CHAPTER 5

中央集中型 Web レポーティングの使用

この章は、次の項で構成されています。

- 「レポーティングの概要」（P.5-1）
- 「Web レポーティングを使用する前に」（P.5-3）
- 「中央集中型 Web レポーティングの設定」（P.5-3）
- 「[Web Reporting] タブの使用」（P.5-5）
- 「Web レポーティング ページの概要」（P.5-12）
- 「レポートのスケジューリング」（P.5-83）
- 「レポートのアーカイブ」（P.5-90）

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集約してデータを記録し、それを Web トラフィック パターンとセキュリティ リスクのモニタに使用できます。リアルタイムにレポートを実行して特定の期間のシステム アクティビティをインタラクティブに表示することも、一定の間隔で実行するようにレポートのスケジュールを設定することもできます。レポーティング機能を使用すると、raw データをファイルにエクスポートすることもできます。

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

ドメイン情報

ドメインに対しては、ドメイン レポートに出力する次のデータ要素を、Web レポーティング機能で生成できます。たとえば、Facebook.com ドメインに関するレポートを生成する場合は、レポートに次のような情報が含まれます。

- 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

ユーザに対しては、ユーザ レポートに出力するデータ要素を、Web レポーティング機能で生成できます。たとえば、「Jamie」というタイトルのユーザ レポートでは、レポートに次のような情報が含まれます。

- 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だった上位 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、カテゴリ「Sports」に対して、レポートに次のような情報が含まれます。

- 「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。

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.13-2）を参照してください。

（注） Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。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得るには、この章で説明する Web トラッキング機能を使用します。

Web レポーティングを使用する前に

（注）　Web セキュリティ アプライアンスの Web レポーティングを表示するには、Web セキュリティ アプライアンスを追加して設定する必要があります。Web セキュリティ アプライアンスの追加については、「管理対象アプライアンスの追加」（P.3-11）を参照してください。また、これらのアプライアンスの設定については、『*Cisco IronPort AsyncOS 7.1 for Web User Guide*』を参照してください。

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

- Web レポーティングをイネーブルにするには、「中央集中型 Web レポーティングの設定」（P.5-3）を参照してください。
- さまざまなインタラクティブ レポート ページを表示および管理するには、「Web レポーティング ページの概要」（P.5-12）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スケジュール設定されたレポートを作成するには、「レポートのスケジューリング」（P.5-83）を参照してください。
- 以前に実行したレポート（スケジュール設定されたレポートと [Generate Report Now] で生成したレポートの両方）のアーカイブ版を表示する方法については、「レポートのアーカイブ」（P.5-90）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

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

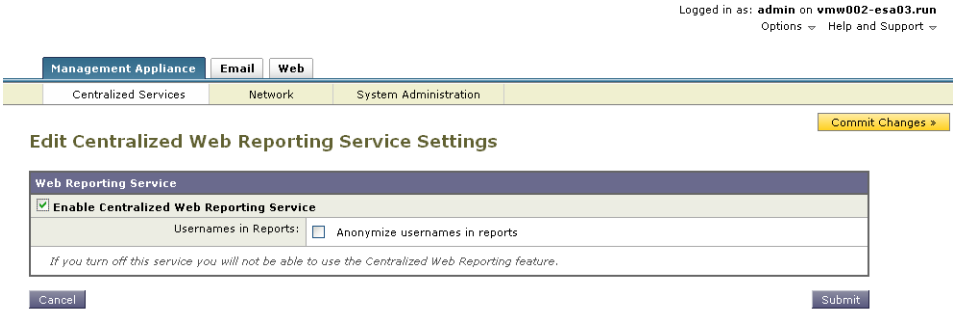
中央集中型 Web レポーティングを設定するには、次の手順を実行します。

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

[Centralized Web Reporting] ページが表示されます。システム セットアップ ウィザードを実行してから初めて中央集中型レポーティングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[Accept] をクリックします。

ステップ 2　[Edit Settings] をクリックします。

ステップ 3　[Edit Centralized Web Reporting Service Settings] ページが表示されます。



ステップ 4　[Enable Centralized Web Report Services] チェックボックスをクリックします。

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になっている場合、Web セキュリティ アプライアンスはシステム キャパシティとシステム ステータスを除いて、レポート データを保持しません。中央集中型 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。

ステップ 5　スケジュール設定されたレポートでユーザ名が認識できない状態でレポートを生成するには、[Anonymize usernames in reports] チェックボックスをオンにします。デフォルト設定では、スケジュール設定されたレポートにすべてのユーザ名が表示されます。

（注）　管理者ステータスを持っている場合は、常にユーザ名が表示されます。

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

（注）　アプライアンスで 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.12-123）を参照してください。

[Web Reporting] タブの使用

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

（注）　[Web Reporting] タブ上のカテゴリの中で、スケジュール設定されたレポートを生成できるものについては、「レポートのスケジューリング」（P.5-83）を参照してください。

表 5-1　[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、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のグラフや要約テーブルが含まれます。詳細については、「Web レポーティングの [Overview] ページ」（P.5-12）を参照してください。
[Users] ページ	[Users] ページには、個々のユーザの Web トラッキング情報を表示するための Web トラッキング リンクがあります。 [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] 表に表示されている個々のユーザをクリックすると、そ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 [Users] 表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。このページから、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。 詳細については、「[Users] ページ」（P.5-16）を参照してください。システム内の特定のユーザについては、「[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を表示できます。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。

表 5-1　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[URL Categories] ページ	[URL Categories] ページでは、サイト上でアクセスされている次のような上位 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。 このページでは、カスタム URL カテゴリの作成、編集、または削除を行うこともできます。詳細については、「[URL Categories] ページ」（P.5-28）を参照してください。
[Application Visibility] ページ	[Application Visibility] ページでは、Security Management 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.5-36）を参照してください。
セキュリティ	
[Anti-Malware] ページ	[Anti-Malware] ページでは、指定した時間範囲内にレイヤ 4 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。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.5-40）を参照してください。

表 5-1　[Web Reporting] タブの詳細（続き）

[Web Reporting] メニュー	アクション
[Client Malware Risk] ページ	[Client Malware Risk] ページは、クライアント マルウェア リスク アクティビティのモニタに使用できる、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。 詳細については、「[Client Malware Risk] ページ」（P.5-50）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.5-58）を参照してください。
[L4 Traffic Monitor Data] 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 Data] ページ」（P.5-64）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.5-67）を参照してください。
レポーティング	

表 5-1　[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、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）をトラッキングし、表示することができます。 これには、時間範囲やユーザ ID とクライアント IP アドレスなどの情報が含まれ、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。 詳細については、「[Web Tracking] ページ」（P.5-70）を参照してください。
[System Capacity] ページ	レポーティング データを Security Management アプライアンスに送信する、全体的なワークロードを表示できます。 詳細については、「[System Capacity] ページ」（P.5-76）を参照してください。
[Data Availability] ページ	各アプライアンスの Security Management アプライアンス上のレポーティング データの影響を把握できます。詳細については、「[Data Availability] ページ」（P.5-81）を参照してください。
レポートのスケジューリング	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、「レポートのスケジューリング」（P.5-83）を参照してください。
レポートのアーカイブ	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、「レポートのアーカイブ」（P.5-90）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、「レポートのスケジューリング」（P.5-83）を参照してください。

Web セキュリティ アプライアンス用のインタラクティブ レポート ページ

すべての Web レポーティング ページは、インタラクティブなレポート ページになっています。このため、システム内の 1 つまたはすべての管理対象 Web セキュリティ アプライアンスの情報をモニタできます。

インタラクティブ レポート ページでは、異なる時間範囲の中央集中型レポートを表示でき、ページごとに表示するカラムのタイプを指定できます。多くのレポート ページにはインタラクティブなカラムがあり、そのページでデータを表示する際に各カラムのデータをニーズに応じてソートできるように、これらのカラムを設定できます。レポート ページ上のインタラクティブなカラムの設定については、「レポート ページのカラムの設定」（P.5-10）を参照してください。

