CHAPTER 4

中央集中型電子メール 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。

レポーティングの概要

電子メール レポーティング機能では、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、個別または複数の電子メール セキュリティ アプライアンスから情報を収集します。リアルタイムに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、一定の間隔で実行するようにレポートのスケジュールを設定することもできます。レポーティング機能を使用すると、raw データをファイルにエクスポートすることもできます。

中央集中型電子メール レポーティング機能では、ネットワークの現状を把握できる概要レポートの収集だけではなく、ドリル ダウンして特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を表示することもできます。

中央集中型トラッキング機能では、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を追跡できます。

電子メール レポーティングを使用する前に

（注）　Email Security アプライアンスの電子メール レポーティングを表示するには、1 つまたは複数の Email Security アプライアンスを追加して設定する必要があります。Email Security アプライアンスの追加の詳細については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。Email Security アプライアンスの設定の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

Security Management アプライアンスで電子メール レポーティング データを表示する方法はいくつかあります。電子メール レポーティングを開始するには、次の手順を使用します。

- 電子メール レポーティングをイネーブルにするには、「中央集中型電子メール レポーティングの設定」（P.4-3）を参照してください。
- 電子メール レポーティング グループを作成するには、「電子メール レポーティング グループの作成」（P.4-4）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 ページを表示して理解するには、「電子メール レポーティング ページの概要」（P.4-12）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、「オンデマンドでのレポートの生成」（P.4-74）を参照してください。
- 指定した間隔や時刻に自動的に実行されるよう、レポートのスケジュールを設定するには、「スケジュール設定されたレポート」（P.4-76）を参照してください。
- アーカイブ済みのオンデマンド レポートおよびスケジュール設定されたレポートを表示するには、「アーカイブ済みのレポート」（P.4-79）を参照してください。

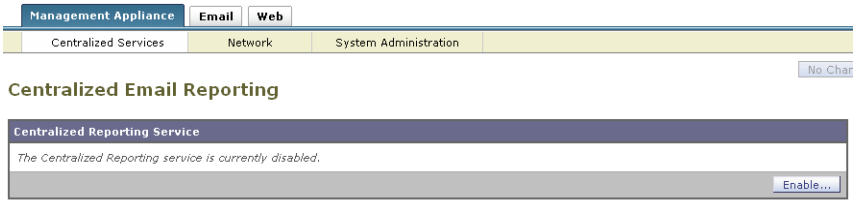
中央集中型電子メール レポーティングの設定

Security Management アプライアンスで電子メール レポーティングを使用するには、すべての電子メール レポーティングがイネーブルになるよう、Security Management アプライアンスを設定する必要があります。

中央集中型電子メール レポーティングを設定するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

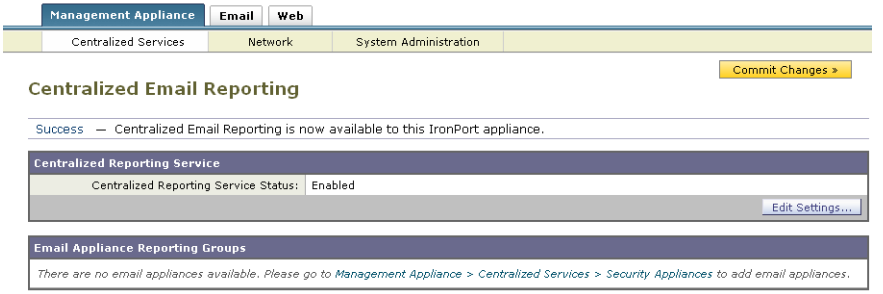
[Centralized Email Reporting] ページが表示されます。



ステップ 2　[Enable] をクリックします。

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、[Accept] をクリックします。

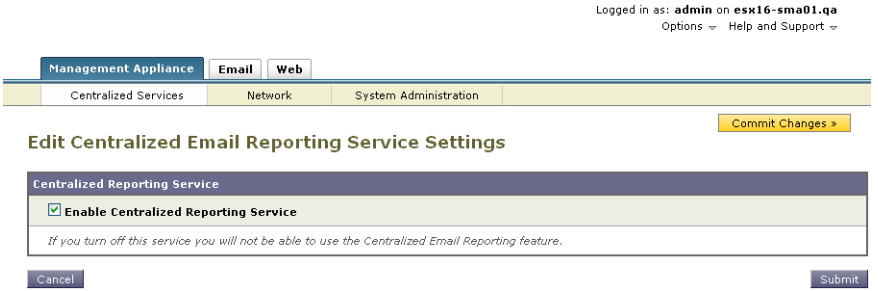
次のウィンドウが表示され、Security Management アプライアンスで中央集中型レポーティングが正常にイネーブルになったことを確認できます。



中央集中型レポーティングをイネーブルにすると、設定を編集できるようになります。

ステップ 3　[Edit Settings] をクリックします。

ステップ 4　[Edit Centralized Email Reporting Service Settings] ページが表示されます。



ステップ 5　[Enable Centralized Reporting Services] チェックボックスをクリックします。

Email Security アプライアンスでデータが保存されるのは、ローカル レポーティングを使用する場合だけです。Email Security 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場合、Email Security アプライアンスはシステム キャパシティとシステム ステータスを除いて、レポート データを保持しません。中央集中型電子メール レポーティングがイネーブルになっていない場合、生成されるレポートはシステム キャパシティとシステム ステータスだけです。

ステップ 6　[Submit] をクリックして変更を送信し、[Commit Changes] をクリックしてアプライアンスでの変更を確定します。

（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.12-123）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

Security Management アプライアンスからのレポーティング データを表示する、Email Security アプライアンスのグループを作成できます。

電子メール レポーティング グループの追加

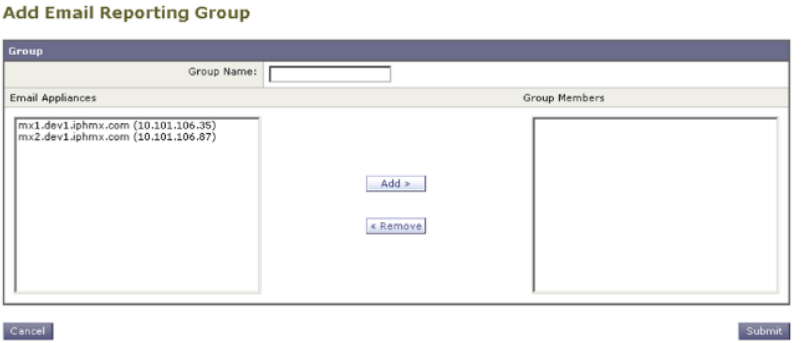
電子メール レポーティング グループを追加するには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

ステップ 2　[Add Group] をクリックします。

[Add Email Reporting Group] ページが表示されます。

図 4-1　[Add Email Reporting Group] ページ



ステップ 3　グループの一意の名前を入力します。

Email Security アプライアンスで、Security Management アプライアンスに追加した Email Security 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）　Email Security アプライアンスを Security Management 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、Security Management 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 Email Security アプライアンスの設定を編集します。

ステップ 4　[Add] をクリックして、[Group Members] リストにアプライアンスを追加します。

ステップ 5　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

（注）　アプライアンスを、複数のグループに含めることができます。

電子メール レポーティング グループの編集と削除

電子メール レポーティング グループを編集または削除するには、次の手順を実行します。

ステップ 1　メイン Security Management アプライアンスのウィンドウで、[Management Appliance] > [Centralized Services] > [Email] > [Centralized Reporting] を選択します。

[Centralized Reporting] ページが表示されます。このページでは、Email Security アプライアンス レポーティング グループを表示できます。

ステップ 2　グループを削除するには、削除するグループの横にある対応するゴミ箱アイコンをクリックします。

または

グループを編集するには、編集するグループの名前をクリックします。

[Edit Email Reporting Group] ページが表示されます。このページでは、グループを編集できます。

ステップ 3　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[Email Reporting] タブの使用

[Email] > [Reporting] タブには、レポーティング データの複数の表示オプションが表示されます。ここでは、このタブに表示される各レポーティング ページ、および各レポーティング ページに表示される情報について説明します。

（注）　レポーティング オプションの要約については、「レポーティング オプション」（P.3-16）を参照してください。

表 4-1　[Email Reporting] タブの詳細

[Email Reporting] メニュー	アクション
電子メール レポーティングの [Overview] ページ	[Overview] ページには、Cisco IronPort 電子メール 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のグラフや要約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 [Overview] ページ」（P.4-12）を参照してください。
[Incoming Mail] ページ	[Incoming Mail] ページには、管理対象の Email Security 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、「[Incoming Mail] ページ」（P.4-17）を参照してください。
[Outgoing Destinations] ページ	[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。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、「[Outgoing Destinations] ページ」（P.4-31）を参照してください。
[Outgoing Senders] ページ	[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、「[Outgoing Senders] ページ」（P.4-33）を参照してください。

表 4-1　[Email Reporting] タブの詳細（続き）

[Email Reporting] メニュー	アクション
[Internal Users] ページ	[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、「[Internal Users] ページ」（P.4-36）を参照してください。
[DLP Incident Summary] ページ	[DLP Incident Summary] ページには、送信メールで発生した、データ損失防止（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 Incident Summary] ページ」（P.4-40）を参照してください。
[Content Filters] ページ	[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。また、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。[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、「[Content Filters] ページ」（P.4-43）を参照してください。
[Virus Types] ページ	[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。[Virus Types] ページには、Email Security アプライアンスで稼動し、Security Management 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、「[Virus Types] ページ」（P.4-45）を参照してください。
[TLS Connections] ページ	[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 Connections] ページ」（P.4-48）を参照してください。

表 4-1　[Email Reporting] タブの詳細（続き）

[Email Reporting] メニュー	アクション
[Outbreak Filters] ページ	[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検疫されたメッセージに関する情報が示されます。このページを使用して、ウイルス攻撃に対する保護をモニタします。 詳細については、「[Outbreak Filters] ページ」（P.4-51）を参照してください。
[System Capacity] ページ	レポーティング データを Security Management 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、「[System Capacity] ページ」（P.4-55）を参照してください。
[Data Availability] ページ	各アプライアンスの Security Management 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、「[Data Availability] ページ」（P.4-65）を参照してください。
スケジュール設定されたレポート	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、「スケジュール設定されたレポート」（P.4-76）を参照してください。
アーカイブ済みのレポート	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、「アーカイブ済みのレポート」（P.4-79）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。「オンデマンドでのレポートの生成」（P.4-74）を参照してください。

インタラクティブ レポートの表示

インタラクティブ レポート ページを表示する場合は、次のことを行ってビューをカスタマイズできます。

- **時間範囲を指定する**。詳細については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

- **表示する表カラムを選択する**。表の下にある [Columns] リンクをクリックして、表示または非表示にするカラムを選択します。各カラムの説明については、「中央集中型電子メール レポーティング ページのインタラクティブ カラム」（P.E-5）を参照してください。
- ドラッグおよびドロップして、**表カラムを並べ替える**。
- **カラム見出しをクリックすると**、そのカラム内のデータで表がソートされます。
- **表示されるデータをフィルタリングする**。詳細については、「Security Management アプライアンスのレポート フィルタ」（P.3-19）を参照してください。
- **含める特定の情報を検索する**。「インタラクティブ レポート ページの検索」（P.4-10）を参照してください。

（注） すべてのレポートにすべてのインタラクティブな機能を使用できるわけではありません。

インタラクティブ レポート ページの検索

インタラクティブな電子メール レポーティング ページの多くには、[Search For:] ドロップダウン メニューが含まれています。

次の図に、[Search For] ドロップダウン メニューを示します。

ドロップダウン メニューでは、次のようないくつかの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。

IP アドレス検索では、入力したテキストが最大で 4 IP オクテット（ドット付き 10 進表記）の先頭部として常に解釈されます。たとえば、「17」は範囲 17.0.0.0 ～ 17.255.255.255 で検索するため、17.0.0.1 には一致しますが、172.0.0.1 には一致しません。完全一致検索の場合は、4 つすべてのオクテットを入力します。IP アドレス検索は、Classless Inter-Domain Routing（CIDR）形式（17.16.0.0/12）もサポートしています。

レポート ページのレポーティング フィルタ

AsyncOS には、前年をカバーするレポート（[Last Year] レポート）のデータの集約を制限できるレポート フィルタがあります。1 ヵ月分に大量の一意のエントリが存在することで、集約されたレポートのパフォーマンスが低下する場合には、これらのフィルタを使用できます。これらのフィルタにより、レポート内の詳細、個々の IP、ドメイン、またはユーザ データを制限できます。概要レポートおよびサマリー情報は、引き続きすべてのレポートで利用できます。

