CHAPTER 4

中央集中型電子メール セキュリティ レポーティングの使用

中央集中型電子メール レポーティングの概要

シスコのコンテンツ セキュリティ管理アプライアンスは、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 リスクを監視できるように、個別または複数の電子メール セキュリティ アプライアンス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、電子メール 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中管理されます。

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、複数の電子メール セキュリティ アプライアンス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） 電子メール 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電子メール 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、電子メール 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 データの可用性の詳細についてはお使いの電子メール セキュリティ アプライアンスの「Centralized Reporting Mode」の項を参照してください。

中央集中型電子メール 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。

- 「セキュリティ管理アプライアンスでの中央集中型電子メール レポーティングのイネーブル化」（P.4-2）
- 「管理対象の各電子メール 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」（P.4-3）
- 「電子メール レポート グループの作成」（P.4-4）
- 「電子メール セキュリティ アプライアンスでの中央集中型電子メール レポーティングのイネーブル化」（P.4-5）

（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電子メール 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、その機能がイネーブルになっている間にのみキャプチャされるためです。

セキュリティ管理アプライアンスでの中央集中型電子メール レポーティングのイネーブル化

はじめる前に

- 中央集中型レポーティングをイネーブルにする前に、すべての電子メール 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。「ディスク使用量の管理」（P.14-56）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [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（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、「ディスク使用量の管理」（P.14-56）を参照してください。

管理対象の各電子メール 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

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] を選択します。

ステップ 2　このページのリストに、すでに電子メール 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.　電子メール 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 3　電子メール 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）] テキスト フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、すぐに IP アドレスに解決されます。

c.　[集約管理レポート（Centralized Reporting）] サービスが事前に選択されています。

d.　[接続の確立（Establish Connection）] をクリックします。

e.　管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

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

f. [成功（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 4　[送信（Submit）] をクリックします。

ステップ 5　中央集中型レポーティングをイネーブルにする各電子メール 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 6　変更を保存します。

電子メール レポート グループの作成

セキュリティ管理アプライアンスからレポーティング データを表示する電子メール 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。

はじめる前に

各アプライアンスで中央集中型レポーティングがイネーブルになっていることを確認します。「管理対象の各電子メール 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」（P.4-3）を参照してください。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [集約管理レポート（Centralized Reporting）] を選択します。

ステップ 2　[グループを追加（Add Group）] をクリックします。

ステップ 3　グループの一意の名前を入力します。

電子メール セキュリティ アプライアンスで、セキュリティ管理アプライアンスに追加した 電子メール 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）　電子メール 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電子メール 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 電子メール 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 4　[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 5　変更を送信し、保存します。

電子メール セキュリティ アプライアンスでの中央集中型電子メール レポーティングのイネーブル化

管理対象の各電子メール セキュリティ アプライアンスで、中央集中型電子メール レポーティングをイネーブルにする必要があります。

手順については、お使いの電子メール セキュリティ アプライアンスに対するマニュアルの「Configuring an Email Security Appliance to Use Centralized Reporting」の項またはオンライン ヘルプ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、「レポーティング データを表示する方法」（P.3-1）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方法については、「レポート データのビューのカスタマイズ」（P.3-3）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」（P.4-6）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 データの印刷およびエクスポート」（P.3-10）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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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、「オンデマンドでの電子メール レポートの生成」（P.4-58）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、「電子メール レポートのスケジュール設定」（P.4-56）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、「アーカイブ電子メール レポートの表示と管理」（P.4-59）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 アプライアンスによるレポート用データの収集方法」（P.3-2）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」（P.3-8）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、そうすることを許可されている場合は、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。これは、メッセージ トラッキングで関連する検索を実行します。結果を表示するには、スクロール ダウンします。

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

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

[メール レポート（Email Reporting）] ページの概要

表 4-1　[メール レポート（Email Reporting）] タブのオプション

[メール レポート（Email Reporting）] メニュー	アクション
電子メール レポーティングの [概要（Overview）] ページ	[概要（Overview）] ページには、お使いの電子メール 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（Overview）] ページ」（P.4-11）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 電子メール 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。 詳細については、「[受信メール（Incoming Mail）] ページ」（P.4-16）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、組織が電子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。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）カラム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」（P.4-24）を参照してください。
[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」（P.4-26）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」（P.4-28）を参照してください。
[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 サマリー（DLP Incident Summary）] ページ」（P.4-31）を参照してください。

表 4-1　[メール レポート（Email Reporting）] タブのオプション （続き）

[メール レポート（Email Reporting）] メニュー	アクション
[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」（P.4-34）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、電子メール セキュリティ アプライアンスで稼働し、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 スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。 詳細については、「[ウイルス タイプ（Virus Types）] ページ」（P.4-35）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」（P.4-37）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、および電子メール 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」（P.4-39）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」（P.4-40）を参照してください。
[アウトブレイク フィルタ（Outbreak Filters）] ページ	[アウトブレイク フィルタ（Outbreak Filters）] ページには、ウイルス感染フィルタによって隔離された最近のアウトブレイクやメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する防御をモニタします。 詳細については、「[アウトブレイク フィルタ（Outbreak Filters）] ページ」（P.4-41）を参照してください。

表 4-1　[メール レポート（Email Reporting）] タブのオプション （続き）

[メール レポート（Email Reporting）] メニュー	アクション
[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」（P.4-44）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」（P.4-50）を参照してください。
電子メール 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、「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。
アーカイブ電子メール レポートの表示と管理	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、「アーカイブ電子メール レポートの表示と管理」（P.4-59）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。「オンデマンドでの電子メール レポートの生成」（P.4-58）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 カラムの説明

表 4-2　電子メール レポーティング ページのテーブル カラムの説明

カラム名	説明
受信メールの詳細（Incoming Mail Details）	
接続拒否（Connections Rejected）	HAT ポリシーによってブロックされたすべての接続。アプライアンスに重い負荷がかけられている場合、拒否された接続の正確な数を送信者別に維持できません。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。
接続承認（Connections Accepted）	受け入れられたすべての接続。
試行されたメッセージの合計数（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 制限のいずれか（1 時間当たりの最大受信者数、メッセージ別の最大受信者数、接続別の最大メッセージ数）を超えたため阻止された受信者メッセージの数を表します。これは、[レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] が発生した、拒否された、または TCP 拒否された接続に関連する受信者メッセージを推定して集計されます。

表 4-2　電子メール レポーティング ページのテーブル カラムの説明 （続き）

カラム名	説明
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「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。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。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。
無効な受信者として停止（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 フィルタによる停止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。
合計脅威件数（Total Threat）	脅威メッセージ（評価により阻止されたもの、無効な受信者、スパム、およびウイルスとして阻止されたもの）の総数。
マーケティング（Marketing）	不要なマーケティング メッセージとして検出されたメッセージの数。
正常（Clean）	すべてのクリーン メッセージ。
User Mail Flow Details（[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。

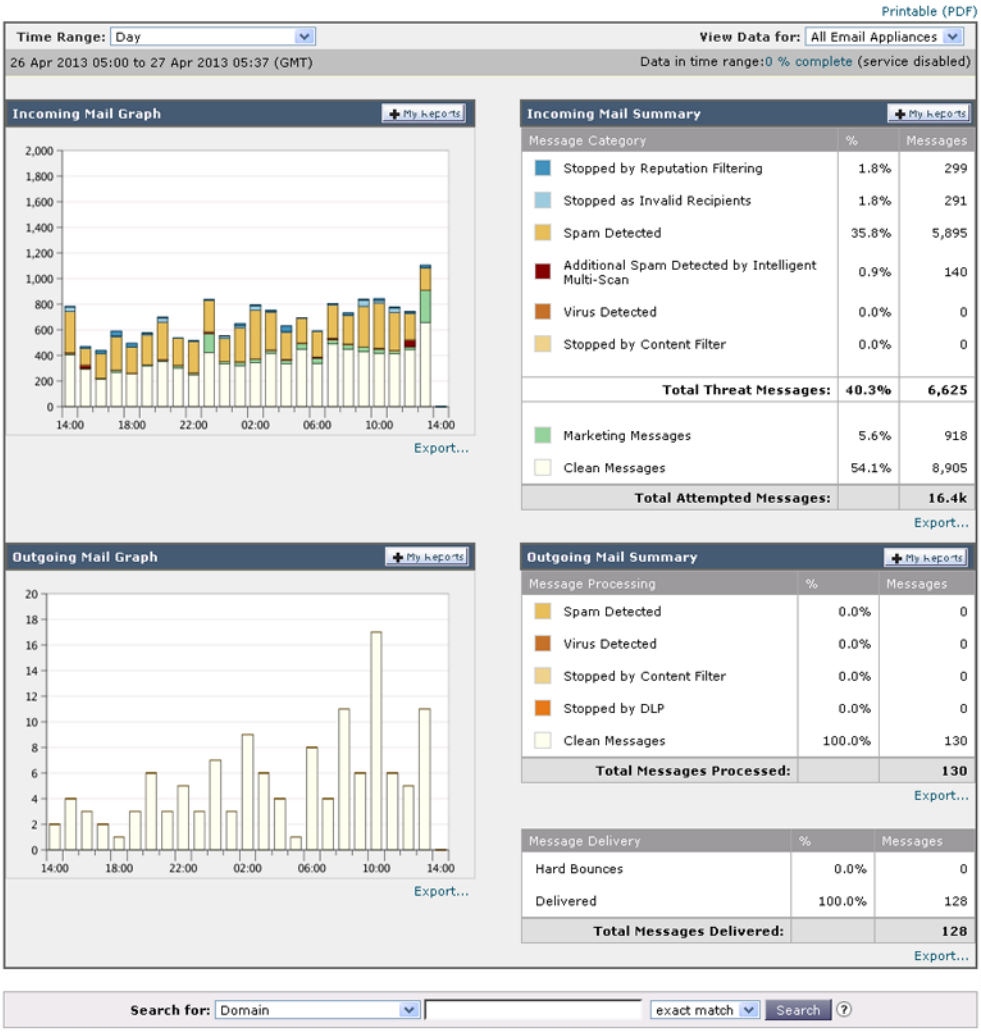
表 4-2　電子メール レポーティング ページのテーブル カラムの説明 （続き）

