中央のコマンド/コントロールサーバに接続しようとするマルウェアに感染しているなど）を調査したりできます。



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

表 49: [L4 トラフィック モニタ (L4 Traffic Monitor) ]レポート ページの内容

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	レポート対象の時間範囲を選択できるメニュー。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[上位クライアント IP (Top Client Ips) ]	<p>このセクションには、組織内で最も頻繁にマルウェアサイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。</p> <p>チャートの下の [チャートオプション (Chart Options) ] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続 (Malware Connections Detected) ] から [モニタされたマルウェア接続 (Malware Connections Monitored) ] または [ブロックされたマルウェア接続 (Malware Connections Blocked) ] に変更できます。</p> <p>このチャートは、<a href="#">クライアントマルウェアリスク (Client Malware Risk) ] レポート (224 ページ)</a> の [L4 トラフィック モニタ : 検出されたマルウェア接続 (L4 Traffic Monitor: Malware Connections Detected) ] チャートと同じです。</p>
[上位マルウェアサイト (Top Malware Sites) ]	<p>このセクションには、L4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。</p> <p>チャートの下の [チャートオプション (Chart Options) ] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続 (Malware Connections Detected) ] から [モニタされたマルウェア接続 (Malware Connections Monitored) ] または [ブロックされたマルウェア接続 (Malware Connections Blocked) ] に変更できます。</p>

セクション	説明
[クライアントソースIP (Client Source Ips) ]	<p>このテーブルには、組織内でマルウェア サイトに頻繁に接続しているコンピュータの IP アドレスが表示されます。</p> <p>特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ (Filter by Port) ]をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェア サイトへ「誘導」しているかを判断できます。</p> <p>各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリーをクリックします。たとえば、ある特定のクライアント IP アドレスの [ブロックされたマルウェア接続 (Malware Connections Blocked) ]が高い数値を示している場合、その列の数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[ウェブ (Web) ]&gt;[レポート (Reporting) ]&gt;[Webトラッキング (Web Tracking) ]ページの [L4 トラフィック モニタ (L4 Traffic Monitor) ]タブに検索結果として表示されます。リストの詳細については、<a href="#">L4 トラフィック モニタによって処理されたトランザクションの検索 (284 ページ)</a> を参照してください。</p> <p>このテーブルは、[クライアントマルウェアリスク (Client Malware Risk) ]レポート (224 ページ) の [L4 トラフィック モニタ - マルウェアリスク別クライアント (L4 Traffic Monitor - Clients by Malware Risk) ]テーブルと同じです。</p>
[マルウェアポート (Malware Ports) ]	<p>このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたポートが表示されます。</p> <p>詳細を表示するには、テーブル内のエントリーをクリックします。たとえば、[検出されたマルウェア接続の総数 (Total Malware Connections Detected) ]の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[ウェブ (Web) ]&gt;[レポート (Reporting) ]&gt;[Webトラッキング (Web Tracking) ]ページの [L4 トラフィック モニタ (L4 Traffic Monitor) ]タブに検索結果として表示されます。リストの詳細については、<a href="#">L4 トラフィック モニタによって処理されたトランザクションの検索 (284 ページ)</a> を参照してください。</p>

セクション	説明
[検出されたマルウェアサイト (Malware Sites Detected)]	<p>このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたドメインが表示されます。</p> <p>特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ (Filter by Port)] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。</p> <p>詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続 (Malware Connections Blocked)] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[ウェブ (Web)] &gt; [レポート (Reporting)] &gt; [Web トラッキング (Web Tracking)] ページの [L4 トラフィック モニタ (L4 Traffic Monitor)] タブに検索結果として表示されます。リストの詳細については、<a href="#">L4 トラフィック モニタによって処理されたトランザクションの検索 (284 ページ)</a> を参照してください。</p>



ヒント このレポートのビューをカスタマイズするには、[Web セキュリティ レポートの使用 \(196 ページ\)](#) を参照してください。

#### 関連項目

- [L4 トラフィック モニタ レポートのトラブルシューティング \(297 ページ\)](#)

## [SOCKS プロキシ (SOCKS Proxy)] レポート

[ウェブ (Web)] > [レポート (Reporting)] > [SOCKS プロキシ (SOCKS Proxy)] ページでは、宛先、ユーザなど、SOCKS プロキシを通じて処理されたトランザクションのデータおよびトレンドを表示できます。



(注) レポートに表示される宛先は、SOCKS クライアント (通常はブラウザ) が SOCKS プロキシに送信するアドレスです。

SOCKS ポリシー設定を変更するには、『Cisco Web Security Appliances User Guide』の「AsyncOS」を参照してください。

#### 関連項目

- [SOCKS プロキシによって処理されるトランザクションの検索 \(285 ページ\)](#)

## ユーザの場所別レポート (Reports by User Location)

[ウェブ (Web)] > [レポート (Reporting)] > [ユーザの場所別のレポート (Reports by User Location)] ページでは、モバイルユーザがローカルシステムまたはリモートシステムから実行しているアクティビティを確認できます。

対象となるアクティビティは次のとおりです。

- ローカルユーザおよびリモートユーザがアクセスしている URL カテゴリ。
- ローカルユーザおよびリモートユーザがアクセスしているサイトによってトリガーされているアンチマルウェアアクティビティ。
- ローカルユーザおよびリモートユーザがアクセスしているサイトの Web レピュテーション。
- ローカルユーザおよびリモートユーザがアクセスしているアプリケーション。
- ユーザ (ローカルおよびリモート)。
- ローカルユーザおよびリモートユーザがアクセスしているドメイン。

[ユーザの場所別のレポート (Reports by User Location)] ページには次の情報が表示されます。

表 50: [ウェブ (Web)] > [レポート (Reporting)] > [ユーザの場所別のレポート (Reports by User Location)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	1~90日間またはカスタム日数範囲を指定できるドロップダウンリスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[Webプロキシアクティビティ総数:リモートユーザ (Total Web Proxy Activity: Remote Users)]	このセクションには、指定した時間 (横方向) におけるリモートユーザのアクティビティ (縦方向) が、グラフ形式で表示されます。
[Webプロキシの概要 (Web Proxy Summary)]	このセクションには、システム上のローカルユーザとリモートユーザのアクティビティの要約が表示されます。
[Webプロキシアクティビティ総数:ローカルユーザ (Total Web Proxy Activity: Local Users)]	このセクションには、指定した時間 (横方向) におけるリモートユーザのアクティビティ (縦方向) が、グラフ形式で表示されます。
[検出された疑わしいトランザクション:リモートユーザ (Suspect Transactions Detected: Remote Users)]	このセクションには、リモートユーザに対して定義したアクセスポリシーによって指定した時間内 (横方向) に検出された疑わしいトランザクション (縦方向) が、グラフ形式で表示されます。
[疑わしいトランザクションの概要 (Suspect Transactions Summary)]	このセクションには、システム上のリモートユーザの疑わしいトランザクションの要約が表示されます。
[検出された疑わしいトランザクション:ローカルユーザ (Suspect Transactions Detected: Local Users)]	このセクションには、リモートユーザに対して定義したアクセスポリシーによって指定した時間内 (横方向) に検出された疑わしいトランザクション (縦方向) が、グラフ形式で表示されます。



セクション	説明
[疑わしいトランザクションの概要 (Suspect Transactions Summary) ]	このセクションには、システム上のローカルユーザの疑わしいトランザクションの要約が表示されます。

[ユーザの場所別のレポート (Reports by User Location) ] ページでは、ローカルユーザとリモートユーザのアクティビティを示すレポートを生成できます。これにより、ユーザのローカルアクティビティとリモートアクティビティを簡単に比較できます。



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。



**(注)** [ユーザの場所別のレポート (Reports by User Location) ] ページの情報について、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、[スケジュール設定されたレポートとオンデマンドWebレポートについて \(272ページ\)](#) を参照してください。

## [システム容量 (System Capacity) ] ページ

[ウェブ (Web) ] > [レポート (Reporting) ] > [システム容量 (System Capacity) ] ページでは、Webセキュリティアプライアンスによってセキュリティ管理アプライアンスで発生する作業負荷全体を表示できます。重要な点は、[システム容量 (System Capacity) ] ページを使用して、経時的に増大をトラッキングしてシステムキャパシティの計画を立てられることです。Web Security Appliances をモニタすると、キャパシティが実際の量に適しているかを確認できます。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。

[システム容量 (System Capacity) ] ページを使用すると、次の情報を確認できます。

- Web Security Appliances が推奨される CPU キャパシティをいつ超えたかを特定します。これによって、設定の最適化や追加アプライアンスがいつ必要になったかがわかります。
- トラブルシューティングのために、システムが最もリソースを使用している部分を識別します。
- 応答時間とプロキシバッファメモリを確認します。
- 1秒あたりのトランザクション、および顕著な接続を確認します。

## [システム容量 (System Capacity) ] レポートの表示

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web) ] > [レポート (Reporting) ] > [システム容量 (System Capacity) ] を選択します。

**ステップ 2** 他のタイプのデータを表示するには、[列 (Columns)] をクリックし、表示するデータを選択します。

**ステップ 3** 単一のアプライアンスのシステム容量を表示するには、[平均使用率およびパフォーマンスの概要 (Overview of Averaged Usage and Performance)] テーブルの [Web セキュリティ アプライアンス (Web Security appliance)] 列で目的のアプライアンスをクリックします。

このアプライアンスに関する [システム容量 (System Capacity)] グラフが表示されます。このページのグラフは次の 2 種類に分かれています。

- [システム容量 (System Capacity)] : [システムの負荷 (System Load)] (234 ページ)
- [システム容量 (System Capacity)] : [ネットワーク負荷 (Network Load)] (235 ページ)

## [システム容量 (System Capacity)] ページに表示されるデータの解釈方法

[システム容量 (System Capacity)] ページにデータを表示する時間範囲を選択する場合、次のことに留意することが重要です。

- **Day レポート** : Day レポートでは、時間テーブルを照会し、24 時間の間に 1 時間ごとにアプライアンスが受信したクエリの正確な数を表示します。この情報は時間テーブルから収集されます。
- **Month レポート** : Month レポートでは、30 日間または 31 日間 (その月の日数に応じる) の日テーブルを照会し、30 日間または 31 日間の正確なクエリ数を表示します。これも正確な数値です。

[システム容量 (System Capacity)] ページの [最大 (Maximum)] 値インジケータは、指定された期間内の最大値を示します。[平均 (Average)] 値は指定された期間内のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合、日付ごとの [平均 (Average)] 値と [最大 (Maximum)] 値を表示することができます。



(注) 他のレポートで時間範囲に [年 (Year)] を選択した場合は、最大の時間範囲である 90 日を選択することを推奨します。

## [システム容量 (System Capacity)] : [システムの負荷 (System Load)]

[システム容量 (System Capacity)] ウィンドウの最初の 4 つのグラフは、システム負荷に関するレポートです。これらのレポートには、アプライアンスでの全体的な CPU 使用状況が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してトランザクションスループットを向上させるように最適化されています。CPU 使用率が高くても、必ずしもシステムキャパシティの問題を示すわけではありません。CPU 使用率が高く、かつ高ボリュームのメモリページスワッピングが発生する場合、キャパシティの問題の可能性があります。このページには、Web Security Appliances のレポートの処理などのさまざまな機能で使われる CPU 量を示すグラフも示されます。機能別 CPU のグラフは、システム上で最も多くのリソース使

用する製品の領域を示す指標です。アプライアンスの最適化が必要な場合、このグラフは、調整やディセーブル化の必要な機能を判断するのに役立ちます。

また、応答時間/遅延のグラフと 1 秒あたりのトランザクションのグラフには、全体的な応答時間 (ミリ秒単位)、および [時間範囲 (Time Range) ] ドロップダウン メニューで指定した日付範囲での 1 秒あたりのトランザクション数が示されます。

## [システム容量 (System Capacity) ] : [ネットワーク負荷 (Network Load) ]

[システム容量 (System Capacity) ] ウィンドウの次のグラフには、発信接続、出力用帯域幅、プロキシバッファ メモリの統計情報が示されます。日、週、月、または年の結果を表示することもできます。ご自身の環境における通常量とスパイクのトレンドを理解しておくことが重要です。

[プロキシバッファ メモリ (Proxy Buffer Memory) ] では、通常動作中にネットワーク トラフィックのスパイクが表れることがあります。しかし、グラフが最大値に向かって着実に上昇している場合は、アプライアンスが最大キャパシティに達しつつある可能性があり、キャパシティの追加を検討する必要があります。

次のチャートは、[システム容量 (System Capacity) ] : [システムの負荷 (System Load) ] (234 ページ) で説明されているチャートと同じページで、それらのチャートの下に表示されます。

## プロキシバッファ メモリ スワッピングに関する注意事項

システムは、定期的にプロキシバッファ メモリをスワップするように設計されているので、一部のプロキシバッファ メモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが常に高ボリュームのプロキシバッファ メモリをスワップする場合以外は、プロキシバッファ メモリ スワッピングは正常であり、起こり得る挙動です。システムが極端に大量の処理を行い、大量であるためにプロキシバッファ メモリを絶えずスワップする場合は、ネットワークに Web セキュリティ アプライアンスを追加するか、またはスループットが最大になるように設定を調整して、パフォーマンスの向上を図る必要があります。

## [使用可能なデータ (Data Availability) ] ページ

[ウェブ (Web) ] > [レポート (Reporting) ] > [使用可能なデータ (Data Availability) ] ページには、管理対象の各 Web セキュリティ アプライアンスに対応するセキュリティ管理アプライアンスでレポートリングおよび Web トラッキング データを使用できる日付範囲の概要が表示されます。



- (注) Web レポートリングがディセーブルになると、セキュリティ管理アプライアンスは Web セキュリティ アプライアンスから新しいデータを取得しなくなりますが、以前に取得したデータはセキュリティ管理アプライアンスに残っています。

[Webレポート (Web Reporting) ] の [開始 (From) ] 列と [終了 (To) ] 列、および [Webレポートとトラッキング (Web Reporting and Tracking) ] の [開始 (From) ] 列と [終了 (To) ] 列でステータスが異なる場合は、[ステータス (Status) ] 列に最も深刻な結果が示されます。

データの消去の詳細については、[ディスク領域の管理 \(567 ページ\)](#) を参照してください。



- (注) URL カテゴリに関するスケジュール設定されたレポートでデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「この時間範囲の一部のデータは使用不可でした。(Some data in this time range was unavailable.)」というメッセージが表示されます。ギャップが存在しない場合は何も表示されません。

## 新しい Web インターフェイスの Web レポート ページの概要

次の表は、Web セキュリティ アプライアンス用 AsyncOS のサポートされている最新リリースで、Web インターフェイスの [レポート (Reports) ] ドロップダウンから利用できるレポートを示します。詳細については、[インタラクティブレポート ページの使用 \(41 ページ\)](#) を参照してください。Web セキュリティ アプライアンスでこれ以前のリリースの AsyncOS を実行している場合、これらのレポートの一部は利用できない場合があります。

表 51: [Webレポート (Web Reports) ] ドロップダウンのオプション

[レポート (Reports) ] ドロップダウンのオプション	操作
一般的なレポート	
[概要 (Overview) ] ページ	[概要 (Overview) ] ページには、お使いの Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。詳細については、 <a href="#">[概要 (Overview) ] ページ (240 ページ)</a> を参照してください。
[アプリケーションの表示 (Application Visibility) ] ページ	[アプリケーションの表示 (Application Visibility) ] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内で特定のアプリケーションタイプに適用されているコントロールを適用し、表示できます。詳細については、 <a href="#">[アプリケーションの表示 (Application Visibility) ] ページ (242 ページ)</a> を参照してください。

[レポート (Reports) ] ドロップダウンのオプション	操作
[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] ページ	指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、 <a href="#">[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] ページ (244 ページ)</a> を参照してください。
[SOCKS プロキシ (SOCKS Proxy) ] ページ	宛先、ユーザなど、SOCKS プロキシ トランザクションのデータを表示できます。詳細については、 <a href="#">[SOCKS プロキシ (SOCKS Proxy) ] ページ (247 ページ)</a> を参照してください。
[URLカテゴリ (URL Categories) ] ページ	<p>[URLカテゴリ (URL Categories) ] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。</p> <ul style="list-style-type: none"> <li>• トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL。</li> <li>• 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブな列見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。</li> </ul> <p>詳細については、<a href="#">[URLカテゴリ (URL Categories) ] ページ (249 ページ)</a> を参照してください。</p>

[レポート (Reports) ] ドロップダウンのオプション	操作
[ユーザ (Users) ] ページ	<p>[ユーザ (Users) ] ページには複数の Web トラッキング リンクが表示され、各ユーザの Web トラッキング情報を確認できます。</p> <p>[ユーザ (Users) ] ページでは、システム上のユーザ (1人または複数) がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。</p> <p>[ユーザ (Users) ] ページのインタラクティブな [ユーザ (Users) ] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [ユーザの詳細 (User Details) ] ページに表示されます。</p> <p>[ユーザの詳細 (User Details) ] ページでは、[ユーザ (Users) ] ページの [ユーザ (Users) ] テーブルで指定したユーザに関する具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。</p> <p>詳細については、<a href="#">[ユーザ (Users) ] ページ (252 ページ)</a> を参照してください。</p> <p>システムにおける各ユーザの情報については、<a href="#">[ユーザの詳細 (User Details) ] ページ (Web レポートリング) (254 ページ)</a> を参照してください。</p>
[Webサイト (Web Sites) ] ページ	<p>[Webサイト (Web Sites) ] ページでは、管理対象アプライアンスで発生しているアクティビティ全体を集約して表示できます。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。詳細については、<a href="#">[Webサイト (Web Sites) ] ページ (257 ページ)</a> を参照してください。</p>
[HTTPSレポート (HTTPS Reports) ]	<p>[HTTPSレポート (HTTPS Reports) ] レポートページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー (トランザクションまたは帯域幅の使用量) のすべてを集約しています。詳細については、<a href="#">[HTTPSレポート (HTTPS Reports) ] ページ (258 ページ)</a> を参照してください。</p>

[レポート (Reports)] ドロップダウンのオプション	操作
脅威レポート	
[マルウェア対策 (Anti-Malware)] ページ	[マルウェア対策 (Anti-Malware)] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、 <a href="#">[マルウェア対策 (Anti-Malware)] ページ (260 ページ)</a> を参照してください。
[クライアント マルウェア リスク (Client Malware Risk)] ページ	[クライアントマルウェアリスク (Client Malware Risk)] ページは、セキュリティ関連のレポートイング ページです。このページを使用して、著しく頻繁にマルウェア サイトへ接続している可能性がある個々のクライアント コンピュータを特定できます。  詳細については、 <a href="#">[クライアントマルウェアリスク (Client Malware Risk)] レポート (267 ページ)</a> を参照してください。
[Web レピュテーション フィルタ (Web Reputation Filters)] ページ	指定した時間範囲内のトランザクションに対する、Web レピュテーション フィルタリングに関するレポートを表示できます。詳細については、 <a href="#">[Web レピュテーション フィルタ (Web Reputation Filters)] ページ (269 ページ)</a> を参照してください。

## [滞留時間 (Time Spent)] について

さまざまなテーブルの [滞留時間 (Time Spent)] 列は、Web ページでユーザが費やした時間を表します。各 URL カテゴリでユーザが費やした時間。ユーザを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。

トランザクション イベントに「viewed」のタグが付けられる (ユーザが特定の URL に進む) と、[滞留時間 (Time Spent)] の値の計算が開始され、Web レポートイング テーブルのフィールドとして追加されます。

費やされた時間を計算するため、AsyncOS はアクティブ ユーザごとに、1 分間のアクティビティに対して 60 秒という時間を割り当てます。この 1 分間の終わりに、各ユーザが費やした時間は、そのユーザが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザは各ドメインで 15 分ずつ費やしたと見なされます。

経過時間の値に関して、以下の注意事項を考慮してください。

- アクティブ ユーザは、アプライアンスを介して HTTP トラフィックを送信し、Web サイトにアクセスした、すなわち AsyncOS が「ページ ビュー」と見なす動作を行ったユーザ名または IP アドレスとして定義されています。
- AsyncOS では、クライアントアプリケーションが開始する要求とは逆に、ユーザが開始する HTTP 要求としてページ ビューを定義します。AsyncOS はヒューリスティック アルゴリズムを使用して、可能な限り効果的にユーザ ページ ビューを識別します。

単位は時間：分形式で表示されます。

## [概要 (Overview)] ページ

[概要 (Overview)] レポート ページには、お使いの Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。

[概要 (Overview)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)] > [概要 (Overview)]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[概要 (Overview)] レポート ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシ アクティビティ、および各種トランザクション サマリーが表示されます。トランザクション サマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしいトランザクションと、そのグラフの隣にそれらのトランザクションがブロックされた数、およびブロックされた方法が表示されます。

[概要 (Overview)] レポート ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位アプリケーション タイプおよびカテゴリ、これらのブロックまたは警告を生成している上位ユーザが表示されます。

表 52: [概要 (Overview)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
次のデータを参照 (View Data for) (ドロップダウン リスト)	概要データを表示する Web セキュリティ アプライアンスを選択するか、[すべての Web アプライアンス (All Web Appliances)] を選択します。 <a href="#">アプライアンスまたはレポート グループのレポートデータの表示 (26 ページ)</a> も参照してください。



セクション	説明
[Webプロキシアクティビティ総数 (Total Web Proxy Activity) ]	<p>現在セキュリティ管理アプライアンスで管理されている Web セキュリティアプライアンスによって報告される Web プロキシアクティビティを表示できます。</p> <p>このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。</p> <p>疑わしい Web プロキシアクティビティまたは正常なプロキシアクティビティの比率を、トランザクションの総数も含めて表示できます。</p>
[疑わしいトランザクション (Suspect Transactions) ]	<p>管理者が疑わしいトランザクションと分類した Web トランザクションをグラフ形式で表示できます。</p> <p>このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。</p> <p>ブロックまたは警告された疑わしいトランザクションの比率も表示できます。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。</p>
[L4トラフィックモニタの概要 (L4 Traffic Monitor Summary) ]	<p>現在セキュリティ管理アプライアンスで管理されている Web セキュリティアプライアンスによって報告される L4 トラフィックをグラフ形式で表示できます。</p>
上位 URL カテゴリ : 総トランザクション数 (Top URL Categories: Total Transactions)	<p>ブロックされている上位の URL カテゴリが、URL カテゴリのタイプおよび特定タイプのカテゴリが実際にブロックされた回数を含め、グラフ形式で表示されます。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URL カテゴリセットの更新とレポート (211 ページ)</a> を参照してください。</p>
上位アプリケーションタイプ : 総トランザクション数 (Top Application Types: Total Transactions)	<p>ブロックされている上位アプリケーションタイプが、実際のアプリケーションタイプ名および特定のアプリケーションがブロックされた回数を含め、グラフ形式で表示されます。</p>
上位マルウェアカテゴリ : モニタまたはブロック済み (Top Malware Categories: Monitored or Blocked)	<p>検出されたすべてのマルウェアカテゴリをグラフ形式で表示できます。</p>

セクション	説明
ブロックまたは警告されたトランザクション数の上位ユーザ (Top Users Blocked or Warned Transactions)	ブロックまたは警告されたトランザクションを生成している実際のユーザをグラフ形式で表示できます。ユーザは IP アドレスまたはユーザ名で表示できます。ユーザ名を識別できないようにするには、 <a href="#">Web レポートでのユーザ名の匿名化 (196 ページ)</a> を参照してください。

## [アプリケーションの表示 (Application Visibility) ] ページ



(注) [アプリケーションの表示 (Application Visibility) ] の詳細については、『User Guide for AsyncOS for Cisco Web Security Appliances』の「Understanding Application Visibility and Control」の章を参照してください。

[アプリケーションの表示 (Application Visibility) ] レポート ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内の特定のアプリケーションタイプに制御を適用することができます。

[アプリケーションの表示 (Application Visibility) ] レポート ページを表示するには、製品ドロップダウンから [Web] を選択し、[モニタリング (Monitoring) ] > [アプリケーションの表示 (Application Visibility) ] を選択します。詳細については、[インタラクティブレポートページの使用 \(41 ページ\)](#) を参照してください。

アプリケーション制御を使用すると、たとえば URL フィルタリングのみを使用する場合よりも Web トラフィックをきめ細かく制御できるだけでなく、次のタイプのアプリケーションおよびアプリケーションタイプに対する制御を強化できます。

- 回避アプリケーション (アノニマイザや暗号化トンネルなど)。
- コラボレーションアプリケーション (Cisco Webex、Facebook、インスタントメッセージングなど)。
- リソースを大量消費するアプリケーション (ストリーミングメディアなど)。

### アプリケーションとアプリケーションタイプの違いについて

レポートに関連するアプリケーションを制御するには、アプリケーションとアプリケーションタイプの違いを理解することが非常に重要です。

- **アプリケーションタイプ**。1つまたは複数のアプリケーションを含むカテゴリです。たとえば検索エンジンは、Google Search や Craigslist などの検索エンジンを含むアプリケーションタイプです。インスタントメッセージングは、Yahoo Instant Messenger や Cisco Webex などを含む別のアプリケーションタイプです。Facebook もアプリケーションタイプです。

- **アプリケーション**。アプリケーションタイプに属している特定のアプリケーションです。たとえば、YouTube はメディア アプリケーションタイプに含まれるアプリケーションです。
- **アプリケーション動作**。アプリケーション内でユーザが実行できる特定のアクションまたは動作です。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション動作が含まれているわけではありません。




- (注) Application Visibility and Control (AVC) エンジンを使用して Facebook アクティビティを制御する方法の詳細については、『User Guide for AsyncOS for Cisco Web Security Appliances』の「Understanding Application Visibility and Control」の章を参照してください。

[アプリケーションの表示 (Application Visibility) ] ページには次の情報が表示されます。

表 53: [アプリケーションの表示 (Application Visibility) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[総トランザクション数の上位アプリケーションタイプ (Top Application Types by Total Transactions) ]	<p>サイト上でアクセスされた上位のアプリケーションタイプがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の <input checked="" type="checkbox"/> をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p> <p>たとえば、Yahoo Instant Messenger などのインスタントメッセージング ツール、Facebook、Presentation というアプリケーションタイプが表示されます。</p>

セクション	説明
[ブロックされたトランザクション数の上位アプリケーション (Top Applications by Blocked Transactions) ]	<p>トランザクションごとに発生するブロックアクションをトリガーした上位アプリケーションタイプが、グラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p> <p>たとえば、ユーザが Google Talk や Yahoo Instant Messenger などの特定のアプリケーションタイプを起動しようとしたが、特定のポリシーが適用されているために、ブロックアクションがトリガーされたとします。このアプリケーションは、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。</p>
[一致したアプリケーションタイプ (Application Types Matched) ]	<p>[一致したアプリケーションタイプ (Application Types Matched) ] インタラクティブテーブルでは、[総トランザクション数の上位アプリケーションタイプ (Top Applications Type by Total Transactions) ] テーブルに表示されているアプリケーションタイプに関するさらに詳しい情報を表示できます。</p> <p>[アプリケーション (Applications) ] カラムで、詳細を表示するアプリケーションをクリックできます。</p>
[一致したアプリケーション (Applications Matched) ]	<p>[一致したアプリケーション (Applications Matched) ] インタラクティブテーブルには、指定した時間範囲内のすべてのアプリケーションが表示されます。</p> <p>さらに、[一致したアプリケーション (Application Matched) ] セクション内で特定のアプリケーションを検索できます。このセクション下部のテキストフィールドに特定のアプリケーション名を入力し、[アプリケーションの検索 (Find Application) ] をクリックします。</p>



(注) このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196 ページ\)](#) を参照してください。

## [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] ページ

[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor Page) ] レポート ページには、指定した時間範囲内にレイヤ4トラフィック モニタによってお使いの Web セキュリティアプライアンス

ス上で検出されたマルウェア ポートとマルウェア サイトに関する情報が表示されます。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

[Webサイト (Web Sites)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)]** > **[Webサイト (Web Sites)]** を選択します。詳細については、[インタラクティブレポートページの使用 \(41 ページ\)](#) を参照してください。

レイヤ 4 トラフィック モニタは、Web セキュリティ アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名および IP アドレスを独自のデータベーステーブルのエントリと照合して、着信トラフィックおよび発信トラフィックを許可するかどうかを決定します。

このレポートのデータを使用して、ポートまたはサイトをブロックするかどうかを判断したり、特定のクライアント IP アドレスが著しく頻繁にマルウェアサイトに接続している理由 (たとえば、その IP アドレスに関連付けられたコンピュータが、中央のコマンド/コントロール サーバに接続しようとするマルウェアに感染しているなど) を調査したりできます。

表 54: [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
上位クライアントIP: 検出されたマルウェア接続 (Top Client IPs: Malware Connections Detected)	組織内で最も頻繁にマルウェアサイトに接続している上位のコンピュータの IP アドレスがグラフ形式で表示されます。  グラフの表示をカスタマイズするには、グラフ上の <input checked="" type="checkbox"/> をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。  このグラフは、 <a href="#">[クライアントマルウェアリスク (Client Malware Risk)] レポート (267 ページ)</a> の [レイヤ4トラフィックモニタ: 検出されたマルウェア接続 (Layer 4 Traffic Monitor: Malware Connections Detected)] グラフと同じです。
上位マルウェアサイト: 検出されたマルウェア接続 (Top Malware Sites: Malware Connections Detected)	レイヤ 4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。  グラフの表示をカスタマイズするには、グラフ上の <input checked="" type="checkbox"/> をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。

セクション	説明
[クライアントソースIP (Client Source Ips) ]	<p>このインタラクティブテーブルを使用すると、組織内でマルウェアサイトに頻繁に接続しているコンピュータの IP アドレスを表示できます。</p> <p>特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[クライアントIPによるフィルタ (Filter by Client IP) ] をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェアサイトへ「誘導」しているかを判断できます。</p> <p>各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリをクリックします。たとえば、ある特定のクライアント IP アドレスの [ブロックされたマルウェア接続 (Malware Connections Blocked) ] が高い数値を示している場合、その列の数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[Webトラッキング検索 (Web Tracking Search) ] ページの [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] タブに検索結果として表示されます。リストの詳細については、<a href="#">L4トラフィックモニタによって処理されたトランザクションの検索 (284 ページ)</a> を参照してください。</p> <p>このグラフは、[クライアントマルウェアリスク (Client Malware Risk) ] レポート (<a href="#">267 ページ</a>) の [レイヤ4トラフィックモニタ：検出されたマルウェア接続 (Layer 4 Traffic Monitor: Malware Connections Detected) ] グラフと同じです。</p>
[マルウェアポート (Malware Ports) ]	<p>このインタラクティブテーブルを使用すると、レイヤ4トラフィックモニタによって最も頻繁にマルウェアが検出されたポートを表示できます。</p> <p>詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[検出されたマルウェア接続の総数 (Total Malware Connections Detected) ] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[Webトラッキング検索 (Web Tracking Search) ] ページの [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ] タブに検索結果として表示されます。リストの詳細については、<a href="#">L4トラフィックモニタによって処理されたトランザクションの検索 (284 ページ)</a> を参照してください。</p>

セクション	説明
[検出されたマルウェアサイト (Malware Sites Detected) ]	<p>このインタラクティブ テーブルを使用すると、レイヤ 4 トラフィック モニタが最も頻繁にマルウェアを検出したドメインを表示できます。</p> <p>特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ (Filter by Port) ] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。</p> <p>詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続 (Malware Connections Blocked) ] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[Web トラッキング 検索 (Web Tracking Search) ] ページの [レイヤ 4 トラフィック モニタ (Layer 4 Traffic Monitor) ] タブに検索結果として表示されます。リストの詳細については、<a href="#">L4 トラフィック モニタによって処理されたトランザクションの検索 (284 ページ)</a> を参照してください。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Web セキュリティ レポートの使用 \(196 ページ\)](#) を参照してください。

#### 関連項目

[L4 トラフィック モニタ レポートのトラブルシューティング \(297 ページ\)](#)

## [SOCKS プロキシ (SOCKS Proxy) ] ページ

[SOCKS プロキシ (SOCKS Proxy) ] レポート ページでは、SOCKS プロキシを通じて処理されたトランザクションを、宛先およびユーザに関する情報を含めてグラフおよび表の形式で表示できます。

[SOCKS プロキシ (SOCKS Proxy) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [Web] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [SOCKS プロキシ (SOCKS Proxy) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。



**(注)** レポートに表示される宛先は、SOCKS クライアント (通常はブラウザ) が SOCKS プロキシに送信するアドレスです。

SOCKS ポリシー設定を変更するには、『User Guide for AsyncOS for Cisco Web Security Appliances』を参照してください。

表 55: [SOCKSプロキシ (SOCKS Proxy) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
上位SOCKS宛先: トランザクション合計 (Top Destinations for SOCKS: Total Transactions)	SOCKS プロキシによって検出された上位の宛先をグラフ形式で表示できます。  グラフの表示をカスタマイズするには、グラフ上の <input checked="" type="checkbox"/> をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。
上位SOCKSユーザ: マルウェア トランザクション (Top Users for SOCKS: Malware Transactions)	SOCKS プロキシによって検出された上位のユーザをグラフ形式で表示できます。  グラフの表示をカスタマイズするには、グラフ上の <input checked="" type="checkbox"/> をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。
[宛先 (Destinations) ]	このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理された宛先ドメインまたはIPアドレスのリストを表示できます。  特定の宛先のデータのみを含めるには、テーブルの下部のボックスにドメイン名または IP アドレスを入力し、[ドメインまたはIPの検索 (Find Domain or IP) ] をクリックします。
Users	このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理されたユーザまたはIPアドレスのリストを表示できます。  特定のユーザのデータのみを含めるには、テーブルの下部のボックスにユーザ名または IP アドレスを入力し、[ユーザID/クライアントIPアドレスの検索 (Find User ID / Client IP Address) ] をクリックします。





**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

#### 関連項目

[SOCKS プロキシによって処理されるトランザクションの検索 \(285 ページ\)](#)


## [URLカテゴリ (URL Categories)] ページ


[URLカテゴリ (URL Categories)] レポート ページを使用して、システム上のユーザがアクセスしているサイトの URL カテゴリを表示できます。

[URLカテゴリ (URL Categories)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)]** > **[URLカテゴリ (URL Categories)]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[URL カテゴリ (URL Categories)] ページには次の情報が表示されます。

表 56: [URLカテゴリ (URL Categories)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
上位URLカテゴリ：総トランザクション数 (Top URL Categories: Total Transactions)	<p>サイト上でアクセスされた上位URLカテゴリがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p>

セクション	説明
上位URLカテゴリ：ブロックおよび警告されたトランザクション (Top URL Categories: Blocked and Warned Transactions)	トランザクションごとに発生するブロックまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロックアクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。  グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。
[一致したURLカテゴリ (URL Categories Matched) ]	[一致したURLカテゴリ (URL Categories Matched) ] インタラクティブ テーブルには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。  未分類の URL が多数ある場合は、 <a href="#">未分類の URL の削減 (210 ページ)</a> を参照してください。



ヒント このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196 ページ\)](#) を参照してください。

## 未分類の URL の削減

未分類の URL の比率が 15 ~ 20 % を上回る場合は、次のオプションを検討してください。

- 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。これらのトランザクションは、代わりに [URL フィルタリングバイパス (URL Filtering Bypassed) ] 統計情報に含まれるようになります。これを行うには、『AsyncOS for Cisco Web Security Appliances User Guide』でカスタム URL カテゴリについて参照してください。
- 既存またはその他のカテゴリに含めるべきサイトについては、[誤って分類された URL と未分類の URL のレポート \(212 ページ\)](#) を参照してください。

## URL カテゴリ セットの更新とレポート

[URL カテゴリ セットの更新の準備および管理 \(421 ページ\)](#) で説明されているように、セキュリティ管理アプライアンスでは一連の定義済み URL カテゴリが定期的に更新される場合があります。

これらの更新が行われた場合、古いカテゴリのデータは、古すぎて価値がなくなるまで、引き続きレポートと Web トラッキング結果に表示されます。カテゴリ セットの更新後に生成されたレポートデータには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

古いカテゴリと新しいカテゴリの間に重複した箇所がある場合、有効な統計情報を得るために、より注意深くレポート結果を検証する必要があります。たとえば、調査対象のタイム フレーム内に「Instant Messaging」カテゴリと「Web-based Chat」カテゴリが「Chat and Instant Messaging」という 1 つのカテゴリにマージされていた場合、「Instant Messaging」および「Web-based Chat」カテゴリに対応するサイトへのマージ前のアクセスは「Chat and Instant Messaging」の合計数にカウントされません。同様に、インスタント メッセージング サイトまたは Web ベース チャット サイトへのマージ後のアクセスは、「Instant Messaging」または「Web-based Chat」カテゴリの合計数には含まれません。

## [URL カテゴリ (URL Categories)] ページとその他のレポート ページの併用

[URL カテゴリ (URL Categories)] ページと [アプリケーションの表示 (Application Visibility)] ページ (242 ページ) および [ユーザ (Users)] ページ (252 ページ) を併用すると、特定のユーザと、特定のユーザがアクセスしようとしているアプリケーション タイプまたは Web サイトを調査できます。

たとえば、[URL カテゴリ (URL Categories)] ページ (249 ページ) で、サイトからアクセスされたすべての URL カテゴリの詳細を表示する、人事部門向けの概要レポートを生成できます。同じページの [URL カテゴリ (URL Categories)] インタラクティブ テーブルでは、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[ストリーミングメディア (Streaming Media)] カテゴリ リンクをクリックすると、特定の [URL カテゴリ (URL Categories)] レポート ページが表示されます。このページには、ストリーミング メディア サイトにアクセスしている上位ユーザが表示されるだけでなく ([カテゴリ別の総トランザクション上位ユーザ (Top Users by Category for Total Transactions)] セクション)、YouTube.com や QuickPlay.com などのアクセスされたドメインも表示されます ([一致したドメイン (Domains Matched)] インタラクティブ テーブル)。

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているため、そのユーザのアクセス先を正確に確認する必要があります。ここから、[ユーザ (Users)] インタラクティブ テーブルのユーザをクリックすることができます。このアクションにより [ユーザ (Users)] ページ (252 ページ) が表示され、そのユーザのトレンドを確認し、そのユーザの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [完了したトランザクション (Transactions Completed)] リンクをクリックして、Web トラッキングの詳細を表示できます。これにより、[Web トラッキング (Web Tracking)] ページに [Web プロキシ サービスによって処理されたトランザクションの検索 \(279 ページ\)](#) が表示され、ユーザがサイトにアクセスした日付、完全な URL、その URL で費やされた時間などについて、実際の詳細情報を確認できます。

[URL カテゴリ (URL Categories)] ページの他の使用例については、[例 3: アクセス数の多い URL カテゴリの調査 \(652 ページ\)](#) を参照してください。

## 誤って分類された URL と未分類の URL のレポート

誤って分類された URL と未分類の URL について、次の URL で報告できます。

[https://securityhub.cisco.com/web/submit\\_urls](https://securityhub.cisco.com/web/submit_urls)

送信内容は評価され、今後のルール更新への組み込みに活用されます。

送信された URL のステータスを確認するには、このページの [送信したURLのステータス (Status on Submitted URLs)] タブをクリックします。

## [ユーザ (Users)] ページ

[ユーザ (Users)] レポート ページには、各ユーザの Web レポートニング情報を表示できる複数のリンクが表示されます。

[ユーザ (Users)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)]** > **[ユーザ (Users)]** を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

[ユーザ (Users)] ページでは、システム上のユーザ (1 人または複数) がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。





(注) セキュリティ管理アプライアンスがサポートできる Web セキュリティアプライアンス上のユーザの最大数は 500 です。

[ユーザ (Users)] ページには、システム上のユーザに関する次の情報が表示されます。

表 57: [ユーザ (Users)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。

セクション	説明
上位ユーザ：ブロックされたトランザクション (Top Users: Transactions Blocked)	<p>上位ユーザ (IP アドレスまたはユーザ名で表示) と、そのユーザがブロックされたトランザクションの数がグラフ形式で表示されます。レポートを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページまたはスケジュール設定されたレポートでユーザ名を認識不可能にする方法の詳細については、<a href="#">セキュリティ管理アプライアンスでの中央集中型 Web レポートのイネーブル化 (194 ページ)</a> を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。ユーザ名を非表示にするには、<a href="#">Web レポートでのユーザ名の匿名化 (196 ページ)</a> を参照してください。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p>
上位ユーザ：使用帯域幅 (Top Users: Bandwidth Used)	<p>システム上で最も多くの帯域幅を使用している上位ユーザ (IP アドレスまたはユーザ名で表示) がグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p>
ユーザ (Users)	<p>このインタラクティブテーブルを使用すると、特定のユーザ ID またはクライアント IP アドレスを検索できます。[ユーザ (User)] テーブル下部のテキストフィールドに特定のユーザ ID またはクライアント IP アドレスを入力し、[ユーザ ID/クライアント IP アドレスの検索 (Find User ID / Client IP Address)] をクリックします。IP アドレスが正確に一致していなくても結果は返されます。</p> <p>特定のユーザをクリックすると、さらに具体的な情報を得ることができます。詳細については、<a href="#">[ユーザの詳細 (User Details)] ページ (Web レポート) (254 ページ)</a> を参照してください。</p>



(注) クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

## [ユーザの詳細 (User Details)] ページ (Web レポート)


[ユーザの詳細 (User Details)] ページでは、[ユーザ (Users)] レポート ページのインタラクティブ テーブルで指定したユーザに関する具体的な情報を確認できます。


[ユーザの詳細 (User Details)] ページでは、システムでの個々のユーザのアクティビティを調査できます。特に、ユーザレベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。

特定のユーザの [ユーザの詳細 (User Details)] ページを表示するには、[ユーザ (Users)] レポート ページの [ユーザ (Users)] インタラクティブ テーブルでそのユーザをクリックします。

[ユーザの詳細 (User Details)] ページには、システム上の個々のユーザに関する次の情報が表示されます。

表 58: [ユーザの詳細 (User Details)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
URL カテゴリ : トランザクション 合計 (URL Categories: Total Transactions)	<p>特定のユーザが使用している特定の URL カテゴリがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URL カテゴリ セットの更新とレポート (211 ページ)</a> を参照してください。</p>

セクション	説明
<p>トレンド: トランザクション合計 (Trend: Total Transactions)</p>	<p>このトレンドグラフを使用すると、特定のユーザのすべての Web トランザクションを表示できます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。</p> <p>たとえば、1日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。[時間範囲 (Time Range)] ドロップダウンリストを使用すると、このグラフを拡張し、このユーザが Web を閲覧していた時間を表示するきめ細かさを増減できます。</p>
<p>[一致したURLカテゴリ (URL Categories Matched)]</p>	<p>[一致したURLカテゴリ (URL Categories Matched)] インタラクティブテーブルは、完了したトランザクションとブロックされたトランザクションの両方について、一致したカテゴリが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して [URLカテゴリの検索 (Find URL Category)] をクリックすると、特定の URL カテゴリを検索できます。カテゴリは正確に一致している必要はありません。</p> <p>すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、<a href="#">URLカテゴリセットの更新とレポート (211 ページ)</a> を参照してください。</p>
<p>[一致したドメイン (Domains Matched)]</p>	<p>[一致したドメイン (Domains Matched)] インタラクティブテーブルは、ユーザがアクセスしたドメインまたは IP アドレスを示します。また、ユーザがこれらのカテゴリで費やした時間、およびカラム ビューで設定したその他のさまざまな情報も参照できます。</p> <p>テーブル下部のテキストフィールドに入力して [ドメインまたはIPの検索 (Find Domain or IP)] をクリックすると、特定のドメインまたは IP アドレスを検索できます。ドメインまたは IP アドレスは正確に一致している必要はありません。</p>

セクション	説明
[一致したアプリケーション (Applications Matched) ]	<p>[一致したアプリケーション (Applications Matched) ] インタラクティブ テーブルには、特定のユーザが使用しているアプリケーションが表示されます。たとえば、Flash ビデオを多用するサイトにユーザがアクセスしている場合は、[アプリケーション (Application) ] 列にそのアプリケーション タイプが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して [アプリケーションの検索 (Find Application) ] をクリックすると、特定のアプリケーション名を検索できます。アプリケーションの名前は正確に一致している必要はありません。</p>
Advanced Malware Protectionで検出された脅威 (Advanced Malware Protection Threats Detected)	<p>[Advance Malware Protectionで検出された脅威 (Advanced Malware Protection Threats Detected) ] インタラクティブ テーブルには、Advanced Malware Protection エンジンによって検出されたマルウェア脅威ファイルが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して [マルウェア脅威ファイルSHA 256の検索 (Find malware Threat File SHA 256) ] をクリックすると、マルウェア脅威ファイルの特定の SHA 値に関するデータを検索できます。アプリケーションの名前は正確に一致している必要はありません。</p>
[検出されたマルウェア脅威 (Malware Threats Detected) ]	<p>[検出されたマルウェア脅威 (Malware Threats Detected) ] インタラクティブ テーブルには、特定のユーザによってトリガーされた上位のマルウェア脅威が表示されます。</p> <p>テーブル下部のテキストフィールドに入力して [マルウェア脅威の検索 (Find Malware Threat) ] をクリックすると、特定のマルウェア脅威名に関するデータを検索できます。マルウェア脅威の名前は正確に一致している必要はありません。</p>
[一致したポリシー (Policies Matched) ]	<p>[一致したポリシー (Policies Matched) ] インタラクティブ テーブルには、Web へのアクセス時にこのユーザに適用されたポリシー グループが表示されます。</p> <p>テーブル下部のテキストフィールドに入力して [ポリシー検索 (Find Policy) ] をクリックすると、特定のポリシー名を検索できます。ポリシーの名前は正確に一致している必要はありません。</p>





- (注) [クライアントマルウェアリスクの詳細 (Client Malware Risk Details)] テーブルのクライアントレポートでは、ユーザ名の末尾にアスタリスク (\*) が付いていることがあります。たとえば、クライアントレポートに「jsmith」と「jsmith\*」の両方のエントリが表示される場合があります。アスタリスク (\*) が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。


## [Webサイト (Web Sites)] ページ

[Webサイト (Web Sites)] レポート ページは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このレポート ページを使用すると、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタすることができます。

[Webサイト (Web Sites)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから **[モニタリング (Monitoring)]** > **[Webサイト (Web Sites)]** を選択します。詳細については、[インタラクティブレポート ページの使用 \(41 ページ\)](#) を参照してください。

[Webサイト (Web Sites)] ページには次の情報が表示されます。

表 59: [Webサイト (Web Sites)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
上位ドメイン: トランザクション合計 (Top Domains: Total Transactions)	Web サイト上でアクセスされた上位のドメインがグラフ形式で表示されます。  グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、 <a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。

セクション	説明
上位ドメイン：ブロックされたトランザクション (Top Domains: Transactions Blocked)	<p>トランザクションごとに発生するブロックアクションをトリガーした上位ドメインが、グラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の <input checked="" type="checkbox"/> をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p> <p>たとえば、ユーザがあるドメインにアクセスしたが、特定のポリシーが適用されていたために、ブロックアクションがトリガーされたとします。このドメインはブロックされたトランザクションとしてこのグラフに追加され、ブロックアクションをトリガーしたドメインサイトが表示されます。</p>
[一致したドメイン (Domains Matched)]	<p>このインタラクティブ テーブルでは、Web サイト上でアクセスされたドメインを検索できます。特定のドメインをクリックすると、より詳細な情報を得ることができます。[Web トラッキング (Web Tracking)] ページに [プロキシサービス (Proxy Services)] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。</p> <p>特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。</p> <p>Web トラッキングの使用例については、<a href="#">例 2 : URL のトラッキング (651 ページ)</a> を参照してください。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Web セキュリティレポートの使用 \(196 ページ\)](#) を参照してください。

## [HTTPSレポート (HTTPS Reports)] ページ

[HTTPSレポート (HTTPS Reports)] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー (トランザクションまたは帯域幅の使用量) のすべてを集約しています。

また、管理対象のアプライアンスを通過する個々の HTTP/HTTPS Web トラフィックの場合、クライアント側接続またはサーバ側接続のいずれかに基づいてサポート対象の暗号のサマリーを確認することもできます。

[HTTPSレポート (HTTPS Reports)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング]

(Monitoring) ]> [HTTPSレポート (HTTPS Reports) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

表 60: [HTTPSレポート (HTTPS Reports) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[Webトラフィックサマリー (Web Traffic Summary) ]	<p>アプライアンスの Web トラフィック サマリーは、次のいずれかの方法で表示できます。</p> <ul style="list-style-type: none"> <li>• <b>トランザクション</b> : グラフ形式の HTTP または HTTPS Web トランザクションの数と表形式の HTTP または HTTPS Web トランザクションの割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。</li> <li>• <b>帯域幅の使用量</b> : グラフ形式の HTTP または HTTPS Web トラフィックで消費される帯域幅の大きさと表形式の HTTP または HTTPS 帯域幅の使用量の割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。</li> </ul>
トレンド : Web トラフィック	<p>次のいずれかの方法に必要な時間範囲に基づいてアプライアンスの Web トラフィックのトレンドグラフを表示することができます。</p> <ul style="list-style-type: none"> <li>• <b>Web トラフィックトレンド</b> : トランザクションまたは帯域幅の使用量に基づいて HTTP と HTTPS Web トラフィックの累積トレンドを表示するには、ドロップダウン リストからこのオプションを選択します。</li> <li>• <b>HTTPSトレンド</b> : トランザクションまたは帯域幅の使用量に基づいて HTTPS Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。</li> <li>• <b>HTTPトレンド</b> : トランザクションまたは帯域幅の使用量に基づいて HTTP Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。</li> </ul>

セクション	説明
暗号	<p>暗号のサマリーは、次のいずれかの方法で表示できます。</p> <ul style="list-style-type: none"> <li>クライアント側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのクライアント側で使用される暗号のサマリーを表示するには、ドロップダウンリストからこのオプションを選択します。</li> <li>サーバ側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのサーバ側で使用される暗号のサマリーを表示するには、ドロップダウンリストからこのオプションを選択します。</li> </ul>

## [マルウェア対策 (Anti-Malware) ] ページ

[マルウェア対策 (Anti-Malware) ] レポート ページはセキュリティ関連のレポートینگ ページであり、イネーブルなスキャンエンジン (Webroot、Sophos、McAfee、または Adaptive Scanning) によるスキャン結果が反映されます。

[マルウェア対策 (Anti-Malware) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [Web] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [マルウェア対策 (Anti-Malware) ] を選択します。詳細については、[インタラクティブ レポート ページの使用 \(41 ページ\)](#) を参照してください。

このページを使用して、Web ベースのマルウェアの脅威を特定およびモニタすることができます。





(注) L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、次を参照してください。[\[レイヤ4トラフィックモニタ \(Layer 4 Traffic Monitor\) \] ページ \(244 ページ\)](#)

[マルウェア対策 (Anti-Malware) ] ページには次の情報が表示されます。

表 61: [マルウェア対策 (Anti-Malware) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウン リスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。

セクション	説明
上位マルウェアカテゴリ (Top Malware Categories)	<p>特定のカテゴリ タイプによって検出された上位のマルウェアカテゴリをグラフ形式で表示できます。有効なマルウェアカテゴリの詳細については、<a href="#">マルウェアのカテゴリについて (216 ページ)</a> を参照してください。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p>
上位マルウェア脅威 (Top Malware Threats)	<p>上位のマルウェア脅威をグラフ形式で表示できます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p>
[マルウェアカテゴリ (Malware Categories) ]	<p>[マルウェアカテゴリ (Malware Categories) ] インタラクティブテーブルには、[上位マルウェアカテゴリ (Top Malware Categories) ] チャートに表示されている個々のマルウェアカテゴリに関する詳細情報が表示されます。</p> <p>[マルウェアカテゴリ (Malware Categories) ] インタラクティブテーブル内のリンクをクリックすると、個々のマルウェアカテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。</p> <p>例外：このテーブルの [アウトブレイクヒューリスティック (Outbreak Heuristics) ] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。</p> <p>有効なマルウェアカテゴリの詳細については、<a href="#">マルウェアのカテゴリについて (216 ページ)</a> を参照してください。</p>
[マルウェア脅威 (Malware Threats) ]	<p>[マルウェアの脅威 (Malware Threats) ] インタラクティブテーブルには、[上位マルウェア脅威 (Top Malware Threats) ] セクションに表示されている個々のマルウェアの脅威に関する詳細情報が表示されます。</p> <p>「アウトブレイク (Outbreak) 」のラベルと番号が付いている脅威は、他のスキャンエンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

## [マルウェアのカテゴリ (Malware Category) ]レポート

[マルウェアのカテゴリ (Malware Category) ]レポート ページでは、個々のマルウェア カテゴリとネットワークでのその動作に関する詳細情報を表示できます。

[マルウェアのカテゴリ (Malware Category) ]レポート ページにアクセスするには、次の手順を実行します。

- ステップ 1** セキュリティ管理アプライアンスで、ドロップダウン リストから **[ウェブ (Web) ]** を選択します。
- ステップ 2** **[モニタリング (Monitoring) ] > [マルウェア対策 (Anti-Malware) ]** ページを選択します。
- ステップ 3** [マルウェアカテゴリ (Malware Categories) ] インタラクティブテーブルで、[マルウェアのカテゴリ (Malware Category) ] 列内のカテゴリをクリックします。
- ステップ 4** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196ページ\)](#) を参照してください。

## [マルウェアの脅威 (Malware Threat) ]レポート

[マルウェア脅威 (Malware Threats) ]レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[クライアントの詳細 (Client Detail) ] ページへのリンクがあります。レポート上部のトレンドグラフには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

このレポートを表示するには、[マルウェア対策 (Anti-Malware) ] レポート ページの [マルウェアのカテゴリ (Malware Category) ] 列でカテゴリをクリックします。

詳細については、テーブルの下の [サポートポータルマルウェア詳細 (Support Portal Malware Details) ] リンクをクリックしてください。

## マルウェアのカテゴリについて

Web セキュリティ アプライアンスは次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザーを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェアアプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザーがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザヘルパーオブジェクト	ブラウザヘルパーオブジェクトは、広告の表示やユーザー設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザプラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザーの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザーを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザーに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザーの完全で有効な承諾なしにユーザーを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザーのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、 <b>Adaptive Scanning</b> によって検出されたマルウェアを示しています。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。

マルウェアのタイプ	説明
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。  公然と、または密かに、システムプロセスやユーザアクションを記録する。  これらの記録を後で取得して確認できるようにする。
トロイのダウンロード	トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンロードはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークションサイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

## [高度なマルウェア防御 (Advanced Malware Protection) ] ページ

高度なマルウェア防御は、次のようにして、ゼロデイ攻撃やファイルベースの標的型脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザ ガイドまたは Web セキュリティ アプライアンスの AsyncOS のオンライン ヘルプを参照してください。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [Web] を選択し、[レポート (Reports) ] ドロップダウンから



ら [モニタリング (Monitoring) ] > [高度なマルウェア防御 (Advanced Malware Protection) ] を選択します。詳細については、[インタラクティブレポート ページの使用 \(41 ページ\)](#) を参照してください。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページには、次のレポート ビューが表示されます。

- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] : \[AMPサマリー \(AMP Summary\) \] \(265 ページ\)](#)
- [\[高度なマルウェア防御 \(Advanced Malware Protection\) \] : \[ファイル分析 \(File Analysis\) \] \(266 ページ\)](#)

#### 関連項目

- [ファイル分析レポートの詳細の要件 \(219 ページ\)](#)
- [SHA-256 ハッシュによるファイルの識別 \(221 ページ\)](#)
- [その他のレポートでのファイルレピュテーションフィルタデータの表示 \(224 ページ\)](#)
- [Web トラッキング機能および高度なマルウェア防御機能について \(293 ページ\)](#)

## [高度なマルウェア防御 (Advanced Malware Protection) ] : [AMPサマリー (AMP Summary) ]

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページの [AMPサマリー (AMP Summary) ] セクションには、ファイルレピュテーションサービスによって識別された、ファイルベースの脅威が表示されます。

各 SHA にアクセスしようとしたユーザ、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。

[マルウェア脅威ファイル (Malware Threat File) ] インタラクティブ テーブルのリンクをクリックすると、レポートに対して選択された時間範囲に関係なく、設定可能な最大時間範囲内で検出されたそのファイルのすべてのインスタンスが [Web トラッキング (Web Tracking) ] に表示されます。

圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御 (Advanced Malware Protection) ] レポートに含まれます。

[高度なマルウェア防御 (Advanced Malware Protection) ] ページの [AMPサマリー (AMP Summary) ] セクションには、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイルレピュテーションサービスによって識別されたファイルの概要 (グラフ形式)。
- 上位のマルウェア脅威ファイル (グラフ形式)。
- ファイルタイプに基づいた上位の脅威ファイル (グラフ形式)。
- 選択した時間範囲のすべてのマルウェア脅威ファイルに関するトレンドグラフ。

- 上位のマルウェア脅威ファイルを一覧表示する [マルウェア脅威ファイル (Malware Threat Files) ] インタラクティブ テーブル。
- このアプライアンスで処理され、トランザクションの処理後に判定が変わったファイルを一覧表示する [レトロスペクティブ判定変更 (Retrospective Verdict Change) ] インタラクティブ テーブルを含むファイル。この状況の詳細については、お使いの Web セキュリティ アプライアンスのマニュアルを参照してください。

1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。

複数の Web Security Appliances で同じファイルの判定アップデートが異なる場合、最新のタイム スタンプが付いた結果が表示されます。

SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内にこの SHA-256 が含まれた、すべてのトランザクションの Web トラッキング結果が表示されます。

## [高度なマルウェア防御 (Advanced Malware Protection) ] : [ファイル分析 (File Analysis) ]

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページの [ファイル分析 (File Analysis) ] セクションには、分析のために送信された各ファイルについて、時刻と判定 (または中間判定) が表示されます。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。

オンプレミスの Cisco AMP Threat Grid Appliance での導入の場合 : Cisco AMP Threat Grid Appliance でホワイトリストに登録されているファイルは、「クリーン」として表示されます。ホワイトリストについては、AMP Threat Grid のオンラインヘルプを参照してください。

ドリルダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。

また、分析を実行したサーバで SHA に関する追加の詳細を直接表示するには、SHA を検索するか、またはファイル分析の詳細ページ下部にある Cisco AMP Threat Grid リンクをクリックします。

ファイルを分析したサーバに関する詳細を表示するには、[ファイル分析レポートの詳細の要件 \(219 ページ\)](#) を参照してください。

圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析 (File Analysis) ] レポートに含まれます。

[高度なマルウェア防御 (Advanced Malware Protection) ] レポート ページの [ファイル分析 (File Analysis) ] セクションを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル分析サービスによってファイル分析のためにアップロードされたファイルの数。
- ファイル分析要求が完了しているファイルのリスト。
- ファイル分析要求の処理待ちとなっているファイルのリスト。

## [クライアントマルウェアリスク (Client Malware Risk)] レポート

[クライアントマルウェアリスク (Client Malware Risk)] レポート ページは、クライアントマルウェアリスク アクティビティのモニタに使用できる、セキュリティ関連のレポートページです。


[クライアントマルウェアリスク (Client Malware Risk)] レポート ページを表示するには、[製品 (Product)] ドロップダウンから [Web] を選択し、[レポート (Reports)] ドロップダウンから [モニタリング (Monitoring)] > [クライアントマルウェアリスク (Client Malware Risk)] を選択します。詳細については、[インタラクティブレポートページの使用 \(41 ページ\)](#) を参照してください。

[クライアントマルウェアリスク (Client Malware Risk)] レポート ページでは、システム管理者が最も多くブロックまたは警告を受けているユーザを確認できます。このページで収集された情報から、管理者はユーザリンクをクリックして、そのユーザが多数のブロックや警告を受けている原因、およびネットワーク上の他のユーザよりも多く検出されている原因となっているユーザの行動を確認できます。

さらに [クライアントマルウェアリスク (Client Malware Risk)] ページには、L4 トラフィック モニタ (L4TM) によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。マルウェア サイトに頻繁に接続するコンピュータは、マルウェアに感染している可能性があります。これらのマルウェアは中央のコマンド/コントロールサーバに接続しようとするので、除去しなければなりません。

次の表で、[クライアントマルウェアリスク (Client Malware Risk)] ページの情報について説明します。

表 62: [クライアントマルウェアリスク (Client Malware Risk)] ページの詳細

セクション	説明
[時間範囲 (Time Range)] (ドロップダウンリスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[Webプロキシ: モニタまたはブロックされた上位クライアント (Web Proxy: Top Clients Monitored or Blocked)]	マルウェアリスクが発生している上位 10 ユーザがグラフ形式で表示されます。  グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、 <a href="#">(Webレポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。

セクション	説明
L4トラフィックモニタ:検出されたマルウェア接続 (L4 Traffic Monitor: Malware Connections Detected)	<p>組織内で最も頻繁にマルウェアサイトに接続している上位 10 台のコンピュータの IP アドレスがグラフ形式で表示されます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p> <p>このチャートは<a href="#">[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ]ページ (244 ページ)</a> の<a href="#">[上位クライアントIP (Top Client IPs) ]チャート</a>と同じです。</p>
[Webプロキシ:クライアントマルウェアリスク (Web Proxy: Client Malware Risk) ]	<p>[Webプロキシ: クライアントマルウェアリスク (Web Proxy: Client Malware Risk) ]インタラクティブテーブルには、[Webプロキシ: マルウェアリスク別上位クライアント (Web Proxy: Top Clients by Malware Risk) ]セクションに表示されている個々のクライアントに関する詳細情報が表示されます。</p> <p>このテーブルで各ユーザをクリックすると、そのクライアントに関連する<a href="#">[ユーザの詳細 (User Details) ]ページ</a>が表示されます。このページの詳細については、<a href="#">[ユーザの詳細 (User Details) ]ページ (Web レポートニング) (254 ページ)</a> を参照してください。</p> <p>テーブルで任意のリンクをクリックすると、個々のユーザと、マルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。</p>
L4トラフィックモニタ:マルウェアリスク別クライアント (L4 Traffic Monitor: Clients by Malware Risk)	<p>[L4トラフィックモニタ: マルウェアリスク別クライアント (L4 Traffic Monitor: Clients by Malware Risk) ]インタラクティブテーブルには、組織内でマルウェアサイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。</p> <p>このテーブルは<a href="#">[レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor) ]ページ (244 ページ)</a> の<a href="#">[クライアントソースIP (Client Source IPs) ]テーブル</a>と同じです。</p>



**ヒント** このレポートのビューをカスタマイズするには、[Webセキュリティレポートの使用 \(196 ページ\)](#) を参照してください。

## [Web レピュテーションフィルタ (Web Reputation Filters) ] ページ

[Web レピュテーションフィルタ (Web Reputation Filters) ] レポート ページでは、指定した時間範囲内のトランザクションに対する Web レピュテーションフィルタ (ユーザが設定) の結果を確認できます。

[Web レピュテーションフィルタ (Web Reputation Filters) ] レポート ページを表示するには、[製品 (Product) ] ドロップダウンから [Web] を選択し、[レポート (Reports) ] ドロップダウンから [モニタリング (Monitoring) ] > [Web レピュテーションフィルタ (Web Reputation Filters) ] を選択します。詳細については、[インタラクティブレポート ページの使用 \(41 ページ\)](#) を参照してください。

### Web レピュテーションフィルタとは

Web レピュテーションフィルタは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーションスコアを URL に割り当てます。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらす URL ベースのマルウェアを防ぐために役立ちます。Web セキュリティ アプライアンスは、URL レピュテーションスコアを使用して、疑わしいアクティビティを特定するとともに、マルウェア攻撃を未然に防ぎます。Web レピュテーションフィルタは、アクセス ポリシーと復号ポリシーの両方と組み合わせ使用できます。

Web レピュテーションフィルタでは、統計データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ~ +10 の Web レピュテーションスコアにマッピングされます (+10 がマルウェアを含む可能性が最も低い)。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書 (EULA) の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在


- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

Web レピュテーションフィルタの詳細については、『User Guide for AsyncOS for Web Security Appliances』の「Web Reputation Filters」を参照してください。

[Web レピュテーションフィルタ (Web Reputation Filters) ] ページには次の情報が表示されません。

表 63: [Web レピュテーションフィルタ (Web Reputation Filters) ] ページの詳細

セクション	説明
[時間範囲 (Time Range) ] (ドロップダウンリスト)	レポートの時間範囲を選択します。詳細については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
[Web レピュテーションアクション(トレンド) (Web Reputation Actions (Trend)) ]	指定した時間における Web レピュテーションアクションの合計数をグラフ形式で表示できます。このセクションでは、時間の経過に伴う Web レピュテーションアクションの潜在的なトレンドを確認できます。
[Web レピュテーションアクション(ボリューム) (Web Reputation Actions (Volume)) ]	Web レピュテーションアクションのボリュームをトランザクション数の比率で表示できます。
[WBRISによってブロックされる Web レピュテーションの脅威タイプ (Web Reputation Threat Types Blocked by WBRIS) ]	Web レピュテーションフィルタリングによってブロックされたトランザクションで発生した脅威のタイプをグラフ形式で表示できます。  (注) WBRIS では、常に、脅威のタイプを識別できるわけではありません。

セクション	説明
[他のトランザクションで脅威タイプが検知されました (Threat Types Detected in Other Transactions) ]	<p>Web レピュテーションフィルタリングによってブロックされなかったトランザクションで発生した脅威のタイプをグラフ形式で表示できます。</p> <p>グラフの表示をカスタマイズするには、グラフ上の  をクリックします。詳細については、<a href="#">(Web レポートのみ) チャート化するデータの選択 (44 ページ)</a> を参照してください。</p> <p>これらの脅威がブロックされなかった理由には、次のようなものがあります。</p> <ul style="list-style-type: none"> <li>• すべての脅威に、ブロッキングのしきい値を満たすスコアがあるわけではありません。ただし、アプライアンスのその他の機能は、これらの脅威を検出する可能性があります。</li> <li>• ポリシーが、脅威を許可するよう設定されている可能性があります。</li> </ul> <p>(注) WBRs では、常に、脅威のタイプを識別できるわけではありません。</p>
Web レピュテーションアクション (スコアによる内訳) (Web Reputation Actions (Breakdown by Score))	Adaptive Scanning がイネーブルでない場合、このインタラクティブ テーブルには各アクションの Web レピュテーションスコアの内訳が表示されます。



**ヒント** このレポートのビューをカスタマイズするには、[Web セキュリティ レポートの使用 \(196 ページ\)](#) を参照してください。

### Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーション設定の詳細については、『*User Guide for AsyncOS for Cisco Web Security Appliances*』を参照してください。

# スケジュール設定されたレポートとオンデマンド Web レポートについて

特記のない限り、次のタイプの Web セキュリティ レポートを、スケジュール設定されたレポートまたはオンデマンド レポートとして作成できます。

- [Web レポートिंगの概要 (Web Reporting Overview)] : このページに表示される情報については、[Web レポートの概要 \(202 ページ\)](#) を参照してください。
- [ユーザ (Users)] : このページに表示される情報については、[ユーザ \(Users\) \] レポート \(Web\) \(204 ページ\)](#) を参照してください。
- [Web サイト (Web Sites)] : このページに表示される情報については、[Web サイト \(Web Sites\) \] レポート \(208 ページ\)](#) を参照してください。
- [URL カテゴリ (URL Categories)] : このページに表示される情報については、[URL カテゴリ \(URL Categories\) \] レポート \(209 ページ\)](#) を参照してください。
- [上位 URL カテゴリ - 拡張 (Top URL Categories — Extended)] : [上位 URL カテゴリ - 拡張 (Top URL Categories — Extended)] のレポートを生成する方法については、[上位 URL カテゴリ - 拡張 \(Top URL Categories — Extended\) \(275 ページ\)](#) を参照してください。

このレポートをオンデマンド レポートとして使用することはできません。

- [アプリケーションの表示 (Application Visibility)] : このページに表示される情報については、[アプリケーションの表示 \(Application Visibility\) \] レポート \(212 ページ\)](#) を参照してください。
- [上位アプリケーションタイプ - 拡張 (Top Application Types — Extended)] : [上位アプリケーションタイプ - 拡張 (Top Application Types — Extended)] のレポートを生成する方法については、[上位アプリケーションタイプ - 拡張 \(Top Application Types — Extended\) \(276 ページ\)](#) を参照してください。

このレポートをオンデマンド レポートとして使用することはできません。

- [マルウェア対策 (Anti-Malware)] : このページに表示される情報については、[マルウェア対策 \(Anti-Malware\) \] レポート \(214 ページ\)](#) を参照してください。
- [クライアントマルウェアリスク (Client Malware Risk)] : このページに表示される情報については、[クライアントマルウェアリスク \(Client Malware Risk\) \] レポート \(224 ページ\)](#) を参照してください。
- [Web レピュテーションフィルタ (Web Reputation Filters)] : このページに表示される情報については、[Web レピュテーションフィルタ \(Web Reputation Filters\) \] レポート \(226 ページ\)](#) を参照してください。
- [L4 トラフィックモニタ (L4 Traffic Monitor)] : このページに表示される情報については、[L4 トラフィック モニタ \(L4 Traffic Monitor\) \] レポート \(228 ページ\)](#) を参照してください。
- [モバイルセキュアソリューション (Mobile Secure Solution)] : このページに表示される情報については、[ユーザの場所別レポート \(Reports by User Location\) \(232 ページ\)](#) を参照してください。



- [システム容量 (System Capacity) ]: このページに表示される情報については、[\[システム容量 \(System Capacity\) \] ページ \(233 ページ\)](#) を参照してください。

## Web レポートのスケジュール設定

このセクションの内容は次のとおりです。

- [スケジュール設定された Web レポートの追加 \(274 ページ\)](#)
- [スケジュール設定された Web レポートの編集 \(274 ページ\)](#)
- [スケジュール設定された Web レポートの削除 \(275 ページ\)](#)
- [追加の拡張 Web レポート \(275 ページ\)](#)



- (注) すべてのレポートで、ユーザ名を認識できないようにすることができます。詳細については、[Web レポートでのユーザ名の匿名化 \(196 ページ\)](#) を参照してください。

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日 (最大 250 日)、過去の月 (最大 12 ヶ月) のデータを含めるように設定できます。また、指定した日数 (2 ~ 100 日) または指定した月数 (2 ~ 12 ヶ月) のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔 (過去 1 時間、1 日、1 週間、または 1 ヶ月) のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

必要に応じた数 (ゼロも含む) のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリングリストを作成するほうが容易です。

## スケジュール設定された Web レポートの保存

セキュリティ管理アプライアンスでは、スケジュール設定された各レポートの最大 30 の最新インスタンスで、生成された最新のレポートをすべてのレポートに対して、合計 1000 バージョンまで保持します。

アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。30 インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

アーカイブ済みのレポートは、アプライアンスの /periodic\_reports ディレクトリに保管されます。(詳細については、[IP インターフェイスおよびアプライアンスへのアクセス \(631 ページ\)](#) を参照してください)。

### 関連項目

- [アーカイブ済みの Web レポートの表示と管理 \(278 ページ\)](#)

## スケジュール設定された Web レポートの追加

- ステップ 1** セキュリティ管理アプライアンスで、[Web]>[レポート (Reporting)]>[スケジュール設定されたレポート (Scheduled Reports)] を選択します。
- ステップ 2** [定期レポートの追加 (Add Scheduled Report)] をクリックします。
- ステップ 3** [タイプ (Type)] の横のドロップダウンメニューから、レポートタイプを選択します。
- ステップ 4** [タイトル (Title)] フィールドに、レポートのタイトルを入力します。  
同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを推奨します。
- ステップ 5** [時間範囲 (Time Range)] ドロップダウンメニューから、レポートの時間範囲を選択します。
- ステップ 6** 生成されるレポートの形式を選択します。  
デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。
- ステップ 7** [アイテム数 (Number of Items)] の横のドロップダウンリストから、生成されるレポートに出力する項目の数を選択します。  
有効な値は 2 ~ 20 です。デフォルト値は 5 です。
- ステップ 8** [チャート (Charts)] では、[表示するデータ (Data to display)] の下のデフォルトチャートをクリックし、レポートの各チャートに表示するデータを選択します。
- ステップ 9** [ソート列 (Sort Column)] の横のドロップダウンリストから、このレポートでデータをソートするための列を選択します。これにより、スケジュール設定されたレポート内の任意の列を基準とする上位「N」個の項目のレポートを作成できます。
- ステップ 10** [スケジュール (Schedule)] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプションボタンを選択します。
- ステップ 11** [メール (Email)] テキストフィールドに、生成されたレポートが送信される電子メールアドレスを入力します。  
電子メールアドレスを指定しなかった場合は、レポートのアーカイブのみが行われます。
- ステップ 12** [送信 (Submit)] をクリックします。

## スケジュール設定された Web レポートの編集

レポートを編集するには、[ウェブ (Web)]>[レポート (Reporting)]>[スケジュール設定されたレポート (Scheduled Reports)] ページに移動し、編集するレポートに対応するチェックボックスをオンにします。設定を変更し、[送信 (Submit)] をクリックしてページでの変更を送信し、[変更を確定 (Commit Changes)] ボタンをクリックしてアプライアンスへの変更を確定します。

## スケジュール設定された Web レポートの削除

レポートを削除するには、[ウェブ (Web)] > [レポート (Reporting)] > [スケジュール設定されたレポート (Scheduled Reports)] ページに移動し、削除するレポートに対応するチェックボックスをオンにします。スケジュール設定されたレポートをすべて削除する場合は、[すべて (All)] チェックボックスを選択し、**削除**を実行して変更を**確定**します。削除されたレポートのアーカイブ版は削除されません。

## 追加の拡張 Web レポート

さらに2種類のレポートを、スケジュール設定されたレポートとしてのみセキュリティ管理アプライアンスで使用することができます。

- [上位URLカテゴリ - 拡張 \(Top URL Categories — Extended\)](#) (275 ページ)
- [上位アプリケーションタイプ - 拡張 \(Top Application Types — Extended\)](#) (276 ページ)

## 上位URLカテゴリ - 拡張 (Top URL Categories — Extended)

[上位URLカテゴリ - 拡張 (Top URL Categories — Extended)] レポートは、管理者が [URLカテゴリ (URL Categories)] レポートよりも詳細な情報を必要とする場合に役立ちます。

たとえば、通常の [URLカテゴリ (URL Categories)] レポートでは、大きい URL カテゴリ レベルで特定の従業員の帯域幅使用状況を評価する情報を収集できます。各 URL カテゴリの上位 10 個の URL、または各 URL カテゴリの上位 5 人のユーザーについて、帯域幅の使用状況をモニタする詳細なレポートを生成するには、[上位URLカテゴリ - 拡張 (Top URL Categories — Extended)] レポートを使用します。



(注) このタイプのレポートで生成できる最大レポート数は 20 です。

- 定義済みの URL カテゴリ リストは更新されることがあります。こうした更新によるレポート結果への影響については、[URL カテゴリ セットの更新とレポート \(211 ページ\)](#) を参照してください。

[上位URLカテゴリ - 拡張 (Top URL Categories — Extended)] レポートを生成するには、次の手順を実行します。

- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [レポート (Reporting)] > [スケジュール設定されたレポート (Scheduled Reports)] を選択します。
- ステップ 2** [定期レポートの追加 (Add Scheduled Report)] をクリックします。
- ステップ 3** [タイプ (Type)] の横のドロップダウンメニューから、[上位URLカテゴリ - 拡張 (Top URL categories — Extended)] を選択します。
- ステップ 4** [タイトル (Title)] テキストフィールドに、URL 拡張レポートのタイトルを入力します。
- ステップ 5** [時間範囲 (Time Range)] ドロップダウンメニューから、レポートの時間範囲を選択します。

## ■ 上位アプリケーションタイプ - 拡張 (Top Application Types — Extended)

- ステップ 6** 生成されるレポートの形式を選択します。  
デフォルト形式は PDF です。
- ステップ 7** [アイテム数 (Number of Items)] の横のドロップダウンリストから、生成されるレポートに出力する URL カテゴリの数を選択します。  
有効な値は 2 ~ 20 です。デフォルト値は 5 です。
- ステップ 8** [ソート列 (Sort Column)] の横のドロップダウンリストから、このレポートでデータをソートするための列を選択します。これにより、スケジュール設定されたレポート内の任意の列を基準とする上位「N」個の項目のレポートを作成できます。
- ステップ 9** [チャート (Charts)] では、[表示するデータ (Data to display)] の下のデフォルトチャートをクリックし、レポートの各チャートに表示するデータを選択します。
- ステップ 10** [スケジュール (Schedule)] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプションボタンを選択します。
- ステップ 11** [メール (Email)] テキストフィールドに、生成されたレポートが送信される電子メールアドレスを入力します。
- ステップ 12** [送信 (Submit)] をクリックします。

---

## 上位アプリケーションタイプ - 拡張 (Top Application Types — Extended)

[上位アプリケーションタイプ - 拡張 (Top Application Type — Extended)] レポートを生成するには、次の手順を実行します。

- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [レポート (Reporting)] > [スケジュール設定されたレポート (Scheduled Reports)] を選択します。
- ステップ 2** [定期レポートの追加 (Add Scheduled Report)] をクリックします。
- ステップ 3** [タイプ (Type)] の横のドロップダウンメニューから、[上位アプリケーションタイプ - 拡張 (Top Application Types — Extended)] を選択します。  
このページのオプションは変更される場合があります。
- ステップ 4** [タイトル (Title)] テキストフィールドにレポートのタイトルを入力します。
- ステップ 5** [時間範囲 (Time Range)] ドロップダウンメニューから、レポートの時間範囲を選択します。
- ステップ 6** 生成されるレポートの形式を選択します。  
デフォルト形式は PDF です。
- ステップ 7** [アイテム数 (Number of Items)] の横のドロップダウンリストから、生成されたレポートに出力するアプリケーションタイプの数を選択します。  
有効な値は 2 ~ 20 です。デフォルト値は 5 です。

- ステップ 8** [列をソート (Sort Column)] の横のドロップダウンリストから、テーブルに表示する列のタイプを選択します。選択肢は、[完了したトランザクション (Transactions Completed)]、[ブロックされたトランザクション (Transactions Blocked)]、[トランザクション合計 (Transaction Totals)] です。
- ステップ 9** [チャート (Charts)] では、[表示するデータ (Data to display)] の下のデフォルトチャートをクリックし、レポートの各チャートに表示するデータを選択します。
- ステップ 10** [スケジュール (Schedule)] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプションボタンを選択します。
- ステップ 11** [メール (Email)] テキスト フィールドに、生成されたレポートが送信される電子メールアドレスを入力します。
- ステップ 12** [送信 (Submit)] をクリックします。

## オンデマンドでの Web レポートの生成

スケジュールを設定できるレポートのほとんどは、オンデマンドでの生成も可能です。



(注) 一部のレポートは、オンデマンドではなくスケジュール設定されたレポートとしてのみ使用できます。追加の拡張 Web レポート (275 ページ) を参照してください。

レポートをオンデマンドで生成するには、次の手順を実行します

- ステップ 1** セキュリティ管理アプライアンスで、[Web] > [レポート (Reporting)] > [アーカイブレポート (Archived Reports)] を選択します。
- ステップ 2** [今すぐレポートを生成 (Generate Report Now)] をクリックします。
- ステップ 3** [レポートタイプ (Report Type)] セクションで、ドロップダウンリストからレポートタイプを選択します。  
このページのオプションは変更される場合があります。
- ステップ 4** [タイトル (Title)] テキスト フィールドに、レポートのタイトル名を入力します。  
AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前でも複数のレポートを作成しないでください。
- ステップ 5** [含める時間範囲 (Time Range to Include)] ドロップダウンリストから、レポートデータの時間範囲を選択します。
- ステップ 6** [フォーマット (Format)] セクションで、レポートの形式を選択します。  
次のオプションがあります。
- PDF 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー (Preview PDF Report)] をクリックすると、ただちに PDF ファイルでレポートを表示できます。

- CSV. カンマ区切りの値の raw データが含まれる ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

**ステップ 7** レポートで使用可能なオプションに応じて次の項目を選択します。

- [行数 (Number of rows)] : テーブルに表示するデータの行数。
- [チャート (Charts)] : レポートのチャートに表示するデータ。
- [表示するデータ (Data to display)] の下のデフォルト オプションを選択します。
- [列をソート (Sort Column)] : 各テーブルのソート基準となる列。

**ステップ 8** [配信オプション (Delivery Option)] セクションから、次のオプションを選択します。

- このレポートを [アーカイブレポート (Archived Reports)] ページに表示するには、[アーカイブレポート (Archive Report)] チェックボックスを選択します。

(注) [ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポートはアーカイブできません。

- レポートを電子メールで送信する場合は、[今すぐ受信者にメールを送る (Email now to recipients)] チェックボックスをオンにします。
- テキストフィールドに、レポートの受信者の電子メールアドレスを入力します。

**ステップ 9** [このレポートを配信 (Deliver This Report)] をクリックして、レポートを生成します。

---

## [アーカイブ Web レポート (Archived Web Reports)] ページ

- [スケジュール設定されたレポートとオンデマンド Web レポートについて \(272 ページ\)](#)
- [オンデマンドでの Web レポートの生成 \(277 ページ\)](#)
- [アーカイブ済みの Web レポートの表示と管理 \(278 ページ\)](#)

## アーカイブ済みの Web レポートの表示と管理

ここでは、スケジュール設定されたレポートとして生成されたレポートの使用方法について説明します。

**ステップ 1** [ウェブ (Web)] > [レポート (Reporting)] > [アーカイブ レポート (Archived Reports)] に移動します。

- ステップ 2** レポートを表示するには、[レポートタイトル (Report Title)] 列でレポート名をクリックします。[表示 (Show)] ドロップダウンメニューでは、[アーカイブレポート (Archived Reports)] ページに表示されるレポートのタイプをフィルタリングできます。
- ステップ 3** リストが長い場合に特定のレポートを見つけるには、[表示 (Show)] メニューからレポートタイプを選択してリストをフィルタリングするか、または列のヘッダーをクリックし、その列でソートします。

#### 次のタスク

##### 関連項目

- [スケジュール設定された Web レポートの保存 \(273 ページ\)](#)
- [スケジュール設定された Web レポートの追加 \(274 ページ\)](#)
- [オンデマンドでの Web レポートの生成 \(277 ページ\)](#)

## Web トラッキング

[Web トラッキング (Web Tracking)] ページを使用して、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を表示します。展開で使用するサービスに基づき、関連するタブで検索を行います。

- [Web プロキシサービスによって処理されたトランザクションの検索 \(279 ページ\)](#)
- [L4 トラフィック モニタによって処理されたトランザクションの検索 \(284 ページ\)](#)
- [SOCKS プロキシによって処理されるトランザクションの検索 \(285 ページ\)](#)
- [Web トラッキングの検索結果の使用 \(291 ページ\)](#)
- [Web トラッキング検索結果のトランザクションの詳細の表示 \(292 ページ\)](#)

Web プロキシと L4 トラフィック モニタの違いについては、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding How the Web Security Appliance Works」セクションを参照してください。

##### 関連項目

- [Web トラッキングおよびアップグレードについて \(294 ページ\)](#)

## Web プロキシ サービスによって処理されたトランザクションの検索

[ウェブ (Web)] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] ページの [プロキシサービス (Proxy Services)] タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブルユース適用コンポーネントから収集された Web トラッキング データを検索します。このデータには、L4 トラフィック モニタリング データ、および SOCKS プロキシによって処理されたトランザクションは含まれません。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。** 所定の期間内の従業員に関するレポートを調査します。

たとえば、[プロキシサービス (Proxy Services)] タブを使用して、ユーザがアクセスしている特定の URL について、ユーザがアクセスした時刻や、それが許可された URL であるかどうか、といった情報を取得できます。

- **ネットワークセキュリティ管理者**。会社のネットワークが従業員のスマートフォンを介してマルウェアの脅威にさらされていないかどうかを調査します。

所定の期間内に記録されたトランザクション (ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど) の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。



(注) Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

Web トラッキングの使用例については、[例 1 : ユーザの調査 \(649 ページ\)](#) を参照してください。

[プロキシサービス (Proxy Services)] タブと他の Web レポートニング ページの併用例については、[\[URL カテゴリ \(URL Categories\)\] ページ](#)とその他のレポートニング ページの併用 ([211 ページ](#)) を参照してください。

- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] を選択します。
- ステップ 2** [プロキシサービス (Proxy Services)] タブをクリックします。
- ステップ 3** 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定 (Advanced)] をクリックします。
- ステップ 4** 検索条件を入力します。

表 64: [プロキシサービス (Proxy Services)] タブの Web トラッキング検索条件

オプション	説明
デフォルトの検索条件	
時間範囲	レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで使用できる時間範囲については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
ユーザ/クライアント IPv4またはIPv6	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。  このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されません。



オプション	説明
Web サイト (Website)	追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクションタイプ (Transaction Type)	追跡対象のトランザクションのタイプを [すべてのトランザクション (All Transactions) ]、[完了 (Completed) ]、[ブロックされた (Blocked) ]、[モニタ対象 (Monitored) ]、または [警告対象 (Warned) ] から選択します。
高度な検索条件	
URL カテゴリ	<p>URL カテゴリでフィルタリングするには、[URLカテゴリによるフィルタ (Filter by URL Category) ] を選択し、フィルタリング対象とするカスタムまたは定義済み URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。</p> <p>一連の URL カテゴリが更新されると、一部のカテゴリに「廃止予定 (Deprecated) 」のラベルが付けられる場合があります。廃止予定のカテゴリは、新しいトランザクションに使用されなくなります。ただし、そのカテゴリが有効な間に発生した最近のトランザクションについては、引き続き検索を実行できます。URL カテゴリセットの更新については、<a href="#">URL カテゴリセットの更新とレポート (211 ページ)</a> を参照してください。</p> <p>ドロップダウンリストに表示されるエンジン名に関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。</p>
アプリケーション (Application)	<p>アプリケーションでフィルタリングするには、[アプリケーションによるフィルタ (Filter by Application) ] を選択し、フィルタリングに使用するアプリケーションを選択します。</p> <p>アプリケーションタイプでフィルタリングするには、[アプリケーションタイプによるフィルタ (Filter by Application Type) ] を選択し、フィルタリングに使用するアプリケーションタイプを選択します。</p>
ポリシー	<p>ポリシー グループでフィルタリングするには、[ポリシーによるフィルタ (Filter by Policy) ] を選択し、フィルタリングに使用するポリシーグループ名を入力します。</p> <p>このポリシーが Web セキュリティアプライアンスで宣言済みであることを確認してください。</p>
マルウェアの脅威	<p>特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ (Filter by Malware Threat) ] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。</p> <p>マルウェアカテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ (Filter by Malware Category) ] を選択し、フィルタリングに使用するマルウェアカテゴリを選択します。説明については、<a href="#">マルウェアのカテゴリについて (216 ページ)</a> を参照してください。</p>

オプション	説明
WBRs	<p>[WBRs] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。</p> <ul style="list-style-type: none"> <li>• Web レピュテーションスコアでフィルタリングするには、[スコア範囲 (Score Range)] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし (No Score)] を選択すると、スコアがない Web サイトをフィルタリングできます。</li> <li>• Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ (Filter by Reputation Threat)] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。</li> </ul> <p>WBRs スコアの詳細は、『IronPort AsyncOS for Web User Guide』を参照してください。</p>
AnyConnect セキュア モビリティ (AnyConnect Secure Mobility)	<p>リモートまたはローカルアクセスでフィルタリングするには、[ユーザの場所によるフィルタ (Filter by User Location)] を選択し、アクセス タイプを選択します。すべてのアクセスタイプを含めるには、[フィルタを無効にする (Disable Filter)] を選択します</p> <p>(旧リリースでは、このオプションは Mobile User Security と呼ばれていました。)</p>
Web アプライアンス	<p>特定の Web アプライアンスでフィルタリングするには、[Web アプライアンスによるフィルタ (Filter by Web Appliance)] の横のラジオ ボタンをクリックし、テキストフィールドに Web アプライアンス名を入力します。</p> <p>[フィルタを無効にする (Disable Filter)] を選択すると、検索にはセキュリティ管理アプライアンスに関連付けられている Web セキュリティアプライアンスがすべて含まれます。</p>
ユーザ リクエスト	<p>ユーザによって実際に開始されたトランザクションでフィルタリングするには、[Web ユーザが要求したトランザクションによるフィルタ (Filter by Web User-Requested Transactions)] を選択します。</p> <p>注：このフィルタを有効にすると、検索結果には「最良の推測」トランザクションが含まれます。</p>

ステップ 5 [検索 (Search)] をクリックします。

## 次のタスク

### 関連項目

- [詳細な Web トラッキング検索結果の表示 \(292 ページ\)](#)
- [Web トラッキング検索結果について \(292 ページ\)](#)
- [Web トラッキング検索結果のトランザクションの詳細の表示 \(292 ページ\)](#)

- [Web トラッキング機能および高度なマルウェア防御機能について \(293 ページ\)](#)

## マルウェアのカテゴリについて

Web セキュリティ アプライアンスは次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザヘルパー オブジェクト	ブラウザヘルパーオブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。

## L4 トラフィック モニタによって処理されたトランザクションの検索

マルウェアのタイプ	説明
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。  公然と、または密かに、システムプロセスやユーザアクションを記録する。  これらの記録を後で取得して確認できるようにする。
トロイのダウンロード	トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンロードはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークションサイト、あるいはオンライン支払サイトに関するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

## L4 トラフィック モニタによって処理されたトランザクションの検索

[ウェブ (Web)] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] ページの [L4 トラフィック モニタ (L4 Traffic Monitor)] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- トランザクションを開始したマシンの IP アドレス (IPv4 または IPv6)
- 接続先 Web サイトのドメインまたは IP アドレス (IPv4 または IPv6)
- [ポート (Port)]
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ
- 接続を処理する Web セキュリティ アプライアンス

一致した検索結果のうち最初の 1000 件が表示されます。

疑わしいサイトにあるホスト名、またはトランザクションを処理した Web セキュリティ アプライアンスを表示するには、[送信先 IP アドレス (Destination IP Address)] 列見出しの [詳細を表示 (Display Details)] リンクをクリックします。

この情報の詳細な使用方法については、[\[L4 トラフィック モニタ \(L4 Traffic Monitor\)\] レポート \(228 ページ\)](#) を参照してください。

## SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、トランザクションを開始したクライアントマシンの IP アドレス、および宛先ドメイン、IP アドレス、またはポートなど、さまざまな条件に一致するトランザクションを検索できます。カスタム URL カテゴリ、一致ポリシー、およびユーザロケーション (ローカルまたはリモート) により、結果をフィルタリングすることもできます。IPv4 および IPv6 アドレスがサポートされます。

**ステップ 1** [ウェブ (Web)] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] を選択します。

**ステップ 2** [SOCKS プロキシ (SOCKS Proxy)] タブをクリックします。

**ステップ 3** 結果をフィルタリングするには、[詳細設定 (Advanced)] をクリックします。

**ステップ 4** 検索条件を入力します。

**ステップ 5** [検索 (Search)] をクリックします。

次のタスク

関連項目

[\[SOCKS プロキシ \(SOCKS Proxy\)\] レポート \(231 ページ\)](#)

## 新しい Web インターフェイスでの Web トラッキング

[Web トラッキング検索 (Web Tracking Search)] ページでは、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を表示することができます。展開で使用するサービスに基づき、関連するタブで検索を行います。

- [Web プロキシ サービスによって処理されたトランザクションの検索 \(286 ページ\)](#)
- [L4 トラフィック モニタによって処理されたトランザクションの検索 \(284 ページ\)](#)
- [SOCKS プロキシによって処理されるトランザクションの検索 \(291 ページ\)](#)
- [Web トラッキングの検索結果の使用 \(291 ページ\)](#)
- [Web トラッキング検索結果のトランザクションの詳細の表示 \(292 ページ\)](#)

Web プロキシと レイヤ 4 トラフィック モニタの違いについては、『*User Guide for AsyncOS for Cisco Web Security Appliances*』の「Understanding How the Web Security Appliance Works」セクションを参照してください。

## Web プロキシ サービスによって処理されたトランザクションの検索

[Web トラッキング検索 (Web Tracking Search)] ページの [プロキシサービス (Proxy Services)] タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブルユース適用コンポーネントから収集された Web トラッキング データを検索できます。このデータには、レイヤ 4 トラフィック モニタリング データまたは SOCKS プロキシによって処理されたトランザクションは含まれません。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。** 所定の期間内の従業員に関するレポートを調査します。  
たとえば、[プロキシサービス (Proxy Services)] タブを使用して、ユーザがアクセスしている特定の URL について、ユーザがアクセスした時刻や、それが許可された URL であるかどうか、といった情報を取得できます。
- **ネットワークセキュリティ管理者。** 会社のネットワークが従業員のスマートフォンを介してマルウェアの脅威にさらされていないかどうかを調査します。

所定の期間内に記録されたトランザクション (ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど) の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。



(注) Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

Web トラッキングの使用例については、[例 1：ユーザの調査 \(649 ページ\)](#) を参照してください。

[プロキシサービス (Proxy Services)] タブと他の Web レポートリング ページの併用例については、[\[URL カテゴリ \(URL Categories\)\] ページとその他のレポートリング ページの併用 \(211 ページ\)](#) を参照してください。

**ステップ 1** セキュリティ管理アプライアンスで、ドロップダウン リストから [Web] を選択します。

**ステップ 2** [トラッキング (Tracking)] > [プロキシサービス (Proxy Services)] を選択します。

**ステップ 3** 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定 (Advanced)] をクリックします。

**ステップ 4** 検索条件を入力します。

表 65:[プロキシサービス (Proxy Services) ]タブの Web トラッキング検索条件

オプション	説明
デフォルトの検索条件	
時間範囲	レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで使用できる時間範囲については、 <a href="#">レポートの時間範囲の選択 (27 ページ)</a> を参照してください。
ユーザ/クライアント IPv4またはIPv6	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。  このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されません。
Web サイト (Website)	追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクションタイプ (Transaction Type)	追跡対象のトランザクションのタイプを [すべてのトランザクション (All Transactions) ]、[完了 (Completed) ]、[ブロックされた (Blocked) ]、[モニタ対象 (Monitored) ]、または [警告対象 (Warned) ] から選択します。
高度な検索条件	
URL カテゴリ	URL カテゴリでフィルタリングするには、[URL カテゴリによるフィルタ (Filter by URL Category) ] を選択し、フィルタリング対象とするカスタムまたは定義済み URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。  一連の URL カテゴリが更新されると、一部のカテゴリに「廃止予定 (Deprecated) 」のラベルが付けられる場合があります。廃止予定のカテゴリは、新しいトランザクションに使用されなくなります。ただし、そのカテゴリが有効な間に発生した最近のトランザクションについては、引き続き検索を実行できます。URL カテゴリセットの更新については、 <a href="#">URL カテゴリセットの更新とレポート (211 ページ)</a> を参照してください。  ドロップダウンリストに表示されるエンジン名に関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。
アプリケーション (Application)	アプリケーションでフィルタリングするには、[アプリケーションによるフィルタ (Filter by Application) ] を選択し、フィルタリングに使用するアプリケーションを選択します。  アプリケーションタイプでフィルタリングするには、[アプリケーションタイプによるフィルタ (Filter by Application Type) ] を選択し、フィルタリングに使用するアプリケーションタイプを選択します。

オプション	説明
ポリシー	<p>ポリシー グループでフィルタリングするには、[ポリシーによるフィルタ (Filter by Policy)] を選択し、フィルタリングに使用するポリシーグループ名を入力します。</p> <p>このポリシーが Web セキュリティ アプライアンスで宣言済みであることを確認してください。</p>
マルウェアの脅威	<p>特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ (Filter by Malware Threat)] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。</p> <p>マルウェアカテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ (Filter by Malware Category)] を選択し、フィルタリングに使用するマルウェアカテゴリを選択します。説明については、<a href="#">マルウェアのカテゴリについて (216 ページ)</a> を参照してください。</p>
WBRs	<p>[WBRs] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。</p> <ul style="list-style-type: none"> <li>• Web レピュテーションスコアでフィルタリングするには、[スコア範囲 (Score Range)] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし (No Score)] を選択すると、スコアがない Web サイトをフィルタリングできます。</li> <li>• Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ (Filter by Reputation Threat)] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。</li> </ul> <p>WBRs スコアの詳細は、『IronPort AsyncOS for Web User Guide』を参照してください。</p>
AnyConnect セキュア モビリティ (AnyConnect Secure Mobility)	<p>リモートまたはローカルアクセスでフィルタリングするには、[ユーザの場所によるフィルタ (Filter by User Location)] を選択し、アクセスタイプを選択します。すべてのアクセスタイプを含めるには、[フィルタを無効にする (Disable Filter)] を選択します</p> <p>(旧リリースでは、このオプションは Mobile User Security と呼ばれていました。)</p>
Web アプライアンス	<p>特定の Web アプライアンスでフィルタリングするには、[Web アプライアンスによるフィルタ (Filter by Web Appliance)] の横のラジオ ボタンをクリックし、テキスト フィールドに Web アプライアンス名を入力します。</p> <p>[フィルタを無効にする (Disable Filter)] を選択すると、検索にはセキュリティ管理アプライアンスに関連付けられている Web セキュリティ アプライアンスがすべて含まれます。</p>



