レポートの使用

この章は、次の項で構成されています。

- レポート データの表示方法 （1 ページ）
- セキュリティ管理アプライアンスによるレポート用データの収集方法 （2 ページ）
- レポート データのビューのカスタマイズ （3 ページ）
- レポートに含まれるメッセージやトランザクションの詳細の表示 （9 ページ）
- 電子メール レポートのパフォーマンスの向上 （9 ページ）
- レポーティング データおよびトラッキング データのエクスポート （11 ページ）
- レポート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 （14 ページ）
- すべてのレポートのトラブルシューティング （14 ページ）
- 電子メール レポートおよび Web レポート （15 ページ）

レポート データの表示方法

表 *1:* レポート データの表示方法

目的	参照先
Webベースのインタラクティブ レポート ページを表示およびカスタマイズする	• レポート データのビューのカスタマイズ （3 ページ） • 中央集中型の電子メール セキュリティ レポーティングの使用 • 集約されたポリシー、ウイルス、およびアウトブレイク隔離
PDF レポートまたは CSV レポートを自動的に繰り返し生成する	• メール レポートのスケジュール設定 • Web レポートのスケジュール設定

目的	参照先
PDF レポートまたは CSV レポートをオンデマンドで生成する	• オンデマンドでのメール レポートの生成 • オンデマンドでの Web レポートの生成
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	• レポーティング データおよびトラッキング データのエクスポート （11 ページ） • 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 （13 ページ）
レポート データの PDF を生成する	レポーティング データおよびトラッキング データのエクスポート （11 ページ）
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	• オンデマンドでのメール レポートの生成 • メール レポートのスケジュール設定 • オンデマンドでの Web レポートの生成 • Web レポートのスケジュール設定
特定のトランザクションに関する情報を検索する	レポートに含まれるメッセージやトランザクションの詳細の表示 （9 ページ）

（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を参照してください。

セキュリティ管理アプライアンスによるレポート用データの収集方法

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取得し、これらのアプライアンスからのデータを集約します。アプライアンスによっては、個々のメッセージにセキュリティ管理アプライアンス上のレポーティング データを含める際に多少時間がかかる場合があります。データの詳細については、[システムステータス（System Status）] ページを確認してください。

レポーティング データには、IPv4 と IPv6 の両方に関係するトランザクションが含まれます。

（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を参照してください。

レポート データの保存方法

すべてのアプライアンスでレポートのデータを格納します。次の表に、各アプライアンスがデータを格納する周期を示します。

表 *2 : E* メール セキュリティ 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ト データの保存

	毎分	毎時	[毎日 (Daily)]	週1回	[月 1 回 (Monthly)]	年次
E 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 レポート**	•	•	•	•	•	
E 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		•	•	•	•	•

レポーティングおよびアップグレードについて

新しいレポーティング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。レポーティング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

レポート データのビューのカスタマイズ

Web インターフェイスでレポート データを表示する場合、ビューをカスタマイズできます。

目的	操作手順
アプライアンスまたはレポート グループごとにデータを表示する	アプライアンスまたはレポーティング グループのレポート データの表示 （4 ページ）
時間範囲を指定する	レポートの時間範囲の選択 （5 ページ）
（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 （5 ページ）

目的	操作手順
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 （6 ページ）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 ページです。 • 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 [検索（Find）] オプションまたは [フィルタ（Filter）] オプションを探してください。 • 一部のテーブルには、集約したデータの詳細へのリンク（青色のテキスト）が含まれます。
レポート関連の設定を指定する	プリファレンスの設定を参照してください
使用したいチャートと表だけを使ったカスタム レポートを作成する	カスタム レポート （6 ページ）を参照してください。

（注） すべてのレポートにすべてのカスタマイズ機能を使用できるわけではありません。

アプライアンスまたはレポーティング グループのレポート データの表示

電子メールに関するメール フロー サマリーとシステム キャパシティの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。

電子メール レポートでは、電子メール レポーティング グループの作成 の説明に従い E メール セキュリティ アプライアンスのグループを作成した場合、各レポーティング グループの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 [次のデータを参照（View Data For）] リストからアプライアンスまたはグループを選択します。

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 データを表示している場合は、最初に、⚙ > [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）] 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）。

レポートの時間範囲の選択

ほとんどの事前定義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、[時間範囲（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 ページに対して使用されます。

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 レポーティングおよび Web レポーティングによって異なります。

（注） 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。

（注） すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時（GMT）オフセットで日付および時刻情報が表示されます。ただし、データ エクスポートでは、世界の複数のタイム ゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。

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列もあります。

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、テーブルの列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 [チャートオプション（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 [完了（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

レポート ページ内のインタラクティブ テーブルの情報を表示、カスタマイズ、ソートできます。選択したビューは、レポート ページにデータを表示するために使用されます。

