CHAPTER 3

レポートでの作業

レポーティングに関する次のトピックは、電子メール レポートと Web レポートの両方に共通します。

レポーティング データを表示する方法

表 3-1　レポーティング データを表示する方法

目的	参照先
インタラクティブ レポート ページを表示およびカスタマイズする	• 「インタラクティブ レポート ページのビューのカスタマイズ」（P.3-3） • 第 4 章「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」 • 第 5 章「中央集中型 Web レポーティングの使用方法」
反復するレポートを自動的に生成する	• 「電子メール レポートのスケジュール設定」（P.4-55） • 「Web レポートのスケジュール設定」（P.5-63）
レポートをオンデマンドで生成する	• 「オンデマンドでの電子メール レポートの生成」（P.4-56） • 「オンデマンドでの Web レポートの生成」（P.5-67）

表 3-1　レポーティング データを表示する方法（続き）

目的	参照先
raw データを CSV（カンマ区切り）ファイルとしてエクスポートする	• 「レポート データの印刷とエクスポート」（P.3-7） • 「カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート」（P.3-8）
レポート データの PDF を生成する	「レポート データの印刷とエクスポート」（P.3-7）
レポート情報を自分自身や他のユーザに電子メールで送信する	• 「オンデマンドでの電子メール レポートの生成」（P.4-56） • 「電子メール レポートのスケジュール設定」（P.4-55） • 「オンデマンドでの Web レポートの生成」（P.5-67） • 「Web レポートのスケジュール設定」（P.5-63）
スケジュールされたレポートまたはオンデマンド レポートのアーカイブ済みのコピーを、システムから削除されるまで表示する	「アーカイブされた Web レポートの表示と管理」（P.5-69）
特定のトランザクションに関する情報を検索する	「[Web Tracking] ページ」（P.5-51）

（注）　ロギングとレポーティングの違いについては、「ロギングとレポーティング」（P.14-1）を参照してください。

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

セキュリティ管理アプライアンスは、約 15 分ごとにすべての管理対象アプライアンスからすべてのレポートのデータをプルし、それらのアプライアンスのデータを集約します。使用するアプライアンスによっては、セキュリティ管理アプライアンスでレポーティング データに特定のメッセージを組み込むのに時間が掛かる場合があります。データの情報については、[System Status] ページを確認してください。

（注）　セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。セキュリティ管理アプライアンス上の時間設定の詳細については、「システム時刻の設定」（P.13-47）を参照してください。

レポーティング データの保存方法

すべてのアプライアンスで、レポーティング データが保存されます。表 3-2 に、各アプライアンスがデータを保存する期間を示します。

表 3-2　電子メール アプライアンスと Web セキュリティ アプライアンスでのレポーティング データの保存

	毎分	毎時	毎日	毎週	毎月	毎年
電子メール セキュリティ アプライアンスまたは Web セキュリティ アプライアンス でのローカル レポーティング	•	•	•	•	•	
電子メール セキュリティ アプライアンスまたは Web セキュリティ アプライアンスでの中央集中型レポーティング	•	•	•	•		
セキュリティ管理アプライアンス		•	•	•	•	•

インタラクティブ レポート ページのビューのカスタマイズ

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。

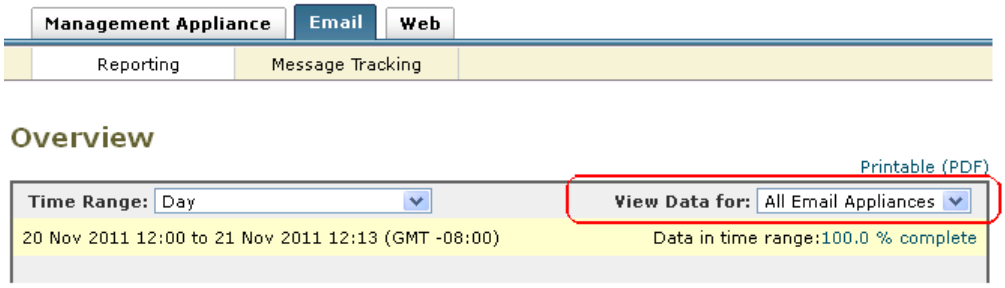
- **アプライアンスごとに、特定のレポートのみのデータを表示する**。詳細については、「アプライアンスによるレポーティング データの制約」（P.3-3）を参照してください。
- **時間範囲を指定する**。詳細については、「インタラクティブ レポートの時間範囲の選択」（P.3-4）を参照してください。
- **（Web レポートの場合）チャート化するデータを選択する**。「（Web レポートのみ）チャート化するデータの選択」（P.3-5）を参照してください。
- **テーブルをカスタマイズする**。「レポート ページのテーブルのカスタマイズ」（P.3-5）を参照してください。
- **表示する特定の情報またはデータのサブセットを検索する**。電子メール レポートについては、「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。Web レポートについては、ほとんどのテーブルの下方にある [Find] オプションまたは [Filter] オプションを探してください。