カラム名	説明
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。
Incoming and Outgoing TLS Connections（[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。
合計接続数（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（Outbreak Filters）	
アウトブレイク名（Outbreak Name）	アウトブレイクの名前。
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（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、電子メール 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。

図 4-1　[メール（Email）] > [レポート（Reporting）] > [概要（Overview）] ページ



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（Overview）] 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」（P.4-53）および「[エグゼクティブ サマリー（Executive Summary）] レポート」（P.4-56）を参照してください。

表 4-3　[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（Time Range）	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」（P.3-4）を参照してください。
データ参照（View Data for）	[概要（Overview）] のデータを表示する電子メール セキュリティ アプライアンスを選択するか、[全メール 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 グループのレポーティング データの表示」（P.3-4）も参照してください。
受信メールのグラフ（Incoming Mail Graph）	[受信メールのグラフ（Incoming Mail Graph）] には、着信メールの内訳をリアルタイムで視覚的に示したグラフが表示されます。
送信メールのグラフ（Outgoing Mail Graph）	[送信メールのグラフ（Outgoing Mail Graph）] には、アプライアンスでの発信メールの内訳を視覚的に示したグラフが表示されます。
受信メール サマリー（Incoming Mail Summary）	[受信メール サマリー（Incoming Mail Summary）] には、レピュテーション フィルタリングによって阻止された（SBRS）メッセージ、無効な受信者として阻止されたメッセージ、スパムが検出されたメッセージ、ウイルスが検出されたメッセージ、およびコンテンツ フィルタによって阻止されたメッセージ、ならびに「クリーン」と見なされたメッセージのパーセンテージと数が表示されます。
送信メール サマリー（Outgoing Mail Summary）	[送信メール サマリー（Outgoing Mail Summary）] セクションには、発信脅威メッセージおよび発信クリーン メッセージの情報が含まれます。また、配信されたメッセージとハードバウンスされたメッセージの内訳も含まれます。

着信メール メッセージのカウント方法

AsyncOS は、メッセージごとの受信者数に応じて着信メールをカウントします。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。

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、実際には作業キューに入らないので、アプライアンスは、着信メッセージの受信者のリストにはアクセスできません。この場合、乗数を使用して受信者の数が予測されます。この乗数は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。

これらの優先ルールに続いて、次のようなさまざまな判定が行われます。

- アウトブレイク フィルタの隔離
  （この場合、メッセージが隔離から解放されるまで集計されず、作業キューによる処理が再び行われます）
- スパム陽性
- ウイルス陽性
- コンテンツ フィルタとの一致

これらの規則に従って、メッセージがスパム陽性とマークされると、アンチスパム設定がスパム陽性のメッセージをドロップするように設定されている場合には、このメッセージがドロップされ、スパム カウンタが増分します。

さらに、スパム陽性のメッセージを引き続き電子メール パイプラインで処理し、以降のコンテンツ フィルタがこのメッセージをドロップ、バウンス、または隔離するようにアンチスパム設定が設定されている場合にも、スパム カウンタは増分します。メッセージがスパム陽性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。

[概要（Overview）] ページでの電子メール メッセージの分類

[概要（Overview）] ページでレポートされるメッセージは、次のように分類されます。

表 4-4　[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（Stopped by Reputation Filtering）	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（「着信メール メッセージのカウント方法」（P.4-13）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。 [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（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 メッセージ検出（Spam Messages Detected）	アンチスパム スキャン エンジンで陽性、または疑いありとして検出されたメッセージの総数。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。

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

カテゴリ	説明
ウィルス メッセージ検出（Virus Messages Detected）	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）] カテゴリにカウントされます。 • ウイルス スキャン結果が [修復（Repaired）] または [感染（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カウント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
コンテンツ フィルタによる停止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。
マーケティング メッセージ（Marketing Messages）	不要なマーケティング メッセージと検出されたメッセージの総数および割合。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。
正常なメッセージ受信（Clean Messages Accepted）	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、スパム陽性またはウイルス陽性というマークを付けられたが、それでも配信されるメッセージはカウントされないため、配信される実際のメッセージ数はクリーン メッセージ数と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。

（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。

[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（Incoming Mail）] ページは、2 つの主要なセクションからなります。つまり、上位送信者（脅威メッセージの合計とクリーン メッセージの合計による）をまとめたメール トレンド グラフと、[受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルです。

[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。[受信メール（Incoming Mail）] ページまたは他の [送信者プロファイル（Sender Profile）] ページの上部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。

[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電子メールを送信したメール送信者の 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」（P.4-6）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」（P.4-23）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（評価フィルタリング、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の分析を行い、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、ドメインが直近に一致した送信者グループなど SenderBase レピュテーション サービスから送信者に関する詳細を取得する。送信者を送信者グループに追加する。
- アンチスパムまたはアンチウイルス セキュリティ サービスによって測定される、大量のスパムまたはウイルス電子メールを送信した特定の送信者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
- 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 IP アドレス（Sender's IP Address）]、[ドメイン名（Domain name）]、または [ネットワーク所有者情報（Network Owner Information）] をクリックすると、特定の [送信者プロファイル情報（Sender Profile Information）] 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」（P.4-20）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、電子メール 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 [送信者グループのレポート（Sender Groups Report）] リンクをクリックします。「[送信者グループ（Sender Groups）] レポート ページ」（P.4-23）を参照してください。

[受信メール（Incoming Mail）] ページでの電子メール メッセージの分類

[受信メール（Incoming Mail）] ページでレポートされるメッセージは、次のように分類されます。

表 4-5　[受信メール（Incoming Mail）] 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（Stopped by Reputation Filtering）	HAT ポリシーによってブロックされたすべての接続数に、固定乗数（「着信メール メッセージのカウント方法」（P.4-13）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「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。代わりに、拒否された接続数は、インターバルごとの最大送信者だけに対して維持されます。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。
無効な受信者（Invalid Recipients）	従来の LDAP 拒否によって拒否されたすべての電子メール受信者数にすべての RAT 拒否数を加えた値。

表 4-5　[受信メール（Incoming Mail）] ページの電子メールのカテゴリ （続き）

カテゴリ	説明
スパム メッセージ検出（Spam Messages Detected）	アンチスパム スキャン エンジンで陽性、または疑いありとして検出されたメッセージの総数。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。
ウィルス メッセージ検出（Virus Messages Detected）	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。
コンテンツ フィルタによる停止（Stopped by Content Filter）	コンテンツ フィルタによって阻止されたメッセージの総数。 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。
マーケティング メッセージ（Marketing Messages）	不要なマーケティング メッセージと検出されたメッセージの総数および割合。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。
正常なメッセージ受信（Clean Messages Accepted）	受け入れられ、ウイルスでもスパムでもないと見なされたメール。受信者単位のスキャン アクション（個々のメール ポリシーで処理される分裂したメッセージなど）を考慮したときに受信されたクリーン メッセージを最も正確に表したものです。ただし、スパム陽性またはウイルス陽性というマークを付けられたが、それでも配信されるメッセージはカウントされないため、配信される実際のメッセージ数はクリーン メッセージ数とは異なる可能性があります。

（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。

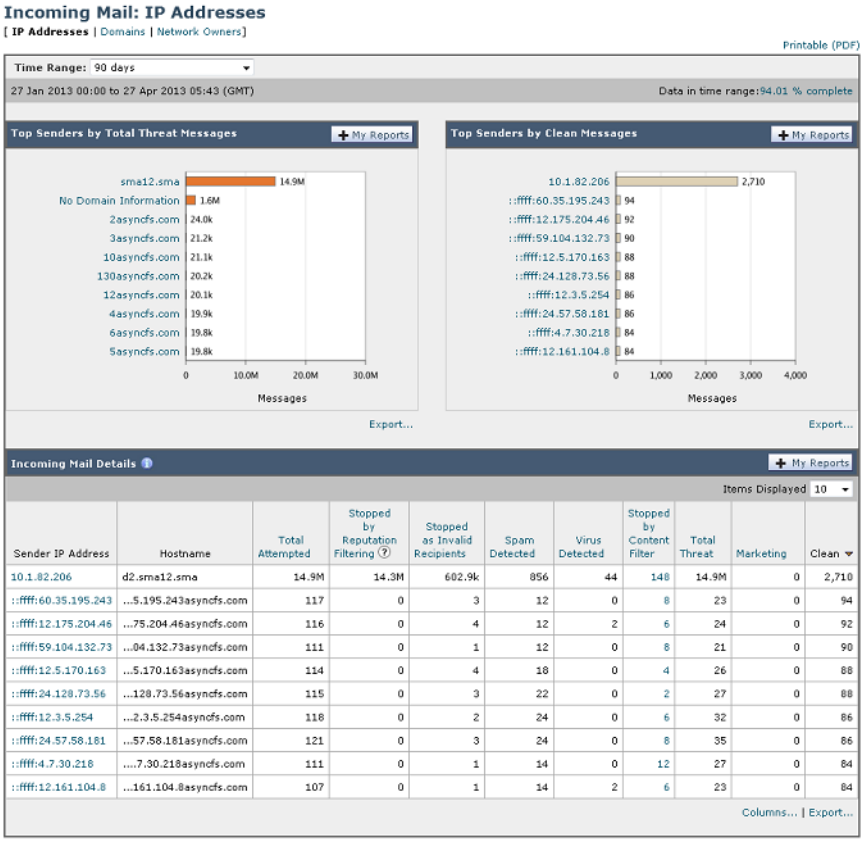
さらに、メッセージが*メッセージ フィルタ*と一致し、フィルタによってドロップされたり、バウンスされたりしていない場合、クリーンなメッセージとして扱われます。メッセージ フィルタによってドロップされたか、バウンスされたメッセージは、総数に含まれません。

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 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。「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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）]