レポーティング フィルタをイネーブルにする方法の詳細については、「Security Management アプライアンスのレポート フィルタ」（P.3-19）を参照してください。

レポート ページからのレポートの印刷とエクスポート

「レポート データの印刷とエクスポート」（P.3-21）を参照してください。

レポートとレポート ページについてのその他の情報

- 「レポーティング オプション」（P.3-16）
- 「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.3-17）

電子メール レポーティング ページの概要

ここでは、Security Management アプライアンスで電子メール レポーティングに使用されるさまざまなレポート ページについて説明します。

次の内容で構成されています。

電子メール レポーティングの [Overview] ページ

Security Management アプライアンスの [Email] > [Reporting] > [Overview] ページには、Email Security アプライアンスからの電子メール メッセージの概要が表示されます。[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。

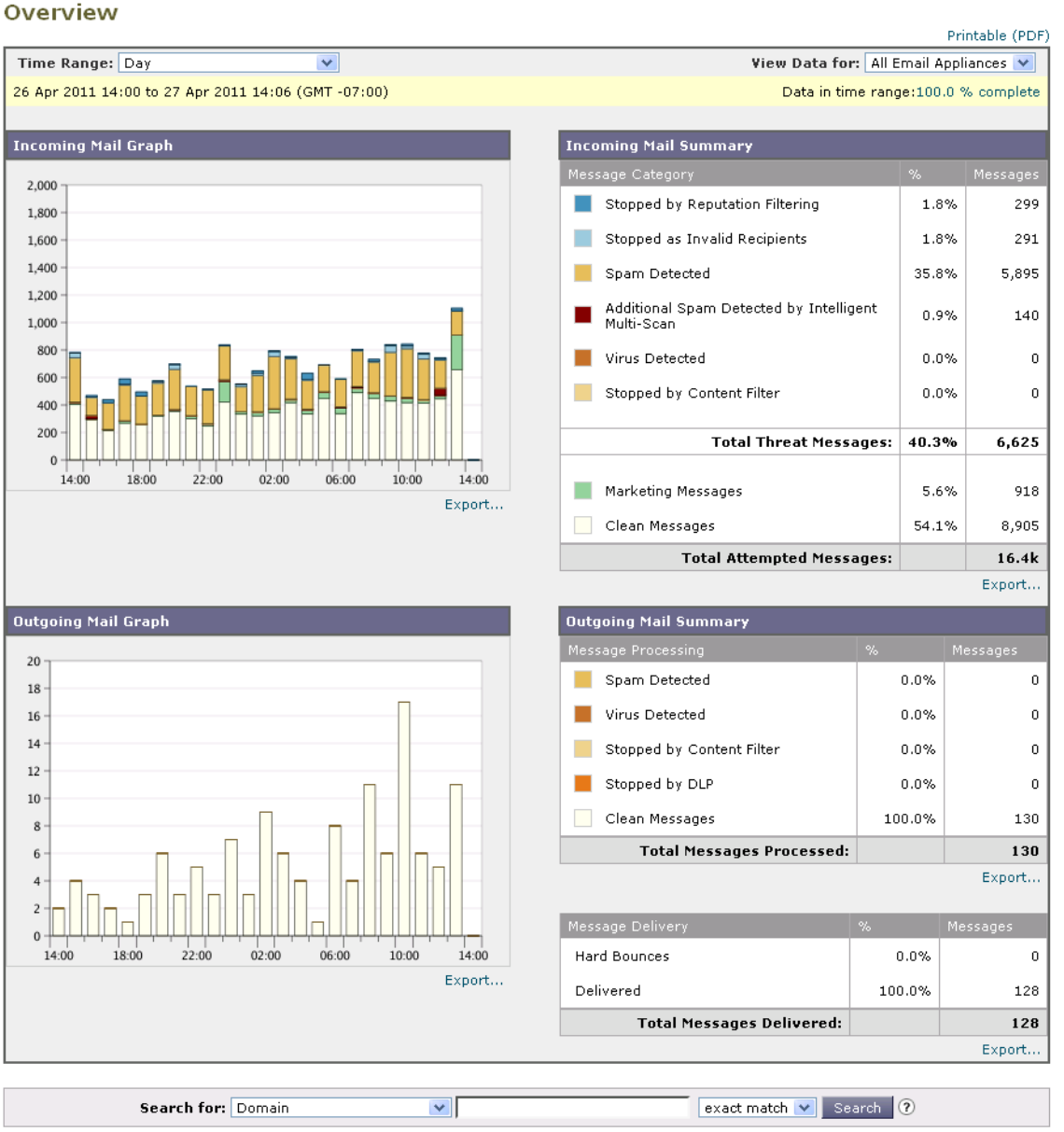
[Overview] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Management Appliance] > [Email] > [Reporting] > [Overview] を選択します。

[Overview] ページが表示されます。

図 4-2 に、[Overview] ページを示します。

図 4-2　[Email] > [Reporting] > [Overview] ページ



概要レベルの [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 グラフを使用すると、アプライアンスとのすべてのメール フローをモニタできます。

（注） [Domain-Based Executive Summary] レポートと [Executive Summary] レポートは、電子メール レポーティングの [Overview] ページに基づいて作成されることに注意してください。[Domain-Based Executive Summary] レポートは、指定されたドメインのグループに制限されます。レポートのスケジュール設定の詳細については、「スケジュール設定されたレポート」（P.4-76）を参照してください。

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

表 4-2　[Email] > [Reporting] > [Overview] ページの詳細

セクション	説明
Time Range	表示する時間範囲を選択するためのオプションのあるドロップダウン リスト。詳細については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
Incoming Mail Graph	[Incoming Mail Graph] には、受信メールの詳細がリアルタムにグラフで表示されます。
Outgoing Mail Graph	[Outgoing Mail Graph] には、送信メールの詳細がリアルタムにグラフで表示されます。
Incoming Mail Summary	[Incoming Mail Summary] では、レピュテーション フィルタリング（SBRS）によって阻止されたメッセージの割合と数、個々の受信者、検出されたスパム、検出されたウイルスとして阻止されたメッセージの割合と数、コンテンツ フィルタによって阻止されたメッセージの割合と数、「クリーン」であると認識されたメッセージの割合と数が表示されます。
Outgoing Mail Summary	[Outgoing Mail Summary] セクションには、発信脅威およびクリーン メッセージについての情報が表示されます。また、配信されたウイルスがハードバウンスされたメッセージの詳細も表示されます。

着信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基づいて受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。

評価フィルタによってブロックされたメッセージは、実際には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 Cisco IronPort Systems によって算出されたもので、既存の顧客データの大規模なサンプリング研究に基づいています。

電子メール メッセージをアプライアンス別に分類する方法

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。

- 感染フィルタの検疫
  (この場合、メッセージが検疫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、または検疫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。

[Overview] ページでの電子メール メッセージの分類

[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 4-3　[Overview] ページの電子メールのカテゴリ

カテゴリ	説明
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（「着信メッセージのカウント方法」（P.4-15）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。 [Overview] ページの [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。
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。
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。
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。
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。

表 4-3　[Overview] ページの電子メールのカテゴリ（続き）

カテゴリ	説明
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。
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。

[Incoming Mail] ページ

Security Management アプライアンスの [Incoming Mail] > [Reporting] > [Incoming Mail] ページには、管理対象の Security Management 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。

[Incoming Mail] ページ。（脅威メッセージの総数およびクリーン メッセージの総数によって）上位送信者を集約するメール トレンド グラフと、[Incoming Mail Details] インタラクティブ テーブルの 2 つのメイン セクションで構成されます。

[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。[Incoming Mail] ページまたは他の [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 [Sender Profile] ページにアクセスできます。

[Incoming Mail] ページでは、次の操作を実行できます。

- Security Management 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。
- 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、「[Sender Groups] レポート ページ」（P.4-30）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。
- Cisco IronPort SenderBase 評価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 Cisco SenderBase 評価スコア、ドメインが直近に一致した送信者グループなど IronPort SenderBase 評価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。

[Incoming Mail] ページ内のビュー

[Incoming Mail] ページには、次の 3 つのビューがあります。

- IP Addresses
- Domains
- Network Owners

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、[Incoming Mail Details] ページの [Incoming Mail Details] セクションでは、[Senders IP Address]、[Domain name]、または [Network Owner Information] をクリックすると、特定の [Sender Profile Information] を取得できます。[Sender Profile] の情報の詳細については、「[Sender Profile] ページ」（P.4-25）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、[Incoming Mail Details] インタラクティブ テーブルに、Email Security 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、[Sender Profile] ページの送信者の詳細にアクセスできます。[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 [Incoming Mail] ページです。

[Incoming Mail] ページの下部にある [Sender Groups Report] リンクをクリックすると、送信者グループ別のメール フロー情報にアクセスできます。

[Incoming Mail] ページでの電子メール メッセージの分類

[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 4-4　[Incoming Mail] ページの電子メールのカテゴリ

カテゴリ	説明
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（「着信メッセージのカウント方法」（P.4-15）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。 [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。
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。
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。
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。
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。

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

カテゴリ	説明
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
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、Security Management アプライアンスの [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 [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。

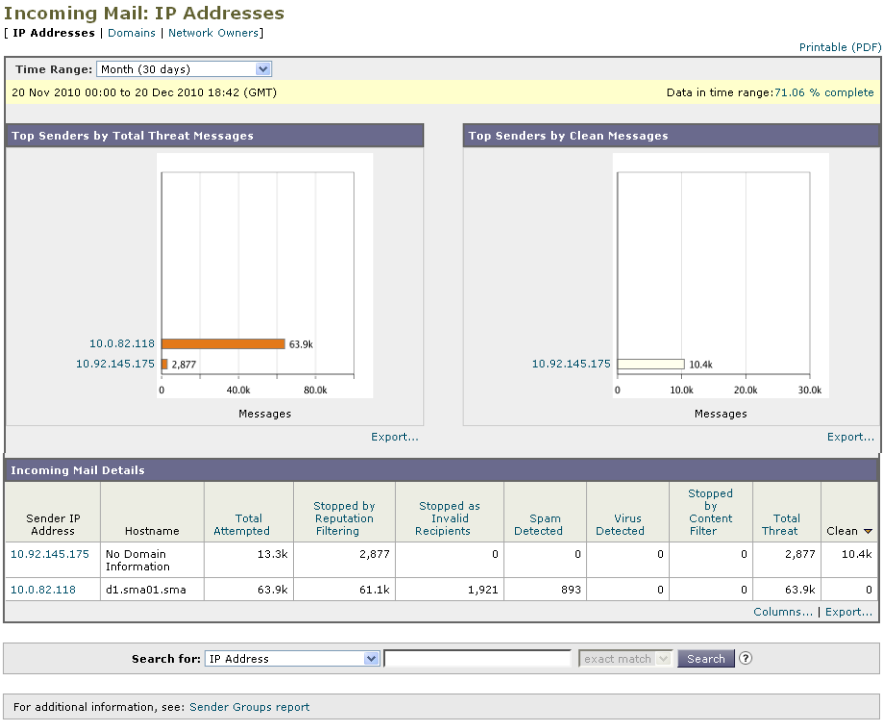
トップレベル ページ（この場合には [Incoming Mail] レポート ページ）の右上にある [Printable PDF] リンクをクリックすると、これらの各サブレポート ページの結果を、1 つの統合レポートに生成できます。「電子メール レポーティング ページの概要」（P.4-12）の重要な情報を参照してください。

[Incoming Mail] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Incoming Mail] を選択します。

