エンドユーザーのアクティビティをモニターするレポートの生成

この章で説明する内容は、次のとおりです。

- レポートの概要 （1 ページ）
- レポート ページの使用 （3 ページ）
- 新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）
- レポートの有効化 （10 ページ）
- レポートのスケジュール設定 （10 ページ）
- オンデマンドでのレポートの生成 （12 ページ）
- アーカイブ レポート （13 ページ）
- L4 トラフィック モニタ レポートのトラブルシューティング （13 ページ）

レポートの概要

Web セキュリティアプライアンス では概要レポートが生成されるので、ネットワークで起きていることを把握したり、特定のドメイン、ユーザ、カテゴリのトラフィックの詳細を表示することができます。レポートを実行して特定の期間内のシステムアクティビティをインタラクティブに表示したり、レポートをスケジュールして定期的に実行することができます。

関連項目

- レポート ページからのレポートの印刷とエクスポート （7 ページ）

レポートでのユーザー名の使用

認証をイネーブルにすると、Webプロキシで認証される際に、ユーザーはユーザー名でレポートに一覧表示されます。デフォルトでは、ユーザー名は認証サーバーに表示されるとおりに書き込まれます。ただし、すべてのレポートでユーザー名を識別できないようにすることができます。

（注） 管理者の場合は、常にレポートにユーザー名が表示されます。

ステップ 1 [セキュリティサービス（Security Services）]>[レポート（Reporting）] を選択し、[設定を編集（Edit Settings）] をクリックします。

ステップ 2 [ローカルレポート（Local Reporting）] で、[レポートでユーザー名を匿名にする（Anonymize usernames in reports）] を選択します。

ステップ 3 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

レポート ページ

Web セキュリティアプライアンス には以下のレポートがあります。

- マイ ダッシュボード（My Dashboard）（レポートの「ホームページ」。メニュー バーの左端にある [ホーム（Home）] アイコンをクリックしてアクセスすることもできます。）
- 概要
- Users
- ユーザ数（User Count）
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- Advanced Malware Protection
- ファイル分析（File Analysis）
- AMP 判定の更新
- クライアント マルウェア リスク（Client Malware Risk）
- Web レピュテーション フィルタ（Web Reputation Filters）
- L4 トラフィック モニター（L4 Traffic Monitor）
- SOCKS プロキシ（SOCKS Proxy）
- ユーザの場所別レポート（Reports by User Location）
- Web トラッキング（Web Tracking）
- システム容量（System Capacity）

- システム ステータス（System Status）
- スケジュール設定されたレポート（Scheduled Reports）
- アーカイブ レポート（Archived Reports）

レポート ページの使用

さまざまなレポート ページにシステム アクティビティの概要が表示され、システム データを表示するための複数のオプションがあります。Webサイトおよびクライアント固有のデータをページごとに検索することもできます。

レポート ページでは、以下のタスクが実行できます。

オプション	タスクへのリンク
レポートで表示する時間範囲を変更する	時間範囲の変更 （3 ページ）
特定のクライアントとドメインを検索する	データの検索 （4 ページ）
チャートに表示するデータを選択する	チャート化するデータの選択 （5 ページ）
レポートを外部ファイルにエクスポートする	レポート ページからのレポートの印刷とエクスポート （7 ページ）

時間範囲の変更

[時間範囲（Time Range）] フィールドを使用して、各セキュリティ コンポーネントの表示データを更新できます。このオプションを使用して、定義済みの時間範囲のアップデートを生成できます。また、開始時刻と終了時刻を指定してカスタム時間範囲を定義することもできます。

（注） 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 ページ全体で使用されます。

時間範囲	返されるデータ
時間（Hour）	60 分間と、追加で最大 5 分間
日（Day）	直近の 24 時間とその時点の 1 時間未満の時間を含めた時間に対して 1 時間間隔
週（Week）	直近の 7 日間にその時点の日にちを足した日数に対して 1 日間隔