図 4-2　[受信メール（Incoming Mail）] ページ : [IP アドレス（IP Address）] ビュー



[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」（P.4-20）を参照してください。

この例では、[ドメイン（Domain）] ビューが選択されています。

[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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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。「電子メール レポートのスケジュール設定」（P.4-56）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されないホストを、送信者の検証によってどのように管理するかを制御できます。送信者の検証の詳細については、ご使用の電子メール 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。

[表示されたアイテム（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」（P.3-4）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、電子メール 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、カラム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、電子メール 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）] テーブルの最初のカラム、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、[送信者のプロファイル（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」（P.4-20）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 [送信者グループのレポート（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」（P.4-23）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）] ページで [受信メールの詳細（Incoming Mail Details）] インタラクティブ テーブルの送信者をクリックすると、[送信者プロファイル（Sender Profile）] ページが表示されます。ここには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）の詳細情報が表示されます。[受信メール（Incoming Mail）] ページまたは他の [送信者プロファイル（Sender Profile）] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [送信者プロファイル（Sender Profile）] ページにアクセスできます。

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

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

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

各 [送信者プロファイル（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 評価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。地震を測定するため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 を底とした対数目盛を使用して計算されるメッセージ量の測定単位です。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。この対数目盛を使用した場合、マグニチュードの 1 ポイントの上昇は、実際の量の 10 倍増加に相当します。

  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。

図 4-3　ネットワーク オーナーの現在の情報

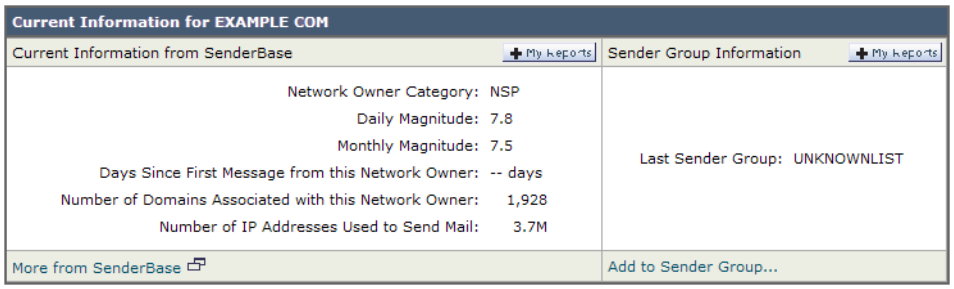
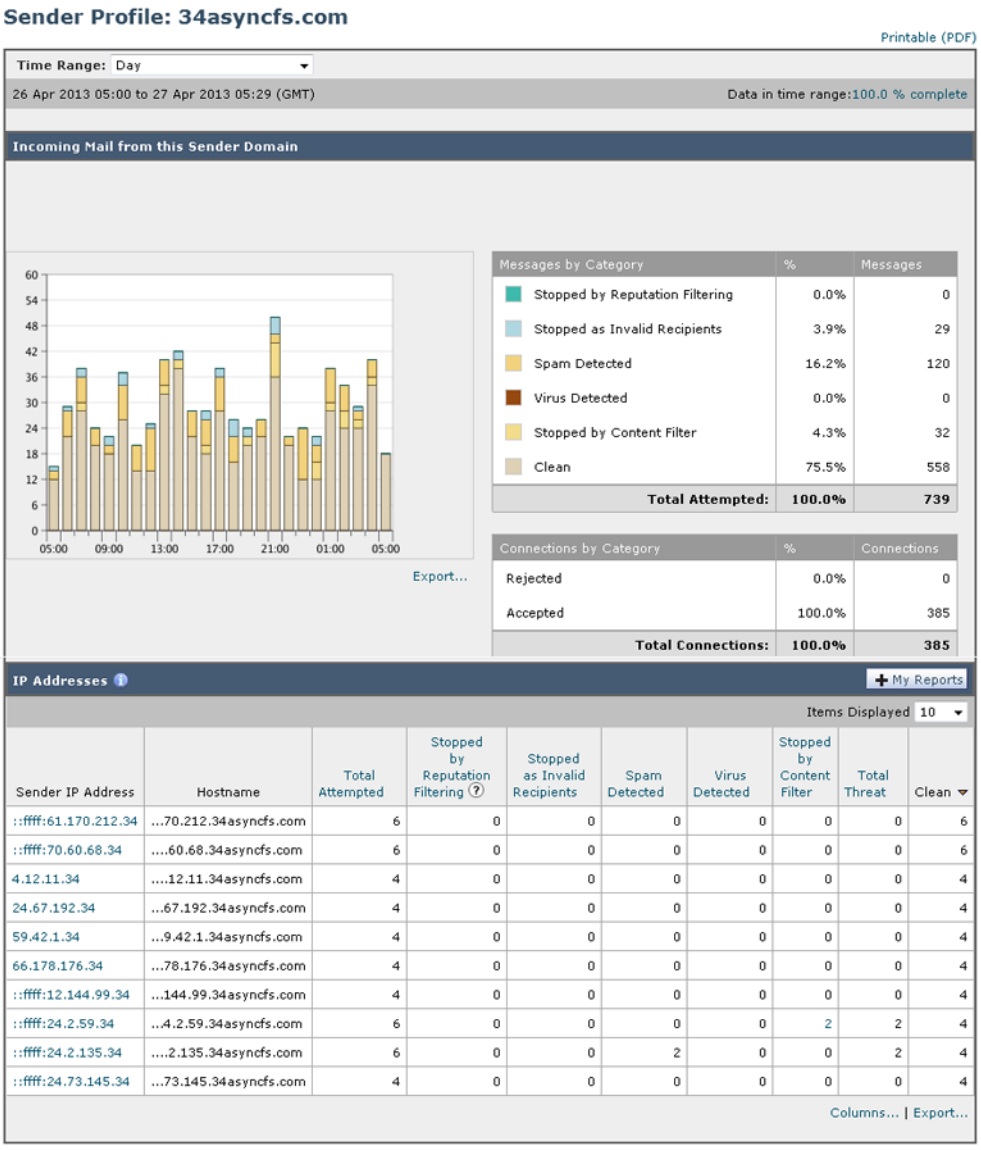


図 4-4　[送信者プロファイル（Sender Profile）] ページ



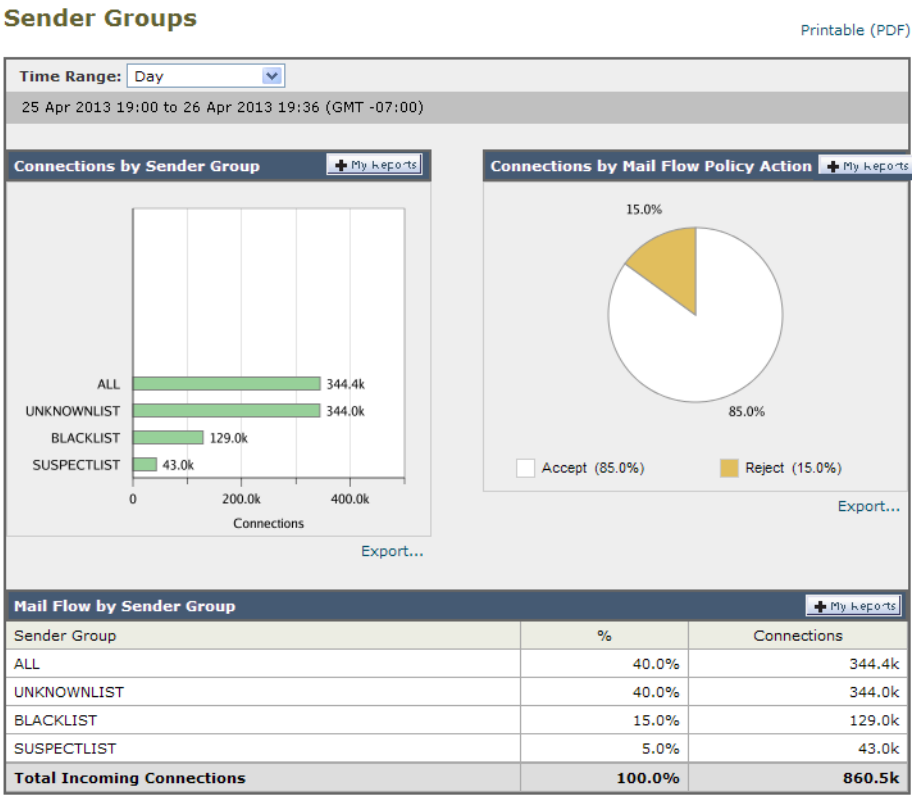
[送信者グループ（Sender Groups）] レポート ページ

[送信者グループ（Sender Groups）] レポート ページは、送信者グループ別およびメール フロー ポリシー アクション別の接続のサマリーを提供し、SMTP 接続およびメール フロー ポリシーのトレンドを確認できるようにします。[送信者グループによるメール フロー（Mail Flow by Sender Group）] リストには、各送信者グループの割合および接続数が示されます。[メール フロー ポリシー アクションによる接続（Connections by Mail Flow Policy Action）] グラフは、各メール フロー ポリシー アクショ

ンの接続の割合を示します。このページには、Host Access Table（HAT; ホスト アクセス テーブル）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、電子メール 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、[受信メール（Incoming Mail）] レポート ページの下部にある [送信者グループのレポート（Sender Groups Report）] リンクをクリックします。

図 4-5　[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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）を参照してください。

（注）　[送信者グループ（Sender Groups）] 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。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[送信先（Outgoing Destinations）] ページ

