電子メール セキュリティ モニタの使用方法

この章は、次の項で構成されています。

電子メール セキュリティ モニタの概要

電子メールセキュリティモニタ機能は、電子メール配信プロセスのすべてのステップからデータを収集します。データベースは、IPアドレスに基づいて各電子メールの送信者を識別して記録します。また、IP レピュテーションサービスと連携してリアルタイムのアイデンティティ情報を収集します。ユーザは、すべての電子メール送信者のローカル メール フロー履歴をただちに報告し、インターネット上の送信者のグローバル情報を含むプロファイルを表示できます。電子メール セキュリティ モニタ機能では、セキュリティ チームが、ユーザへのメール送信者、ユーザによって送受信されるメールの量、およびセキュリティ ポリシーの有効性の「ループを閉じる」ことができます。

この章では、次の方法について説明します。

- 発着するメッセージ フローをモニタするための電子メール セキュリティ モニタ機能へのアクセス。
- 送信者の IP レピュテーションスコアを照会したメールフローポリシーの決定（許可リスト、ブロックリスト、およびグレーリストの更新）。ネットワーク オーナー、ドメイン、さらには個別の IP アドレスについてもクエリーを実行できます。
- メール フロー、メール ステータスおよびシステムに送受信されたメールに関する報告。

電子メール セキュリティ モニタ データベースでは、着信メールの所定の電子メール送信者について、次の重要パラメータを取得します。

- メッセージの量
- 接続履歴
- 受け入れられた接続と拒否された接続の比率
- 受け入れ率と調整上限値
- 送信者レピュテーション フィルタの一致率
- スパムの疑いのある、および明白にスパムと識別されるアンチスパム メッセージの数
- アンチ ウイルス スキャンによって検出されたウイルス陽性メッセージの数

アンチスパム スキャンの詳細については、スパムおよびグレイメールの管理を参照してください。アンチウイルス スキャンについては、アンチウイルスを参照してください。

電子メール セキュリティ モニタ機能は、内部ユーザ（電子メール受信者）またはメッセージの送信者を含む、特定のメッセージによってトリガーされたコンテンツ フィルタに関する情報も取得します。

電子メールセキュリティモニタ機能は GUI だけで使用でき、電子メールトラフィックおよびアプライアンス（隔離、ワークキュー、感染など）のステータスへのビューを提供します。アプライアンスは、送信者が標準のトラフィックプロファイルの範囲に該当しない場合に識別します。識別された送信者はインターフェイスで強調表示されるので、送信者を送信者グループに割り当てるか、送信者のアクセスプロファイルを変更することによって是正措置を取ることができます。または、引き続き AsyncOS のセキュリティ サービスに対応させることができます。送信メールにも同様のモニタリング機能があり、メールキューの上位ドメインおよび受信ホストのステータスにビューを提供します（[送信処理ステータス詳細（Delivery Status Details）] ページ （21 ページ）を参照）。

（注） 電子メールセキュリティモニタ機能では、アプライアンスの再起動時にワークキューに存在したメッセージの情報は報告されません。

関連項目

- 電子メール セキュリティ モニタと集中管理 （2 ページ）

電子メール セキュリティ モニタと集中管理

集約レポートデータを表示するには、Cisco コンテンツ セキュリティ管理アプライアンスを導入します。

クラスタ化されたアプライアンスの電子メール セキュリティ モニタ レポートは集約できません。すべてのレポートは、マシン レベルに制限されます。つまりレポートは、グループ レベルまたはクラスタ レベルでは実行できません。個別のマシンのみで実行できます。

[アーカイブ レポート（Archived Reports）]ページについても同様です。設定されている各マシンは、独自のアーカイブを備えています。したがって、「レポート生成」機能は、選択したマシンのみで実行されます。

[定期レポート（Scheduled Reports）]ページは、マシン レベルに制限されません。したがって、複数のマシンで設定を共有できます。マシン レベルで実行された、個別のスケジュール設定されたレポートは、インタラクティブ レポートとまったく同様なので、クラスタ レベルでスケジュール設定されたレポートを設定する場合、クラスタ内の各マシンが独自のレポートを送信します。

[このレポートをプレビュー（Preview This Report）]ボタンは、ログインホストに対して常に実行できます。

電子メール セキュリティ モニタ ページ

電子メール セキュリティ モニタ機能は、[モニタ（Monitor）] メニューで使用可能なすべてのページ（ただし [隔離（Quarantines）] ページは除く）で構成されます。

GUI でこれらのページを使用して、アプライアンスのリスナーに接続しているドメインをモニタできます。お使いのアプライアンスの「メールフロー」のモニタ、ソート、分析、および分類を実行し、正規メールの大量送信者と「スパマー」（未承諾の商業用メールの大量送信者）またはウイルス送信者の疑いのあるユーザとを区別できます。これらのページは、システムへの着信接続のトラブルシューティングにも役立ちます（IP レピュテーションスコア、ドメインに対する直近の送信グループの一致など重要情報を含みます）。

これらのページは、アプライアンスに関連するメール、さらにゲートウェイの範囲を超えて存在するサービス（IP レピュテーションサービス、アンチスパム スキャン サービス、アンチウイルス スキャン セキュリティ サービス、コンテンツフィルタ、およびアウトブレイクフィルタ）に関連するメールの分類に役立ちます。

ページ右上の [印刷用 PDF（Printable PDF）] リンクをクリックすると、すべての電子メール セキュリティ モニタ ページを読みやすい印刷形式の PDF 版で生成できます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）を参照してください。

[エクスポート（Export）] リンクでは、グラフおよび他のデータを Comma Separated Value（CSV; カンマ区切り値）形式にエクスポートできます。

エクスポートされた CSV データは、アプライアンスでの設定にかかわらず、すべてのメッセージトラッキングおよびレポーティングデータを GMT で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数の時間帯にあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

（注） ローカライズされた CSV データをエクスポートする場合、一部のブラウザでは見出しが正しく表示されないことがあります。これは、ローカライズされたテキストに対して、一部のブラウザが適切な文字セットを使用していないためです。この問題を回避するには、ファイルをディスクに保存し、[ファイル（File）]>[開く（Open）] を使用して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 データのエクスポートの自動化の詳細については、CSV データの取得 （42 ページ）を参照してください。

電子メール セキュリティ モニタ ページのリスト

検索と電子メール セキュリティ モニタ

電子メール セキュリティ モニタ ページの多くには、検索フォームが含まれています。次の各種項目を検索できます。

- IP アドレス（IPv4 および IPv6）

- 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
- 発信ドメインの配信ステータス

ドメイン、ネットワーク オーナー、および内部ユーザの検索では、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（たとえば、「ex」で始まる場合は「example.com」に一致します）を検索するかを選択します。

IPv4 アドレス検索では、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」と入力すると、17.0.0.0 ～ 17.255.255.255 の範囲が検索されます。17.0.0.1 には一致しますが、172.0.0.1 には一致しません。完全一致検索の場合は、4 オクテットすべてを入力するだけです。IP アドレス検索は、CIDR 形式（17.16.0.0/12）もサポートしています。

IPv6 アドレス検索では、AsyncOS は次の形式をサポートします。

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

すべての検索は、ページで現在選択されている時間範囲に限定されます。

レポートに含まれるメッセージの詳細の表示

この機能は、レポートとトラッキングが両方ともローカルの場合（Cisco コンテンツ セキュリティ管理アプライアンスで中央管理されていない場合）にのみ、機能します。

手順

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）。

この番号に関連するメッセージがメッセージ トラッキングで表示されます。

ステップ 2 下にスクロールして、リストを表示します。

次のタスク

関連項目

- メッセージ トラッキングの検索結果の使用

[マイ ダッシュボード（My Dashboard）] ページ

既存のレポートのページからチャート（グラフ）とテーブルを組み合わせてカスタム電子メール セキュリティ レポートのページを作成できます。

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	**1.** **[モニタ（Monitor）] >** [マイダッシュボード（My Dashboard）] に移動し、モジュールの右上にある [X] をクリックして不要なサンプル モジュールを削除します。 **2.** 次のいずれかを実行します。 • カスタム レポートにモジュールを追加するには、[モニタ（Monitor）] メニューの下のレポート ページ内のモジュール上の [+] ボタンをクリックします。 • **[モニタ（Monitor）] >** [マイダッシュボード（My Dashboard）] に移動し、いずれかのセクションの [+] ボタンをクリックし、追加するレポート モジュールを選択します。必要なレポートを見つけるために、各セクションの [+レポートモジュール（+ Report Module）] を確認する必要がある場合があります。 **3.** モジュールがデフォルト設定に追加されます。カスタマイズした（たとえば、列を追加、削除、または並べ替えしたり、）モジュールを追加する場合は、これらのモジュールを追加した後、再度カスタマイズします。元のモジュールの時間範囲は保持されません。 **4.** 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。 （注） • 特定のレポート ページの特定のモジュールは、上記の方法のいずれかを使用した場合のみ使用できます。ある方式を使用してモジュールを追加できない場合は、他の方法を試してください。 • 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。

目的	操作手順
カスタム レポート ページの表示	1. **[モニタ（Monitor）] >** [マイダッシュボード（My Dashboard）] を選択します。 2. [時間範囲（Time Range）] セクションのレポートの場合：すべてのレポートのページ用に選定された時間範囲は [マイ ダッシュボード（My Dashboard）] ページのすべてのモジュールに適用されます。表示する時間範囲を選択します。 新しく追加されたモジュールは関連するセクションの上部に表示されます。
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。

[概要（Overview）] ページ

[概要（Overview）] ページには、隔離および（このページの [システム概要（System Overview）] セクションの）アウトブレイクフィルタのステータスの概要など、お使いのアプライアンスのメッセージアクティビティの概要が示されます。[概要（Overview）] ページには、グラフや、送受信メッセージの詳細なメッセージ数も表示されます。このページを使用して、ゲートウェイから出入りするすべてのメールのフローをモニタできます。

[概要（Overview）] ページには、受信メール（レピュテーション フィルタリングによって停止されたメッセージなど）に関して、アプライアンス と IP レピュテーションサービスの連携方法が分かりやすく示されています。[概要（Overview）] ページでは、次の操作を実行できます。

- ゲートウェイを「出入り」するすべてのメールのメール トレンド グラフを表示する。
- 試行されたメッセージ、IP レピュテーション フィルタリングによって停止されたメッセージ、受信者が無効なメッセージ、スパムとしてマークされたメッセージ、ウイルス検出としてマークされたメッセージ、およびクリーンメッセージの数を経時的に表示する。
- システム ステータスおよびローカル隔離のサマリーを表示する。
- Threat Operations Center（TOC）で入手可能な情報に基づいて、現在のウイルスの発生情報やウイルス以外の発生情報を確認する。

[概要（Overview）] ページは、[システム概要（System Overview）] セクションおよび送受信メールのグラフとサマリーのセクションの 2 つに分かれています。

関連項目

- システム概要 （8 ページ）
- 送受信のサマリーとグラフ （9 ページ）

• 電子メールの分類 （10 ページ）
• メッセージの分類方法 （11 ページ）

システム概要

[概要（Overview）]ページの[システム概要（System Overview）]セクションは、システムダッシュボードとして機能し、システムおよびワークキューステータス、隔離ステータス、発生アクティビティなどのアプライアンス に関する詳細を示します。

関連項目

• ステータス（Status） （8 ページ）
• システム隔離（System Quarantines） （8 ページ）
• ウイルス脅威レベル （8 ページ）

ステータス（Status）

このセクションでは、アプライアンス および着信メール処理の現在の状態の概要が示されます。

[システム ステータス（System Status）]：次のいずれかの状態です。

- オンライン（Online）
- リソース節約（Resource Conservation）
- 配信停止（Delivery Suspended）
- 受信停止（Receiving Suspended）
- ワーク キュー一時停止（Work Queue Paused）
- オフライン

詳細については、CLI による管理およびモニタリング を参照してください。

[受信メッセージ（Incoming Messages）]：1 時間あたりの着信メールの平均レート。

[ワーク キュー（Work Queue）]：ワーク キュー内の処理待ちメッセージの数。

[システム ステータス（System Status）] ページに移動するには、[システム ステータス詳細（System Status Details）] リンクをクリックします。

システム隔離（System Quarantines）

このセクションには、アプライアンスでのディスク使用量別の上位 3 つの隔離に関する情報（隔離の名前、隔離の使用度（ディスク領域）、現在の隔離エリア内のメッセージ数など）が表示されます。

[内部隔離（Local Quarantines）] ページに移動するには、[内部隔離（Local Quarantines）] リンクをクリックします。

ウイルス脅威レベル

ここでは、Threat Operations Center（TOC）から報告される、Outbreak のステータスを示します。また、隔離の使用度（ディスク領域）、隔離内のメッセージ数など、アウトブレイク隔離