（注）　レポート ページによっては、一部のカラムを使用できないことがあります。特定のレポート ページで使用可能なカラムを確認するには、各レポート ページの [Column] リンクをクリックします。「中央集中型 Web レポーティング ページのインタラクティブ カラム」（P.E-1）に、このリリースのレポーティング ページで使用可能なカラムの説明があります。

また、カラムの内容が得られた [Web Tracking] ページへのリンクが、そのカラムに表示されることがあります。

レポーティング ページでの時間範囲の設定については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

レポート ページのカラムの設定

レポート ページのカラムを設定するには、次の手順を実行します。

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

ステップ 2　[Columns] をクリックします。

表示するカラムを選択するためのポップアップ ウィンドウが表示されます。

ステップ 3　ポップアップ ウィンドウで、各カテゴリの横のチェックボックスをオンにします。
オプションを選択したら、[Done] をクリックします。これで、インタラクティブなカラム見出しを使用して、各カラムのデータをニーズに合わせてソートすることができます。

（注）　各レポート ページのいくつかのカラムには、Web トラッキングの詳細へのリンクが表示されます。

レポート ページからのレポートの印刷

ページ右上の [Printable PDF] リンクをクリックすると、すべてのレポート ページを読みやすい印刷形式の PDF 版で生成できます。[Export] リンクをクリックすると、グラフやその他のデータをカンマ区切り値（CSV）形式でエクスポートできます。大部分のレポートでは、CSV 形式のスケジューリングを行うことができます。ただし、CSV 形式で拡張レポートをスケジュールすることはできません。

レポート ページからの印刷の詳細については、「レポート データの印刷とエクスポート」（P.3-21）を参照してください。

各ページに表示される [Export] リンクは、raw データをエクスポートするために使用されます。

レポート ページのレポーティング フィルタ

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

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

Web レポーティング ページの概要

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

次の内容で構成されています。

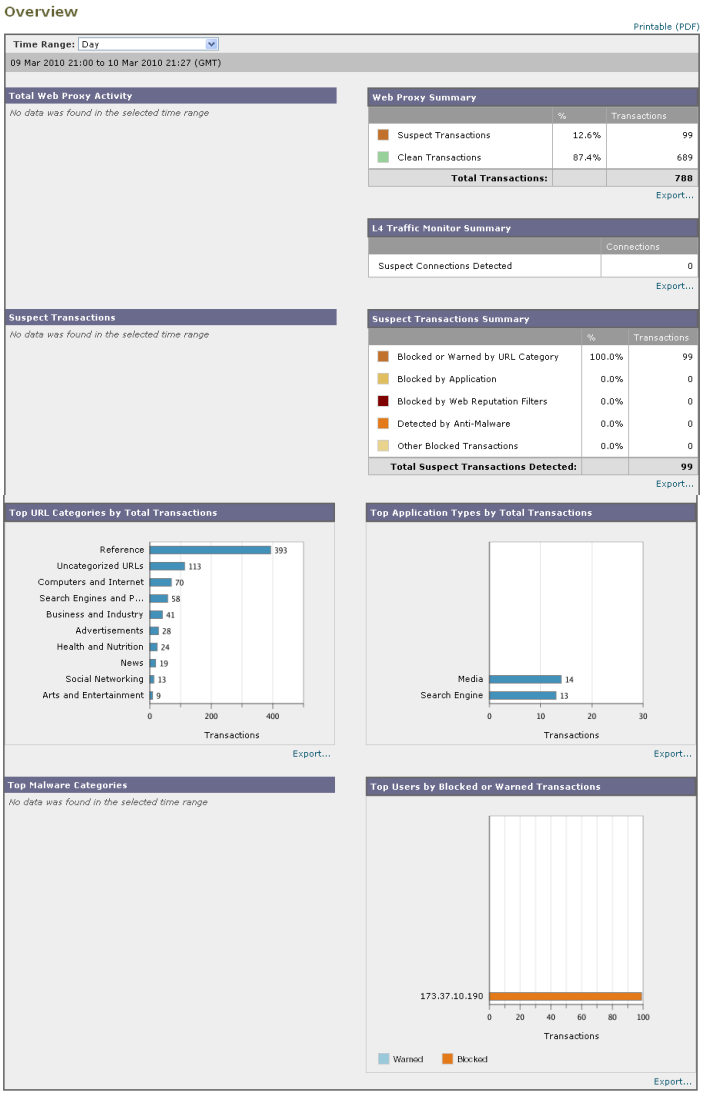
- 「Web レポーティングの [Overview] ページ」（P.5-12）
- 「[Users] ページ」（P.5-16）
- 「[User Details] ページ」（P.5-20）
- 「[Web Sites] ページ」（P.5-24）
- 「[URL Categories] ページ」（P.5-28）
- 「[Application Visibility] ページ」（P.5-36）
- 「[Anti-Malware] ページ」（P.5-40）
- 「[Client Malware Risk] ページ」（P.5-50）
- 「[Web Reputation Filters] ページ」（P.5-58）
- 「[L4 Traffic Monitor Data] ページ」（P.5-64）
- 「[Reports by User Location] ページ」（P.5-67）
- 「[Web Tracking] ページ」（P.5-70）
- 「[System Capacity] ページ」（P.5-76）
- 「[Data Availability] ページ」（P.5-81）

Web レポーティングの [Overview] ページ

[Web] > [Reporting] > [Overview] ページには、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のグラフや要約テーブルが含まれます。

図 5-1 に、[Overview] ページを示します。

図 5-1　[Web] > [Reporting] > [Overview] ページ



[Overview] ページの上の部分には、URL とユーザの使用状況に関する統計、Web プロキシ アクティビティ、およびトランザクションに関するさまざまな要約が表示されます。トランザクションの要約には、たとえば疑わしいトランザク

ションに関する詳細なトレンドが表示され、このグラフの横に、ブロックされた疑わしいトランザクションの数およびどの方法でブロックされているかが示されます。

[Overview] ページの下半分には、使用状況に関する情報が表示されます。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 タイプとカテゴリ、およびこれらのブロックや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] ページのさまざまなセクションについて説明します。

表 5-2　[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.3-18）を参照してください。
Total Web Proxy Activity	このセクションでは、Security Management アプライアンスによって現在管理されている Web セキュリティ アプライアンスからレポートされる 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、または問題のないプロキシ アクティビティの比率を、トランザクションの総数とともに表示できます。
L4 Traffic Monitor Summary	このセクションには、Security Management アプライアンスによって現在管理されている Web セキュリティ アプライアンスから報告されるレイヤ 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。

表 5-2　[Web] > [Reporting] > [Overview] ページの詳細（続き）

セクション	説明
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。
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のアプリケーション タイプが表示されます。実際のアプリケーション タイプの名前（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）などがあります。
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、ブロックまたは警告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。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、「中央集中型 Web レポーティングの設定」（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。その方法の例については、「例 4：プライバシーおよびユーザ名の非表示」（P.D-12）を参照してください。

[Overview] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポートすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

（注）　ユーザ向けに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リング」（P.5-83）を参照してください。

[Users] ページ

[Web] > [Reporting] > [Users] ページには、個々のユーザの Web レポーティング情報を表示するためのリンクが提供されています。

[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。

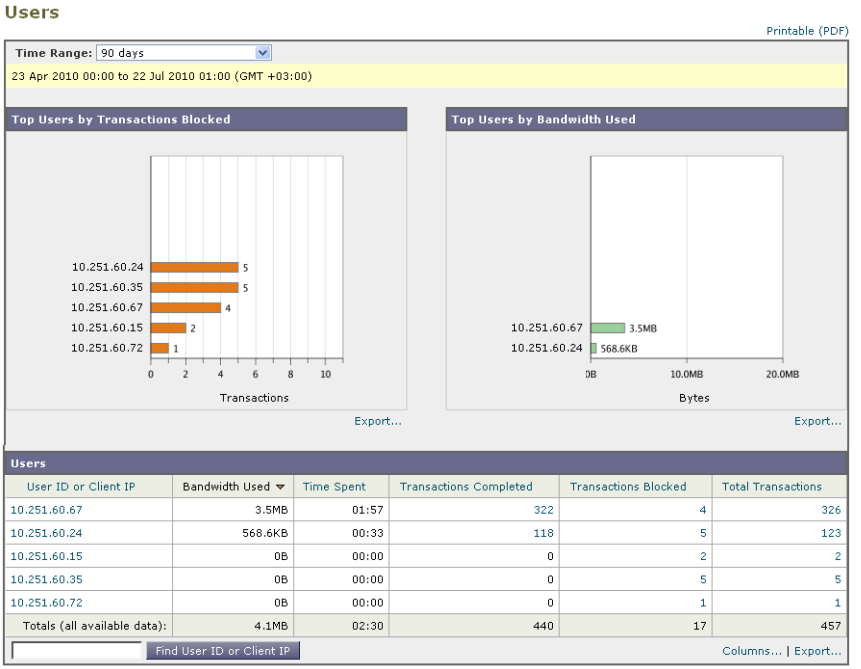
（注）　Security Management アプライアンスがサポートできる Web セキュリティ アプライアンス上の最大ユーザ数は 500 です。