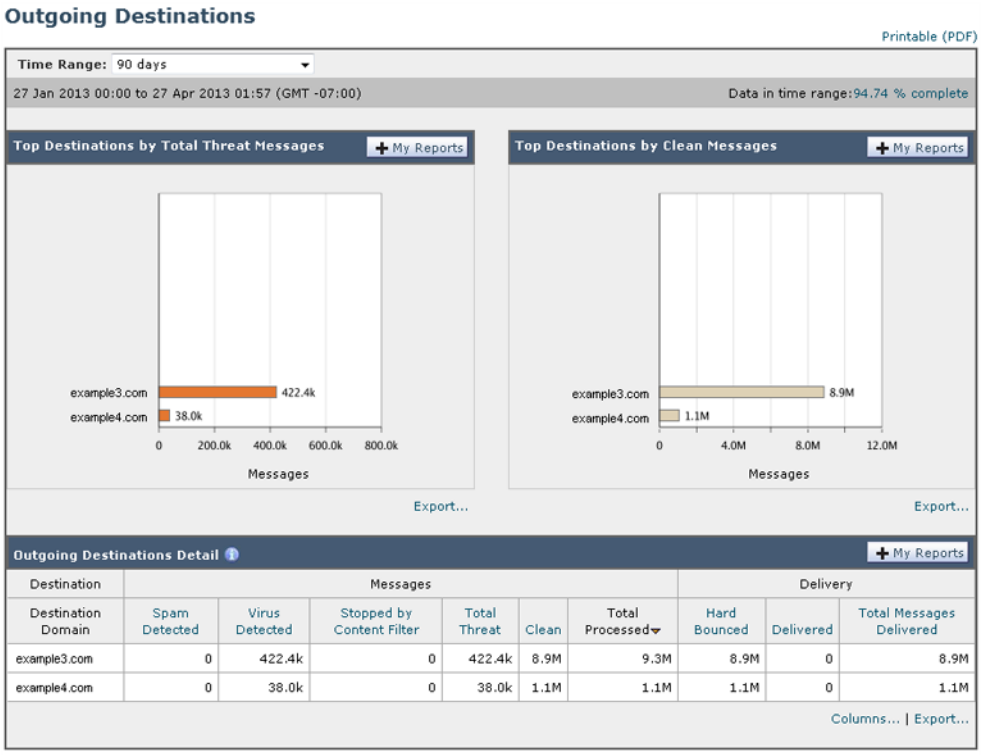
[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページには、組織が電子メールを送信する宛先のドメインについての情報が表示されます。

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

- 電子メール セキュリティ アプライアンスが電子メールを送信する宛先ドメイン
- 各ドメインに送信される電子メールの量

- クリーン、スパム陽性、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

図 4-6　[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページ



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 4-6　[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」（P.3-4）を参照してください。
脅威メッセージの送信先上位（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。

表 4-6　[メール（Email）] > [レポート（Reporting）] > [送信先（Outgoing Destinations）] ページの詳細 （続き）

セクション	説明
正常なメッセージの送信先上位（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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[送信メッセージ送信者（Outgoing Senders）] ページ

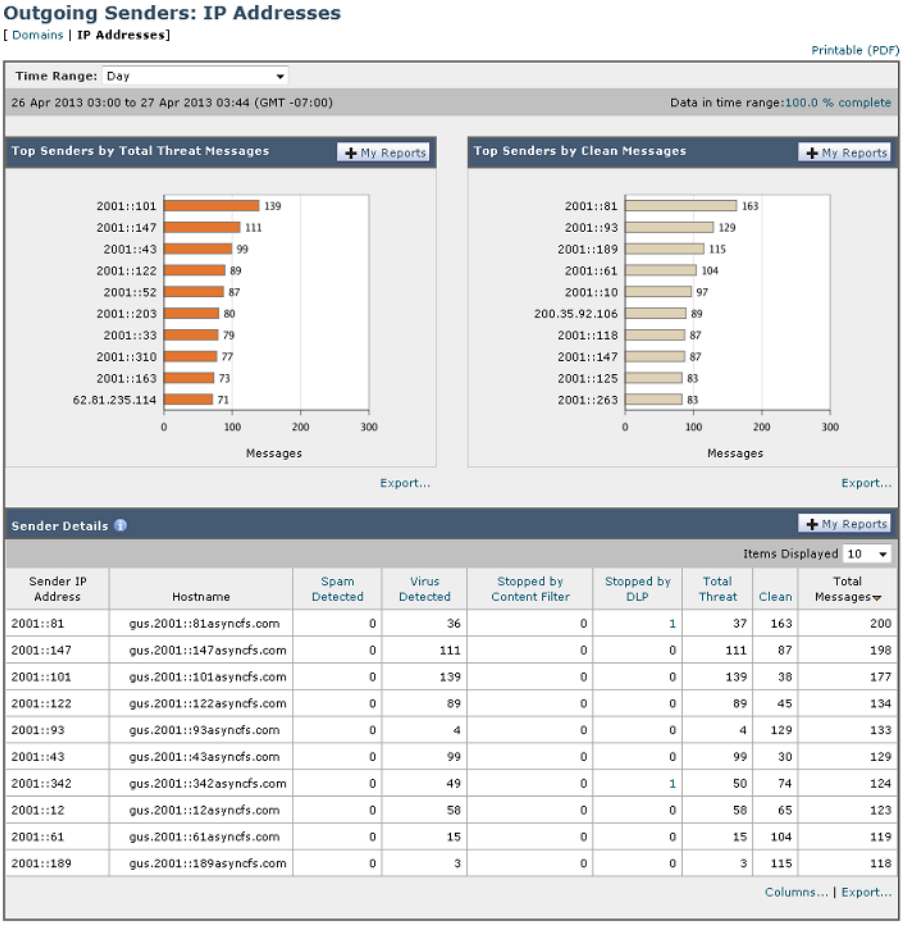
[メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Senders）] ページには、ネットワーク内の IP アドレスおよびドメインから送信された電子メールの数と種類についての情報が表示されます。

[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またはスパム陽性の電子メールを送信した 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。

図 4-7　[メール（Email）] > [レポート（Reporting）] > [送信メッセージ送信者（Outgoing Senders）] ページ（IP アドレスを表示中）



[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 4-7　[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」（P.3-4）を参照してください。
脅威メッセージの送信者上位（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）。

表 4-7　[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 （続き）

セクション	説明
正常なメッセージの送信者上位（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）。
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、適切な電子メール 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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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。「電子メール レポートのスケジュール設定」（P.4-56）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
- 最も多くのスパムを受信したユーザ
- 特定のコンテンツ フィルタをトリガーしたユーザ
- 特定のユーザからの電子メールを阻止したコンテンツ フィルタ

図 4-8　[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページ

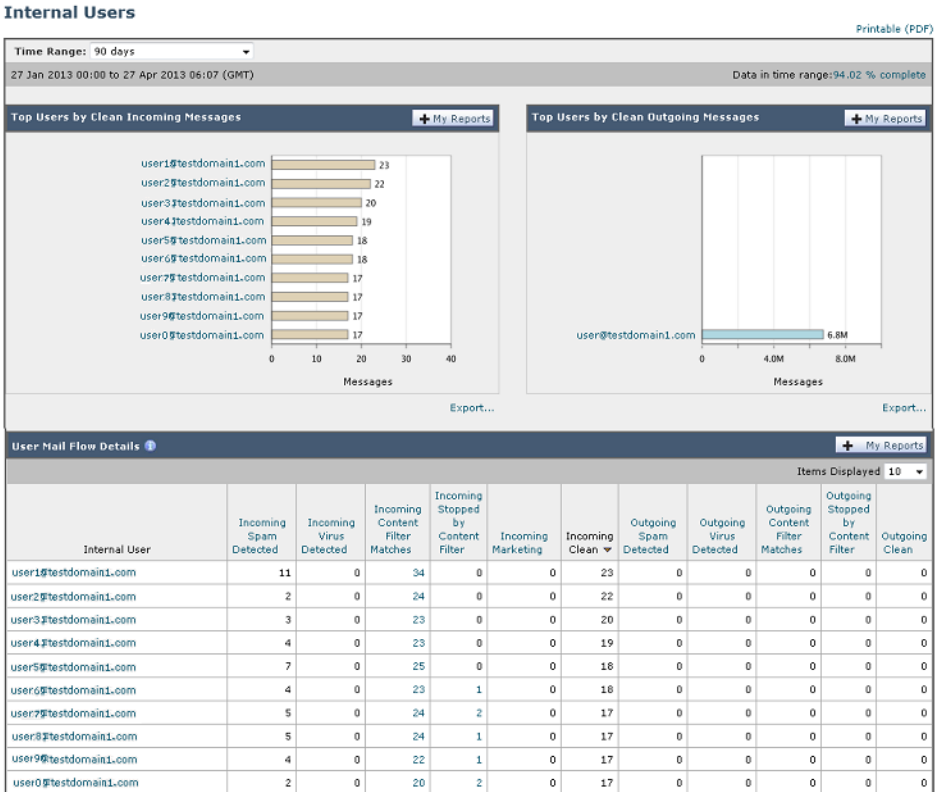


表 4-8　[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページの詳細

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」（P.3-4）を参照してください。
上位ユーザ（正常な受信メッセージ）（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）。

表 4-8　[メール（Email）] > [レポート（Reporting）] > [内部ユーザ（Internal Users）] ページの詳細 （続き）

セクション	説明
上位ユーザ（正常な送信メッセージ）（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、各電子メール アドレスで送受信した電子メールが [正常（Clean）]、[スパム検出（Spam Detected）]（受信のみ）、[ウイルス検出（Virus Detected）]、[コンテンツフィルタの一致（Content Filter Matches）] に分類されます。カラム 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 Users）] カラム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」（P.4-30）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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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。「電子メール レポートのスケジュール設定」（P.4-56）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）]、[コンテンツフィルタによる停止（Stopped By Content Filter）]、および [正常（Clean）]）のメッセージ数を示す着信および発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」（P.4-34）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

[内部ユーザ（Internal Users）] ページおよび [内部ユーザの詳細（Internal User Details）] ページの下部にある検索フォームで、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。

