CHAPTER 5

中央集中型 Web レポーティングの使用方法

中央集中型 Web レポーティングの概要

Web レポーティング機能は、個々のセキュリティ機能から情報を収集し、Web トラフィック パターンやセキュリティ リスクのモニタに使用できるデータを記録します。レポートをリアルタイムで実行して所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、スケジュールを作成してレポートを定期的に実行したりできます。また、レポーティング機能を使用して、raw データをファイルにエクスポートすることもできます。

中央集中型 Web レポーティング機能を使用すると、管理者は概要レポートを作成してネットワークの現状を把握できるだけでなく、特定のドメイン、ユーザ、またはカテゴリのトラフィックの詳細を、ドリルダウンして確認できます。

ドメイン情報

ドメインについては、Web レポーティング機能で以下のデータ要素を生成し、ドメイン レポートに含めることができます。たとえば Facebook.com ドメインに関するレポートを作成している場合、レポートに次の情報を出力できます。

- Facebook.com にアクセスした上位ユーザのリスト
- Facebook.com 内でアクセスされた上位 URL のリスト

ユーザ

ユーザについては、Web レポーティング機能で以下のデータ要素を生成し、ユーザ レポートに含めることができます。たとえば、「Jamie」というタイトルのレポートに次の情報を含めることができます。

- ユーザ「Jamie」がアクセスした上位ドメインのリスト

- マルウェアまたはウイルスが陽性であった上位 URL のリスト
- ユーザ「Jamie」がアクセスした上位カテゴリのリスト

カテゴリ

カテゴリに対しては、カテゴリ レポートに含めるデータを、Web レポーティング機能で生成できます。たとえば、「Sports」というカテゴリに次の情報を含めることができます。

- 「Sports」カテゴリに含まれていた上位ドメインのリスト
- 「Sports」カテゴリにアクセスした上位ユーザのリスト

上記のどの例のレポートも、ネットワーク上の特定の項目に関する包括的なビューを提供して、管理者が対処できるようにすることを目的としています。

一般

ロギング ページとレポーティング ページの詳細については、「ロギングとレポーティング」（P.14-1）を参照してください。

（注） アクセスされた特定の URL だけでなく、ユーザが利用するすべてのドメイン情報を取得することができます。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を入手するには、[Web Tracking] ページの [Proxy Services] タブを使用します。

（注） Web セキュリティ アプライアンスでデータが保存されるのは、ローカル レポーティングが使用される場合だけです。Web セキュリティ 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な場合、その Web セキュリティ アプライアンスではシステム キャパシティとシステム ステータスのデータのみが維持されます。中央集中型 Web 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。

セキュリティ管理アプライアンスでレポーティング データを表示するには、いくつかの方法があります。

- インタラクティブ レポート ページを表示する場合は、「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。
- 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 Web レポートの生成」（P.5-67）を参照してください。
- レポートが定期的に繰り返し作成されるようにスケジュールを設定する場合は、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。
- 以前に実行されたレポート（スケジュール設定されたレポートとオンデマンドで生成されたレポートの両方）のアーカイブ版を表示する方法については、「アーカイブされた Web レポートの表示と管理」（P.5-69）を参照してください。

中央集中型 Web レポーティングの設定

中央集中型 Web レポーティングを設定するには、次の手順を順序どおり実行します。

- 「セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化」（P.5-3）
  - Web レポートでのユーザ名の匿名化

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

セキュリティ管理アプライアンスで Web レポーティングを使用する前に、セキュリティ管理アプライアンスで Web レポーティングをイネーブルにする必要があります。

ステップ 1　中央集中型 Web レポーティングをイネーブルにする前に、十分なディスク領域がサービスに割り当てられていることを確認します。「ディスク使用量の管理」（P.13-58）を参照してください。

ステップ 2　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

ステップ 3　システム セットアップ ウィザードの実行後初めて中央集中型レポーティングをイネーブルにする場合は、次の手順を実行します

a.　[Enable] をクリックします。

b.　エンド ユーザ ライセンス契約書を確認して、[Accept] をクリックします。

ステップ 4　以前に中央集中型レポーティングをディセーブルにし、その後イネーブルにする場合は、次の手順を実行します。

a.　[Edit Settings] をクリックします。

b.　[Enable Centralized Web Report Services] チェックボックスを選択します。

c.　「Web レポートでのユーザ名の匿名化」（P.5-4）はここで実行することも、後で実行することもできます。

ステップ 5　変更を送信し、保存します。

（注）　アプライアンスで Web 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 Web レポーティングが機能しません。Web 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、Web 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.13-58）を参照してください。

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のイネーブル化

中央集中型レポーティングをイネーブルにする前に、すべての Web セキュリティ アプライアンスが設定され、想定どおりに動作している必要があります。

中央集中型レポーティングは、それを使用する各 Web セキュリティ アプライアンスごとにイネーブルにする必要があります。

『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Enabling Centralized Reporting」を参照してください。

管理対象の各 Web セキュリティ アプライアンスへの中央集中型 Web レポーティング サービスの追加

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

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

ステップ 2　リストに Web セキュリティ アプライアンスを追加済みの場合は、次の手順を実行します。

a. Web セキュリティ アプライアンスの名前をクリックします。

b. [Centralized Reporting] サービスを選択します。

ステップ 3　Web セキュリティ アプライアンスをまだ追加していない場合は、次の手順を実行します。

a. [Add Web Appliance] をクリックします。

b. [Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注） [IP Address] テキスト フィールドに DNS 名を入力した場合でも、[Submit] をクリックすると、すぐに IP アドレスに解決されます。

c. [Centralized Reporting] サービスが事前に選択されています。

d. [Establish Connection] をクリックします。

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

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

f. [Success] メッセージがページのテーブルの上に表示されるまで待機します。

g. [Test Connection] をクリックします。

h. テーブルの上のテスト結果を確認します。

ステップ 4　[Submit] をクリックします。

ステップ 5　中央集中型レポーティングをイネーブルにする各 Web セキュリティ アプライアンスに対してこの手順を繰り返します。

ステップ 6　変更を保存します。

Web レポートでのユーザ名の匿名化

デフォルトでは、レポーティング ページと PDF にユーザ名が表示されます。ただし、ユーザのプライバシーを保護するために、Web レポートでユーザ名を識別できないようにすることができます。

（注）　このアプライアンスの管理者権限を持つユーザは、インタラクティブ レポートを表示する際、常にユーザ名を表示できます。

図 5-1　ユーザ名が表示されたレポーティング ページ

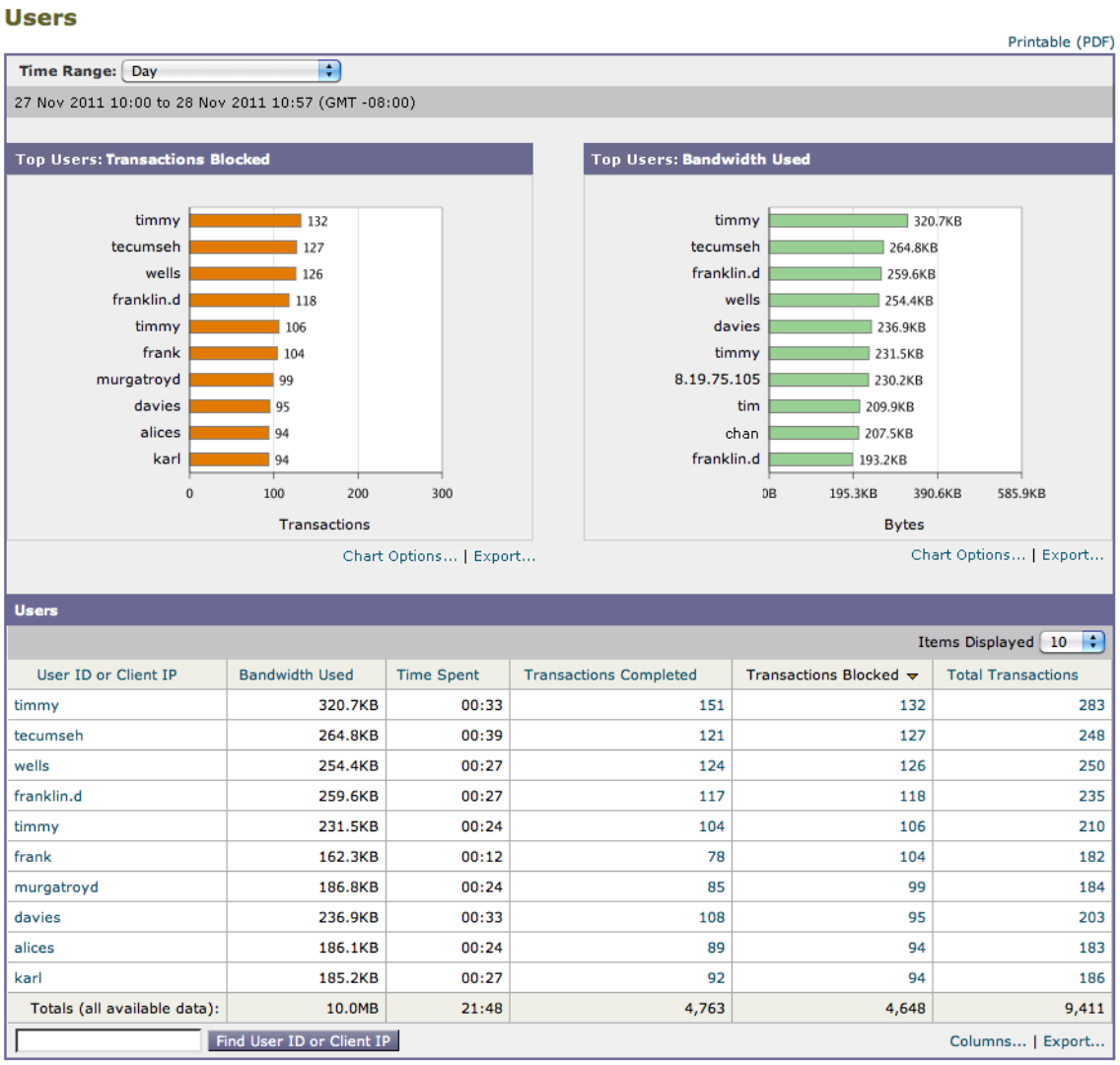
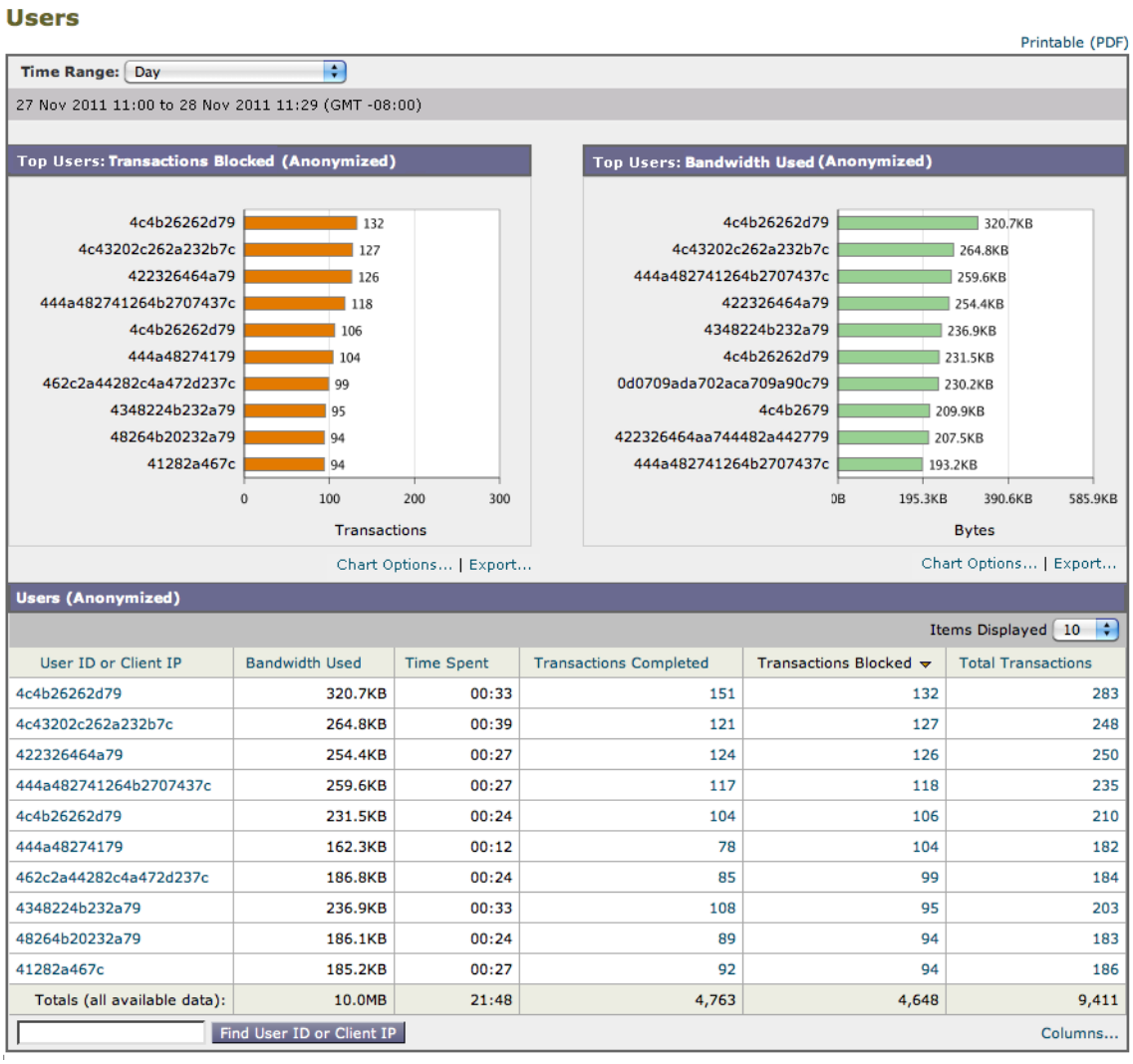


図 5-2　ユーザを匿名にしたレポーティング ページ



レポートでユーザ名を識別できないようにするには、次の手順を実行します。

ステップ 1　[Management Appliance] > [Centralized Services] > [Web] > [Centralized Reporting] を選択します。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Anonymize usernames in reports] チェックボックスをオンにします。

ステップ 4　変更を送信し、保存します。

インタラクティブ Web レポーティング ページの操作

インタラクティブ Web レポーティング ページでは、システム内で管理対象とする 1 つまたはすべての Web セキュリティ アプライアンスアプライアンスに関する情報をモニタできます。

これらのページの操作については、次の項目を参照してください。

表 5-1　インタラクティブ Web レポーティング ページの操作

目的	参照先
レポート データのアクセスおよび表示オプションを確認する	「レポーティング データを表示する方法」（P.3-1）
テーブル内のデータの意味を理解する	「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）
インタラクティブ レポート ページのビューをカスタマイズする	「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）
データ内の情報を検索する	「[Web Tracking] ページ」（P.5-51）
レポート情報を印刷またはエクスポートする	「レポート データの印刷とエクスポート」（P.3-7）
さまざまなインタラクティブ レポート ページについて理解する	「Web レポーティング ページについて」（P.5-7）
レポートをオンデマンドで生成する	「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）
レポートが指定した間隔で所定の時刻に自動的に実行されるようスケジュールを設定する	「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）
アーカイブ済みのオンデマンド レポートとスケジュールされたレポートを表示する	「アーカイブされた Web レポートの表示と管理」（P.5-69）
データの収集方法を理解する	「セキュリティ アプライアンスによるレポート用データの収集方法」（P.3-2）

Web レポーティング ページについて

[Web] > [Reporting] タブには、レポート データを表示するためのオプションがいくつかあります。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）　[Web Reporting] タブのどのオプションをオンデマンドまたはスケジュール済みレポートとして使用できるかについては、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

表 5-2　[Web Reporting] タブの詳細

[Web Reporting] メニュー	アクション
Web レポーティングの [Overview] ページ	[Overview] ページには、お使いの Cisco IronPort 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、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。詳細については、「Web レポーティングの [Overview] ページ」（P.5-13）を参照してください。
[Users] ページ	[Users] ページには複数の Web トラッキング リンクが表示され、各ユーザの Web トラッキング情報を確認できます。 [Users] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。 [Users] ページのインタラクティブな [Users] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [User Details] ページに表示されます。 [User Details] ページでは、[Web] > [Reporting] > [Users] ページのインタラクティブな [Users] テーブルで指定したユーザについて具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。 詳細については、「[Users] ページ」（P.5-17）を参照してください。システムにおける各ユーザの情報については、「[User Details] ページ」（P.5-20）を参照してください。
[Web Sites] ページ	[Web Sites] ページでは、管理対象アプライアンスで発生しているアクティビティ全体を集約して表示できます。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。詳細については、「[Web Sites] ページ」（P.5-24）を参照してください。
[URL Categories] ページ	[URL Categories] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。 • トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL。 • 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブなカラム見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。 詳細については、「[URL Categories] ページ」（P.5-26）を参照してください。

表 5-2　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[Application Visibility] ページ	[Application Visibility] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内で特定のアプリケーション タイプに適用されている制御を適用し、表示することができます。詳細については、「[Application Visibility] ページ」（P.5-30）を参照してください。
Security	
[Anti-Malware] ページ	[Anti-Malware] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、「[Anti-Malware] ページ」（P.5-33）を参照してください。
[Client Malware Risk] ページ	[Client Malware Risk] ページは、セキュリティ関連のレポーティング ページです。このページを使用して、著しく頻繁にマルウェア サイトへ接続している可能性がある個々のクライアント コンピュータを特定できます。 詳細については、「[Client Malware Risk] ページ」（P.5-39）を参照してください。
[Web Reputation Filters] ページ	指定した時間範囲内のトランザクションに対する、Web レピュテーション フィルタリングに関するレポートを表示できます。詳細については、「[Web Reputation Filters] ページ」（P.5-41）を参照してください。
[L4 Traffic Monitor] ページ	指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、「[L4 Traffic Monitor] ページ」（P.5-44）を参照してください。
[Reports by User Location] ページ	[Reports by User Location] ページでは、モバイル ユーザがローカル システムまたはリモート システムから実行しているアクティビティを確認できます。 詳細については、「[Reports by User Location] ページ」（P.5-49）を参照してください。
Reporting	

表 5-2　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[Web Tracking] ページ	[Web Tracking] ページでは、次の 2 種類の情報を検索できます。 • [Proxy Services] タブでは、基本的な Web 関連情報（アプライアンスで処理されている Web トラフィックのタイプなど）を追跡して表示することができます。 これには、時間範囲、ユーザ ID、クライアント IP アドレスなどの情報が含まれるほか、特定のタイプの URL、各接続が占有している帯域幅の量、特定のユーザの Web 使用状況のトラッキングなどの情報も含まれます。 • [L4 Traffic Monitor] タブでは、マルウェアの転送アクティビティに関与しているサイト、ポート、およびクライアント IP アドレスの L4TM データを検索できます。 詳細については、「[Web Tracking] ページ」（P.5-51）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 セキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。 詳細については、「[System Capacity] ページ」（P.5-57）を参照してください。
[Data Availability] ページ	各アプライアンスの セキュリティ管理アプライアンス上のレポーティング データの影響を把握できます。詳細については、「[Data Availability] ページ」（P.5-62）を参照してください。
Scheduled Reports	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とオンデマンド Web レポートについて」（P.5-63）を参照してください。
Archived Reports	指定した時間範囲のレポートをアーカイブできます。詳細については、「アーカイブされた Web レポートの表示と管理」（P.5-69）を参照してください。