のステータスを示します。アウトブレイク隔離は、アプライアンス でアウトブレイクフィルタ機能をイネーブルに設定した場合のみ表示されます。

（注） 脅威レベル インジケータを機能させるためには、ファイアウォールで「**downloads.ironport.com**」に対してポート 80 を開く必要があります。あるいは、ローカル更新サーバを指定した場合は、脅威レベルインジケータがそのアドレスを使用します。また、[サービスのアップデート（Service Updates）] ページを使用してダウンロード用のプロキシを設定済みの場合、脅威レベルインジケータは、正しくアップデートされます。詳細については、サービス アップデートを参照してください。

外部 Threat Operations Center ウェブ サイトを表示するには、[アウトブレイクの詳細（Outbreak Details）] をクリックします。このリンクを機能させるには、お使いのアプライアンス でインターネットに接続できる必要があります。[個別のウィンドウ（Separate Window）] アイコンは、クリックすると別個のウィンドウにリンクが開かれることを示します。これらのウィンドウを表示できるようにするには、ブラウザのポップアップ ブロッカを設定する必要があります。

送受信のサマリーとグラフ

送受信のサマリーのセクションでは、システム上のすべてのメールアクティビティのリアルタイム アクティビティへのアクセスが提供され、送受信メールのグラフとメール サマリーで構成されています。ユーザは、[時間範囲（Time Range）] メニューを使用して報告対象となるタイムフレームを選択できます。選択したタイムフレームは、すべての電子メールセキュリティ モニタ ページで使用されます。メッセージの各タイプまたはカテゴリに関する説明は以下のとおりです（電子メールの分類 （10 ページ）を参照）。

メール トレンド グラフでは、メール フローが視覚的に表示されますが、サマリー テーブルでは、同じ情報の数値的な内訳が示されます。サマリー テーブルには、各メッセージ タイプの割合と実数（試行されたメッセージ、脅威メッセージ、クリーン メッセージの総数を含む）が含まれています。

送信グラフおよびサマリーでも、送信メールに関する同様の情報が示されます。

関連項目

- 電子メール セキュリティ モニタでのメッセージ集計に関する注意事項 （9 ページ）

電子メール セキュリティ モニタでのメッセージ集計に関する注意事項

電子メール セキュリティ モニタが着信メールの集計に使用する方法は、メッセージあたりの受信者の数によって異なります。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、この送信者からの 3 通として集計されます。

送信者レピュテーションフィルタ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 は着信メッセージの受信者のリストには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。この乗数はシスコによって算出されたもので、既存の顧客データの大規模なサンプリング研究に基づいています。

電子メールの分類

[概要（Overview）]ページおよび[受信メール（Incoming Mail）]ページで報告されるメッセージは、次のように分類されます。

- [IPレピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）]：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（電子メール セキュリティ モニタでのメッセージ集計に関する注意事項 （9 ページ）を参照）を乗じた値に受信調整によってブロックされたすべての受信者数を加えた値。
- [無効な受信者（Invalid Recipients）]：従来の LDAP 拒否によって拒否されたすべての受信者数にすべての RAT 拒否数を加えた値。
- [スパムメッセージ検出（Spam Messages Detected）]：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メッセージ、および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。
- [ウイルスメッセージ検出（Virus Messages Detected）]：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。

- [高度なマルウェア防御による検出（Detected by Advanced Malware Protection）]：ファイルレピュテーションフィルタリングにより、メッセージの添付ファイルが悪意のある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。
- [悪意のあるURLを含むメッセージ（Messages with Malicious URLs）]：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。
- [コンテンツフィルタによる停止（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 によるサポート（Stopped by DMARC）]：DMARC 検証後に阻止されたメッセージの総数。

（注） 電子メールゲートウェイは、「失敗 - 拒否」、「失敗 - 隔離」、および「失敗 - アクションなし」の結果に基づいて、「DMARC による停止」メッセージの総数を表示します。

- [S/MIME 検証または復号に失敗しました（S/MIME Verification/Decryption）]：S/MIME 検証または復号、あるいはその両方に失敗したメッセージの総数。

- [S/MIME 検証/復号が成功しました（S/MIME Verification/Decryption Successful）]：S/MIME を使用した検証または復号、あるいは復号と検証が成功したメッセージの総数。
- [正常なメッセージ（Clean Messages）]：受け入れられ、ウイルスでもスパムでもないと見なされたメール。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正常な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ので、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。
- グレイメール メッセージ
  - [マーケティングメッセージ（Marketing Messages）]：たとえば、Amazon.com のような、プロフェッショナルなマーケティング グループによって送信されたアドバタイジング メッセージの総数。
  - [ソーシャル ネットワーキング メッセージ（Social Networking Messages）]：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。
  - [バルク メッセージ（Bulk Messages）]：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広告メッセージの総数。

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、上記の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。

（注） メッセージフィルタに一致し、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ないメッセージは、クリーンとして処理されます。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。

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、スパム陽性、ウイルス陽性、またはマルウェア陽性とマークされたメッセージが、コンテンツ フィルタにも一致することがありますこれらの優先ルールに続いて、アウトブレイク フィルタによる隔離（この場合、メッセージが隔離から解放されるまで集計されず、ワーク キューによる処理が再び行われます）の次にスパム陽性、ウイルス陽性、マルウェア陽性、およびコンテンツ フィルタとの一致などさまざまな判定が行われます。

たとえば、メッセージがスパム陽性とマークされると、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る場合には、このメッセージがドロップされ、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パイプラインで処理し、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、または隔離するようにアンチスパム設定が設定されている場合にも、スパム カウンタは増分します。メッセージがスパム陽性、ウイルス陽性、またはマルウェア陽性ではない場合、コンテンツ フィルタ カウントが増分するだけです。

[受信メール（Incoming Mail）] ページ

[受信メール（Incoming Mail）] ページでは、お使いのアプライアンス に接続するすべてのリモートホストの電子メールセキュリティモニタ機能によって収集されたリアルタイム情報に関して報告を行うメカニズムが提供されます。これにより、メール送信者の IP アドレス、ドメイン、および組織（ネットワーク オーナー）に関する詳細を収集できます。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できます。

[受信メール（Incoming Mail）] ページには、[ドメイン（Domain）]、[IP アドレス（IP Addressl）]、および [ネットワーク所有者（Network Owner）] の 3 種類のビューが用意されており、システムに接続するリモートホストのスナップショットが選択したビューで提供されます。

アプライアンス で設定済みのすべてのパブリックリスナーにメールを送信した上位ドメイン（またはビューに応じて、IP アドレスまたはネットワークオーナー）の表（[受信メールの詳細（Incoming Mail Details）]）が表示されます。ゲートウェイに入ったすべてのメールのフローをモニタできます。任意のドメイン/IP/ネットワーク オーナーをクリックしてドリルダウンし、送信者プロファイル ページ（クリックしたドメイン/IP/ネットワーク オーナーに固有の [受信メール（Incoming Mail）] ページ）のこの送信者に関する詳細にアクセスできます。

使用可能なすべての列がデフォルトで表示されるわけではありません。テーブルの下の [列（Columns)] リンクをクリックすると、異なる情報セットが表示されます。たとえば、デフォルトでは非表示になっている [高度なマルウェア防御による検出（Detected by Advanced Malware Protection）] 列を表示できます。

[受信メール（Incoming Mail）] は、一連のページ（[受信メール（Incoming Mail）]、送信者プロファイル、および送信者グループ レポート）を含むように拡張することもできます。[受信メール（Incoming Mail）] ページでは、次の操作を実行できます。

- メール送信者の IP アドレス、ドメイン、または組織（ネットワーク オーナー）に関する検索を実行する。
- 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よる接続を確認する。詳細については、送信者グループ レポート （18 ページ）を参照してください。
- 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、グレイメール他）によってブロックされたメッセージの数など、メール送信者に関する詳細な統計情報を確認する。
- 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送信者別にソートする。
- IP 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のドリルダウンと分析を行い、送信者に関する詳細を取得する。
- 特定の送信者をドリルダウンして、送信者の IP レピュテーションスコア、ドメインが直近に一致した送信者グループなど、IP レピュテーションサービスから送信者に関する詳細を取得する。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をドリルダウンする。

- ドメインに関する情報を収集したら、（必要に応じて）ドメイン、IP アドレス、またはネットワーク オーナーのプロファイル ページから [送信者グループに追加（Add to Sender Group）] をクリックして、既存の送信者グループに IP アドレス、ドメイン、または組織を追加できます。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。

関連項目

- 受信メール （13 ページ）
- [受信メールの詳細（Incoming Mail Details）] リスト （14 ページ）
- データが読み込まれる報告ページ：送信者プロファイル ページ （16 ページ）
- 送信者グループ レポート （18 ページ）

受信メール

[受信メール（Incoming Mail）] ページでは、システムで設定済みのすべてのパブリック リスナーのリアルタイム アクティビティへのアクセスが提供され、受信数の上位送信者のドメイン（脅威メッセージの総数別、クリーン メッセージの総数別、グレーメール メッセージの総数別）および [受信メールの詳細（Incoming Mail Details）] リストという 2 つのセクションで構成されます。

[受信メールの詳細（Incoming Mail Details）] リスト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）] リスト （14 ページ）を参照してください。

関連項目

メール トレンド グラフにおける時間範囲に関する注意事項 （13 ページ）

メール トレンド グラフにおける時間範囲に関する注意事項

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。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。

時間範囲は、次の表に記載のオプションから選択します。

表 *1*: 電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時間（Hour）	直近の 60 分 + 最大 5 分
日（Day）	直近の 24 時間と直近の 60 分
Week	直近の 7 日 + 当日の経過した時間
30 日（30 days）	直近の 30 日 + 当日の経過した時間
90 日（90 days）	直近の 90 日 + 当日の経過した時間

GUI で選択した時間範囲	定義
昨日 （Yesterday）	00:00 ～ 23:59（午前 0 時～午後 11:59）
先月 （Previous Calendar Month）	その月の最初の日の 00:00 ～その月の最後の日の 23:59
カスタム範囲（Custom Range）	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

集中化レポーティングをイネーブルにしていると、表示される時間範囲オプションが異なります。集中管理レポート モードの詳細については、Cisco コンテンツ（M シリーズ）セキュリティ管理アプライアンス の集中型サービスを参照してください。

[受信メールの詳細（Incoming Mail Details）] リスト

アプライアンスのパブリックリスナーに接続した上位送信者が、[受信メール（Incoming Mail）] ページの下部にある受信された外部ドメインリストの表に選択したビューで表示されます。データをソートするには、カラム見出しをクリックします。各種のカテゴリの説明については、電子メールの分類 （10 ページ）を参照してください。

ダブル DNS ルックアップの実行によって、リモート ホストの IP アドレス（つまり、ドメイン）が取得され、有効性が検証されます。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、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。

送信者の詳細のリストには、[サマリー（Summary）] と [すべて（All）] の 2 つのビューがあります。

デフォルトの [送信者の詳細（Sender Detail）] ビューでは、各送信者が試行したメッセージの総数が示され、カテゴリ別の内訳が含まれます。カテゴリは、[概要（Overview）] ページの [受信メールサマリー（Incoming Mail Summary）] グラフと同じです。

[IP レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。

- この送信者からの「調整された」メッセージの数。
- 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）。
- 接続ごとのメッセージ数に対する控えめな乗数。

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。

（注） [概要（Overview）] ページの [IP レピュテーションフィルタによる停止（Stopped by IP 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が、負荷のために常に限定的です。

表示できる追加のカラムは次のとおりです。

[接続拒否（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（Connections Accepted）]：受け入れられたすべての接続。

[受信者スロットルによる停止（Stopped by Recipient Throttling）]：[レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] のコンポーネントです。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。

[高度なマルウェア防御による検出（Detected by Advanced Malware Protection）]：ファイル レピュテーションフィルタリングにより、添付ファイルが悪意のあるファイルとして検出されたメッセージ。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。

[合計脅威件数（Total Threat）]：（送信者レピュテーションにより阻止された、無効な受信者、スパム、およびウイルスとして阻止された）脅威メッセージの総数

テーブルの下部にある [列（Column）] リンクをクリックすると、カラムの表示/非表示が切り替わります。

このリストは、カラム見出しリンクをクリックするとソートされます。カラム見出しの横にある小さな三角形は、データの現在のソートに使用されているカラムを示します。

関連項目

- [ドメイン情報がありません（No Domain Information）]（15 ページ）
- 詳細の問い合わせ （15 ページ）

[ドメイン情報がありません（No Domain Information）]