表 *3:* レポート ページのテーブルのカスタマイズ

目的	操作手順	詳細情報
• 追加の列を表示する • 表示可能な列を非表示にする • テーブルに使用可能な列を判断する	1. をクリックします。 2. 表示する列を選択し、[閉じる（Close）]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列が非表示になります。 レポート ページごとに、異なる列が提供されます。 それぞれのテーブルのテーブル列の説明を参照してください。
選択した見出しでテーブルをソートする	列の見出しをクリックします。	-
テーブルの列の順序を変える	列の見出しを目的の位置までドラッグします。	-
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。	レポートに含まれるメッセージやトランザクションの詳細の表示 （9 ページ）も参照してください。
追加する行の詳細を表示します。	追加する行の詳細を表示するには、テーブルを下方向にスクロールします。	-
特定のサブセットにデータをフィルタリングする	可能な場合は、特定のテーブルの下にあるフィルタ設定で値を入力します。	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。新しい Web インターフェイスの Web レポート ページの概要を参照してください。

カスタム レポート

既存のレポート ページのチャート（グラフ）とテーブルを組み合わせて、カスタムの電子メール セキュリティ レポート ページを作成できます。

（注） Email Security Appliances のリリース 9.6 以降では、[マイレポート（My Reports）] は [マイダッシュボード（My Dashboard）] と呼ばれます。

目的	操作手順
カスタム レポート ページにモジュールを追加	参照先： • カスタム レポートに追加できないモジュール （7 ページ） • カスタム レポート ページの作成 （8 ページ）
カスタム レポート ページの表示	1. [メール（Email）] > [レポート（Reporting）] > [マイレポート（My Reports）] を選択します。 2. 表示する時間範囲を選択します。選択した時間範囲は [マイレポート（My Reports）] ページのすべてのモジュールを含むすべてのレポートに適用されます。 新しく追加されたモジュールはカスタム レポートの上部に表示されます。
カスタム レポート ページでのモジュールの再配置	目的の場所にモジュールをドラッグアンドドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。
カスタム レポートの CSV バージョンの生成	参照先： • オンデマンドでのメール レポートの生成 • オンデマンドでの Web レポートの生成
カスタム レポートの CSV バージョンの定期的な生成	参照先： • メール レポートのスケジュール設定 • Web レポートのスケジュール設定

カスタム レポートに追加できないモジュール

- **[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システムステータス（System Status）]** ページのすべてのモジュール
- **[メール（Email）] > [レポート（Reporting）] > [有効なレポートデータ（Reporting Data Availability）]** ページのすべてのモジュール

- **[メール（Email）] > [メッセージ トラッキング（Message Tracking）] > [有効なメッセージ トラッキング データ（Message Tracking Data Availability）]** ページのすべてのモジュール
- 送信者プロファイル詳細レポートのページからの、[SenderBase からの最新情報（Current Information from SenderBase）]、[送信者グループ情報（Sender Group Information）]、および [ネットワーク情報（Network Information）] といったドメイン単位のモジュール
- アウトブレイク フィルタ レポート ページの [過去 1 年間のウイルス アウトブレイク サマリー（Past Year Virus Outbreak Summary）] チャートおよび [過去 1 年間のウイルス アウトブレイク（Past Year Virus Outbreaks）] テーブル

カスタム レポート ページの作成

始める前に

- 追加するモジュールが追加可能であることを確認します。カスタム レポートに追加できないモジュール （7 ページ）を参照してください。
- モジュールの右上の [X] をクリックして、不要なデフォルト モジュールを削除します。

ステップ 1 以下のいずれかの方法でカスタム レポート ページにモジュールを追加します。

（注） 一部のモジュールは、以下のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- 追加するモジュールがある [メール（Email）] タブまたはのレポート ページに移動し、モジュールの上部にある [+] ボタンをクリックします。
- [メール（Email）] > [レポート（Reporting）] > [マイレポート（My Reports）] に移動し、いずれかのセクションの上部にある [+] [レポートモジュール（Report Module）] ボタンをクリックしてから、追加するレポートモジュールを選択します。検索しているモジュールを表示するには、[マイレポート（My Reports）] ページの各セクションの[+][レポートモジュール（Report Module）]ボタンをクリックする必要があります。

各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

ステップ 2 カスタマイズした（たとえば、カラムの追加、削除、または順序変更をした、あるいはチャートにデフォルト以外のデータを表示した）モジュールを追加する場合は、これらのモジュールを [マイレポート（My Reports）] ページでカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

ステップ 3 別に凡例を持つチャート（たとえば、[概要（Overview）] ページからのグラフ）を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。

レポートに含まれるメッセージやトランザクションの詳細の表示

ステップ 1 レポート ページのテーブルにある青色の番号をクリックします

（一部のテーブルにのみ、これらのリンクはあります）。

この数に含まれるメッセージまたはトランザクションは[メッセージトラッキング（Message Tracking）] または [Webトラッキング（Web Tracking）] にそれぞれ表示されます。

