中央集中型の電子メール セキュリティ レポーティングの使用

この章は、次の項で構成されています。

中央集中型の電子メール レポーティングの概要

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

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

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

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

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

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

中央集中型の電子メール レポーティングの設定

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

1. 中央集中型電子メール レポーティングの有効化 （3 ページ）
2. （レガシー Web インターフェイスのみ） 電子メール レポーティング グループの作成 （3 ページ）。
3. 管理対象の各 E メール セキュリティ アプライアンスへの中央集中型電子メール レポーティング サービスの追加 （4 ページ）
4. E メール セキュリティ アプライアンスでの中央集中型の電子メール レポーティングの有効化 （5 ページ）

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

中央集中型電子メールレポーティングの有効化

レガシーWebインターフェイスでの中央集中型電子メールレポーティングの有効化

始める前に

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

ステップ 1 **[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [メール（Email）] > [集約管理レポート（Centralized Reporting）]** を選択します。

ステップ 2 [有効化（Enable）] をクリックします。

ステップ 3 システム セットアップ ウィザードを実行してから初めて中央集中型電子メール レポーティングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 4 変更を送信し、保存します。

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

電子メール レポーティング グループの作成

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

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

始める前に

（注） このセクションは、レガシー Web インターフェイスにのみ適用されます。

各アプライアンスで中央集中型レポーティングがイネーブルになっていることを確認します。管理対象の各 E メール セキュリティ アプライアンスへの中央集中型電子メール レポーティング サービスの追加 （4 ページ）を参照してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [集約管理レポート（Centralized Reporting）] を選択します。

ステップ 3 [グループの追加（Add Group）] をクリックします。

ステップ 4 グループの一意の名前を入力します。

E メール セキュリティ アプライアンスのリストには、セキュリティ管理アプライアンスに追加した E メール セキュリティ アプライアンスが表示されます。グループに追加するアプライアンスを選択します。

追加できるグループの最大数は、接続可能な電子メール アプライアンスの最大数以下です。

（注） E メール セキュリティ アプライアンスをセキュリティ管理アプライアンスに追加したものの、それがリストに表示されない場合は、セキュリティ管理アプライアンスが E メール セキュリティ アプライアンスからレポーティング データを収集するように、その E メール セキュリティ アプライアンスの設定を編集します。

ステップ 5 [追加（Add）] をクリックして、[グループメンバー（Group Members）] リストにアプライアンスを追加します。

ステップ 6 変更を送信し、保存します。

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

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

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

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

ステップ 3 このページのリストに、すでにEメールセキュリティアプライアンスを追加している場合は、次の手順を実行します。

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

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

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

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

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

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

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

ステップ 5 [送信（Submit）] をクリックします。

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

ステップ 7 変更を保存します。

次のタスク

E メール セキュリティ アプライアンスでの中央集中型の電子メール レポーティングの有効化（5 ページ）

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

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

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

電子メール レポート データの操作

- レポート データのアクセスおよび表示に関するオプションついては、レポート データの表示方法を参照してください。
- レポート データのビューをカスタマイズするには、レポート データのビューのカスタマイズを参照してください。
- データ内の特定の情報を検索するには、検索およびインタラクティブ電子メール レポート ページ （7 ページ）を参照してください。
- レポート情報を印刷またはエクスポートするには、レポーティング データおよびトラッキング データのエクスポートを参照してください。
- さまざまなインタラクティブ レポート ページを理解するには、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ）を参照してください。
- レポートをオンデマンドで生成するには、オンデマンドでのメール レポートの生成 （135 ページ）を参照してください。
- 指定した間隔および時刻に自動的に実行されるようにレポートをスケジュール設定するには、メール レポートのスケジュール設定 （133 ページ）を参照してください。
- アーカイブしたオンデマンドのレポートおよびスケジュール設定したレポートを表示するには、[アーカイブ メール レポート（Archived Email Reports）] の表示と管理 （137 ページ）を参照してください。
- バックグラウンド情報については、セキュリティ管理アプライアンスによるレポート用データの収集方法を参照してください。
- 大量のデータを処理するときにパフォーマンスを向上させるには、電子メール レポートのパフォーマンスの向上を参照してください。
- チャートまたはテーブル内に青色のリンクとして表示されるエンティティまたは番号に関する詳細を取得するには、エンティティまたは番号をクリックします。

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

新しい Web インターフェイスでの電子メール レポート データの使用

- レポート データのアクセスおよび表示に関するオプションついては、レポート データの表示方法を参照してください。
- レポート データのビューをカスタマイズするには、レポート データのビューのカスタマイズを参照してください。
- レポート情報を印刷またはエクスポートするには、レポーティング データおよびトラッキング データのエクスポートを参照してください。
- さまざまなインタラクティブ レポート ページを理解するには、インタラクティブ レポート ページの使用を参照してください。
- レポートをオンデマンドで生成するには、オンデマンドでのメール レポートの生成 （135 ページ）を参照してください。
- 指定した間隔および時刻に自動的に実行されるようにレポートをスケジュール設定するには、メール レポートのスケジュール設定 （133 ページ）を参照してください。
- アーカイブしたオンデマンドのレポートおよびスケジュール設定したレポートを表示するには、[アーカイブ メール レポート（Archived Email Reports）] の表示と管理 （137 ページ）を参照してください。
- バックグラウンド情報については、セキュリティ管理アプライアンスによるレポート用データの収集方法を参照してください。
- 大量のデータを処理するときにパフォーマンスを向上させるには、電子メール レポートのパフォーマンスの向上を参照してください。
- チャートまたはテーブル内に青色のリンクとして表示されるエンティティまたは番号に関する詳細を取得するには、エンティティまたは番号をクリックします。

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

検索およびインタラクティブ電子メールレポートページ

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

ドロップダウン メニューから、次のような数種類の条件で検索できます。

- IP アドレス

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

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

IPv4 検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば、「17.*」は 17.0.0.0 ～ 17.255.255.255 の範囲で検索されるので、17.0.0.1 は一致しますが、172.0.0.1 は一致しません。完全一致検索の場合は、4 つすべてのオクテットを入力します。IP アドレス検索は、クラスレス ドメイン間ルーティング（CIDR）形式（17.16.0.0/12）もサポートします。

IPv6 検索の場合、次の例の形式を使用して、アドレスを入力できます。

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

[電子メール レポート（Email Reporting）] ページの概要

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

表 *1* : *[電子メールレポート（Email Reporting）] タブのオプション*

[電子メールレポート（Email Reporting）] メニュー	**操作**
[電子メール レポーティングの概要（Email Reporting Overview）] ページ	[概要（Overview）] ページには、お使いの E メール セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。 詳細については、[電子メール レポーティングの概要（Email Reporting Overview）] ページ （18 ページ）を参照してください。
[受信メール（Incoming Mail）] ページ	[受信メール（Incoming Mail）] ページには、管理対象の E メール セキュリティ アプライアンスに接続されているすべてのリモート ホストのリアルタイム情報に関するインタラクティブなレポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。 詳細については、[受信メール（Incoming Mail）] ページ （23 ページ）を参照してください。
[送信者グループ（Sender Groups）] レポート ページ	[送信者グループ（Sender Groups）] レポート ページには、送信者グループ別およびメール フロー ポリシー アクション別に接続の要約が表示され、SMTP 接続およびメール フロー ポリシーのトレンドを確認できます。 詳細については、[送信者グループ（Sender Groups）] レポート ページ （28 ページ）を参照してください。
[送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ	このレポート ページでは、SDR サービスで受信した判定や脅威カテゴリに基づいて着信メッセージを表示できます。 詳細については、[送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ （28 ページ）を参照してください。
[送信先（Outgoing Destinations）] ページ	[送信先（Outgoing Destinations）] ページには、組織がメールを送信する宛先ドメインについての情報が表示されます。ページの上部には、発信脅威メッセージごとの上位の宛先、および発信クリーン メッセージ別の上位の宛先を示すグラフが表示されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）列を示す表が表示されます。 詳細については、[送信先（Outgoing Destinations）] ページ （29 ページ）を参照してください。

[電子メールレポート（Email Reporting）] メニュー	操作
[送信メッセージ送信者（Outgoing Senders）] ページ	[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。 詳細については、[送信メッセージ送信者（Outgoing Senders）] ページ （30 ページ）を参照してください。
[内部ユーザ（Internal Users）] ページ	[内部ユーザ（Internal Users）] には、電子メール アドレスごとに内部ユーザによって送受信された電子メールについての情報が表示されます。1 人のユーザが複数の電子メール アドレスを持っている場合があります。レポートでは、電子メール アドレスがまとめられません。 詳細については、[内部ユーザ（Internal Users）] ページ （31 ページ）を参照してください。
DLP インシデント	[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。 詳細については、DLP インシデント （33 ページ）を参照してください。
メッセージ フィルタ	[メッセージフィルタ（Message Filters）] ページには、送受信メッセージのメッセージフィルタの上位一致（最も多くのメッセージに一致したメッセージ フィルタ）に関する情報が表示されます。 詳細については、メッセージ フィルタ （35 ページ）を参照してください。
地理的分散	[地理的分散（Geo Distribution）] ページには、次の情報が表示されます。 • 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）。 詳細については、地理的分散 （35 ページ）を参照してください。

[電子メールレポート（Email Reporting）] メニュー	操作
大容量のメール	[大容量のメール（High Volume Mail）] ページでは、1 人の送信者から送られていたり、件名が同じであったりする、特定の 1 時間の間に送られた多数のメッセージに関係する攻撃が特定されます。 詳細については、大容量のメール （35 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）に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツフィルタ（Content Filters）] ページを使用すると、コンテンツ フィルタごとまたはユーザごとに企業ポリシーを確認できます。 詳細については、[コンテンツフィルタ（Content Filters）] ページ （36 ページ）を参照してください。
DMARC 検証	[DMARC検証（DMARC Verification）] ページには、Domain-based Message Authentication, Reporting and Conformance（DMARC）検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。 詳細については、DMARC 検証 （37 ページ）を参照してください。
マクロ検出	[マクロ検出（Macro Detection）] レポート ページには、コンテンツ フィルタまたはメッセージ フィルタによって最も多く検出された、マクロが有効化された受信/発信添付ファイルがファイル タイプごとに表示されます。 詳細については、マクロ検出 （37 ページ）を参照してください。

[電子メールレポート（Email Reporting）] メニュー	操作
[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）] ページには、次のレポートが表示されます。 • 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。 • メッセージで検出された脅威に一致する上位 IOC。 • 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。 詳細については、[外部脅威フィード（External Threat Feeds）] ページ （38 ページ）を参照してください。
[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、ネットワークで送受信されたウイルスの概要が示されます。[ウイルス タイプ（Virus Types）] ページには、E メール セキュリティ アプライアンスで動作するウイルス スキャン エンジンによって検出され、セキュリティ管理アプライアンスに表示されるウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。 詳細については、[ウイルス タイプ（Virus Types）] ページ （38 ページ）を参照してください。
[URL フィルタリング（URL Filtering）] ページ	このページでは、メッセージ内で最も頻繁に生じる URL カテゴリ、スパム メッセージ内の最も一般的な URL、メッセージに表示される悪意のある URL およびニュートラル URL の数を確認します。 詳細については、[URL フィルタリング（URL Filtering）] ページ （40 ページ）を参照してください。
[Web インタラクション トラッキング（Web Interaction Tracking）] ページ	ポリシーまたはアウトブレイク フィルタによって書き換えられた URL をクリックしたエンドユーザと、各ユーザ クリックに関連付けられたアクションを識別します。 詳細については、[Webインタラクショントラッキング（Web Interaction Tracking）] ページ （40 ページ）を参照してください。

[電子メールレポート（Email Reporting）] メニュー	操作
[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。 [偽装メールの検出（Forged Email Detection）] ページ （42 ページ）を参照してください。
[高度なマルウェア防御（ファイル レピュテーションとファイル分析）（Advanced Malware Protection (File Reputation and File Analysis)）] レポート ページ	ファイル レピュテーションおよび分析データは 3 つのレポーティング ページに表示されます。 詳細については、[高度なマルウェア防御（ファイル レピュテーションとファイル分析）（Advanced Malware Protection (File Reputation and File Analysis)）] レポート ページ （42 ページ）を参照してください。
メールボックスの自動修復	メールボックスの修復結果の詳細を表示するには、このページを使用します。 メールボックスの自動修復 （49 ページ）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。 詳細については、[TLS 接続（TLS Connections）] ページ （50 ページ）を参照してください。
[受信 SMTP 認証（Inbound SMTP Authentication）] ページ	[受信SMTP認証（Inbound SMTP Authentication）] ページには、クライアント証明書の使用情報、および Email Security Appliance とユーザのメール クライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。 詳細については、[受信 SMTP 認証（Inbound SMTP Authentication）] ページ （51 ページ）を参照してください。

[電子メールレポート（Email Reporting）] メニュー	操作
[アウトブレイク フィルタ（Outbreak Filters）] ページ	[アウトブレイクフィルタ（Outbreak Filters）] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する防御をモニタします。 詳細については、[アウトブレイク フィルタ（Outbreak Filters）] ページ （52 ページ）を参照してください。
[レート制限（Rate Limits）] ページ	[レート制限（Rate Limits）] ページには、送信者あたりのメッセージ受信者数に対して設定したしきい値を超える電子メール送信者（MAIL-FROM アドレスに基づく）が表示されます。 詳細については、[レート制限（Rate Limits）] ページ （52 ページ）を参照してください。
[システム容量（System Capacity）] ページ	レポーティング データをセキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。 詳細については、[システム容量（System Capacity）] ページ （56 ページ）を参照してください。
[有効なレポートデータ（Reporting Data Availability）] ページ	各アプライアンスのセキュリティ管理アプライアンス上のレポーティングデータの影響を把握できます。詳細については、[有効なレポートデータ（Reporting Data Availability）] ページ （60 ページ）を参照してください。
メール レポートのスケジュール設定	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、メール レポートのスケジュール設定 （133 ページ）を参照してください。
[アーカイブ メール レポート（Archived Email Reports）] の表示と管理	アーカイブ済みのレポートを表示および管理できます。詳細については、[アーカイブ メール レポート（Archived Email Reports）] の表示と管理 （137 ページ）を参照してください。 また、オンデマンド レポートを生成することもできます。オンデマンドでのメール レポートの生成 （135 ページ） を参照してください。

電子メール レポーティング ページのテーブルの列の説明

表 *2:* 電子メール レポーティング ページのテーブルの列の説明

列名	
受信メールの詳細	

列名	
[拒否された接続（Connections Rejected）]	HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけられている場合、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。
[承認された接続（Connections Accepted）]	受け入れられたすべての接続。
[試行回数の合計（Total Attempted）]	すべての受け入れられた接続試行と、拒否された接続試行。
[受信者スロットルによる停止（Stopped by Recipient Throttling）]	これは、レピュテーション フィルタリングによる阻止の 1 要素です。HAT 上限値（1 時間当たりの最大受信者数、メッセージあたりの最大受信者数、または接続あたりの最大メッセージ数）のいずれかを超えたために、阻止された受信メッセージの数を表します。この値と、拒否されたか、TCP 拒否の接続に関連する受信メッセージの予測値とが合計されて、[レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] が算出されます。