（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。

アプライアンスによるレポーティング データの制約

電子メールおよび Web の概要レポートについて、および電子メールのシステム キャパシティ レポートについては、すべてのアプライアンスから、または中央で管理されている 1 台のアプライアンスからデータを表示できます。

ビューを指定するには、サポートされるページの [View Data for] リストからアプライアンスを選択します。



最近、別のセキュリティ管理アプライアンスからのデータをバックアップしたセキュリティ管理アプライアンスでレポート データを表示する場合は、まず、[Management Appliance] > [Centralized Services] > [Security Appliances] で各アプライアンスを追加する必要があります（ただし、各アプライアンスとの接続は確立しないでください）。

インタラクティブ レポートの時間範囲の選択

ほとんどのインタラクティブ レポート ページでは、含まれるデータの時間範囲を選択できます。選択した時間範囲は、[Time Range] メニューで異なる値を選択するまで、すべてのレポート ページを通して使用されます。

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

表 3-3　レポートの時間範囲オプション

オプション	説明	SMA 電子メール レポート	ESA	SMA Web レポート	WSA
Hour	過去 60 分間と最大 5 分間の延長時間		•		•
Day	過去 24 時間	•	•	•	•
Week	当日の経過時間を含む、過去 7 日間	•	•	•	•
30 days	当日の経過時間を含む、過去 30 日間	•	•	•	•
90 days	当日の経過時間を含む、過去 90 日間	•	•	•	
Year	過去 12 ヵ月と現在月の経過日数	•			
Yesterday	アプライアンスで定義された時間帯を使用した、前日の 24 時間（00:00 ～ 23:59）	•	•	•	•
Previous Calendar Month	月の第 1 日目の 00:00 からその月の最終日の 23:59 まで	•	•	•	
Custom Range	ユーザ指定の時間範囲。 開始日時と終了日時を選択する場合は、このオプションを選択します。	•	•	•	•

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

ヒント　ログインするたびに常に表示する、デフォルトの時間範囲を指定できます。詳細については、「プリファレンスの 設定」（P.13-60）を参照してください。

（Web レポートのみ）チャート化するデータの選択

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

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できないカラムもあります。カラムの見出しについては、「Web レポーティング ページのテーブル カラムの説明」（P.5-10）を参照してください。

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

ステップ 1　チャートの下の [Chart Options] をクリックします。

ステップ 2　表示するデータを選択します。

ステップ 3　[Done] をクリックします。

レポート ページのテーブルのカスタマイズ

表 3-4　Web レポート ページのテーブルのカスタマイズ

目的	操作内容	追加情報
• 追加のカラムを表示する • 表示可能なカラムを非表示にする • テーブルに使用可能なカラムを判断する	テーブルの下の [Columns] リンクをクリックし、表示するカラムを選択して、[Done] をクリックします。	ほとんどのテーブルでは、デフォルトで一部のカラムが非表示になります。 レポート ページごとに、異なるカラムが提供されます。 カラムの詳細については、次の項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」（P.4-9） • 「Web レポーティング ページのテーブル カラムの説明」（P.5-10）
テーブル カラムの順序を変える	カラムの見出しを目的の位置までドラッグします。	—

表 3-4　Web レポート ページのテーブルのカスタマイズ（続き）

目的	操作内容	追加情報
選択した見出しでテーブルをソートする	カラムの見出しをクリックします。	—
表示するデータの行数を加減する	テーブルの右上にある [Items Displayed] ドロップダウン リストから、表示する行数を選択します。	Web レポートの場合、デフォルトの表示行数を設定することもできます。「プリファレンスの 設定」（P.13-60）を参照してください。
可能な場合は、テーブル エントリの詳細を表示する	テーブル内の青色のエントリをクリックします。	—
データのプールを特定のサブセットに絞り込む	可能な場合は、テーブルの下のフィルタ設定で値を選択するか、入力します。	Web レポートの使用可能なフィルタについては、各レポート ページの説明に記載されています。「Web レポーティング ページについて」（P.5-7）を参照してください。

電子メール レポートのパフォーマンスの向上

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

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

- [IP Connection Level Detail]。このフィルタをイネーブルにすると、セキュリティ管理アプライアンスは、個々の IP アドレスに関する情報を記録しません。このフィルタは、攻撃による大量の受信 IP アドレスを処理するシステムに適しています。

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

  - Sender Profile for Incoming Mail
  - IP Addresses for Incoming Mail
  - IP Addresses for Outgoing Senders