（注）　ほとんどの Web レポーティング カテゴリでレポートをスケジュール設定できます。これには、拡張された上位 URL カテゴリおよび上位アプリケーション タイプに関する追加のレポートが含まれます。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とオンデマンド Web レポートについて」（P.5-63）を参照してください。

Web レポーティング ページのテーブル カラムの説明

ここでは、さまざまな Web レポート ページのテーブルで使用されるカラム見出しについて説明します。

（注）すべてのカラムを各レポート ページで使用できるわけではありません。また、使用可能なすべてのカラムがデフォルトで表示されるわけではありません。テーブルで使用可能なカラムを表示するには、テーブルの下の [Column] リンクをクリックします。

レポートでのテーブルの操作の詳細については、「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 5-3　Web レポーティング ページのテーブル カラムの説明

カラム名	説明
Domain or Realm	テキスト形式で表示されるユーザのドメインまたはレルム。
UserID or Client IP	テキスト形式で表示されるユーザのユーザ ID またはクライアント IP。
Bandwidth Used	特定のユーザまたはアクションによって使用される帯域幅の量。帯域幅の単位は、バイトまたは % で表示されます。
Bandwidth Saved by Blocking	特定のトランザクションのブロックのため節約された帯域幅の量。帯域幅単位はバイトで表示されます。

表 5-3　Web レポーティング ページのテーブル カラムの説明（続き）

カラム名	説明
Time Spent	Web ページに費やされた時間。各 URL カテゴリでユーザが費やした時間。ユーザを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。 トランザクション イベントに「viewed」のタグが付けられる（ユーザが特定の URL に進む）と、[Time Spent] の値の計算が開始され、Web レポーティング テーブルのフィールドとして追加されます。 費やされた時間を計算するため、AsyncOS はアクティブ ユーザごとに、1 分間のアクティビティに対して 60 秒という時間を割り当てます。この 1 分間の終わりに、各ユーザが費やした時間は、そのユーザが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザは各ドメインで 15 分ずつ費やしたと見なされます。 経過時間の値に関して、以下の注意事項を考慮してください。 • アクティブ ユーザは、アプライアンスを介して HTTP トラフィックを送信し、Web サイトにアクセスした、すなわち AsyncOS が「ページ ビュー」と見なす動作を行ったユーザ名または IP アドレスとして定義されています。 • AsyncOS では、クライアント アプリケーションが開始する要求とは逆に、ユーザが開始する HTTP 要求としてページ ビューを定義します。AsyncOS はヒューリスティック アルゴリズムを使用して、可能な限り効果的にユーザ ページ ビューを識別します。 単位は時間：分形式で表示されます。
Allowed URL Category	許可されたカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
Monitored URL Category	モニタリングされているカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
Warned URL Category	警告が発行されたカテゴリの数とタイプ。単位はトランザクション タイプで表示されます。
Blocked by URL Category	URL カテゴリが原因でブロックされたトランザクション。単位はトランザクション タイプで表示されます。
Blocked by Application or Application Type	アプリケーション タイプが原因でブロックされたアプリケーション。単位はトランザクション タイプで表示されます。
Blocked by Web Reputation	Web レピュテーションのためブロックされたトランザクション。単位はトランザクション タイプで表示されます。
Blocked by Anti-Malware	Anti-Malware によってブロックされたトランザクション。単位はトランザクション タイプで表示されます。

表 5-3　Web レポーティング ページのテーブル カラムの説明（続き）

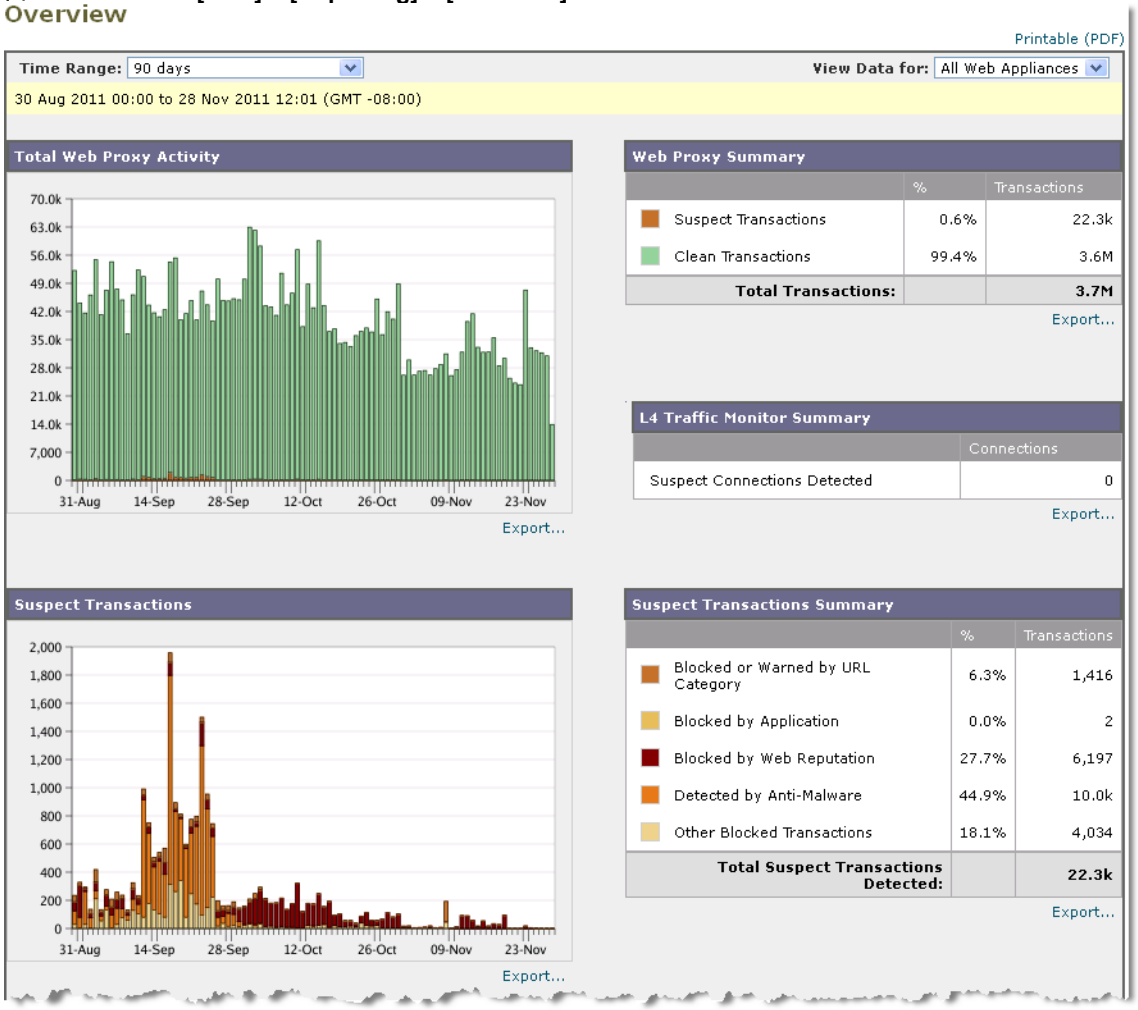
カラム名	説明
Other Blocked Transactions	ブロックされた他のすべてのトランザクション。単位はトランザクション タイプで表示されます。
Transactions with Bandwidth Limit	帯域幅の制限があるトランザクションの数。
Transactions without Bandwidth Limit	帯域幅の制限がないトランザクションの数。
Transactions Blocked by Application	特定のアプリケーション タイプによってブロックされたトランザクションの数。
Warned Transactions	ユーザに警告が発せられたすべてのトランザクション。単位はトランザクション タイプで表示されます。
Transactions Completed	ユーザが完了したトランザクション。単位はトランザクション タイプで表示されます。
Transactions Blocked	ブロックされたすべてのトランザクション。単位はトランザクション タイプで表示されます。
Total Transactions	発生したトランザクションの合計数。

Web レポーティングの [Overview] ページ

[Web] > [Reporting] > [Overview] ページでは、お使いの Cisco IronPort 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、着信および発信トランザクションに関するグラフやサマリーテーブルも含まれます。

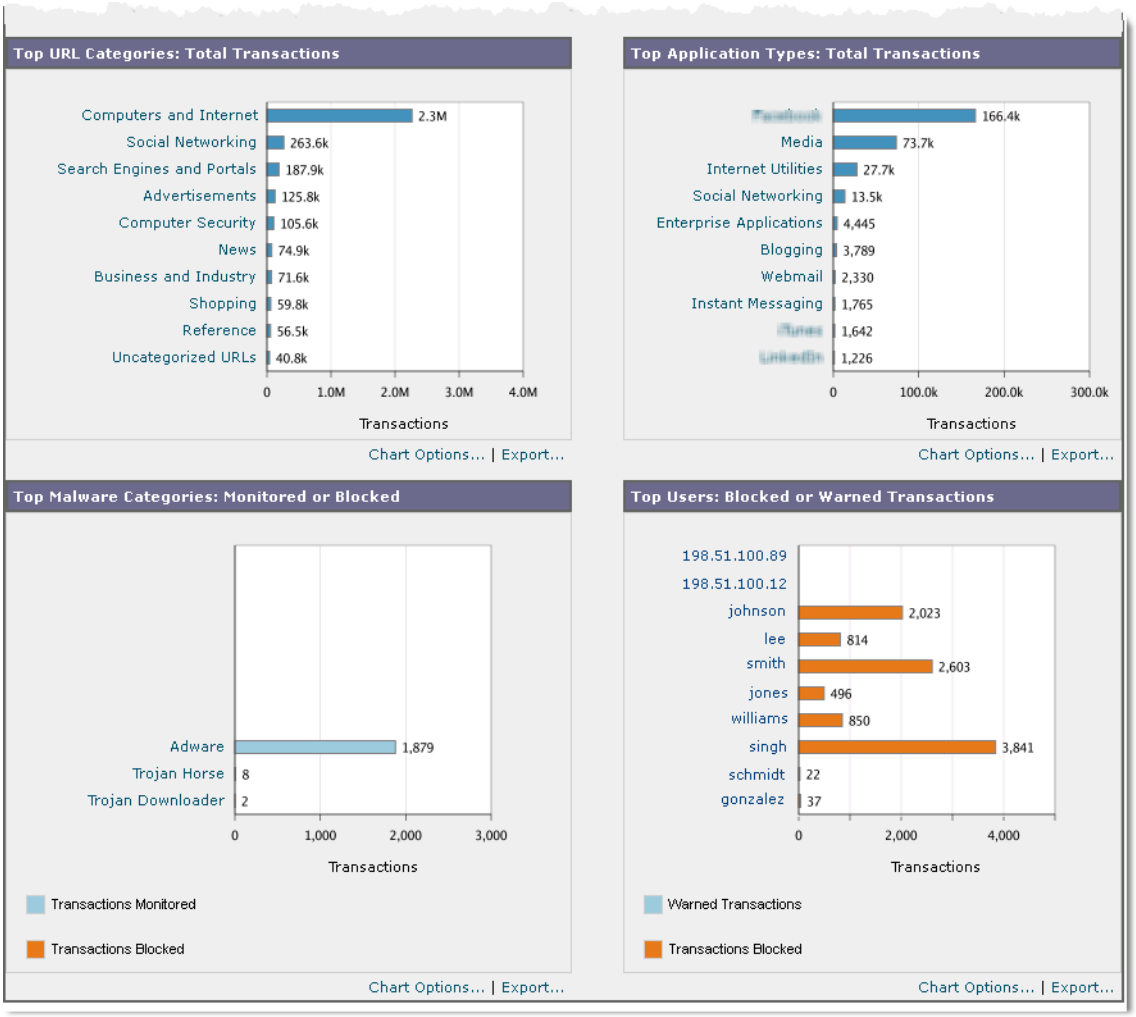
図 5-3 に、[Overview] ページを示します。

図 5-3　[Web] > [Reporting] > [Overview] ページ



（次のページに続く）

（前ページからの続き）



[Overview] ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシ アクティビティ、および各種トランザクション サマリーが表示されます。トランザクション サマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしいトランザクションと、そのグラフの隣にそれらのトランザクションがブロックされた数、およびブロックされた方法が表示されます。

[Overview] ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位アプリケーション タイプおよびカテゴリ、これらのブロックまたは警告を生成している上位ユーザが表示されます。

次のリストでは、[Overview] ページの各セクションについて説明します。

表 5-4　[Web] > [Reporting] > [Overview] 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.3-4）を参照してください。
View Data for	概要データを表示する Web セキュリティ アプライアンスを選択するか、[All Web Appliances] を選択します。 「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）も参照してください。
Total Web Proxy Activity	このセクションでは、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される Web プロキシ アクティビティを表示できます。 このセクションには、トランザクションの実際の数（縦の目盛り）、およびアクティビティが発生したおよその日付（横の時間軸）が表示されます。
Web Proxy Summary	このセクションでは、疑わしい Web プロキシ アクティビティまたは正常なプロキシ アクティビティの比率を、トランザクションの総数も含めて表示できます。
L4 Traffic Monitor Summary	このセクションには、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告されるレイヤ 4 トラフィックが表示されます。
Suspect Transactions	このセクションでは、管理者が疑わしいトランザクションと分類した Web トランザクションを表示できます。 このセクションには、トランザクションの実際の数（縦の目盛り）、およびアクティビティが発生したおよその日付（横の時間軸）が表示されます。
Suspect Transactions Summary	このセクションでは、ブロックまたは警告された疑わしいトランザクションの比率を表示できます。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。
Top URL Categories by Total Transactions	このセクションには、ブロックされている上位 10 の URL カテゴリが表示されます。URL カテゴリのタイプ（縦の目盛り）、特定タイプのカテゴリが実際にブロックされた回数（横の目盛り）などがあります。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。
Top Application Types by Total Transactions	このセクションには、ブロックされている上位アプリケーション タイプが表示されます。これには、実際のアプリケーション タイプ名（縦の目盛り）、特定のアプリケーションがブロックされた回数（横の目盛り）が含まれます。

表 5-4　[Web] > [Reporting] > [Overview] ページの詳細（続き）

セクション	説明
Top Malware Categories Detected	このセクションには、検出されたすべてのマルウェア カテゴリが表示されます。
Top Users Blocked or Warned Transactions	このセクションには、ブロックされたトランザクションまたは警告が発行されたトランザクションを生成している実際のユーザが表示されます。ユーザは IP アドレスまたはユーザ名で表示できます。ユーザ名を識別できないようにするには、「Web レポートでのユーザ名の匿名化」（P.5-4）を参照してください。

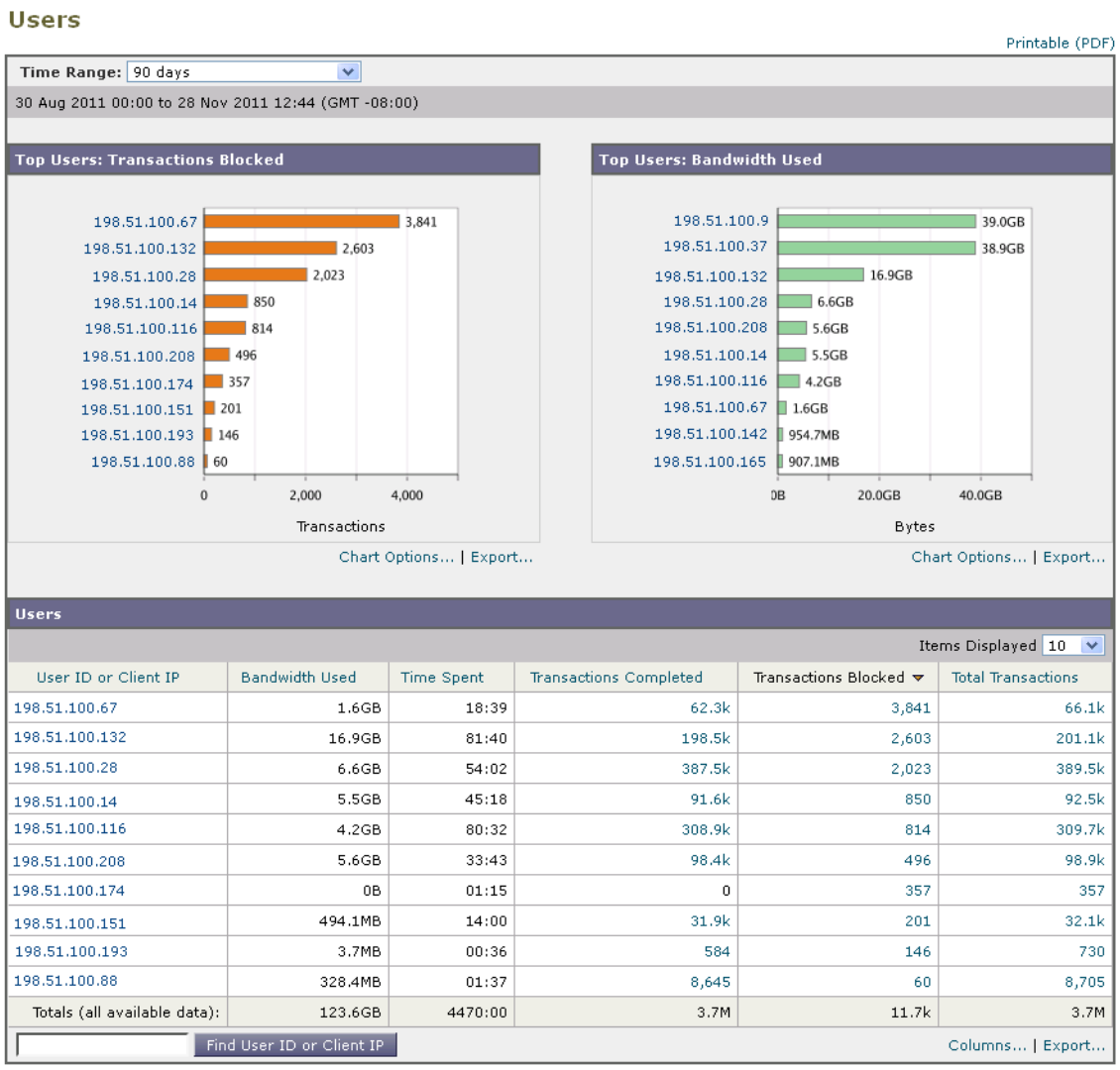
[Users] ページ

[Web] > [Reporting] > [Users] ページには、各ユーザの Web レポーティング情報を表示できる複数のリンクが表示されます。

[Users] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。

（注）　セキュリティ管理アプライアンスがサポートできる Web セキュリティ アプライアンス上の最大ユーザ数は 500 です。

図 5-4　[Web] > [Reporting] > [Users] ページ



[Users] ページには、システム上のユーザに関する次の情報が表示されます。

表 5-5　[Web] > [Reporting] > [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.3-4）を参照してください。
Top Users by Transactions Blocked	このセクションには、IP アドレスまたはユーザ名で示された上位ユーザ（縦の目盛り）、そのユーザがブロックされたトランザクションの数（横の目盛り）が表示されます。レポーティングを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページまたはスケジュール設定されたレポートでユーザ名を認識不可能にする方法の詳細については、「セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化」（P.5-3）を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。ユーザ名を非表示にするには、「Web レポートでのユーザ名の匿名化」（P.5-4）を参照してください。
Top Users by Bandwidth Used	このセクションには、システム上で最も帯域幅（ギガバイト単位の使用量を示す横の目盛り）を使用している上位ユーザが、IP アドレスまたはユーザ名（縦の目盛り）で表示されます。
[Users] テーブル	このテーブルのデータの詳細については、「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。 さらに、特定のユーザ ID またはクライアント IP アドレスを検索できます。[User] セクション下部のテキスト フィールドに特定のユーザ ID またはクライアント IP アドレスを入力し、[Find User ID or Client IP Address] をクリックします。IP アドレスが正確に一致していなくても結果は返されます。 [Users] テーブルでは、特定のユーザをクリックして、さらに具体的な情報を得ることができます。この情報は、[User Details] ページに表示されます。[User Details] ページの詳細については、「[User Details] ページ」（P.5-20）を参照してください。