列名	
[レピュテーションフィルタによる停止（Stopped by Reputation Filtering）]	[レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • 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） [概要（Overview）] ページの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
[無効な受信者の場合に停止（Stopped as Invalid Recipients）]	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
[スパム検出（Spam Detected）]	検出されたすべてのスパム。
[ウイルス検出（Virus Detected）]	検出されたすべてのウイルス。
コンテンツフィルタによる阻止	コンテンツ フィルタによって阻止されたメッセージの総数。
合計脅威件数（Total Threat）	脅威メッセージ（評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの）の総数
Marketing	不要なマーケティング メッセージとして検出されたメッセージの数。

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

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

[電子メール レポーティングの概要（Email Reporting Overview）] ページ

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

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

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

（注） [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートおよび [エグゼクティブサマリー（Executive Summary）] レポートは、[電子メール レポーティングの概要（Email Reporting Overview）] ページ （18 ページ）に基づきます。詳細については、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート （129 ページ）および[エグゼクティブサマリー（Executive Summary）] レポート （133 ページ）を参照してください。

表 3 : [メール（*Email*）] > [レポート（*Reporting*）] > [概要（*Overview*）] ページの詳細

セクション	説明
時間範囲	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。

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

受信メール メッセージのカウント方法

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

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

アプライアンスによる電子メール メッセージの分類方法

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

上記の例では、各種判定は次の優先ルールに従います。

- スパム陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

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

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

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

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

[概要（Overview）] ページでの電子メール メッセージの分類

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

表 *4 : [*概要（*Overview***）*]* ページの電子メールのカテゴリ**

カテゴリ	説明
レピュテーションフィルタによる停止	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（受信メール メッセージのカウント方法（19ページ）を参照）を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • 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。 [概要（Overview）] ページの [レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] の総数は、すべての拒否された接続の完全な集計値に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
無効な受信者数	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。
検出されたスパム メッセージ数	スパム対策スキャン エンジンで陽性、または疑いありとして検出されたメッセージの総数。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。

カテゴリ	説明
検出されたウイルス メッセージ数	ウイルス陽性だがスパムではないと検出されたメッセージの総数および割合。 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で検出	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。
悪意のあるURLを含むメッセージ	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阻止	コンテンツ フィルタによって阻止されたメッセージの総数。 アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
DMARCによる停止（	DMARC 検証に失敗したメッセージの総数。
S/Mime 検証/復号化の失敗	S/MIME 検証または復号化、あるいはその両方に失敗したメッセージの総数。
マーケティングメッセージ	Amazon.com など、認識されているプロフェッショナル マーケティング グループからのアドバタイジング メッセージの総数。 このページのこのリスト項目は、システムにマーケティング データが存在している場合にだけ表示されます。 この数には、グレイメール機能が有効になっている E メール セキュリティ アプライアンスと、スパム対策設定でマーケティング電子メール スキャニングが有効になっているアプライアンスの両方によって識別されたマーケティング メッセージが含まれています。
ソーシャルネットワーキングメッセージ	ソーシャル ネットワーク、出会い/結婚 Web サイト、フォーラムなどからの通知メッセージの総数。たとえば、LinkedIn フォーラム、CNET フォーラムなどがあります。この情報は、グレイメール機能によって判別されます。

カテゴリ	説明
バルクメッセージ	テクノロジー メディア企業の TechTarget など、認識されていないマーケティング グループによって送信されたアドバタイジング メッセージの総数。 この情報は、グレイメール機能によって判別されます。
グレーメール メッセージ	この数には、グレイメール機能によって検出されたマーケティング メッセージと、ソーシャル ネットワーク メッセージおよびバルク メールが含まれます。これらの総数がマーケティング メッセージ値に含まれる場合でも、グレイメール機能が有効になっていないアプライアンスで識別されたマーケティング メッセージは含まれません。 メッセージ トラッキングを使用して、そのカテゴリに所属するメッセージのリストを表示するには、任意のグレイメール カテゴリに対応する番号をクリックします。 グレイメールのレポート （54 ページ）も参照してください。
S/MIME 検証/復号化の成功	正常に検証、復号化されたか、S/MIME を使用して復号化および検証されたメッセージの総数。
承認されたクリーン メッセージ数	このカテゴリは、受け入れられ、ウイルスでもスパムでもないと見なされたメールです。 受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。 ただし、ウイルス陽性またはスパム陽性としてマークされたにもかかわらず配信されたメッセージは集計されないので、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。 メッセージがメッセージ フィルタと一致し、フィルタによってドロップされたり、バウンスされたりしていない場合は、クリーンなメッセージとして扱われます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。 グレイメール機能が有効になっていないアプライアンスで処理されるメッセージは、クリーンとして集計されます。
試行されたメッセージの合計数	この数には、スパム、マーケティング メッセージ（グレイメール機能またはスパム対策機能の電子メール スキャン機能によって検出）、ソーシャル ネットワーキング メッセージ、バルク メール、およびクリーン メッセージが含まれます。

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

[受信メール（Incoming Mail）] ページ

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

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

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

- セキュリティ管理アプライアンスにメールを送信した送信者の IP アドレス、ドメイン、またはネットワーク オーナー（組織）に関する検索を実行する。検索およびインタラクティブ電子メール レポート ページ （7 ページ）を参照してください。
- 送信者グループ レポートを表示して、特定の送信者グループおよびメール フロー ポリシー アクションに従って接続をモニタする。詳細については、[送信者グループ（Sender Groups）] レポート ページ （28 ページ）を参照してください。
- 電子メールをアプライアンスに送信した送信者の詳細な統計情報を表示する。統計情報には、セキュリティ サービス（送信者レピュテーション フィルタリング、アンチスパム、アンチウイルスなど）によってブロックされたメッセージの数が含まれます。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した送信者別にソートする。
- SenderBase レピュテーション サービスを使用して特定の IP アドレス、ドメイン、および組織の間の関係を分析し、送信者に関する情報を取得する。
- 送信者の SenderBase レピュテーション スコア（SBRS）、ドメインが直近に一致した送信者グループなど、送信者に関する詳細を SenderBase レピュテーション サービスから取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者についての詳細情報を取得する。

[受信メール（Incoming Mail）] ページ内のビュー

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

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

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

さらに、[受信メール（Incoming Mail）] ページの [受信メールの詳細（Incoming Mail Details）] セクションでは、送信者の IP アドレス、ドメイン名、またはネットワーク オーナー情報をクリックすると、特定の送信者プロファイル情報を取得できます。[送信者プロファイル（Sender Profile）] の情報の詳細については、[送信者プロファイル（Sender Profile）] ページ （26 ページ）を参照してください。

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

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

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

送信者グループ別のメール フロー情報にアクセスするには、[受信メール（Incoming Mail）] ページの下部にある [送信者グループ レポート（Sender Groups Report）] リンクをクリックします。[送信者プロファイル（Sender Profile）] ページ （26 ページ）を参照してください。

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

トップレベル ページ（この場合には[受信メール（Incoming Mail）] レポート ページ）の右上にある [印刷可能なPDF（Printable PDF）] リンクをクリックすると、これらの各サブレポート ページの結果を、1 つの統合レポートに生成できます。[電子メール レポート（Email Reporting）] ページの概要 （8 ページ）の重要な情報を参照してください。

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

[受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルに含まれるデータの説明については、[受信メールの詳細（Incoming Mail Details）] テーブル （25 ページ）を参照してください。

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

については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ）を参照してください。

（注） [受信メール（Incoming Mail）] レポート ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

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

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

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

メール トレンド グラフにおける時間範囲

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

時間範囲の詳細については、レポートの時間範囲の選択を参照してください。

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

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

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

[受信メールの詳細（Incoming Mail Details）] テーブルの最初の列、または [脅威メッセージの送信者上位（Top Senders by Total Threat Messages）] に表示される送信者、つまりネットワーク オーナー、IP アドレスまたはドメインについては、[送信者（Sender）] または [ドメイン情報がありません（No Domain Information）] リンクをクリックすると、送信者の詳細情報が表示されます。結果は、[送信者プロファイル（Sender Profile）] ページに表示され、SenderBase レピュテーション サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、[送信者プロファイル（Sender Profile）] ページ （26 ページ）を参照してください。

[受信メール（Incoming Mail）] ページの下部にある [送信者グループレポート（Sender Groups Report）] をクリックして、[送信者グループ（Sender Groups）] レポートを表示することもできます。[送信者グループ（Sender Groups）] レポート ページの詳細については、[送信者グループ（Sender Groups）] レポート ページ （28 ページ）を参照してください。

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

[送信者プロファイル（Sender Profile）] ページ

[受信メール（Incoming Mail] インタラクティブ テーブル（ [メールフローの詳細（**Mail Flow Details**）]（新しい Web インターフェイス）または [受信メール（**Incoming Mail**）] ページ）の送信者をクリックすると、[送信者プロファイル（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。[メールフローの詳細（Mail Flow Details）] ページまたは他の [送信者プロファイル（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。

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

- IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
- この送信者から最初のメッセージを受信してからの日数
- 最後の送信者グループと DNS が検証されたかどうか（IP アドレス送信者プロファイル 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）
- SenderBase 評価スコア（IP アドレス プロファイル ページのみ）
- 最初のメッセージからの日数（ネットワーク オーナーとドメイン プロファイル ページのみ）
- このネットワーク オーナーに関連するドメインの数（ネットワーク オーナープロファイル ページおよびドメイン プロファイル ページのみ）
- このネットワーク オーナーの IP アドレスの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
- 電子メールの送信に使用された IP アドレスの数（ネットワーク オーナー ページのみ）

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

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

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

[送信者グループ（Sender Groups）] レポート ページ

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

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

[送信者グループ（Sender Group）] レポート ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ） を参照してください。

（注） [送信者グループ（Sender Group）] レポート ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

[送信者ドメインのレピュテーション（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「非常に問題がある」または「悪い」メッセージのみが、「スパム」や「悪意あり」などの SDR 脅威カテゴリに分類されます。

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

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

[送信先（Outgoing Destinations）] ページ

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

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

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

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

表 *5 : [メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページの詳細*

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

[送信先（Outgoing Destinations）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ） を参照してください。

（注） [送信先（Outgoing Destinations）] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

[送信メッセージ送信者（Outgoing Senders）] ページ

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

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

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

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

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

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

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

表 *6 : [メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Sender）] ページの詳細*

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

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

（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を追跡するには、適切な E メール セキュリティ アプライアンスにログインし、[モニタ（Monitor）]> [送信処理ステータス（Delivery Status）] を選択します。

[送信メッセージ送信者（Outgoing Senders）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ） を参照してください。

（注） [送信メッセージ送信者（Outgoing Senders）] レポート ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

[内部ユーザ（Internal Users）] ページ

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

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

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

表 7 : [メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、レポートの時間範囲の選択を参照してください。
[正常な受信メッセージ数の上位ユーザ（Top Users by Clean Incoming Messages）]	組織内で送信されたクリーンな着信メッセージの上位ユーザ（IPアドレス別またはドメイン別）。
[正常な送信メッセージ数の上位ユーザ（Top Users by Clean Outgoing Messages）]	組織内で送信されたクリーンな発信メッセージの上位ユーザ（IPアドレス別またはドメイン別）。
[ユーザメールフローの詳細（User Mail Flow Details）]	[ユーザメールフローの詳細（User Mail Flow Details）] インタラクティブ セクションでは、電子メールアドレスごとに送受信メールが分類されます。列ヘッダーをクリックすることにより、表示をソートできます。 ユーザの詳細を参照するには、[内部ユーザ（Internal User）] 列でユーザ名をクリックします。詳細については、[内部ユーザの詳細（Internal User Details）] ページ （32 ページ）を参照してください。 アクセス権限でメッセージ トラッキング データを表示できる場合、このレポートのコンテンツ フィルタ違反に対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[内部ユーザ（Internal Users）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ） を参照してください。

（注） [内部ユーザ（Internal Users）] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

[内部ユーザの詳細（Internal User Details）] ページ

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

着信内部ユーザとは、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。

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（36 ページ）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したすべてのユーザのリストも表示できます。

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

特定の内部ユーザの検索

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

DLP インシデント

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

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

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

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

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

表 *8 : [メール（Email）] > [レポート（Reporting）] > [DLP インシデント サマリー（DLP Incident Summary）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、レポートの時間範囲の選択を参照してください。
[重大度別上位インシデント（Top Incidents by Severity）]	重大度別の上位 DLP インシデント。
[インシデントサマリー（Incident Summary）]	各電子メールアプライアンスの送信メールポリシーで現在有効になっている DLP ポリシーは、[DLPインシデントサマリー（DLP Incident Summary）] ページの下部にある [DLPインシデントの詳細（DLP Incident Details）] インタラクティブ テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。
[上位DLPポリシー一致数（Top DLP Policy Matches）]	一致している上位 DLP ポリシー。
[DLPインシデントの詳細（DLP Incident Details）]	[DLPインシデントの詳細（DLP Incident Details）] テーブルには、ポリシーごとの DLP インシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。 [DLPインシデントの詳細（DLP Incidents Details）] テーブルの詳細については、[DLPインシデントの詳細（DLP Incidents Details）] テーブル （34 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。

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

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

このテーブルに表示される DLP ポリシーの詳細情報を検索するには、DLP ポリシー名をクリックして、その DLP ポリシーのページを表示します。詳細については、[DLP ポリシー詳細（DLP Policy Detail）] ページ （35 ページ）を参照してください。

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

[DLP ポリシー詳細（DLP Policy Detail）] ページ

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

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

インシデント詳細ページの送信者名をクリックすると [内部ユーザ（Internal Users）] ページが開きます。詳細については、[内部ユーザ（Internal Users）] ページ （31 ページ）を参照してください。

メッセージ フィルタ

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

地理的分散

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

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

国情報を表示しない受信メール接続の上位と合計数の例を次に示します。

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

大容量のメール

このページのレポートは、次の目的で使用します。

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

- フィルタを適宜調整できるように、誤検出を特定します。

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

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

関連項目

- [レート制限（Rate Limits）] ページ （52 ページ）

[コンテンツフィルタ（Content Filters）] ページ

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

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

特定のフィルタの詳細情報を表示するには、フィルタ名をクリックします。[コンテンツフィルタの詳細（Content Filter Details）] ページが表示されます。[コンテンツフィルタの詳細（Content Filter Details）] ページの詳細については、[コンテンツフィルタの詳細（Content Filter Details）] ページ （37 ページ） を参照してください。

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

[コンテンツフィルタ（Content Filters）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ） を参照してください。

（注） [コンテンツフィルタ（Content Filter）] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ） を参照してください。

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

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

[内部ユーザ別の一致（Matches by Internal User）] セクションで、内部ユーザ（電子メール アドレス）の詳細ページを表示するユーザ名をクリックします。詳細については、[内部ユーザの詳細（Internal User Details）] ページ （32 ページ）を参照してください。

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

DMARC 検証

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

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

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

マクロ検出

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

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

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

（注） レポート生成中に次の処理が発生します。

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

[外部脅威フィード（External Threat Feeds）] ページ

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

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

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

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

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

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

[ウイルス タイプ（Virus Types）] ページ

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

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

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

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

表 *9 : [メール（Email）] > [レポート（Reporting）] > [ウイルスタイプ（Virus Types）] ページの詳細*

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

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

[ウイルスタイプ（Virus Types）] ページから、PDF を生成したり、raw データを CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、[電子メール レポート（Email Reporting）] ページの概要 （8 ページ） を参照してください。