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されないホストは、送信者の検証によって管理できます。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。

リストに表示される送信者の数は、[表示された項目（Items Displayed）] メニューから選択できます。

詳細の問い合わせ

電子メール セキュリティ モニタのテーブルに表示された送信者については、その送信者（または [ドメイン情報がありません（No Domain Information）] リンク）をクリックして特定の送信者に関する詳細をドリルダウンします。結果は送信者プロファイルページに表示され、IP 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ドリルダウンできます（データが読み込まれる報告ページ：送信者プロファイル ページ （16 ページ）を参照）。

[受信メール（Incoming Mail）] ページの下部にある [送信者グループのレポート（Sender Groups Report）] リンクをクリックして、別のレポート（送信者グループ レポート）を表示することもできます。送信者グループ レポートの詳細については、送信者グループ レポート （18 ページ）を参照してください。

データが読み込まれる報告ページ：送信者プロファイル ページ

[受信メール（Incoming Mail）] ページにある [受信メールの詳細（Incoming Mail Details）] テーブルをクリックすると、その結果として送信者プロファイルページが表示されます。このページには、特定の IP アドレス、ドメイン、または組織（ネットワーク オーナー）のデータが含まれています。送信者プロファイルページには、送信者の詳細情報が示されます。任意のネットワーク オーナーまたは IP アドレスの送信者プロファイル ページは、[受信メール（Incoming Mail）] ページまたは他の送信者プロファイル ページで特定の項目をクリックしてアクセスできます。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あり、ドメインは、IP アドレスを含むエンティティです。この関係および IP レピュテーションサービスとの関係の詳細については、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。

IP アドレス、ネットワーク オーナーおよびドメインに関して表示される送信者プロファイル ページは、多少異なります。それぞれのページには、こ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。グラフの下には、この送信者に関連するドメインまたは IP アドレスを表示する表（個々の IP アドレスの送信者プロファイル ページには、詳細なリストは含まれません）、およびこの送信者の現在の SenderBase 情報、送信者グループ情報、およびネットワーク情報を含む情報セクションがあります。

- 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 アドレスのみに関する情報が含まれます。

各送信者プロファイルページには、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。

- IP 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ァイル 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（約 100 億メッセー

ジ/日）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）
- IP レピュテーションスコア（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 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）

IP レピュテーションサービスによって提供されるすべての情報が記載されたページを表示するには、[SenderBaseからの詳細情報（More from SenderBase）] リンクをクリックします。

- **メール フロー統計**情報。送信者について収集された、指定した時間範囲にわたる電子メール セキュリティ モニタ情報を含みます。
- 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 ページから特定の IP アドレスをドリルダウンするか、ドリルアップして組織プロファイル ページを表示できます。また、テーブルの下部にある [列（Columns）] リンクをクリックして、[IPアドレス（IP Addresses）] テーブル内の送信者アドレスごとに。[DNS検証（DNS Verified）] ステータス、[IP レピュテーションスコア（IP Reputation Score）]、および [最新の送信者グループ（Last Sender Group）] を表示することもできます。そのテーブル内の任意のカラムを非表示にすることもできます。

  ネットワーク オーナー プロファイル ページから、そのテーブルの下部にある [列（Columns）] リンクをクリックすることにより、[ドメイン（Domains）] テーブル内のドメインごとの [接続拒否（Connections Rejected）]、[接続承認（Connections Accepted）]、[受信者スロットルによる停止（Stopped by Recipient Throttling）]、および [高度なマルウェア防御による検出（Detected by Advanced Malware Protection）] などの情報を表示できます。そのテーブル内の任意のカラムを非表示にすることもできます。

  システムの管理者の場合は、これらの各ページで（必要に応じて）エンティティのチェックボックスをクリックしてから [送信者グループに追加（Add to Sender Group）] をクリックし、送信者グループにネットワーク オーナー、ドメイン、または IP アドレスを追加することもできます。

また、送信者の現在の情報テーブルの送信者グループ情報の下にある [送信者グループに追加（Add to Sender Group）] リンクをクリックして、送信者グループに送信者を追加することもできます。送信者を送信者グループに追加する方法の詳細については、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。当然ながら、必ずしも変更を行う必要はありません。セキュリティ サービスに着信メールを処理させることもできます。

関連項目

- 送信者プロファイルの検索 （18 ページ）

送信者プロファイルの検索

特定の送信者を検索するには、[クイック検索（Quick Search）] ボックスに IP アドレス、ドメイン、または組織名を入力します。

送信者プロファイル ページが送信者の情報と共に表示されます。データが読み込まれる報告ページ：送信者プロファイル ページ （16 ページ） を参照してください。

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。

[送信者ドメインのレピュテーション（SenderDomainReputation）]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「Untrusted」または「Questionable」メッセージのみが、「Spam」や「Malicious」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

[送信先（Outgoing Destinations）] ページには、メールの送信先ドメインに関する情報が示されます。このページは、2 つのセクションで構成されます。ページの上部は、発信脅威メッセージ別の上位宛先および発信クリーンメッセージの上位宛先を示すグラフで構成されます。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）全カラムを示す表が表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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。

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

- アプライアンスのメール送信先
- 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スされたメッセージの数

送信者

[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。このページを表示すると、ドメイン別または IP アドレス別に結果を表示できます。各ドメインによって送信されたメールの量を確認する場合にはドメイン別の結果、最も多いウイルス メッセージを送信している、または最も多くコンテンツ フィルタをトリガーしている IP アドレスを表示する場合には IP アドレス別の結果を表示することが推奨されます。

このページは、2 つのセクションで構成されます。ページの左側は、総脅威メッセージ別の上位送信者を示すグラフです。合計脅威メッセージには、スパム陽性、ウイルス陽性、マルウェアのメッセージ、またはコンテンツ フィルタをトリガーしたメッセージが含まれます。ページの上部の右側は、クリーン メッセージ別の上位送信者を表示するグラフです。ページの下部には、総メッセージ数別にソートされた（デフォルト設定）全カラムを示す表が表示されます。

（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スされたメッセージの数などの配信情報は、[送信処理ステータス（Delivery Status）]ページを使用して追跡できます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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。

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

- 最も多くのウイルスに感染、スパム陽性、また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

地理的分散ページ

[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）。

特定の位置情報の受信メールの接続の数をクリックすると、メッセージ トラッキングに関連メッセージを表示できます。

[合計メッセージ数（Total Messages）] 列には、SMTP 接続レベルで受け入れられるメッセージのみ表示されます。

（注） レポート生成中に次の処理が発生します。

- プライベート IP アドレスとして 1 つ以上の受信メール接続が検出されると、受信メール接続がレポートの「プライベート IP アドレス」として分類されます。
- 有効ではない IP レピュテーションスコアとして 1 つ以上の受信メール接続が検出されると、受信メール接続がレポートで「国情報なし」に分類されます。

[送信処理ステータス（Delivery Status）] ページ

特定の受信者ドメインに対する配信の問題を疑ったり、仮想ゲートウェイ アドレスに関する情報収集を行ったりする場合には、[モニター（Monitor）]>[送信処理ステータス ページ（Delivery Status Page）] をクリックすると、特定の受信者ドメインに関連する電子メール操作に関するモニタリング情報が提供されます。

[送信処理ステータス（Delivery Status）] ページには、CLI で tophosts コマンドを使用した場合と同じ情報が表示されます（詳細については、CLI による管理およびモニタリングの「電子メール キューの構成の確認」を参照してください）。

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。各統計情報のカラム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。

- 特定のドメインを検索するには、[ドメイン名：（Domain Name:）] フィールドにドメイン名を入力し、[検索（Search）] をクリックします。
- 表示されているドメインをドリルダウンするには、ドメイン名のリンクをクリックします。

[送信処理ステータス詳細（Delivery Status Details）] ページに結果が表示されます。

（注） 受信者ドメインで任意のアクティビティが発生すると、このドメインが「アクティブ」となり、[概要（Overview）] ページに表示されます。たとえば、配信の問題があるためにメールが発信キューにとどまると、この受信者ドメインは、引き続き発信メールの概要に表示されます。

関連項目

- 配信の再試行 （21 ページ）
- [送信処理ステータス詳細（Delivery Status Details）] ページ （21 ページ）

配信の再試行

後で配信されるようにスケジュール設定されているメッセージは、[すべての送信を再試行（Retry All Delivery）] をクリックすると、ただちに再試行できます。[すべての送信を再試行（Retry All Delivery）] では、キューに含まれるメッセージがただちに配信されるようにスケジュールを変更できます。down のマークが付いたすべてのドメインと、スケジュールされたメッセージまたはソフト バウンスされたメッセージが、即時配信のキューに入れられます。

特定の宛先ドメインに向けての配信を再施行するには、ドメイン名のリンクをクリックします。[送信処理ステータス詳細（Delivery Status Details）] ページで、[送信を再試行（Retry Delivery）] をクリックします。

CLI で delivernow コマンドを使用して、ただちに配信するようにメッセージのスケジュールを変更することもできます。詳細については、電子メールの即時配信スケジュールを参照してください。

[送信処理ステータス詳細（Delivery Status Details）] ページ

特定の受信者ドメインに関する統計情報を検索するには、[送信処理ステータス詳細（Delivery Status Details）] ページを使用します。このページには、CLI 内で **hoststatus** コマンドを使

用した場合と同じ情報（メール ステータス、カウンタ、およびゲージ）が表示されます。（詳細については、CLIによる管理およびモニタリングを参照してください）特定のドメインを検索するには、[ドメイン名：（Domain Name:）] フィールドにドメイン名を入力し、[検索（Search）] をクリックします。**altsrchost** 機能を使用している場合、仮想ゲートウェイのアドレス情報が表示されます。

[内部ユーザ（Internal Users）] ページ

[内部ユーザ（Internal Users）] 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。
- ユーザー 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。非表示のテーブル カラムを表示するか、またはデフォルト カラムを非表示にするには、テーブルの下の [列（Columns)] リンクをクリックします。

[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。

デフォルトで非表示のカラム（[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）] カラムまたは [高度なマルウェア防御で検出された

送信メール（Outgoing Detected by Advanced Malware Protection）] など）を表示するには、テーブルの下の [列（Column）] リンクをクリックします。

関連項目

- 内部ユーザの詳細 （23 ページ）
- 特定の内部ユーザの検索 （23 ページ）

内部ユーザの詳細

[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 フィルタによる受信停止（Stopped By Content Filter）]、[グレーメール検出（Graymail Detected）]、および[正常（Clean）]）のメッセージ数を示す送受信メッセージの内訳など指定したユーザに関する詳細情報が示されます。受信メッセージの場合は任意で、テーブルの下の [列（Column）] リンクをクリックすると、[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）] カラムが表示されます。この値は、ファイル レピュテーション フィルタリングにより悪意のあるファイルと判断された添付ファイルを含むメッセージの数を表します。この値には、判定のアップデートまたはファイル分析により悪意があるファイルとして検出されたファイルは含まれません。送受信コンテンツ フィルタおよび DLP ポリシーの一致も示されます。

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（25 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ユーザのリストも取得できます。

特定の内部ユーザの検索

特定の内部ユーザ（電子メール アドレス）は、[内部ユーザ（Internal Users）]ページおよび[内部ユーザの詳細（Internal User Details）] ページの下部にある検索フォームから検索できます。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.com」が一致します）を選択します。

[DLP インシデント（DLP Incidents）] ページ

[DLP インシデント（DLP Incidents）] 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。アプライアンスでは、[送信メールポリシー（Outgoing Mail Policies）] テーブルでイネーブルにした 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 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（DLP Incidents）] ページは、次の 2 つの主なセクションで構成されます。

- 重大度（[低（Low）]、[中（Medium）]、[高（High）]、[クリティカル（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 Incidents Details）] リスト

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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するか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）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。

関連項目

- DLP インシデントの詳細（DLP Incidents Details） （24 ページ）
- [DLP ポリシー詳細（DLP Policy Detail）] ページ （24 ページ）

DLP インシデントの詳細（DLP Incidents Details）

アプライアンスの送信メールポリシーで現在イネーブルの DLP ポリシーは、[DLPインシデント（DLP Incidents）] ページの下部にある [DLPインシデントの詳細（DLP Incidents Details）] 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。

[DLP インシデントの詳細（DLP Incidents Details）] テーブルは、ポリシーごとの DLP インシデントの合計数と、重大度レベル別の内訳を示します。重大度レベルには、バウンスされたメッセージの数と、クリアで配信、暗号化で配信、または削除されたメッセージの数も含まれます。データをソートするには、カラム見出しをクリックします。