[Users] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Users] を選択します。

[Users] ページが表示されます。

図 5-2　[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 5-3　[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.3-18）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、「中央集中型 Web レポーティングの設定」（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。その方法の例については、「例 4：プライバシーおよびユーザ名の非表示」（P.D-12）を参照してください。

表 5-3　[Web] > [Reporting] > [Users] ページの詳細（続き）

セクション	説明
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	[Users] テーブルはインタラクティブなテーブルになっていて、ユーザ情報を無数の方法でソートし、テーブルを表示するたびにルックアンドフィールを変えることができます。各カラムの情報は、カラム見出しをクリックすることで昇順または降順にソートできます。 このテーブルに表示されるカラムはカスタマイズ可能です。[Users] テーブルのカラムの設定については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。 インタラクティブな [Users] テーブルに表示するカラム カテゴリを選択した後に、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、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）　**このページでユーザを追加または削除することはできません。**

ユーザの追加または削除の詳細については、「GUI でのユーザ管理」（P.12-59）を参照してください。ユーザ ロール自体の詳細については、「ユーザ ロール」（P.12-43）および表 12-2（P.12-44）を参照してください。ユーザ ロールのカスタマイズについては、「Custom Web User ロールの作成」（P.12-56）を参照してください。

（注）クライアント IP アドレスではなくクライアント ユーザ ID を表示するには、LDAP 認証を設定する必要があります。LDAP 認証を使用しない場合、システムでは IP アドレスによるユーザの参照のみができます。
Security Management アプライアンスで LDAP 認証を設定するには、[Management Appliance] > [System Administration] > [LDAP] > [Add LDAP Server Profile] を選択します。[Use Password] オプション ボタンを選択して、ユーザ名とパスワードを入力します。これで、[Users] ページと [User Details] ページにユーザ名が表示されるようになります。

[Users] ページから、印刷用の PDF を CSV ファイルに印刷またはエクスポートすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。ユーザ向けにスケジュール設定されたレポートを生成することもできます。「レポートのスケジューリング」（P.5-83）を参照してください。

（注）このページのスケジュール設定されたレポート内で、ユーザ情報を認識できないようにすることができます。ユーザ情報を認識不可能にする方法については、「Security Management 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とディセーブル化」（P.3-5）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-2）を参照してください。

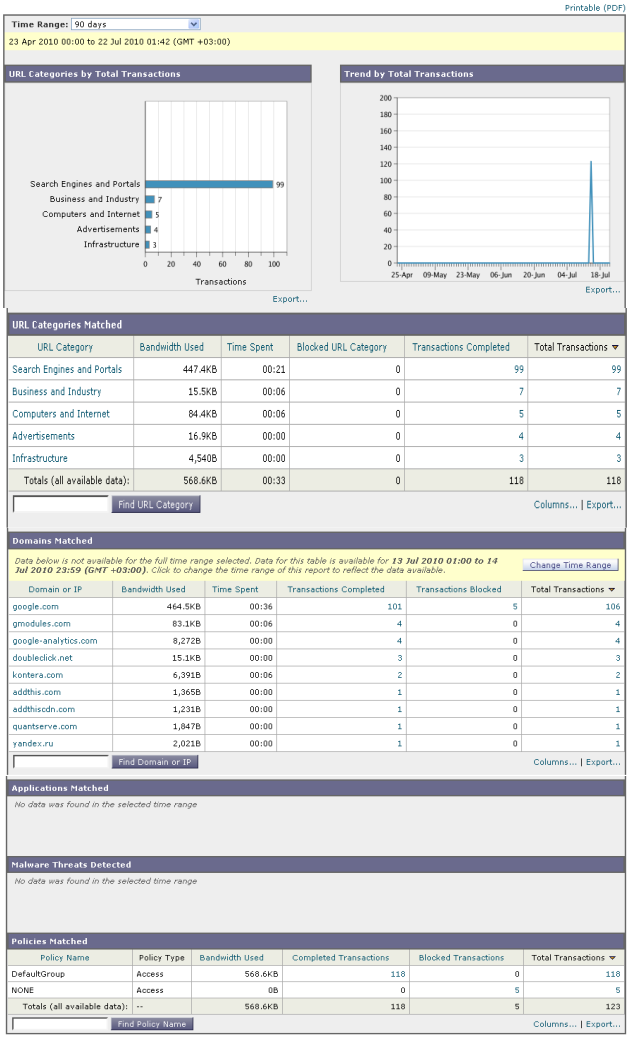
[User Details] ページ

[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 5-3　[User Details] ページ



[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 5-4　[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）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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。
Trend by Total Transaction	このグラフには、特定のユーザの Web トランザクションの経時的なトレンドが示されます。基本的には、この特定のユーザがその Web にいつアクセスしたか、および閲覧トラフィックを送信した回数が示されます。 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関して、指定した時間範囲内の一致したすべてのカテゴリが表示されます。インタラクティブなカラム見出しを使用するとデータをソートできます。また、[Items Displayed] メニューによって、リストに表示される URL カテゴリの数を変更できます。 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。

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

セクション	説明
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。
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。セクション下部のテキスト フィールドにマルウェア脅威の名前を入力し、[Find Malware Threat] をクリックします。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、この特定のユーザに適用されている特定のポリシーを検索できます。 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。

[User Details] ページのいくつかのセクションでは、表示するカラムを設定できます。カラムの設定については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。

インタラクティブなセクションに表示するカテゴリを選択後、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。

[Users Details] ページの使用例については、「例 1：ユーザの調査」（P.D-2）を参照してください。

[Web Sites] ページ

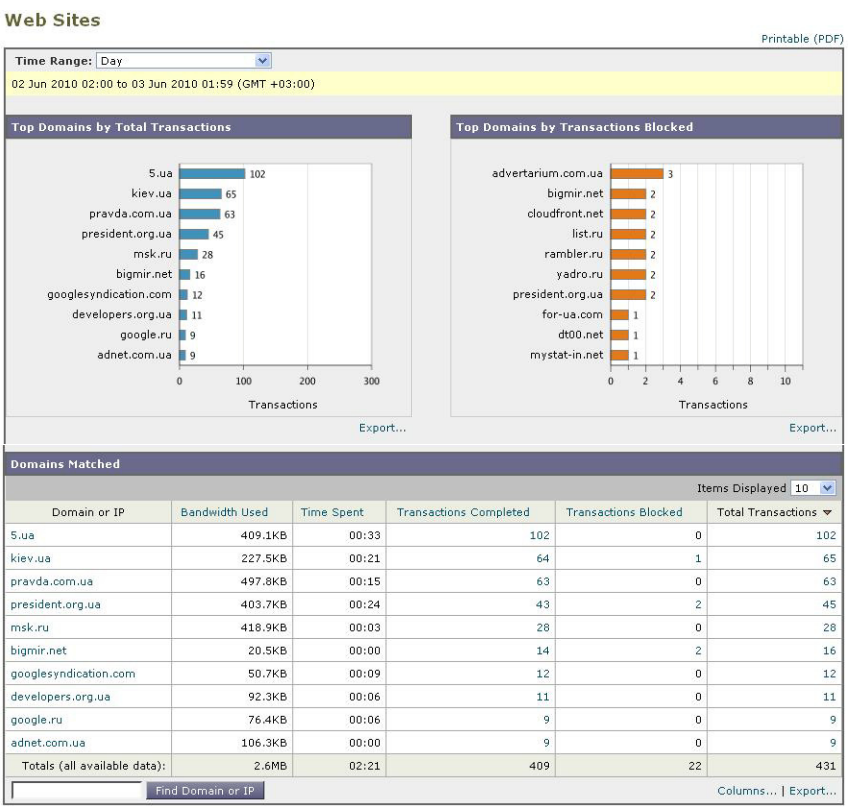
[Web] > [Reporting] > [Web Sites] ページでは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。