時間範囲	返されるデータ
月（30 日）（Month (30 days)）	直近の 30 日間にその時点の日にちを足した日数に対して 1 日間隔
昨日（Yesterday）	Web セキュリティアプライアンス に定義されているタイム ゾーンを使用した直近の 24 時間（00:00 から 23:59）
カスタム範囲（Custom Range）	定義済みのカスタム時間範囲。 [カスタム範囲（Custom Range）] を選択すると、開始時刻と終了時刻を入力できるダイアログボックスが表示されます。

（注） すべてのレポートで、システム設定のタイム ゾーンに基づき、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のみ、GMT で時刻が表示されます。

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。

データの検索

一部のレポートには、特定のデータ ポイントを検索するために使用できるフィールドがあります。データを検索するときに、レポートは検索する特定のデータ セットのレポート データを

調整します。入力する文字列に完全に一致する値や入力する文字列で始まる値を検索できます。以下のレポート ページには検索フィールドがあります。

検索フィールド	説明
ユーザー（**Users**）	ユーザー名またはクライアント IP アドレスでユーザーを検索します。
Web サイト（Web Sites）	ドメインまたはサーバーの IP アドレスでサーバーを検索します。
URL カテゴリ（URL Categories）	URL カテゴリを検索します。
アプリケーションの表示（**Application Visibility**）	AVC エンジンがモニターし、ブロックするアプリケーション名を検索します。
クライアント マルウェア リスク（**Client Malware Risk**）	ユーザー名またはクライアント IP アドレスでユーザーを検索します。

（注） クライアント IP アドレスおよびクライアント ユーザー ID を表示するには、認証を設定する必要があります。

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。チャートのオプションは、レポートのテーブルの列見出しと同じです。

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。

カスタム レポート

既存のレポートのページからチャート（グラフ）とテーブルを組み合わせてカスタム レポートのページを作成できます。

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 （6 ページ）。 • カスタム レポート ページの作成 （6 ページ）
カスタム レポート ページの表示	1. [モニター（Monitor）] > [メール（Email）] または [Web] > [レポート（Reporting）] > [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関連するセクション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 PDF または CSV バージョンの生成	[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択し、[今すぐレポートを生成（Generate Report Now）] をクリックします。
カスタム レポートの PDF または CSV バージョンの定期的な生成	[レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

カスタム レポートに追加できないモジュール

- 検索結果（Web トラッキングの検索結果を含む）

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 （6 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 [Web] タブのレポート 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。
- [レポート（Reporting）]>[マイ レポート（My Reports）] に移動し、[+]ボタン（いずれかのセクションの上部にあります）をクリックして、追加するレポート モジュールを選択します。目的のモジュールを見つけるには、[マイ レポート（My Reports）] ページの各セクションにある [+] ボタンをクリックしなければならない場合があります。

  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。

レポート ページからのレポートの印刷とエクスポート

ページ右上隅の [印刷可能（PDF）（Printable (PDF)）] リンクをクリックすると、すべてのレポート ページを印刷形式の PDF 版で生成できます。また、[エクスポート（Export）] リンクを

クリックして、未処理データをカンマ区切り形式（CSV）ファイルとしてエクスポートすることもできます。

CSV エクスポートには未処理データのみが含まれるため、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る場合でも、含まれていない場合があります）。

レポート データのエクスポート

ほとんどのレポートには、未処理データをカンマ区切り形式（CSV）のファイルにエクスポートできる [エクスポート（Export）] リンクが用意されています。CSV ファイルにデータをエクスポートすると、Microsoft Excel などのアプリケーションを使用し、データにアクセスして処理することができます。

エクスポートされた CSV データは、Web セキュリティアプライアンス でのタイム ゾーン設定にかかわらず、すべてのメッセージ トラッキングおよびレポーティング データをグリニッジ標準時（GMT）で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数のタイムゾーンにあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