（注） クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。詳細については、第 9 章の「Creating the LDAP Server Profile」を参照してください。

ヒント このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Users] ページの使用例については、「例 1：ユーザの調査」（P.D-1）を参照してください。

（注）　[Users] ページについて、レポートを生成またはスケジュールすることができます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

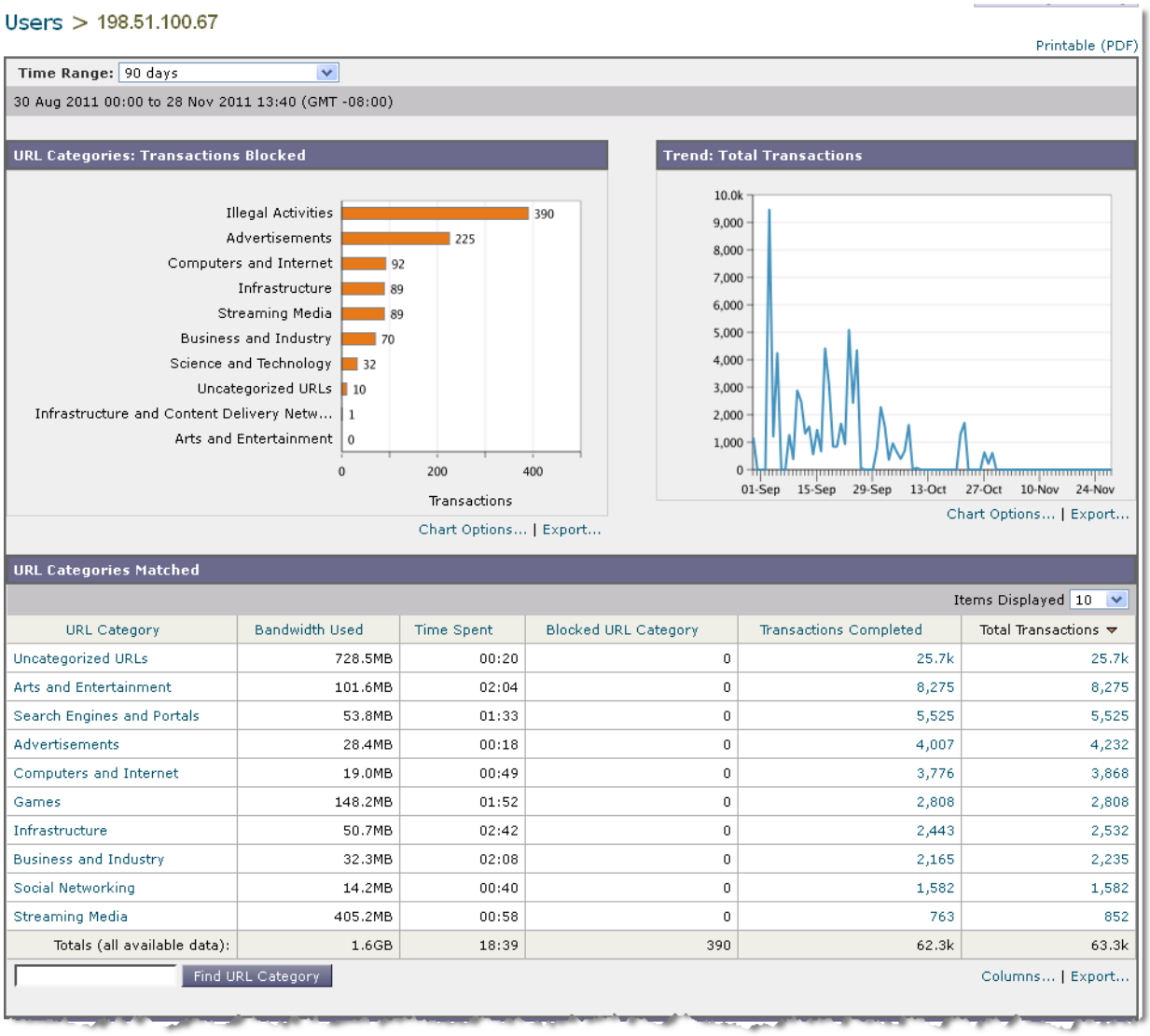
[User Details] ページ

[User Details] ページでは、[Web] > [Reporting] > [Users] ページのインタラクティブな [Users] テーブルで指定したユーザに関する具体的な情報を確認できます。

[User Details] ページでは、システムでの個々のユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。

特定のユーザの [User Details] ページを表示するには、[Web] > [Users] ページの [User] テーブルで対象のユーザをクリックします。

図 5-5　[User Details] ページ



（次のページに続く）

（前ページからの続き）

Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted].com	713.4MB	00:29	24.5k	0	24.5k
[redacted].com	92.4MB	02:02	8,037	0	8,037
[redacted].com	31.2MB	00:38	3,095	0	3,095
[redacted].com	1.7MB	00:56	179	1,769	1,948
[redacted].com	3.7MB	00:00	1,841	0	1,841
[redacted].com	2.4MB	02:12	1,539	80	1,619
[redacted].tv	12.6MB	00:03	1,033	0	1,033
[redacted].net	10.5MB	00:00	1,001	0	1,001
[redacted].com	46.5KB	00:57	4	898	902
[redacted].com	8.8MB	00:09	778	0	778

Find Domain or IP　　Columns... | Export...

Applications Matched

Items Displayed 10

Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions
[redacted]	Internet Utilities	3.7MB	1,832	0	1,832
[redacted] Video	Media	380.6MB	1,517	0	1,517
[redacted] General	[redacted]	10.2MB	1,283	0	1,283
[redacted]	Media	274.2MB	517	0	517
[redacted]	Instant Messaging	337.3KB	95	0	95
[redacted]	Webmail	1.4MB	68	0	68
[redacted] Mail	Webmail	425.8KB	61	0	61
[redacted]	Social Networking	364.5KB	58	0	58
[redacted] Photos	[redacted]	2.2MB	54	0	54
[redacted]	Media	157.6MB	40	0	40
Totals (all available data):	--	832.1MB	5,621	0	5,621

Find Application　　Columns... | Export...

Malware Threats Detected

Malware Threat	Malware Category	Bandwidth Saved by Blocking	Transactions Monitored	Transactions Blocked	Total Malware Transactions Detected
[redacted]	Adware	0B	82	0	82
[redacted]	Adware	0B	8	0	8
[redacted]	Trojan Horse	36.0KB	0	3	3
Totals (all available data):	--	36.0KB	90	3	93

Find Malware Threat　　Columns... | Export...

Policies Matched

Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions
Policy 1	Access	1.6GB	62.2k	1,174	63.4k
Policy 2	Access	0B	0	2,667	2,667
Policy 3	Decryption	768.3KB	91	0	91
Totals (all available data):	--	1.6GB	62.3k	3,841	66.1k

Find Policy Name　　Columns... | Export...

[User Details] ページには、システム上の個々のユーザに関係する次の情報が表示されます。

表 5-6　[Web] > [Reporting] > [User] > [User Details] 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）	レポートに含めるデータの時間範囲を選択できるメニュー。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.3-4）を参照してください。
URL Categories by Total Transactions	このセクションには、特定のユーザが使用している特定の URL カテゴリのリストが表示されます。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。
Trend by Total Transactions	このグラフには、ユーザが Web にいつアクセスしたかが表示されます。 たとえば、1 日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。[Time Range] ドロップダウン リストを使用すると、このグラフを拡張し、このユーザが Web を閲覧していた時間を表示するきめ細かさを増減できます。
URL Categories Matched	[URL Categories Matched] セクションには、完了したトランザクションとブロックされたトランザクションの両方について、一致したカテゴリが表示されます。 このセクションでは、特定の URL カテゴリを検索することもできます。セクション下部のテキスト フィールドに URL カテゴリを入力し、[Find URL Category] をクリックします。カテゴリは正確に一致している必要はありません。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。
Domains Matched	このセクションでは、このユーザがアクセスした特定のドメインまたは IP アドレスを確認できます。また、ユーザがこれらのカテゴリで費やした時間、およびカラム ビューで設定したその他のさまざまな情報も参照できます。セクション下部のテキスト フィールドにドメインまたは IP アドレスを入力し、[Find Domain or IP] をクリックします。ドメインまたは IP アドレスは正確に一致している必要はありません。
Applications Matched	このセクションでは、特定のユーザが使用している特定のアプリケーションを検索できます。たとえば、Flash ビデオを多用するサイトにユーザがアクセスしている場合は、[Application] カラムにそのアプリケーション タイプが表示されます。 セクション下部のテキスト フィールドにアプリケーション名を入力し、[Find Application] をクリックします。アプリケーションの名前は正確に一致している必要はありません。

表 5-6　[Web] > [Reporting] > [User] > [User Details] ページの詳細（続き）

セクション	説明
Malware Threats Detected	このテーブルでは、特定のユーザがトリガーしている上位のマルウェア脅威を確認できます。 特定のマルウェア脅威の名前に関するデータを [Find Malware Threat] フィールドで検索できます。マルウェア脅威の名前を入力し、[Find Malware Threat] をクリックしてください。マルウェア脅威の名前は正確に一致している必要はありません。
Policies Matched	このセクションでは、Web にアクセスする際にこのユーザに適用されるポリシー グループを検索できます。 セクション下部のテキスト フィールドにポリシー名を入力し、[Find Policy] をクリックします。ポリシーの名前は正確に一致している必要はありません。

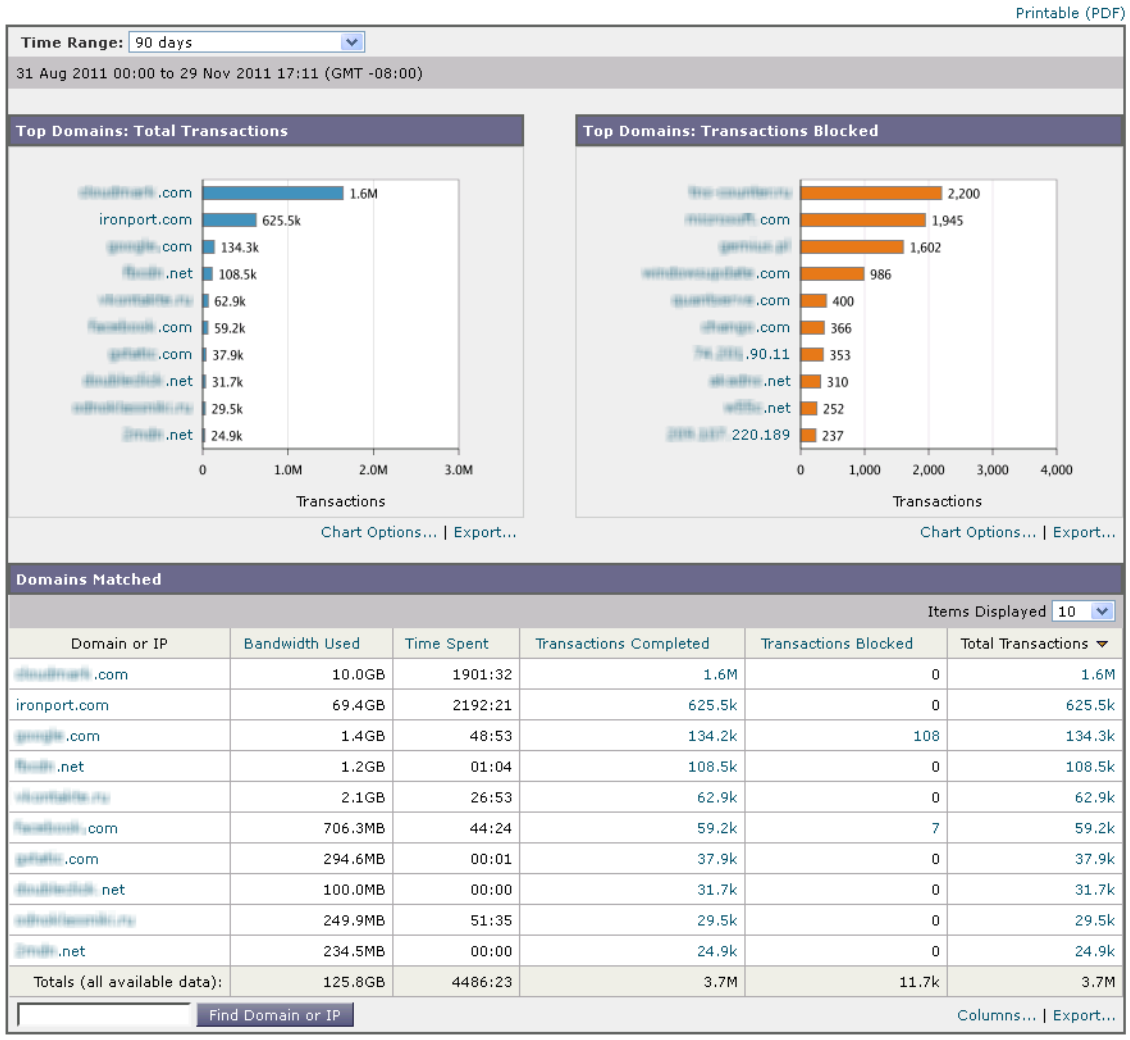
（注）　[Client Malware Risk Details] テーブルのクライアント レポートでは、ユーザ名の末尾にアスタリスク（*）が付いていることがあります。たとえば、クライアント レポートに「jsmith」と「jsmith*」の両方のエントリが表示される場合があります。アスタリスク（*）が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

[Users Details] ページの使用例については、「例 1：ユーザの調査」（P.D-1）を参照してください。

[Web Sites] ページ

[Web] > [Reporting] > [Web Sites] ページでは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。

図 5-6　[Web Sites] ページ



[Web Sites] ページには次の情報が表示されます。

表 5-7　[Web] > [Reporting] > [Web Sites] 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.3-4）を参照してください。
Top Domains by Total Transactions	このセクションには、サイト上でアクセスされた上位ドメインがグラフ形式で表示されます。

表 5-7　[Web] > [Reporting] > [Web Sites] ページの詳細（続き）

セクション	説明
Top Domains by Transactions Blocked	このセクションには、トランザクションごとに発生するブロック アクションをトリガーした上位ドメインが、グラフ形式で表示されます。たとえば、ユーザがあるドメインにアクセスしたが、特定のポリシーが適用されていたために、ブロック アクションがトリガーされたとします。このドメインはブロックされたトランザクションとしてこのグラフに追加され、ブロック アクションをトリガーしたドメイン サイトが表示されます。
Domains Matched	このセクションでは、サイト上でアクセスされたドメインがインタラクティブなテーブルに表示されます。このテーブルでは、特定のドメインをクリックすることで、そのドメインに関するさらに詳細な情報にアクセスできます。[Web Tracking] ページに [Proxy Services] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。 このテーブルのデータの詳細については、「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。 特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。 Web トラッキングの使用例については、「例 2：URL のトラッキング」（P.D-5）を参照してください。

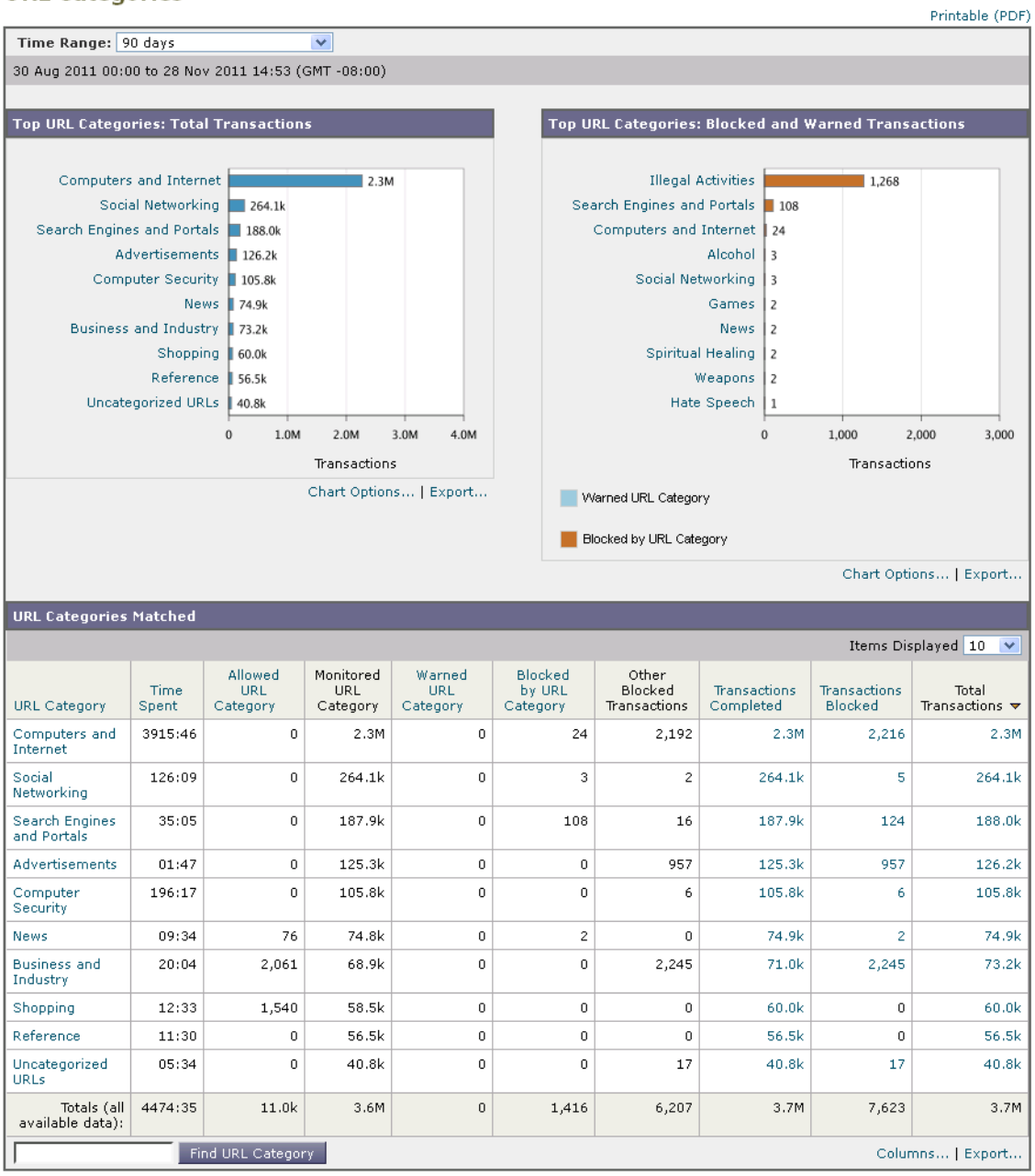
ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）　[Web Sites] ページの情報について、レポートを生成またはスケジュールすることができます。詳細については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

[URL Categories] ページ

[Web] > [Reporting] > [URL Categories] ページを使用して、システム上のユーザがアクセスしているサイトの URL カテゴリを表示できます。

図 5-7　[URL Categories] ページ



URL Category	Time Spent	Allowed URL Category	Monitored URL Category	Warned URL Category	Blocked by URL Category	Other Blocked Transactions	Transactions Completed	Transactions Blocked	Total Transactions
Computers and Internet	3915:46	0	2.3M	0	24	2,192	2.3M	2,216	2.3M
Social Networking	126:09	0	264.1k	0	3	2	264.1k	5	264.1k
Search Engines and Portals	35:05	0	187.9k	0	108	16	187.9k	124	188.0k
Advertisements	01:47	0	125.3k	0	0	957	125.3k	957	126.2k
Computer Security	196:17	0	105.8k	0	0	6	105.8k	6	105.8k
News	09:34	76	74.8k	0	2	0	74.9k	2	74.9k
Business and Industry	20:04	2,061	68.9k	0	0	2,245	71.0k	2,245	73.2k
Shopping	12:33	1,540	58.5k	0	0	0	60.0k	0	60.0k
Reference	11:30	0	56.5k	0	0	0	56.5k	0	56.5k
Uncategorized URLs	05:34	0	40.8k	0	0	17	40.8k	17	40.8k
Totals (all available data):	4474:35	11.0k	3.6M	0	1,416	6,207	3.7M	7,623	3.7M