（注） [ウイルスタイプ（Virus Types）] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

[URL フィルタリング（URL Filtering）] ページ

- URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。
- URL フィルタリング レポートは、送受信メッセージに対して使用できます。
- URL フィルタリングエンジンによって（アンチスパム/アウトブレイク フィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して）スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではできません。
- [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。
- 各メッセージを関連付けることができるレピュテーション レベルは 1 つのみです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。
- [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] で設定したグローバル許可リストの 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であると判定された URL です。したがって、ニュートラル URL は Cisco Web セキュリティ プロキシにリダイレクトするために書き換えられています。
- URL カテゴリ ベースのフィルタの結果はコンテンツおよびメッセージ フィルタ レポートに反映されます。
- Cisco Web セキュリティ プロキシによるクリック時の URL 評価の結果は、レポートに反映されません。

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

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

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

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

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

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

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

  Web インタラクション トラッキングの詳細。次の情報が含まれています。

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

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

  - 書き換えられた URL をエンドユーザがクリックした回数。クリックされた URL を含むすべてのメッセージのリストを表示するには、番号をクリックします。

- 次の点に注意してください。

  - 悪意のあるURLを書き換えた後に、メッセージを送信して別のユーザ（管理者など）に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクション トラッキング データが増分します。
  - 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用して元の受信者以外のユーザ（管理者など）に送信する場合、その他のユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクション トラッキング データが増分します。

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

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

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

ファイル分析レポートの詳細の要件

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

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

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

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

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

ステップ 1 Web インターフェイスの [ファイル分析（File Analysis）] セクションにアクセスします。

- レガシー Web インターフェイスで、[管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] をクリックし、[ファイル分析（File Analysis）] セクションまで下にスクロールします。
- 新しい Web インターフェイスで、[サービスステータス（Service Status）] をクリックし、[ファイル分析（File Analysis）] セクションまでスクロールダウンします。

ステップ 2 管理対象アプライアンスが別のファイル分析クラウドサーバを指している場合は、結果の詳細の表示元となるサーバを選択します。

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

ステップ 3 分析グループ ID を入力します。

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

ステップ 4 [今すぐグループ化（Group Now）] をクリックします。

ステップ 5 このアプライアンスとデータを共有する各 E メールセキュリティ アプライアンスで、同じグループを設定します。

次のタスク

関連項目

クラウドで詳細なファイル分析結果が表示されるファイル （48 ページ）

（オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する

オンプレミス（プライベート クラウド）の Cisco AMP Threat Grid Appliance を導入した場合、Threat Grid Appliance で使用可能なレポート詳細を表示するために、Cisco コンテンツ セキュリ

ティ管理アプライアンスのファイル分析アカウントをアクティブ化する必要があります。通常、これは 1 回のみ必要です。

始める前に

重大レベルでシステム アラートを受信していることを確認します。

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

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

ステップ 2 アラート メッセージ内のリンクをクリックします。

ステップ 3 管理アプライアンスのアカウントをアクティブ化します。

追加の要件

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

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、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。

ファイル レピュテーションとファイル分析レポートのページ

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

レポート	説明
	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 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。 （注） AsyncOS 9.6.5 以降、高度なマルウェア防御レポートが、追加フィールド、グラフなどを表示するように強化されました。アップグレード後に表示されるレポートには、アップグレード前のレポートのデータは含まれません。AsyncOS 9.6.5 アップグレード前の高度なマルウェア防御レポートを表示するには、ページの下部にあるハイパーリンクをクリックします。 [カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] セクションには次の内容が表示されます。 • [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るブロックされたファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで [シンプルカスタム検出（Simple Custom Detection）] として表示されます。 • [カスタムしきい値（Custom Threshold）] に分類される 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。 レポートの [詳細（More Details）] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブ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詳細を表示できます。

レポート	説明
	[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（Advanced Malware Protection）]におけるファイル分析	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。 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 Appliance での導入の場合：AMP Threat Grid Appliance でホワイトリストに登録されているファイルは、「クリーン」として表示されます。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。 ファイルを分析したサーバに関する詳細を表示するには、ファイル分析レポートの詳細の要件 （42 ページ）を参照してください。 圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析（File Analysis）] レポートに含まれます。 （注） AsyncOS 9.6.5 以降、ファイル分析レポートが、追加フィールド、グラフなどを表示するように強化されました。アップグレード後に表示されるレポートには、アップグレード前のレポートのデータは含まれません。AsyncOS 9.6.5 アップグレード前のファイル分析レポートを表示するには、ページの下部にあるハイパーリンクをクリックします。

レポート	説明
[高度なマルウェア防御判定の更新（Advanced Malware Protection Verdict Updates）]	高度なマルウェア防御は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。 [AMP判定のアップデート（AMP Verdict Updates）] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、お使いのEメールセキュリティアプライアンスのマニュアルを参照してください。 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。

その他のレポートでのファイル レピュテーション フィルタ データの表示

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

クラウドで詳細なファイル分析結果が表示されるファイル

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

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

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

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

関連項目

- （クラウドファイル分析）詳細なファイル分析結果が表示されるように管理アプライアンスを設定する （42 ページ）

メールボックスの自動修復

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

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

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

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

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

（注） AsyncOS 13.6.1 にアップグレードすると、アップグレード前に受信したメッセージのメッセージ トラッキング ステータスは、[修正済み（Remediated）] ではなく [配信済み（Remediated）] のままになります。

[TLS 接続（TLS Connections）] ページ

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

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

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

表 *10 : [メール（Email）] > [レポート（Reporting）] > [TLS 接続（TLS Connections）] ページの詳細*

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

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

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

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

次の情報を確認するには、このレポートを使用します。

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

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

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

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

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

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

[レート制限（Rate Limits）] ページ

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

このレポートは、以下を特定する場合に役立ちます。

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

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

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

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

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

関連項目

- 大容量のメール （35 ページ）

[アウトブレイク フィルタ（Outbreak Filters）] ページ

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

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

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

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

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

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

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

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

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

このページの他のモジュールには次の情報が表示されます。

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

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

- アウトブレイク フィルタで検出された脅威の重大度。

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

- メッセージがアウトブレイク隔離にとどまっていた時間。

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

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

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

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

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

グレイメールのレポート

グレイメールの統計情報は、次のレポートに反映されます。

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

関連項目

- AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート （55 ページ）

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

AsyncOS 9.5 へのアップグレード後：

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

[システム容量（System Capacity）] ページ

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

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

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

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

- **量**：「正常」なメッセージ量と環境内での「通常」のスパイクを把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール（Incoming Mail）] ページおよび [送信メール（Outgoing Mail）] ページを使用すると、経時的に量を追跡できます。詳細については、[システム容量（System Capacity）] : [受信メール（Incoming Mail）] （58 ページ）および[システム容量（System Capacity）] : [送信メール（Outgoing Mail）] （58 ページ）を参照してください。
- **ワーク キュー**：ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、非スパム メッセージの異常な増加を処理する、「緩衝装置」として設計されています。ただし、作業キューは負荷のかかっているシステムを示す指標でもあります。長く、頻繁な作業キューのバックアップは、キャパシティの問題を示している可能性があります。[システム容量（System Capacity）] : [ワークキュー（Workqueue）] ページを使用すると、作業キュー内のアクティビティを追跡できます。詳細については、[システム容量（System Capacity）] : [ワークキュー（Workqueue）] （57 ページ）を参照してください。
- **リソース節約モード**：アプライアンスがオーバーロードになると、リソース節約モード（RCM）になり、CRITICAL システム アラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。リソース節約アクティビティ （59 ページ） を参照してください。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

システムの負荷レポートに、次が表示されます。

- 全体のCPU使用率（Overall CPU Usage） （58 ページ）
- メモリページスワップ（Memory Page Swapping） （59 ページ）
- リソース節約アクティビティ （59 ページ）

全体のCPU使用率（Overall CPU Usage）

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

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

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

メモリページスワップ（Memory Page Swapping）

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

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

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

リソース節約アクティビティ

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

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

[システム容量（System Capacity）]：[すべて（All）]

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

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

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

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

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

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

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

新しいWebインターフェイスの電子メールレポートページの概要

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

表 *11 : [*電子メールレポート（*Email Reports*）*]* ドロップダウンのオプション

[レポート（Reports）] ドロップダウンのオプション	操作
[メール フロー概要（Mail Flow Summary）] ページ	[メール フロー概要（Mail Flow Summary）] レポート ページは、E メール セキュリティ アプライアンス上のアクティビティの概要を示します。これには、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。 詳細については、[メール フロー概要（Mail Flow Summary）] ページ （66 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[システム容量（System Capacity）] ページ	[システム容量（System Capacity）] レポート ページには、セキュリティ管理アプライアンスに送信された、レポート データの全体的なワークロードに関する詳細情報が表示されます。 詳細については、[システム容量（System Capacity）] ページ （73 ページ）を参照してください。
ファイルおよびマルウェアのレポート	
[高度なマルウェア防御（Advanced Malware Protection）] ページ（ファイル レピュテーションおよびファイル分析）	[高度なマルウェア防御（Advanced Malware Protection）] レポート ページには、着信および送信ファイルベースの脅威についての、サマリー、ファイル レピュテーション、ファイル分析、ファイル レトロスペクション、およびメールボックス自動修復の詳細を表示するレポート ビューが表示されます。 詳細については、[高度なマルウェア防御（Advanced Malware Protection）] ページ （77 ページ）を参照してください。
[ウイルス フィルタリング（Virus Filtering）] ページ	[ウイルス フィルタリング（Virus Filtering）] レポート ページでは、ネットワークで送受信されたウイルスの概要が示されます。このページには、E メール セキュリティ アプライアンスで動作するウイルス スキャン エンジンによって検出され、セキュリティ管理アプライアンスに表示されるウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。 詳細については、[ウイルス フィルタリング（Virus Filtering）] ページ （85 ページ）を参照してください。
[マクロ検出（Macro Detection）] ページ	[マクロ検出（Macro Detection）] レポート ページには、コンテンツ フィルタとメッセージ フィルタによって最も多く検出された、マクロが有効化された受信/発信添付ファイルがファイル タイプごとに表示されます。 詳細については、[マクロ検出（Macro Detection）] ページ （87 ページ）を参照してください。
電子メール脅威のレポート	
[DMARC検証（DMARC Verification）] ページ	[DMARC 検証（DMARC Verification）] レポート ページには、Domain-based Message Authentication, Reporting and Conformance（DMARC）検証に失敗した上位送信者のドメイン、および各ドメインからの受信メッセージに対して実行されたアクションの要約が表示されます。 詳細については、[DMARC検証（DMARC Verification）] ページ （88 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[アウトブレイク フィルタリング（Outbreak Filtering）] ページ	[アウトブレイクフィルタ（Outbreak Filters）] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、フィッシング、詐欺、ウイルス、およびマルウェア攻撃に対する防御をモニタします。 詳細については、[アウトブレイク フィルタリング（Outbreak Filtering）] ページ（89 ページ）を参照してください。
[URL フィルタリング（URL Filtering）] ページ	メッセージ内で最も頻繁に使用される URL カテゴリ、スパム メッセージ内の最も一般的な URL、メッセージに表示される悪意のある URL およびニュートラル URL の数を確認するには、このページを使用します。 詳細については、[URL フィルタリング（URL Filtering）] ページ（92 ページ）を参照してください。
[偽装メールの検出（Forged Email Detection）] ページ	[偽造メールの検出（Forged Email Detection）] レポート ページには、次のレポートが含まれています。 • 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。 詳細については、[偽装メールの検出（Forged Email Detection）] ページ（93 ページ）を参照してください。
[送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ	このレポート ページでは、SDR サービスで受信した判定や脅威カテゴリに基づいて着信メッセージを表示できます。 詳細については、[送信者ドメインのレピュテーション（Sender Domain Reputation）] ページ（94 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[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）] ページには、次のレポートが表示されます。 • 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。 • メッセージで検出された脅威に一致する上位 IOC。 • 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。 詳細については、[外部脅威フィード（External Threat Feeds）] ページ （94 ページ）を参照してください。
接続およびフローのレポート	
[メール フローの詳細（Mail Flow Details）] ページ	[メール フローの詳細（Mail Flow Details）] レポート ページには、管理対象の E メール セキュリティ アプライアンスに接続するすべてのリモート ホストのリアルタイム情報に関するインタラクティブ レポートが表示されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。 詳細については、[メール フローの詳細（Mail Flow Details）] ページ （95 ページ）を参照してください。
[送信者グループ（Sender Groups）] レポート ページ	[送信者グループ（Sender Groups）] レポート ページには、送信者グループ別およびメール フロー ポリシー アクション別に接続の要約が表示され、SMTP 接続およびメール フロー ポリシーのトレンドを確認できます。 詳細については、[送信者グループ（Sender Groups）] レポート ページ （104 ページ）を参照してください。
[送信先（Outgoing Destinations）] ページ	[送信先（Outgoing Destinations）] レポート ページには、組織がメールを送信するドメインについての情報が表示されます。ページの上部には、発信脅威メッセージごとの上位の宛先、および発信クリーン メッセージ別の上位の宛先を示すグラフが表示されます。ページの下部には、総受信者数別にソートされた（デフォルト設定）列を示す表が表示されます。 詳細については、[送信先（Outgoing Destinations）] ページ （105 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[TLS 接続（TLS Connections）] ページ	[TLS 暗号化（TLS Encryption）] レポート ページには、メールの送受信に使用される TLS 接続の全体的な使用状況が表示されます。このレポートでは、TLS 接続を使用してメールを送信する各ドメインの詳細についても示されます。 詳細については、[TLS暗号化（TLS Encryption）] ページ （107 ページ）を参照してください。
[受信 SMTP 認証（Inbound SMTP Authentication）] ページ	[受信SMTP認証（Inbound SMTP Authentication）] レポート ページには、クライアント証明書の使用情報、および E メール セキュリティ アプライアンスとユーザのメール クライアント間で SMTP セッションを認証するための SMTP AUTH コマンドが表示されます。 詳細については、[受信 SMTP 認証（Inbound SMTP Authentication）] ページ （111 ページ）を参照してください。
[レート制限（Rate Limits）] ページ	[レート制限（Rate Limits）] レポート ページには、送信者あたりのメッセージ受信者数に対して設定したしきい値を超える電子メール送信者（MAIL-FROM アドレスに基づく）が表示されます。 詳細については、[レート制限（Rate Limits）] ページ （113 ページ）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 ページには以下が表示されます。 • 発信国別の受信メール接続数の上位（グラフィカルな形式）。 • 発信国別の受信メール接続およびメッセージの合計数（表形式）。 詳細については、[国別の接続（Connections by Country）] ページ （114 ページ）を参照してください。
ユーザ レポート	
[ユーザ メール サマリー（User Mail Summary）] ページ	[ユーザ メール サマリー（User Mail Summary）] レポートには、電子メール アドレスごとに内部ユーザによって送受信された電子メールについての情報が表示されます。1 人のユーザが複数の電子メール アドレスを持っている場合があります。レポートでは、電子メール アドレスがまとめられません。 詳細については、ユーザメール概要（User Mail Summary） （114 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[DLP インシデント サマリー（DLP Incident Summary）] ページ	[DLP インシデント サマリー（DLP Incident Summary）] ページには、送信メールで発生したデータ漏洩防止（DLP）ポリシー違反のインシデントに関する情報が表示されます。 詳細については、[DLP インシデント サマリー（DLP Incident Summary）] ページ （118 ページ）を参照してください。
[Web インタラクション（Web Interaction）] ページ	[Web インタラクション（Web Interaction）] レポート ページは、ポリシーまたはアウトブレイク フィルタによって書き換えられた URL をクリックしたエンドユーザと、各ユーザ クリックに関連付けられたアクションを示します。 詳細については、[Web インタラクション（Web Interaction）] ページ （120 ページ）を参照してください。
[修復レポート（Remediation Reports）] 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るようになりました。 このレポートには、次の概要が表示されます。 • [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。 修復が試行されたメッセージに関する詳細情報を表示するには、レポート内の [メールボックスの自動修復（Mailbox Auto Remediation）] タブと [メールボックスの検索と修復（Mailbox Search and Remediate）] タブをクリックします。 詳細については、[修復レポート（Remediation Reports）] ページ （122 ページ）を参照してください。
フィルタのレポート	