[Web Site] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Sites] を選択します。

[Web Sites] ページが表示されます。

図 5-4　[Web Sites] ページ



[Web Sites] ページには次の情報が表示されます。

表 5-5　[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.3-18）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 5-5　[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] ページが表示され、トラッキング情報および特定のドメインがブロックされた原因を確認できます。 [Domains 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、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。 [Domains Matched] テーブルに表示するカテゴリを選択後、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。 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。[Time Range] ドロップダウン リストを使用して、特定の時間範囲（時間、日、または週）でドメインの使用状況が表示されるようにこのテーブルを変更できます。 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-7）を参照してください。

[Web Sites] ページから、[Top Domains by Total Transaction] および [Domains Matched] の情報を印刷したり、CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

（注）　[Web Sites] 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、「レポートのスケジューリング」（P.5-83）を参照してください。

[URL Categories] ページ

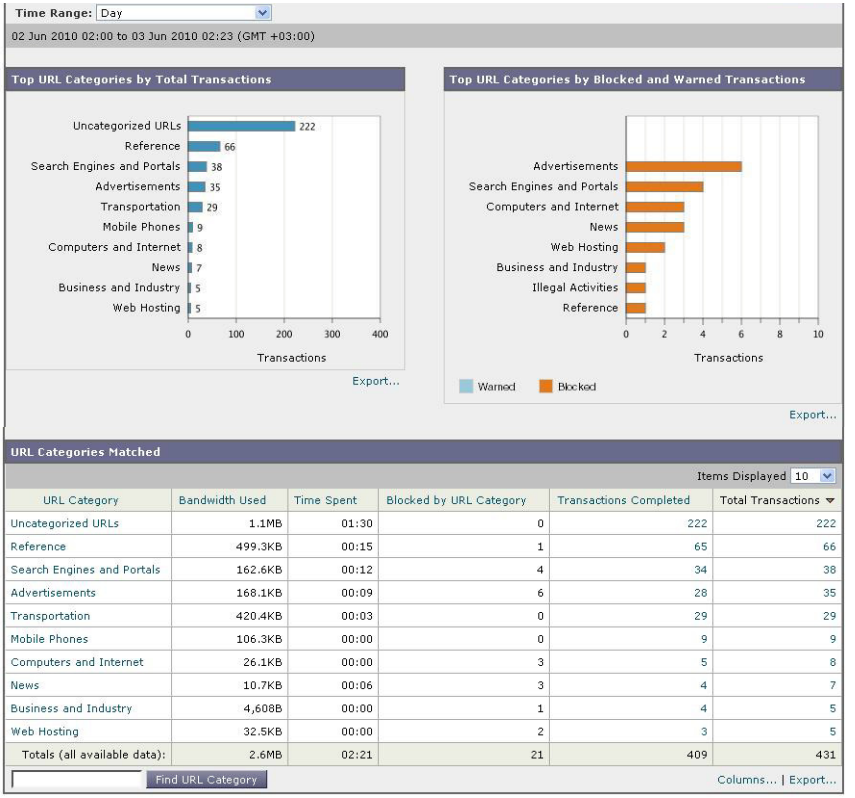
[Web] > [Reporting] > [URL Categories] ページでは、システム上のユーザがアクセスしている URL カテゴリを表示できます。

[URL Categories] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [URL Categories] を選択します。

[URL Categories] ページが表示されます。

図 5-5　[URL Categories] ページ



[URL Categories] ページには次の情報が表示されます。

表 5-6　[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）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
Top 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 5-6　[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、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。[Items Displayed] メニューから、リストに表示する URL カテゴリの数を変更できます。 [URL Categories] 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、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。 [URL Categories Matched] 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、[URL Category] セクション内で特定の URL カテゴリを検索できます。セクション下部のテキスト フィールドに特定の URL カテゴリ名を入力し、[Find URL Category] をクリックします。 [URL Categories] ページでの未分類の URL の比率は、通常 15 ～ 20% 程度です。未分類の URL の比率がこれを上回る場合は、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、「カスタム URL カテゴリ」（P.5-33）を参照してください。

[URL Categories] ページから、ページの各セクションを印刷したり、CSV ファイルにエクスポートしたりすることもできます。ファイルを印刷またはエクスポートする方法の詳細については、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

（注）　[URL Categories] 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、「レポートのスケジューリング」（P.5-83）を参照してください。さらに、URL カテゴリに関してより詳細なレポートを生成できます。「Top URL Categories — Extended」（P.5-87）および「Top Application Types — Extended」（P.5-88）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。欠落が存在しない場合は何も表示されません。

[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] ページの利点の 1 つは、[Application Visibility] ページおよび [Users] ページと組み合わせて使用して、特定のユーザだけでなく、特定のユーザがアクセスを試みているアプリケーションまたは Web サイトのタイプも調査できることです。

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。同じページのインタラクティブな [URL Categories] 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、特定のユーザの使用状況が目立っているので、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関する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：アクセスの多い URL カテゴリの調査」（P.D-8）を参照してください。

カスタム URL カテゴリ

Security Management アプライアンスでは、Web セキュリティ アプライアンスと同様に、多数の定義済み URL カテゴリ（Web-based Reporting など）がデフォルトで用意されています。ただし、特定のホスト名と IP アドレスを指定する、ユーザ定義のカスタム URL カテゴリを作成することもできます。内部サイトや確実に信頼できる外部サイトのグループには、カスタム URL カテゴリを作成することを推奨します。

（注）Security Management アプライアンスでは、先頭に文字「c_」が付加されたカスタム URL カテゴリ名の最初の 4 文字が、アクセス ログで使用されます。Sawmill for Cisco IronPort を使用してアクセス ログを解析する場合は、カスタム URL カテゴリの名前に注意してください。カスタム URL カテゴリの最初の 4 文字にスペースが含まれていると、Sawmill for Cisco IronPort はアクセス ログ エントリを正しく解析できません。Sawmill for Cisco IronPort を使用してアクセス ログを解析する場合は、この最初の 4 文字に、サポートされている文字のみを使用してください。カスタム URL カテゴリの完全な名前をアクセス ログに記録する場合は、%XF フォーマット指定子をアクセス ログに追加します。

複数のカスタム URL カテゴリを作成し、各カテゴリに同じ URL を含めることができます。カスタム URL カテゴリの順序は重要です。リストの上位にあるカテゴリが、下位にあるカテゴリよりも優先されます。これらのカスタム URL カテゴリを同じアクセス ポリシー グループ、復号化ポリシー グループ、または Cisco IronPort Data Security ポリシー グループに入れ、各カテゴリに異なるアクションを定義した場合は、より上位にあるカスタム URL カテゴリのアクションが有効となります。

カスタム URL カテゴリを作成、編集、または削除するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Configuration Master 7.1] > [Custom URL Categories] を選択します。