オプション	説明
ユーザ リクエスト	<p>ユーザによって実際に開始されたトランザクションでフィルタリングするには、[Web ユーザが要求したトランザクションによるフィルタ (Filter by Web User-Requested Transactions)] を選択します。</p> <p>注：このフィルタを有効にすると、検索結果には「最良の推測」トランザクションが含まれます。</p>

## マルウェアのカテゴリについて

Web セキュリティ アプライアンスは次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェアアプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザヘルパーオブジェクト	ブラウザヘルパーオブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザプラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイクヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。

マルウェアのタイプ	説明
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。  公然と、または密かに、システムプロセスやユーザアクションを記録する。  これらの記録を後で取得して確認できるようにする。
トロイのダウンロード	トロイのダウンロードは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンロードはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークションサイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

## レイヤ4トラフィック モニタによって処理されたトランザクションの検索

[Webトラッキング検索 (Web Tracking Search)] ページの [レイヤ4トラフィックモニタ (Layer 4 Traffic Monitor)] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- トランザクションを開始したマシンの IP アドレス (IPv4 または IPv6)
- 接続先 Web サイトのドメインまたは IP アドレス (IPv4 または IPv6)
- [ポート (Port) ]
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ
- 接続を処理する Web セキュリティ アプライアンス

疑わしいサイトにあるホスト名、またはトランザクションを処理した Web セキュリティ アプライアンスを表示するには、[送信先 IP アドレス (Destination IP Address) ] 列見出しの [詳細を表示 (Display Details) ] リンクをクリックします。

この情報の詳細な使用方法については、[\[レイヤ4トラフィックモニタ \(Layer4 Traffic Monitor\) \] ページ \(244 ページ\)](#) を参照してください。

## SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、トランザクションを開始したクライアントマシンの IP アドレス、および宛先ドメイン、IP アドレス、またはポートなど、さまざまな条件に一致するトランザクションを検索できます。カスタム URL カテゴリ、一致ポリシー、およびユーザロケーション (ローカルまたはリモート) により、結果をフィルタリングすることもできます。IPv4 および IPv6 アドレスがサポートされます。

- 
- ステップ 1** セキュリティ管理アプライアンスで、ドロップダウンリストから [Web] を選択します。
  - ステップ 2** [トラッキング (Tracking) ] > [SOCKS プロキシ (SOCKS Proxy) ] を選択します。
  - ステップ 3** 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定 (Advanced) ] をクリックします。
  - ステップ 4** 検索条件を入力します。
  - ステップ 5** [検索 (Search) ] をクリックします。
- 

次のタスク

関連項目

[\[SOCKS プロキシ \(SOCKS Proxy\) \] レポート \(231 ページ\)](#)

## Web トラッキングの検索結果の使用

- [詳細な Web トラッキング検索結果の表示 \(292 ページ\)](#)

- [Web トラッキング検索結果について \(292 ページ\)](#)
- [Web トラッキング検索結果のトランザクションの詳細の表示 \(292 ページ\)](#)
- [Web トラッキングおよびアップグレードについて \(294 ページ\)](#)

## 詳細な Web トラッキング検索結果の表示

**ステップ 1** 返された結果のページをすべて確認してください。

**ステップ 2** 現在表示されている数よりも多くの結果を各ページに表示するには、[表示された項目 (Items Displayed)] メニューからオプションを選択します。

**ステップ 3** 条件に一致するトランザクションが、[表示された項目 (Items Displayed)] メニューで選択できる最大トランザクション数より多い場合は、[印刷可能なダウンロード (Printable Download)] リンクをクリックし、一致するすべてのトランザクションを含む CSV ファイルを取得すると、完全な結果を確認できます。

この CSV ファイルには、関連トランザクションの詳細を除く、raw データ一式が含まれます。

## Web トラッキング検索結果について

デフォルトでは、結果はタイムスタンプでソートされ、最新の結果が最上部に表示されます。

検索結果に表示される情報：

- URL がアクセスされた時刻。
- ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数。関連トランザクションの数は、列見出しの [すべての詳細を表示(Display All Details)] リンクの下の各行に表示されます。
- 処理 (トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます)。

## Web トラッキング検索結果のトランザクションの詳細の表示

目的	操作手順
リスト内の短縮 URL の完全な URL	トランザクションを処理したホスト Web セキュリティ アプライアンスをメモして、そのアプライアンスのアクセスログを確認します。
個々のトランザクションの詳細	[Web サイト (Website)] 列の URL をクリックします。
すべてのトランザクションの詳細	[Web サイト (Website)] 列見出しの [すべての詳細を表示...(Display All Details...)] リンクをクリックします。

目的	操作手順
500 件までの関連トランザクションのリスト	<p>関連トランザクションの数は、検索結果リストの列見出しにある [詳細を表示 (Display Details)] リンクの下のカッコ内に表示されます。</p> <p>トランザクションの [詳細 (Details)] ビューで [関連トランザクション (Related Transactions)] リンクをクリックします。</p>

## Web トラッキング機能および高度なマルウェア防御機能について

Web トラッキングでファイルの脅威情報を検索する場合は、次の点に注意してください。

- ファイル レピュテーション サービスで検出された悪意のあるファイルを検索するには、Web トラッキングの [詳細設定 (Advanced)] セクションにある [マルウェアの脅威 (Malware Threat)] 領域で、[マルウェアカテゴリ別フィルタ (Filter by Malware Category)] オプションの [悪意のある既知の高リスクファイル (Known Malicious and High-Risk Files)] を選択します。
- Web トラッキングには、ファイル レピュテーション 処理についての情報と、トランザクションが処理されたときに返された元のファイル レピュテーションの判定のみが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

検索結果の [ブロック - AMP (Block - AMP)] は、ファイルのレピュテーション判定が原因でトランザクションがブロックされたことを意味します。

トラッキングの詳細に表示される [AMP 脅威スコア (AMP Threat Score)] は、ファイルを明確に判定できないときにクラウドレピュテーションサービスが提示するベストエフォート型のスコアです。この場合、スコアは 1~100 です。(AMP 判定が返された場合、またはスコアがゼロの場合は [AMP 脅威スコア (AMP Threat Score)] を無視してください)。アプライアンスはこのスコアをしきい値スコア ([セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページで設定) と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60~100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアの変更は推奨されません。WBRIS コアは、ファイルのダウンロード元サイトのレピュテーションであり、ファイル レピュテーションとは関係ありません。

- 判定のアップデートは [AMP 判定のアップデート (AMP Verdict Updates)] レポートだけに表示されます。Web トラッキングの元のトランザクションの詳細は、判定が変更されても更新されません。特定のファイルが関係するトランザクションを表示するには、判定アップデート レポートで SHA-256 をクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析 (File Analysis)] レポートにのみ表示されます。

分析済みファイルのその他の情報は、クラウドから入手できます。ファイルの使用可能なファイル分析情報を表示するには、[レポート (Reporting)] > [ファイル分析 (File Analysis)] を選択して、ファイルを検索する SHA-256 を入力するか、Web トラッキングの詳細で SHA-256 リンクをクリックします。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

分析用に送信されたファイルの後続インスタンスをアプライアンスが処理すると、そのインスタンスは Web トラッキングの検索結果に表示されるようになります。

#### 関連項目

- [SHA-256 ハッシュによるファイルの識別 \(221 ページ\)](#)

## Web トラッキングおよびアップグレードについて

新しい Web トラッキング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。Web トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

## Web レポートニングおよびトラッキングのトラブルシューティング

- [中央集中型レポートニングが適切に有効化されているのに機能しない \(294 ページ\)](#)
- [\[高度なマルウェア保護判定のアップデート \(Advanced Malware Protection Verdict Updates\)\] レポートの結果が異なる \(295 ページ\)](#)
- [ファイル分析レポートの詳細の表示に関する問題 \(295 ページ\)](#)
- [予想されるデータがレポートニングまたはトラッキングの結果に表示されない \(296 ページ\)](#)
- [PDF に Web トラッキングデータのサブセットのみが表示される \(297 ページ\)](#)
- [L4 トラフィック モニタ レポートのトラブルシューティング \(297 ページ\)](#)
- [エクスポートされた .CSV ファイルが Web インターフェイスのデータと異なる \(297 ページ\)](#)

「すべてのレポートのトラブルシューティング (36 ページ)」も参照してください。

## 中央集中型レポートニングが適切に有効化されているのに機能しない

### 問題

指示どおりに中央集中型 Web レポートニングを有効にしても機能しません。

### ソリューション

レポートिंगにディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポートングは機能しません。Web レポートングおよびトラッキングに設定するクォータが、現在使用しているディスク領域よりも大きい場合、Web レポートングおよびトラッキングのデータは失われません。詳細については、[ディスク領域の管理 \(567 ページ\)](#) を参照してください。

## [高度なマルウェア保護判定のアップデート (Advanced Malware Protection Verdict Updates) ] レポートの結果が異なる

### 問題

Web セキュリティ アプライアンスおよび E メール セキュリティ アプライアンスが同じファイル进行分析用に送信し、Web および電子メールの [AMP 判定のアップデート (AMP Verdict Updates) ] レポートに、そのファイルの異なる判定が表示されます。

### 解決方法

この状況は一時的です。判定アップデートがすべてダウンロードされると、結果が一致します。これには最大で 30 分かかります。

## ファイル分析レポートの詳細の表示に関する問題

- [ファイル分析レポートの詳細を使用できない \(295 ページ\)](#)
- [ファイル分析レポートの詳細を表示する際のエラー \(295 ページ\)](#)

### ファイル分析レポートの詳細を使用できない

#### 問題

ファイル分析レポートの詳細を使用できません。

#### 解決方法

「[ファイル分析レポートの詳細の要件 \(219 ページ\)](#)」を参照してください。

### ファイル分析レポートの詳細を表示する際のエラー

#### 問題

ファイル分析レポートの詳細を表示しようとする、「使用可能なクラウドサーバ構成がありません (No cloud server configuration is available)」エラーが表示されます。

#### ソリューション

[管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ]>[セキュリティアプライアンス (Security Appliances) ]に移動して、ファイル分析機能が有効になっている Web セキュリティ アプライアンスを少なくとも 1 つ追加します。

## ファイル分析レポートの詳細をプライベートクラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー

### 問題

ファイル分析レポートの詳細を表示しようとする時、API キーエラー、登録エラー、またはアクティベーションエラーが表示されます。

### ソリューション

プライベートクラウド（オンプレミス）の Cisco AMP Threat Grid Appliance を使用している場合は、[（オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する（220 ページ）](#) を参照してください。

Threat Grid Appliance のホスト名が変更される場合は、参照先の手順のプロセスを繰り返す必要があります。

## 予想されるデータがレポートリングまたはトラッキングの結果に表示されない

### 問題

予想されるデータがレポートリングまたはトラッキングの結果に表示されません。

### 解決方法

考えられる原因：

- 目的の時間範囲を選択したことを確認します。
- トラッキング結果の場合は、一致したすべての結果が表示されていることを確認します。[詳細な Web トラッキング検索結果の表示（292 ページ）](#) を参照してください。
- Web セキュリティ アプライアンスおよび Cisco コンテンツ セキュリティ管理アプライアンス間のデータ転送が中断されたか、データが消去された可能性があります。[\[使用可能なデータ \(Data Availability\)\] ページ（235 ページ）](#) を参照してください。
- アップグレードによって情報のレポート方法または追跡方法が変更された場合は、アップグレード前に発生したトランザクションが想定どおりに表示されないことがあります。お使いのリリースでこのような変更が行われたかどうかを確認するには、[資料（655 ページ）](#) に示された場所で該当するリリース ノートを参照してください。
- Web プロキシサービスのトラッキング検索結果に表示されない結果については、[Web プロキシサービスによって処理されたトランザクションの検索（279 ページ）](#) を参照してください。
- ユーザがリクエストしたトランザクションによるフィルタリング時の予期しない結果については、[Web プロキシサービスによって処理されたトランザクションの検索（279 ページ）](#) の表の「ユーザ要求 (User Request)」行を参照してください。



## PDF に Web トラッキング データのサブセットのみが表示される

### 問題

PDF に [Web トラッキング (Web Tracking)] ページに表示されるデータの一部だけが表示されます。

### ソリューション

PDF および CSV ファイルで表示されるデータと除外されるデータについては、[レポート データおよびトラッキング データのエクスポート \(33 ページ\)](#) の表で Web トラッキング の情報を参照してください。

## L4 トラフィック モニタ レポートのトラブルシューティング

Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合、プロキシのデータ ポートの IP アドレスが記録され、クライアント IP アドレスとしてレポートに表示されます。Web プロキシがトランスペアレント プロキシとして設定されている場合は、クライアント IP アドレスが正しく記録され、表示されるように IP スプーフィングを有効にします。これを行うには、『IronPort AsyncOS for Web User Guide』を参照してください。

### 関連項目

- [クライアント マルウェア リスク \(Client Malware Risk\) レポート \(224 ページ\)](#)
- [L4 トラフィック モニタによって処理されたトランザクションの検索 \(284 ページ\)](#)

## エクスポートされた .CSV ファイルが Web インターフェイスのデータと異なる

### 問題

.csv ファイルにエクスポートされた [一致したドメイン (Domains Matched)] データが、Web インターフェイスに表示されているデータと異なります。

### ソリューション

パフォーマンス上の理由から、最初の 300,000 エントリのみが .csv としてエクスポートされます。

## Web トラッキング検索結果のエクスポートの問題

### 問題

同時に複数の大規模な検索クエリを実行すると、Web トラッキング検索の結果に "メモリ不足" エラーが表示されます。

### ソリューション

回避策として、メモリのヒープサイズを 1024 MB 以上に増やすか、検索基準の時間範囲を減らすことができます。メモリのヒープサイズを増やすと、メモリ関連の問題が発生することに注意してください。



## 第 7 章

# メッセージのトラッキング

この章は、次の項で構成されています。

- [トラッキング サービスの概要 \(299 ページ\)](#)
- [中央集中型メッセージトラッキングの設定 \(300 ページ\)](#)
- [メッセージトラッキングデータの有効性の検査 \(303 ページ\)](#)
- [電子メールメッセージの検索 \(303 ページ\)](#)
- [トラッキングクエリ結果について \(311 ページ\)](#)
- [メッセージトラッキングのトラブルシューティング \(316 ページ\)](#)

## トラッキング サービスの概要

シスコのコンテンツセキュリティ管理アプライアンスのトラッキングサービスは、Eメールセキュリティアプライアンスを補完します。セキュリティ管理アプライアンスによって、電子メール管理者はすべてのEメールセキュリティアプライアンスを通過するメッセージのステータスを1箇所から追跡できます。

セキュリティ管理アプライアンスを使用すると、Eメールセキュリティアプライアンスによって処理されるメッセージの状態を簡単に把握できるようになります。電子メール管理者は、メッセージの正確な場所を判断することで、ヘルプデスクコールを迅速に解決できます。管理者はセキュリティ管理アプライアンスを使用して、特定のメッセージについて、配信されたか、ウイルス感染が検出されたか、スパム隔離に入れられたか、あるいはメールストリーム以外の場所にあるのかを判断できます。

grep や同様のツールを使用してログファイルを検索する代わりに、セキュリティ管理アプライアンスの柔軟なトラッキングインターフェイスを使用してメッセージの場所を特定できます。さまざまな検索パラメータを組み合わせて使用できます。

トラッキングクエリには次の項目を含めることができます。

- **タイム フレーム**：指定された日数と時間内に送信されたメッセージを検索します。
- **エンベロープ情報**：照合するテキスト文字列を入力し、特定のエンベロープ送信者または受信者からのメッセージを検索します。

- **件名**：件名行のテキスト文字列を照合します。警告：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
- **添付ファイル名**：メッセージを添付ファイル名で検索できます。照会した名前の添付ファイルが少なくとも1つ含まれているメッセージが検索結果に表示されます。

パフォーマンス上の理由から、OLE オブジェクトなどの添付ファイルや .ZIP ファイルなどのアーカイブに含まれるファイル名は追跡されません。

トラッキングできない添付ファイルもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは他のスキャン動作の一環としてのみ実行されます。たとえば、メッセージまたはコンテンツフィルタリング、DLP、免責事項スタンプなどです。添付ファイル名は、添付ファイルがまだ添付されている間に本文スキャンを通過するメッセージに対してのみ使用できます。添付ファイル名が表示されない例を次に示します（ただしこれらに限られるわけではありません）。

- システムがコンテンツフィルタのみを使用しているときに、メッセージがドロップされるか、またはその添付ファイルがアンチスパムまたはアンチウイルス フィルタによって削除された場合
- 本文スキャンが実行される前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが削除された場合
- **ファイル SHA256**：メッセージ ファイルの SHA-256 値を持つメッセージを検索します。
- **Cisco ホスト**：検索条件を特定の E メールセキュリティ アプライアンスに絞り込むか、管理されているすべてのアプライアンスを検索対象とします。
- **メッセージ ID ヘッダーおよび Cisco MID**：SMTP 「Message-ID:」 ヘッダー、または Cisco メッセージ ID (MID) を識別してメッセージを検索します。
- **送信者 IP アドレス/ドメイン/ネットワーク所有者**：特定の IP アドレス、ドメイン名、またはネットワーク所有者からのメッセージを検索します。
- **メッセージイベント**：ウイルス陽性、スパム陽性、またはスパムの疑いのフラグが設定されたメッセージや、配信された、ハードバウンスされた、ソフトバウンスされた、またはウイルスアウトブレイク隔離に送信されたメッセージなど、指定されたイベントに一致するメッセージを検索します。
- **拒否された接続**：拒否された接続の特定の IP アドレス、ドメイン名またはネットワーク所有者からのメッセージを検索結果で検索します。

## 中央集中型メッセージトラッキングの設定

中央集中型メッセージトラッキングを設定するには、次の手順を順序どおりに実行します。

- [セキュリティ管理アプライアンスでの中央集中型電子メールトラッキングのイネーブル化 \(301 ページ\)](#)

- [Eメールセキュリティアプライアンスでの中央集中型メッセージトラッキングの設定 \(301 ページ\)](#)
- [管理対象の各 Eメールセキュリティアプライアンスへの中央集中型メッセージトラッキングサービスの追加 \(302 ページ\)](#)

## セキュリティ管理アプライアンスでの中央集中型電子メールトラッキングのイネーブル化

- ステップ 1** (新しい Web インターフェイスのみ) クラウド Eメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] を選択します。
- ステップ 3** [メッセージトラッキングサービス (Message Tracking Service)] セクションで [有効化 (Enable)] をクリックします。
- ステップ 4** システムセットアップウィザードを実行してから初めて中央集中型電子メッセージトラッキングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 5** 変更を送信し、保存します。

## Eメールセキュリティアプライアンスでの中央集中型メッセージトラッキングの設定

- ステップ 1** Eメールセキュリティアプライアンスでメッセージトラッキングが設定され、正常に動作していることを確認します。
- ステップ 2** [セキュリティサービス (Security Services)] > [メッセージトラッキング (Message Tracking)] に移動します。
- ステップ 3** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 4** [集約管理トラッキング (Centralized Tracking)] を選択します。
- ステップ 5** [送信 (Submit)] をクリックします。
- ステップ 6** 電子メールの添付ファイル名を検索および記録できるようにする場合は、次の点に注意してください。  
少なくとも 1 つの受信コンテンツ フィルタまたはその他の本文スキャン機能が Eメールセキュリティアプライアンスで設定され、有効になっていることを確認します。コンテンツフィルタおよび本文スキャンの詳細については、ご使用の Eメールセキュリティアプライアンスのマニュアルまたはオンラインヘルプを参照してください。
- ステップ 7** 変更を保存します。
- ステップ 8** 管理対象の各 Eメールセキュリティアプライアンスに同様の手順を繰り返します。

## 管理対象の各 E メール セキュリティ アプライアンスへの中央集中型メッセージトラッキングサービスの追加

他の中央集中型管理機能を設定する際、すでにアプライアンスを追加したかどうかによって、ここでの手順は異なります。


- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。
- ステップ 3** このページのリストに、すでに E メール セキュリティアプライアンスを追加している場合は、次の手順を実行します。
- E メール セキュリティアプライアンスの名前をクリックします。
  - [集約メッセージトラッキング (Centralized Message Tracking)] サービスを選択します。
- ステップ 4** E メール セキュリティアプライアンスをまだ追加していない場合は、次の手順を実行します。
- [メールアプライアンスの追加 (Add Email Appliance)] をクリックします。
  - [アプライアンス名 (Appliance Name)] および [IP アドレス (IP Address)] テキストフィールドに、E メール セキュリティアプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。  
(注) [IP アドレス (IP Address)] フィールドに DNS 名を入力した場合でも、[送信 (Submit)] をクリックすると、IP アドレスに変換されます。
  - [集約メッセージトラッキング (Centralized Message Tracking)] サービスが事前に選択されています。
  - [接続の確立 (Establish Connection)] をクリックします。
  - 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection)] をクリックします。  
(注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。
  - 「Success」メッセージがページのテーブルの上に表示されるまで待機します。
  - [テスト接続 (Test Connection)] をクリックします。
  - テーブルの上のテスト結果を確認します。
- ステップ 5** [送信 (Submit)] をクリックします。
- ステップ 6** 中央集中型メッセージトラッキングを有効にする各 E メール セキュリティアプライアンスに対し、この手順を繰り返します。
- ステップ 7** 変更を保存します。
-

## 機密情報へのアクセスの管理

管理タスクを数人で分配する場合、データ消失防止（DLP）ポリシーに違反するメッセージに表示される機密情報へのアクセスを制限するには、[メッセージトラッキングでの機密情報へのアクセスの制御](#)（498 ページ）を参照してください。

## メッセージトラッキングデータの有効性の検査

メッセージトラッキングデータに含まれる日付範囲を確認すること、およびそのデータの欠落インターバルを識別することができます。

**ステップ 1**（新しい Web インターフェイスのみ）クラウド E メールセキュリティ管理コンソールで、歯車（）アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [メール (Email)] > [メッセージトラッキング (Message Tracking)] > [有効なメッセージトラッキングデータ (Message Tracking Data Availability)] を選択します。

## 電子メールメッセージの検索

- [新しい Web インターフェイスでの電子メールメッセージの検索](#)（303 ページ）
- [レガシー Web インターフェイスでの電子メールメッセージの検索](#)（306 ページ）

## 新しい Web インターフェイスでの電子メールメッセージの検索

アプライアンスのトラッキングサービスを使用して、メッセージ件名行、日時の範囲、エンベロープ送信者または受信者、処理イベント（たとえば、メッセージがウイルス陽性またはスパム陽性かどうかや、ハードバウンスまたは配信されたかどうか）など、指定した条件に一致する特定の電子メールメッセージまたはメッセージのグループを検索できます。メッセージトラッキングでは、メッセージフローの詳細なビューが表示されます。また、特定の電子メールメッセージをドリルダウンし、処理イベント、添付ファイル名、エンベロープおよびヘッダー情報など、メッセージの詳細情報を確認することもできます。



(注) このトラッキングコンポーネントにより個々の電子メールメッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

**ステップ 1** クラウド電子メールセキュリティ管理コンソールで、[トラッキング (Tracking)] > [検索 (Search)] を選択します。

**ステップ 2** [メッセージ (Messages)] タブまたは [拒否された接続 (Connections Rejected)] タブを選択し、検索結果を絞り込みます。

(注) 送信者 IP アドレス、ドメイン、またはネットワーク所有者に基づいて拒否された接続を検索することができます。

**ステップ 3** (任意) [詳細検索 (Advanced Search)] をクリックし、その他の検索オプションを表示します。

**ステップ 4** 次の検索条件を入力します。

(注) トラッキング検索では、ワイルドカード文字や正規表現はサポートされません。トラッキング検索では大文字と小文字は区別されません。

- (メッセージと拒否された接続の場合) [受信したメッセージ数 (Message Received)] : [前日 (Last Day)]、[最近1週間 (Last 7 Days)]、または [カスタム範囲 (Custom Range)] を使用してクエリの日時の範囲を指定します。過去 24 時間以内のメッセージを検索するには [前日 (Last Day)] オプションを使用し、過去 7 日間のメッセージを検索するには [最近1週間 (Last 7 Days)] オプションと当日の経過時間を使用します。

日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。終了日と終了時刻に現在の日付と 23:59 を指定すると、クエリーは現在の日付に関するすべてのデータを返します。

日付と時間は、データベースに保管される際に GMT 形式に変換されます。アプライアンス上で日付と時刻を表示する場合は、そのアプライアンスの現地時間で表示されます。

E メールセキュリティアプライアンスのログに記録され、セキュリティ管理アプライアンスが取得済みのメッセージのみが検索結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メールメッセージが送信された時間と、それがトラッキングとレポートの結果に実際に表示される時間との間にわずかな差が生じることがあります。

- [エンベロープ送信者 (Envelope Sender)] : [次で始まる (Begins With)]、[次に合致する (IS)]、または [次を含む (Contains)] を選択し、テキスト文字列を入力してエンベロープ送信者を検索します。電子メールアドレス、ユーザ名、またはドメインを入力できます。次の形式を使用します。
  - E メール ドメインの場合 : *example.com*, *[203.0.113.15]*, *[ipv6:2001:db8:80:1::5]*
  - 完全 E メール アドレスの場合 : *user@example.com*, *user@[203.0.113.15]* or *user@[ipv6:2001:db8:80:1::5]*。
  - 文字を入力できます。入力した内容は実行されません。
- [件名 (Subject)] : [次で始まる (Begins With)]、[次に合致する (IS)]、[次を含む (Contains)]、または [空である (Is Empty)] を選択し、テキスト文字列を入力してメッセージ件名行を検索します。
- [エンベロープ受信者 (Envelope Recipient)] : [次で始まる (Begins With)]、[次に合致する (IS)]、または [次を含む (Contains)] を選択し、テキストを入力してエンベロープ受信者を検索します。電子メールアドレス、ユーザ名、またはドメインを入力できます。

E メールセキュリティアプライアンスでエイリアス拡張にエイリアステーブルを使用している場合は、本来のエンベロープアドレスではなく、拡張された受信者アドレスが検索されます。それ以外の



あらゆる場合においては、メッセージトラッキングクエリによって本来のエンベロープ受信者アドレスが検索されます。

この点を除けば、エンベロープ受信者の有効な検索条件はエンベロープ送信者の場合と同じです。

文字を入力できます。入力した内容は実行されません。

- [添付ファイル名 (Attachment Name)] : [次で始まる (Begins With)]、[次に合致する (IS)]、または [次を含む (Contains)] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。
- Reply-To : [次で始まる (Begins With)]、[次に合致する (Is)]、または [含む (Contains)] を選択して、メッセージの「Reply-To」ヘッダーに基づいてメッセージを検索する文字列を入力します。
- [ファイルSHA256 (File SHA256)] : メッセージのファイルの SHA-256 値を入力します。  
SHA-256 ハッシュに基づいたファイルの識別方法については、[SHA-256 ハッシュによるファイルの識別 \(97 ページ\)](#) を参照してください。
- [シスコのホスト (Cisco Host)] : [すべてのホスト (All Host)] を選択してすべての E メールセキュリティ アプライアンス間で検索するか、ドロップダウンメニューから必要な E メールセキュリティ アプライアンスを選択します。
- [メッセージIDヘッダーおよびCisco MID (Message ID Header and Cisco MID)] : メッセージ ID ヘッダーのテキスト文字列、Cisco IronPort メッセージ ID (MID)、またはその両方を入力します。
- (メッセージと拒否された接続の場合) [送信者IPアドレス/ドメイン/ネットワーク所有者 (Sender IP Address/ Domain / Network Owner)] : 送信元 IP アドレス、ドメインまたはネットワーク所有者の詳細を入力します。
  - IPv4 アドレスは、ピリオドで区切られた 4 つの数値であり、それぞれの数値は 0 ~ 255 でなければなりません (例 : 203.0.113.15)。
  - IPv6 アドレスでは、8 つの 16 ビットの 16 進数値がコロンで区切られて構成されます。  
いずれか 1 箇所、2001:db8:80:1::5 のようにゼロ圧縮を使用できます。
- [メッセージイベント (Message Event)] : 追跡対象のイベントを選択します。オプションは、[ウイルス検出 (Virus Positive)]、[明確なスパム (Spam Positive)]、[サスペクトスパム (Suspect Spam)]、[含まれている悪意のある URL (contained malicious URLs)]、[指定されたカテゴリに含まれている URL (contained URL in specified category)]、[DLP 違反 (DLP Violations)] (DLP ポリシーの名前を入力して、違反の重大度または実行アクションを選択できます)、[DMARC 違反 (DMARC violations)]、[送信完了 (Delivered)]、[高度なマルウェア保護ポジティブ (Advanced Malware Protection Positive)] (添付ファイルで検出されるマルウェア用)、[ハードバウンス (Hard Bounced)]、[ソフトバウンス (Soft Bounced)]、[現在、ポリシー隔離に隔離 (currently in policy quarantine)]、[現在、ウイルス隔離に隔離 (currently in virus quarantine)]、[現在、アウトブレイク隔離に隔離 (currently in outbreak quarantine)]、[メッセージフィルタで検出 (caught by message filters)]、[コンテンツフィルタで検出 (caught by content filters)]、[スパムとして隔離 (Quarantined as Spam)] です。トラッキングクエリに追加する多くの条件と違い、イベントは「OR」演算子を使用して追加します。複数のイベントを選択すると、検索結果は拡大します。

すべてのフィールドに入力する必要はありません。[メッセージイベント (Message Event) ] オプションを除き、クエリは「AND」検索になります。このクエリは、検索フィールドで指定された「AND」条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行のパラメータにテキストストリングを指定すると、クエリは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。

**ステップ 5** [検索 (Search) ] をクリックします。

各行が 1 つの電子メールメッセージに対応します。ビューでメッセージをさらにロードするにはスクロールダウンします。

必要に応じて、新しい検索基準を入力することにより検索を精密化し、クエリを再実行します。あるいは、次の項で説明するように、結果セットを絞り込んで検索精度を高めることもできます。

#### 次のタスク

- [結果セットの絞り込み \(309 ページ\)](#)
- [メッセージトラッキングおよび高度なマルウェア防御機能について \(310 ページ\)](#)
- [トラッキングクエリ結果について \(311 ページ\)](#)

## レガシー Web インターフェイスでの電子メールメッセージの検索

セキュリティ管理アプライアンスのトラッキングサービスを使用して、メッセージ件名行、日時の範囲、エンベロープ送信者または受信者、処理イベント（たとえば、メッセージがウイルス陽性またはスパム陽性かどうかや、ハードバウンスまたは配信されたかどうか）など、指定した条件に一致する特定の電子メールメッセージまたはメッセージのグループを検索できます。メッセージトラッキングでは、メッセージフローの詳細なビューが表示されます。また、特定の電子メールメッセージをドリルダウンし、処理イベント、添付ファイル名、エンベロープおよびヘッダー情報など、メッセージの詳細情報を確認することもできます。



(注) このトラッキングコンポーネントにより個々の電子メールメッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

**ステップ 1** [メール (Email) ] > [メッセージトラッキング (Message Tracking) ] > [メッセージトラッキング (Message Tracking) ] を選択します。

**ステップ 2** (任意) [詳細設定 (Advanced) ] リンクをクリックし、その他の検索オプションを表示します。

**ステップ 3** 検索条件を入力します。

(注) トラッキング検索では、ワイルドカード文字や正規表現はサポートされません。トラッキング検索では大文字と小文字は区別されません。

- [エンベロープ送信者 (Envelope Sender) ] : [次で始まる (Begins With) ]、[次に合致する (IS) ]、または[次を含む (Contains) ]を選択し、テキスト文字列を入力してエンベロープ送信者を検索します。電子メールアドレス、ユーザ名、またはドメインを入力できます。次の形式を使用します。
  - E メール ドメインの場合 : `example.com`, `[203.0.113.15]`, `[ipv6:2001:db8:80:1::5]`
  - 完全 E メール アドレスの場合 : `user@example.com`, `user@[203.0.113.15]` または `user@[ipv6:2001:db8:80:1::5]`。
  - 文字を入力できます。入力した内容は実行されません。
- [エンベロープ受信者 (Envelope Recipient) ] : [次で始まる (Begins With) ]、[次に合致する (IS) ]、または[次を含む (Contains) ]を選択し、テキストを入力してエンベロープ受信者を検索します。電子メールアドレス、ユーザ名、またはドメインを入力できます。

Eメールセキュリティアプライアンスでエイリアス拡張にエイリアステーブルを使用している場合は、本来のエンベロープアドレスではなく、拡張された受信者アドレスが検索されます。それ以外のあらゆる場合においては、メッセージトラッキングクエリによって本来のエンベロープ受信者アドレスが検索されません。

この点を除けば、エンベロープ受信者の有効な検索条件はエンベロープ送信者の場合と同じです。文字を入力できます。入力した内容は実行されません。

- [件名 (Subject) ] : [次で始まる (Begins With) ]、[次に合致する (IS) ]、[次を含む (Contains) ]、または[空である (Is Empty) ]を選択し、テキスト文字列を入力してメッセージ件名行を検索します。
- [受信したメッセージ数 (Message Received) ] : [前日 (Last Day) ]、[最近1週間 (Last 7 Days) ]、または[カスタム範囲 (Custom Range) ]を使用してクエリの日時の範囲を指定します。過去 24 時間以内のメッセージを検索するには [前日 (Last Day) ] オプションを使用し、過去 7 日間のメッセージを検索するには [最近1週間 (Last 7 Days) ] オプションと当日の経過時間を使用します。

日付を指定しなければ、クエリは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。終了日と終了時刻に現在の日付と 23:59 を指定すると、クエリは現在の日付に関するすべてのデータを返します。

日付と時間は、データベースに保管される際に GMT 形式に変換されます。アプライアンス上で日付と時刻を表示する場合は、そのアプライアンスの現地時間で表示されます。

Eメールセキュリティアプライアンスのログに記録され、セキュリティ管理アプライアンスが取得済みのメッセージのみが検索結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メールメッセージが送信された時間と、それがトラッキングとレポートの結果に実際に表示される時間との間にわずかな差が生じることがあります。

- [送信者 IP アドレス (Sender IP Address) ] : 送信者の IP アドレスを入力し、メッセージを検索するか、あるいは拒否された接続だけを検索するかを選択します。
  - IPv4 アドレスは、ピリオドで区切られた 4 つの数値であり、それぞれの数値は 0 ~ 255 でなければなりません (例 : 203.0.113.15) 。
  - IPv6 アドレスでは、8 つの 16 ビットの 16 進数値がコロンで区切られて構成されます。いずれか 1 箇所で、`2001:db8:80:1::5` のようにゼロ圧縮を使用できます。
- [メッセージイベント (Message Event) ] : 追跡対象のイベントを選択します。オプションは、[ウイルス検出 (Virus Positive) ]、[明確なスパム (Spam Positive) ]、[サスペクトスパム (Suspect Spam) ]、

[含まれている悪意のある URL (contained malicious URLs) ]、[指定されたカテゴリに含まれている URL (contained URL in specified category) ]、[DLP 違反 (DLP Violations) ] (DLP ポリシーの名前を入力して、違反の重大度または実行アクションを選択できます)、[DMARC 違反 (DMARC violations) ]、[送信完了 (Delivered) ]、[高度なマルウェア防御ポジティブ (Advanced Malware Protection Positive) ] (添付ファイルで検出されるマルウェア用)、[ハードバウンス (Hard Bounced) ]、[ソフトバウンス (Soft Bounced) ]、[現在、ポリシー隔離に隔離 (currently in policy quarantine) ]、[現在、ウイルス隔離に隔離 (currently in virus quarantine) ]、[現在、アウトブレイク隔離に隔離 (currently in outbreak quarantine) ]、[メッセージフィルタで検出 (caught by message filters) ]、[コンテンツ フィルタで検出 (caught by content filters) ]、[検出されたマクロ ファイル タイプ (Macro File Types Detected) ]、[地理位置情報 (Geolocation) ]、[低リスク (Low Risk) ]、[スパムとして隔離 (Quarantined as Spam) ]です。トラッキングクエリに追加する多くの条件と違い、イベントは「OR」演算子を使用して追加します。複数のイベントを選択すると、検索結果は拡大します。

- [メッセージIDヘッダーとCisco IronPort MID (Message ID Header and Cisco IronPort MID) ]: メッセージ ID ヘッダーのテキスト文字列、Cisco IronPort メッセージ ID (MID)、またはその両方を入力します。
- [クエリ設定 (Query Settings) ]: ドロップダウンメニューから、タイムアウトまでのクエリの実行時間を選択します。オプションは、[1分 (1 minutes) ]、[2分 (2 minutes) ]、[5分 (5 minutes) ]、[10分 (10 minutes) ]、および [時間制限なし (No time limit) ]です。また、クエリが返す結果の最大数を選択します (最大 1000)。
- [添付ファイル名 (Attachment name) ]: [次で始まる (Begins With) ]、[次に合致する (IS) ]、または [次を含む (Contains) ]を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。

すべてのフィールドに入力する必要はありません。[メッセージイベント (Message Event) ] オプションを除き、クエリは「AND」検索になります。このクエリは、検索フィールドで指定された「AND」条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行のパラメータにテキストストリングを指定すると、クエリは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。

#### ステップ 4 [検索 (Search) ] をクリックします。

ページの下部にクエリ結果が表示されます。各行が 1 つの電子メールメッセージに対応します。

各行で検索条件が強調表示されます。

返された行数が [ページ当たりの項目数 (Items per page) ] フィールドで指定した値よりも大きい場合、結果は複数のページに表示されます。ページ間を移動するには、リストの上部または下部にあるページ番号をクリックします。

必要に応じて、新しい検索基準を入力することにより検索を精密化し、クエリを再実行します。あるいは、次の項で説明するように、結果セットを絞り込んで検索精度を高めることもできます。

#### 次のタスク

- [結果セットの絞り込み \(309 ページ\)](#)
- [メッセージトラッキングおよび高度なマルウェア防御機能について \(310 ページ\)](#)

- [トラッキング クエリ結果について \(311 ページ\)](#)

## 結果セットの絞り込み

クエリを実行すると、結果セットに必要以上の情報が含まれていることがあります。新しいクエリを作成するのではなく、結果リストの行内の値をクリックし、結果セットを絞り込みます。値をクリックすると、そのパラメータ値が検索の条件として追加されます。たとえば、クエリ結果に複数の日付のメッセージが含まれている場合、行内の特定の日付をクリックすると、その日付に受信されたメッセージだけが表示されます。

**ステップ 1** 条件として追加する値の上にカーソルを移動します。値が黄色で強調表示されます。

次のパラメータ値を使用して、検索を精密化します。

- Date and time
- メッセージ ID (MID)
- ホスト (E メールセキュリティ アプライアンス)
- Sender
- 受信者 (Recipient)
- メッセージの件名行、または件名の先頭語

**ステップ 2** (新しい Web インターフェイスのみ) メッセージトラッキング検索条件で [変更 (Modify)] をクリックします。

次のパラメータ値を使用して、検索を精密化します。

- Date and time
- メッセージ ID (MID)
- Cisco ホスト (E メールセキュリティ アプライアンス)
- Sender
- 受信者 (Recipient)
- メッセージの件名行、または件名の先頭語
- メッセージ イベント (Message Event)
- その他の詳細 (メッセージの最後の状態、SBRs、送信者 IP、およびグループ)

**ステップ 3** 値をクリックして、検索を精密化します。

[結果 (Results)] セクションに、元のクエリ パラメータおよび追加した新しい条件に一致するメッセージが表示されます。

**ステップ 4** 必要に応じて、結果内の他の値をクリックして、検索をさらに精密化します。

- (注) クエリ条件を削除するには、[クリア (Clear)] をクリックし、新しいトラッキングクエリを実行します。

## メッセージトラッキングおよび高度なマルウェア防御機能について

メッセージトラッキングのファイル脅威情報を検索する際は、次の点に注意してください。

- ファイルレピュテーションサービスで検出された悪質なファイルを検索するには、メッセージトラッキングの [詳細設定 (Advanced)] セクションで、[メッセージイベント (Message Event)] オプションの [高度なマルウェア保護ポジティブ (Advanced Malware Protection Positive)] を選択します。
- メッセージトラッキングにはファイルレピュテーション処理についての情報と、メッセージが処理されたときに返された元のファイルレピュテーションの判定のみが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

メッセージトラッキングの詳細の [処理詳細 (Action Details)] セクションには、以下の情報が表示されます。

- メッセージの各添付ファイルの SHA-256
- メッセージ全体に対する高度なマルウェア防御の最終判定
- マルウェアが検出された添付ファイル  
クリーンな添付ファイルおよびスキャンできない添付ファイルの情報は表示されません。
- 判定のアップデートは [AMP判定のアップデート (AMP Verdict Updates)] レポートでのみ使用できます。メッセージトラッキングの元のメッセージの詳細は、判定が変更されても更新されません。特定の添付ファイルを含むメッセージを表示するには、判定アップデートレポートで SHA-256 をクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析 (File Analysis)] レポートにのみ表示されます。

分析済みファイルのその他の情報は、クラウドから入手できます。ファイルの使用可能なファイル分析情報を表示するには、[モニタ (Monitor)] > [ファイル分析 (File Analysis)] を選択して、ファイルを検索する SHA-256 を入力します。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

分析用に送信されたファイルの後続インスタンスをアプライアンスが処理すると、そのインスタンスはメッセージトラッキングの検索結果に表示されるようになります。

## トラッキングクエリ結果について

結果が予期したものでない場合は、[メッセージトラッキングのトラブルシューティング \(316 ページ\)](#) を参照してください。

トラッキングクエリ結果には、トラッキングクエリで指定した条件に一致するすべてのメッセージがリストされます。[メッセージイベント (Message Event) ]オプションを除き、クエリ条件は「AND」演算子を使用して追加します。結果セット内のメッセージは、すべての「AND」条件を満たしている必要があります。たとえば、エンベロープ送信者はJで始まり、件名はTで始まることを指定すると、クエリは、両方の条件を満たすメッセージだけを返します。

メッセージの詳細情報を表示するには、そのメッセージの新しい Web インターフェイスで [詳細の表示 (More Details) ] または、レガシー Web インターフェイスで [詳細の表示 (Show Details) ] リンクをクリックします。詳細については、[メッセージの詳細 \(312 ページ\)](#) を参照してください。



(注)

- 50 名以上の受信者がいるメッセージは、トラッキングクエリ結果に表示されません。この問題は、今後のリリースで解決される予定です。
- (新しい Web インターフェイスのみ) クエリを指定する場合は、検索結果を表示するために下方向にスクロールすることができます。下方向へスクロールすると、より多くの結果がビューに表示されます。
- 検索結果セクションの上部にある [エクスポート (Export) ] リンクを使用すると、検索結果を .csv ファイルにエクスポートできます。

クエリを指定するとき、最大 1000 件の検索結果を表示するを選択できます。条件に一致したメッセージを最大 50,000 件表示するには、検索結果セクションの上の [すべてをエクスポート (Export All) ] リンクをクリックし、別のアプリケーションで結果の .csv ファイルを開きます。

- レポート ページのリンクをクリックして、メッセージトラッキングのメッセージ詳細を表示し、その結果が予期しないものであった場合、これは、確認期間中にレポートイングとトラッキングを両方同時におよび継続して有効にしていない場合に発生する可能性があります。
- メッセージトラッキングの検索結果の印刷およびエクスポートについては、[レポートイングデータおよびトラッキングデータのエクスポート \(33 ページ\)](#) を参照してください。

### 関連項目

[メッセージの詳細 \(312 ページ\)](#)

## メッセージの詳細

メッセージヘッダー情報や処理の詳細など、特定の電子メールメッセージの詳細情報を表示するには、検索結果リストの任意のアイテムで [詳細の表示 (More Details)] リンクをクリックします。メッセージの詳細が表示された新しいウィンドウが開きます。

メッセージの詳細には次のセクションが含まれます。

- [判定チャートと最後の状態の判定 \(312 ページ\)](#)
- [エンベロープとヘッダーのサマリー \(314 ページ\)](#)
- [ホスト サマリートの送信 \(315 ページ\)](#)
- [処理詳細 \(315 ページ\)](#)

### 判定チャートと最後の状態の判定

判定チャートには、Eメールセキュリティ アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。



---

(注) 12.0 よりも前の AsyncOS では判定チャートが表示されず、最後の状態の判定は [最後の状態が使用不可 (Last State Not Available)] として表示されます。

---

次の表に、各エンジンのさまざまな判定を示します。



表 66: 判定チャート

接続動作	メッセージフィルタ	スパム対策	ウイルス対策	AMP	グレイメール	コンテンツフィルタ	アウトブレイクフィルタ	DLP
N/A 承認 (Accepted)	未評価 (Not Evaluated)	未評価 (Not Evaluated)	未評価 (Not Evaluated)	未評価 (Not Evaluated)	未評価 (Not Evaluated)	未評価 (Not Evaluated)	未評価 (Not Evaluated)	未評価 (Not Evaluated)
リレー済み (Relayed)	一致 (Match) 不一致 (No Match)	負値 疑わしい (Suspect) バルクメール ソーシャルメール マーケティングメール 正值	負値 修復されている (Repaired) 暗号化 (Encryption) スキャン不可 (Unscannable) 正值	クリーン (Clean) 保留中のFA 不明 (Unknown) 省略 (Skipped) 悪意のある (Malicious) スキャン不可 (Unscannable) 低リスク (Low Risk)	負値 正值	一致 (Match) 不一致 (No Match)	一致 (Match) 不一致 (No Match)	トリガーなし (No Trigger) 違反 (Violation) 違反なし (No Violation)

メッセージの最後の状態に関する判定によって、アプライアンス内の各エンジンのすべての可能な判定の後にトリガーされる最終判定が決まります。

次に、いくつかの最後の状態の判定を示します。

- 配信済み (Delivered) : メッセージが配信された場合。
- ドロップ済み (Dropped) : メッセージがドロップされた場合。
- 中止 (Aborted) : メッセージが中止された場合。(例: メールポリシー制限により)
- バウンス済み (Bounced) : メッセージがバウンスされた場合。
- 分裂済み (Splintered) : メッセージの MID が複数の最終状態を持つ複数の MID に分割された場合。
- 隔離済み (Quarantined) : メッセージがエンジンによって隔離された場合。

- キュー登録済み (Queued) : メッセージが、エンド受信者、オフボックス スпам隔離や一元化されたポリシー、ウイルスやアウトブレイクの隔離への配信のキューに登録された場合。
- 処理中 (Processing) : メッセージがすべてのエンジンによって完全に処理されていない場合。または、メッセージがキュー内で特定のエンジンを待機中の場合。
- 最後の状態が使用不可 (Last State Not Available) : メッセージの最後の状態を取得できない場合。(例: メッセージがエンジンによって処理されている場合、まだ最終状態に到達していない場合。)

## エンベロープとヘッダーのサマリー

このセクションには、エンベロープ送信者や受信者など、メッセージのエンベロープとヘッダーの情報が表示されます。収集する情報は次のとおりです。

[受信時間 (Received Time) ] : Eメールセキュリティアプライアンスがメッセージを受信した時間。

[MID] : メッセージ ID。

[件名 (Subject) ] : メッセージの件名行。

メッセージに件名がない場合、またはEメールセキュリティアプライアンスがログファイルに件名行を記録するように設定されていない場合、トラッキング結果内の件名行は「(No Subject)」という値になることがあります。

[エンベロープ送信者 (Envelope Sender) ] : SMTP エンベロープ内の送信者のアドレス。

[エンベロープ受信者 (Envelope Recipients) ] : SMTP エンベロープ内の受信者のアドレス。

[メッセージIDヘッダー (Message ID Header) ] : 各電子メールメッセージを一意に識別する「Message-ID:」ヘッダー。これは最初にメッセージが作成される時に挿入されます。「Message-ID:」ヘッダーは、特定のメッセージを検索する際に役立つ場合があります。

[Cisco ホスト (Cisco Host) ] : メッセージを処理した Eメールセキュリティアプライアンス

[SMTP 認証ユーザ ID (SMTP Auth User ID) ] : 送信者が SMTP 認証を使用して電子メールを送信した場合は、送信者の SMTP 認証ユーザ名。それ以外の場合、この値は「なし (N/A)」となります。

[添付ファイル (Attachments) ] : メッセージに添付されたファイルの名前。

[送信者グループ (Sender Group) ] : メッセージを受信した送信者グループ

[メッセージサイズ (Message Size) ] : メッセージのサイズ

[ポリシー一致 (受信または送信) (Policy Match (Incoming or Outgoing)) ] : メッセージを受信したポリシー



(注) エンジンが詳細を取得できない場合は、値が「N/A」として表示されます。

## ホスト サマリーの送信

[逆引き DNS ホスト名 (Reverse DNS Hostname) ]: 送信側ホストのホスト名。逆引き DNS (PTR) ルックアップで検証されます。

[IPアドレス (IP Address) ]: 送信側ホストの IP アドレス。

[SBRs スコア (SBRs Score) ]: (SenderBase レピュテーションスコア)。範囲は、10 (最も信頼できる送信者) ~ -10 (明らかなスパム送信者) です。スコアが「なし (None)」の場合、そのメッセージが処理された時点で、このホストに関する情報が存在しなかったことを意味します。

## 処理詳細

このセクションには、メッセージの処理中にログに記録されたさまざまなステータスイベントが表示されます。

エントリには、アンチスパムおよびアンチウイルス スキャンなどの電子メール ポリシーの処理や、メッセージ分割などその他のイベントに関する情報が含まれます。

メッセージが配信されると、配信の詳細情報がここに表示されます。たとえば、メッセージが配信され、コピーが隔離に保存されている場合があります。

記録された最新のイベントは、処理の詳細内で強調表示されます。

### [サマリー (Summary) ] タブ

このタブには、メッセージ処理中のすべてのイベントのサマリー ログが表示されます。

### [DLPに一致した内容 (DLP Matched Content) ] タブ

このタブには、データ損失の防止 (DLP) ポリシーに違反するコンテンツが表示されます。

通常、このコンテンツには機密情報、たとえば企業秘密や、クレジットカード番号、健康診断の結果などの個人情報が含まれるため、セキュリティ管理アプライアンスへのアクセス権はあるが管理者レベルの権限を所持していないユーザに対し、このコンテンツへのアクセスを無効化する必要が生じることがあります。「[メッセージトラッキングでの機密情報へのアクセスの制御 \(498 ページ\)](#)」を参照してください。

### [URL 詳細 (URL Details) ] タブ

このタブは、URL レピュテーションおよび URL カテゴリ コンテンツ フィルタ、(メッセージ フィルタではなく) アウトブレイク フィルタで検索されたメッセージのみに表示されます。

このタブには、次の情報が表示されます。

- URL に関連付けられているレピュテーション スコアまたはカテゴリ
- URL に対して実行されたアクション (書き換え、危険の除去、またはリダイレクト)
- メッセージに複数の URL が含まれる場合、フィルタ アクションをトリガーした URL

Eメールセキュリティ アプライアンスが上記の情報を表示するように設定した場合のみ、このタブを表示できます。『*User Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

このタブへのアクセスを制御するには、[メッセージトラッキングでの機密情報へのアクセスの制御](#) (498 ページ)

### [SMTPログ (SMTP Log)] タブ

このセクションでは、電子メールの送信者が SMTP 認証に失敗した場合のメッセージのログを表示します。

### [AMPログ (AMP Log)] タブ

このセクションには、高度なマルウェア防御ファイル レピュテーションおよびファイル分析サービスで検出されたメッセージのログが表示されます

## メッセージトラッキングのトラブルシューティング

- [予想されるメッセージが検索結果に表示されない](#) (316 ページ)
- [添付ファイルが検索結果に表示されない](#) (316 ページ)

### 予想されるメッセージが検索結果に表示されない

#### 問題

条件に一致するメッセージが検索結果に含まれていません。

#### 解決方法

- 多くの検索（特にメッセージイベント検索）は、アプライアンスの設定によって結果が異なります。たとえばフィルタ処理していない URL カテゴリを検索すると、メッセージにそのカテゴリの URL が含まれていても、結果には表示されません。意図した動作を実現するように Eメールセキュリティ アプライアンスが正しく設定されていることを確認します。メールポリシー、コンテンツ フィルタおよびメッセージフィルタ、隔離の設定などを確認してください。
- [メッセージトラッキングデータの有効性の検査](#) (303 ページ) を参照してください。

### 添付ファイルが検索結果に表示されない

#### 問題

添付ファイル名が検出されず、検索結果に表示されません。

#### 解決方法

少なくとも 1 つの受信コンテンツ フィルタまたは本文スキャン機能が ESA で設定され、有効になっています。設定要件 ([セキュリティ管理アプライアンスでの中央集中型電子メールト](#)

[ラッキングのイネーブル化 \(301 ページ\)](#) ) および添付ファイル名検索の制約事項 ([トラッキング サービスの概要 \(299 ページ\)](#) ) を参照してください。

添付ファイルが検索結果に表示されない



## 第 8 章

# スパム隔離

この章は、次の項で構成されています。

- [スパム隔離の概要 \(319 ページ\)](#)
- [ローカルのスパム隔離と外部のスパム隔離 \(320 ページ\)](#)
- [中央集中型スパム隔離の設定 \(320 ページ\)](#)
- [\[スパム隔離の編集 \(Edit Spam Quarantine\)\] ページ \(327 ページ\)](#)
- [セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御 \(328 ページ\)](#)
- [エンドユーザーのためのスパム管理機能の設定 \(340 ページ\)](#)
- [スパム隔離内のメッセージの管理 \(350 ページ\)](#)
- [スパム隔離のディスク領域 \(353 ページ\)](#)
- [外部スパム隔離の無効化について \(353 ページ\)](#)
- [スパム隔離機能のトラブルシューティング \(354 ページ\)](#)

## スパム隔離の概要

スパム隔離 (別名 ISQ) およびエンドユーザー隔離 (別名 EUQ) は、「誤検出」 (アプライアンスが正規の電子メールメッセージをスパムと見なすこと) が問題とされる組織でのセーフガードメカニズムとなります。メッセージがスパムである、またはスパムの疑いがあるとアプライアンスが判断した場合、メッセージを配信または削除する前に、受信者または管理者にそのメッセージを確認してもらうことができます。スパム隔離はこのためにメッセージを保存します。

E メールセキュリティアプライアンスの管理ユーザは、スパム隔離内のすべてのメッセージを閲覧できます。エンドユーザ (通常はメッセージの受信者) は、そのユーザ宛の隔離されたメッセージを、若干異なる Web インターフェイスで表示できます。

スパム隔離は、ポリシー、ウイルス、アウトブレイク隔離とは異なります。

### 関連項目

- [集約されたポリシー、ウイルス、およびアウトブレイク隔離 \(355 ページ\)](#)

## ローカルのスパム隔離と外部のスパム隔離

ローカルのスパム隔離では、Eメールセキュリティ アプライアンスでスパムおよびスパムの疑いがあるメッセージなどを保存します。外部のスパム隔離は、別のCisco コンテンツセキュリティ管理アプライアンスでこれらのメッセージを保存できます。

次の場合は外部のスパム隔離の使用を検討してください。

- 複数のEメールセキュリティ アプライアンスからのスパムを集約して保存および管理する必要がある。
- Eメールセキュリティ アプライアンスで保持可能な量より多くのスパムを保存する必要がある。
- スパム隔離とそのメッセージを定期的にバックアップする必要がある。

## 中央集中型スパム隔離の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	セキュリティ管理アプライアンスで、中央集中型スパム隔離を有効にします。	スパム隔離の有効化と設定 (321 ページ)
ステップ 2	セキュリティ管理アプライアンスで、中央集中型スパム隔離に含めるEメールセキュリティアプライアンスを指定します。	管理対象の各Eメールセキュリティアプライアンスへの中央集中型スパム隔離サービスの追加 (323 ページ)
ステップ 3	通知およびリリースされたスパムの送信用にセキュリティ管理アプライアンスを設定します。	セキュリティ管理アプライアンスでの発信IPインターフェイスの設定 (324 ページ)
ステップ 4	セキュリティ管理アプライアンスで、スパム隔離ブラウザインターフェイスを設定します。	スパム隔離へのブラウザアクセス用IPインターフェイスの設定 (325 ページ)
ステップ 5	Eメールセキュリティアプライアンスがスパム隔離にメールを送信するように設定されていることを確認します。	スパム対策およびメールポリシーの設定の詳細については、『User Guide for AsyncOS for Email Security Appliances』の「Anti-Spam」セクションを参照してください。
ステップ 6	Eメールセキュリティアプライアンスで外部スパム隔離を有効にし、設定します。	詳細については、『User Guide for AsyncOS for Email Security Appliances』を参照してください。
ステップ 7	Eメールセキュリティアプライアンスで、内部隔離を無効にします。	外部スパム隔離をアクティブ化するためのローカルスパム隔離の無効化に関する詳細については、『User Guide for AsyncOS for Email Security Appliances』を参照してください。



## スパム隔離の有効化と設定



(注) 外部のスパム隔離を使用する場合、ここで説明する設定をセキュリティ管理アプライアンスで行います。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] を選択します。
- ステップ 3** システムセットアップウィザードの実行後、スパム隔離を初めて有効にする場合は、次の手順を実行します。
  - a) [有効 (Enable)] をクリックします。
  - b) エンド ユーザ ライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 4** スパム隔離の設定を編集する場合は、[設定の編集 (Edit Settings)] をクリックします。
- ステップ 5** 次のオプションを指定します。

オプション	説明
隔離IPインターフェイス (Quarantine IP Interface) 隔離ポート (Quarantine Port)	デフォルトでは、スパム隔離は管理インターフェイスとポート 6025 を使用します。IP インターフェイスは、着信メールをリスンするように設定されているセキュリティ管理アプライアンスのインターフェイスです。隔離ポートは、送信アプライアンスが外部隔離設定で使用しているポート番号です。  E メールセキュリティアプライアンスがセキュリティ管理アプライアンスと同じネットワークに存在しない場合、管理インターフェイスを使用する必要があります。

オプション	説明
<p>[次を使用してメッセージを配信 (Deliver Messages Via) ]</p>	<p>隔離関係のすべての送信電子メール（スパム通知やスパム隔離からリリースされたメッセージなど）は、メッセージ送信が設定されている他のアプライアンスまたはサーバを経由して配信する必要があります。</p> <p>これらのメッセージは、SMTPまたはグループウェアサーバを使用してルーティングできます。また、Eメールセキュリティアプライアンスの発信リスナーインターフェイス（通常は Data 2 インターフェイス）を指定することもできます。</p> <p>代替用アドレスは、ロードバランシングとフェールオーバーに使用します。</p> <p>Eメールセキュリティアプライアンスが複数台ある場合は、管理対象の任意のEメールセキュリティアプライアンスの発信リスナーインターフェイスをプライマリアドレスまたは代替用アドレスとして使用できます。これらはいずれも同じインターフェイス（Data 1 または Data 2）を発信リスナーとして使用する必要があります。</p> <p>これらのアドレスについての他の注意事項を画面で確認してください。</p>
<p>[隔離サイズ (Quarantine Size) ]</p>	<p>[ディスクに空き容量がない場合、自動的に古いメッセージから順番に削除する (When storage space is full, automatically delete oldest messages first) ]の選択を解除すると、満杯になった隔離エリアに新しいメッセージが追加されなくなります。隔離エリアが満杯になることでアプライアンス上にメッセージの待ち行列（渋滞）ができることがないように、このオプションを有効にすることを推奨します。</p> <p>隔離のディスク領域を管理するには、<a href="#">ディスク領域の管理 (567 ページ)</a> を参照してください。</p>
<p>次の日数の経過後に削除 (Schedule Delete After)</p>	<p>メッセージを削除する前に保持する日数を指定します。</p> <p>隔離エリアの容量が満杯になるのを防ぐために、古いメッセージから削除するように隔離を設定することを推奨します。自動削除をスケジュールしないという選択も可能です。</p>
<p>[メッセージのリリース時にCiscoに通知 (Notify Cisco Upon Message Release) ]</p>	<p>—</p>

オプション	説明
[スパム隔離のアピアランス (Spam Quarantine Appearance) ]	<p><b>ロゴ (Logo)</b></p> <p>デフォルトでは、ユーザがログインして隔離されたメッセージを確認するときに、スパム隔離のページの最上部にシスコロゴが表示されます。</p> <p>ロゴは、新しい Web インターフェイスとレガシー Web インターフェイスの両方で表示できます。</p> <p>代わりにカスタムロゴを使用するには、そのロゴをアップロードします。ロゴは、高さ 50 ピクセル、幅 500 ピクセルまでの .jpg、.gif、または .png ファイルにする必要があります。</p> <p><b>ログインページメッセージ (Login page message)</b></p> <p>(任意) ログインページメッセージを指定します。このメッセージは、隔離を閲覧するためにエンドユーザおよび管理者がログインするときに表示されます。</p> <p>メッセージを指定しない場合、次のメッセージが表示されます。</p> <p>ログイン情報を入力してください。入力する情報がわからない場合は、管理者に問い合わせてください。(Enter your login information below. If you are unsure what to enter, please contact your administrator.)</p>
管理ユーザ (Administrative Users)	<p><a href="#">スパム隔離への管理ユーザアクセスの設定 (326ページ)</a> を参照してください。</p>

**ステップ 6** 変更を送信し、保存します。

次のタスク

- [中央集中型スパム隔離の設定 \(320 ページ\)](#) に戻ります。

## 管理対象の各 E メールセキュリティ アプライアンスへの中央集中型スパム隔離サービスの追加

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

- ステップ 2** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] を選択します。
- ステップ 3** このページのリストに、すでに E メールセキュリティアプライアンスを追加している場合は、次の手順を実行します。
- E メールセキュリティアプライアンスの名前をクリックします。
  - [スパム隔離 (Spam Quarantine) ] サービスを選択します。
- ステップ 4** E メールセキュリティアプライアンスをまだ追加していない場合は、次の手順を実行します。
- [メールアプライアンスの追加 (Add Email Appliance) ] をクリックします。
  - [アプライアンス名 (Appliance Name) ] および [IP アドレス (IP Address) ] テキストフィールドに、アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。
- (注) [IP アドレス (IP Address) ] フィールドに DNS 名を入力した場合でも、[送信 (Submit) ] をクリックすると、IP アドレスに変換されます。
- Spam Quarantine サービスが事前に選択されています。
  - [接続の確立 (Establish Connection) ] をクリックします。
  - 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection) ] をクリックします。
- (注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。
- 「Success」メッセージがページのテーブルの上に表示されるまで待機します。
  - [テスト接続 (Test Connection) ] をクリックします。
  - テーブルの上のテスト結果を確認します。
- ステップ 5** [送信 (Submit) ] をクリックします。
- ステップ 6** スパム隔離を有効にする E メールセキュリティアプライアンスごとに、この手順を繰り返します。
- ステップ 7** 変更を保存します。

---

## セキュリティ管理アプライアンスでの発信 IP インターフェイスの設定

セキュリティ管理アプライアンスで、隔離に関するメッセージ（通知やリリースされた電子メールなど）を E メールセキュリティアプライアンスに送信するインターフェイスを設定します。

### 始める前に

発信インターフェイスに使用する IP アドレスを入手または特定します。通常、これはセキュリティ管理アプライアンスの Data2 インターフェイスのものになります。ネットワーク要件の詳細については、を参照してください。 [ネットワークと IP アドレスの割り当て \(639 ページ\)](#)

**ステップ 1** この手順は、次の説明と併せて実行してください [IP インターフェイスの設定](#) (632 ページ)

**ステップ 2**

**ステップ 3** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理 コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 4** [管理アプライアンス (Management Appliance) ]>[ネットワーク IP インターフェイス (Network IP Interfaces) ] を選択します。

**ステップ 5** [IP インターフェイスの追加 (Add IP Interface) ] をクリックします。

**ステップ 6** 次の設定値を入力します。

- [名前 (Name) ]

- イーサネット ポート (Ethernet Port)

通常は Data 2 になります。具体的には、この設定は [管理アプライアンス (Management Appliance) ]> [集約管理サービス (Centralized Services) ]> [スパム隔離 (Spam Quarantine) ] の [スパム隔離設定 (Spam Quarantine Settings) ] ページにおいて、[次を使用してメッセージを配信 (Deliver Messages Via) ] セクションで [プライマリサーバ (Primary Server) ] に指定した E メール セキュリティ アプライアンスのデータ インターフェイスと同じである必要があります。

- [IP アドレス (IP Address) ]

上で指定したインターフェイスの IP アドレス。

- ネットマスク

- ホストネーム

たとえば、Data 2 インターフェイスの場合は、data2.sma.example.com を使用します。

このインターフェイスの [スパム隔離 (Spam Quarantine) ] セクションには入力しないでください。

**ステップ 7** 変更を送信し、保存します。

## スパム隔離へのブラウザアクセス用 IP インターフェイスの設定

管理者およびエンド ユーザがスパム隔離にアクセスするときには、別のブラウザ ウィンドウが開きます。

**ステップ 1**

**ステップ 2** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理 コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 3** [管理アプライアンス (Management Appliance) ]>[ネットワーク (Network) ]> [IP インターフェイス (IP Interfaces) ] を選択します。

**ステップ 4** 管理インターフェイスの名前をクリックします。

**ステップ 5** [スパム隔離 (Spam Quarantine)] セクションで、スパム隔離にアクセスするための設定を行います。

- デフォルトでは、HTTP がポート 82 を使用し、HTTPS がポート 83 を使用します。
- 通知とスパム隔離のブラウザ ウィンドウに記載される URL を指定します。

使用しているセキュリティ管理アプライアンスのホスト名をエンドユーザに表示したくない場合は、代替りのホスト名を指定できます。

**ステップ 6** 変更を送信し、保存します。

### 次のタスク

スパム隔離アクセス用に指定したホスト名を DNS サーバが解決できることを確認します。

## スパム隔離への管理ユーザアクセスの設定

管理者権限を持つすべてのユーザは、スパム隔離設定を変更したり、スパム隔離内のメッセージを表示および管理したりすることができます。管理者ユーザに対してスパム隔離アクセスを設定する必要はありません。

次のロールのユーザに対してスパム隔離へのアクセスを設定すると、これらのユーザはスパム隔離内のメッセージを表示、リリース、削除できます。

- Email administrator
- 演算子
- Read-Only Operator
- Help desk user
- ゲスト
- スпам隔離権限を持つカスタム ユーザ ロール

これらのユーザはスパム隔離設定にアクセスできません。

### 始める前に

スパム隔離にアクセスできるユーザまたはカスタム ユーザ ロールを作成します。詳細については、の項で[カスタム ユーザ ロールの隔離へのアクセス \(476 ページ\)](#) に関する情報 [管理タスクの分散 \(469 ページ\)](#) を参照してください。

**ステップ 1** スпам隔離設定ページをまだ編集していない場合は、次の手順を実行します。

- a)
- b) (新しいWebインターフェイスのみ) クラウドEメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- c) [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [モニター (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。

- d) **[設定の編集 (Edit Settings)]** **[スパム隔離 (Spam Quarantine)]** セクションの **[隔離名 (Quarantine Name)]** 列の **[スパム隔離 (Spam Quarantine)]** リンクをクリックします。

**ステップ 2** 追加するユーザタイプ (ローカル、外部認証、またはカスタム ロール) のリンクをクリックします。

ユーザまたはロールを追加済みの場合は、ユーザ名かロールをクリックすると、すべての対象ユーザまたはロールが表示されます。

**ステップ 3** 追加するユーザまたはロールを選択します。

管理者権限を持つユーザ (電子メール管理者を含む) は、スパム隔離へのフルアクセスが自動的に与えられるため、表示されません。

**ステップ 4** **[OK]** をクリックします。

**ステップ 5** 変更を送信し、保存します。

---

次のタスク

関連項目

[スパム隔離へのエンドユーザ アクセスの設定 \(343 ページ\)](#)

## 隔離対象のメールの受信者の制限

複数のメール ポリシーを使用して (**[メールポリシー (Mail Policies)]** > **[受信メールポリシー (Incoming Mail Policy)]**)、メールの隔離対象から除外する受信者アドレスのリストを指定できます。そのメールポリシーにアンチスパムを設定する際、隔離の代わりに **[配信 (Deliver)]** または **[ドロップ (Drop)]** を選択します。

## スパム隔離の言語

各ユーザは、ウィンドウの右上にある **[オプション (Options)]** メニューからスパム隔離の言語を選択します。

## **[スパム隔離の編集 (Edit Spam Quarantine)]** ページ

- [スパム隔離の有効化と設定 \(321 ページ\)](#)
- [ローカルのスパム隔離と外部のスパム隔離 \(320 ページ\)](#)
- [スパム隔離へのエンドユーザ アクセスの設定 \(343 ページ\)](#)
- [エンドユーザへの隔離されたメッセージに関する通知 \(346 ページ\)](#)

## セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御

管理者およびエンドユーザは、メッセージがスパムであるかどうかを判断するためにセーフリストとブロックリストを使用できます。セーフリストでは、スパムとして処理しない送信者およびドメインが指定されます。ブロックリストでは、常にスパムとして処理する送信者およびドメインが指定されます。

エンドユーザ（電子メールユーザ）に各自の電子メールアカウントのセーフリストとブロックリストの管理を許可することができます。たとえば、エンドユーザは、もう興味のないメーリングリストから電子メールを受信している場合があります。そのようなユーザは、このメーリングリストからの電子メールが自分の受信箱に送信されないように、その送信者を自分のブロックリストに追加できます。また、エンドユーザは、スパムではない特定の送信者からの電子メールが自分のスパム隔離に送信されていることに気づくこともあります。これらの送信者からのメッセージが隔離されないようにするために、エンドユーザはそれらの送信者を自分のセーフリストに追加できます。

エンドユーザおよび管理者が行った変更はお互いに表示され、両者が変更できます。

### 関連項目

- [セーフリストとブロックリストのメッセージ処理](#) (328 ページ)
- [セーフリストとブロックリストの有効化](#) (329 ページ)
- [外部スパム隔離およびセーフリスト/ブロックリスト](#) (330 ページ)
- [セーフリストおよびブロックリストへの送信者とドメインの追加 \(管理者\)](#) (330 ページ)
- [セーフリストおよびブロックリストへのエンドユーザ アクセスについて](#) (336 ページ)
- [セーフリスト/ブロックリストのバックアップと復元](#) (338 ページ)
- [セーフリストとブロックリストのトラブルシューティング](#) (339 ページ)

## セーフリストとブロックリストのメッセージ処理

セーフリストまたはブロックリストに送信者を追加しても、アプライアンスではメッセージに対するウイルスのスキャンや、内容に関連したメールポリシーの基準をメッセージが満たすかどうかの判定が行われます。受信者のセーフリストにメッセージの送信者が含まれていても、他のスキャン設定と結果によってはメッセージが配信されない場合があります。

セーフリストとブロックリストを有効にすると、アプライアンスは、アンチスパムスキャンの直前にセーフリスト/ブロックリストデータベースと照合してメッセージをスキャンします。アプライアンスがセーフリストまたはブロックリストのエントリに一致する送信者またはドメインを検出した場合、受信者が複数存在すると（かつ各受信者のセーフリスト/ブロックリスト設定が異なると）、そのメッセージは分裂します。たとえば、受信者 A と受信者 B の両方に送信されるメッセージがあるとします。受信者 A のセーフリストにはこの送信者のエントリがありますが、受信者 B のセーフリストおよびブロックリストにはエントリがありません。こ



の場合、メッセージは2つのメッセージ ID で2つのメッセージに分割されます。受信者 A に送信されるメッセージは、セーフリストに一致していることが X-SLBL-Result-セーフリストヘッダーによってマークされ、アンチスパム スキャンをスキップします。一方、受信者 B 宛のメッセージは、アンチスパム スキャン エンジンによってスキャンされます。その後、どちらのメッセージもパイプライン（アンチウイルス スキャン、コンテンツ ポリシーなど）を続行し、設定されているすべての設定に従います。

メッセージの送信者またはドメインがブロックリストに含まれる場合の配信の動作は、セーフリスト/ブロックリスト機能を有効にするときに指定したブロックリストアクションによって決まります。セーフリストの配信の場合と同様に、セーフリスト/ブロックリスト設定の異なる複数の受信者が存在すると、そのメッセージは分裂します。分裂したメッセージのうちブロックリストに含まれるものは、ブロックリストアクション設定に応じて隔離されるかドロップされます。隔離を実行するようにブロックリストアクションが設定されている場合、そのメッセージはスキャンされ、最終的に隔離されます。削除するようにブロックリストアクションが設定されている場合、そのメッセージは、セーフリスト/ブロックリスト スキャンの直後にドロップされます。

セーフリストとブロックリストはスパム隔離内に保持されているため、配信の動作は、他のアンチスパム設定にも左右されます。たとえば、アンチスパムスキャンをスキップするようにホストアクセス テーブル (HAT) で「承認 (Accept)」メールフロー ポリシーを設定すると、そのリスナー上でメールを受信するユーザは、自分のセーフリストとブロックリストの設定がそのリスナー上で受信されたメールに適用されなくなります。同様に、一部のメッセージ受信者についてアンチスパム スキャンをスキップするメール フロー ポリシーを作成すると、それらの受信者は、自分のセーフリストとブロックリストの設定が適用されなくなります。

#### 関連項目

- [セーフリストとブロックリストの有効化 \(329 ページ\)](#)
- [外部スパム隔離およびセーフリスト/ブロックリスト \(330 ページ\)](#)

## セーフリストとブロックリストの有効化

#### 始める前に

- スпам隔離を有効にする必要があります。「[中央集中型スパム隔離の設定 \(320ページ\)](#)」を参照してください。

#### ステップ 1

**ステップ 2** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理 コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 3** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。

**ステップ 4** [エンドユーザセーフリスト/ブロックリスト(スパム隔離) (End-User Safelist/Blocklist (Spam Quarantine))] セクションで [有効 (Enable)] を選択します。

**ステップ5** [エンドユーザセーフリスト/ブロックリスト機能を有効にする (Enable End User Safelist/Blocklist Feature) ] を選択します。

**ステップ6** [ユーザごとの最大一覧項目数 (Maximum List Items Per User) ] を指定します。

これは、各受信者のリストごとのアドレスまたはドメインの最大数です。ユーザごとのリストエントリ数を大きくすると、システムのパフォーマンスに悪影響を与えることがあります。

**ステップ7** 変更を送信し、保存します。

## 外部スパム隔離およびセーフリスト/ブロックリスト

E メールセキュリティ アプライアンスは受信メールの処理時にセーフリストとブロックリスト内の送信者を評価するため、セキュリティ管理アプライアンスに保存されているセーフリストおよびブロックリストが受信メールに適用されるように、これらをEメールセキュリティアプライアンスに送信する必要があります。セキュリティ管理アプライアンスでセーフリスト/ブロックリスト機能を設定する際に、その更新頻度を設定します。

## セーフリストおよびブロックリストへの送信者とドメインの追加 (管理者)

スパム隔離のインターフェイスでセーフリストとブロックリストを管理します。

多数の受信者 (組織のエンドユーザ) が特定の送信者またはドメインをホワイトリストまたはブラックリストに追加しているかどうかを確認できます。

管理者は、各エンドユーザが表示および操作する同じエントリのスーパーセットを表示して操作します。

### 始める前に

- スパム隔離にアクセスできることを確認します。 [スパム隔離へのアクセス \(管理ユーザ\) \(351 ページ\)](#) を参照してください。
- セーフリスト/ブロックリストへのアクセスを有効にします。 [セーフリストとブロックリストの有効化 \(329 ページ\)](#) を参照してください。
- (任意) このセクションの手順を使用してこれらのリストを作成する代わりに、セーフリスト/ブロックリストをインポートするには、 [セーフリスト/ブロックリストのバックアップと復元 \(338 ページ\)](#) で説明する手順を使用します。
- セーフリストとブロックリストのエントリの必須形式を把握します。 [セーフリストエントリとブロックリストエントリの構文 \(335 ページ\)](#) を参照してください。

**ステップ1** (新しいWebインターフェイスのみ) クラウドメールセキュリティ管理コンソールで、[隔離 (Quarantine) ] > [スパム隔離 (Spam Quarantine) ] > [検索 (Search) ] をクリックします。

または

[電子メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [スパム隔離 (Spam Quarantine)] を選択し、ページの右上隅にある [オプション (Options)] ドロップダウンメニューを選択します。

**ステップ 2** [セーフリスト (Safelist)] または [ブロックリスト (Blocklist)] を選択します。

**ステップ 3** (任意) 送信者または受信者を検索します。

**ステップ 4** 次の 1 つまたは複数の操作を実行します。

目的	操作手順
<p>1 人の受信者に対して複数の送信者を追加する</p>	<p>新しい Web インターフェイスで 1 人の受信者に複数の送信者を追加する場合</p> <ol style="list-style-type: none"> <li>1. [受信者 (Recipients)] タブを選択します。</li> <li>2. +アイコンをクリックして、受信者のアドレスと送信者リストを追加します。</li> <li>3. 受信者の電子メールアドレスを入力します。</li> <li>4. 送信者の電子メールアドレスとドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。</li> <li>5. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</li> </ol> <p>既存の送信者アドレスを変更するには、必要な受信者アドレスの横にあるチェックボックスをオンにして編集アイコンをクリックし、送信者のアドレスを変更してから <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</p> <p>レガシー Web インターフェイスで 1 人の受信者に複数の送信者を追加する場合</p> <ol style="list-style-type: none"> <li>1. [表示方法 : 受信者 (View by: Recipient)] を選択します。</li> <li>2. [追加 (Add)] をクリックするか、受信者の [編集 (Edit)] をクリックします。</li> <li>3. 受信者の電子メールアドレスを入力または編集します。</li> <li>4. 送信者の電子メールアドレスおよびドメインを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。</li> <li>5. [送信 (Submit)] をクリックします。</li> </ol>

目的	操作手順
<p>1 人の送信者に対して複数の受信者を追加する</p>	<p>新しい Web インターフェイスで 1 人の送信者に複数の受信者を追加する場合</p> <ol style="list-style-type: none"> <li>1. [送信者 (Sender) ] タブを選択します。</li> <li>2. + をクリックして、送信者のアドレスと受信者リストを追加します。</li> <li>3. 送信者のアドレスまたはドメインを入力します。</li> <li>4. 受信者の電子メールアドレスを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。</li> <li>5. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</li> </ol> <p>既存の受信者アドレスを変更するには、必要な送信者アドレスの横にあるチェックボックスをオンにして編集アイコンをクリックし、送信者のアドレスを変更してから <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</p> <p>レガシー Web インターフェイスで 1 人の送信者に複数の受信者を追加する場合</p> <ol style="list-style-type: none"> <li>1. [表示方法：送信者 (View by: Sender) ] を選択します。</li> <li>2. [追加 (Add) ] をクリックするか、または送信者の [編集 (Edit) ] をクリックします。</li> <li>3. 送信者アドレスまたはドメインを入力または編集します。</li> <li>4. 受信者の電子メールアドレスを入力します。 各エントリを別の行に入力するか、各エントリをカンマで区切ります。</li> <li>5. [送信 (Submit) ] をクリックします。</li> </ol>

目的	操作手順
<p>受信者に関連付けられたすべての送信者を削除する</p>	<p>新しい Web インターフェイスで 1 人の受信者に関連付けられたすべての送信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 すべてのエントリを選択し、削除することができます。</li> <li>2. ごみ箱アイコンをクリックしてテーブル行全体を削除できます。</li> </ol> <p>レガシー Web インターフェイスで 1 人の受信者に関連付けられたすべての送信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. [表示方法 (View by) ] オプションを選択します。</li> <li>2. ゴミ箱アイコンをクリックしてテーブル行全体を削除します。</li> </ol>
<p>送信者に関連付けられたすべての受信者を削除する</p>	<p>新しい Web インターフェイスで 1 人の送信者に関連付けられたすべての受信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 すべてのエントリを選択し、削除することができます。</li> <li>2. ごみ箱アイコンをクリックしてテーブル行全体を削除できます。</li> </ol> <p>レガシー Web インターフェイスで 1 人の送信者に関連付けられたすべての受信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. [表示方法 (View by) ] オプションを選択します。</li> <li>2. ゴミ箱アイコンをクリックしてテーブル行全体を削除します。</li> </ol>

目的	操作手順
受信者の個々の送信者を削除する	<p>新しい Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 複数のエントリを選択、削除することができます。</li> <li>2. 編集アイコンをクリックして、個々の受信者または送信者を変更します。</li> <li>3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。</li> <li>4. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</li> </ol> <p>レガシー Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. [表示方法 (View by) ] オプションを選択します。</li> <li>2. 個々の受信者または送信者の [編集 (Edit) ] をクリックします。</li> <li>3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。</li> <li>4. [送信 (Submit) ] をクリックします。</li> </ol>

目的	操作手順
送信者の個々の受信者を削除する	<p>新しい Web インターフェイスで 1 人の送信者の個々の受信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. 受信者または送信者のアドレスの横にあるチェックボックスをオンにしてエントリを選択します。 複数のエントリを選択、削除することができます。</li> <li>2. 編集アイコンをクリックして、個々の受信者または送信者を変更します。</li> <li>3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。</li> <li>4. <input checked="" type="checkbox"/> をクリックしてエントリを保存します。</li> </ol> <p>レガシー Web インターフェイスで 1 人の受信者の個々の送信者を削除する場合</p> <ol style="list-style-type: none"> <li>1. [表示方法 (View by)] オプションを選択します。</li> <li>2. 個々の受信者または送信者の [編集 (Edit)] をクリックします。</li> <li>3. テキストボックスでエントリを追加または削除します。少なくとも 1 つはエントリを残す必要があります。</li> <li>4. [送信 (Submit)] をクリックします。</li> </ol>

次のタスク

関連項目

- [セーフリスト エントリとブロックリスト エントリの構文 \(335 ページ\)](#)
- [すべてのセーフリストおよびブロックリストのクリア \(336 ページ\)](#)

## セーフリスト エントリとブロックリスト エントリの構文

送信者を次の形式でセーフリストとブロックリストに追加できます。

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

送信者アドレスやドメインなどの同一エントリを、セーフリストとブロックリストの両方に同時に追加することはできません。ただし、ドメインをセーフリストに追加し、そのドメインに所属する送信者の電子メールアドレスをブロックリストに追加すること(またはその逆)は可能です。両方のルールが適用されます。たとえば `example.com` がセーフリストに含まれている場合、`george@example.com` をブロックリストに追加することができます。この場合アプライアンスは、スパムとして処理される `george@example.com` からのメールを除いて、`example.com` からのすべてのメールをスパムのスキャンなしで配信します。

`.domain.com` のような構文を使用して、サブドメインの範囲を許可したり、ブロックしたりすることはできません。ただし、構文 `server.domain.com` を使用して特定のドメインをブロックすることは可能です。

## すべてのセーフリストおよびブロックリストのクリア

すべての送信者と受信者を含む、セーフリストおよびブロックリストのすべてのエントリを削除する必要がある場合は、[セーフリスト/ブロックリストのバックアップと復元 \(338 ページ\)](#) の手順を使用してエントリなしでファイルをインポートします。

## セーフリストおよびブロックリストへのエンドユーザアクセスについて

エンドユーザはスパム隔離から各自のセーフリストとブロックリストにアクセスします。スパム隔離へのエンドユーザアクセスを設定するには、[Web ブラウザからのスパム隔離へのエンドユーザアクセスの設定 \(343 ページ\)](#) を参照してください。

必要に応じて、スパム隔離の URL と下記の手順をエンドユーザに提供してください。

### 関連項目

- [セーフリストへのエントリの追加 \(エンドユーザ\) \(336 ページ\)](#)
- [ブロックリストへの送信者の追加 \(エンドユーザ\) \(337 ページ\)](#)

## セーフリストへのエントリの追加 (エンドユーザ)



(注) セーフリストに登録されている送信者からのメッセージの配信は、システムの他の設定によって異なります。[セーフリストとブロックリストのメッセージ処理 \(328 ページ\)](#) を参照してください。

エンドユーザは、次の 2 つの方法で送信者をセーフリストに追加できます。

- [隔離されたメッセージの送信者のセーフリストへの追加 \(337 ページ\)](#)
- [隔離されたメッセージのない送信者のセーフリストへの追加 \(337 ページ\)](#)



## 隔離されたメッセージの送信者のセーフリストへの追加

エンドユーザは、スパム隔離に送信されたメッセージの送信者をセーフリストに追加できません。

---

(新しい Web インターフェイスのみ) [リリースしてセーフリストに追加 (Release and Add to Safelist)] アイコンをクリックしてメッセージをリリースし、セーフリストに追加します。

または

ドロップダウンメニューから [リリースしてセーフリストに追加 (Release and Add to Safelist)] を選択します。

指定したメールのエンベロープ送信者と差出人ヘッダーが両方ともセーフリストに追加されます。解放されたメッセージは、それ以降の電子メールパイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。

---

## 隔離されたメッセージのない送信者のセーフリストへの追加

**ステップ 1** (新しい Web インターフェイスのみ) [セーフリスト (Safelist)] を選択します。

**ステップ 2** (新しい Web インターフェイスのみ) 電子メールアドレスまたはドメインを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。

**ステップ 3** (新しい Web インターフェイスのみ)  をクリックしてエントリを保存します。

**ステップ 4** [スパム隔離 (Spam Quarantine)] ページにアクセスします。

- [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。
  - ページの右上隅にある [オプション (Options)] ドロップダウンメニューを選択します。
  - [セーフリスト (Safelist)] を選択します。
  - [セーフリスト (Safelist)] ダイアログボックスから、電子メールアドレスまたはドメインを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
  - [一覧に追加 (Add to List)] をクリックします。
- 

## ブロックリストへの送信者の追加 (エンドユーザ)

ブロックリストに登録されている送信者からのメッセージは、管理者が定義したセーフリスト/ブロックリストアクション設定に応じて、拒否または隔離されます。



---

(注) この手順でのみブロックリスト エントリを追加できます。

---

- ステップ 1** (新しい Web インターフェイスのみ) [ブロックリスト (Blocklist)] を選択し、[+] アイコンをクリックして、ブロックリストに追加するドメインまたは電子メールアドレスを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
- ステップ 2** (新しい Web インターフェイスのみ)  をクリックしてエントリを保存します。
- ステップ 3** [スパム隔離 (Spam Quarantine)] ページにアクセスします。
- [モニタ (Monitor)] > [スパム隔離 (Spam Quarantine)] を選択します。
  - ページの右上にある [オプション (Options)] ドロップダウンメニューから [ブロックリスト (Blocklist)] を選択します。
  - ブロックリストに追加するドメインまたは電子メールアドレスを入力します。ドメインと電子メールアドレスは、コンマで区切って複数入力できます。
  - [一覧に追加 (Add to List)] をクリックします。

## セーフリスト/ブロックリストのバックアップと復元

アプライアンスをアップグレードする場合、またはインストールウィザードを実行する場合、事前にセーフリスト/ブロックリスト データベースをバックアップする必要があります。セーフリスト/ブロックリストの情報は、アプライアンスの設定が格納されるメインの XML コンフィギュレーションファイルには含まれていません。

セーフリスト/ブロックリスト エントリは、セキュリティ管理アプライアンスの他のデータと共にバックアップすることもできます。[セキュリティ管理アプライアンスのデータのバックアップ \(513 ページ\)](#) を参照してください。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [設定ファイル (Configuration File)] を選択します。
- ステップ 3** [エンドユーザセーフリスト/ブロックリストデータベース(スパム隔離) (End-User Safelist/Blocklist Database (Spam Quarantine))] セクションまでスクロールします。

目的	操作手順
セーフリスト/ブロックリストをエクスポートする	.csv ファイルのパスおよびファイル名をメモし、必要に応じて変更します。 [すぐにバックアップ (Backup Now)] をクリックします。 アプライアンスは次の命名規則を使用して、アプライアンスの /configuration ディレクトリに .csv ファイルを保存します。 <i>slbl-&lt;serial number&gt;-&lt;timestamp&gt;.csv</i>

目的	操作手順
セーフリスト/ブロックリストをインポートする	<p><b>注意</b> このプロセスによって、すべてのユーザのセーフリストおよびブロックリストの既存のエントリがすべて上書きされます。</p> <p>[リストアするファイルを選択 (Select File to Restore) ] をクリックします。</p> <p>configuration ディレクトリ内のファイル リストから目的のファイルを選択します。</p> <p>復元するセーフリスト/ブロックリストバックアップファイルを選択します。</p> <p>[復元 (Restore) ] をクリックします。</p>

## セーフリストとブロックリストのトラブルシューティング

セーフリストとブロックリストに関する問題をトラブルシューティングするために、ログファイルまたはシステム アラートを表示できます。

電子メールがセーフリスト/ブロックリスト設定によってブロックされると、そのアクションが `ISQ_log` ファイルまたはアンチスパム ログ ファイルに記録されます。セーフリストに含まれる電子メールは、セーフリストに一致していることが `X-SLBL-Result`-セーフリストヘッダーによってマークされます。ブロックリストに含まれる電子メールは、ブロックリストに一致していることが `X-SLBL-Result`-ブロックリストヘッダーによってマークされます。

アラートは、データベースが作成または更新されたり、データベースの変更またはセーフリスト/ブロックリスト プロセスの実行においてエラーが発生したりすると送信されます。

アラートの詳細については、[アラートの管理 \(541 ページ\)](#) を参照してください。

ログ ファイルの詳細については、[ログ \(585 ページ\)](#) を参照してください。

### 関連項目

- [セーフリストに登録されている送信者からのメッセージが配信されない \(339 ページ\)](#)

## セーフリストに登録されている送信者からのメッセージが配信されない

### 問題

セーフリストに登録されている送信者からのメッセージが配信されませんでした。

### 解決方法

考えられる原因 :

- マルウェアまたはコンテンツ違反のためメッセージがドロップされました。[セーフリストとブロックリストのメッセージ処理 \(328 ページ\)](#) を参照してください。
- アプライアンスが複数あり、その送信者をセーフリストに最近追加した場合、メッセージが処理された時点ではセーフリスト/ブロックリストが同期されていなかった可能性があります。

ります。外部スパム隔離およびセーフリスト/ブロックリスト (330 ページ) を参照してください。

## エンドユーザーのためのスパム管理機能の設定

目的	参照先
スパム管理機能へのエンドユーザーアクセスのさまざまな認証方式について、利点と制限事項を把握します。	スパム隔離へのエンドユーザーアクセスの設定 (343 ページ) およびサブセクション
エンドユーザーがブラウザから直接スパム隔離にアクセスすることを許可します。	スパム管理機能にアクセスするエンドユーザーの認証オプション (340 ページ)
メッセージがスパム隔離にルーティングされたときに、その宛先のユーザーに通知を送信します。 通知にはスパム隔離へのリンクを含めることができます。	エンドユーザーへの隔離されたメッセージに関する通知 (346 ページ)
ユーザーが、安全であると判断した送信者、およびスパムまたはその他の無用なメールを送信すると判断した送信者の電子メールアドレスとドメインを指定できるようにします。	セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御 (328 ページ)

### 関連項目

- スпам管理機能にアクセスするエンドユーザーの認証オプション (340 ページ)
- Web ブラウザからのスパム隔離へのエンドユーザーアクセスの設定 (343 ページ)
- エンドユーザーへの隔離されたメッセージに関する通知 (346 ページ)

## スパム管理機能にアクセスするエンドユーザーの認証オプション



(注) メールボックス認証では、ユーザーが電子メールエイリアス宛てのメッセージを表示することはできません。

エンドユーザによるスパム隔離へのアクセスの場合	操作手順
Web ブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証必須	<ol style="list-style-type: none"> <li>[エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、[LDAP]、[SAML 2.0] または [メールボックス (IMAP/POP) (Mailbox (IMAP/POP))] を選択します。</li> <li>[スパム通知 (Spam Notifications)] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする (Enable login without credentials for quarantine access)] の選択を解除します。</li> </ol>
Web ブラウザから直接アクセス、認証必須 および 通知内のリンク経由でアクセス、認証不要	<ol style="list-style-type: none"> <li>[エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、[LDAP]、[SAML 2.0] または [メールボックス (IMAP/POP) (Mailbox (IMAP/POP))] を選択します。</li> <li>[スパム通知 (Spam Notifications)] 設定で、[隔離へのアクセスに証明書なしのログインを有効にする (Enable login without credentials for quarantine access)] をオンにします。</li> </ol>
通知内のリンク経由でのみアクセス、認証不要	[エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、認証方式として [なし (None)] を選択します。
アクセスなし	[エンドユーザ隔離アクセス (End User Quarantine Access)] 設定で、[エンドユーザの隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] の選択を解除します。

関連項目

- [LDAP 認証プロセス \(341 ページ\)](#)
- [IMAP/POP 認証プロセス \(342 ページ\)](#)
- [SAML 2.0 認証プロセス \(343 ページ\)](#)
- [スパム隔離へのエンドユーザ アクセスの設定 \(343 ページ\)](#)
- [エンドユーザへの隔離されたメッセージに関する通知 \(346 ページ\)](#)
- [スパム隔離と連携させるための LDAP の設定 \(434 ページ\)](#)
- [セーフリストおよびブロックリストへのエンドユーザ アクセスについて \(336 ページ\)](#)

## LDAP 認証プロセス

1. ユーザは、自分のユーザ名とパスワードを Web UI ログイン ページに入力します。
2. スパム隔離は、匿名検索を実行するように、または指定された「サーバログイン」DN とパスワードによる認証ユーザとして、指定された LDAP サーバに接続します。Active Directory の場合、一般に「グローバル カタログ ポート」(6000 番台) 上でサーバ接続を

確立する必要があり、検索を実行するために、スパム隔離がバインドできる低い特権LDAPユーザを作成する必要があります。

- 次に、スパム隔離は、指定された BaseDN とクエリ ストリングを使用してユーザを検索します。ユーザの LDAP レコードが見つかり、スパム隔離は、そのレコードの DN を抽出し、ユーザレコードの DN と最初にユーザが入力したパスワードを使用してディレクトリへのバインドを試みます。このパスワードチェックに成功すると、ユーザは正しく認証されます。しかしまだ、スパム隔離は、そのユーザに対してどのメールボックスの内容を表示するのかが決定する必要があります。
- メッセージは、受信者のエンベロープ アドレスを使用してスパム隔離に保管されます。ユーザのパスワードが LDAP に対して検証された後、スパム隔離は、「プライマリ電子メール属性」を LDAP レコードから取得して、どのエンベロープ アドレスの隔離されたメッセージを表示する必要があるのかが決定します。「プライマリ電子メール属性」には、電子メールアドレスが複数格納されている場合があります、これらのアドレスを使用して、隔離からどのエンベロープ アドレスが認証ユーザに対して表示される必要があるのかが決定されます。

#### 関連項目

- [スパム管理機能にアクセスするエンドユーザの認証オプション \(340 ページ\)](#)
- [LDAP との統合 \(433 ページ\)](#)

## IMAP/POP 認証プロセス

- メール サーバ設定に応じて、ユーザは、自分のユーザ名 (joe) または電子メールアドレス (joe@example.com) と、パスワードを Web UI ログインページに入力します。ユーザに電子メールアドレスをフルに入力する必要があるのか、ユーザ名だけを入力すればよいのか知らせるために、ログインページメッセージを変更できます ([スパム隔離へのエンドユーザアクセスの設定 \(343 ページ\)](#) を参照)。
- スパム隔離は、IMAP サーバまたは POP サーバに接続し、入力されたログイン名 (ユーザ名または電子メールアドレス) とパスワードを使用して IMAP/POP サーバへのログインを試みます。パスワードが受け入れられると、そのユーザは認証されたと見なされ、スパム隔離はただちに IMAP/POP サーバからログアウトします。
- ユーザが認証された後、スパム隔離は、ユーザの電子メールアドレスに基づいて、そのユーザ宛の電子メールのリストを作成します。
  - スпам隔離の設定において、修飾のないユーザ名 (joe など) に追加するドメインを指定している場合は、このドメインを後ろに追加してできる完全修飾電子メールアドレスを使用して、隔離エリア内の一致するエンベロープが検索されます。
  - それ以外の場合、スパム隔離は、入力された電子メールアドレスを使用して、一致するエンベロープを検索します。

IMAP の詳細については、ワシントン大学の Web サイトを参照してください。

<http://www.washington.edu/imap/>

## SAML 2.0 認証プロセス

『Cisco Content Security Management Appliance Guide』の「SSO Using SAML 2.0」セクションを参照してください。

## Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	スパム管理機能へのエンドユーザアクセスのさまざまな認証方式について、利点と制限事項を把握します。	『Cisco Content Security Management Appliance Guide』の「SSO Using SAML 2.0」セクションを参照してください。
ステップ 2	LDAP を使用してエンドユーザを認証する場合は、 [システム管理 (System Administration) ] > [LDAP] > [LDAPサーバプロファイル (LDAP Server Profile) ] ページの [スパム隔離エンドユーザ認証クエリー (Spam Quarantine End-User Authentication Query) ] 設定などで、LDAPサーバプロファイルを設定します。  例： If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the <b>System Administration &gt; SAML</b> page.	<a href="#">LDAP との統合 (433 ページ)</a> およびサブセクション  <a href="#">SAML 2.0 による SSO (572 ページ)</a>
ステップ 3	スパム隔離へのエンドユーザアクセスを設定します。	<a href="#">スパム隔離へのエンドユーザアクセスの設定 (343 ページ)</a>
ステップ 4	スパム隔離へのエンドユーザアクセスの URL を決定します。	<a href="#">スパム隔離へのエンドユーザアクセス用 URL の決定 (345 ページ)</a>