[URL Categories] ページには次の情報が表示されます。

表 5-8　[Web] > [Reporting] > [URL Categories] 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）	レポートの時間範囲を選択します。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。
Top URL Categories by Total Transactions	このセクションには、サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。

表 5-8　[Web] > [Reporting] > [URL Categories] ページの詳細（続き）

セクション	説明
Top URL Categories by Blocked and Warned Transactions	このセクションには、トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロック アクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
URL Categories Matched	[URL Categories Matched] セクションには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。 未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。 • 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループ ポリシーに適用できます。詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Custom URL Categories」を参照してください。 • 既存またはその他のカテゴリに含めるべきサイトについては、「誤って分類された URL と未分類の URL のレポート」（P.5-29）を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）
- このページよりもさらに詳細なレポートを生成するには、「Top URL Categories — Extended」（P.5-65）を参照してください。
- URL カテゴリに関するスケジュール設定されたレポート内でデータ アベイラビリティが使用されている場合に、いずれかのアプライアンスでデータに欠落があると、ページの下部に「`Some data in this time range was unavailable.`」というメッセージが表示されます。欠落がない場合は何も表示されません。

URL カテゴリ セットの更新とレポート

「URL カテゴリ セットの更新と中央集中型コンフィギュレーション管理」（P.8-23）で説明されているように、セキュリティ管理アプライアンスでは一連の定義済み URL カテゴリが定期的に更新される場合があります。

これらの更新が行われた場合、古いカテゴリのデータは、古すぎて価値がなくなるまで、引き続きレポートと Web トラッキング結果に表示されます。カテゴリ セットの更新後に生成されたレポート データには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

古いカテゴリと新しいカテゴリの間で重複した箇所がある場合、有効な統計情報を得るために、より注意深くレポート結果を検証する必要が生じることがあります。たとえば、調査対象のタイム フレーム内に「Instant Messaging」カテゴリと「Web-based Chat」カテゴリが「Chat and Instant Messaging」という 1 つのカテゴリにマージされていた場合、「Instant Messaging」および「Web-based Chat」カテゴリに対応するサイトへのマージ前のアクセスは「Chat and Instant Messaging」の合計数にカウントされません。同様に、インスタント メッセージング サイトまたは Web ベース チャット サイトへのマージ後のアクセスは、「Instant Messaging」または「Web-based Chat」カテゴリの合計数には含まれません。

[URL Categories] ページとその他のレポーティング ページの併用

[URL Categories] ページと [Application Visibility] ページおよび [Users] ページを併用すると、特定のユーザと、特定のユーザがアクセスしようとしているアプリケーション タイプまたは Web サイトを調査できます。

たとえば、[URL Categories] ページで、サイトからアクセスされたすべての URL カテゴリの詳細を表示する、人事部門向けの概要レポートを生成できます。同じページの [URL Categories] インタラクティブ テーブルでは、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[Streaming Media] カテゴリ リンクをクリックすると、特定の [URL Categories] レポート ページが表示されます。このページには、ストリーミング メディア サイトにアクセスしている上位ユーザが表示されるだけでなく（[Top Users by Category for Total Transactions] セクション）、YouTube.com や QuickPlay.com などのアクセスされたドメインも表示されます（[Domains Matched] インタラクティブ テーブル）。

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているので、そのユーザのアクセス先を正確に確認する必要があるとします。ここから、[Users] インタラクティブ テーブルのユーザをクリックすることができます。このアクションにより [User Details] ページが表示され、そのユーザのトレンドを確認し、そのユーザの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [Transactions Completed] リンクをクリックして、Web トラッキングの詳細を表示できます。これにより、[Web Tracking] ページに [Proxy Services] タブが表示され、ユーザがサイトにアクセスした日付、完全な URL、その URL で費やされた時間などについて、実際の詳細情報を確認できます。

[URL Categories] ページの他の使用例については、「例 3：アクセス数の多い URL カテゴリの調査」（P.D-6）を参照してください。

誤って分類された URL と未分類の URL のレポート

誤って分類された URL と未分類の URL について、次の URL で報告できます。

https://securityhub.cisco.com/web/submit_urls

送信内容は評価され、今後のルール更新に活用されます。

送信された URL のステータスを確認するには、このページの [Status on Submitted URLs] タブをクリックします。

[Application Visibility] ページ

（注）　[Application Visibility] の詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Understanding Application Visibility and Control」を参照してください。

[Web] > [Reporting] > [Application Visibility] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内の特定のアプリケーション タイプに制御を適用できます。

アプリケーション制御を使用すると、URL フィルタリングのみを使用する場合よりも Web トラフィックをきめ細かく制御できるだけでなく、次のタイプのアプリケーションおよびアプリケーション タイプの制御を強化できます。

- 回避アプリケーション（アノニマイザや暗号化トンネルなど）。
- コラボレーション アプリケーション（Cisco WebEx、Facebook、インスタント メッセージングなど）。
- リソースを大量消費するアプリケーション（ストリーミング メディアなど）。

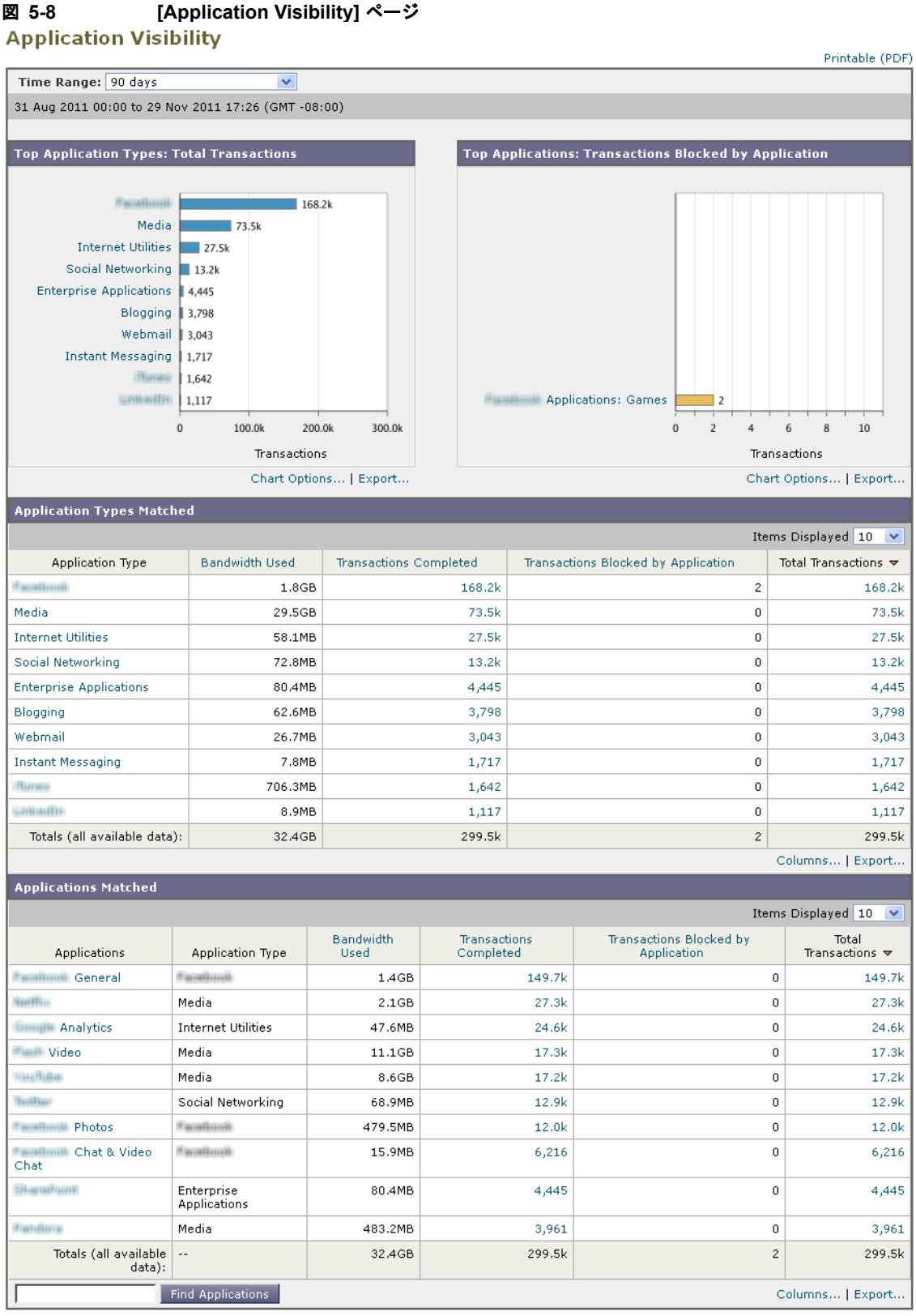
アプリケーションとアプリケーション タイプの違いについて

レポートに関連するアプリケーションを制御するには、アプリケーションとアプリケーション タイプの違いを理解することが非常に重要です。

- **アプリケーション タイプ。**1 つまたは複数のアプリケーションを含むカテゴリです。たとえば**検索エンジン**は、Google Search や Craigslist などの検索エンジンを含むアプリケーション タイプです。インスタント メッセージングは、Yahoo Instant Messenger や Cisco WebEx などを含む別のアプリケーション タイプです。Facebook もアプリケーション タイプです。
- **アプリケーション。**アプリケーション タイプに属している特定のアプリケーションです。たとえば、YouTube はメディア アプリケーション タイプに含まれるアプリケーションです。
- **アプリケーション動作。**アプリケーション内でユーザが実行できる特定のアクションまたは動作です。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション動作が含まれているわけではありません。

（注）　Application Visibility and Control（AVC）エンジンを使用して Facebook アクティビティを制御する方法の詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Understanding Application Visibility and Control」を参照してください。

図 5-8　[Application Visibility] ページ



[Application Visibility] ページには次の情報が表示されます。

表 5-9　[Web] > [Reporting] > [Application Visibility] 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.3-4）を参照してください。
Top Application Types by Total Transactions	このセクションには、サイト上でアクセスされた上位アプリケーション タイプがグラフ形式で表示されます。たとえば、Yahoo Instant Messenger などのインスタント メッセージング ツール、Facebook、Presentation というアプリケーション タイプが表示されます。
Top Applications by Blocked Transactions	このセクションには、トランザクションごとに発生するブロック アクションをトリガーした上位アプリケーション タイプがグラフ形式で表示されます。たとえば、ユーザが Google Talk や Yahoo Instant Messenger などの特定のアプリケーション タイプを起動しようとしたが、特定のポリシーが適用されているために、ブロック アクションがトリガーされたとします。このアプリケーションは、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
Application Types Matched	[Application Types Matched] インタラクティブ テーブルでは、[Top Applications Type by Total Transactions] テーブルに表示されているアプリケーション タイプに関するさらに詳しい情報を表示できます。[Applications] カラムで、詳細を表示するアプリケーションをクリックできます。
Applications Matched	[Applications Matched] セクションには、指定した時間範囲内のすべてのアプリケーションが表示されます。これはインタラクティブなカラム見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。 [Applications Matched] セクションに表示するカラムを設定することができます。このセクションのカラムの設定については、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。 [Applications] テーブルに表示する項目を選択後、表示する項目の数を [Items Displayed] ドロップダウン メニューから選択できます。選択肢は [10]、[20]、[50]、[100] です。 さらに、[Application Matched] セクション内で特定のアプリケーションを検索できます。このセクション下部のテキスト フィールドに特定のアプリケーション名を入力し、[Find Application] をクリックします。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）　[Application Visibility] ページの情報に関して、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

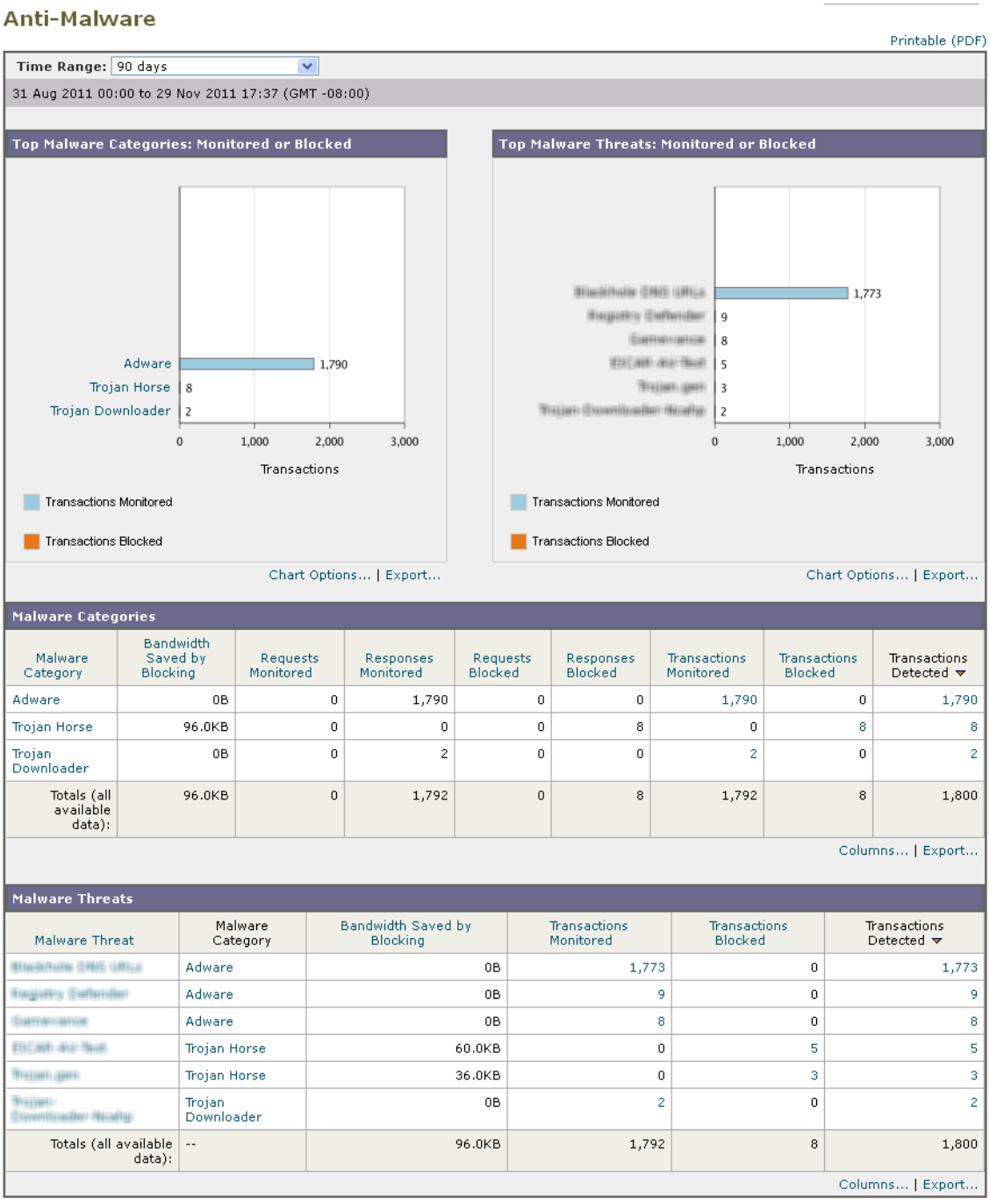
[Anti-Malware] ページ

[Web] > [Reporting] > [Anti-Malware] ページはセキュリティ関連のレポーティング ページであり、イネーブルなスキャン エンジン（Webroot、Sophos、McAfee、または Adaptive Scanning）によるスキャン結果が反映されます。

このページを使用して、Web ベースのマルウェアの脅威を特定およびモニタすることができます。

（注）　L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、「[L4 Traffic Monitor] ページ」（P.5-44）を参照してください。

図 5-9　[Anti-Malware] ページ



[Anti-Malware] ページには次の情報が表示されます。

表 5-10　[Web] > [Reporting] > [Anti-Malware] 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.3-4）を参照してください。
Top Malware Categories: Monitored or Blocked	このセクションには、所定のカテゴリ タイプによって検出された上位マルウェア カテゴリが表示されます。この情報はグラフ形式で表示されます。有効なマルウェア カテゴリの詳細については、表 5-10（P.5-38）を参照してください。
Top Malware Threats: Monitored or Blocked	このセクションには、上位のマルウェアの脅威が表示されます。この情報はグラフ形式で表示されます。
Malware Categories	[Malware Categories] インタラクティブ テーブルには、[Top Malware Categories] チャートに表示されている個々のマルウェア カテゴリに関する詳細情報が表示されます。 [Malware Categories] インタラクティブ テーブル内のリンクをクリックすると、個々のマルウェア カテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。 例外：このテーブルの [Outbreak Heuristics] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。 有効なマルウェア カテゴリの詳細については、表 5-10（P.5-38）を参照してください。
Malware Threats	[Malware Threats] インタラクティブ テーブルには、[Top Malware Threats] セクションに表示されている個々のマルウェアの脅威に関する詳細情報が表示されます。 「Outbreak」のラベルと番号が付いている脅威は、他のスキャン エンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。 **（注）** [Malware Threat] でテーブルを昇順にソートすると、リストの最上部に [Unnamed Malware] が表示されます。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Malware Category] レポート ページ

[Malware Category] レポート ページでは、個々のマルウェア カテゴリとネットワークでのその動作に関する詳細情報を表示できます。

[Malware Category] レポート ページにアクセスするには、次の手順を実行します。

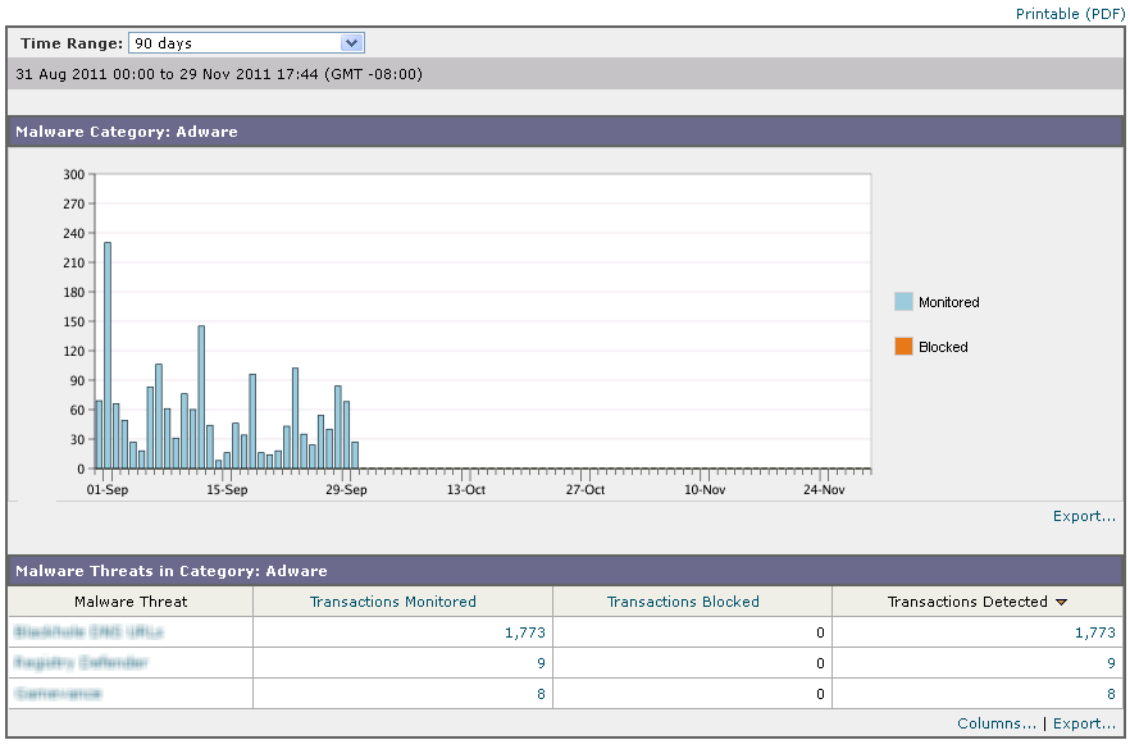
ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[Anti-Malware] ページが表示されます。