[レポート（Reports）] ドロップダウンのオプション	操作
[メッセージフィルタ（Message Filters）] ページ	[メッセージフィルタ（Message Filters）] レポート ページには、送受信メッセージのメッセージフィルタの上位一致（最も多くのメッセージに一致したメッセージフィルタ）に関する情報が表示されます。 詳細については、[メッセージフィルタ（Message Filters）] ページ（124 ページ）を参照してください。
[大容量のメール（High Volume Mail）] ページ	[大容量のメール（High Volume Mail）] レポート ページでは、1 人の送信者から送られていたり、件名が同じであったりする、特定の 1 時間の間に送られた多数のメッセージに関係する攻撃が特定されます。 詳細については、[大容量のメール（High Volume Mail）] ページ（125 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）] レポート ページには、送受信コンテンツ フィルタの上位一致（最も多くのメッセージに一致したコンテンツ フィルタ）に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。 詳細については、[コンテンツフィルタ（Content Filters）] ページ（126 ページ）を参照してください。

[メール フロー概要（Mail Flow Summary）] ページ

セキュリティ管理アプライアンスの [メール フロー概要（Mail Flow Summary）] レポート ページは、E メール セキュリティ アプライアンスからの E メール メッセージ アクティビティの概要を示します。[メール フロー概要（Mail Flow Summary）] レポート ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。

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

このページのメール トレンド グラフを使用して、選択した時間範囲に基づいてアプライアンスで処理およびブロックされたすべての着信メールのフローをモニタできます。詳細については、レポートの時間範囲の選択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 （7 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を参照してください。

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

このページのメール トレンド グラフを使用して、選択した時間範囲に基づいてアプライアンスによって処理および配信されたすべての送信メールのフローをモニタできます。詳細については、レポートの時間範囲の選択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 *12 : [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、E メール セキュリティ アプライアンスによってブロックされたメッセージの合計数を視覚的に表現します。

セクション	説明
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。 • [接続およびレピュテーションのフィルタリング（Connection and Reputation Filtering）]：レピュテーション フィルタリングと無効な受信者によって脅威として分類されるメッセージ。 • [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。
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。

セクション	説明
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 （19 ページ）
- 受信メール メッセージのカウント方法 （19 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 （70 ページ）

受信メール メッセージのカウント方法

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

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

アプライアンスによる電子メール メッセージの分類方法

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

上記の例では、各種判定は次の優先ルールに従います。

- スパム陽性

- ウイルス陽性
- コンテンツ フィルタとの一致

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

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

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

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

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

カテゴリ（Category）	説明
メール フロー概要：着信	

カテゴリ（Category）	説明
評価フィルタリング	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（受信メール メッセージのカウント方法 （19 ページ）を参照）を掛けたものに、受信者のスロットリングによってブロックされたすべての受信者数を加えた値。 [レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の値は、次の要素に基づいて算出されます。 • 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 ページ上の評価フィルタリングの総数および割合は、すべての拒否された接続の数に常に基づいています。送信者別の接続数だけは、負荷が原因で限定的なものになります。
無効な受信者	従来の LDAP 拒否によって拒否されたすべてのメール受信者数にすべての RAT 拒否数を加えた総数および割合。
スパム対策	アンチスパム スキャン エンジンで陽性、または疑いありとして検出された受信メッセージの総数および割合。さらに、スパムとウイルスの両方で陽性と検出されたメッセージの総数。

カテゴリ（Category）	説明
ウイルス対策	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。
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 （95 ページ）

[システム容量（System Capacity）] ページ

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

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

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

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

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

- **量**：「正常」なメッセージ量と環境内での「通常」のスパイクを把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[受信メール（Incoming Mail）] ページおよび [送信メール（Outgoing Mail）] ページを使用すると、経時的に量を追跡できます。詳細については、[システム容量（System Capacity）] : [受信メール（Incoming Mail）] （58 ページ）および[システム容量（System Capacity）] : [送信メール（Outgoing Mail）] （58 ページ）を参照してください。

- **ワーク キュー**：ワーク キューは、スパム攻撃の吸収とフィルタリングを行い、非スパム メッセージの異常な増加を処理する、「緩衝装置」として設計されています。ただし、作業キューは負荷のかかっているシステムを示す指標でもあります。長く、頻繁な作業キューのバックアップは、キャパシティの問題を示している可能性があります。[システム容量（System Capacity）] : [ワークキュー（Workqueue）] ページを使用すると、作業キュー内のアクティビティを追跡できます。詳細については、[システム容量（System Capacity）] : [ワークキュー（Workqueue）] （57 ページ）を参照してください。
- **リソース節約モード**：アプライアンスがオーバーロードになると、リソース節約モード（RCM）になり、CRITICAL システム アラートが送信されます。このモードは、デバイスを保護し、未処理分のメッセージを処理できるように設計されています。お使いのアプライアンスは、頻繁に RCM になるのではなく、メール量が非常に多い場合または異常に増加した場合にのみ RCM になる必要があります。頻繁な RCM アラートは、システムがオーバーロードになりつつあることを示している可能性があります。リソース節約アクティビティ （59 ページ）を参照してください。

関連項目

- [システム容量（System Capacity）] ページに表示されるデータの解釈方法 （56 ページ）
- [システム容量（System Capacity）] : [ワークキュー（Workqueue）] （57 ページ）
- [システム容量（System Capacity）] : [受信メール（Incoming Mail）] （58 ページ）
- [システム容量（System Capacity）] : [送信メール（Outgoing Mail）] （58 ページ）
- [システム容量（System Capacity）] : [すべて（All）] （59 ページ）
- [システム容量（System Capacity）] グラフのしきい値インジケータ （60 ページ）

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

システムの負荷レポートに、次が表示されます。

- 全体のCPU使用率（Overall CPU Usage） （58 ページ）
- メモリページスワップ（Memory Page Swapping） （59 ページ）
- リソース節約アクティビティ （59 ページ）

全体のCPU使用率（Overall CPU Usage）

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

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

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

メモリページスワップ（Memory Page Swapping）

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

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

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

リソース節約アクティビティ

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

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

[システム容量（System Capacity）]：[すべて（All）]

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

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

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

[高度なマルウェア防御（Advanced Malware Protection）] ページ

高度なマルウェア防御は、次によりゼロデイや電子メールの添付ファイル内のファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。

- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

この機能は着信メッセージと発信メッセージに使用できます。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザ ガイドまたはEメール セキュリティ アプライアンスのAsyncOSのオンライン ヘルプを参照してください。

レポート ページを表示するには、[レポート（Reports）] ドロップダウンの [フィルタおよびマルウェアのレポート（Filter and Malware Reports）] セクションから [高度なマルウェア防御（Advanced Malware Protection）] を選択します。

[高度なマルウェア防御（Advanced Malware Protection）] レポート ページには、次のレポート ビューが表示されます。

- [高度なマルウェア防御（Advanced Malware Protection）] : [概要（Summary）] （79 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）] （79 ページ）
- [高度なマルウェア防御（Advanced Malware Protection）] – [ファイル分析（File Analysis）] （81 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）] （81 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）] （82 ページ）

セキュリティ管理アプライアンスで [高度なマルウェア防御（Advanced Malware Protection）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レポート（Reports）] ドロップダウンから [モニタリング（Monitoring）] > [高度なマルウェア防御（Advanced Malware Protection）] を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[高度なマルウェア防御（Advanced Malware Protection）] レポート ページには、Cisco Threat Grid アプライアンスに接続されたすべての管理対象のアプライアンスのリアルタイム データを提供するメトリック バーが表示されます。

（注）

- メトリック バーでデータを設定するには、CLI で `trailblazerconfig > enable` コマンドを使用する必要があります。詳細については、trailblazerconfig コマンド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 （44 ページ）
- ファイル分析レポートの詳細の要件 （42 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 （48 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）]（79 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）]（81 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るブロックされたファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル（Incoming Malware Threat Files）]セクションで [シンプルカスタム検出（Simple Custom Detection）] として表示されます。
- [カスタムしきい値（Custom Threshold）] に分類されるしきい値設定に基づくブ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）] セクションで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 トラジェクトリ詳細を表示できます。

[リスク低（Low Risk）] 判定の詳細をレポートの [AMPにより渡された受信ファイル（Incoming Files Handed by AMP）] セクションに表示できます。

[高度なマルウェア防御：受信（Advanced Malware Protection: Incoming）] レポート ページの [AMP レピュテーション（AMP Reputation）] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル レピュテーション サービスによって識別された受信ファイルの概要（グラフ形式）。
- 選択した時間範囲に受信されたすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位の受信マルウェア脅威ファイル。
- 上位の受信マルウェア脅威ファイル（ファイル タイプ別）。
- 上位の受信マルウェア脅威ファイルを一覧表示する [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] インタラクティブ テーブル。

  ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

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

[高度なマルウェア防御：送信（Advanced Malware Protection: Outgoing）] レポート ページの [AMP レピュテーション（AMP Reputation）] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル レピュテーション サービスによって識別された送信ファイルの概要（グラフ形式）。
- 選択した時間範囲に送信されたすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位の送信マルウェア脅威ファイル。
- 上位の送信マルウェア脅威ファイル（ファイル タイプ別）。
- 上位の送信マルウェア脅威ファイルを一覧表示する [送信したマルウェア脅威ファイル（Outgoing Malware Threat Files）] インタラクティブ テーブル。

  ドリル ダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。

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

[高度なマルウェア防御（Advanced Malware Protection）]–[ファイル分析（File Analysis）]

[高度なマルウェア防御（Advanced Malware Protection）]–[ファイル分析（File Analysis）]ページには、分析のために送信された各ファイルについて、時刻と判定（または中間判定）が表示されます。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。

1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。

オンプレミスの Cisco AMP Threat Grid Appliance での導入の場合：AMP Threat Grid Appliance で許可リストに含ま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 （44 ページ）を参照してください。

アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の [詳細（Details）] リンクをクリックします。

ファイルを分析したサーバに関する詳細を表示するには、ファイル分析レポートの詳細の要件（42 ページ）を参照してください。

圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析（File Analysis）] レポートに含まれます。

[高度なマルウェア防御（Advanced Malware Protection）] レポート ページの [ファイル分析（File Analysis）] ビューを使用すると、次の情報を表示できます。

- 高度なマルウェア防御エンジンのファイル分析サービスによってファイル分析のためにアップロードされた受信ファイルおよび送信ファイルの数。
- ファイル分析要求が完了している受信ファイルおよび送信ファイルのリスト。
- ファイル分析要求の処理待ちとなっている受信ファイルおよび送信ファイルのリスト。

[高度なマルウェア防御（Advanced Malware Protection）]–[ファイル レトロスペクション（File Retrospection）]

[高度なマルウェア防御（Advanced Malware Protection）] の [ファイル レトロスペクション（File Retrospection）] ページには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。このシナリオの詳細については、お使いの E メール セキュリティ アプライアンスのマニュアルを参照してください。

高度なマルウェア防御は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が明らかになると、脅威の判定が変わる可能性があります。

1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。

1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。

使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。

[高度なマルウェア防御（Advanced Malware Protection）] レポート ページの [ファイル レトロスペクション（File Retrospection）] ビューを使用できます。

- レトロスペクティブな判定変更がある着信ファイルおよび発信ファイルのリスト。

[高度なマルウェア防御（Advanced Malware Protection）] - [メールボックスの自動修復（Mailbox Auto Remediation）]

[高度なマルウェア防御（Advanced Malware Protection）] - [メールボックスの自動修復（Mailbox Auto Remediation）] レポート ページには、受信ファイルに対するメールボックス修復の結果の詳細が表示されます。

[高度なマルウェア防御（Advanced Malware Protection）] - [メールボックスの自動修復（Mailbox Auto Remediation）] ページを使用すると、次などのレトロスペクティブ セキュリティ情報を表示することができます。

- SHA-256 ハッシュに関連付けられているファイル名。
- メッセージに対して行われた修復処理。
- メールボックス修復が成功または失敗した受信者の一覧。

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

- アプライアンスが設定済みの修復のアクションを実行しようとしたときにアプライアンスと Office 365 サービス間の接続に問題があった。

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

ファイル分析レポートの詳細の要件

- （クラウドファイル分析）管理アプライアンスがファイル分析サーバに到達できることを確認する （42 ページ）
- （クラウドファイル分析）詳細なファイル分析結果が表示されるように管理アプライアンスを設定する （42 ページ）
- （オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する （43 ページ）
- 追加の要件 （44 ページ）

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

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

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

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の Cisco E メール セキュリティ アプライアンスまたは Cisco Web セキュリティ アプライアンスから分析用に送信されるファイルに関するクラウド内の詳細な結果が表示されるようにするには、すべてのアプライアンスを同じアプライアンス グループに結合する必要があります。

ステップ 1 Web インターフェイスの [ファイル分析（File Analysis）] セクションにアクセスします。

- レガシー Web インターフェイスで、[管理アプライアンス（Management Appliance）] > [集約サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] をクリックし、[ファイル分析（File Analysis）] セクションまで下にスクロールします。
- 新しい Web インターフェイスで、[サービスステータス（Service Status）] をクリックし、[ファイル分析（File Analysis）] セクションまでスクロールダウンします。

ステップ 2 管理対象アプライアンスが別のファイル分析クラウド サーバを指している場合は、結果の詳細の表示元となるサーバを選択します。

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

ステップ 3 分析グループ ID を入力します。

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

ステップ 4 [今すぐグループ化（Group Now）] をクリックします。

ステップ 5 このアプライアンスとデータを共有する各 E メール セキュリティ アプライアンスで、同じグループを設定します。

次のタスク

関連項目

クラウドで詳細なファイル分析結果が表示されるファイル （48 ページ）

（オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する

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

始める前に

重大レベルでシステム アラートを受信していることを確認します。

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

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

ステップ 2 アラート メッセージ内のリンクをクリックします。

ステップ 3 管理アプライアンスのアカウントをアクティブ化します。

追加の要件

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

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、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。追加列を表示するには、テーブル下部の [列（Columns）] リンクをクリックします。