[Custom URL Categories] ページが表示されます。

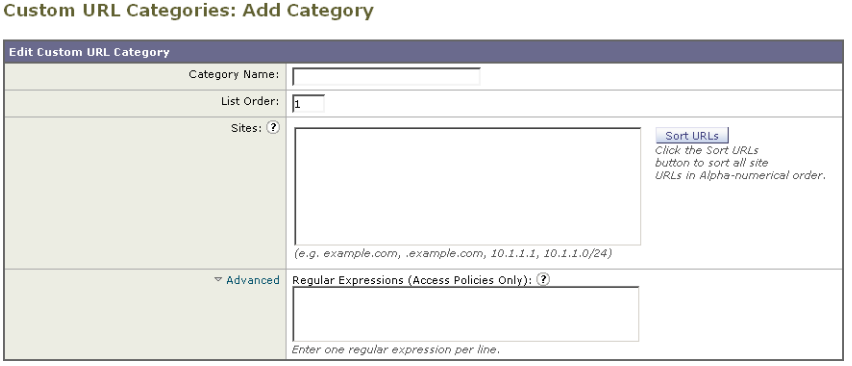
既存のカスタム URL カテゴリを編集するには、URL カテゴリの名前をクリックします。カスタム URL カテゴリを削除するには、削除するカスタム URL カテゴリの横にあるごみ箱をクリックします。

図 5-6　[Custom URL Categories] ページ

ステップ 2　カスタム URL カテゴリを作成または編集するには、[Add Custom Category] をクリックします。

[Create Custom URL Categories: Add Category] ページが表示されます。

図 5-7　カスタム URL カテゴリの作成



ステップ 3　カスタム URL カテゴリを作成または編集するには、次の設定を該当するフィールドに入力します。

- [Category Name] : URL カテゴリの名前を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。

- [List Order] : カスタム URL カテゴリのリストにおけるこのカテゴリの順序をテキスト フィールドに入力します。最上位の URL カテゴリには、**1** を入力します。URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。
- [Sites] : カスタム カテゴリに属する 1 つまたは複数のアドレスを入力します。

  複数のアドレスは、改行またはカンマで区切って入力します。アドレスは次のいずれかの形式を使用して入力できます。

  - IP アドレス。10.1.1.0 など
  - CIDR アドレス。10.1.1.0/24 など
  - ドメイン名。example.com など
  - ホスト名。crm.example.com など
  - ホスト名の一部。.example.com など

（注） .example.com などのホスト名の一部を入力すると、www.example.com も一致します。

- [Advanced] : [Regular Expressions] テキスト フィールドに、入力したパターンと一致する複数の Web サーバを指定するための正規表現を入力できます。

（注） URL フィルタリング エンジンでは、URL がまず [Sites] フィールドに入力したアドレスと比較されます。トランザクションの URL が [Sites] フィールドの入力内容と一致した場合は、ここで入力した式との比較は行われません。

ステップ 4　（任意）[Sort URLs] をクリックして、[Sites] フィールド内のすべてのアドレスをソートします。

[Sort URLs] をクリックすると、サイト URL が英数字順にソートされます。リスト順序でサイトに対して入力した元の順序は、ソートすると無効になります。

ステップ 5　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] をクリックしてアプライアンスへの変更を確定します。

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 は、次の URL の Cisco IronPort サポート ポータルに報告できます。

http://cisco.com/web/ironport/index.html

報告内容は、今後のルール アップデート用に評価されます。

Web レピュテーション フィルタリングと、アンチマルウェア フィルタリングがイネーブルになっていることを確認してください。

多くの場合、疑わしいコンテンツを含む URL とマルウェアの相関性は高く、今後のフィルタで検出される可能性が高くなります。URL フィルタリングで判定できない場合は、他のダウンストリーム フィルタで悪質なトラフィックが検出されるように、システム パイプラインが設定されます。この機能の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

[Application Visibility] ページ

（注） Application Visibility の詳細については、『*Cisco IronPort AsyncOS for Web 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、Security Management 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。

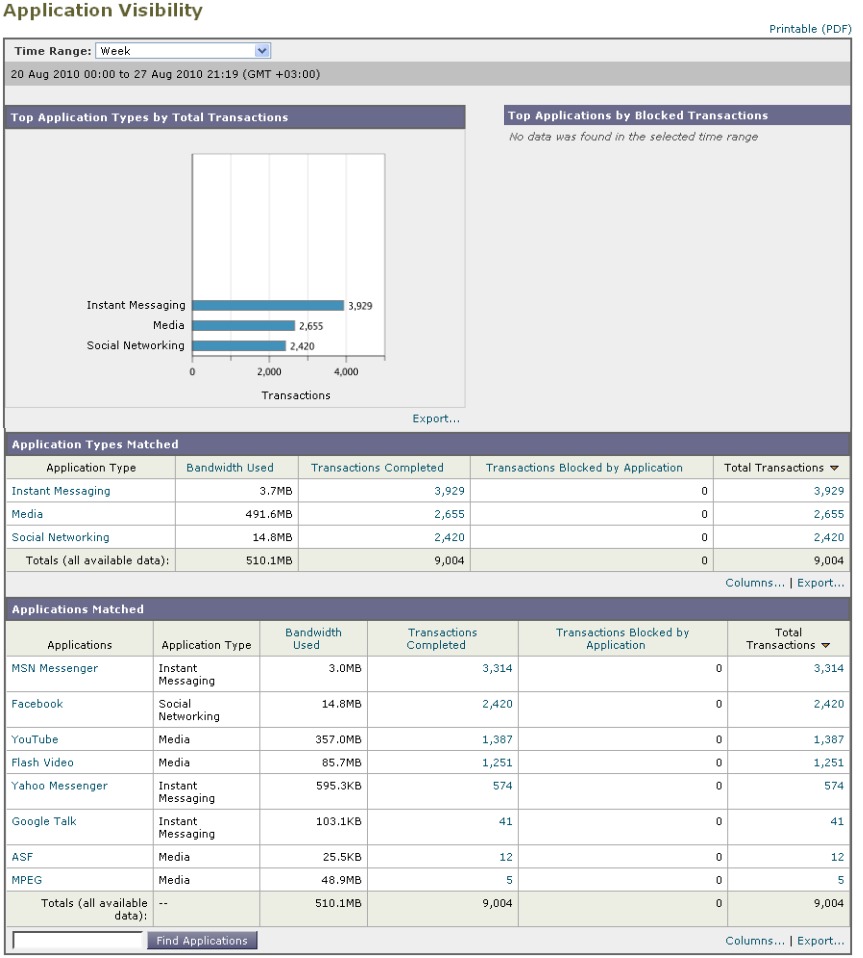
（注） Application Visibility and Control（AVC）エンジンを使用して Facebook アクティビティを制御する方法の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Understanding Application Visibility and Control」を参照してください。

[Application Visibility] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Application Visibility] を選択します。

[Application Visibility] ページが表示されます。

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 5-7　[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.3-18）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。

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

セクション	説明
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、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）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。

（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、「レポートのスケジューリング」（P.5-83）を参照してください。

[Anti-Malware] ページ

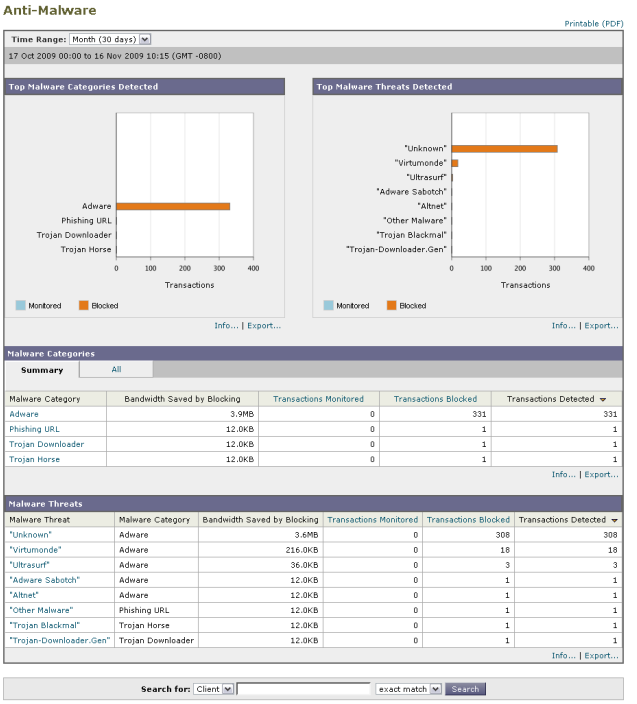
[Web] > [Reporting] > [Anti-Malware] ページは、特に DVS エンジン（WebRoot、Sophos、McAfee など）に基づいた、セキュリティ関連のレポーティング ページです。このページでは、さまざまな Web ベースのマルウェア脅威を識別および停止でき、検出されたマルウェアをモニタできます。