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

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

  - Internal Users
  - Internal User Details
  - IP Addresses for Outgoing Senders
  - Content Filters

- [Mail Traffic Detail]。このフィルタをイネーブルにすると、セキュリティ管理アプライアンスは、アプライアンスがモニタする個々のドメインおよびネットワークに関する情報を記録しません。このフィルタは、有効な着信または発信ドメインの数が数千万の単位で測定される場合に適しています。

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

  - Domains for Incoming Mail
  - Sender Profile for Incoming Mail
  - Internal User Details
  - Domains for Outgoing Senders

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

レポート データの印刷とエクスポート

表 3-5　レポート データの印刷とエクスポート

取得対象	PDF	CSV	操作内容	コメント
インタラクティブ レポート ページの PDF	•		インタラクティブ レポート ページの右上にある [Printable (PDF)] リンクをクリックします。	PDF には、現在表示しているカスタマイゼーションが反映されます。 PDF は、プリンタ対応の形式に設定されます。
レポート データの PDF	•		スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。次の各項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」（P.4-56） • 「電子メール レポートのスケジュール設定」（P.4-55） • 「オンデマンドでの Web レポートの生成」（P.5-67） • 「Web レポートのスケジュール設定」（P.5-63）	—

表 3-5　レポート データの印刷とエクスポート（続き）

取得対象	PDF	CSV	操作内容	コメント
raw データ		•	チャートまたはテーブルの下にある [Export] リンクをクリックします。	CSV ファイルには、チャートまたはテーブルに表示できるデータだけではなく、適用可能な最大限のデータがすべて含まれます。
「カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート」（P.3-8）も参照してください。		•	スケジュール設定されたレポートまたはオンデマンドのレポートを作成します。次の各項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」（P.4-56） • 「電子メール レポートのスケジュール設定」（P.4-55） • 「オンデマンドでの Web レポートの生成」（P.5-67） • 「Web レポートのスケジュール設定」（P.5-63）	各 CSV ファイルには、最大 100 行を含めることができます。 レポートに複数のテーブルが含まれる場合、各テーブルに対して別個の CSV ファイルが作成されます。 一部の拡張レポートは、CSV 形式で使用できません。
さまざまな言語によるレポート	•		レポートをスケジュール設定するか、オンデマンドで作成するときは、必要なレポート言語を選択します。	Windows コンピュータ上で中国語、日本語、または韓国語で PDF を生成するには、該当するフォント パックを Adobe.com からダウンロードして、ローカル コンピュータにインストールする必要があります。
（Web セキュリティ）レポート データのカスタム サブセット（特定のユーザ用のデータなど）。	•	•	[Web Tracking] で検索を実行し、[Web Tracking] ページの [Printable Download] リンクをクリックします。PDF 形式または CSV 形式を選択します。	PDF には、最大 1,000 件のトランザクションが含まれます。 CSV ファイルには、検索条件に一致するすべての raw データが含まれます。
（電子メール セキュリティ）データのカスタム サブセット（特定のユーザ用のデータなど）。		•	[Message Tracking] で検索を実行し、結果の上にある [Export] リンクをクリックします。	メッセージ トラッキング検索結果および CSV ファイルには最大 250 件の結果が含まれます。

カンマ区切り（CSV）ファイルとしてのレポート データのエクスポート

raw データをカンマ区切り（CSV）ファイルにエクスポートし、Microsoft Excel などのデータベース アプリケーションを使用してアクセスおよび処理できます。データをエクスポートするその他の方法については、「レポート データの印刷とエクスポート」（P.3-7）を参照してください。

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

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

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

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

表 3-6　raw データ エントリの表示

カテゴリ ヘッダー	値	説明
Begin Timestamp	1159772400.0	エポックからの秒数で表されたクエリー開始時刻。
End Timestamp	1159858799.0	エポックからの秒数で表されたクエリー終了時刻。
Begin Date	2006-10-02 07:00 GMT	クエリーの開始日。
End Date	2006-10-03 06:59 GMT	クエリーの終了日。
Name	アドウェア	マルウェア カテゴリの名前。
Transactions Monitored	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。
Transactions Detected	2625	トランザクションの合計数： 検出されたトランザクション数 + ブロックされたトランザクション数。

（注） カテゴリ ヘッダーは、レポートのタイプごとに異なります。

ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策としては、ローカル マシンにファイルを保存し、[File] > [Open] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

レポーティングおよびトラッキングにおけるサブドメインとセカンドレベル ドメインの比較

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

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

電子メール レポートおよび Web レポート

電子メール レポートに固有の情報については、第 4 章「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」を参照してください。

Web レポートに固有の情報については、第 5 章「中央集中型 Web レポーティングの使用方法」を参照してください。