以下の例は、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
```

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。
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。
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総数 =（検出されたトランザクションの数）+（ブロックされたトランザクションの数）。

（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。

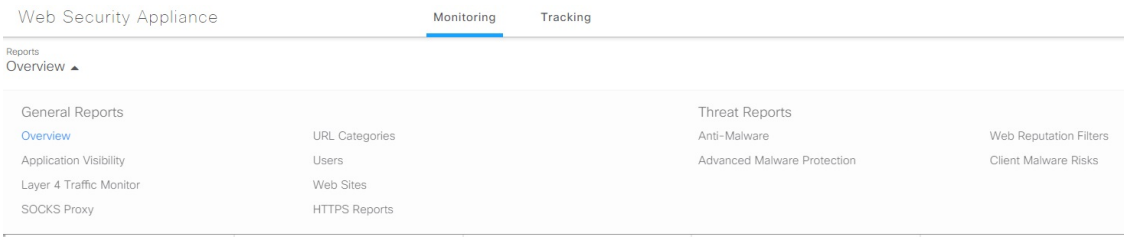
ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策として、ローカルマシンにファイルを保存し、[ファイル（File）]>[開く（Open）] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

新しい Web インターフェイスでのインタラクティブ レポート ページの使用

次の図に示す [レポート（Reports）] ドロップダウンを使用すると、Web セキュリティアプライアンス のレポートを表示することができます。

（注） [概要（Overview）] レポートページは、ランディングページ（ログイン後に表示されるページ）です。レポートまたはトラッキングページから新しい Web インターフェイスをリロードすると、デフォルトのランディングページ（[概要（Overview）] レポートページ）がロードされます。

図 *1 :* **レポートドロップダウン**



Web レポートは、**一般的なレポート**と**脅威レポート**に分類されます。

新しい Web インターフェイスにアクセスするには、「新しい Web インターフェイスでのセキュア アプライアンス レポート」を参照してください。

関連項目

- （Web レポートのみ）チャート化するデータの選択

レポートの有効化

組織に複数の Web セキュリティアプライアンス があり、Cisco コンテンツ セキュリティ管理アプライアンスを使用して集約レポートのデータを管理および表示する場合、各 Web セキュリティアプライアンス で集約管理レポートを有効にする必要があります。

アプライアンスの設定に基づいてレポートのタイプを選択できます。すべてのレポートをローカルで保存できます。あるいは、Cisco Defense Orchestrator を介してレポートにアクセスすることもできます（アプライアンスがオンボーディング済みの場合）。組織に複数の Web セキュリティアプライアンス があり、Cisco コンテンツセキュリティ管理アプライアンスを 1 つ使用している場合は、集約管理レポートを選択して集約したレポートデータを管理および表示できます。集約管理レポート、または Cisco Defense Orchestrator を介したローカルレポートを選択すると、各 Web セキュリティアプライアンス にこれらの設定が適用されます。

ステップ 1 **[セキュリティサービス（Security Services）]** > **[レポート（Reporting）]** を選択し、[設定を編集（Edit Settings）] をクリックします。

a) アプライアンスでレポートを有効にする場合は、[ローカル レポート（Local Reporting）] をオンにします。アプライアンス ポータルにログインした後、レポートにアクセス可能になります。

b) Cisco Defense Orchestrator を介してレポートを使用可能にする場合は、[ローカル レポート（Local Reporting）] および [Cisco Defense Orchestrator のレポート（Cisco Defense Orchestrator Reporting）] をオンにします。

c) Cisco コンテンツ セキュリティ管理アプライアンスを介してレポートを使用可能にする場合は、[集中管理レポート（Centralized Reporting）] をオンにします。

Web セキュリティアプライアンス のみが、ローカル レポートについて収集されたすべてのデータを保存します。集約管理レポートがアプライアンスで有効な場合、Web セキュリティアプライアンス はシステム容量データとシステムステータスデータのみを保持します。これらは Web セキュリティアプライアンス でローカルに使用できる唯一のレポートです。

管理アプライアンスでのこの機能の設定については、Cisco コンテンツ セキュリティ管理アプライアンス ユーザー ガイドの集約管理 Web レポートの使用とトラッキングに関する章を参照してください。

ステップ 2 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

レポートのスケジュール設定

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール化したレポートは、前日、過去 7 日間、前月のデータを含めるように設定できます。

レポートをスケジュール設定できるレポート タイプは以下のとおりです。

- 概要

- Users
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- Advanced Malware Protection
- Advanced Malware Protection 判定の更新
- クライアント マルウェア リスク（Client Malware Risk）
- Web レピュテーション フィルタ（Web Reputation Filters）
- L4 トラフィック モニター（L4 Traffic Monitor）
- SOCKS プロキシ（SOCKS Proxy）
- ユーザの場所別レポート（Reports by User Location）
- システム容量（System Capacity）