クラウドで詳細なファイル分析結果が表示されるファイル

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

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

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

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

関連項目

- （クラウドファイル分析）詳細なファイル分析結果が表示されるように管理アプライアンスを設定する （42 ページ）

[ウイルス フィルタリング（Virus Filtering）] ページ

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

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

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

次のリストでは、[ウイルスフィルタリング（Virus Filtering）] レポート ページのさまざまなセクションについて説明します。

表 *14 : [ウイルスフィルタリング（Virus Filtering）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウン リスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
[検出した受信ウイルスタイプの上位（Top Incoming Virus Types Detected）]	このセクションでは、ネットワークに送信されたメッセージ内で検出されたウイルスのチャート ビューが表示されます。
[検出した送信ウイルスタイプの上位（Top Outgoing Virus Types Detected）]	このセクションでは、ネットワークから送信されたメッセージ内で検出されたウイルスのチャート ビューが表示されます。
[ウイルスタイプ詳細（Virus Types Detail）]	各ウイルス タイプの詳細が表示されるインタラクティブ テーブル。 詳細については、[ウイルス タイプ詳細（Virus Types Detail）] テーブル （87 ページ）を参照してください。

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

[ウイルスフィルタリング（Virus Filtering）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

[ウイルスフィルタリング（Virus Filtering）] レポート ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定（133 ページ）を参照してください。

[ウイルス タイプ詳細（Virus Types Detail）] テーブル

[ウイルス タイプ詳細（Virus Types Detail）] テーブルは、ウイルスに感染したメッセージの合計数と、着信および発信メッセージ別の内訳を示すインタラクティブ テーブルです。データをソートするには、列見出しをクリックします。

次の表は、[ウイルス タイプ詳細（Virus Types Detail）] テーブルのテーブル列の説明を示しています。

表 *15 : [ウイルス タイプ詳細（Virus Types Detail）] テーブルのテーブル列の説明*

列名	説明
ウイルス タイプ	ウイルス タイプの名前。
着信メッセージ（Incoming Messages）	ウイルスとして検出された着信メッセージの数。
発信メッセージ（Outgoing Messages）	ウイルスとして検出された送信メッセージの数。
感染したメッセージの合計数	感染したメッセージ（受信および送信）の合計数。

[マクロ検出（Macro Detection）] ページ

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

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

- マクロが有効な送信添付ファイルの総数（ファイル タイプ別、表形式）。

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

[マクロ検出（Macro Detection）] レポート ページから、raw データを CSV ファイルにエクスポートすることができます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

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

（注） レポート生成中に次の処理が発生します。

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

[DMARC検証（DMARC Verification）] ページ

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

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

[DMARC検証（DMARC Verification）] レポート ページを使用すると、次の情報を表示できます。

- 上位ドメイン（DMARC 検証の失敗別、グラフ形式）。
- ドメインの合計（DMARC検証の詳細別、表形式）。詳細については、[DMARC検証の詳細別のドメイン（Domains by DMARC Verification Details）] テーブル （89 ページ）を参照してください。

セキュリティ管理アプライアンスで [DMARC検証（DMARC Verification）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レ

ポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [DMARC検証（DMARC Verification）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

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

[DMARC 検証（DMARC Verification）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

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

[DMARC検証の詳細別のドメイン（Domains by DMARC Verification Details）] テーブル

[DMARC検証の詳細別のドメイン（Domains by DMARC Verification Details）] テーブルは、Domain-based Message Authentication, Reporting and Conformance（DMARC）の失敗（拒否、隔離、またはアクションなし）、試行、および成功があった送信者ドメインの詳細を表示するインタラクティブ テーブルです。

テーブルの情報をカスタマイズしてソートするには、レポート ページのテーブルのカスタマイズ を参照してください。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[アウトブレイク フィルタリング（Outbreak Filtering）] ページ

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

[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

セキュリティ管理アプライアンスで [アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [アウトブレイクフィルタリング（Outbreak Filtering）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

次の表では、[アウトブレイクフィルタリング（Outbreak Filtering）] レポート ページのさまざまなセクションについて説明します。

表 *16 : [アウトブレイクフィルタリング（Outbreak Filtering）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウンリスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポートデータの表示も参照してください。
タイプ別脅威	[タイプ別脅威（Threats By Type）] セクションには、アプライアンスによって受信された脅威メッセージのさまざまなタイプが示されます。
脅威サマリー	[脅威サマリー（Threat Summary）] セクションには、[マルウェア（Malware）]、[フィッシング（Phish）]、[詐欺（Scam）]、および [ウイルス（Virus）] によるメッセージの内訳が示されます。 このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
脅威の詳細	[脅威の詳細（Threat Details）] インタラクティブ テーブルには、脅威のカテゴリ（ウイルス、詐欺、またはフィッシング）、脅威の名前、脅威の説明、識別されたメッセージの数などの、特定の発生に関する詳細が表示されます。 このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
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。

セクション	説明
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 E メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドを参照してください。
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。
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。

詳細については、お使いの E メール セキュリティ アプライアンスのオンライン ヘルプまたはユーザ ガイドの「Outbreak Filters」の章を参照してください。

[URL フィルタリング（URL Filtering）] ページ

URL フィルタリング レポートは、送受信メッセージに対して使用できます。

URL フィルタリング エンジンによって（アンチスパム/アウトブレイク フィルタ スキャンの一部として、またはメッセージ/コンテンツ フィルタを使用して）スキャンされるメッセージのみが、これらのモジュールに含まれます。ただし、必ずしもすべての結果が URL フィルタリング機能のみに起因するわけではできません。

（注） URL フィルタリング レポート モジュールは、URL フィルタリングが有効の場合にのみ入力されます。

[URLフィルタリング（URL Filtering）] レポート ページでは、次の情報を表示できます。

- [上位URLカテゴリ（Top URL Categories）] モジュールには、コンテンツ フィルタまたはメッセージフィルタに一致するかどうかにかかわらず、スキャンされたメッセージで検出されたすべてのカテゴリが含まれます。

  各メッセージを関連付けることができるレピュテーション レベルは 1 つのみです。メッセージに複数の URL がある場合、メッセージ内の URL の最も低いレピュテーションが統計情報に反映されます。

- 上位URLスパムメッセージ（Top URL Spam Messages）

  E メール セキュリティ アプライアンスの [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] ページで設定したグローバル許可リストの 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。

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

次の表では、[URLフィルタリング（URL Filtering）] レポート ページのさまざまなセクションについて説明します。

表 *17 : [URL*フィルタリング（*URL Filtering*）*]* ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウン リスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポートデータの表示も参照してください。
上位URLカテゴリ（Top URL Categories）	このセクションには、着信および発信メッセージの上位 URL カテゴリの概要とグラフィカル ビューが表示されます。 このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。
上位URLスパムメッセージ（Top URL Spam Messages）	このセクションには、着信および発信の上位 URL スパム メッセージの概要とグラフィカル ビューが表示されます。
悪意のあるURLおよびニュートラルなURL（Malicious and Neutral URLs）	このセクションには、着信および発信メッセージの悪意のある URL とニュートラル URL のチャート ビューおよび概要が表示されます。 このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[URLフィルタリング（URL Filtering）] レポート ページから raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

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

[偽装メールの検出（Forged Email Detection）] ページには、次のレポートが含まれています。

- **偽装メールの検出数の上位。**受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書の上位 10 人のユーザを表示します。
- **偽装メールの検出：詳細。**受信したメッセージの偽装された From: ヘッダーと一致する、コンテンツ辞書のすべてのユーザの一覧と、指定したユーザの、一致したメッセージ数を表示します。

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

[偽装メールの検出（Forged Email Detection）] レポートは、[偽装メールの検出（Forged Email Detection）] コンテンツ フィルタまたは `forged-email-detection` メッセージ フィルタを使用している場合にのみ自動入力されます。

[偽装メールの検出（Forged Email Detection）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポート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「非常に問題がある」または「悪い」メッセージのみが、「スパム」や「悪意あり」などの SDR 脅威カテゴリに分類されます。

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

セキュリティ管理アプライアンスで [送信者ドメインのレピュテーション（Sender Domain Reputation）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [送信者ドメインのレピュテーション（Sender Domain Reputation）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[外部脅威フィード（External Threat Feeds）] ページ

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

- メッセージで脅威を検出するために使用される上位 ETF ソース（グラフ形式）。
- メッセージで脅威を検出するために使用される ETF ソースの概要（表形式）。

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

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

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

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

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

セキュリティ管理アプライアンスで [外部脅威フィード（External Threat Feeds）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）]>[外部脅威フィード（External Threat Feeds）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[メール フローの詳細（Mail Flow Details）] ページ

セキュリティ管理アプライアンスの [メールフローの詳細（Mail Flow Details）] レポート ページでは、お使いの管理対象のセキュリティ管理アプライアンスに接続するすべてのリモート ホストのリアルタイム情報がインタラクティブに報告されます。システムに電子メールを送信している IP アドレス、ドメイン、およびネットワーク オーナー（組織）の情報を収集できます。送信メッセージ送信者の IP アドレスおよびドメインに関する情報も収集できます。

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

[メールフローの詳細（Mail Flow Details）] レポート ページには、次のタブがあります。

- 受信メール（Incoming Mails）
- 送信者

データ内の特定の情報を検索するには、検索およびインタラクティブ電子メール レポート ページ （7 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 （98 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 （103 ページ）を参照してください。

  アクセス権限でこのレポートに記載されるメッセージに対するメッセージ トラッキング データを表示するには、表の番号付きハイパーリンクをクリックします。

関連項目

- [ドメイン情報がありません（No Domain Information）] リンク （25 ページ）
- メール トレンド グラフにおける時間範囲 （25 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 （26 ページ）を参照してください。

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

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

IP アドレス、ドメイン、またはネットワーク オーナーをクリックすると、[送信者プロファイル（Sender Profile）] ページの送信者の詳細にアクセスできます。[送信者プロファイル（Sender Profile）] ページは、特定の IP アドレス、ドメインまたはネットワーク オーナーに固有の [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 （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）] ページから、raw データを CSV ファイルにエクスポートできます。

[メールフローの詳細（Mail Flow Details）]：[送信（Outgoing）] レポート ページには次の 2 種類のビューがあります。

- IP アドレス

- ドメイン（Domains）

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

選択したビューに応じて、[送信者の詳細（Sender Details）] インタラクティブ テーブルに、E メール セキュリティ アプライアンスで設定されたパブリック リスナーから電子メールを送信した上位 IP アドレス、ドメイン、または送信者が表示されます。アプライアンスから出たすべてのメールのフローをモニタできます。

[送信者の詳細（Sender Details）] インタラクティブ テーブルに含まれるデータの説明については、[送信者の詳細（Sender Details）] テーブル （103 ページ）を参照してください。

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

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

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

メール トレンド グラフにおける時間範囲

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

時間範囲の詳細については、レポートの時間範囲の選択を参照してください。

[受信メール（Incoming Mails）] テーブル

[メールフローの詳細：受信メール（Mail Flow Details: Incoming Mails）] ページの下部にあるインタラクティブな [受信メール（Incoming Mails）] テーブルには、E メール セキュリティ ア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、AsyncOS E メール セキュリティ アプライアンスのユーザ ガイドまたはオンライン ヘルプを参照してください。

[受信メール（Incoming Mails）] テーブルの最初の列、または [脅威メッセージの送信者上位（Top Senders by Total Threat Messages）] に表示される送信者、つまりネットワーク オーナー、IP アドレスまたはドメインについては、[送信者（Sender）] または [ドメイン情報がありません（No Domain Information）] リンクをクリックすると、送信者の詳細情報が表示されます。結果は、[送信者プロファイル（Sender Profile）] ページに表示され、SenderBase レピュテーショ

ン サービスからのリアルタイム情報が含まれます。送信者プロファイル ページからは、特定の IP アドレスまたはネットワーク オーナーに関する詳細を表示できます。詳細については、[送信者プロファイル（Sender Profile）] ページ （26 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（Sender Groups）] レポート ページ （104 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 *18 : [*受信メール（*Incoming Mail*）*]* テーブル内の列の詳細

列名	説明
送信者ドメイン（ドメイン）（Sender Domain (Domains)）	送信者のドメイン名。
送信者 IP アドレス（IP アドレス）（Sender IP Address (IP Addresses)）	送信者の IP アドレス。
ホスト名（IP アドレス）（Hostname (IP Addresses)）	送信者のホスト名。
DNS検証（IPアドレス）（DNS Verified (IP Addresses)）	DNS によって検証された IP アドレス。
SBRS（IPアドレス）（SBRS (IP Addresses)）	送信者の SenderBase レピュテーション スコア。
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 Reputation Filtering）]	[レピュテーションフィルタによる停止（Stopped by Reputation Filtering）] の値は、次の複数の要素に基づいて算出されます。 • 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（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。
合計脅威件数（Total Threat）	脅威メッセージ（評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの）の総数
Marketing	不要なマーケティング メッセージとして検出されたメッセージの数。
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] 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。[メールフローの詳細（Mail Flow Details）] ページまたは他の [送信者プロファ

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。

- SenderBase レピュテーション サービスからのグローバル情報。たとえば、次の情報です。
  - IP アドレス、ドメイン名、またはネットワーク オーナー
  - ネットワーク オーナーのカテゴリ（ネットワーク オーナーのみ）
  - CIDR 範囲（IP アドレスのみ）
  - IP アドレス、ドメイン、またはネットワーク オーナーの日単位マグニチュードおよび月単位マグニチュード
  - この送信者から最初のメッセージを受信してからの日数
  - 最後の送信者グループと DNS が検証されたかどうか（IP アドレス送信者プロファイル 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）
- SenderBase 評価スコア（IP アドレス プロファイル ページのみ）
- 最初のメッセージからの日数（ネットワーク オーナーとドメイン プロファイル ページのみ）
- このネットワーク オーナーに関連するドメインの数（ネットワーク オーナープロファイル ページおよびドメイン プロファイル ページのみ）
- このネットワーク オーナーの IP アドレスの数（ネットワーク オーナー プロファイル ページおよびドメイン プロファイル ページのみ）
- 電子メールの送信に使用された IP アドレスの数（ネットワーク オーナー ページのみ）

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

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

ドメイン プロファイルのページから、特定の IP アドレスをクリックして特定の情報を表示することも、組織プロフ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、E メール セキュリティ アプライアンス上のパブリック リスナーに接続された上位送信者が表示されます。このテーブルには、選択したビューに基づいて、ドメインまたは IP アドレスが表示されます。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表に、[送信者の詳細（Sender Details）] テーブル内の列の詳細を示します。

表 *19 : [*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。

列名	説明
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（Sender Groups）] レポート ページ

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

セキュリティ管理アプライアンスで [送信者グループ（Sender Groups）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レポー

ト（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [送信者グループ（Sender Groups）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[送信者グループ（Sender Group）] レポート ページから、raw データを CSV ファイルにエクスポートすることができます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポート を参照してください。

（注） [送信者グループ（Sender Group）] レポート ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

[送信先（Outgoing Destinations）] ページ

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

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

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

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

データ内の特定の情報を検索するには、検索およびインタラクティブ電子メール レポート ページ （7 ページ）を参照してください。

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

表 *20 : [送信先（Outgoing Destinations）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。

セクション	説明
[次のデータを参照（View Data For）]（ドロップダウンリスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）]を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
脅威メッセージの配信先上位（Top Destinations by Total Threat Messages）	組織によって送信された発信脅威メッセージ（スパム、アンチウイルスなど）の上位の宛先ドメイン。合計脅威メッセージには、スパムやウイルス検出、またはコンテンツ フィルタによってトリガーされたメッセージが含まれます。
正常なメッセージの配信先上位（Top Destinations by Clean Messages）	組織によって送信されたクリーンな発信脅威メッセージの上位の宛先ドメイン。
送信先の詳細（Outgoing Destinations Details）	組織によって送信されたすべての発信メッセージの宛先ドメインに関する、総受信者数別にソートされたすべての詳細情報。詳細情報には検出されたスパム、ウイルス、クリーンメッセージなどが含まれます。 詳細については、送信先の詳細の表 （106 ページ）を参照してください。 このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[送信先（Outgoing Destinations）] レポート ページから raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポート を参照してください。