[Incoming Mail Page] ページが表示されます。この例では、[IP Address] ビューが選択されています。

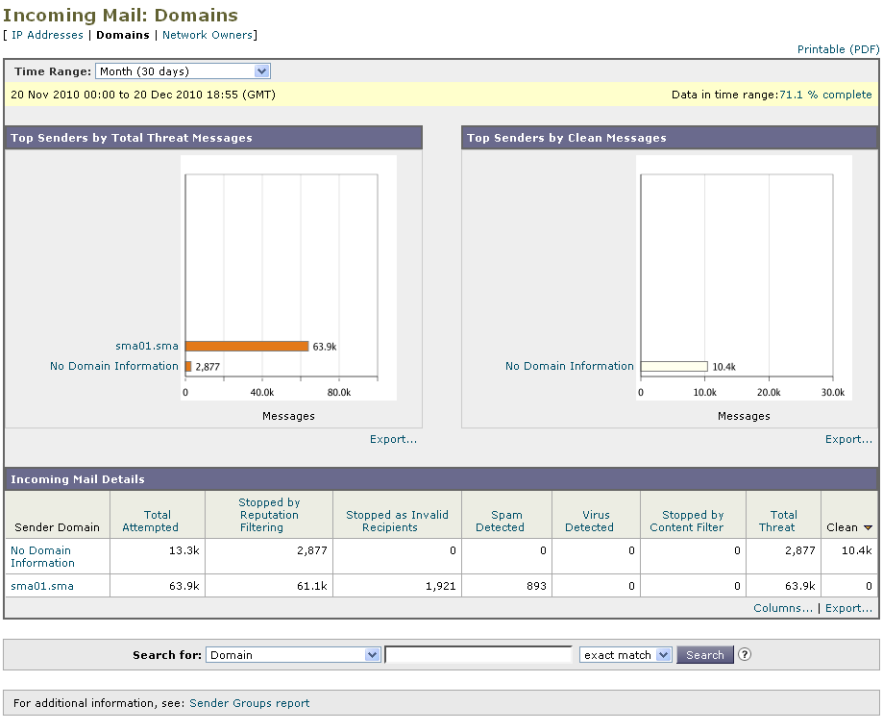
図 4-3　[Incoming Mail] ページ：[IP Address] ビュー



[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、「[Incoming Mail Details] テーブル」（P.4-24）を参照してください。

この例では、[Domain] ビューが選択されています。

図 4-4　[Incoming Mail] ページ：[Domain] ビュー



[Incoming Mail] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

（注）　[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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[No Domain Information] リンク

Security Management 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 [No Domain Information] に自動的に分類されます。これらの種類の検証されないホストは、送信者の検証によって管理できます。送信者検証の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

[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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

[Incoming Mail Details] テーブル

[Incoming Mail] ページの下部にあるインタラクティブな [Incoming Mail Details] テーブルには、Email Security 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。

*二重 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。二重 DNS ルックアップと送信者検証の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

[Incoming Mail Details] テーブルの最初のカラム、または [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、[Sender] または [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、[Sender Profile] ページに表示され、IronPort SenderBase 評価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、「[Sender Profile] ページ」（P.4-25）を参照してください。

[Incoming Mail] ページの下部にある [Sender Groups Report] をクリックして、[Sender Groups] レポートを表示することもできます。[Sender Groups] レポートページの詳細については、「[Sender Groups] レポート ページ」（P.4-30）を参照してください。

[Sender Profile] ページ

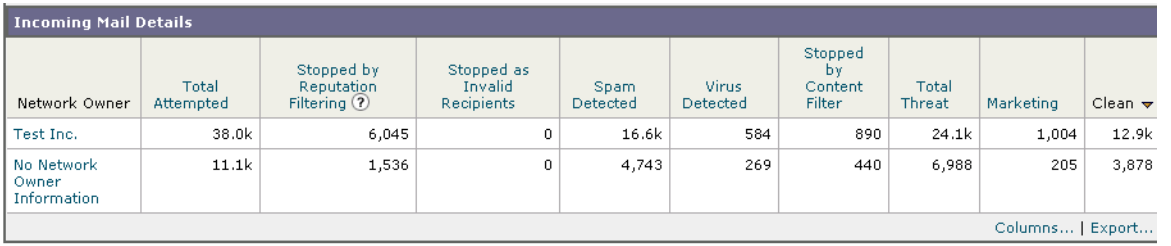
[Incoming Mail] ページで [Incoming Mail Details] インタラクティブ テーブルの送信者をクリックすると、[Sender Profile] ページが表示されます。ここには、特定の IP アドレス、ドメイン、またはネットワーク オーナー（組織）の詳細情報が表示されます。[Incoming Mail] ページまたは他の [Sender Profile] ページにある対応するリンクをクリックすると、IP アドレス、ドメイン、またはネットワーク オーナーの [Sender Profile] ページにアクセスできます。

*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 ページに、詳細なリストは含まれません）。[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。

図 4-5　　ネットワーク オーナーのドメイン リスト


Incoming Mail Details

Network Owner	Total Attempted	Stopped by Reputation Filtering	Stopped as Invalid Recipients	Spam Detected	Virus Detected	Stopped by Content Filter	Total Threat	Marketing	Clean
Test Inc.	38.0k	6,045	0	16.6k	584	890	24.1k	1,004	12.9k
No Network Owner Information	11.1k	1,536	0	4,743	269	440	6,988	205	3,878

Columns... | Export...

各 [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、[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 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か、組織プロファイル ページを表示できます。

図 4-6　ネットワーク オーナーの現在の情報

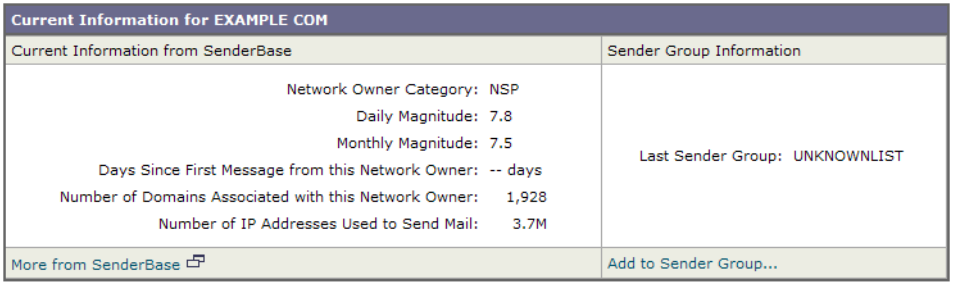


図 4-7　ドメイン プロファイル ページ

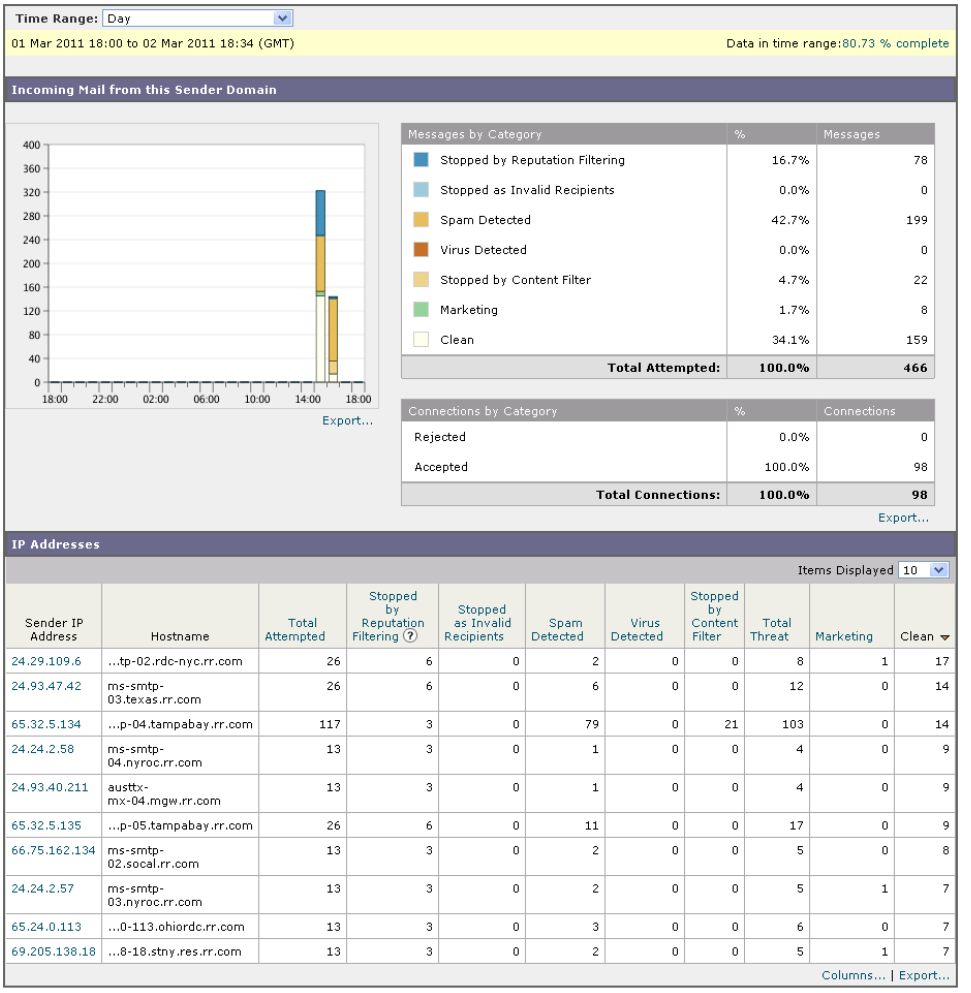


図 4-8　ネットワーク オーナー プロファイル ページ

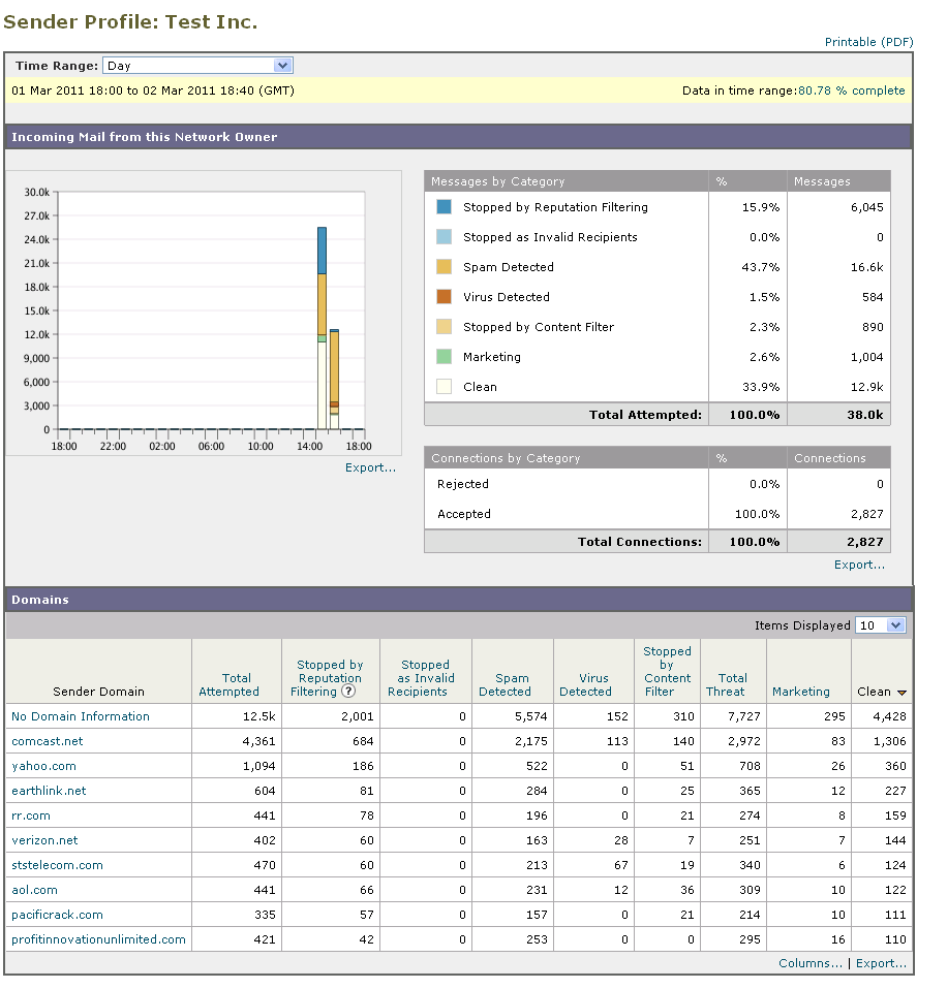
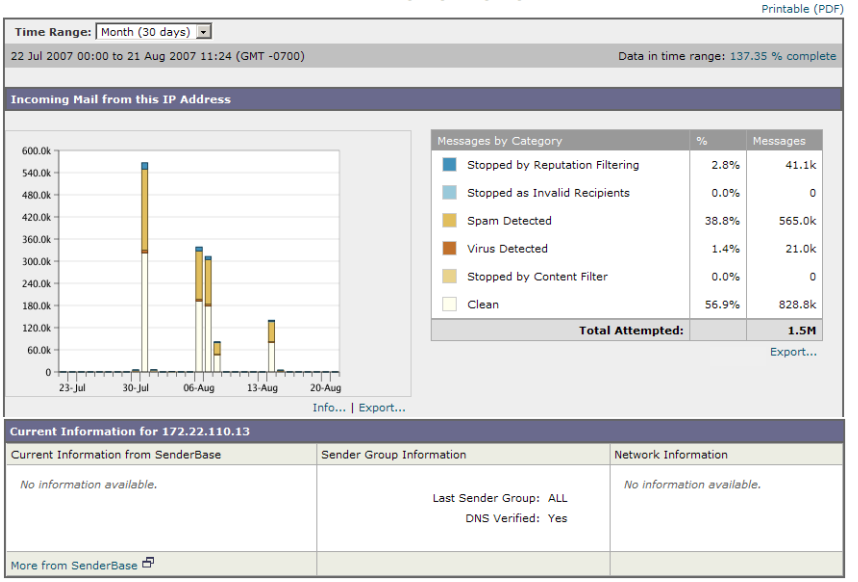