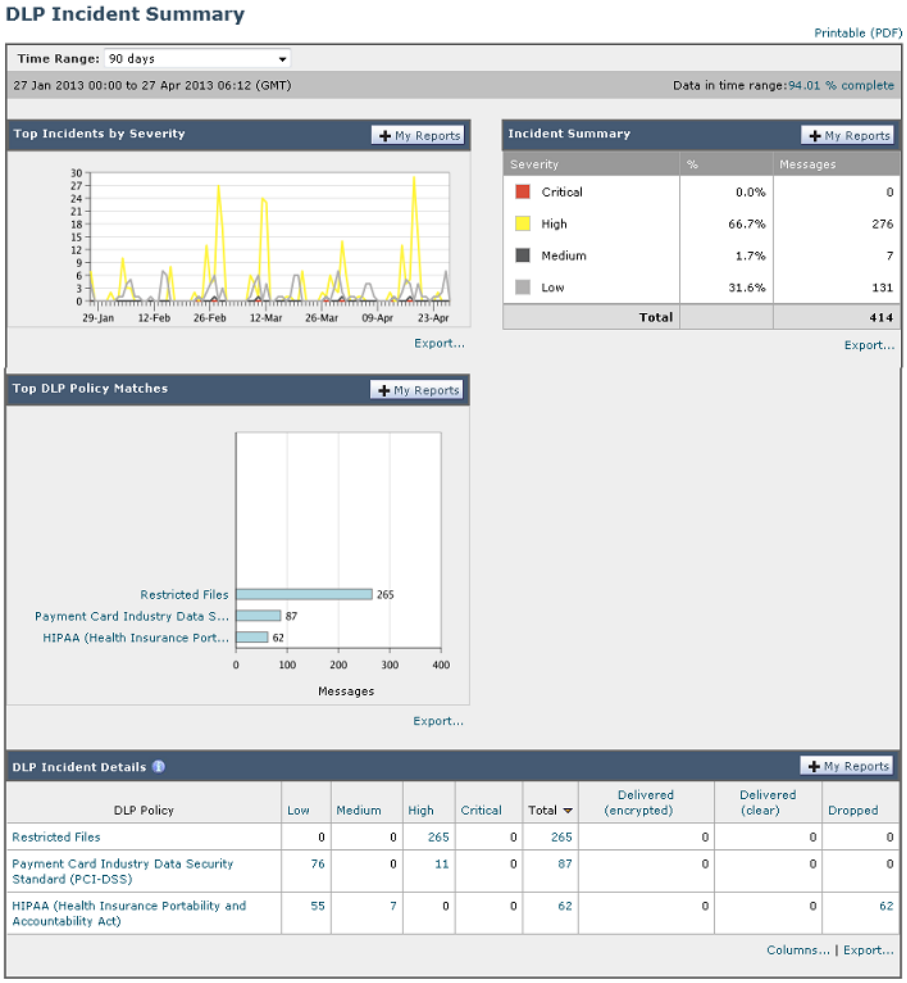
[DLP インシデント サマリー（DLP Incident Summary）] ページ

[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。電子メール 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）] テーブルでイネーブルにした DLP 電子メール ポリシーを使用して、ユーザが送信した機密データを検出します。DLP ポリシーに違反する送信メッセージが発生するたびに、インシデントとして報告されます。

[DLP インシデント 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

図 4-9　[メール（Email）] > [レポート（Reporting）] > [DLP サマリー（DLP Summary）] ページ



[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）]、[クリティカル（Critical）]）別の上位 DLP インシデントおよびポリシーの一致数を集約する DLP インシデントのトレンド グラフ
- [DLP インシデントの詳細（DLP Incident Details）] リスト

表 4-9　[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」（P.3-4）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。

表 4-9　[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 （続き）

セクション	説明
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 ポリシーで現在イネーブルになっている 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。
DLP ポリシー一致の上位（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 Incident Details）] テーブルの詳細については、「[DLP インシデントの詳細（DLP Incident Details）] テーブル」（P.4-33）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 Incident 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、カラム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」（P.4-33）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 インシデントの詳細（DLP Incident Details）] 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検索できます。

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」（P.4-28）を参照してください。

[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」（P.4-34）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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

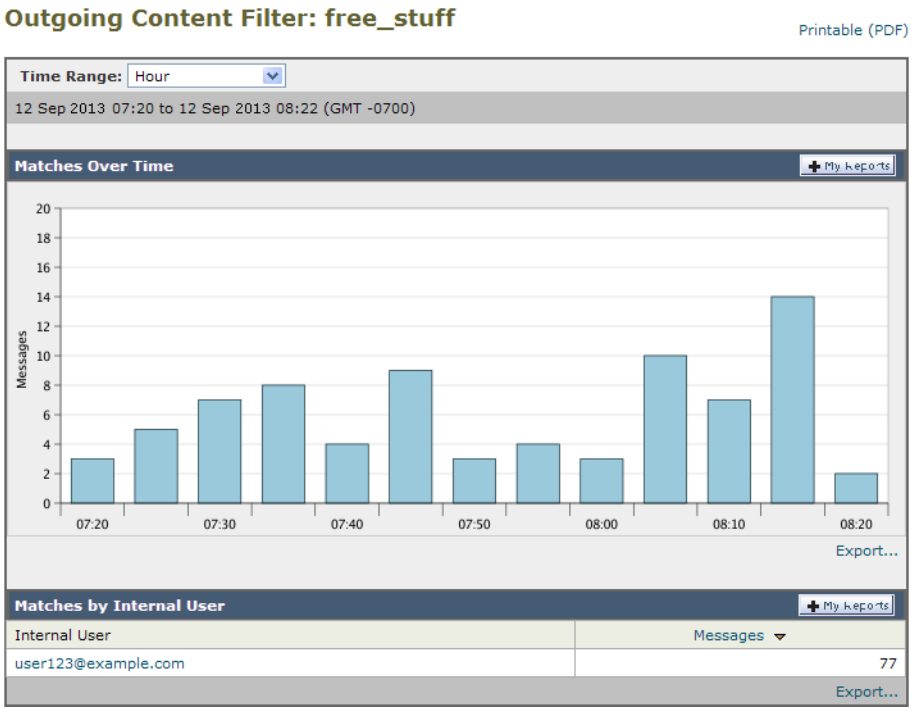
[コンテンツ フィルタの詳細（Content Filter Details）] ページ

[コンテンツ フィルタの詳細（Content Filter Details）] 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」（P.4-30）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。

図 4-10　[コンテンツ フィルタの詳細（Content Filters Details）] ページ

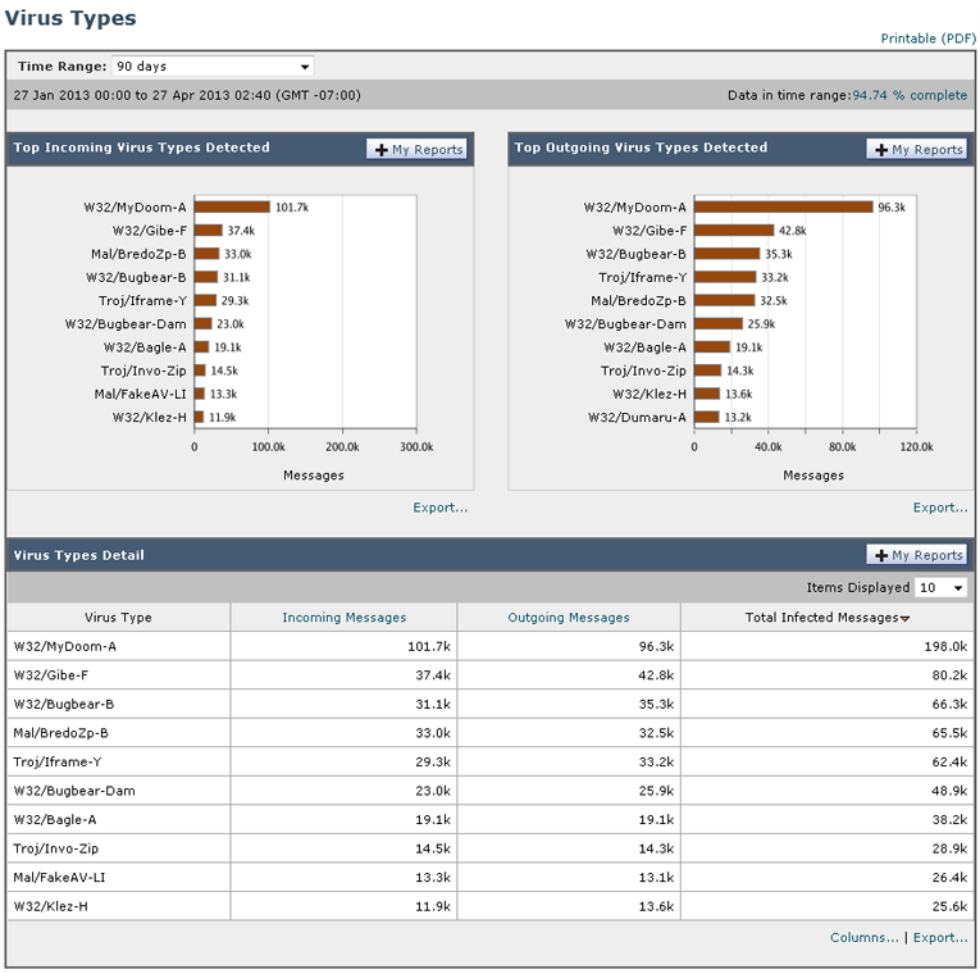


[ウイルス タイプ（Virus Types）] ページ

[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、電子メール セキュリティ アプライアンスで稼働し、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 スキャン エンジンによって検出されたウイルスが表示されます。このレポートを使用して、特定のウイルスに対して処置を行います。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。

図 4-11　[メール（Email）] > [レポート（Reporting）] > [ウイルス タイプ（Virus Types）] ページ



Virus Type	Incoming Messages	Outgoing Messages	Total Infected Messages
W32/MyDoom-A	101.7k	96.3k	198.0k
W32/Gibe-F	37.4k	42.8k	80.2k
W32/Bugbear-B	31.1k	35.3k	66.3k
Mal/BredoZp-B	33.0k	32.5k	65.5k
Troj/Iframe-Y	29.3k	33.2k	62.4k
W32/Bugbear-Dam	23.0k	25.9k	48.9k
W32/Bagle-A	19.1k	19.1k	38.2k
Troj/Invo-Zip	14.5k	14.3k	28.9k
Mal/FakeAV-LI	13.3k	13.1k	26.4k
W32/Klez-H	11.9k	13.6k	25.6k

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 4-10　[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」（P.3-4）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、「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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。「電子メール レポートのスケジュール設定」（P.4-56）を参照してください。