[送信先（Outgoing Destinations）] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

関連項目

送信先の詳細の表 （106 ページ）

送信先の詳細の表

[送信先の詳細（Outgoing Destinations Detail）] テーブルは、処理されて配信されたメッセージの合計数、脅威（スパム、ウイルス等）またはクリーンであるとして処理されたメッセージの内訳、ハードバウンス済みまたは配信済みメッセージを示すインタラクティブ テーブルです。データをソートするには、列見出しをクリックします。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

次の表は、[送信先の詳細（Outgoing Destinations Detail）] テーブルのテーブル列の説明を示しています。

表 *21 : [*送信先の詳細（*Outgoing Destinations Detail***）*]* テーブルのテーブル列の説明**

列名	説明
宛先ドメイン	宛先ドメインの名前。
スパム検出（Spam Detected）	スパムとして検出されたメッセージ数。
ウイルス検出（Virus Detected）	スパムとして検出されたメッセージ数。
コンテンツフィルタによる阻止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの数。
合計脅威件数（Total Threat）	脅威（スパム、ウイルス等）として検出されたメッセージの合計数。
クリーン（Clean）	クリーンであると検出されたメッセージの数
処理済みメッセージの合計（Total Proceed）	脅威またはクリーンであるとして処理されたメッセージの合計数。
ハード バウンス（Hard Bounces）	永続的に配信不能としてマークされたメッセージの数。
配信済み（Delivered）	配信されるメッセージの数。
送信済みメッセージの合計（Total Messages Delivered）	配信されるメッセージの合計数（ハード バウンスを含む）。

[TLS暗号化（TLS Encryption）] ページ

[TLS暗号化（TLS Encryptions）] 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送信 TLS 接続に成功したパートナー。
- DANE がサポートされている送信 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。

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

[TLS暗号化（TLS Encryptions）] レポート ページには、次のタブがあります。

- 着信
- 発信

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 （7 ページ）を参照してください。

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

表 *22 : [TLS*暗号化（*TLS Encryptions*）*]* ページの詳細

[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウンリスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。

TLS接続数グラフ（TLS Connections Graph）	[TLS暗号化：着信（TLS Encryption: Incoming）] ページには、選択された時間枠に応じ、直近 1 時間、1 日間、1 週間、1 ヵ月間、または 1 年間に着信した、暗号化された/暗号化されていないTLS接続がグラフ形式で表示されます。 [TLS暗号化：発信（TLS Encryption: Outgoing）] ページには、選択された時間枠に応じ、直近 1 時間、1 日間、1 週間、1 ヵ月間、または 1 年間に発信された、暗号化された/暗号化されていない TLS 接続がグラフ形式で表示されます。
TLS接続数サマリー（TLS Connections Summary）	[TLS暗号化：着信（TLS Encryption: Incoming）] ページでは、着信メッセージの総量、暗号化された/暗号化されていないメッセージの量、成功/失敗した受信TLS暗号化メッセージの量が表形式で表示されます。 [TLS暗号化：発信（TLS Encryption: Outgoing）] ページでは、発信メッセージの総量、暗号化された/暗号化されていないメッセージの量、成功/失敗した送信 TLS 暗号化メッセージの量、および成功/失敗したDANEがサポートされている発信 TLS 接続の量が表形式で表示されます。
TLSメッセージ（TLS Messages）	[TLS暗号化：着信（TLS Encryption: Incoming）] ページでは、TLS 暗号化されている/されていない着信メッセージの総数と割合が、グラフ形式で表示されます。 [TLS暗号化：発信（TLS Encryption: Outgoing）] ページでは、TLS 暗号化されている/されていない発信メッセージの総数と割合が、グラフ形式で表示されます。
TLSメッセージ数サマリー（TLS Messages Summary）	この表には、TLS 暗号化されている/されていない着信メッセージおよび発信メッセージの総数および割合の概要が表示されます。

TLS接続数詳細（TLS Connections Details）	この表には、暗号化されたメッセージを送受信するドメインの詳細が表示されます。各ドメインについて、接続の総数、送信されたメッセージ、および成功/失敗したTLS接続の数を表示できます。各ドメインについて、成功/失敗した接続の割合を表示することもできます。 詳細については、TLS 接続数詳細テーブル （110 ページ）を参照してください。

関連項目

TLS 接続数詳細テーブル （110 ページ）

TLS 接続数詳細テーブル

TLS 接続数詳細テーブルは、接続、送信したメッセージ、および成功または失敗した TLS 接続の数の合計数、着信および発信メッセージの最終TLS ステータスを表示する、対話型のテーブルです。各ドメインについて、成功/失敗した接続の割合を表示することもできます。

次の表は、TLS 接続数詳細テーブルの列の説明を示しています。

表 *23 : TLS* 接続数詳細テーブルの列の説明

列名	説明
ドメイン	送信者のドメイン名。
成功したTLS必須失敗しました（Failed）	失敗した、必要なすべての TLS 接続。
成功した TLS 必須Success	成功した、必要なすべての TLS 接続。
失敗したTLS推奨（TLS Pref. Failed）	失敗した、優先するすべての TLS 接続。
成功したTLS推奨（TLS Pref. Success）	成功した、優先するすべての TLS 接続。
最終 TLS ステータス	次の条件に基づいて割り当てられた TLS 接続のステータス： • 0：なし • 1：必須 - 失敗 • 2：推奨 - 失敗 • 3：必須 - 成功 • 4：推奨 - 成功

列名	説明
DANE失敗（DANE Failure）	DANE がサポートされている送信 TLS 接続の失敗の合計数。
DANE成功（DANE Success）	DANE がサポートされている送信 TLS 接続の成功の合計数。
合計TLS接続数（Total TLS Connections）	TLS 接続の合計数。
暗号化されていない接続（Unencrypted Connections）	暗号化されていない TLS 接続の合計数。
TLSの割合(%%)（% TLS of all Connections）	すべての TLS 接続に対する TLS 暗号化の割合。
TLS経由のメッセージ（Messages by TLS）	TLS メッセージの総数。

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

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

次の情報を確認するには、このレポートを使用します。

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

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

[受信SMTP認証（Inbound SMTP Authentication）] には 2 つのビューがあります。

- ドメイン（Domains）

- IP アドレス

これらのビューでは、SMTP認証のスナップショットが、選択したビューのコンテキストで提供されます。

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

次のリストでは、[受信SMTP認証（Inbound SMTP Authentication）] レポート ページのさまざまなセクションについて説明します。

表 *24 : [受信SMTP認証（Inbound SMTP Authentication）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウンリスト）	データを表示するEメールセキュリティアプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
[受信した接続（Received Connections）] グラフ	[受信した接続（Received Connections）] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメール クライアントの着信接続が示されます。このグラフには、アプライアンスが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。
[受信した受信者（Received Recipients）] グラフ	[受信した受信者（Received Recipients）] グラフには、SMTP認証を使用して、メッセージを送信するためにEmail Security Appliances への接続を認証しようとしたメール クライアントを所有する受信者の数が表示されます。このグラフでは、接続が認証された受信者の数、および接続が認証されなかった受信者の数も示されます。

セクション	説明
（ドメイン名または IP アドレスによる）SMTP 認証の詳細。	（ドメイン名または IP アドレスによる）SMTP 認証の詳細テーブルには、メッセージを送信するために E メール セキュリティ アプライアンスへの接続を認証しようとするユーザの詳細が表示されます。ドメインごとに、クライアント証明書を使用した接続試行（成功または失敗）の数、SMTP AUTH コマンドを使用した接続試行（成功または失敗）の数、およびクライアント証明書接続試行が失敗した後、SMTP AUTH にフェールバックした接続の数を表示できます。

[レート制限（Rate Limits）] ページ

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

このレポートは、以下を特定する場合に役立ちます。

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

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

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

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

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

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

関連項目

[大容量のメール（High Volume Mail）] ページ （125 ページ）

[国別の接続（Connections by Country）] ページ

[国別の接続（Connections by Country）] レポート ページを使用すると、次の情報を表示できます。

- 発信国別の受信メール接続数の上位（グラフィカルな形式）。
- 発信国別の受信メール接続およびメッセージの合計数（表形式）。

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

国情報を表示しない受信メール接続の上位と合計数の例を次に示します。

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

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

[国別の接続（Connections by Country）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

ユーザメール概要（User Mail Summary）

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

[ユーザメール概要（User Mail Summary）] レポート ページを使用すると、次の情報を表示することができます。

- 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

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

データ内の特定の情報を検索するには、検索およびインタラクティブ電子メール レポート ページ （7 ページ）を参照してください。

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

表 *25 : [ユーザメール概要（User Mail Summary）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウン リスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
[正常な受信メッセージ数の上位ユーザ（Top Users by Clean Incoming Messages）]	組織内で受信された正常な着信メッセージの上位ユーザ（ドメイン別）。
[正常な送信メッセージ数の上位ユーザ（Top Users by Clean Outgoing Messages）]	組織によって送信された正常な発信メッセージの上位ユーザ（ドメイン別）。
[グレイメールの上位ユーザ（Top Users by Graymail）]	グレイメール メッセージの上位ユーザ（ドメイン別）。

セクション	説明
[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）] インタラクティブ テーブルでは、電子メール アドレスごとに送受信メールが分類されます。列ヘッダーをクリックすることにより、表示をソートできます。 詳細については、[ユーザメールフローの詳細（User Mail Flow Details）] テーブル （116 ページ）を参照してください。 このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[ユーザメール概要（User Mail Summary）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

（注） [ユーザメール概要（User Mail Summary）] レポート ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

関連項目

- [ユーザメールフローの詳細（User Mail Flow Details）] テーブル （116 ページ）
- 特定の内部ユーザの検索 （33 ページ）

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

[ユーザメールフローの詳細（User Mail Flow Details）] テーブルでは、受信および送信メッセージの内訳、各カテゴリ（[スパム検出（Spam Detected）]、[ウイルス検出（Virus Detected）]、[コンテンツフィルタによる停止（Stopped By Content Filter）] など）のメッセージ数など、ユーザに関する詳細情報が示されます。送受信コンテンツ フィルタの一致も示されます。

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

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

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の番号リンクをクリックします。

次の表は、[ユーザメールフローの詳細（User Mail Flow Details）] テーブルの列の説明を示しています。

表 *26 : [*ユーザメールフローの詳細（*User Mail Flow Details*）*]* テーブルの列の説明

列名	説明
内部ユーザ	内部ユーザのドメイン名。
[受信スパム検出（Incoming Spam Detected）]	検出されたすべての受信スパム。
[受信ウイルス検出（Incoming Virus Detected）]	検出された受信ウイルス。
高度なマルウェア防御で検出された受信メール（Incoming Detected by Advanced Malware Protection）	高度なマルウェア防御（ファイル分析とファイル レピュテーション）で検出された受信メッセージ。
[受信コンテンツフィルタの一致数（Incoming Content Filter Matches）]	検出された受信コンテンツ フィルタの一致。
[コンテンツフィルタによる受信停止（Incoming Stopped by Content Filter）]	設定したコンテンツ フィルタによって阻止された受信メッセージ。
受信マーケティング（Incoming Marketing）	マーケティングとして検出された受信メッセージ。
受信ソーシャルネットワーキング（Incoming Social Networking）	ソーシャル ネットワーキングとして検出された受信メッセージ。
受信バルク（Incoming Bulk）	バルクとして検出された受信メッセージ。
受信グレイメール（Incoming Graymails）	グレイメールとして検出された受信メッセージ。
[正常な受信（Incoming Clean）]	すべての着信クリーン メッセージ。
[送信スパム検出（Outgoing Spam Detected）]	検出された発信スパム。
[送信ウイルス検出（Outgoing Virus Detected）]	検出された送信ウイルス。
[送信コンテンツフィルタの一致数（Outgoing Content Filter Matches）]	検出された送信コンテンツ フィルタの一致。

列名	説明
[コンテンツフィルタによる送信停止（Outgoing Stopped by Content Filter）]	設定されていたコンテンツ フィルタのため阻止された発信メッセージ。
[正常な送信（Outgoing Clean）]	すべての発信クリーン メッセージ。

特定の内部ユーザの検索

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

[DLP インシデント サマリー（DLP Incident Summary）] ページ

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

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

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

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

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

セキュリティ管理アプライアンスで [DLPインシデントサマリー（DLP Incident Summary）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）]

を選択し、[レポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [DLPインシデントサマリー（DLP Incident Summary）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[DLPインシデント（DLP Incidents）] レポート ページから raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

データ内の特定の情報を検索するには、検索およびインタラクティブ電子メール レポート ページ （7 ページ）を参照してください。

次のリストでは、[DLPインシデントサマリー（DLP Incident Summary）] レポート ページのさまざまなセクションについて説明します。

表 *27 : [DLPインシデントサマリー（DLP Incident Summary）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウンリスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
[重大度別上位インシデント（Top Incidents by Severity）]	重大度別の上位 DLP インシデント。
[インシデントサマリー（Incident Summary）]	各電子メール アプライアンスの送信メール ポリシーで現在有効になっている DLP ポリシーは、[DLPインシデントサマリー（DLP Incident Summary）] ページの下部にある [DLPインシデントの詳細（DLP Incident Details）] インタラクティブ テーブルに表示されます。詳細情報を表示するには、DLP ポリシーの名前をクリックします。
[上位DLPポリシー一致数（Top DLP Policy Matches）]	一致している上位 DLP ポリシー。

セクション	説明
[DLPインシデントの詳細（DLP Incident Details）]	[DLPインシデントの詳細（DLP Incidents Details）] テーブルには、ポリシーごとのDLPインシデントの数に加えて、重大度レベル別の内訳、メッセージのいずれかがクリアに配信されたか、暗号化されて配信されたか、ドロップされたかが示されます。 このレポートに記載されるメッセージに対するメッセージトラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[Web インタラクション（Web Interaction）] ページ

[Webインタラクション（Web Interaction）] レポート ページでは、次の情報を表示できます。

- 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）。
- 書き換えられた悪意のある URL をクリックした上位ユーザ（Top 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）。

（注） Web インタラクション レポート モジュールは、Web インタラクション トラッキング機能が管理対象のEメールセキュリティアプライアンスで有効になっている場合にのみ入力されます。

Web インタラクション レポートは、送受信メッセージに対して使用できます。エンドユーザがクリックした、書き換えられた URL（ポリシーまたはアウトブレイク フィルタによって）のみが、これらのモジュールに含まれます。

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

[Webインタラクション（Web Interaction）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

次のリストでは、[Webインタラクション（Web Interaction）] 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 *28 : [Web*インタラクション（*Web Interaction*）*]* ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	表示する時間範囲を選択するためのオプションを伴うドロップダウン リスト。詳細については、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data For）]（ドロップダウンリスト）	データを表示する E メール セキュリティ アプライアンスを選択するか、[全Eメールアプライアンス（All Email Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
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）	このセクションには、エンド ユーザによって最も多くクリックされた悪意のある URL の概要が表示されます。
悪意のあるURLをクリックした上位ユーザ（Top 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）	このセクションには、着信および発信メッセージの悪意のある URL とニュートラル URL のチャート ビューおよび概要が表示されます。 このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