### 次のタスク

#### 関連項目

- [スパム隔離へのエンドユーザアクセスの設定 \(343 ページ\)](#)
- [スパム隔離へのエンドユーザアクセス用 URL の決定 \(345 ページ\)](#)
- [エンドユーザに表示されるメッセージ \(346 ページ\)](#)

## スパム隔離へのエンドユーザアクセスの設定

管理ユーザは、エンドユーザアクセスがイネーブルにされているかどうかに関わらず、スパム隔離にアクセスできます。

始める前に

[スパム管理機能にアクセスするエンドユーザの認証オプション \(340 ページ\)](#) で要件を参照してください。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2**

**ステップ 3** [管理アプライアンス (Management Appliance) ]> [集約管理サービス (Centralized Services) ]>> [スパム隔離 (Spam Quarantine) ] を選択します。

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

**ステップ 5** [エンドユーザ隔離アクセス (End-User Quarantine Access) ] セクションまでスクロールします。

**ステップ 6** [エンドユーザの隔離へのアクセスを有効にする (Enable End-User Quarantine Access) ] を選択します。

**ステップ 7** エンドユーザが隔離されたメッセージを表示しようとしたときに、エンドユーザの認証に使用する方式を指定します。

選択オプション	追加情報
なし	—
メールボックス (IMAP/POP)	<p>認証に LDAP ディレクトリを使用しないサイトの場合、隔離は、ユーザの電子メールアドレスとパスワードの正当性を、それらのユーザのメールボックスが保持されている標準ベースの IMAP または POP サーバに対して検証することもできます。</p> <p>スパム隔離にログインするとき、エンドユーザは自身の完全な電子メールアドレスとメールボックスのパスワードを入力します。</p> <p>POP サーバがバナー内で APOP サポートをアドバタイズしている場合、セキュリティ上の理由から (つまり、パスワードが平文で送信されるのを回避するために)、Cisco アプライアンスは APOP のみを使用します。一部またはすべてのユーザに対して APOP がサポートされていない場合は、APOP をアドバタイズしないように POP サーバを設定する必要があります。</p> <p>サーバで SSL を使用するように設定している場合は、SSL を選択します。ユーザがユーザ名だけを入力した場合に、電子メールアドレスを自動入力するために追加するドメインを指定できます。「権限のないユーザ名にドメインを追加 (Append Domain to Unqualified Usernames)」するには、ログインするユーザ用のエンベロープのドメインを入力します。</p>
LDAP	このトピックの「始める前に」で触れたセクションの説明に従って、LDAP を設定します。



選択オプション	追加情報
SAML 2.0	<p>スパム隔離用のシングル サインオンを有効にします。</p> <p>このオプションを使用する前に、[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [SAML] ページのすべての設定が行われていることを確認します。『Cisco Content Security Management Appliance Guide』の「SSO Using SAML 2.0」のセクションを参照してください。</p>

**ステップ 8** メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。

このチェックボックスをオンにすると、ユーザは、スパム隔離ページからメッセージ本文を表示できなくなります。この場合、隔離されたメッセージの本文を表示するには、そのメッセージを解放してから、ユーザのメールアプリケーション (Microsoft Outlook など) で表示する必要があります。この機能は、ポリシーおよび規制 (表示したすべての電子メールをアーカイブすることが要求されている場合など) へのコンプライアンスの目的で使用できます。

**ステップ 9** 変更を送信し、保存します。

#### 次のタスク

(任意) ユーザがスパム隔離にアクセスしたときに表示されるページをカスタマイズします (まだ行っていない場合)。 [スパム隔離の有効化と設定 \(321ページ\)](#) の設定の説明を参照してください。

## スパム隔離へのエンドユーザ アクセス用 URL の決定

エンドユーザがスパム隔離に直接アクセスするために使用できる URL は、マシンのホスト名と、隔離が有効になっている IP インターフェイス上の設定 (HTTP/S とポート番号) から作成されます。たとえば、`HTTP://mail3.example.com:82` となります。

エンドユーザは、以下のいずれかの方法で、新しい Web インターフェイスのスパム検疫にアクセスできます。

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

ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている先駆者の HTTPS ポートです。
- `trailblazerconfig CLI` コマンドが無効になっているときに、`https://example.com:<https-port>/euq-login` の URL を使用します。

ここで、`example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。



---

(注) ローカルおよび外部認証のユーザは、エンドユーザのスパム隔離ポータルにログインできません。

---

## エンドユーザに表示されるメッセージ

通常、エンドユーザにはスパム隔離内にある自身のメッセージだけが表示されます。

アクセス方法（通知経由またはWebブラウザから直接）と認証方式（LDAPまたはIMAP/POP）によっては、スパム隔離内にある複数の電子メールアドレス宛のメールが表示される場合があります。

LDAP 認証を使用する場合、LDAP ディレクトリ内でプライマリ電子メール属性に複数の値が設定されていると、それらの値（アドレス）のすべてがユーザに関連付けられます。したがって、検疫エリア内には、LDAP ディレクトリでエンドユーザに関連付けられたすべての電子メールアドレス宛の検疫されたメッセージが存在します。

認証方式がIMAP/POPの場合、またはユーザが通知から直接隔離にアクセスした場合は、そのユーザの電子メールアドレス（または通知の送信先アドレス）宛のメッセージのみが隔離に表示されます。

メンバーになっているエイリアスに送信されたメッセージについては、[受信者の電子メールのメーリングリストエイリアスおよびスパム通知（348 ページ）](#) を参照してください。

### 関連項目

- [スパム隔離へのエンドユーザアクセスの設定（343 ページ）](#)
- [受信者の電子メールのメーリングリストエイリアスおよびスパム通知（348 ページ）](#)

## エンドユーザへの隔離されたメッセージに関する通知

特定またはすべてのユーザに、スパム隔離内にスパムまたはその疑いのあるメッセージがあることを通知する電子メールを送信するように、システムを設定できます。

デフォルトでは、そのユーザの隔離されたメッセージがスパム通知に表示されます。ユーザがスパム隔離内の隔離されたメッセージを表示できるように、リンクを通知に含めることもできます。このリンクに有効期限はありません。ユーザは隔離されたメッセージを確認し、自分の受信箱に配信するか、削除するかを決定できます。



---

(注) クラスタ設定では、マシン レベルでのみ通知を受信するユーザを選択できます。

---

## 始める前に

- エンドユーザが通知に表示されるメッセージを管理するには、スパム隔離にアクセスする必要があります。 [スパム隔離へのエンドユーザアクセスの設定 \(343 ページ\)](#) を参照してください。
- 通知を使用してスパムを管理するための認証オプションを把握します。 [スパム管理機能にアクセスするエンドユーザの認証オプション \(340 ページ\)](#) を参照してください。
- エンドユーザが複数のエイリアスで電子メールを受信する場合には、 [受信者の電子メールのメーリングリストエイリアスおよびスパム通知 \(348 ページ\)](#) を参照してください。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2**

**ステップ 3** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [スパム隔離 (Spam Quarantine) ] を選択します。

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

**ステップ 5** [スパム通知 (Spam Notifications) ] セクションまでスクロールします。

**ステップ 6** [スパム通知を有効にする (Enable Spam Notification) ] を選択します。

**ステップ 7** オプションを指定します。

メッセージ本文をカスタマイズするには、次の手順を実行します。

a) (任意) デフォルトのテキストおよび変数をカスタマイズします。

変数を挿入するには、挿入する位置にカーソルを置いて、右側のメッセージ変数リストで変数の名前をクリックします。または変数を入力します。

次のメッセージ変数は、特定のエンドユーザに対応した実際の値に展開されます。

- [新規メッセージ数 (New Message Count) ] (%new\_message\_count%) : ユーザの最後のログイン以後の新しいメッセージの数。
- [総メッセージ数 (Total Message Count) ] (%total\_message\_count%) : スпам隔離内にあるこのユーザ宛のメッセージの数。
- [メッセージ保存期間 (Days Until Message Expires) ] (%days\_until\_expire%)
- [隔離 URL (Quarantine URL) ] (%quarantine\_url%) : 隔離にログインし、メッセージを表示するための URL。
- [ユーザ名 (Username) ] (%username%)
- [新しいメッセージテーブル (New Message Table) ] (%new\_quarantine\_messages%) : ユーザの新しい隔離メッセージのリスト。送信者、メッセージ件名、日付、およびメッセージをリリースするリンクを示します。ユーザは、メッセージ件名をクリックしてスパム隔離のメッセージを表示します。
- [新しいメッセージテーブル (件名なし) ] (%new\_quarantine\_messages\_no\_subject%) : [新しいメッセージテーブル (New Message Table) ] と似ていますが、各メッセージの件名の場所には [メッセージの表示 (View Message) ] リンクのみが表示されています。

- b) このページの [エンドユーザ隔離アクセス (End User Quarantine Access)] セクションで認証方式を有効にしている場合は、次を実行します。
- 通知内のリンクをクリックしてアクセスしたユーザを自動的にスパム隔離にログインさせるには、[隔離へのアクセスに証明書なしのログインを有効にする (Enable login without credentials for quarantine access)] を選択します。エンドユーザは、通知の [リリース (Release)] リンクをクリックするだけでメッセージをリリースできます。
  - 通知内のリンクをクリックしてアクセスしたユーザにスパム隔離へのログインを要求する場合は、このオプションの選択を解除します。エンドユーザは、通知の [リリース (Release)] リンクをクリックするだけではメッセージをリリースできません。
- c) [メッセージのプレビュー (Preview Message)] をクリックして、メッセージの内容を確認します。

**ステップ 8** 変更を送信し、保存します。

### 次のタスク

これらの通知を確実に受信できるように、エンドユーザにスパム隔離からの通知電子メールの差出人アドレスを各自のメールアプリケーション (Microsoft Outlook、Mozilla Thunderbird など) の迷惑メール設定にある「ホワイトリスト」に追加することを推奨してください。

### 関連項目

- [受信者の電子メールのメーリングリストエイリアスおよびスパム通知 \(348 ページ\)](#)
- [通知のテスト \(349 ページ\)](#)
- [スパム通知のトラブルシューティング \(349 ページ\)](#)

## 受信者の電子メールのメーリングリストエイリアスおよびスパム通知

電子メールが隔離されている各エンベロープ受信者 (メーリングリストおよびその他のエイリアスを含む) に通知を送信できます。メーリングリストごとに1つの要約を受信します。メーリングリストに通知を送信すると、リストの購読者全員に通知が届きます。複数の電子メールエイリアスに属するユーザ、通知を受信するLDAPグループに属するユーザ、または複数の電子メールアドレスを使用するユーザは、複数のスパム通知を受信する場合があります。次の表に、ユーザが複数の通知を受け取る状況の例を示します。

表 67: アドレス/エイリアスに応じた通知数

ユーザ (User)	電子メール アドレス	エイリアス	通知
Sam	sam@example.com	—	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com、 admin@example.com	hr@example.com	3

LDAP 認証を使用する場合、メーリングリストエイリアスに通知を送信しないように選択することができます。または、メーリングリストエイリアスにスパム通知を送信することを選択した場合、複数の通知が送信されないようにすることができます。[スパム隔離のエイリアス統合クエリ](#)を参照してください。

アプライアンスが電子メール通知にスパム隔離のエイリアス統合クエリを使用していない限り、通知内のリンクをクリックしてスパム隔離にアクセスしたユーザに、そのエンドユーザが所有する他のエイリアス宛の隔離対象メッセージは表示されません。アプライアンスで処理した後に展開される配布リストに通知が送信された場合、複数の受信者がそのリストの同じ隔離にアクセスできます。

つまり、各メーリングリストの購読者は、全員が同じ通知を受信することになり、その検疫にログインしてメッセージを解放したり、削除したりできます。この場合、エンドユーザが隔離にアクセスして、通知に示されたメッセージを表示しようとしても、それらのメッセージは他のユーザによってすでに削除されている可能性もあります。



(注) LDAPを使用していない場合で、エンドユーザが複数の電子メール通知を受信することがないようにする必要がある場合は、通知をディセーブルにすることを検討します。この場合、代わりとして、エンドユーザが検疫に直接アクセスできるようにし、LDAPまたはPOP/IMAPで認証します。

## 通知のテスト

テスト用のメールポリシーを設定し、単一のユーザに対してのみスパムを隔離することで通知をテストできます。その後、スパム隔離の通知設定で、[スパム通知を有効にする (Enable Spam Notification)] チェックボックスをオンにし、[エンドユーザの隔離へのアクセスを有効にする (Enable End-User Quarantine Access)] チェックボックスをオフにします。これにより、[バウンスされたメッセージの送信先 (Deliver Bounced Messages To)] フィールドに設定された管理者だけが、隔離内の新しいスパムについて通知されます。

## スパム通知のトラブルシューティング

### 関連項目

- ユーザが複数の通知を受信する (349 ページ)
- 受信者が通知を受信しない (350 ページ)
- ユーザが複数の通知を受信する (349 ページ)
- 受信者が通知を受信しない (350 ページ)

### ユーザが複数の通知を受信する

#### 問題

ユーザが1つのメッセージに対して複数のスパム通知を受信します。

#### 解決方法

考えられる原因：

- ユーザが複数の電子メールアドレスを所有し、スパムメッセージがその内の2つ以上のアドレスに送信されました。
- ユーザが、スパムメッセージを受信した1つ以上の電子メールエイリアスのメンバーです。重複を最小限にするための詳細については、[受信者の電子メールのメーリングリストエイリアスおよびスパム通知 \(348 ページ\)](#) を参照してください。

## 受信者が通知を受信しない

### 問題

受信者にスパム通知が届きません。

### 解決方法

- スпам受信者ではなく [バウンスメッセージの送信先： (Deliver Bounce Messages To:)] のアドレスに通知が送信される場合は、スパム通知が有効になっていても、スパム隔離へのアクセスが有効になっていないことを意味します。[スパム管理機能にアクセスするエンドユーザの認証オプション \(340 ページ\)](#) を参照してください。
- ユーザに各自の電子メールクライアントの迷惑メール設定を確認してもらいます。
- [スパム隔離の有効化と設定 \(321 ページ\)](#) で [次を使用してメッセージを配信 (Deliver Messages Via)] に指定したアプライアンスまたはサーバに問題がないかを確認します。

## スパム隔離内のメッセージの管理

ここでは、ローカルまたは外部のスパム隔離内にあるメッセージの操作方法について説明します。

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

### 関連項目

- [スパム隔離へのアクセス \(管理ユーザ\) \(351 ページ\)](#)
- [スパム隔離内でのメッセージの検索 \(351 ページ\)](#)
- [スパム隔離内のメッセージの表示 \(352 ページ\)](#)
- [スパム隔離内のメッセージの配信 \(352 ページ\)](#)
- [スパム隔離からのメッセージの削除 \(353 ページ\)](#)

## スパム隔離へのアクセス (管理ユーザ)

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

## スパム隔離へのアクセス（管理ユーザ）

管理ユーザはスパム隔離内のすべてのメッセージを表示および管理できます。

- 
- ステップ 1** （新しいWebインターフェイスのみ）クラウドメールセキュリティ管理コンソールで、[隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）] を選択します。
- ステップ 2** [メール（Email）] > [メッセージの隔離（Message Quarantine）] > [スパム隔離（Spam Quarantine）] を選択し、[スパム隔離（Spam Quarantine）] リンクをクリックします。  
スパム隔離が別のブラウザ ウィンドウで開きます。
- 

## スパム隔離内でのメッセージの検索

- ステップ 1** エンベロープ受信者を指定します。  
(注) アドレスの一部を入力できます。
- ステップ 2** 入力した受信者に検索結果が厳密に一致する必要があるか、あるいは入力した値が検索結果のアドレスの一部、先頭、または末尾のいずれと一致する必要があるかを選択します。
- ステップ 3** 検索の対象期間を入力します。カレンダー アイコンをクリックして、日付を選択します。
- ステップ 4** 差出人アドレスを指定し、入力した値が検索結果のアドレスの一部、全体、先頭、または末尾のいずれと一致する必要があるかを選択します。
- ステップ 5** [検索（Search）] をクリックします。検索基準に一致するメッセージがページの [検索（Search）] セクションの下に表示されます。
- 

次のタスク

関連項目

[大量メッセージの検索（351 ページ）](#)

## 大量メッセージの検索

スパム隔離内に大量のメッセージが収集されている場合、および検索条件が絞り込まれていない場合、クエリーの結果が返されるまでに非常に長い時間がかかる可能性があります。場合によってはタイムアウトします。

その場合、検索を再実行するかどうか確認されます。大量の検索が同時に複数実行されると、パフォーマンスに悪影響を与える可能性があることに注意してください。

## スパム隔離内のメッセージの表示

メッセージのリストにより、スパム隔離内のメッセージが表示されます。一度に表示されるメッセージの件数を選択できます。列見出しをクリックすることにより、表示をソートできます。同じ列を再びクリックすると、逆順にソートされます。

メッセージの件名をクリックしてメッセージを表示します。これには、本文とヘッダーが含まれます。メッセージは、[メッセージの詳細 (Message Details)] ページに表示されます。メッセージの最初の 20 KB が表示されます。メッセージがそれよりも長い場合、表示は 20 KB で打ち切れ、メッセージの最後にあるリンクからメッセージをダウンロードできます。

[メッセージの詳細 (Message Details)] ページから、メッセージを削除したり ([削除 (Delete)] を選択)、[リリース (Release)] を選択してメッセージを解放したりできます。メッセージを解放すると、そのメッセージは配信されます。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング (Message Tracking)] リンクをクリックします。

次の点に注意してください。

### • 添付ファイルを含むメッセージの表示

添付ファイルを含むメッセージを表示すると、メッセージの本文が表示された後、添付ファイルのリストが続いて表示されます。

新しい Web インターフェイスでは、メッセージに添付ファイルが含まれている場合、メッセージの [添付ファイル (Attachment)] セクションに添付ファイルの詳細が表示されます。

### • HTML メッセージの表示

スパム隔離では、HTML ベースのメッセージは近似で表示されます。画像は表示されません。

### • エンコーディングされたメッセージの表示

Base64 でエンコーディングされたメッセージは、復号化されてから表示されます。

## スパム隔離内のメッセージの配信

メッセージをリリースして配信するには、リリースする 1 つまたは複数のメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから [リリース (Release)] を選択します。その後、[送信 (Submit)] をクリックします。

ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

リリースされたメッセージは、それ以降の電子メールパイプライン内の作業キューの処理をスキップして、宛先キューへ直接進みます。



## スパム隔離からのメッセージの削除

スパム隔離では、メッセージが一定時間後に自動で削除されるように設定できます。また、スパム隔離が最大サイズに達したら、古いものから順にメッセージが自動で削除されるように設定することもできます。スパム隔離からメッセージを手動で削除することも可能です。

個別のメッセージを削除するには、削除するメッセージの隣にあるチェックボックスをクリックし、ドロップダウンメニューから[削除 (Delete)]を選択します。その後、[送信 (Submit)]をクリックします。ページに現在表示されているすべてのメッセージを自動で選択するには、見出し行にあるチェックボックスをクリックします。

スパム隔離内のすべてのメッセージを削除するには、その隔離を無効にし ([外部スパム隔離の無効化について \(353 ページ\)](#) を参照)、[すべてのメッセージを削除 (Delete All Messages)] リンクをクリックします。リンクの末尾にある括弧内の数字は、スパム隔離内のメッセージの件数です。

## スパム隔離のディスク領域

隔離に使用できるディスク領域は、アプライアンス モデルによって異なります。[ディスク領域、クォータ、および使用状況の表示 \(568 ページ\)](#) を参照してください。

デフォルトでは、スパム隔離内のメッセージは一定期間後に自動的に削除されます。検疫エリアが満杯になった場合は、古いスパムから削除されます。この設定を変更するには、[スパム隔離の有効化と設定 \(321 ページ\)](#) を参照してください。

### 関連項目

## 外部スパム隔離の無効化について

スパム隔離をディセーブルにする場合は、次を参照してください。

- ディセーブルになっているスパム隔離内にメッセージが存在する場合は、すべてのメッセージの削除を選択できます。
- スパムまたはその疑いのあるメッセージを隔離するように設定されたメールポリシーは、メッセージを配信するように設定が変更されます。E メールセキュリティ アプライアンスでメール ポリシーの調整が必要になる場合があります。
- 外部スパム隔離を完全にディセーブルにするには、E メールセキュリティ アプライアンスとセキュリティ管理アプライアンスの両方でディセーブルにします。

E メールセキュリティ アプライアンスのみで外部スパム隔離をディセーブルにしても、外部隔離またはそのメッセージとデータは削除されません。

## スパム隔離機能のトラブルシューティング

- [セーフリストとブロックリストのトラブルシューティング](#) (339 ページ)
- [スパム通知のトラブルシューティング](#) (349 ページ)



## 第 9 章

# 集約されたポリシー、ウイルス、およびアウトブレイク隔離

この章は、次の項で構成されています。

- [集約隔離の概要 \(355 ページ\)](#)
- [ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#)
- [ポリシー、ウイルス、およびアウトブレイク隔離の管理 \(367 ページ\)](#)
- [ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作 \(378 ページ\)](#)
- [集約されたポリシー隔離のトラブルシューティング \(388 ページ\)](#)

## 集約隔離の概要

E メールセキュリティアプライアンス上で特定のフィルタ、ポリシー、およびスキャン操作により処理されたメッセージは、次の作業に備えて一時的に隔離しておくことができます。Cisco コンテンツセキュリティ管理アプライアンス上の複数の E メールセキュリティアプライアンスから隔離を集約管理できます。

この集約隔離には次のような利点があります。

- 複数の E メールセキュリティアプライアンスで隔離されたメッセージを 1 か所で管理できます。
- セキュリティリスクを減らすため、隔離されたメッセージは DMZ 内ではなくファイアウォールの内側に保管されます。
- 集約隔離は、セキュリティ管理アプライアンスの標準バックアップ機能の一部としてバックアップされることができます。

ウイルス対策スキャン、アウトブレイクフィルタ、および高度なマルウェア防御（ファイル分析）には、それぞれ専用の隔離場所があります。メッセージフィルタリング、コンテンツフィルタリング、およびデータ漏洩防止ポリシーで検出されたメッセージを保持するための「ポリシー隔離」を作成します。

レガシー Web インターフェイスの [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus and Outbreak Quarantines) ] セクションは、新しい Web インターフェイスでは [その他の隔離 (Other Quarantines) ] としてラベル付けされています。詳細については、[隔離内のメッセージの表示 \(378 ページ\)](#) を参照してください。

隔離の詳細については、お使いの E メール セキュリティ アプライアンスのドキュメントを参照してください。

## 隔離の種類

隔離タイプ	隔離名	デフォルトで作成される	説明	詳細情報
高度なマルウェア防御 (Advanced Malware Protection)	ファイル分析 (File Analysis)	○	判定が返されるまで、ファイル分析のために送信されたメッセージを保持します。	<ul style="list-style-type: none"> <li>• <a href="#">ポリシー、ウイルス、およびアウトブレイク隔離の管理</a></li> <li>• <a href="#">ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作</a></li> </ul>
ウイルス	ウイルス	○	アンチウイルスエンジンによる判定に従って、マルウェアを送信する可能性のあるメッセージを保持します。	
アウトブレイク	アウトブレイク	○	アウトブレイクフィルタでスパムまたはマルウェアの可能性があると検出されたメッセージを保持します。	
ポリシー	ポリシー	○	メッセージフィルタ、コンテンツフィルタ、およびDLPメッセージアクションによって検出されたメッセージを保留します。  デフォルトのポリシー隔離が用意されています。	
	Unclassified	○		

隔離タイプ	隔離名	デフォルトで作成される	説明	詳細情報
			<p>メッセージフィルタ、コンテンツフィルタ、またはDLPメッセージアクションで指定した隔離が削除された場合にのみ、メッセージを保持します。</p> <p>この隔離をフィルタやメッセージアクションに割り当てることはできません。</p>	
	(自分で作成する「ポリシー隔離」)	なし	<p>メッセージフィルタ、コンテンツフィルタおよびDLPメッセージアクションで使用するために作成する「ポリシー隔離」。</p>	
スパム	スパム	○	<p>スパムおよびその疑いのあるメッセージを保持して、メッセージの受信者や管理者が確認できるようにします。</p> <p>スパム隔離は、ポリシー、ウイルス、およびアウトブレイクの隔離グループに含まれておらず、これらの隔離とは別に管理します。</p>	<p><a href="#">スパム隔離 (319ページ)</a></p>

# ポリシー、ウイルス、およびアウトブレイク隔離の集約

## 手順

	コマンドまたはアクション	目的
ステップ 1	E メールセキュリティ アプライアンスが DMZ 内にあり、セキュリティ管理アプライアンスがファイアウォールの背後にある場合は、これらのアプライアンスが集約されたポリシー、ウイルス、およびアウトブレイクの隔離データを交換できるようにファイアウォールのポートを開放する必要があります。	ファイアウォール情報 (643 ページ)
ステップ 2	セキュリティ管理アプライアンス上で、この機能を有効にします。	セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離の有効化 (361 ページ)
ステップ 3	セキュリティ管理アプライアンスで、スパム以外の隔離に割り当てるディスク領域を指定します。	ディスク領域の管理 (567 ページ)
ステップ 4	<p>(オプション)</p> <ul style="list-style-type: none"> <li>セキュリティ管理アプライアンス上に、集約されたポリシー隔離を必要な設定で作成します。</li> <li>集約するウイルス隔離とアウトブレイク隔離、およびデフォルトの「ポリシー隔離」を設定します。</li> </ul> <p>移行の前にこれらを設定済みの場合は、既存の設定を E メールセキュリティ アプライアンス上で参照できます。</p> <p>カスタムの移行を設定するときに隔離を作成したり、自動移行時に隔離を自動作成したりできます。移行時に作成されるすべての隔離には、デフォルトの設定が適用されます。</p> <p>ローカルの隔離の設定は、隔離名が同じでも集約隔離には継承されません。</p>	<ul style="list-style-type: none"> <li>ポリシー、ウイルス、およびアウトブレイク隔離の設定 (370 ページ)</li> <li>システム作成の隔離の設定を確認 (369 ページ)。</li> </ul>
ステップ 5	セキュリティ管理アプライアンス上で、管理する E メールセキュリティ アプライアンスを追加するか、追加済みのアプライアンスの集約管理サービスから [ポリシー、ウイルスおよびアウトブレイク	管理対象の各 E メールセキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加 (362 ページ)

	コマンドまたはアクション	目的
	<p>隔離 (Policy, Virus and Outbreak Quarantines) ] オプションを選択します。</p> <ul style="list-style-type: none"> <li>ご使用の E メールセキュリティ アプライアンスがクラスタ化されている場合、特定のレベル (マシン、グループ、またはクラスタ) に属するすべてのアプライアンスは、そのクラスタ内の任意の E メールセキュリティ アプライアンスで集約された [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus and Outbreak Quarantines) ] を有効にする前に、セキュリティ管理アプライアンスに追加する必要があります。</li> </ul>	
ステップ 6	変更を保存します。	
ステップ 7	セキュリティ管理アプライアンスで、E メールセキュリティ アプライアンスからの既存の隔離の移行を設定します。	<a href="#">ポリシー、ウイルス、アウトブレイク隔離の移行の設定 (363 ページ)</a>
ステップ 8	<p>E メールセキュリティ アプライアンスで、集約されたポリシー、ウイルス、およびアウトブレイク隔離機能を有効にします。</p> <ul style="list-style-type: none"> <li><b>重要</b> E メールセキュリティ アプライアンスでポリシー、ウイルス、およびアウトブレイク隔離を設定済みの場合、隔離およびすべてのメッセージの移行はこの変更を確定するとすぐに開始されます。</li> </ul>	<p>お使いのセキュリティ管理アプライアンスのマニュアルで、「Centralizing Services on a Cisco Content Security Management appliance」の章の以下の項を参照してください。</p> <ul style="list-style-type: none"> <li>「About Migration of Policy, Virus, and Outbreak Quarantines」</li> <li>「ポリシー、ウイルス、およびアウトブレイク隔離の集約 (Centralizing Policy, Virus, and Outbreak Quarantines) 」</li> </ul>
ステップ 9	<p>追加の E メールセキュリティ アプライアンスを移行します。</p> <ul style="list-style-type: none"> <li>同時に移行できるのは 1 つのアプライアンスのみです。前の移行が完了する前に、別の E メールセキュリティ アプライアンスでポリシー、ウイルス、およびアウトブレイク隔離の集約を有効にしないでください。</li> </ul>	
ステップ 10	<p>必要に応じて集約隔離設定を編集します。</p> <ul style="list-style-type: none"> <li>移行時に作成される隔離には、隔離名が同じでも、元のローカルの隔離での設定ではなくデフォルトの設定が適用されます。</li> </ul>	<a href="#">ポリシー、ウイルス、およびアウトブレイク隔離の設定 (370 ページ)</a>



	コマンドまたはアクション	目的
ステップ 11	メッセージフィルタ、コンテンツフィルタ、およびDLPメッセージアクションが集約隔離の名前で自動的に更新されない場合は、Eメールセキュリティアプライアンス上でこれらの設定を手動で更新する必要があります。  <ul style="list-style-type: none"> <li>クラスタ構成では、フィルタおよびメッセージアクションが特定のレベルで定義されている場合に限り、それらの設定がそのレベルで自動的に更新されます。</li> </ul>	詳しくは、お使いのEメールセキュリティアプライアンスのオンラインヘルプまたはユーザガイドのメッセージフィルタ、コンテンツフィルタ、およびDLPメッセージアクションについての説明を参照してください。
ステップ 12	(推奨) 元のEメールセキュリティアプライアンスが使用できない場合に備えて、隔離からリリースされたメッセージを処理するアプライアンスを指定します。	リリースされたメッセージを処理する代替アプライアンスの指定 (365 ページ)
ステップ 13	カスタム ユーザ ロールに管理タスクを委任する場合は、特定の 방법으로アクセスを設定する必要があります。	カスタム ユーザ ロールの集約隔離アクセスの設定 (366 ページ)

## セキュリティ管理アプライアンスでの集約ポリシー、ウイルス、およびアウトブレイク隔離の有効化

### 始める前に

ポリシー、ウイルス、およびアウトブレイク隔離の集約 (359 ページ) の表に記載されているここまでの手順を完了してください。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド Eメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ]>[ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ] の順に選択します。

**ステップ 3** [有効 (Enable) ] をクリックします。

**ステップ 4** Eメールセキュリティアプライアンスと通信するためインターフェイスとポートを指定します。

- これらを変更する理由がない限り、デフォルトの選択を受け入れます。
- Eメールセキュリティアプライアンスがセキュリティ管理アプライアンスと同じネットワークに存在しない場合、管理インターフェイスを使用する必要があります。
- ファイアウォールで開放したポートを使用する必要があります。

ステップ 5 [送信 (Submit) ] をクリックします。

#### 次のタスク

[ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#) の表に戻り、次のステップに進みます。

## 管理対象の各 E メール セキュリティ アプライアンスへの集約ポリシー、ウイルス、アウトブレイク隔離サービスの追加

すべての E メール セキュリティ アプライアンスで、すべての隔離の統合されたビューを表示するには、隔離を集中化する前に、すべての E メール セキュリティ アプライアンスの追加を検討します。

#### 始める前に

[ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#) の表に記載されているここまでの手順を完了してください。

- ステップ 1 (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2 [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] を選択します。
- ステップ 3 このページのリストに、すでに E メール セキュリティ アプライアンスを追加している場合は、次の手順を実行します。
- E メール セキュリティ アプライアンスの名前をクリックします。
  - [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ] サービスを選択します。
- ステップ 4 E メール セキュリティ アプライアンスをまだ追加していない場合は、次の手順を実行します。
- [メールアプライアンスの追加 (Add Email Appliance) ] をクリックします。
  - [アプライアンス名 (Appliance Name) ] および [IP アドレス (IP Address) ] フィールドに、追加するアプライアンス名前と管理インターフェイスの IP アドレスを入力します。
- (注) [IP アドレス (IP Address) ] フィールドに DNS 名を入力しても、[送信 (Submit) ] をクリックすると IP アドレスに変換されます。
- [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ] サービスはあらかじめ選択されています。
  - [接続の確立 (Establish Connection) ] をクリックします。
  - 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection) ] をクリックします。

(注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。

f) 「Success」メッセージがページのテーブルの上に表示されるまで待機します。

**ステップ 5** [送信 (Submit) ] をクリックします。

**ステップ 6** [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ] を有効にする各 E メールセキュリティアプライアンスについてこの手順を繰り返します。

たとえば、クラスタ内の他のアプライアンスを追加します。

**ステップ 7** 変更を保存します。

---

### 次のタスク

[ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#) の表に戻り、次のステップに進みます。

## ポリシー、ウイルス、アウトブレイク隔離の移行の設定

### 始める前に

- 次の項の表に記載されているここまでの手順を完了してください。 [ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#)
- 移行プロセスに関する警告や情報については、お使いの E メールセキュリティアプライアンスのマニュアルの「Centralizing Services on a Cisco Content Security Management appliance」の章の「About Migration of Policy, Virus, and Outbreak Quarantines」の項を参照してください。

---

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance) ] > [集約管理サービス (Centralized Services) ] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ] の順に選択します。

**ステップ 3** [移行ウィザードを起動 (Launch Migration Wizard) ] をクリックします。

**ステップ 4** 移行方法を選択します。

条件 (IF)	移行方法	その他の情報
<ul style="list-style-type: none"> <li>関連付けられているすべてのEメールセキュリティアプライアンスから既存のすべてのポリシー隔離を移行する場合 および</li> <li>同じ名前のポリシー隔離がすべてのEメールセキュリティアプライアンス上で同一設定である場合 および</li> <li>すべてのEメールセキュリティアプライアンスから同名のすべてのポリシー隔離を同名の単一のポリシー隔離に集約する場合</li> </ul>	[自動 (Automatic)]	<p>この移行方法で作成されるすべての集約されたポリシー隔離には、Eメールセキュリティアプライアンスの同名の隔離の設定に関係なく、デフォルトの設定が適用されます。</p> <p>移行後に、これらの設定を更新する必要があります。</p>
<ul style="list-style-type: none"> <li>複数のEメールセキュリティアプライアンス上で同名のポリシー隔離の設定が異なっており、この違いを保持したまま移行する場合 または</li> <li>ローカル隔離の一部を移行し、他のすべてを削除する場合 または</li> <li>ローカル隔離を別名の集約隔離に移行する場合 または</li> <li>異なる名前のローカル隔離を単一の集約隔離にマージする場合</li> </ul>	カスタム (Custom)	<p>移行前ではなく移行時に作成するすべての集約されたポリシー隔離には、新しい隔離用のデフォルトの設定が適用されません。</p> <p>移行後に、これらの設定を更新する必要があります。</p>

**ステップ 5** [Next] をクリックします。

**ステップ 6** [自動 (Automatic)] を選択した場合は、次の手順に従います。

移行するポリシー隔離およびこのページの他の情報を確認します。

ウイルス、アウトブレイク、およびファイル分析の隔離も移行されます。

**ステップ 7** [カスタム (Custom)] を選択した場合は、次の手順に従います。

- [隔離の表示元 (Show Quarantines from)] リストで、すべてのEメールセキュリティアプライアンスの隔離を表示するか、特定のアプライアンスの隔離を表示するかを選択します。

- 各集約されたポリシー隔離に移行するローカルのポリシー隔離を選択します。
- 必要に応じて、追加の集約されたポリシー隔離を作成します。これらはデフォルト設定になります。
- 隔離名は大文字と小文字が区別されます。
- 左のテーブルに残っている隔離は移行されず、移行時にEメールセキュリティアプライアンスから削除されます。
- 隔離のマッピングを変更するには、右のテーブルで隔離を選択し、[集約隔離から削除 (Remove from Centralized Quarantine)] をクリックします。

**ステップ 8** 必要に応じて [次へ (Next)] をクリックします。

**ステップ 9** 変更を送信し、保存します。

### 次のタスク

[ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#) の表に戻り、次のステップに進みます。

## リリースされたメッセージを処理する代替アプライアンスの指定

通常、メッセージが集約隔離からリリースされると、セキュリティ管理アプライアンスによりそのメッセージが元のEメールセキュリティアプライアンスに返され、そこで処理されます。

元のEメールセキュリティアプライアンスが使用できない場合は、リリースされたメッセージを別のEメールセキュリティアプライアンスで処理し配信できます。この目的で使用するアプライアンスを指定します。

### 始める前に

- 代替アプライアンスが、リリースされたメッセージの処理および配信に適しているかどうかを確認します。たとえば、暗号化とアンチウイルス再スキャンの設定が、元のアプライアンスの設定と同じである必要があります。
- 代替アプライアンスは、集約されたポリシー、ウイルス、およびアウトブレイク隔離用に正しく設定されている必要があります。そのアプライアンスについて、[ポリシー、ウイルス、およびアウトブレイク隔離の集約 \(359 ページ\)](#) の表の手順を実行します。

**ステップ 1** (新しい Web インターフェイスのみ) クラウドEメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。

**ステップ 3** [フォールバック ホストアプライアンスを指定 (Specify Alternate Release Appliance)] ボタンをクリックします。

**ステップ 4** E メール セキュリティ アプライアンスを選択します。

**ステップ 5** 変更を送信し、保存します。

#### 次のタスク

##### 関連項目

[Eメールセキュリティアプライアンスを使用できないときのメッセージのリリース \(366 ページ\)](#)

## カスタム ユーザ ロールの集約隔離アクセスの設定

カスタム ユーザ ロールを持つ管理者が E メール セキュリティ アプライアンス上のメッセージ およびコンテンツ フィルタ内および DLP メッセージアクション内で集約されたポリシー隔離を指定できるようにするためには、セキュリティ管理アプライアンスの関連ポリシー隔離への ユーザ アクセスを許可し、セキュリティ管理アプライアンスに作成するカスタム ユーザ ロール名が E メール セキュリティ アプライアンス上のものと一致する必要があります。

##### 関連項目

- [Custom Email User ロールの作成 \(476 ページ\)](#)

## 中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化

通常、これらの集約隔離を無効にする場合は、E メール セキュリティ アプライアンス上で行います。

ポリシー、ウイルス、およびアウトブレイク隔離の集約を無効にした場合の影響など、詳細については、お使いの E メール セキュリティ アプライアンスのオンラインヘルプまたはマニュアルを参照してください。

## Eメールセキュリティアプライアンスを使用できないときのメッセージのリリース

通常、メッセージが集約隔離からリリースされると、セキュリティ管理アプライアンスによりそのメッセージが元の E メール セキュリティ アプライアンスに返され、そこで処理されます。

元の E メール セキュリティ アプライアンスが使用できない場合は、リリースされたメッセージを別の E メール セキュリティ アプライアンスで処理し配信できます。この目的で使用する代替アプライアンスを指定します。

代替アプライアンスが使用できない場合は、代替リリース アプライアンスとして別の E メール セキュリティ アプライアンスを指定でき、そのアプライアンスがキューに入っているメッセージを処理して配信します。

E メール セキュリティ アプライアンスへのアクセスに繰り返し失敗すると、アラートが送信されます。

#### 関連項目

- [リリースされたメッセージを処理する代替アプライアンスの指定 \(365 ページ\)](#)

## ポリシー、ウイルス、およびアウトブレイク隔離の管理

- [ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て \(367 ページ\)](#)
- [隔離内のメッセージの保持期間 \(368 ページ\)](#)
- [隔離メッセージに自動的に適用されるデフォルト アクション \(369 ページ\)](#)
- [システム作成の隔離の設定を確認 \(369 ページ\)](#)
- [ポリシー、ウイルス、およびアウトブレイク隔離の設定 \(370 ページ\)](#)
- [ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について \(372 ページ\)](#)
- [ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定 \(372 ページ\)](#)
- [ポリシー隔離の削除について \(373 ページ\)](#)
- [隔離のステータス、容量、およびアクティビティのモニタリング \(373 ページ\)](#)
- [隔離用のディスク容量の使用率に関するアラート \(376 ページ\)](#)
- [ポリシー隔離とロギング \(376 ページ\)](#)
- [メッセージ処理タスクの他のユーザへの割り当てについて \(377 ページ\)](#)

## ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て

ディスク領域の割り当てについては、[ディスク領域の管理 \(567 ページ\)](#) を参照してください。

複数の隔離のメッセージは、1つの隔離のメッセージと同じ容量のディスク領域を消費します。

アウトブレイク フィルタと集約隔離の両方が有効な場合、以下のようになります。

- ローカルのポリシー隔離、ウイルス隔離、およびアウトブレイク隔離に割り当てられるべき E メール セキュリティ アプライアンス上のすべてのディスク領域が、アウトブレイク隔離内のメッセージのコピーを保持するために使用されます。これらのメッセージは、アウトブレイク ルールが更新されるたびにスキャンされます。
- 特定の管理対象 E メール セキュリティ アプライアンスから隔離された、アウトブレイク隔離内のメッセージに使用できるセキュリティ管理アプライアンスのディスク領域は、その E メール セキュリティ アプライアンスで隔離メッセージに使用できるディスク領域の量によって制限される場合があります。
- この状況の詳細については、次を参照してください。 [隔離内のメッセージの保持期間 \(368 ページ\)](#)

## 関連項目

- [隔離のステータス、容量、およびアクティビティのモニタリング](#) (373 ページ)
- [隔離用のディスク容量の使用率に関するアラート](#) (376 ページ)
- [隔離内のメッセージの保持期間](#) (368 ページ)

## 隔離内のメッセージの保持期間

メッセージは次のタイミングで隔離から自動的に削除されます。

- **通常の期限切れ**：隔離エリア内のメッセージが設定された保存期間を満了した場合です。各隔離エリアのメッセージの保存期間を指定します。各メッセージには一定の保持期間があり、その期間のみ隔離のリストに表示されます。このトピックで説明する別の状況が発生しない限り、メッセージは指定された期間が経過するまで保持されます。



(注) アウトブレイク フィルタ隔離でのメッセージの通常の保持期間は、アウトブレイク隔離ではなく各メールのアウトブレイク フィルタ セクションで設定します。

- **早期の期限切れ**：設定した保持期間が経過する前にメッセージが隔離から強制的に削除された場合です。これは次の場合に発生します。
  - [ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て](#) (367 ページ) で定義した、すべての隔離に対するサイズ制限に達した場合。

サイズ制限に達すると、隔離に関係なく、古いメッセージからデフォルトアクションが適用されます。すべての隔離のサイズが制限値未満に戻るまで、各メッセージに対してデフォルトアクションが実行されます。このポリシーは、**First In First Out (FIFO)** (先入れ先出し) です。複数の隔離内に保持されたメッセージの場合は、最新の保持期間に基づいて期限切れになります。

(任意) ディスク容量が不足したときのリリースまたは削除の対象から、特定の隔離を除外することができます。除外するようにすべての隔離を設定して、ディスク領域が満杯になった場合、。

セキュリティ管理アプライアンスはメッセージをスキャンしないため、集約アウトブレイク隔離内の各メッセージのコピーは、最初にメッセージを処理した E メール セキュリティ アプライアンスに保存されます。これにより、E メール セキュリティ アプライアンスはアウトブレイク フィルタルールが更新されるたびに隔離内のメッセージを再スキャンし、安全と判断したメッセージをリリースするようセキュリティ管理アプライアンスに通知できます。アウトブレイク隔離の両方のコピーは常にメッセージの同じセットを保持する必要があります。したがって、E メール セキュリティ アプライアンスのディスク領域に空きがなくなるというまれな状況では、両方のアプライアンスのアウトブレイク隔離内のメッセージのコピーは、集約隔離にまだ領域がある場合でも、早く期限切れになります。



ディスク領域の容量が一定の値に達すると、アラートが送信されます。[隔離用のディスク容量の使用率に関するアラート \(376 ページ\)](#) を参照してください。

- メッセージを保持している隔離を削除した場合。

メッセージが隔離から自動的に削除されるときに、そのメッセージに対してデフォルトアクションが実行されます。[隔離メッセージに自動的に適用されるデフォルトアクション \(369 ページ\)](#) を参照してください。



(注) これらのシナリオに加えて、スキャン操作の結果に基づいて、メッセージを隔離から自動的に削除できます (アウトブレイク フィルタまたはファイル分析)。

#### 保存期間への時間調整の影響

- サマータイムとアプライアンスのタイムゾーンの変更は保持期間に影響しません。
- 隔離の保持期間を変更すると、その保持期間は新しいメッセージにのみ適用され、既存のメッセージには適用されません。
- システムクロックを変更してメッセージの保持期間が過ぎた場合は、次の最も適切な時間に期限切れになります。
- システムクロックの変更は期限切れの処理中のメッセージには適用されません。

## 隔離メッセージに自動的に適用されるデフォルトアクション

[隔離内のメッセージの保持期間 \(368 ページ\)](#) に記述されるいずれかの状況が発生した場合、ポリシー、ウイルス、またはアウトブレイク隔離内のメッセージに対してデフォルトアクションが実行されます。

デフォルトアクションには、以下の2つがあります。

- 削除：メッセージを削除します。
- [リリース (Release)]：メッセージが解放されて配信されます。

メッセージのリリース時に、脅威に対する再スキャンが実行される場合があります。詳細については、[隔離されたメッセージの再スキャンについて \(385 ページ\)](#) を参照してください。

また、指定した保持期間よりも前にリリースされるメッセージには、X-Headerの追加などの操作が行われる場合があります。詳細については、[ポリシー、ウイルス、およびアウトブレイク隔離の設定 \(370 ページ\)](#) を参照してください。

集約隔離からリリースされたメッセージは元のEメールセキュリティアプライアンスに返され、そこで処理されます。

## システム作成の隔離の設定を確認

隔離を使用する前に、デフォルトの隔離設定 (未分類隔離など) をカスタマイズします。

## 関連項目

- [ポリシー、ウイルス、およびアウトブレイク隔離の設定 \(370 ページ\)](#)

# ポリシー、ウイルス、およびアウトブレイク隔離の設定

## 始める前に

- 既存の隔離を編集する場合は、[ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について \(372 ページ\)](#) を参照してください。
- 保持期間やデフォルトアクションなど、隔離内のメッセージを自動的に管理する方法を確認します。[隔離内のメッセージの保持期間 \(368 ページ\)](#) および [隔離メッセージに自動的に適用されるデフォルトアクション \(369 ページ\)](#) を参照してください。
- 各隔離にアクセスできるユーザを決め、ユーザおよびカスタムユーザロールを作成します。詳細は、[ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザグループの指定 \(377 ページ\)](#) を参照してください。

**ステップ 1** ポリシー、ウイルス、およびアウトブレイク隔離は、次のいずれかの方法で設定できます。

- (新しい Web インターフェイスのみ) [隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] > [表示 (View)] > [+] を選択します。
- [メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、次のいずれかを実行します。
  - [ポリシー隔離の追加 (Add Policy Quarantine)] をクリックします。
  - 編集する隔離をクリックします。

**ステップ 2** 次の情報を入力します。

次の点を考慮してください。

- ファイル分析隔離の保持期間をデフォルトの 1 時間から変更することは推奨されません。
- 隔離ディスク領域が一杯になった場合でも、指定した保存期間の終了前にこの隔離メッセージを処理されたくない場合、[メッセージに対してデフォルトのアクションを適用して空き容量を増やす (Free up space by applying default action on messages upon space overflow)] の選択を解除します。  
このオプションはすべての隔離では選択しないでください。システムは、少なくとも 1 つの隔離エリアからメッセージを削除して、領域を確保する必要があります。
- デフォルトアクションとして [リリース (Release)] を選択すると、保持期間前にリリースされるメッセージに適用する追加のアクションを指定できます。

オプション	情報
件名の変更 (Modify Subject)	追加するテキストを入力し、そのテキストを元の件名の前と後ろのどちらに追加するかを選択します。  たとえば、受信者に不適切なコンテンツを含む可能性があるメッセージであることを警告するテキストを追加します。  (注) 非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。
[X-Header の追加 (Add X-Header) ]	X-Header にはメッセージに対して実行されたアクションを記録できます。この情報は、特定のメッセージが配信された理由についての照会を処理するときなどに役立ちます。  名前と値を入力します。  例：  Name = Inappropriate-release-early  Value = True
添付ファイルを除去 (Strip Attachments)	添付ファイルを除去すると、そのファイルに存在する潜在的なウイルスから保護できます。

**ステップ 3** この隔離へのアクセスを付与するユーザを指定します。

ユーザ	情報
ローカル ユーザ (Local Users)	ローカル ユーザのリストには、隔離にアクセスできるロールを持つユーザだけが含まれます。  すべての管理者は隔離に完全なアクセス権限を持つため、リストでは管理者が除外されます。
外部認証されたユーザ (Externally Authenticated Users)	外部認証を設定しておく必要があります。
カスタムユーザロール (Custom User Roles)	このオプションは、隔離へのアクセス権限を持つ少なくとも1つのカスタムユーザロールを作成している場合にのみ表示されます。

**ステップ 4** 変更を送信し、保存します。

### 次のタスク

[\[メッセージフィルタ \(Message Filters\) \] ページ \(172 ページ\)](#) および [\[コンテンツフィルタ \(Content Filters\) \] ページ \(173 ページ\)](#) を参照してください。

- まだ E メールセキュリティ アプライアンスから隔離を移行していない場合は、次の手順に従います。

移行処理の一部としてこれらの隔離をメッセージフィルタ、コンテンツ フィルタ、および DLP メッセージアクションに割り当てます。

- すでに集約隔離に移行した場合は、次の手順に従います。


メッセージを隔離するためのメッセージフィルタ、コンテンツ フィルタ、および DLP メッセージアクションが E メールセキュリティ アプライアンスに定義されていることを確認します。詳しくは、E メールセキュリティ アプライアンスのユーザガイドまたはオンライン ヘルプを参照してください。

## ポリシー、ウイルス、およびアウトブレイク隔離の設定の編集について



- (注)
- 隔離の名前は変更できません。
  - [隔離内のメッセージの保持期間](#) (368 ページ) も参照してください。

隔離の設定を変更するには、[メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離の名前をクリックします。


新しい Web インターフェイスで隔離の設定を変更するには、[隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] > [表示 (View)] に移動し、必要な隔離で  をクリックします。

レガシー Web インターフェイスで隔離の設定を変更するには、[メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離の名前をクリックします。

## ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定

ポリシー隔離に関連付けられているメッセージフィルタ、コンテンツ フィルタ、データ損失の防止 (DLP) メッセージアクション、DMARC 検証プロファイル、およびそれぞれが設定されている E メールセキュリティ アプライアンスを表示できます。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティの管理コンソールで、[隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] > [表示 (View)] をクリックします。

**ステップ 2** (新しい Web インターフェイスのみ) 必要な隔離を選択して  ボタンをクリックします。

**ステップ 3** [メール (Email) ]>[メッセージの隔離 (Message Quarantine) ]>[ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ]を選択します。

**ステップ 4** ポリシー隔離の名前をクリックします。

**ステップ 5** ページの下部までスクロールし、[関連付けられたメッセージフィルタ/コンテンツ フィルタ/DLP メッセージアクション (Associated Message Filters/Content Filters/DLP Message Actions) ]を確認します。

## ポリシー隔離の削除について

- ポリシー隔離を削除する前に、アクティブなフィルタやメッセージアクションに関連付けられているかどうかを確認します。[ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定 \(372 ページ\)](#) を参照してください。
- フィルタやメッセージアクションが割り当てられている場合でも、ポリシー隔離を削除できます。
- 空でない隔離を削除する場合、ディスクがいっぱいになった際にメッセージを削除しないオプションを選択した場合でも、隔離で定義されたデフォルトアクションはすべてのメッセージに適用されます。[隔離メッセージに自動的に適用されるデフォルトアクション \(369 ページ\)](#) を参照してください。
- フィルタまたはメッセージアクションに関連付けられた隔離を削除した後でそのフィルタまたはメッセージアクションにより隔離されたメッセージは、未分類隔離に格納されます。隔離を削除する前に、未分類隔離のデフォルト設定をカスタマイズしておく必要があります。
- 未分類隔離は削除できません。

## 隔離のステータス、容量、およびアクティビティのモニタリング

目的	操作手順
すべての非スパム隔離に割り当てられている領域の合計	<p>(新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance) ]&gt;[集約管理サービス (Centralized Services) ]&gt;[ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ]を選択し、そのページの最初のセクションを確認します。</p> <p>割り当ての変更方法については、<a href="#">ディスク領域の管理 (567 ページ)</a> を参照してください。</p>

目的	操作手順
スパム隔離以外のすべての隔離で使用可能な領域を確認する	<p>(新しい Web インターフェイスのみ) [隔離 (Quarantine)] &gt; [その他の隔離 (Other Quarantine)] を選択します。</p> <p>または</p> <p>[メール (Email)] &gt; [メッセージの隔離 (Message Quarantine)] &gt; [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、テーブルのすぐ下で確認します。</p> <p>ポリシー、ウイルス、アウトブレイク隔離のために使用可能な領域が [隔離 (Quarantines)] セクションの表の上に表示されます。</p>
現在すべての隔離が使用している合計容量を確認する	<p>(新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [集約管理サービス (Centralized Services)] &gt; [システムステータス (System Status)] を選択します。</p>
現在各隔離に使用されている容量を確認する	<p>(新しい Web インターフェイスのみ) [隔離 (Quarantines Quarantine)] &gt; [その他の隔離 (Other Quarantine)] &gt; [表示 (View)] を選択します。</p> <p>この表には、各隔離で現在使用されている容量が表示されます。</p> <p>または</p> <p>[メール (Email)] &gt; [メッセージの隔離 (Message Quarantine)] &gt; [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します。</p>
現在すべての隔離にあるメッセージの総数を確認する	<p>(新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [集約管理サービス (Centralized Services)] &gt; [システムステータス (System Status)] を選択します。</p>

目的	操作手順
<p>現在各隔離にあるメッセージ数を確認する</p>	<p>(新しい Web インターフェイスのみ) [隔離 (Quarantines Quarantine) ]&gt;[その他の隔離 (Other Quarantine) ]&gt;[表示 (View) ]を選択します。</p> <p>この表には、各隔離で現在使用可能なメッセージの総数が表示されます。</p> <p>または</p> <p>[メール (Email) ]&gt;[メッセージの隔離 (Message Quarantine) ]&gt;[ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ]を選択し、テーブル行でその隔離を確認します。</p>
<p>すべての隔離による総 CPU 使用率を確認する</p>	<p>(新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance) ]&gt;[集約管理サービス (Centralized Services) ]&gt;[システムステータス (System Status) ]を選択して [システム情報 (System Information) ]セクションで確認します。</p>
<p>最後のメッセージが各隔離に送信された日時 (ポリシー隔離間の移動を除く) を確認する</p>	<p>(新しい Web インターフェイスのみ) [隔離 (Quarantine) ]&gt;[その他の隔離 (Other Quarantine) ]&gt;[表示 (View) ]を選択します。</p> <p>この表には、最後のメッセージが隔離された日時が表示されます。</p> <p>または</p> <p>[メール (Email) ]&gt;[メッセージの隔離 (Message Quarantine) ]&gt;[ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines) ]を選択し、テーブル行でその隔離を確認します。</p>

目的	操作手順
ポリシー隔離が作成された日時を確認する	<p>(新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[メール (Email)] &gt; [メッセージの隔離 (Message Quarantine)] &gt; [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択し、隔離名をクリックして、テーブルの隔離名のすぐ下にある行でこの情報を確認します。</p> <p>作成日および作成者の名前はシステムが作成した隔離では使用されません。</p>
ポリシー隔離の作成者の名前	
ポリシー隔離に関連付けられたフィルタおよびメッセージアクションを確認する	「 <a href="#">ポリシー隔離を割り当てるフィルタおよびメッセージアクションの決定 (372 ページ)</a> 」を参照してください。

## 隔離用のディスク容量の使用率に関するアラート

ポリシー、ウイルス、およびアウトブレイク隔離の合計容量が 75%、85%、および 95% になると、アラートが送信されます。使用率は、メッセージが隔離内に格納されたときにチェックされます。たとえば、メッセージが隔離に追加されたときに隔離エリアの合計サイズが指定容量の 75% 以上に増加すると、アラートが送信されます。

アラートの詳細については、[アラートの管理 \(541 ページ\)](#) を参照してください。

## ポリシー隔離とロギング

AsyncOS により、隔離されるすべてのメッセージが個別にロギングされます。

Info: MID 482 quarantined to "Policy" (message filter:policy\_violation)

そのメッセージを隔離したメッセージフィルタまたはアウトブレイク フィルタ機能のルールがかっこ内に出力されます。メッセージを格納する隔離ごとに個別のログエントリが生成されます。

また、隔離から削除されるメッセージも個別にロギングされます。

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

すべての隔離から削除されたメッセージが完全に削除されたり配信がスケジュールされたりすると、次のように個別にロギングされます。

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines



メッセージが再注入されると、新しいメッセージID (MID) を持つ新しいメッセージオブジェクトが作成されます。これは、次のように新しいMID「by 行」がある既存のログメッセージを使用してロギングされます。

Info: MID 483 rewritten to 513 by Policy Quarantine

## メッセージ処理タスクの他のユーザへの割り当てについて

メッセージの処理および確認タスクを、他の管理者ユーザに割り当てることができます。次に例を示します。

- 人事部門ではポリシー隔離の確認と管理を行います。
- 法務部門では Confidential Material 隔離を管理します。

隔離の設定を指定するときに、これらの部門のユーザにアクセス権限を割り当てます。隔離のアクセス権限は、既存のユーザのみに割り当てることができます。

すべてまたは一部の隔離へのアクセスを付与したり、すべての隔離にアクセスできないようにしたりできます。隔離を閲覧するための権限が付与されていないユーザには、GUIまたはCLIの隔離リストにその隔離が表示されません。

### 関連項目

- [ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザグループの指定 \(377 ページ\)](#)
- [管理タスクの分散 \(469 ページ\)](#)

## ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザグループの指定

管理ユーザに隔離へのアクセスを許可した場合、実行できるアクションはそのユーザグループにより異なります。

- 管理者または電子メール管理者グループのユーザは、隔離の作成、設定、削除、および集約ができ、隔離メッセージを管理できます。
- オペレータ、ゲスト、読み込み専用オペレータ、およびヘルプデスク ユーザグループに属するユーザに加え、隔離管理権限を持つカスタム ユーザ ロールのユーザは、隔離エリア内のメッセージの検索、閲覧および処理が可能ですが、隔離の設定変更、作成、削除、または集約はできません。各隔離にどのユーザがアクセスできるかを指定できます。
- Technicians グループに属するユーザは隔離にアクセスできません。

また、メッセージトラッキングおよびデータ消失防止など、関連機能のアクセス権限により、[隔離 (Quarantine)] ページに表示されるオプションおよび情報が異なります。たとえば、メッセージトラッキングにアクセスできないユーザの場合、そのユーザにはメッセージトラッキング、隔離されたメッセージに関する情報が表示されません。

注：セキュリティ管理アプライアンスで設定したカスタム ユーザ ロールがフィルタおよびDLPメッセージアクションのポリシー隔離を指定できるようにする方法については、[カスタム ユーザ ロールの集約隔離アクセスの設定 \(366 ページ\)](#) を参照してください。

エンドユーザは、ポリシー、ウイルス、およびアウトブレイク隔離を閲覧したりアクセスしたりすることはできません。


## ポリシー、ウイルス、またはアウトブレイク隔離のメッセージの操作

### 関連項目

- [隔離内のメッセージの表示 \(378 ページ\)](#)
- [ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの検 \(380 ページ\)](#)
- [隔離内のメッセージの手動処理 \(381 ページ\)](#)
- [複数の隔離内にあるメッセージ \(382 ページ\)](#)
- [メッセージの詳細およびメッセージ内容の表示 \(383 ページ\)](#)
- [隔離されたメッセージの再スキャンについて \(385 ページ\)](#)
- [アウトブレイク隔離 \(386 ページ\)](#)

### 隔離内のメッセージの表示

目的	操作手順
隔離のすべてのメッセージを表示する	<p>(新しい Web インターフェイスのみ) [隔離 (Quarantine)] &gt; [その他の隔離 (Other Quarantine)] &gt; [表示 (View)] を選択します。</p> <p>または</p> <p>[メール (Email)] &gt; [メッセージの隔離 (Message Quarantine)] &gt; [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。</p> <p>テーブル内の隔離の行で、[メッセージ (Messages)] 列の青い番号をクリックします。</p>

目的	操作手順
アウトブレイク隔離エリアのメッセージを表示する	<p>(新しい Web インターフェイス) [隔離 (Quarantine)] &gt; [その他の隔離 (Other Quarantine)] &gt; [表示 (View)] を選択します。</p> <p>または</p> <p>[メール (Email)] &gt; [メッセージの隔離 (Message Quarantine)] &gt; [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。</p> <p>テーブル内の隔離の行で、[メッセージ (Messages)] 列の青い番号をクリックします。</p> <p><a href="#">[ルールサマリー管理 (Manage by Rule Summary)] リンク (387 ページ)</a> または <a href="#">ルールサマリー ビュー (387 ページ)</a> (新しい Web インターフェイスのみ) を参照してください。</p>
隔離のメッセージのリスト表示を移動する	<p>[前へ (Previous)]、[次へ (Next)]、ページ番号、または二重矢印のリンクをクリックします。二重矢印を使用すると、リストの先頭 ([&lt;&lt;]) または最後 ([&gt;&gt;]) のページに移動します。</p> <p>(新しい Web インターフェイスのみ) すべての新しいメッセージの詳細を表示するには、テーブルを下方向にスクロールします。</p>
隔離エリアのメッセージのリストをソートする	列見出しをクリックします (列に複数の項目が含まれる場合と [その他の隔離 (In other quarantines)] 列を除く)。
テーブルの列サイズを変更する	列見出し間の境界線をドラッグします。
テーブル カラムのカスタマイズ	 をクリックして、表示する列を選択し、[閉じる (Close)] をクリックします
メッセージの隔離の原因となったコンテンツを表示する	<a href="#">一致した内容の表示 (384 ページ)</a> を参照してください。

#### 関連項目

- [隔離されたメッセージおよび国際文字セット \(379 ページ\)](#)

## 隔離されたメッセージおよび国際文字セット

メッセージの件名に国際文字セット (2 バイト、可変長、および非 ASCII エンコーディング) の文字が含まれる場合、[ポリシー隔離 (Policy Quarantine)] ページでは、非 ASCII 文字の件名行が復号されて表示されます。

## ポリシー、ウイルス、およびアウトブレイク隔離でのメッセージの検



- (注)
- ユーザは、アクセス権限が付与された隔離内のメッセージだけを検索および表示できません。
  - ポリシー、ウイルスおよびアウトブレイク隔離の検索では、スパム隔離内のメッセージは見つかりません。

**ステップ 1** (新しい Web インターフェイスのみ) クラウドメールセキュリティ管理コンソールで、[隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] > [検索 (Search)] を選択します。

**ステップ 2** (新しい Web インターフェイスのみ) 該当する隔離の青い番号のリンクをクリックします。

**ヒント** (新しい Web インターフェイスのみ) アウトブレイク隔離では、各アウトブレイクルールにより隔離されたすべてのメッセージを検索することもできます。アウトブレイク隔離で [ルールサマリー (Rule Summary)] タブをクリックして、関連するルールをクリックします。

**ステップ 3** [メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。

**ステップ 4** [隔離全体を検索 (Search Across Quarantines)] ボタンをクリックします。

**ヒント** アウトブレイク隔離では、各アウトブレイクルールにより隔離されたすべてのメッセージを検索することもできます。アウトブレイク テーブル行で [ルールサマリー管理 (Manage by Rule Summary)] リンクをクリックします

**ステップ 5** (任意) 他の検索条件を入力します。

- [エンベロープ送信者 (Envelope Sender)] および [エンベロープ受信者 (Envelope Recipient)] には任意の文字を入力できます。エントリの検証は実行されません。
- 検索結果には、指定した条件のすべてに一致するメッセージだけが含まれます。たとえば、[エンベロープ受信者 (Envelope Recipient)] および [件名 (Subject)] を指定した場合は、[エンベロープ受信者 (Envelope Recipient)] および [件名 (Subject)] に指定した条件の両方に一致するメッセージだけが検索結果として表示されます。

### 次のタスク

これらの検索結果は、隔離のリストと同じように操作できます。詳細については、[隔離内のメッセージの手動処理 \(381 ページ\)](#) を参照してください。

検索条件の変更については、[検索条件の変更 \(381 ページ\)](#) を参照してください。

## 検索条件の変更






検索条件をカスタム時間範囲または別の隔離に変更できます。

検索条件を変更するには、[変更 (Modify)] をクリックします。

## 隔離内のメッセージの手動処理

手動でメッセージを処理する場合は、[メッセージアクション (Message Actions)] ページからメッセージアクションを選択します。

メッセージに対し、次の処理を実行できます。

- 削除 
- リリース 
- 隔離からの予定していた終了の遅延 
- 指定した電子メールアドレスへのメッセージのコピーの送信 
- 別の隔離へのメッセージの移動 

通常、以下の状況でリストのメッセージを処理できます。ただし、すべての状況ですべてのアクションが使用できるわけではありません。

- [メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] ページまたは (新しい Web インターフェイスのみ) [隔離 (Quarantine)] > [その他の隔離 (Other Quarantine)] > [表示 (View)] ページの隔離のリストから、隔離内のメッセージ数をクリックします。
- 隔離メッセージのチェックボックスをオンにし、必要な操作を選択します。

複数のメッセージに同時にアクションを実行するには、次の操作を行います。

- メッセージリストの上部の選択リストからオプションを選択する。
- ページの各メッセージの横のチェックボックスを選択する。
- メッセージリストの上部のテーブル見出しでチェックボックスを選択する。これにより、画面に表示されているすべてのメッセージにアクションが適用されます。他のページのメッセージは影響を受けません。

アウトブレイク隔離のメッセージのみに実行できるオプションもあります。Eメールセキュリティ アプライアンスの AsyncOS 向けのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章の [ルールサマリーによる管理 (Manage by Rule Summary)] ビューについての情報を参照してください。

### 関連項目

- [メッセージのコピーの送信 \(382 ページ\)](#)

- [ポリシー隔離間のメッセージの移動について](#) (382 ページ)
- [複数の隔離内にあるメッセージ](#) (382 ページ)
- [隔離メッセージに自動的に適用されるデフォルトアクション](#) (369 ページ)

## メッセージのコピーの送信

メッセージのコピーは、Administrators グループに属しているユーザだけが送信できます。

メッセージのコピーを送信するには、[コピーの送信先 (Send Copy To)] フィールドに電子メールアドレスを入力し、[送信 (Submit)] をクリックします。メッセージのコピーを送信しても、そのメッセージに対してその他のアクションが実行されることはありません。

## ポリシー隔離間のメッセージの移動について

1つのアプライアンス上で、1つのポリシー隔離から別のポリシー隔離へ手動でメッセージを移動できます。

別の隔離にメッセージを移動する場合次のようになります。

- 有効期限は変更されません。メッセージには、元の隔離での保持期限が適用されます。
- 一致したコンテンツおよび他の関連情報を含め、メッセージの隔離理由は変更されません。
- あるメッセージが複数の隔離にあり、すでにメッセージのコピーを保持している場所にメッセージを移動した場合、移動したメッセージのコピーの有効期限および隔離の理由は、移動先の隔離エリアに元からあるメッセージのコピーを上書きします。

## 複数の隔離内にあるメッセージ

同じメッセージが複数の隔離内に格納されている場合、これらの隔離へのアクセス権限があるかどうかにかかわらず、隔離メッセージリストの[その他の隔離 (In other quarantines)] 列に[はい (Yes)] が表示されます。

複数の隔離内にメッセージが格納されている場合、以下の点に注意してください。

- すべての隔離からリリースされるまで、そのメッセージは配信されません。いずれかの隔離から削除されたメッセージは配信されなくなります。
- すべての隔離から削除またはリリースされるまで、そのメッセージはいずれの隔離からも削除されません。

複数の隔離内に格納されているメッセージをリリースする場合、それらのすべての隔離に対するアクセス権限が付与されていない場合があるため、次のルールが適用されます。

- すべての隔離からリリースされるまで、そのメッセージはリリースされません。
- いずれかの隔離内で削除済みとしてマークされると、他の隔離からも配信できなくなります (ただしリリースは可能です)。

メッセージが複数の隔離内にキューイングされ、ユーザがそのうちの1つまたは複数の隔離にアクセスできない場合は、次の処理が行われます。

- ユーザは、ユーザがアクセスできる各隔離についてそのメッセージが存在するかどうか通知されます。
- ユーザがアクセスできる隔離での保持期間の情報のみが GUI に表示されます（同じメッセージに対して、隔離ごとに別々の終了日時が存在します）。
- ユーザは、そのメッセージを保管している他の隔離の名前を知らされません。
- メッセージの隔離先にユーザがアクセスできない場合、その隔離理由は表示されません。
- ユーザがアクセスできるキューのメッセージのみリリースできます。
- ユーザがアクセスできない他の隔離にもメッセージがキューイングされている場合、それらの隔離にアクセスできるユーザによって処理されるまで（あるいは早期または通常の期限切れによって「正常に」メッセージがリリースされるまで）、そのメッセージは変更されずに隔離内に残ります。

## メッセージの詳細およびメッセージ内容の表示

メッセージの内容を表示したり、[隔離されたメッセージ (Quarantined Message)] ページにアクセスしたりするには、メッセージの件名行をクリックします。

[隔離されたメッセージ (Quarantined Message)] ページには、[隔離の詳細 (Quarantine Details)] と [メッセージの詳細 (Message Details)] の 2 つのセクションがあります。

[隔離されたメッセージ (Quarantined Message)] ページから、メッセージを読んだり、メッセージアクションを選択したり、メッセージのコピーを送信したり、。また、メッセージが隔離エリアから解放されるときに Encrypt on Delivery フィルタ アクションによって暗号化されるかどうかを確認することもできます。

[メッセージの詳細 (Message Details)] セクションには、メッセージ本文、メッセージヘッダー、および添付ファイルが表示されます。メッセージ本文は最初の 100 K だけが表示されます。メッセージがそれよりも長い場合は、最初の 100 K が表示され、その後省略記号 (...) が続きます。実際のメッセージが切り捨てられることはありません。この処置は表示目的のためだけに行われます。[メッセージの詳細 (Message Details)] の下部にある [メッセージ部分 (Message Parts)] セクション内の [message body] をクリックすることにより、メッセージ本文をダウンロードできます。また、添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードすることもできます。



(注) [メッセージの詳細 (Message Details)] ページの添付ファイルのダウンロードの上限は 25 MB に制限されています。

ウイルスの含まれるメッセージを表示する場合、ご使用のコンピュータにデスクトップアンチウイルスソフトウェアがインストールされていると、そのアンチウイルスソフトウェアから、ウイルスが検出されると警告される場合があります。これは、ご使用のコンピュータに対して脅威ではないため、無視しても問題ありません。

メッセージについてさらに詳細な情報を表示するには、[メッセージトラッキング (Message Tracking)] リンクをクリックします。



- (注) 特別な **Outbreak** 検疫の場合、追加の機能を利用できます。[アウトブレイク隔離 \(386 ページ\)](#) を参照してください。

#### 関連項目

- [一致した内容の表示 \(384 ページ\)](#)
- [添付ファイルのダウンロード \(385 ページ\)](#)

## 一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して検疫アクションを設定した場合、検疫されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示する場合、DLP ポリシー違反の一致を除き、一致した内容が黄色で強調表示されます。また、`$MatchedContent` アクション変数を使用して、メッセージの一致した内容やコンテンツフィルタの一致をメッセージの件名に含めることもできます。

一致した内容が添付ファイルに含まれる場合は、その判定結果が DLP ポリシー違反、コンテンツフィルタ条件、メッセージフィルタ条件、または画像解析のいずれによるものかに関係なく、添付ファイルの内容がその隔離理由と共に表示されます。

メッセージフィルタまたはコンテンツフィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタアクションを実際にはトリガーしなかった内容が（フィルタアクションをトリガーした内容と共に）GUI で表示されることがあります。GUI の表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。これは、GUI で使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタルールと共に一覧表示するテーブルは正しく表示されます。



図 5: Policy 検疫エリア内で表示された一致内容

The screenshot shows a 'Matched Content' section with a table of attachments. Below the table are 'Headers' and 'Message Parts' sections.

Attachment Name	Matched Content	Condition
FP1.1.txt	<ul style="list-style-type: none"> <li>MS 38930 USA Facilities 662-646-0523 jsamuelson@acmecorp.com 7/17/06 4929132070312710 Acme Corp Irene Gibbs 808 Sumner Street Greenwood MS 38930 USA Publishing 662-646-0522 igibbs@acmecorp.com 2/1/07 4485231592071860 Acme Corp Kathy Lopez 808 Sumner Street Greenwood MS 38930 USA Marketing 662-646-0541 klopez@acmecorp.com 2/1/07 4716298862510192 Acme Corp Marty Smith 808 Sumner Street Greenwood MS 38930 USA Engineering 662-646-0542</li> </ul>	DLP Classifier: Contact Information

**Headers**

```
X-IronPort-AV: E=Sophos;j="4.43,282,1246818600";
d="txt?scan/208";a="178202"
Received: from d2.vmw023-bsd04.jbqa (HELO vmw023-bsd04.jbqa) ([172.22.107.1])
by c360d02.jbqa with ESMTF; 28 Jul 2009 16:25:03 +0530
Message-ID: <792087.518002035-sendEmail@vmw023-bsd04>
From: "user@test.com" <user@test.com>
To: "user1@test.com" <user1@test.com>
Subject: DLPTTEST
Date: Tue, 28 Jul 2009 08:42:11 +0000
X-Mailer: sendEmail-1.55
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----MIME delimiter for sendEmail-538525.714612664"
```

**Message**

Test

Name	Size	Details
[message body]		6 ASCII text, with CRLF line terminators
FP1.1.txt	1K	ASCII text

## 添付ファイルのダウンロード

[メッセージ部分 (Message Parts)] または [一致した内容 (Matched Content)] セクション内の添付ファイルのファイル名をクリックすることにより、メッセージの添付ファイルをダウンロードできます。AsyncOS から、未知の送信元からの添付ファイルにはウイルスが含まれる可能性があることを示す警告が表示され、続行するかどうか尋ねられます。ウイルスが含まれる可能性がある添付ファイルは、ユーザ自身の自己責任においてダウンロードしてください。[メッセージ部分 (Message Parts)] セクション内の [メッセージ本文 (message body)] をクリックすることにより、メッセージ本文をダウンロードすることもできます。

## 隔離されたメッセージの再スキャンについて

隔離されたすべてのキューからメッセージが解放される時、アプライアンスおよび最初にメッセージを隔離したメールポリシーで有効化されている機能によって、次の再スキャンが発生します。

- ポリシーおよびウイルス隔離から解放されるメッセージはアンチウイルス、高度なマルウェア防御、グレイメールエンジンによって再スキャンされます。
- アウトブレイク隔離から解放されたメッセージは、アンチスパム、AMP、およびアンチウイルスエンジンによって再スキャンされます。

- ファイル分析隔離から解放されるメッセージは、脅威に対する再スキャンが実行されません。
- 添付ファイルを含むメッセージは、ポリシー、ウイルス、およびアウトブレイク隔離から解放されるときにファイルレピュテーションサービスによって再スキャンされます。

再スキャン時に、判定結果が前回そのメッセージを処理したときの判定結果と一致する場合、そのメッセージは再隔離されません。逆に、判定が異なると、そのメッセージは別の隔離に送信される可能性があります。

原理的に、メッセージの検疫が無限に繰り返されることはないようになっています。たとえば、メッセージが暗号化されていて、その結果、Virus 検疫に送信されるとします。管理者がそのメッセージを解放しても、アンチウイルスエンジンはまだそのメッセージを復号化できません。しかし、そのメッセージは再隔離されない必要があります。再隔離されるとループ状態となり、そのメッセージは隔離からまったく解放されなくなります。2 回とも判定は同じ結果になるので、システムは 2 回めには Virus 検疫を無視します。

## アウトブレイク隔離

Outbreak 検疫は、Outbreak フィルタ機能の有効なライセンスキーが入力されている場合に存在します。Outbreak フィルタ機能では、しきい値セットに従ってメッセージが Outbreak 検疫に送信されます。詳細については、E メールセキュリティ アプライアンスのオンラインヘルプまたはユーザガイドの「Outbreak Filters」の章を参照してください。

アウトブレイク隔離は、他の隔離と同様の機能を持ち、メッセージを検索したり、メッセージを解放または削除したりなどできます。

アウトブレイク隔離には次のビューがあります。

アウトブレイク隔離には、他の隔離では使用できない追加の機能があります ([ルールサマリー (Rule Summary)] ビュー、メッセージの詳細を表示しているときの **シスコへの送信機能**、およびスケジュールされた保存期間の終了日時で検索結果内のメッセージを並べ替えるオプション)。

アウトブレイクフィルタ機能のライセンスの有効期限が切れると、メッセージをアウトブレイク隔離にそれ以上追加できなくなります。隔離エリア内に現在存在するメッセージの保存期間が終了してアウトブレイク隔離が空になると、GUI の隔離リストにアウトブレイク隔離は表示されなくなります。

### 関連項目

- [アウトブレイク隔離のメッセージの再スキャン \(387 ページ\)](#)
- [ルールサマリー ビュー \(387 ページ\)](#)
- [シスコへの偽陽性または不審なメッセージの報告 \(387 ページ\)](#)

## アウトブレイク隔離のメッセージの再スキャン

アウトブレイク隔離に入れられたメッセージは、新しく公開されたルールによってもう脅威ではないと見なされると、自動的に解放されます。

アプライアンス上でアンチスパムおよびアンチウイルスがイネーブルになっている場合、スキャンエンジンは、メッセージに適用されるメールフローポリシーに基づいて、Outbreak 検疫から解放されたすべてのメッセージをスキャンします。

## ルール サマリー ビュー

[ルール サマリー (Rule Summary)] ビューは、新しい Web インターフェイスでのみ利用可能です。

アウトブレイク隔離で、[ルールサマリー (Rule Summary)] タブをクリックして、アウトブレイク隔離のコンテンツのリストをルール ID ごとにグループ化して表示します。

検疫エリア内のすべてのメッセージに対し、それらのメッセージを検疫させた感染防止ルールに基づいてメッセージアクション (リリースおよび削除) を実行できます。これは、アウトブレイク隔離から多数のメッセージを片付ける場合に適しています。詳細については、Eメールセキュリティアプライアンス向け *AsyncOS* のオンラインヘルプまたはユーザガイドの「Outbreak Filters」の章の「Outbreak Quarantine and the Manage by Rule Summary View」の項を参照してください。

## [ルール サマリー管理 (Manage by Rule Summary)] リンク

検疫リストで Outbreak 検疫の横にある [ルール概要による管理 (Manage by Rule Summary)] リンクをクリックして、[ルール概要による管理 (Manage by Rule Summary)] ページを表示します。検疫エリア内のすべてのメッセージに対し、それらのメッセージを検疫させた感染防止ルールに基づいてメッセージアクション (Release, Delete, Delay Exit) を実行できます。これは、アウトブレイク隔離から多数のメッセージを片付ける場合に適しています。詳細については、Eメールセキュリティアプライアンスのオンラインヘルプまたはユーザガイドの「Outbreak Filters」の章の [ルールサマリーによる管理 (Manage by Rule Summary)] ビューについての情報を参照してください。

## シスコへの偽陽性または不審なメッセージの報告

アウトブレイク隔離内のメッセージについてメッセージの詳細を表示しているとき、偽陽性または不審なメッセージを報告するためにそのメッセージをシスコへ送信できます。

---

**ステップ 1** アウトブレイク隔離内のメッセージの移動

**ステップ 2** 受信者のアドレスを入力し、[送信 (Send)] をクリックします。

---

## 集約されたポリシー隔離のトラブルシューティング

- [管理ユーザがフィルタおよびDLPメッセージアクションの隔離を選択できない \(388 ページ\)](#)
- [集約アウトブレイク隔離から解放されたメッセージが再スキャンされない \(388 ページ\)](#)

### 管理ユーザがフィルタおよびDLPメッセージアクションの隔離を選択できない

#### 問題

管理ユーザが、Eメールセキュリティアプライアンスに対するコンテンツフィルタおよびメッセージフィルタまたはDLPアクションの隔離を表示することも選択することもできません。

#### 解決方法

[カスタムユーザロールの集約隔離アクセスの設定 \(366 ページ\)](#) を参照してください

### 集約アウトブレイク隔離から解放されたメッセージが再スキャンされない

#### 問題

アウトブレイク隔離から解放されたメッセージは配信前に再スキャンされるはずですが、一部の汚染されたメッセージが隔離から配信されました。

#### 解決方法

これは、次で説明した状況で発生する可能性があります [隔離されたメッセージの再スキャンについて \(385 ページ\)](#)



## 第 10 章

# Web セキュリティ アプライアンスの管理

この章は、次の項で構成されています。

- [中央集中型コンフィギュレーション管理について \(389 ページ\)](#)
- [適切な設定公開方式の決定 \(390 ページ\)](#)
- [Configuration Master を使用して中央集中型で Web セキュリティ アプライアンスを管理する \(390 ページ\)](#)
- [Configuration Master の初期化と設定 \(395 ページ\)](#)
- [拡張ファイル公開を使用するための設定 \(407 ページ\)](#)
- [Web セキュリティ アプライアンスへの設定の公開 \(407 ページ\)](#)
- [公開ジョブのステータスと履歴の表示 \(413 ページ\)](#)
- [中央管理型アップグレード管理 \(414 ページ\)](#)
- [Web セキュリティ アプライアンスのステータスの表示 \(420 ページ\)](#)
- [URL カテゴリ セットの更新の準備および管理 \(421 ページ\)](#)
- [Application Visibility and Control \(AVC\) の更新 \(423 ページ\)](#)
- [コンフィギュレーション管理上の問題のトラブルシューティング \(423 ページ\)](#)

## 中央集中型コンフィギュレーション管理について

中央集中型コンフィギュレーション管理を使用すると、Cisco コンテンツ セキュリティ管理アプライアンスから最大 150 の関連する Web セキュリティ アプライアンスに設定を公開できるようになり、次のような利点が得られます。

- Web セキュリティ ポリシーの設定や設定の更新を個々の Web セキュリティ アプライアンスではなくセキュリティ管理アプライアンスで一度行うだけで済み、管理を簡便化および迅速化できます。
- 展開されているネットワーク全体で、ポリシーを均一に適用できます。

設定を Web セキュリティ アプライアンスに公開するには、次の 2 つの方法があります。

- Configuration Master を使用する
- Web セキュリティ アプライアンスからの設定ファイルを使用する (拡張ファイル公開の使用)

## 適切な設定公開方式の決定

セキュリティ管理アプライアンスから設定を公開するには異なる2つの方法があり、それぞれ異なる設定を公開します。設定の中には中央集中型で管理できないものもあります。

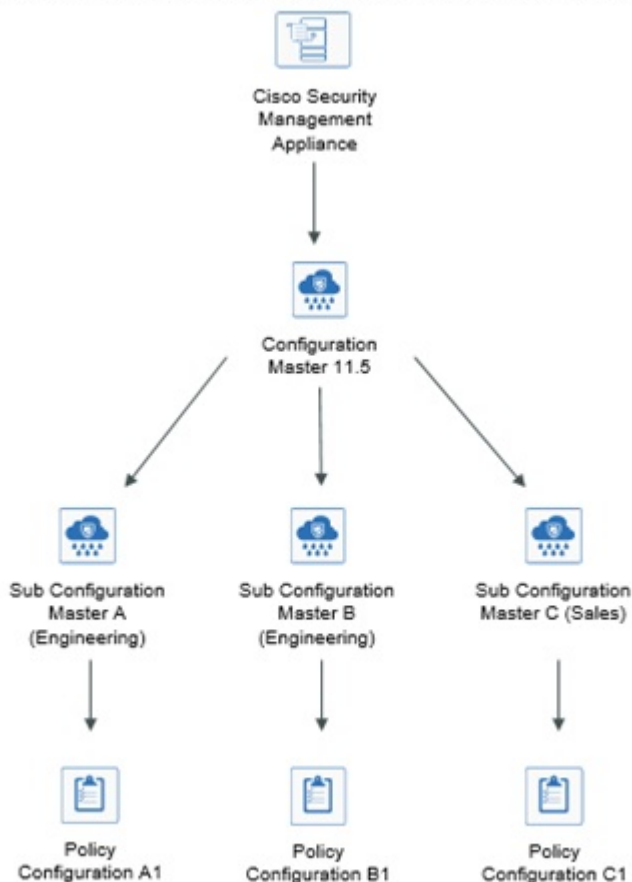
設定の対象	操作手順
<p>Web セキュリティ アプライアンスの [Webセキュリティマネージャ (Web Security Manager) ]メニューに表示される機能。ポリシーやカスタム URL のカテゴリなど。</p> <p>例外：L4 トラフィック モニタの (L4TM) の設定は、Configuration Master の対象に含まれません。</p> <p>サポートの対象となる機能は、Configuration Master のバージョンによって変わります。このバージョンは AsyncOS for Web Security のバージョンに対応します。</p>	<p>Configuration Master を公開します。</p> <p>設定マスターで設定できる機能の多くは、動作させるために、Web セキュリティ アプライアンスでも直接設定する必要があります。たとえば、SOCKS ポリシーは設定マスターで設定可能ですが、最初に SOCKS プロキシを Web セキュリティ アプライアンスで直接設定する必要があります。</p>
<p>注：Cisco Identity Services Engine (ISE) との統合は、各 Web セキュリティ アプライアンスで個別に設定する必要があります。Cisco Identity Services Engine の設定は、Cisco コンテンツセキュリティ管理アプライアンスから発行できません。</p>	<p>拡張ファイル公開を使用します。</p>
<p>連邦情報処理標準の FIPS モード、ネットワーク/インターフェイス設定、DNS、Web Cache Communication Protocol (WCCP)、アップストリーム プロキシグループ、証明書、プロキシモード、NTP などの時間設定、L4 トラフィック モニタ (L4TM) 設定、および認証リダイレクト ホスト名。</p>	<p>管理対象 Web セキュリティ アプライアンスで直接設定します。</p> <p>『AsyncOS for Cisco Web Security Appliances ユーザ ガイド』を参照</p>

## Configuration Master を使用して中央集中型で Web セキュリティ アプライアンスを管理する

セキュリティ管理アプライアンスには異なるバージョンの Configuration Master があるため、Web セキュリティ アプライアンスを中央集中型で管理できます。各 Configuration Master は、配下の複数のサブ Configuration Master をサポートしています。サブ Configuration Master を使用すると、同じ Configuration Master 内で異なるポリシー設定を定義できます。

エンジニアリング チームとセールス チームが Web セキュリティ アプライアンスの AsyncOS 11.7 を使用していると仮定します。組織のポリシーでは、これらのチームに異なるポリシーを定義する必要があります。この場合は、次の図に示すように、Configuration Master 11.7 に 2 つ

のサブ Configuration Master を作成し、各サブ Configuration Master に異なるポリシー設定を定義できます。



### 中央集中型で Web Security Appliances を管理する Configuration Master の設定

次の表に、Configuration Master およびサブ Configuration Master を初期化して設定する手順を示します。

手順	操作内容	対象アプライアンス	詳細情報
ステップ 1	設定のための一般的な要件や注意事項を確認します。	—	<a href="#">Configuration Master を使用するための重要な注意事項 (393 ページ)</a> を参照してください。
ステップ 2	各 Web セキュリティ アプライアンスで使用する設定マスターのバージョンを確認します。	—	使用する <a href="#">Configuration Master のバージョンの確認 (394 ページ)</a> を参照してください。

手順	操作内容	対象アプライアンス	詳細情報
ステップ 3	すべてのターゲット Web セキュリティアプライアンスで、セキュリティ管理アプライアンスの設定マスターで設定するポリシーおよびその他の設定をサポートするために必要な機能を有効にし、設定します。	Web セキュリティアプライアンス	—
ステップ 4 :	(オプション) すべての Web セキュリティアプライアンスの設定モデルとして機能できる実行中の Web セキュリティアプライアンスがある場合、Web セキュリティアプライアンスからの設定ファイルを使用して、セキュリティ管理アプライアンスの設定マスターを迅速に設定できます。	Web セキュリティアプライアンス	Web セキュリティアプライアンスから設定ファイルをダウンロードする方法については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Saving and Loading the Appliance Configuration」を参照してください。
ステップ 5 :	集約設定管理を有効化し、設定します。	セキュリティ管理アプライアンス	セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理の有効化 (394 ページ) を参照してください。
ステップ 6	Configuration Master を初期化します。	セキュリティ管理アプライアンス	Configuration Master の初期化と設定 (395 ページ) を参照してください。
ステップ 7	(任意) サブ Configuration Master を設定します。	セキュリティ管理アプライアンス	サブ Configuration Master の設定 (397 ページ) を参照してください
ステップ 8 :	(任意) サブ Configuration Master をアクティブ設定として選択します。	セキュリティ管理アプライアンス	サブ Configuration Master をアクティブ設定として選択 (399 ページ) を参照してください
ステップ 9	Web セキュリティアプライアンスを設定マスターに関連付けます。	セキュリティ管理アプライアンス	Web Security Appliances と Configuration Master の関連付けについて (395 ページ) を参照してください。



手順	操作内容	対象アプライアンス	詳細情報
ステップ 10	ポリシー、カスタム URL カテゴリ、および Web プロキシ バイパス リストを Configuration Master にインポートするか、手動で設定します。	セキュリティ管理アプライアンス	<a href="#">公開のための設定 (399 ページ)</a> を参照してください
ステップ 11	それぞれの Web セキュリティ アプライアンスで有効にされている機能が、そのアプライアンスに割り当てられている設定マスターで有効化されている機能と一致していることを確認します。	セキュリティ管理アプライアンス	<a href="#">機能が常に有効化されていることの確認 (404 ページ)</a> を参照してください。
ステップ 12	必要とする設定マスターを設定し、必要な機能を有効にしたら、Web セキュリティ アプライアンスに設定を公開します。	セキュリティ管理アプライアンス	<a href="#">Configuration Master の公開 (407 ページ)</a> を参照してください。
ステップ 13	既存の Configuration Master 設定が変更される可能性がある、URL カテゴリ セットの更新のために事前に準備します。	セキュリティ管理アプライアンス	<a href="#">URL カテゴリ セットの更新の準備および管理 (421 ページ)</a>

## Configuration Master を使用するための重要な注意事項



**重要** AsyncOS 12.0 以降にアップグレードする前に、Configuration Master の設定をバックアップする必要があります。Configuration Master バージョン 10.0 以前は Configuration Master バージョン 11.7 以降に置き換えられます。

このリリースにアップグレードしたら、新しい Configuration Master を初期化するか、既存の Configuration Master から設定をインポートする必要があります。以前のリリースの既存の Configuration Master (9.1 など) を使用する場合は、設定を新しい Configuration Master (11.5 など) にコピーできます。

Configuration Master のバージョンが変更されるため、アプライアンス リストは ID およびポリシーから失われます。Configuration Master で Web セキュリティ アプライアンスを関連付ける必要があります。



- (注) 中央集中型で管理する Web セキュリティ アプライアンスのそれぞれについて、同名のレルムに対する設定が同一である場合を除いて、[ネットワーク (Network)] > [認証 (Authentication)] ですべての [レルム名 (Realm Names)] がアプライアンス全体で一意になっていることを確認します。

## 使用する Configuration Master のバージョンの確認

セキュリティ管理アプライアンスには複数の設定マスターがあるため、異なる機能をサポートするさまざまなバージョンの AsyncOS for Web Security を実行する Web セキュリティ アプライアンスを中央集中型で管理できます。

それぞれの Configuration Master には、AsyncOS for Web Security の特定のバージョンで使用する設定が行われています。

お使いの AsyncOS for Web Security のバージョンで使用できる設定マスターを判断するには、互換性マトリクス

(<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>) を参照してください。



- (注) 互換性マトリクスに示されているように、設定マスターのバージョンが、Web セキュリティ アプライアンスの AsyncOS のバージョンと一致する必要があります。古いバージョンの設定マスターから新しいバージョンの Web セキュリティ アプライアンスに対して公開を行うと、Web セキュリティ アプライアンスの設定が設定マスターの設定と一致していない場合には、処理に失敗するおそれがあります。この問題は、[Webアプライアンスステータスの詳細 (Web Appliance Status Details)] ページに不一致が見られない場合でも発生することがあります。この場合は、各アプライアンスでの設定を手動で比較する必要があります。

## セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理の有効化

- ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [集中型設定マネージャ (Centralized Configuration Manager)] を選択します。
- ステップ 2** [有効 (Enable)] をクリックします。
- ステップ 3** システムセットアップウィザードを実行してから初めて集約設定管理を有効にする場合は、エンドユーザーライセンス契約書を確認し、[承認 (Accept)] をクリックします。
- ステップ 4** 変更を送信し、保存します。

# Configuration Master の初期化と設定

- [Configuration Master の初期化](#) (395 ページ)
- [Web セキュリティ アプライアンスからの設定のインポート](#) (401 ページ)
- [公開のための設定](#) (399 ページ)

## Configuration Master の初期化

注：設定マスターを初期化すると、[初期化 (Initialize) ]オプションは使用できなくなります。その代わりに、[公開のための設定](#) (399 ページ) で説明されている方法のいずれかを使用して設定マスターを設定します。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web) ]>[ユーティリティ (Utilities) ]>[設定マスター (Configuration Masters) ]を選択します。

**ステップ 2** [オプション (Options) ]列の [初期化 (Initialize) ]をクリックします。

**ステップ 3** [Configuration Masterの初期化 (Initialize Configuration Master) ]ページで、次の手順を実行します。

- 以前のリリース用の Configuration Master がすでにあり、新しい Configuration Master で同じ設定を適用したい場合は、[Configuration Masterのコピー (Copy Configuration Master) ]を選択します。また、この後の作業で、既存の Configuration Master から設定をインポートすることもできます。
- 上記に該当しない場合は、[デフォルト設定を使用 (Use default settings) ]を選択します。

**ステップ 4** [初期化 (Initialize) ]をクリックします。

これで Configuration Master が使用可能な状態になります。

**ステップ 5** それぞれの Configuration Master のバージョンに対して初期化作業を繰り返します。

## Web Security Appliances と Configuration Master の関連付けについて

Web セキュリティのバージョンと Configuration Master の互換性については、[使用する Configuration Master のバージョンの確認](#) (394 ページ) を参照してください。

Configuration Master にアプライアンスを追加する最も簡単な方法は、状況に応じて異なります。

条件 (IF)	参照する手順
Web セキュリティ アプライアンスをセキュリティ管理アプライアンスにまだ追加していません。	<a href="#">Web Security Appliances の追加と Configuration Master のバージョンとの関連付け</a> (396 ページ)

条件 (IF)	参照する手順
Web セキュリティ アプライアンスを追加済みです。	<a href="#">Configuration Master と Web セキュリティ アプライアンスとの関連付け (397 ページ)</a>
関連する Configuration Master をアプライアンス リストに表示します。	<a href="#">アプライアンス リストでの関連する Configuration Master の表示 (398 ページ)</a>

## Web Security Appliances の追加と Configuration Master のバージョンとの関連付け

まだ Web セキュリティ アプライアンスを中央集中管理の対象に追加していない場合は、この手順を実行してください。

### 始める前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。 [使用する Configuration Master のバージョンの確認 \(394 ページ\)](#) を参照してください。

- 
- ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティ アプライアンス (Security Appliances)] を選択します。
- ステップ 2** [Webアプライアンスの追加 (Add Web Appliance)] をクリックします。
- ステップ 3** [アプライアンス名 (Appliance Name)] および [IP アドレス (IP Address)] テキスト フィールドに、Web セキュリティアプライアンスの管理インターフェイスのアプライアンス名と IP アドレスまたは変換可能なホスト名を入力します。
- (注) [IP アドレス (IP Address)] フィールドに DNS 名を入力した場合でも、[送信 (Submit)] をクリックすると、IP アドレスに変換されます。
- ステップ 4** Centralized Configuration Manager サービスが事前に選択されています。
- ステップ 5** [接続の確立 (Establish Connection)] をクリックします。
- ステップ 6** 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection)] をクリックします。
- (注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。
- ステップ 7** 「Success」メッセージがページのテーブルの上に表示されるまで待機します。
- ステップ 8** アプライアンスに関連付ける Configuration Master のバージョンを選択します。
- (注) 特定のバージョンの Configuration Master のサブセットを設定し、Web セキュリティアプライアンスを割り当てると、Web セキュリティアプライアンスに関連付けられているサブ Configuration Master バージョンがドロップダウン リストに表示されます。
- ステップ 9** 変更を送信し、保存します。

**ステップ 10** 中央集中型コンフィギュレーション管理をイネーブルにする Web Security Appliance ごとに、この手順を繰り返します。

---

## Configuration Master と Web セキュリティ アプライアンスとの関連付け

Web セキュリティ アプライアンスをセキュリティ管理アプライアンスにすでに追加している場合、次の手順を使用して、Web セキュリティ アプライアンスと設定マスターバージョンをすぐに関連付けることができます。