[DLP ポリシー詳細（DLP Policy Detail）] ページ

[DLP インシデントの詳細（DLP Incidents 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）] リストも含まれます。このリストには、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）] リストを使用

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検索できます。

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 （22 ページ）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）] 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2種類の形式（棒グラフとリスト）で表示されます。[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

リストのコンテンツ フィルタ名をクリックすると、[コンテンツフィルタの詳細（Content Filter Details）] ページにこのフィルタに関する詳細を表示できます。

関連項目

- コンテンツ フィルタの詳細 （25 ページ）

コンテンツ フィルタの詳細

[コンテンツフィルタの詳細（Content Filter Details）] 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）] セクションでは、ユーザ名をクリックして内部ユーザ（電子メール アドレス）の [内部ユーザの詳細（Internal User Details）] ページを表示できます（内部ユーザの詳細 （23 ページ）を参照）。

[DMARC検証（DMARC Verification）] ページ

[DMARC検証（DMARC Verification）] ページには、DMARC 検証が失敗した上位のドメインと、DMARC 検証に失敗したメッセージに対して AsyncOS が実行したアクションの詳細情報が表示されます。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。

- 最も多く DMARC 準拠ではないメッセージを送信したドメインはどれか。
- 各ドメインで、DMARC 検証に失敗したメッセージに対して AsyncOS がどのようなアクションを実行したか。

[DMARC検証（DMARC Verification）] ページの内容は次のとおりです。

- DMARC 検証の失敗数に基づく上位ドメインを示す横棒グラフ。
- ドメイン別に次の情報を示す表。

- アクションなしで承認、隔離、または拒否されたメッセージの数。数値をクリックすると、選択されているカテゴリのメッセージのリストが表示されます。
- DMARC 検証に合格したメッセージの数。
- DMARC 検証試行回数の合計。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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するか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。

[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）。
- 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。

[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、お使いのアプライアンスのアウトブレイクフィルタの現在のステータスおよび設定に加えて、最近の発生状況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。

[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、[マルウェア（Malware）]、[フィッシング（Phish）]、[詐欺（Scam）]、および [ウィルス（Virus）] による脅威メッセージの内訳が示されます。数値をクリックすると、メッセージ トラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

[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。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。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。数値をクリックすると、メッセージ トラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

[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 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。

[受信メッセージからのヒット メッセージ（Hit Messages from Incoming Messages）] セクションには、ウィルス性添付ファイル、その他の脅威（非ウィルス性）、正常な受信メッセージの割合と数が示されます。

[脅威レベル別のヒット メッセージ（Hit Messages by Threat Level）] セクションには、脅威レベル（レベル 1 ～ 5）に基づいて受信脅威メッセージ（ウィルス性および非ウィルス性）の割合と数が示されます。

[アウトブレイク隔離されているメッセージ（Messages resided in Outbreak Quarantine）] セクションには、アウトブレイク隔離エリアに入っていた脅威メッセージの数が、その期間に基づいて示されます。

[書き換えられた上位URL（Top URL's Rewritten）] セクションには、発生回数に基づいて、書き換えられた上位 10 件の URL がリストで示されます。書き換えられた URL をさらに表示するには、[表示されたアイテム（Items Displayed）] ドロップダウンを使用します。数値をクリッ

クすると、[メッセージトラッキング（Message Tracking）] ページで選択した書き換えられた URL を含むすべてのメッセージのリストが表示されます。

[アウトブレイク フィルタ（Outbreak Filters）]ページを使用すると、次の情報を取得できます。

- 隔離されているメッセージの数と、それらの脅威のタイプ
- ウイルス発生に対するアウトブレイク フィルタ機能のリード タイム
- グローバル ウイルス発生と比較したローカル ウイルスの発生状況

[ウイルス タイプ（Virus Types）] ページ

[ウイルス タイプ（Virus Types）] ページでは、ネットワークに浸入したウイルスおよびネットワークから送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、お使いのアプライアンスで稼働するウイルススキャンエンジンによって検出された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特定のアクションを実行することが推奨されます。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。

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。

[ウイルス タイプ（Virus Types）] ページには、ネットワークに浸入したウイルスおよび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。[検出した受信ウイルスの上位（Top Incoming Virus Detected）] セクションには、ネットワークに送信されたウイルスのチャート ビューが降順で表示されます。[検出した送信ウイルスの上位（Top Outgoing Virus Detected）] セクションには、ネットワークから送信されたウイルスのチャート ビューが降順で表示されます。

（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 タイプの詳細（Virus Types Details）] リストには、感染した送受信メッセージ、および感染メッセージの総数など特定のウイルスに関する情報が表示されます。感染した受信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した受信メッセージの総数が表示されます。同様に、送信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した送信メッセージの総数が表示されます。ウイルスの種類の詳細は、[受信メッセージ（Incoming Messages）]、[送信メッセージ（Outgoing Messages）]、または [感染したメッセージの合計数（Total Infected Messages）] 別にソートできます。

[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できません。
- [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。
- 各メッセージに関連付けることができる URL レピュテーション レベルは 1 つだけです。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許可リストの 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許可リストの 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。

[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に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、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。

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（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、システム時刻を協定世界時（UTC）と同期するようにしてください。

偽造メールの一致レポート

偽装メールの検出結果の監視 を参照してください。

ファイル レピュテーションおよびファイル分析レポート

次に示すレポートについては、ファイル レピュテーションおよびファイル分析のレポートとトラッキングを参照してください。

- 高度なマルウェア防御（Advanced Malware Protection）
- ファイル分析（File Analysis）
- AMP判定のアップデート（AMP Verdict Updates）

[メールボックスの自動修復（Mailbox Auto Remediation）] レポート

[メールボックスの自動修復レポート（Mailbox Auto Remediation report）]ページを使用して（[モニタ（Monitor）] > [メールボックスの自動修復（Mailbox Auto Remediation）]）、メールボックス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。

- 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
- メールボックス修復が成功または失敗した受信者について定義されているプロファイル名の一覧
- 修復が失敗した理由
- ドメインにマッピングされたプロファイルがない

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。

詳細については、メールボックスでのメッセージの修復を参照してください。

[TLS 接続（TLS Connections）] ページ

[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
- DANE がサポートされている TLS 接続に成功したパートナー
- DANE がサポートされている TLS 接続に失敗したパートナー
- 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
- DANE がサポートされている送信 TLS 接続に成功した割合
- DANE がサポートされている送信接続に失敗した割合

[TLS 接続（TLS Connections）] 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、成功/失敗した DANE 接続の量が表示されます。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）、暗号化されていない接続の総数、DANE 接続の総数（成功したか失敗したかに応じて）を表示できます。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。この表の下部にある [列（Columns）] リンクをクリックすることにより、カラムの表示/非表示を切り替えることができます。

[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

[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アプライアンス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アプライアンス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によるレート制限の設定、または既存のレート制限の変更については、メール フロー ポリシーを使用した着信メッセージのルールの定義を参照してください。

[システム容量（System Capacity）] ページ

[システム容量（System Capacity）]ページでは、ワーク キュー内のメッセージ数、ワーク キューで費やした平均時間、送受信メッセージ（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。

- アプライアンスが推奨キャパシティを超えて、設定の最適化または追加アプライアンスが必要になった時間
- 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
- 最も多くのリソースを使用したシステムの部分（トラブルシューティングを支援するため）

お使いのアプライアンスをモニタして、メッセージの量に対してキャパシティが適切であることを確認することが重要です。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、ワーク 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**：「通常」のメッセージ量と環境内での「異常」な増加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）]（37 ページ）および[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]（37 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、有害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。しかしワーク キューは、負荷のかかっているシステムを示す最良の指標であり、長く、頻繁なワーク 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。[ワーク キュー（WorkQueue）] ページを使用すると、ワーク キュー内でメッセージが費やした平均時間およびワーク 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）]（36 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。[システム容量（System Capacity）]：[システムの負荷（System Load）]（37 ページ） を参照してください。

関連項目

- [システム容量（System Capacity）]：[ワークキュー（Workqueue）]（36 ページ）
- [システム容量（System Capacity）]：[受信メール（Incoming Mail）]（37 ページ）
- [システム容量（System Capacity）]：[送信メール（Outgoing Mail）]（37 ページ）
- [システム容量（System Capacity）]：[システムの負荷（System Load）]（37 ページ）
- メモリ ページ スワッピングに関する注意事項（38 ページ）
- [システム容量（System Capacity）]：[すべて（All）]（38 ページ）

[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手順については、システム状態パラメータのしきい値の設定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）]

[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。結果を、指定した時間範囲に制限できます。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。[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ァイ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）]

[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、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。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。[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発信宛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）
- メモリページスワップ（Memory Page Swapping）
- リソース節約アクティビティ

全体のCPU使用率（Overall CPU Usage）

アプライアンスは、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、CPU使用率のしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定を参照してください。

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。このグラフには、メモリ ページ スワッピングのしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定を参照してください。

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、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 RCS 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。

メモリ ページ スワッピングに関する注意事項

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 スワッピングを行っている場合を除き、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 および C190 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。

[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 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。英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）を参照してください。

[システムステータス（System Status）] ページ

[システムステータス（System Status）] ページには、システムのすべてのリアルタイム メールおよび DNS アクティビティの詳細が表示されます。表示される情報は、CLI で status detail コマンドおよび **dnsstatus** コマンドを使用して入手できる情報と同じです。status detail コマンドの詳細については、CLIによる管理およびモニタリングの「詳細な電子メール ステータスのモニタリング」を参照してください。**dnsstatus** コマンドの詳細については、同章の「DNS ステータスの確認」を参照してください。

[システム ステータス（System Status）] ページは、[システム ステータス（System Status）]、[ゲージ（Gauges）]、[レート（Rates）]、および [カウンタ（Counters）] の 4 つのセクションで構成されます。

関連項目

- システム ステータス （39 ページ）
- ゲージ （40 ページ）
- レート （40 ページ）
- カウンタ （40 ページ）

システム ステータス

[システム ステータス（System Status）] セクションには、[メール システムのステータス（Mail System Status）] および [バージョン情報（Version Information）] が示されます。

関連項目

- メール システムのステータス（Mail System Status） （39 ページ）
- バージョン情報 （39 ページ）

メール システムのステータス（Mail System Status）

[メール システムのステータス（Mail System Status）] セクションには、次の情報が含まれます。

- システム ステータス（システム ステータスの詳細については、ステータス（Status） （8 ページ）を参照してください）。
- ステータスが報告された最終時刻。
- アプライアンスのアップタイム。
- システム内の最も古いメッセージ（配信用にまだキューに入っていないメッセージも含む）。

バージョン情報

[バージョン情報（Version Information）] セクションには、次の情報が含まれます。

- アプライアンスのモデル名。
- インストールされている AsyncOS オペレーティング システムのバージョンとビルド日。

- AsyncOS オペレーティング システムのインストール日。
- 接続先のシステムのシリアル番号。

この情報は、シスコ カスタマー サポートに問い合わせる場合に役立ちます。（テクニカル サポートの使用 を参照。）

ゲージ

[ゲージ（Gauges）] には、次のようにキューおよびリソース使用率について示されます。

- メール処理キュー（Mail Processing Queue）
- キュー内のアクティブ受信者（Active Recipients in Queue）
- キュー スペース（Queue Space）
- CPU 使用率

メール ゲートウェイ アプライアンスは、AsyncOS プロセスが消費している CPU 率を参照します。CASE は、アンチスパム スキャン エンジンおよびアウトブレイク フィルタ プロセスなど複数のアイテムを参照します。

- 一般的なリソース使用率（General Resource Utilization）
- ログに使用されているディスク容量（Logging Disk Utilization）

レート

[レート（Rates）] セクションには、次の受信者に関する処理率が示されます。

- メール処理レート（Mail Handling Rates）
- 処理済みの割合（Completion Rates）

カウンタ

クラウド E メール セキュリティ アプライアンスでは、カウンタをリセットしないようにすることを推奨します。

システム統計情報用の累積電子メール モニタリング カウンタをリセットし、カウンタの最終リセット日時を表示することができます。リセットは、システム カウンタおよびドメインごとのカウンタに影響します。リセットは、再試行スケジュールに関連する配信キュー内のメッセージのカウンタには影響しません。

（注） 管理者グループまたはオペレータ グループに属するユーザ アカウントのみが、カウンタをリセットできます。ゲスト グループ内で作成したユーザ アカウントでは、カウンタをリセットできません。詳細については、ユーザ アカウントを使用する作業を参照してください。

カウンタをリセットするには、[カウンタをリセット（Reset Counters）] をクリックします。このボタンは、CLI の **resetcounters** コマンドと同様の機能を提供します。詳細については、電子メール モニタリング カウンタのリセットを参照してください。