[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

図 4-12　[TLS 接続レポート（TLS Connections Report）] ページ : [受信接続数（Incoming Connections）]

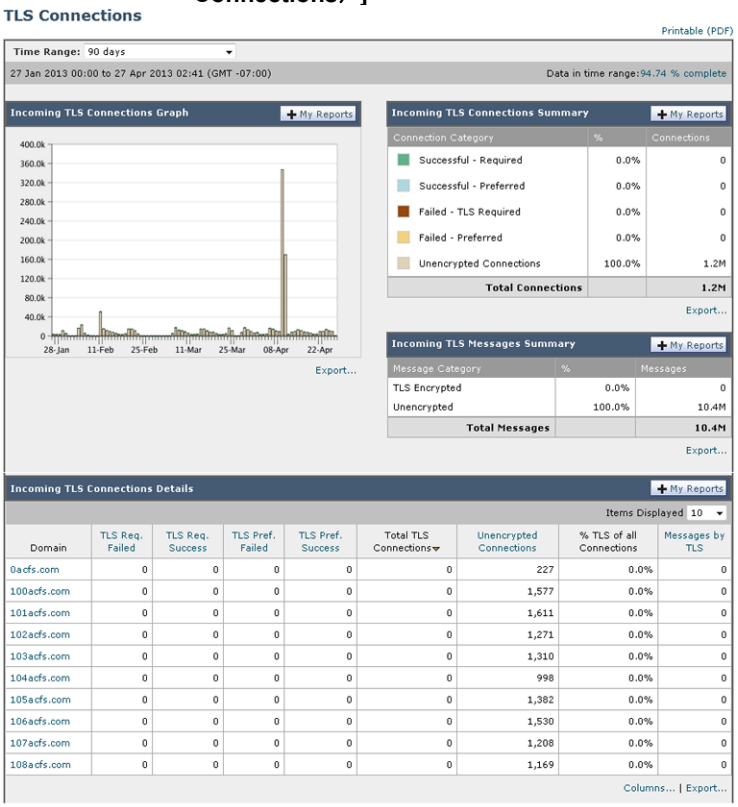


表 4-11　[メール（Email）] > [レポート（Reporting）] > [TLS 接続（TLS Connections）] ページの詳細

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」（P.3-4）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。

表 4-11　[メール（Email）] > [レポート（Reporting）] > [TLS 接続（TLS Connections）] ページの詳細 （続き）

セクション	説明
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。
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。
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、および電子メール 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

[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。

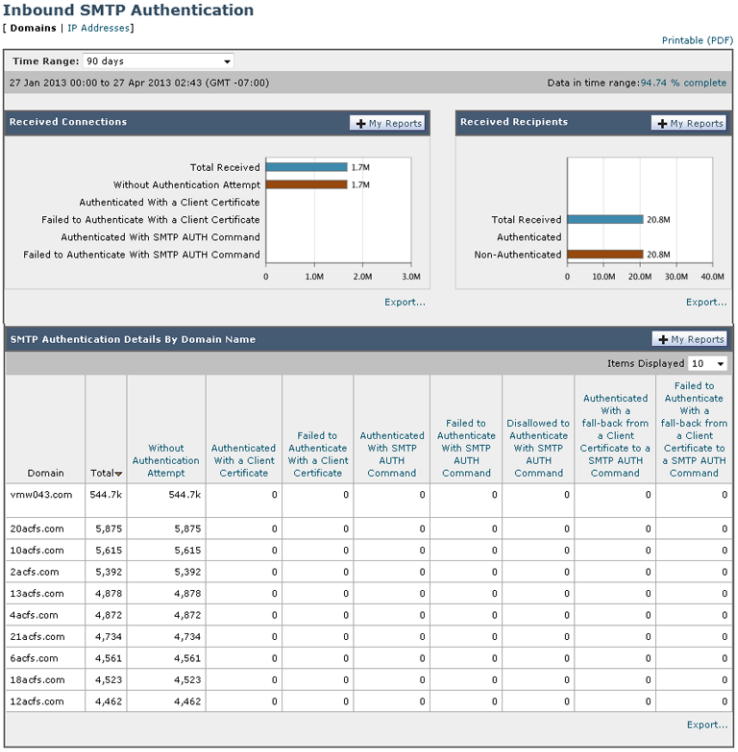
[受信した接続（Received Connections）] グラフでは、指定した時間範囲において SMTP 認証を使用して接続を認証しようとしたメール クライアントの着信接続が示されます。このグラフには、アプライアンスが受信した接続の総数、SMTP 認証を使用して認証を試行しなかった接続の数、クライアント証明書を使用して認証が失敗および成功した接続の数、SMTP AUTH コマンドを使用して認証が失敗および成功した接続の数が表示されます。

[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電子メール 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電子メール 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。

図 4-13　[受信 SMTP 認証（Inbound SMTP Authentication）] ページ



[レート制限（Rate Limits）] ページ

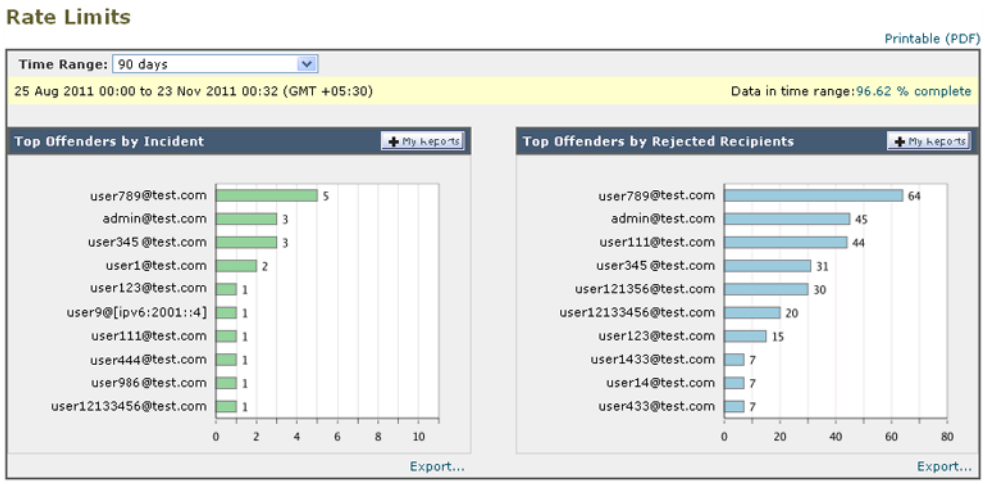
エンベロープ送信者ごとのレート制限を使用すると、メール送信者アドレスに基づいて、個々の送信者からの時間間隔ごとの電子メール メッセージ受信者数を制限できます。[レート制限（Rate Limits）] レポートには、この制限を最も上回った送信者が表示されます。

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。

図 4-14　[レート制限（Rate Limits）] ページ



[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（拒否した受信者別）（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、電子メール 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 ポリシーの設定（Mail Flow Policies settings）] で行います。レート制限の詳細については、ご使用の電子メール 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。

[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。このページを使用すると、攻撃対象となったウイルス、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

[タイプ別脅威（Threats By Type）] セクションには、アプライアンスで受信したさまざまな種類の脅威メッセージが表示されます。[脅威サマリー（Threat Summary）] セクションには、ウイルス、フィッシング攻撃、および詐欺によるメッセージの内訳が表示されます。

[過去 1 年間のアウトブレイク サマリー（Past Year Outbreak Summary）] には、前年のグローバルな発生およびローカルでの発生が表示されるので、ローカル ネットワーク トレンドとグローバル 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。ローカル発生データには非ウイルス性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、Cisco IronPort Threat Operations Center によって検出されたすべての感染を表します。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、Cisco IronPort Threat Operations Center による各ウイルス感染の検出と、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。