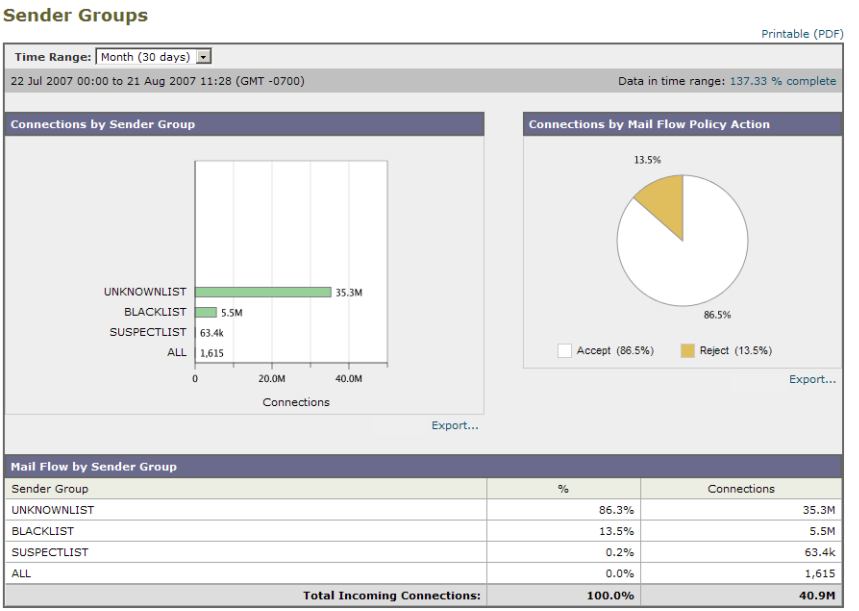
図 4-9　IP アドレス プロファイル ページ



[Sender Groups] レポート ページ

[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。[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。[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 の詳細については、『*Cisco IronPort AsyncOS for Email Security Configuration Guide*』を参照してください。

図 4-10　[Sender Groups] レポート ページ



[Sender Groups] レポート ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

（注）　[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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[Outgoing Destinations] ページ

[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。

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

- Email Security 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。

[Outgoing Destinations] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Outgoing Destinations] を選択します。

[Outgoing Destinations] ページが表示されます。

図 4-11　[Email] > [Reporting] > [Outgoing Destinations] ページ

次のリストでは、[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 4-5　[Email] > [Reporting] > [Outgoing Destinations] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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。
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。
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。

[Outgoing Destinations] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

（注） [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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[Outgoing Senders] ページ

[Email] > [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。

[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。

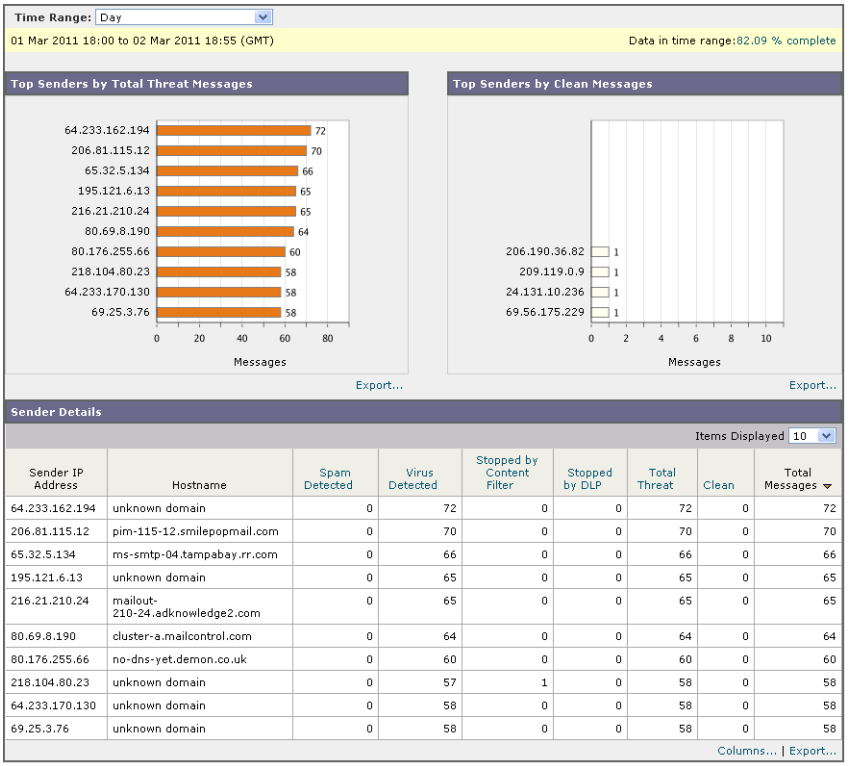
- 最も多くのメールを送信するドメイン
- 配信が試行された場所で処理された受信者の総数。

[Outgoing Sender] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Outgoing Sender] を選択します。

[Outgoing Sender] ページが表示されます。

図 4-12　[Email] > [Reporting] > [Outgoing Senders] ページ（IP アドレスを表示中）



[Outgoing Senders] の結果は次の 2 種類のビューで表示できます。

- [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 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、[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 4-6　[Email] > [Reporting] > [Outgoing Sender] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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）。
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）。
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。

（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 Email Security アプライアンスにログインし、[Monitor]> [Delivery Status] を選択します。

[Outgoing Senders] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

（注） [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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[Internal Users] ページ

[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。

[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。

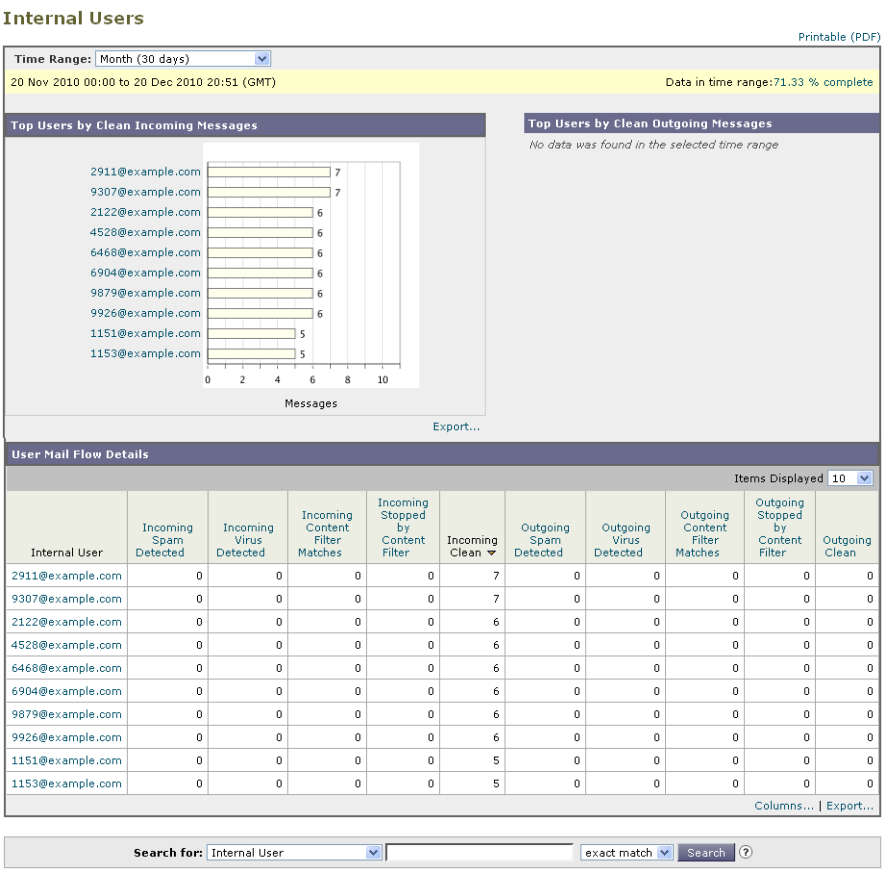
- 最も多くの外部メールを送信したユーザ。
- 最も多くのクリーン電子メールを受信したユーザ
- 最も多くのスパムを受信したユーザ
- 特定のコンテンツ フィルタをトリガーしたユーザ。
- 特定のユーザからの電子メールを阻止したコンテンツ フィルタ。

[Internal Users] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Internal Users] を選択します。

[Internal Users] ページが表示されます。

図 4-13　[Email] > [Reporting] > [Internal Users] ページ



次のリストでは、[Internal Users] 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　[Email] > [Reporting] > [Internal Users] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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）。
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）。
User Mail Flow Details	[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 [Clean]、[Spam Detected]（受信のみ）、[Virus Detected]、[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。 内部ユーザの [Internal User Detail] ページを表示するには、[Internal User] カラムの内部ユーザをクリックします。[Internal Users Details] ページの詳細については、「[Internal User Details] ページ」（P.4-39）を参照してください。

[Internal Users] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

（注） [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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[Internal User Details] ページ

[Internal User Details] ページでは、各カテゴリ（[Spam Detected]、[Virus Detected]、[Sopped By Content Filter]、および [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。

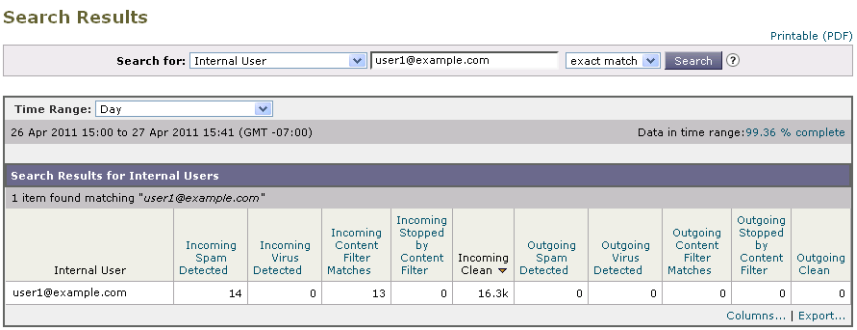
コンテンツ フィルタの詳細情報を対応するコンテンツ フィルタ情報ページに表示するには、そのコンテンツ フィルタ名をクリックします（「[Content Filters] ページ」（P.4-43）を参照）。この方法を使用すると、特定のコンテンツ フィルタに一致したメールを送受信したすべてのユーザのリストも表示できます。

（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

[Internal Users] ページおよび [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。

図 4-14　内部ユーザ検索の結果



[DLP Incident Summary] ページ

[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。Cisco IronPort アプライアンスでは、[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 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。

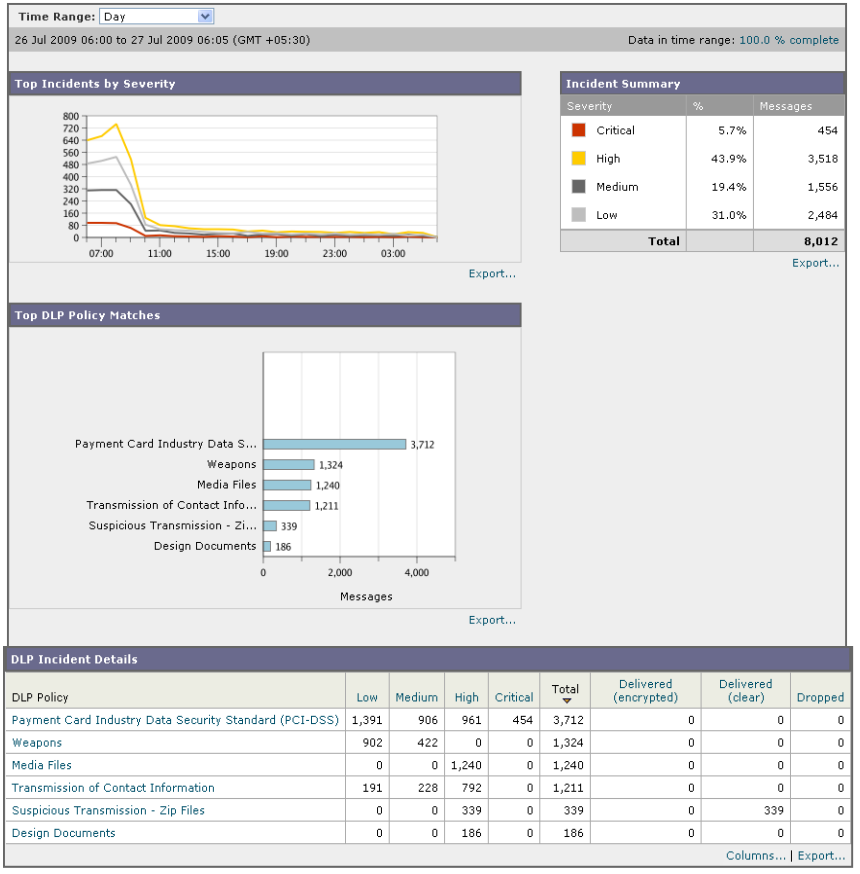
- ユーザが送信した機密データの種類
- これらの DLP インシデントの重大度
- これらのメッセージのうち、配信されたメッセージの数
- これらのメッセージのうち、ドロップされたメッセージの数
- これらのメッセージの送信者