- マイ ダッシュボード（My Dashboard）

スケジュール設定されたレポートの追加

ステップ 1 [レポート（Reporting）]>[スケジュールされたレポート（Scheduled Reports）] を選択し、[定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 2 レポート [タイプ（Type）] を選択します。

ステップ 3 レポートのわかりやすい [タイトル（Title）] を入力します。

同じ名前のレポートを複数作成しないでください。

ステップ 4 レポートに含めるデータの時間範囲を選択します。

ステップ 5 生成されるレポートの [形式（Format）] を選択します。

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

ステップ 6 設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。

ステップ 7 [スケジュール（Schedule）]セクションで、レポートを実行する周期（毎日、毎週、または毎月）と時間を選択します。

ステップ 8 [メールの送信先（Email to）]フィールドに、生成されたレポートを送信する相手の電子メール アドレスを入力します。

電子メール アドレスを指定しなかった場合は、レポートのアーカイブのみが行われます。

ステップ 9 データの [レポート言語（Report Language）] を選択します。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

スケジュール設定されたレポートの編集

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

ステップ 2 リストからレポートのタイトルを選択します。

ステップ 3 設定を変更します。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

スケジュール設定されたレポートの削除

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

ステップ 2 削除するレポートに対応するチェックボックスをオンにします。

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

ステップ 4 削除して変更を確定します（[削除（Delete）] と [変更を確定（Commit Changes）]）。

（注） 削除されたレポートのアーカイブ版は削除されません。

オンデマンドでのレポートの生成

ステップ 1 [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（Type）] を選択します。

ステップ 4 レポートのわかりやすい [タイトル（Title）] を入力します。

同じ名前のレポートを複数作成しないでください。

ステップ 5 レポートに含めるデータ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（Format）] を選択します。

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

ステップ 7 設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。

ステップ 8 [配信オプション（Delivery Options）] のいずれかを選択します。

- レポートの [アーカイブ（Archive）]（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）。
- [今すぐ受信者にメールを送信（Email now to recipients）]（1 つまたは複数の電子メール アドレスを指定します）。

ステップ 9 データの [レポート言語（Report Language）] を選択します。

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

ステップ 11 変更を確定します。

アーカイブ レポート

[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページには、使用可能なアーカイブ済みのレポートが一覧表示されます。[レポートのタイトル（Report Title）] 列のそれぞれの名前は、そのレポートのビューにリンクしています。[表示（Show）] メニューは、一覧表示されたレポートのタイプをフィルタリングします。列見出しをクリックして、各列のデータをソートすることができます。

アプライアンスでは、スケジュール設定されたレポートごとに最大 12 のインスタンスが保存されます（最大で合計 1000 レポート）。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。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。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。

L4 トラフィック モニタ レポートのトラブルシューティング

Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合、プロキシのデータ ポートの IP アドレスが記録され、クライアント IP アドレスとしてレポートに表示されます。Web プロキシがトランスペアレント プロキシとして設定されている場合は、クライアント IP アドレスが正しく記録され、表示されるように IP スプーフィングを有効にします。これを行うには、『IronPort AsyncOS for Web User Guide』を参照してください。

関連項目

- [クライアント マルウェア リスク（Client Malware Risk）] ページ
- L4 トラフィック モニタによって処理されたトランザクションの検索

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。