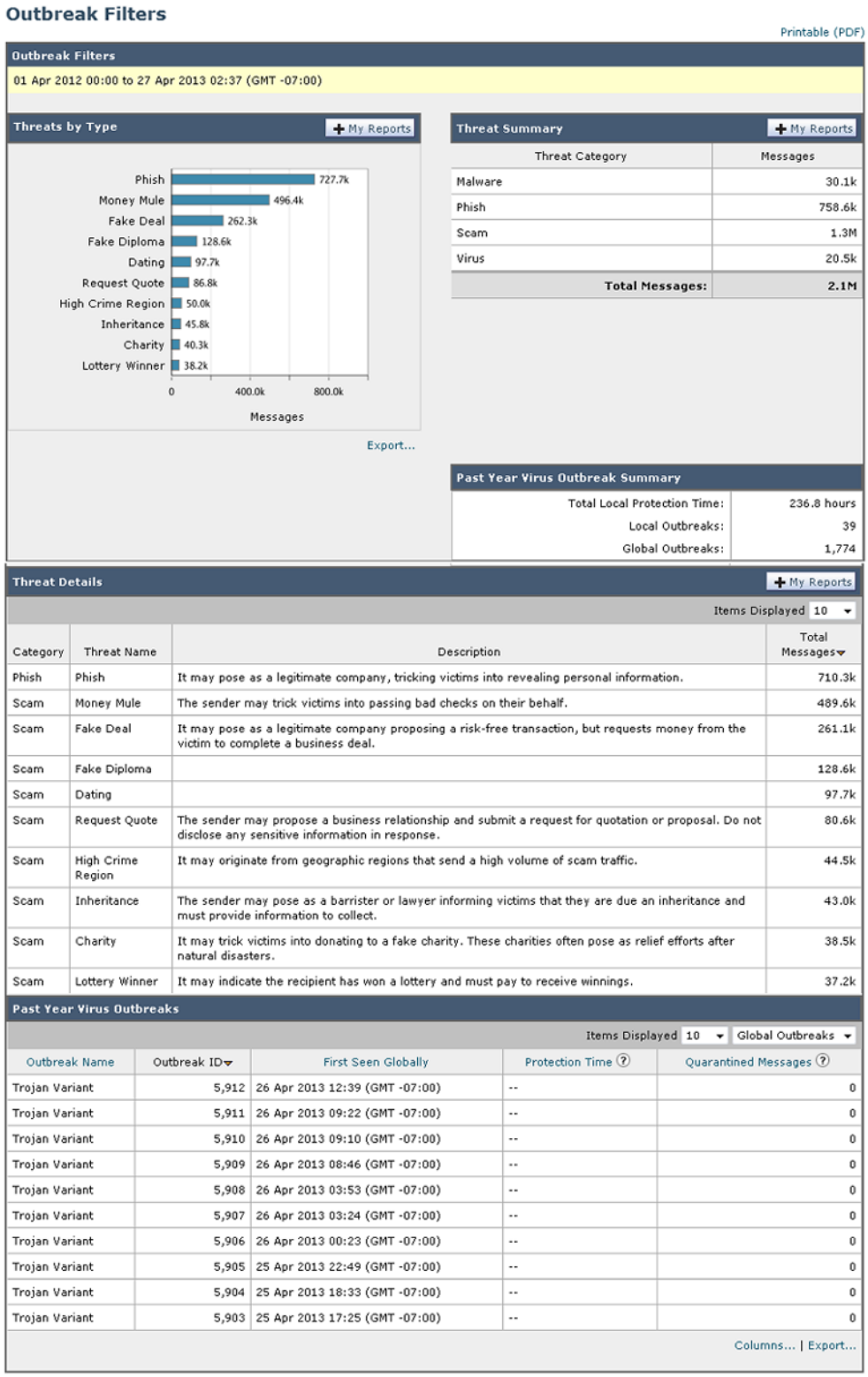
[隔離されたメッセージ（Quarantined Messages）] セクションでは、感染フィルタの隔離状況の概要が示されます。これは、感染フィルタが捕捉した潜在的な脅威メッセージの数を把握するのに役立つ尺度です。隔離されたメッセージは、解放時に集計されます。通常、アンチウイルス ルールおよびアンチスパム ルールが使用可能になる前に、メッセージが隔離されます。メッセージが解放されると、アンチウイルス ソフトウェアおよびアンチスパム ソフトウェアによってスキャンされ、ウイルス陽性か、クリーンかを判定されます。感染トラッキングの動的性質により、メッセージが隔離領域内にあるときでも、メッセージの隔離ルール（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）、脅威名、脅威の説明、識別されたメッセージ数など、特定の発生についての情報が表示されます。ウイルス感染発生の場合、[過去 1 年間のウイルス アウトブレイク（Past Year Virus Outbreaks）] に感染名、および ID、ウイルス感染が最初にグローバルに発見された時刻と日付、感染フィルタによって保護された時刻、および隔離されたメッセージ数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。カラム 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。

[最初にグローバルで確認した日時（First Seen Globally）] の時刻は、世界最大規模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 からのデータに基づき、Cisco IronPort Threat Operations Center によって決定されます。[保護時間（Protection Time）] は、Cisco IronPort 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常に基づいています。

「--」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。

図 4-15　[アウトブレイク フィルタ（Outbreak Filters）] ページ



（注）　[アウトブレイク フィルタ（Outbreak Filters）] ページにテーブルが正しく表示されるためには、セキュリティ管理アプライアンスが downloads.cisco.com と通信できる必要があります。

[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。

- 電子メール セキュリティ アプライアンスが推奨キャパシティをいつ超えたか。これによって、設定の最適化または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。

Monitor your 電子メール 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）]」（P.4-46）および「[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]」（P.4-47）を参照してください。
- **作業キュー**：作業キューは、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）]」（P.4-45）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。RCM は、[システム容量（System Capacity）] ページでは追跡できません。

[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ー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ー数を表示します。これも正確な数値です。

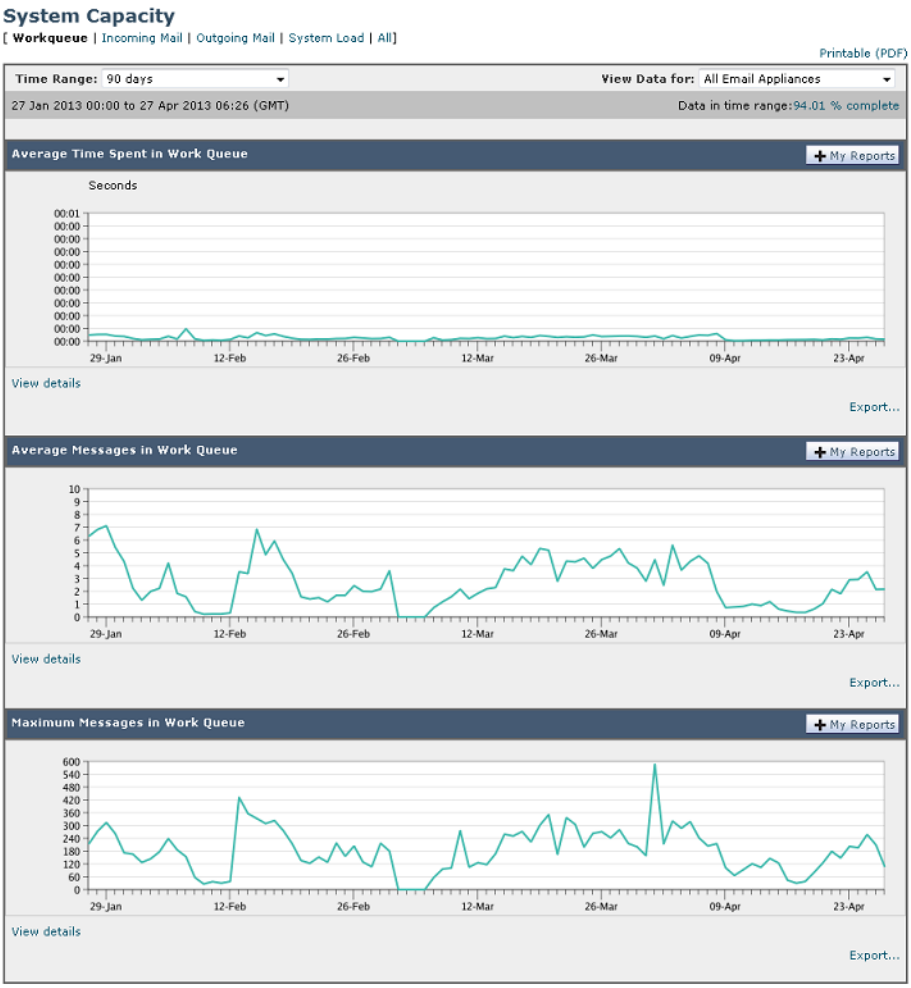
[システム容量（System Capacity）] ページの [最大（Maximum）] 値インジケータは、指定された期間の最大値を示します。[平均（Average）] 値は指定された期間のすべての値の平均です。集計期間は、レポートに対して選択された間隔に応じて異なります。たとえば、月単位のチャートの場合は、日付ごとの [平均（Average）] 値と [最大（Maximum）] 値を表示することができます。

特定のグラフの [詳細表示（View Details）] リンクをクリックすると、個々の電子メール 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）]

[システム容量（System Capacity）] : [ワークキュー（Workqueue）] ページには、指定された期間の作業キュー内のメッセージ量が表示されます。また、同じ期間の作業キュー内の最大メッセージも表示されます。日、週、月、または年のデータを表示することもできます。[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。スパイクの発生頻度が高くなり、長期間にわたって同様の状態が続く場合、キャパシティの問題を示している可能性があります。[ワークキュー（Workqueue）] ページを確認するときは、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。

図 4-16　[システム容量（System Capacity）] : [ワークキュー（Workqueue）]



[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。

図 4-17　[システム容量（System Capacity）] : [受信メール（Incoming Mail）]

[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 データと発信宛先データを比較して、特定のドメインまたは IP アドレスから送信される電子メール 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。

図 4-18　[システム容量（System Capacity）] : [送信メール（Outgoing Mail）]

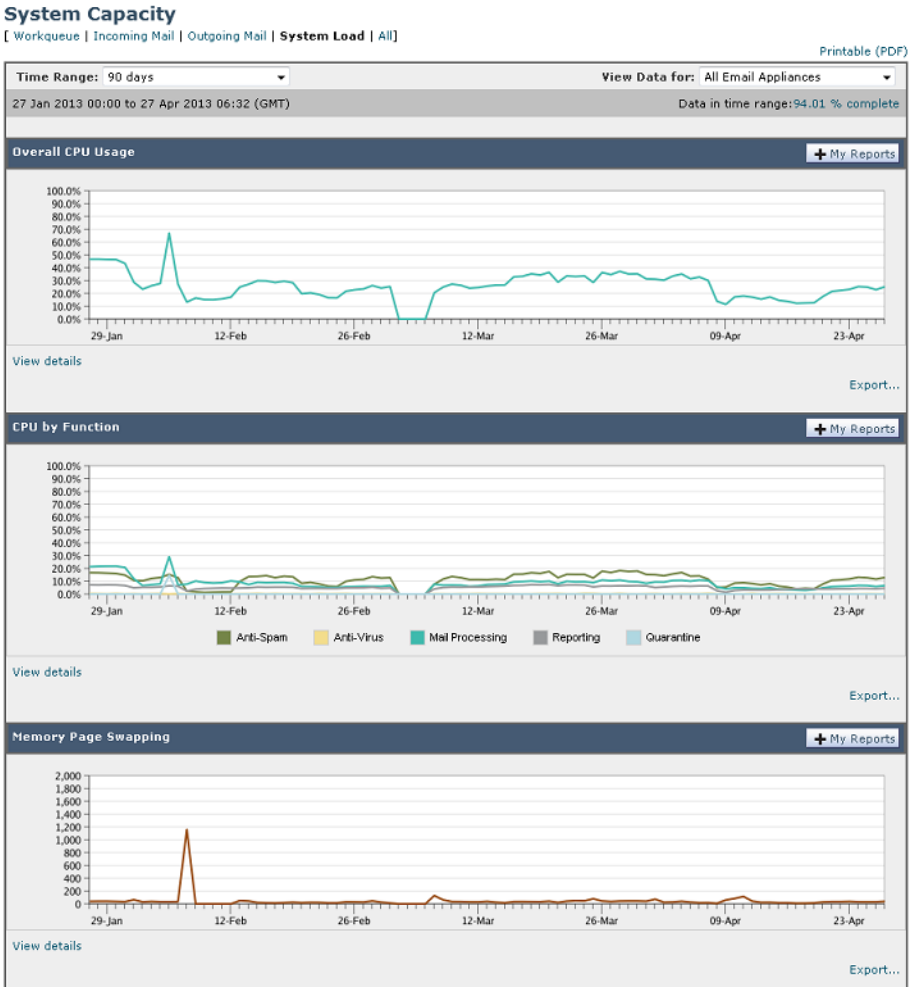
[システム容量（System Capacity）] : [システムの負荷（System Load）]