[Anti-Malware] 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　Security Management 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。

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 5-8　[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.3-18）を参照してください。
Top Malware Categories Detected	このセクションには、選択した DVS エンジンによって所定のカテゴリ タイプで検出された上位のマルウェア 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 5-9（P.5-45）を参照してください。
Top Malware Threats Detected	このセクションには、使用する DVS エンジンで検出された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 Detected] セクション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。 有効なマルウェア カテゴリの詳細については、表 5-9（P.5-45）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。

[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。

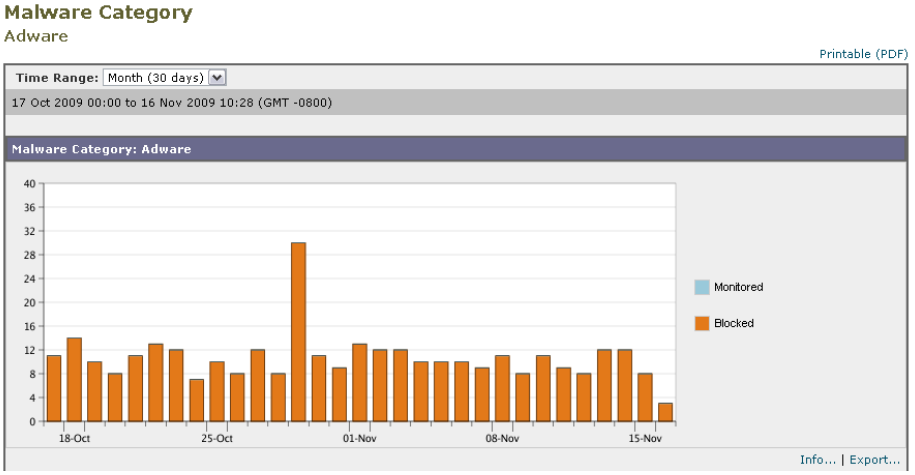
ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[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



[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。

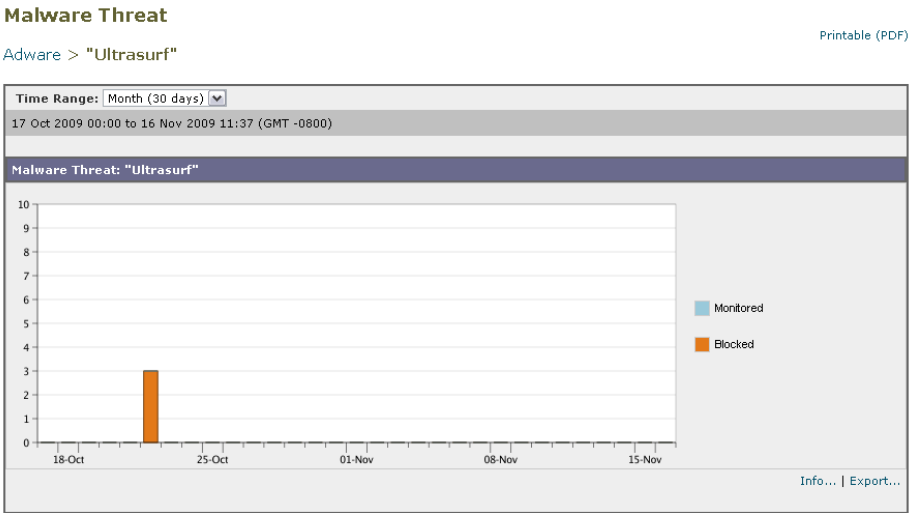
ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Anti-Malware] を選択します。

[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



（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、「レポートのスケジューリング」（P.5-83）を参照してください。

マルウェアのカテゴリについて

表 5-9 に、Security Management アプライアンスおよび 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

表 5-9　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。バリアントの中には、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。
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。
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。

表 5-9　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、通常はユーザが気付く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/サイトからダウンロードで命令を取得するため、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。
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。

アンチマルウェアの設定

（注） Security Management アプライアンスでアンチマルウェア機能を使用するには、事前に Web セキュリティ アプライアンスでグローバル設定を指定し、各種のポリシーに特定の設定を適用する必要があります。詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Configuring Anti-Malware Scanning」を参照してください。

アンチマルウェアを設定するには、まず次の 2 つの設定を指定する必要があります。

- **グローバルなアンチマルウェア設定。**オブジェクト スキャン パラメータを設定し、URL を照合するためのグローバル設定を指定します。さらに、どのようなときに URL をブロックするか、または処理の続行を許可するかを制御します。

- **アクセス ポリシーのアンチマルウェア設定。**マルウェア スキャンの判定に基づいたマルウェア カテゴリのモニタまたはブロックをイネーブルにします。

ステップ 1　Security Management アプライアンスのウィンドウで、[Configuration Master 7.1] > [Access Policies] を選択します。

[Access Policies] ウィンドウが表示されます。

ステップ 2　[Web Reputation and Anti-Malware Filtering] カラムで、設定するアクセス ポリシーのポリシー名のリンクをクリックします。

そのポリシーの [Access Policies: Reputation and Anti-Malware Settings] ウィンドウが表示されます。

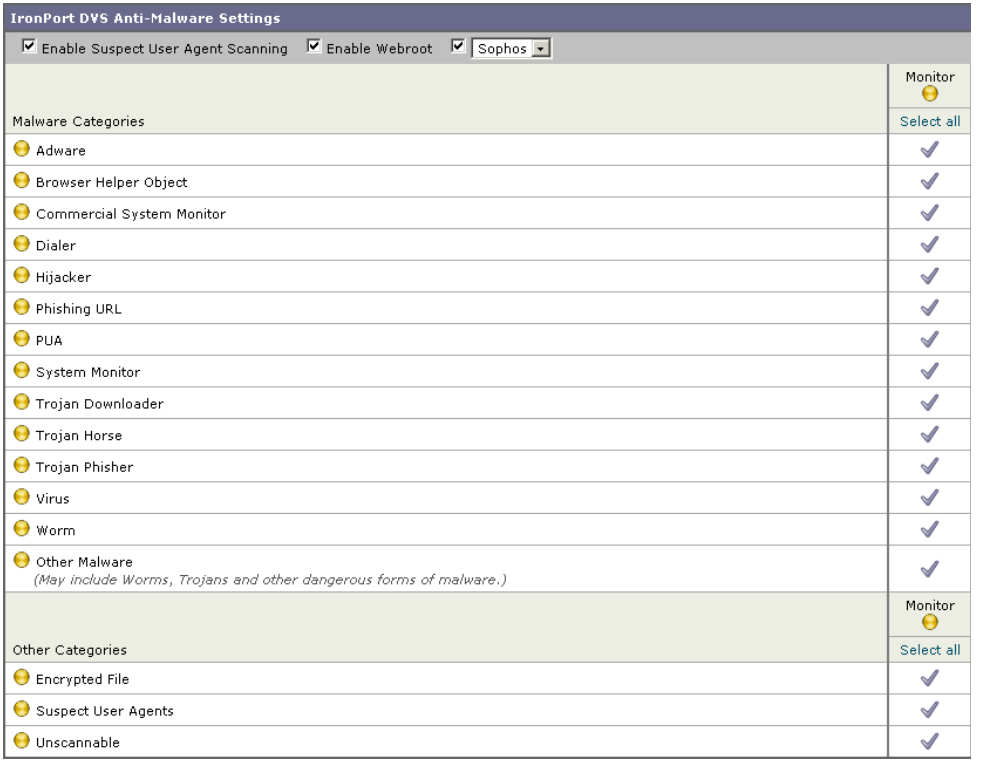
このページでは、マルウェア スキャンの判定に基づいたマルウェア カテゴリのモニタまたはブロックをイネーブルにすることができます。

ステップ 3　[Web Reputation and Anti-Malware Settings] セクションで、ドロップダウン メニューから [Define Web Reputation and Anti-Malware Custom Settings] を選択します（まだ選択されていない場合）。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーション設定およびアンチマルウェア設定を指定できます。