Webインタラクショントラッキングの詳細（Web Interaction Tracking Details）

[Webインタラクショントラッキングの詳細（Web Interaction Tracking Details）] テーブルは、次の情報を含むインタラクティブ テーブルです。

- 書き換えられたすべての URL のリスト（悪意のあるものとないもの）。
- 書き換えられた URL がクリックされた場合に実行されたアクション（許可、ブロック、または不明）。
- エンドユーザが URL をクリックしたときにその URL の判定（クリーンまたは悪意のある）が不明である場合、ステータスは不明として表示されます。これは、ユーザのクリック時に、URL がさらに調査されていたか、Web サーバがダウンしていたか、到達不可能であったためである可能性があります。
- 書き換えられた URL をエンドユーザがクリックした回数。
- 次の点に注意してください。

- 悪意のあるURLを書き換えた後に、メッセージを送信して別のユーザ（管理者など）に通知するようにコンテンツまたはメッセージフィルタを設定している場合、通知されたユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクション トラッキング データが増分します。
- 書き換えられた URL を含む隔離されたメッセージのコピーを、Web インターフェイスを使用して元の受信者以外のユーザ（管理者など）に送信する場合、その他のユーザがその書き換えられた URL をクリックすると、元の受信者の Web インタラクション トラッキング データが増分します。

このレポートに記載されるメッセージに対するメッセージ トラッキングの詳細を表示するには、表の青い番号のリンクをクリックします。

[修復レポート（Remediation Reports）] ページ

[修復レポート（Remediation Report）] ページには、[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）] を使用して修復を試行したメッセージの修復結果が表示されます。

セキュリティ管理アプライアンスで、[モニタリング（Monitoring）] タブをクリックし、[メールフローの概要（Mail Flow Summary）] > [ユーザレポート（User Reports）] > [修復レポート（Remediation Report）] を選択します。

このレポートを使用して、次を行うことができます。

- [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）] を使用して修復を試行したメッセージを表示します。
- 修復失敗の理由を確認します。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、[修復レポート（Remediation Report）]ページのさまざまなセクションについて説明します。

表 *29 : [*修復レポート（*Remediation Reports***）*] ページの詳細**

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）] レポート	[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修復処理。 • 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。 • 修復に失敗した理由。 （注） AsyncOS 13.6.1 にアップグレードすると、アップグレード前に受信したメッセージのメッセージ トラッキング ステータスは、「修正済み」ではなく「配信済み」のままになります。

セクション	説明

[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。
	  • 修復が開始された日付と時刻。
	  • 修復が開始された送信元。
	  • メッセージの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）] レポート ページには、送受信メッセージのメッセージ フィルタの上位一致（最も多くのメッセージに一致したメッセージ フィルタ）に関する情報が表示されます。

[メッセージ フィルタ（Message Filters）] レポート ページを使用すると、次を表示できます。

- グラフィカル形式での、一致数による上位メッセージ フィルタ。
- 表形式での、一致数による上位メッセージ フィルタ。

セキュリティ管理アプライアンスで [メッセージフィルタ（Message Filters）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レ

ポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [メッセージフィルタ（Message Filters）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[メッセージ フィルタ（Message Filters）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

[大容量のメール（High Volume Mail）] ページ

[大容量のメール（High Volume Mail）] レポート ページを使用すると、次の操作を実行することができます。

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

[大容量のメール（High Volume Mail）] レポート ページを使用すると、次の情報を表示することができます。

- 上位の件名を持つメッセージ（グラフ形式）。
- 上位のエンベロープ送信者を持つメッセージ（グラフ形式）。
- 上位のメッセージ フィルタ（一致数別、グラフ形式）。
- メッセージ フィルタの合計（一致数別、表形式）。

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

[大容量のメール（High Volume Mail）] レポート ページから、raw データを CSV ファイルにエクスポートすることができます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

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

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

[コンテンツフィルタ（Content Filters）] ページ

[コンテンツフィルタ（Content Filters）] レポート ページには、送受信コンテンツ フィルタの上位一致（最も多くのメッセージに一致したコンテンツ フィルタ）に関する情報が表示されます。このページでは、データが棒グラフとリストの形式でも表示されます。[コンテンツ フィルタ（Content Filters）] レポート ページを使用して、次のタイプの質問に答えることができます。

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

[コンテンツ フィルタ（Content Filters）] レポート ページを使用すると、次を表示できます。

- グラフィカル形式での、上位の着信および発信コンテンツ フィルタの一致。
- 表形式での、上位の着信および発信コンテンツ フィルタの一致。

セキュリティ管理アプライアンスで [コンテンツフィルタ（Content Filters）] レポート ページを表示するには、[製品（Product）] ドロップダウンから [電子メール（Email）] を選択し、[レポート（Reports）] ドロップダウンから **[モニタリング（Monitoring）] > [コンテンツフィルタ（Content Filters）]** を選択します。詳細については、インタラクティブ レポート ページの使用を参照してください。

[コンテンツ フィルタ（Content Filters）] レポート ページから、raw データを CSV ファイルにエクスポートできます。ファイルを印刷またはエクスポートする方法の詳細については、レポーティング データおよびトラッキング データのエクスポートを参照してください。

（注） 注：[コンテンツフィルタ（Content Filter）] ページのスケジュール設定されたレポートを生成できます。メール レポートのスケジュール設定 （133 ページ）を参照してください。

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

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

[内部ユーザ別の一致（Matches by Internal User）] セクションで、内部ユーザ（電子メール アドレス）の詳細ページを表示するユーザ名をクリックします。詳細については、ユーザメール概要（User Mail Summary） （114 ページ）を参照してください。

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

グレイメールのレポート

グレイメールの統計情報は、次のレポートに反映されます。

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

関連項目

- AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート （55 ページ）

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

AsyncOS 9.5 へのアップグレード後：

- マーケティング メッセージの数は、アップグレードの前後に検出されたマーケティング メッセージの合計です。
- グレイメール メッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数は含まれません。
- 試行されたメッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数も含まれます。

- 管理対象の E メール セキュリティ アプライアンスでグレイメール機能が有効になっていない場合、マーケティング メッセージはクリーン メッセージとしてカウントされます。

スケジュール設定された電子メールレポートとオンデマンドの電子メール レポートについて

使用可能なレポートの種類

特記のない限り、次のタイプの電子メール セキュリティ レポートは、スケジュール設定されたレポートおよびオンデマンド レポートとして使用できます。

- [コンテンツフィルタ（Content Filters）]：このレポートには最大 40 のコンテンツ フィルタが表示されます。このページに表示されるその他の情報については、[コンテンツフィルタ（Content Filters）] ページ （126 ページ）を参照してください。
- [DLPインシデントサマリー（DLP Incident Summary）]：このページに表示される情報については、[DLP インシデント サマリー（DLP Incident Summary）] ページ （118 ページ）を参照してください。
- [送信処理ステータス（Delivery Status）]：このレポート ページには、特定の受信者ドメインまた仮想ゲートウェイ アドレスへの配信の問題についての情報が表示されます。また、このページには、直近 3 時間以内にシステムによって配信されたメッセージの上位 20、50、または 100 の受信者ドメインのリストが表示されます。各統計情報の列見出しのリンクをクリックすることによって、最新のホスト ステータス、アクティブな受信者（デフォルト）、切断した接続、配信された受信者、ソフト バウンス イベント、およびハード バウンス受信者別にソートできます。E メール セキュリティ アプライアンスでの [送信処理ステータス（Delivery Status）] ページの役割の詳細については、お使いの E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。
- [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）]：このレポートは [メール フロー概要（Mail Flow Summary）] ページ （66 ページ）に基づき、指定されたドメインのグループに制限されます。表示される情報については、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート （129 ページ）を参照してください。
- [エグゼクティブサマリー（Executive Summary）]：このレポートは [メール フロー概要（Mail Flow Summary）] ページ （66 ページ）の情報に基づきます。表示される情報については、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート （129 ページ）を参照してください。
- [メールフローの詳細（Mail Flow Details）]：このページに表示される情報については、[メール フローの詳細（Mail Flow Details）] ページ （95 ページ）を参照してください。
- [ユーザメール概要（User Mail Summary）]：このページに表示される情報については、ユーザメール概要（User Mail Summary） （114 ページ）を参照してください。
- [送信先（Outgoing Destinations）]：このページに表示される情報については、[送信先（Outgoing Destinations）] ページ （105 ページ）を参照してください。
- [送信者グループ（Sender Groups）]：このページに表示される情報については、[送信者グループ（Sender Groups）] レポート ページ （104 ページ）を参照してください。

- [TLS暗号化（TLS Encryption）]：このページに表示される情報については、[TLS暗号化（TLS Encryption）] ページ （107 ページ）を参照してください。
- [ウイルスタイプ（Virus Types）]：このページに表示される情報については、[ウイルス フィルタリング（Virus Filtering）] ページ （85 ページ）を参照してください。

時間範囲

各レポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、または過去の月（最大 12 ヵ月）のデータを含めるように設定できます。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヵ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

言語とロケール

（注） 個々のレポートに特定のロケールを使用して、PDF レポートをスケジュール設定したり、raw データを CSV ファイルとしてエクスポートしたりすることができます。[スケジュール設定されたレポート（Scheduled Reports）] ページの言語ドロップダウン メニューでは、ユーザが現在選択しているロケールおよび言語で PDF レポートを表示またはスケジュールすることができます。レポーティング データおよびトラッキング データのエクスポートの重要な情報を参照してください。

アーカイブ済みレポートの保存

レポートの保存期間や、アーカイブ済みレポートがいつシステムから削除されるかについては、[アーカイブ メール レポート（Archived Email Reports）] の表示と管理 （137 ページ）を参照してください。

その他のレポート タイプ

セキュリティ管理アプライアンスの [メール（Email）] > [レポート（Reporting）] セクションでは、次の 2 種類の特別なレポートを生成できます。

- [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート （129 ページ）
- [エグゼクティブサマリー（Executive Summary）] レポート （133 ページ）

[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート

[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートには、ネットワーク内の 1 つまたは複数のドメインの着信および発信メッセージの概要が表示されます。これは [エグゼクティブサマリー（Executive Summary）] レポートと似ていますが、レポート データが、指定したドメインで送受信されるメッセージに制限されます。[送信メールサマ

リー（Outgoing Mail Summary）] には、送信サーバの PTR（ポインタ レコード）のドメインが、指定したドメインに一致する場合にのみデータが表示されます。複数のドメインが指定されている場合、このアプライアンスはすべてのドメインのデータを1つのレポートに集約します。

サブドメインのレポートを生成するには、E メールセキュリティアプライアンスおよびセキュリティ管理アプライアンスのレポーティング システムで、親ドメインをセカンドレベル ドメインとして追加する必要があります。たとえば、example.com をセカンドレベル ドメインとして追加した場合、subdomain.example.com のようなサブドメインをレポーティングに使用できるようになります。セカンドレベル ドメインを追加するには、E メール セキュリティ アプライアンスの CLI で **reportingconfig -> mailsetup -> tld** を実行し、セキュリティ管理アプライアンスの CLI で **reportingconfig -> domain -> tld** を実行します。

その他のスケジュール設定されたレポートとは異なり、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートはアーカイブされません。

[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートと送信者レピュテーション フィルタリングによってブロックされたメッセージ

送信者レピュテーション フィルタリングによってブロックされたメッセージはワーク キューに入らないため、AsyncOS はこれらのメッセージに対して、宛先ドメインを判定するための処理は行いません。アルゴリズムによって、ドメインごとに拒否されたメッセージ数が推定されます。ドメインごとのブロックされたメッセージの正確な数を知るには、メッセージが受信者レベル（RCPT TO）に達するまでセキュリティ管理アプライアンスでの HAT 拒否を遅らせます。そうすることで、AsyncOS が着信メッセージから受信者データを収集できるようになります。E メール セキュリティ アプライアンスで **listenerconfig -> setup** コマンドを使用して拒否を遅らせることができます。ただし、このオプションはシステムのパフォーマンスに影響を及ぼす可能性があります。遅延した HAT 拒否の詳細については、ご使用の E メール セキュリティ アプライアンスのマニュアルを参照してください。

（注） セキュリティ管理アプライアンスのドメインごとのエグゼクティブ サマリー レポートでレピュテーション フィルタによる停止を表示するには、E メール セキュリティ アプライアンスとセキュリティ管理アプライアンスの両方で **hat_reject_info** を有効にする必要があります。セキュリティ管理アプライアンス上で **hat_reject_info** を有効にするには、**reportingconfig > domain > hat_reject_info** コマンドを実行します。

[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートのドメインおよび受信者のリストの管理

コンフィギュレーション ファイルを使用して、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートのドメインおよび受信者を管理できます。コンフィギュレーション ファイルは、アプライアンスのコンフィギュレーション ディレクトリに保存されるテキスト ファイルです。このファイルの行ごとに、個別のレポートが生成されます。これによって、大量のドメインおよび受信者を1つのレポートに含めることができ、複数のドメイン レポートを 1 つのコンフィギュレーション ファイルで定義できます。

コンフィギュレーションファイルの各行には、ドメイン名のスペース区切りリストと、レポート受信者の電子メールアドレスのスペース区切りリストが含まれます。ドメイン名のリストと電子メール アドレスのリストはカンマで区切られます。subdomain.example.com のように、親ドメイン名の前にサブドメイン名とピリオドを追加すると、サブドメインを含めることができます。

次に示すファイルは、3 つのレポートを生成する 1 つのレポート コンフィギュレーション ファイルです。

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```

（注） コンフィギュレーション ファイルと 1 つの名前付きレポートに定義された設定を使用して、複数のレポートを同時に生成することができます。たとえば、Bigfish という名前の会社が Redfish と Bluefish という名前の会社を買収し、Redfish と Bluefish のドメインを引き続き維持するとします。Bigfish 社は、個々のドメイン レポートに対応する 3 行が含まれるコンフィギュレーション ファイルを使用して 1 つの [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートを作成します。アプライアンスで [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートが生成されると、Bigfish 社の管理者は Bigfish.com、Redfish.com、および Bluefish.com ドメインのレポートを受信し、Redfish 社の管理者は Redfish.com ドメインのレポートを受信し、Bluefish 社の管理者は Bluefish.com ドメインのレポートを受信します。

名前付きレポートごとに異なるコンフィギュレーション ファイルをアプライアンスにアップロードできます。また、複数のレポートに対して同じコンフィギュレーションファイルを使用することもできます。たとえば、異なる期間の同じドメインに関するデータが表示される、複数の名前付きレポートを作成できます。アプライアンスにコンフィギュレーションファイルをアップロードする場合は、ファイル名を変更しない限り、GUI でレポート設定を更新する必要がありません。

[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートの作成

ステップ 1 セキュリティ管理アプライアンスでレポートのスケジュールを設定することも、すぐにレポートを生成することもできます。

レポートのスケジュールを設定するには、次の手順を実行します。

a) （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。
b) [メール（Email）]>[レポート（Reporting）]>[スケジュール設定されたレポート（Scheduled Reports）] を選択します。
c) [定期レポートの追加（Add Scheduled Report）] をクリックします。