[DLP Summary] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [DLP Summary] を選択します。

[DLP Summary] ページが表示されます。

図 4-15　[Email] > [Reporting] > [DLP Summary] ページ



[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（[Low]、[Medium]、[High]、[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 Incident Details] リスト

次のリストでは、[DLP Incident Summary] ページのさまざまなセクションについて説明します。

表 4-8　[Email] > [Reporting] > [DLP Incident Summary] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
Top Incidents by Severity	重大度別の上位 DLP インシデント。
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 Incident Summary] ページの下部にある [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。
Top DLP Policy Matches	一致している上位 DLP ポリシー。
DLP Incident Details	[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。 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 Incidents Details] ページの詳細については、「[DLP Incidents Details] テーブル」（P.4-42）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 Incidents Details] テーブル

[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。このインタラクティブ 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すると、その DLP ポリシーのページが表示されます。詳細については、「[DLP Policy Detail] ページ」（P.4-43）を参照してください。

[DLP Policy Detail] ページ

[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 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 [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。[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。

送信者名をクリックすると、[Internal Users] ページが開きます。詳細については、「[Internal Users] ページ」（P.4-36）を参照してください。

[Content Filters] ページ

[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。[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。

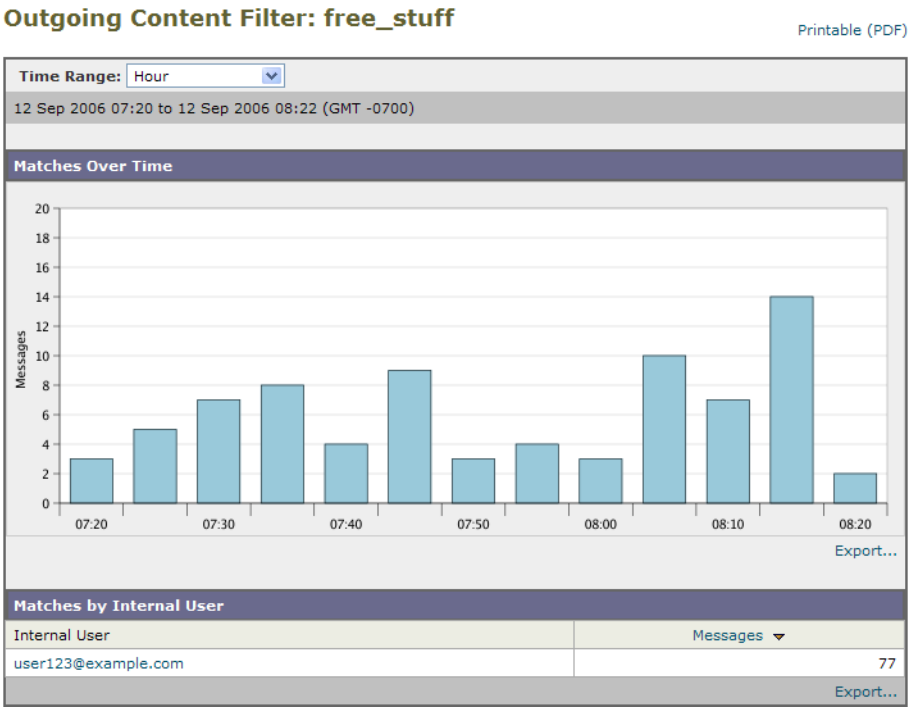
- 受信メールまたは送信メールによってトリガーされた回数の最も多いコンテンツ フィルタ。
- 特定のコンテンツ フィルタをトリガーしたメールを送受信した上位ユーザ。

[Content Filter] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Content Filter] を選択します。

[Content Filter] ページが表示されます。

図 4-16　[Email] > [Reporting] > [Content Filter] ページ



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。[Content Filter Details] ページが表示されます。[Content Filter Details] ページの詳細については、「[Content Filter Details] ページ」（P.4-45）を参照してください。

[Content Filters] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

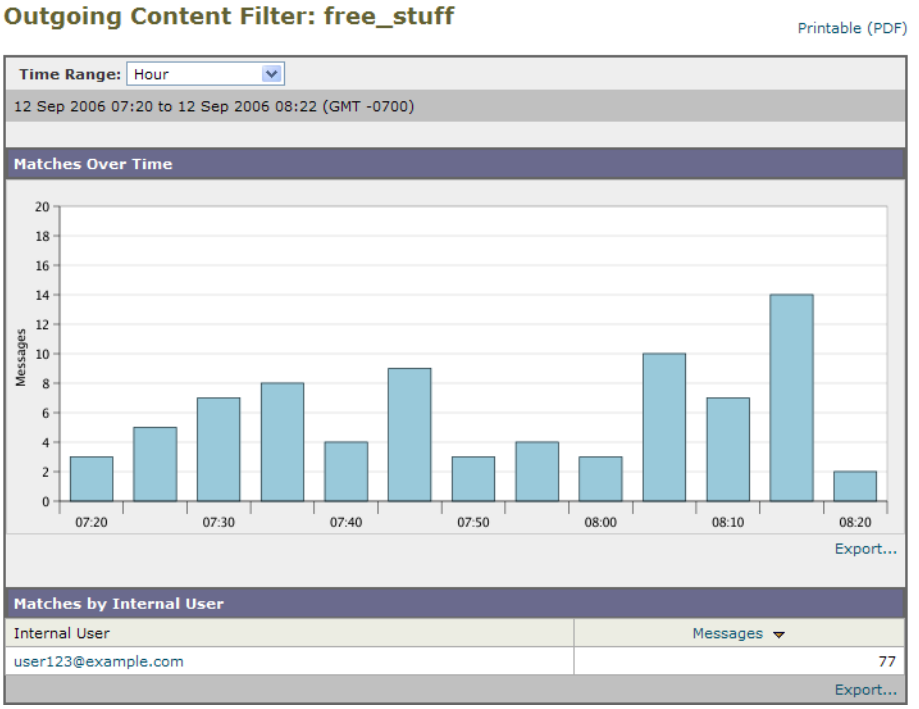
（注）　[Content Filter] ページのスケジュール設定されたレポートを生成できます。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[Content Filter Details] ページ

[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。

[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、「[Internal User Details] ページ」（P.4-39）を参照してください。

図 4-17　[Content Filters Details] ページ



[Virus Types] ページ

[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。[Virus Types] ページには、Email Security アプライアンスで稼動し、Security Management 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検疫するフィルタ アクションを作成することが推奨されます。

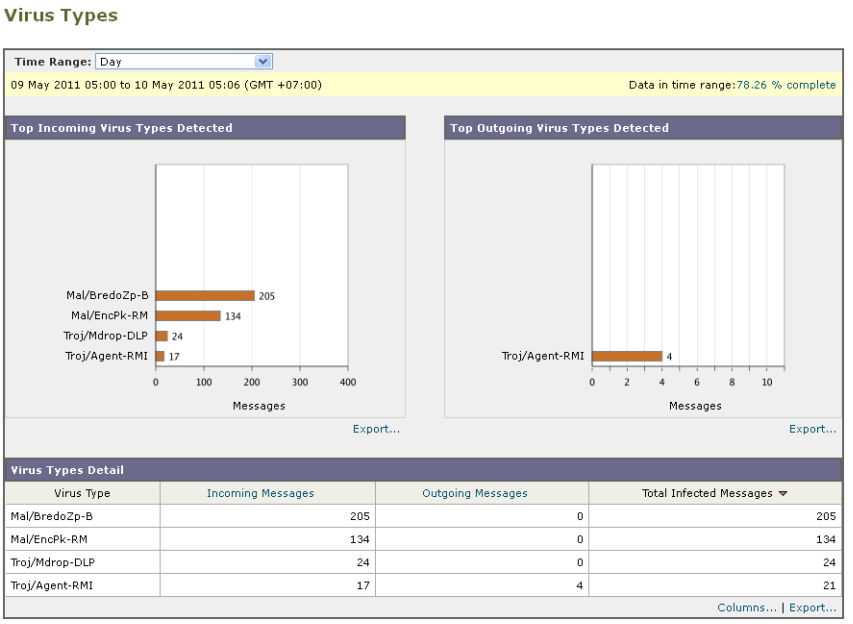
（注）　ウイルス感染フィルタでは、ユーザが介入することなく、これらの種類のウイルスに感染したメッセージを隔離することができます。

[Virus Types] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Virus Types] を選択します。

[Virus Types] ページが表示されます。

図 4-18　[Email] > [Reporting] > [Virus Types] ページ



複数のウイルス スキャン エンジンを実行している場合、[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。

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

表 4-9　[Email] > [Reporting] > [Virus Types] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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。
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。
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、[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、[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。

[Virus Types] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポート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 レポーティング ページの概要」（P.4-12）を参照してください。

（注） [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。「スケジュール設定されたレポート」（P.4-76）を参照してください。

[TLS Connections] ページ

[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 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。

[TLS Connections] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [TLS Connections] を選択します。

[TLS Connections Report] ページが表示されます。

[TLS Connections Report] ページは、2 つのセクションに分かれています。

- 「[TLS Connections Report] ページ：[Incoming Connections]」
- 「[TLS Connections Report] ページ：[Outgoing Connections]」

図 4-19　[TLS Connections Report] ページ：[Incoming Connections]