ステップ 4　[Cisco IronPort DVS Anti-Malware Settings] セクションで、ポリシーのアンチマルウェア設定を必要に応じて指定します。

図 5-12　アクセス ポリシーのアンチマルウェア設定



ステップ 5　ポリシーのアンチマルウェア設定を必要に応じて指定します。

表 5-10 に、アクセス ポリシーに対して指定できるアンチマルウェア設定を示します。

表 5-10　アクセス ポリシーに対するアンチマルウェア設定

設定	説明
Enable Suspect User Agent Scanning	HTTP 要求ヘッダーに指定されたユーザ エージェント フィールドに基づいて、アプライアンスがトラフィックをスキャンできるようにするかどうかを選択します。 この設定をオンにした場合は、ページ下部の [Additional Scanning] セクションで、疑わしいユーザ エージェントをモニタするかブロックするかを選択できます。
Enable Webroot	アプライアンスがトラフィックをスキャンする際に、Webroot スキャン エンジンを使用できるようにするかどうかを選択します。Webroot スキャンをイネーブルにすると、このページの [Malware Categories] で、追加カテゴリをモニタするかブロックするかを選択できます。
Enable Sophos	アプライアンスがトラフィックをスキャンする際に、Sophos スキャン エンジンを使用できるようにするかどうかを選択します。Sophos スキャンをイネーブルにすると、このページの [Malware Categories] で、追加カテゴリをモニタするかブロックするかを選択できます。
Enable McAfee	アプライアンスがトラフィックをスキャンする際に、McAfee スキャン エンジンを使用できるようにするかどうかを選択します。McAfee スキャンをイネーブルにすると、このページの [Malware Categories] で、追加カテゴリをモニタするかブロックするかを選択できます。

表 5-10　アクセス ポリシーに対するアンチマルウェア設定（続き）

設定	説明
Malware Categories	各種のマルウェア カテゴリを、マルウェア スキャンの判定に基づいてモニタするかブロックするかを選択します。 このセクションに表示されるカテゴリは、上でイネーブルにするスキャン エンジンによって異なります。
Additional Scanning	このセクションに表示されたオブジェクトおよび応答のタイプを、モニタするかブロックするかを選択します。 **注：**設定された最大時間に達するか、またはシステムが一時的なエラー状態に陥ると、URL トランザクションがスキャン不可と分類されます。たとえば、スキャン エンジンのアップデートや AsyncOS のアップグレードが行われている間は、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定である SV_TIMEOUT および SV_ERROR は、スキャン不可のトランザクションと見なされます。

ステップ 6　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] をクリックしてアプライアンスへの変更を確定します。

アンチマルウェアの詳細および Web セキュリティ アプライアンスでこの機能を設定する方法については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Configuring Anti-Malware Scanning」を参照してください。

[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。

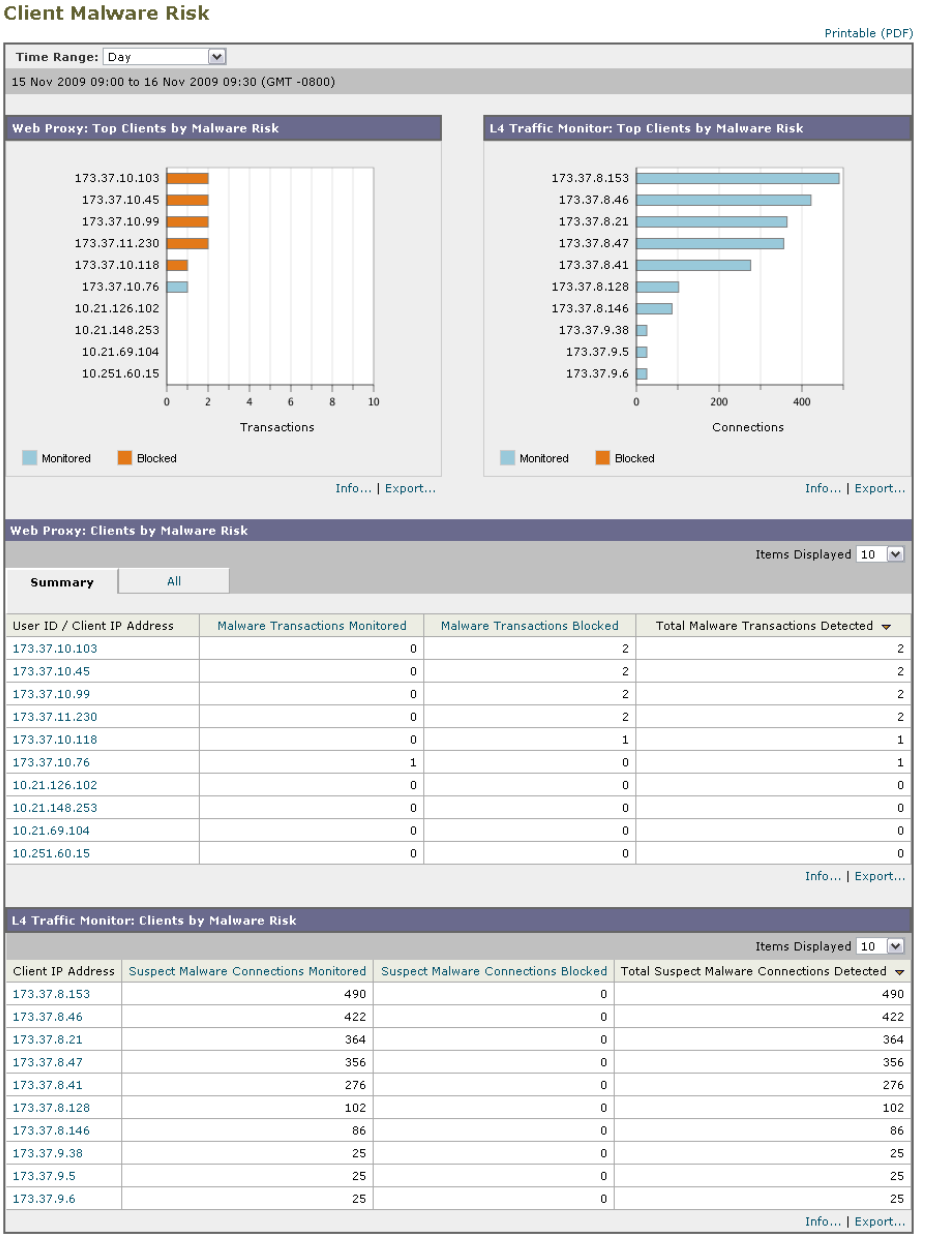
さらに [Client Malware Risk] ページでは、特定の IP アドレスの L4TM アクティビティを確認できます。

[Client Malware Risk] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Client Malware Risk] を選択します。

[Client Malware Risk] ページが表示されます。

図 5-13　[Client Malware Risk] ページ



[Client Malware Risk] ページには次の情報が表示されます。

表 5-11　[Web] > [Reporting] > [Client Malware Risk] ページの詳細

セクション	説明
Time Range（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
Web Proxy: Top Clients by Malware Risk	このセクションには、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。この情報はグラフ形式で表示されます。
L4 Traffic Monitor: Top Clients by Malware Risk	このセクションには、L4 トラフィック モニタリングのリスクが発生した上位 10 人のユーザが表示されます。この情報はグラフ形式で表示されます。
Web Proxy: Clients by Malware Risk	[Web Proxy: Clients by Malware Risk] インタラクティブ 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。 ユーザ ID とクライアント IP アドレスはインタラクティブになっており、各クライアントの詳細情報を提供する [Client Details] ページへのリンクがあります。クライアント ページの詳細については、[Client Details] ページを参照してください。 インタラクティブ テーブルのリンクをクリックすると、個々のユーザ、および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、ユーザ/IP アドレスのカラム内のリンクをクリックすると、その IP アドレスのユーザ ページが表示されます。
L4 Traffic Monitor: Clients by Malware Risk	[Web Proxy: Clients Malware Risk] インタラクティブ テーブルには、個々のユーザおよび L4 トラフィック モニタリング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に関する詳細情報が表示されます。ユーザ/IP アドレスのカラム内のリンクをクリックすると、その IP アドレスのユーザ ページが表示されます。