ステップ 2　[Malware Categories] インタラクティブ テーブルで、[Malware Category] カラム内のカテゴリをクリックします。

[Malware Category] レポート ページが表示されます。

図 5-10　[Malware Category] レポート ページ



ステップ 3　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Malware Threat] レポート ページ

[Malware Threat] レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[Client Detail] ページへのリンクがあります。レポート上部のトレンド グラフには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニタされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

[Malware Threat] レポート ページにアクセスするには、次の手順を実行します。

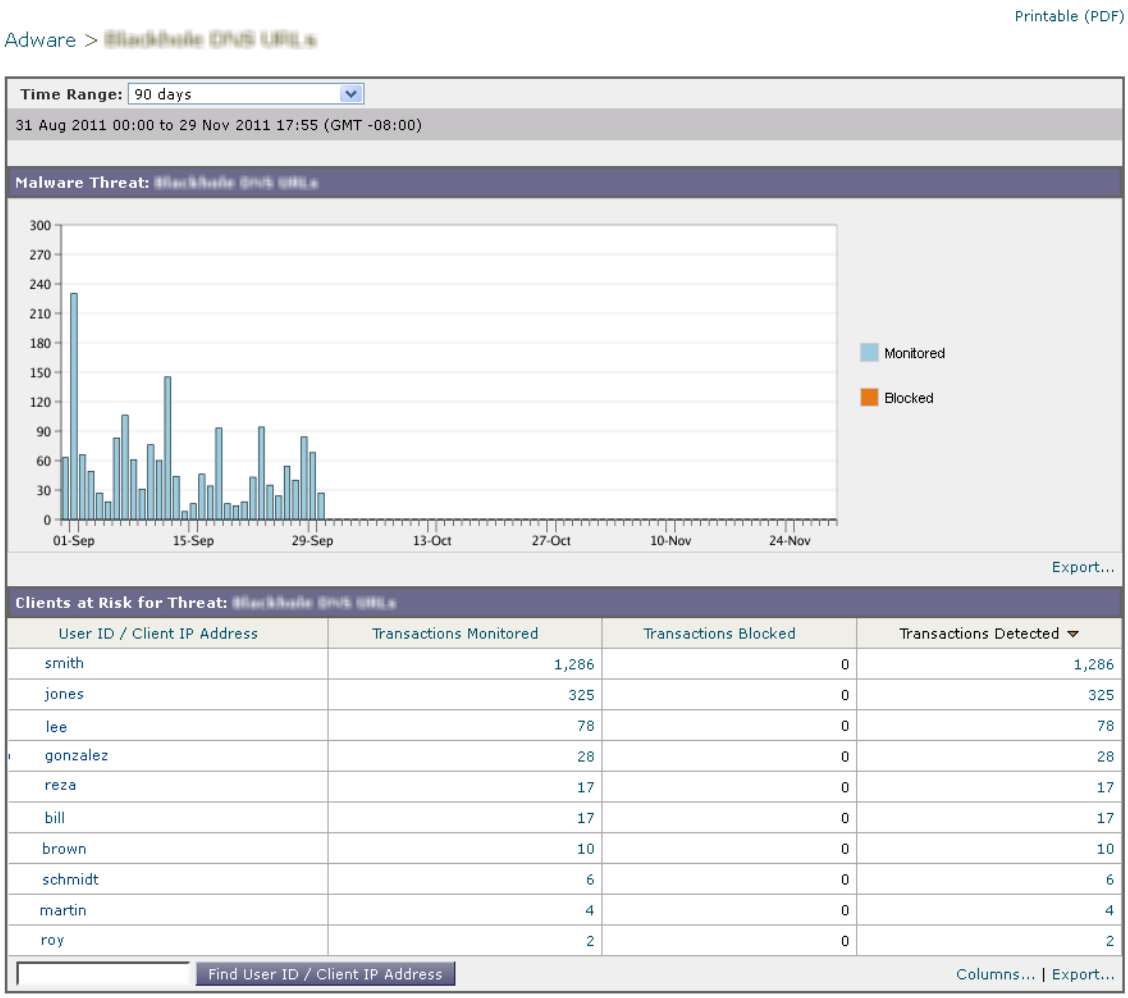
ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[Anti-Malware] ページが表示されます。

ステップ 2　[Malware Threat] インタラクティブ テーブルで、[Malware Category] カラム内のカテゴリをクリックします。

[Malware Threat] レポート ページが表示されます。

図 5-11　[Malware Threat] レポート ページ



ステップ 3　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

ステップ 4　詳細については、テーブルの下の [Support Portal Malware Details] リンクをクリックしてください。

（注）　[Anti-Malware] ページの [Top Malware Categories Detected] および [Top Malware Threats Detected] に関して、スケジュール設定されたレポートを生成することができます。ただし、[Malware Categories] および [Malware Threats] レポート ページから生成されるレポートを、スケジュール設定することはできません。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

マルウェアのカテゴリについて

次の表に、Web セキュリティ アプライアンスでブロックできるさまざまなマルウェアのカテゴリを示します

マルウェアのカテゴリについて

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャル エンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモート ホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。

マルウェアのカテゴリについて（続き）

マルウェアのタイプ	説明
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

[Client Malware Risk] ページ

[Web] > [Reporting] > [Client Malware Risk] ページは、クライアント マルウェア リスク アクティビティをモニタするために使用できるセキュリティ関連のレポーティング ページです。

[Client Malware Risk] ページでは、システム管理者が最も多くブロックまたは警告を受けているユーザを確認できます。このページで収集された情報から、管理者はユーザ リンクをクリックして、そのユーザが多数のブロックや警告を受けている原因、およびネットワーク上の他のユーザよりも多く検出されている原因となっているユーザの行動を確認できます。

さらに [Client Malware Risk] ページには、L4 トラフィック モニタ（L4TM）によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。マルウェア サイトに頻繁に接続するコンピュータは、マルウェアに感染している可能性があります。これらのマルウェアは中央のコマンド/コントロール サーバに接続しようとするので、除去しなければなりません。

図 5-12 に [Client Malware Risk] ページを示します。

図 5-12　[Client Malware Risk] ページ

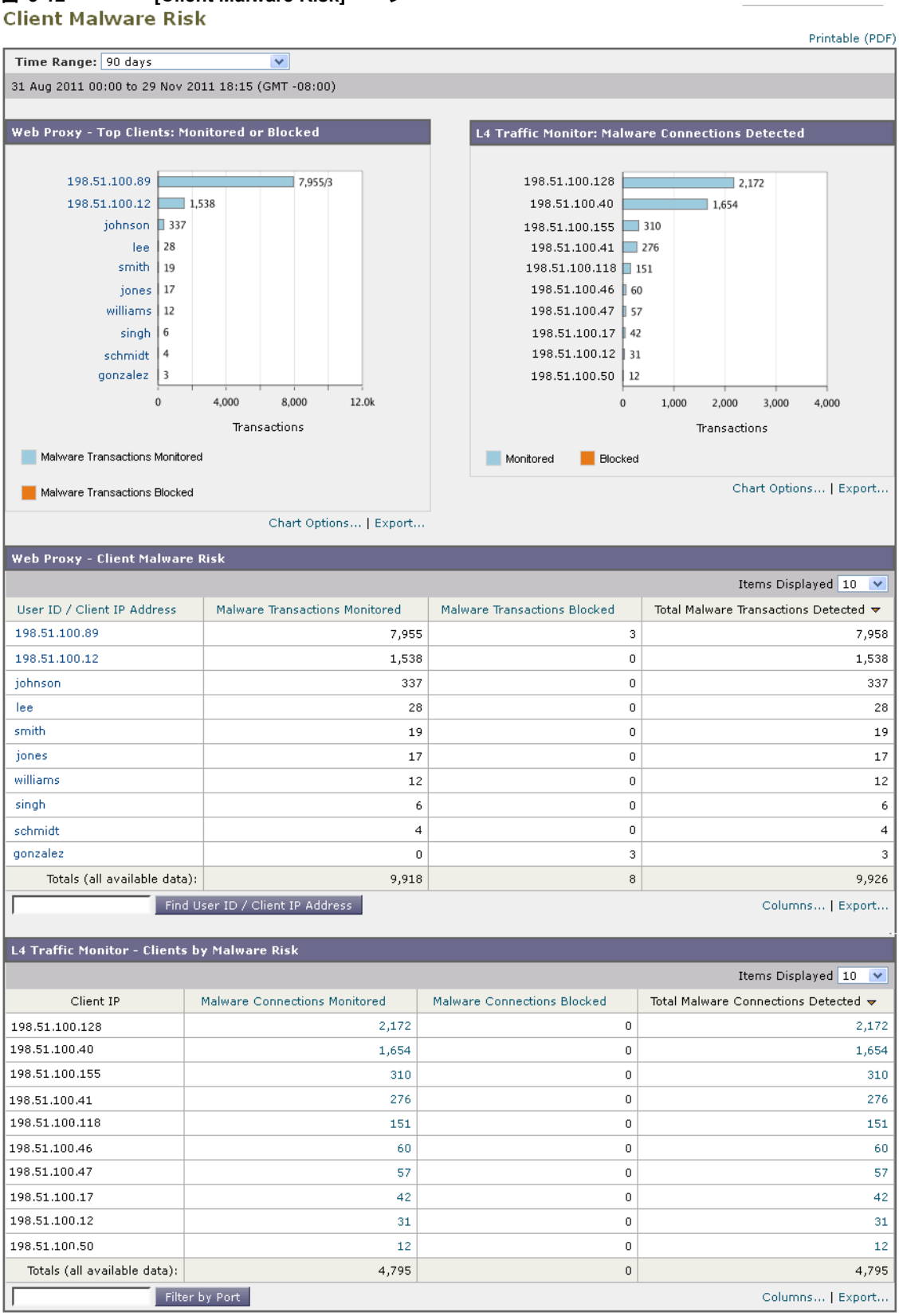


表 5-11 で [Client Malware Risk] ページの情報について説明します。

表 5-11　[Client Malware Risk] レポート ページの内容

セクション	説明
Time Range（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。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 Proxy: Top Clients Monitored or Blocked	このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。
L4 Traffic Monitor: Malware Connections Detected	このチャートには、組織内で最も頻繁にマルウェア サイトに接続している 10 台のコンピュータの IP アドレスが表示されます。 このチャートは「[L4 Traffic Monitor] ページ」（P.5-44）の [Top Client IPs] チャートと同じです。詳細およびチャート オプションについてはこの項を参照してください。
Web Proxy: Client Malware Risk	[Web Proxy: Client Malware Risk] テーブルには、[Web Proxy: Top Clients by Malware Risk] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。 このテーブルで各ユーザをクリックすると、そのクライアントに関連する [User Details] ページが表示されます。このページの詳細については、「[User Details] ページ」（P.5-20）を参照してください。 テーブルで任意のリンクをクリックすると、個々のユーザと、マルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。たとえば [User ID / Client IP Address] カラムのリンクをクリックすると、そのユーザの [User] ページに移動します。
L4 Traffic Monitor: Clients by Malware Risk	このテーブルには、組織内でマルウェア サイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。 このテーブルは「[L4 Traffic Monitor] ページ」（P.5-44）の [Client Source IPs] テーブルと同じです。テーブルの操作についてはこの項を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

[Web Reputation Filters] ページ

[Web] > [Reporting] > [Web Reputation Filters] は、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ（ユーザが設定）の結果を表示する、セキュリティ関連のレポーティング ページです。

Web レピュテーション フィルタとは

Web レピュテーション フィルタは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーション スコアを URL に割り当てます。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらす URL ベースのマルウェアを防ぐために役立ち

ます。Web セキュリティ アプライアンスは、URL レピュテーション スコアを使用して、疑わしいアクティビティを特定するとともに、マルウェア攻撃を未然に防ぎます。Web レピュテーション フィルタは、アクセス ポリシーと復号化ポリシーの両方と組み合わせて使用できます。

Web レピュテーション フィルタでは、統計的に有意なデータを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば次のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

Web レピュテーション フィルタリングの詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Web Reputation Filters」を参照してください。

図 5-13　[Web Reputation Filters] ページ

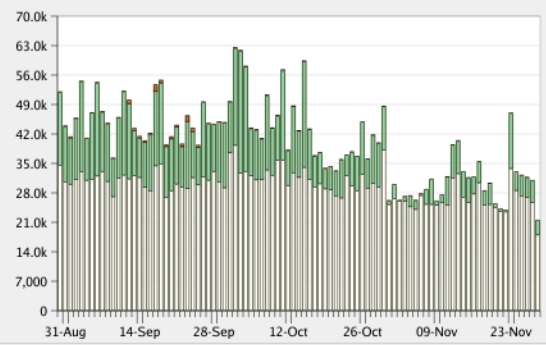
Web Reputation Filters

Printable (PDF)

Time Range: 90 days

30 Aug 2011 00:00 to 28 Nov 2011 15:20 (GMT -08:00)

Web Reputation Actions (Trend)



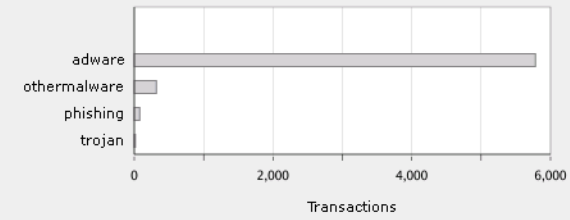
Export...

Web Reputation Actions (Volume)

Action	%	Transactions
Block	0.2%	6,197
Scan Further: Malware Detected	0.3%	10.0k
Scan Further: Clean	25.4%	927.4k
Allow	74.2%	2.7M
Total		**3.7M**

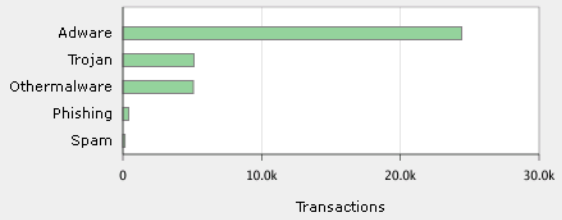
Export...

Web Reputation Threat Types by Blocked Transactions



Export...

Web Reputation Threat Types by Scanned Further Transactions



Export...

Web Reputation Actions (Breakdown by Score)

Score ▲	Block	Scan Further: Malware Detected	Scan Further: Clean	Allow
-10.0 ... -9.1	170	0	0	0
-9.0 ... -8.1	58	0	0	0
-8.0 ... -7.1	4,594	0	0	0
-7.0 ... -6.1	1,288	0	75	0
-6.0 ... -5.1	87	265	28.6k	0
-5.0 ... -4.1	0	414	4,208	0
-4.0 ... -3.1	0	5	10.7k	0
-3.0 ... -2.1	0	1,023	46.2k	0
-2.0 ... -1.1	0	179	17.9k	0
-1.0 ... -0.1	0	1,771	15.9k	0
0.0 ... 0.9	0	910	176.6k	0
1.0 ... 1.9	0	61	60.1k	0
2.0 ... 2.9	0	321	39.5k	0
3.0 ... 3.9	0	3,393	48.5k	0
4.0 ... 4.9	0	777	308.5k	0
5.0 ... 5.9	0	391	128.1k	0
6.0 ... 6.9	0	0	0	1.8M
7.0 ... 7.9	0	0	0	94.0k
8.0 ... 8.9	0	0	0	135.3k
9.0 ... 10.0	0	0	0	636.9k
No score	0	513	42.5k	0

Export...

[Web Reputation Filters] ページには次の情報が表示されます。

表 5-12　[Web] > [Reporting] > [Web Reputation Filters] 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.3-4）を参照してください。
Web Reputation Actions (Trend)	このセクションには、指定した時間（横方向の時間軸）に対する Web レピュテーション アクションの総数（縦方向の目盛り）が、グラフ形式で表示されます。このセクションでは、時間の経過に伴う Web レピュテーション アクションの潜在的なトレンドを確認できます。
Web Reputation Actions (Volume)	このセクションには、Web レピュテーション アクションのボリュームがトランザクション数の比率で表示されます。
Web Reputation Threat Types by Blocked Transactions	このセクションには、ブロックされた Web レピュテーション タイプが表示されます。
Web Reputation Threat Types by Scanned Further Transactions	Adaptive Scanning がイネーブルの場合、このセクションには脅威の可能性が検出されたトランザクションの数が表示されます。 Adaptive Scanning がイネーブルでない場合、このセクションにはブロックされたためにさらにスキャンを必要とする Web レピュテーション タイプが表示されます。Web レピュテーション フィルタリングの結果が「Scan Further」の場合、トランザクションはアンチマルウェア ツールに渡されて追加のスキャンが行われます。
Web Reputation Actions (Breakdown by Score)	Adaptive Scanning がイネーブルでない場合、このインタラクティブ テーブルには各アクションの Web レピュテーション スコアの内訳が表示されます。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーションの設定に関する詳細については、お使いの Cisco IronPort AsyncOS for Web Security のバージョンに対応するユーザ ガイドを参照してください。

[L4 Traffic Monitor] ページ

[Web] > [Reporting] > [L4 Traffic Monitor] ページはセキュリティ関連のレポーティング ページであり、指定した時間範囲内に L4 トラフィック モニタによって Web セキュリティ アプライアンス上で検出されたマルウェア ポートとマルウェア サイトに関する情報が表示されます。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