- メール処理イベント（Mail Handling Events）

- 処理済みイベント（Completion Events）
- ドメイン キー イベント（Domain Key Events）
- DNS ステータス（DNS Status）

[大容量のメール（High Volume Mail）] ページ

（注） [大容量のメール（High Volume Mail）] ページには、Header Repeats ルールを使用するメッセージ フィルタのデータだけが表示されます。

[大容量のメール（High Volume Mail）] ページには、次のレポートが横棒グラフの形式で表示されます。

- [上位件名（Top Subjects）]。このグラフから、AsyncOS が受信したメッセージの上位件名を確認できます。
- [上位エンベロープ送信者（Top Envelope Senders）]。このグラフから、AsyncOS が受信したメッセージの上位エンベロープ送信者を確認できます。
- [一致数別上位メッセージフィルタ（Top Message Filters by Number of Matches）]。このグラフから、一致数に基づく（Header Repeats ルールを使用する）上位メッセージ フィルタを確認できます。

[大容量のメール（High Volume Mail）] ページには、上位メッセージ フィルタと、該当するメッセージフィルタに一致したメッセージの数を示す表も表示されます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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するか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。

[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）] ページには、一致数の上位メッセージ フィルタ（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2種類の形式（棒グラフと表）で表示されます。

棒グラフでは、送受信メッセージによって最も多くトリガーされるメッセージフィルタを確認できます。表には、上位メッセージフィルタと、該当するメッセージフィルタに一致したメッセージの数が示されます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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するか、[印刷用（PDF）（Printable (PDF)）] リンクを使用して PDF 形式にエクスポートできます。

[Safe Print] ページ

[Safe Print] レポート ページを使用して、次の内容を表示できます。

- ファイル タイプ別の、Safe Print で出力された添付ファイルの数（グラフ形式）。
- ファイル タイプ別の、Safe Print で出力された添付ファイルの概要（表形式）。

[Safe Printで出力されたファイル種類の概要（Summary of Safe Print File Types）] セクションで Safe Print で出力された添付ファイルの合計数をクリックすると、[メッセージトラッキング（Message Tracking）] にメッセージの詳細が表示されます。

CSV データの取得

電子メール セキュリティ モニタで図やグラフの作成に使用されたデータは、CSV 形式で取得できます。CSV データにアクセスする方法は、次の 2 つです。

- **電子メールによる CSV レポートの配信**。電子メールで配信される、またはアーカイブされる CSV レポートを生成できます。この配信方法は、[レポート（Reports）] ページに表示される各表に関する個別レポートを必要とする場合、または内部ネットワークにアクセスできないユーザに CSV データを送信する場合に便利です。

  Comma-Separated Value（CSV; カンマ区切り）レポート タイプは、スケジュール設定されたレポートの表形式データを含む ASCII テキスト ファイルです。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。単一のレポートの複数の CSV ファイルは、単一の .zip ファイルに圧縮されて、アーカイブ ファイルの保存オプションを提供するか、個別の電子メール メッセージに添付されて電子メールで配信されます。

- **HTTP による CSV ファイルの取得**。電子メール セキュリティ モニタ機能で図やグラフの作成に使用されたデータは、HTTP を使用して取得できます。この配信方法は、他のツールを使用してデータの詳細分析を実行する予定の場合に役立ちます。たとえば、未加工データのダウンロード、処理、および他のシステムでの結果表示を行う自動スクリプトによって、データの取得を自動化できます。

関連項目

- 自動プロセスによる CSV データの取得 （42 ページ）

自動プロセスによる CSV データの取得

必要とする HTTP クエリーを最も容易に取得する方法は、必要な種類のデータを表示するように電子メール セキュリティ モニタ ページの 1 つを設定することです。次に、[エクスポート（Export）] リンクをコピーできます。これがダウンロード URL です。このようにデータ取得を自動化した場合、ダウンロード URL 内のパラメータを固定し、変更しないことが重要です（下記を参照）。

ダウンロード URL はコード化されるので、（適切な HTTP 認証を使用して）同じクエリーを実行し、同様のデータセットを取得できる外部スクリプトにコピーできます。このスクリプトでは、Basic HTTP 認証またはクッキー認証を使用できます。自動プロセスで CSV データを取得する場合は、次の事項に注意する必要があります。

- URL の再利用時に関する時間範囲の選択（過去 1 時間、1 日、1 週間など）。URL をコピーして「過去 1 日」の CSV データ セットを取得する場合、この URL を次に使用するときには、URL の再送信時から「過去 1 日」を対象とする新しいデータ セットを取得します。時間範囲の選択は保持され、CSV クエリ文字列（たとえば date_range=current_day）に表示されます。
- データセットのフィルタリングおよび分類の優先順位。フィルタは保持され、クエリー文字列に表示されます。レポートでは、フィルタはほとんど使用されません。1 つの例としては、発生レポートにおける「グローバル/ローカル」発生セレクタが挙げられます。
- CVS ダウンロードでは、選択した時間範囲について表内のデータのすべての行が返されます。
- CSV では、タイムスタンプおよびキーで指示された表内のデータの行が返されます。スプレッドシートアプリケーションを使用するなどして、別個のステップで更にソートできます。
- 最初の行には、レポートに示される表示名に一致するカラム見出しが含まれています。タイムスタンプ（タイムスタンプ （44 ページ）を参照）およびキー（オプション キー（Keys） （44 ページ）を参照）も表示されます。

関連項目

- URL のサンプル （43 ページ）
- Basic HTTP 認証クレデンシャルの追加 （43 ページ）
- ファイル形式（File Format） （44 ページ）
- タイムスタンプ （44 ページ）
- オプション キー（Keys） （44 ページ）
- ストリーミング （44 ページ）

URL のサンプル

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=
MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0
&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

Basic HTTP 認証クレデンシャルの追加

URL に Basic HTTP 認証クレデンシャルを指定する例を次に示します。

http://example.com/monitor/

次のようになります。

http://username:password@example.com/monitor/

ファイル形式（File Format）

ダウンロードされるファイルは CSV 形式であり、ファイル拡張子は .csv です。ファイル見出しは、デフォルトのファイル名であり、レポートの名前に始まり、レポートのセクションが続きます。

タイムスタンプ

データのストリーミングを行うエクスポートには、各行の時間「間隔」について開始タイムスタンプおよび終了タイムスタンプが示されます。2 種類の開始タイムスタンプおよび終了タイムスタンプ（数値形式および人間が読み取れる文字列形式）が提供されます。タイムスタンプは GMT 時間です。これにより、アプライアンスが複数の時間帯にある場合、ログの集約が容易になります。

あまりないことですが、データが他のソースのデータとマージされる場合には、エクスポートファイルにタイムスタンプは含まれません。たとえば、発生の詳細のエクスポートでは、レポートのデータと Threat Operations Center（TOC）データがマージされ、タイムスタンプが不適切になります。これは、間隔が存在しないためです。

オプション キー（Keys）

レポートにキーが表示されない場合であっても、エクスポートには、レポート テーブル キーが含まれます。キーが表示される場合、レポートに表示される表示名がカラム見出しとして使用されます。それ以外の場合は、「key0」、「key1」などのカラム見出しが表示されます。

ストリーミング

大部分のエクスポートでは、データをクライアントにストリーミングで戻します。これは、データ量が非常に大きい可能性があるからです。しかし、一部のエクスポートでは、ストリーミング データではなく結果セット全体を返します。通常、レポート データが非レポート データ（発生の詳細など）と集約される場合が該当します。

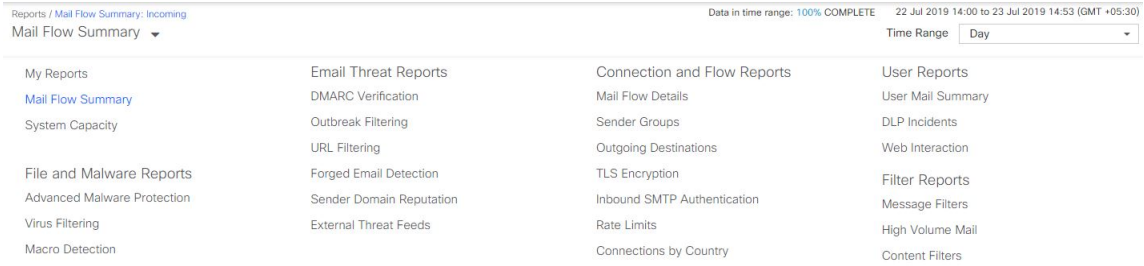
新しいWebインターフェイスの電子メールセキュリティモニタ ページ

新しい Web インターフェイスにログインするには、レガシー インターフェイスの [Eメールセキュリティアプライアンスの外観が新しくなりました。お試しください（Secure Email Gateway is getting a new look. Try it!!）] リンクをクリックします。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセスを参照してください。

次の図に示す [レポート（Reports）] ドロップダウンを使用すると、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 *1 : [*レポート（***Reports***）*]* ドロップダウン



GUI でこれらのページを使用して、アプライアンスのリスナーに接続しているドメインをモニタできます。お使いのアプライアンスの「メールフロー」のモニタ、ソート、分析、および分類を実行し、正規メールの大量送信者と「スパマー」（未承諾の商業用メールの大量送信者）またはウイルス送信者の疑いのあるユーザとを区別できます。これらのページは、システムへの着信接続のトラブルシューティングにも役立ちます（IP レピュテーションスコア、ドメインに対する直近の送信グループの一致など重要情報を含みます）。

これらのページは、アプライアンスに関連するメール、さらにゲートウェイの範囲を超えて存在するサービス（IP レピュテーションサービス、アンチスパム スキャン サービス、アンチウイルス スキャン セキュリティ サービス、コンテンツフィルタ、およびアウトブレイクフィルタ）に関連するメールの分類に役立ちます。

[エクスポート（Export）] リンクでは、グラフおよび他のデータを Comma Separated Value（CSV; カンマ区切り値）形式にエクスポートできます。

エクスポートされた CSV データは、アプライアンスでの設定にかかわらず、すべてのメッセージトラッキングおよびレポーティングデータを GMT で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数の時間帯にあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

（注） ローカライズされた CSV データをエクスポートする場合、一部のブラウザでは見出しが正しく表示されないことがあります。これは、ローカライズされたテキストに対して、一部のブラウザが適切な文字セットを使用していないためです。この問題を回避するには、ファイルをディスクに保存し、[ファイル（File）]>[開く（Open）] を使用して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 データのエクスポートの自動化の詳細については、CSV データの取得 （42 ページ）を参照してください。

電子メール セキュリティ モニタ ページのリスト

- [お気に入り レポート（My Favorite Reports）] ページ （48 ページ）
- [メール フロー概要（Mail Flow Summary）] ページ （51 ページ）
- [システム容量（System Capacity）] ページ （35 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

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

レポートに含まれるメッセージの詳細の表示

この機能は、レポートとトラッキングが両方ともローカルの場合（Cisco コンテンツ セキュリティ管理アプライアンスで中央管理されていない場合）にのみ、機能します。

手順

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）。

この番号に関連するメッセージがメッセージ トラッキングで表示されます。

ステップ 2 下にスクロールして、リストを表示します。

次のタスク

関連項目

- メッセージ トラッキングの検索結果の使用

レポートの時間範囲

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。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。

時間範囲は、次の表に記載のオプションから選択します。

表 *2:* 電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時間（Hour）	直近の 60 分 + 最大 5 分
日（Day）	直近の 24 時間と直近の 60 分
Week	直近の 7 日 + 当日の経過した時間
30 日（30 days）	直近の 30 日 + 当日の経過した時間
90 日（90 days）	直近の 90 日 + 当日の経過した時間
昨日（Yesterday）	00:00 ～ 23:59（午前 0 時～午後 11:59）
先月（Previous Calendar Month）	その月の最初の日の 00:00 ～その月の最後の日の 23:59
カスタム範囲（Custom Range）	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

[お気に入りレポート（My Favorite 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てカスタム レポート ページを作成できます。

目的	操作手順
[お気に入りレポート（My Favorite Reports）]ページへのモジュールの追加	参照先： • [マイレポート（My Reports）] ページに追加できないモジュール （49 ページ） • [お気に入りレポート（My Favorite Reports）] ページでのレポートの追加 （50 ページ）