### 始める前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。使用する Configuration Master のバージョンの確認 (394 ページ) を参照してください。

---

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] を選択します。

(注) Configuration Master が [無効 (Disabled)] と表示されている場合にイネーブルにするには、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [セキュリティサービス表示 (Security Services Display)] の順にクリックし、次に [表示設定の編集 (Edit Display Settings)] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、[公開する機能の有効化 \(405 ページ\)](#) を参照してください。

**ステップ 2** [セキュリティアプライアンス (Security Appliances)] をクリックします。

**ステップ 3** 必要な Web セキュリティ アプライアンスをクリックします。

**ステップ 4** Configuration Master の必要な設定を選択します。

[Web] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] ページに Configuration Master のさまざまな設定が表示されます。

**ステップ 5** 変更を送信し、保存します。

---

## サブ Configuration Master の設定

---

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] を選択します。

(注) Configuration Master 設定が [無効 (Disabled)] と表示されている場合にイネーブルにするには、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [セキュリティサービス表示 (Security Services Display)] の順にクリックし、次に [表示設定の編集 (Edit Display Settings)] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、[公開する機能の有効化 \(405 ページ\)](#) を参照してください。

## アプライアンス リストでの関連する Configuration Master の表示

ステップ 2 [新しい Configuration Master (New Configuration Master) ] ページで、[新規 (New) ] をクリックします。

ステップ 3 Configuration Master に一意の名前を入力します (11\_5\_new など)。

(注) 名前には、英文字、数字、およびアンダースコアのみを使用できます。先頭にアンダースコアを付けることはできません。

ステップ 4 ドロップダウン リストから Configuration Master のバージョンを選択します。

ステップ 5 [設定ソースの選択 (Select Configuration Source) ] で、ドロップダウン リストから [設定マスター (Configuration Master) ] を選択します。

ステップ 6 [送信 (Submit) ] をクリックし、変更をコミットします。

---

## アプライアンス リストでの関連する Configuration Master の表示

### 始める前に

まだ追加していない場合は、各 Web セキュリティ アプライアンスに適した Configuration Master のバージョンを選択してください。 [使用する Configuration Master のバージョンの確認 \(394 ページ\)](#) を参照してください。

Web セキュリティ アプライアンスがセキュリティ管理アプライアンスにすでに追加されている場合、次の手順を使用して、関連する Configuration Master のバージョンを Web セキュリティ アプライアンス リストに表示できます。

---

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ (Web) ] > [ユーティリティ (Utilities) ] > [設定マスター (Configuration Masters) ] を選択します。

(注) Configuration Master が [無効 (Disabled) ] と表示されている場合にイネーブルにするには、[ウェブ (Web) ] > [ユーティリティ (Utilities) ] > [セキュリティサービス表示 (Security Services Display) ] の順にクリックし、次に [表示設定の編集 (Edit Display Settings) ] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、 [公開する機能の有効化 \(405 ページ\)](#) を参照してください。

ステップ 2 [セキュリティアプライアンス (Security Appliances) ] をクリックします。

[セキュリティアプライアンス (Security Appliances) ] ページは、[管理アプライアンス (Management Appliances) ] > [集約管理サービス (Centralized Services) ] > [セキュリティアプライアンス (Security Appliances) ] ページと同じです。Web セキュリティ アプライアンスおよび関連付けられた Configuration Master を追加済みである場合は、Web セキュリティ アプライアンスに関連付けられている Configuration Master と AsyncOS バージョンを表示できます。

---

## サブ Configuration Master の削除

サブ Configuration Master の設定 (397 ページ) でサブ Configuration Master を設定した場合、この設定を削除するには次の手順を使用します。

- 
- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] を選択します。
- (注) Configuration Master が [無効 (Disabled)] と表示されている場合にイネーブルにするには、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [セキュリティサービス表示 (Security Services Display)] の順にクリックし、次に [表示設定の編集 (Edit Display Settings)] をクリックします。対象とする Configuration Master のチェックボックスを選択して、イネーブルにします。詳細については、[公開する機能の有効化 \(405 ページ\)](#) を参照してください。
- ステップ 2** 該当するサブ Configuration Master でゴミ箱アイコンをクリックします。
- (注) Web セキュリティ アプライアンスに関連付けられている Configuration Master は削除できません。
- ステップ 3** 変更を送信し、保存します。
- 

## サブ Configuration Master をアクティブ設定として選択

サブ Configuration Master を設定する場合は、必要な設定をアクティブ設定として割り当てる必要があります。

- 
- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] を選択します。
- ステップ 2** Configuration Master の必要な設定バージョンで [編集 (Edit)] をクリックします。Configuration Master のバージョンを選択すると、Configuration Master の既存の設定が置き換えられます。
- ステップ 3** 変更を保存します。
- 変更を確定すると、[設定マスター (Configuration Master)] ドロップダウンのラベルが、選択した Configuration Master のバージョンに変更されたことを確認できます。
- 

## 公開のための設定

公開する設定を Configuration Master に設定します。

Configuration Master の設定には、いくつかの方法があります。

条件 (IF)	操作手順
<p>AsyncOS for Security Management の以前のリリースからアップグレードする場合および</p> <p>新しい Configuration Master のバージョンを初期化 (以前の既存の Configuration Master を新しいバージョンにコピー) していない場合</p>	<p>古いバージョンをインポートします。 <a href="#">既存の Configuration Master からのインポート (400 ページ)</a> を参照してください。</p>
<p>Web セキュリティ アプライアンスを設定済みで、同じ設定を複数の Web セキュリティ アプライアンスで使用する場合</p>	<p>その Web セキュリティ アプライアンスから保存したコンフィギュレーションファイルを Configuration Master にインポートします</p> <p>(Configuration Master を使用して中央集中型で Web セキュリティアプライアンスを管理する (390 ページ) でコンフィギュレーションファイルを保存した場合)。</p> <p>インポートの手順については、 <a href="#">Web セキュリティアプライアンスからの設定のインポート (401 ページ)</a> を参照してください。</p>
<p>インポートした設定を変更する必要がある場合</p>	<p><a href="#">Configuration Master での Web セキュリティ機能の直接設定 (401 ページ)</a> を参照してください。</p>
<p>ポリシー設定、URL カテゴリ、バイパス設定を Web セキュリティ アプライアンスでまだ設定していない場合</p>	<p>これらの設定をセキュリティ管理アプライアンスの該当する Configuration Master に直接設定します。</p> <p>「<a href="#">Configuration Master での Web セキュリティ機能の直接設定 (401 ページ)</a>」を参照してください。</p>

## 既存の Configuration Master からのインポート

既存の Configuration Master を新しい Configuration Master のバージョンにアップグレードすることができます。

- 
- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] を選択します。
- ステップ 2** [オプション (Options)] 列で、[設定のインポート (Import Configuration)] をクリックします。
- ステップ 3** [設定ソースの選択 (Select Configuration Source)] で、リストから [設定マスター (Configuration Master)] を選択します。
- ステップ 4** この設定に、既存のカスタム ユーザ ロールを取り込むかどうかを選択します。
- ステップ 5** [インポート (Import)] をクリックします。
-



## 次のタスク

[Custom Web User ロールについて \(478 ページ\)](#)

## Web セキュリティ アプライアンスからの設定のインポート

Web セキュリティ アプライアンスで機能している既存の設定を使用する場合は、そのコンフィギュレーションファイルをセキュリティ管理アプライアンスにインポートして、設定マスターにポリシー設定を作成できます。

### 始める前に

コンフィギュレーション ファイルと Configuration Master のバージョンの互換性を確認してください。使用する Configuration Master のバージョンの確認 (394 ページ) を参照してください。



#### 注意

管理対象の Web セキュリティ アプライアンスに設定をすでに公開してある場合でも、互換性のある Web コンフィギュレーション ファイルを何回でもインポートすることができます。コンフィギュレーション ファイルを設定マスターにインポートすると、選択した設定マスターに関連付けられている設定が上書きされます。また、[セキュリティサービス表示 (Security Services Display)] ページのセキュリティ サービスの設定は、インポートしたファイルと一致するように設定されます。



#### (注)

セキュリティ管理アプライアンスより古い URL カテゴリ セットを使用するコンフィギュレーション ファイルをインポートしようとする、ロードに失敗します。

- ステップ 1 Web セキュリティ アプライアンスのコンフィギュレーション ファイルを保存します。
- ステップ 2 セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [設定マスター (Configuration Masters)] を選択します。
- ステップ 3 [オプション (Options)] 列で、[設定のインポート (Import Configuration)] をクリックします。
- ステップ 4 [設定の選択 (Select Configuration)] ドロップダウン リストから、[Web 設定ファイル (Web Configuration File)] を選択します。
- ステップ 5 [新しいマスターのデフォルト (New Master Defaults)] セクションで、[参照 (Browse)] をクリックし、Web セキュリティ アプライアンスから有効なコンフィギュレーション ファイルを選択します。
- ステップ 6 [ファイルのインポート (Import File)] をクリックします。
- ステップ 7 [インポート (Import)] をクリックします。

## Configuration Master での Web セキュリティ 機能の直接設定

Configuration Master では、バージョンに応じて次の機能を設定できます。

## 設定マスターで機能を設定する場合の SMA 特有の違い

<ul style="list-style-type: none"> <li>• ID/識別プロファイル</li> <li>• SaaS ポリシー</li> <li>• 復号ポリシー (Decryption Policies)</li> <li>• ルーティング ポリシー</li> <li>• アクセス ポリシー</li> <li>• Web トラフィック タップ ポリシー (注) Web トラフィック タップ ポリシーを定義するには、Web セキュリティ アプライアンスの Web トラフィック のタップ機能を有効にする必要があります。</li> <li>• 全体の帯域幅の制限 (Overall Bandwidth Limits)</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco データ セキュリティ</li> <li>• 発信マルウェア スキャン (Outbound Malware Scanning)</li> <li>• 外部データ消失 防止</li> </ul>	<ul style="list-style-type: none"> <li>• SOCKS ポリシー (SOCKS Policies)</li> <li>• カスタム URL カテゴリ</li> <li>• 定義されている時間範囲とクォータ</li> <li>• バイパス設定</li> <li>• L4 トラフィック モニタ (L4 Traffic Monitor)</li> </ul>
--	--	--

設定マスターで各機能を直接設定するには、[Web] > [設定マスター (Configuration Master)] <version> > <feature> を選択します。

設定マスターで機能を設定する場合の SMA 特有の違い (402 ページ) で説明する一部の項目を除いて、設定マスターで機能を設定する方法は、Web セキュリティ アプライアンスで同じ機能を設定する場合と同じです。各説明については、ご使用の Web セキュリティ アプライアンスのオンライン ヘルプ、または設定マスターのバージョンに対応する AsyncOS バージョンの『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。必要な場合は、使用する Configuration Master のバージョンの確認 (394 ページ) を参照して、使用している Web セキュリティ アプライアンスに対応する正しい設定マスターを判別してください。

Web セキュリティ ユーザ ガイドのすべてのバージョンが <https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html> から利用可能です。

## 設定マスターで機能を設定する場合の SMA 特有の違い

設定マスターで機能を設定するときには、以下で説明する Web セキュリティ アプライアンスで同じ機能を直接設定する場合との違いに注意してください。

表 68: 機能の設定 : Configuration Master と Web Security Appliance との違い

機能またはページ	詳細 (Details)
すべての機能、特に各リリースでの新機能	設定マスターで設定する各機能について、セキュリティ管理アプライアンスで [Web] > [ユーティリティ (Utilities)] > [セキュリティサービス表示 (Security Services Display)] にある機能を有効にする必要があります。詳細については、 <a href="#">機能が常に有効化されていることの確認 (404 ページ)</a> を参照してください。

機能またはページ	詳細 (Details)
ID (Identities) / 識別プロファイル (Identification Profiles)	<ul style="list-style-type: none"> <li>• <a href="#">Configuration Master</a> で ID/識別プロファイルを使用する場合のヒント (404 ページ) を参照してください。</li> <li>• トランスペアレント ユーザ ID をサポートする認証レムがある Web セキュリティアプライアンスが管理対象アプライアンスとして追加されている場合、ID/識別プロファイルの追加または編集時に [ユーザを透過的に識別 (Identify Users Transparently) ] オプションを使用できます。</li> </ul>
Cisco Identity Services Engine (ISE) を使用してユーザを識別するポリシー	<p>セキュリティグループタグ (SGT) 情報は、Web セキュリティアプライアンスから約5分ごとに更新されます。管理アプライアンスは、ISE サーバと直接通信することはありません。</p> <p>SGT のリストをオンデマンドで更新するには、[Web]&gt;[ユーティリティ (Utilities) ]&gt;[Webアプライアンスステータス (Web Appliance Status) ] を選択し、ISE サーバに接続されている Web セキュリティアプライアンスをクリックして、[データの更新 (Refresh Data) ] をクリックします。他のアプライアンスについて必要に応じて繰り返します。</p> <p>一般的な導入シナリオでは、会社には、すべての WSA が接続する ISE サーバは1台だけあります (これが ISE の本質です) 。異なるデータを持つ複数の ISE サーバはサポートされません。</p>
[アクセスポリシー (Access Policies) ]>[グループの編集 (Edit Group) ]	<p>[ポリシーメンバの定義 (Policy Member Definition) ] セクションで [ID (Identities) ]/[識別プロファイルおよびユーザ (Identification Profiles and Users) ] オプションを設定する際、外部ディレクトリ サーバを使用している場合には以下が適用されます。</p> <p>[グループの編集 (Edit Group) ] ページでグループを検索した場合、検索結果の最初の 500 項目しか表示されません。目的のグループが見つからない場合は、そのグループを [ディレクトリ (Directory) ] 検索フィールドに入力して、[追加 (Add) ] ボタンをクリックすると、[承認済みグループ (Authorized Groups) ] リストに追加することができます。</p>
[アクセスポリシー (Access Policies) ]>[Webレピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings) ]	
SaaS ポリシー (SaaS Policies)	<p>認証オプションの [透過的なユーザ識別によって検出されたSaaSユーザにプロンプトを出力する (Prompt SaaS users who have been discovered by transparent user identification) ] は、トランスペアレント ユーザ ID をサポートする認証レムが設定された Web セキュリティアプライアンスが管理対象アプライアンスとして追加されている場合のみ有効になります。</p>

## Configuration Master で ID/識別プロファイルを使用する場合のヒント

セキュリティ管理アプライアンスで ID/識別プロファイルを作成する際には、特定のアプライアンスのみに適用されるオプションがあります。たとえば、セキュリティ管理アプライアンスを購入し、Web セキュリティ アプライアンスごとに作成された既存の Web セキュリティ アプライアンスのコンフィギュレーションとポリシーを保持する場合は、1つのファイルをマシンにロードし、次に他のマシンから手動でポリシーを追加する必要があります。

これを実行するための方法の1つとして、各アプライアンスに ID/識別プロファイルのセットを作成し、これらの ID/識別プロファイルを参照するポリシーを設定する方法があります。セキュリティ管理アプライアンスが設定を公開すると、これらの ID/識別プロファイルと、ID/識別プロファイルを参照するポリシーは自動的に削除され、無効になります。この方法を使用すると、手動で何も設定する必要がありません。これは基本的に「アプライアンスごと」の ID/識別プロファイルです。

この方法の唯一の問題は、デフォルトのポリシーまたは ID/識別プロファイルが、サイト間で異なる場合です。たとえば、あるサイトではポリシーを「default allow with auth」に設定し、別のサイトでは「default deny」に設定している場合です。この場合、アプライアンスごとの ID/識別プロファイルとポリシーをデフォルトのすぐ上に作成する必要があります。基本的には独自の「デフォルト」ポリシーを作成します。

## 機能が常に有効化されていることの確認

Configuration Master を公開する前に、それが公開されることと、公開後に目的の機能がイネーブルになり、意図するように設定されていることを確認します。

このためには、次の両方を実行してください。

- [イネーブルにされている機能の比較 \(404 ページ\)](#)
- [公開する機能の有効化 \(405 ページ\)](#)



- 
- (注) 異なる機能を持つ複数の Web セキュリティ アプライアンスが同じ設定マスターに割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこれらの手順を実行する必要があります。
- 

## イネーブルにされている機能の比較

それぞれの Web セキュリティ アプライアンスで有効にされている機能が、そのアプライアンスに関連付けられている設定マスターで有効化されている機能と一致していることを確認します。



- 
- (注) 異なる機能を持つ複数の Web セキュリティ アプライアンスが同じ設定マスターに割り当てられている場合は、各アプライアンスを別個に公開するようにし、公開前にこのチェックを実行する必要があります。
-

- ステップ 1 セキュリティ管理アプライアンスで、[Web]>[ユーティリティ (Utilities)]>[Webアプライアンスステータス (Web Appliance Status)] を選択します。
- ステップ 2 設定マスターを公開する Web セキュリティ アプライアンスの名前をクリックします。
- ステップ 3 [セキュリティサービス (Security Services)] テーブルまでスクロールします。
- ステップ 4 イネーブルにされているすべての機能の機能キーがアクティブで、期限切れでないことを確認します。
- ステップ 5 [サービス (Services)] 列の設定を比較します。

[Webアプライアンスサービス (Web Appliance Service)] 列と、[管理アプライアンス上でサービスを表示しますか? (Is Service Displayed on Management Appliance?)] 列が一致している必要があります。

- [有効化 (Enable)] = [はい (Yes)]
- [無効 (Disabled)] および [未設定 (Not Configured)] = [いいえ (No)] または [無効 (Disabled)]
- N/A = 適用されません。たとえば、そのオプションは Configuration Master で設定できませんが、一覧には表示されて、機能キーのステータスを確認することができます。

コンフィギュレーションの不一致は、赤色のテキストで表示されます。

### 次のタスク

ある機能についてのイネーブルおよびディセーブルの設定が一致していない場合は、次のいずれかを実行します。

- Configuration Master の対応する設定を変更します。[公開する機能の有効化 \(405 ページ\)](#) を参照してください。
- Web Security Appliance の当該の機能をイネーブルまたはディセーブルにします。変更内容によっては、複数の機能に影響が生じる場合があります。関連する機能については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

## 公開する機能の有効化

Configuration Master を使用して設定を公開する機能をイネーブルにします。

### 始める前に

イネーブルにする機能とディセーブルにする機能を確認します。[イネーブルにされている機能の比較 \(404 ページ\)](#) を参照してください。

- ステップ 1 セキュリティ管理アプライアンスで、[ウェブ (Web)]>[ユーティリティ (Utilities)]>[セキュリティサービス表示 (Security Services Display)] を選択します。
- ステップ 2 [設定の編集 (Edit Settings)] をクリックします。  
[セキュリティサービス表示の編集 (Edit Security Services Display)] ページに、各 Configuration Master に表示される機能が一覧されます。

横に [なし (N/A)] と表示されている機能は、その Configuration Master のバージョンで使用できないことを意味します。

(注) Web プロキシは機能として一覧されていません。これは、Web プロキシは Web セキュリティ アプライアンスで管理されているプロキシタイプのいずれかを実行するために有効になっていると見なされているためです。Web プロキシを無効にすると、Web セキュリティ アプライアンスに公開されたすべてのポリシーが無視されます。

**ステップ 3** (任意) 使用しない Configuration Master は非表示にします。手順および注意については、[使用しない Configuration Master のディセーブル化 \(406 ページ\)](#) を参照してください。

**ステップ 4** 使用する各設定マスターについて、有効にする各機能に対する [はい (Yes)] チェックボックスを選択または選択解除します。

次の特定機能には特に注意してください (使用可能なオプションは、Configuration Master のバージョンによって異なります)。

- トランスペアレント モード。フォワード モードを使用した場合、プロキシ バイパス機能は使用できなくなります。
- HTTPS プロキシ。HTTPS プロキシは、復号ポリシーを実行するためにイネーブルにする必要があります。
- アップストリーム プロキシグループ。ルーティング ポリシーを使用する場合は、Web セキュリティ アプライアンスでアップストリーム プロキシグループが使用できるようになっている必要があります。

**ステップ 5** [送信 (Submit)] をクリックします。セキュリティ サービスの設定に加えた変更が、Web セキュリティ アプライアンスで設定されたポリシーに影響する場合、GUI に特定の警告メッセージが表示されます。変更を送信することが確実な場合は、[続行 (Continue)] をクリックします。

**ステップ 6** [セキュリティ サービス表示 (Security Services Display)] ページで、選択した各オプションの横に [はい (Yes)] と表示されることを確認します。

**ステップ 7** 変更を保存します。

#### 次のタスク

- 公開先のアプライアンスに対して、すべての機能が正しく有効または無効になっていることを確認します。[イネーブルにされている機能の比較 \(404 ページ\)](#) を参照してください。
- 公開先の各 Web セキュリティ アプライアンスで、設定マスターに対して有効にした機能と一致する機能が有効になっていることを確認します。

## 使用しない Configuration Master のディセーブル化

使用しない Configuration Master を表示しないようにすることができます。

ただし、少なくとも 1 つの Configuration Master は有効にする必要があります。



- (注) Configuration Master をディセーブルにすると、それに対するすべての参照が、対応する [設定マスター (Configuration Master) ] タブを含めて GUI から削除されます。その Configuration Master を使用する保留中の公開ジョブは削除され、非表示の Configuration Master に割り当てられていたすべての Web セキュリティ アプライアンスが、割り当てられていないものとして再分類されます。

- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web) ]>[ユーティリティ (Utilities) ]>[セキュリティサービス表示 (Security Services Display) ] を選択します。
- ステップ 2** [設定の編集 (Edit Settings) ] をクリックします。
- ステップ 3** 使用しない Configuration Master に対するチェックボックスを選択解除します。
- ステップ 4** 変更を送信し、保存します。

## 拡張ファイル公開を使用するための設定

システムで Configuration Master を使用するよう設定されている場合は、拡張ファイル公開に対する設定も行われています。

そうでない場合は、次の項で説明する手順を実行してください。これらは、拡張ファイル公開だけでなく、Configuration Master の公開にも適用されます。

- [セキュリティ管理アプライアンスでの中央集中型コンフィギュレーション管理の有効化 \(394 ページ\)](#)
- [Configuration Master の初期化 \(395 ページ\)](#)
- [Web Security Appliances と Configuration Master の関連付けについて \(395 ページ\)](#)

## Web セキュリティ アプライアンスへの設定の公開

- [Configuration Master の公開 \(407 ページ\)](#)
- [拡張ファイル公開による設定の公開 \(412 ページ\)](#)

## Configuration Master の公開

Configuration Master で設定を編集またはインポートした後、その設定を、Configuration Master に関連付けられている Web セキュリティ アプライアンスへ公開できます。

- [Configuration Master を公開する前に \(408 ページ\)](#)
- [Configuration Master の公開 \(409 ページ\)](#)
- [Configuration Master を後日公開 \(410 ページ\)](#)
- [コマンドラインインターフェイスによる Configuration Master の公開 \(411 ページ\)](#)

## Configuration Master を公開する前に

Configuration Master を公開すると、その Configuration Master に関連付けられている Web セキュリティ アプライアンスの既存のポリシー情報が上書きされます。

Configuration Master を使用して設定できる設定の詳細については、[適切な設定公開方式の決定 \(390 ページ\)](#) を参照してください。

すべての公開ジョブ

- (初回のみ) [Configuration Master を使用して中央集中型で Web セキュリティ アプライアンスを管理する \(390 ページ\)](#) で説明する手順に従います。
- Configuration Master を公開し、公開後に意図する機能がイネーブルになるようにするには、各 Web セキュリティ アプライアンスと、これに対応する Configuration Master の機能を確認し、必要に応じて変更を加えます。[イネーブルにされている機能の比較 \(404 ページ\)](#)、および必要に応じて[公開する機能の有効化 \(405 ページ\)](#) を参照してください。ターゲットアプライアンスで有効にされていない機能の設定を公開しても、これらの設定は適用されません。

同じ Configuration Master に割り当てられている複数の Web セキュリティ アプライアンスで異なる機能が有効になっている場合は、各アプライアンスに個別に公開する必要があります。それぞれの公開前に機能が有効になっていることを確認してください。

公開中に検出された設定の不一致を特定するには、[公開履歴の表示 \(414 ページ\)](#) を参照してください。

- 公開前に、対象とする各 Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存して、公開された設定によって問題が生じた場合に既存の設定を復元できるようにしておきます。詳細については、『[AsyncOS for Cisco Web Security Appliances User Guide](#)』を参照してください。
- Web セキュリティ アプライアンスでコミットしたときに Web プロキシの再起動が必要になる変更内容は、それをセキュリティ管理アプライアンスから公開したときにもプロキシの再起動が必要になります。この場合は、警告が発生します。

Web プロキシの再起動により、Web セキュリティ サービスは一時的に中断されます。

- ID/識別プロファイルに対する変更を公開すると、すべてのエンドユーザが再認証を受ける必要が生じます。

特殊な状況

- 対象の Web セキュリティ アプライアンスで AsyncOS を復元した場合は、そのアプライアンスを異なる Configuration Master と関連付けなければならない場合があります。
- Configuration Master を、トランスペアレント ユーザ ID が有効化されたレルムを持たない Web セキュリティ アプライアンスに公開したものの、[ID (Identity)]/[識別プロファイル (Identification Profile)] または [SaaSポリシー (SaaS Policy)] でトランスペアレント ユーザ ID を選択していると、次のようになります。
  - [ID (Identity)]/[識別プロファイル (Identification Profiles)] の場合、トランスペアレント ユーザ ID は無効になり、代わりに [認証が必要 (Require Authentication)] オプションが選択されます。



- [SaaSポリシー (SaaS Policies)] の場合、トランスペアレント ユーザ ID のオプションは無効になり、代わりにデフォルトのオプション (SaaS ユーザに対して常にプロキシ認証を要求) が選択されます。
- RSA サーバ用に設定されていない複数の Web セキュリティ アプライアンスにセキュリティ管理アプライアンスから外部 DLP ポリシーを公開すると、セキュリティ管理アプライアンスによって次の公開ステータス警告が送信されます。

**「The Security Services display settings configured for Configuration Master <version> do not currently reflect the state of one or more Security Services on Web Appliances associated with this publish request. The affected appliances are: “<WSA Appliance Names>”. This may indicate a misconfiguration of the Security Services display settings for this particular Configuration Master. Go to the Web Appliance Status page for each appliance provides a detailed view to troubleshooting this issue. Do you want to continue publishing the configuration now?」**

公開を続行した場合、RSA サーバ用に設定されていない Web セキュリティ アプライアンスは、外部 DLP ポリシーを受信しますが、これらのポリシーはディセーブルにされます。外部 DLP サーバが設定されていない場合、Web セキュリティ アプライアンスの [外部 DLP (External DLP)] ページには公開されたポリシーが表示されません。

Configuration Master の ID/識別プロファイルのスキーム	Web Security Appliance の ID/識別プロファイル
Kerberos 認証を使用	NTLMSSP 認証または Basic 認証を使用
Kerberos 認証または NTLMSSP 認証を使用	NTLMSSP 認証を使用
Kerberos 認証、NTLMSSP 認証、または Basic 認証を使用	NTLMSSP 認証または Basic 認証を使用

外部で認証されたユーザの場合は、Web セキュリティ アプライアンスに割り当てられているすべての Configuration Master のリストを表示し、現在初期化されている設定を公開することはできません。Configuration Master の別のサブセットを公開する場合は、管理者に問い合わせてください。

## Configuration Master の公開

始める前に

[Configuration Master を公開する前に \(408 ページ\)](#) の重要な要件と情報を参照してください。

- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Webアプライアンスへの公開 (Publish to Web Appliances)] を選択します。
- ステップ 2** [今すぐ設定を公開する (Publish Configuration Now)] をクリックします。
- ステップ 3** デフォルトでは [システム生成のジョブ名 (System-generated job name)] が選択されています。あるいは、ユーザ定義のジョブ名 (80 文字以下) を入力します。
- ステップ 4** 公開する Configuration Master を選択します。

(注) 特定のバージョンの Configuration Master のサブセットを設定し、Web セキュリティ アプライアンスを割り当てると、Web セキュリティ アプライアンスに関連付けられているサブ Configuration Master バージョンがドロップダウン リストに表示されます。

**ステップ 5** Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[割り当てられたすべてのアプライアンス (All assigned appliances) ] を選択します。

または

[リスト内のアプライアンスを選択してください (Select appliances in list) ] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

**ステップ 6** [公開 (Publish) ] をクリックします。

[公開中 (Publish in Progress) ] ページに表示される赤色の経過表示バーとテキストは、公開中にエラーが発生したことを表します。別のジョブが現在公開中の場合、要求は前のジョブが完了すると実行されます。

(注) 進行中のジョブの詳細は、[ウェブ (Web) ] > [ユーティリティ (Utilities) ] > [Web アプライアンスへの公開 (Publish to Web Appliances) ] ページにも表示されます。[公開中 (Publish in Progress) ] にアクセスするには、[進捗ステータスの確認 (Check Progress) ] をクリックします。

---

### 次のタスク

公開が正しく完了したことを確認します。[公開履歴の表示 \(414 ページ\)](#) を参照してください。完全に公開されなかった項目が表示されます。

## Configuration Master を後日公開

### 始める前に

[Configuration Master を公開する前に \(408 ページ\)](#) の重要な要件と情報を参照してください。

---

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web) ] > [ユーティリティ (Utilities) ] > [Web アプライアンスへの公開 (Publish to Web Appliances) ] を選択します。

**ステップ 2** [ジョブをスケジュールする (Schedule a Job) ] をクリックします。

**ステップ 3** デフォルトでは [システム生成のジョブ名 (System-generated job name) ] が選択されています。あるいは、ユーザ定義のジョブ名 (80 文字以下) を入力します。

**ステップ 4** Configuration Master を公開する日時を入力します。

**ステップ 5** 公開する Configuration Master を選択します。

**ステップ 6** Configuration Master の公開先となる Web セキュリティ アプライアンスを選択します。Configuration Master に割り当てられているすべてのアプライアンスに設定を公開するには、[割り当てられたすべてのアプライアンス (All assigned appliances) ] を選択します。

または

[リスト内のアプライアンスを選択してください (Select appliances in list)] を選択して、Configuration Master に割り当てられているアプライアンスの一覧を表示します。設定の公開先となるアプライアンスを選択します。

**ステップ 7** [送信 (Submit)] をクリックします。

**ステップ 8** スケジュールされているジョブのリストは、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Webアプライアンスへの公開 (Publish to Web Appliances)] ページに表示されます。スケジュールされているジョブを編集するには、そのジョブの名前をクリックします。保留中のジョブをキャンセルするには、対応するごみ箱アイコンをクリックして、ジョブの削除を確認します。

**ステップ 9** スケジュールされた公開時刻の後に公開が正しく完了したことを確認するために、自分自身に対する覚え書きを (カレンダーなどに) 作成することもできます。

(注) スケジュールされた公開ジョブが発生する前に、アプライアンスをリブートまたはアップグレードした場合は、ジョブを再度スケジュールする必要があります。

#### 次のタスク

公開が正しく完了したことを確認します。[公開履歴の表示 \(414 ページ\)](#) を参照してください。完全に公開されなかった項目が表示されます。

## コマンドラインインターフェイスによる Configuration Master の公開



(注) [Configuration Master を公開する前に \(408 ページ\)](#) の重要な要件と情報を参照してください。

セキュリティ管理アプライアンスでは、次の CLI コマンドを使用して Configuration Master から変更を公開できます。

```
publishconfig config_master [--job_name] [--host_list | host_ip]
```

**config\_master** は、サポートされている Configuration Master のバージョンです。このキーワードは必須です。**job\_name** オプションは省略可能で、指定しなかった場合は生成されます。

オプション **host\_list** は、公開される Web セキュリティ アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は、Configuration Master に割り当てられているすべてのホストに公開されます。**host\_ip** オプションには、カンマで区切って複数のホスト IP アドレスを指定できます。

**publishconfig** コマンドが成功したことを確認するには、**smad\_logs** ファイルを調べます。[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Webアプライアンスステータス (Web Appliance Status)] を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [公開 (Publish)] > [公開履歴 (Publish History)] により、[公開履歴 (Publish History)] ページに進むことができます。

## 拡張ファイル公開による設定の公開

拡張ファイル公開を使用して、互換性のある XML コンフィギュレーションファイルを、ローカルファイルシステムから管理対象の Web セキュリティ アプライアンスにプッシュします。

拡張ファイル公開を使用して設定できる設定の詳細については、[適切な設定公開方式の決定 \(390 ページ\)](#) を参照してください。

拡張ファイル公開を実行するには、次を参照してください。

- [拡張ファイル公開 : \[今すぐ設定を公開する \(Publish Configuration Now\) \] \(412 ページ\)](#)
- [拡張ファイル公開 : \[後日公開 \(Publish Later\) \] \(413 ページ\)](#)

### 拡張ファイル公開 : [今すぐ設定を公開する (Publish Configuration Now) ]

#### 始める前に

- 公開するコンフィギュレーションバージョンが、公開先アプライアンスの AsyncOS バージョンと互換性があることを確認します。互換性マトリクス (<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>) を参照してください。
- 各宛先の Web セキュリティ アプライアンスで、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーションファイルにバックアップします。詳細については、『[AsyncOS for Cisco Web Security Appliances User Guide](#)』を参照してください。

---

**ステップ 1** 元となる Web セキュリティ アプライアンスから、コンフィギュレーションファイルを保存します。

Web セキュリティ アプライアンスからコンフィギュレーションファイルを保存する方法については、『[AsyncOS for Cisco Web Security Appliances User Guide](#)』を参照してください。

**ステップ 2** セキュリティ管理アプライアンスのウィンドウで、[ウェブ (Web) ]>[ユーティリティ (Utilities) ]>[Web アプライアンスへの公開 (Publish to Web Appliances) ]を選択します。

**ステップ 3** [今すぐ設定を公開する (Publish Configuration Now) ]をクリックします。

**ステップ 4** デフォルトでは [システム生成のジョブ名 (System-generated job name) ] が選択されています。あるいはジョブ名 (80 文字まで) を入力します。

**ステップ 5** [公開する設定マスター (Configuration Master to Publish) ] で、[拡張ファイルオプション (Advanced file options) ] を選択します。

**ステップ 6** [参照 (Browse) ] をクリックして、手順 1 で保存したファイルを選択します。

**ステップ 7** [Web アプライアンス (Web Appliances) ] ドロップダウンリストから、[リスト内のアプライアンスを選択してください (Select appliances in list) ] または [マスターに割り当てられたすべて (All assigned to Master) ] を選択して、コンフィギュレーションファイルの公開先となるアプライアンスを選択します。

**ステップ 8** [公開 (Publish) ] をクリックします。

---

## 拡張ファイル公開 : [後日公開 (Publish Later)]

### 始める前に

- 公開するコンフィギュレーションバージョンが、公開先アプライアンスの AsyncOS バージョンと互換性があることを確認します。互換性マトリクス (<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>) を参照してください。
- 各宛先の Web セキュリティ アプライアンスで、Web セキュリティ アプライアンスの既存の設定をコンフィギュレーション ファイルにバックアップします。詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

- 
- ステップ 1** 元となる Web セキュリティ アプライアンスから、コンフィギュレーション ファイルを保存します。Web セキュリティ アプライアンスからコンフィギュレーション ファイルを保存する方法については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。
- ステップ 2** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Web アプライアンスへの公開 (Publish to Web Appliances)] を選択します。
- ステップ 3** [ジョブをスケジュールする (Schedule a Job)] をクリックします。
- ステップ 4** デフォルトでは [システム生成のジョブ名 (System-generated job name)] が選択されています。あるいはジョブ名 (80 文字まで) を入力します。
- ステップ 5** 設定を公開する日時を入力します。
- ステップ 6** [公開する設定マスター (Configuration Master to Publish)] で、[拡張ファイル オプション (Advanced file options)] を選択し、次に [参照 (Browse)] をクリックして、手順 1 で保存したコンフィギュレーション ファイルを選択します。
- ステップ 7** [Web アプライアンス (Web Appliances)] ドロップダウン リストから、[リスト内のアプライアンスを選択してください (Select appliances in list)] または [マスターに割り当てられたすべて (All assigned to Master)] を選択して、コンフィギュレーション ファイルの公開先となるアプライアンスを選択します。
- ステップ 8** [公開 (Publish)] をクリックします。
- 

## 公開ジョブのステータスと履歴の表示

目的	操作手順
スケジュール済みで実行されていない公開ジョブのリスト	[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Web アプライアンスへの公開 (Publish to Web Appliances)] を選択し、[保留中のジョブ (Pending Jobs)] セクションを確認してください。

目的	操作手順
各アプライアンスで最後に公開された設定のリスト	[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Web アプライアンスステータス (Web Appliance Status)] を選択し、[最新公開設定 (Last Published Configuration)] の情報を参照してください。
現在進行中の公開ジョブのステータス	[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Web アプライアンスへの公開 (Publish to Web Appliances)] を選択し、[公開の進捗ステータス (Publishing Progress)] セクションを確認してください。
すべてまたは一部のアプライアンスに対するすべてまたは一部の公開ジョブの履歴	<a href="#">公開履歴の表示</a> を参照してください。

## 公開履歴の表示

公開履歴を表示すると、公開中に発生した可能性があるエラーをチェックしたり、設定されている機能とターゲットアプライアンスで有効になっている機能の不一致を特定したりするのに役立ちます。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [公開履歴 (Publish History)] を選択します。

**ステップ 2** 特定のジョブに関してさらに詳細を表示するには、[ジョブ名 (Job Name)] 列で特定のジョブ名をクリックします。

**ステップ 3** 詳細を確認します。

- ジョブの特定のアプライアンスに関するステータスの詳細を表示するには、[詳細 (Details)] リンクをクリックします。

[Webアプライアンス公開の詳細 (Web Appliance Publish Details)] ページが表示されます。

- ジョブの特定のアプライアンスに関する詳細を表示するには、アプライアンス名をクリックします。

[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Webアプライアンスステータス (Web Appliance Status)] ページが表示されます。

## 中央管理型アップグレード管理

単一のセキュリティ管理アプライアンス (SMA) を使用して、複数の Web セキュリティ アプライアンス (WSA) を同時にアップグレードすることができます。各 WSA に異なるソフトウェア アップグレードを適用することもできます。

- [Web セキュリティ アプライアンスのアップグレードの一元管理を設定 \(415 ページ\)](#)
- [WSA アップグレードの選択とダウンロード \(417 ページ\)](#)
- [インストール ウィザードの使用 \(418 ページ\)](#)

## Webセキュリティアプライアンスのアップグレードの一元管理を設定

このセキュリティ管理アプライアンスの一元化されたアップグレードサービスを構成するには、次の手順を実行します。

- [一元管理アップグレードマネージャの有効化 \(415 ページ\)](#)
- [管理対象の各 Web セキュリティ アプライアンスへの一元管理アップグレードサービスの追加 \(416 ページ\)](#)

### 一元管理アップグレード マネージャの有効化

#### 始める前に

- アップグレードの一元管理を有効にする前に、すべての Web セキュリティ アプライアンスが設定され、想定どおりに動作している必要があります。
- 一元管理アップグレードを受信する Web セキュリティ アプライアンスごとに、個別に一元管理アップグレードを有効にする必要があります。



(注) CLI での一元管理アップグレードを有効にするには、次を使用します。

```
applianceconfig > services > [...] > Enable Centralized Upgrade  
> Y
```

- 適切な機能キーがセキュリティ管理アプライアンスにインストールされていることを確認します。

**ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] ページを選択し、さらに、[集約管理サービス (Centralized Services)] > [一元管理アップグレードマネージャ (Centralized Upgrade Manager)] を選択します。

**ステップ 2** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 3** [有効 (Enable)] をオンにします。

**ステップ 4** 変更を送信し、保存します。

## 管理対象の各 Web セキュリティ アプライアンスへの一元管理アップグレード サービスの追加

セキュリティ管理アプライアンスで一元管理アップグレードマネージャを有効にした後、個々の管理対象 WSA で一元管理アップグレードを有効にして、アップグレードマネージャ名簿に必要な Web セキュリティ アプライアンスを追加する必要があります。

**ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] ページを選択し、その後、[集約管理サービス (Centralized Services)] > [セキュリティ アプライアンス (Security Appliances)] を選択します。

**ステップ 2** Web セキュリティ アプライアンスをまだ追加していない場合、またはアップグレードの一元管理のためアプライアンスを追加する必要がある場合：

- a) [Web アプライアンスの追加 (Add Web Appliance)] をクリックします。
- b) [アプライアンス名 (Appliance Name)] および [IP アドレス (IP Address)] テキスト フィールドに、Web セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

(注) [IP アドレス (IP Address)] テキスト フィールドに DNS 名を入力した場合でも、[送信 (Submit)] をクリックすると、IP アドレスに変換されます。

- c) [一元管理アップグレード (Centralized Upgrades)] を確認してください。
- d) [接続の確立 (Establish Connection)] をクリックします。
- e) 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立 (Establish Connection)] をクリックします。

(注) ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモートアプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は Security Management Appliance に保存されません。

「Success」メッセージがページのテーブルの上に表示されるまで待機します。

- f) [Test Connection] をクリックします。

テーブルの上のテスト結果を確認します。

- g) [送信 (Submit)] をクリックします。

同時にアップグレードの一元管理を有効にしながら、管理対象の Web セキュリティ アプライアンスのリストに追加する WSA ごとに、この手順を繰り返します。

**ステップ 3** この管理対象アプライアンスのリストに既存の WSA でアップグレードの一元管理を有効にするには、次の手順を実行します。

- a) Web セキュリティ アプライアンスの名前をクリックして、[Web セキュリティ アプライアンス設定の編集 (Edit Web Security Appliance Settings)] ページを開きます。
- b) [WSA 集約管理サービス (WSA Centralized Services)] セクションで、[一元管理アップグレード (Centralized Upgrades)] を選択します。
- c) [送信 (Submit)] をクリックします。



アップグレードの一元管理を有効にする WSA ごとに、この手順を繰り返します。

**ステップ 4** 変更を保存します。

#### 次のタスク

管理対象アプライアンスのリストへの追加方法およびリストの編集方法の詳細については、[管理対象アプライアンスの追加について \(19 ページ\)](#) を参照してください。

## WSA アップグレードの選択とダウンロード

- ステップ 1** セキュリティ管理アプライアンスで、[Web]ページを選択し、[ユーティリティ (Utilities)] > [一元管理アップグレード (Centralized Upgrade)] を選択します。
- アップグレード用に最近選択されたアプライアンスと、アップグレードステータスがリストされます。
- ステップ 2** [一元管理アップグレード (Centralized Upgrade)] ページで [アプライアンスのアップグレード (Upgrade Appliances)] ボタンをクリックします。
- アップグレードが可能なすべての管理対象 WSA がリストされます。
- ステップ 3** リストで名前のあるボックスをチェックして、アップグレードする各 Web セキュリティアプライアンスを選択します。
- ステップ 4** [ダウンロードウィザード (Download Wizard)] または [ダウンロードおよびインストールウィザード (Download and Install Wizard)] のいずれかをクリックします。
- ダウンロードウィザードでは、選択した WSA にダウンロードするアップグレードパッケージを選択できます。この操作はダウンロード専用です。後から、各システムにダウンロードしたパッケージをインストールし、再起動できます。
- ダウンロードおよびインストールウィザードでは、ダウンロードするアップグレードパッケージと選択した WSA への即時インストールを選択できます。インストール後、各システムは自動的に再起動されます。
- ステップ 5** 起動したウィザードの [アップグレードの取得 (Fetch Upgrades)] ページが表示されます。選択した WSA で利用可能なすべてのアップグレードが取得された場合は (WSA マトリックスの [ステータス (Status)] 列に「利用可能なアップグレードの取得が完了しました (Completed Fetching Available Upgrades)」と表示される)、[次へ (Next)] をクリックして続行します。
- ステップ 6** [利用可能なアップグレード (Available Upgrades)] ページでは、選択した WSA ごとに利用可能なアップグレードビルドがすべてリストされます。比較用に最大 5 つまでを選択し、[次へ (Next)] をクリックします。
- ステップ 7** ウィザードの [アップグレードの選択 (Upgrade Selection)] ページでは、WSA ごとに選択したアップグレードの互換性マトリックスが示されます。WSA ごとに目的のアップグレードビルドをチェックし、[次へ (Next)] をクリックします。
- ステップ 8** [サマリ (Summary)] ページに、選択した WSA とアップグレードビルドごとの概要情報がリストされます。[次へ (Next)] をクリックして、ウィザードを続行します。

**ステップ 9** WSA 接続ステータスなどの一連のダウンロードチェックに続き、[レビュー (Review)] ページで各 WSA のダウンロードステータスのリストが提供されます。[ダウンロードの開始 (Begin Download)] をクリックして、選択した各 WSA へアップグレードパッケージをダウンロードします。

[一元管理アップグレード (Centralized Upgrade)] ページには、プロセス全体を通じてダウンロードステータス情報が表示されます。

### 次のタスク

- [ダウンロードウィザード (Download Wizard)] - この手順の初めにこのボタンをクリックした場合は、ダウンロードの完了時に、[Web] > [ユーティリティ (Utilities)] > [一元管理アップグレード (Centralized Upgrade)] を選択するか、またはブラウザウィンドウのページ更新ボタンをクリックすることで、[一元管理アップグレード (Centralized Upgrade)] ページを更新します。

アップグレード可能なすべての管理対象 WSA のリストに加え、[一元管理アップグレード (Centralized Upgrade)] ページの別のセクションではアップグレードパッケージがダウンロードされているすべての WSA がリストされます (エントリごとに表示されているゴミ箱ボタンをクリックすると、その WSA からダウンロードされたアップグレードパッケージを削除できます)。

いつでも、このリストで 1 つまたは複数の WSA を選択し、その後、[インストールウィザード (Install Wizard)] をクリックして、ダウンロードされたアップグレードパッケージの選択した各 WSA へのインストールを開始できます。WSA でインストールが完了すると、それが再起動されます。このウィザードの使用の詳細については [インストールウィザードの使用 \(418 ページ\)](#) を参照してください。

- [ダウンロードおよびインストールウィザード (Download and Install Wizard)] - この手順の初めにこのボタンをクリックした場合は、ダウンロードの完了時に、アップグレードのインストールが自動的に始まります。このプロセスの詳細については、[インストールウィザードの使用 \(418 ページ\)](#) のステップ 2 以降を参照してください。インストールが完了すると、WSA が再起動します。

## インストールウィザードの使用

ダウンロードおよびインストールプロセスの一部として自動的に行うかどうかに関係なくインストールウィザードを開始する場合、またはアップグレードパッケージがダウンロードされたが、まだインストールされていない 1 つ以上の WSA を選択後 [一元管理アップグレード (Centralized Upgrade)] ページで [インストールウィザード (Install Wizard)] ボタンをクリックした場合は、次の手順に従ってインストールを設定します。

**ステップ 1** 以前にダウンロードしたアップグレードパッケージをインストールする場合：

- a) [一元管理アップグレード (Centralized Upgrade)] ページの [ダウンロードした AsyncOS バージョンの Web アプライアンス (Web Appliances with Downloaded AsyncOS Versions)] セクションで目的の WSA

を選択します ([Web] > [ユーティリティ (Utilities)] > [一元管理アップグレード (Centralized Upgrade)] )。

b) [インストール ウィザード (Install Wizard)] をクリックします。

**ステップ 2** ウィザードの [アップグレードの準備 (Upgrade Preparation)] ページで、選択した WSA ごとに次を実行します。

- WSA の現在の設定のバックアップ コピーをそのシステムの `configuration` ディレクトリに保存する場合は、[アップグレードする前に現在の設定を `configuration` ディレクトリに保存する (Save the current configuration to the configuration directory before upgrading)] をオンにします。
- [現在の設定を保存 (Save current configuration)] オプションがオンになっている場合、[設定ファイル内のパスワードを隠す (Mask passphrases in the configuration file)] をオンにしてバックアップ コピー内の現在のすべての構成パスフレーズをマスクすることができます。[設定のロード (Load Configuration)] コマンドは、マスク付きパスフレーズを使用したバックアップファイルの再ロードには使用できない点に注意してください。
- [現在の設定を保存 (Save current configuration)] オプションがオンになっている場合、[ファイルをメールで送信 (Email file to)] フィールドに 1 つ以上の電子メール アドレスを入力できます。入力した各アドレスに、バックアップ設定ファイルのコピーが電子メールで送信されます。カンマで複数のアドレスを区切ります。

**ステップ 3** [Next] をクリックします。

**ステップ 4** [アップグレードの概要 (Upgrade Summary)] ページには、選択した各 WSA のアップグレードの準備情報がリストされます。[次へ (Next)] をクリックして、ウィザードを続行します。

**ステップ 5** 接続ステータスなどの一連のデバイス チェックに続き、[レビュー (Review)] ページで各 WSA のインストールステータスのリストが提供されます。エラーが表示されているデバイスを選択解除できます。[インストールの開始 (Begin Install)] をクリックして、選択した各 WSA へのアップグレードパッケージのインストールを開始します。

インストール ステータス情報が表示された [一元管理アップグレード (Centralized Upgrade)] ページに戻ります。

(注) 各 WSA は、インストールの完了時に再起動されます。

---

### 次のタスク



- (注) また、WSA 自体から以前にダウンロードしたパッケージのインストーラを実行することもできます。つまり、ダウンロードされたアップグレードパッケージは、WSA 上の [システム管理 (System Administration)] > [システムアップグレード (System Upgrade)] ページに [インストール (Install)] ボタンとともにリストされます。詳細については、『Cisco Web Security Appliances ユーザガイド』の AsyncOS とセキュリティ サービス コンポーネントのアップグレードおよび更新に関する説明を参照してください。
-

## Web セキュリティ アプライアンスのステータスの表示

- [イネーブルにされている機能の比較 \(404 ページ\)](#)
- [Web アプライアンス ステータスの概要の表示 \(420 ページ\)](#)
- [個々の Web セキュリティ アプライアンスのステータスの表示 \(420 ページ\)](#)
- [Web アプライアンス ステータスの詳細 \(421 ページ\)](#)

### Web アプライアンス ステータスの概要の表示

[ウェブ (Web) ] > [ユーティリティ (Utilities) ] > [Web アプライアンス ステータス (Web Appliance Status) ] ページは、セキュリティ管理アプライアンスに接続されている Web セキュリティ アプライアンスの概要を提供します。

[Web アプライアンス ステータス (Web Appliance Status) ] ページには、接続されている Web セキュリティ アプライアンスのリストが、アプライアンス名、IP アドレス、AsyncOS バージョン、最後に公開された設定情報 (ユーザ、ジョブ名、コンフィギュレーションバージョン)、使用可能または使用不可にされているセキュリティサービスの数、および接続しているアプライアンスの総数 (最大 150) とともに表示されます。警告アイコンは、接続されたアプライアンスの 1 つに注意が必要なことを示しています。

### 個々の Web セキュリティ アプライアンスのステータスの表示

[アプライアンスステータス (Appliance Status) ] ページには、接続されている各アプライアンスの状態が詳細に表示されます。

[Web アプライアンスステータス (Web Appliance Status) ] ページで管理対象 Web セキュリティ アプライアンスの詳細を表示するには、アプライアンスの名前をクリックします。

ステータス情報としては、接続されている Web セキュリティ アプライアンスに関する一般情報、それらの公開された設定、公開履歴、機能キーのステータスなどがあります。



---

(注) 表示可能なデータがあるのは、集中管理をサポートするマシンのみです。

---



---

(注) Web セキュリティアプライアンスの Acceptable Use Control Engine の各種バージョンが、セキュリティ管理アプライアンスのバージョンと一致しない場合は、警告メッセージが表示されます。そのサービスが Web セキュリティアプライアンスで無効になっているか、そこに存在しない場合は、[なし (N/A) ] と表示されます。

---

## Web アプライアンス ステータスの詳細

このページの情報のほとんどは、Web セキュリティ アプライアンスから取得されます。

- セキュリティステータス情報（稼働時間、アプライアンスモデル、シリアル番号、AsyncOS のバージョン、ビルド日、AsyncOS のインストール日時、ホスト名）
- 設定公開履歴（公開日時、ジョブ名、コンフィギュレーションバージョン、公開の結果、ユーザ）
- 直近に試行されたデータ転送の時刻など、中央集中型レポートイングのステータス
- Web セキュリティ アプライアンスの各機能のステータス（各機能が有効になっているかどうか、機能キーのステータス）
- 管理対象および管理側のアプライアンスの Acceptable Use Controls Engine のバージョン
- Web セキュリティ アプライアンスの AnyConnect セキュア モビリティ設定
- この Web セキュリティ アプライアンスが接続された Cisco Identity Services Engine (ISE) サーバ
- Web セキュリティ アプライアンスのプロキシ設定（アップストリーム プロキシとプロキシの HTTP ポート）
- 認証サービス情報（サーバ、スキーム、レルム、シーケンス、トランスペアレントユーザ ID のサポートの有無、認証に失敗した場合のトラフィックのブロックまたは許可）



### ヒント

Web セキュリティ アプライアンスで発生した最新の設定変更が [Web アプライアンス ステータス (Web Appliance Status)] ページに反映されるまでに、数分かかることがあります。データをすぐに更新するには、[データの更新 (Refresh Data)] リンクをクリックします。ページのタイムスタンプは、データが最後にリフレッシュされた時刻を示しています。

## URL カテゴリ セットの更新の準備および管理

システムで Web の使用率を管理するために事前定義されている URL カテゴリを最新の状態に維持するためには、Web Usage Controls (WUC) の URL カテゴリ セットを時折更新します。デフォルトでは、Web セキュリティ アプライアンスが URL カテゴリ セットの更新を Cisco から自動的にダウンロードし、セキュリティ管理アプライアンスがこれらの更新を管理対象の Web セキュリティ アプライアンスから数分以内に自動的に受信します。

これらの更新は既存の設定およびアプライアンスの動作に影響を与える可能性があるため、事前に準備して更新後に対処する必要があります。

以下のことを実施してください。

- [URL カテゴリ セットの更新による影響の理解](#) (422 ページ)
- [URL カテゴリ セットの更新に関する通知およびアラートの受信](#) (422 ページ)
- [新規または変更されたカテゴリのデフォルト設定の指定](#) (422 ページ)
- [URL カテゴリ セットの更新時にポリシーと ID/識別プロファイルの設定を確認](#) (422 ページ)

## URL カテゴリ セットの更新による影響の理解

URL カテゴリ セットが更新されると、Configuration Master の既存のポリシーの動作が変化する可能性があります。

URL カテゴリ セットの更新前後に必要な処理の重要情報については、[資料 \(655 ページ\)](#)に掲載されているリンクで、『AsyncOS for Cisco Web Security Appliances User Guide』の「URL Filters」の章の「Managing Updates to the Set of URL Categories」セクションを参照してください。カテゴリについては、同じ章の「URL Category Descriptions」で説明されています。

## URL カテゴリ セットの更新に関する通知およびアラートの受信

受信対象	操作手順
URL カテゴリ セットの更新の事前通知	Cisco コンテンツ セキュリティ アプライアンスに関する通知 (URL カテゴリ セットの更新に関する通知を含む) を受け取るには今すぐサインアップしてください。 <a href="#">Cisco Notification Service (655 ページ)</a> を参照してください。
URL カテゴリ セットの更新が既存のポリシー設定に影響する場合のアラート	[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アラート (Alerts)] に移動し、[システム (System)] カテゴリで警告レベルのアラートを受信するように設定されていることを確認します。アラートについての詳細は、 <a href="#">アラートの管理 (541 ページ)</a> を参照してください。

## 新規または変更されたカテゴリのデフォルト設定の指定

URL カテゴリ セットを更新する前に、URL フィルタリングを行うポリシーの新規カテゴリやマージされたカテゴリにデフォルトの動作を指定するか、これらがすでに設定されている Web セキュリティ アプライアンスから設定をインポートする必要があります。

詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「URL Filters」の章の「Choosing Default Settings for New and Changed Categories」セクションまたは Web セキュリティ アプライアンスのオンラインヘルプを参照してください。

## URL カテゴリ セットの更新時にポリシーと ID/識別プロファイルの設定を確認

URL カテゴリ セットの更新によって、次の 2 種類のアラートがトリガーされます。

- カテゴリの変更についてのアラート
- カテゴリの変更によって変更された、またはディセーブルにされたポリシーについてのアラート

URL カテゴリ セットの変更に関するアラートを受信した場合は、既存の URL カテゴリに基づくポリシーと ID/識別プロファイルが引き続きポリシーの目的を満たしていることを確認してください。

注意が必要な変更の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Responding to Alerts about URL Category Set Updates」を参照してください。

## Application Visibility and Control (AVC) の更新

SMA は管理対象の Web セキュリティ アプライアンスの多くに存在する AVC エンジンのバージョンを自動的に使用します。

### コンフィギュレーション管理上の問題のトラブルシューティング

- [設定マスター (Configuration Master)] > [ID (Identities)]/[識別プロファイル (Identification Profiles)] に [グループ (Groups)] が表示されない (423 ページ)
- [設定マスター (Configuration Master)] > [アクセス ポリシー (Access Policies)] > [Web レピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings)] ページの設定が想定とは異なる (424 ページ)
- 設定公開失敗のトラブルシューティング (424 ページ)

### [設定マスター (Configuration Master)] > [ID (Identities)]/[識別プロファイル (Identification Profiles)] に [グループ (Groups)] が表示されない

#### 問題

[ウェブ (Web)] > [設定マスター (Configuration Master)] > [ID (Identities)]/[識別プロファイル (Identification Profiles)] のポリシー メンバーシップの定義ページで、[選択されたグループとユーザ (Selected groups and Users)] に [グループ (Groups)] オプションが表示されません。

#### ソリューション

複数の Web セキュリティ アプライアンスがある場合、[ネットワーク (Network)] > [認証 (Authentication)] の各 WSA で、同じ名前のレルムに対してすべての設定が同一でない限り、すべての WSA でレルム名が一意であることを確認します。



#### ヒント

各 WSA についてレルム名を確認するには、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Web アプライアンス ステータス (Web Appliance Status)] に移動して、各アプライアンス名をクリックし、詳細ページの下部までスクロールします。

[設定マスター (Configuration Master)] > [アクセス ポリシー (Access Policies)] > [Web レピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings)] ページの設定が想定とは異なる

## [設定マスター (Configuration Master)] > [アクセス ポリシー (Access Policies)] > [Web レピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings)] ページの設定が想定とは異なる

### 問題

Configuration Master の [アクセス ポリシー (Access Policies)] > [Web レピュテーションとマルウェア対策の設定 (Web Reputation and Anti-Malware Settings)] ページに、Web レピュテーション スコアのしきい値設定やマルウェア対策 スキャン エンジンを選択する機能など、想定される設定が表示されません。または、Web セキュリティ アプライアンスで 適応型セキュリティ を使用している場合にこれらの設定が含まれます。

### ソリューション

使用可能なオプションは、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [セキュリティ サービス表示 (Security Services Display)] で、Adaptive Security がその Configuration Master に対して選択されているかどうかによって異なります。

## 設定公開失敗のトラブルシューティング

### 問題

設定を公開できません。

### ソリューション

[ウェブ (Web)] > [ユーティリティ (Utilities)] > [Web アプライアンスステータス (Web Appliance Status)] ページを確認します。公開が失敗する理由は次のとおりです。

- [Webアプライアンスサービス (Web Appliance Service)] 列のステータスと、[管理アプライアンス上でサービスを表示しますか? (Is Service Displayed on Management Appliance?)] 列のステータスとの間に不一致があります。
- 両方の列で、機能が有効になっているものの、対応する機能キーがアクティブになっていません (期限切れなど)。
- Configuration Master のバージョンが、Web セキュリティ アプライアンスの AsyncOS のバージョンと一致している必要があります。古いバージョンの Configuration Master から新しいバージョンの Web セキュリティ アプライアンスに対して公開を行うと、Web セキュリティ アプライアンスの設定が Configuration Master の設定と一致していない場合には、処理に失敗するおそれがあります。この問題は、[Webアプライアンスステータス (Web Appliance Status Details)] ページに不一致が見られない場合でも発生することがあります。

### 次の作業

- [公開履歴の表示 \(414 ページ\)](#)
- [イネーブルにされている機能の比較 \(404 ページ\)](#)
- [公開する機能の有効化 \(405 ページ\)](#)





## 第 11 章

# システムステータスのモニタリング

この章は、次の項で構成されています。

- [セキュリティ管理アプライアンスのステータスについて \(425 ページ\)](#)
- [セキュリティ管理アプライアンス 容量のモニタリング \(426 ページ\)](#)
- [管理アプライアンスからのデータ転送のステータスのモニタリング \(427 ページ\)](#)
- [管理対象アプライアンスの設定ステータスの表示 \(429 ページ\)](#)
- [レポートングデータ アベイラビリティ ステータスのモニタリング \(430 ページ\)](#)
- [電子メールトラッキングデータ ステータスのモニタリング \(431 ページ\)](#)
- [管理対象アプライアンスのキャパシティのモニタリング \(431 ページ\)](#)
- [アクティブな TCP/IP サービスの識別 \(432 ページ\)](#)
- [ハードウェア障害発生時の管理対象アプライアンスの交換 \(432 ページ\)](#)

## セキュリティ管理アプライアンスのステータスについて

デフォルトでは、[システムステータス (System Status)] ページはブラウザから Cisco コンテンツセキュリティ管理アプライアンスにアクセスするときに最初に表示されるページです。  
(ランディングページを変更するには、[プリファレンスの設定 \(582 ページ\)](#) を参照してください)

それ以外の場合に [システムステータス (System Status)] ページにアクセスするには、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [システムステータス (System Status)] を選択します。

サービスのモニタリングをイネーブルにして、管理対象アプライアンスを追加するまでは、[システム情報 (System Information)] セクションでのみステータス情報が提供されます。システムセットアップウィザードを実行し、集約管理サービスを有効にして、管理対象アプライアンスを追加すると、[集約管理サービス (Centralized Services)] セクションおよび [セキュリティアプライアンスデータ転送ステータス (Security Appliance Data Transfer Status)] セクションにデータが表示されます。

ステータス情報には、次の内容が含まれます。

- 集約管理サービス：処理キューの使用状況などの各集約管理サービスの状態
- システム稼働時間：アプライアンスが動作している時間の長さ

- CPU 使用率：各モニタリング サービスによって使用されている CPU 容量
- システムバージョン情報：モデル番号、AsyncOS（オペレーティングシステム）バージョン、ビルド日、インストール日、およびシリアル番号

#### 関連項目

- [キューの処理のモニタリング](#)（426 ページ）
- [CPU 使用率のモニタリング](#)（427 ページ）
- [管理アプライアンスからのデータ転送のステータスのモニタリング](#)（427 ページ）

## セキュリティ管理アプライアンス 容量のモニタリング

- [キューの処理のモニタリング](#)（426 ページ）
- [CPU 使用率のモニタリング](#)（427 ページ）

### キューの処理のモニタリング

電子メールと Web レポート、およびアプライアンスが最適な容量で実行されているかを判断するためのトラッキングレポートに使用される処理キューの使用率を定期的に確認できます。

処理キューには、セキュリティ管理アプライアンスによる処理を待機している集中型レポートングファイルおよびトラッキングファイルが保存されます。通常、セキュリティ管理アプライアンスは、処理対象のレポートングファイルとトラッキングファイルのバッチを受信します。処理キューのレポートングファイルまたはトラッキングファイルの割合は、通常、ファイルが管理アプライアンスから転送され、セキュリティ管理アプライアンスで処理されると変動します。



- (注) 処理キューの割合は、キューにあるファイルの数で測定されます。ファイルサイズは考慮されません。割合は、セキュリティ管理アプライアンスの処理負荷の概算のみを示します。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [システムステータス (System Status)] を選択します。
- ステップ 3** ページ上部の [集約管理サービス (Centralized Services)] セクションで、次に対する処理キューの割合を参照してください。
- [集約管理レポート (Centralized Reporting)] ([Eメールセキュリティ (Email Security)] サブセクション)
  - 集約メッセージトラッキング (Centralized Message Tracking)
  - [集約管理レポート (Centralized Reporting)] ([Webセキュリティ (Web Security)] サブセクション)

**ステップ 4** 処理キューの使用率が数時間または数日にわたって高いままである場合は、システムが容量以上に稼働しています。

この場合、管理対象アプライアンスの一部をセキュリティ管理アプライアンスから移動する、追加のセキュリティ管理アプライアンスをインストールする、またはその両方を検討してください。

## CPU 使用率のモニタリング

各集約管理サービスでセキュリティ管理アプライアンスが使用している CPU 容量の割合を表示するには、次の手順に従ってください。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [システムステータス (System Status)] を選択します。

**ステップ 3** [システム情報 (System Information)] セクションまでスクロールし、[CPU 使用率 (CPU Utilization)] サブセクションを表示します。

[CPU 使用率 (CPU Utilization)] の割合は、主要な集約管理サービスのそれぞれに使われるセキュリティ管理アプライアンスの CPU 処理の割合を示します。いくつかのサービスの使用率の割合は統合されている可能性があります。たとえば、電子メールレポーティングは、[レポートサービス (Reporting Service)] 下で統合され、スパム、ポリシー、ウイルス、およびアウトブレイク隔離は [隔離サービス (Quarantine Services)] 下で統合されます。セキュリティ管理アプライアンスのその他の動作は、汎用見出し [セキュリティ管理アプライアンス (Security Management Appliance)] 以下にまとめられます。

**ステップ 4** 最新のデータを表示するには、ブラウザを更新します。

CPU 使用率の割合は、常に変化します。

## 管理アプライアンスからのデータ転送のステータスのモニタリング

集中管理機能を実行するうえで、セキュリティ管理アプライアンスは、管理対象アプライアンスからセキュリティ管理アプライアンスにデータが正常に転送されることを前提としています。[セキュリティアプライアンスデータ転送ステータス (Security Appliance Data Transfer Status)] セクションでは、セキュリティ管理アプライアンスに管理される各アプライアンスのステータス情報が表示されます。

デフォルトで、[セキュリティアプライアンスデータ転送ステータス (Security Appliance Data Transfer Status)] セクションには最大 10 台のアプライアンスが表示されます。セキュリティ管

理アプライアンスが 10 台を超えるアプライアンスを管理する場合、[表示された項目 (Items Displayed) ] メニューを使用して表示するアプライアンスの数を選択できます。



(注) [システムステータス (System Status) ] ページの [サービス (Services) ] セクションに、データ転送ステータスの概要情報が表示されます。[セキュリティアプライアンスデータ転送ステータス (Security Appliance Data Transfer Status) ] セクションには、アプライアンス固有のデータ転送ステータスが表示されます。

[システムステータス (System Status) ] ページの [セキュリティアプライアンスデータ転送ステータス (Security Appliance Data Transfer Status) ] セクションで、特定のアプライアンスの接続ステータスの問題を表示できます。アプライアンスの各サービスのステータスに関する詳細情報については、アプライアンス名をクリックしてアプライアンスの [データ転送ステータス (Data Transfer Status) ] ページを表示します。

[データ転送ステータス : *Appliance Name* (Data Transfer Status: *Appliance Name*) ] ページには、各モニタリング サービスで最後にデータ転送が発生した時刻が表示されます。

E メールセキュリティアプライアンスのデータ転送ステータスは、次のいずれかの値になります。

- [有効化されていない (Not enabled) ] : モニタリング サービスが E メールセキュリティアプライアンスで有効になっていません。
- [接続されていません (Never connected) ] : モニタリング サービスは E メールセキュリティアプライアンスで有効ですが、E メールセキュリティアプライアンスとセキュリティ管理アプライアンスの接続が確立されていません。
- [データ待機中 (Waiting for data) ] : E メールセキュリティアプライアンスは、セキュリティ管理アプライアンスに接続して、データの受信を待機しています。
- [接続し、データ転送されました (Connected and transferred data) ] : E メールセキュリティアプライアンスとセキュリティ管理アプライアンス間の接続が確立され、データが正常に転送されました。
- [ファイル転送失敗 (File transfer failure) ] : E メールセキュリティアプライアンスとセキュリティ管理アプライアンス間の接続が確立されましたが、データ転送は失敗しました。

Webセキュリティアプライアンスのデータ転送ステータスは、次のいずれかの値になります。

- [有効化されていない (Not enabled) ] : 中央集中型設定マネージャは、Webセキュリティアプライアンスで有効になっていません。
- [接続されていません (Never connected) ] : 中央集中型設定マネージャは、Webセキュリティアプライアンスで有効ですが、Webセキュリティアプライアンスとセキュリティ管理アプライアンスの接続が確立されていません。
- [データ待機中 (Waiting for data) ] : Webセキュリティアプライアンスは、セキュリティ管理アプライアンスに接続して、データの受信を待機しています。

- [接続し、データ転送されました (Connected and transferred data)] : Web セキュリティアプライアンスとセキュリティ管理アプライアンス間の接続が確立され、データが正常に転送されました。
- [設定転送失敗 (Configuration push failure)] : セキュリティ管理アプライアンスは設定ファイルを Web セキュリティアプライアンスにプッシュしようとしたましたが、転送に失敗しました。
- [設定転送保留 (Configuration push pending)] : セキュリティ管理アプライアンスは設定ファイルの Web セキュリティアプライアンスへのプッシュを実行中です。
- [設定転送成功 (Configuration push success)] : セキュリティ管理アプライアンスは設定ファイルを Web セキュリティアプライアンスに正常にプッシュしました。

データ転送の問題は、一時的なネットワークの問題またはアプライアンスの設定の問題を反映していることがあります。ステータス [接続されていません (Never connected)] および [データ待機中 (Waiting for data)] は、最初に管理対象アプライアンスをセキュリティ管理アプライアンスに追加したときの、通常の移行ステータスです。ステータスが最終的に [接続し、データ転送されました (Connected and transferred data)] に変化しなかった場合、このデータ転送ステータスは、設定の問題を示している可能性があります。

アプライアンスに [ファイル転送失敗 (File transfer failure)] ステータスが表示された場合は、そのアプライアンスをモニタして、その失敗がネットワークの問題によるものなのか、アプライアンスの設定の問題によるものなのかを判断します。データを転送できない理由がネットワークの問題ではなく、ステータスが [接続し、データ転送されました (Connected and transferred data)] に変化しない場合、データ転送ができるようにアプライアンスの設定を変更する必要があります。

## 管理対象アプライアンスの設定ステータスの表示

セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。

[集約管理サービスのステータス (Centralized Service Status)] セクションに、有効化されているサービスと、サービスごとに使用中のライセンス数が表示されます。[セキュリティアプライアンス (Security Appliances)] セクションには、追加したアプライアンスがリスト表示されます。チェックマークは有効になっているサービスを示し、[接続が確立されていますか? (Connection Established?)] 列は、ファイル転送アクセスが正しく設定されているかどうかを示します。

### 関連項目

- リリースされたメッセージを処理する代替アプライアンスの指定 (365 ページ)
- 管理対象アプライアンスの追加について (19 ページ)

## Web セキュリティ アプライアンスの追加ステータス情報

Web セキュリティ アプライアンスの追加ステータス情報については、個々の [Web セキュリティ アプライアンスのステータスの表示](#) (420 ページ) を参照してください。

## レポーティング データ アベイラビリティ ステータスのモニタリング

セキュリティ管理アプライアンスによって、指定した期間のレポーティングデータのアベイラビリティをモニタできるようになります。アプライアンスに応じたセクションを参照してください。

- [電子メールセキュリティ レポート データのアベイラビリティのモニタリング](#) (430 ページ)

## 電子メールセキュリティ レポート データのアベイラビリティのモニタリング

セキュリティ管理アプライアンスの E メールセキュリティ アプライアンスからレポート データをモニタするには、[電子メール (Email)] > [レポート (Reporting)] > [有効なレポート データ (Reporting Data Availability)] ページを表示します。

[有効なレポート データ (Reporting Data Availability)] ページから、指定された期間にセキュリティ管理アプライアンスが E メールセキュリティ アプライアンスから受信したレポート データの割合を表示できます。棒グラフは、時間範囲内に受信したデータの完全性を示します。

レポーティングデータアベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが E メールセキュリティ アプライアンスから受信したレポート データが 100% 未満の場合は、データが不完全なことがすぐにわかります。データアベイラビリティ情報を使用して、レポーティングデータの検証およびシステムの問題のトラブルシューティングができます。

## Web セキュリティ レポート データのアベイラビリティのモニタリング

セキュリティ管理アプライアンスで Web セキュリティ アプライアンスからのレポーティング データをモニタするには、[ウェブ (Web)] > [レポート (Reporting)] > [使用可能なデータ (Data Availability)] ページを表示します。

[使用可能なデータ (Data Availability)] ページからデータの更新およびソートができ、リソース使用率および Web トラフィックの問題箇所をリアルタイムに表示できます。



- (注) [有効なWebレポートデータ (Web Reporting Data Availability)] ウィンドウでは、Web Reporting と Email Reporting の両方がディセーブルの場合にのみ、Web Reporting がディセーブルであると表示されます。

このページから、すべてのデータ リソース使用率および Web トラフィックの問題箇所を表示できます。リスト表示されている Web Security Appliance リンクのいずれかをクリックすると、そのアプライアンスのレポートングデータ アベイラビリティを表示できます。

レポートングデータアベイラビリティは、前の日、週、年についてモニタできます。セキュリティ管理アプライアンスが Web セキュリティ アプライアンスから受信したレポートングデータが 100% 未満の場合は、データが不完全なことがすぐにわかります。データアベイラビリティ情報を使用して、レポートングデータの検証およびシステムの問題のトラブルシューティングができます。

URL カテゴリに関するスケジュール設定されたレポートでデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「この時間範囲の一部のデータは使用不可でした。(Some data in this time range was unavailable.)」というメッセージが表示されます。ギャップが存在しない場合は何も表示されません。

Web セキュリティ アプライアンスの [使用可能なデータ (Data Availability)] ページの詳細については、[\[使用可能なデータ \(Data Availability\)\] ページ \(235 ページ\)](#) を参照してください。

## 電子メールトラッキングデータステータスのモニタリング

電子メールトラッキングデータのステータスをモニタするには、[メール (Email)] > [メッセージトラッキング (Message Tracking)] > [有効なメッセージトラッキングデータ (Message Tracking Data Availability)] ページを表示します。

## 管理対象アプライアンスのキャパシティのモニタリング

セキュリティ管理アプライアンスから管理対象アプライアンスの容量をモニタできます。すべての電子メールまたは Web Security Appliance の総合的な容量および個別のアプライアンスの容量を確認できます。

次のキャパシティを表示	参照先
管理対象 Web セキュリティ アプライアンス	<a href="#">[システム容量 (System Capacity)] ページ (233 ページ)</a>
管理対象Eメールセキュリティアプライアンス	<a href="#">[システム容量 (System Capacity)] ページ (109 ページ)</a>

## アクティブな TCP/IP サービスの識別

セキュリティ管理アプライアンスで使用されるアクティブな TCP/IP サービスを識別するには、コマンドラインインターフェイスで `tcp services` コマンドを使用します。

## ハードウェア障害発生時の管理対象アプライアンスの交換

ハードウェア障害または他の理由で管理対象アプライアンスの交換が必要になった場合、置き換えられたアプライアンスからのデータは失われませんが、そのデータはセキュリティ管理アプライアンスで正常に表示されません。

管理対象アプライアンスを交換する際に、SMA の上のホストのリストに新しいアプライアンスを追加し、新しいアプライアンスに接続します。IP アドレスに変更がない場合は、古いホストエントリの IP を存在しない値に変更します。





## 第 12 章

# LDAP との統合

この章は、次の項で構成されています。

- [概要 \(433 ページ\)](#)
- [スパム隔離と連携させるための LDAP の設定 \(434 ページ\)](#)
- [LDAP サーバ プロファイルの作成 \(434 ページ\)](#)
- [LDAP クエリの設定 \(436 ページ\)](#)
- [ドメインベース クエリ \(441 ページ\)](#)
- [チェーンクエリ \(443 ページ\)](#)
- [AsyncOS を複数の LDAP サーバと連携させるための設定 \(445 ページ\)](#)
- [LDAP を使用した管理ユーザの外部認証の設定 \(448 ページ\)](#)

## 概要

企業の LDAP ディレクトリ（例：Microsoft Active Directory、SunONE Directory Server、OpenLDAP ディレクトリなど）のエンドユーザのパスワードおよび電子メールエイリアスを管理する場合、LDAP ディレクトリを使用して次のユーザを認証することができます。

- スпам隔離にアクセスするエンドユーザおよび管理ユーザ。

ユーザがスパム隔離の Web UI にログインする場合、LDAP サーバはログイン名とパスワードを検証し、AsyncOS は対応する電子メールエイリアスのリストを取得します。そのユーザの電子メールエイリアスのいずれかに送信された隔離メッセージは、アプライアンスが書き換えられない限りスパム隔離で表示できます。

[スパム隔離と連携させるための LDAP の設定 \(434 ページ\)](#) を参照してください。

- 外部認証が有効で、設定されている場合に、Cisco コンテンツセキュリティ管理アプライアンスにサインインする管理ユーザ。

「[LDAP を使用した管理ユーザの外部認証の設定 \(448 ページ\)](#)」を参照してください。

## スパム隔離と連携させるための LDAP の設定

Cisco コンテンツセキュリティアプライアンスを LDAP ディレクトリと連携させるには、以下の手順に従って、受け入れ、ルーティング、エイリアシング、およびマスカレードを設定する必要があります。

### ステップ 1 LDAP サーバプロファイルを設定します。

サーバプロファイルの内容は、AsyncOS から LDAP サーバに接続するための、次のような情報です。

- サーバ名およびポート
- ベース DN (Base DN)
- サーバをバインディングするための認証要件

サーバプロファイルの設定方法の詳細については、[LDAP サーバプロファイルの作成 \(434 ページ\)](#) を参照してください。

LDAP サーバプロファイルを作成するときに、AsyncOS からの接続先となる LDAP サーバを複数設定できます。詳細については、[AsyncOS を複数の LDAP サーバと連携させるための設定 \(445 ページ\)](#) を参照してください。

### ステップ 2 LDAP クエリを設定します。

LDAP サーバプロファイル用に生成されたデフォルトのスパム隔離クエリを使用するか、または実際に使用する LDAP の実装とスキーマに合わせて自分のクエリを作成することができます。次に、スパム通知、および隔離へのエンドユーザアクセス検証に使用するアクティブクエリを指定します。

クエリの詳細については、[LDAP クエリの設定 \(436 ページ\)](#) を参照してください。

### ステップ 3 スпам隔離に対して、LDAP エンドユーザアクセスおよびスパム通知を有効にします。

スパム隔離への LDAP エンドユーザアクセスを有効にして、エンドユーザが隔離内のメッセージを表示および管理できるようにします。ユーザが複数の通知を受信しないように、スパム通知のエイリアス統合をイネーブルにすることもできます。

詳細については、[中央集中型スパム隔離の設定 \(320 ページ\)](#) を参照してください。

## LDAP サーバプロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定するには、LDAP サーバに関する情報を格納する LDAP サーバプロファイルを作成します。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [LDAP] を選択します。
- ステップ 3** [LDAPサーバプロファイルを追加 (Add LDAP Server Profile)] をクリックします。
- ステップ 4** [LDAPサーバプロファイル名 (LDAP Server Profile Name)] テキスト フィールドにサーバ プロファイルの名前を入力します。
- ステップ 5** [ホスト名 (Host Name(s))] テキスト フィールドに、LDAP サーバのホスト名を入力します。
- 複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロード バランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、[AsyncOS を複数の LDAP サーバと連携させるための設定 \(445 ページ\)](#) を参照してください。
- ステップ 6** 認証方法を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。
- (注) レポート上のクライアント IP アドレスではなくクライアントユーザ ID を表示するには、LDAP 認証を設定する必要があります。LDAP 認証を使用しない場合、システムでは IP アドレスによるユーザの参照のみができます。[パスワードを使用 (Use Passphrase)] オプション ボタンを選択して、ユーザ名とパスワードを入力します。[ユーザメール概要 (User Mail Summary)] ページにユーザ名が表示されます。
- ステップ 7** LDAP サーバのタイプを、[Active Directory]、[OpenLDAP]、[不明またはそれ以外 (Unknown or Other)] から選択します。
- ステップ 8** ポート番号を入力します。
- デフォルト ポートは 3268 です。これは Active Directory のデフォルト ポートであり、複数サーバ環境のグローバル カタログへのアクセスが可能になります。
- ステップ 9** LDAP サーバのベース DN (識別名) を入力します。
- ユーザ名とパスワードを使用して認証する場合は、パスワードが格納されているエントリへの完全 DN がユーザ名に含まれている必要があります。たとえば、電子メールアドレスが joe@example.com というユーザがマーケティング グループのユーザだとします。このユーザのエントリは、次のようになります。
- ```
uid=joe, ou=marketing, dc=example dc=com
```
- ステップ 10** [詳細設定 (Advanced)] で、LDAP サーバとの通信に SSL を使用するかどうかを選択します。
- ステップ 11** キャッシュ 存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。
- ステップ 12** 保持するキャッシュ エントリの最大数を入力します。
- ステップ 13** 同時接続の最大数を入力します。
- ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロード バランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。詳細については、[ロード バランシング \(447 ページ\)](#) を参照してください。

(注) 同時接続の最大数には、LDAP クエリに使用される LDAP 接続が含まれます。ただし、スパム隔離の LDAP 認証を有効にした場合、アプライアンスはエンド ユーザ隔離に対して 20 の追加接続を許可し、接続の総数は 30 となります。

**ステップ 14** サーバへの接続をテストするために、[テストサーバ (Test Server(s))] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス (Connection Status)] フィールドに表示されます。詳細については、[LDAP サーバのテスト \(436 ページ\)](#) を参照してください。

**ステップ 15** スпам隔離クエリを作成します。該当するチェックボックスをオンにして、フィールドに入力します。ユーザがエンドユーザ隔離にログインするときにそのユーザを検証する、隔離エンドユーザ認証クエリを設定できます。エンドユーザが電子メールエイリアスごとに隔離通知を受け取らないように、エイリアス統合クエリを設定できます。これらのクエリを使用するには、[有効なクエリとして指定する (Designate as the active query)] チェックボックスをオンにします。詳細については、[LDAP クエリの設定 \(436 ページ\)](#) を参照してください。

**ステップ 16** [クエリのテスト (Test Query)] ボタンをクリックして、スパム隔離クエリをテストします。テストパラメータを入力して [テストの実行 (Run Test)] をクリックします。テストの結果が [接続ステータス (Connection Status)] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新 (Update)] をクリックします。

(注) 空パスフレーズでのバインドを許可するように LDAP サーバが設定されている場合は、パスフレーズフィールドが空でもクエリのテストは合格となります。

**ステップ 17** 変更を送信し、保存します。

Active Directory サーバ設定では、Windows 2000 で TLS 経由の認証が許可されません。これは、Active Directory の既知の問題です。Active Directory および Windows 2003 の TLS 認証は、動作します。

(注) サーバ設定の数は無制限ですが、サーバごとに、エンドユーザ認証クエリを 1 つとエイリアス統合クエリを 1 つだけ設定できます。

## LDAP サーバのテスト

[LDAP サーバプロファイルの追加/編集 (Add/Edit LDAP Server Profile)] ページの [テストサーバ (Test Server(s))] ボタン (または CLI の `ldapconfig` コマンドの `test` サブコマンド) を使用して、LDAP サーバへの接続をテストします。サーバポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバが設定されている場合は、各サーバのテストが実行されて、結果が個別に表示されます。

## LDAP クエリの設定

次のセクションで、スパム隔離クエリのタイプごとに、デフォルトのクエリ文字列と設定の詳細を示します。

- [スパム隔離へのエンドユーザ認証のクエリ](#)。詳細については、[スパム隔離へのエンドユーザ認証のクエリ \(438 ページ\)](#) を参照してください。
- [スパム隔離エイリアス統合クエリ](#)。詳細については、[スパム隔離のエイリアス統合クエリ \(439 ページ\)](#) を参照してください。

隔離でエンドユーザ アクセスまたはスパム通知の LDAP クエリを使用するには、[有効なクエリとして指定する (Designate as the active query)] チェックボックスをオンにします。隔離アクセスを制御するエンドユーザ認証クエリを1つと、スパム通知用のエイリアス統合クエリを1つ指定できます。既存のアクティブクエリはすべてディセーブルになります。セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [LDAP] ページを選択します。アスタリスク (\*) がアクティブクエリの横に表示されます。

ドメインベースのクエリまたはチェーンクエリも、アクティブなエンドユーザアクセスクエリまたはスパム通知クエリとして指定できます。詳細については、[ドメインベースクエリ \(441 ページ\)](#) および [チェーンクエリ \(443 ページ\)](#) を参照してください。



(注) [LDAP] ページの [クエリのテスト (Test Query)] ボタン (または `ldaptest` コマンド) を使用して、クエリから返される結果が期待したとおりであることを確認します。

- [LDAP クエリの構文 \(437 ページ\)](#)
- [置換可能なトークン \(437 ページ\)](#)

## LDAP クエリの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

Cn=First Last,oU=user,dc=domain,DC=COM

クエリに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで `mailLocalAddress` と入力したときに実行されるクエリは、`maillocaladdress` と入力したときとは異なります。

## 置換可能なトークン

次のトークンを LDAP クエリ内で使用できます。

- {a} ユーザ名@ドメイン名
- {d} ドメイン
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAILFROM: アドレス



(注) {f} トークンを使用できるのは、受け入れクエリのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリは、**((mail={a})(proxyAddresses=smtp:{a}))** になります。



(注) 作成したクエリは、[LDAP] ページの [テスト (Test)] 機能（または **ldapconfig** コマンドの **test** サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、[LDAP クエリのテスト \(441 ページ\)](#) を参照してください。

## スパム隔離へのエンドユーザ認証のクエリ

エンドユーザ認証クエリとは、スパム隔離にログインするユーザを検証するためのクエリです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メールアドレスを示します。LDAP クエリによって「SMTP:」が電子メールアドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

サーバタイプに基づいて、次のデフォルト クエリ文字列がエンドユーザ認証クエリに使用されます。

- Active Directory : (sAMAccountName={u})
- OpenLDAP : (uid={u})
- 不明またはそれ以外 (Unknown or Other) : (ブランク)

デフォルトでは、プライマリ メール属性は **mail** です。独自のクエリとメール属性を入力できます。クエリを CLI で作成するには、**ldapconfig** コマンドの **isqauth** サブコマンドを使用します。



(注) ユーザのログイン時に各自の電子メールアドレス全体を入力させる場合は、**(mail=smtp:{a})** というクエリ文字列を使用します。

## Active Directory エンドユーザ認証の設定例

ここでは、Active Directory サーバとエンドユーザ認証クエリの設定の例を示します。この例では、Active Directory サーバに対してパスフレーズ認証を使用し、Active Directory サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列、メール属性は **mail** と **proxyAddresses** を使用しています。

表 69: LDAP サーバとスパム隔離へのエンドユーザ認証の設定例: Active Directory

|                      |                                                         |
|----------------------|---------------------------------------------------------|
| 認証方式                 | パスフレーズを使用（検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります。） |
| サーバタイプ (Server Type) | Active Directory                                        |
| [ポート (Port) ]        | 3268                                                    |
| ベース DN (Base DN)     | (ブランク)                                                  |
| 接続プロトコル              | (ブランク)                                                  |
| クエリ文字列               | (sAMAccountName={u})                                    |
| メール属性                | mail,proxyAddresses                                     |

## OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリの設定の例を示します。この例では、OpenLDAP サーバの匿名認証、OpenLDAP サーバのエンドユーザ認証用のデフォルトクエリ文字列、mail および mailLocalAddress メール属性を使用します。

表 70: LDAP サーバとスパム隔離へのエンドユーザ認証の設定例: OpenLDAP

|                      |                                              |
|----------------------|----------------------------------------------|
| 認証方式                 | 匿名 (Anonymous)                               |
| サーバタイプ (Server Type) | OpenLDAP                                     |
| [ポート (Port) ]        | 389                                          |
| ベース DN (Base DN)     | (ブランク) (古いスキーマでは具体的なベース DN の使用が要求されることがあります) |
| 接続プロトコル              | (ブランク)                                       |
| クエリ文字列               | (uid={u})                                    |
| メール属性                | mail,mailLocalAddress                        |

## スパム隔離のエイリアス統合クエリ

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリを使用して電子メールエイリアスを1つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメールアドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は1通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ電子メールアドレスとして選択されたアドレスです。

メッセージを統合してプライマリ電子メールアドレスに送信するには、受信者の代替電子メールエイリアスを検索するためのクエリを作成してから、受信者のプライマリ電子メールアドレスの属性を [メール属性 (Email Attribute) ] フィールドに入力します。

Active Directory サーバの場合、デフォルトクエリ文字列 (実際の展開では異なることもあります) は `((proxyAddresses={a})(proxyAddresses=smtp:{a}))` で、デフォルトの電子メール属性は `mail` です。OpenLDAP サーバの場合は、デフォルトのクエリ文字列は `(mail={a})` で、デフォルトのメール属性は `mail` です。独自のクエリとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。入力する電子メール属性が複数ある場合は、最初の電子メール属性として、変動する可能性のある値を複数持つ属性 (たとえば `proxyAddresses`) ではなく、値を 1 つだけ使用する一意の属性 (たとえば `mail`) を入力することを推奨します。

クエリを CLI で作成するには、`ldapconfig` コマンドの `isqalias` サブコマンドを使用します。

- [Active Directory エイリアス統合の設定例 \(440 ページ\)](#)
- [OpenLDAP エイリアス統合の設定例 \(440 ページ\)](#)

## Active Directory エイリアス統合の設定例

ここでは、Active Directory サーバとエイリアス統合クエリの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリ文字列を指定し、メール属性は `mail` を使用します。

表 71: LDAP サーバとスパム隔離エイリアス統合の設定例: Active Directory

|                      |                                          |
|----------------------|------------------------------------------|
| 認証方式                 | 匿名 (Anonymous)                           |
| サーバタイプ (Server Type) | Active Directory                         |
| [ポート (Port) ]        | 3268                                     |
| ベース DN (Base DN)     | (ブランク)                                   |
| 接続プロトコル              | SSL を使用する (Use SSL)                      |
| クエリ文字列               | <code>((mail={a})(mail=smtp:{a}))</code> |
| メール属性                | メールアドレス                                  |

## OpenLDAP エイリアス統合の設定例

ここでは、OpenLDAP サーバとエイリアス統合クエリの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリ文字列を指定し、メール属性は `mail` を使用します。



表 72: LDAP サーバとスパム隔離エイリアス統合の設定例: OpenLDAP

|                      |                                              |
|----------------------|----------------------------------------------|
| 認証方式                 | 匿名 (Anonymous)                               |
| サーバタイプ (Server Type) | OpenLDAP                                     |
| [ポート (Port) ]        | 389                                          |
| ベース DN (Base DN)     | (ブランク) (古いスキーマでは具体的なベース DN の使用が要求されることがあります) |
| 接続プロトコル              | SSL を使用する (Use SSL)                          |
| クエリ文字列               | (mail={a}))                                  |
| メール属性                | メールアドレス                                      |

## LDAP クエリのテスト

[LDAPサーバプロファイルの追加/編集 (Add/Edit LDAP Server Profile) ] ページの [クエリのテスト (Test Query) ] ボタン (または CLI の `ldaptest` コマンド) を使用して、クエリをテストします。AsyncOS に、クエリ接続テストの各ステージの詳細が表示されます。たとえば、最初のステージの SMTP 認証に成功したか失敗したか、バインド照合の返された結果が `true` か `false` か、などです。