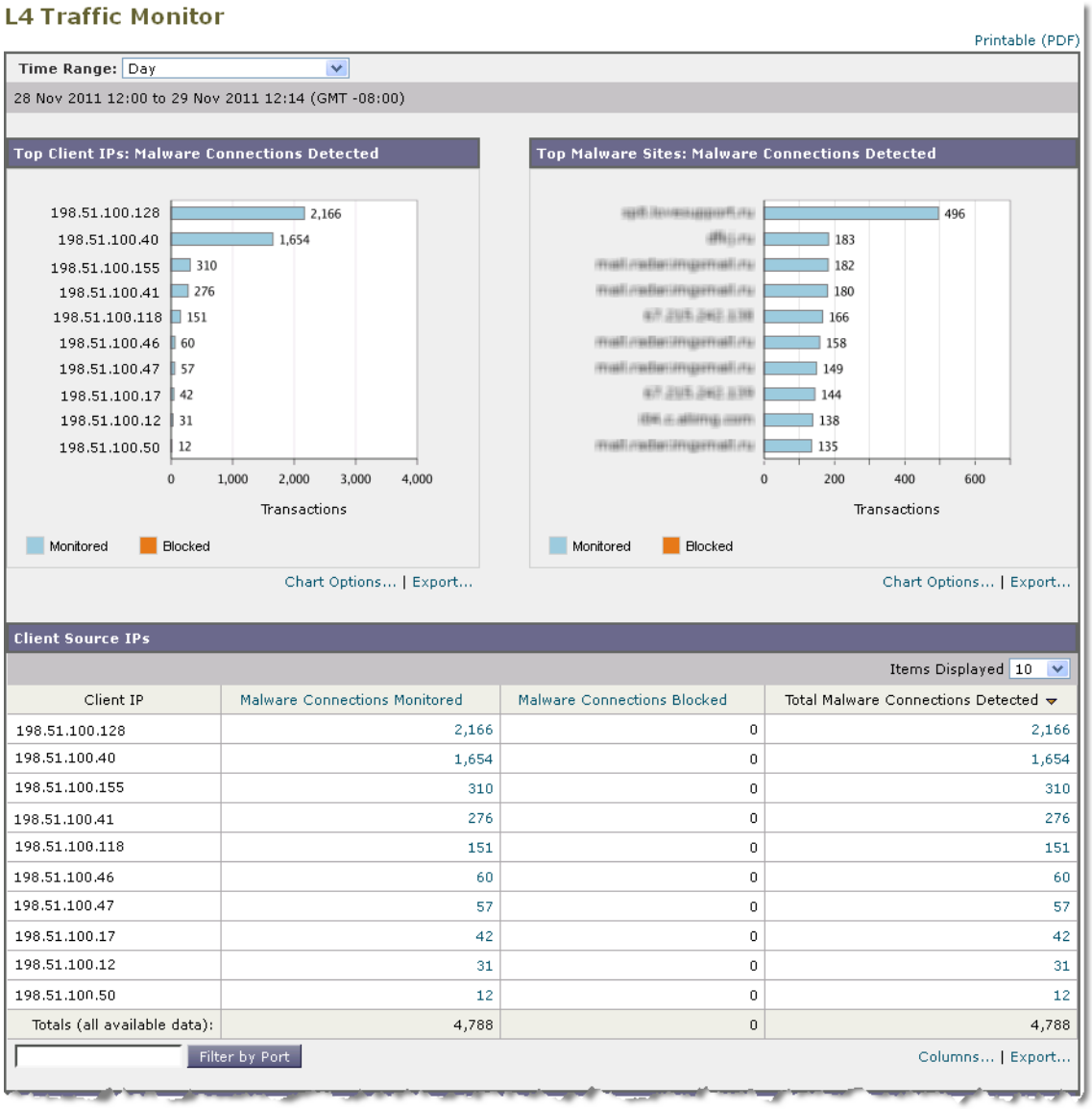
L4 トラフィック モニタは、各 Web セキュリティ アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベース テーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

このレポートのデータを使用して、ポートまたはサイトをブロックするかどうかを判断したり、特定のクライアント IP アドレスが著しく頻繁にマルウェア サイトに接続している理由（たとえば、その IP アドレスに関連付けられたコンピュータが、中央のコマンド/コントロール サーバに接続しようとするマルウェアに感染しているなど）を調査したりできます。

図 5-14 に [L4 Traffic Monitor] ページを示します。

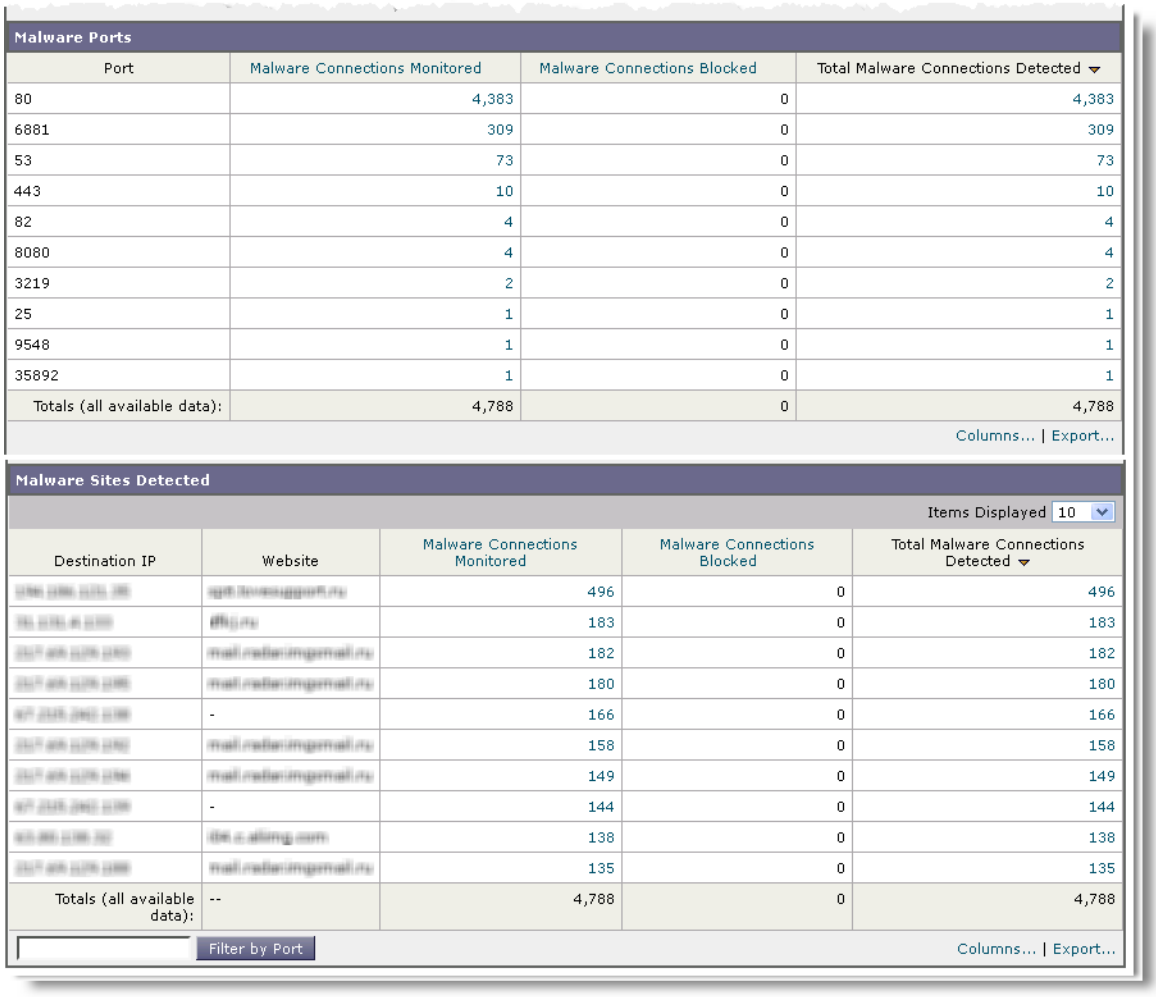
ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

図 5-14　[L4 Traffic Monitor] ページ



（次のページに続く）

（前ページからの続き）



Malware Ports

Port	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
80	4,383	0	4,383
6881	309	0	309
53	73	0	73
443	10	0	10
82	4	0	4
8080	4	0	4
3219	2	0	2
25	1	0	1
9548	1	0	1
35892	1	0	1
Totals (all available data):	4,788	0	4,788

Columns... | Export...

Malware Sites Detected

Items Displayed 10

Destination IP	Website	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
[redacted]	[redacted]	496	0	496
[redacted]	[redacted]	183	0	183
[redacted]	[redacted]	182	0	182
[redacted]	[redacted]	180	0	180
[redacted]	-	166	0	166
[redacted]	[redacted]	158	0	158
[redacted]	[redacted]	149	0	149
[redacted]	-	144	0	144
[redacted]	[redacted]	138	0	138
[redacted]	[redacted]	135	0	135
Totals (all available data):	--	4,788	0	4,788

Filter by Port

Columns... | Export...

表 5-13 で [L4 Traffic Monitor] ページに表示される情報を説明します。

表 5-13　[L4 Traffic Monitor] レポート ページの内容

セクション	説明
Time Range（ドロップダウン リスト）	レポート対象の時間範囲を選択できるメニュー。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。
Top Client IPs	このセクションには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。 チャートの下の [Chart Options] リンクをクリックすると、表示を総合的な [Malware Connections Detected] から [Malware Connections Monitored] または [Malware Connections Blocked] に変更できます。 このチャートは、「[Client Malware Risk] ページ」（P.5-39）の [L4 Traffic Monitor: Malware Connections Detected] と同じです。

表 5-13　[L4 Traffic Monitor] レポート ページの内容（続き）

セクション	説明
Top Malware Sites	このセクションには、L4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。 チャートの下の [Chart Options] リンクをクリックすると、表示を総合的な [Malware Connections Detected] から [Malware Connections Monitored] または [Malware Connections Blocked] に変更できます。
Client Source IPs	このテーブルには、組織内でマルウェア サイトに頻繁に接続しているコンピュータの IP アドレスが表示されます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[Filter by Port] をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェア サイトへ「誘導」しているかを判断できます。 各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリをクリックします。たとえば、ある特定のクライアント IP アドレスの [Malware Connections Blocked] が高い数値を示している場合、そのカラムの数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[Web] > [Reporting] > [Web Tracking] ページの [L4 Traffic Monitor] タブに検索結果として表示されます。リストの詳細については、「[L4 Traffic Monitor] タブ」（P.5-56）を参照してください。 このテーブルは、「[Client Malware Risk] ページ」（P.5-39）の [L4 Traffic Monitor: Clients by Malware Risk] テーブルと同じです。
Malware Ports	このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたポートが表示されます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[Total Malware Connections Detected] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[Web] > [Reporting] > [Web Tracking] ページの [L4 Traffic Monitor] タブに検索結果として表示されます。リストの詳細については、「[L4 Traffic Monitor] タブ」（P.5-56）を参照してください。
Malware Sites Detected	このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたドメインが表示されます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[Filter by Port] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[Malware Connections Blocked] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[Web] > [Reporting] > [Web Tracking] ページの [L4 Traffic Monitor] タブに検索結果として表示されます。リストの詳細については、「[L4 Traffic Monitor] タブ」（P.5-56）を参照してください。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

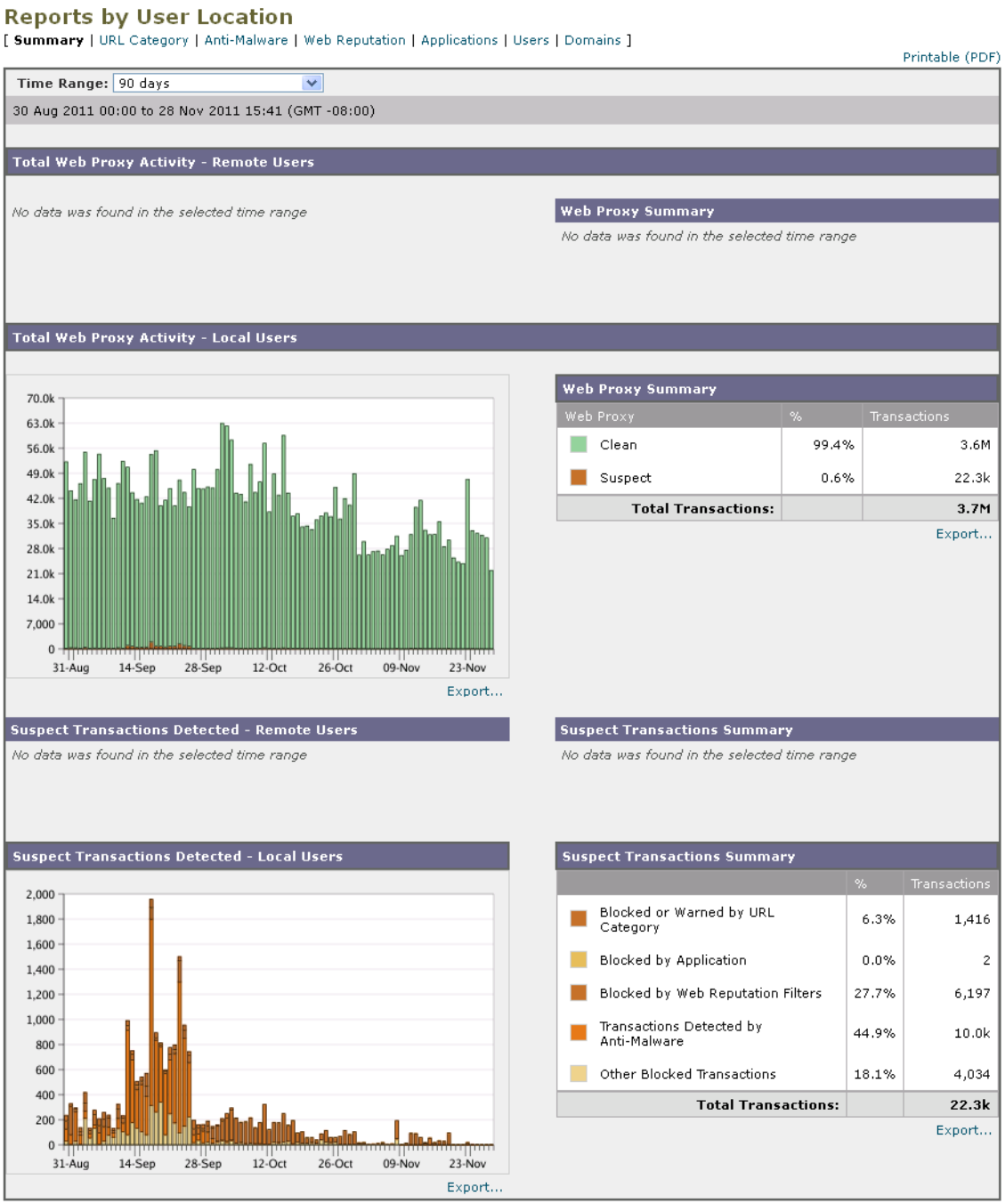
[Reports by User Location] ページ

[Web] > [Reporting] > [Reports by User Location] ページでは、モバイル ユーザがローカル システムまたはリモート システムから実行しているアクティビティを確認できます。

対象となるアクティビティは次のとおりです。

- ローカル ユーザおよびリモート ユーザがアクセスしている URL カテゴリ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザおよびリモート ユーザがアクセスしているアプリケーション。
- ユーザ（ローカルおよびリモート）。
- ローカル ユーザおよびリモート ユーザがアクセスしているドメイン。

図 5-15　[Reports by User Location] ページ



[Reports by User Location] ページには次の情報が表示されます。

表 5-14　[Web] > [Reporting] > [Reports by User Location] 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.3-4）を参照してください。
Total Web Proxy Activity: Remote Users	このセクションには、指定した時間（横方向）におけるリモート ユーザのアクティビティ（縦方向）が、グラフ形式で表示されます。
Web Proxy Summary	このセクションには、システム上のローカル ユーザとリモート ユーザのアクティビティの要約が表示されます。
Total Web Proxy Activity: Local Users	このセクションには、指定した時間（横方向）におけるリモート ユーザのアクティビティ（縦方向）が、グラフ形式で表示されます。
Suspect Transactions Detected: Remote Users	このセクションには、リモート ユーザに対して定義したアクセス ポリシーによって指定した時間内（横方向）に検出された疑わしいトランザクション（縦方向）が、グラフ形式で表示されます。
Suspect Transactions Summary	このセクションには、システム上のリモート ユーザの疑わしいトランザクションの要約が表示されます。
Suspect Transactions Detected: Local Users	このセクションには、リモート ユーザに対して定義したアクセス ポリシーによって指定した時間内（横方向）に検出された疑わしいトランザクション（縦方向）が、グラフ形式で表示されます。
Suspect Transactions Summary	このセクションには、システム上のローカル ユーザの疑わしいトランザクションの要約が表示されます。

[Reports by User Location] ページでは、ローカル ユーザとリモート ユーザのアクティビティを示すレポートを生成できます。これにより、ユーザのローカル アクティビティとリモート アクティビティを簡単に比較できます。

ヒント　このレポートのビューをカスタマイズするには、「インタラクティブ Web レポーティング ページの操作」（P.5-6）を参照してください。

（注）　[Reports by User Location] ページの情報について、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、「スケジュール設定されたレポートとオンデマンド Web レポートについて」（P.5-63）を参照してください。

[Web Tracking] ページ

[Web Tracking] ページを使用して、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を表示します。目的に応じて、次のタブのいずれかまたは両方で検索を行います。

- 「[Proxy Services] タブ」（P.5-52）
- 「[L4 Traffic Monitor] タブ」（P.5-56）

Web プロキシと L4 トラフィック モニタの違いについては、『*Cisco IronPort AsyncOS for Web Security User Guide*』の「Understanding How the Web Security Appliance Works」を参照してください。

[Proxy Services] タブ

[Web] > [Reporting] > [Web Tracking] ページの [Proxy Services] タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブル ユース適用コンポーネントから収集された Web トラッキング データを検索します。このデータに L4 トラフィック モニタリング データは含まれません。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。**所定の期間内の従業員に関するレポートを調査します。

  たとえば、[Proxy Services] タブを使用して、ユーザがアクセスしている特定の URL について、ユーザがアクセスした時刻や、それが許可された URL であるかどうか、といった情報を取得できます。

- **ネットワーク セキュリティ管理者。**会社のネットワークが従業員のスマートフォンを介してマルウェアの脅威にさらされていないかどうかを調査します。

所定の期間内に記録されたトランザクション（ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど）の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。

Web トラッキングの使用例については、「例 1：ユーザの調査」（P.D-1）を参照してください。

[Proxy Services] タブと他の Web レポーティング ページの併用例については、「[URL Categories] ページとその他のレポーティング ページの併用」（P.5-29）を参照してください。

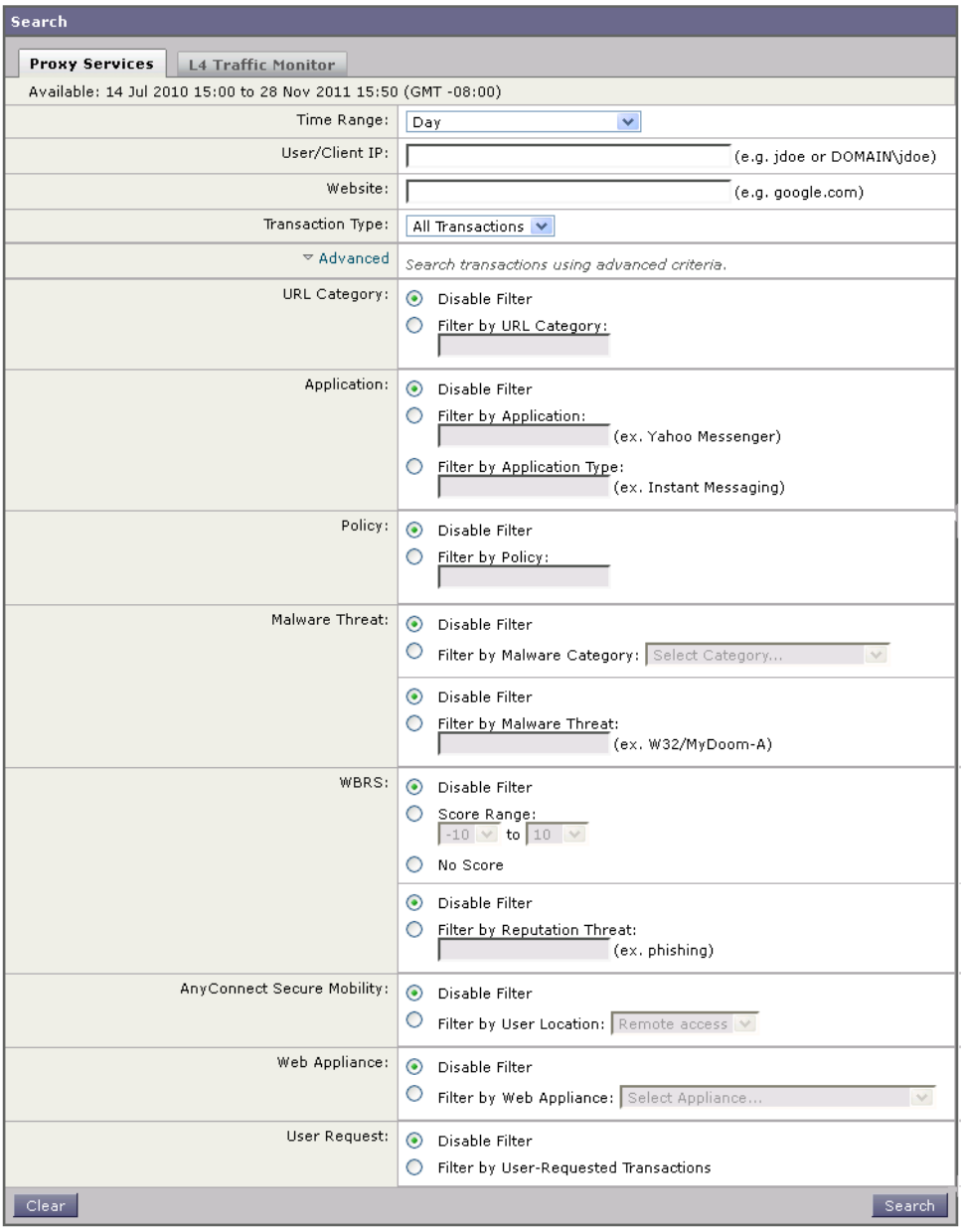
関心のある Web アクティビティのインスタンスを検索するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Tracking] を選択します。