目的	操作手順
[お気に入りレポート（My Favorite Reports）] ページの表示	1. [レポート（Reports）] ドロップダウンから [お気に入りレポート（My Favorite Reports）] を選択します。 2. 表示する時間範囲を選択します。選択した時間範囲は、[お気に入りレポート（My Favorite Reports）] ページのすべてのモジュールを含めて、すべてのレポートに適用されます。 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。 （注） 新しい Web インターフェイスの [お気に入りレポート（My Favorite Reports）] ページに追加するレポートモジュールは、レガシー Web インターフェイスに追加され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 ロールによって異なる場合もあります。
[お気に入りレポート（My Favorite Reports）] ページでのモジュールの再配置	[お気に入りレポート（My Favorite Reports）] ページで、モジュールを目的の場所にドラッグアンドドロップします。
[お気に入りレポート（My Favorite Reports）] ページからのモジュールの削除	次のいずれかの方法で、[お気に入りレポート（My Favorite Reports）] ページからレポートモジュールを削除できます。 • 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。 • [お気に入りレポート（My Favorite Reports）] ページに移動し、[お気に入りの管理（Manage Favorites）] を選択して該当するレポートモジュールを削除します。

[マイ レポート（My Reports）] ページに追加できないモジュール

- [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。

[お気に入りレポート（My Favorite 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 （49 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。

手順

ステップ 1 [お気に入りレポート（My Favorite Reports）] ページには、次のいずれかの方法で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（Reports）] ドロップダウンから [マイレポート（My Reports）] を選択し、[お気に入りの管理（Manage Favorites）] をクリックします。

  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 [お気に入りレポート（My Favorite Reports）] ページに追加します。[お気に入りレポート（My Favorites 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） [お気に入りレポート（My Favorite 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す。

ステップ 2 カスタマイズしたレポートモジュール（列を追加、削除、または順序変更したり、チャートにデフォルト以外のデータを表示するなど）を追加する場合は、[お気に入りレポート（My Favorite Reports）] ページでモジュールを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。

[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、アプライアンス上の電子メールメッセージ 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 （48 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 （46 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、カウンタを使用しての、トレンド グラフ上のデータのフィルタリング（57 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 （48 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、カウンタを使用しての、トレンド グラフ上のデータのフィルタリング （57 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 *3 : [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。
脅威メッセージ（Threat Messages）	[脅威メッセージ（Threat Messages）] グラフは、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）	[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。 • [接続およびIPレピュテーションのフィルタリング（Connection and IP 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。 • [スパム検出（Spam Detection）]：スパム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。 • [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。 • [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。 • [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。 • [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。

セクション	説明
コンテンツ サマリー（Content Summary）	[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。 • [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。 • [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。 • [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。
メール フロー概要：発信	
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（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。 • スパム検出（Spam Detected） • ウイルス検出（Virus Detected） • AMP で検出（Detected by AMP） • コンテンツ フィルタによる停止（Stopped by Content Filters） • DLP による停止（Stopped by DLP）

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 （54 ページ）
- 送受信のサマリーとグラフ （9 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 （55 ページ）
- 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 （57 ページ）

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、お使いのアプライアンスのオンラインヘルプまたはユーザーガイドで、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。

送受信のサマリーとグラフ

送受信のサマリーのセクションでは、システム上のすべてのメールアクティビティのリアルタイム アクティビティへのアクセスが提供され、送受信メールのグラフとメール サマリーで構成されています。ユーザは、[時間範囲（Time Range）] メニューを使用して報告対象となるタイムフレームを選択できます。選択したタイムフレームは、すべての電子メールセキュリティ モニタ ページで使用されます。メッセージの各タイプまたはカテゴリに関する説明は以下のとおりです（電子メールの分類 （10 ページ）を参照）。

メール トレンド グラフでは、メール フローが視覚的に表示されますが、サマリー テーブルでは、同じ情報の数値的な内訳が示されます。サマリー テーブルには、各メッセージ タイプの割合と実数（試行されたメッセージ、脅威メッセージ、クリーン メッセージの総数を含む）が含まれています。

送信グラフおよびサマリーでも、送信メールに関する同様の情報が示されます。

関連項目

- 電子メール セキュリティ モニタでのメッセージ集計に関する注意事項 （9 ページ）

電子メール セキュリティ モニタでのメッセージ集計に関する注意事項

電子メール セキュリティ モニタが着信メールの集計に使用する方法は、メッセージあたりの受信者の数によって異なります。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、この送信者からの 3 通として集計されます。

送信者レピュテーションフィルタ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 は着信メッセージの受信者のリストには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。この乗数はシスコによって算出されたもので、既存の顧客データの大規模なサンプリング研究に基づいています。

[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 *4 : [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	
レピュテーション フィルタリング	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。 [レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の値は、次の要素に基づいて算出されます。 • この送信者からの「調整された」メッセージの数。 • 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）。 • 接続ごとのメッセージ数に対する控えめな乗数。 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。 [メールフロー概要（Mail Flow Summary）] レポートページ上のレピュテーション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。
送信者ドメイン レピュテーション フィルタリング	送信者ドメインのレピュテーション判定に基づいてブロックされたメッセージの総数。

カテゴリ（Category）	説明
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。
ウイルス対策	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。 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。 • 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 • 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 • 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 • 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 • 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
高度なマルウェア防御	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。 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。
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。

カテゴリ（Category）	説明
メール フロー概要：発信	
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 （74 ページ）

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

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。

[システム容量（System Capacity）] ページ

[システム容量（System Capacity）]ページでは、ワーク キュー内のメッセージ数、ワーク キューで費やした平均時間、送受信メッセージ（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。

- アプライアンスが推奨キャパシティを超えて、設定の最適化または追加アプライアンスが必要になった時間
- 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
- 最も多くのリソースを使用したシステムの部分（トラブルシューティングを支援するため）

お使いのアプライアンスをモニタして、メッセージの量に対してキャパシティが適切であることを確認することが重要です。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、ワーク 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**：「通常」のメッセージ量と環境内での「異常」な増加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）]（37 ページ）および[システム容量（System Capacity）]：[送信メール（Outgoing Mail）]（37 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、有害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。しかしワーク キューは、負荷のかかっているシステムを示す最良の指標であり、長く、頻繁なワーク 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。[ワーク キュー（WorkQueue）] ページを使用すると、ワーク キュー内でメッセージが費やした平均時間およびワーク 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）]（36 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。[システム容量（System Capacity）]：[システムの負荷（System Load）]（37 ページ） を参照してください。

関連項目

- [システム容量（System Capacity）]：[ワークキュー（Workqueue）]（36 ページ）
- [システム容量（System Capacity）]：[受信メール（Incoming Mail）]（37 ページ）
- [システム容量（System Capacity）]：[送信メール（Outgoing Mail）]（37 ページ）
- [システム容量（System Capacity）]：[システムの負荷（System Load）]（37 ページ）
- メモリ ページ スワッピングに関する注意事項（38 ページ）
- [システム容量（System Capacity）]：[すべて（All）]（38 ページ）

[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手順については、システム状態パラメータのしきい値の設定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）]

[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。結果を、指定した時間範囲に制限できます。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。[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ァイ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）]

[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、着信メッセージの総サイズが示されます。結果を、指定した時間範囲に制限できます。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。[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発信宛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）
- メモリページスワップ（Memory Page Swapping）
- リソース節約アクティビティ

全体のCPU使用率（Overall CPU Usage）

アプライアンスは、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、CPU使用率のしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定を参照してください。

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。このグラフには、メモリ ページ スワッピングのしきい値レベルも表示されます。しきい値レベルを変更する場合は、Web インターフェイスで [システム管理（System Administration）] > [システムの状態（System Health）] ページを使用するか、CLI で **healthconfig** コマンドを使用します。システム状態パラメータのしきい値の設定を参照してください。

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、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 RCS 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。

メモリ ページ スワッピングに関する注意事項

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 スワッピングを行っている場合を除き、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 および C190 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。

[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 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。英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）を参照してください。

レポート データの有効性

[レポートデータの有効性（Reporting Data Availability）] ページでは、リソース使用率や電子メールトラフィックの障害発生場所をリアルタイムに確認できるようにデータを表示できます。

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。

[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、ユーザーガイドまたはEメール セキュリティ アプライアンスのAsyncOS 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 [ファイルおよびマルウェアのレポート（File 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）]（62 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）]（63 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] – [ファイル分析（File Analysis）]（64 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）]（65 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）]（65 ページ）

[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、『*Cisco Email Security Command Reference Guide*』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 （67 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 （67 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）]（63 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）]（64 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（Unscanable）]、[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ロックリストに登録されているファイル 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ロックリストに登録されているファイル SHA の割合。AMP for Endpoints コンソールから取得されたブロックリストに登録されるファイル 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いてブロックリストに登録されているファイル SHA の割合。

レポートの [詳細（More Details）] セクションのリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリの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。アプライアンスは 30 分ごとに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展開の場合：AMP Threat Grid アプライアンスで許可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。許可リストについては、AMP Threat Grid のドキュメント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 （67 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。

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。

- 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
- メールボックス修復が成功または失敗した受信者について定義されているプロファイル名の一覧
- 修復が失敗した理由
- ドメインにマッピングされたプロファイルがない

[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。

- 無効なメールボックス：受信者が有効な Microsoft Exchange Online ユーザまたは Microsoft Exchange オンプレミスユーザではないか、アプライアンスに設定された Microsoft Exchange Online または Microsoft Exchange オンプレミスの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。
- 認証エラー：Microsoft Exchange オンプレミスのメールボックスに接続するためにアプライアンスで指定されたユーザアカウントが正しくない。
- 接続エラー：アプライアンスが修復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 Microsoft Exchange Online または Microsoft Exchange オンプレミスサービスとの間に接続の問題が発生した。
- 権限に関するエラー：
  - Microsoft Exchange オンプレミスアカウントの場合、Microsoft Exchange オンプレミスのメールボックスに接続するためにアプライアンスで指定されたユーザアカウントに偽装ロールが割り当てられていない。
  - Microsoft Exchange Online アカウントの場合、Office 365 アプリケーションに、受信者のメールボックスにアクセスするために必要な権限がない。
- ドメインにプロファイルがマッピングされていない：受信者ドメインにマッピングされたプロファイルがない。
- メールボックスがアクセス不能または無効：
  - メールボックスへのアクセスに使用されるアカウント プロファイルのプロファイル タイプが正しくない。
  - 受信者が有効な Microsoft Exchange Online ユーザまたは Microsoft Exchange オンプレミス ユーザではない。
  - 受信者が、アプライアンスに設定された Microsoft Exchange Online または Microsoft Exchange オンプレミスのドメインアカウントに属していない。

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。

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を処理する場合、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を処理する場合、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。追加の列を表示するには、テーブルの右上にある [列をカスタマイズ（Customize Columns）] アイコンをクリックします。

[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）] ページでは、ネットワークに浸入したウイルスおよびネットワークから送信されたウイルスの概要が示されます。[ウイルスフィルタリング（Virus Filtering）] ページには、お使いのアプライアンスで稼働するウイルススキャンエンジンによって検出された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特定のアクションを実行することが推奨されます。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。

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）] 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。

[ウイルスフィルタリング（Virus Filtering）] ページには、ネットワークに侵入したウイルスおよび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。[検出した受信ウイルスの上位（Top Incoming Virus Detected）] セクションには、ネットワークに送信されたウイルスのチャート ビューが降順で表示されます。[検出した送信ウイルスの上位（Top Outgoing Virus Detected）] セクションには、ネットワークから送信されたウイルスのチャート ビューが降順で表示されます。

（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 タイプの詳細（Virus Types Details）] リストには、感染した送受信メッセージ、および感染メッセージの総数など特定のウイルスに関する情報が表示されます。感染した受信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した受信メッセージの総数が表示されます。同様に、送信メッセージの詳細リストには、ウイルスの名前およびこのウイルスに感染した送信メッセージの総数が表示されます。ウイルスの種類の詳細は、[受信メッセージ（Incoming Messages）]、[送信メッセージ（Outgoing Messages）]、または [感染したメッセージの合計数（Total Infected Messages）] 別にソートできます。

[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および概要（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および概要（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。

アプライアンスで [マクロ検出（Macro Detection）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから **[マクロ検出（Macro Detection）]** を選択します。

（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）] ページには、DMARC 検証が失敗した上位のドメインと、DMARC 検証に失敗したメッセージに対して AsyncOS が実行したアクションの詳細情報が表示されます。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。

- 最も多く DMARC 準拠ではないメッセージを送信したドメインはどれか。
- 各ドメインで、DMARC 検証に失敗したメッセージに対して AsyncOS がどのようなアクションを実行したか。

[DMARC検証（DMARC Verification）] ページの内容は次のとおりです。

- DMARC 検証の失敗数に基づく上位ドメインを示すグラフ表示。
- ドメイン別に次の情報を示す表。
  - アクションなしで承認、隔離、または拒否されたメッセージの数。数値をクリックすると、選択されているカテゴリのメッセージのリストが表示されます。
  - DMARC 検証に合格したメッセージの数。
  - DMARC 検証試行回数の合計。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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。