`ldaptest` コマンドを、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP:isqalias foo@cisco.com
```

クエリに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、メール属性に `mailLocalAddress` と入力すると、`maillocaladdress` と入力する場合とは異なるクエリを実行します。

クエリをテストするには、テスト パラメータを入力して、[テストの実行 (Run Test) ] をクリックします。[テスト接続 (Test Connection) ] フィールドに結果が表示されます。エンドユーザ認証クエリが成功した場合、「成功: アクション: 一致ポジティブ (Success: Action: match positive) 」という結果が表示されます。エイリアス統合クエリの場合は、統合されたスパム通知用の電子メールアドレスと共に、「成功: アクション: エイリアス統合 (Success: Action: alias consolidation) 」という結果が表示されます。クエリが失敗すると、一致する LDAP レコードが見つからない、一致したレコードにメール属性が含まれていないなど、失敗の原因が表示されます。複数の LDAP サーバを使用している場合、Cisco コンテンツセキュリティアプライアンスは、LDAP サーバごとにクエリをテストします。

## ドメインベースクエリ

ドメインベースクエリとは、LDAP クエリをタイプ別にグループ化し、ドメインに関連付けたものです。複数の別の LDAP サーバが異なるドメインに関連付けられているが、エンドユーザ

隔離アクセスに対し、すべての LDAP サーバでクエリを実行する必要がある場合、ドメインベース クエリの使用を推奨します。たとえば、Bigfish という名前の会社が Bigfish.com、Redfish.com、および Bluefish.com というドメインを所持していて、それぞれのドメインに関連する従業員用に別の LDAP サーバを管理するとします。Bigfish は、ドメインベース クエリを使用して、3 つのドメインすべての LDAP ディレクトリに対してエンドユーザを認証することができます。

ドメインベース クエリを使用してスパム隔離のエンドユーザ アクセスまたは通知を制御するには、次の手順を実行します。

- 
- ステップ 1** ドメインベース クエリで使用する各ドメインについて LDAP サーバ プロファイルを作成します。各サーバ プロファイルでは、ドメインベース クエリで使用するクエリを設定します。詳細については、[LDAP サーバ プロファイルの作成 \(434 ページ\)](#) を参照してください。
  - ステップ 2** ドメインベース クエリを作成します。ドメインベース クエリを作成するときに、各サーバ プロファイルからクエリを選択し、ドメインベース クエリをスパム隔離のアクティブクエリとして指定します。クエリの作成方法の詳細については、[ドメインベース クエリの作成 \(442 ページ\)](#) を参照してください。
  - ステップ 3** スпам隔離に対して、エンドユーザ アクセスおよびスパム通知を有効にします。詳細については、[Web ブラウザからのスパム隔離へのエンドユーザ アクセスの設定 \(343 ページ\)](#) を参照してください。
- 

## ドメインベース クエリの作成

---

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [LDAP] を選択します。
- ステップ 3** [LDAP] ページで、[詳細設定 (Advanced)] をクリックします。
- ステップ 4** ドメインベース クエリの名前を入力します。
- ステップ 5** クエリ タイプを選択します。

(注) ドメインベースクエリを作成するときは、シングルクエリタイプを指定します。クエリのタイプを選択すると、該当するクエリが LDAP サーバプロファイルからクエリ フィールド ドロップダウンリストに含まれるようになります。
- ステップ 6** [ドメイン割り当て (Domain Assignments)] フィールドに、ドメインを入力します。
- ステップ 7** このドメインに関連付けるクエリを選択します。
- ステップ 8** 行を追加して、ドメインベース クエリのドメインごとにクエリを選択します。
- ステップ 9** どのクエリにも一致しないときに実行する、デフォルトのクエリを入力します。デフォルトのクエリを入力しない場合は、[なし (None)] を選択します。

図 6: ドメインベースクエリの例

Add Domain Assignments

| Domain Assignments       |                                                                                                                                                                                                                                                                                                                                                                            |                                        |       |         |              |                        |                                        |             |                       |                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------|---------|--------------|------------------------|----------------------------------------|-------------|-----------------------|----------------------------------------|
| Name:                    | Bigfish_Auth                                                                                                                                                                                                                                                                                                                                                               |                                        |       |         |              |                        |                                        |             |                       |                                        |
| Query Type:              | Spam Quarantine End-User Authentication <input type="checkbox"/> Designate as the active query                                                                                                                                                                                                                                                                             |                                        |       |         |              |                        |                                        |             |                       |                                        |
| Domain Assignments:      | <table border="1"> <thead> <tr> <th>Domain or Partial Domain</th> <th>Query</th> <th>Add Row</th> </tr> </thead> <tbody> <tr> <td>bluefish.com</td> <td>Bluefish.isq_user_auth</td> <td><input type="button" value="Add Row"/></td> </tr> <tr> <td>redfish.com</td> <td>Redfish.isq_user_auth</td> <td><input type="button" value="Add Row"/></td> </tr> </tbody> </table> | Domain or Partial Domain               | Query | Add Row | bluefish.com | Bluefish.isq_user_auth | <input type="button" value="Add Row"/> | redfish.com | Redfish.isq_user_auth | <input type="button" value="Add Row"/> |
| Domain or Partial Domain | Query                                                                                                                                                                                                                                                                                                                                                                      | Add Row                                |       |         |              |                        |                                        |             |                       |                                        |
| bluefish.com             | Bluefish.isq_user_auth                                                                                                                                                                                                                                                                                                                                                     | <input type="button" value="Add Row"/> |       |         |              |                        |                                        |             |                       |                                        |
| redfish.com              | Redfish.isq_user_auth                                                                                                                                                                                                                                                                                                                                                      | <input type="button" value="Add Row"/> |       |         |              |                        |                                        |             |                       |                                        |
| Default Query:           | None                                                                                                                                                                                                                                                                                                                                                                       |                                        |       |         |              |                        |                                        |             |                       |                                        |
| Test:                    | <input type="button" value="Test Query"/>                                                                                                                                                                                                                                                                                                                                  |                                        |       |         |              |                        |                                        |             |                       |                                        |

**ステップ 10** クエリをテストします。[クエリのテスト (Test Query)] ボタンをクリックし、テストするユーザログインとパスフレーズまたはメールアドレスを [テストパラメータ (Test Parameters)] のフィールドに入力します。結果が [接続ステータス (Connection Status)] フィールドに表示されます。

**ステップ 11** スпам隔離でドメインベースクエリを使用するには、[有効なクエリとして指定する (Designate as the active query)] チェックボックスをオンにします。

(注) ドメインベースクエリが、指定されたクエリタイプのアクティブ LDAP クエリになります。たとえば、ドメインベースクエリがエンドユーザ認証に使用されている場合は、スパム隔離のアクティブエンドユーザ認証クエリになります。

**ステップ 12** [送信 (Submit)] をクリックし、[確定する (Commit)] をクリックして変更を保存します。

(注) 同じ設定をコマンドラインインターフェイスで行うには、コマンドラインプロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

## チェーンクエリ

チェーンクエリは、AsyncOS が連続して実行する一連の LDAP クエリです。AsyncOS は LDAP サーバから肯定的なレスポンスが返されるまで、または最後のクエリで否定的なレスポンスが返されるか失敗するまで、シリーズ内の各クエリ、「チェーン」内の各クエリを実行します。チェーンクエリが役立つのは、LDAP ディレクトリ内のエン트리において、さまざまな属性に類似の (または同一の) 値が格納されている場合です。たとえば、組織の各部門が、異なるタイプの LDAP ディレクトリを使用していることがあります。IT 部門が OpenLDAP を使用し、営業部門が Active Directory を使用しているとします。クエリが両方のタイプの LDAP ディレクトリに対して実行されていることを確認するために、チェーンクエリを使用できます。

チェーンクエリを使用してスパム隔離のエンドユーザアクセスまたは通知を制御するには、次の手順を実行します。

**ステップ 1** チェーンクエリで使用するクエリごとに1つずつ、LDAP サーバプロファイルを作成します。このサーバプロファイルのそれぞれについて、チェーンクエリに使用するクエリを設定します。詳細については、[LDAP サーバプロファイルの作成 \(434 ページ\)](#) を参照してください。

**ステップ 2** チェーンクエリを作成し、スパム隔離のアクティブクエリとして指定します。詳細については、[チェーンクエリの作成 \(444 ページ\)](#) を参照してください。

**ステップ3** スпам隔離に対して、LDAP エンドユーザ アクセスおよびスパム通知を有効にします。スパム隔離の詳細については、[中央集中型スパム隔離の設定（320 ページ）](#)を参照してください。

## チェーンクエリの作成



**ヒント** CLI から、`ldapconfig` コマンドの `advanced` サブコマンドも使用できます。

**ステップ1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [LDAP] > [LDAPサーバ (LDAP Server)] を選択します。

**ステップ3** [LDAPサーバプロファイル (LDAP Server Profiles)] ページの [詳細設定 (Advanced)] をクリックします。

**ステップ4** [連鎖クエリを追加 (Add Chained Query)] をクリックします。

**ステップ5** チェーンクエリの名前を入力します。

**ステップ6** クエリのタイプを選択します。

チェーンクエリを作成するときは、そのコンポーネントのクエリすべてを同じクエリタイプにします。クエリのタイプを選択すると、該当するクエリが LDAP からクエリ フィールド ドロップダウンリストに表示されます。

**ステップ7** チェーンの最初のクエリを選択します。

Cisco コンテンツ セキュリティ アプライアンスによって、ここで設定した順にクエリが実行されます。チェーンクエリに複数のクエリを追加する場合は、詳細なクエリの後に広範なクエリが続くように順序付けることを推奨します。

図 7: チェーンクエリの例

Add Chained Query

| Chained Query     |                                                                                                                                                                                                                                                                                                                            |                                        |       |  |   |                       |                                        |   |                       |                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------|--|---|-----------------------|----------------------------------------|---|-----------------------|----------------------------------------|
| Name:             | Chain_Query                                                                                                                                                                                                                                                                                                                |                                        |       |  |   |                       |                                        |   |                       |                                        |
| Query Type:       | Spam Quarantine End-User Authentication <input type="checkbox"/> Designate as the active query                                                                                                                                                                                                                             |                                        |       |  |   |                       |                                        |   |                       |                                        |
| Order of Queries: | <table border="1"> <thead> <tr> <th>Order</th> <th>Query</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Server1.isq_user_auth</td> <td><input type="button" value="Add Row"/></td> </tr> <tr> <td>2</td> <td>Server2.isq_user_auth</td> <td><input type="button" value="Add Row"/></td> </tr> </tbody> </table> | Order                                  | Query |  | 1 | Server1.isq_user_auth | <input type="button" value="Add Row"/> | 2 | Server2.isq_user_auth | <input type="button" value="Add Row"/> |
| Order             | Query                                                                                                                                                                                                                                                                                                                      |                                        |       |  |   |                       |                                        |   |                       |                                        |
| 1                 | Server1.isq_user_auth                                                                                                                                                                                                                                                                                                      | <input type="button" value="Add Row"/> |       |  |   |                       |                                        |   |                       |                                        |
| 2                 | Server2.isq_user_auth                                                                                                                                                                                                                                                                                                      | <input type="button" value="Add Row"/> |       |  |   |                       |                                        |   |                       |                                        |
| Test:             | <input type="button" value="Test Query"/>                                                                                                                                                                                                                                                                                  |                                        |       |  |   |                       |                                        |   |                       |                                        |

**ステップ8** クエリをテストします。[クエリのテスト (Test Query)] ボタンをクリックし、ユーザログインとパスワードまたはメールアドレスを [テストパラメータ (Test Parameters)] のフィールドに入力します。結果が [接続ステータス (Connection Status)] フィールドに表示されます。

**ステップ9** スпам隔離でドメインクエリを使用するには、[有効なクエリとして指定する (Designate as the active query)] チェックボックスをオンにします。

- (注) チェーンクエリが、指定されたクエリ タイプのアクティブ LDAP クエリになります。たとえば、チェーンクエリがエンドユーザ認証に使用されている場合は、スパム隔離のアクティブエンドユーザ認証クエリになります。

**ステップ 10** 変更を送信し、保存します。

- (注) 同じ設定をコマンドラインインターフェイスで行うには、コマンドラインプロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

## AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP サーバプロファイルを設定するときに、Cisco コンテンツセキュリティアプライアンスからの接続先となる複数の LDAP サーバをリストとして設定できます。複数の LDAP サーバを使用するには、格納されている情報、構造、使用する認証情報を同一にする必要があります。レコードを統合できる製品がサードパーティから提供されています。

次の機能を使用する場合は、冗長 LDAP サーバに接続するように Cisco コンテンツセキュリティアプライアンスを設定します。

- **フェールオーバー**。Cisco コンテンツセキュリティアプライアンスが LDAP サーバに接続できない場合、リストで次に指定されているサーバに接続します。
- **ロードバランシング**。Cisco コンテンツセキュリティアプライアンスは、LDAP クエリを実行するときに、リストで指定されている LDAP サーバの間で接続を分散します。

冗長 LDAP サーバを設定するには、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [LDAP] ページまたは CLI の `ldapconfig` コマンドを使用します。

## サーバとクエリのテスト

[LDAP サーバプロファイルを追加 (または編集) (Add (or Edit) LDAP Server Profile)] ページの [テストサーバ (Test Server(s))] ボタン (または CLI の `test` サブコマンド) を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリのテストも実行されて、結果が個別に表示されます。

## フェールオーバー

LDAP サーバで確実にクエリを解決できるようにするには、フェールオーバー用に LDAP プロファイルを設定できます。LDAP サーバへの接続が失敗するか、またはクエリからエラーが返される場合にそうすることが適切であれば、アプライアンスはリストに指定されている次の LDAP サーバに対してクエリを試行します。

Cisco コンテンツセキュリティアプライアンスは、LDAP サーバリスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。アプライアンスがリスト内の最初の LDAP

サーバに接続できない場合、またはクエリからエラーが返される場合、リスト内の次の LDAP サーバへの接続が試行されます。デフォルトでは、アプライアンスは常にリスト内の最初のサーバへの接続を試行し、それ以降の各サーバへの接続を、リスト内で指定されている順に試行します。Cisco コンテンツ セキュリティ アプライアンスが確実にプライマリ LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバリストの先頭に入力されていることを確認してください。



(注) 指定された LDAP サーバを問い合わせる試行のみがフェールオーバーします。指定された LDAP サーバに関連付けられた参照サーバまたは継続サーバを問い合わせる試行はフェールオーバーしません。

Cisco コンテンツ セキュリティ アプライアンスが 2 番目の、または後続の LDAP サーバに接続する場合、そのサーバへの接続は所定の時間が経過するまで維持されます。この時間が経過すると、アプライアンスはリスト内の最初のサーバに対して再接続を試行します。

## LDAP フェールオーバーのための Cisco コンテンツ セキュリティ アプライアンスの設定

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [LDAP] を選択します。

**ステップ 3** 編集する LDAP サーバプロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 8: LDAP フェールオーバー コンフィギュレーションの例

**ステップ 4** [ホスト名 (Hostname)] テキストフィールドに、LDAP サーバ (ldapsrvr.example.com など) を入力します。

**ステップ 5** [各ホストの最大同時接続数 (Maximum number of simultaneous connections for each host)] テキストフィールドに、最大接続数を入力します。

この例では、最大接続数が 10 です。

- ステップ 6** [一覧されている順序での接続のフェールオーバー (Failover connections in the order list) ]の横にあるオプション ボタンをクリックします。
- ステップ 7** その他の LDAP オプションを必要に応じて設定します。
- ステップ 8** 変更を送信し、保存します。

## ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロード バランシングを使用した場合、Cisco コンテンツ セキュリティ アプライアンスからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、アプライアンスは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。アプライアンスは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

## ロード バランシングのための Cisco コンテンツ セキュリティ アプライアンスの設定

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理コンソールで、歯車 (⚙) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[LDAP] を選択します。
- ステップ 3** 編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 9: ロードバランシングの設定例

- ステップ 4** [ホスト名 (Hostname) ]テキスト フィールドに、LDAP サーバ (ldapsrv.example.com など) を入力します。

- ステップ 5** [各ホストの最大同時接続数 (Maximum number of simultaneous connections for each host) ] テキスト フィールドに、最大接続数を入力します。
- この例では、最大接続数が **10** です。
- ステップ 6** [すべてのホスト間での負荷分散接続 (Load balance connections among all hosts) ] の横にあるオプション ボタンをクリックします。
- ステップ 7** その他の LDAP オプションを必要に応じて設定します。
- ステップ 8** 変更を送信し、保存します。

---

## LDAP を使用した管理ユーザの外部認証の設定

ネットワーク上の LDAP ディレクトリを使用して管理ユーザを認証するように Cisco コンテンツセキュリティ アプライアンスを設定できます。このように設定すると、ユーザが各自の LDAP ユーザ名とパスワードを使用して、アプライアンスにログインできるようになります。

- ステップ 1** LDAP サーバプロファイルを設定します。[LDAP サーバプロファイルの作成 \(434 ページ\)](#) を参照してください。
- ステップ 2** ユーザ アカウントを見つけるためのクエリを作成します。LDAP サーバプロファイルの、[外部認証クエリ (External Authentication Queries) ] セクションで、クエリを作成して LDAP ディレクトリ内のユーザ アカウントを検索します。[管理ユーザの認証のためのユーザアカウントクエリ \(448 ページ\)](#) を参照してください。
- ステップ 3** グループ メンバーシップ クエリを作成します。あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリを作成し、あるグループのすべてのメンバーを検索する別のクエリを作成します。詳細については、[管理ユーザの認証のためのグループメンバーシップクエリ \(449 ページ\)](#) およびご使用の E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。
- (注) そのページの [外部認証クエリ (External Authentication Queries) ] セクションにある [テスト クエリ (Test Queries) ] ボタン (または `ldaptest` コマンド) を使用して、クエリから返される結果が期待したとおりであることを確認します。関連情報については、[LDAP クエリのテスト \(441 ページ\)](#) を参照してください。
- ステップ 4** LDAP サーバを使用するように外部認証をセットアップします。この LDAP サーバをユーザ認証に使用するようにアプライアンスを設定し、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。詳細については、[管理ユーザの外部認証のイネーブル化 \(451 ページ\)](#) および E メールセキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Adding Users」を参照してください。

---

## 管理ユーザの認証のためのユーザ アカウント クエリ

外部ユーザを認証するために、AsyncOS はクエリを使用してそのユーザのレコードを LDAP ディレクトリ内で検索し、ユーザのフルネームが格納されている属性を見つけます。選択した



サーバタイプに応じて、AsyncOS によってデフォルトクエリーとデフォルト属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されている必要があります (**shadowLastChange**、**shadowMax**、および **shadowExpire**)。ユーザレコードが存在するドメインレベルのベース DN が必須です。

次の表に、AsyncOS がユーザアカウントを Active Directory サーバ上で検索するときを使用されるデフォルトのクエリ文字列とユーザのフルネーム属性を示します。

表 73: Active Directory サーバのデフォルトクエリ文字列

| サーバタイプ (Server Type)                                            | Active Directory                               |
|-----------------------------------------------------------------|------------------------------------------------|
| ベース DN (Base DN)                                                | (ブランク) (ユーザレコードを見つけるには具体的なベース DN を使用する必要があります) |
| クエリ文字列                                                          | (&(objectClass=user)(sAMAccountName={u}))      |
| ユーザのフルネームが格納されている属性 (Attribute containing the user's full name) | displayName                                    |

次の表に、AsyncOS がユーザアカウントを OpenLDAP サーバ上で検索するときを使用されるデフォルトのクエリ文字列とユーザのフルネーム属性を示します。

表 74: Open LDAP サーバのデフォルトクエリ文字列

| サーバタイプ (Server Type)                                            | OpenLDAP                                       |
|-----------------------------------------------------------------|------------------------------------------------|
| ベース DN (Base DN)                                                | (ブランク) (ユーザレコードを見つけるには具体的なベース DN を使用する必要があります) |
| クエリ文字列                                                          | (&(objectClass=posixAccount)(uid={u}))         |
| ユーザのフルネームが格納されている属性 (Attribute containing the user's full name) | gecos                                          |

## 管理ユーザの認証のためのグループメンバーシップクエリ

LDAP グループをアプライアンスにアクセスするためのユーザロールと関連付けることができます。

AsyncOS は、あるユーザがディレクトリグループのメンバーであるかどうかを判断するクエリや、あるグループのすべてのメンバーを検索する別のクエリを使用することもできます。ディレクトリグループメンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザ (Users)] ページ (または CLI の userconfig) で外部認証を有効にするときに、ユーザロールを LDAP ディレクトリ内のグループに割り当

てます。ユーザロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリグループに割り当てられます。たとえば、IT というディレクトリグループ内のユーザに Administrator ロールを割り当て、Support というディレクトリグループのユーザに Help Desk User ロールを割り当てます。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループメンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループレコードが格納されているディレクトリレベルのベース DN、グループメンバーのユーザ名が格納されている属性、およびグループ名が格納されている属性を入力します。LDAP サーバプロファイルに対して選択されたサーバタイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルトクエリ文字列が AsyncOS によって入力されます。



- (注) Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリ文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

次の表に、AsyncOS が Active Directory サーバ上でグループメンバーシップ情報を検索するとき使用されるデフォルトのクエリ文字列と属性を示します。

表 75: Active Directory サーバのデフォルトクエリ文字列および属性

| クエリ文字列                                    | Active Directory                                                                                                      |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| ベース DN (Base DN)                          | (ブランク) (グループレコードを見つけるには具体的なベース DN を使用する必要があります)                                                                       |
| ユーザが特定のグループのメンバーかどうかを判断するためのクエリ文字列        | (&(objectClass=group)(member={u}))<br>(注) 使用する LDAP スキーマにおいてメンバーのリストの中でユーザ名ではなく識別名が使用されている場合は、{u} の代わりに {dn} を使用できます。 |
| グループのすべてのメンバーを判別するクエリ文字列                  | (&(objectClass=group)(cn={g}))                                                                                        |
| 各メンバーのユーザ名 (またはそのユーザのレコードの DN) が格納されている属性 | member                                                                                                                |
| グループ名が格納されている属性                           | cn                                                                                                                    |

次の表に、AsyncOS が OpenLDAP サーバ上でグループメンバーシップ情報を検索するとき使用されるデフォルトのクエリ文字列と属性を示します。

表 76: Open LDAP サーバのデフォルト クエリ文字列および属性

| クエリ文字列                                    | OpenLDAP                                        |
|-------------------------------------------|-------------------------------------------------|
| ベース DN (Base DN)                          | (ブランク) (グループレコードを見つけるには具体的なベース DN を使用する必要があります) |
| ユーザが特定のグループのメンバーかどうかを判断するためのクエリ文字列        | (&(objectClass=posixGroup)(memberUid={u}))      |
| グループのすべてのメンバーを判別するクエリ文字列                  | (&(objectClass=posixGroup)(cn={g}))             |
| 各メンバーのユーザ名 (またはそのユーザのレコードの DN) が格納されている属性 | memberUid                                       |
| グループ名が格納されている属性                           | cn                                              |

## 管理ユーザの外部認証のイネーブル化

LDAP サーバプロファイルおよびクエリを設定した後で、LDAP を使用する外部認証をイネーブルにすることができます。

- 
- ステップ 1 (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
  - ステップ 2 [管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [ユーザ (Users) ] ページを選択します。
  - ステップ 3 [有効 (Enable) ] をクリックします。
  - ステップ 4 [外部認証を有効にする (Enable External Authentication) ] チェックボックスをオンにします。
  - ステップ 5 認証タイプとして [LDAP] を選択します。
  - ステップ 6 ユーザを認証する LDAP 外部認証クエリを選択します。
  - ステップ 7 タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。
  - ステップ 8 アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。
  - ステップ 9 また、[行の追加 (Add Row) ] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対してステップ 7 とステップ 8 を繰り返します。
  - ステップ 10 変更を送信し、保存します。
-





## 第 13 章

# SMTP ルーティングの設定

この章は、次の項で構成されています。

- [SMTP ルートの概要 \(453 ページ\)](#)
- [ローカル ドメインの電子メールのルーティング \(454 ページ\)](#)
- [SMTP ルートの管理 \(455 ページ\)](#)

## SMTP ルートの概要

この章では、Cisco コンテンツ セキュリティ管理アプライアンスを通過する電子メールのルーティングおよび配信に影響を与える機能、および [SMTP ルート (SMTP Routes) ] ページと `smtproutes` コマンドの使用について説明します。

SMTP ルートを使用すると、特定ドメインのすべての電子メールを別の Mail eXchange (MX; メール交換) ホストへリダイレクトできます。たとえば、`example.com` から `groupware.example.com` へのマッピングを作成できます。このマッピングにより、エンベロップ受信者アドレスに `@example.com` が含まれる電子メールは、代わりに `groupware.example.com` に転送されます。システムは、通常の電子メール配信のように、`groupware.example.com` で「MX」ルックアップを実行し、次にホストで「A」ルックアップを実行します。この代替 MX ホストは、DNS の MX レコードにリストされている必要はなく、電子メールがリダイレクトされているドメインのメンバである必要もありません。オペレーティングシステムでは、最大 10,000 件の SMTP ルートマッピングを Cisco コンテンツ セキュリティ アプライアンスに設定できます ([SMTP ルートの制限 \(456 ページ\)](#) を参照)。

この機能を使用すると、ホストを「ひとかたまりにする」ことができます。`example.com` などの部分ドメインを指定すると、`example.com` で終わるすべてのドメインがエントリに一致します。たとえば、`fred@foo.example.com` と `wilma@bar.example.com` は、両方ともマッピングに一致します。

SMTP ルートテーブルにホストがない場合は、DNS を使用して MX ルックアップが実行されます。結果は、SMTP ルートテーブルに対して再チェックされません。`foo.domain` の DNS MX エントリが `bar.domain` の場合、`foo.domain` に送信されるすべての電子メールが `bar.domain` に配信されます。`bar.domain` から他のホストへのマッピングを作成した場合、`foo.domain` へ送信される電子メールは影響を受けません。

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがある場合、メールのループは作成されません。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

すべての電子メール配信で、SMTP ルートテーブルは、上から順に読み取られます。マッピングと一致する最も具体的なエントリが選択されます。たとえば、SMTP ルートテーブルに host1.example.com と example.com の両方のマッピングがある場合は、host1.example.com の方が具体的なエントリになっているため、こちらが使用されます。具体的でない方の example.com エントリが先にあっても、同じ結果になります。そうでない場合は、エンベロープ受信者のドメインで通常の MX ルックアップが実行されます。

## SMTP ルート、メール配信、およびメッセージ分裂

着信：1つのメッセージに10人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を1つ開き、メールストアには10の別々のメッセージではなく、メッセージを1つのみ配置します。

発信：動作は同様ですが、1つのメッセージが10の異なるドメインの10人の受信者に送信される場合、AsyncOS では10のMTAに対する10の接続を開き、それぞれ1つの電子メールを配信します。

分裂：1つの着信メッセージに10人の受信者がいて、全員が別々の着信ポリシーグループ（10グループ）に属する場合、10人の受信者全員が同じ Exchange サーバに属していても、メッセージは分裂されます。つまり、10の別々の電子メールが1つの TCP 接続で配信されます。

## SMTP ルートと発信 SMTP 認証

発信 SMTP 認証プロファイルを作成したら、SMTP ルートに適用できます。これにより、ネットワークのエッジにあるメールリレーサーバの背後に Cisco コンテンツセキュリティアプライアンスが位置する場合に、発信メールの認証が可能になります。

## ローカルドメインの電子メールのルーティング

セキュリティ管理アプライアンスは、次のメールをルーティングします。

- ISQ によりリリースされた、SMTP ルーティングを無視するメッセージ
- アラート (Alerts)
- 指定した宛先にメールできるコンフィギュレーションファイル
- 定義された受信者にも送信できるサポート要求メッセージ

最後の2種類のメッセージは、宛先への配信に SMTP ルートが使用されます。

Email Security Appliance はローカルドメイン宛てのメールを、[管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [SMTP ルート (SMTP Routes)] ページ (または `smtproutes` コマンド) を使用して指定されたホストにルーティングします。この機能は、

sendmail の **mailertable** 機能に似ています。 ([SMTP ルート (SMTP Routes) ] ページと **smtproutes** コマンドは、AsyncOS 2.0 ドメイン リダイレクト機能を拡張したものです)。



(注) GUI のシステム設定ウィザードを完了し、変更を保存した場合、その時点で入力した各 RAT エントリに対してアプライアンス上の最初の SMTP ルート エントリを定義します。

## デフォルトの SMTP ルート

特殊なキーワード ALL を使用して、デフォルトの SMTP ルートを定義することもできます。ドメインが SMTP ルート リストで前のマッピングと一致しない場合のデフォルトは、ALL エントリで指定された MX ホストにリダイレクトされます。

SMTP ルート エントリを印刷する場合、デフォルトの SMTP ルートは ALL: として一覧表示されます。デフォルトの SMTP ルートは削除できません。入力した値をクリアすることのみ可能です。

[管理アプライアンス (Management Appliance) ] > [ネットワーク (Network) ] > [SMTP ルート (SMTP Routes) ] ページを使用するか、または **smtproutes** コマンドを使用して、デフォルトの SMTP ルートを設定します。

## SMTP ルートの管理

- [SMTP ルートの定義 \(455 ページ\)](#)
- [SMTP ルートの制限 \(456 ページ\)](#)
- [SMTP ルートの追加 \(456 ページ\)](#)
- [SMTP ルートのエクスポート \(456 ページ\)](#)
- [SMTP ルートのインポート \(457 ページ\)](#)
- [SMTP ルートと DNS \(458 ページ\)](#)

## SMTP ルートの定義

Email Security Appliance はローカルドメイン宛てのメールを、[管理アプライアンス (Management Appliance) ] > [ネットワーク (Network) ] > [SMTP ルート (SMTP Routes) ] ページ (または **smtproutes** コマンド) を使用して指定されたホストにルーティングします。この機能は、sendmail の mailer table 機能に似ています。 ([SMTP ルート (SMTP Routes) ] ページと **smtproutes** コマンドは、AsyncOS 2.0 ドメイン リダイレクト機能を拡張したものです)。

[管理アプライアンス (Management Appliance) ] > [ネットワーク (Network) ] > [SMTP ルート (SMTP Routes) ] ページ (または **smtproutes** コマンド) を使用してルートを作成します。新しいルートを作成するには、まず、永続的なルートを作成するドメインまたはドメインの一部を指定する必要があります。次に、宛先ホストを指定します。宛先ホストは、完全修飾ホスト名として入力することも、IP アドレスとして入力することもできます。特殊な宛先ホスト /dev/null を指定して、エントリに一致するメッセージを廃棄することもできます。(つまり、

デフォルト ルートに /dev/null を指定することで、アプライアンスで受信されたメールが配信されないようにすることができます)。

複数の宛先ホスト エントリに、完全修飾ホスト名と IP アドレスの両方を含めることができます。複数のエントリを指定する場合は、カンマで区切ります。

1 つまたは複数のホストが応答しない場合、メッセージは到達可能なホストの 1 つに配信されます。設定されたすべてのホストが応答しない場合、メールはそのホストのキューに格納されます (MX レコードの使用にフェールオーバーしません)。

## SMTP ルートの制限

最大 10,000 ルートまで定義できます。ALL による最終的なデフォルト ルートは、この制限に含まれます。したがって、定義できるのは最大 9,999 のカスタム ルートと、特殊キーワード ALL を使用する 1 つのルートです。

## SMTP ルートの追加

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
  - ステップ 2** [管理アプライアンス (Management Appliance) ] > [ネットワーク (Network) ] > [SMTP ルート (SMTP Routes) ] を選択します。
  - ステップ 3** [ルートを追加 (Add Route) ] をクリックします。
  - ステップ 4** 受信側ドメインと宛先ホストを入力します。複数の宛先ホストを追加するには、[行の追加 (Add Row) ] をクリックし、新しい行に次の宛先ホストを入力します。
  - ステップ 5** ポート番号を指定するには、宛先ホストに「:<port number>」を追加します (例 : example.com:25)
  - ステップ 6** 変更を送信し、保存します。
- 

## SMTP ルートのエクスポート

Host Access Table (HAT) および Recipient Access Table (RAT) の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。

- 
- ステップ 1** [SMTP ルート (SMTP Routes) ] ページの [SMTP ルートをエクスポート (Export SMTP Routes) ] をクリックします。
  - ステップ 2** ファイルの名前を入力し、[送信 (Submit) ] をクリックします。
-



## SMTP ルートのインポート

Host Access Table (HAT) および Recipient Access Table (RAT) の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。

- ステップ 1** [SMTPルート (SMTP Routes) ] ページの [SMTPルートをインポート (Import SMTP Routes) ] をクリックします。
- ステップ 2** エクスポートした SMTP ルートを含むファイルを選択します。
- ステップ 3** [送信 (Submit) ] をクリックします。インポートによって既存の SMTP ルートがすべて置き換えられることが警告されます。テキストファイル内のすべての SMTP ルートがインポートされます。
- ステップ 4** [インポート (Import) ] をクリックします。

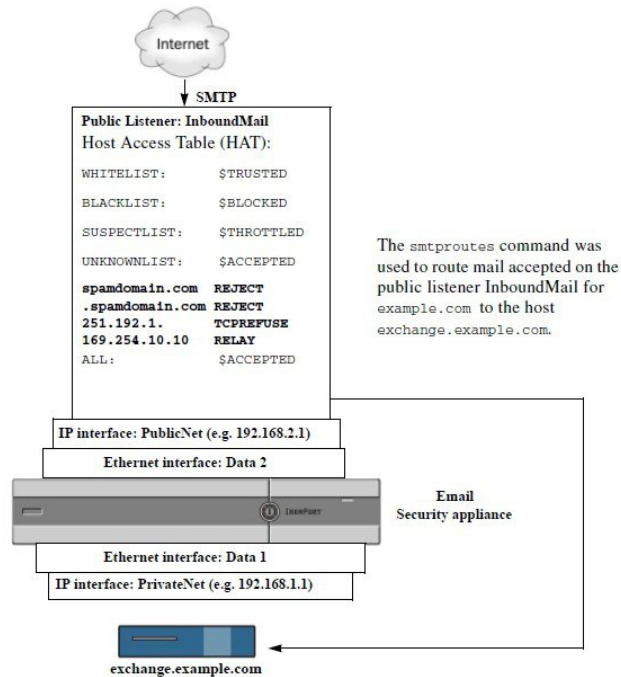
ファイル内に「コメント」を配置できます。文字「#」で始まる行はコメントと見なされ、AsyncOSによって無視されます。次に例を示します。

```
# this is a comment, but the next line is not
```

```
ALL:
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 10: Eメール ゲートウェイの設定



## SMTP ルートと DNS

特殊なキーワード `USEDNS` を使用すると、特定ドメインの次のホップを決定する MX ルックアップがアプライアンスで実行されます。これは、サブドメイン宛のメールを特定ホストへルーティングする必要があるときに便利です。たとえば、`example.com` へのメールが企業の Exchange サーバに送信されるようにする場合、SMTP ルートは次のようになります。

```
example.com exchange.example.com
```

ただし、さまざまなサブドメイン (`foo.example.com`) 宛のメールの場合は、次のような SMTP ルートを追加します。

```
.example.com USEDNS
```



## 第 14 章

# Cisco Threat Response ポータルとの統合

この章は、次の項で構成されています。

- [Cisco Threat Response ポータルへのアプライアンスの統合](#) (459 ページ)
- [CLI を使用した Cisco Threat Response ポータルへのアプライアンスの統合](#) (461 ページ)
- [ケースブックを使用した脅威分析の実行](#) (464 ページ)

## Cisco Threat Response ポータルへのアプライアンスの統合

Cisco Threat Response ポータルにアプライアンスを統合すると、Cisco Threat Response ポータルで次のアクションを実行できます。

- 組織内の複数のアプライアンスから電子メール レポート、メッセージ トラッキング、および Web トラッキングのデータを確認します。
- 電子メール レポート、メッセージ トラッキング、Web トラッキングで検出された脅威を特定、調査、および修正します。
- 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。
- ポータルで脅威をドキュメント化して調査を保存し、ポータル内の他のデバイス間で情報を共有します。

Cisco Threat Response ポータルにアプライアンスを統合するには、Cisco Threat Response ポータルにアプライアンスを登録する必要があります。

Cisco Threat Response ポータルにアクセスするには、次の URL を使用します。

- <https://visibility.amp.cisco.com>
- <https://visibility.eu.amp.cisco.com/>



- (注) 地域 URL (<https://visibility.apjc.amp.cisco.com>) を使用して Cisco Threat Response ポータルにアクセスする場合、Cisco Threat Response とアプライアンスの統合は現在のところサポートされていません。

### 始める前に

- 管理者アクセス権限を使用して Cisco Threat Response ポータルでユーザ アカウントが作成されていることを確認します。新しいユーザ アカウントを作成するには、URL (<https://visibility.amp.cisco.com>) を使用して Cisco Threat Response ポータル ログイン ページに移動し、ログイン ページで [シスコセキュリティアカウントの作成 (Create a Cisco Security account)] をクリックします。新しいユーザ アカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。
- Cisco Security Services Exchange (SSE) ポータルで Cisco Threat Response の統合が有効になっていることを確認します。詳細については、<https://visibility.amp.cisco.com/#/help/module-sma> で Cisco Threat Response ドキュメントを参照してください。
- アプライアンスを Cisco Threat Response ポータルに登録する場合、次の FQDN に関してファイアウォールで HTTPS (インおよびアウト) 443 ポートがオープンになっていることを確認してください。
  - [api-sse.cisco.com](https://api-sse.cisco.com) (アメリカ地域のユーザのみに対応)
  - [api.eu.sse.itd.cisco.com](https://api.eu.sse.itd.cisco.com) (欧州連合 (EU) のユーザのみに対応)
  - [est.sco.cisco.com](https://est.sco.cisco.com) (アメリカ地域と EU 両方のユーザに対応)

詳細については、[ファイアウォール情報 \(643 ページ\)](#) を参照してください。

- 
- ステップ 1** アプライアンスにログインします。
  - ステップ 2** [ネットワーク (Networks)] > [クラウドサービス設定 (Cloud Service Settings)] を選択します。
  - ステップ 3** [設定の編集 (Edit Settings)] をクリックします。
  - ステップ 4** [有効 (Enable)] をオンにします。
  - ステップ 5** アプライアンスを Cisco Threat Response ポータルに接続するために必要な Cisco Threat Response サーバを選択します。
  - ステップ 6** 変更を送信し、保存します。
  - ステップ 7** Cisco Threat Response ポータルにアプライアンスを登録するのに数分かかり、その後でクラウドサービスの設定ページに移動します。
  - ステップ 8** Cisco Threat Response ポータルでアプライアンスを登録する際に使用する Cisco Threat Response ポータルから登録トークンを生成します。詳細については、<https://visibility.amp.cisco.com/#/help/module-sma> で Cisco Threat Response ドキュメントを参照してください。
  - ステップ 9** Cisco Threat Response ポータルから取得した登録トークンを入力し、[登録 (Register)] をクリックします。

**ステップ 10** Cisco Threat Response ポータルにアプライアンスを統合モジュールとして追加します。詳細については、<https://visibility.amp.cisco.com/#/help/module-sma> で Cisco Threat Response ドキュメントを参照してください。

#### 次のタスク

- Cisco Threat Response ポータルにアプライアンスを統合モジュールとして追加すると、Cisco Threat Response ポータルのアプライアンスから電子メール レポート、メッセージ トラッキング、Web トラッキング情報を表示できます。詳細については、<https://visibility.amp.cisco.com/#/help/module-sma> で Cisco Threat Response ドキュメントを参照してください。



(注) Cisco Threat Response ポータルからアプライアンスの接続を登録解除するには、アプライアンスの [クラウドサービス設定 (Cloud Services Settings)] ページで [登録解除 (Deregister)] をクリックします。

- 別の Cisco Threat Response サーバ (欧州用の「api.eu.sse.itd.cisco.com」など) に切り替える場合は、最初に Cisco Threat Response ポータルからアプライアンスの登録を解除して、「Cisco Threat Response ポータルへのアプライアンスの統合 (Integrating the Appliance with Cisco Threat Response Portal)」のステップ 1 ~ 9 を実行する必要があります。



(注) Cisco Threat Response ポータルにアプライアンスを統合した後は、電子メールと Web のレポート機能が集中管理されるため、電子メールセキュリティアプライアンスを Cisco Threat Response ポータルに統合する必要はありません。

## CLI を使用した Cisco Threat Response ポータルへのアプライアンスの統合

ここでは、次の CLI コマンドについて説明します。

- [threatresponseconfig \(462 ページ\)](#)
- [cloudserviceconfig \(463 ページ\)](#)

## threatresponseconfig

### 説明

threatresponseconfig コマンドは次の目的で使用します。

- アプライアンスの Cisco Threat Response 機能を有効にします。
- アプライアンスの Cisco Threat Response 機能を無効にします。

### 使用法

**確定** : このコマンドは「commit」が必要です。

**クラスタ管理** : このコマンドはマシンモードでのみ使用できます。

**バッチ コマンド** : このコマンドはバッチ形式をサポートしています。

### 例

次の例では、threatresponseconfig コマンドを使用してアプライアンスの Cisco Threat Response 機能を有効にします。

```
mail1.example.com> threatresponseconfig
```

```
Choose the operation you want to perform:
```

```
- ENABLE - To enable the Cisco Threat Response feature on your appliance.  
[]> enable
```

```
The Cisco Threat Response feature is currently enabled on your appliance. Use the  
cloudserviceconfig command to register your appliance with the Cisco Threat  
Response portal.
```

```
mail1.example.com> commit
```

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

```
[]>
```

```
Changes committed: Mon Nov 19 10:04:35 2018 GMT
```

次の例では、threatresponseconfig コマンドを使用してアプライアンスの Cisco Threat Response 機能を無効にします。

```
mail1.example.com> threatresponseconfig
```

```
Choose the operation you want to perform:
```

```
- DISABLE - To disable the Cisco Threat Response feature on your appliance.  
[]> disable
```

```
The Cisco Threat Response feature is currently disabled on your appliance.
```

```
mail1.example.com> commit
```

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

```
[]>
```

```
Changes committed: Mon Nov 19 10:04:35 2018 GMT
```

## cloudserviceconfig

### 説明

cloudserviceconfig コマンドは次の目的で使用します。

- Cisco Threat Response ポータルにアプライアンスを登録します。
- Cisco Threat Response ポータルからアプライアンスを登録解除します。
- アプライアンスを Cisco Threat Response ポータルに接続するための Cisco Threat Response サーバを選択します。

### 使用法

**確定** : このコマンドに **commit** は必要ありません。

**クラスタ管理** : このコマンドはマシン モードでのみ使用できます。

**バッチ コマンド** : このコマンドはバッチ形式をサポートしています。

### 例

次の例では、cloudserviceconfig コマンドを使用してアプライアンスを Cisco Threat Response ポータルに登録できます。

```
mail1.example.com> cloudserviceconfig
```

```
Choose the operation you want to perform:
```

```
- REGISTER - To register the appliance with the Cisco Threat Response portal.  
-SETTRS - Set the Threat Response Server to connect to the Cisco Threat Response portal.  
[]> register
```

```
Enter a registration token key to register your appliance with the Cisco Threat Response portal.
```

```
[]> de7c55f3ff0absdfs4a25aae94dfb064642
```

```
The appliance registration is in progress.
```

次の例では、cloudserviceconfig コマンドを使用して、アプライアンスを Cisco Threat Response ポータルに接続するための Cisco Threat Response サーバを選択します。

```
mail1.example.com> cloudserviceconfig
```

```
Choose the operation you want to perform:
```

```
- DEREGISTER - To deregister the appliance from the Cisco Threat Response portal.  
-SETTRS - Set the Threat Response Server to connect to the Cisco Threat Response portal.  
[]> settrs
```

```
Available list of Threat Response Servers:
```

1. AMERICAS (api-sse.cisco.com)
2. EUROPE (api.eu.sse.itd.cisco.com)

```
Enter threat response server to connect to the Cisco Threat Response portal.:
```

```
[]> 2
```

```
Selected threat response server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
```

```
mail1.example.com> commit
Please enter some comments describing your changes:
[]>
```

```
Changes committed: Mon Jun 19 10:04:35 2019 GMT
```

次の例では、`cloudserviceconfig` コマンドを使用して、Cisco Threat Response ポータルからアプライアンスの登録を解除します。

```
mail1.example.com> cloudserviceconfig
```

```
The Content Security Management appliance is successfully registered with the
Cisco Threat Response portal.
```

```
Choose the operation you want to perform:
```

```
- DEREGISTER - To deregister the appliance from the Cisco Threat Response
portal.
-SETTRS - Set the Threat Response Server to connect to the Cisco Threat Response portal.
[]> deregister
```

```
Do you want to deregister your appliance from the Cisco Threat Response portal.
```

```
If you deregister, you will not be able to access the Cloud Service features. [N]> yes
```

```
The Content Security Management appliance deregistration is in progress.
```

## ケースブックを使用した脅威分析の実行

ケースブックとピボットメニューは Cisco Threat Response ポータルで使用できるウィジェットです。

ケースブックは、調査および攻撃分析の際に主要な観測対象のグループを記録、整理、共有するために使用します。ケースブックを使用して、観測対象の現在の判定または傾向を取得できます。詳細については、<https://visibility.amp.cisco.com/#/help/casebooks> で Cisco Threat Response ドキュメントを参照してください。

ピボットメニューは、新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス（AMP for Endpoints、Cisco Umbrella、Cisco Talos Intelligence など）の観測対象をピボットし、攻撃分析に関する調査を行うために使用します。詳細については、<https://visibility.amp.cisco.com/#/help/pivot-menus> で Cisco Threat Response ドキュメントを参照してください。

コンテンツセキュリティ管理アプライアンスで、ケースブックとピボットメニューのウィジェットが使用できるようになりました。[ケースブック (Casebook)] ウィジェットと [ピボットメニュー (Pivot Menu)] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。

- 観測対象をケースブックに追加し、脅威分析の調査を実行します。



- 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス（エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など）の監視対象をピボットし、脅威分析のために調査します。

次にこのリリースでサポートされている観測対象のリストを示します。

- IP アドレス
- ドメイン
- URL
- ファイルハッシュ（SHA-256 のみ）



- (注)
- ピボットメニュー ウィジェットは、アプライアンスの電子メール レポートおよび Web レポート ページの観測対象の横にあります。
  - ケースブック ウィジェットは、アプライアンスの電子メール レポート、Web レポート、および Web トラッキング ページの右下隅にあります。

#### 関連トピック

- [クライアント ID およびクライアント パスワード クレデンシャルの取得](#)（465 ページ）
- [攻撃分析のケースブックへ観測対象を追加](#)（467 ページ）

## クライアント ID およびクライアント パスワード クレデンシャルの取得

アプライアンスのケースブックとピボットメニュー ウィジェットにアクセスするには、クライアント ID とクライアント パスワードが必要です。

#### 始める前に

次の「は始める前に」セクションに記載されているすべての前提条件を満たしていることを確認してください。 [Cisco Threat Response ポータルへのアプライアンスの統合](#)（459 ページ）

**ステップ 1** アプライアンスの新しい Web インターフェイスにログインします。詳細については、[Web インターフェイスへのアクセス](#)（12 ページ）を参照してください。

**ステップ 2** [ケースブック (Casebook)]  ボタンをクリックします。

**ステップ 3** 新しい API クライアントを追加します。

- a) [Threat Response APIクライアント (Threat Response API Clients)] リンクをクリックします。

[Threat Response APIクライアント (Threat Response API Clients)] リンクをクリックすると、Cisco Threat Response ポータル ログイン ページにリダイレクトされます。

- b) Cisco Threat Response ポータルにログインします。
- c) [APIクレデンシャルの追加 (Add API Credentials)] をクリックします。
- d) アプライアンスの名前 (「Management\_Appliance」など) をクライアント名として入力します。
- e) ケースブックとピボットメニューウィジェットへのフルアクセスを付与する次のスコープを選択します。

- ケースブック (Casebook)
- 強化 (Enrich)
- プライベート インテリジェンス (Private Intelligence)
- 応答 (Response)
- 検査 (Inspect)

- (注)
- ケースブック ウィジェットにのみアクセスする場合は、[ケースブック (Casebook)]、[プライベートインテリジェンス (Private Intelligence)]、および [検査 (Inspect)] をスコープとして選択します。
  - ピボットメニューウィジェットにのみアクセスする場合は、[強化 (Enrich)] および [応答 (Response)] をスコープとして選択します。

- f) [新しいクライアントの追加 (Add New Client)] をクリックします。
- g) クライアント ID とクライアント パスワードをクリップボードにコピーします。

- (注) [新しいクライアントの追加 (Add New Client)] ダイアログ ボックスを閉じる前に、クライアント ID とクライアント パスワードをメモしてください。


- h) [閉じる (Close)] をクリックします。

- (注) 新しい API クライアントを追加する場合は、既存の API クライアントを削除する必要はありません。

**ステップ 4** アプライアンスの [ログインしてケースブック/ピボットメニューを使用 (Login to use Casebook/Pivot Menu)] ダイアログ ボックスのステップ 3 で取得したクライアント ID とクライアントパスワードを入力します。

**ステップ 5** [ログインしてケースブック/ピボットメニューを使用 (Login to use Casebook/Pivot Menu)] ダイアログ ボックスで必要な Cisco Threat Response サーバを選択します。

**ステップ 6** [認証 (Authenticate)] をクリックします。

- (注) クライアント ID、クライアント パスワード、および Cisco Threat Response サーバを編集する場合は、[ケースブック (Casebook)]  ボタンを右クリックして詳細を追加します。


### 次のタスク

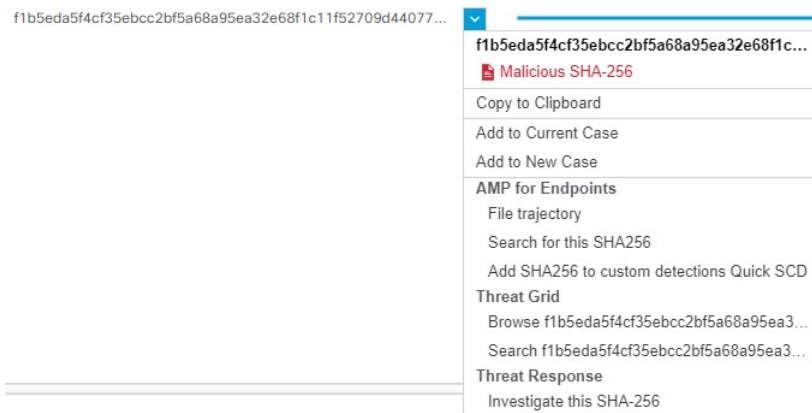
観測対象をケースブックに追加し、攻撃分析の調査を実行します。「[攻撃分析のケースブックへ観測対象を追加 \(467 ページ\)](#)」を参照してください。



## 攻撃分析のケースブックへ観測対象を追加


### 始める前に


アプライアンスのケースブックとピボットメニュー ウィジェットにアクセスするには、クライアント ID とクライアントパスワードを取得します。詳細については、[クライアント ID およびクライアントパスワードクレデンシャルの取得 \(465 ページ\)](#) を参照してください。

- ステップ 1** アプライアンスの新しい Web インターフェイスにログインします。詳細については、[Web インターフェイスへのアクセス \(12 ページ\)](#) を参照してください。
- ステップ 2** [メールレポート (Email Reporting)] または [Web レポート (Web Reporting)] ページへ移動して、該当する観測対象 (bit.ly など) の横にあるピボットメニュー  ボタンをクリックし、[新しいケースに追加 (Add to New Case)] または [現在のケースに追加 (Add to Current Case)] をクリックします。



- (注)
- 観測対象の横にあるドラッグアンドドロップ  ボタンを使用して、観測対象を既存のケースへドラッグアンドドロップします。
  - ピボットメニュー  ボタンを使用して、ポータルに登録された他のデバイスの観測対象 (AMP for Endpoints など) をピボットし、攻撃分析の調査を実行します。

**ステップ 3** [ケースブック (Casebook)]  ボタンをクリックして、観測対象が新しいまたは既存のケースに追加されたかを確認します。

**ステップ 4** (オプション)  ボタンをクリックして、タイトル、説明、またはメモをケースブックに追加します。

**ステップ 5** [このケースを調査 (Investigate this Case) ] をクリックして、攻撃分析の観測対象を調査します。詳細については、<https://visibility.amp.cisco.com/#/help/introduction> で Cisco Threat Response ドキュメントを参照してください。

---



## 第 15 章

# 管理タスクの分散

この章は、次の項で構成されています。

- [管理タスクの分散について](#) (469 ページ)
- [ユーザ ロールの割り当て](#) (469 ページ)
- [\[ユーザ \(Users\) \] ページ](#) (480 ページ)
- [管理ユーザの認証について](#) (481 ページ)
- [セキュリティ管理アプライアンスへのアクセスに対する追加の制御](#) (494 ページ)
- [メッセージトラッキングでの機密情報へのアクセスの制御](#) (498 ページ)
- [管理ユーザ向けメッセージの表示](#) (499 ページ)
- [管理ユーザ アクティビティの表示](#) (499 ページ)
- [管理ユーザ アクセスのトラブルシューティング](#) (501 ページ)

## 管理タスクの分散について

ユーザ アカウントに割り当てたユーザ ロールに基づいて、他のユーザに Cisco コンテンツ セキュリティ管理仮想アプライアンスの管理タスクを分散できます。

管理タスクが分散されるように設定するには、事前定義されたユーザ ロールがニーズを満たしているかどうかを判断して、必要なカスタムユーザ ロールを作成します。次に、セキュリティアプライアンスでローカルに管理ユーザの認証を行う、および（または）独自の中央集中型の LDAP や RADIUS システムを使用して外部で管理ユーザの認証を行うようにアプライアンスを設定します。

さらに、アプライアンスおよびアプライアンス上の特定の情報へのアクセスに追加の制御を指定できます。

## ユーザ ロールの割り当て

- [事前定義済みユーザ ロール](#) (470 ページ)
- [カスタムユーザ ロール](#) (473 ページ)

隔離アクセスには追加設定が必要です。「[隔離へのアクセス \(480ページ\)](#)」を参照してください。

## 事前定義済みユーザ ロール

特記のない限り、次の表で説明されている権限を持つ事前設定ユーザ ロール、またはカスタムユーザ ロールを各ユーザに割り当てることができます。

表 77: ユーザ ロールの説明

| ユーザ ロール名 | 説明                                                                                                                                                                                                                                                                                                                                                     | Web レポートニング/スケジュール設定されたレポート機能 |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| admin    | <p><b>admin</b> ユーザはシステムのデフォルトユーザアカウントであり、すべての管理権限を持っています。便宜上、<b>admin</b> ユーザアカウントをここに記載しましたが、これはユーザロールを使用して割り当てることができず、パスワードの変更以外、編集や削除もできません。</p> <p><b>resetconfig</b> コマンドと <b>revert</b> コマンドを発行できるのは、<b>admin</b> ユーザだけです。</p>                                                                                                                  | はい/はい                         |
| 管理者      | Administrator ロールを持つユーザアカウントはシステムのすべての設定に対する完全なアクセス権を持っています。                                                                                                                                                                                                                                                                                           | はい/はい                         |
| オペレータ    | <p>Operator ロールを持つユーザアカウントは次のことができません。</p> <ul style="list-style-type: none"> <li>ユーザアカウントの作成または編集</li> <li>アプライアンスのアップグレード</li> <li><b>resetconfig</b> コマンドの発行</li> <li>システム セットアップ ウィザードの実行</li> <li>ユーザ名とパスワード以外の LDAP サーバプロファイル設定の変更 (LDAP が外部認証に対して有効になっている場合)。</li> <li>隔離の設定、編集、削除、または集約。</li> </ul> <p>これら以外は、Administrator ロールと同じ権限を持ちます。</p> | はい/はい                         |

| ユーザ ロール名          | 説明                                                                                                                                                                                                                                                                                                                                                | Web レポートिंग/スケジュール設定されたレポート機能                              |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Technician        | Technician ロールを持つユーザ アカウントは、アップグレードおよびリブート、アプリケーションからのコンフィギュレーションファイルの保存、機能キーの管理などのシステム管理アクティビティを開始できます。                                                                                                                                                                                                                                          | [ウェブ (Web) ]および [電子メール (Email) ] タブのシステム キャパシティ レポートへのアクセス |
| オペレータ (読み取り専用)    | <p>Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために大部分の変更を行って送信できますが、保存できません。または保存を必要としない変更を行うことができます。このロールのユーザは、アクセスが有効の場合、隔離内のメッセージを管理できます。</p> <p>このロールのユーザは、以下にはアクセスできません。</p> <ul style="list-style-type: none"> <li>• ファイル システム、FTP、SCP。</li> <li>• 隔離を作成、編集、削除、または集中管理するための設定。</li> </ul> | はい/いいえ                                                     |
| Guest             | <p>Guest ロールを持つユーザ アカウントは、アクセス権限が有効であれば、レポートおよび Web トラッキングを含むステータス情報を表示し、隔離内のメッセージを管理できます。Guest ロールを持つユーザはメッセージトラッキングにアクセスできません。</p>                                                                                                                                                                                                              | はい/いいえ                                                     |
| Web Administrator | Web Administrator ロールを持つユーザ アカウントは、[ウェブ (Web) ] タブに表示されるすべての設定に対するアクセス権を持ちます。                                                                                                                                                                                                                                                                     | はい/はい                                                      |

| ユーザ ロール名                               | 説明                                                                                                                                                                                                                                          | Web レポートニング/スケジュール設定されたレポート機能 |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Web ポリシー管理者 (Web Policy Administrator) | Web Policy Administrator ロールを持つユーザアカウントは、[Webアプライアンスステータス (Web Appliance Status) ] ページと、Configuration Master のすべてのページにアクセスできます。Web ポリシー管理者は、ID、アクセス ポリシー、暗号化ポリシー、ルーティング ポリシー、プロキシバイパス、カスタム URL カテゴリ、および時間範囲を設定できます。Web ポリシー管理者は、設定を公開できません。 | いいえ/いいえ                       |
| メール管理者 (Email Administrator)           | Email Administrator ロールを持つユーザアカウントは、隔離など、[メール (Email) ] メニューにあるすべての設定へのアクセス権のみを持ちます。                                                                                                                                                        | いいえ/いいえ                       |
| ヘルプ デスク ユーザ                            | ヘルプ デスク ユーザ ロールを持つユーザがアクセスできるのは次のものに制限されます。 <ul style="list-style-type: none"> <li>• メッセージ トラッキング</li> <li>• 隔離内のメッセージ管理</li> </ul> このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。ユーザにこのロールを割り当てた後、このユーザがアクセスできるように隔離を設定する必要があります。              | いいえ/いいえ                       |



| ユーザロール名  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Web レポートिंग/スケジュール設定されたレポート機能 |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| カスタム ロール | <p>カスタム ユーザ ロールに割り当てられているユーザアカウントは、ポリシー、機能、またはこのロールに特に与えられた特定のポリシーまたは機能インスタンスに対してのみ、表示および設定を行えます。</p> <p>新しい Custom Email User ロールまたは新しい Custom Web User ロールは、[ローカルユーザの追加 (Add Local User)] ページから作成できます。ただし、ロールを使用できるようにするには、このカスタム ユーザ ロールに権限を割り当てる必要があります。権限を割り当てるには、[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [ユーザロール (User Roles)] に移動して、ユーザ名をクリックします。</p> <p>(注) Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。</p> <p>詳細については、<a href="#">カスタムユーザロール (473 ページ)</a> を参照してください。</p> | いいえ/いいえ                       |

## カスタムユーザロール

Administration 権限を持つユーザは、セキュリティ管理アプライアンスを使用してカスタムロールに管理権限を委任できます。カスタムロールは、事前定義されたユーザロールよりも、ユーザのアクセス権に対して柔軟な制御を行えます。

カスタム ユーザ ロールを割り当てたユーザは、アプライアンス、機能、またはエンドユーザのサブセットに関して、ポリシーの管理またはレポートへのアクセスを行えます。たとえば、別の国にある組織の支社では、許容可能な使用ポリシーが組織の本社とは異なっている場合に、Web サービスに関して委任を受けた管理者に、支社のポリシーの管理を許可できます。カスタム ユーザ ロールを作成して、それらのロールにアクセス権を割り当てることで、管理を委任します。委任された管理者が表示および編集できるポリシー、機能、レポート、カスタム URL カテゴリなどを決定します。

詳細については、以下を参照してください。

- [Custom Email User ロールについて \(474 ページ\)](#)
- [カスタム ユーザ ロールの削除 \(480 ページ\)](#)

## Custom Email User ロールについて

カスタムロールを割り当てると、委任された管理者がセキュリティ管理アプライアンスにある次の項目にアクセスすることを許可できます。

- すべてのレポート（オプションでレポーティンググループによって制限）
- メールポリシーレポート（オプションでレポーティンググループによって制限）
- DLP レポート（オプションでレポーティンググループによって制限）
- メッセージトラッキング
- 隔離

これらの各項目の詳細については、以下のセクションで説明します。また、これらの権限を付与されたすべてのユーザは、[管理アプライアンス（Management Appliance）] タブ > [集約管理サービス（Centralized Services）] メニューを使用して、[システムステータス（System Status）] を表示できます。Custom Email User ロールに割り当てられているユーザは、CLI にアクセスできません。



- (注) Eメールセキュリティアプライアンスのカスタムユーザロールは、セキュリティ管理アプライアンスのユーザロールよりも、より詳細なアクセス権を提供します。たとえば、メールおよびDLPポリシーと、コンテンツフィルタへのアクセス権を委任できます。詳細については、お使いのEメールセキュリティアプライアンスのマニュアルまたはオンラインヘルプの「Common Administration」の章の「Managing Custom User Roles for Delegated Administration」の項を参照してください。

### 電子メールレポーティングへのアクセス

次のセクションで説明するように、電子メールレポートへのアクセス権をカスタムユーザロールに付与できます。

セキュリティ管理アプライアンスの[電子メールセキュリティモニタ（Email Security Monitor）] ページの詳細については、[中央集中型の電子メールセキュリティレポーティングの使用（55ページ）](#)の該当する章を参照してください。

#### すべてのレポート

カスタムロールにすべてのレポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべてのEメールセキュリティアプライアンス、または選択したレポーティンググループのいずれかに対する、次の[電子メールセキュリティモニタ（Email Security Monitor）] ページを表示できます。

- メールフロー概要
- メールフローの詳細
- 送信先
- ユーザメールの概要

- DLP インシデント
- コンテンツ フィルタ
- ウイルス フィルタリング
- TLS 暗号化
- スケジュール設定されたレポート (Scheduled Reports)
- アーカイブ レポート (Archived Reports)

### メール ポリシー レポート

カスタム ロールにメール ポリシー レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての E メールセキュリティ アプライアンス、または選択したレポート グループのいずれかに対する、次の [電子メールセキュリティ モニタ (Email Security Monitor) ] ページを表示できます。

- メール フロー 概要
- メール フローの詳細
- 送信先
- ユーザ メール の概要
- コンテンツ フィルタ
- ウイルス フィルタリング
- アーカイブ レポート (Archived Reports)

### DLP レポート

カスタム ロールに DLP レポートへのアクセス権を付与すると、このロールを割り当てられたユーザは、すべての E メールセキュリティ アプライアンス、または選択したレポート グループのいずれかに対する、次の [電子メールセキュリティ モニタ (Email Security Monitor) ] ページを表示できます。

- DLP インシデント
- アーカイブ レポート (Archived Reports)

### メッセージトラッキングデータへのアクセス

カスタム ロールにメッセージトラッキングへのアクセス権を付与すると、このロールを割り当てられたユーザは、セキュリティ管理アプライアンスによってトラッキングされたすべてのメッセージのステータスを表示できます。

DLP ポリシーに違反するメッセージ内の機密情報へのアクセスを制御するには、[メッセージトラッキングでの機密情報へのアクセスの制御 \(498 ページ\)](#) を参照してください。

セキュリティ管理アプライアンスでメッセージトラッキングへのアクセスを有効にするためのアプライアンスの設定方法など、メッセージトラッキングの詳細については、[メッセージのトラッキング \(299 ページ\)](#) を参照してください。

### カスタム ユーザ ロールの隔離へのアクセス

カスタムロールに隔離へのアクセス権を付与すると、このロールを割り当てられたユーザは、このセキュリティ管理アプライアンスのすべての隔離メッセージを検索、表示、リリース、または削除できます。

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。「[隔離へのアクセス \(480 ページ\)](#)」を参照してください。

### Custom Email User ロールの作成

電子メール レポート、メッセージトラッキング、および隔離へのアクセスに対して、カスタムのメール ユーザ ロールを作成できます。

これらの各オプションに許可されたアクセス権の詳細については、[Custom Email User ロールについて \(474 ページ\)](#) とそのサブセクションを参照してください。



(注) より詳細なアクセス権、または他の機能、レポート、ポリシーへのアクセス権を付与するには、各 E メールセキュリティ アプライアンスで直接カスタム ユーザ ロールを作成してください。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ユーザロール (User Roles) ]を選択します。

**ステップ 3** [メールユーザ役割の追加 (Add Email User Role) ]をクリックします。

**ヒント** または、既存の Email User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複 (Duplicate) ] アイコンをクリックし、生成されたコピーを編集します。

**ステップ 4** ユーザ ロールの一意の名前 (たとえば「dlp-auditor」) と説明を入力します。

- Email と Web のカスタム ユーザ ロール名を同じにしないでください。
- 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュまたは数字にすることはできません。
- このロールのユーザに集約ポリシー隔離へのアクセス権を許可し、このロールのユーザが E メールセキュリティアプライアンスのメッセージフィルタやコンテンツ フィルタおよび DLP メッセージアクション内にもこれらの集約隔離を指定できるようにする場合、カスタム ロールの名前を両方のアプライアンスで同じにする必要があります。

- ステップ 5** このロールに対してイネーブルにするアクセス権限を選択します。
- ステップ 6** [送信 (Submit) ] をクリックして [ユーザ ロール (User Roles) ] ページに戻ると、新しいユーザ ロールが表示されます。
- ステップ 7** レポートिंग グループごとにアクセス権を制限する場合は、該当するユーザ ロールの [メールレポート (Email Reporting) ] 列にある [グループが選択されていません (no groups selected) ] リンクをクリックして、少なくとも 1 つのレポートング グループを選択します。
- ステップ 8** 変更を保存します。
- ステップ 9** このロールに隔離へのアクセス権を付与する場合は、このロールに対してアクセス権を有効にします。
- 参照先 :

- [スパム隔離への管理ユーザ アクセスの設定 \(326 ページ\)](#)
- [ポリシー、ウイルス、およびアウトブレイク隔離の設定 \(370 ページ\)](#)

## Custom Email User ロールの使用

Custom Email User ロールに割り当てられているユーザがアプライアンスにログインすると、そのユーザには、ユーザがアクセス権を持つセキュリティ機能へのリンクだけが表示されます。そのユーザは、[オプション (Options) ] メニューで [アカウント権限 (Account Privileges) ] を選択することで、いつでもこのメインページに戻ることができます。これらのユーザは、Web ページの上部にあるメニューを使用して、アクセス権を持つ機能にアクセスすることもできます。次の例では、ユーザは Custom Email User ロールによって、セキュリティ管理アプライアンスで使用可能なすべての機能へのアクセス権を持ちます。

図 11 : Custom Email User ロールが割り当てられている委任管理者の [アカウント権限 (Account Privileges) ] ページ

Logged in as: **full-access** on **example.com**  
Options ▾ Help and Support ▾

### Account Privileges (full-access)

|                         |                                                                                           |
|-------------------------|-------------------------------------------------------------------------------------------|
| <b>Email Reporting</b>  | Mail Policy Reports from all Email Appliances<br><i>View and analyze email traffic.</i>   |
| <b>Message Tracking</b> | Message Tracking<br><i>Track messages.</i>                                                |
| <b>Quarantines</b>      | Manage messages in the Spam Quarantine<br><i>Manage messages in assigned Quarantines.</i> |

## Custom Web User ロールについて

Custom Web User ロールでは、ユーザがポリシーを別の Web セキュリティ アプライアンスに公開することができ、カスタム設定を編集したり、別のアプライアンスに公開できるようになります。

セキュリティ管理アプライアンスの [ウェブ (Web)] > [設定マスター (Configuration Master)] > [カスタム URL カテゴリ (Custom URL Categories)] ページでは、管理および公開できる URL カテゴリとポリシーを表示できます。また、[ウェブ (Web)] > [ユーティリティ (Utilities)] > [今すぐ設定を公開する (Publish Configuration Now)] ページに移動して、可能な設定を表示することもできます。



- (注) 公開権限を持つカスタムロールを作成した場合、ユーザがログインすると、使用可能なメニューが表示されないことに注意してください。URL やポリシー タブが機能を持たないため、このようなユーザには公開メニューが表示されず、編集不可の固定画面が表示されます。これは、ご使用のユーザでは、カテゴリまたはポリシーの公開および管理ができないということです。この問題の回避策としては、ユーザが公開はできるが、どのカテゴリまたはポリシーも管理できないようにする場合、どのポリシーでも使用されていないカスタムカテゴリを作成し、そのユーザに、そのカスタムカテゴリを管理する権限と公開する権限を付与する必要があります。このようにすると、ユーザがそのカテゴリで URL を追加または削除しても、他に影響が及びません。

カスタム ユーザ ロールを作成および編集して、Web 管理を委任できます。

- [Custom Web User ロールの作成 \(478 ページ\)](#)
- [Custom Web User ロールの編集 \(479 ページ\)](#)
- [カスタム ユーザ ロールの削除 \(480 ページ\)](#)

## Custom Web User ロールの作成

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザロール (User Roles)] を選択します。
- ステップ 3** [Web ユーザ役割の追加 (Add Web User Role)] をクリックします。
- ヒント** または、既存の Web User ロールを複製して、新しいロールを作成できます。それには、該当するテーブルの行で [重複 (Duplicate)] アイコンをクリックし、生成されたコピーを編集します。
- ステップ 4** ユーザ ロールの一意的な名前 (たとえば「canadian-admins」) と説明を入力します。

- (注) 名前には、小文字、数字、およびダッシュのみを使用してください。先頭をダッシュにすることはできません。

**ステップ5** デフォルトで、ポリシーとカスタム URL カテゴリを表示するか、非表示にするかを選択します。

**ステップ6** 公開権限をオンにするか、オフにするかを選択します。

この権限を持つユーザは、ユーザがアクセス ポリシーまたは URL カテゴリを編集できるすべての Configuration Master を公開できます。

**ステップ7** 新しい（空の）設定で始めるか、既存のカスタムユーザロールをコピーするかを選択します。既存のユーザロールをコピーする場合は、コピーするロールをリストから選択します。

**ステップ8** [送信 (Submit)] をクリックして [ユーザロール (User Roles)] ページに戻ると、新しいユーザロールが表示されます。

(注) Web レポートで匿名機能をイネーブルにしていた場合、Web レポートへのアクセス権を持つすべてのユーザロールには、インタラクティブなレポートページで認識できないユーザ名とロールが表示されるようになります。[中央集中型 Web レポートおよびトラッキングの使用 \(191 ページ\)](#) の章の [Web レポートのスケジュール設定 \(273 ページ\)](#) のセクションを参照してください。Administrator ロールの場合には例外的に、スケジュール設定されたレポートで実際のユーザ名を確認できます。匿名機能がイネーブルになっている場合、オペレータおよび Web 管理者によって作成されたスケジュール設定されたレポートは匿名になります。

[Web] > [ユーティリティ (Utilities)] > [セキュリティ (Security)] > [サービス表示 (Services Display)] > [セキュリティサービス表示の編集 (Edit Security Services Display)] ページを使用して設定マスターの1つを非表示にしている場合、[ユーザロール (User Roles)] ページでも対応する [設定マスター (Configuration Master)] 列が非表示になりますが、非表示になっている設定マスターに対する権限設定は保持されます。

---

## Custom Web User ロールの編集

---

**ステップ1** [ユーザロール (User Roles)] ページでロール名をクリックし、[ユーザロールの編集 (Edit User Role)] ページを表示します。

**ステップ2** 名前、説明、およびポリシーとカスタム URL カテゴリを表示するかどうかなどの設定を編集します。

**ステップ3** [送信 (Submit)] をクリックします。

カスタムユーザロールの権限を編集するには、次の手順を実行します。

[ユーザロール (User Roles)] ページに移動します。

- アクセスポリシー権限を編集するには、[アクセスポリシー (Access policies)] をクリックして、Configuration Master に設定されているアクセスポリシーのリストを表示します。[含める (Include)] 列で、ユーザ編集アクセス権を付与するポリシーのチェックボックスをオンにします。[送信 (Submit)] をクリックして、[ユーザロール (User Roles)] ページに戻ります。

または

- カスタム URL カテゴリ権限を編集するには、カスタム URL カテゴリをクリックして、Configuration Master に定義されているカスタム URL カテゴリのリストを表示します。[含める (Include)] 列で、

ユーザ編集アクセス権を付与するカスタム URL カテゴリのチェックボックスをオンにします。[送信 (Submit)] をクリックして、[ユーザロール (User Roles)] ページに戻ります。

## カスタム ユーザ ロールの削除

1人以上のユーザに割り当てられているカスタムユーザロールを削除する場合、エラーは受信しません。

## CLI へのアクセス権を持つユーザ ロール

一部のロール (Administrator、Operator、Guest、Technician、および Read-Only Operator) は、GUI と CLI の両方にアクセスできます。他のロール (ヘルプデスク ユーザ、メール管理者、Web 管理者、Web ポリシー管理者、URL フィルタリング管理者 (Web セキュリティ)、およびカスタム ユーザ) は GUI だけにアクセスできます。

## LDAP の使用

ユーザを認証するために LDAP ディレクトリを使用する場合は、個々のユーザではなくユーザロールにディレクトリ グループを割り当てます。ユーザロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザロールで定義された権限を受け取ります。詳細については、[外部ユーザ認証 \(490 ページ\)](#) を参照してください。

## 隔離へのアクセス

ユーザが隔離にアクセスする前にそのアクセスを有効にする必要があります。次の情報を参照してください。

- [スパム隔離への管理ユーザ アクセスの設定 \(326 ページ\)](#)
- [メッセージ処理タスクの他のユーザへの割り当てについて \(377 ページ\)](#) (ポリシー隔離の場合)、および [ポリシー、ウイルス、およびアウトブレイク隔離の設定 \(370 ページ\)](#)
- [カスタム ユーザ ロールの集約隔離アクセスの設定 \(366 ページ\)](#)。

## [ユーザ (Users)] ページ

| 次のセクションの詳細について                       | 参照先                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------|
| Users                                | <a href="#">管理タスクの分散について (469 ページ)</a>                                                              |
| [パスワードのリセット (Reset Passphrases)] ボタン | <a href="#">ローカルに定義された管理ユーザの管理 (482 ページ)</a><br><a href="#">ユーザに対するオンデマンドでのパスワード変更の要求 (488 ページ)</a> |



| 次のセクションの詳細について                                                    | 参照先                                                  |
|-------------------------------------------------------------------|------------------------------------------------------|
| ローカルユーザアカウントとパスフレーズの設定 (Local User Account & Passphrase Settings) | <a href="#">パスフレーズの設定およびログインの要件 (484 ページ)</a>        |
| 外部認証 (External Authentication)                                    | <a href="#">外部ユーザ認証 (490 ページ)</a>                    |
| DLPトラッキング権限 (DLP Tracking Privileges)                             | <a href="#">メッセージトラッキングでの機密情報へのアクセスの制御 (498 ページ)</a> |

## 管理ユーザの認証について

認可されたユーザをアプライアンスでローカルに定義したり、外部認証を使用したりすることで、アプライアンスに対するアクセスを制御できます。

- [admin ユーザのパスフレーズの変更 \(481 ページ\)](#)
- [有効期限後のユーザパスフレーズの変更 \(482 ページ\)](#)
- [ローカルに定義された管理ユーザの管理 \(482 ページ\)](#)
- [外部ユーザ認証 \(490 ページ\)](#)

## admin ユーザのパスフレーズの変更

管理者レベルのユーザは、GUI または CLI を使用して「admin」ユーザのパスフレーズを変更できます。



(注) 初めてアプライアンスにログインするか、設定を出荷時の初期設定にリセットする場合、パスフレーズを変更することをお勧めします。

GUI を使用してパスフレーズを変更するには、次の手順を実行します。

- (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザ (Users)] ページを選択し、管理者ユーザを選択します。

admin ユーザのパスフレーズを CLI から変更するには、`passphrase` コマンドを使用します。`passphrase` コマンドでは、セキュリティのために古いパスフレーズの入力が必要です。

「admin」ユーザアカウントのパスフレーズを忘れた場合は、パスフレーズをリセットするためにカスタマー サポート プロバイダーにご連絡ください。



---

(注) パスフレーズの変更はすぐに有効になり、変更の確定は必要ではありません。

---

## 有効期限後のユーザ パスフレーズの変更

アカウントの有効期限が切れると、「お使いのパスフレーズは有効期限が切れています。変更してください、パスフレーズは、ここをクリックしています。」

リンクをクリックして、期限切れのパスフレーズでログインの詳細を入力し、[パスフレーズの変更 (Change Passphrase)] ページに進みます。のパスワードの設定の詳細については [パスフレーズの設定およびログインの要件 \(484 ページ\)](#)。



---

(注) パスフレーズの変更はすぐに有効になり、変更の確定は必要ではありません。

---

## ローカルに定義された管理ユーザの管理

- [ローカルに定義されたユーザの追加 \(482 ページ\)](#)
- [ローカルに定義されたユーザの編集 \(483 ページ\)](#)
- [ローカルに定義されたユーザの削除 \(483 ページ\)](#)
- [ローカルに定義されたユーザのリストの表示 \(484 ページ\)](#)
- [パスフレーズの設定と変更 \(484 ページ\)](#)
- [パスフレーズの設定およびログインの要件 \(484 ページ\)](#)
- [ユーザに対するオンデマンドでのパスフレーズ変更の要求 \(488 ページ\)](#)
- [ローカル ユーザ アカウントのロックおよびロック解除 \(489 ページ\)](#)

## ローカルに定義されたユーザの追加

外部認証を使用していない場合は、次の手順に従って、ユーザをセキュリティ管理アプライアンスに直接追加します。または、CLI で `userconfig` コマンドを使用します。



---

(注) 外部認証もイネーブルである場合は、ローカルユーザ名が外部認証されたユーザ名と重複しないことを確認してください。

---

アプライアンスに作成できるユーザ アカウントの数に制限はありません。

---

**ステップ 1** カスタムユーザロールを割り当てる場合は、そのロールを先に定義しておくことを推奨します。 [カスタムユーザロール \(473 ページ\)](#) を参照してください。

- ステップ 2** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 3** [管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [ユーザ (Users) ] を選択します。
- ステップ 4** [ユーザの追加 (Add User) ] をクリックします。
- ステップ 5** ユーザの一意的名前を入力します。システムで予約されている語 (「operator」や「root」など) を入力することはできません。
- 外部認証も使用する場合は、ユーザ名を外部認証されたユーザ名と重複させることはできません。
- ステップ 6** ユーザの氏名を入力します。
- ステップ 7** 事前定義されたロールまたはカスタムロールを選択します。ユーザロールの詳細については、[事前定義済みユーザロール \(470 ページ\)](#) セクションの表「ユーザロールの説明」を参照してください。
- 新しい Email ロールまたは Web ロールをここに追加する場合は、ロールの名前を入力します。命名上の制限については、[Custom Email User ロールの作成 \(476 ページ\)](#) または [Custom Web User ロールの作成 \(478 ページ\)](#) を参照してください。
- ステップ 8** セキュリティ検証のために現在のパスワードを確認します。
- ステップ 9** パスワードを生成または入力して、確認のためにパスワードをもう一度入力します。
- ステップ 10** 変更を送信し、保存します。
- ステップ 11** このページにカスタムユーザロールを追加する場合は、この時点でそのロールに権限を割り当てます。「[カスタムユーザロール \(473 ページ\)](#)」を参照してください。

---

## ローカルに定義されたユーザの編集

たとえば、パスワードを変更するには、この手順を実行します。

- 
- ステップ 1** [ユーザ (Users) ] 一覧でユーザの名前をクリックします。
- ステップ 2** ユーザに対して変更を行います。
- ステップ 3** セキュリティ検証のために現在のパスワードを確認します。
- ステップ 4** 変更を送信し、保存します。

---

## ローカルに定義されたユーザの削除

- 
- ステップ 1** [ユーザ (Users) ] 一覧でユーザの名前に対応するゴミ箱アイコンをクリックします。
- ステップ 2** 表示される警告ダイアログで [削除 (Delete) ] をクリックして削除を確認します。
- ステップ 3** [確定する (Commit) ] をクリックして変更を保存します。
-

## ローカルに定義されたユーザのリストの表示

ローカルで定義されたユーザの一覧を表示するには、次の手順を実行します。

- (新しいWebインターフェイスのみ) クラウドEメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ユーザ (Users) ]を選択します。



(注) アスタリスクは、委任された管理に応じてユーザに割り当てられたカスタム ユーザ ロールを示します。ユーザのカスタム ロールが削除されている場合は、[未定義 (Unassigned) ]と赤く表示されます。カスタム ユーザ ロールの詳細については、[カスタムユーザロール \(473 ページ\)](#) を参照してください。

## パスフレーズの設定と変更

- ユーザを追加する場合は、そのユーザに初期パスフレーズを指定します。
- システムに設定されたユーザのパスフレーズを変更するには、GUIの[ユーザの編集 (Edit User) ]ページを使用します (詳細は、[ローカルに定義されたユーザの編集 \(483 ページ\)](#) を参照してください)。



(注) 初めてアプライアンスにログインする場合や、システム セットアップウィザードを完了した後は、パスフレーズを変更することをお勧めします。

- システムのデフォルト管理ユーザアカウントのパスフレーズを変更するには、[adminユーザのパスフレーズの変更 \(481 ページ\)](#) を参照してください。
- ユーザにパスフレーズの変更を強制するには、[ユーザに対するオンデマンドでのパスフレーズ変更の要求 \(488 ページ\)](#) を参照してください。
- GUI 右側上部の [オプション (Options) ]メニューをクリックして、[パスフレーズの変更 (Change Passphrase) ]オプションを選択することで、ユーザは自分のパスフレーズを変更できます。

## パスフレーズの設定およびログインの要件

ユーザアカウントとパスフレーズの制限を定義して、組織全体にパスフレーズ ポリシーを強制的に適用することができます。ユーザアカウントとパスフレーズの制限は、セキュリティ管理アプライアンスで定義されているローカルユーザに適用されます。次の設定値を設定できます。

- **ユーザアカウントのロック。**ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。
- **パスフレーズ存続期間のルール。**ログイン後にユーザがパスフレーズの変更を要求されるまでの、パスフレーズの存続期間を定義できます。
- **パスフレーズルール。**任意指定の文字や必須の文字など、ユーザが選択できるパスフレーズの種類を定義できます。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ユーザ (Users) ] を選択します。
- ステップ 3** [ローカルユーザアカウントとパスワードの設定 (Local Account and Passphrase Settings) ] セクションまで下にスクロールします。
- ステップ 4** [設定の編集 (Edit Settings) ] をクリックします。
- ステップ 5** 設定を次のように構成します。

| 設定                                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ユーザアカウントのロック (User Account Lock) ] | <p>ユーザが正常にログインできない場合に、ユーザアカウントをロックするかどうかを決定します。アカウントをロックすることになる失敗ログイン試行の回数を指定します。1 から 60 までの任意の数を入力できます。デフォルトは 5 です。</p> <p>アカウントのロックを設定する場合は、ログインを試みているユーザに表示するメッセージを入力します。テキストは 7 ビット ASCII 文字を使用して入力します。このメッセージは、ユーザがロックされているアカウントの正しいパスフレーズを入力した場合のみ表示されます。</p> <p>ユーザアカウントがロックされた場合、管理者は GUI で [ユーザの編集 (Edit User) ] ページを使用するか、userconfig CLI コマンドを使用してロックを解除できます。</p> <p>失敗したログインの試行は、ユーザが接続しているマシンや、接続のタイプ (SSH または HTTP など) に関係なく、ユーザ別に追跡されます。ユーザがログインに成功すると、失敗ログイン試行の回数は 0 にリセットされます。</p> <p>失敗ログイン試行の最大回数に達したためにユーザアカウントがロックアウトされると、管理者にアラートが送信されます。このアラートは「Info」重大度レベルに設定されます。</p> <p>(注) 個々のユーザアカウントを手動でロックすることもできます。<a href="#">手動によるユーザアカウントのロック (489 ページ)</a> を参照してください。</p> |

| 設定                                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスワードのリセット                            | <p>管理者がユーザのパスワードを変更した後で、ユーザにパスワードを強制的に変更させるかどうかを選択します。</p> <p>パスワードが期限切れになった後で、ユーザにパスワードを強制的に変更させるかどうかを選択することもできます。ユーザによるパスワードの変更が必要になるまでの、パスワードの有効日数を入力します。1 から 366 までの任意の数を入力できます。デフォルトは 90 です。スケジュール外の時間に、ユーザにパスワードの変更を強制するには、<a href="#">ユーザに対するオンデマンドでのパスワード変更の要求 (488 ページ)</a> を参照してください。</p> <p>期限切れ後にユーザにパスワードを強制的に変更させる場合は、次のパスワード期限に関する通知を表示できます。期限切れの何日前にユーザに通知するかを選択します。</p> <p>(注) ユーザアカウントがパスワードチャレンジの代わりに SSH キーを使用している場合でも、パスワードリセットルールが適用されます。SSH キーを使用しているユーザアカウントが期限切れになった場合、ユーザは古いパスワードを入力するか、アカウントに関連付けられているキーを変更するためにパスワードを手動で変更するよう管理者に依頼する必要があります。</p> |
| パスワードルール：<br><number> 文字以上にする必要があります。 | <p>パスワードに含める最小文字数を入力します。</p> <p>0 (ゼロ) から 128 までの数字を入力してください。</p> <p>デフォルトは 8 です。</p> <p>パスワードには、ここで指定した数より多い文字を使用できます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| パスワードルール：<br>数字(0~9)が1文字以上必要です。       | <p>パスワードに数字を少なくとも 1 文字含める必要があるかどうかを選択します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| パスワードルール：<br>特殊文字が1文字以上必要です。          | <p>パスワードに 1 文字以上の特殊文字を含める必要があるかどうかを決定します。パスワードには、次の特殊文字を使用できます。</p> <p>~?!@#\$%^&amp;*-_+=</p> <p>\/[]()&lt;&gt;{}`'"';:.,</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| 設定                                                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>パスワードルール：<br/>ユーザ名とその変形をパスワードとして使用することはできません。</p>          | <p>対応するユーザ名またはユーザ名の変形と同じものを、パスワードに使用できるかどうかを決定します。ユーザ名の変形の使用を禁止する場合、次のルールがパスワードに適用されます。</p> <ul style="list-style-type: none"> <li>• 大文字か小文字かに関係なく、パスワードはユーザ名と同じであってはならない。</li> <li>• 大文字か小文字かに関係なく、パスワードはユーザ名を逆にしたものと同じであってはならない。</li> <li>• パスワードは、次の文字置換が行われたユーザ名、またはユーザ名を逆にしたものと同じであってはならない。 <ul style="list-style-type: none"> <li>• 「a」の代わりに「@」または「4」</li> <li>• 「e」を「3」に置換</li> <li>• 「i」を「 」、「!」、または「1」に置換</li> <li>• 「o」を「0」に置換</li> <li>• 「s」を「\$」または「5」に置換</li> <li>• 「t」を「+」または「7」に置換</li> </ul> </li> </ul> |
| <p>パスワードルール：<br/>直近 &lt;number&gt; 個のパスワードを再使用することはできません。</p> | <p>ユーザにパスワードの変更を強制する場合に、最近使用したパスワードを選択できるかどうかを決定します。最近のパスワードの再使用を禁止する場合、再使用を禁止する最近のパスワードの個数を入力します。</p> <p>1 から 15 までの任意の数を入力できます。デフォルトは 3 です。</p>                                                                                                                                                                                                                                                                                                                                                                        |
| <p>パスワードルール：<br/>パスワードで許可しない単語の一覧</p>                         | <p>パスワードでの使用を禁止する単語のリストを作成できます。</p> <p>このファイルは、許可しない単語ごとに行を分けたテキストファイルにします。forbidden_passphrase_words.txt という名前でファイルを保存し、SCP や FTP を使用してアプライアンスにファイルをアップロードします。</p> <p>この制限を選択しても単語のリストをアップロードしないと、この制限は無視されます。</p>                                                                                                                                                                                                                                                                                                      |

| 設定       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスワードの強度 | <p>管理者またはユーザが新しいパスワードを入力するときに、パスワード強度インジケータを表示できます。</p> <p>この設定によって強固なパスワードが作成されるわけではありません。この設定は、入力したパスワードの推測されやすさを示すだけです。</p> <p>インジケータを表示する対象ロールを選択します。次に、選択したロールごとにゼロより大きい数字を入力します。数字が大きいほど、強力であるとして登録されるパスワードは推測されにくいことを意味します。この設定に最大値はありません。</p> <p>例：</p> <ul style="list-style-type: none"> <li>• 30 と入力した場合は、少なくとも 1 つの大文字と小文字、数字、特殊文字を含む 8 文字のパスワードが強力なパスワードとして登録されます。</li> <li>• 18 と入力した場合は、すべて小文字で数字と特殊文字を含まない 8 文字のパスワードが強固なパスワードとして登録されます。</li> </ul> <p>パスワードの強度は対数目盛で測定されます。評価は、NIST SP 800-63 付則 A の定義に準拠する、米国国立標準技術研究所のエントロピールールに基づいています。</p> <p>一般的に、強固なパスワードは次のような特徴を備えています。</p> <ul style="list-style-type: none"> <li>• 長い。</li> <li>• 大文字、小文字、数字、および特殊文字を含む。</li> <li>• あらゆる言語の辞書にある語を含まない。</li> </ul> <p>これらの特徴を備えたパスワードを適用するには、このページの他の設定を使用します。</p> |

**ステップ 6** 変更を送信し、保存します。

### 次のタスク

ユーザにパスワードを新しい要件を満たす新しいパスワードに変更するよう要求します。  
[ユーザに対するオンデマンドでのパスワード変更の要求 \(488 ページ\)](#) を参照してください

## ユーザに対するオンデマンドでのパスワード変更の要求

すべての、または選択したユーザに、アドホックベースでパスワードを変更するように要求するには、次の手順を実行します。これは 1 回限りのアクションです。



パスフレーズを変更するための定期的な要求を自動化するには、[パスフレーズの設定およびログインの要件 \(484 ページ\)](#) で説明されている [パスワードのリセット (Passphrase Reset) ] オプションを使用します。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ユーザ (Users) ] を選択します。
- ステップ 3** [ユーザ (Users) ] セクションで、パスフレーズの変更が必要なユーザの横のチェック ボックスをオンにします。
- ステップ 4** [パスワードの変更を実施 (Enforce Passphrase Changes) ] を選択します。
- ステップ 5** オプションを選択します。
- 猶予期間のグローバル設定は [ローカルユーザアカウントとパスワードの設定 (Local User Account & Passphrase Settings) ] で設定します。
- ステップ 6** [OK] をクリックします。
- 

## ローカル ユーザ アカウントのロックおよびロック解除

ユーザ アカウントのロックは、ローカル ユーザがアプライアンスにログインするのを防止します。ユーザ アカウントは、次のいずれかの場合にロックされることがあります。

- すべてのローカル ユーザ アカウントを、設定した試行回数の後にユーザが正常なログインに失敗するとロックするように、設定することができます。[パスフレーズの設定およびログインの要件 \(484 ページ\)](#) を参照してください。
- 管理者はユーザアカウントを手動でロックできます。[手動によるユーザアカウントのロック \(489 ページ\)](#) を参照してください。

[ユーザの編集 (Edit User) ] ページでユーザアカウントを表示すると、AsyncOS によりユーザアカウントがロックされた理由が表示されます。

### 手動によるユーザ アカウントのロック

---

- ステップ 1** 初回のみ : アプライアンスを設定して、ユーザ アカウントのロックをイネーブルにします。
- ステップ 2**
- a) (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
  - b) [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ユーザ (Users) ] に移動します。
  - c) [ローカルユーザアカウントとパスワードの設定 (Local User Account & Passphrase Settings) ] セクションで、[設定の編集 (Edit Settings) ] をクリックします。

- d) [管理者が手動でユーザアカウントをロックした場合、ロックされたアカウントメッセージを表示します。(Display Locked Account Message if Administrator has manually locked a user account)] に対するチェックボックスを選択して、メッセージを入力します。
- e) 変更を送信します。

**ステップ 3** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザ (Users)] に移動して、ユーザ名をクリックします。

(注) admin アカウントをロックする前に、ロック解除できることを確認してください。[ユーザアカウントのロック解除 \(490 ページ\)](#) の (注) を参照してください。

**ステップ 4** [アカウントのロック (Lock Account)] をクリックします。

AsyncOS は、ユーザがアプライアンスにログインできなくなるというメッセージを表示し、継続するかどうかを問い合わせてきます。

## ユーザアカウントのロック解除

ユーザアカウントをロック解除するには、[ユーザ (Users)] 一覧でユーザ名をクリックしてユーザアカウントを開き、[アカウントのロック解除 (Unlock Account)] をクリックします。



(注) admin アカウントをロックした場合は、シリアルコンソールポートへのシリアル通信接続経由で admin としてログインしてロック解除するしかありません。admin ユーザは、admin アカウントがロックされた場合でも、シリアルコンソールポートを使用して常にアプライアンスにアクセスできます。シリアルコンソールポートを使用してアプライアンスにアクセスする方法の詳細については、お使いの E メールセキュリティアプライアンスのマニュアルまたはオンラインヘルプの「Setup and Installation」の章を参照してください。

## 外部ユーザ認証

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するようセキュリティ管理アプライアンスを設定できます。



(注) [ビューのカスタマイズ \(581 ページ\)](#) で説明されている一部の機能は、外部認証ユーザには使用できません。

- 展開でローカル認証と外部認証の両方を使用している場合、ローカルユーザ名と外部認証ユーザ名を同じにしないでください。
- アプライアンスが外部ディレクトリと通信できない場合、外部アカウントとローカルアカウントの両方を持つユーザは、ローカルユーザアカウントを使用してアプライアンスにログインできます。

参照先：

- [LDAP を使用した管理ユーザの外部認証の設定](#) (448 ページ)
- [RADIUS 認証の有効化](#) (491 ページ)

## LDAP 認証の設定

LDAP 認証を設定するには、[LDAP を使用した管理ユーザの外部認証の設定](#) (448 ページ) を参照してください。

## RADIUS 認証の有効化

ユーザを認証し、アプライアンスを管理しているユーザ ロールにユーザ グループを割り当てるために RADIUS ディレクトリを使用できます。RADIUS サーバは CLASS 属性をサポートする必要があります (AsyncOS は RADIUS ディレクトリのユーザをユーザ ロールに割り当てるために CLASS 属性を使用します)。



(注) 外部ユーザが RADIUS グループのユーザ ロールを変更する場合は、アプライアンスからログアウトして再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

### 始める前に

RADIUS サーバへの共有シークレット キーの長さは 48 文字以下でなければなりません。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザ (Users)] ページを選択して、[有効化 (Enable)] をクリックします。
- ステップ 3** [外部認証を有効にする (Enable External Authentication)] チェックボックスをオンにします。
- ステップ 4** 認証タイプとして RADIUS を選択します。
- ステップ 5** RADIUS サーバのホスト名を入力します。
- ステップ 6** RADIUS サーバのポート番号を入力します。デフォルト ポート番号は、1812 です。
- ステップ 7** RADIUS サーバの共有シークレット キーを入力します。

(注) E メールセキュリティアプライアンスのクラスタに対して外部認証を有効にするには、クラスタ内のすべてのアプライアンスで同じ共有シークレット キーを入力します。
- ステップ 8** タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。
- ステップ 9** 認証プロトコルとして、パズフレーズ認証プロトコル (PAP) を使用するか、またはチャレンジハンドシェイク認証プロトコル (CHAP) を使用するか選択します。
- ステップ 10** (任意) [行の追加 (Add Row)] をクリックして別の RADIUS サーバを追加します。認証のためにアプライアンスで使用する各 RADIUS サーバに対してステップ 6 とステップ 7 を繰り返します。

複数の外部サーバを定義する場合、アプライアンスは、アプライアンスに定義されている順序でサーバに接続します。1つのサーバが一時的に使用できない場合、フェールオーバーを実行できるように、複数の外部サーバを定義する場合があります。

**ステップ 11** Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

(注) RADIUSサーバがワンタイムパスワード（たとえば、トークンから作成されるパスワード）を使用する場合、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバに再アクセスしません。

**ステップ 12** グループ マッピングの設定

| 設定                                                                                                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[外部認証されたユーザを複数のローカルロールに割り当てます (推奨) (Map externally authenticated users to multiple local roles (Recommended) ) ]</p> | <p>AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件：</p> <ul style="list-style-type: none"> <li>• 3 文字以上</li> <li>• 253 文字以下</li> <li>• コロン、カンマ、または改行文字なし</li> <li>• 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性 (この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します)。</li> </ul> <p>複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。</p> <p>次のアプライアンス ロールは、制限の少ないものから順番に並べられています。</p> <ul style="list-style-type: none"> <li>• 管理者 (Administrator)</li> <li>• Email Administrator</li> <li>• Web Administrator</li> <li>• Web Policy Administrator</li> <li>• URL Filtering Administrator (Web セキュリティ)</li> <li>• カスタム ユーザ ロール (電子メールまたは Web)</li> </ul> <p>ユーザにカスタムユーザロールにマッピングされた複数のクラス属性が割り当てられている場合、RADIUS サーバのリストの最後のクラス属性が使用されます。</p> <ul style="list-style-type: none"> <li>• 専門技術者</li> <li>• 演算子</li> <li>• Read-Only Operator</li> <li>• ヘルプ デスク ユーザ</li> <li>• ゲスト</li> </ul> |

| 設定                                                                                                 | 説明                                              |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------|
| [外部認証されたすべてのユーザを管理者ロールに割り当てます (Map all externally authenticated users to the Administrator role) ] | AsyncOS は RADIUS ユーザを Administrator ロールに割り当てます。 |

**ステップ 13** (任意) [行の追加 (Add Row) ] をクリックして別のグループを追加します。アプライアンスが認証するユーザの各グループに対してステップ 11 を繰り返します。

**ステップ 14** 変更を送信し、保存します。

## セキュリティ管理アプライアンスへのアクセスに対する追加の制御

- [IP ベースのネットワーク アクセスの設定 \(494 ページ\)](#)
- [Web UI セッションタイムアウトの設定 \(497 ページ\)](#)

### IP ベースのネットワーク アクセスの設定

組織がリモートユーザに逆プロキシを使用する場合、アプライアンスに直接接続するユーザ、および逆プロキシを介して接続するユーザのためのアクセスリストを作成することで、ユーザがどの IP アドレスからセキュリティ管理アプライアンスにアクセスするのかを制御できます。

- [直接接続 \(494 ページ\)](#)
- [プロキシ経由の接続 \(494 ページ\)](#)
- [アクセス リストの作成 \(495 ページ\)](#)

#### 直接接続

セキュリティ管理アプライアンスに接続できるマシンの IP アドレス、サブネット、または CIDR アドレスを指定できます。ユーザは、アクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。リストに含まれていないアドレスからアプライアンスに接続しようとするユーザのアクセスは拒否されます。

#### プロキシ経由の接続

リモート ユーザのマシンとセキュリティ管理アプライアンスの間で逆プロキシ サーバが使用される組織のネットワークの場合、AsyncOS ではアプライアンスに接続可能なプロキシの IP アドレスを含むアクセス リストを作成できます。

逆プロキシを使用している場合でも、AsyncOS は、ユーザ接続が許可されている IP アドレスのリストと照合して、リモート ユーザのマシンの IP アドレスを検証します。リモートユーザ

の IP アドレスを E メールセキュリティ アプライアンスに送信するには、プロキシで x-forwarded-for HTTP ヘッダーをアプライアンスへの接続要求に含める必要があります。

x-forwarded-for ヘッダーは RFC 非準拠の HTTP ヘッダーであり、次の形式になります。

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF.