ステップ 2　[Proxy Services] タブをクリックします。

ステップ 3　検索オプションとフィルタリング オプションをすべて表示するには、[Advanced] をクリックします。

図 5-16　[Web Tracking] ページの [Proxy Services] タブ



ステップ 4　検索条件を入力します。

表 5-15　[Proxy Services] タブの Web トラッキング検索条件

オプション	説明
デフォルトの検索条件	
時間範囲	レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで使用できる時間範囲については、「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。

表 5-15　[Proxy Services] タブの Web トラッキング検索条件 （続き）

オプション	説明
ユーザ / クライアント IP	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。
Web サイト	追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクション タイプ	追跡対象のトランザクションのタイプを [All Transactions]、[Completed]、[Blocked]、[Monitored]、または [Warned] から選択します。
高度な検索条件	
URL カテゴリ	URL カテゴリでフィルタリングするには、[Filter by URL Category] を選択し、フィルタリング対象とするカスタムまたは定義済み URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。 カスタム URL カテゴリの名前が定義済みカテゴリと同じ場合、または、システムの URL フィルタリング エンジンが変更されている場合、そのカテゴリに関連付けられた URL フィルタリング エンジン名は想定と異なる場合があります。ただし検索結果は、関連付けられたエンジンではなくカテゴリ名のみに基づきます。 一連の URL カテゴリが更新されると、一部のカテゴリに「Deprecated」のラベルが付けられる場合があります。これらのカテゴリは、少なくとも 1 つの管理対象 Web セキュリティ アプライアンスでの新しいトランザクションでは使用できなくなります。ただし、そのカテゴリが有効な間に発生した最近のトランザクションについては、引き続き検索を実行できます。URL カテゴリ セットの更新については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。 お使いの Web セキュリティ アプライアンスで、現在の URL フィルタリング エンジンとは別のエンジンを使用したことがある場合、非アクティブなエンジンのみに関連付けられたカテゴリに、それを示すラベルが付けられます。 ドロップダウン リストに表示されるエンジン名またはカテゴリ ステータスに関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。
アプリケーション	アプリケーションでフィルタリングするには、[Filter by Application] を選択し、フィルタリングに使用するアプリケーションを選択します。 アプリケーション タイプでフィルタリングするには、[Filter by Application Type] を選択し、フィルタリングに使用するアプリケーション タイプを選択します。

表 5-15　[Proxy Services] タブの Web トラッキング検索条件 （続き）

オプション	説明
ポリシー	ポリシー グループでフィルタリングするには、[Filter by Policy] を選択し、フィルタリングに使用するポリシー グループ名を入力します。 このポリシーが Web セキュリティ アプライアンスで宣言済みであることを確認してください。
マルウェアの脅威	特定のマルウェアの脅威でフィルタリングするには、[Filter by Malware Threat] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[Filter by Malware Category] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。
WBRS	[WBRS] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。 • Web レピュテーション スコアでフィルタリングするには、[Score Range] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[No Score] を選択すると、スコアがない Web サイトをフィルタリングできます。 • Web レピュテーションの脅威でフィルタリングするには、[Filter by Reputation Threat] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。 WBRS スコアの詳細については、『*Cisco IronPort AsyncOS for Web Security User Guide*』を参照してください。
AnyConnect セキュア モビリティ	リモートまたはローカル アクセスでフィルタリングするには、[Filter by User Location] を選択し、アクセス タイプを選択します。すべてのアクセス タイプを含めるには、[Disable Filter] を選択します (旧リリースでは、このオプションは Mobile User Security と呼ばれていました。
ユーザ要求	ユーザによって実際に開始されたトランザクションでフィルタリングするには、[Filter by User-Requested Transactions] を選択します。 （注）このフィルタをイネーブルにすると、検索結果には「最良の推測」トランザクションが含まれます。
Web アプライアンス	特定の Web アプライアンスでフィルタリングするには、[Filter by Web Appliance] の横のオプション ボタンをクリックし、テキスト フィールドに Web アプライアンス名を入力します。 [Disable Filter] を選択すると、検索にはセキュリティ管理アプライアンスに関連付けられたすべての Web セキュリティ アプライアンスが含まれます。

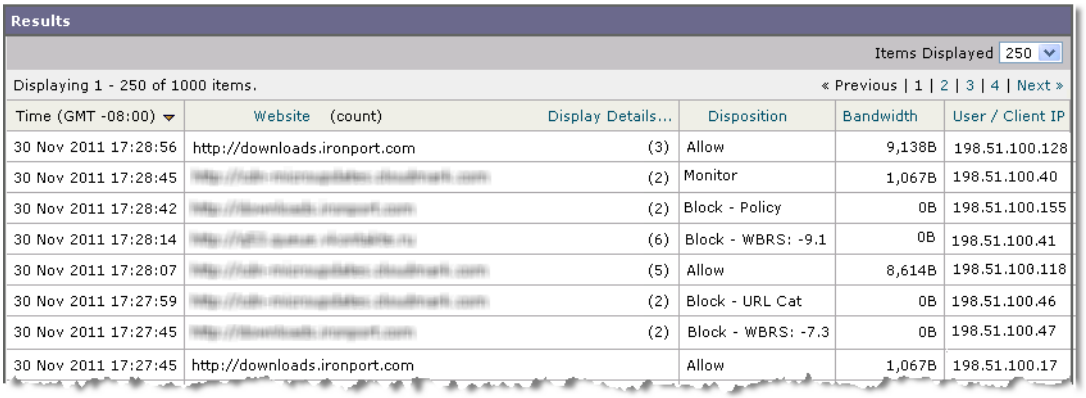
ステップ 5　[Search] をクリックします。

Web トラッキングの検索結果が表示されます。

Web トラッキング結果について

デフォルトでは、結果はタイム スタンプでソートされ、最新の結果が最上部に表示されます。

図 5-17　Web トラッキング検索結果（[Proxy Services] タブ）


Results

Items Displayed 250

Displaying 1 - 250 of 1000 items.　« Previous | 1 | 2 | 3 | 4 | Next »

Time (GMT -08:00)	Website (count)	Display Details...	Disposition	Bandwidth	User / Client IP
30 Nov 2011 17:28:56	http://downloads.ironport.com	(3)	Allow	9,138B	198.51.100.128
30 Nov 2011 17:28:45	[redacted]	(2)	Monitor	1,067B	198.51.100.40
30 Nov 2011 17:28:42	[redacted]	(2)	Block - Policy	0B	198.51.100.155
30 Nov 2011 17:28:14	[redacted]	(6)	Block - WBRS: -9.1	0B	198.51.100.41
30 Nov 2011 17:28:07	[redacted]	(5)	Allow	8,614B	198.51.100.118
30 Nov 2011 17:27:59	[redacted]	(2)	Block - URL Cat	0B	198.51.100.46
30 Nov 2011 17:27:45	[redacted]	(2)	Block - WBRS: -7.3	0B	198.51.100.47
30 Nov 2011 17:27:45	http://downloads.ironport.com		Allow	1,067B	198.51.100.17

[Results] ウィンドウには次の情報が表示されます。

- URL がアクセスされた時刻
- トランザクションに関係した Web サイト
- ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数。この数値は、カラム見出しの [Display Details] リンクの下にカッコで囲まれて表示されます。
- 処理（トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます）。
- トランザクションの帯域幅
- ユーザ ID/ クライアント IP アドレス

ステップ 6　トランザクションについてさらに詳細な情報を表示するには、[Website] カラム見出しの [Display Details...] リンクをクリックします。

（注）　1000 件を超える結果を表示する必要がある場合は、[Printable Download] リンクをクリックすると、関連するトランザクションの詳細を除く raw データ一式が含まれた CSV ファイルを取得できます。

ヒント　結果の URL が切り詰められている場合は、どのホスト Web セキュリティ アプライアンスでトランザクションが処理されたかに注目し、そのアプライアンスのアクセスログを確認すると、完全な URL を特定できます。

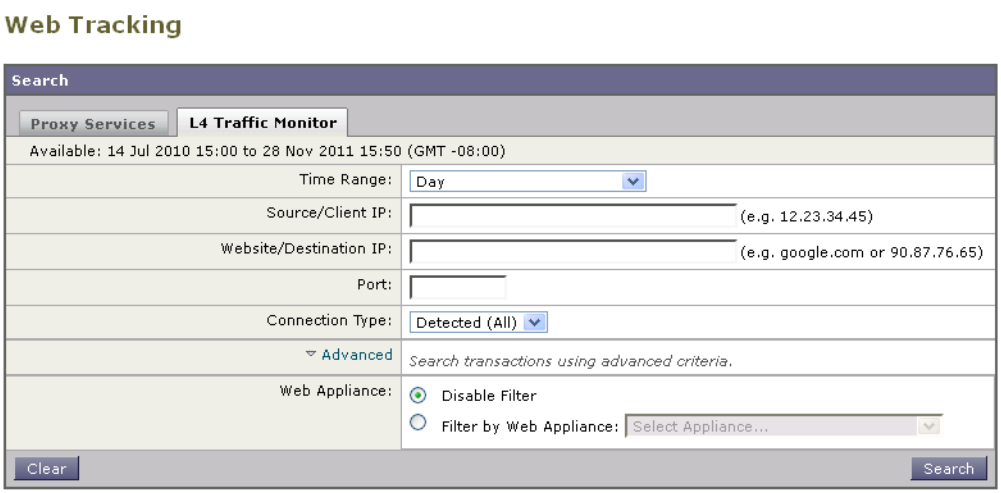
500 件までの関連トランザクションの詳細を表示するには、[Related Transactions] リンクをクリックします。

[L4 Traffic Monitor] タブ

[Web] > [Reporting] > [Web Tracking] ページの [L4 Traffic Monitor] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- サイト、使用された IP アドレスまたはドメイン
- ポート
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ
- 接続を処理した Web セキュリティ アプライアンス

図 5-18　[Web Tracking] ページの [L4 Traffic Monitor] タブ



一致した検索結果のうち最初の 1000 件が表示されます。

疑わしいサイトにあるホスト名、またはトランザクションを処理した Web セキュリティ アプライアンスを表示するには、[Destination IP Address] カラム見出しの [Display Details] リンクをクリックします。

この情報の詳細な使用方法については、「[L4 Traffic Monitor] ページ」（P.5-44）を参照してください。

[System Capacity] ページ

[Web] > [Reporting] > [System Capacity] ページでは、Web セキュリティ アプライアンスによってセキュリティ管理アプライアンスで発生する作業負荷全体を表示できます。重要な点は、[System Capacity] ページを使用して、経時的に増大をトラッキングしてシステム キャパシティの計画を立てられることです。Web セキュリティ アプライアンスをモニタすると、キャパシティが実際の量に適しているかを確認できます。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。

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

- Web セキュリティ アプライアンスが推奨される CPU キャパシティをいつ超えたかを特定します。これによって、設定の最適化や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。
- 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。
- 応答時間とプロキシ バッファ メモリを確認します。
- 1 秒あたりのトランザクション、および顕著な接続を確認します。

[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。
- 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。

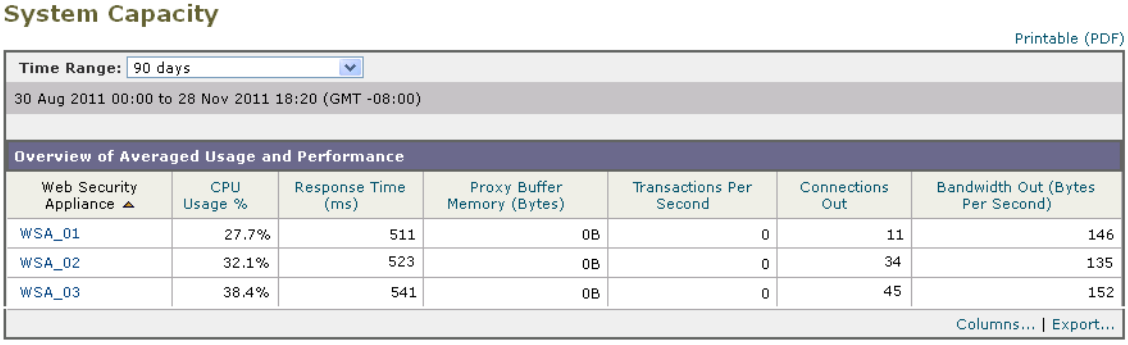
（注）　他のレポートで時間範囲に [Year] を選択した場合は、最大の時間範囲である 90 日を選択することを推奨します。

[System Capacity] ページにアクセスするには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [System Capacity] を選択します。

[System Capacity] ページが表示されます。

図 5-19　[System Capacity] ページ



ステップ 2　他のタイプのデータを表示するには、[Columns] をクリックし、表示するデータを選択します。

ステップ 3　単一のアプライアンスのシステム キャパシティを表示するには、[Overview of Averaged Usage and Performance] テーブルの [Web セキュリティ アプライアンス] カラムで目的のアプライアンスをクリックします。

このアプライアンスに関する [System Capacity] グラフが表示されます。このページのグラフは次の 2 種類に分かれています。

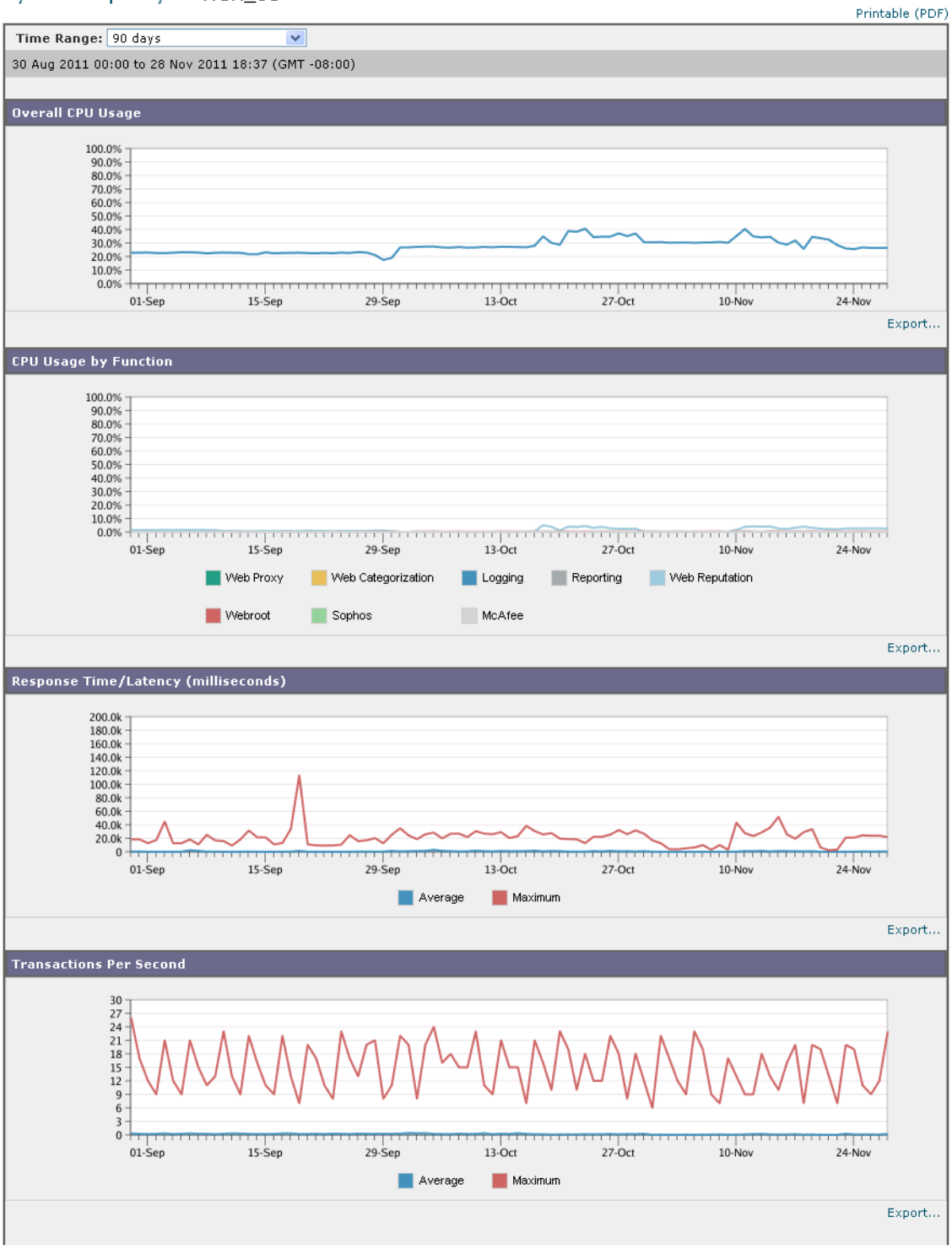
- [System Capacity]：[System Load]
- 「[System Capacity]：[Network Load]」

[System Capacity]：[System Load]

[System Capacity] ウィンドウの最初の 4 つのグラフは、システム負荷に関するレポートです。これらのレポートには、アプライアンスでの全体的な CPU 使用状況が示されます。AsyncOS は、アイドル状態の CPU リソースを使用してトランザクション 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。このページには、Web セキュリティ アプライアンスのレポーティングの処理などのさまざまな機能で使用される CPU 量を示す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。

また、応答時間 / 遅延のグラフと 1 秒あたりのトランザクションのグラフには、全体的な応答時間（ミリ秒単位）、および [Time Range] ドロップダウン メニューで指定した日付範囲での 1 秒あたりのトランザクション数が示されます。

図 5-20　[System Capacity] : [System Load]