[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できません。
- [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。
- 各メッセージに関連付けることができる URL レピュテーション レベルは 1 つだけです。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許可リストの 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許可リストの 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。

[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す。

[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

[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、[レポート（Reports）] ドロップダウンから [アウトブレイクフィルタリング（Outbreak Filtering）] を選択します。

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 *5 : [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。
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。

セクション	説明
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。
着信メッセージからのヒット メッセージ	[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。 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。
脅威レベル別のヒット メッセージ	[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。 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、お使いのアプライアンスのオンラインヘルプまたはユーザーガイドを参照してください。
アウトブレイク検疫内のメッセージ	[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。 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。

セクション	説明
書き換えられた上位 URL	[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。 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。 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。

（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。

[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、[レポート（Reports）] ドロップダウンから [偽装メールの検出（Forged Email Detection）] を選択します。

[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。

[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。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。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。

[送信者ドメインのレピュテーション（SenderDomainReputation）]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に基づく着信メッセージ（グラフ形式）。

（注） SDR 判定が「Untrusted」または「Questionable」メッセージのみが、「Spam」や「Malicious」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、[レポート（Reports）] ドロップダウンから [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。

[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。

[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、[レポート（Reports）] ドロップダウンから [外部脅威フィード（External Threat Feeds）] を選択します。

[メール フローの詳細（Mail Flow Details）] ページ

[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。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。

[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、[レポート（Reports）] ドロップダウンから [メールフローの詳細（Mail Flow Details）] を選択します。

[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 （46 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 （77 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 （82 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

- [受信メール（Incoming Mails）] テーブル （77 ページ）
- [ドメイン情報がありません（No Domain Information）] （76 ページ）
- レポートの時間範囲 （48 ページ）
- メール フローの詳細ページ内のビュー （75 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 （81 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、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 [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 （77 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。

（注） [メールフローの詳細（Mail Flow Details）] 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。スケジュール設定されたレポート （98 ページ）を参照してください。

[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 （82 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）]

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されないホストは、送信者の検証によって管理できます。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。

リストに表示される送信者の数は、[表示された項目（Items Displayed）] メニューから選択できます。

レポートの時間範囲

電子メール セキュリティ モニタ機能は、ゲートウェイに流入するメールに関するデータを常に記録します。データは 60 秒ごとに更新されますが、システムに表示されるデータは、現在のシステム時間よりも 120 秒遅れます。表示される結果に含める時間範囲を指定できます。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。

時間範囲は、次の表に記載のオプションから選択します。

表 *6*：電子メール セキュリティ モニタ機能で使用可能な時間範囲

GUI で選択した時間範囲	定義
時間（Hour）	直近の 60 分 + 最大 5 分
日（Day）	直近の 24 時間と直近の 60 分
Week	直近の 7 日 + 当日の経過した時間
30 日（30 days）	直近の 30 日 + 当日の経過した時間
90 日（90 days）	直近の 90 日 + 当日の経過した時間
昨日（Yesterday）	00:00 ～ 23:59（午前 0 時～午後 11:59）
先月（Previous Calendar Month）	その月の最初の日の 00:00 ～その月の最後の日の 23:59
カスタム範囲（Custom Range）	指定した開始の日付と時間および終了の日付と時間で囲まれた範囲

[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、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。

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、アプライアンスのユーザー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、IP 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 （81 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 レポート （83 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 7: [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。
IP レピュテーションスコア（IP アドレス）	送信者の IP レピュテーションスコア
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。

列名	説明
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。
[レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）]	[レピュテーションフィルタによる停止（Stopped by IP Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • この送信者からの「数が絞り込まれた」メッセージの数 • 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） • 接続ごとのメッセージ数に対する控えめな乗数。 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。 （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（IP 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。

列名	説明
[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。 （注） 電子メールゲートウェイは、「失敗 - 拒否」、「失敗 - 隔離」、および「失敗 - アクションなし」の結果に基づいて、「DMARC による停止」メッセージの総数を表示します。
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
マーケティング（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。

[送信者プロファイル（Sender Profile）] ページ

[受信メール（Incoming Mail Details] 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、[送信者プロファイル（Sender Profile）] ページが表示されます。ここには、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）の詳細情報が表示されます。[受信メール（Incoming Mail）] ページまたは他の [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 [送信者プロファイル（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ァイル 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 [送信者プロファイル（Sender Profile）] ページには、詳細なリストが含まれません。）[送信者プロファイル（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 アドレスのみに関する情報が含まれます。

各 [送信者プロファイル（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。

- IP 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ァイル 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）
- IP レピュテーションスコア（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）

IP レピュテーションサービスによって提供されるすべての情報が記載された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、組織プロファイ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、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 *8 : [*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。
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

[送信先（Outgoing Destinations）]ページには、メールの送信先ドメインに関する情報が示されます。このページは、2つのセクションで構成されます。ページの上部は、発信脅威メッセージ別の上位宛先および発信クリーンメッセージの上位宛先を示すグラフで構成されます。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）全カラムを示す表が表示されます。

レポート対象の時間範囲（日、週、またはカスタムの範囲など）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。

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

- アプライアンスのメール送信先
- 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スされたメッセージの数

[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
- DANEがサポートされているTLS接続に成功したパートナー
- DANEがサポートされているTLS接続に失敗したパートナー
- 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
- DANEがサポートされている送信TLS接続に成功した割合
- DANEがサポートされている送信接続に失敗した割合

[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、成功/失敗した DANE 接続の量が表示されます。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）、暗号化されていない接続の総数、DANE 接続の総数（成功したか失敗したかに応じて）を表示できます。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。

[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

[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アプライアンス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アプライアンス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。ページ上部のタブを使用して、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によるレート制限の設定、または既存のレート制限の変更については、メール フロー ポリシーを使用した着信メッセージのルールの定義を参照してください。

[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の合計数（表形式）。

特定の位置情報の受信メールの接続の数をクリックすると、メッセージ トラッキングに関連メッセージを表示できます。

[合計メッセージ数（Total Messages）] 列には、SMTP 接続レベルで受け入れられるメッセージのみ表示されます。

（注） レポート生成中に次の処理が発生します。

- プライベート IP アドレスとして 1 つ以上の受信メール接続が検出されると、受信メール接続がレポートの「プライベート IP アドレス」として分類されます。
- 有効ではない IP レピュテーションスコアとして 1 つ以上の受信メール接続が検出されると、その受信メール接続はレポートで「国情報なし」に分類されます。

[ユーザー メール サマリー（User Mail Summary）] ページ

[ユーザメール概要（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。
- ユーザー 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 [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）] （88 ページ）
- 特定の内部ユーザの検索 （23 ページ）

[ユーザメールフローの詳細（User Mail Flow Details）]

[ユーザメールフローの詳細（User Mail Flow Details）] セクションでは、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受信停止（Stopped By Content Filter）]、[グレイメール検出（Graymail Detected）]、および [正常（Clean）]）のメッセージ数を示す送受信メッセージの内訳など指定したユーザに関する詳細情報が示されます。着信メッセージの場合は、必要に応じて、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）] 列を表示できます。この値は、ファイル レピュテーション フィルタリングにより悪意のあるファイルと判断された添付ファイルを含むメッセージの数を表します。この値には、判定のアップデートまたはファイル分析により悪意があるファイルとして検出されたファイルは含まれません。送受信コンテンツ フィルタおよび DLP ポリシーの一致も示されます。

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（25 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ユーザのリストも取得できます。

特定の内部ユーザの検索

特定の内部ユーザ（電子メール アドレス）は、[ユーザメール概要（User Mail Summary）] ページの下部にある検索フォームから検索できます。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.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。アプライアンスでは、[送信メールポリシー（Outgoing Mail Policies）] テーブルでイネーブルにした 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 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）] ページは、次の 2 つの主なセクションで構成されます。

- 重大度（[低（Low）]、[中（Medium）]、[高（High）]、[クリティカル（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 Incidents Details）] リスト

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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。英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）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。

関連項目

- [DLPインシデントの詳細（DLP Incident Details）] （90 ページ）
- [DLP ポリシー詳細（DLP Policy Detail）] ページ （90 ページ）

[DLPインシデントの詳細（DLP Incident Details）]

アプライアンスの送信メールポリシーで現在イネーブルの DLP ポリシーは、[DLPインシデントの詳細（DLP Incident Details）]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。

[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 インシデントの合計数と、重大度レベル別の内訳を示します。重大度レベルには、バウンスされたメッセージの数と、クリアで配信、暗号化で配信、または削除されたメッセージの数も含まれます。データをソートするには、列見出しをクリックします。

[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）] リストも含まれます。このリストには、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）] リストを使用すると、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検索できます。

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、#unique_1492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 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に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、システム時刻を協定世界時（UTC）と同期するようにしてください。

[修復レポート（Remediation Report）] ページ

[修復レポート（Remediation Report）] を使用して、[メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] の修復結果をモニタできます。

このレポートを使用して、以下のことを行います。

- [メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] で試行されたメッセージの一覧を表示する。
- 修復失敗の理由を把握する。たとえば、接続エラー、認証エラーなどです。

次のリストでは、[レート期限（Rate Limit）] レポートのさまざまなセクションについて説明します。

セクション	説明
要約	[概要（Summary）] セクションには、次の情報が表示されます。 • [メールボックスの自動修復（Mailbox Auto Remediation）] と [メールボックスの検索と修復（Mailbox Search and Remediate）] を使用して修復が試行されたメッセージの合計数。 • 設定された修正アクションに対して正常に修復されたメッセージの数。 • 修復が失敗したメッセージの数。

セクション	説明
[メールボックスの自動修復（Mailbox Auto Remediation）]	[メールボックス自動修復（Mailbox Auto Remediation）] レポートセクションには、次の情報が表示されます。 • メールボックス自動修復が成功または失敗した受信者の一覧。 • メッセージに対して行われた自動修復アクション。 • SHA-256 ハッシュに関連付けられているファイル名。SHA-256 ハッシュをクリックして、[メッセージトラッキング（Message Tracking）] ページ内の関連メッセージを表示します。 • メールボックスの自動修復が成功または失敗した受信者に定義されたプロファイル名の一覧。 • 自動修復に失敗した理由。

[メールボックスの検索と修復（Mailbox Search and Remediate）]	[メールボックスの検索と修復（Mailbox Search and Remediate）] セクションには、次の詳細情報が表示されます。
	• 進行中または完了した修復バッチの一覧。
	• バッチ内のメッセージの修復ステータス。
	• バッチ名とバッチ ID。バッチの詳細を表示するには、バッチ名をクリックします。
	  • メールボックスの検索と修復が開始された日時。
	  • メールボックスの検索と修復が開始された送信元。
	  • メールボックスの検索と修復を開始したホスト。
	  • メッセージに対して実行された修復アクション。
	  • メッセージの Cisco IronPort メッセージ ID。
	  • メッセージが正常に修復される前に、メッセージが受信者によって読み取られたかどうかを示す開封確認アイコン。
	  • 特定のバッチ内のメッセージの修復ステータス（[成功（Success）]、[失敗（Failed）]、または [進行中（In Progress）]）。
	  • メッセージを送信した送信者の電子メールアドレス。
	  • メッセージが配信され、その後で修復が試行された受信者の電子メールアドレス。
	  • メッセージが受信者に送信された日付と時刻。

[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）] ページには、一致数の上位メッセージ フィルタ（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2種類の形式（棒グラフと表）で表示されます。

棒グラフでは、送受信メッセージによって最も多くトリガーされるメッセージフィルタを確認できます。表には、上位メッセージフィルタと、該当するメッセージフィルタに一致したメッセージの数が示されます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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。

[大容量のメール（High Volume Mail）] ページ

（注） [大容量のメール（High Volume Mail）] ページには、Header Repeats ルールを使用するメッセージ フィルタのデータだけが表示されます。

[大容量のメール（High Volume Mail）] ページには、次のレポートが横棒グラフの形式で表示されます。

- [上位件名（Top Subjects）]。このグラフから、AsyncOS が受信したメッセージの上位件名を確認できます。
- [上位エンベロープ送信者（Top Envelope Senders）]。このグラフから、AsyncOS が受信したメッセージの上位エンベロープ送信者を確認できます。
- [一致数別上位メッセージフィルタ（Top Message Filters by Number of Matches）]。このグラフから、一致数に基づく（Header Repeats ルールを使用する）上位メッセージ フィルタを確認できます。

[大容量のメール（High Volume Mail）] ページには、上位メッセージ フィルタと、該当するメッセージフィルタに一致したメッセージの数を示す表も表示されます。数値をクリックすると、メッセージトラッキングを使用してその数に含まれているすべてのメッセージのリストが表示されます。