このヘッダーの値はカンマ区切りの IP アドレスのリストです。左端のアドレスがリモートユーザマシンのアドレスで、その後に、接続要求を転送した一連の各プロキシのアドレスが続きます（ヘッダー名は設定可能です）。セキュリティ管理アプライアンスは、ヘッダーのリモートユーザの IP アドレスおよび接続プロキシの IP アドレスを、アクセスリストで許可されたユーザ IP アドレスやプロキシ IP アドレスと照合します。



(注) AsyncOS は x-forwarded-for ヘッダーでは IPv4 アドレスだけをサポートします。

## アクセス リストの作成

GUI の [ネットワークアクセス (Network Access)] ページまたは CLI の `adminaccessconfig > ipaccess` コマンドを介して、ネットワークアクセスリストを作成できます。次の図は、セキュリティ管理アプライアンスへの直接的な接続が許可されているユーザ IP アドレスのリストが表示された [ネットワークアクセス (Network Access)] ページを示しています。

次の設定は、アプライアンスのレガシー Web インターフェイスおよび新しい Web インターフェイスに適用できます。

図 12: ネットワーク アクセス設定の例

### Network Access

| Network Access                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web UI Inactivity Timeout:                              | 30 Minutes<br><small>Enter a value between 5 - 1440 Minutes (24 hours).</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| User Access:                                            | <p>Control system access by IP Address, IP Range or CIDR.</p> <p>Only Allow Specific Connections</p> <p>10.0.0.33/32, 10.0.0.52/32, 10.0.0.130/32, 10.0.0.105/32, 10.0.0.155/32, 10.0.0.23/32, 10.0.0.28/32, 10.0.0.209/32, 10.0.0.31/32, 10.0.0.60/32, 10.0.0.51/32</p> <p><small>(Valid entries are an IP address, IP range or CIDR range. Separate multiple entries with commas. Examples: 10.0.0.1, 10.0.0.1-24, 10.0.0.0/8)</small></p> <p>IP Address of Proxy Server:</p> <p><small>(Separate multiple entries with commas.)</small></p> <p>Origin IP Header:</p> <p>x-forwarded-for</p> |
| <p>Cancel <span style="float: right;">Submit</span></p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

AsyncOS はアクセス リストの制御で 4 種類のモードを用意しています。

- **[すべて許可 (Allow All)]**。このモードはアプライアンスへの接続をすべて許可します。これが操作のデフォルト モードです。
- **[特定の接続のみを許可 (Only Allow Specific Connections)]**。このモードは、ユーザの IP アドレスが、アクセス リストに含まれている IP アドレス、IP 範囲、または CIDR 範囲と一致する場合に、ユーザのアプライアンスへの接続を許可します。
- **[特定のプロキシ経由接続のみを許可 (Only Allow Specific Connections Through Proxy)]**。このモードは、次の条件を満たせば、逆プロキシ経由でアプライアンスへの接続を許可します。
  - 接続プロキシの IP アドレスが、アクセス リストの [プロキシサーバの IP アドレス (IP Address of Proxy Server)] フィールドに含まれている。
  - プロキシの接続要求に x-forwarded-header HTTP ヘッダーが記載されている。
  - x-forwarded-header の値が空ではない。
  - リモートユーザの IP アドレスが x-forwarded-header に含まれ、それがアクセス リスト内のユーザに対して定義された IP アドレス、IP 範囲、または CIDR 範囲と一致する。
- **[特定の直接接続またはプロキシ経由接続のみを許可 (Only Allow Specific Connections Directly or Through Proxy)]**。このモードは、アクセス リストに含まれる IP アドレス、IP 範囲、CIDR 範囲のいずれかにユーザの IP アドレスが一致すれば、アプライアンスへの逆プロキシ経由接続または直接接続を許可します。プロキシ経由接続の条件は、[特定のプロキシ経由接続のみを許可 (Only Allow Specific Connections Through Proxy)] モードと同じです。

次のいずれかの条件が true の場合、変更を送信して確定した後、アプライアンスにアクセスできなくなることがありますので注意してください。

- [特定の接続のみを許可 (Only Allow Specific Connections)] を選択し、現在のマシンの IP アドレスがリストに含まれていない場合。
- [特定のプロキシ経由接続のみを許可 (Only Allow Specific Connections Through Proxy)] を選択し、現在アプライアンスに接続されているプロキシの IP アドレスがプロキシ リストに存在せず、許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合。
- [特定の直接接続またはプロキシ経由接続のみを許可 (Only Allow Specific Connections Directly or Through Proxy)] を選択し、
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在しない場合  
または
  - 許可されている IP アドレスのリストに送信元 IP ヘッダーの値が存在せず、アプライアンスに接続されたプロキシの IP アドレスが許可されているプロキシのリストに存在しない場合。

アクセス リストを修正せずに続行した場合、ユーザが変更を確定すると、AsyncOS はアプライアンスからユーザのマシンまたはプロキシを切断します。



**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [システム管理 (System Administration)] > [ネットワークアクセス (Network Access)] を選択します。

**ステップ 3** [設定の編集 (Edit Settings)] をクリックします。

**ステップ 4** アクセスリストの制御モードを選択します。

**ステップ 5** アプライアンスへの接続を許可するユーザの IP アドレスを入力します。

IP アドレス、IP アドレス範囲または CIDR 範囲を入力できます。複数のエントリを指定する場合は、カンマで区切ります。

**ステップ 6** プロキシ経由接続が許可されている場合は、次の情報を入力します。

- アプライアンスへの接続を許可するプロキシの IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。
- プロキシがアプライアンスに送信する発信元の IP ヘッダーの名前。これには、リモートユーザマシンの IP アドレスと、要求を転送したプロキシサーバの IP アドレスが含まれます。デフォルトのヘッダー名は x-forwarded-for です。

**ステップ 7** 変更を送信し、保存します。

## Web UI セッションタイムアウトの設定

セキュリティ管理アプライアンスの Web UI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。この Web UI セッションタイムアウトは、admin を含むユーザ全員に適用されます。また、HTTP セッションと HTTPS セッションのいずれにも使用されます。

AsyncOS によってユーザがログアウトされると、アプライアンスはユーザの Web ブラウザをログインページにリダイレクトします。



(注) Web UI セッションタイムアウトはスパム隔離セッションには適用されません。このセッションには 30 分のタイムアウトが設定されており、変更できません。

**ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [システム管理 (System Administration)] > [ネットワークアクセス (Network Access)] ページを使用します。

**ステップ 3** [設定の編集 (Edit Settings)] をクリックします。

**ステップ4** ログアウトまでにユーザを非アクティブにできる分数を [Web UI 非アクティブ タイムアウト (Web UI Inactivity Timeout) ] フィールドに入力します。5 ~ 1440 分のタイムアウト期間を定義できます。

**ステップ5** 変更を送信し、保存します。

## CLI セッションタイムアウトの設定

セキュリティ管理アプライアンスの CLI から AsyncOS が、非アクティブなユーザをログアウトするまでの時間を指定できます。以下に CLI セッションタイムアウトが適用されます。

- すべてのユーザ (管理者を含む)
- セキュア シェル (SSH) 、SCP、および直接シリアル接続を使用している接続のみ



(注) CLIセッションタイムアウト時に未確定の設定変更は失われます。設定を変更したらすぐに確定してください。

**ステップ1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ2** [システム管理 (System Administration) ] > [ネットワークアクセス (Network Access) ] ページを使用します。

**ステップ3** [設定の編集 (Edit Settings) ] をクリックします。

**ステップ4** [CLI 非アクティブ タイムアウト (CLI Inactivity Timeout) ] フィールドに、ログアウトされるまでにユーザを非アクティブにできる分数を入力します。5 ~ 1440 分のタイムアウト期間を定義できます。

**ステップ5** 変更を送信し、保存します。

### 次のタスク

また、CLI で `adminaccessconfig` コマンドを使用して CLI セッションタイムアウトを設定することもできます。『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

## メッセージトラッキングでの機密情報へのアクセスの制御

**ステップ1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 2** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ユーザ (Users) ] ページに移動します。

**ステップ 3** [トラッキング権限 (Tracking Privileges) ] セクションで、[設定の編集 (Edit Settings) ] をクリックします。

**ステップ 4** メッセージトラッキングで機密情報へのアクセス権を付与するロールを選択します。  
メッセージトラッキングへのアクセス権を持つカスタム ロールだけが一覧表示されます。

**ステップ 5** 変更を送信し、保存します。

この設定を有効にするには、[管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ] で中央集中型電子メール メッセージトラッキング機能をイネーブルにする必要があります。

---

## 管理ユーザ向けメッセージの表示

管理ユーザがアプライアンスにサインインするときにメッセージを表示できます。

メッセージを設定またはクリアするには、次の手順を実行します。

---

**ステップ 1** テキスト ファイルをインポートする場合は、アプライアンスの `/data/pub/configuration` ディレクトリにインポートします。

**ステップ 2** コマンドライン インターフェイス (CLI) にアクセスします。

**ステップ 3** `adminaccessconfig > BANNER` コマンドとサブコマンドを使用します。

**ステップ 4** 変更を確定します。

---

## 管理ユーザ アクティビティの表示

- [Web を使用したアクティブなセッションの表示 \(499 ページ\)](#)
- [最近のログイン試行の表示 \(500 ページ\)](#)
- [コマンドライン インターフェイスを介した管理ユーザ アクティビティの表示 \(500 ページ\)](#)

---

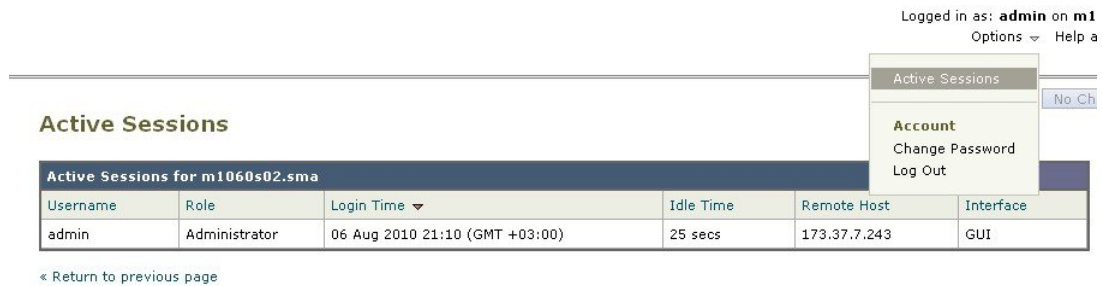
## Web を使用したアクティブなセッションの表示

セキュリティ管理アプライアンスでは、すべてのアクティブなセッションと、アプライアンスにログインしているユーザを表示できます。

---

ウィンドウの右上から、[オプション (Options) ]>[アクティブなセッション (Active Sessions) ] を選択します。

図 13: [アクティブなセッション (Active Sessions) ]メニュー



[アクティブなセッション (Active Sessions) ]ページから、ユーザ名、ユーザが持っているロール、ユーザのログイン時間、アイドル時間、およびユーザがコマンドラインと GUI のどちらからログインしたかを表示できます。

## 最近のログイン試行の表示

Web インターフェイス、SSH、または FTP 経由で直近のいくつかのログイン試行（失敗または成功）を表示するには、次を実行します。

**ステップ 1** ログインします。

**ステップ 2** 画面の右上部付近にある [次のユーザとしてログイン (Logged in as) ]の横の [図アイコン (Figure-icon) ]アイコンをクリックします。

## コマンドラインインターフェイスを介した管理ユーザアクティビティの表示

次に、アプライアンスへの複数ユーザアクセスをサポートするコマンドを示します。

- **who** コマンドは、CLI または Web ユーザ インターフェイスを介してシステムにログインしたすべてのユーザ、ユーザのロール、ログイン時刻、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。
- **whoami** コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com>
whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- **last** コマンドは、アプライアンスに最近ログインしたユーザを表示します。リモートホストの IP アドレス、ログイン、ログアウト、および合計時間も表示されます。

```
mail3.example.com> last
Username Remote Host Login Time Logout Time Total Time
=====
admin 10.1.3.67 Sat May 15 23:42 still logged in 15m
admin 10.1.3.67 Sat May 15 22:52 Sat May 15 23:42 50m
admin 10.1.3.67 Sat May 15 11:02 Sat May 15 14:14 3h 12m
admin 10.1.3.67 Fri May 14 16:29 Fri May 14 17:43 1h 13m
shutdown shutdown Fri May 14 16:22
shutdown shutdown Fri May 14 16:15
admin 10.1.3.67 Fri May 14 16:05 Fri May 14 16:15 9m
admin 10.1.3.103 Fri May 14 16:12 Fri May 14 16:15 2m
admin 10.1.3.103 Thu May 13 09:31 Fri May 14 14:11 1d 4h 39m
admin 10.1.3.135 Fri May 14 10:57 Fri May 14 10:58 0m
admin 10.1.3.67 Thu May 13 17:00 Thu May 13 19:24 2h 24m
```

## 管理ユーザ アクセスのトラブルシューティング

- エラー：ユーザにアクセス権限が割り当てられていません ([User Has No Access Privileges Assigned](#)) (501 ページ)
- アクティブメニューがありません ([User Has No Active Menus](#)) (502 ページ)
- 外部認証されたユーザに設定オプションが表示されます ([Externally-Authenticated Users See Preferences Option](#)) (502 ページ)

### エラー：ユーザにアクセス権限が割り当てられていません (User Has No Access Privileges Assigned)

#### 問題

管理を委任されたユーザはセキュリティ管理アプライアンスにログインできますが、アクセス権限が割り当てられていないというメッセージが表示されます。

#### ソリューション

このユーザに割り当てられたカスタム ユーザ ロールに権限を割り当てたことを確認します。[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザ (Users)] を表示して、割り当てられているユーザ ロールを特定してから、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザロール (User Roles)] に移動し、ユーザ ロールの名前をクリックしてロールに権限を割り当てます。

レポーティング グループに基づいてアクセスを割り当てた場合は、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ユーザロール (User Roles)] ページで、そのユーザのレポーティング グループが選択されていることを確認します。グループを割り当てるには、[委任管理用のユーザ役割 (User Roles for Delegated Administration)] テーブルの [メールレポート (Email Reporting)] 列で [グループが選択されていません (No groups selected)] リンクをクリックします。

## アクティブメニューがありません (User Has No Active Menus)

### 問題

公開権限を付与されたユーザのログイン時に、アクティブメニューがありません。

### ソリューション

少なくとも1つのアクセスポリシーまたはカスタムURLカテゴリへのアクセス権があることを確認します。いずれかを編集できるこのユーザ権限を付与しない場合は、どのポリシーでも使用されていないカスタムURLカテゴリを作成し、[カスタムユーザ役割 (Custom User Role)] ページでこのカテゴリにこのユーザロール権限を付与します。

## 外部認証されたユーザに設定オプションが表示されます (Externally-Authenticated Users See Preferences Option)

### 問題

外部認証されたユーザに設定オプションが表示されます。

### ソリューション

セキュリティ管理アプライアンスで直接追加するユーザのユーザ名が、外部認証データベースで使用されていない一意のユーザ名であることを確認します。



## 第 16 章

# 一般的な管理タスク

---

この章は、次の項で構成されています。

- [管理タスクの実行 \(504 ページ\)](#)
- [Cisco コンテンツ セキュリティ管理アプライアンスのライセンス \(504 ページ\)](#)
- [CLI コマンドを使用したメンテナンス作業の実行 \(506 ページ\)](#)
- [リモート電源再投入の有効化 \(510 ページ\)](#)
- [SNMP を使用したシステムの状態のモニタリング \(511 ページ\)](#)
- [セキュリティ管理アプライアンスのデータのバックアップ \(513 ページ\)](#)
- [セキュリティ管理アプライアンスでのディザスタ リカバリ \(522 ページ\)](#)
- [アプライアンス ハードウェアのアップグレード \(524 ページ\)](#)
- [AsyncOS のアップグレード \(524 ページ\)](#)
- [AsyncOS の以前のバージョンへの復元について \(538 ページ\)](#)
- [アップデートについて \(540 ページ\)](#)
- [生成されたメッセージの返信アドレスの設定 \(540 ページ\)](#)
- [アラートの管理 \(541 ページ\)](#)
- [ネットワーク設定値の変更 \(550 ページ\)](#)
- [セキュア通信プロトコルの指定 \(555 ページ\)](#)
- [システム時刻の設定 \(556 ページ\)](#)
- [\[設定ファイル \(Configuration File\) \] ページ \(558 ページ\)](#)
- [設定の保存とインポート \(559 ページ\)](#)
- [ディスク領域の管理 \(567 ページ\)](#)
- [E メールセキュリティ アプライアンスのシステムの状態グラフの参照のしきい値の調整 \(571 ページ\)](#)
- [SAML 2.0 による SSO \(572 ページ\)](#)
- [ビューのカスタマイズ \(581 ページ\)](#)
- [アプライアンスで有効なサービスの再起動とステータスの表示 \(583 ページ\)](#)

## 管理タスクの実行

システム管理タスクのほとんどは、グラフィカルユーザインターフェイス（GUI）の [システム管理（System Administration）] メニューを使用して実行できます。ただし、一部のシステム管理機能は、コマンドラインインターフェイス（CLI）からのみ実行できます。

また、[システム ステータスのモニタリング](#)（425 ページ）



(注) この章で説明する機能やコマンドの中には、ルーティングの優先順位に影響を及ぼすものがあります。詳細については、[IP アドレス、インターフェイス、およびルーティング](#)（641 ページ）を参照してください。

## Cisco コンテンツ セキュリティ管理アプライアンスのライセンス

- [機能キーの使用](#)（504 ページ）

### 機能キーの使用

キーは、アプライアンスのシリアル番号に固有のものであり、またイネーブルする機能にも固有です。1つのシステムのキーを、別のシステムで再利用することはできません。

ここで説明するタスクをコマンドラインプロンプトから実行するには、`featurekey` コマンドを使用します。



| 目的                                                                                                                                                                                                    | 操作手順                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• アプライアンスのアクティブな機能キーをすべて表示する</li> <li>• アクティベーションを保留中のすべての機能キーを表示する</li> <li>• 発行された新しいキーを検索する</li> <li>• 機能キーを手動でインストールする</li> <li>• 機能キーをアクティブ化する</li> </ul> | <p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance) ]&gt;[システム管理 (System Administration) ]&gt;[機能キー (Feature Keys) ]を選択します。</p> <p>新しい機能キーを手動で追加するには、[機能キー (Feature Key) ] フィールドにキーを貼り付けるか、または入力し、[キーを送信 (Submit Key) ] をクリックします。機能が追加されない場合は、エラーメッセージが表示されます (たとえば、キーが正しくない場合など)。それ以外の場合は、機能キーがリストに追加されます。</p> <p>発行されたときに自動的に新しいキーをダウンロードおよびインストールするようにアプライアンスを設定した場合、[保留中のライセンス (Pending Activation) ] リストは常に空白になります。</p> |
| 機能キーの自動ダウンロードおよびアクティベーションを有効または無効にする                                                                                                                                                                  | <p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance) ]&gt;[システム管理 (System Administration) ]&gt;[機能キーの設定 (Feature Key Settings) ]を選択します</p> <p>デフォルトでは、アプライアンスは、新しいキーを定期的に確認します。</p>                                                                                                                                                                                                                                           |
| 期限切れ機能キーを更新する                                                                                                                                                                                         | Cisco の担当者にお問い合わせください                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 仮想アプライアンスのライセンスおよび機能キー

ライセンスおよび機能キーの期限が切れたときのアプライアンスの動作については、<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html> から入手できる『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

ライセンス情報を表示するには、コマンドライン インターフェイス (CLI) で show license コマンドを使用します。

## CLI コマンドを使用したメンテナンス作業の実行

ここで説明する操作とコマンドを利用すると、セキュリティ管理アプライアンス上でメンテナンスに関連する作業を実行できます。ここでは、次の操作とコマンドについて説明します。

- shutdown
- reboot
- suspend
- suspendtransfers
- 復帰
- resumetransfers
- resetconfig
- version

## セキュリティ管理アプライアンスのシャットダウン

セキュリティ管理アプライアンスをシャットダウンするには、次の手順を実行します。

- (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- [管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [シャットダウン/再起動 (Shutdown/Reboot) ] ページを使用します。  
または
- コマンドラインプロンプトで shutdown コマンドを使用します。

アプライアンスをシャットダウンすると、AsyncOS が終了し、アプライアンスの電源を安全にオフにできます。アプライアンスは、配信キューのメッセージを失わずに後で再起動できます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。

## セキュリティ管理アプライアンスのリブート

セキュリティ管理アプライアンスをリブートするには、GUI の [システム管理 (System Administration) ] メニューで利用可能な [シャットダウン/再起動 (Shutdown/Reboot) ] ページを使用するか、CLI で reboot コマンドを使用します。

アプライアンスをリブートすると、AsyncOS が再起動されるため、アプライアンスの電源を安全にオフにし、アプライアンスをリブートできます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。アプライアンスは、配信キュー内のメッセージを失わずに再起動できます。

## セキュリティ管理アプライアンスの停止

システムメンテナンスを実行する場合など、アプライアンスをオフラインにするには、次のコマンドのいずれかを使用します。

| コマンド             | 説明                                                                                                                                                                                                                                                                       | 永続化            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| suspend          | <ul style="list-style-type: none"> <li>• Eメールセキュリティアプライアンスからセキュリティ管理アプライアンスへの隔離されたメッセージの転送を一時停止します。</li> <li>• 隔離からリリースされたメッセージの配信を一時停止します。</li> <li>• 着信電子メール接続が許可されません。</li> <li>• 発信電子メール配信は停止されます。</li> <li>• ログ転送が停止されます。</li> <li>• CLIはアクセス可能のままになります。</li> </ul> | リブート後も永続化されます。 |
| suspendtransfers | <p>管理対象の電子メールおよび Web Security Appliances から Content Security Management Appliance へのレポートングデータおよびトラッキングデータの転送を一時停止します。</p> <p>このコマンドでは、Eメールセキュリティアプライアンスからの隔離されたメッセージの受信も一時停止されます。</p> <p>バックアップアプライアンスをプライマリアプライアンスとして再開するための準備段階でこのコマンドを使用します。</p>                      | リブート後も維持されます。  |

これらのコマンドの使用時には、アプライアンスの遅延値を入力する必要があります。デフォルト遅延値は30秒です。AsyncOSでは、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。オープン中の接続が存在しない場合は、すぐにサービスが停止されます。

suspendまたはsuspendtransfersコマンドで停止したサービスを再アクティブ化するには、resumeまたはresumetransfersコマンドをそれぞれ使用します。

管理アプライアンスの現在のステータス（オンラインまたは一時停止）を特定するには、Web インターフェイスで [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [シャットダウン/再起動 (Shutdown/Reboot)] を選択します。

関連項目：

- お使いの E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Suspending Email Delivery」、「Resuming Email Delivery」、「Suspending Receiving」、および「Resuming Receiving」。

## CLI の例 : suspend および suspendtransfers コマンド

```
sma.example.com> suspend
Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
sma.example.com>
sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

## 一時停止状態からの再開

resume コマンドは、suspend または suspenddel コマンドの使用後にアプライアンスを通常の動作状態に戻します。

resumetransfers コマンドは、suspendtransfers コマンドの使用後にアプライアンスを通常の動作状態に戻します。

## CLI の例 : resume および resumetransfers コマンド

```
sma.example.com> resume
Receiving resumed.
Mail delivery resumed.
sma.example.com>
sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.example.com>
```

## 工場出荷時の初期状態への設定のリセット

アプライアンスを物理的に転送するとき、または構成の問題を解決する最後の手段として、工場出荷時の初期状態にアプライアンスをリセットすることもできます。



**注意** 設定をリセットすると CLI から切り離すことになり、アプライアンス (FTP、Telnet、SSH、HTTP、HTTPS) への接続に使用しているサービスが無効になり、ユーザアカウントが削除されます。

| 目的                                                                                                                                                                                              | 操作手順                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>工場出荷時の初期状態へすべての設定をリセット</li> <li>すべてのレポートカウンタをクリア</li> </ul> <p>ただし、</p> <ul style="list-style-type: none"> <li>ログ ファイルを保持</li> <li>隔離メッセージを保持</li> </ul> | <ol style="list-style-type: none"> <li>デフォルトの <code>admin</code> ユーザアカウントとパスワードを使用し、シリアルインターフェイスを使用して CLI に接続するかまたはデフォルト設定を使用して管理ポートに接続して、リセット後にアプライアンスに接続できることを確認します。デフォルト設定のアプライアンスへのアクセスの詳細については、<a href="#">セットアップ、インストール、および基本設定 (5 ページ)</a> を参照してください。</li> <li>アプライアンスのサービスを一時停止します。</li> <li>[管理アプライアンス (Management Appliance) ]&gt;[システム管理 (System Administration) ]&gt;[設定ファイル (Configuration File) ]を選択し、[リセット (Reset) ]をクリックします。</li> </ol> <p>(注) リセット後、アプライアンスがオフライン状態に自動的に戻ります。リセット前に電子メールの送信が中断されている場合、配信はリセット後に再試行されます。</p> |
| <ul style="list-style-type: none"> <li>工場出荷時の初期状態へすべての設定をリセット</li> <li>すべてのデータを削除</li> </ul>                                                                                                    | <p>diagnostic &gt; reload CLI コマンドを使用します。</p> <p><b>注意</b> このコマンドは、Cisco ルータまたはスイッチで使用される類似のコマンドと同じではありません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                              |

## resetconfig コマンド

```
mail3.example.com> suspend
Delay (seconds, minimum 30):
[30]> 45
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com> resetconfig
Are you sure you want to reset all configuration values? [N]> Y
All settings have been restored to the factory default.
```

## AsyncOS のバージョン情報の表示

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ]>[システムステータス (System Status) ]を選択します。

**ステップ3** ページの下部までスクロールして、[バージョン情報 (Version Information)] で、現在インストールされている AsyncOS のバージョンを確認します。

あるいは、コマンドラインプロンプトで **version** コマンドを使用することもできます。

## リモート電源再投入の有効化

アプライアンスシャーシの電源をリモートでリセットする機能は、80 および 90 シリーズハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

### 始める前に

- 専用のリモート電源再投入 (RPC) ポートをセキュアネットワークに直接、ケーブル接続します。詳細については、ご使用のモデルのハードウェアマニュアルを参照してください ([資料 \(655 ページ\)](#) に記載されている場所から入手できます)。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモートアクセス可能であることを確認します。
- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。ipconfig コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface (IPMI) バージョン 2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドラインインターフェイスへのアクセスに関する詳細については、CLI のリファレンス ガイドを参照してください。

**ステップ1** SSH、Telnet、またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

**ステップ2** 管理者権限を持つアカウントを使用してログインします。

**ステップ3** 以下のコマンドを入力します。

```
remotepower
setup
```

**ステップ4** プロンプトに従って、以下の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスワード。

これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

**ステップ 5** `commit` を入力して変更を保存します。

**ステップ 6** 設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

**ステップ 7** 入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

### 次のタスク

[アプライアンスの電源のリモートリセット \(629 ページ\)](#)

## SNMP を使用したシステムの状態のモニタリング

AsyncOS は、Simple Network Management Protocol (SNMP) バージョン v1、v2、および v3 を使用したシステム ステータスのモニタリングをサポートします。

- SNMP を有効にし、設定するには、コマンドライン インターフェイスで `snmpconfig` コマンドを使用します。
- MIB は <http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html> から入手できます (使用可能な最新ファイルを使用)。
- このサービスをイネーブルにするには、パズフレーズ認証と DES 暗号化を伴う SNMPv3 の使用が必須です。(SNMPv3 の詳細については、RFC 2571 ~ 2575 を参照してください)。SNMP システム ステータスのモニタリングをイネーブルにするには、少なくとも 8 文字の SNMPv3 パズフレーズを設定する必要があります。最初に SNMPv3 パズフレーズを入力するときは、確認のためにそのパズフレーズを再入力する必要があります。次に `snmpconfig` コマンドを実行するときは、コマンドにこのフレーズが「記憶」されています。
- 接続をモニタするように SNMP を設定する場合：
  - connectivityFailure SNMP トラップの設定時に `url-attribute` を入力する場合、URL がディレクトリまたはファイルのいずれを指すかを決定します。
    - ディレクトリの場合は、末尾にスラッシュ (/) を追加します。
    - ファイルの場合は、末尾にスラッシュを追加しません。
- AsyncOS での SNMP の使用の詳細については、Web または Email Security Appliance のオンライン ヘルプを参照してください。

### 例 : snmpconfig コマンド

```
sma.example.com> snmpconfig
```

```

Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[ ]> SETUP
Do you want to enable SNMP?
[ Y ]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: sma.example.com)
[ 1 ]>
Which port shall the SNMP daemon listen on interface "Management"?
[ 161 ]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[ 1 ]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[ 1 ]> 2
Enter the SNMPv3 authentication passphrase.
[ ]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[ ]>
Enter the SNMPv3 privacy passphrase.
[ ]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[ ]>
Service SNMP V1/V2c requests?
[ N ]> Y
Enter the SNMP V1/V2c community string.
[ ironport ]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[ Y ]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[ 127.0.0.1/32 ]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[ 127.0.0.1 ]> 203.0.113.1
Enter the Trap Community string.
[ ironport ]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded           Disabled
2. FIPSMoDeDisableFailure           Enabled
3. FIPSMoDeEnableFailure            Enabled
4. FailoverHealthy                  Enabled
5. FailoverUnhealthy                Enabled
6. RAIDStatusChange                Enabled
7. connectivityFailure              Disabled
8. fanFailure                       Enabled
9. highTemperature                  Enabled
10. keyExpiration                   Enabled
11. linkUpDown                      Enabled
12. memoryUtilizationExceeded       Disabled
13. powerSupplyStatusChange         Enabled
14. resourceConservationMode        Enabled
15. updateFailure                   Enabled
Do you want to change any of these settings?
[ N ]> Y
Do you want to disable any of these traps?
[ Y ]> n
Do you want to enable any of these traps?
[ Y ]> y

```



```
Enter number or numbers of traps to enable. Separate multiple numbers with
commas.
[> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> SMA.Administrator@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: SMA.Administrator@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[>
sma.example.com> commit
Please enter some comments describing your changes:
[> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
sma.example.com>
```

## セキュリティ管理アプライアンスのデータのバックアップ

- [バックアップされるデータ \(514 ページ\)](#)
- [バックアップの制約事項および要件 \(514 ページ\)](#)
- [バックアップ期間 \(516 ページ\)](#)
- [バックアップ中のサービスのアベイラビリティ \(516 ページ\)](#)
- [バックアッププロセスの中断 \(517 ページ\)](#)
- [ターゲットアプライアンスによる管理対象アプライアンスからのデータの直接取得の防止 \(517 ページ\)](#)
- [バックアップステータスに関するアラートの受信 \(518 ページ\)](#)
- [単一または定期バックアップのスケジュール設定 \(518 ページ\)](#)
- [即時バックアップの開始 \(519 ページ\)](#)
- [バックアップステータスの確認 \(519 ページ\)](#)
- [その他の重要なバックアップタスク \(520 ページ\)](#)
- [バックアップアプライアンスのプライマリアプライアンスとしての使用 \(520 ページ\)](#)

## バックアップされるデータ

すべてのデータをバックアップすること、または次のデータの任意の組み合わせをバックアップすることを選択できます。

- メッセージ、メタデータを含むスパム隔離
- メッセージおよびメタデータを含んでいる集約されたポリシー、ウイルス、およびアウトブレイク隔離
- メッセージ、メタデータを含む電子メール トラッキング (メッセージ トラッキング)
- Web トラッキング
- レポートイング (電子メールおよび Web)
- セーフリスト/ブロックリスト

データの転送が完了すると、2つのアプライアンスのデータが同一になります。

この処理を行っても、設定とログはバックアップされません。これらの項目をバックアップする方法については、[その他の重要なバックアップタスク \(520 ページ\)](#) を参照してください。

最初のバックアップ後の各バックアップは、前回のバックアップ後に生成された情報のみをコピーします。

## バックアップの制約事項および要件

バックアップをスケジュール設定する前に、次の制約事項および要件を考慮してください。

| 制約事項                 | 要件                                                                                                                                                                  |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AsyncOS バージョン        | ソース セキュリティ管理アプライアンスおよびターゲット セキュリティ管理アプライアンスの AsyncOS バージョンが同じである必要があります。バージョンの非互換性がある場合、バックアップをスケジュールする前に、同じリリースにアプライアンスをアップグレードします。                                |
| ネットワーク上のターゲットアプライアンス | ターゲットアプライアンスがネットワーク上に設定されている必要があります。<br><br>ターゲットアプライアンスが新規の場合は、システム セットアップ ウィザードを実行して必要な情報を入力します。手順については、 <a href="#">セットアップ、インストール、および基本設定 (5 ページ)</a> を参照してください。 |

| 制約事項                          | 要件                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ソース アプライアンスとターゲット アプライアンス間の通信 | <p>ソースおよびターゲットのセキュリティ管理アプライアンスは、SSHを使用して通信できるようになっている必要があります。したがって、次のようにします。</p> <ul style="list-style-type: none"> <li>両方のアプライアンスのポート 22 を開いておく必要があります。デフォルトでは、このポートはシステムセットアップウィザードを実行すると開きます。</li> <li>ドメイン ネーム サーバ (DNS) で、A レコードと PTR レコードの両方を使用して、両方のアプライアンスのホスト名を解決する必要があります。</li> </ul>                                                                                                                                                                                                                                                          |
| ターゲット アプライアンスを停止する必要があります。    | <p>プライマリ アプライアンスのみが、管理対象の電子メールおよび Web Security Appliances からデータを取得する必要があります。確実に実行するために、<a href="#">ターゲット アプライアンスによる管理対象アプライアンスからのデータの直接取得の防止 (517ページ)</a> を参照してください。</p> <p>また、バックアップ アプライアンスでスケジュール設定されている設定公開ジョブをキャンセルしてください。</p>                                                                                                                                                                                                                                                                                                                      |
| アプライアンス キャパシティ                | <p>ターゲットアプライアンスのディスク領域キャパシティが、ソースアプライアンスのキャパシティと同等以上である必要があります。ターゲットアプライアンスで各データタイプ（レポート、トラッキング、隔離など）に割り当てるディスク領域は、ソースアプライアンスの対応する割り当てより少なくすることはできません。</p> <p>各データタイプのすべてのデータのバックアップに十分なスペースがターゲットアプライアンス上にあれば、大きいソースから小さいターゲットセキュリティ管理アプライアンスへのバックアップをスケジュール設定できます。ソースアプライアンスがターゲットアプライアンスよりも大きい場合、ターゲットアプライアンスで使用可能な領域に合わせて、ソースアプライアンスで割り当てられている領域を削減します。</p> <p>ディスク領域の割り当てとキャパシティを表示および管理するには、<a href="#">ディスク領域の管理 (567ページ)</a> を参照してください。</p> <p>仮想アプライアンスのディスク容量については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。</p> |

| 制約事項                | 要件                                                                                                                                                                                                |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 複数、同時、およびチェーンバックアップ | <p>バックアッププロセスは一度に1つだけ実行できます。前のバックアップが完了する前に実行がスケジュールされているバックアップはスキップされ、警告が送信されます。</p> <p>セキュリティ管理アプライアンスからのデータは、単一のセキュリティ管理アプライアンスにバックアップできます。</p> <p>チェーンバックアップ（バックアップへのバックアップ）はサポートされていません。</p> |

## バックアップ期間

最初の完全バックアップでは、800GBのバックアップに最大10時間かかります。毎日のバックアップは、それぞれ最大3時間かかります。毎週または毎月のバックアップはより長くかかる場合があります。これらの数は場合によって異なります。

初期バックアップ後のバックアッププロセスでは、最後のバックアップから変更されたファイルのみが転送されます。このため、その後のバックアップにかかる時間は初期バックアップの場合よりも短くなります。後続のバックアップに必要な時間は、累積されたデータ量、変更されたファイル数、および最後のバックアップ以降どの程度のファイルが変更されたかによって異なります。

## バックアップ中のサービスのアベイラビリティ

セキュリティ管理アプライアンスをバックアップすると、「ソース」セキュリティ管理アプライアンスから「ターゲット」セキュリティ管理アプライアンスにアクティブデータセットがコピーされます。このとき、コピー元の「ソース」アプライアンスの中断は最小限に抑えられます。

バックアッププロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- フェーズ1：バックアッププロセスのフェーズ1は、ソースアプライアンスとターゲットアプライアンス間のデータの転送で開始されます。データの転送中、ソースアプライアンスでのサービスは実行されたままになるため、データ収集をそのまま継続できます。ただし、ターゲットアプライアンスではサービスがシャットダウンされます。ソースからターゲットアプライアンスへのデータの転送が完了すると、フェーズ2が開始されます。
- フェーズ2：フェーズ2が始まると、ソースアプライアンスでサービスがシャットダウンされます。最初のシャットダウン以降、ソースアプライアンスとターゲットアプライアンス間でのデータ転送中に収集された相違点がターゲットアプライアンスにコピーされ、ソースアプライアンスとターゲットアプライアンスの両方で、サービスがバックアップ開始時の状態に戻ります。これにより、ソースアプライアンス上で最大の稼働時間を維持でき、いずれかのアプライアンスのデータが損失することがなくなります。

バックアップ中に、データアベイラビリティレポートが機能しなくなる場合があります。また、メッセージトラッキング結果を表示すると、各メッセージのホスト名に「未解決 (unresolved)」というラベルが付くことがあります。

レポートをスケジュール設定しようとしているときに、バックアップが進行中であることを忘れていた場合は、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] を選択して、システムのステータスを確認できます。このウィンドウでは、ページの上部にシステムのバックアップが進行中であるという警告が表示されます。

## バックアッププロセスの中断



(注) バックアップの実行中にソースアプライアンスの予期しないリブートがあっても、ターゲットアプライアンスはこの停止を認識しません。ターゲットアプライアンスでバックアップをキャンセルする必要があります。

バックアッププロセスの中断があり、そのバックアッププロセスが完了していない場合、バックアップを次に試行したときに、セキュリティ管理アプライアンスは停止した部分からバックアッププロセスを開始できます。

進行中のバックアップをキャンセルすることは推奨されません。これは、既存のデータが不完全になり、エラーが発生した場合は、次のバックアップが完了するまで使用できないことがあります。進行中のバックアップのキャンセルが必要な場合は、できるだけ早く完全バックアップを実行し、常に使用可能な現在のバックアップを確保してください。

## ターゲットアプライアンスによる管理対象アプライアンスからのデータの直接取得の防止

- ステップ1 ターゲットアプライアンスのコマンドラインインターフェイスにアクセスします。この説明については、[コマンドラインインターフェイスへのアクセス \(14 ページ\)](#) を参照してください。
- ステップ2 `suspendtransfers` コマンドを実行します。
- ステップ3 プロンプトが再表示されるまで待ちます。
- ステップ4 `suspend` コマンドを実行します。
- ステップ5 プロンプトが再表示されるまで待ちます。
- ステップ6 ターゲットアプライアンスのコマンドラインインターフェイスを終了します。

## バックアップステータスに関するアラートの受信

バックアップの完了時に問題を通知するアラートを受信するには、タイプが [システム (System) ] で重大度が [情報 (Info) ] のアラートを送信するようにアプライアンスを設定します。「アラートの管理 (541 ページ)」を参照してください。

## 単一または定期バックアップのスケジュール設定

単一または定期バックアップを事前設定した時間に行うようにスケジュール設定できます。



(注) リモートマシンに実行中のバックアップがある場合、バックアッププロセスは開始されません。

### 始める前に

- バックアップの制約事項および要件 (514 ページ) の項目に対処します。

- 
- ステップ 1** ソースアプライアンスのコマンドラインインターフェイスに、管理者としてログインします。
- ステップ 2** コマンドプロンプトで **backupconfig** と入力し、Enter を押します。
- ステップ 3** ソースアプライアンスおよびターゲットアプライアンス間の接続が低速である場合は、データ圧縮をオンにします。
- setup** と入力して、Y を押します。
- ステップ 4** **Schedule** と入力して、Enter を押します。
- ステップ 5** ターゲットセキュリティ管理アプライアンスの IP アドレスを入力します。
- ステップ 6** ターゲットアプライアンスを識別する有効な名前を入力します (最大 20 文字)。
- ステップ 7** ターゲットアプライアンスの管理ユーザの名前およびパスワードを入力します。
- ステップ 8** バックアップするデータに関するプロンプトに応答します。
- ステップ 9** 単一バックアップをスケジュール設定するには、**Schedule a single backup** に **2** を入力して、Enter を押します。
- ステップ 10** 定期バックアップをスケジュール設定する場合は、次の手順を実行します。
- 繰り返しバックアップをスケジュール設定するには、**1** を入力して、Enter を押します。
  - 定期バックアップの頻度を選択し、Enter を押します。
- ステップ 11** バックアップを開始する特定の日付または日および時間を入力して、Enter を押します。
- ステップ 12** バックアッププロセスの名前を入力します。
- ステップ 13** バックアップが正常にスケジュール設定されたことを確認します。コマンドプロンプトで **View** と入力して、Enter を押します。

ステップ 14 「その他の重要なバックアップタスク (520 ページ)」も参照してください。

## 即時バックアップの開始



(注) ターゲットマシンでバックアップが実行中の場合、バックアッププロセスは開始されません。

### 始める前に

バックアップの制約事項および要件 (514 ページ) のすべての要件を満たします。

- ステップ 1 ソース アプライアンスのコマンドラインインターフェイスに、管理者としてログインします。
- ステップ 2 コマンドプロンプトで `backupconfig` と入力し、Enter を押します。
- ステップ 3 ソースアプライアンスおよびターゲットアプライアンス間の接続が低速である場合は、データ圧縮をオンにします。
- `setup` と入力して、Y を押します。
- ステップ 4 `Schedule` と入力して、Enter を押します。
- ステップ 5 ターゲットセキュリティ管理アプライアンスの IP アドレスを入力します。
- ステップ 6 ターゲットアプライアンスを識別する有効な名前を入力します (最大 20 文字)。
- ステップ 7 ターゲットアプライアンスの管理ユーザの名前およびパスワードを入力します。
- ステップ 8 バックアップするデータに関するプロンプトに応答します。
- ステップ 9 単一バックアップをすぐに開始するため、`3` を入力して Enter を押します。
- ステップ 10 バックアップジョブの有効な名前を入力します。
- バックアッププロセスが数分で開始されます。
- ステップ 11 (任意) バックアップの進捗状況を表示するには、コマンドラインプロンプトで `Status` と入力します。
- ステップ 12 「その他の重要なバックアップタスク (520 ページ)」も参照してください。

## バックアップステータスの確認

- ステップ 1 プライマリ アプライアンスのコマンドラインインターフェイスに、管理者としてログインします。
- ステップ 2 コマンドプロンプトで `backupconfig` と入力し、Enter を押します。

| ステータスの確認対象        | 操作手順           |
|-------------------|----------------|
| スケジュール設定されたバックアップ | View 操作を選択します。 |

| ステータスの確認対象 | 操作手順                                                                                           |
|------------|------------------------------------------------------------------------------------------------|
| 進行中のバックアップ | Status 操作を選択します。<br>アラートを設定している場合は、電子メールを確認するか、 <a href="#">最新アラートの表示 (543 ページ)</a> を参照してください。 |

### 次のタスク

#### 関連項目

[ログファイルのバックアップ情報 \(520 ページ\)](#)

## ログファイルのバックアップ情報

バックアップ ログはバックアップ プロセスを開始から終了まで記録します。

バックアップ スケジューリングに関する情報は、SMA ログ内にあります。

#### 関連項目

- [バックアップ ステータスの確認 \(519 ページ\)](#)

## その他の重要なバックアップ タスク

ここで説明されているバックアッププロセスではバックアップされない項目が失われることを防止するため、およびアプライアンスの障害が発生した場合にセキュリティ管理アプライアンスの交換を速めるため、次のことを検討してください。

- プライマリセキュリティ管理アプライアンスから設定を保存するには、[設定の保存とインポート \(559 ページ\)](#) を参照してください。プライマリセキュリティ管理アプライアンスとは別の安全な場所にコンフィギュレーション ファイルを保存します。
- Configuration Master の設定に使用した、Web セキュリティアプライアンスのコンフィギュレーション ファイルをすべて保存します。
- セキュリティ管理アプライアンスから別の場所にログ ファイルを保存する方法については、[ログサブスクリプション \(611 ページ\)](#) を参照してください。

さらに、バックアップ ログのログサブスクリプションを設定できます。「[GUIでのログサブスクリプションの作成 \(613 ページ\)](#)」を参照してください。

## バックアップアプライアンスのプライマリアプライアンスとしての使用

アプライアンスハードウェアをアップグレードする場合、またはその他の理由でアプライアンスを切り替える場合は、次の手順を使用します。



### 始める前に

[セキュリティ管理アプライアンスのデータのバックアップ \(513 ページ\)](#) の情報を確認してください。

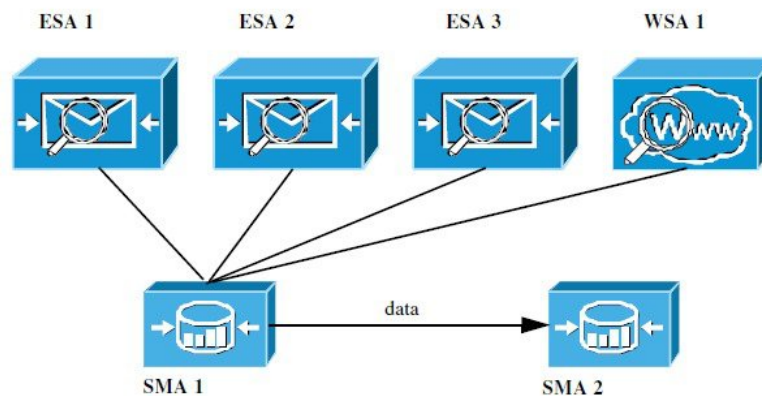
- 
- ステップ 1** 旧/プライマリ/ソース アプライアンスのコンフィギュレーション ファイルのコピーを、新しいアプライアンスから到達できる場所に保存します。[設定の保存とインポート \(559 ページ\)](#) を参照してください。
- ステップ 2** 新規/バックアップ/ターゲット アプライアンスでシステム セットアップ ウィザードを実行します。
- ステップ 3** [バックアップの制約事項および要件 \(514 ページ\)](#) の要件を満たします。
- ステップ 4** 旧/プライマリ/ソース アプライアンスからバックアップを実行します。[即時バックアップの開始 \(519 ページ\)](#) の手順を参照してください。
- ステップ 5** バックアップが完了するまで待ちます。
- ステップ 6** 旧/プライマリ/ソース アプライアンスで `suspendtransfers` および `suspend` コマンドを実行します。
- ステップ 7** 2 番目のバックアップを実行して、旧/プライマリ/ソースアプライアンスから新規/バックアップ/ターゲット アプライアンスに直前のデータを転送します。
- ステップ 8** コンフィギュレーションファイルを新規/バックアップ/ターゲットアプライアンスにインポートします。
- ステップ 9** 新規/バックアップ/ターゲット アプライアンスで `resumetransfers` および `resume` コマンドを実行します。旧/元プライマリ/ソース アプライアンスでこのコマンドを実行しないでください。
- ステップ 10** 新規/バックアップ/ターゲット アプライアンスと管理対象の電子メールおよび Web Security Appliances の間の接続を確立します。
- ステップ 11**
- (新しい Web インターフェイスのみ) クラウド Eメールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
  - [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティアプライアンス (Security Appliances)] を選択します。
  - アプライアンス名をクリックします。
  - [接続の確立 (Establish Connection)] ボタンをクリックします。
  - [テスト接続 (Test Connection)] をクリックします。
  - アプライアンスのリストに戻ります。
  - 管理対象の各アプライアンスに対して、この手順を繰り返します。
- ステップ 12** 新規/ターゲット アプライアンスがプライマリ アプライアンスとして機能していることを確認します。  
[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [システムステータス (System Status)] を選択し、データ転送の状態を確認します。
-

# セキュリティ管理アプライアンスでのディザスタリカバリ

セキュリティ管理アプライアンスが予期せず失敗した場合は、次の手順を使用して、セキュリティ管理サービスおよびバックアップしたデータを復元します。これは[セキュリティ管理アプライアンスのデータのバックアップ](#)（513 ページ）の情報をを使用して定期的に保存しています。

典型的なアプライアンス設定は、次の図に示すようになります。

図 14: ディザスタリカバリ：一般的な環境



この環境で、SMA 1 は ESA 1～3 および WSA 1 からデータを受信しているプライマリセキュリティ管理アプライアンスです。SMA 2 は SMA 1 からバックアップデータを受信しているバックアップセキュリティ管理アプライアンスです。

失敗した場合は、SMA 2 がプライマリセキュリティ管理アプライアンスになるように設定する必要があります。

SMA 2 を新しいプライマリセキュリティ管理アプライアンスとして設定し、サービスを復元するには、次の手順を実行します。

## 手順

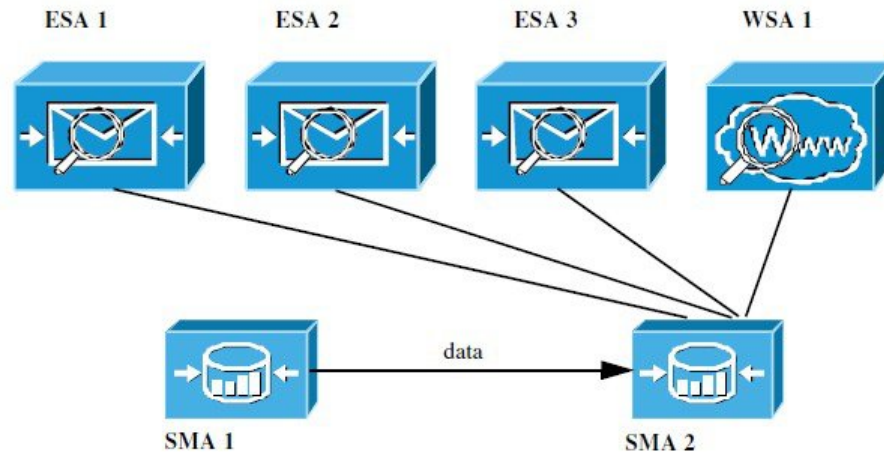
|        | コマンドまたはアクション                                                                                                                     | 目的                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | 集約ポリシー、ウイルス、およびアウトブレイク隔離を使用している場合は以下を実行します。 <ul style="list-style-type: none"> <li>各 E メールセキュリティアプライアンスで、集約隔離を無効にします。</li> </ul> | E メールセキュリティアプライアンスのマニュアルで集約されたポリシー、ウイルス、およびアウトブレイク隔離を無効にする方法を参照してください。これは各 E メールセキュリティアプライアンスで内部隔離を作成し、それを後で新しいセキュリティ管理アプライアンスに移行します。 |

|        | コマンドまたはアクション                                                                                                                                                          | 目的                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | プライマリ セキュリティ管理アプライアンス (SMA1) から保存した設定ファイルを、バックアップセキュリティ管理アプライアンス (SMA2) にロードします。                                                                                      | <a href="#">コンフィギュレーションファイルのロード (561 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                  |
| ステップ 3 | 障害が発生した SMA 1 から IP アドレスを再作成し、SMA 2 の IP アドレスに設定します。                                                                                                                  | <ol style="list-style-type: none"> <li>SMA 2 で、[ネットワーク (Network)] &gt; [IP インターフェイス (IP Interfaces)] &gt; [IP インターフェイスの追加 (Add IP Interfaces)] を選択します。</li> <li>[IP インターフェイスの追加 (Add IP Interfaces)] ページで、障害が発生した SMA1 のすべての関連 IP 情報をテキスト フィールドに入力して、SMA 2 のインターフェイスを再作成します。</li> </ol> <p>IP インターフェイスの追加の詳細については、<a href="#">IP インターフェイスの設定 (632 ページ)</a> を参照してください。</p> |
| ステップ 4 | 変更を送信し、保存します。                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                           |
| ステップ 5 | 新しいセキュリティ管理アプライアンス (SMA 2) で、適用可能なすべての中央集中型サービスを有効にします。                                                                                                               | <a href="#">セキュリティ管理アプライアンスでのサービスの設定 (21 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                              |
| ステップ 6 | すべてのアプライアンスを新しいセキュリティ管理アプライアンス (SMA 2) に追加します。 <ul style="list-style-type: none"> <li>アプライアンスへの接続を確立し、その接続をテストすることで、各アプライアンスがイネーブルとなり、機能していることをテストして確認します。</li> </ul> | <a href="#">管理対象アプライアンスの追加について (19 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                    |
| ステップ 7 | 集約ポリシー、ウイルス、およびアウトブレイク隔離を使用している場合、新しいセキュリティ管理アプライアンス上に隔離の移行を設定し、その後必要な E メールセキュリティアプライアンスごとに移行を有効にして設定します。                                                            | <a href="#">ポリシー、ウイルス、およびアウトブレイク隔離の集約 (359 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                            |
| ステップ 8 | 必要に応じて、追加データを復元します。                                                                                                                                                   | <a href="#">その他の重要なバックアップタスク (520 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                                     |

### 次のタスク

このプロセスが完了した後、SMA 2 がプライマリ セキュリティ管理アプライアンスになります。これで、次の図に示すように、ESA 1～3 と WSA 1 からすべてのデータが SMA 2 に送られるようになりました。

図 15: ディザスタ リカバリ: 最終結果



## アプライアンスハードウェアのアップグレード

「バックアップアプライアンスのプライマリアプライアンスとしての使用 (520 ページ)」を参照してください。

## AsyncOS のアップグレード

- アップグレード用のバッチ コマンド (524 ページ)
- アップグレードとアップデートのネットワーク要件の決定 (524 ページ)
- アップグレード方式の選択: リモートまたはストリーミング (525 ページ)
- アップグレードおよびサービス アップデートの設定 (528 ページ)
- アップグレードする前に: 重要な手順 (534 ページ)
- AsyncOS のアップグレード (524 ページ)
- バックグラウンドダウンロードのキャンセルまたは削除ステータスの表示 (537 ページ)
- アップグレード後 (537 ページ)

## アップグレード用のバッチ コマンド

アップグレード手順用のバッチ コマンドの詳細については、AsyncOS for Email の CLI リファレンス ガイドを参照してください <http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html>

## アップグレードとアップデートのネットワーク要件の決定

Cisco コンテンツ セキュリティ アプライアンスのアップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、AsyncOS アッ

プグレードに対して静的な参照先を設定する必要がある場合があります。アップグレードに関して、ファイアウォール設定にスタティック IP が必要であると判断した場合は、Cisco カスタマーサポートに連絡して、必要な URL アドレスを取得してください。



(注) 既存のファイアウォールルールで `upgrades.cisco.com` ポート (22、25、80、4766 など) からのレガシーアップグレードのダウンロードが許可されている場合は、それらを削除するか、修正したファイアウォールルールに置き換える必要があります。

## アップグレード方式の選択：リモートまたはストリーミング

Cisco はアプライアンスでの AsyncOS のアップグレード用に、以下の 2 種類の方法 (または「ソース」) を提供しています。

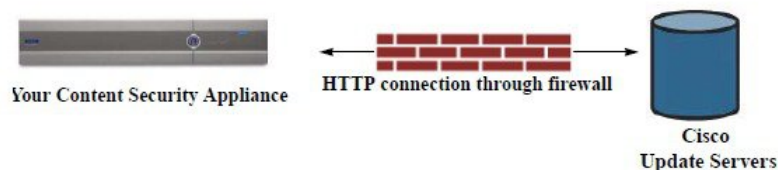
- ストリーミングアップグレード：各アプライアンスは Cisco コンテンツセキュリティアップグレードサーバから HTTP を介して AsyncOS アップグレードを直接ダウンロードします。
- リモートアップグレード：Cisco からアップグレードイメージを 1 回だけダウンロードし、アプライアンスに保存します。次に、アプライアンスは、ネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。

[アップグレードおよびサービスアップデートの設定 \(528 ページ\)](#) にある、アップグレード方式を設定します。オプションで、CLI で `updateconfig` コマンドを使用します。

### ストリーミングアップグレードの概要

ストリーミングアップグレードでは、各 Cisco コンテンツセキュリティアプライアンスが直接 Cisco コンテンツセキュリティアップデートサーバに接続して、アップグレードを検索してダウンロードします。

図 16: ストリーミングアップデートの方法



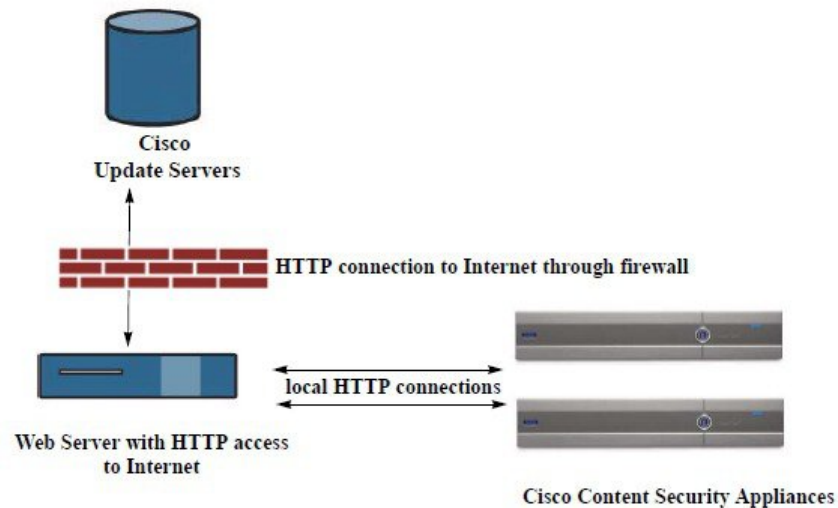
この方式では、アプライアンスが Cisco コンテンツセキュリティアップデートサーバにネットワークから直接接続する必要があります。

### リモートアップグレードの概要


また、Cisco アップデートサーバから直接アップデートを取得する (ストリーミングアップグレード) のではなく、ネットワーク内からローカルで AsyncOS にアップデートをダウンロードおよびホストする (リモートアップグレード) こともできます。この機能を使用して、イン

ターネットにアクセスできるネットワーク上のすべてのサーバにHTTPで暗号化されたアップデートイメージをダウンロードします。アップデートイメージをダウンロードする場合は、内部HTTPサーバ（アップデートマネージャ）を設定し、セキュリティ管理アプライアンスでAsyncOSイメージをホスティングできます。

図 17: リモートアップデートの方法



基本的なプロセスは、次のとおりです。

- 
- ステップ 1** リモートアップグレードのハードウェア要件およびソフトウェア要件（527ページ）およびリモートアップグレードイメージのホスティング（527ページ）の情報をお読みください。
- ステップ 2** アップグレードファイルを取得および供給するようにローカルサーバを設定します。
- ステップ 3** アップグレードファイルをダウンロードします。
- ステップ 4** （新しい Web インターフェイスのみ）クラウド E メールセキュリティ管理コンソールで、歯車（) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 5** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アップデート設定の選択 (Update SettingsChoose)] を選択します。
- このページで、ローカルサーバを使用するようにアプライアンスを設定することを指定します。
- ステップ 6** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [システムのアップグレード (System Upgrade)] を選択します
- ステップ 7** [利用可能なアップグレード (Available Upgrades)] をクリックします。
- (注) コマンドラインプロンプトから **updateconfig** コマンドを実行し、次に **upgrade** コマンドを実行することもできます。
- 詳細については、[AsyncOS のアップグレード \(524 ページ\)](#) を参照してください。
-

## リモートアップグレードのハードウェア要件およびソフトウェア要件

AsyncOS アップグレードファイルのダウンロードでは、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- Cisco コンテンツセキュリティアプライアンスのアップデートサーバへのインターネットアクセス。
- Web ブラウザ。



- (注) 今回のリリースでアップデートサーバのアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用する必要があります。

AsyncOS アップデートファイルのホスティングでは、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- Web サーバ。たとえば、次のような Microsoft IIS (Internet Information Services) または Apache オープンソースサーバ。
  - 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
  - ディレクトリの参照ができること
  - 匿名認証 (認証不要) または基本 (「シンプル」) 認証用に設定されていること
  - 各 AsyncOS アップデートイメージ用に最低 350 MB 以上の空きディスク領域が存在すること

## リモートアップグレードイメージのホスティング

ローカルサーバの設定が完了したら、[http://updates.ironport.com/fetch\\_manifest.html](http://updates.ironport.com/fetch_manifest.html) にアクセスしてアップグレードイメージの zip ファイルをダウンロードします。イメージをダウンロードするには、Cisco コンテンツセキュリティアプライアンスのシリアル番号とバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。アップグレードイメージの zip ファイルをダウンロードするアップグレードバージョンをクリックします。AsyncOS アップグレードのアップグレードイメージを使用するには、ローカルサーバの基本 URL を [更新設定を編集 (Edit Update Settings)] ページに入力します (または CLI の updateconfig を使用します)。

ネットワーク上の Cisco コンテンツセキュリティアプライアンスに使用可能なアップグレードを、[http://updates.ironport.com/fetch\\_manifest.html](http://updates.ironport.com/fetch_manifest.html) で選択したバージョンに限定する XML ファイルを、ローカルサーバでホスティングすることもできます。この場合でも、Cisco コンテンツセキュリティアプライアンスはアップグレードをシスコサーバからダウンロードします。アップグレードリストをローカルサーバにホスティングする場合は、zip ファイルをダウンロードして、`asyncos/phoebe-my-upgrade.xml` ファイルをローカルサーバのルートディレクトリに展開します。AsyncOS アップグレードのアップグレードリストを使用するには、XML ファイルの完全 URL を [更新設定を編集 (Edit Update Settings)] ページに入力します (または CLI の updateconfig を使用します)。

リモートアップグレードの詳細については、ナレッジベース（[ナレッジベースの記事（657ページ）](#)）を参照を確認するか、サポートプロバイダーにお問い合わせください。

## リモートアップグレード方式における重要な違い

ストリーミングアップグレード方式と比較して、AsyncOSをローカルサーバからアップグレード（リモートアップグレード）する場合には、次の違いがあることに注意してください。

- ダウンロード中に、アップグレードによるインストールがすぐに実行されます。
- アップグレードプロセスの最初の10秒間、バナーが表示されます。このバナーが表示されている間は、Ctrlを押した状態でCを押すと、ダウンロードの開始前にアップグレードプロセスを終了できます。

## アップグレードおよびサービスアップデートの設定

Cisco コンテンツ セキュリティ アプライアンスがセキュリティ サービス アップデート（時間帯ルールなど）および AsyncOS アップグレードをダウンロードする方法を設定できます。たとえば、イメージを利用できる場所にシスコサーバまたはローカルサーバのどちらからアップグレードおよびアップデートを動的にダウンロードするかを選択したり、アップデート間隔を設定したり、自動アップデートを無効にしたりすることができます。

AsyncOSは、新しい AsyncOS アップグレードを除く、すべてのセキュリティ サービス コンポーネントへの新しいアップデートがないか、定期的にアップデートサーバに問い合わせます。AsyncOSをアップグレードするには、AsyncOSが使用可能なアップグレードを問い合わせるよう、手動で要求する必要があります。

アップグレードおよびアップデート設定は、GUI（次の2つの項を参照）で、またはCLIでupdateconfig コマンドを使用して設定できます。

アップグレード通知を設定することもできます。

## アップグレードとアップデートの設定

次の表に、設定可能なアップデートおよびアップグレード設定を示します。



表 78: セキュリティ サービスのアップデート設定

| 設定                                             | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アップデート サーバ<br>(イメージ) (Update Servers (images)) | <p>シスコサーバまたはローカル Web サーバのどちらから、AsyncOS アップグレードおよびサービス アップデート ソフトウェア イメージ (時間帯ルールや機能キーのアップデートなど) をダウンロードするかを選択します。デフォルトでは、アップグレードおよびアップデートの両方でシスコ サーバが選択されます。</p> <p>次の場合、ローカル Web サーバを使用する場合があります。</p> <ul style="list-style-type: none"> <li>• スタティック アドレスからアプライアンスにイメージをダウンロードする必要がある。<a href="#">厳格なファイアウォールポリシーを適用している環境のスタティックアップグレードおよびアップデートサーバ設定 (530 ページ)</a> を参照してください。</li> <li>• 適宜、アプライアンスに AsyncOS アップグレードイメージをダウンロードする (この場合でも、Cisco アップデートサーバからサービス アップデート イメージを動的にダウンロードできます)。</li> </ul> <p>ローカルアップデートサーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。</p> <p>詳細については、<a href="#">アップグレード方式の選択: リモートまたはストリーミング (525 ページ)</a> および <a href="#">リモートアップグレードの概要 (525 ページ)</a> を参照してください。</p> |
| アップデートサーバ<br>(リスト) (Update Servers (lists))    | <p>利用可能なアップグレードおよびサービス アップデートのリスト (マニフェスト XML ファイル) を、シスコサーバとローカル Web サーバのどちらからダウンロードするかを選択します。</p> <p>アップグレードおよびアップデートの両方で、デフォルトはシスコサーバです。アップグレードとアップデートには、それぞれ異なる設定を選択できます。</p> <p>該当する場合は、<a href="#">厳格なファイアウォールポリシーを適用している環境のスタティックアップグレードおよびアップデートサーバ設定 (530 ページ)</a> を参照してください。</p> <p>ローカルアップデートサーバを選択した場合、サーバのファイル名およびポート番号を含む、各リストのマニフェスト XML ファイルのフルパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスワードも入力します。</p> <p>詳細については、<a href="#">アップグレード方式の選択: リモートまたはストリーミング (525 ページ)</a> および <a href="#">リモートアップグレードの概要 (525 ページ)</a> を参照してください。</p>                                                                                                                                                                       |
| 自動更新                                           | <p>時間帯ルールの自動アップデートをイネーブルにするかどうかを選択します。イネーブルにする場合は、アップデートを確認する間隔を入力します。分の場合は <b>m</b>、時間の場合は <b>h</b>、日の場合は <b>d</b> を末尾に追加します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| 設定                                    | 説明                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| インターフェイス<br>(Interface)               | 時間帯ルールやAsyncOSアップグレードなどをアップデートサーバに問い合わせるときに、どのネットワークインターフェイスを使用するかを選択します。利用可能なプロキシデータインターフェイスが表示されます。デフォルトでは、アプライアンスは使用するインターフェイスを選択します。                                                                                                                                                                                    |
| HTTP プロキシサーバ<br>(HTTP Proxy Server)   | <p>アップストリームの HTTP プロキシサーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。</p> <p>プロキシサーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。</p> <p>このプロキシサーバは、クラウドからファイル分析レポートの詳細を取得するためにも使用されます。<a href="#">ファイル分析レポートの詳細の要件 (95 ページ)</a> (Web レポート)、または<a href="#">ファイル分析レポートの詳細の要件 (219 ページ)</a> (電子メール レポート) も参照してください。</p>  |
| HTTPS プロキシサーバ<br>(HTTPS Proxy Server) | <p>アップストリームの HTTPS プロキシサーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスワードをここに入力します。</p> <p>プロキシサーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。</p> <p>このプロキシサーバは、クラウドからファイル分析レポートの詳細を取得するためにも使用されます。<a href="#">ファイル分析レポートの詳細の要件 (95 ページ)</a> (Web レポート)、または<a href="#">ファイル分析レポートの詳細の要件 (219 ページ)</a> (電子メール レポート) も参照してください。</p> |

## 厳格なファイアウォールポリシーを適用している環境のスタティックアップグレードおよびアップデートサーバ設定

AsyncOS アップデートサーバは、ダイナミック IP アドレスを使用します。環境にスタティック IP アドレスが必要な厳格なファイアウォールポリシーを適用している場合は、[アップデート設定 (Update Settings)] ページで次の設定を使用します。

図 18: [アップデートサーバ(イメージ) (Update Servers (images))] 設定のスタティック URL

|                                                                                     |                                                                                                                                                                                                                                                 |                                                  |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Update Servers (images):                                                            | <p>The update servers will be used to obtain <b>update images</b> for the following services:</p> <ul style="list-style-type: none"> <li>- Feature Key updates</li> <li>- Time zone rules</li> <li>- Cisco IronPort AsyncOS upgrades</li> </ul> |                                                  |
|                                                                                     | <input type="radio"/> Cisco IronPort Update Servers                                                                                                                                                                                             |                                                  |
|                                                                                     | <input checked="" type="radio"/> Local Update Servers (location of update image files)                                                                                                                                                          |                                                  |
| Base Url (all services except Time zone rules and Cisco IronPort AsyncOS upgrades): | <input type="text" value="http://downloads-static.ironport.com"/>                                                                                                                                                                               | Port: <input type="text" value="80"/>            |
|                                                                                     | <small>http://downloads.example.com</small>                                                                                                                                                                                                     |                                                  |
|                                                                                     | Authentication (optional):                                                                                                                                                                                                                      |                                                  |
|                                                                                     | Username: <input type="text"/>                                                                                                                                                                                                                  |                                                  |
|                                                                                     | Password: <input type="text"/>                                                                                                                                                                                                                  |                                                  |
|                                                                                     | Retype Password: <input type="text"/>                                                                                                                                                                                                           |                                                  |
| Base Url (Time zone rules):                                                         | <input type="text" value="downloads-static.ironport.com:80"/>                                                                                                                                                                                   |                                                  |
|                                                                                     | <small>format: downloads.example.com:80</small>                                                                                                                                                                                                 |                                                  |
|                                                                                     | <input type="button" value="Click to use different settings for AsyncOS upgrades:"/>                                                                                                                                                            |                                                  |
|                                                                                     | <b>AsyncOS Upgrade settings</b>                                                                                                                                                                                                                 |                                                  |
|                                                                                     | <input type="radio"/> Cisco IronPort Update Servers                                                                                                                                                                                             |                                                  |
|                                                                                     | <input checked="" type="radio"/> Local Update Servers (location of update image files)                                                                                                                                                          |                                                  |
| Host (Cisco IronPort AsyncOS upgrades):                                             | <input type="text" value="updates-static.ironport.com."/>                                                                                                                                                                                       | Port: <input type="text" value="80"/> (optional) |
|                                                                                     | <small>Ex. downloads.example.com</small>                                                                                                                                                                                                        |                                                  |

図 19: [アップデートサーバ(リスト) (Update Servers (list))] 設定のスタティック URL

|                        |                                                                                                                                                                                            |                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Update Servers (list): | <p>The URL will be used to obtain the <b>list of available updates</b> for the following services:</p> <ul style="list-style-type: none"> <li>- Time zone rules</li> </ul>                 |                                        |
|                        | <input type="radio"/> Cisco IronPort Update Servers                                                                                                                                        |                                        |
|                        | <input checked="" type="radio"/> Local Update Servers (location of list of available updates file)                                                                                         |                                        |
| Full Url               | <input type="text" value="http://update-manifests.ironport.com"/>                                                                                                                          | Port: <input type="text" value="443"/> |
|                        | <small>http://updates.example.com/my_updates.xml</small>                                                                                                                                   |                                        |
|                        | Authentication (optional):                                                                                                                                                                 |                                        |
|                        | Username: <input type="text"/>                                                                                                                                                             |                                        |
|                        | Password: <input type="text"/>                                                                                                                                                             |                                        |
|                        | Retype Password: <input type="text"/>                                                                                                                                                      |                                        |
|                        | <p>The URL will be used to obtain the <b>list of available updates</b> for the following services:</p> <ul style="list-style-type: none"> <li>- Cisco IronPort AsyncOS upgrades</li> </ul> |                                        |
|                        | <input type="radio"/> Cisco IronPort Update Servers                                                                                                                                        |                                        |
|                        | <input checked="" type="radio"/> Local Update Servers (location of list of available updates file)                                                                                         |                                        |
| Full Url               | <input type="text" value="http://update-manifests.ironport.com"/>                                                                                                                          | Port: <input type="text" value="443"/> |
|                        | <small>http://updates.example.com/my_updates.xml</small>                                                                                                                                   |                                        |
|                        | Authentication (optional):                                                                                                                                                                 |                                        |
|                        | Username: <input type="text"/>                                                                                                                                                             |                                        |
|                        | Password: <input type="text"/>                                                                                                                                                             |                                        |
|                        | Retype Password: <input type="text"/>                                                                                                                                                      |                                        |

表 79: 厳格なファイアウォールポリシーを適用している環境のスタティックアドレス

| セクション                   | 設定                                                                                                                    | スタティック URL/IP アドレスおよびポート                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Update Servers (images) | ベースURL (タイムゾーンルールおよび AsyncOSアップグレード以外のすべてのサービス) (Base URL (all services except Time zone rules and AsyncOS upgrades)) | http://downloads-static.ironport.com<br>204.15.82.8<br>Port 80 |
|                         | ベースURL (タイムゾーンルール) (Base URL (Time zone rules))                                                                       | downloads-static.ironport.com<br>204.15.82.8<br>Port 80        |
|                         | ホスト (AsyncOSアップグレード) (Host (AsyncOS upgrades))                                                                        | updates-static.ironport.com<br>208.90.58.25<br>Port 80         |
| Update Servers (list):  | 物理ハードウェア アプライアンスでのアップデート用 :<br>フルURL (Full URL)                                                                       | update-manifests.ironport.com<br>208.90.58.5<br>Port 443       |
|                         | 仮想アプライアンスでのアップデート用 : フルURL (For updates on virtual appliances: Full URL)                                              | update-manifests.sco.cisco.com<br>Port 443                     |
|                         | アップグレード用 : フルURL (For upgrades: Full URL)                                                                             | update-manifests.ironport.com<br>208.90.58.5<br>Port 443       |



**重要** CLI で `updateconfig` コマンドの `dynamichost` サブコマンドを使用して、`update-manifests` URL とポート番号を設定する必要があります。これにより、サービスの更新が検証されます。

## GUIからのアップデートおよびアップグレード設定値の設定

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アップデート設定 (Update Settings)] を選択します。
- ステップ 3** [更新設定を編集 (Edit Update Settings)] をクリックします。
- [アップグレードとアップデートの設定 \(528 ページ\)](#) の説明を使用して、この手順の設定を構成します。

- ステップ 4** [アップデートサーバ(イメージ) (Update Servers (images)) ] セクションで、アップデートのイメージのダウンロード元のサーバを指定します。
- ステップ 5** AsyncOS アップグレードのイメージをダウンロードする元のサーバを指定します。
- 同じセクションの下部で、[クリックして AsyncOS アップグレードの異なる設定を使用する (Click to use different settings for AsyncOS upgrades) ] リンクをクリックします。
  - AsyncOS アップグレードのイメージをダウンロードするためのサーバ設定を指定します。
- ステップ 6** [アップデートサーバ(リスト) (Update Servers (list)) ] セクションで、使用可能なアップデートおよび AsyncOS アップグレードのリストを取得するサーバを指定します。
- 上部のサブセクションはアップデートに適用されます。下部のサブセクションはアップグレードに適用されます。
- ステップ 7** 時間帯ルールおよびインターフェイスの設定を指定します。
- ステップ 8** (任意) プロキシサーバの設定を指定します。
- ステップ 9** 変更を送信し、保存します。
- ステップ 10** 結果が予定通りか確認します。

[アップデート設定 (Update Settings) ] ページが表示されていない場合は、[管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [アップデート設定 (Update Settings) ] を選択します。

一部の URL では、サーバ URL に「asyncos」ディレクトリが追加されます。この不一致は無視してかまいません。

## アップグレードの通知

デフォルトでは、AsyncOS アップグレードがアプライアンスで使用可能な場合、管理者および技術者の権限を持つユーザには、Web インターフェイスの上部に通知が表示されます。

| 目的                                                     | 操作手順                                                                           |
|--------------------------------------------------------|--------------------------------------------------------------------------------|
| 最新のアップグレードの詳細情報を表示する                                   | アップグレード通知にカーソルを合わせます。                                                          |
| 使用できるすべてのアップグレードのリストを表示する                              | 通知の下向き矢印をクリックします。                                                              |
| 現在の通知を閉じる<br>新しいアップグレードが入手可能になるまで、アプライアンスは別の通知を表示しません。 | 下向き矢印をクリックして[通知を消去 (Clear the notification) ] を選択してから、[閉じる (Close) ] をクリックします。 |

| 目的                        | 操作手順                                                                                                   |
|---------------------------|--------------------------------------------------------------------------------------------------------|
| 今後の通知を中止する（管理者権限を持つユーザのみ） | [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[システムアップグレード（System Upgrade）]に移動します。 |

## アップグレードする前に：重要な手順

### 始める前に

[アップグレードとアップデートのネットワーク要件の決定（524ページ）](#) でネットワーク要件を参照してください。

**ステップ1** 次のようにして、データの消失を防止する、または最小限に抑えます。

- 新しいアプライアンスに十分なディスク容量があり、転送される各データタイプに同等以上のサイズが割り当てられていることを確認します。[最大ディスク領域と割り当てについて（569ページ）](#)を参照してください。
- ディスク領域についての何らかの警告を受け取った場合は、アップグレードを開始する前に、ディスク領域に関する問題をすべて解決してください。

**ステップ2** アプライアンスから、XML コンフィギュレーションファイルを保存します。[現在の設定ファイルの保存およびエクスポート（560ページ）](#)で説明する警告を参照してください。

何らかの理由でアップグレード前のリリースに戻す場合は、このファイルが必要です。

**ステップ3** セーフリスト/ブロックリスト機能を使用している場合は、リストをボックスからエクスポートします。

[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[設定ファイル（Configuration File）]をクリックしてスクロールダウンします。

**ステップ4** CLI からアップグレードを実行している場合は、**suspendlistener** コマンドを使用してリスナーを停止します。GUI からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。

**ステップ5** メールキューとデリバリキューを解放します。

**ステップ6** アップグレード設定が希望どおりに設定されていることを確認します。「[アップグレードおよびサービスアップデートの設定（528ページ）](#)」を参照してください。

## AsyncOS のアップグレード

1回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードした後でインストールできます。



- (注) AsyncOS を Cisco サーバからではなくローカルサーバから 1 回の操作でダウンロードとアップグレードする場合は、アップグレードはダウンロード中に即座に実行されます。アップグレードプロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレードプロセスを終了できます。

### 始める前に

- Cisco から直接アップグレードをダウンロードするか、またはネットワーク上のサーバからアップグレードイメージをホストするかを選択します。次に、選択した方式をサポートするようにネットワークをセットアップします。そして、選択した入手先からアップグレードを入手するためにアプライアンスを設定します。[アップグレード方式の選択：リモートまたはストリーミング \(525 ページ\)](#) および [アップグレードおよびサービスアップデートの設定 \(528 ページ\)](#) を参照してください。
- アップグレードをインストールする前に、[アップグレードする前に：重要な手順 \(534 ページ\)](#) の手順を実行してください。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [システムのアップグレード (System Upgrade) ] を選択します。
- ステップ 3** [アップグレードオプション (Upgrade Options) ] をクリックします。
- ステップ 4** 次のオプションを選択します。

| 目的                                | 操作手順                                                                                                                                 |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| 1 回の操作でアップグレードのダウンロードとインストールを実行する | [ダウンロードしてインストール (Download and Install) ] をクリックします。<br>すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。                                |
| アップグレードインストーラをダウンロードする            | [ダウンロードのみ (Download only) ] をクリックします。<br>すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。<br>インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。 |

| 目的                             | 操作手順                                                                                                                                                  |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| ダウンロードしたアップグレードインストーラをインストールする | <p>[Install (インストール)] をクリックします。</p> <p>このオプションは、インストーラがダウンロードされている場合にのみ表示されます。</p> <p>インストールする AsyncOS のバージョンは、[インストール (Install)] オプションの下に表示されます。</p> |

**ステップ 5** 以前にダウンロードしたインストーラでインストールする場合を除き、利用可能なアップグレードのリストから AsyncOS のバージョンを選択します。

**ステップ 6** インストール中の場合、次に従います。

- 現在の設定をアプライアンス上の `configuration` ディレクトリに保存するかどうかを選択します。
- コンフィギュレーションファイルでパスフレーズをマスクするかどうかを選択します。

(注) マスクされたパスフレーズが記載されたコンフィギュレーションファイルは、GUI の [設定ファイル (Configuration File)] ページや CLI の `loadconfig` コマンドからロードできません。

- コンフィギュレーションファイルのコピーを電子メールで送信する場合は、ファイルを送信する電子メールアドレスを入力します。複数の電子メールアドレスを指定する場合は、カンマで区切ります。

**ステップ 7** [続行 (Proceed)] をクリックします。

**ステップ 8** インストール中の場合、次に従います。

- プロセス中のプロンプトに応答できるようにしてください。

応答するまでプロセスは中断されます。

ページの上部の近くに、経過表示バーが表示されます。

- プロンプトで、[今すぐ再起動 (Reboot Now)] をクリックします。

(注) リブートしてから少なくとも 20 分経過するまで、いかなる理由があっても (アップグレードの問題をトラブルシューティングするためであっても) アプライアンスの電源を中断しないでください。

- 約 10 分後、アプライアンスにアクセスしてログインします。

### 次のタスク

- プロセスが中断された場合、プロセスを再開する必要があります。
- アップグレードをダウンロードしてインストールしなかった場合は次のとおりです。  
アップグレードをインストールする準備ができたなら、「始める前に」の項の前提条件も含め次の手順を最初から実行しますが、[インストール (Install)] オプションを選択します。
- アップグレードをインストールしている場合は、[アップグレード後 \(537 ページ\)](#) を参照してください。



## バックグラウンドダウンロードのキャンセルまたは削除ステータスの表示

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [システムのアップグレード (System Upgrade) ] を選択します。
- ステップ 3** [アップグレードオプション (Upgrade Options) ] をクリックします。
- ステップ 4** 次のオプションを選択します。

| 目的                 | 操作手順                                                                                                                                               |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| ダウンロードステータスの表示     | ページの中央を確認してください。<br>進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。<br>アップグレードのステータスは <code>upgrade_logs</code> でも確認できます。 |
| ダウンロードのキャンセル       | ページの中央にある、[ダウンロードをキャンセル (Cancel Download) ] ボタンをクリックします。<br>このオプションは、ダウンロード進行中にのみ表示されます。                                                           |
| ダウンロードされたインストーラの削除 | ページの中央にある、[ファイルを削除 (Delete File) ] ボタンをクリックします。<br>このオプションは、インストーラがダウンロードされている場合にのみ表示されます。                                                         |

## アップグレード後

アップグレードが完了したら、次の手順を実行します。

- (関連する E メールセキュリティアプライアンスのある導入環境の場合) リスナーを再度イネーブルにします。
- (関連する Web セキュリティアプライアンスのある導入環境の場合) 最新の Configuration Master をサポートするようにシステムを設定します。 [Configuration Master を使用して中央集中型で Web セキュリティアプライアンスを管理する \(390 ページ\)](#) を参照してください。

- 設定を保存するかどうか判断します。詳細については、[設定の保存とインポート \(559 ページ\)](#) を参照してください。
- アップグレード後オンライン ヘルプを表示するには、ブラウザ キャッシュをクリアし、ブラウザを終了してもう一度開きます。これにより、期限切れのコンテンツのブラウザ キャッシュがクリアされます。

## AsyncOS の以前のバージョンへの復元について

緊急時には、前の認定バージョンの AsyncOS に戻すことができます。

アプライアンス上のすべてのデータをクリアし、新しい、クリーンな設定から始める場合は、現在実行中のビルドに戻すこともできます。

### 関連項目

- [復元の影響に関する重要な注意事項 \(538 ページ\)](#)
- [AsyncOS の復元 \(538 ページ\)](#)

## 復元の影響に関する重要な注意事項

Cisco コンテンツ セキュリティ アプライアンスにおける `revert` コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての既存の設定およびデータを永久破壊します。さらに、復元ではアプライアンスが再設定されるまでメール処理が中断されます。

復元によって機能キーまたは仮想アプライアンスライセンスの有効期限日に影響が及ぶことはありません。

## AsyncOS の復元

### 始める前に

- 保持する必要があるデータをアプライアンス以外の場所にバックアップまたは保存します。
- 戻し先のバージョンのコンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルに下位互換性はありません。
- このコマンドはすべての設定を破壊するため、復元を実行する場合は、アプライアンスへの物理的なローカル アクセスを必ず用意するようにしてください。
- お使いの E メール セキュリティ アプライアンスで隔離が有効になっている場合は、それらのアプライアンスでローカルにメッセージが隔離されるように集約化を無効にします。

---

**ステップ 1** 戻し先のバージョンのコンフィギュレーション ファイルがあることを確認してください。コンフィギュレーション ファイルに下位互換性はありません。

**ステップ 2** アプライアンスの現在の設定のバックアップ コピーを、（パスフレーズをマスクしない状態で）別のマシンに保存します。コンフィギュレーションファイルを取得するには、ファイルを電子メールでユーザ自身に送信するか、ファイルを FTP で取得します。簡単に行うには、`mailconfig CLI` コマンドを実行すると、アプライアンスの現在のコンフィギュレーションファイルが指定したメールアドレスに送信されます。

（注） このコピーは、バージョンを戻した後にロードする設定ファイルではありません。

**ステップ 3** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースを別のマシンにエクスポートします。

**ステップ 4** Email Security Appliances で、すべてのリスナーを一時停止します。

**ステップ 5** メール キューが空になるまで待ちます。

**ステップ 6** バージョンを戻すアプライアンスの CLI にログインします。

`revert` コマンドの実行時には、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元前の手順を完了するまで、復元プロセスを開始しないでください。

**ステップ 7** コマンドラインプロンプトから `revert` コマンドを入力し、プロンプトに応答します。

次に、`revert` コマンドの例を示します。

例：

```
m650p03.prep> revert
This command will revert the appliance to a previous version of AsyncOS.
WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
  quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco Spam Quarantine message and end-user safelist/blocklist data
Only the network settings will be preseved.
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passphrases
  unmasked)
- exported the Cisco Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty
Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired version.
Do you want to continue? yes
Are you sure you want to continue? yes
Available versions
=====
  1. 7.2.0-390
  2. 6.7.6-020
Please select an AsyncOS version: 1
You have selected "7.2.0-390".
Reverting to "testing" preconfigure install mode.
The system will now reboot to perform the revert operation.
```

**ステップ 8** アプライアンスが 2 回リブートするまで待ちます。

- ステップ 9** CLI を使用してアプライアンスにログインします。
- ステップ 10** 少なくとも 1 つの Web セキュリティ アプライアンスを追加し、URL カテゴリ アップデートがそのアプライアンスからダウンロードされるまで数分待ちます。
- ステップ 11** URL カテゴリのアップデートが完了したら、戻し先のバージョンのコンフィギュレーションファイルをロードします。
- ステップ 12** セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリストデータベースをインポートして復元します。
- ステップ 13** Email Security Appliances で、すべてのリスナーを再びイネーブルにします。
- ステップ 14** 変更を保存します。

これで、復元が完了した Cisco コンテンツ セキュリティ アプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

(注) 復元が完了して、Cisco コンテンツ セキュリティ アプライアンスへのコンソールアクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

---

## アップデートについて

サービスアップデートは定期的にダウンロード可能にできます。これらのダウンロードの設定を指定するには、[アップグレードおよびサービス アップデートの設定 \(528 ページ\)](#)

### 関連項目

- [アップグレードおよびサービス アップデートの設定 \(528 ページ\)](#)

## Web 使用率制御の URL カテゴリ セット アップデートについて

- [URL カテゴリ セットの更新の準備および管理 \(421 ページ\)](#)
- [URL カテゴリ セットの更新とレポート \(211 ページ\)](#)

## 生成されたメッセージの返信アドレスの設定

次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

- バウンス メッセージ
- レポート

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

GUI の [システム管理 (System Administration)] メニューから利用できる [返信先アドレス (Return Addresses)] ページを使用するか、CLI で **addressconfig** コマンドを使用します。

システムで生成された電子メールメッセージの返信アドレスを GUI で変更するには、[返信先アドレス (Return Addresses)] ページで [設定の編集 (Edit Settings)] をクリックします。1 つまたは複数のアドレスを変更して [送信 (Submit)] をクリックし、変更を保存します。

## アラートの管理

アプライアンスから、アプライアンスで発生しているイベントに関する電子メールアラートが送信されます。

| 目的                                                                                                                                       | 操作手順                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| タイプの異なるアラートが別の管理ユーザに送信されるようにする                                                                                                           | <p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [アラート (Alerts)] を選択します。</p> <p>システムのセットアップ時に <b>AutoSupport</b> をイネーブルにした場合、指定した電子メールアドレスはデフォルトで、すべての重大度およびクラスのアラートを受信します。この設定はいつでも変更できます。</p> <p>複数のアドレスを指定する場合は、カンマで区切ります。</p> |
| 次のようなアラートのグローバル設定を行う <ul style="list-style-type: none"> <li>アラート送信者 (FROM:) アドレス</li> <li>重複したアラートの制御</li> <li>AutoSupport 設定</li> </ul> | <p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [アラート (Alerts)] を選択します。</p> <p><a href="#">重複したアラートについて (543 ページ)</a> を参照してください</p> <p><a href="#">Cisco AutoSupport (543 ページ)</a> を参照してください</p>                                 |
| 最近のアラートのリストを表示する<br><br>このリストの設定を管理する                                                                                                    | <p><a href="#">最新アラートの表示 (543 ページ)</a> を参照してください</p>                                                                                                                                                                                                                                                                                                                  |
| アラートのリストと説明を表示する                                                                                                                         | <p>参照先 :</p> <p><a href="#">ハードウェアアラートの説明 (544 ページ)</a> 。</p> <p><a href="#">システムアラートの説明 (544 ページ)</a></p>                                                                                                                                                                                                                                                            |

| 目的                | 操作手順                                        |
|-------------------|---------------------------------------------|
| アラートの配信メカニズムを理解する | <a href="#">アラートの配信 (542 ページ)</a> を参照してください |

## アラート タイプおよび重大度

アラート タイプは次のとおりです。

- ハードウェア アラート。[ハードウェア アラートの説明 \(544 ページ\)](#) を参照してください。
- システム アラート。[システム アラートの説明 \(544 ページ\)](#) を参照してください。
- アップデータ アラート。

アラートの重大度は次のとおりです。

- **Critical** : すぐに対処が必要な問題
- **Warning** : 今後モニタリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります
- **Info** : このデバイスのルーティン機能で生成される情報

## アラートの配信

アラートメッセージは Cisco コンテンツ セキュリティ アプライアンス内の問題の通知に使用されるため、送信に AsyncOS の標準メール配信システムを使用しません。代わりに、アラートメッセージは AsyncOS で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メール システムで処理されます。

アラートメール システムは、AsyncOS と同一の設定を共有しません。このため、アラートメッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラートメッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - アラートメッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- 導入環境に E メールセキュリティ アプライアンスが含まれている場合：
  - アラートメッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージフィルタまたはコンテンツ フィルタの処理対象にも含まれません。
  - アラートメッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

## 最新アラートの表示

| 目的                      | 操作手順                                                                                                                                                                                                   |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 最近のアラートのリストを表示する        | 管理者およびオペレータのアクセス権のあるユーザは、[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アラート (Alerts)] を選択し、[上位アラートを表示 (View Top Alerts)] ボタンをクリックします。<br><br>アラートは、電子メールで通知する問題があっても表示されます。 |
| リストをソートする               | 列の見出しをクリックします。                                                                                                                                                                                         |
| このリストに保存するアラートの最大数を指定する | コマンドライン インターフェイス (CLI) で <code>alertconfig</code> コマンドを使用します。                                                                                                                                          |
| この機能を無効にする              | コマンドライン インターフェイス (CLI) で <code>alertconfig</code> コマンドを使用してアラートの最大数をゼロ (0) に設定します。                                                                                                                     |

## 重複したアラートについて

AsyncOS が重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、待機時間が 5 秒の場合、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。

最終的に、送信間隔は非常に長くなります。[重複するアラートを送信する前に待機する最大秒数 (Maximum Number of Seconds to Wait Before Sending a Duplicate Alert)] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、60 秒後、120 秒後といった間隔で送信されます。

## Cisco AutoSupport

シスコによる十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラートメッセージをシスコに送信するように Cisco コンテンツセキュリティアプライアンスを設定できます。「AutoSupport」と呼ばれるこの機能は、カスタマーサポートによるお客様のニーズへのプロアクティブな対応に役立ちます。また、AutoSupport はシステムの稼働時間、`status` コマンドの出力、および使用されている AsyncOS バージョンを通知するレポートを毎週送信します。

デフォルトでは、アラートタイプが System で重大度レベルが Information のアラートを受信するように設定されているアラート受信者は、Cisco に送信される各メッセージのコピーを受信します。内部にアラートメッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能を有効または無効にするには、[管理アプライアンス (Management Appliance)] > [システム管理アラート (System Administration Alerts)] を選択し、[設定の編集 (Edit Settings)] をクリックします。

AutoSupport が有効の場合、Information レベルのシステムアラートを受信するように設定されたアラート受信者に、デフォルトで毎週 AutoSupport レポートが送信されます。

## ハードウェアアラートの説明

表 80: ハードウェアアラートの説明

| アラート名                                 | 説明                                                    | 重大度    |
|---------------------------------------|-------------------------------------------------------|--------|
| INTERFACE.ERRORS                      | インターフェイスエラーを検出した場合に送信されます。                            | 警告     |
| MAIL.MEASUREMENTS_FILESYSTEM          | ディスクパーティションが 75% の使用率に近づいた場合に送信されます。                  | 警告     |
| MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL | ディスクパーティションが 90% の使用率に達した場合 (95%、96%、97% など) に送信されます。 | クリティカル |
| SYSTEM.RAID_EVENT_ALERT               | 重大な RAID-event が発生した場合に送信されます。                        | 警告     |
| SYSTEM.RAID_EVENT_ALERT_INFO          | RAID-event が発生した場合に送信されます。                            | 情報     |

## システムアラートの説明

表 81: システムアラートの説明

| アラート名                    | 説明                           | 重大度               |
|--------------------------|------------------------------|-------------------|
| COMMON.APP_FAILURE       | 不明なアプリケーション障害が発生した場合に送信されます。 | クリティカル (Critical) |
| COMMON.KEY_EXPIRED_ALERT | 機能キーの有効期限が切れた場合に送信されます。      | 警告                |



| アラート名                           | 説明                                        | 重大度 |
|---------------------------------|-------------------------------------------|-----|
| COMMON.KEY_EXPIRING_ALERT       | 機能キーの有効期限が切れる場合に送信されます。                   | 警告  |
| COMMON.KEY_FINAL_EXPIRING_ALERT | 機能キーの有効期限が切れる場合の最後の通知として送信されます。           | 警告  |
| DNS.BOOTSTRAP_FAILED            | アプライアンスがルートDNSサーバに問い合わせることができない場合に送信されます。 | 警告  |
| COMMON.INVALID_FILTER           | 無効なフィルタが存在する場合に送信されます。                    | 警告  |

| アラート名                                                                                                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 重大度               |
|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| IPBLOCKD.HOST_ADDED_TO_WHITELIST<br>IPBLOCKD.HOST_ADDED_TO_BLACKLIST<br>IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST | <p>アラートメッセージ：</p> <ul style="list-style-type: none"> <li>• &lt;IP address&gt;のホストがSSH DoS 攻撃のためブラックリストに追加されました。（The host at &lt;IP address&gt; has been added to the blacklist because of an SSH DOS attack.）</li> <li>• &lt;IP address&gt;のホストがSSH ホワイトリストに追加されました。（The host at &lt;IP address&gt; has been permanently added to the ssh whitelist.）</li> <li>• &lt;IP address&gt;のホストがブラックリストから削除されました（The host at &lt;IP address&gt; has been removed from the blacklist）</li> </ul> <p>SSH を介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しない IP アドレスは、2 分以内に 11 回以上試行に失敗した場合、SSH のブラックリストに追加されます。</p> <p>同じ IP アドレスからユーザが正常にログインすると、その IP アドレスはホワイトリストに追加されます。</p> <p>ホワイトリストのアドレスは、ブラックリストにも登録されていてもアクセスが許可されます。</p> | 警告                |
| LDAP.GROUP_QUERY_FAILED_ALERT                                                                                | LDAP グループクエリに失敗した場合に送信されます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | クリティカル (Critical) |

| アラート名                                | 説明                                            | 重大度                  |
|--------------------------------------|-----------------------------------------------|----------------------|
| LDAP.HARD_ERROR                      | LDAP クエリが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。     | クリティカル<br>(Critical) |
| LOG.ERROR.*                          | さまざまなロギングエラー。                                 | クリティカル               |
| MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED | 各受信者のスキャン時に LDAP グループ クエリーに失敗した場合に送信されます。     | クリティカル               |
| MAIL.QUEUE.ERROR.*                   | メール キューのさまざまなハードエラー。                          | クリティカル               |
| MAIL.RES_CON_START_ALERT.MEMORY      | メモリ使用率がシステムリソース節約しきい値を超過した場合に送信されます。          | クリティカル               |
| MAIL.RES_CON_START_ALERT.QUEUE_SLOW  | メール キューが過負荷となり、システムリソース節約がイネーブルになった場合に送信されます。 | クリティカル               |
| MAIL.RES_CON_START_ALERT.QUEUE       | キュー使用率がシステムリソース節約しきい値を超過した場合に送信されます。          | クリティカル               |
| MAIL.RES_CON_START_ALERT.WORKQ       | ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。    | クリティカル               |
| MAIL.RES_CON_START_ALERT             | アプライアンスが「リソース節約」モードになった場合に送信されます。             | クリティカル               |
| MAIL.RES_CON_STOP_ALERT              | アプライアンスの「リソース節約」モードが解除された場合に送信されます。           | クリティカル               |
| MAIL.WORK_QUEUE_PAUSED_NATURAL       | ワーク キューが中断された場合に送信されます。                       | クリティカル               |

| アラート名                                             | 説明                                                                                             | 重大度                  |
|---------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------|
| MAIL.WORK_QUEUE_UNPAUSED_NATURAL                  | ワークキューが再開された場合に送信されます。                                                                         | クリティカル<br>(Critical) |
| NTP.NOT_ROOT                                      | rootとしてNTPが実行されていないためにアプライアンスが時刻を調整できない場合に送信されます。                                              | 警告                   |
| PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS | ドメイン指定ファイルでエラーが検出された場合に送信されます。                                                                 | クリティカル               |
| PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY         | ドメイン指定ファイルが空の場合に送信されます。                                                                        | クリティカル               |
| PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING       | ドメイン指定ファイルが見つからない場合に送信されます。                                                                    | クリティカル               |
| REPORTD.DATABASE_OPEN_FAILED_ALERT                | レポートエンジンがデータベースを開けない場合に送信されます。                                                                 | クリティカル<br>(Critical) |
| REPORTD.AGGREGATION_DISABLED_ALERT                | システムのディスク領域が不足している場合に送信されます。ログエントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportdは集約をディセーブルにし、アラートを送信します。 | 警告                   |
| REPORTING.CLIENT.UPDATE_FAILED_ALERT              | レポートエンジンがレポートデータを保存できなかった場合に送信されます。                                                            | 警告                   |
| REPORTING.CLIENT.JOURNAL.FULL                     | レポートエンジンが新規データを保存できない場合に送信されます。                                                                | クリティカル               |
| REPORTING.CLIENT.JOURNAL.FREE                     | レポートエンジンが再び新規データを保存できるようになった場合に送信されます。                                                         | 情報                   |

| アラート名                                                  | 説明                                                                | 重大度                  |
|--------------------------------------------------------|-------------------------------------------------------------------|----------------------|
| PERIODIC_REPORTS.REPORT_TASK.<br>BUILD_FAILURE_ALERT   | レポート エンジンがレポートを作成できない場合に送信されます。                                   | クリティカル               |
| PERIODIC_REPORTS.REPORT_TASK.<br>EMAIL_FAILURE_ALERT   | レポートを電子メールで送信できなかった場合に送信されます。                                     | クリティカル               |
| PERIODIC_REPORTS.REPORT_TASK.<br>ARCHIVE_FAILURE_ALERT | レポートをアーカイブできなかった場合に送信されます。                                        | クリティカル<br>(Critical) |
| SENDERBASE.ERROR                                       | SenderBase からの応答を処理中にエラーが発生した場合に送信されます。                           | 情報                   |
| SMAD.ICCM.ALERT_PUSH_FAILED                            | 1台以上のホストでコンフィギュレーションのプッシュに失敗した場合に送信されます。                          | 警告                   |
| SMAD.TRANSFER.TRANSFERS_STALLED                        | SMA ログがトラッキングデータを2時間取得できなかった場合、またはレポートングデータを6時間取得できなかった場合に送信されます。 | 警告                   |
| SMTPAUTH.FWD_SERVER_FAILED_ALERT                       | SMTP 認証転送サーバが到達不能である場合に送信されます。                                    | 警告                   |
| SMTPAUTH.LDAP_QUERY_FAILED                             | LDAP クエリが失敗した場合に送信されます。                                           | 警告                   |
| SYSTEM.HERMES_SHUTDOWN_FAILURE.<br>REBOOT              | リブート中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。                         | 警告                   |
| SYSTEM.HERMES_SHUTDOWN_FAILURE.<br>SHUTDOWN            | システムをシャットダウンしている際に問題が発生した場合に送信されます。                               | 警告                   |

| アラート名                               | 説明                                   | 重大度    |
|-------------------------------------|--------------------------------------|--------|
| SYSTEM.RCPTVALIDATION.UPDATE_FAILED | 受信者検証のアップデートに失敗した場合に送信されます。          | クリティカル |
| SYSTEM.SERVICE_TUNNEL.DISABLED      | シスコサポートサービス用に作成されたトンネルが無効の場合に送信されます。 | 情報     |
| SYSTEM.SERVICE_TUNNEL.ENABLED       | シスコサポートサービス用に作成されたトンネルが有効の場合に送信されます。 | 情報     |

## ネットワーク設定値の変更

このセクションでは、アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、[システムセットアップウィザードの実行 \(15 ページ\)](#) でシステムセットアップウィザードを利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- `sethostname`
- DNS 設定 (GUI で設定。および CLI で `dnsconfig` コマンドを使用して設定)
- ルーティング設定 (GUI で設定。および CLI で `routeconfig` コマンドと `setgateway` コマンドを使用して設定)
- `dnsflush`
- パスフレーズ

## システム ホスト名の変更

ホスト名は、CLI プロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。`sethostname` コマンドは、コンテンツセキュリティアプライアンスの名前を設定します。新規ホスト名は、`commit` コマンドを発行して初めて有効になります。

### sethostname コマンド

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

ホスト名の変更を有効にするには、`commit` コマンドを入力する必要があります。ホスト名の変更を確定すると、CLI プロンプトに新しいホスト名が表示されます。