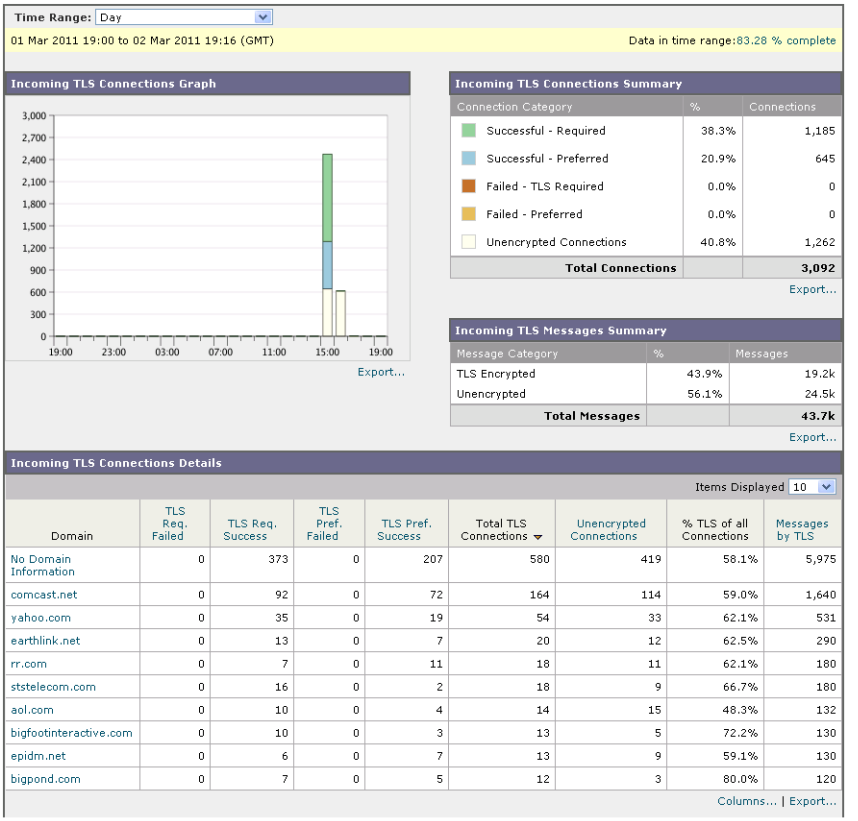
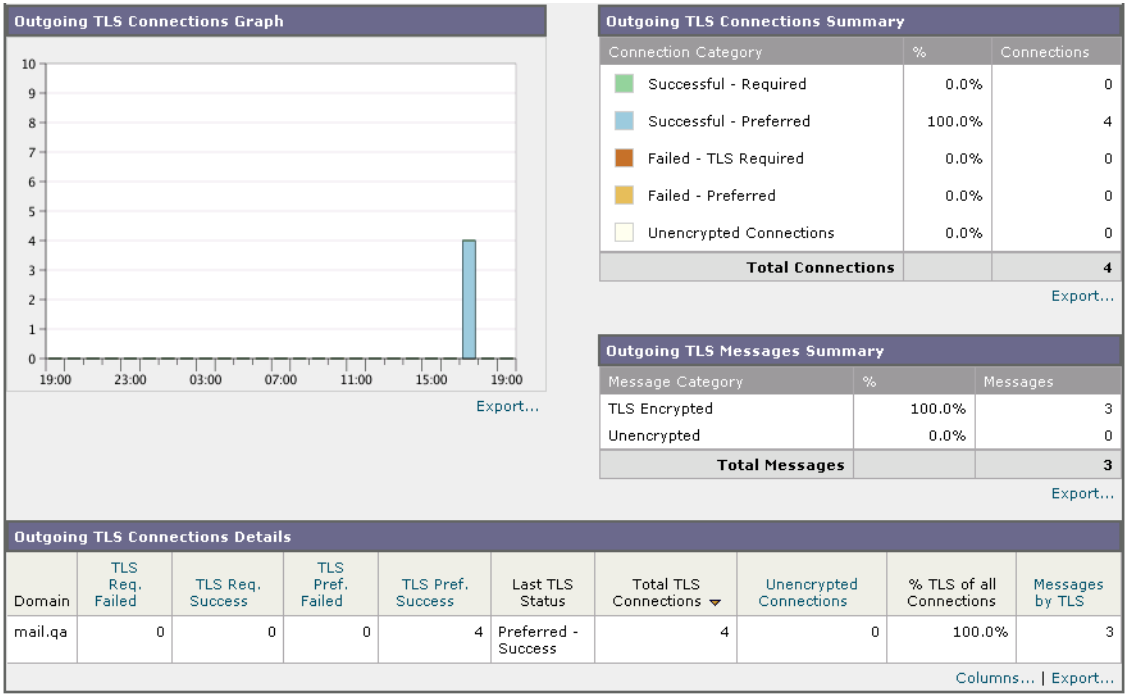


図 4-20　[TLS Connections Report] ページ : [Outgoing Connections]



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

表 4-10　[Email] > [Reporting] > [TLS Connections] ページの詳細

セクション	説明
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、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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。
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。

表 4-10　[Email] > [Reporting] > [TLS Connections] ページの詳細（続き）

セクション	説明
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。
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。
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。
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。
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。

[Outbreak Filters] ページ

[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検疫されたメッセージに関する情報が示されます。このページを使用すると、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。

[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 ルールによって検疫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。

[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。[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。

[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、ウイルス性と非ウイルス性の両方のすべての発生の上位集合です。これに対して、ローカル発生は、お使いの Cisco IronPort アプライアンスに影響を与えたウイルス感染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、Outbreak 検疫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、Outbreak 検疫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。[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 Cisco IronPort 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。

[Quarantined Messages] セクションでは、感染フィルタの検疫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。検疫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、メッセージが検疫エリア内にあるときでも、メッセージの検疫ルール（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。（検疫エリア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。

[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、[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

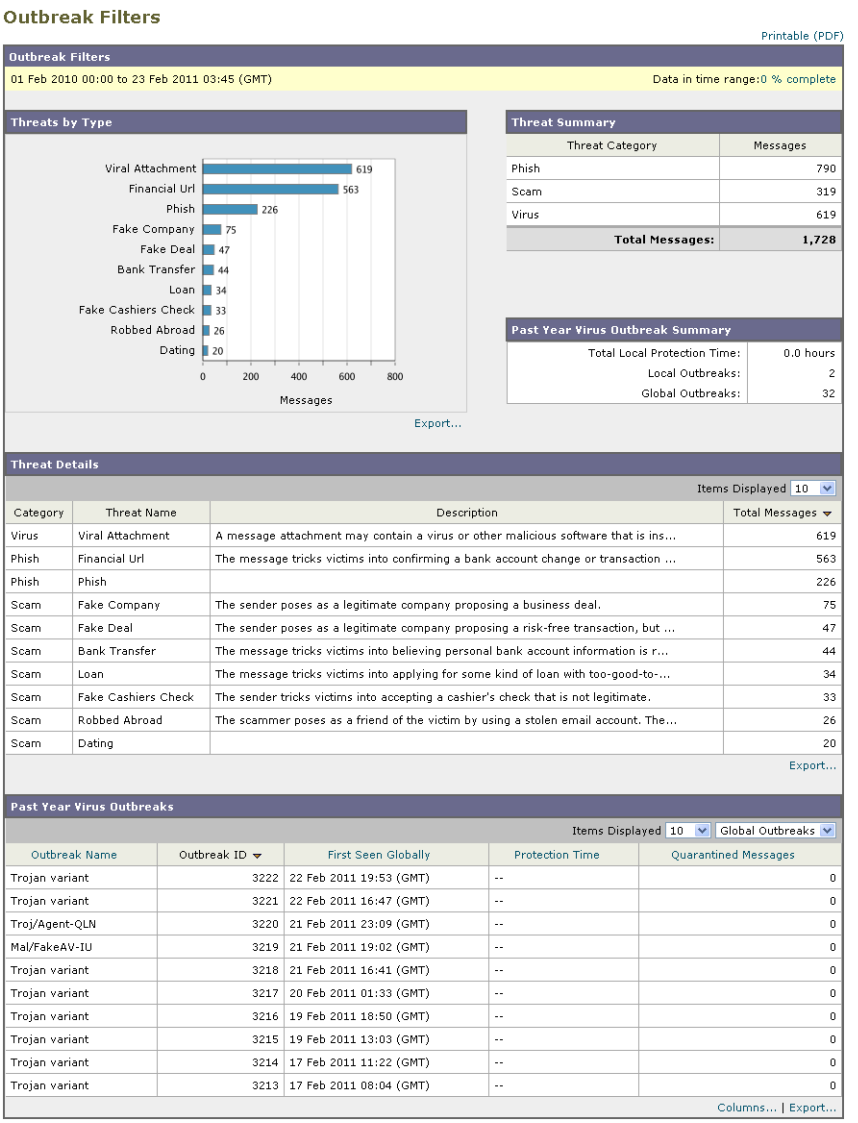
セージ数が含まれます。左側のメニューを使用して、グローバル発生またはローカル発生のいずれか、および表示するメッセージの数を選択できます。カラムヘッダーをクリックすることにより、表示をソートできます。

[First Seen Globally] の時間は、世界最大の電子メールおよび Web モニタリングネットワークである SenderBase のデータに基づいて、Cisco IronPort Threat Operations Center によって決定されます。[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。

[Outbreak Filters] ページを表示するには、[Email] > [Reporting] > [Outbreak Filters] を選択します。図 4-21 に、[Outbreak Filters] ページの表示例を示します。

図 4-21　[Outbreaks] ページ



（注）　[Outbreak Filters] ページにテーブルが正しく表示されるためには、Security Management アプライアンスが downloads.cisco.com と通信できる必要があります。

[System Capacity] ページ

[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。

[System Capacity] ページを使用すると、次の情報を確認できます。

- Email Security 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 Email Security 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**：「通常」のメッセージ量と環境内での「異常」な増加を把握することが重要です。経時的にこのデータを追跡して、量の増加を測定します。[Incoming Mail] ページおよび [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、「[System Capacity] : [Incoming Mail]」（P.4-57）および「[System Capacity] : [Outgoing Mail]」（P.4-60）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。[System Capacity] : [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、「[System Capacity] : [Workqueue]」（P.4-56）を参照してください。

- **リソース節約モード**：Cisco IronPort 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 Cisco IronPort 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、[System Capacity] ページでは追跡できません。

[System Capacity] ページに表示されるデータの解釈方法

[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。

[System Capacity] ページの [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。[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 [Average] 値と [Maximum] 値を表示することができます。

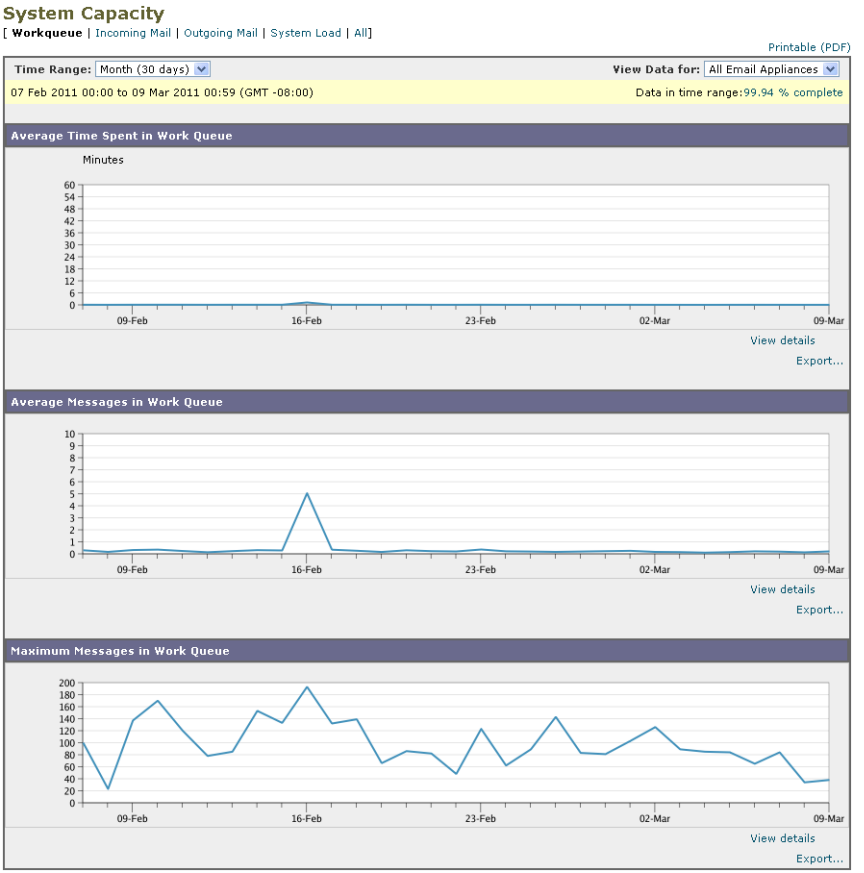
特定のグラフの [View Details] リンクをクリックすると、個々の電子メール セキュリティ アプライアンスのデータおよびセキュリティ管理アプライアンスに接続されたアプライアンスのデータ全体が表示されます。

[System Capacity]：[Workqueue]

[System Capacity]：[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。[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。[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 4-22　[System Capacity] : [Workqueue]