オンデマンド レポートを作成するには、次の手順を実行します。

- [メール（Email）] > [レポート（Reporting）] > [アーカイブレポート（Archived Reports）] を選択します。
- [今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 2 [レポートタイプ（Report Type）] ドロップダウン リストから、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート タイプを選択します。

ステップ 3 レポートを含めるドメインおよびレポート受信者の電子メール アドレスを指定します。レポートを生成するための、次のいずれかのオプションを選択できます。

- [ドメインを個別に指定してレポートを生成（Generate report by specifying individual domains）]。レポートのドメインおよびレポート受信者の電子メール アドレスを入力します。複数のエントリを指定する場合は、カンマで区切ります。また、subdomain.yourdomain.com のようなサブドメインを使用することもできます。あまり頻繁には変更されないと予測される少数のドメインのレポートを作成する場合は、ドメインを個別に指定することを推奨します。
- [ファイルをアップロードしてレポートを生成（Generate reports by uploading file）]。レポートのドメイン、および受信者の電子メールアドレスのリストが含まれるコンフィギュレーション ファイルをインポートします。アプライアンスのコンフィギュレーション ディレクトリからコンフィギュレーション ファイルを選択することも、ローカル コンピュータからアップロードすることもできます。頻繁に変更される多数のドメインのレポートを作成する場合は、コンフィギュレーション ファイルの使用を推奨します。ドメインベースのレポートのコンフィギュレーション ファイルの詳細については、[ドメイン毎のエグゼクティブ サマリー（Domain-Based Executive Summary）] レポートのドメインおよび受信者のリストの管理 （130 ページ） を参照してください。

（注） レポートを外部アカウント（Yahoo! メールやGmail など）に送信する場合は、レポートメッセージが誤ってスパムに分類されないように外部アカウントの許可リストにレポーティング返信アドレスを追加する必要がある場合があります。

ステップ 4 [タイトル（Title）] テキスト フィールドに、レポートのタイトル名を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

ステップ 5 [送信ドメイン（Outgoing Domain）] セクションで、発信メール サマリーのドメイン タイプを選択します。選択肢は [サーバ別（By Server）] または [電子メールアドレス別（By Email Address）] です。

ステップ 6 [時間範囲（Time Range to Include）] ドロップダウン リストから、レポート データの時間範囲を選択します。

ステップ 7 [フォーマット（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

- PDF. 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- CSV. カンマ区切りの値の raw データが含まれる ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 8 [スケジュール（Schedule）] セクションから、レポートを生成するスケジュールを選択します。

選択肢は [日単位（Daily）]、[週単位（Weekly）]（曜日のドロップダウン リストがあります）または [月単位（monthly）] です。

ステップ 9 （任意）レポートのカスタム ロゴをアップロードします。ロゴは、レポートの上部に表示されます。

- このロゴは、最大で 550 X 50 ピクセルの .jpg、.gif、または .png ファイルにする必要があります。
- ロゴ ファイルをアップロードしなかった場合、デフォルトのシスコ ロゴが使用されます。

ステップ 10 このレポートの言語を選択します。アジア言語での PDF ファイルの生成については、レポーティング データおよびトラッキング データのエクスポートの重要な情報を参照してください。

ステップ 11 [送信（Submit）] をクリックして、ページ上の変更を送信し、[変更を確定（Commit Changes）] をクリックして変更を保存します。

[エグゼクティブサマリー（Executive Summary）] レポート

[エグゼクティブ サマリー（Executive Summary）] レポートは、E メール セキュリティ アプライアンスからの送受信電子メール メッセージ アクティビティの大まかな概要です。セキュリティ管理アプライアンスで表示できます。

このレポート ページには、[メール フロー概要（Mail Flow Summary）] ページ （66 ページ）で表示できる情報の概要が表示されます。[電子メールレポーティングの概要（Email Reporting Overview）] ページの詳細については、[メール フロー概要（Mail Flow Summary）] ページ （66 ページ）を参照してください。

[スケジュールされたレポート（ScheduledReports）]ページ

- メール レポートのスケジュール設定 （133 ページ）
- Web レポートのスケジュール設定

メール レポートのスケジュール設定

スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて（128 ページ）に示されているすべてのレポートをスケジュール設定できます。

レポートのスケジュール設定の管理方法については、次を参照してください。

- スケジュール設定されたレポートの追加 （134 ページ）
- スケジュール設定されたレポートの編集 （135 ページ）
- スケジュール設定されたレポートの中止 （135 ページ）

スケジュール設定されたレポートの追加

スケジュール設定された電子メール レポートを追加するには、次の手順を実行します。

ステップ 1 [メール（Email）] > [レポート（Reporting）] > [スケジュール設定されたレポート（Scheduled Reports）] を選択します。

ステップ 2 [定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 3 レポート タイプを選択します。

レポート タイプの説明については、スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて （128 ページ）を参照してください。

（注） - [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートの設定の詳細については、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート （129 ページ）を参照してください。

- スケジュール設定されたレポートに使用できるオプションは、レポート タイプによって異なります。この手順の残りの部分で説明するオプションを、すべてのレポートに適用する必要はありません。

ステップ 4 [タイトル（Title）] フィールドに、レポートのタイトルを入力します。

同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを推奨します。

ステップ 5 [含める時間範囲（Time Range to Include）] ドロップダウン メニューからレポートの時間範囲を選択します。

ステップ 6 生成されるレポートの形式を選択します。

デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。

ステップ 7 レポートに応じて、[行数（Number of Rows）] で、レポートに含めるデータの量を選択します。

ステップ 8 レポートに応じて、レポートをソートする基準となる列を選択します。

ステップ 9 [スケジュール（Schedule）]領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。また、レポートのスケジュール設定に時刻を含めることもできます。時刻は、深夜 0 時を基準とした増分になります（00:00 ～ 23:59 が 1 日）。

ステップ 10 [メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

電子メール受信者を指定しない場合でも、レポートはアーカイブされます。

必要に応じた数（ゼロも含む）のレポート受信者を追加できます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリング リストを作成するほうが容易です。

ステップ 11 レポートの言語を選択します。

アジア言語については、レポーティング データおよびトラッキング データのエクスポートの重要な情報を参照してください。

ステップ 12 **[送信（Submit）]** をクリックします。

スケジュール設定されたレポートの編集

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [メール（Email）] > [レポート（Reporting）] > [スケジュール設定されたレポート（Scheduled Reports）] を選択します。

ステップ 3 [レポートタイトル（Report Title）] 列の、変更するレポート名リンクをクリックします。

ステップ 4 レポート設定値を変更します。

ステップ 5 変更を送信し、保存します。

スケジュール設定されたレポートの中止

スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、次のステップを実行します。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [メール（Email）] > [レポート（Reporting）] > [スケジュール設定されたレポート（Scheduled Reports）] を選択します。

ステップ 3 生成を中止するレポートに対応するチェックボックスを選択します。スケジュール設定されたすべてのレポートを削除するには、[すべて（All）] チェックボックスを選択します。

ステップ 4 [削除（Delete）] をクリックします。

（注） 削除されたレポートのアーカイブ版は、自動的に削除されるわけではありません。以前に生成されたレポートを削除するには、アーカイブ済みのレポートの削除 （138 ページ）を参照してください。

オンデマンドでのメール レポートの生成

および新しい Web インターフェイスの電子メール レポート ページの概要 （60 ページ）で説明したインタラクティブ レポート ページを使用して表示（および PDF を生成）できるレポー

トに加えて、スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて （128 ページ）に示したレポートの、指定したタイム フレームの PDF ファイルまたは raw データ CSV ファイルをいつでも保存できます。

オンデマンド レポートを生成するには、次の手順を実行します。

ステップ 1 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [メール（Email）]>[レポート（Reporting）]>[アーカイブレポート（Archived Reports）] を選択します。

ステップ 3 [今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 4 レポート タイプを選択します。

レポート タイプの説明については、スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて （128 ページ）を参照してください。

ステップ 5 [タイトル（Title）] テキスト フィールドに、レポートのタイトル名を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

（注） [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートの設定の詳細については、[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポート （129 ページ） を参照してください。

スケジュール設定されたレポートに使用できるオプションは、レポート タイプによって異なります。この手順の残りの部分で説明するオプションを、すべてのレポートに適用する必要はありません。

ステップ 6 [含める時間範囲（Time Range to Include）] ドロップダウン リストから、レポート データの時間範囲を選択します。

これはカスタム時間範囲オプションです。

ステップ 7 [フォーマット（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

- PDF. 配信用、アーカイブ用、またはその両方の用途で PDF 形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。
- CSV. カンマ区切りの値の raw データが含まれる ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 8 レポートを実行するアプライアンスまたはアプライアンス グループを選択します。アプライアンス グループを作成していない場合、このオプションは表示されません。

ステップ 9 [配信オプション（Delivery Option）] セクションから、次のオプションを選択します。

- [アーカイブレポート（Archive Report）] チェックボックスをオンにして、レポートをアーカイブします。

このオプションを選択すると、レポートが [アーカイブレポート（Archived Reports）] ページに表示されます。

（注） [ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートはアーカイブできません。

- [今すぐ受信者にメールを送る（Email now to recipients）] チェックボックスをオンにして、レポートを電子メールで送信します。

テキスト フィールドに、レポートの受信者の電子メールアドレスを入力します。

ステップ 10 このレポートの言語を選択します。アジア言語での PDF ファイルの生成については、レポーティング データおよびトラッキング データのエクスポートの重要な情報を参照してください。

ステップ 11 [このレポートを配信（Deliver This Report）] をクリックして、レポートを生成します。

[アーカイブ メール レポート（Archived Email Reports）] ページ

- スケジュール設定された電子メール レポートとオンデマンドの電子メール レポートについて （128 ページ）
- オンデマンドでのメール レポートの生成 （135 ページ）
- [アーカイブ メール レポート（Archived Email Reports）] の表示と管理 （137 ページ）

[アーカイブ メール レポート（Archived Email Reports）] の表示と管理

スケジュール設定されたレポートおよびオンデマンド レポートは、一定期間アーカイブされます。

セキュリティ管理アプライアンスでは、スケジュール設定された各レポートの最大 30 のインスタンスで、生成された最新のレポートをすべてのレポートに対して、合計 1000 バージョンまで保持します。30インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。

アーカイブ済みのレポートは、アプライアンスの /periodic_reports ディレクトリに保管されます。（詳細については、IPインターフェイスおよびアプライアンスへのアクセスを参照してください）。

アーカイブ レポートへのアクセス

[メール（Email）]>[レポート（Reporting）]>[アーカイブ レポート（Archived Reports）]ページには、生成されたがまだ消去されておらず、アーカイブすることを指定した、スケジュール設定されたレポートとオンデマンド レポートが表示されます。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [メール（Email）]>[レポート（Reporting）]>[アーカイブレポート（Archived Reports）]を選択します。

ステップ 3 リストが長い場合に特定のレポートを見つけるには、[表示（Show）]メニューからレポートタイプを選択してリストをフィルタリングするか、または列のヘッダーをクリックし、その列でソートします。

ステップ 4 [レポートタイトル（Report Title）]をクリックすると、そのレポートが表示されます。

アーカイブ済みのレポートの削除

[アーカイブ メール レポート（Archived Email Reports）]の表示と管理 （137 ページ）で説明したルールに従って、レポートは自動的にシステムから削除されます。ただし、不要なレポートを手動で削除することもできます。

アーカイブ済みのレポートを手動で削除するには、次の手順を実行します。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [メール（Email）]>[レポート（Reporting）]>[アーカイブレポート（Archived Reports）]を選択します。

選択可能なアーカイブ済みのレポートが表示されます。

ステップ 3 削除する 1 つまたは複数のレポートのチェックボックスを選択します。

ステップ 4 [削除（Delete）]をクリックします。

ステップ 5 スケジュール設定されたレポートで、今後のインスタンスが生成されないようにするには、スケジュール設定されたレポートの中止 （135 ページ）を参照してください。

メール レポートのトラブルシューティング

• アウトブレイク フィルタ レポートに情報が正しく表示されない （139 ページ）

- レポートのリンクをクリックした後のメッセージトラッキング結果がレポート結果と一致しない （139 ページ）
- [高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる （139 ページ）
- ファイル分析レポートの詳細の表示に関する問題 （140 ページ）

すべてのレポートのトラブルシューティングも参照してください。

アウトブレイク フィルタ レポートに情報が正しく表示されない

問題

アウトブレイク フィルタ レポートに脅威情報が正しく表示されません。

ソリューション

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）] で指定した Cisco アップデート サーバとアプライアンスが通信できることを確認します。

レポートのリンクをクリックした後のメッセージトラッキング結果がレポート結果と一致しない

問題

レポートからドリルダウンしたときのメッセージ トラッキング結果が、予期した結果に一致しません。

ソリューション

これは、レポーティングとトラッキングが常に同時に有効にならずに適切に機能しない場合、または、レポーティングとトラッキングが各 E メール セキュリティ アプライアンスで常に同時に集中管理またはローカル保存されない場合に発生する可能性があります。各機能（レポーティング、トラッキング）のデータは、その機能が有効になっている間だけキャプチャされます。

関連項目

- メッセージ トラッキング データの有効性の検査

[高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる

問題

Web セキュリティ アプライアンスおよび E メール セキュリティ アプライアンスが同じファイルを分析用に送信し、Web および電子メールの [AMP 判定のアップデート（AMP Verdict Updates）] レポートに、そのファイルの異なる判定が表示されます。

解決方法

この状況は一時的です。判定アップデートがすべてダウンロードされると、結果が一致します。これには最大で 30 分かかります。

ファイル分析レポートの詳細の表示に関する問題

ファイル分析レポートの詳細を使用できない

問題

ファイル分析レポートの詳細を使用できません。

解決方法

ファイル分析レポートの詳細の要件 （42 ページ） を参照してください。

ファイル分析レポートの詳細を表示する際のエラー

問題

ファイル分析レポートの詳細を表示しようとすると、「使用可能なクラウド サーバ構成がありません（No cloud server configuration is available）」エラーが表示されます。

ソリューション

[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] に移動して、ファイル分析機能が有効になっている E メール セキュリティ アプライアンスを少なくとも 1 つ追加します。

ファイル分析レポートの詳細をプライベート クラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー

問題

ファイル分析レポートの詳細を表示しようとすると、API キー エラー、登録エラー、またはアクティベーション エラーが表示されます。

ソリューション

プライベート クラウド（オンプレミス）の Cisco AMP Threat Grid Appliance を使用している場合は、（オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する （43 ページ）を参照してください。

Threat Grid Appliance のホスト名が変更される場合は、参照先の手順のプロセスを繰り返す必要があります。

ファイル分析関連エラーのロギング

登録エラーおよびその他のファイル分析関連のエラーが GUI ログに記録されます。

不正なグレイメールメッセージまたはマーケティングメッセージの総数

問題

マーケティング メール、ソーシャル メール、およびバルク メールの数が、グレイメール メッセージの総数を超える。

ソリューション

マーケティング メッセージの総数には、AsyncOS 9.5 へのアップグレードの前後に受信したマーケティング メッセージが含まれますが、グレイメール メッセージの総数にはアップグレード後に受信したメッセージだけが含まれます。AsyncOS 9.5 へのアップグレード後のマーケティング メッセージのレポート （55 ページ） を参照してください。

不正なグレイメール メッセージまたはマーケティングメッセージの総数