```
oldname.example.com> commit
Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

プロンプトに新規ホスト名が次のように表示されます。mail3.example.com>

## ドメインネーム システムの設定

コンテンツ セキュリティ アプライアンスのドメインネーム システム (DNS) は、GUI の [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [DNS] ページ、または `dnsconfig` コマンドを使用して設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバまたはユーザ独自の DNS サーバのどちらを使用するか、および使用するサーバ
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数
- DNS キャッシュのクリア

### DNS サーバの指定

AsyncOS では、インターネットのルート DNS サーバ、ユーザ独自の DNS サーバ、またはインターネットのルート DNS サーバと指定した信頼できる DNS サーバを使用できます。インターネットのルートサーバを使用するときは、特定のドメインに使用する代替サーバを指定することもできます。代替 DNS サーバは単一のドメインに適用されるため、該当ドメインに対する信頼できるサーバ (最終的な DNS レコードを提供) になっている必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリット DNS」を設定する場合は、`in-addr.arpa` (PTR) エントリも同様に設定する必要があります。このため、たとえば「`eng`」クエリをネームサーバ `1.2.3.4` にリダイレクトする際に、すべての `.eng` エントリが `172.16` ネットワークにある場合、スプリット DNS 設定に「`eng.16.172.in-addr.arpa`」をドメインとして指定する必要があります。

### 複数エントリとプライオリティ

入力する各 DNS サーバに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバの使用を試みます。その DNS サーバが応答しない場合、AsyncOS は次のプライオリティを持つサーバの使用を試みます。同じプライオリティを持つ DNS サーバに複数のエントリを指定する場合、システムはクエリを実行するたびに同じプライオリティを持つ DNS サーバをリストからランダムに選びます。次にシステムは最初のクエリが期限切れになるか、「タイムアウト」になるまで短時間待機した後、さらにそれよりわずかに長い秒数待機するという動作を続けます。待機時間の長さは、DNS サーバの実際の総数と、設定されたプライオリティによって異なります。タイムアウトの長さはプライオリティに関係

なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1つのプライオリティを設定している場合、該当のプライオリティに対する各サーバのタイムアウトは 60 秒になります。2つのプライオリティを設定している場合、最初のプライオリティに対する各サーバのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 82: DNS サーバ、プライオリティ、およびタイムアウト間隔の例

| [プライオリティ (Priority)] | サーバ                 | タイムアウト (秒) |
|----------------------|---------------------|------------|
| 0                    | 1.2.3.4、<br>1.2.3.5 | 5、5        |
| 1                    | 1.2.3.6             | 10         |
| 2                    | 1.2.3.7             | 45         |

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバをランダムに選択します。プライオリティ 0 のサーバの 1 つがダウンしている場合は、もう 1 つのサーバが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ (1.2.3.6) が使用され、最終的にプライオリティ 2 (1.2.3.7) のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

## インターネット ルート サーバの使用

AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。



- (注) デフォルト DNS サーバにインターネット ルートサーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリを再帰的に解決できる必要があります。

## 逆引き DNS ルックアップのタイムアウト

Cisco コンテンツセキュリティ アプライアンスは電子メールの送受信の際、リスナーに接続しているすべてのリモート ホストに対して「二重 DNS ルックアップ」の実行を試みます。つまり、ダブル DNS ルックアップを実行することで、システムはリモートホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS (PTR) ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS (A) ルック



アップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しないか、A レコードが存在しない場合、システムはホスト アクセス テーブル (HAT) 内のエントリと一致する IP アドレスのみを使用します。この特別なタイムアウト時間はこのルックアップにのみ適用され、[複数エントリとプライオリティ \(551 ページ\)](#) で説明されている一般的な DNS タイムアウトには適用されません。

デフォルト値は20秒です。秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトを無効にできます。値を0秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されません。

## DNS アラート

アプライアンスの再起動時に、まれにメッセージ「DNS キャッシュのブートストラップに失敗しました (Failed to bootstrap the DNS cache)」が付与されたアラートが生成される場合があります。このメッセージは、システムによるプライマリ DNS サーバへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

## DNS キャッシュのクリア

GUI の [キャッシュを消去 (Clear Cache)] ボタン、または `dnsflush` コマンドを使用して、DNS キャッシュのすべての情報をクリアします (`dnsflush` コマンドの詳細については、[資料 \(655 ページ\)](#) に指定された場所で入手可能な『IronPort AsyncOS CLI Reference Guide』を参照してください)。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

## グラフィカル ユーザ インターフェイスを使用した DNS 設定値の設定

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [DNS] ページを選択し、[設定の編集 (Edit Settings)] ボタンをクリックします。
- ステップ 3** インターネットのルート DNS サーバまたはユーザ独自の内部 DNS サーバのどちらかを使用するかを選択して、権威 DNS サーバを指定します。
- ステップ 4** ユーザ独自の DNS サーバを使用するか、権威 DNS サーバを指定する場合は、サーバ ID を入力し [行の追加 (Add Row)] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、[DNS サーバの指定 \(551 ページ\)](#) を参照してください。
- ステップ 5** DNS トラフィック用のインターフェイスを選択します。
- ステップ 6** 逆引き DNS ルックアップをキャンセルするまでに待機する秒数を入力します。

- ステップ7 必要に応じて、[キャッシュのクリア (Clear Chashe)] をクリックして、DNS キャッシュをクリアします。
- ステップ8 変更を送信し、保存します。

---

## TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。スタティック ルートの管理は、GUI の [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [ルーティング (Routing)] ページ、または CLI の `routeconfig` コマンドを使用して行います。

- [GUI でのスタティック ルートの管理 \(554 ページ\)](#)
- [デフォルト ゲートウェイの変更 \(GUI\) \(554 ページ\)](#)

### GUI でのスタティック ルートの管理

[管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [ルーティング (Routing)] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

- ステップ1 (新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ2 [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [ルーティング (Routing)] ページで、ルートリストの [ルートを追加 (Add Route)] をクリックします。ルートの名前を入力します。
- ステップ3 宛先 IP アドレスを入力します。
- ステップ4 ゲートウェイの IP アドレスを入力します。
- ステップ5 変更を送信し、保存します。

---

### デフォルト ゲートウェイの変更 (GUI)

- ステップ1 [ルーティング (Routing)] ページのルート リストで [デフォルトルート (Default Route)] をクリックします。
- ステップ2 ゲートウェイの IP アドレスを変更します。
- ステップ3 変更を送信し、保存します。

---

## デフォルト ゲートウェイの設定

GUI の [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [ルーティング (Routing)] ページ ([デフォルト ゲートウェイの変更 \(GUI\) \(554 ページ\)](#)) を参照

してください)、または CLI の `setgateway` コマンドを使用して、デフォルト ゲートウェイを設定できます。

## セキュア通信プロトコルの指定

- SSL v3 および TLS v1.0 ではなく TLS v1.1 および TLS v1.2 方式を使用することをお勧めします。SSL v3 はセキュアではないため、使用しないでください。
- 次のそれぞれに対して、使用する通信プロトコルを選択できます。
  - アップデート サーバ
  - スпам隔離へのエンドユーザ アクセス
  - アプライアンスの Web ベース管理インターフェイス
  - LDAPS



(注) デフォルトでは、新規に設置したアプライアンスのアップデートサーバ、Web インターフェイス、および LDAP サーバで TLS v1.1 および TLS v1.2 方式を使用します。スパム隔離へのエンドユーザのアクセスについては、SSL v3 は無効になっています。

- 現在選択されているプロトコルと利用可能なオプションを表示する場合、またはプロトコルを変更する場合は、コマンドライン インターフェイスで `sslconfig` コマンドを使用します。
- Cisco アップデート サーバでは SSL v3 をサポートしていません。
- ローカル (リモート) アップデートサーバを使用する場合、他のすべてのサービスおよび Web ブラウザに選択するプロトコルは、使用しているサーバとツールでサポートされて有効にされていなければなりません。
- 使用するサーバごとに、利用可能なオプションのいずれかを有効にする必要があります。
- `sslconfig` コマンドを使用して変更した場合は、変更をコミットする必要があります。
- `sslconfig` コマンドを使用して行った変更をコミットした後、該当するサービスが短時間中断されます。

## システム時刻の設定



(注) セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイムスタンプを適用します。詳細については、[セキュリティ管理アプライアンスによるレポート用データの収集方法 \(24 ページ\)](#) を参照してください。

コマンドラインインターフェイスを使用して時間に関連する設定を行うには、`ntpconfig`、`settime`、および `settz` コマンドを使用します。

| 目的          | 操作手順                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| システム時刻を設定する | <p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [時刻設定 (Time Settings)] を選択します。</p> <p><a href="#">ネットワーク タイム プロトコル (NTP) サーバの使用 (556 ページ)</a> も参照してください。</p>                                                                             |
| 時間帯を設定する    | <p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [タイムゾーン (Time Zone)] を選択します。</p> <p>関連項目：</p> <ul style="list-style-type: none"> <li>• <a href="#">GMT オフセットの選択 (557 ページ)</a></li> <li>• <a href="#">時間帯ファイルの更新 (558 ページ)</a></li> </ul> |

## ネットワーク タイム プロトコル (NTP) サーバの使用

ネットワーク タイム プロトコル (NTP) サーバを使用して、セキュリティ管理アプライアンスのシステムクロックをネットワークまたはインターネット上の他のコンピュータと同期できます。

デフォルトの NTP サーバは `time.sco.cisco.com` です。

デフォルトの NTP サーバを含め、外部 NTP サーバを使用する場合は、ファイアウォールで必要なポートを開きます。[ファイアウォール情報 \(643 ページ\)](#) を参照してください

関連項目

- システム時刻の設定 (556 ページ)
- 時間帯ファイルの手動更新 (558 ページ)

## (推奨) ネットワーク タイム プロトコル (NTP) を使用したアプライアンスのシステム時刻の設定

これは、特にアプライアンスが他のデバイスに統合されている場合に推奨される、時刻の設定方法です。統合されたデバイスはすべて、同じの NTP サーバを使用する必要があります。

NTP サーバを使用して時間を設定するには、CLI の `ntpconfig` コマンドを使用します。

- ステップ 1** [システム管理 (System Administration)] > [時刻設定 (Time Settings)] ページに移動します。
- ステップ 2** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 3** [時刻の設定方法 (Time Keeping Method)] セクションで、[NTP (Network Time Protocol) を使用 (Use Network Time Protocol)] を選択します。
- ステップ 4** NTP サーバのアドレスを入力し、[行を追加 (Add Row)] をクリックします。複数の NTP サーバを追加できます。
- ステップ 5** NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。
- ステップ 6** NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。
- ステップ 7** [NTP 認証の使用 (Use NTP Authentication)] チェック ボックスをオンにすると、タイムスタンプが信頼できるソースによって生成され、NTP が悪意のあるアクティビティや傍受から保護されます。
- ステップ 8** 変更を送信し、保存します。

## GMT オフセットの選択

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [タイムゾーン (Time Zone)] を選択します。
- ステップ 3** [設定の編集 (Edit Settings)] をクリックします。
- ステップ 4** 地域のリストから [GMT オフセット (GMT Offset)] を選択します。[タイムゾーンの設定 (Time Zone Setting)] ページが更新され、[タイムゾーン (Time Zone)] フィールドに GMT オフセットが含まれるようになります。
- ステップ 5** [タイムゾーン (Time Zone)] フィールドでオフセットを選択します。オフセットとは、グリニッジ子午線のローカル時間であるグリニッジ標準時 (GMT) に、加算または減算する時間のことです。時間の前にマイナス記号 (「-」) が付いている場合、グリニッジ子午線の西側にあたります。プラス記号 (「+」) の場合、グリニッジ子午線の東側にあたります。

ステップ6 変更を送信し、保存します。

## 時間帯ファイルの更新

いずれかの国の時間帯ルールに変更があった場合は必ず、アプライアンスの時間帯ファイルを更新する必要があります。

- [時間帯ファイルの自動更新](#) (558 ページ)
- [時間帯ファイルの手動更新](#) (558 ページ)

### 時間帯ファイルの自動更新

- ステップ1 (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ2 [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [アップデート設定 (Update Settings)] を選択します。
- ステップ3 [時間帯ルールの自動アップデートを有効にする (Enable automatic updates for Time zone rules)] チェックボックスをオンにします。
- ステップ4 間隔を入力します。重要な情報については、ページ上の [?] ヘルプをクリックします。
- ステップ5 変更を送信し、保存します。

### 時間帯ファイルの手動更新

- ステップ1 (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ2 [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [時刻設定 (Time Settings)] を選択します。
- ステップ3 [タイムゾーンファイルの更新 (Time Zone File Updates)] セクションを確認します。
- ステップ4 使用可能な時間帯ファイルの更新がある場合、[今すぐ更新 (Update Now)] をクリックします。

## [設定ファイル (Configuration File)] ページ

| 次のセクションの詳細について | 参照先                                   |
|----------------|---------------------------------------|
| 現在の設定の保存       | <a href="#">設定の保存とインポート</a> (559 ページ) |
| 保存されている設定のロード  | <a href="#">設定の保存とインポート</a> (559 ページ) |

| 次のセクションの詳細について                    | 参照先                                               |
|-----------------------------------|---------------------------------------------------|
| エンドユーザセーフリスト/ブロックリストデータベース（スパム隔離） | <a href="#">セーフリスト/ブロックリストのバックアップと復元（338 ページ）</a> |
| 設定のリセット                           | <a href="#">工場出荷時の初期状態への設定のリセット（508 ページ）</a>      |

## 設定の保存とインポート



(注) ここで説明されている設定ファイルは、セキュリティ管理アプライアンスの設定に使用されません。

セキュリティ管理アプライアンス内の大部分の設定は、1つの設定ファイルで管理できます。このファイルは Extensible Markup Language (XML) フォーマットで保持されます。

このファイルは次の複数の方法で使用できます。

- プライマリセキュリティ管理アプライアンスで予期しない障害が発生した場合に、2番目のセキュリティ管理アプライアンスをすばやく設定し、サービスを復元できます。
- 設定ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。アプライアンスの設定を間違えた場合、保存した最新のコンフィギュレーションファイルに「ロールバック」できます。
- 既存のコンフィギュレーションファイルをダウンロードし、アプライアンスの全体の設定を素早く確認できます（新しいブラウザの多くに、XML ファイルを直接レンダリングする機能が含まれています）。現在の設定にマイナーエラー（誤入力など）があった場合、この機能がトラブルシューティングに役立つことがあります。
- 既存のコンフィギュレーションファイルをダウンロードし、変更を行い、そのファイルを同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と GUI の両方が「バイパス」されます。
- FTP を介してコンフィギュレーションファイル全体をアップロードしたり、コンフィギュレーションファイルの一部を CLI に直接貼り付けたりすることができます。
- このファイルは XML 形式になっているため、設定ファイルのすべての XML エンティティが記述された、関連する文書型定義 (DTD) も提供されます。XML コンフィギュレーションファイルをアップロードする前にこの DTD をダウンロードして XML コンフィギュレーションファイルを検証できます (XML 検証ツールはインターネットで簡単に入手できます)。
- コンフィギュレーションファイルを使用して、別のアプライアンス（クローン作成された仮想アプライアンスなど）を迅速に設定できます。

## コンフィギュレーションファイルの管理

- [セーフリスト/ブロックリストのバックアップと復元 \(338 ページ\)](#)
- [工場出荷時の初期状態への設定のリセット \(508 ページ\)](#)
- [以前コミットしたコンフィギュレーションへのロールバック \(563 ページ\)](#)

### 現在の設定ファイルの保存およびエクスポート

[管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [設定ファイル (Configuration File) ] ページの [現在の構成 (Current Configuration) ] セクションを使用すると、現在のコンフィギュレーションファイルをローカルマシンに保存したり、アプライアンスで保存したり (FTP/SCP ルートの設定ディレクトリに保存されます)、指定されたアドレスに電子メールで送信したりできます。

#### パスフレーズのマスク

必要に応じてチェックボックスをオンにして、ユーザのパスフレーズをマスクします。パスフレーズをマスクすると、元の暗号化されたパスフレーズが、エクスポートまたは保存されたファイルで「\*\*\*\*」に置き換えられます。



(注) パスフレーズがマスクされたコンフィギュレーションファイルをロードして AsyncOS に戻すことはできません。

#### パスフレーズの暗号化

[設定ファイル内のパスフレーズを隠す (Encrypt passphrases in the Configuration Files) ] チェックボックスをクリックして、ユーザのパスフレーズをマスクできます。次に、暗号化される、設定ファイル内の重要なセキュリティパラメータを示します。

- 証明書の秘密キー
- RADIUS パスワード
- LDAP バインドのパスワード
- ローカルユーザのパスワードのハッシュ
- SNMP パスワード
- 発信 SMTP 認証パスワード
- PostX 暗号化キー
- PostX 暗号化プロキシパスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード



- アップデータ サーバの URL

これは、saveconfig コマンドを使用してコマンドラインインターフェイスでも構成できます。

## コンフィギュレーション ファイルのロード

コンフィギュレーション ファイルは、設定をロードするアプライアンスと同じバージョンの AsyncOS を実行しているアプライアンスから保存される必要があります。

パスフレーズがマスクされたコンフィギュレーション ファイルはロードできません。

どの方法の場合でも、設定の上部に次のタグを含める必要があります。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
... your configuration information in valid XML
</config>
```

</config> 閉じタグは設定情報の後に指定する必要があります。XML 構文の値は、Cisco コンテンツ セキュリティ アプライアンスの configuration ディレクトリにある DTD を使用して解析および検証されます。DTD ファイルの名前は config.dtd です。loadconfig コマンドを使用したときにコマンドラインで検証エラーが報告された場合、変更はロードされません。設定ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、設定ファイルを検証できます。

いずれのインポート方法でも、コンフィギュレーション ファイル全体（最上位のタグである <config></config> 間で定義された情報）またはコンフィギュレーションファイルの complete および unique サブセクション（上記の宣言タグを含み、<config></config> タグ内に存在する場合）をインポートできます。

「complete（完全）」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次のコードをアップロードまたは貼り付けると、検証エラーが発生します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

しかし、次のコードをアップロードまたは貼り付けても、検証エラーは発生しません。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

「unique（一意）」とは、アップロードまたは貼り付けられるコンフィギュレーションファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは1つのホスト名しか持てないため、次のコード（宣言および <config></config> タグを含む）をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

しかし、システムにはそれぞれ異なる受信者アクセステーブルが定義された複数のリスナーが定義されている可能性があるため、次のコードのみをアップロードすることは多義的であると見なされます。

```
<rat>
  <rat_entry>
    <rat_address>ALL</rat_address>
    <access>RELAY</access>
  </rat_entry>
</rat>
```

多義的であるため、「完全」な構文であっても許可されません。



**注意** コンフィギュレーション ファイルまたはコンフィギュレーション ファイルのサブセクションをアップロードまたは解析する場合は、待機中の可能性がある、保存されていない変更が破壊されることがあります。

## 空のタグと省略されたタグ

設定ファイルのセクションをアップロードまたは解析する場合は注意が必要です。タグを含めないと、コンフィギュレーションファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、次のコードをアップロードすると、システムからすべてのリスナーが削除されます。

```
<listeners></listeners>
```



**注意** コンフィギュレーションファイルのサブセクションをアップロードしたり、貼り付けたりした場合、GUI または CLI から切断され、大量の設定データが破壊されることがあります。管理ポートで別のプロトコル、シリアルインターフェイス、またはデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しいコンフィギュレーションファイルをロードする前に、必ず設定データをバックアップしてください。

## ログサブスクリプションのパスフレーズのロードについての注意事項

パスフレーズが必要なログサブスクリプションを含むコンフィギュレーションファイルをロードしようとしても（たとえば、FTP プッシュを使用）、loadconfig コマンドは不明なパスフレーズについて警告しません。FTP プッシュが失敗し、logconfig コマンドを使用して正しいパスフレーズを設定するまで警告が生成されます。

## 文字セットエンコーディングについての注意事項

XML 設定ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「ISO-8859-1」である必要があります。showconfig コマンド、saveconfig コマンド、または mailconfig コマンドを発行するたびに、エンコーディング属性がファイルで指定されます。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

## 現在の設定のリセット

現在の設定をリセットすると、Cisco コンテンツセキュリティアプライアンスは設定を元の出荷時デフォルト値に戻します。リセットする前に設定を保存してください。

「[工場出荷時の初期状態への設定のリセット \(508 ページ\)](#)」を参照してください。

## 以前コミットしたコンフィギュレーションへのロールバック

以前コミットされた設定にロールバックできます。

コマンドラインインターフェイスで rollbackconfig コマンドを使用して、直近の 10 件のコミットから 1 件を選択します。

ロールバックをコミットすることを促されたときに No を入力した場合、このロールバックは、次回変更をコミットする際にコミットされます。

管理者アクセス権を持つユーザだけが rollbackconfig コマンドを使用できます。



---

(注) 以前の設定が復元されてもログ メッセージまたはアラートは生成されません。

---



---

(注) 既存のデータを保持する十分なサイズにディスク領域を再割り当てするなどの一部のコミットでは、データ漏洩が発生する可能性があります。

---

## 設定ファイル用の CLI コマンド

次のコマンドを使用すると、コンフィギュレーション ファイルを操作できます。

- showconfig
- mailconfig
- saveconfig
- loadconfig
- rollbackconfig
- resetconfig ([工場出荷時の初期状態への設定のリセット \(508 ページ\)](#) を参照)
- publishconfig

- backupconfig (セキュリティ管理アプライアンスのデータのバックアップ (513 ページ) を参照)
- trailblazerconfig

## showconfig、mailconfig、および saveconfig コマンド

設定コマンドの showconfig、mailconfig、および saveconfig の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスフレーズを含めるかどうかを選択することを求められます。パスフレーズを含めないことを選択すると、パスフレーズフィールドが空白のままになります。セキュリティ違反を心配する場合は、パスフレーズを含めないことを選択できません。ただし、loadconfig コマンドを使用してロードされた場合、パスフレーズがないコンフィギュレーションファイルは失敗します。ログサブスクリプションのパスフレーズのロードについての注意事項 (562 ページ) を参照してください。



- (注) コンフィギュレーションファイルを保存、表示、または電子メールで送信するときに、パスフレーズを含めることを選択すると (「Do you want to include passphrases?」に「yes」と回答した場合)、パスフレーズは暗号化されます。ただし、秘密キーと証明書は暗号化されない PEM 形式で含まれます。

showconfig コマンドは、現在の設定を画面に出力します。

```
mail3.example.com> showconfig
Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: model number
Messaging Gateway Appliance(tm)
  Model Number: model number
  Version: version of AsyncOS installed
  Serial Number: serial number
  Current Time: current time and date
[The remainder of the configuration file is printed to the screen.]
```

mailconfig コマンドを使用して、現在の設定をユーザに電子メールで送信します。メッセージには config.xml という名前の XML 形式のコンフィギュレーションファイルが添付されます。

```
mail3.example.com> mailconfig
Please enter the email address to which you want to send
the configuration file.
[ ]> administrator@example.com
Do you want to include passphrases? Please be aware that a configuration
without passphrases will fail when reloaded with loadconfig. [N]> y
The configuration file has been sent to administrator@example.com.
```

セキュリティ管理アプライアンスで saveconfig コマンドを使用すると、一意のファイル名を使用して、すべての Configuration Master ファイル (ESA) が configuration ディレクトリに保存されます。

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

```
Do you want to include passphrases? Please be aware that a configuration without
passphrases
will fail when reloaded with loadconfig. [N]> y
The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
directory.
mail3.example.com>
```

## loadconfig コマンド

アプライアンスに新しい設定情報をロードするには、loadconfig コマンドを使用します。情報は次の2つのいずれかの方法でロードできます。

- configuration ディレクトリに情報を格納し、アップロードする。
- CLI に設定情報を直接貼り付ける。

詳細については、「[コンフィギュレーションファイルのロード \(561 ページ\)](#)」を参照してください。

## rollbackconfig コマンド

「[以前コミットしたコンフィギュレーションへのロールバック \(563 ページ\)](#)」を参照してください。

## publishconfig コマンド

変更を Configuration Master に公開するには、publishconfig コマンドを使用します。構文は次のようになります。

```
publishconfig config_master [job_name ] [host_list | host_ip
```

ここで、*config\_master* は、サポートされている Configuration Master です。これらの Configuration Master のリストは、このリリースのリリース ノートの「[Compatibility Matrix](#)」

([http://www.cisco.com/en/US/products/ps10155/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html)) にあります。このキーワードは必須です。キーワード *job\_name* は省略可能で、指定しなかった場合は生成されます。

キーワード *host\_list* は、公開される WSA アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は、Configuration Master に割り当てられているすべてのホストに公開されます。オプションの *host\_ip* には、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、smad\_logs ファイルを調べます。[ウェブ (Web) ]>[ユーティリティ (Utilities) ]>[Webアプライアンスステータス (Web Appliance Status) ]を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライアンスを選択します。また、[ウェブ (Web) ]>[ユーティリティ (Utilities) ]>[公開 (Publish) ]>[公開履歴 (Publish History) ]により、[公開履歴 (Publish History) ]ページに進むことができます。

## trailblazerconfig コマンド

trailblazerconfig コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。

インラインヘルプを参照するには、CLI で `help trailblazerconfig` コマンドを使用します。

構文は次のようになります。

```
trailblazerconfig enable <https_port> <http_port>
```

```
trailblazerconfig disable
```

```
trailblazerconfig status
```

ここで、

'enable' は、デフォルトのポート（HTTPS: 4431）で trailblazer 設定を実行します。

'disable' は、trailblazer 設定を無効にします。

'status' は trailblazer 設定のステータスをチェックします。



**重要** デフォルトで、trailblazerconfig の CLI コマンドはアプライアンスで有効になっています。HTTPS ポートがファイアウォールで開かれていることを確認します。また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。

trailblazerconfig コマンドを使用すると、次の問題を回避できます。

- 特定のブラウザで API ポートの複数の証明書を追加する必要がある。
- スпам隔離、セーフリスト、またはブロックリストのページを更新するときに、レガシー Web インターフェイスにリダイレクトされる。
- 高度なマルウェア防御レポート ページのメトリック バーにデータが含まれない。



(注) アプライアンスで trailblazerconfig コマンドを有効にすると、リクエスト URL にはホスト名に付加された trailblazerconfig HTTPS ポート番号が含まれます。

## CLI を使用した設定変更のアップロード

**ステップ 1** CLI の外部で、アプライアンスの configuration ディレクトリにアクセスできることを確認します。詳細については、[IP インターフェイスおよびアプライアンスへのアクセス（631 ページ）](#) を参照してください。

**ステップ 2** 設定ファイル全体または設定ファイルのサブセクションをアプライアンスの configuration ディレクトリに格納するか、saveconfig コマンドで作成した既存の設定を編集します。

**ステップ 3** CLI 内で、loadconfig コマンドを使用して、ステップ 2 で示されたディレクトリに格納したコンフィギュレーションファイルをロードするか、テキスト（XML 構文）を CLI に直接貼り付けます。

この例では、`changed.config.xml` という名前のファイルがアップロードされ、変更が保存されます。

例：

```
mail3.example.com>
1
oadconfig
1. Paste via CLI
2. Load from file
[1]> 2
Enter the name of the file to import:
[]> changed.config.xml
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
```

この例では、新しいコンフィギュレーション ファイルをコマンドラインに直接貼り付けます（空白行で `Ctrl+D` を押すと貼り付けコマンドが終了します）。次に、システムセットアップウィザードを使用して、デフォルトのホスト名、IP アドレス、およびゲートウェイ情報を変更します（詳細については、[システムセットアップウィザードの実行（15 ページ）](#) を参照してください）。最後に、変更を確定します。

例：

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 1
Paste the configuration file now. Press CTRL-D on a blank line when done.
[The configuration file is pasted until the end tag
</config>
. Control-D is entered on a separate line.]
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings
```

## ディスク領域の管理

組織で使用する各機能に、使用可能な最大量まで、使用可能なディスク領域を割り当てることができます。

- [（仮想アプライアンスのみ）使用可能なディスク領域の拡大（568 ページ）](#)
- [ディスク領域、クォータ、および使用状況の表示（568 ページ）](#)
- [最大ディスク領域と割り当てについて（569 ページ）](#)
- [ディスク領域に関するアラートの受信の確認（570 ページ）](#)
- [その他のクォータのディスク領域の管理（570 ページ）](#)
- [ディスク領域量の再割り当て（571 ページ）](#)

## (仮想アプライアンスのみ) 使用可能なディスク領域の拡大

ESXi 5.5 および VMFS 5 を実行する仮想アプライアンスの場合、2 TB を超えるディスク領域を割り当てることができます。ESXi 5.1 を実行するアプライアンスの場合は 2 TB に制限されます。



(注) ESXi でのディスク領域の削減はサポートされません。詳細については、VMware のマニュアルを参照してください。

仮想アプライアンス インスタンスにディスク領域を追加するには、次の手順を実行します。

### 始める前に

必要な追加ディスク領域を慎重に検討します。

**ステップ 1** Cisco コンテンツ セキュリティ管理アプライアンス インスタンスを停止します。

**ステップ 2** VMware が提供するユーティリティまたは管理ツールを使用してディスク領域を増やします。

VMware のマニュアルで仮想ディスク設定の変更に関する情報を参照してください。

ESXi 5.5 の情報は、次のサイトから入手できます。 <http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html>

**ステップ 3** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。

**ステップ 4** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ディスク管理 (Disk Management) ] に移動して、変更が反映されていることを確認します。

## ディスク領域、クォータ、および使用状況の表示

目的	操作手順
アプライアンスで利用可能な合計ディスク領域を表示する	<p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance) ]&gt;[システム管理 (System Administration) ]&gt;[ディスク管理 (Disk Management) ] を選択します。</p> <p>[合計割当て容量 (Total Space Allocated) ] に示されている値 (例: 184G of 204G) を確認します。</p>



目的	操作手順
セキュリティ管理アプライアンスのモニタリングサービスごとに、割り当てられているディスク領域および現在使用されているディスク領域の量を表示する	<p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [ディスク管理 (Disk Management)] を選択します。</p>
現在使用されている隔離のクォータの割合を表示する	<p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [集約管理サービス (Centralized Services)] &gt; [システムステータス (System Status)] を選択して、[集約管理サービス (Centralized Services)] セクションで確認します。</p>

## 最大ディスク領域と割り当てについて



(注) セキュリティ管理アプライアンスの中央集中型レポートディスク領域は、電子メールと Web の両方のデータに使用されます。中央集中型電子メールレポートと中央集中型 Web レポートのどちらか一方をイネーブルにすると、すべての領域がイネーブルにした機能専用になります。両方をイネーブルにした場合、電子メールおよび Web レポートデータは領域を共有し、領域はファーストカム ベースで割り当てられます。

- 中央集中型 Web レポートをイネーブルにしているが、レポートにディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポートが機能しません。
- その他のクォータを現在の使用量より少なくする前に、不要なデータを削除する必要があります。[その他のクォータのディスク領域の管理 \(570 ページ\)](#) を参照してください。
- ポリシー、ウイルス、およびアウトブレイク隔離のディスク領域を管理する方法については、[ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当て \(367 ページ\)](#) および [隔離内のメッセージの保持期間 \(368 ページ\)](#) を参照してください。
- 他のすべてのデータタイプでは、既存の割り当て量を現在の使用量より少なくした場合、新しい割り当て量内にすべてのデータが収まるまで、最も古いデータから削除されます。
- 新しいクォータが現在使用されているディスク領域よりも大きい場合、データは失われません。
- 割り当て量をゼロに設定すると、データは保持されなくなります。

## ディスク領域に関するアラートの受信の確認

その他のディスク使用量がクォータの 75% に達すると、警告レベルのシステム アラートを受信します。これらのアラートを受信した場合は、対処する必要があります。

確実にアラートが届くようにするには、[アラートの管理 \(541 ページ\)](#) を参照してください。

## その他のクォータのディスク領域の管理

その他のクォータにはシステム データとユーザ データが含まれます。システム データは削除できません。管理できるユーザ データには次のファイルタイプがあります。

管理対象	手順
ログ ファイル	<p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[管理アプライアンス (Management Appliance)] &gt; [システム管理 (System Administration)] &gt; [ログサブスクリプション (Log Subscriptions)] に移動して、以下を実行します。</p> <ul style="list-style-type: none"> <li>• [サイズ (Size)] 列見出しをクリックして、最も多くのディスク領域を消費しているログを確認します。</li> <li>• 生成されるすべてのログ サブスクリプションが必要であることを確認します。</li> <li>• 必要以上に詳細なログレベルになっていないかを確認します。</li> <li>• 可能な場合は、ロールオーバー ファイル サイズを小さくします。</li> </ul>
パケット キャプチャ	[ヘルプとサポート (Help and Support)] (画面上部の右側付近) > [パケットキャプチャ (Packet Capture)] に移動します。不要なキャプチャを削除します。
コンフィギュレーションファイル	<p>アプライアンスの /data/pub ディレクトリに FTP でアクセスします。アプライアンスへの FTP アクセスを設定するには、次を参照してください。 <a href="#">FTP 経由でのアプライアンスへのアクセス (634 ページ)</a></p> <p>(これらのファイルが多くのディスク領域を消費する可能性は低いと考えられます)。</p>
クォータ サイズ	<p>(新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。</p> <p>[システム管理 (System Administration)] &gt; [ディスク管理 (Disk Management)] に移動します。</p>

## ディスク領域量の再割り当て

ディスク領域が使用していない機能に割り当てられている場合、または、アプライアンスで特定の機能については頻繁にディスク領域が不足するものの他の機能については過剰な領域がある場合は、ディスク領域量の割り当てを変更できます。

すべての機能にさらに領域が必要な場合は、ハードウェアのアップグレード、または仮想アプライアンスへの追加ディスク領域の割り当てを検討してください。「[\(仮想アプライアンスのみ\) 使用可能なディスク領域の拡大 \(568 ページ\)](#)」を参照してください。

### 始める前に

- ディスク割り当てを変更すると、既存のデータまたは機能の可用性に影響する場合があります。[最大ディスク領域と割り当てについて \(569 ページ\)](#) で情報を参照してください。
- 隔離からメッセージを手動で解放または削除することで、隔離用の領域を一時的に作成できます。

- 
- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
  - ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ディスク管理 (Disk Management)] を選択します。
  - ステップ 3** [ディスククォータの編集 (Edit Disk Quotas)] をクリックします。
  - ステップ 4** [ディスククォータの編集 (Edit Disk Quotas)] ページで、各サービスに割り当てるディスク領域の量 (ギガバイト単位) を入力します。
  - ステップ 5** [送信 (Submit)] をクリックします。
  - ステップ 6** 確認ダイアログボックスで、[新しいクォータの設定 (Set New Quotas)] をクリックします。
  - ステップ 7** [確定する (Commit)] をクリックして変更を保存します。
- 

## E メールセキュリティ アプライアンスのシステムの状態グラフの参照のしきい値の調整



- (注) これらのしきい値に関連するアラートを受信するには、各管理対象 E メールセキュリティ アプライアンスのしきい値を設定します。詳細については、お使いの E メールセキュリティ アプライアンス リリースのユーザガイドまたはオンライン ヘルプで、システムの状態のしきい値の設定に関する情報を参照してください。個々のアプライアンスからオンデマンドのシステムの状態チェックを実行できます。アプライアンスの状態のチェックについては、お使いの E メールセキュリティ アプライアンス リリースのユーザガイドまたはオンラインヘルプを参照してください。
-

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[システムの状態 (System Health) ] をクリックします。
- ステップ 3** [設定の編集 (Edit Settings) ] をクリックします。
- ステップ 4** オプションを設定します。

オプション	説明
全体のCPU使用率 (Overall CPU Usage)	デフォルト : 85%
メモリページスワップ (Memory Page Swapping)	デフォルト : 5000 ページ
ワークキュー内の最大メッセージ (Maximum Messages in Work Queue)	デフォルト : 500 メッセージ

- ステップ 5** 変更を送信し、保存します。

## SAML 2.0 による SSO

- [SSO および SAML 2.0 について \(572 ページ\)](#)
- [SAML 2.0 SSO のワークフロー \(572 ページ\)](#)
- [SAML 2.0 に関する注意事項と制約事項 \(574 ページ\)](#)
- [スパム隔離用の SSO の設定方法 \(574 ページ\)](#)

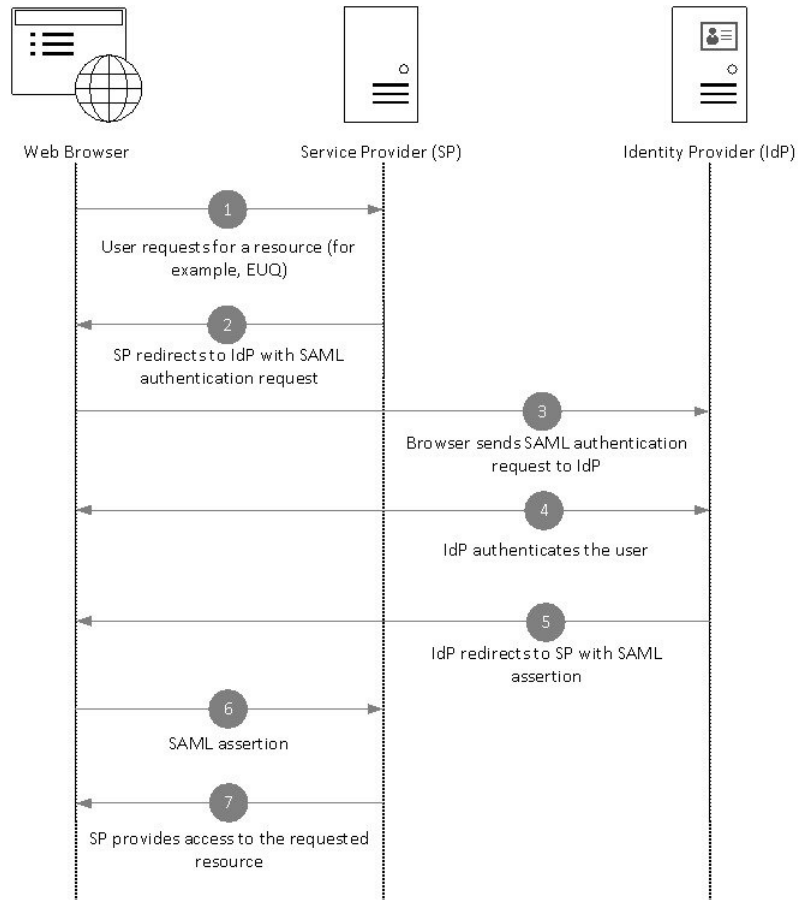
## SSO および SAML 2.0 について

Cisco コンテンツ セキュリティ管理アプライアンスは SAML 2.0 SSO をサポートするようになりました。これによりエンドユーザーはその組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用している同じクレデンシャルを使用してスパム隔離にアクセスできます。たとえば、SAML ID プロバイダー (IdP) として Ping 認証を有効にしており、SAML 2.0 SSO 対応の Rally、Salesforce、および Dropbox のアカウントを持っています。サービスプロバイダー (SP) として SAML 2.0 SSO をサポートするように Cisco コンテンツ セキュリティ管理アプライアンスを構成すると、エンドユーザーは一度サインインするだけでスパム隔離を含むすべてのサービスにアクセスできるようになります。

## SAML 2.0 SSO のワークフロー

SAML 2.0 SSO ワークフローを、次の図に表示します。

図 20: SAML 2.0 SSO のワークフロー



### ワークフロー

1. エンドユーザは、Web ブラウザを使用して、サービス プロバイダー（アプライアンス）からリソースを要求します。たとえば、エンドユーザは、スパム通知のスパム隔離リンクをクリックします。
2. サービス プロバイダは、SAML 認証要求で Web ブラウザに要求をリダイレクトします。
3. Web ブラウザは、ID プロバイダーに SAML 認証要求をリレーします。
4. ID プロバイダーは、エンドユーザを認証します。ID プロバイダーはエンドユーザにログインページを表示し、エンドユーザがログインします。
5. ID プロバイダーは、SAML アサーションを生成して、Web ブラウザに送り返します。
6. Web ブラウザは、サービス プロバイダーに SAML アサーションをリレーします。
7. サービス プロバイダーは、要求されたリソースへのアクセスを付与します。

## SAML 2.0 に関する注意事項と制約事項

- ログアウト (574 ページ)
- 一般 (574 ページ)
- 管理者のスパム隔離へのアクセス (574 ページ)

### ログアウト

エンドユーザが、スパム隔離からログアウトしても、他の SAML 2.0 SSO が有効なアプリケーションからはログアウトされません。

### 一般

Cisco コンテンツ セキュリティ管理アプライアンス上では、サービス プロバイダーと ID プロバイダーのインスタンスを 1 つのみ構成できます。

### 管理者のスパム隔離へのアクセス

スパム隔離用の SSO を有効にしている場合、管理者はスパム隔離の URL (`http://<appliance_hostname>:<port>`) を使用してスパム隔離へアクセスできなくなることを覚えておいてください。管理者は Web インターフェイスを使用してスパム隔離にアクセスできます ([メール (Email)] > [メッセージの隔離 (Message Quarantine)] > [スパム隔離 (Spam Quarantine)] )。

## スパム隔離用の SSO の設定方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	前提条件 (575 ページ)
ステップ 2	サービス プロバイダーとして、アプライアンスを設定します。	サービス プロバイダーとしての Cisco コンテンツセキュリティ管理アプライアンスの設定 (575 ページ)
ステップ 3:	[IDP で] アプライアンスを操作するように ID プロバイダーを設定します。	Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成 (577 ページ)
ステップ 4:	アプライアンスで ID プロバイダーを設定します。	Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成 (579 ページ)
ステップ 5	アプライアンスでスパム隔離用の SSO を有効にします。	スパム隔離のための SSO の有効化 (580 ページ)
ステップ 6:	エンドユーザに新しい認証メカニズムについて通知します。	

## 前提条件

- 組織で使用される ID プロバイダーが Cisco コンテンツ セキュリティ管理アプライアンスでサポートされているかどうかを確認します。次に、サポートされる ID プロバイダーを示します。
  - Microsoft Active Directory Federation Services (AD FS) 2.0
  - Ping Identity PingFederate 7.2
  - Cisco Web Security Appliance 9.1
- アプライアンスと ID プロバイダーの間の通信をセキュリティで保護するために必要な次の証明書を取得します。
  - アプライアンスで SAML 認証要求に署名する、または ID プロバイダーで SAML アサーションを暗号化する場合、自己署名証明書または信頼されている CA と関連付けられている秘密キーから証明書を取得します。
  - ID プロバイダーで SAML アサーションに署名する場合は、ID プロバイダーの証明書を取得します。アプライアンスはこの証明書を使用して、署名済み SAML アサーションを確認します。

## サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定

### 始める前に

まず、[前提条件 \(575 ページ\)](#)

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [SAML] を選択します。
- ステップ 3** [サービスプロバイダー (Service Provider)] セクションで [サービスプロバイダーの追加 (Add Service Provider)] をクリックします。
- ステップ 4** 次の詳細を入力します。

フィールド	説明
プロファイル名 (Profile Name)	サービス プロバイダー プロファイルの名前を入力します。
コンフィギュレーション設定	

フィールド	説明
エンティティ ID	サービスプロバイダー（この場合、ご使用のアプライアンス）のグローバルな固有の名前を入力します。通常、サービスプロバイダーエンティティ ID の形式は URI です。
名前 ID の形式	ID プロバイダーが SAML アサーションでユーザを指定するのに使用する形式。  このフィールドは設定できません。ID プロバイダーを設定する際にこの値が必要になります。
アサーション コンシューマ URL	認証が正常に完了した後で、ID プロバイダーが SAML アサーションを送信する URL。この場合、スパム隔離の URL です。  このフィールドは設定できません。ID プロバイダーを設定する際にこの値が必要になります。
SP 証明書	<p>(注) 秘密キーは .pem 形式である必要があります。</p> <p><b>認証要求の署名</b></p> <p>アプライアンスで SAML 認証要求に署名する場合、</p> <ol style="list-style-type: none"> <li>1. 証明書と関連付けられている秘密キーをアップロードします。</li> <li>2. 秘密キーのパスフレーズを入力します。</li> <li>3. [署名要求 (Sign Request) ] を選択します。</li> </ol> <p><b>暗号化されたアサーションの復号</b></p> <p>SAML アサーションを暗号化するように ID プロバイダーを設定する場合、</p> <ol style="list-style-type: none"> <li>1. 証明書と関連付けられている秘密キーをアップロードします。</li> <li>2. 秘密キーのパスフレーズを入力します。</li> </ol>
署名アサーション	SAML アサーションに署名するように ID プロバイダーを設定する場合、[署名アサーション (Sign Assertions) ] を選択します。  このオプションを選択すると、アプライアンスに ID プロバイダーの証明書を追加する必要があります。Cisco コンテンツ セキュリティ 管理アプライアンスと通信するための ID プロバイダーの構成 (577 ページ) を参照してください。
組織詳細	組織の詳細を入力します。  ID プロバイダーは、エラー ログでこの情報を使用します。
技術的な問い合わせ先	技術的な問い合わせ先の電子メールアドレスを入力します。  ID プロバイダーは、エラー ログでこの情報を使用します。

ステップ 5 [送信 (Submit) ] をクリックします。



**ステップ 6** [SSOの設定 (SSO Settings)] ページに表示されるサービス プロバイダーのメタデータ (エンティティ ID とアサーション顧客 URL) と、[サービスプロバイダー設定 (Service Provider Settings)] ページに表示される名前 ID の形式を書き留めます。ID プロバイダーでサービス プロバイダーを設定するときに、これらの詳細が必要になります。

必要に応じて、メタデータをファイルとしてエクスポートできます。[メタデータのエクスポート (Export Metadata)] をクリックして、メタデータ ファイルを保存します。一部の ID プロバイダーでは、メタデータ ファイルからサービス プロバイダーの詳細をロードできます。

### 次のタスク

アプライアンスと通信するように ID プロバイダーを設定します。「[Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成 \(577 ページ\)](#)」を参照してください。

## Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成

### 始める前に

次の内容について確認してください。

- アプライアンスがサービス プロバイダーとして構成されている。[サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定 \(575 ページ\)](#) を参照してください。
- サービスプロバイダーのメタデータの詳細がコピーされているか、またはメタデータ ファイルがエクスポートされている。[サービスプロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定 \(575 ページ\)](#) を参照してください。

**ステップ 1** ID プロバイダーで、次のいずれかを実行します。

- サービス プロバイダー (アプライアンス) の詳細を手動で構成します。
- ID プロバイダーがメタデータ ファイルからサービス プロバイダーの詳細をロードすることを許可している場合は、メタデータ ファイルをインポートします。

アプライアンスが SAML 認証要求に署名するように構成済みの場合、または SAML アサーションを暗号化する予定の場合は、必ず関連する証明書を ID プロバイダーに追加します。

ID プロバイダー固有の手順については、以下を参照してください。

- [Cisco コンテンツ セキュリティ管理アプライアンスとの通信のための ADFS 2.0 の構成 \(578 ページ\)](#)
- [PingFederate 7.2 を Cisco コンテンツ セキュリティ管理アプライアンスと通信させるための設定 \(579 ページ\)](#)

- 『*User Guide for AsyncOS for Cisco Web Security Appliances* <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html>』の「**Configuring the Appliance as an Identity Provider**」セクション

**ステップ 2** ID プロバイダーのメタデータを書き留めるかまたはメタデータをファイルとしてエクスポートします。

### 次のタスク

アプライアンス上で ID プロバイダーの設定を構成します。「[Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成 \(579 ページ\)](#)」を参照してください。

### Cisco コンテンツ セキュリティ管理アプライアンスとの通信のための AD FS 2.0 の構成

次に示すのは、アプライアンスと通信する AD FS 2.0 を構成するために実行する必要がある高レベルのタスクです。完全かつ詳細な手順については、Microsoft のマニュアルを参照してください。

- リレー パーティとしてサービス プロバイダー (アプライアンス) のアサーション コンシューマ URL を追加します。
- [リレー パーティ トラスト (Relaying Party Trusts)] > [プロパティ (Properties)] > [ID (Identifiers)] > [リレー パーティ ID (Relaying Party Identifier)] で、サービス プロバイダー (アプライアンス) のエンティティ ID を入力します。この値が、アプライアンスのサービス プロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー (アプライアンス) を構成済みの場合は、サービス プロバイダーの証明書 (認証要求を署名するために使用される) を [リレー パーティ トラスト (Relaying Party Trusts)] > [プロパティ (Properties)] > [署名 (Signature)] の下で .cer 形式でアップロードします。
- 暗号化された SAML アサーションを送信するように AD FS を構成する場合は、サービス プロバイダー (アプライアンス) の証明書を [リレー パーティ トラスト (Relaying Party Trusts)] > [プロパティ (Properties)] > [暗号化 (Encryption)] の下で .cer 形式でアップロードします。
- [リレー パーティ トラスト (Relaying Party Trusts)] > [プロパティ (Properties)] > [詳細 (Advanced)] の下で、セキュアハッシュ アルゴリズムを SHA-1 に設定します。
- 要求ルールを編集し、電子メールアドレスの LDAP 属性を発信要求タイプ (電子メールアドレス) として送信する発行変換規則を追加します。
- 応答に SPNameQualifier を含めるためのカスタム ルールを追加します。次のファイルは、サンプルのカスタム ルールです。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer =
  c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"http://<appliance-hostname>:83");
```

## PingFederate 7.2 を Cisco コンテンツ セキュリティ管理アプライアンスと通信させるための設定

以下は、お使いのアプライアンスと通信するように PingFederate 7.2 を設定するために実行する必要があるタスクの概要です。包括的かつ詳細な手順については、Ping Identity のマニュアルを参照してください。


- お使いのサービスプロバイダ（アプライアンス）のアサーション コンシューマ URL を、プロトコル設定におけるエンドポイントとして追加します。
- [SP Connection] > [General Info] > [Partner's Entity ID (Connection ID)] にサービスプロバイダ（アプライアンス）のエンティティ ID を入力します。この値が、アプライアンスのサービスプロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名付き SAML 認証要求を送信するようにサービスプロバイダ（アプライアンス）を設定している場合、[Signature Verification] セクション（[SP Connection] > [Credentials] > [Signature Verification] > [Signature Verification Certificate]）で、サービスプロバイダの証明書をアップロードします。
- 暗号化された SAML アサーションを送信するように PingFederate を設定する場合は、[Signature Verification] セクション（[SP Connection] > [Credentials] > [Signature Verification] > [Select XML Encryption Certificate]）で、サービスプロバイダ（アプライアンス）の証明書をアップロードします。
- 属性コントラクトを編集し、LDAP 属性の電子メールアドレスを送信するようにします（[Attribute Sources & User Lookup] > [Attribute Contract Fulfillment]）。

## Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成

### 始める前に

次の内容について確認してください。

- アプライアンスとの通信のための ID プロバイダーが構成されている。[Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成 \(577 ページ\)](#) を参照してください。
- ID プロバイダーのメタデータの詳細またはエクスポートされたメタデータ ファイルがコピーされている。

- 
- ステップ 1** （新しい Web インターフェイスのみ）クラウド E メールセキュリティ管理コンソールで、歯車（）アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [SAML] を選択します。
- ステップ 3** [ID プロバイダー（Identity Provider）] セクションで、[ID プロバイダーの追加（Add Identity Provider）] をクリックします。
- ステップ 4** 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	ID プロバイダー プロファイルの名前を入力します。

フィールド	説明
構成設定 (ID プロバイダー設定の手動構成)	
エンティティ ID	ID プロバイダーのグローバルに一意の名前を入力します。通常、ID プロバイダー エンティティ ID の形式は URI です。
SSO URL	サービスプロバイダーが SAML 認証要求を送信する必要がある URL を指定します。
証明書	ID プロバイダーが SAML アサーションに署名する場合、ID プロバイダーの署名証明書をアップロードする必要があります。
構成設定 (ID プロバイダー メタデータのインポート)	
IDP メタデータのインポート	[メタデータのインポート (Import Metadata)] をクリックして、メタデータ ファイルを選択します。

**ステップ 5** 変更を送信し、保存します。

### 次のタスク

[スパム隔離のための SSO の有効化 \(580 ページ\)](#)

## スパム隔離のための SSO の有効化

### 始める前に

次の内容について確認してください。

- [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [SAML] ページですべての設定が構成済みである。
- スパム隔離が有効になっている。「[スパム隔離 \(319 ページ\)](#)」を参照してください。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [スパム隔離 (Spam Quarantine)] に移動します。
- ステップ 3** [設定の編集 (Edit Settings)] をクリックして、[エンドユーザ隔離アクセス (End-User Quarantine Access)] セクションまでスクロールします。
- ステップ 4** エンドユーザ隔離アクセスが有効になっていることを確認します。
- ステップ 5** エンドユーザ認証方式を **SAML2.0** に設定します。
- ステップ 6** (任意) メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。

ステップ7 変更を送信し、保存します。

### 次のタスク

エンドユーザに新しい認証メカニズムについて通知します。

## ビューのカスタマイズ

- [お気に入りページの使用](#) (581 ページ)
- [プリファレンスの設定](#) (582 ページ)
- [全般設定](#) (582 ページ)

### お気に入りページの使用

(ローカル認証された管理ユーザ限定) よく利用するページのクイック アクセス リストを作成できます。

目的	操作手順
お気に入りリストにページを追加する	追加するページに移動し、ウィンドウの右上隅付近にある [お気に入り (My Favorites) ] メニューから [このページをお気に入りに追加 (Add This Page To My Favorites) ] を選択します。 お気に入りへの変更では確定操作は必要ありません。
お気に入りの順序を変更する	[お気に入り (My Favorites) ] > [お気に入りをすべて表示 (View All My Favorites) ] を選択し、適切な順序にお気に入りをドラッグします。
お気に入りページ、名前、または説明を編集する	[お気に入り (My Favorites) ] > [すべてのお気に入りを表示 (View All My Favorites) ] を選択し、編集するお気に入りの名前をクリックします。
お気に入りを削除する	[お気に入り (My Favorites) ] > [お気に入りをすべて表示 (View All My Favorites) ] を選択し、お気に入りを削除します。
お気に入りページに移動する	ウィンドウの右上隅付近にある [お気に入り (My Favorites) ] からページを選択します。
-メインインターフェイスに戻る	お気に入りを選択するか、ページ下部の [前のページに戻る (Return to previous page) ] をクリックします。

## プリファレンスの設定

### セキュリティ管理アプライアンスで設定された管理ユーザ

ローカル認証されたユーザは次のプリファレンスを選択できます。このプリファレンスは、ユーザがセキュリティ管理アプライアンスにログインするたびに適用されます。

- 言語（GUI に適用）
- ランディング ページ（ログイン後に表示されるページ）
- レポート ページのデフォルトの時間範囲（使用可能なオプションは、電子メールおよび Web レポーティング ページのサブセットです）
- レポート ページの表に表示する行数

実際のオプションは、ユーザ ロールによって異なります。

これらのプリファレンスを設定するには、[オプション (Options)] > [環境設定 (Preferences)] を設定します。([オプション (Options)] メニューは、GUI ウィンドウの上部右側にあります)。完了したら変更を送信します。確定する必要はありません。



**ヒント** [環境設定 (Preferences)] ページにアクセスする前に表示していたページに戻るには、ページ下部の [前のページに戻る (Return to previous page)] リンクをクリックします。

### 外部認証されたユーザ

外部認証されたユーザは、[オプション (Options)] メニューで表示言語を直接選択できます。

## 全般設定

- [Web インターフェイスのレンダリングの改善 \(583 ページ\)](#)
- [Web 使用状況分析のモニタリング \(582 ページ\)](#)

### Web 使用状況分析のモニタリング

統計分析のために Web サイトの使用状況またはアクティビティの送信を有効または無効にすることができます。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [全般設定 (General Settings)] を選択します。
- ステップ 3** [設定の編集 (Edit Settings)] をクリックします。

- ステップ4 [使用状況分析 (Usage Analytics)] フィールドで [有効 (Enable)] チェック ボックスをオンにします。
- ステップ5 変更を送信し、保存します。

## Web インターフェイスのレンダリングの改善

優れた Web インターフェイスのレンダリングのために、Internet Explorer 互換モードのオーバーライドを有効にすることを推奨します。



(注) この機能を有効にすることが組織のポリシーに違反する場合は、この機能を無効にすることができます。

- ステップ1 (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ2 [管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [全般設定 (General Settings)] を選択します。
- ステップ3 [設定の編集 (Edit Settings)] をクリックします。
- ステップ4 [IE互換モードの上書き (Override IE Compatibility Mode)] フィールドで [有効 (Enable)] チェック ボックスをオンにします。
- ステップ5 変更を送信し、保存します。

## アプライアンスで有効なサービスの再起動とステータスの表示

CLI で `diagnostic > services` サブコマンドを使用して、以下を実行できます。

- アプライアンスで有効になっているサービスを再起動します。アプライアンスを再起動する必要はありません。
- アプライアンスで有効になっているサービスのステータスを表示します。

### 例：レポート サービスのステータスの表示

次の例では、`services` コマンドを使用して、アプライアンスで有効になっているレポートサービスのステータスを表示します。

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
```

```
- REPORTING - Reporting Utilities.  
- TRACKING - Tracking Utilities.  
- RELOAD - Reset configuration to the initial manufacturer values.  
- SERVICES - Service Utilities.
```

```
[ ]> services
```

```
Choose one of the following services:  
- REPORTING - Reporting associated services  
- TRACKING - Tracking associated services  
- EUQWEB - End User Quarantine GUI  
- WEBUI - Web GUI
```

```
[ ]> reporting
```

```
Choose the operation you want to perform:  
- RESTART - Restart the service  
- STATUS - View status of the service
```

```
[ ]> status
```

```
Reporting has been up for 28d 20h 45m 35s.
```

### 例：メッセージトラッキングサービスの再起動

次の例では、`services` コマンドを使用して、アプライアンスで有効になっているメッセージトラッキングサービスを再起動します。

```
mail.example.com> diagnostic
```

```
Choose the operation you want to perform:  
- RAID - Disk Verify Utility.  
- DISK_USAGE - Check Disk Usage.  
- NETWORK - Network Utilities.  
- REPORTING - Reporting Utilities.  
- TRACKING - Tracking Utilities.  
- RELOAD - Reset configuration to the initial manufacturer values.  
- SERVICES - Service Utilities.
```

```
[ ]> services
```

```
Choose one of the following services:  
- REPORTING - Reporting associated services  
- TRACKING - Tracking associated services  
- EUQWEB - End User Quarantine GUI  
- WEBUI - Web GUI
```

```
[ ]> tracking
```

```
Choose the operation you want to perform:  
- RESTART - Restart the service  
- STATUS - View status of the service
```

```
[ ]> restart
```





## 第 17 章

# ログ

この章は、次の項で構成されています。

- [ロギングの概要 \(585 ページ\)](#)
- [ログタイプ \(589 ページ\)](#)
- [ログサブスクリプション \(611 ページ\)](#)

## ロギングの概要

ログファイルには、システムのアクティビティの例外に加えて、通常の動作が記録されます。Cisco コンテンツセキュリティアプライアンスのモニタリング、トラブルシューティング、およびシステムパフォーマンスの評価のためにログを使用します。

ほとんどのログは、プレーンテキスト (ASCII) 形式で記録されますが、トラッキングログはリソースの効率性を保つためにバイナリ形式で記録されます。ASCII テキスト情報は、任意のテキストエディタで読むことができます。

## ロギングとレポート

ロギングデータは、メッセージフローのデバッグ、基本的な日常の動作に関する情報の確認 (FTP 接続の詳細、HTTP ログファイルなど)、アーカイブのコンプライアンスの目的に使用します。

このロギングデータには、E メールセキュリティアプライアンスから直接アクセスすることも、任意の外部 FTP サーバに送信してアーカイブまたは読み取ることもできます。アプライアンスに FTP 接続してログにアクセスすることも、バックアップの目的でプレーンテキストのログを外部サーバにプッシュすることもできます。

レポートデータを表示するには、アプライアンスのグラフィカルユーザインターフェイスの [レポート (Report)] ページを使用します。元データにはアクセスできません。また、Cisco コンテンツセキュリティ管理アプライアンス以外には送信できません。



- (注) セキュリティ管理アプライアンスは、スパム隔離データの例外を含む、すべてのレポートイン  
グおよびトラッキング情報を取り出します。このデータは ESA からプッシュされます。

## ログの取得

ログファイルは、次の表に示すファイル転送プロトコルを使用して取得できます。プロトコルは、グラフィカルユーザインターフェイスでサブスクリプションを作成または編集するとき  
に設定するか、CLI の `logconfig` コマンドを使用して設定します。

FTP ポーリング	このタイプのファイル転送では、リモート FTP クライアントは管理者レベルまたはオペレータレベルのユーザのユーザ名およびパスワードを使用して、アプライアンスにアクセスし、ログ ファイルを取得します。FTP ポーリング方法を使用するようにログ サブスクリプションを設定する場合は、保持するログ ファイルの最大数を指定する必要があります。最大数に達すると、最も古いファイルが削除されます。
FTP プッシュ	このタイプのファイル転送では、Cisco コンテンツセキュリティアプライアンスがリモートコンピュータの FTP サーバに、定期的にログ ファイルをプッシュします。サブスクリプションには、リモートコンピュータ上のユーザ名、パスワード、および宛先ディレクトリが必要です。ログ ファイルは、設定されたロールオーバー スケジュールに基づいて転送されます。
SCP プッシュ	このタイプのファイル転送では、Cisco コンテンツセキュリティアプライアンスがリモートコンピュータの SCP サーバに、定期的にログ ファイルをプッシュします。この方法には、SSH2 プロトコルを使用するリモートコンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、ユーザ名、SSH キー、およびリモートコンピュータ上の宛先ディレクトリが必要です。ログ ファイルは、設定されたロールオーバー スケジュールに基づいて転送されます。

Syslog プッシュ	このタイプのファイル転送では、Cisco コンテンツセキュリティアプライアンスがリモート Syslog サーバにログメッセージを送信します。この方法は、RFC 3164 に準拠しています。Syslog サーバのホスト名を指定し、ログの送信に UDP または TCP を使用する必要があります。使用するポートは514です。ログのファシリティは選択できますが、ログタイプのデフォルトはドロップダウンメニューであらかじめ選択されています。syslog プッシュを使用して転送できるのは、テキストベースのログだけです。
-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## ファイル名およびディレクトリ構造

AsyncOS はログサブスクリプションで指定したログ名に基づいて、各ログサブスクリプションのディレクトリを作成します。ディレクトリ内のログのファイル名は、ログサブスクリプションで指定されたファイル名、ログファイルが開始されたタイムスタンプ、および単一文字のステータスコードで構成されています。次に、ディレクトリおよびファイル名の規則の例を示します。

```
<Log_Name>/<Log_Filename>.@<timestamp>.<statuscode>
```

ステータスコードは、.c (「current (現在)」の意味)、または.s (「saved (保存済み)」の意味) です。保存済みのステータスのログファイルのみを転送する必要があります。

## ログのロールオーバーおよび転送スケジュール

ログサブスクリプションを作成するときに、ログのロールオーバー、古いファイルの転送、および新しいファイルの作成のトリガーを指定します。

次のトリガーのいずれかを選択します。

- ファイルサイズ (File size)
- 時刻 (Time)
  - 指定した間隔で (秒、分、時間、または日数)
 

値を入力するときは、画面の例に従います。

2 時間半などの複合間隔を入力するには、例の 2h30m に従います。

または
  - 毎日、指定した時刻に
 

または
  - 選択した週の曜日の指定した時刻に

時刻を指定する場合は、24 時間形式を使用します。たとえば 11pm は 23:00 です。

1日に複数のロールオーバー時間をスケジュール設定するには、時間をカンマで区切ります。たとえば、深夜と正午にログをロールオーバーするには、00:00,12:00 と入力します

アスタリスク (\*) をワイルドカードとして使用できます。たとえば、正確に毎時および30分ごとにログをロールオーバーするには、\*:00,\*:30 と入力します

指定した制限に達すると（またはサイズおよび時間の両方に基づいた制限を設定している場合は最初の制限に達すると）、ログファイルがロールオーバーされます。FTP ポーリング転送メカニズムに基づいたログサブスクリプションでは、ファイルが作成されると、それらのファイルが取得されるか、システムでログファイル用にさらにスペースが必要になるまで、アプライアンスのFTP ディレクトリにそれらのファイルが保存されます。



(注) 次の制限に達したときにロールオーバーが実行中の場合、新しいロールオーバーはスキップされます。エラーが記録され、アラートが送信されます。

## ログファイル内のタイムスタンプ

次のログファイルには、ログ自体の開始日と終了日、AsyncOS のバージョン、およびGMT オフセット（ログの開始時からの秒数）が含まれています。

- メール ログ
- セーフリスト/ブロックリスト ログ
- システム ログ

## デフォルトで有効になるログ

セキュリティ管理アプライアンスでは、次のログサブスクリプションが有効に事前設定されています。

表 83: 事前設定されたログサブスクリプション

ログ名	ログタイプ	取得方法
cli_logs	CLI 監査ログ	FTP ポーリング
euq_logs	スパム隔離ログ	FTP ポーリング
euqgui_logs	スパム隔離 GUI ログ	FTP ポーリング
gui_logs	HTTP ログ	FTP ポーリング
mail_logs	テキスト メール ログ	FTP ポーリング
reportd_logs	レポートログ	FTP ポーリング

ログ名	ログタイプ	取得方法
reportqueryd_logs	レポーティングクエリログ	FTP ポーリング
slbld_logs	セーフリスト/ブロックリストログ	FTP ポーリング
smad_logs	SMA ログ	FTP ポーリング
system_logs	システムログ	FTP ポーリング
trackerd_logs	トラッキングログ	FTP ポーリング

事前定義されているすべてのログサブスクリプションでは、ログレベルが **Information** に設定されています。ログレベルの詳細については、[ログレベルの設定 \(612 ページ\)](#) を参照してください。

適用されているライセンスキーによっては、追加のログサブスクリプションを設定できます。ログサブスクリプションの作成および編集については、[ログサブスクリプション \(611 ページ\)](#) を参照してください。

## ログタイプ

- [ログタイプの概要 \(590 ページ\)](#)
- [コンフィギュレーション履歴ログの使用 \(594 ページ\)](#)
- [CLI 監査ログの使用 \(595 ページ\)](#)
- [FTP サーバログの使用 \(596 ページ\)](#)
- [HTTP ログの使用 \(596 ページ\)](#)
- [スパム隔離ログの使用 \(597 ページ\)](#)
- [スパム隔離 GUI ログの使用 \(598 ページ\)](#)
- [テキスト メールログの使用 \(598 ページ\)](#)
- [NTP ログの使用 \(604 ページ\)](#)
- [レポーティングログの使用 \(604 ページ\)](#)
- [レポーティングクエリーログの使用 \(605 ページ\)](#)
- [セーフリスト/ブロックリストログの使用 \(606 ページ\)](#)
- [SMA ログの使用 \(606 ページ\)](#)
- [ステータスログの使用 \(607 ページ\)](#)
- [システムログの使用 \(610 ページ\)](#)
- [トラッキングログについて \(610 ページ\)](#)

## ログタイプの概要

ログサブスクリプションはログタイプを名前、ログレベル、およびファイルサイズや宛先情報などのその他の特性に関連付けます。コンフィギュレーション履歴ログ以外のすべてのログタイプで、複数のサブスクリプションを使用できます。ログタイプによってログに記録されるデータが決まります。ログサブスクリプションを作成するときにログタイプを選択します。詳細については、[ログサブスクリプション \(611 ページ\)](#) を参照してください。

AsyncOS では、次のログタイプが生成されます。

表 84: ログタイプ

ログタイプ	説明
認証ログ	<p>認証ログには、ローカルまたは外部認証されたユーザおよびセキュリティ管理アプライアンスへの GUI および CLI の両方のアクセスについて、成功したログインと失敗したログイン試行が記録されます。</p> <p>外部認証がオンの場合、デバッグおよびより詳細なモードでは、すべての LDAP クエリがこれらのログに表示されます。</p>
バックアップログ	<p>バックアップログはバックアッププロセスを開始から終了まで記録します。</p> <p>バックアップスケジューリングに関する情報は、SMA ログ内にあります。</p>
CLI 監査ログ	CLI 監査ログには、システム上のすべての CLI アクティビティが記録されます。
設定履歴ログ	コンフィギュレーション履歴ログは、どのようなセキュリティ管理アプライアンスの変更がいつ行われたかの情報を記録します。ユーザが変更をコミットするたびに、新しいコンフィギュレーション履歴ログが作成されます。
FTP サーバログ	FTP ログには、インターフェイスで有効になっている FTP サービスの情報が記録されます。接続の詳細とユーザアクティビティが記録されます。
GUI ログ	<p>GUI ログには、Web インターフェイスでのページ更新の履歴、セッションデータ、およびユーザがアクセスしたページが記録されます。GUI ログを使用して、ユーザアクティビティを追跡することや、GUI でユーザに表示されたエラーを調査できます。エラートレースバックは、通常、このログに記録されます。</p> <p>GUI ログには、SMTP トランザクションに関する情報（たとえば、アプライアンスから電子メールで送信されるスケジュール済みレポートに関する情報）も記録されます。</p>

ログタイプ	説明
HTTP ログ	HTTP ログには、インターフェイスで有効になっている HTTP サービスおよびセキュア HTTP サービスに関する情報が記録されます。HTTP を介してグラフィカルユーザインターフェイス (GUI) にアクセスするため、HTTP ログは基本的に、CLI 監査ログの GUI 版になっています。セッションデータ (新規セッション、期限切れセッションなど)、およびグラフィカルユーザインターフェイスでアクセスされたページが記録されます。
Haystack ログ	Haystack ログには、データ処理をトラッキングする Web トランザクションが記録されます。
テキスト メール ログ	テキスト メール ログには、電子メール システムの動作 (メッセージの受信、メッセージの配信試行、接続の開始と終了、メッセージのバウンスなど) に関する情報が記録されます。  メール ログに添付ファイル名が含まれる場合に関する重要な情報については、 <a href="#">トラッキングサービスの概要 (299 ページ)</a> を参照してください。
LDAP デバッグ ログ	[システム管理 (System Administration)] > [LDAP] で LDAP を設定している場合は、これらのログを問題のデバッグに使用します。  たとえば、これらのログには、[テストサーバ (Test Server)] および [テストクエリ (Test Queries)] ボタンをクリックした結果が記録されます。  失敗した LDAP 認証の詳細については、 <a href="#">認証ログ</a> を参照してください。
NTP ログ	NTP ログには、アプライアンスと任意の設定済みネットワーク タイム プロトコル (NTP) サーバとの通信が記録されます。NTP サーバの設定の詳細については、 <a href="#">システム時刻の設定 (556 ページ)</a> を参照してください。
レポートログ	レポートログには、中央集中型レポートサービスのプロセスに関連付けられたアクションが記録されます。
レポートクエリー ログ	レポートクエリー ログには、アプライアンスで実行されるレポートクエリーに関連付けられたアクションが記録されます。
SMA ログ	SMA ログには、一般的なセキュリティ管理アプライアンスプロセスに関連付けられたアクションが記録されます。中央集中型レポート、中央集中型トラッキング、スパム隔離サービスのプロセスは含まれません。  これらのログには、バックアップ スケジューリングに関する情報が含まれます。

ログタイプ	説明
SNMP ログ	SNMP ログには、SNMP ネットワーク管理エンジンに関連するデバッグメッセージが記録されます。トレースまたはデバッグモードでは、セキュリティ管理アプライアンスへの SNMP 要求が含まれます。
セーフリスト/ブロックリスト ログ	セーフリスト/ブロックリスト ログには、セーフリスト/ブロックリストの設定およびデータベースに関するデータが記録されます。
スパム隔離 GUI ログ	スパム隔離 GUI ログには、GUI を介した隔離設定、エンドユーザ認証、エンドユーザアクション（例：電子メールの解放）など、スパム隔離 GUI に関連付けられたアクションが記録されます。
スパム隔離 ログ	スパム隔離 ログには、スパム隔離プロセスに関連付けられたアクションが記録されます。
ステータス ログ	ステータス ログには、 <code>status detail</code> および <code>dnsstatus</code> を含む CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、 <code>logconfig</code> の <code>setup</code> サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。
システム ログ	システム ログには、ブート情報、DNS ステータス情報、および <code>commit</code> コマンドを使用してユーザが入力したコメントが記録されます。システム ログは、アプライアンスの状態のトラブルシューティングに役立ちます。
トラッキング ログ	トラッキング ログには、トラッキング サービスのプロセスに関連付けられたアクションが記録されます。トラッキング ログは、メール ログのサブセットになっています。
アップデート ログ	時間帯のアップデートなど、サービス アップデートに関する情報。
アップグレード ログ	アップグレードのダウンロードとインストールに関するステータス情報。

## ログタイプの比較

次の表に、各ログタイプの特徴をまとめます。



表 85: ログタイプの比較

						記載内容					
	取引	ステートレス	テキストとして記録	バイナリとして記録	ヘッダーロギング	定期的なステータス情報	メッセージ受信情報	配信情報	個別のハードバウンズ	個別のソフトバウンズ	設定情報
認証ログ	•		•								
バックアップログ	•		•								
CLI 監査ログ	•		•			•					
設定履歴ログ	•		•								•
FTP サーバログ	•		•			•					
HTTP ログ	•		•			•					
Haystack ログ	•		•								
テキストメールログ	•		•		•	•	•	•	•	•	
LDAP デバッグログ	•		•								
NTP ログ	•		•			•					
レポートイングログ	•		•			•					

						記載内容					
レポー ティング クエリ ログ	•		•			•					
SMA ログ	•		•			•					
SNMP ログ	•		•								
セーフリ スト/ブ ロックリ ストログ	•		•			•					
スパム隔 離 GUI	•		•			•					
スパム隔 離	•		•			•					
ステータ ス ログ		•	•			•					
システム ログ	•		•			•					
トラッキ ング ログ	•			•	•		•	•	•	•	
アップ データ ログ	•		•								

## コンフィギュレーション履歴ログの使用

コンフィギュレーション履歴ログは、ユーザの名前、ユーザが変更を行った設定の場所の説明、および変更を保存するときにユーザが入力したコメントがリストされた追加のセクションを持つコンフィギュレーションファイルで構成されます。ユーザが変更を保存するたびに、変更後のコンフィギュレーションファイルを含む新しいログが作成されます。

例

次の設定履歴ログの例は、システムへのログインを許可されているローカルユーザを定義するテーブルにユーザ (admin) がゲストユーザを追加したことを示しています。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
XML generated by configuration change.
Change comment: added guest user
User: admin
Configuration are described as:
  This table defines which local users are allowed to log into the system.
Product: M160 Messaging Gateway(tm) Appliance
Model Number: M160
Version: 6.7.0-231
Serial Number: 000000000ABC-D000000
Number of CPUs: 1
Memory (GB): 4
Current Time: Thu Mar 26 05:34:36 2009
Feature "Centralized Configuration Manager": Quantity = 10, Time Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"
Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"
Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"
-->
<config>
```

## CLI 監査ログの使用

次の表に、CLI 監査ログに記録される統計情報を示します。

表 86: CLI 監査ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
PID	コマンドが入力された特定の CLI セッションのプロセス ID。
Message	メッセージは、入力された CLI コマンド、CLI 出力 (メニュー、リストなど)、および表示されるプロンプトで構成されます。

例

次の CLI 監査ログの例は、who および textconfig CLI コマンドが入力された PID 16434 の情報を示しています。

```
Thu Sep  9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '
Thu Sep  9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n
=====
admin      Wed 11AM   3m 45s   10.1.3.14  tail\nadmin   02:32PM    0s
10.1.3.14  cli\nmail3.example.com> '
Thu Sep  9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
```

```
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[ ]>
```

## FTP サーバ ログの使用

次の表に、FTP サーバ ログに記録される統計情報を示します。

表 87: FTP サーバ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	接続 ID。FTP 接続ごとの別個の ID。
Message	ログエントリのメッセージセクションは、ログファイルのステータス情報、または FTP 接続情報（ログイン、アップロード、ダウンロード、ログアウトなど）になります。

例

次の FTP サーバ ログの例には、接続（ID:1）が記録されています。着信接続の IP アドレスのほか、アクティビティ（ファイルのアップロードとダウンロード）およびログアウトが示されています。

```
Wed Sep  8 18:03:06 2004 Info: Begin Logfile
Wed Sep  8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21
Wed Sep  8 18:03:06 2004 Info: Time offset from UTC: 0 seconds
Wed Sep  8 18:03:06 2004 Info: System is coming up
Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds
Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86
Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS
Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes
Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes
Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

## HTTP ログの使用

次の表に、HTTP ログに記録される統計情報を示します。

表 88: HTTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
ID	セッション ID。
req	接続元マシンの IP アドレス。

統計	説明
ユーザ	接続ユーザのユーザ名。
メッセージ	実行されたアクションに関する情報。GET コマンド、POST コマンド、またはシステム ステータスなどが含まれる場合があります。

例

次の HTTP ログの例は、admin ユーザによる GUI の使用（システムセットアップウィザードの実行など）を示しています。

```

Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443
Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80
Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443
Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds
Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST /system_administration/system_setup_wizard HTTP/1.1 303
Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /system_administration/ssw_done HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/incoming_mail_overview HTTP/1.1 200
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190 HTTP/1.1 200
Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=190 HTTP/1.1 200
Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET /monitor/quarantines HTTP/1.1 200
    
```

## スパム隔離ログの使用

次の表に、スパム隔離ログに記録される統計情報を示します。

表 89: スパム隔離ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、実行されたアクション（メッセージの隔離、隔離領域からの解放など）で構成されます。

例

次のログの例は、隔離から admin@example.com に 2 個のメッセージ（MID 8298624 と MID 8298625）が解放されたことを示しています。

```

Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com
    
```

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work queue)
Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

## スパム隔離 GUI ログの使用

次の表に、スパム隔離 GUI ログに記録される統計情報を示します。

表 90: スパム隔離 GUI ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

例

次のログの例は、成功した認証、ログイン、およびログアウトを示しています。

表 91: スパム隔離 GUI ログの例

Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82
Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83
Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin
Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCf0 session:10.251.23.228
Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCf0 session:10.251.23.228
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin

## テキスト メール ログの使用

これらのログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。これらのログは、特定のメッセージの配信を理解し、システムパフォーマンスを分析するうえで有益な情報源となります。

これらのログに、特別な設定は必要ありません。ただし、添付ファイル名を表示するには、適切なシステムの設定が必要です。添付ファイル名は、常に記録されるわけではありません。詳細については、[トラッキング サービスの概要 \(299 ページ\)](#) を参照してください。

次の表に、テキスト メール ログに表示される情報を示します。

表 92: テキスト メール ログの統計情報

統計	説明
ICID	インジェクション接続ID。システムに対する個々のSMTP接続を表す数値IDです。システムへの1つのSMTP接続で、単一のメッセージまたは多数のメッセージを送信できます。
DCID	配信接続ID。別のサーバに対する個々のSMTP接続を表す数値IDであり、この接続で1個から数千個のメッセージが配信されます。1つのメッセージ送信で一部または全部のRIDと一緒に配信されます。
RCID	RPC Connection ID (RPC 接続 ID)。スパム隔離に対する個々のRPC接続を表す数値IDです。このIDを使用して、スパム隔離との間で送受信されるメッセージを追跡します。
MID	メッセージID。このIDを使用して、メッセージのフローをログで追跡します。
RID	受信者ID。各メッセージ受信者には、IDが割り当てられます。
新規作成 (New)	新規の接続が開始されました。
開始	新規のメッセージが開始されました。

## テキストメール ログのサンプル

ログ ファイルを解釈するためのガイドとして、次のサンプルを使用してください。



- (注) ログファイルの各行には、番号が割り当てられません。ここでは、単にサンプル用として番号が割り当てられています。

表 93: テキスト メール ログの詳細

1	Mon Apr 17 19:56:22 2003 Info: New SMTP ICID 5 interface Management (10.1.1.1) address 10.1.1.209 reverse dns host remotehost.com verified yes
2	Mon Apr 17 19:57:20 2003 Info: Start MID 6 ICID 5
3	Mon Apr 17 19:57:20 2003 Info: MID 6 ICID 5 From: <sender@remotehost.com>
4	Mon Apr 17 19:58:06 2003 Info: MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>

5	Mon Apr 17 19:59:52 2003 Info: MID 6 ready 100 bytes from <sender@remotehost.com>
6	Mon Apr 17 19:59:59 2003 Info: ICID 5 close
7	Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25
8	Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 8 MID 6 to RID [0]
9	Mon Mar 31 20:10:58 2003 Info: Message done DCID 8 MID 6 to RID [0]
10	Mon Mar 31 20:11:03 2003 Info: DCID 8 close

前述のログ ファイルを読み取るためのガイドとして、次の表を使用してください。

表 94: テキストメール ログの例の詳細

行番号	説明
1	システムに対して新しい接続が開始され、インジェクション ID (ICID) 「5」が割り当てられました。接続は管理 IP インターフェイスで受信され、10.1.1.209 のリモートホストで開始されました。
2	クライアントから MAIL FROM コマンドが実行された後、メッセージにメッセージ ID (MID) 「6」が割り当てられました。
3	送信者アドレスが識別され、受け入れられます。
4	受信者が識別され、受信者 ID (RID) 「0」が割り当てられました。
5	MID 5 が受け入れられ、ディスクに書き込まれ、承認されます。
6	受信に成功し、受信接続がクローズします。
7	メッセージ配信プロセスが開始されました。192.168.42.42 から 10.5.3.25 への配信に、配信接続 ID (DCID) 「8」が割り当てられました。
8	RID 「0」へのメッセージ配信が開始されました。
9	RID 「0」への MID 6 の配信に成功しました。
10	配信接続がクローズします。



## テキストメール ログ エントリの例

次の例で、さまざまなケースに基づくログ エントリを示します。

### メッセージ受信

1 人の受信者に対するメッセージがアプライアンスにインジェクトされます。メッセージは正常に配信されます。

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com (1.2.3.4)
  address 2.3.4.5 reverse dns host unknown verified no
Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None
Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970
Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>
Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID '<37gva9$5uvbhe@mail.example.com>'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'
Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>
Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative
Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery
Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4
Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]
Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close
Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
(['X-SBRS', 'None'])
Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery
Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

### 正常なメッセージ配信の例

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]
Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]
Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

### 失敗したメッセージ配信（ハードバウンス）

2 人の受信者が指定されたメッセージがアプライアンスにインジェクトされます。配信時に、宛先ホストが 5XX エラーを返しました。これは、メッセージをどちらの受信者にも配信できなかったことを示します。アプライアンスは、送信者に通知して、キューからそれらの受信者を削除します。

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address 64.81.204.225
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
  error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
  error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

### 最終的に正常に配信されるソフトバウンスの例

メッセージがアプライアンスにインジェクトされます。最初の配信試行で、メッセージはソフトバウンスして、その後の配信キューに入れられます。2 回目の試行でメッセージは正常に配信されます。

## メッセージスキャン結果 (scanconfig)

```

Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address 63.251.108.110
Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
  error ('466', ['Mailbox temporarily full.'])[]
Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23
  2003
Mon Mar 31 20:01:28 2003 Info: DCID 5 close
Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113
Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]
Mon Mar 31 20:01:33 2003 Info: DCID 16 close

```

## メッセージスキャン結果 (scanconfig)

次のプロンプトで、メッセージの構成要素を分解できない場合（添付ファイルを削除する場合）の動作を `scanconfig` コマンドを使用して決定した場合、

```

If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[3]>

```

メール ログに以下が表示されます。

`scanconfig` で、メッセージを分解できない場合に配信するように設定した場合。

```

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>
Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'
Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:36:29 2004 Info: ICID 44784 close
Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'
Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus
Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done

```

`scanconfig` で、メッセージを分解できない場合にドロップするように設定した場合。

```

Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org
Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 257 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 257 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close

```

## 添付ファイルを含むメッセージ

この例では、添付ファイル名の識別を有効にするように、条件「Message Body Contains」を含むコンテンツ フィルタが設定されています。

```

Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes
Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRs 0.0
Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$ff24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery

```

3つの添付ファイルの2番目が Unicode であることに注意してください。Unicode を表示できない端末では、このような添付ファイルは quoted-printable 形式で表示されます。

## 生成またはリライトされたメッセージ

リライト/リダイレクトアクションなどの一部の機能 (alt-rcpt-to フィルタ、アンチスパム RCPT リライト、bcc() アクション、アンチウイルス リダイレクションなど) によって、新しいメッセージが作成されます。ログに目を通して結果を確認し、必要に応じて MID や、場合によっては DCID を追加します。次のようなエントリが可能です。

```

Tue Jun 1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
または

```

```

Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispaM
Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter 'testfilt'

```



(注) 「Rewritten」 エントリは、新しい MID の使用を示すログの行の後に表示されます。

## スパム隔離へのメッセージの送信

メッセージを隔離領域に送信すると、メールログでは、RPC 接続を識別する RPC 接続 ID (RCID) を使用して、隔離領域との間の移動が追跡されます。次のメールログでは、スパムとしてタグが付けられたメッセージがスパム隔離に送信されています。

```

Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To: <stevell@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'

```

```

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect
Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local Spam
Quarantine
Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877
Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877
Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done

```

## NTP ログの使用

次の表に、NTP ログに記録される統計情報を示します。

表 95: NTP ログに記録される統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、サーバへの簡易ネットワーク タイム プロトコル (SNTP) クエリまたは adjust: メッセージで構成されます。

例

次の NTP ログの例は、アプライアンスから NTP ホストへの 2 度のポーリングを示しています。

```

Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652
Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096
Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152
Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096

```

## レポーティング ログの使用

次の表に、レポーティング ログに記録される統計情報を示します。

表 96: レポーティング ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

例

次のレポートクエリ ログの例は、情報ログ レベルに設定されたアプライアンスを示しています。

```

Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40
Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692
Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds
Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41
Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692
Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)
Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)
Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)
Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)
Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
    
```

## レポートクエリ ログの使用

次の表に、レポートクエリ ログに記録される統計情報を示します。

表 97: レポートクエリ ログの統計情報

統計	説明
タイムスタンプ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

例

次のレポートクエリ ログの例は、アプライアンスによって、2007年8月29日から10月10日までの期間で毎日の発信メールトラフィッククエリが実行されていることを示しています。

```

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENT_FILTER',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_PROCESSED'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constraints
None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
0 to 2 sort_ascending=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.
Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.
    
```

```
TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMM
ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to 2007-10-01
with key constra
ints None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort
_ascending=False.
Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

## セーフリスト/ブロックリスト ログの使用

次の表に、セーフリスト/ブロックリスト ログに記録される統計情報を示します。

表 98: セーフリスト/ブロックリスト ログの統計情報

統計	説明
タイムスタン プ	バイトが送信された時刻。
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

例

次のセーフリスト/ブロックリスト ログの例は、アプライアンスによって2時間ごとにデータベースのスナップショットが作成されていることを示しています。送信者がデータベースに追加された時刻も示されます。

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC: 10800
seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.
Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.
Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.
.....
Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.
Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.
Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.
Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

## SMA ログの使用

次の表に、SMA ログに記録される統計情報を示します。

表 99: SMA ログの統計情報

統計	説明
タイムスタン プ	バイトが送信された時刻。

統計	説明
メッセージ	メッセージは、ユーザ認証など、実行されたアクションで構成されます。

例

次の SMA ログの例は、Email Security Appliance からトラッキング ファイルをダウンロードする中央集中型トラッキング サービスと、Email Security Appliance からレポートング ファイルをダウンロードする中央集中型レポートング サービスを示しています。

```

Wed Oct 3 13:26:39 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202244Z_20071003T202544Z.s
Wed Oct 3 13:28:11 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T202443Z_20071003T202743Z.s
Wed Oct 3 13:28:46 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202544Z_20071003T202844Z.s
Wed Oct 3 13:31:27 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T202743Z_20071003T203043Z.s
Wed Oct 3 13:31:28 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.15 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.000F1F6ECA7C-2RWDB51.v1.tgz
Wed Oct 3 13:31:53 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.17
- /export/tracki
ng/tracking.@20071003T202844Z_20071003T203144Z.s
Wed Oct 3 13:32:31 2007 Info: TRANSFER: Plugin REPORTINGPLUGIN downloading from
172.29.0.17 - /reporting/ou
tgoing_queue/rpx.2007-10-03-20-15Z.0019B9B316E4-JZ41PC1.v1.tgz
Wed Oct 3 13:34:40 2007 Info: TRANSFER: Plugin TRACKINGPLUGIN downloading from 172.29.0.15
- /export/tracki
ng/tracking.@20071003T203043Z_20071003T203343Z.s
    
```

## ステータス ログの使用

ステータス ログには、status、status detail、および dnsstatus などの CLI ステータス コマンドで検出されたシステム統計情報が記録されます。記録期間は、logconfig の setup サブコマンドを使用して設定します。ステータス ログでレポートされるカウンタまたはレートは、前回カウンタがリセットされた時点からの値です。

表 100: ステータス ログの統計情報

統計	説明
CPULd	CPU 使用率。
DskIO	ディスク I/O 使用率。
RAMUtil	RAM 使用率。
QKUsd	使用されているキュー (キロバイト単位)。

統計	説明
QKFre	空いているキュー（キロバイト単位）。
CrtMID	メッセージ ID（MID）。
CrtICID	インジェクション接続 ID（ICID）。
CRTDCID	配信接続 ID（DCID）。
InjMsg	インジェクトされたメッセージ。
InjRcp	インジェクトされた受信者。
GenBncRcp	生成されたバウンス受信者。
RejRcp	拒否された受信者。
DrpMsg	ドロップされたメッセージ。
SftBncEvt	ソフトバウンスされたイベント。
CmpRcp	完了した受信者。
HrdBncRcp	ハードバウンスされた受信者。
DnsHrdBnc	DNS ハードバウンス。
5XXHrdBnc	5XX ハードバウンス。
FltrHrdBnc	フィルタ ハードバウンス。
ExpHrdBnc	期限切れハードバウンス。
OtrHrdBnc	その他のハードバウンス。
DlvRcp	配信された受信者。
DelRcp	削除された受信者。
GlbUnsbHt	グローバル配信停止リストとの一致数。
ActvRcp	アクティブ受信者。
UnatmptRcp	未試行受信者。
AtmptRcp	試行受信者。
CrtCncIn	現在の着信接続。
CrtCncOut	現在の発信接続。
DnsReq	DNS 要求。



統計	説明
NetReq	ネットワーク要求。
CchHit	キャッシュ ヒット。
CchMis	キャッシュ ミス。
CchEct	キャッシュ 例外。
CchExp	キャッシュ 期限切れ。
CPUTTm	アプリケーションが使用した合計 CPU 時間。
CPUETm	アプリケーションが開始されてからの経過時間。
MaxIO	メール プロセスに対する 1 秒あたりの最大ディスク I/O 動作。
RamUsd	割り当て済みのメモリ (バイト単位)。
SwIn	スワップインされたメモリ。
SwOut	スワップアウトされたメモリ。
SwPgIn	ページインされたメモリ。
SwPgOut	ページアウトされたメモリ。
MMLen	システム内の合計メッセージ数。
DstInMem	メモリ内の宛先オブジェクト数。
ResCon	リソース保持の tarpit 値 (大量のシステム負荷により、着信メールの受け入れがこの秒数だけ遅延します)。
WorkQ	作業キューにある現在のメッセージ数。
QuarMsgs	システム隔離にある個々のメッセージ数 (複数の隔離領域に存在するメッセージは一度だけ集計されます)。
QuarQKUsd	システム隔離メッセージによって使用されたキロバイト数。
LogUsd	使用されたログパーティションの割合。
CASELd	CASE スキャンで使用された CPU の割合。
TotalLd	CPU の合計消費量。
LogAvail	ログファイルに使用できるディスク領域の大きさ。
EuQ	スパム隔離内のメッセージ数。

統計	説明
EuqRls	スパム隔離解放キュー内のメッセージ数。

例

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861 InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp
6318 DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc 15
FltrHrdBnc 0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp
0 AtmptRcp 0 CrtCncIn 0 CrtCncOut 0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis
504791 CchEct 15395 CchExp 55085 CPUTm 228 CPUETm 181380 MaxIO 350 RAMUsd 21528056 MMLen
0 DstInMem 4 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0 CASELd 3
TotalLd 3 LogAvail 17G EuQ 0 EuqRls 0
```