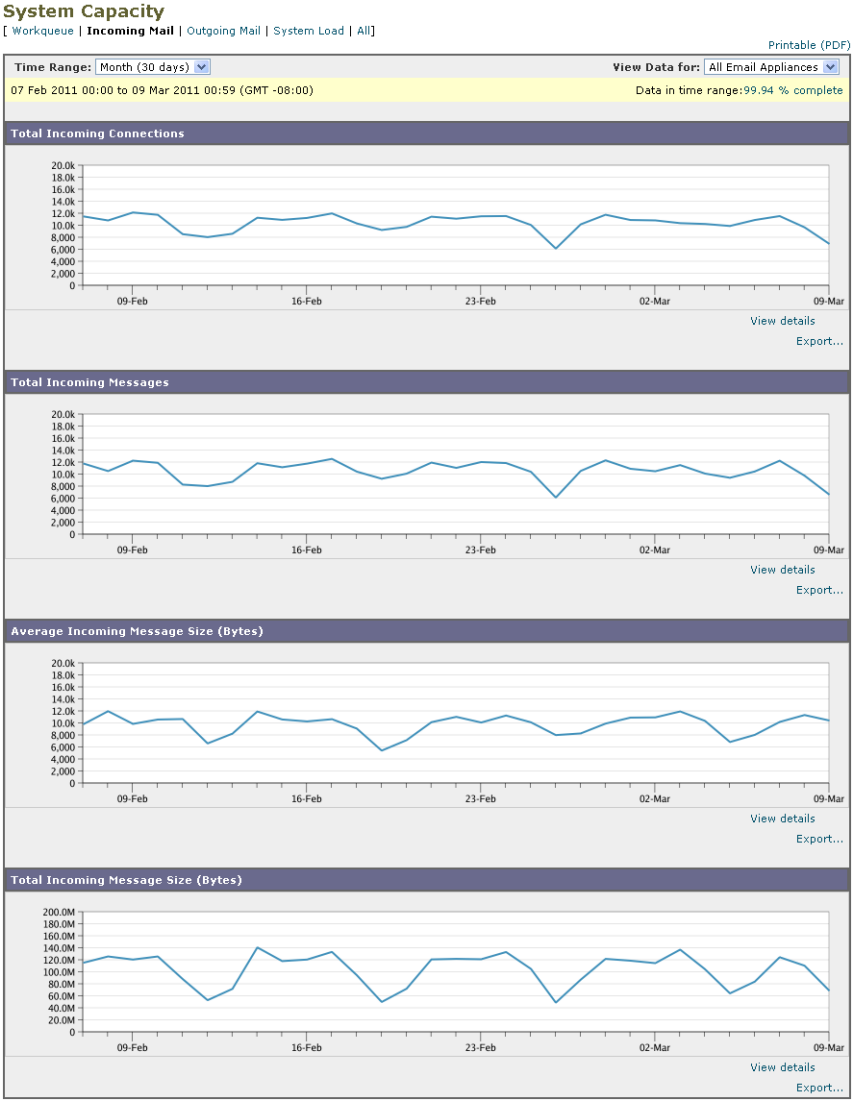
[System Capacity] : [Incoming Mail]

[System Capacity] : [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。[System

Capacity] : [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。

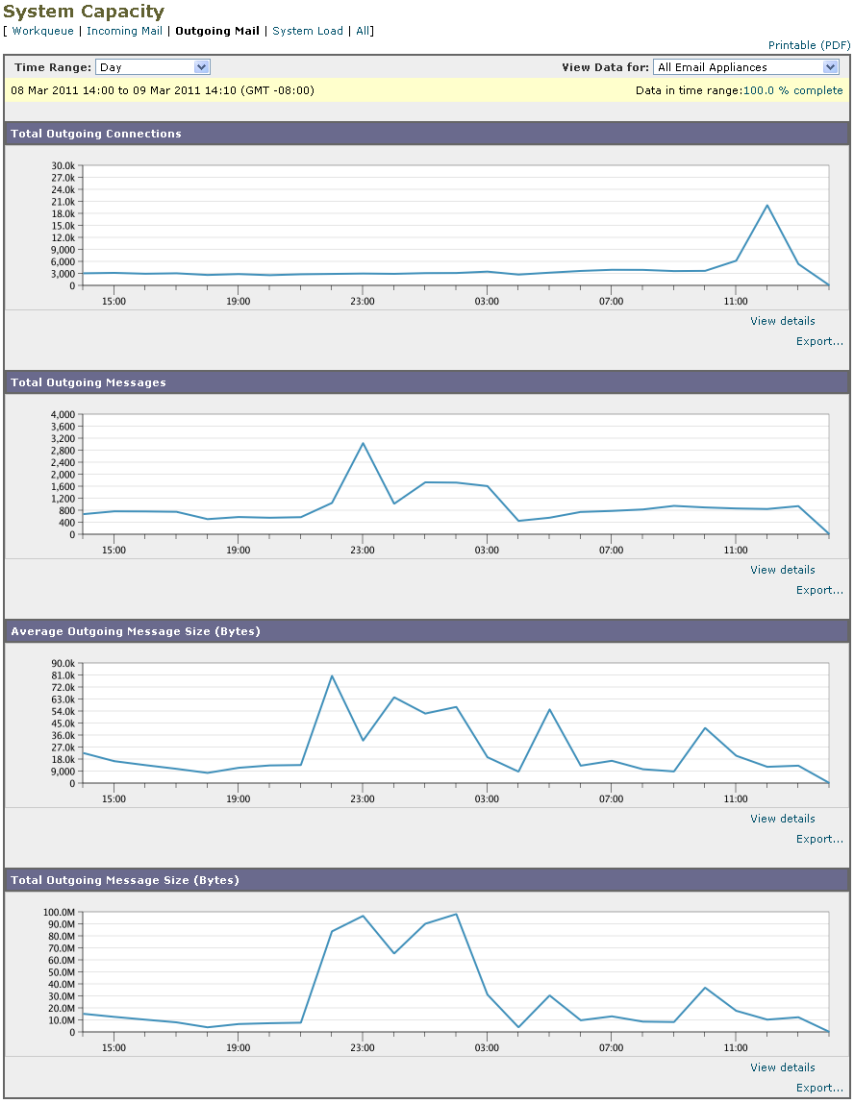
図 4-23　[System Capacity] : [Incoming Mail]



[System Capacity]：[Outgoing Mail]

[System Capacity]：[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。[System Capacity]：[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 4-24　[System Capacity] : [Outgoing Mail]



[System Capacity]：[System Load]

システム負荷レポートには、Email Security 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、および検疫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。

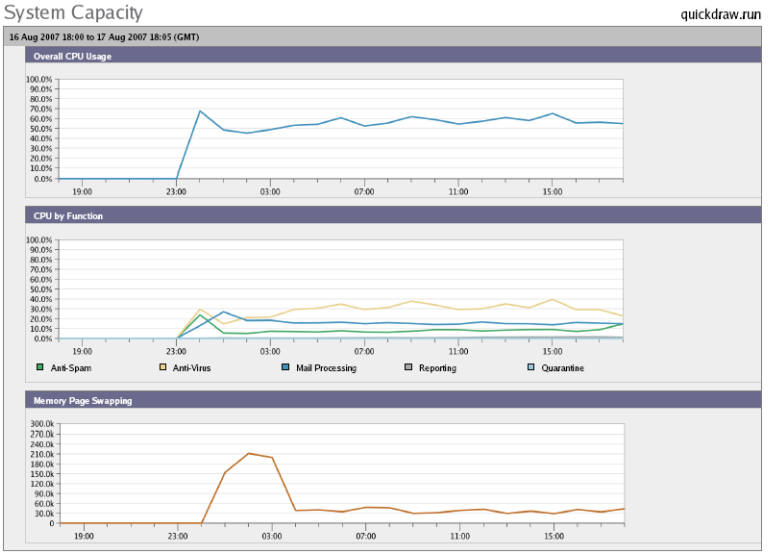
図 4-25　[System Capacity] : [System Load]

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 4-26 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 Cisco IronPort 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 4-26　[System Capacity]：[System Load]（高負荷時のシステム）



[System Capacity]：[All]

[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。

[Data Availability] ページ

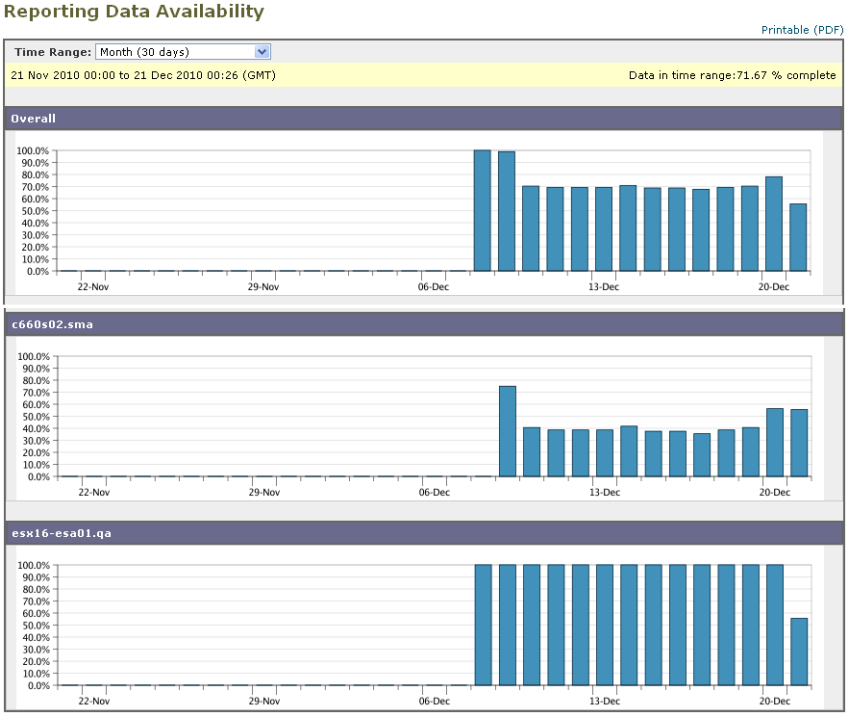
[Email] > [Reporting] > [Data Availability] ページでは、リソース使用率および電子メール トラフィックの障害のある場所がリアルタイムに表示されるようにデータを表示、更新およびソートできます。

[Data Availability] ページを表示するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのページで、[Email] > [Reporting] > [Data Availability] を選択します。

[Reporting Data Availability] ページが表示されます。

図 4-27　[Email Reporting Data Availability] ページ



このページから、Security Management 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レポートとオンデマンド レポートについて

使用可能なレポートの種類

インタラクティブ レポート ページから使用できるレポートに加えて、次の種類のレポートを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。

- [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、「[Content Filters] ページ」（P.4-43）を参照してください。
- [DLP Incident Summary] : このページに表示される情報については、「[DLP Incident Summary] ページ」（P.4-40）を参照してください。
- [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。Email Security アプライアンスの [Delivery Status] の詳細については、『*Cisco IronPort AsyncOS for Email Security Daily Management Guide*』を参照してください。
- [Domain-Based Executive Summary] : このレポートは 電子メール レポーティングの [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、「[Domain-Based Executive Summary] レポート」（P.4-68）を参照してください。
- [Executive Summary] : このレポートは 電子メール レポーティングの [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、「[Domain-Based Executive Summary] レポート」（P.4-68）を参照してください。

- [Incoming Mail Summary]：このページに表示される情報については、「[Incoming Mail] ページ」（P.4-17）を参照してください。
- [Internal Users Summary]：このページに表示される情報については、「[Internal Users] ページ」（P.4-36）を参照してください。
- [Outbreak Filters]：このページに表示される情報については、「[Outbreak Filters] ページ」（P.4-51）を参照してください。
- [Outgoing Destinations]：このページに表示される情報については、「[Outgoing Destinations] ページ」（P.4-31）を参照してください。
- [Outgoing Mail Summary]：このページに表示される情報については、「[Outgoing Senders] ページ」（P.4-33）を参照してください。
- [Outgoing Senders]：このページに表示される情報については、「[Outgoing Senders] ページ」（P.4-33）を参照してください。
- [Sender Groups]：このページに表示される情報については、「[Sender Groups] レポート ページ」（P.4-30）を参照してください。
- [System Capacity]：このページに表示される情報については、「[System Capacity] ページ」（P.4-55）を参照してください。
- [TLS Connections]：このページに表示される情報については、「[TLS Connections] ページ」（P.4-48）を参照してください。
- [Virus Types]：このページに表示される情報については、「[Virus Types] ページ」（P.4-45）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） PDF レポートまたは CSV レポートを、その個々のレポートの特定のロケールでスケジュールすることができます。[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。「レポート データの印刷とエクスポート」（P.3-21）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、「アーカイブ済みのレポート」（P.4-79）を参照してください。

その他のレポート タイプ

Security Management アプライアンスの [Email] > [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。

- [Domain-Based Executive Summary] レポート
- [Executive Summary] レポート

[Domain-Based Executive Summary] レポート

[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 [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。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。その他のスケジュール設定されたレポートとは異なり、[Domain-Based Executive Summary] レポートはアーカイブされません。

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 Cisco IronPort Security Management アプライアンスで 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。Cisco IronPort Email Security アプライアンスで **listenerconfig -> setup** コマンドを使用すると、拒否を遅延できます。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。HAT 遅延拒否の詳細については、『Cisco IronPort AsyncOS for Email Security』関連のマニュアルを参照してください。

（注）　Security Management アプライアンスで [Domain-Based Executive Summary] レポートの [Stopped by Reputation Filtering] の結果を表示するには、Email Security アプライアンスと Security Management 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。