システム負荷レポートには、電子メール セキュリティ アプライアンスでの総 CPU 使用率が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してメッセージ 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。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）。

図 4-19　[システム容量（System Capacity）] : [システムの負荷（System Load）]



メモリ ページ スワッピングに関する注意事項

システムは、定期的にメモリをスワップするように設計されているので、一部のメモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが *常に* 高ボリュームのメモリ スワッピングを行う場合以外は、メモリ スワッピングは正常であり、起こり得る挙動です（特に C150 アプライアンスの場合）。たとえば、図 4-20 に、高ボリュームのメモリ スワッピングを常に行うシステムを示します。パフォーマンスを向上させるには、ネットワークにシスコ コンテンツ 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。

図 4-20　[システム容量（System Capacity）] : [システムの負荷（System Load）]（高負荷時のシステム）

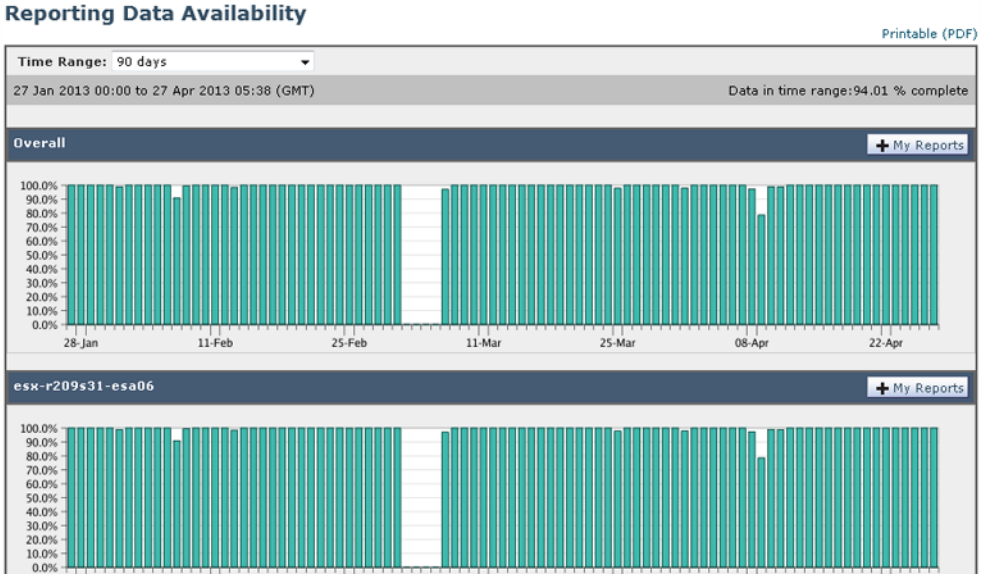
[システム容量（System Capacity）] : [すべて（All）]

[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。

[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。

図 4-21　[有効なメール レポート データ（Email Reporting Data Availability）] ページ



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。

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」（P.4-34）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」（P.4-31）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。各統計情報のカラム見出しのリンクをクリックすることによって、最新のホスト ステータス、アクティブな受信者（デフォルト）、切断した接続、配信された受信者、ソフト バウンス イベント、およびハード バウンス受信者別にソートできます。電子

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、お使いの電子メール 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）]：このレポートは電子メール レポーティングの [概要（Overview）] 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」（P.4-53）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 電子メール レポーティングの [概要（Overview）] 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」（P.4-53）を参照してください。
- [受信メール サマリー（Incoming Mail Summary）]：このページに表示される情報については、「[受信メール（Incoming Mail）] ページ」（P.4-16）を参照してください。
- [内部ユーザのサマリー（Internal Users Summary）]：このページに表示される情報については、「[内部ユーザ（Internal Users）] ページ」（P.4-28）を参照してください。
- [アウトブレイク フィルタ（Outbreak Filters）]：このページに表示される情報については、「[アウトブレイク フィルタ（Outbreak Filters）] ページ」（P.4-41）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」（P.4-24）を参照してください。
- [送信メール サマリー（Outgoing Mail Summary）]：このページに表示される情報については、「[送信メッセージ送信者（Outgoing Senders）] ページ」（P.4-26）を参照してください。
- [送信メッセージ送信者（Outgoing Senders）]：このページに表示される情報については、「[送信メッセージ送信者（Outgoing Senders）] ページ」（P.4-26）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」（P.4-23）を参照してください。
- [システム容量（System Capacity）]：このページに表示される情報については、「[システム容量（System Capacity）] ページ」（P.4-44）を参照してください。
- [TLS 接続（TLS Connections）]：このページに表示される情報については、「[TLS 接続（TLS Connections）] ページ」（P.4-37）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 タイプ（Virus Types）] ページ」（P.4-35）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。[定期レポート（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 データの印刷およびエクスポート」（P.3-10）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、「アーカイブ電子メール レポートの表示と管理」（P.4-59）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
- [エグゼクティブ サマリー（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

[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、電子メール セキュリティ アプライアンスおよび セキュリティ管理アプライアンスのレポーティング 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、電子メール 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

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作業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 HAT 拒否を遅延します。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。電子メール 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、ご使用の電子メール 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）] レポートの [レピュテーション フィルタによる停止（Stopped by Reputation Filtering）] の結果を表示するには、電子メール 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** をイネーブルにする必要があります。

セキュリティ管理アプライアンスで **hat_reject_info** をイネーブルにするには、**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 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

手順

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. [メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

b. [定期レポートを追加（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。

a. [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。

b. [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。

- [個別のドメインを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。複数のエントリを区切るには、カンマを使用します。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」（P.4-54）を参照してください。

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

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

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

ステップ 5　[送信ドメイン（Outgoing Domain）] セクションで、発信メール サマリーのドメイン タイプを選択します。選択肢は [サーバ別（By Server）] または [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　[形式（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]。カンマ区切りの値として 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 [毎日（Daily）]、[毎週（Weekly）]（曜日のドロップダウン リストがあります）または [毎月（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 Cisco 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 データの印刷およびエクスポート」（P.3-10）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、電子メール セキュリティ アプライアンスからの着信および発信メッセージ アクティビティの概要です。セキュリティ管理アプライアンス上で表示できます。

このレポート ページには、電子メール レポーティングの [概要（Overview）] 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、「電子メール レポーティングの [概要（Overview）] ページ」（P.4-11）を参照してください。

電子メール 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」（P.4-51）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」（P.4-56）
- 「スケジュール設定されたレポートの編集」（P.4-57）
- 「スケジュール設定されたレポートの中止」（P.4-58）

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。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[定期レポートを追加（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」（P.4-51）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」（P.4-53）を参照してください。

（注）　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　[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は、raw データを CSV ファイルとして保存することも可能です。

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カラムを選択します。

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 データの印刷およびエクスポート」（P.3-10）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

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　[レポートのタイトル（Report Title）] カラムの、変更するレポート名リンクをクリックします。

ステップ 3　レポート設定値を変更します。

ステップ 4　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。

手順

ステップ 1　セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [定期レポート（Scheduled Reports）] を選択します。

ステップ 2　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 3　[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」（P.4-60）を参照してください。

オンデマンドでの電子メール レポートの生成

「[メール レポート（Email Reporting）] ページの概要」（P.4-7）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」（P.4-51）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。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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 2　[今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 3　レポート タイプを選択します。

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」（P.4-51）を参照してください。

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。

（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」（P.4-53）を参照してください。

（注）　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 5　[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 6　[形式（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

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

ステップ 7　レポート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 8　[送信オプション（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 9　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 データの印刷およびエクスポート」（P.3-10）の重要な情報を参照してください。

ステップ 10　[このレポートを送信（Deliver This Report）] をクリックして、レポートを生成します。

アーカイブ電子メール レポートの表示と管理

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 12 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。12 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、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください）。

アーカイブ済みのレポートへのアクセス

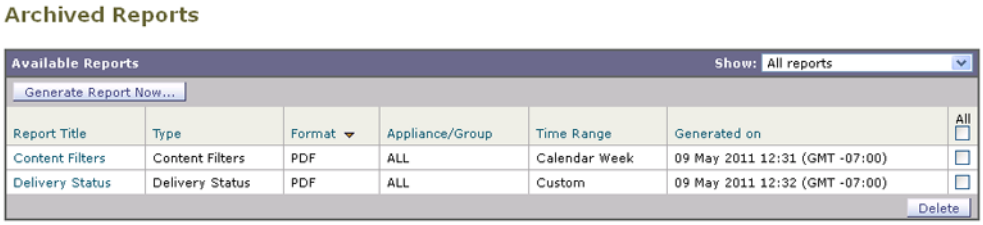
[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページには、生成されたがまだ消去されておらず、アーカイブすることを指定した、スケジュール設定されたレポートとオンデマンド レポートが表示されます。

手順

ステップ 1　[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。

[アーカイブ レポート（Archived Reports）] のリストが表示されます。

図 4-22　　アーカイブ レポート（Archived Reports）



ステップ 2　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、またはカラムのヘッダーをクリックし、そのカラムでソートします。

ステップ 3　[レポートのタイトル（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

「アーカイブ電子メール レポートの表示と管理」（P.4-59）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。

手順

ステップ 1　セキュリティ管理アプライアンスで、[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 2　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 3　[削除（Delete）] をクリックします。

ステップ 4　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」（P.4-58）を参照してください。