## システム ログの使用

次の表に、システム ログに記録される統計情報を示します。

表 101: システム ログの統計情報

統計	説明
タイムスタン プ	バイトが送信された時刻。
メッセージ	ログに記録されたイベント。

例

次のシステム ログの例は、**commit** を実行したユーザの名前と入力されたコメントを含む、いくつかの **commit** エントリを示しています。

```
Wed Sep 8 18:02:45 2004 Info: Version: 6.0.0-206 SN: XXXXXXXXXXXXX-XXX
Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds
Wed Sep 8 18:02:45 2004 Info: System is coming up
Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache
Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped
Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Passphrase
Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW
Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds
Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples
Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

## トラッキング ログについて

トラッキング ログには、AsyncOS の電子メール動作に関する情報が記録されます。ログ メッセージは、メール ログに記録されたメッセージのサブセットです。

トラッキング ログは、メッセージトラッキングデータベースを作成するため、メッセージトラッキング コンポーネントで使用されます。ログ ファイルはデータベースの作成プロセスで

消費されるので、トラッキングログは一過性のものになります。トラッキングログの情報は、人による読み取りや解析を目的とした設計になっていません。

トラッキングログは、リソースの効率性を保つためにバイナリ形式で記録され、転送されます。情報は、論理的にレイアウトされ、Cisco が提供するユーティリティを使用して変換した後は人による読み取りが可能になります。変換ツールは、URL : <http://tinyurl.com/3c518r> にあります。

## ログサブスクリプション

- [ログサブスクリプションの設定 \(611 ページ\)](#)
- [GUI でのログサブスクリプションの作成 \(613 ページ\)](#)
- [ロギングのグローバル設定 \(614 ページ\)](#)
- [ログサブスクリプションのロールオーバー \(616 ページ\)](#)
- [ホストキーの設定 \(618 ページ\)](#)

## ログサブスクリプションの設定

ログサブスクリプションによって、Cisco コンテンツセキュリティアプライアンスに、またはリモートに保存される個々のログファイルが作成されます。ログサブスクリプションは、プッシュ（別のコンピュータに配信）またはプル（アプライアンスから取得）されます。一般に、ログサブスクリプションには次の属性があります。

表 102: ログファイルの属性

属性	説明
ログタイプ (Log Type)	記録される情報のタイプと、ログサブスクリプションの形式を定義します。詳細については、 <a href="#">ログタイプの概要 (590 ページ)</a> を参照してください。
名前 (Name)	後で参照するための、ログサブスクリプションのわかりやすい名前。
ログファイル名 (Log Filename)	ディスクに書き込むときのファイルの物理名。システムに複数のコンテンツセキュリティアプライアンスがある場合、ログファイルを生成したアプライアンスを識別できる一意のログファイル名を使用します。
ファイルサイズによりロールオーバー (Rollover by File Size)	ファイルの最大サイズ。このサイズに到達すると、ロールオーバーされます。
時刻によりロールオーバー (Rollover by Time)	時間に基づいてログファイルをロールオーバーするタイミング。 <a href="#">ログのロールオーバーおよび転送スケジュール (587 ページ)</a> のオプションを参照してください。

属性	説明
レート制限 (Rate Limit)	指定した時間範囲 (秒単位) 内での、ログファイルのログ記録されるイベントの最大数を設定します。  デフォルトの時間範囲の値は 10 秒です。
ログレベル (Log Level)	各ログサブスクリプションの詳細レベル。
取得方法 (Retrieval Method)	ログファイルをアプライアンスから転送するときを使用する方式。

[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] ページ (または CLI の `logconfig` コマンド) を使用して、ログサブスクリプションを設定します。ログタイプを入力するプロンプトが表示されます (ログタイプの概要 (590 ページ) を参照)。ほとんどのログタイプで、ログサブスクリプションのログレベルの入力も要求されます。



- (注) コンフィギュレーション履歴ログのみ：コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、コンフィギュレーションにマスクされたパスフレーズが含まれているとロードできないことに注意してください。[管理アプライアンス (Management Appliance)] > [システム管理 (System Administration)] > [ログサブスクリプション (Log Subscriptions)] ページで、パスフレーズをログに含めるかどうかを尋ねるプロンプトが表示されたら、[はい (Yes)] を選択します。CLI の `logconfig` コマンドを使用する場合は、プロンプトで `y` を入力します。

## ログレベルの設定

ログレベルによって、ログに送信される情報量が決定します。ログには、5つの詳細レベルのいずれかを設定できます。詳細なログレベルを設定すると、省略されたログレベルを設定した場合と比べて、大きなログファイルが作成され、システムパフォーマンスに大きな影響を与えます。詳細なログレベル設定には、省略されたログレベル設定に含まれるすべてのメッセージと、追加のメッセージが含まれます。詳細レベルを上げるほど、システムのパフォーマンスは低下します。



- (注) ログタイプごとに異なるログレベルを指定できます。

表 103: ログレベル

ログレベル	説明
クリティカル	エラーだけがログに記録されます。最も省略されたログレベル設定です。このログレベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。ただし、詳細ログレベルのように、ログファイルがすぐに最大サイズに達することはありません。このログレベルは、syslog レベル Alert と同等です。
警告	すべてのシステムエラーと警告が記録されます。このログレベルでは、パフォーマンスおよび重要なアプライアンスのアクティビティをモニタすることはできません。Critical ログレベルよりは早く、ログファイルが最大サイズに達します。このログレベルは、syslog レベル Warning と同等です。
情報	システムの動作が逐次記録されます。たとえば、接続のオープンや配信試行が記録されます。Information レベルは、ログに推奨される設定です。このログレベルは、syslog レベル Info と同等です。
デバッグ	Information ログレベルよりも詳細な情報が記録されます。エラーをトラブルシューティングするときは、Debug ログレベルを使用します。この設定は一時的に使用し、後でデフォルトレベルに戻します。このログレベルは、syslog レベル Debug と同等です。
トレース	使用可能なすべての情報が記録されます。Trace ログレベルは、開発者にのみ推奨されます。このレベルを使用すると、システムのパフォーマンスが大きく低下するので、推奨されません。このログレベルは、syslog レベル Debug と同等です。

## GUIでのログサブスクリプションの作成

- ステップ1 (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ2 [管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ログサブスクリプション (Log Subscriptions) ] ページで、[ログサブスクリプションの追加 (Add Log Subscription) ] をクリックします。
- ステップ3 ログタイプを選択し、ログ名 (ログディレクトリ用) とログファイル自体の名前を入力します。
- ステップ4 該当する場合は、最大ファイルサイズを指定します。
- ステップ5 該当する場合は、ログをロールオーバーする日、時刻、または時間間隔を指定します。詳細については、[ログのロールオーバーおよび転送スケジュール \(587 ページ\)](#) を参照してください。
- ステップ6 該当する場合は、指定した時間範囲 (秒単位) 内にログファイルに記録されるイベントの最大数を設定します。
- ステップ7 該当する場合は、ログレベルを指定します。

**ステップ 8** (コンフィギュレーション履歴ログのみ) パスフレーズをログに含めるかどうかを選択します。

(注) マスクされたパスフレーズが含まれているコンフィギュレーションはロードできません。コンフィギュレーション履歴ログからコンフィギュレーションをロードする可能性がある場合は、[はい (Yes)] を選択してパスフレーズをログに含めます。

**ステップ 9** ログの取得方法を設定します。

**ステップ 10** 変更を送信し、保存します。

## ログサブスクリプションの編集

**ステップ 1** [ログサブスクリプション (Log Subscriptions)] ページの [ログ名 (Log Name)] 列にあるログ名をクリックします。

**ステップ 2** ログサブスクリプションを更新します。

**ステップ 3** 変更を送信し、保存します。

## ロギングのグローバル設定

システムは、テキストメールログおよびステータスログ内にシステムメトリックを定期的に記録します。[ログサブスクリプション (Log Subscriptions)] ページの [グローバル設定 (Global Settings)] セクションにある [設定の編集 (Edit Settings)] ボタン (または、CLI の `logconfig -> setup` コマンド) を使用して、次の情報を設定します。

- システムが測定を記録するまで待機する時間 (秒単位)
- メッセージ ID ヘッダーを記録するかどうか
- リモート応答ステータス コードを記録するかどうか
- 元のメッセージのサブジェクトヘッダーを記録するかどうか
- メッセージごとにログに記録するヘッダー

すべての Cisco コンテンツセキュリティアプライアンスログには、次の 3 項目を任意で記録できます。

- [メッセージ ID (Message-ID)] : このオプションを設定すると、可能な場合はすべてのメッセージのメッセージ ID ヘッダーがログに記録されます。このメッセージ ID は、受信したメッセージから取得される場合と、AsyncOS で生成される場合があります。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

- [リモート応答 (Remote Response)] : このオプションを設定すると、可能な場合はすべてのメッセージのリモート応答ステータス コードがログに記録されます。次に例を示します。

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

リモート応答文字列は、SMTP カンバセーション配信時の DATA コマンドへの応答後に受信される、人が読み取ることのできるテキストです。この例では、接続ホストが data コマンドを実行した後のリモート応答が、「queued as 9C8B425DA7」となります。

```
[...]
250 ok hostname
250 Ok: queued as 9C8B425DA7
```

文字列の先頭にある空白や句読点、および 250 応答の OK 文字は除去されます。文字列の末尾については、空白だけが除去されます。たとえば、Cisco コンテンツセキュリティアプライアンスはデフォルトで、DATA コマンドに対して 250 Ok: Message MID accepted という文字列で応答します。したがって、リモートホストが別の Cisco コンテンツセキュリティアプライアンスである場合は、エントリ「Message MID accepted」がログに記録されます。

- [元のサブジェクトヘッダー (Original Subject Header) ]: このオプションをイネーブルにすると、各メッセージの元のサブジェクトヘッダーがログに記録されます。

```
Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>
Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'
Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
```

## メッセージヘッダーのロギング

場合によっては、メッセージがシステムを通過するときに、メッセージのヘッダーの存在と内容を記録する必要があります。[ログ設定のグローバル設定 (Log Subscriptions Global Settings) ] ページ (または、CLI の logconfig -> logheaders サブコマンド) で、記録するヘッダーを指定します。アプライアンスは、指定されたメッセージヘッダーをテキストメールログおよびトラッキングログに記録します。ヘッダーが存在する場合、システムはヘッダーの名前と値を記録します。ヘッダーが存在しない場合は、ログに何も記録されません。



- (注) システムは、ロギングに指定したヘッダーに関係なく、メッセージの記録処理中に随時、メッセージに存在するすべてのヘッダーを評価します。



- (注) SMTP プロトコルについての RFC は、<http://www.faqs.org/rfcs/rfc2821.html> にあります。この RFC には、ユーザ定義のヘッダーが規定されています。



- (注) logheaders コマンドを使用してヘッダーをログに記録するように設定している場合、ヘッダー情報は配信情報の後に表示されます。

表 104: ヘッダーのログ (Log Headers)

ヘッダー名	ヘッダーの名前
値	ログに記録されるヘッダーの内容

たとえば、ログに記録するヘッダーとして「date,x-subject」を指定すると、メールログに次の行が表示されます。

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0] [('date', 'Tue, 31
May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

## GUI を使用したロギングのグローバル設定

**ステップ 1** [ログサブスクリプション (Log Subscriptions) ] ページの [グローバル設定 (Global Settings) ] セクションにある [設定の編集 (Edit Settings) ] ボタンをクリックします。

**ステップ 2** システム メトリクスの頻度、メール ログにメッセージ ID ヘッダーを加えるかどうか、リモート応答を加えるかどうか、および各メッセージの元のサブジェクト ヘッダーを加えるかどうかを指定します。

これらの設定の詳細については、[ロギングのグローバル設定 \(614 ページ\)](#) を参照してください。

**ステップ 3** ログに加えるその他のヘッダーを入力します。各エントリはカンマで区切ります。

**ステップ 4** 変更を送信し、保存します。

## ログサブスクリプションのロールオーバー

AsyncOS がログ ファイルをロールオーバーすると、次のことが行われます。

- ロールオーバーのタイムスタンプで新規ログファイルを作成し、文字「c」の拡張子によって現在のファイルとして指定します。
- 現在のログ ファイルの名前を、保存済みを示す文字「s」の拡張子付きに変更します。
- 新たに保存されたログ ファイルがリモート ホストに転送されます (プッシュ ベースの場合)。
- 同じサブスクリプションから以前に失敗したログファイルが転送されます (プッシュベースの場合)。
- 保持するファイルの合計数を超えた場合は、ログサブスクリプション内の最も古いファイルが削除されます (ポーリング ベースの場合)。

次の作業

### ログサブスクリプション内のログのロールオーバー

「[ログのロールオーバーおよび転送スケジュール \(587 ページ\)](#)」を参照してください。



## GUI を使用したログの即時ロールオーバー

- ステップ 1** [ログサブスクリプション (Log Subscriptions) ] ページで、ロールオーバーするログの右側のチェックボックスをオンにします。
- ステップ 2** [すべて (All) ] チェックボックスをオンにして、すべてのログをロールオーバー対象として選択することもできます。
- ステップ 3** [今すぐロールオーバー (Rollover Now) ] ボタンをクリックします。

### 次のタスク

- [ログサブスクリプション内のログのロールオーバー \(616 ページ\)](#)
- [CLI を介したログの即時ロールオーバー \(617 ページ\)](#)

## CLI を介したログの即時ロールオーバー

rollovernow コマンドを使用して、一度にすべてのログ ファイルをロールオーバーするか、リストから特定のログ ファイルを選択します。

## グラフィカル ユーザ インターフェイスでの最近のログ エントリの表示

GUI を介してログ ファイルを表示するには、[ログサブスクリプション (Log Subscriptions) ] ページのテーブルの[ログファイル (Log Files) ] 列にあるログサブスクリプションをクリックします。ログサブスクリプションへのリンクをクリックすると、パスフレーズを入力するプロンプトが表示されます。次に、そのサブスクリプションのログファイルのリストが表示されます。いずれかのログファイルをクリックして、ブラウザに表示したり、ディスクに保存したりすることができます。グラフィカル ユーザ インターフェイスを介してログを表示するには、管理インターフェイスで FTP サービスをイネーブルにしておく必要があります。

## 最新のログ エントリの表示 (tail コマンド)

AsyncOS は、アプライアンスに設定されたログの最新エントリを表示する tail コマンドをサポートしています。tail コマンドを実行して現在設定されているログの番号を選択すると、そのログが表示されます。Ctrl を押した状態で C を押して、tail コマンドを終了します。



(注) コンフィギュレーション履歴ログは、tail コマンドを使用して表示することができません。FTP または SCP を使用する必要があります。

例

次の例では、`tail` コマンドを使用してシステムログを表示します。`tail` コマンドは、`tail mail_logs` のように、表示するログの名前をパラメータとして指定することもできます

```
Welcome to the M600 Messaging Gateway(tm) Appliance
example.srv> tail
Currently configured logs:
1. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
2. "euq_logs" Type: "Spam Quarantine Logs" Retrieval: FTP Poll
3. "euqgui_logs" Type: "Spam Quarantine GUI Logs" Retrieval: FTP Poll
4. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
5. "mail_logs" Type: "Text Mail Logs" Retrieval: FTP Poll
6. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
7. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
8. "sblld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
9. "smad_logs" Type: "SMA Logs" Retrieval: FTP Poll
10. "system_logs" Type: "System Logs" Retrieval: FTP Poll
11. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
Enter the number of the log you wish to tail.
[]> 10
Press Ctrl-C to stop.
Thu Sep 27 00:18:56 2007 Info: Begin Logfile
Thu Sep 27 00:18:56 2007 Info: Version: 6.0.0-422 SN: 001143583D73-FT9GP61
Thu Sep 27 00:18:56 2007 Info: Time offset from UTC: 0 seconds
Thu Sep 27 00:18:47 2007 Info: System is coming up.
Thu Sep 27 00:23:05 2007 Warning: DNS query network error '[Errno 64] Host is down' to
'172.16.0.3' looking up 'downloads.cisco.com'
Fri Sep 28 22:20:08 2007 Info: PID 688: User admin commit changes:
Fri Sep 28 23:06:15 2007 Info: PID 688: User admin commit changes:
^Cexample.srv>
```

## ホストキーの設定

`logconfig -> hostkeyconfig` サブコマンドを使用して、Cisco コンテンツセキュリティアプライアンスから他のサーバにログをプッシュするときに、SSH で使用するホストキーを管理します。SSH サーバには、秘密キーと公開キーの2つのホストキーが必要です。秘密ホストキーはSSH サーバにあり、リモートマシンから読み取ることはできません。公開ホストキーは、SSH サーバと対話する必要がある任意のクライアントマシンに配信されます。



(注) ユーザキーを管理するには、お使いのEメールセキュリティアプライアンスのユーザガイドまたはオンラインヘルプの「Managing Secure Shell (SSH) Keys」を参照してください。

`hostkeyconfig` サブコマンドによって、次の機能が実行されます。

表 105: ホストキーの管理 : サブコマンドのリスト

コマンド	説明
新規作成 (New)	新しいキーを追加します。
編集 (Edit)	既存のキーを変更します。

コマンド	説明
削除 (Delete)	既存のキーを削除します。
スキャン (Scan)	ホスト キーを自動的にダウンロードします。
印刷 (Print)	キーを表示します。
ホスト	システムホストキーを表示します。これは、リモートシステムの「known_hosts」ファイルに配置される値です。
フィンガープリント (Fingerprint)	システムホストキーのフィンガープリントを表示します。
ユーザ (User)	リモートマシンにログをプッシュするシステムアカウントの公開キーを表示します。これは、SCP プッシュ サブスクリプションを設定するときに表示されるキーと同じです。これは、リモートシステムの「authorized_keys」ファイルに配置される値です。

例

次の例では、コマンドによってホスト キーがスキャンされ、ホストに追加されます。

```
mail3.example.com> logconfig
Currently configured logs:
[ list of logs
]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[ ]> hostkeyconfig
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[ ]> scan
Please enter the host or IP address to lookup.
[ ]> mail3.example.com
Choose the ssh protocol type:
1. SSH2:rsa
2. SSH2:dsa
3. All
[3]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed
]
```

```
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed
]
Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed
]
2. mail3.example.com ssh-rsa [ key displayed
]
3. mail3.example.com 1024 35 [ key displayed
]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
Currently configured logs:
[ list of configured logs
]
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>
mail3.example.com> commit
```



## 第 18 章

# トラブルシューティング

この章は、次の項で構成されています。

- システム情報の収集 (621 ページ)
- ハードウェア問題のトラブルシューティング (621 ページ)
- 機能の設定に関する問題のトラブルシューティング (622 ページ)
- 一般的なトラブルシューティング リソース (622 ページ)
- 特定の機能で発生する問題のトラブルシューティング (622 ページ)
- テクニカル サポートの使用 (624 ページ)
- パケット キャプチャの実行 (627 ページ)
- アプライアンスの電源のリモートリセット (629 ページ)

## システム情報の収集

シリアル番号を含む、アプライアンスとそのステータスについての情報を取得できます。参照 [システム ステータスのモニタリング \(425 ページ\)](#)

## ハードウェア問題のトラブルシューティング

ハードウェア アプライアンスの前面/背面パネルのライトは、アプライアンスの状態およびステータスを示します。これらのインジケータの説明については、『*Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*』などのハードウェア ガイドを参照してください (に記載されている場所から入手できます)。

温度範囲など、アプライアンスの仕様についてもこれらのマニュアルで確認できます。



- (注) x80 または x90 アプライアンスの電源を再投入する場合は、アプライアンスが起動するまで (すべての LED が緑色になるまで) 少なくとも 20 分間待ってから、電源ボタンを押してください。

## 機能の設定に関する問題のトラブルシューティング

機能を設定できない問題が発生した場合は、各機能で実行する必要があるタスクの概要を参照してください。概要には、それぞれの具体的な情報へのリンクが記載されています。

- [中央集中型 Web レポートニングおよびトラッキングの設定](#) (193 ページ)
- [中央集中型の電子メール レポートニングの設定](#) (56 ページ)
- [中央集中型メッセージトラッキングの設定](#) (300 ページ)
- [中央集中型スパム隔離の設定](#) (320 ページ)
- [集約されたポリシー、ウイルス、およびアウトブレイク隔離](#) (355 ページ)
- [Configuration Master を使用して中央集中型で Web セキュリティアプライアンスを管理する](#) (390 ページ)

## 一般的なトラブルシューティング リソース

一般的なトラブルシューティング リソースは次のとおりです。

- [最新アラート。最新アラートの表示](#) (543 ページ) を参照してください。
- [ログ ファイル。ログ](#) (585 ページ) を参照してください。
- 「マニュアルの更新」セクションを含むリリース ノート。 [資料](#) (655 ページ) を参照してください。
- [Cisco Bug Search Tool](#) (アクセスの手順はリリース ノートを参照してください)
- [ナレッジ ベースの記事](#) (657 ページ)
- [シスコ サポート コミュニティ](#) (657 ページ)

## 特定の機能で発生する問題のトラブルシューティング

[機能の設定に関する問題のトラブルシューティング](#) (622 ページ) も参照してください。

### Web セキュリティ関連の問題

- [すべてのレポートのトラブルシューティング](#) (36 ページ)
- [Web レポートニングおよびトラッキングのトラブルシューティング](#) (294 ページ)
- [コンフィギュレーション管理上の問題のトラブルシューティング](#) (423 ページ)
- 機能に関連する問題は、Web セキュリティアプライアンスの設定が原因の場合もあります。 [資料](#) (655 ページ) に記載されている場所で、ご使用のリリースのリリース ノートおよびオンライン ヘルプかユーザ ガイドを参照してください。

### 電子メール セキュリティ関連の問題

- [すべてのレポートのトラブルシューティング](#) (36 ページ)
- [メッセージ トラッキングのトラブルシューティング](#) (316 ページ)
- [スパム隔離機能のトラブルシューティング](#) (354 ページ)
- [集約されたポリシー隔離のトラブルシューティング](#) (388 ページ)
- 機能に関連する問題は、E メール セキュリティ アプライアンスの設定が原因の場合もあります。[資料](#) (655 ページ) に記載されている場所で、ご使用のリリースのリリース ノートおよびオンライン ヘルプかユーザ ガイドを参照してください。

### 一般的な問題

- コンフィギュレーション ファイルをロードできない場合は、[管理アプライアンス (Management Appliance) ]>[システム管理 (System Administration) ]>[ディスク管理 (Disk Management) ] ページのテーブルでディスク領域量が各機能の現在のサイズよりも大きいことを確認します。
- アップグレードを最近実行し、オンラインヘルプの表示が古い場合や、新しい機能に関する情報が見つからない場合は、ブラウザのキャッシュをクリアしてからブラウザウィンドウを再度開きます。
- 複数のブラウザ ウィンドウまたはタブを同時に使用している場合、Web インターフェイスを使用して設定を行うと、予期しない動作が発生することがあります。
- [アラートへの応答](#) (623 ページ) を参照してください。
- [管理ユーザアクセスのトラブルシューティング](#) (501 ページ) を参照してください。

## アラートへの応答

- [アラート : 380 または 680 ハードウェアでバッテリー再学習タイムアウト \(RAID イベント\) \(Battery Relearn Timed Out \(RAID Event\) on 380 or 680 Hardware\)](#) (623 ページ)
- [追加のアラートの説明](#) (624 ページ)

### アラート : 380 または 680 ハードウェアでバッテリー再学習タイムアウト (RAID イベント) (Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware)

問題 : 380 または 680 ハードウェアに関して、件名 [バッテリー再学習タイムアウト (Battery Relearn Timed Out) ] のアラートを受信します。

解決策 : このアラートは、問題を示している場合と示していない場合があります。バッテリー再学習タイムアウト自体は、RAID コントローラに問題があることを示すものではありません。コントローラは、後続の再学習で回復します。以降 48 時間他の RAID アラートに関する電子メールを監視して、この問題が他の問題の副作用ではないことを確認してください。システムから他の RAID 関連のアラートが表示されない場合は、この警告を無視してかまいません。

## 追加のアラートの説明

追加のアラートについては、次を参照してください。

- [ハードウェア アラートの説明 \(544 ページ\)](#)
- [システム アラートの説明 \(544 ページ\)](#)

次の作業

- [アラートの管理 \(541 ページ\)](#)

## テクニカル サポートの使用

- [アプライアンスからのサポート ケースのオープンおよび更新 \(624 ページ\)](#)
- [仮想アプライアンスのサポートの取得 \(625 ページ\)](#)
- [シスコのテクニカル サポート担当者のリモート アクセスの有効化 \(625 ページ\)](#)

## アプライアンスからのサポート ケースのオープンおよび更新

この方法を使用して Cisco TAC または独自のサポート サービスに連絡することができます。

始める前に

Cisco TAC に連絡する場合：

- 緊急の問題の場合、この方法は使用しないでください。代わりに、[カスタマー サポート \(657 ページ\)](#) に示されるその他の方法の 1 つを使用してサポートください。
- ヘルプに関しては別の選択肢を検討してみてください。
- この手順を使用してサポート事例を開くと、アプライアンスの設定ファイルがシスコカスタマーサポートに送信されます。アプライアンスの設定を送信したくない場合、別の方法を使用してカスタマー サポートにお問い合わせください。
- アプライアンスがインターネットに接続され電子メールを送信する必要があります。
- 既存の事例に関する情報を送信する場合は、ケース番号を確認してください。

**ステップ 1** アプライアンスへのログイン

**ステップ 2** [ヘルプとサポート (Help and Support)] > [テクニカルサポートに問い合わせる (Contact Technical Support)] を選択します。

**ステップ 3** サポート リクエストの受信者を設定します。

要求を Cisco TAC に送信する	[Ciscoテクニカルサポート (Cisco Technical Support)] チェックボックスをオンにします。
内部サポート デスクにだけ要求を送信する	<ul style="list-style-type: none"> <li>• [Ciscoテクニカルサポート (Cisco Technical Support)] チェックボックスをオフにします。</li> <li>• サポート デスクの電子メールアドレスを入力します。</li> </ul>



(任意) 他の受信者を追加する	電子メール アドレスを入力します。
-----------------	-------------------

**ステップ 4** フォームに入力します。

**ステップ 5** [送信 (Send) ] をクリックします。

## 仮想アプライアンスのサポートの取得

Cisco Content Security 仮想アプライアンスのサポート ケースを報告する場合は、仮想ライセンス番号 (VLN) 、契約番号、および製品 ID コード (PID) を提供する必要があります。

発注書を参照するか以下の表を使用すると、仮想アプライアンスで動作中のソフトウェアライセンスに基づく PID を特定できます。

機能	PID	説明
すべての中央集中型 Web セキュリティ機能	SMA-WMGT-LIC=	—
すべての中央集中型電子メールセキュリティ機能	SMA-EMGT-LIC=	

## シスコのテクニカル サポート担当者のリモート アクセスの有効化

シスコのカスタマーアシスタンスのみ、次の方法を使用してアプライアンスにアクセスできません。

- [シスコのテクニカル サポート担当者のリモート アクセスの有効化 \(625 ページ\)](#)
- [インターネットに直接接続されていないアプライアンスへのリモート アクセスの有効化 \(626 ページ\)](#)
- [テクニカル サポートのトンネルの無効化 \(626 ページ\)](#)
- [リモート アクセスの無効化 \(627 ページ\)](#)
- [サポートの接続状態の確認 \(627 ページ\)](#)

## インターネット接続されたアプライアンスへのリモート アクセスの有効化

サポートは、この手順でアプライアンスと [upgrades.ironport.com](http://upgrades.ironport.com) のサーバ間で作成される SSH トンネル経由でアプライアンスにアクセスします。

### 始める前に

インターネットから到達可能なポートを識別します。デフォルトでは、ポート25で、このポートは大部分の環境で機能します。このポート経由の接続は、ほとんどのファイアウォール設定で許可されます。

**ステップ 1** アプライアンスへのログイン

**ステップ 2** GUI ウィンドウの右上にある、[ヘルプとサポート (Help and Support)] > [リモートアクセス (Remote Access)] を選択します。

**ステップ 3** [有効 (Enable)] をクリックします。

**ステップ 4** 情報を入力します。

**ステップ 5** [送信 (Submit)] をクリックします。

---

### 次のタスク

サポート担当者のリモートアクセスが必要なくなったときは、[テクニカルサポートのトンネルの無効化 \(626 ページ\)](#) を参照してください。

## インターネットに直接接続されていないアプライアンスへのリモートアクセスの有効化

インターネットに直接接続されていないアプライアンスの場合、インターネットに接続されている第 2 のアプライアンスを介してアクセスされます。

### 始める前に

- アプライアンスは、インターネットに接続されている第 2 のアプライアンスにポート 22 で接続する必要があります。
- インターネットに接続されているアプライアンスで該当アプライアンスへのサポートトンネルを作成するには、[インターネット接続されたアプライアンスへのリモートアクセスの有効化 \(625 ページ\)](#) の手順を実行します。

---

**ステップ 1** サポートが必要なアプライアンスのコマンドラインインターフェイスから、`techsupport` コマンドを入力します。

**ステップ 2** `sshaccess` と入力します。

**ステップ 3** プロンプトに従います。

---

### 次のタスク

サポート担当者のリモートアクセスが必要なくなったときは、次のトピックを参照してください。

- [リモートアクセスの無効化 \(627 ページ\)](#)
- [テクニカルサポートのトンネルの無効化 \(626 ページ\)](#)

## テクニカルサポートのトンネルの無効化

有効にした `techsupport` トンネルは、`upgrades.ironport.com` に 7 日間接続されたままになります。その後、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。

---

**ステップ1** アプライアンスへのログイン

**ステップ2** GUI ウィンドウの右上にある、[ヘルプとサポート (Help and Support)] > [リモートアクセス (Remote Access)] を選択します。

**ステップ3** [無効 (Disable)] をクリックします。

---

## リモートアクセスの無効化

techsupport コマンドを使用して作成したリモートアクセス アカウントは、非アクティブ化されるまでアクティブのままです。

---

**ステップ1** コマンドライン インターフェイスから、techsupport コマンドを入力します。

**ステップ2** sshaccess と入力します。

**ステップ3** disable と入力します。

---

## サポートの接続状態の確認

**ステップ1** コマンドライン インターフェイスから、techsupport コマンドを入力します。

**ステップ2** status と入力します。

---

## パケット キャプチャの実行

パケット キャプチャは、サポート担当者が TCP/IP データおよびその他にアプライアンスから出入りするパケットを表示できるようにします。これはネットワーク設定をデバッグしたり、どのようなネットワークトラフィックがアプライアンスに到達または送出されているかを検出することができます。

---

**ステップ1** [ヘルプとサポート (Help and Support)] > [パケットキャプチャ (Packet Capture)] を選択します。

**ステップ2** パケット キャプチャ設定の指定：

- a) [パケットキャプチャ設定 (Packet Capture Settings)] セクションで、[設定を編集 (Edit Settings)] をクリックします。
- b) (任意) パケット キャプチャの期間、制限およびフィルタを入力します。

サポート担当者が、これらの設定の方法を説明する場合があります。

時間の単位を指定しないでキャプチャ期間を入力すると、AsyncOS はデフォルトで秒を使用します。

[フィルタ (Filters)] セクションで次を実行します。

- カスタム フィルタでは UNIX の `tcpdump` コマンドでサポートされる `host 10.10.10.10 && port 80` のような構文を使用できます。
- クライアント IP は、E メールセキュリティ アプライアンスを介してメッセージを送信するメールクライアントなどのアプライアンスに接続しているマシンの IP アドレスです。
- サーバ IP は、アプライアンスがメッセージを配信する Exchange サーバなどのアプライアンスが接続しているマシンの IP アドレスです。

クライアントとサーバの IP アドレスを使用して、中間に E メールセキュリティ アプライアンスがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。

c) [送信 (Submit) ] をクリックします。

**ステップ 3** [キャプチャを開始 (Start Capture) ] をクリックします。

- キャプチャは一度に 1 つだけ実行できます。
- パケットキャプチャが実行されている場合、[パケットキャプチャ (Packet Capture) ] ページには、実行中のキャプチャのステータス (ファイル サイズや経過時間などの現在の統計情報) が表示されます。
- GUI に表示されるのは GUI で開始されたパケットキャプチャだけで、CLI で開始されたパケットキャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケットキャプチャのステータスだけが表示されます。
- パケットキャプチャファイルは 10 個の部分に分割されます。パケットキャプチャが終了する前にパケットキャプチャファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され (データが破棄されます) 、現在のパケットキャプチャデータで新しい部分が開始されます。パケットキャプチャファイルは一度に 1/10 だけ破棄されます。
- GUI で開始されたキャプチャはセッション間で維持されます。 (CLI で実行したキャプチャは、セッションが終了したときに停止します) 。

**ステップ 4** キャプチャを指定した期間実行するようにします。またはキャプチャを無期限に実行する場合、[キャプチャを停止 (Stop Capture) ] をクリックして停止します。

**ステップ 5** パケットキャプチャファイルへアクセスします。

- [パケットキャプチャファイルの管理 (Manage Packet Capture Files) ] リストでファイルをクリックして、[ファイルのダウンロード (Download File) ] をクリックします。
- アプライアンスの `captures` サブディレクトリ内のファイルにアクセスするには、FTP または SCP を使用します。

## 次のタスク

サポートでファイルを使用できるようにします。

- アプライアンスへのリモートアクセスを許可した場合、Technician が FTP または SCP を使用してパケットキャプチャファイルにアクセスできます。 [シスコのテクニカルサポート担当者のリモートアクセスの有効化 \(625 ページ\)](#) を参照してください。
- 電子メールでファイルをサポートに送信します。

# アプライアンスの電源のリモートリセット

アプライアンスのハードリセットが必要な場合は、サードパーティの Platform Management (IPMI) ツールを使用してアプライアンス シャーシをリモートからリブートできます。

## 制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。  
詳細については、[リモート電源再投入の有効化 \(510 ページ\)](#) を参照してください。
- この機能を使用可能にするには、事前に有効にする必要があります。  
詳細については、[リモート電源再投入の有効化 \(510 ページ\)](#) を参照してください。
- 次の IPMI コマンドのみがサポートされています。  
`status`、`on`、`off`、`cycle`、`reset`、`diag`、`soft`  
サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

## 始める前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

---

**ステップ 1** IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

ここで `192.0.2.1` は、リモート電源管理ポートに割り当てられた IP アドレスであり、`remoteresetuser` および `passphrase` は、この機能を有効にしたときに入力したクレデンシャルです。

**ステップ 2** アプライアンスが再起動されるまで、少なくとも 11 分間待ちます。

---





## 付録 **A**

# IP インターフェイスおよびアプライアンスへのアクセス

この章は、次の項で構成されています。

- [IP インターフェイスおよびアプライアンスへのアクセス \(631 ページ\)](#)
- [IP インターフェイス \(632 ページ\)](#)

## IP インターフェイスおよびアプライアンスへのアクセス

Cisco コンテンツ セキュリティ アプライアンスで作成する任意の IP インターフェイスには、さまざまなサービスを通してアクセスできます。

デフォルトでは、各インターフェイスに対して次のサービスが有効または無効に設定されています。

表 106: IP インターフェイスに対してデフォルトで有効になるサービス

		デフォルトで有効かどうか	
サービス	デフォルトポート	管理インターフェイス	新規作成された IP インターフェイス
FTP	21	×	×
Telnet	23	○	×
SSH	22	○	×
HTTP	80	○	×
HTTPS	443	○	×

## IP インターフェイス

IP インターフェイスには、ネットワークへの個別の接続に必要なネットワーク設定データが含まれています。1つの物理イーサネット インターフェイスに対して複数の IP インターフェイスを設定できます。IP インターフェイス経由でのスパム隔離へのアクセスも設定できます。電子メール配信および仮想ゲートウェイの場合、各 IP インターフェイスは特定の IP アドレスおよびホスト名を持つ1つの仮想ゲートウェイアドレスとして機能します。インターフェイスを独立したグループに（CLI を使用して）「参加」させることもできます。システムは、電子メールの配信時にこれらのグループを順番に使用します。仮想ゲートウェイの参加またはグループ化は、大規模な電子メール キャンペーンを複数のインターフェイス間でロード バランシングする際に役立ちます。VLAN を作成し、他のインターフェイスと同様に（CLI を使用して）設定することもできます。詳細については、お使いの E メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプの「Advanced Networking」の章を参照してください。

## IP インターフェイスの設定

[管理アプライアンス (Management Appliance) ]>[ネットワーク (Network) ]>[IP インターフェイス (IP Interfaces) ] ページ (および interface config コマンド) では、IP インターフェイスを追加、編集、または削除できます。



- (注) セキュリティ管理アプライアンス上の管理インターフェイスに関連付けられた名前またはイーサネットポートを変更することはできません。さらに、セキュリティ管理アプライアンスは後述のすべての機能をサポートしているわけではありません (たとえば、Virtual Gateway) 。

IP インターフェイスを設定する場合は、次の情報が必要です。

表 107: IP インターフェイス コンポーネント

名前	インターフェイスのニックネーム。
IP アドレス	同じサブネットに含まれる IP アドレスを、別々の物理イーサネット インターフェイスには設定できません。
ネットマスク (サブネットマスク)	ネットマスクを標準のドット付きオクテット形式 (たとえば、255.255.255.0) または 16 進形式 (たとえば、0xfffff00) で入力できます。デフォルトのネットマスクは 255.255.255.0、一般的なクラス C 値です。
ブロードキャストアドレス	AsyncOS はデフォルトのブロードキャストアドレスを IP アドレスおよびネットマスクから自動的に計算します。



名前	インターフェイスのニックネーム。
ホストネーム	インターフェイスに関連するホスト名。ホスト名は、SMTP カンパセッション中のサーバの特定に使用されます。各 IP アドレスに関連付けられた有効なホスト名を入力する必要があります。ソフトウェアは、DNS によってホスト名が一致する IP アドレスに正しく変換されたり、または逆引き DNS によって所定のホスト名が変換されることをチェックしません。
許可されるサービス	FTP、SSH、Telnet、スパム隔離、HTTP、および HTTPS はインターフェイス上で有効または無効にできます。サービスごとにポートを設定できます。スパム隔離の HTTP/HTTPS、ポート、および URL も設定できます。



(注) [セットアップ、インストール、および基本設定 \(5 ページ\)](#) の説明に従ってシステムセットアップウィザードを完了し、変更を保存している場合は、アプライアンス上に管理インターフェイスがすでに設定されているはずです。

## GUI を使用した IP インターフェイスの作成

- ステップ 1 (新しい Web インターフェイスのみ) クラウド E メールセキュリティ管理コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2 [管理アプライアンス (Management Appliance)] > [ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] を選択します。
- ステップ 3 [IP インターフェイスの追加 (Add IP Interface)] をクリックします。
- ステップ 4 インターフェイスの名前を入力します。
- ステップ 5 イーサネットポートを選択し、IP アドレスを入力します。
- ステップ 6 IP アドレスに対応するネットマスクを入力します。
- ステップ 7 インターフェイスのホスト名を入力します。
- ステップ 8 この IP インターフェイス上で有効にする各サービスの横にあるチェックボックスをオンにします。必要に応じて、対応するポートを変更します。
- ステップ 9 アプライアンス管理用にインターフェイスで HTTP から HTTPS へのリダイレクトを有効にするかどうかを選択します。
- ステップ 10 スパム隔離を使用している場合は、HTTP、HTTPS、またはその両方を選択し、それぞれにポート番号を指定できます。HTTP 要求を HTTPS にリダイレクトするかどうかも選択できます。最後に、IP インターフェイスをスパム隔離のデフォルトインターフェイスにするかどうか、ホスト名を URL として使用するかどうか、およびカスタム URL を指定するかどうかを指定できます。
- ステップ 11 変更を送信し、保存します。

## FTP 経由でのアプライアンスへのアクセス



**注意** [管理アプライアンス (Management Appliance) ]>[ネットワーク (Network) ]>[IPインターフェイス (IP Interfaces) ]ページまたは `interfaceconfig` コマンドからサービスをディセーブルにすることにより、アプライアンスへの接続方法に応じて、GUIまたはCLIから切断できます。別のプロトコル、シリアルインターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。

- ステップ 1** (新しい Web インターフェイスのみ) クラウド E メール セキュリティ 管理 コンソールで、歯車 (⚙️) アイコンをクリックして、レガシー Web インターフェイスをロードします。
- ステップ 2** [管理アプライアンス (Management Appliance) ]>[ネットワーク (Network) ]>[IPインターフェイス (IP Interfaces) ]ページ (または `interfaceconfig` コマンド) を選択して、インターフェイスに対して FTP アクセスを有効にします。
- (注) 次のステップに移る前に、変更を保存することを忘れないでください。
- ステップ 3** FTP 経由でインターフェイスにアクセスします。インターフェイスに対して正しい IP アドレスを使用していることを確認します。
- 例: `ftp 192.168.42.42`
- ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。
- 例: `ftp://192.10.10.10`
- ステップ 4** 実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照し、ファイルをコピーおよび追加 (「GET」および「PUT」) できます。次の表を参照してください。

表 108: アクセスできるディレクトリ

ディレクトリ名	説明
/avarchive /bounces /cli_logs /delivery /error_logs /ftpd_logs /gui_logs /mail_logs /rptd_logs /sntpd.logs /status /system_logs	[管理アプライアンス (Management Appliance) ] > [システム管理 (System Administration) ] > [ログサブスクリプション (Log Subscriptions) ] ページまたは、logconfig および rollovernow コマンドを使用してロギング用に、自動的に作成されます。各ログの詳しい説明については、お使いの E メールセキュリティアプライアンスのユーザガイドまたはオンラインヘルプの「Logging」の章を参照してください。  各ログ ファイル タイプの違いについては、「Logging」の章の「Log File Type Comparison」を参照してください。
/configuration	次のページおよびコマンドからのデータのエクスポート先ディレクトリ、またはインポート元 (保存) ディレクトリ。 <ul style="list-style-type: none"> <li>• Virtual Gateway マッピング (altsrghost)</li> <li>• XML 形式の設定データ (saveconfig、loadconfig)</li> <li>• [ホストアクセステーブル (HAT) (Host Access Table (HAT)) ] ページ (hostaccess)</li> <li>• [受信者アクセステーブル (RAT) (Recipient Access Table (RAT)) ] ページ (rcptaccess)</li> <li>• [SMTPルート (SMTP Routes) ] ページ (smtproutes)</li> <li>• エイリアス テーブル (aliasconfig)</li> <li>• マスカレード テーブル (masquerade)</li> <li>• メッセージ フィルタ (filters)</li> <li>• グローバル配信停止データ (unsubscribe)</li> <li>• trace コマンドのテスト メッセージ</li> </ul>
/MFM	メールフロー モニタリング データベース ディレクトリには、GUI から使用できるメールフロー モニタ機能のデータが含まれます。各サブディレクトリには、各ファイルのレコード形式を文書化した README ファイルが含まれます。  記録を残すためにこれらのファイルを異なるマシンにコピーしたり、ファイルをデータベースにロードして独自の分析アプリケーションを作成したりできます。レコード形式は、すべてのディレクトリ内にあるすべてのファイルで同じです。この形式は今後のリリースで変更される場合があります。
/periodic_reports	システムで設定されているすべてのアーカイブ済みレポートが保管されます。

**ステップ 5** ご使用の FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

## セキュアコピー (scp) アクセス

クライアントオペレーティングシステムでセキュアコピー (scp) コマンドがサポートされている場合は、表「アクセスできるディレクトリ」に示すディレクトリ間でファイルをコピーできます。たとえば、次の例ではファイル /tmp/test.txt はクライアントマシンからホスト名「mail3.example.com」のアプライアンスの設定ディレクトリにコピーされます。



(注) このコマンドでは、ユーザ (admin) のパスワードを求めるプロンプトが表示されます。この例は参考用です。オペレーティングシステムの secure copy の実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration
The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.
admin@mail3.example.com's passphrase: (type the passphrase)
test.txt          100% |*****| 1007      00:00
%
```

この例では、同じファイルがアプライアンスからクライアントマシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .
admin@mail3.example.com's passphrase: (type the passphrase)
test.txt          100% |*****| 1007      00:00
```

コンテンツセキュリティアプライアンスに対するファイルの転送および取得には、セキュアコピー (scp) を FTP に代わる方法として使用できます。



(注) operators グループおよび administrators グループのユーザのみが、アプライアンスへのアクセスにセキュアコピー (scp) を使用できます。詳細については、[AsyncOS の以前のバージョンへの復元について \(538 ページ\)](#) を参照してください。

## シリアル接続によるアクセス

シリアル接続を介してアプライアンスに接続する場合は、コンソールポートに関する次の情報を使用します。

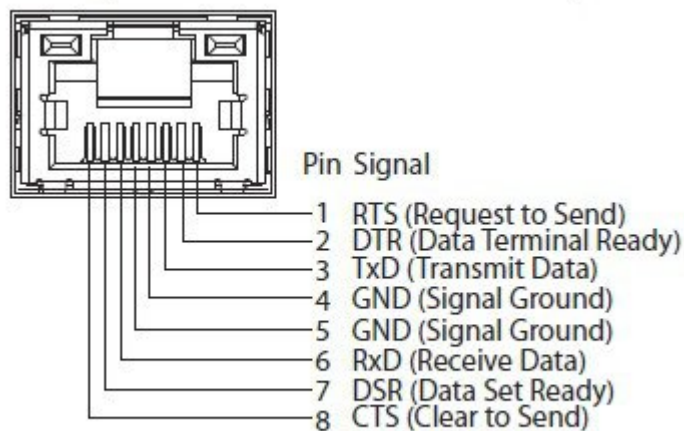
このポートの詳細については、アプライアンスのハードウェアインストールガイドを参照してください。

## 関連項目

- 資料 (655 ページ)

## 80 および 90 シリーズ ハードウェアでのシリアルポートのピン割り当ての詳細

図 21: 80 および 90 シリーズ ハードウェアでのシリアルポートのピン割り当ての詳細



## 70 シリーズ ハードウェアでのシリアルポートのピン割り当ての詳細

次の図はシリアルポートコネクタのピン番号を示しています。また、表「シリアルポートのピン割り当て」では、シリアルポートコネクタのピン割り当てとインターフェイス信号を定義しています。

図 22: シリアルポートのピン番号

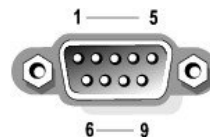


表 109: シリアルポートのピン割り当て

ピン	信号 (Signal)	I/O	定義 (Definition)
1	DCD		データ キャリア検出
2	SIN		シリアル入力
3	SOUT		シリアル出力
4	DTR		データ ターミナルレディ

ピン	信号 (Signal)	I/O	定義 (Definition)
5	GND	適用対象 外	信号用接地
6	DSR		データセット レディ
7	RTS		送信要求
8	CTS		送信可
9	RI		リング インジケータ
シ ェ ル	適用対象外	適用対象 外	シャーシアース



## 付録 **B**

# ネットワークと IP アドレスの割り当て

この付録の構成は、次のとおりです。

- [イーサネット インターフェイス \(639 ページ\)](#)
- [IP アドレスとネットマスクの選択 \(639 ページ\)](#)
- [コンテンツ セキュリティ アプライアンスを接続するための戦略 \(642 ページ\)](#)

## イーサネット インターフェイス

Cisco コンテンツ セキュリティ アプライアンスには、構成（任意選択の光ネットワーク インターフェイスがあるかどうか）に応じて、システムの背面パネルに最大4つのイーサネット インターフェイスがあります。次のラベルが付いています。

- 管理
- Data1
- Data2
- Data3
- Data4

## IP アドレスとネットマスクの選択

ネットワークを設定するとき、コンテンツ セキュリティ アプライアンスが発信パケットの送信に一意のインターフェイスを選択できる必要があります。この要件によって、イーサネット インターフェイスの IP アドレスとネットマスクの選択に関して、いくつかのことが決まります。単一のネットワークに配置できるインターフェイスは1つのみというのがルールです（ネットマスクがインターフェイスの IP アドレスに適用されることでそのように定められます）。

IP アドレスは、指定されたネットワークの物理インターフェイスを識別します。物理イーサネット インターフェイスは、パケットを受け取る IP アドレスを複数持つことができます。複数の IP アドレスを持つイーサネット インターフェイスは、パケットの送信元アドレスとしていずれか1つの IP アドレスを使用して、インターフェイスからパケットを送信できます。このプロパティは、仮想ゲートウェイテクノロジーの実装で使用されます。

ネットマスクの目的は、IP アドレスをネットワーク アドレスとホスト アドレスに分割することです。ネットワーク アドレスは、IP アドレスのネットワーク部分（ネットマスクと一致するビット）と見なすことができます。ホスト アドレスは IP アドレスの残りのビットです。4 オクテットアドレス内の有効なビット数は、クラスレス ドメイン間ルーティング（CIDR）形式で表現されることがあります。これは、スラッシュ記号、後にビット数（1～32）が続きます。

この方法では、単純にバイナリ表記で 1 を数えることでネットマスクを表現できます。したがって 255.255.255.0 は「/24」となり、255.255.240.0 は「/20」となります。

## インターフェイス設定のサンプル

ここでは、いくつかの代表的なネットワークに基づいたインターフェイスの設定例を示します。この例では、Int1 と Int2 の 2 つのインターフェイスを使用します。コンテンツ セキュリティ アプライアンスの場合、これらのインターフェイス名は、3 つのインターフェイス（Management、Data1、Data2）の中の 2 つのインターフェイスを示します。

### ネットワーク 1:

個別のインターフェイスは別のネットワーク上に存在するように示す必要があります。

インターフェイス	IPアドレス	ネットマスク	ネットアドレス
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

192.168.1.X宛てのデータ（Xは自分のアドレスを除く1～255の任意の数字、この場合は10）は Int1 に出力されます。192.168.0.X宛てのすべてのデータは Int2 に出力されます。この形式ではない他のアドレス（最も考えられるのは WAN またはインターネット上）に向かうパケットは、デフォルト ゲートウェイに送信されます。デフォルト ゲートウェイはこれらのネットワークのどちらかの上に存在する必要があります。その後、デフォルトゲートウェイがパケットを転送します。

### ネットワーク 2:

2つの異なるインターフェイスのネットワークアドレス（IPアドレスのネットワーク部分）は同じにすることができません。

イーサネットインターフェイス	IPアドレス	ネットマスク	ネットアドレス
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

これは、2つのイーサネットインターフェイスが同じネットワークアドレスを持つという、競合した状態を表しています。コンテンツ セキュリティ アプライアンスからのパケットが



192.168.1.11 に送信された場合、パケットの配信にどのイーサネット インターフェイスを使用すべきかは特定できません。2つのイーサネット インターフェイスが2つの物理ネットワークに別々に接続されている場合、パケットは誤ったネットワークに配信される可能性があり、そうするとそのパケットの送信先を見つけることはできません。コンテンツ セキュリティ アプライアンスでは、競合するネットワークを設定できません。

2つのイーサネット インターフェイスを同じ物理ネットワークに接続することはできますが、コンテンツ セキュリティ アプライアンスが一意的配信インターフェイスを選択できるように IP アドレスとネットマスクを設定する必要があります。

## IP アドレス、インターフェイス、およびルーティング

GUI または CLI で、インターフェイスを選択可能なコマンドや関数を実行する際にインターフェイスを選択した場合（たとえば、AsyncOS のアップグレードや DNS の設定など）、ルーティング（デフォルト ゲートウェイ）が選択した内容よりも優先されます。

たとえば、次のように3つのネットワーク インターフェイスがそれぞれ別のネットワーク セグメントに設定されたコンテンツ セキュリティ アプライアンスがあるとします（すべて /24 と仮定）。

イーサネット	IP
管理	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

デフォルト ゲートウェイは 192.19.0.1 です。

ここで、AsyncOS のアップグレード（またはインターフェイスを選択できる他のコマンドや関数）を実行し、Data1 上の IP（192.19.1.100）を選択した場合、すべての TCP トラフィックが Data1 イーサネット インターフェイス経由になると予想されることと思います。しかし、実際には、デフォルトゲートウェイとして設定されているインターフェイス（ここでは Management）からトラフィックが送出されます。ただし、トラフィックの送信元アドレスには Data1 の IP が設定されています。

## 要約

コンテンツ セキュリティ アプライアンスは、配信可能なパケットが経由する一意のインターフェイスを常に識別できなければなりません。この決定を行うために、コンテンツ セキュリティ アプライアンスは、パケットの宛先 IP アドレスと、そのイーサネット インターフェイスのネットワークおよび IP アドレス設定を組み合わせ使用します。次の表に、ここまで説明してきた例をまとめます。

	同じネットワーク	異なるネットワーク
同じ物理インターフェイス	許可	許可
異なる物理インターフェイス	不可	許可

## コンテンツセキュリティアプライアンスを接続するための戦略

アプライアンスを接続するには、次の点に留意してください。

- 通常、管理トラフィック（CLI、Web インターフェイス、ログ配信）は、電子メールトラフィックよりもはるかに少量です。
- 2つのイーサネットインターフェイスが同じネットワークスイッチに接続されているが最終的にダウンストリームの別のホスト上の単一インターフェイスと通信するだけの場合、あるいはすべてのデータがすべてのポートにエコーされるネットワークハブにそれらが接続されている場合、2つのインターフェイスを使用しても得られる利点はありません。
- 1000Base-T で動作しているインターフェイスでの SMTP カンパセーションは、100Base-T で動作している同じインターフェイスでのカンパセーションよりも少し高速ですが、速くなるのは理想的な条件下でのみです。
- 配信ネットワークのその他の部分にボトルネックがある場合、ネットワークへの接続を最適化しても意味がありません。ボトルネックは、インターネットへの接続や、接続プロバイダーによるアップストリームへの接続で最も頻繁に発生します。

接続に使用するインターフェイスの数とそれらへのアドレス指定の方法は、基礎となるネットワークの複雑性によって決める必要があります。ご使用のネットワークトポロジやデータのボリュームから判断して不要であれば、複数のインターフェイスに接続する必要はありません。また、最初は単純な接続にしておき、ゲートウェイに慣れてきたら、ボリュームやネットワークトポロジでの必要に応じて接続を増やすこともできます。



## 付録 C

# ファイアウォール情報

この章は、次の項で構成されています。

- [ファイアウォール情報 \(643 ページ\)](#)

## ファイアウォール情報

次の表は、Cisco コンテンツセキュリティアプライアンスを正常に動作させるために開けなければならないことがあるポートのリストです（デフォルト値を示す）。

表 110: ファイアウォールポート

デフォルトポート	プロトコル	内外 (In/Out)	ホストネーム	目的
20/21	TCP	In または Out	AsyncOS IP、FTP サーバ	ログファイルのアグリゲーション用 FTP。 データポート TCP 1024 以上はすべて開いている必要があります。 詳細については、ナレッジベースの FTP ポート情報を検索してください。 <a href="#">ナレッジベースの記事 (657 ページ)</a> を参照してください。
22	SSH	発信 (Out)	AsyncOS IP	中央集中型コンフィギュレーションマネージャのコンフィギュレーションの配信。 バックアップにも使用されます。

22	TCP	入力	AsyncOS IP	CLI への SSH アクセス、ログ ファイルのアグリゲーション。
22	[TCP]	発信 (Out)	SCP サーバ	ログ サーバへの SCP 配信。
23	Telnet	入力	AsyncOS IP	CLI への Telnet アクセス。
23	Telnet	発信	Telnet サーバ	Telnet アップグレード
25	[TCP]	発信 (Out)	任意 (Any)	電子メール送信用 SMTP。
25	TCP	入力	AsyncOS IP	バウンスされた電子メールを受信する SMTP または外部のファイアウォールから電子メールをインジェクトする場合。
53	UDP/TCP	発信 (Out)	DNS サーバ	インターネットルートサーバまたはファイアウォール外部の DNS サーバを使用するように設定されている場合の DNS。また、SenderBase クエリの場合。
80	HTTP	入力	AsyncOS IP	システム モニタリングのための GUI への HTTP アクセス。
80	HTTP	発信 (Out)	downloads.ironport.com	AsyncOS アップグレードおよび。
80	HTTP	発信 (Out)	upgrades.ironport.com	AsyncOS アップグレード。
801	HTTP	入力および出力	AsyncOS IP	trailblazerconfig CLI コマンドを使用した、GUI への HTTP アクセス。
82	HTTP	入力	AsyncOS IP	スパム隔離の表示に使用されます。
83	HTTPS	入力	AsyncOS IP	スパム隔離の表示に使用されます。
110	[TCP]	発信 (Out)	POP サーバ	スパム隔離のためのエンドユーザの POP 認証。

123	UDP	入力および出力	NTP サーバ	タイム サーバがファイアウォールの外側にある場合の NTP。
143	[TCP]	発信 (Out)	IMAP サーバ	スパム隔離のためのエンドユーザの IMAP 認証。
161	UDP	入力	AsyncOS IP	SNMP クエリ。
162	UDP	発信 (Out)	管理ステーション	SNMP トラップ。
389 または 3268	LDAP	発信 (Out)	LDAP サーバ	LDAP ディレクトリ サーバがファイアウォールの外側にある場合の LDAP。Cisco スパム隔離のための LDAP 認証。
636 または 3269	LDAPS	発信 (Out)	LDAPS	LDAPS — ActiveDirectory のグローバルカタログサーバ (SSL 使用)
443	TCP	入力	AsyncOS IP	システム モニタリングのための GUI への Secure HTTP (https) アクセス。
443	[TCP]	発信 (Out)	update-static.ironport.com	アップデート サーバの最新のファイルを確認します。
443	[TCP]	発信 (Out)	update-manifests.ironport.com	アップデート サーバから最新のファイルのリストを取得します (物理ハードウェア アプライアンスの場合)。
443	[TCP]	発信 (Out)	update-manifests.sco.cisco.com	アップデート サーバから最新のファイルのリストを取得します (仮想アプライアンスの場合)。
443	[TCP]	発信 (Out)	phonehome.senderbase.org	アウトブレイク フィルタの受信/送信。

443	[TCP]	発信 (Out)	<p>Web Security Appliances の [セキュリティサービス (Security Services) ] &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] ページの [詳細設定 (Advanced) ] セクション &gt; [ファイル分析の詳細設定 (Advanced Settings for File Analysis) ] で設定されているファイル分析サーバ URL。</p> <p>Email Security Appliance の [セキュリティサービス (Security Services) ] &gt; [ファイルレピュテーションと分析 (File Reputation and Analysis) ] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis) ] セクションで設定されているファイル分析サーバ URL。</p>	<p>ファイル分析サーバに詳細なファイル分析結果を表示します。</p> <ul style="list-style-type: none"> <li>• Web セキュリティレポート : (クラウドファイル分析) 管理アプライアンスがファイル分析サーバに到達できることを確認する (219 ページ)</li> </ul>
443	HTTPS	入力および出力	api.sse.cisco.com	Cisco Threat Response ポータルにアプライアンスを登録するために使用します。
443	HTTPS	入力および出力	api.eu.sse.itd.cisco.com	Cisco Threat Response ポータルにアプライアンスを登録するために使用します。
443	HTTPS	入力および出力	est.sco.cisco.com	証明書をダウンロードして、Cisco Threat Response ポータルに登録する際にアプライアンスが検証済みのサイトにアクセスしているかどうかを検証するために使用します。
443	HTTPS	入力および出力	AsyncOS IP	trailblazerconfig CLI コマンドを使用した、GUI への HTTPS アクセス。
514	UDP/TCP	発信 (Out)	Syslog サーバ	Syslog ロギング。

1024 以降	—	—	—	ポート 21 (FTP) に関する上記の情報を参照してください。
7025	TCP	In および Out	AsyncOS IP	この機能を集中化する場合、Eメールセキュリティアプライアンスとセキュリティ管理アプライアンス間でポリシー、ウイルス、アウトブレイク隔離データを渡します。
32137	[TCP]			
6080	HTTP	入力または出力		HTTP サーバの API ポートへのアクセス
6443	HTTPS	入力または出力		HTTPS サーバの API ポートへのアクセス







## 付録 **D**

# Web セキュリティ管理の例

---

この章は、次の項で構成されています。

- [Web セキュリティ管理の例 \(649 ページ\)](#)

## Web セキュリティ管理の例

この付録では、Cisco コンテンツ セキュリティ管理アプライアンスの機能を導入するいくつかの一般的な方法について説明します。内容は次のとおりです。

- [例 1 : ユーザの調査 \(649 ページ\)](#)
- [例 2 : URL のトラッキング \(651 ページ\)](#)
- [例 3 : アクセス数の多い URL カテゴリの調査 \(652 ページ\)](#)

## Web セキュリティ アプライアンスの例

このセクションでは、セキュリティ管理アプライアンスと Web セキュリティ アプライアンスを使用する例について説明します。



- (注) これらのシナリオはすべて、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンスで Web レポートおよび Web トラッキングが有効であることを前提としています。Web トラッキングおよび Web レポートをイネーブルにする方法については、[中央集中型 Web レポートおよびトラッキングの使用 \(191 ページ\)](#) を参照してください。

### 例 1 : ユーザの調査

次に、システム管理者が会社で特定のユーザを調査する例を示します。

このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。それを調査するには、システム管理者が Web アクティビティの詳細をトラッキングする必要があります。

Web アクティビティをトラッキングすると、従業員の参照履歴に関する情報が記載された Web レポートが作成されます。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web)] > [レポート (Reporting)] > [ユーザ (Users)] を選択します。

**ステップ 2** [ユーザ (Users)] テーブルで、調査する [ユーザ ID (User ID)] または [クライアント IP アドレス (Client IP address)] をクリックします。

ユーザ ID またはクライアント IP アドレスがわからない場合は、ユーザ ID またはクライアント IP アドレスをわかる範囲でテキストフィールドに入力し、[ユーザ ID またはクライアント IP アドレスの検索 (Find User ID or Client IP address)] をクリックします。IP アドレスが正確に一致していても結果は返されます。[ユーザ (Users)] テーブルに、指定したユーザ ID およびクライアント IP アドレスが入力されます。この例では、クライアント IP アドレス 10.251.60.24 の情報について検索しています。

**ステップ 3** IP アドレス [10.251.60.24] をクリックします。

10.251.60.24 の [ユーザの詳細 (User Details)] ページが表示されます。

ユーザの詳細ページから総トランザクション別の URL カテゴリ、総トランザクション別のトレンド、一致する URL カテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

これらのカテゴリによって、10.251.60.24 のユーザがブロックされている URL (ページの [ドメイン (Domains)] セクションに含まれる [ブロックされたトランザクション (Transactions Blocked)] 列に表示) にアクセスしようとしていたことなどがわかります。

**ステップ 4** [一致したドメイン (Domains Matched)] テーブルの下の [エクスポート (Export)] をクリックし、ユーザがアクセスしようとしていたドメインおよび URL のリストを表示します。

ここから Web トラッキング機能を使用して、この特定のユーザの Web 使用状況をトラッキングし、表示できます。

(注) Web レポートでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web トラッキング (Web Tracking)] ページの [プロキシサービス (Proxy Services)] タブを使用します。

**ステップ 5** [ウェブ (Web)] > [レポート (Reporting)] > [Web トラッキング (Web Tracking)] を選択します。

**ステップ 6** [プロキシサービス (Proxy Services)] タブをクリックします。

**ステップ 7** [ユーザ/クライアント IP アドレス (User/Client IP Address)] テキストフィールドにユーザ名または IP アドレスを入力します。

この例では、ユーザ 10.251.60.24 の Web トラッキング情報を検索します。

検索結果が表示されます。

このページから、IP アドレス 10.251.60.24 に割り当てられているコンピュータのユーザがアクセスしたトランザクションおよび URL のすべてのリストを確認できます。

## 関連項目

次の表にこの例で説明する各トピックをリストします。各項目の詳細については、リンクをクリックしてください。

表 111: ユーザの調査の関連項目

機能名	機能情報
[ユーザ (User) ] ページ	[ユーザ (Users) ] レポート (Web) (204 ページ)
[ユーザの詳細 (User Details) ] ページ	[ユーザの詳細 (User Details) ] (Web レポートイング) (206 ページ)
レポート データのエクスポート	レポート データおよびトラッキング データのエクスポート (33 ページ)
[Web トラッキング (Web Tracking) ] ページの [プロキシサービス (Proxy Services) ] タブ	Web プロキシ サービスによって処理されたトランザクションの検索 (279 ページ)

## 例 2 : URL のトラッキング

このシナリオでは、セールスマネージャが、会社のサイトへのアクセスで、先週の上位5位を知りたい場合を考えます。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

- 
- ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web) ] > [レポート (Reporting) ] > [Web サイト (Web Sites) ] を選択します。
- ステップ 2** [時間範囲 (Time Range) ] ドロップダウン リストから [週 (Week) ] を選択します。
- ステップ 3** [ドメイン (Domains) ] セクションをスクロール ダウンすると、アクセスされているドメインまたは Web サイトが表示されます。

アクセス上位 25 位までの Web サイトは、[一致したドメイン (Domains Matched) ] テーブルに表示されます。同じテーブルで [ドメイン (Domain) ] または [IP] 列のリンクをクリックすると、特定のアドレスまたはユーザが参照した実際の Web サイトを確認できます。

---

## 関連項目

次の表にこの例で説明する各トピックをリストします。各項目の詳細については、リンクをクリックしてください。

## 例 3 : アクセス数の多い URL カテゴリの調査

表 112: URL のトラッキングの関連項目

機能名	機能情報
[Web サイト (Web Sites) ] ページ	[Web サイト (Web Sites) ] レポート (208 ページ)

## 例 3 : アクセス数の多い URL カテゴリの調査

このシナリオでは、従業員が最近 30 日間にアクセスした上位 3 位までの URL を、人事部長が知りたい場合を考えます。また、ネットワーク管理者が、帯域幅の使用上をモニタしたり、ネットワークで最も帯域幅を使用している URL を特定したりするためにこの情報を取得するとします。

次の例は、複数の観点を持つ複数の人のためにデータを収集するが、生成するレポートは1つだけで済む方法を示します。

**ステップ 1** セキュリティ管理アプライアンスで、[ウェブ (Web) ] > [レポート (Reporting) ] > [URL カテゴリ (URL Categories) ] を選択します。

この例の [URL カテゴリ (URL Categories) ] ページによると、総トランザクション別の上位 10 の URL カテゴリ グラフから、Instant Messaging、Hate Speech、Tattoo サイトなどの他に、282 k の未分類の URL にアクセスしていることがわかります。

ここで、[エクスポート (Export) ] リンクをクリックして raw データを Excel スプレッドシートにエクスポートすると、このファイルを人事部長に送信できます。ネットワーク マネージャに URL ごとの帯域幅の使用量を知らせる必要があります。

**ステップ 2** 新しい ILLO が必要です - スキップ [使用帯域幅 (Bandwidth Used) ] 列を表示するには、[一致した URL カテゴリ (URL Categories Matched) ] テーブルまでスクロールします。

[一致した URL カテゴリ (URL Categories Matched) ] テーブルで、すべての URL カテゴリの帯域幅の使用量を確認することができます。もう一度 [エクスポート (Export) ] リンクをクリックして、このファイルをネットワーク管理者に送信します。さらに細かく調べるには、[インスタントメッセージ (Instant Messaging) ] リンクをクリックすると、どのユーザが帯域幅を大量に使用しているかが特定されます。次のページが表示されます。

このページから、ネットワーク管理者が Instant Messaging サイトの上位 10 ユーザを知ることができます。

このページから、最近 30 日間で 10.128.4.64 のユーザが Instant Messaging サイトに 19 時間 57 分アクセスしており、この期間の帯域幅の使用量が 10.1 MB であることがわかります。

## 関連項目

次の表にこの例で説明する各トピックをリストします。各項目の詳細については、リンクをクリックしてください。

表 113: アクセスの多い URL カテゴリの調査の関連項目

機能名	機能情報
[URLカテゴリ (URL Categories) ] ページ	[URLカテゴリ (URL Categories) ] レポート (209 ページ)
レポート データのエクスポート	レポート データおよびトラッキング データのエクスポート (33 ページ)





## 付録 E

# 関連リソース

この章は、次の項で構成されています。

- [Cisco Notification Service](#) (655 ページ)
- [資料](#) (655 ページ)
- [サードパーティ コントリビュータ](#) (656 ページ)
- [トレーニング](#) (657 ページ)
- [ナレッジベースの記事](#) (657 ページ)
- [シスコ サポート コミュニティ](#) (657 ページ)
- [カスタマー サポート](#) (657 ページ)
- [シスコ アカウントの登録](#) (658 ページ)
- [マニュアルに関するフィードバック](#) (658 ページ)

## Cisco Notification Service

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

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

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

Cisco.com アカウントが必要です。ない場合は、[シスコ アカウントの登録](#) (658 ページ) を参照してください。

## 資料

この製品および関連製品のマニュアルは、次の Web サイトで入手可能です。

<b>Cisco Content Security 製品のマニュアル :</b>	入手場所
セキュリティ管理アプライアンス	<a href="http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html</a> ハードウェアおよび仮想アプライアンスの情報 : <a href="http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html">http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html</a> MIB : <a href="#">SNMP を使用したシステムの状態のモニタリング (511 ページ)</a> を参照してください。
Web セキュリティアプライアンス	<a href="http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html</a>
Eメールセキュリティアプライアンス	<a href="http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html</a>
コンテンツセキュリティ製品用コマンドラインリファレンスガイド	<a href="http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html">http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html</a>
Cisco 電子メール暗号化	<a href="http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html</a>

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

## サードパーティコントリビュータ

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

サードパーティのライセンスに関する情報は、<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html> および [https://support.ironport.com/3rdparty/AsyncOS\\_User\\_Guide-1-1.html](https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html) にあるライセンシングドキュメントで利用できます。

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



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

## トレーニング

Cisco では、技術者、パートナー、学生など、それぞれのニーズに合わせた、さまざまなトレーニングプログラムおよびトレーニングコースを用意しています。日本のトレーニングと認定試験の情報については、以下の Web サイトをご覧ください。

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

## ナレッジ ベースの記事

### 手順

	コマンドまたはアクション	目的
ステップ 1	メイン製品ページにアクセスします ( <a href="http://www.cisco.com/c/en/us/products/content-security-management/index.html">http://www.cisco.com/c/en/us/products/content-security-management/index.html</a> )	
ステップ 2	名前に <b>TechNotes</b> が付くリンクを探します。	

## シスコ サポート コミュニティ

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

シスコ サポート コミュニティへのアクセス先：

- 電子メール セキュリティと関連管理：  
<https://supportforums.cisco.com/community/5756/email-security>
- Web セキュリティと関連管理：  
<https://supportforums.cisco.com/community/5786/web-security>

## カスタマー サポート

サポートを受けるには、次の方法を使用してください。

Cisco TAC : [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)

従来の IronPort のサポート サイト : <http://www.cisco.com/web/services/acquisitions/ironport.html>

リセラーまたは他のサプライヤからサポートを購入した場合、製品に関するサポートについては、直接そのリセラーもしくはサプライヤにお問い合わせください。

[アプライアンスからのサポートケースのオープンおよび更新 \(624 ページ\)](#) も参照してください。

仮想アプライアンスについては、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。

## シスコ アカウントの登録

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

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

### 関連項目

- [Cisco Notification Service \(655 ページ\)](#)
- [ナレッジ ベースの記事 \(657 ページ\)](#)

## マニュアルに関するフィードバック

テクニカル マニュアル チームは、製品マニュアルの改善に努めています。コメントや提案がございましたら、ぜひ以下の電子メールまでお知らせください。

[contentsecuritydocs@cisco.com](mailto:contentsecuritydocs@cisco.com)

メッセージの件名行に、このマニュアルのタイトルとタイトルページに記載されている発行日をご記入ください。



## 付録 F

# エンドユーザライセンス契約書

この章は、次の項で構成されています。

- [Cisco Systems エンドユーザライセンス契約書 \(659 ページ\)](#)
- [Cisco コンテンツセキュリティソフトウェア用エンドユーザライセンス契約補則 \(666 ページ\)](#)

## Cisco Systems エンドユーザライセンス契約書

**重要：**本エンドユーザライセンス契約書をよくお読みください。お客様がシスコのソフトウェアまたは機器を認定販売元から購入したかどうか、また、お客様ご自身またはお客様が代表する法人（総称して「お客様」）がこのシスコ エンドユーザライセンス契約におけるエンドユーザとして登録済みかどうかを確認することは、非常に重要です。エンドユーザとして登録されていないお客様は本ソフトウェアを使用するライセンスを有しておらず、このエンドユーザライセンス契約の限定保証は適用されません。お客様が認定販売元から購入されたことを前提として、シスコのソフトウェア、またはシスコが提供するソフトウェアをダウンロード、インストールまたは使用することにより、お客様はこの契約に同意したものと見なされます。

Cisco Systems, Inc. Cisco Systems, Inc.、または同社に代わり本ソフトウェアのライセンスを許諾する同社の関連会社（以下、「シスコ」）は、お客様が本ソフトウェアを認定販売元から購入し、かつ本エンドユーザライセンス契約書に含まれるすべての条件、および本製品に添付され、お客様の発注時に入手可能になる補遺ライセンス契約書に記載の、ライセンスに関する一切の追加制限条件（以下総称して「本契約」）に同意する場合に限り、お客様に対し本ソフトウェアのライセンスを許諾します。本エンドユーザライセンス契約書内の各規定と補遺ライセンス契約書内の各規定が相反する場合、補遺ライセンス契約書内の各規定が優先します。本ソフトウェアをダウンロード、インストールまたは使用することにより、お客様は本ソフトウェアをご自身が認定販売元から購入したことを表明したこととなり、お客様に本契約の拘束力が及びます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、(A) お客様は、本件ソフトウェアをダウンロード、インストール、または使用できません、また、(B) お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられません。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および代金払い戻しの有効期限は、認定販売元から本ソフトウェアを購入後 30 日間であり、お客様が最初の登録済み

エンドユーザ購入者である場合にのみ適用されます。本エンドユーザライセンス契約において、「認定販売元」とは、(A) シスコ、(B) 対象地域内でエンドユーザにシスコの機器、ソフトウェアおよびサービスを配布および/もしくは販売することについてシスコより認定を受けたディストリビュータもしくはシステムインテグレータ、または (C) シスコの機器、ソフトウェアおよびサービスをお客様の地域内でエンドユーザに配布および/もしくは販売することについて、ディストリビュータとシスコとの契約の条件に従い、ディストリビュータもしくはシステムインテグレータにより認定された再販業者を意味します。

本契約の以下の条件は、本ソフトウェア（後に定義）のお客様による使用に適用されます。ただし、(a) 本ソフトウェアのお客様による使用に適用される、お客様とシスコとの間の別段の署名済み契約が存在する場合、または (b) 本ソフトウェアに、導入もしくはダウンロードの手続きの一部として、本ソフトウェアのお客様による使用に適用される別段の「クリック同意」ライセンス契約もしくは第三者ライセンス契約が含まれている場合は、この限りではありません。上記各契約書内の各規定が矛盾する場合、その優先順位は、以下のとおりです。(1) 署名済みの契約、(2) クリック同意契約または第三者のライセンス契約、(3) 本契約。本契約において、「本ソフトウェア」とは、認定販売元からお客様に提供されるシスコ機器に組み込まれたファームウェアおよびコンピュータ プログラムを含むコンピュータ プログラム、ならびに一切のアップグレード、更新、バグ修正またはこれらの修正バージョン（総称して「アップグレード」）であって、*Cisco Software Transfer and Re-licensing Policy*（随時シスコによりなされる修正を含む）に基づいて再許諾されたもの、またはこれらのいずれかのバックアップコピーを意味します。

**本件ライセンス**本契約の各契約条件に従うことを条件として、シスコはお客様に対し、お客様が必要なライセンス料を認定販売元に支払った本ソフトウェアおよび本文書を社内業務目的で使用するための、非排他的かつ譲渡不能なライセンスを付与します。「本文書」とは、本ソフトウェアに関する情報を文書化したもの（当該情報がユーザマニュアル、技術マニュアル、研修資料、仕様書その他のいずれに含まれているか否かは問わない）であって、認定販売元が何らかの形式（CD-ROMやオンラインを含む）により本ソフトウェアとともに提供するものを意味します。本ソフトウェアを使用するには、登録番号または製品認証キーを入力し、シスコの Web サイトにてお手持ちの本ソフトウェアをオンライン登録した上で、必要なライセンスキーまたはライセンス ファイルを入手する必要があります。

お客様が本ソフトウェアを使用するためのライセンスは、単一のハードウェアシャーシもしくはカード、または該当する補遺ライセンス契約書、もしくは認定販売元が同意済みで、お客様が必要なライセンス料を認定販売元に支払済みの該当する発注書（以下、「本発注書」）に記載されているその他の制限に限定され、お客様はこの制限を超えて本ソフトウェアを使用してはなりません。

本文書または該当する補遺ライセンス契約書に別途明記されていない限り、お客様は、以下のいずれかのみを目的として本ソフトウェアを使用する必要があります。お客様が所有または賃借しており、お客様の社内業務目的に使用されるシスコ機器に本ソフトウェアを組み込んで使用すること。当該シスコ機器上で本ソフトウェアを実行すること。（対応する本文書が、シスコ以外の機器に本ソフトウェアをインストールすることを許可している場合に）当該シスコ機器と通信すること。お客様には上記以外のいかなるライセンス（黙示のライセンス、禁反言の法理が適用されるライセンス、またはその他のライセンス）も付与されません。

シスコがライセンス料を徴収しない評価版またはベータ版については、上記のライセンス料の支払い要件は適用されません。

一般的な各種制限。本契約は、ソフトウェアおよび資料の使用許諾であり、所有権を譲渡するものではありません。すべてのソフトウェアおよび資料の所有権はシスコが保有しています。お客様は、本件ソフトウェアおよび本文書に、シスコまたはそのサプライヤもしくはライセンサの営業秘密が含まれていることを認識しているものとします。この営業秘密には、各プログラムの固有の内部設計および構造ならびに関連インターフェイス情報が含まれますが、これらのみには限定されません。本契約に明示的に別段の規定がない限り、お客様は、お客様が認定販売元から購入したシスコ機器の使用に関連する場合にのみ本ソフトウェアを使用するものとし、以下のいずれについてもこれを行う権利を有しておらず、またこれを行わないことについて特に同意するものとします。

(i) 他の個人もしくは法人に、ライセンス権を移転もしくは譲渡するか、本ライセンスのサブライセンスを付与すること（その時点で有効な、シスコのライセンスの再許諾および移転に関するポリシーに従って行う場合は除きます）、または、お客様が認定販売元から購入したものではないシスコ機器もしくは中古のシスコ機器上で本ソフトウェアを使用すること。なお、お客様は、計画された移転、譲渡、サブライセンスの付与または使用はいずれも無効となることを了解するものとします。

(ii) 以下のいずれかを行うこと。(a) 本件ソフトウェアのエラーを修正するか、本件ソフトウェアを変更または改変すること、(b) 本件ソフトウェアをもとに派生物を作成するか、第三者による当該行為を許可すること。

(iii) 本ソフトウェアを対象とするリバースエンジニアリング、逆コンパイル、復号化、逆アセンブルを行うか、その他の方法で本ソフトウェアを人間の可読形式に変換すること。なお、本制限事項にかかわらず、適用法に基づいて明示的に許可されている場合、または適用されるオープンソースライセンスに基づいて当該特定の行為を許容すべきことがシスコに義務づけられている場合は除きます。

(iv) 本ソフトウェアで実行したベンチマークテストの結果を公表すること。

(v) シスコの書面による許可なく、サービスビューロ、タイムシェアリング、またはその他の方法により、第三者へのサービス提供を目的として本ソフトウェアを使用、または使用を許可すること。

(vi) シスコの書面による事前の同意なしに、本ソフトウェアおよび本文書に含まれる企業秘密を第三者に対して開示、提供、またはその他の何らかの方法により公開すること。お客様は、かかる営業秘密を保護するため、相当のセキュリティ対策を講じる必要があります。

シスコは、準拠法により求められている範囲内で、お客様からの書面による依頼に応じて、本ソフトウェアと独自に開発された他のプログラムとの互換性を実現するために必要なインターフェイス情報を、シスコが妥当とみなす料金が支払われた場合にお客様に提供するものとします。お客様は、上記情報について厳格な秘密保持義務を遵守すると共に、その提供条件としてシスコが提示した準拠規定に従って上記情報を使用する必要があります。

**本件ソフトウェア、本件アップグレード版、および追加コピー版。NOT WITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS**

THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

所有権表示。お客様は、いかなる形式であれ、本ソフトウェアのすべての複製物について、あらゆる著作権、財産権およびその他の表示を、それらの著作権およびその他の所有権の表示が本ソフトウェアに含まれているのと同じ形式かつ方法で保持し、複製することに同意します。本契約に基づき明示的に許可される場合でなければ、お客様は、シスコから書面による事前の許可を得ることなく本件ソフトウェアのコピー版または複製物を作成してはなりません。

契約の期間および終了。本契約および本契約において供与されるライセンスは、終了時まで有効に存続します。お客様は、本件ソフトウェアおよび本件文書のすべてのコピーを破棄することにより、随時、本契約および本件ライセンスを終了させることができます。お客様が本契約のいずれかの規定に従わなかった場合、本契約に基づくお客様の権利は、シスコからの通知なしにただちに終了します。お客様は、上記終了時に、保有または管理している本件ソフトウェアおよび本件文書のすべてのコピーを破棄する必要があります。お客様のあらゆる守秘義務、「一般的な制限」と題する条項に基づいてお客様に課されたあらゆる制約および制限、あらゆる責任制限、および保証の否認と制限はすべて、本契約終了後も存続するものとします。また「米国政府がエンドユーザ購入者の場合」および「限定保証表明およびエンドユーザライセンス契約書に適用される一般規定」と題された各条項の各規定の効力は、本契約の終了後も存続します。

お客様の記録の検査。お客様は、シスコとその独立会計士に対して、お客様の通常の営業時間中にお客様の帳簿、記録、財務諸表を査察し、本契約の条項に従っていることを確認する権利を認めるものとします。上記監査の結果、本契約に反する行為が発覚した場合、お客様は、相当のライセンス料に上記監査の実施に伴う相当の費用を加えた額を、速やかにシスコへ支払う必要があります。

輸出、再輸出、移転、および使用に関する規制本契約に基づいてシスコによって供給されるソフトウェア、本文書、および技術、またはそれらの直接的な製品（「本製品および技術」）は、アメリカ合衆国（「米国」）の法令およびその他関連国の法令に基づく輸出規制の対象となっています。お客様は、シスコの本件ソフトウェアと付帯技術の輸出、再輸出、移転、および使用に適用される各種法規に従う必要があると共に、必要となる米国および現地の各種許可、認可、または許諾をすべて取得するものとします。シスコとお客様の各々は、上記許認可または許諾の取得に関連して相手方当事者から相当の根拠に基づき請求を受けたその他の情報、裏付け文書、および各種支援を提供することに同意しているものとします。コンプライアンス、輸出、再輸出、移転、および使用についての法律に関する情報は、以下の URL に掲載されています。

<https://www.cisco.com/c/en/us/about/legal/global-export-trade/general-export/contract-compliance.html>.

米国政府機関がエンドユーザ購入者である場合。本ソフトウェアおよび資料は、連邦調達規則（FAR）（以下「FAR」）（48 C.F.R.）2.101 で定義される「商用品目」に分類されます。これは、「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」で構成されます（当該用語は FAR 12.212 で使用されています）。FAR 12.212 および DoD FAR 補則 227.7202-1 から 227.7202-4 で定められているとおり、また、他の FAR 条項、または本契約の組み込み先である契約書内のこれと矛盾する他の契約条項にかかわらず、お客様は、連邦政府機関エンドユーザに対して、本ソフトウェアおよび本文書とともに本契約に定める権利のみを提供することができ、または、本契約が直接契約である場合は、連邦政府機関エンドユー

ずは、本ソフトウェアおよび本文書とともに本契約に定める権利のみを取得します。ソフトウェアと資料のいずれか、または両方を使用することにより、政府機関は、本ソフトウェアと資料が「商用コンピュータソフトウェア」および「商用コンピュータソフトウェア関連資料」であることに同意し、この契約書に規定されている権利および制限に同意したことになります。

指定コンポーネントおよび追加条件。The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on <https://www.cisco.com/>) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. お客様は、かかる指定コンポーネントについて該当する追加条件に同意するものとします。

### 限定保証

本契約に規定の各種制限および条件を前提として、シスコは、お客様への出荷日（シスコ以外の認定販売元による再販の場合、シスコの初回出荷より90日以内の日）を始期として、(a) 90日間、または (b) 本ソフトウェアを組み込んでいる製品（以下、「本製品」）に添付される保証カード（存在する場合）に明記されている、本ソフトウェアに固有の保証期間（設定されている場合）、のいずれか長い方の期間内で、(a) 通常の使用において、本ソフトウェアの提供媒体に材質上および製造上の欠陥がないこと、ならびに (b) 本ソフトウェアが本文書に実質的に適合していること、を保証します。シスコによる本件製品の出荷日は、本件製品の出荷に用いられる梱包材に記載されています。上記を除き、本ソフトウェアは「現状のまま」で提供されます。この限定保証は、最初の登録済みエンドユーザたるお客様が認定販売元から購入した本ソフトウェアに対してのみ適用されます。この限定保証のもとでは、お客様の唯一の救済、かつシスコおよびそのサプライヤの全責任は、(i) 欠陥のある媒体の交換、および/または (ii) シスコの選択により、本ソフトウェアの修理、交換、もしくは代金の返金に限定されます。いずれの場合も、この限定保証に反するようなエラーまたは欠陥が、保証期間内に、お客様に本ソフトウェアを提供した認定販売元に報告されることを条件とします。シスコ、またはお客様に本ソフトウェアを提供した認定販売元は、救済の条件として、自らの判断で、本ソフトウェアおよび/または本文書の返却を請求できます。シスコはいかなる場合でも以下の2点について保証しません。(i) 本件ソフトウェアにエラーが生じないこと、(ii) お客様が、問題または障害なく本件ソフトウェアを使用できること。また、ネットワークへの侵入やネットワークの攻撃を目的とする新技術が日々開発されているため、シスコは、本件ソフトウェアまたは本件ソフトウェアが使用される各種機器、システムもしくはネットワークが、侵入または攻撃に耐えられることについても保証しません。

制約事項。この保証は、本件ソフトウェア、本件製品、または本件ソフトウェアの使用先として許可されているその他の機器が以下のいずれかに該当するもの場合には適用されません。

(a) シスコまたはシスコ認定代理人以外によって改変されたもの、(b) シスコが提示した指示に従ってインストール、運用、メンテナンスされていないもの、(c) 異常な物理的もしくは電氣的負荷、異常な環境条件、誤使用、過失、事故による影響を受けたもの、(d) ベータ版、評価版、テスト版、実演版としてその使用が許諾されているもの。本ソフトウェアの保証は、以下のいずれかに該当するものには適用されません。(e) 一時的に使用される本ソフトウェアの各種モジュール、(f) シスコのソフトウェアセンターに掲載されていないあらゆる本ソフトウェア、(g) シスコがシスコのソフトウェアセンターにて「現状のまま」で明示的に提供しているあらゆる本ソフトウェア、(h) 認定販売元がライセンス料を受領していない

あらゆる本ソフトウェア、および (i) 認定販売元以外の第三者から供給された本ソフトウェア。

### 保証の放棄

**EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE.** 州または司法管轄区域によっては、黙示保証の有効期間を限定することが許可されていないため、お客様に上記の制限が適用されない場合があります。この保証は、お客様に特定の法的権利を付与するものですが、お客様は、法域によってはその他の権利を有する場合があります。この放棄および除外は、上記の明示保証がその本質的な目的を達成できない場合にも適用されるものとします。

責任の否認-責任の制限。本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カナダ、日本またはカリブ海沿岸諸国の場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為（過失を含む）、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様が認定販売元に支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。（すなわち、複数の請求が行われた場合でも制限が拡大されることはありません）。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、本契約中の別段の規定にかかわらず、お客様に対するシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーの合算での全責任は、契約、不法行為（過失を含む）、保証違反またはその他の原因に基づくかを問わず、当該請求を生じさせた本ソフトウェアについてお客様がシスコに支払った価格、または本ソフトウェアが対象外製品の一部である場合には当該対象外製品について支払われた価格を超えないものとします。ソフトウェアの当該責任の制限は累積的なものであり、一件毎のものではありません。（すなわち、複数の請求が行われた場合でも制限が拡大されることはありません）。本契約のいかなる規定も、(i) シスコ、ならびにその関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが、その過失に起因する身体障害または死亡に関してお客様に対して負う責任、(ii) 詐欺的な不実表示に関するシスコの責任、または (iii) 適用法のもとで排除できないシスコの責任を限定するものではありません。

責任の否認-結果的損害および他の損失に関する免責。本ソフトウェアの取得地が米国、ラテンアメリカ諸国、カリブ海沿岸諸国またはカナダの場合、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコまたはそのサプライヤは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生し



たかどうにかかわらず、上記損害が発生する可能性についてシスコまたはそのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。一部の州または法域では、結果的な損害または偶発的な損害の制限または除外が許可されていないため、上記制限がお客様に適用されない場合があります。

本ソフトウェアの取得地が日本の場合、死亡もしくは人身傷害または詐欺的な不実表示に起因または関連する責任を除き、本契約に定められている救済措置が、その本質的な目的を達成できないものであるかどうかにかかわらず、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、いかなる場合でも、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、発生原因を問わず、責任論の種類、または本ソフトウェアの使用もしくは使用不能によって発生したかどうかにかかわらず、上記損害が発生する可能性についてシスコもしくは認定販売元またはそれらのサプライヤもしくはライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。

本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニアの場合、シスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーは、収益もしくは利益の損失、データの喪失もしくは破損、事業の中断、資本喪失、または特別、間接、結果的、偶発的もしくは懲罰的な損害について、その発生原因（契約、不法行為（過失を含む）または本ソフトウェアの使用もしくは使用不能に起因するものを含むが、これらに限定されない）にかかわらず、それぞれの場合において、たとえ当該損害が発生する可能性についてシスコ、その関連会社、役員、取締役、従業員、代理人、サプライヤおよびライセンサーが事前に告知を受けていた場合であっても、一切責任を負いません。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が完全には適用されない場合があります。上記の排除は、(i) 死亡または人身傷害、(ii) 詐欺的な不実表示、または (iii) 適用法のもとで排除できない条件に関連するシスコの責任、に起因または関連する責任には適用されません。

お客様は以下の3点について認識および同意しているものとします。(i) シスコは、本契約内の保証の放棄および責任の制限に依拠して価格を決定し本契約を結んでいること、(ii) これは、両当事者間のリスク配分（契約上の救済措置が、その本質的な目的を達成できず、結果的に損失を被るというリスクを含む）にも反映されていること、(iii) これは、両当事者間での取引の基幹を成す事項であること。

準拠法、管轄裁判所。本ソフトウェアの取得地が、認定販売元により受諾された発注書上の住所の記載から判断して、米国、ラテンアメリカ諸国またはカリブ海沿岸諸国の場合、本契約および保証（「本保証」）に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がカナダの場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず、カナダのオンタリオ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、オンタリオ州内の各裁判所が専属的に管轄します。本ソフトウェアの取得地が欧州、中東、アフリカ、アジアまたはオセアニア（オーストラリアを除く）の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず英国の各法に準拠し、同法に従って解釈されます。本契約または本保証に起因する各種申し立てについては、英国内の各裁判所が専属的に管轄します。また、本契約が英国法に準拠する場合、本契約

の当事者ではない者は、本契約のいずれの条項についても、Contracts (Rights of Third Parties) Act 1999 (1999年契約 (第三者の権利) 法) に基づいて権利行使を行ったり、利益を享受したりする権利を有しません。本ソフトウェアの取得地が日本の場合、現地法が明示的に禁止していない限り、本契約および本保証は、法の抵触に関する条文にかかわらず日本国の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、日本国内の東京地方裁判所が専属的に管轄します。本ソフトウェアの取得地がオーストラリアの場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらずオーストラリア連邦ニュー サウス ウェールズ州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、ニュー サウス ウェールズ州内の州裁判所および連邦裁判所が専属的に管轄します。本ソフトウェアの取得地がその他の国の場合、現地法が明示的に禁止していない限り、本契約および本保証に関する規定は、法の抵触に関する条文にかかわらず米国カリフォルニア州の各法に準拠し、同法に従って解釈されます。また、本契約または本保証に起因する各種申し立てについては、カリフォルニア州内の州裁判所および連邦裁判所が専属的に管轄します。

上記のすべての国について、両当事者は、国際物品売買契約に関する国際連合条約の規定の適用を明示的に否定します。上記にかかわらず、いずれの当事者も、当事者の知的所有権または所有権の侵害の申し立てに対して、適切な司法管轄区域の裁判所において暫定的な差し止めによる救済を求めることができます。本契約のいずれかの規定が無効または施行不能なものとなった場合でも、本契約の残りの規定および本件保証書は有効に存続します。本契約内に別段の明示規定がない限り、本契約は、本件ソフトウェアおよび本件文書の使用許諾に関する両当事者の合意事項をまとめた唯一の文書となり、本件注文書またはその他の文書内の抵触規定または追加規定に優先し、これらの規定はすべて除外されます。本契約書は英語で記述されており、両当事者は、英語版が優先することに同意しているものとします。

各種製品保証規定やシスコ製品に関するその他の情報は、以下の URL でご確認ください。

<https://www.cisco.com/c/en/us/products/warranty-listing.html>

## Cisco コンテンツ セキュリティ ソフトウェア用 エンド ユーザ ライセンス 契約補則

重要 (よくお読みください)

本エンド ユーザ ライセンス 契約補則 (以下「SEULA」) には、お客様とシスコとの間のエンド ユーザ ライセンス 契約 (以下「EULA」) に基づいてライセンスされているソフトウェア製品に対する追加条項 (以下、総称して「契約」) が記載されています。この SEULA 内で定義されずに使用されている大文字の用語は、EULA で定義されたとおりの意味となります。この SEULA と EULA の条項に不一致がある場合は、この SEULA の条項が優先して適用されます。

お客様は、EULA により定められたお客様による本ソフトウェアへのアクセスおよび使用における制限事項の他に、本 SEULA に記載されている条項に同意したものと見なされます。

本ソフトウェアのダウンロード、インストール、または本ソフトウェアを内蔵する機器の使用により、お客様およびお客様が代表する企業体は本契約に法的に拘束されます。お客様が本契約のすべての規定に同意しない場合、シスコは、お客様による本件ソフトウェアの使用を許諾しません。その場合、(A) お客様は、本件ソフトウェアをダウンロード、インストール、ま

たは使用できません、また、(B) お客様は、本件ソフトウェア（あらゆる未開封の CD パッケージや関連文書を含む）を返却して全額払い戻しを受けられます。または、本件ソフトウェアと関連文書が、別の製品の一部として提供されたものである場合には、当該製品全体を返却して全額払い戻しを受けられます。返却および払い戻しに関するお客様の権利は、シスコまたはシスコ認定リセラーからの購入後 30 日で失効し、お客様が最初のエンドユーザ購入者である場合にのみ適用されます。

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

## Secure Mailbox License for Encryption Appliances

### Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at <http://www.cisco.com/c/en/us/about/legal/service-descriptions.html>.

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

### Additional License Terms and Conditions

#### LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

##### License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds

the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

**Consent and License to Use Data.**

Subject to the Cisco Privacy Statement at <http://www.cisco.com/web/siteassets/legal/privacy.html>, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

**Description of Other Rights and Obligations**

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.





## 索引

### 記号

[TLS 接続 (TLS Connections)] ページ [62](#)  
[ドメイン毎のエグゼクティブサマリー (Domain-Based Executive Summary)] レポート [177](#)

### D

DNS [78, 551](#)  
サーバ [551](#)  
スプリット [551](#)  
権威サーバ [551](#)  
二重検索 [78](#)

### E

E メールセキュリティ アプライアンス [57, 323](#)  
管理対象アプライアンスとして追加 [57, 323](#)

### I

IMAP 認証 [343](#)  
IronPort スпам隔離。「スパム隔離」を参照 [357](#)

### L

LDAP [340, 343](#)

### P

POP 認証 [343](#)  
PVO。「隔離、ポリシー、ウイルス、およびアウトブレイク」  
を参照 [357](#)

### S

SenderBase [78](#)

### W

Web UI セッションのタイムアウト [497, 498](#)

### あ

アンチウイルス隔離。「隔離、ウイルス」を参照 [357](#)

### う

ウイルス メッセージ [73](#)  
ウイルス隔離。「隔離」を参照 [357](#)  
ウイルス。 [357](#)

### え

エンドユーザ隔離 [343](#)  
スパム隔離、エンドユーザアクセスを参照 [343](#)

### く

グレーメール [73](#)

### こ

コンテンツ フィルタ [357](#)  
コンテンツ フィルタによる阻止 [68, 73](#)

### し

システム隔離。「隔離、ポリシー、ウイルス、およびアウトブレイク」  
を参照 [357](#)  
システム容量レポート [110, 111, 112, 127, 128, 129](#)  
E メール [110, 111, 112, 127, 128, 129](#)  
システムの負荷レポート [111, 128](#)  
メモリ ページスワッピング [112, 128](#)  
ワークキュー ページ [110, 127](#)

### す

スパム メッセージ [73](#)  
スパム隔離 [320, 321, 340, 341, 342, 343, 346, 348, 349, 352, 353](#)  
IMAP/POP 認証 [342](#)  
LDAP 認証 [341](#)

## スパム隔離 (続き)

- エイリアス統合 [348](#)
- エンド ユーザ アクセス [343](#)
- エンドユーザ アクセス [340](#)
- すべてのメッセージの削除 [353](#)
- メッセージの詳細 [352](#)
- メッセージ変数 [346](#)
- リリースされたメッセージと電子メールパイプライン [352](#)
- ローカル (local) [320](#)
- 外部 [320](#)
- 通知 [346](#)
- 通知のテスト [349](#)
- 複数の通知の受信 [348](#)
- 満杯時の動作 [321](#)
- 無効化 [353](#)
- スパム隔離内の全メッセージの削除 [353](#)

## せ

- セーフリスト/ブロックリスト [328, 329, 330, 338, 339](#)
- workqueue [328](#)
- インポートとエクスポート [338](#)
- トラブルシューティング [339](#)
- バックアップと復元 [338](#)
- 外部スパム隔離 [330](#)
- 管理 [330](#)
- 有効化 [329](#)

## た

- ダブル DNS で検証済み [78, 150](#)

## て

- データ損失防止 [357](#)

## は

- パスワード [484](#)
- 要件 [484](#)

## へ

- ベース エントロピー値、パスワードの強度 [484](#)

## ま

- マーケティング メッセージ [73](#)

## め

- メーリングリスト [348](#)
- 通知 [348](#)
- メッセージフィルタ [357](#)
- メッセージ変数 [346](#)
- スパム隔離の通知 [346](#)

## も

- モニタリング [55, 181](#)
- レポートのスケジュール設定 [181](#)
- 要約データ [55](#)

## ゆ

- ユーザアカウント [482, 484, 489](#)
- ロックとロック解除 [484, 489](#)
- ユーザグループ [470](#)
- ユーザ ロール [470](#)
- 説明 [470](#)

## れ

- レピュテーションフィルタによる停止 [73](#)
- レポート [181](#)
- スケジュール設定 [181](#)
- 時間範囲 [181](#)
- スケジュールされたレポート (メール) [181](#)