Security Management 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。

サブドメインのレポートを生成するには、Email Security アプライアンスおよび Security Management 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、Email Security アプライアンスの CLI で **reportingconfig -> mailsetup -> tld** を実行し、Security Management アプライアンスの CLI で **reportingconfig -> domain -> tld** を実行します。

[Domain-Based Executive Summary] レポートを作成するには、次の手順を実行します。

ステップ 1　Security Management 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. [Email] > [Reporting] > [Scheduled Reports] を選択します。

b. [Add Scheduled Report] をクリックします。

[Add Scheduled Report] ページが表示されます。

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。

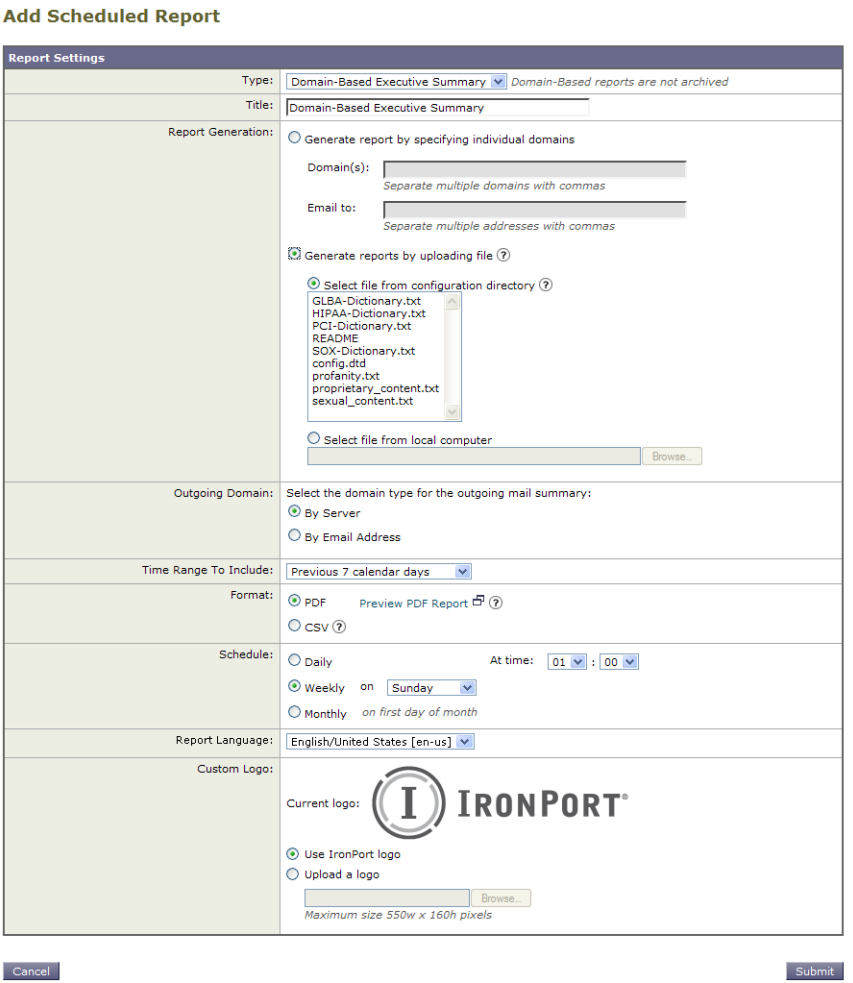
a. [Email] > [Reporting] > [Archived Reports] を選択します。

b. [Generate Report Now] をクリックします。

[Generate Report] ページが表示されます。

ステップ 2　[Report Type] ドロップダウン リストから、[Domain-Based Executive Summary] レポート タイプを選択します。

図 4-28　[Domain-Based Executive Summary] レポートの追加



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。

- [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。
- [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、「[Domain-Based Executive Summary] レポートのコンフィギュレーション ファイル」（P.4-72）を参照してください。

（注） 外部アカウント（Yahoo! Mail や Gmail）にレポートを送信する場合、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して、レポートの電子メールが誤ってスパムに分類されないようにすることが推奨されます。

ステップ 4　[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　[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 [By Server] または [By Email Address] です。

ステップ 6　[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　[Format] セクションで、レポートの形式を選択します。

選択肢は次のとおりです。

- [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。[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]。カンマ区切りの表データを含む ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

ステップ 8　[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 [Daily]、[Weekly]（曜日のドロップダウン リストがあります）または [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 IronPort 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、「レポート データの印刷とエクスポート」（P.3-21）の重要な情報を参照してください。

ステップ 11　[Submit] をクリックしてページでの変更を送信し、[Commit Changes] をクリックして変更を確定します。

[Domain-Based Executive Summary] レポートのコンフィギュレーション ファイル

コンフィギュレーション ファイルを使用して、[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 [Domain-Based Executive Summary] レポートを作成します。アプライアンスで [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。

[Executive Summary] レポート

[Executive Summary] レポートは、Email Security 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。Security Management 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 [Overview] ページで表示できる情報の概要が表示されます。[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 [Overview] ページ」（P.4-12）を参照してください。

オンデマンドでのレポートの生成

「電子メール レポーティング ページの概要」（P.4-12）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レポートとオンデマンド レポートについて」（P.4-66）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 CSV ファイルをいつでも生成できます。

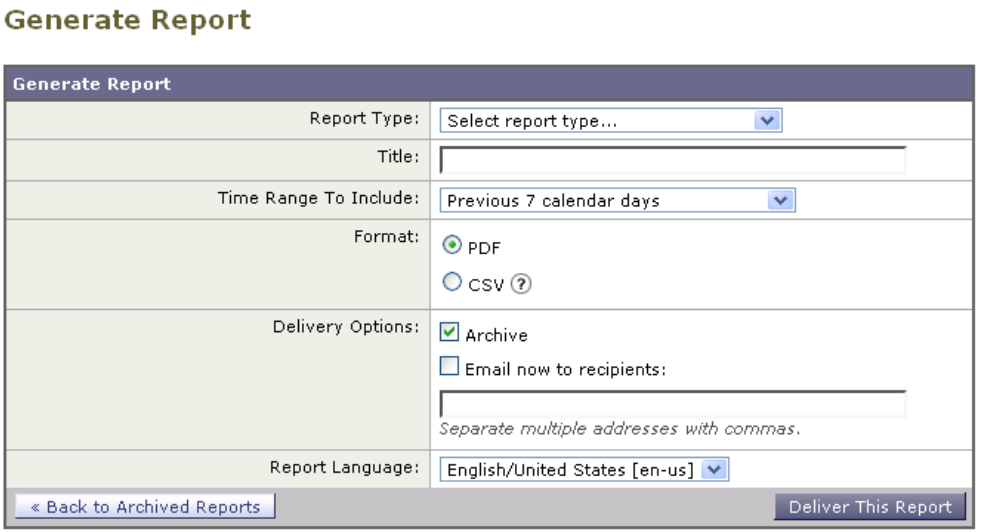
オンデマンド レポートを生成するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスで、[Email] > [Reporting] > [Archived Reports] を選択します。

ステップ 2　[Generate Report Now] をクリックします。

[Generate Report] ページが表示されます。

図 4-29　[Generate Report] ページ



ステップ 3　[Report type] セクションで、ドロップダウン リストからレポート タイプを選択します。

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レポートとオンデマンド レポートについて」（P.4-66）を参照してください。

ステップ 4　[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）　[Domain-Based Executive Summary] レポートの設定の詳細については、「[Domain-Based Executive Summary] レポート」（P.4-68）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　[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。（ウイルス発生レポートでは、このオプションを使用できません）。

これはカスタム時間範囲オプションです。

ステップ 6　[Format] セクションで、レポートの形式を選択します。

選択肢は次のとおりです。

- [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。[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]。カンマ区切りの表データを含む ASCII テキスト ファイルを作成します。各 CSV ファイルには、最大 100 行を含めることができます。レポートに複数の種類の表が含まれる場合、各表に対して別個の CSV ファイルが作成されます。

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

- [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 [Archived Reports] ページに表示されます。

（注）　[Domain-Based Executive Summary] レポートはアーカイブできません。

- [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、「レポート データの印刷とエクスポート」（P.3-21）の重要な情報を参照してください。

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

スケジュール設定されたレポート

「スケジュール設定されたレポートとオンデマンド レポートについて」（P.4-66）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.4-76）
- 「スケジュール設定されたレポートの編集」（P.4-78）
- 「スケジュール設定されたレポートの中止」（P.4-79）

スケジュール設定されたレポートの追加

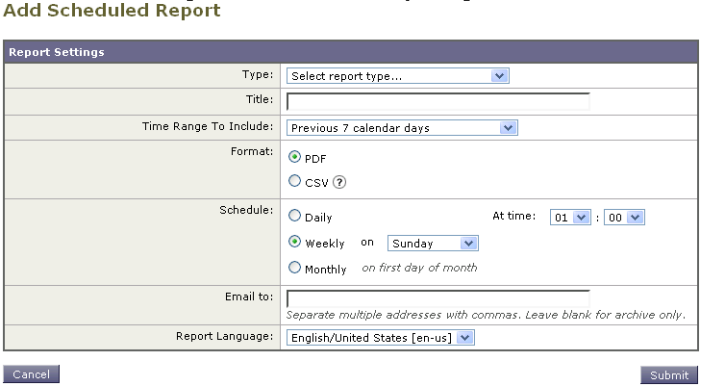
スケジュール設定された電子メール レポートを追加するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Reporting] > [Scheduled Reports] を選択します。

ステップ 2　[Add Scheduled Report] をクリックします。

[Add Scheduled Report] ページが表示されます。

図 4-30　[Add Scheduled Reports] ページ



ステップ 3　[Type] の横のドロップダウン メニューから、レポート タイプを選択します。

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レポートとオンデマンド レポートについて」（P.4-66）を参照してください。

（注）　[Domain-Based Executive Summary] レポートの設定の詳細については、「[Domain-Based Executive Summary] レポート」（P.4-68）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　[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　[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。（ウイルス発生レポートでは、このオプションを使用できません）。

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。大部分のレポートでは、CSV のスケジューリングを行うことができます。

ステップ 7　レポートに応じて、[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　[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　[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、「レポート データの印刷とエクスポート」（P.3-21）の重要な情報を参照してください。

ステップ 12　[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

スケジュール設定されたレポートを編集するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Reporting] > [Scheduled Reports] を選択します。

ステップ 2　[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。

[Edit Scheduled Report] ページが表示されます。

ステップ 3　[Edit Scheduled Report] ページから、レポート設定を変更します。

ステップ 4　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] ボタンをクリックしてアプライアンスへの変更を確定します。

スケジュール設定されたレポートの中止

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　Security Management アプライアンスのウィンドウで、[Email] > [Reporting] > [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、[All] チェックボックスを選択します。

ステップ 3　[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.4-81）を参照してください。

アーカイブ済みのレポート

（注）　[Generate Report Now] をクリックしてレポートをすぐに生成する方法の詳細については、「オンデマンドでのレポートの生成」（P.4-74）を参照してください。

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。

Security Management 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「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

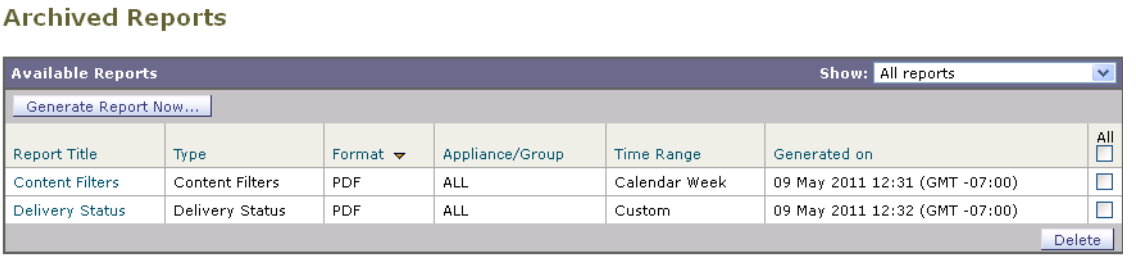
[Email] > [Reporting] > [Archived Reports] ページには、生成されたがまだ消去されておらず、アーカイブすることを指定した、スケジュール設定されたレポートとオンデマンド レポートが表示されます。

アーカイブ済みのレポートにアクセスするには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Reporting] > [Archived Reports] を選択します。

[Archived Reports] ページが表示されます。

図 4-31　　アーカイブ済みのレポート



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、[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　[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

「アーカイブ済みのレポート」（P.4-79）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　Security Management アプライアンスで、[Email] > [Reporting] > [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　[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.4-79）を参照してください。