レポート対象の時間範囲（時間や週など）、またはカスタムの範囲を選択できます。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。

[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）] 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2種類の形式（棒グラフとリスト）で表示されます。[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

リストのコンテンツ フィルタ名をクリックすると、[コンテンツフィルタの詳細（Content Filter Details）] ページにこのフィルタに関する詳細を表示できます。

関連項目

- コンテンツ フィルタの詳細 （95 ページ）

コンテンツ フィルタの詳細

コンテンツ フィルタ名リンクをクリックすると、コンテンツ フィルタの詳細が表示されます。[コンテンツ フィルタの詳細（Content Filter Details）] 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 Users）] セクションでは、ユーザ名をクリックして内部ユーザ（電子メール アドレス）の [内部ユーザの詳細（Internal User Details）] ページを表示できます（#unique_1492を参照）。

[Safe Print] ページ

[Safe Print] レポート ページを使用して、次の内容を表示できます。

- ファイル タイプ別の、Safe Print で出力された添付ファイルの数（グラフ形式）。
- ファイル タイプ別の、Safe Print で出力された添付ファイルの概要（表形式）。

[Safe Printで出力されたファイル種類の概要（Summary of Safe Print File Types）] セクションで Safe Print で出力された添付ファイルの合計数をクリックすると、[メッセージトラッキング（Message Tracking）] にメッセージの詳細が表示されます。

[高度なフィッシング防御レポート（Advanced Phishing Protection Reports）] ページ

[レポート（Reports）]>[メールフロー概要（Mail Flow Summary）]>[高度なフィッシング防御（Advanced Phishing Protection] レポートページには、次の情報が表示されます。

- Cisco Advanced Phishing Protection クラウドサービスに正常に転送されたメッセージの合計数。
- Cisco Advanced Phishing Protection クラウドサービスに転送されなかったメッセージの合計数。

（注） メッセージメタデータの転送に失敗した場合は、高度なフィッシング防御機能の設定を検証する必要があります。詳細については、電子メールゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合方法を参照してください。

[高度なフィッシングからの保護（Advanced Phishing Protection）] レポートページを使用すると、次の情報を確認できます。

- ダッシュボードで組織レベルのすべてのアプライアンスから Cisco Advanced Phishing Protection クラウドサービスに送信されたメッセージの合計数。
- Cisco Advanced Phishing Protection クラウドサービスへの転送を試行したメッセージの総数（グラフィック形式）

Cisco Advanced Phishing Protection クラウドサービスに転送されるメッセージのメタデータの詳細情報を表示するには、リンクをクリックして Cisco Advanced Phishing Protection クラウドサービスにログインします。詳細については、Cisco Advanced Phishing Protection クラウドサービスでのメッセージメタデータのモニタリングを参照してください。

レポート作成の概要

AsyncOS におけるレポーティングには、次の 3 つの基本動作が含まれます。

- 日単位、週単位、または月単位で実行されるスケジュール設定されたレポートを作成できます。
- ただちにレポートを生成できます（「オンデマンド」レポート）。
- 以前実行したレポートのアーカイブ版を表示できます（スケジュール設定されたレポートおよびオンデマンド レポートの両方）。

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、[モニタ（Monitor）] > [定期レポート（Scheduled Reports）] ページから設定できます。アーカイブ済みレポートは、[モニタ（Monitor）] > [アーカイブ レポート（Archived Reports）] ページから表示できます。

アプライアンスは、生成した最新のレポートを保持します（すべてのレポートに対して、最大で合計 1000 バージョン）。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 リストを作成する方が容易です。

デフォルトでは、スケジュール設定された各レポートのうち、直近の 12 のレポートがアプライアンスにアーカイブされます。レポートは、アプライアンスの /saved_reports ディレクトリに保管されます。（詳細については、FTP、SSH、および SCP アクセスを参照してください。）

関連項目

- スケジュール設定されたレポートまたはアーカイブ レポートのタイプ （96 ページ）
- レポート用返信アドレスの設定 （98 ページ）

スケジュール設定されたレポートまたはアーカイブレポートのタイプ

次のレポートの種類から選択できます。

- AMP レピュテーション

- [高度なマルウェア防御（Advanced Malware Protection）] におけるファイル分析
- [高度なマルウェア防御（Advanced Malware Protection）] におけるファイルレトロスペクション
- 国別の接続
- コンテンツ フィルタ
- DLP インシデント サマリー
- DMARC 検証レポート
- 成功もしくは失敗（Delivery Status）
- 要約
- 外部脅威フィード
- 偽装メールの検出
- 大容量のメール
- 受信 SMTP 認証
- マクロ検出
- メール フローの概要：着信
- メールボックスの自動修復
- メールフローの詳細（発信送信者：ドメイン）
- メール フロー概要：発信
- メッセージ フィルタ
- 電子メール レポート
- 発信先
- レート制限
- 送信者ドメインのレピュテーション
- 送信者グループ
- システム容量
- TLS 暗号化
- ユーザメール概要（User Mail Summary）
- URL フィルタリング
- アウトブレイク フィルタ
- ウイルス フィルタリング
- Web インタラクション

各レポートは、対応する電子メール セキュリティ モニタ ページのサマリーで構成されます。

関連項目

- レポートに関する注意事項 （97 ページ）

レポートに関する注意事項

PDF 形式のコンテンツ フィルタ レポートは、最大 40 のコンテンツ フィルタに制限されます。完全なリストは、CSV 形式のレポートで入手できます。

（注） Windows コンピュータ上で中国語、日本語、または韓国語の PDF を生成するには、Adobe.com から該当するフォント パックをダウンロードしてローカル コンピュータにインストールすることも必要です。

レポート用返信アドレスの設定

レポートに返信アドレスを設定するには、アプライアンスに生成されるメッセージの返信アドレスの設定を参照してください。CLI から、**addressconfig** コマンドを使用します。

レポートの管理

アーカイブ済みのスケジュール設定されたレポートは、作成、編集、削除、および表示を行うことができます。ただちにレポートを実行することもできます（オンデマンド レポート）。これらのレポートの管理および表示については、後述します。

（注） クラスタ モードでは、レポートを表示できません。マシン モードの場合、レポートを表示できます。

[モニタ（Monitor）] > [定期レポート（Scheduled Reports）] ページには、アプライアンスで生成済みのスケジュール設定されたレポートのリストが示されます。

関連項目

- スケジュール設定されたレポート （98 ページ）
- アーカイブ レポート （100 ページ）

スケジュール設定されたレポート

スケジュール設定されたレポートは、日単位、週単位、または月単位で実行するようにスケジュール設定できます。レポートを実行する時間を選択できます。レポートを実行する時間には関係なく、指定した期間（たとえば、過去 3 日または前の 1 か月）のデータのみが含まれます。午前 1 時に実行するようにスケジュール設定されている日単位のレポートには、前の日（午前 0 時～午前 0 時）のデータが含まれることに注意してください。

お使いのアプライアンスは、デフォルトのレポートセットがスケジュール設定された状態で出荷されています。このレポートセットのいずれかを使用したり、変更や削除を行ったりすることができます。

関連項目

- 自動的に生成するレポートのスケジュール （99 ページ）

• スケジュール設定されたレポートの編集 （100 ページ）
• スケジュール設定されたレポートの削除 （100 ページ）

自動的に生成するレポートのスケジュール

手順

ステップ 1 [モニタ（Monitor）] > [定期レポート（Scheduled Reports）] ページで、[定期レポートを追加（Add Scheduled Report）] をクリックします。

ステップ 2 レポートの種類を選択します。選択したレポートの種類に応じて、異なるオプションを使用できます。

使用可能なスケジュール設定されたレポートの種類の詳細については、スケジュール設定されたレポートまたはアーカイブ レポートのタイプ （96 ページ）を参照してください。

ステップ 3 レポートのわかりやすいタイトルを入力します。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 4 レポート データの時間範囲を選択します（アウトブレイク フィルタ レポートでは、このオプションを使用できません）。

ステップ 5 レポートの形式を選択します。

- 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。

  英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）を参照してください。

- CSV。カンマ区切りの表データを含む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 6 使用可能な場合は、レポート オプションを指定します。レポートによっては、レポート オプションはありません。

ステップ 7 スケジュールおよび配信オプションを指定します。電子メールアドレスを指定しない場合、レポートはアーカイブされますが、いずれの受信者にも送信されません。

（注） 外部アカウント（Yahoo や Gmail など）にレポートを送信する場合、外部アカウントの許可リストにレポーティング返信アドレスを追加して、レポートの電子メールが誤ってスパムに分類されないようにしてください。

ステップ 8 [送信（Submit）] をクリックします。変更を保存します。

スケジュール設定されたレポートの編集

手順

ステップ 1 [サービス（Services）] > [集約管理レポート（Centralized Reporting）] ページでリストのレポート タイトルをクリックします。

ステップ 2 変更を行います。

ステップ 3 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削除

手順

ステップ 1 [サービス（Services）] > [集約管理レポート（Centralized Reporting）] ページで、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。

（注） スケジュール設定されたレポートをすべて削除するには、[すべて（All）] チェックボックスをオンにします。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 削除を確認し、変更内容を確定させます。

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。

アーカイブ レポート

[モニタ（Monitor）] > [アーカイブレポート（Archived Reports）] ページでは、使用可能なアーカイブ済みのレポートのリストが表示されます。[レポートのタイトル（Report Title）] カラムの名前をクリックすると、レポートを表示できます。[今すぐレポートを生成（Generate Report Now）] をクリックすると、ただちにレポートを生成できます。

リストに表示されるレポートの種類をフィルタリングするには、[表示（Show）] メニューを使用します。リストをソートするには、カラム見出しをクリックします。

アーカイブ済みのレポートは、自動的に削除されます。スケジュール設定された各レポートの最大 30 インスタンス（最大 1000 レポート）が保存され、新たなレポートが追加されると、古いレポートが削除されてレポートの数は 1000 に維持されます。30 インスタンスという制限は、レポートの種類に対してではなく、個別のスケジュール設定された各レポートに対して適用されます。

関連項目

- オンデマンド レポートの生成 （101 ページ）

オンデマンド レポートの生成

レポートは、スケジュールを設定しなくても生成できます。これらのオンデマンド レポートも指定したタイム フレームに基づいていますが、ただちに生成できます。

手順

ステップ 1 [アーカイブ レポート（Archived Reports）] ページで [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 レポートの種類を選択し、必要に応じてタイトルを編集します。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。

使用可能なスケジュール設定されたレポートの種類の詳細については、スケジュール設定されたレポートまたはアーカイブ レポートのタイプ （96 ページ）を参照してください。

ステップ 3 レポート データの時間範囲を選択します（ウイルス発生レポートでは、このオプションを使用できません）。

カスタムの範囲を作成した場合は、その範囲がリンクとして表示されます。範囲を変更するには、そのリンクをクリックします。

ステップ 4 レポートの形式を選択します。

- 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。

  英語以外の言語での PDF の生成については、レポートに関する注意事項 （97 ページ）を参照してください。

- CSV。カンマ区切りの表データを含む 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。任意のレポート オプションを指定します。

ステップ 5 レポートをアーカイブするかどうかを選択します（アーカイブする場合には、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）。

ステップ 6 レポートを電子メールで送信するかどうか、レポートの送信先の電子メール アドレスを指定します。

ステップ 7 [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、受信者に配信するか、このレポートをアーカイブします。

ステップ 8 変更を保存します。

メール レポートのトラブルシューティング

メッセージ トラッキングへのリンクが予期しない結果になる

問題

メッセージ トラッキングで詳細情報を表示するためにドリル ダウンすると、予期しない結果が表示されます。

解決方法

これはレポーティングおよびメッセージトラッキングが同時にイネーブルにされていない、正常に動作していない、そして（セキュリティ管理アプライアンス上に集中的に保存するのではなく）データをローカルに保存している場合に発生する可能性があります。各機能のデータ（レポートおよびメッセージトラッキング）は、他の機能（レポートまたはメッセージトラッキング）がイネーブルおよび動作しているかどうかに関係なく、機能がイネーブルにされてアプライアンス上で動作している間のみ保存されます。そのため、レポートにはメッセージ トラッキングで使用できないデータが含まれることがあり、その反対も起こり得ます。

クラウド内のファイル分析の詳細が完全でない

問題

パブリッククラウド内の完全なファイル分析結果は、組織のその他のアプライアンスからアップロードされたファイルでは取得できません。

解決方法

ファイルの分析結果データを共有するすべてのアプライアンスをグループ化してください。（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定を参照してください。この設定は、グループの各アプライアンスで実行する必要があります。

翻訳について
このドキュメントは、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。