ステップ 2 メッセージまたはトランザクションのリストを表示するには、スクロール ダウンします。

次のタスク

- メッセージのトラッキング

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（[前年（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** のメニューを使用すると、1 つ以上のレポーティング フィルタを有効にできます。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接続レベルの詳細（IP Connection Level Detail）]。このフィルタを有効にすると、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、攻撃による大量の着信 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 [前年（Last Year）] レポートに影響を与えます。

  - 受信メールの送信者プロファイル
  - 受信メールの IP アドレス
  - 送信メッセージ送信者の IP アドレス

- [ユーザの詳細（User Detail）]。このフィルタを有効にすると、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 [前年（Last Year）] レポートに影響を与えます。

- 内部ユーザ
- 内部ユーザの詳細
- 送信メッセージ送信者の IP アドレス
- コンテンツ フィルタ

- [メールトラフィックの詳細（Mail Traffic Detail）]。このフィルタを有効にすると、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 [前年（Last Year）] レポートに影響を与えます。

  - 受信メールのドメイン
  - 受信メールの送信者プロファイル
  - 内部ユーザの詳細
  - 送信メッセージ送信者のドメイン

（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。

レポーティングデータおよびトラッキングデータのエクスポート

表 *4:* 新しい *Web* インターフェイスでのレポーティング データおよびトラッキング データのエクスポート

取得対象	CSV	操作手順	注記（Notes）
raw データ 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 （13 ページ）も参照してください。	•	1. レポートページの上部にある [エクスポート（Export）] リンクをクリックします。 2. エクスポートする必要があるレポートモジュールを選択し、[ダウンロード（Download）] をクリックします。	CSV ファイルには、チャートや表で見ることのできるデータを含む、すべての適用可能なデータが含まれます。
	•	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。参照先： • オンデマンドでのメール レポートの生成 • メール レポートのスケジュール設定	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。 一部の拡張レポートは、CSV 形式で使用できません。

取得対象	CSV	操作手順	注記（Notes）
（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）。	•	1. [製品（Product）] ドロップダウンから [Web] を選択し、[トラッキング（Tracking）] > [Webトラッキング（Web Tracking）] を選択します。 2. 検索を実行し、検索結果の上にある [エクスポート（Export）] リンクまたは [すべてをエクスポート（Export All）] リンクをクリックします。	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）。	•	1. [製品（Product）] ドロップダウンから [メール（Email）] を選択し、[トラッキング（Tracking）] > [メッセージトラッキング（Message Tracking）] を選択します。 2. 検索を実行し、検索結果の上にある [エクスポート（Export）] リンクまたは [すべてをエクスポート（Export All）] リンクをクリックします。	[エクスポート（Export）] リンクでは、表示された検索結果を使用して検索基準で指定された制限までCSVファイルをダウンロードします。 [すべてをエクスポート（Export All）] リンクでは、検索条件に一致する最大50,000件のメッセージを含むCSVファイルをダウンロードします。 ヒント：50,000件を超えるメッセージをエクスポートする必要がある場合は、短い時間範囲のエクスポートのセットを実行します。

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、レポーティング データおよびトラッキング データのエクスポート（11 ページ）を参照してください。

CSV エクスポートには raw データのみ含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります（そのデータが Web ベースのレポートで表示された場合でも、含まれていない場合があります）。

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 *5 : raw* データ エントリの表示

カテゴリ ヘッダー	値	説明
タイムスタンプ開始（Begin Timestamp）	1159772400.0	エポックからの秒数で表されたクエリ開始時刻。
タイムスタンプ終了（End Timestamp）	1159858799.0	エポックからの秒数で表されたクエリ終了時刻。
開始日（Begin Date）	2006-10-02 07:00 GMT	クエリの開始日。
End Date	2006-10-03 06:59 GMT	クエリの終了日。
Name	Adware	マルウェア カテゴリの名前。
モニタリングされたトランザクション（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。

カテゴリ ヘッダー	値	説明
検出されたトランザクション（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、レポートの種類ごとに異なります。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ヘッダーが正しくレンダリング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、[ファイル（File）] > [開く（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。

レポート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。

すべてのレポートのトラブルシューティング

- バックアップ セキュリティ管理アプライアンスのレポート データを表示できない （14 ページ）
- レポーティングがディセーブルになっている （15 ページ）

バックアップ セキュリティ管理アプライアンスのレポート データを表示できない

問題

レポート データを表示するのに、単一の E メール セキュリティ アプライアンスを選択できません。[次のデータを参照（View Data For）] オプションはレポート ページには表示されません。

ソリューション

「バックアップ中のサービスのアベイラビリティ」も参照してください。

レポーティングがディセーブルになっている

問題

進行中のバックアップをキャンセルすると、レポーティングがディセーブルになる場合があります。

ソリューション

レポーティング機能は、バックアップが完了すると回復します。

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、中央集中型の電子メール セキュリティ レポーティングの使用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、中央集中型 Web レポーティングおよびトラッキングの使用を参照してください。