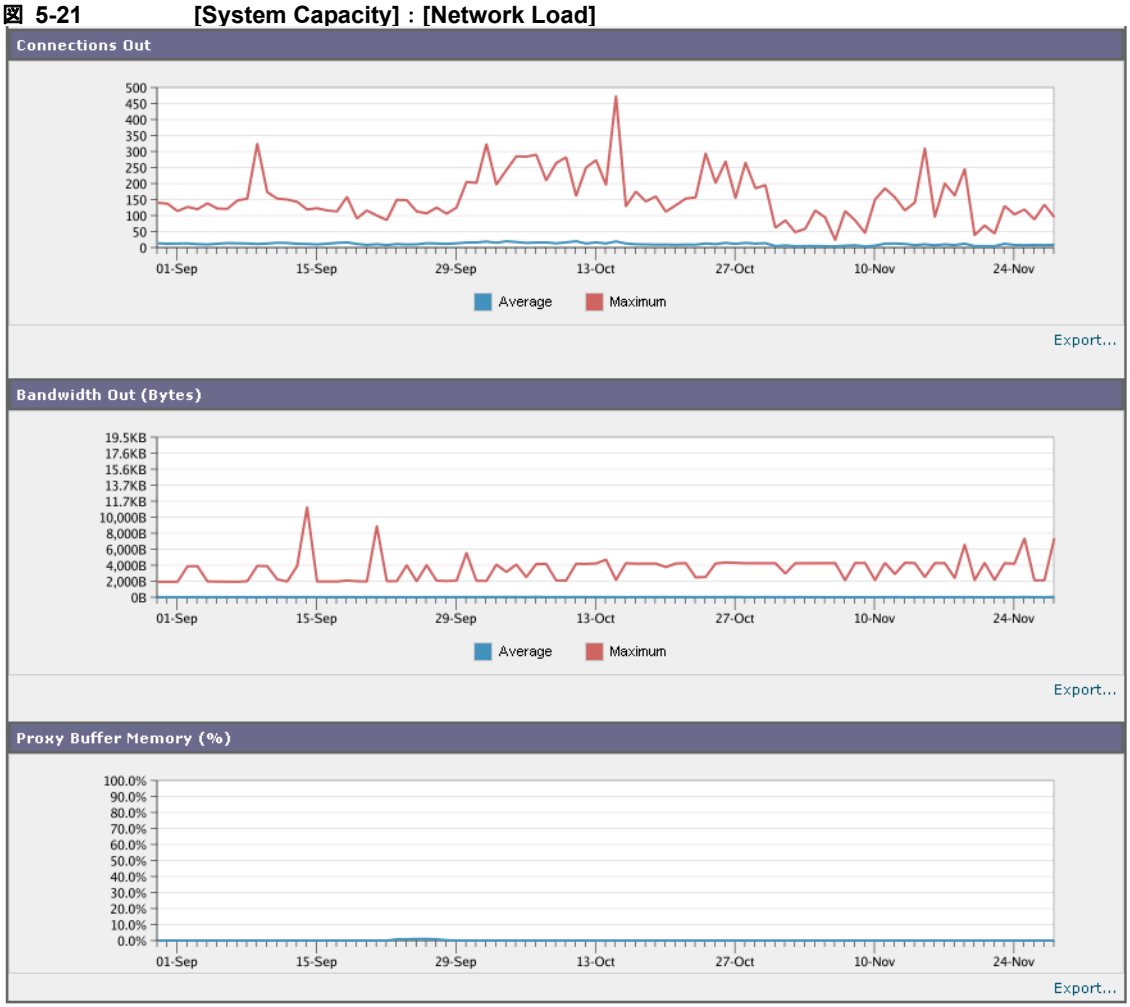
[System Capacity]：[Network Load]

[System Capacity] ウィンドウの次のグラフには、発信接続、出力用帯域幅、プロキシ バッファ メモリの統計情報が示されます。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。

[Proxy Buffer Memory] は、通常動作時におけるネットワーク トラフィックの急増を示している場合もありますが、グラフが最大値まで徐々に上昇している場合は、アプライアンスがのキャパシティが最大値に達しており、キャパシティの追加を検討すべきである可能性もあります。

次のチャートは、「[System Capacity]：[System Load]」、図 5-20 と同じページでこれらのチャートの下に表示されます。

図 5-21　[System Capacity]：[Network Load]



プロキシ バッファ メモリ スワッピングに関する注意事項

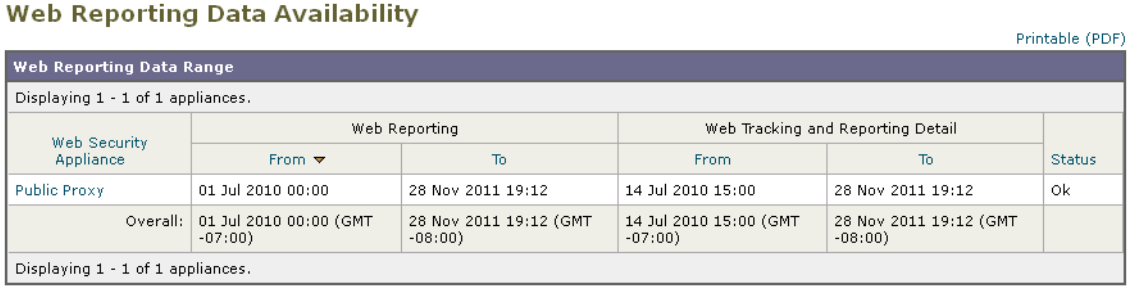
システムは、定期的にプロキシ バッファ メモリをスワップするように設計されているので、一部のプロキシ バッファ メモリ スワッピングは起こり得るものであり、アプライアンスの問題を示すものではありません。システムが*継続的に*高ボリュームのプロキシ バッファ メモリをスワップする場合を除き、プロキシ バッファ メモリのスワッピングは正常かつ通常の動作です。システムが極端に大量の処理を

行い、大量であるためにプロキシ バッファ メモリを絶えずスワップする場合は、ネットワークに Cisco IronPort アプライアンスを追加するか、またはスループットが最大になるように設定を調整して、パフォーマンスの向上を図る必要があります。

[Data Availability] ページ

[Web] > [Reporting] > [Data Availability] ページには、管理対象の各 Web セキュリティ アプライアンスに対応するセキュリティ管理アプライアンスでレポーティングおよび Web トラッキング データを使用できる日付範囲の概要が表示されます。

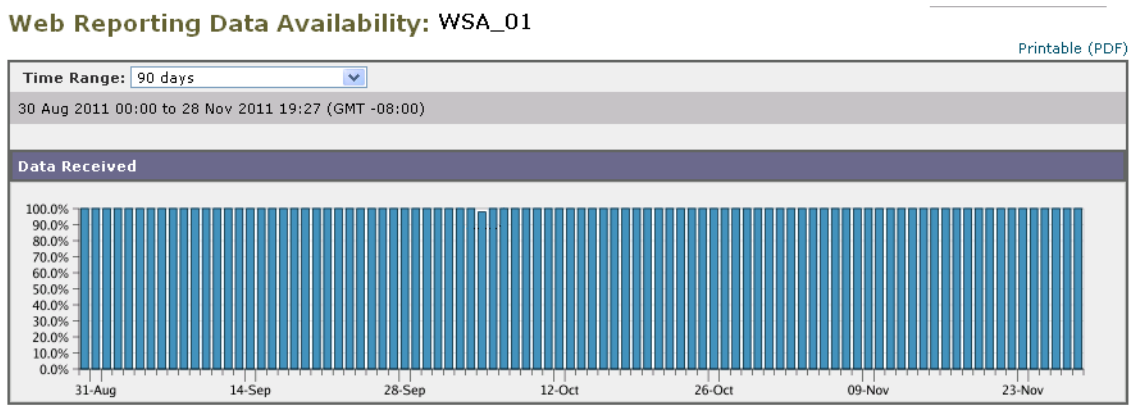
図 5-22　[Web Reporting Data Availability] ページ



（注） Web レポーティングがディセーブルになると、セキュリティ管理アプライアンスは Web セキュリティ アプライアンスから新しいデータを取得しなくなりますが、以前に取得したデータは セキュリティ管理アプライアンスに残っています。ディスク使用率の管理方法については、「ディスク使用量の管理」（P.13-58）を参照してください。

[Web Reporting] の [From] カラムと [To] カラム、および [Web Reporting and Tracking] の [From] カラムと [To] カラムでステータスが異なる場合は、[Status] カラムに最も深刻な結果が示されます。

特定のアプライアンスのデータ アベイラビリティをグラフ形式で表示するには、[Web セキュリティ アプライアンス] カラムでアプライアンスをクリックします。



（注） URL カテゴリに関するスケジュール済みレポートでデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「Some data in this time range was unavailable.」というメッセージが表示されます。
ギャップが存在しない場合は何も表示されません。

スケジュール設定されたレポートとオンデマンド Web レポートについて

特記のない限り、次のタイプの Web セキュリティ レポートを、スケジュール設定されたレポートまたはオンデマンド レポートとして作成できます。

- [Web Reporting Overview]：このページに表示される情報については、「Web レポーティングの [Overview] ページ」（P.5-13）を参照してください。
- [Users]：このページに表示される情報については、「[Users] ページ」（P.5-17）を参照してください。
- [Web Sites]：このページに表示される情報については、「[Web Sites] ページ」（P.5-24）を参照してください。
- [URL Categories]：このページに表示される情報については、「[URL Categories] ページ」（P.5-26）を参照してください。
- [Top URL Categories — Extended]：[Top URL Categories — Extended] のレポートを生成する方法については、「Top URL Categories — Extended」（P.5-65）を参照してください。

  このレポートをオンデマンド レポートとして使用することはできません。
- [Application Visibility]：このページに表示される情報については、「[Application Visibility] ページ」（P.5-30）を参照してください。
- [Top Application Types — Extended]：[Top URL Categories — Extended] のレポートを生成する方法については、「Top Application Types — Extended」（P.5-66）を参照してください。

  このレポートをオンデマンド レポートとして使用することはできません。
- [Anti-Malware]：このページに表示される情報については、「[Anti-Malware] ページ」（P.5-33）を参照してください。
- [Client Malware Risk]：このページに表示される情報については、「[Client Malware Risk] ページ」（P.5-39）を参照してください。
- [Web Reputation Filters]：このページに表示される情報については、「[Web Reputation Filters] ページ」（P.5-41）を参照してください。
- [L4 Traffic Monitor]：このページに表示される情報については、「[L4 Traffic Monitor] ページ」（P.5-44）を参照してください。
- [Mobile Secure Solution]：このページに表示される情報については、「[Reports by User Location] ページ」（P.5-49）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.5-57）を参照してください。

Web レポートのスケジュール設定

ここでは、次の内容について説明します。

（注）　すべてのレポートで、ユーザ名を認識できないようにすることができます。詳細については、「Web レポートでのユーザ名の匿名化」（P.5-4）を参照してください。

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。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、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。

セキュリティ管理アプライアンスは、生成した最新のレポートを保持します（すべてのレポートに対して、最大で 1000 バージョン）。必要に応じた数（ゼロも含む）のレポート受信者を定義できます。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。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。

デフォルトでは、スケジュール設定された各レポートのうち、直近の 12 のレポートがアーカイブされます。レポートは、アプライアンスの **/periodic_reports** ディレクトリに保管されます。（詳細については、付録 A「IP インターフェイスおよびアプライアンスへのアクセス」を参照してください）。

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 Web 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　セキュリティ管理アプライアンスのウィンドウで、[Web] > [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。

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。

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] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6　生成されるレポートの形式を選択します。

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

ステップ 7　[Number of Items] の横のドロップダウン リストから、生成されるレポートに出力する項目の数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は 5 です。

ステップ 8　[Charts] では、[Data to display] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 9　[Sort Column] の横のドロップダウン リストから、このレポートでデータをソートするためのカラムを選択します。これにより、スケジュール設定されたレポート内の任意のカラムを基準とする上位「N」個の項目のレポートを作成できます。

ステップ 10　[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。

ステップ 11　[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 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 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

レポートを編集するには、[Web] > [Reporting] > [Scheduled Reports] ページに移動し、編集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。設定を変更し、[Submit] をクリックしてページでの変更を送信し、[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削除

レポートを削除するには、[Web] > [Reporting] > [Scheduled Reports] ページに移動し、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。スケジュール設定されたレポートをすべて削除する場合は、[All] チェックボックスを選択し、**削除**を実行して変更を**確定**します。削除されたレポートのアーカイブ版は削除されません。

追加の拡張レポート

さらに 2 種類のレポートを、スケジュール設定されたレポートとしてのみセキュリティ管理アプライアンスで使用することができます。

- Top URL Categories — Extended
- Top Application Types — Extended

Top URL Categories — Extended

[Top URL Categories — Extended] レポートは、管理者が [URL Categories] レポートよりも詳細な情報を必要とする場合に役立ちます。

たとえば、通常の [URL Categories] レポートでは、大きい URL カテゴリ レベルで特定の従業員の帯域幅使用状況を評価する情報を収集できます。各 URL カテゴリの上位 10 個の URL、または各 URL カテゴリの上位 5 人のユーザについて、帯域幅の使用状況をモニタする詳細なレポートを生成するには、[Top URL Categories —Extended] レポートを使用します。

（注）

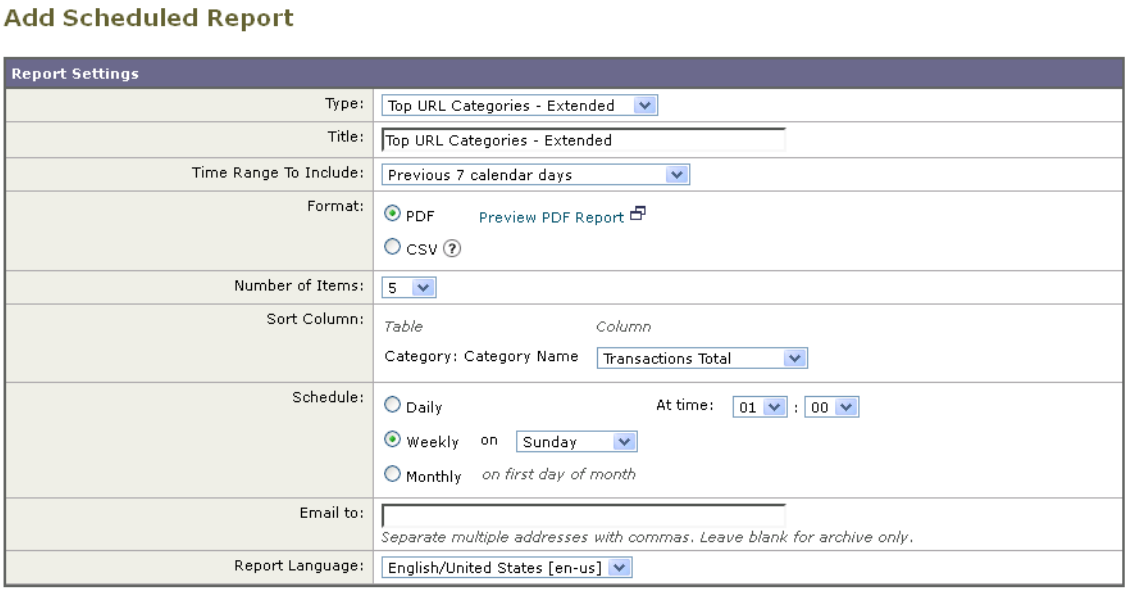
- このタイプのレポートで生成できる最大レポート数は 20 です。
- 定義済みの URL カテゴリ リストは更新されることがあります。こうした更新によるレポート結果への影響については、「URL カテゴリ セットの更新とレポート」（P.5-28）を参照してください。

[Top URL Categories — Extended] 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　セキュリティ管理アプライアンスのウィンドウで、[Web] > [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。

ステップ 3　[Type] の横のドロップダウン メニューから、[Top URL categories — Extended] を選択します。



ステップ 4　[Title] テキスト フィールドに、URL 拡張レポートのタイトルを入力します。

ステップ 5　[Time Range] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6　生成されるレポートの形式を選択します。

デフォルト形式は PDF です。

ステップ 7　[Number of Items] の横のドロップダウン リストから、生成されるレポートに出力する URL カテゴリの数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は 5 です。

ステップ 8　[Sort Column] の横のドロップダウン リストから、このレポートでデータをソートするためのカラムを選択します。これにより、スケジュール設定されたレポート内の任意のカラムを基準とする上位「N」個の項目のレポートを作成できます。

ステップ 9　[Charts] では、[Data to display] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 10　[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。

ステップ 11　[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。

ステップ 12　[Submit] をクリックします。

Top Application Types — Extended

[Top Application Type — Extended] レポートを生成するには、次の手順を実行します。

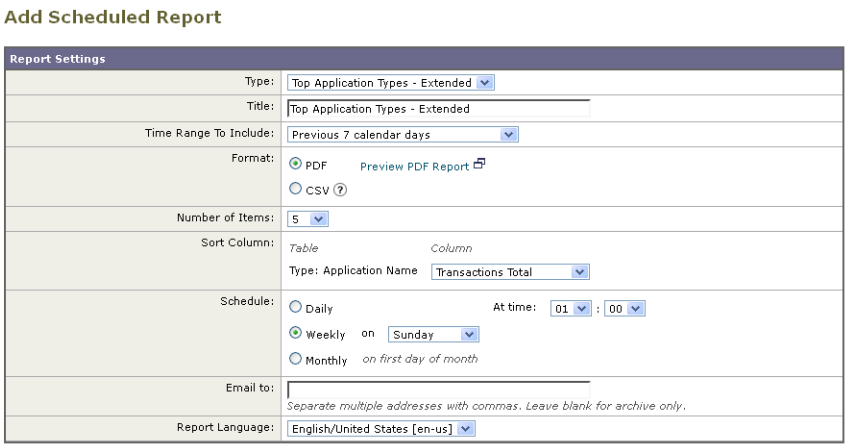
ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [Reporting] > [Scheduled Reports] を選択します。

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

[Add Scheduled Report] ウィンドウが表示されます。

ステップ 3　[Type] の横のドロップダウン メニューから、[Top Application Types — Extended] を選択します。

このページのデフォルト オプションは変更される場合があります。



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を入力します。

ステップ 5　[Time Range] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6　生成されるレポートの形式を選択します。

デフォルト形式は PDF です。

ステップ 7　[Number of Items] の横のドロップダウン リストから、生成されたレポートに出力するアプリケーション タイプの数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は **5** です。

ステップ 8　[Sort Column] の横のドロップダウン リストから、テーブルに表示するカラムのタイプを選択します。選択肢は、[Transactions Completed]、[Transactions Blocked]、[Transaction Totals] です。

ステップ 9　[Charts] では、[Data to display] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 10　[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。

ステップ 11　[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。

ステップ 12　[Submit] をクリックします。

オンデマンドでの Web レポートの生成

スケジュールを設定できるレポートのほとんどは、オンデマンドでの作成も可能です。

（注）　一部のレポートは、オンデマンドではなくスケジュール設定されたレポートとしてのみ使用できます。「追加の拡張レポート」（P.5-65）を参照してください。

レポートをオンデマンドで作成するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスのウィンドウで、[Web] > [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。

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。

このページのオプションは変更される場合があります。

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　[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 6　[Format] セクションで、レポートの形式を選択します。

次のオプションがあります。

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

ステップ 7　レポートで使用可能なオプションに応じて次の項目を選択します。

- [Number of rows]：テーブルに表示するデータの行数。
- [Charts]：レポートのチャートに表示するデータ。

  [Data to display] の下のデフォルト オプションを選択します。
- [Sort Column]：各テーブルのソート基準となるカラム。

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。

- このレポートを [Archived Reports] ページに表示するには、[Archive Report] チェックボックスを選択します。

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

- レポートを電子メールで送信する場合は、[Email now to recipients] チェックボックスをオンにします。
- 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　[Deliver This Report] をクリックして、レポートを生成します。

[Archived Web Reports] ページ

アーカイブされた Web レポートの表示と管理

[Web] > [Reporting] > [Archived Reports] ページには次の内容が表示されます。

- 「スケジュール設定されたレポートの追加」（P.5-64）の手順を使用してスケジュールを設定したレポート
- 「オンデマンドでの Web レポートの生成」（P.5-67）の手順を使用して作成したレポート

レポートを表示するには、[Report Title] カラムでレポート名をクリックします。[Show] ドロップダウン メニューでは、[Archived Reports] ページに表示されるレポートのタイプをフィルタリングできます。

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。

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 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。