（注）　[Anti-Malware] 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、「レポートのスケジューリング」（P.5-83）を参照してください。

[Client Details] ページ

[Web Proxy: Clients by Malware Risk] セクションで個々のクライアントのハイパーテキスト リンクをクリックすると、特定のユーザのページが表示され、指定した時間範囲における特定のクライアントの Web アクティビティおよびマルウェア リスクのデータがすべて示されます。

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

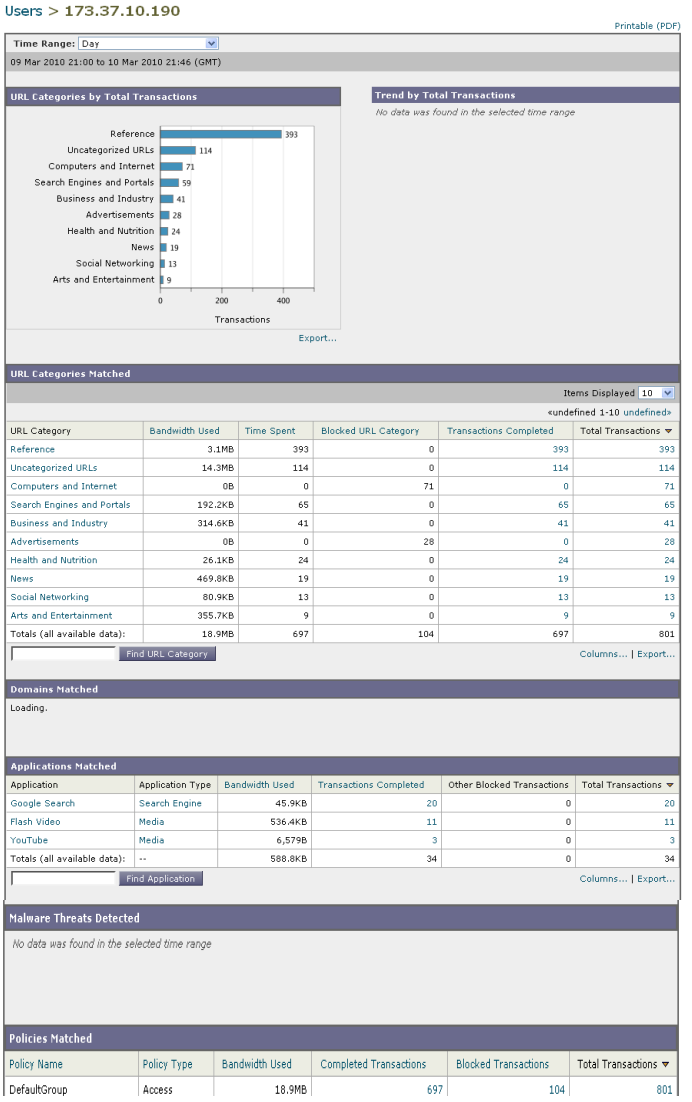
ステップ 1　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Client Malware Risk] を選択します。

[Client Malware Risk] ページが表示されます。

ステップ 2　[User/IP address] カラム内のリンクをクリックします。

[Client Details] ページが表示されます。

図 5-14　[Client Details] ページ



[Client Details] ページには次の情報が表示されます。

表 5-12　[Web] > [Reporting] > [Client Malware Risk] > [Client 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）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
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。
Trend by Total Transaction	このグラフには、特定のユーザの Web トランザクションの経時的なトレンドが示されます。基本的には、この特定のユーザがその Web にいつアクセスしたか、および閲覧トラフィックを送信した回数が示されます。 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、指定した時間範囲内にマルウェア リスクとなる可能性があった一致カテゴリがすべて表示されます。インタラクティブなカラム見出しを使用するとデータをソートできます。また、[Items Displayed] メニューによって、リストに表示される URL カテゴリの数を変更できます。 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。 URL カテゴリの詳細については、「[URL Categories] ページ」（P.5-28）を参照してください。

表 5-12　[Web] > [Reporting] > [Client Malware Risk] > [Client Details] ページの詳細（続き）

セクション	説明
Domains Matched	[Domains Matched] セクションでは、このユーザがアクセスした、マルウェア リスクの可能性がある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、マルウェア リスクの可能性がある特定のアプリケーションを確認できます。 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。システム管理者が、すべての Flash ビデオにマルウェア リスクがあると判断した可能性があります。このため、このアプリケーションは [Applications Matched] セクションに表示されます。 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。
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、マルウェア リスクの可能性がある上位のマルウェア脅威を確認できます。セクション下部のテキスト フィールドにマルウェア脅威の名前を入力し、[Find Malware Threat] をクリックします。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、この特定のユーザに適用され、特定のアクションを潜在的なマルウェア リスクと定義している特定のポリシーを確認できます。 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。

他の Web レポーティング ページと同様に、[Client Details] ページのすべてのテーブルでは、インタラクティブ リンクを通じて他の詳細情報を表示でき、ページのデータをユーザのニーズに合わせて表示できるように、対話型カラム見出しを設定して各カラムのデータをソートすることができます。カラムの設定の詳細については、「Web セキュリティ アプライアンス用のインタラクティブ レポート ページ」（P.5-10）を参照してください。

（注）　クライアント レポートで、ユーザ名の末尾にアスタリスク（*）が表示されることがあります。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。

[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

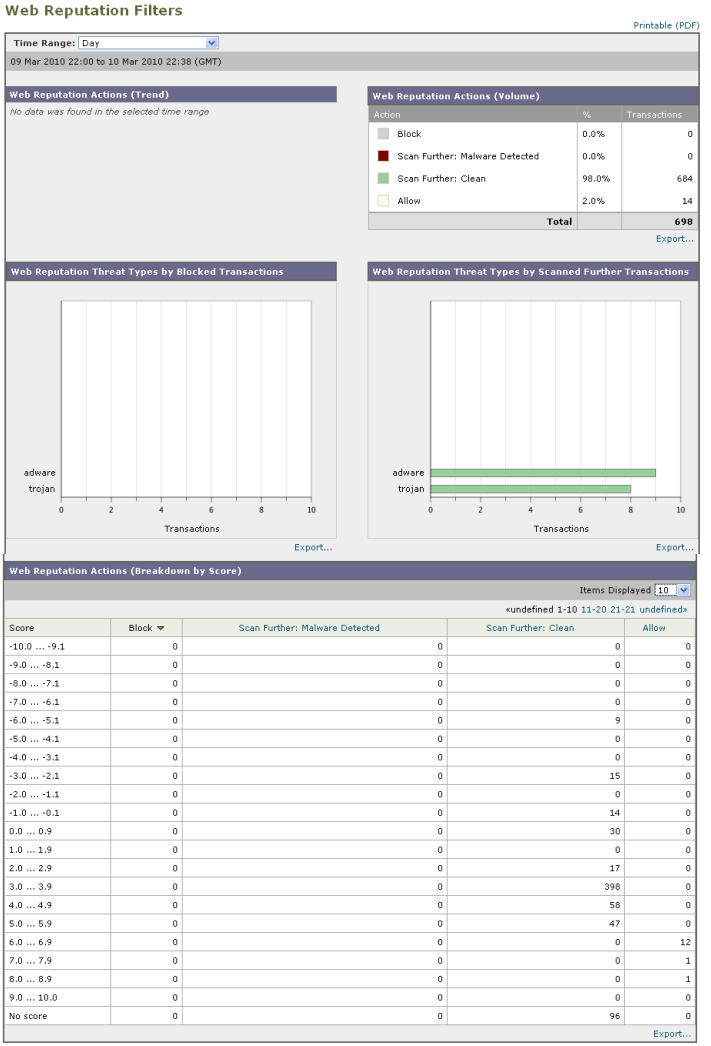
Web レピュテーション フィルタリングの詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Web Reputation Filters」を参照してください。

[Web Reputation Filters] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Reputation Filters] を選択します。

[Web Reputation Filters] ページが表示されます。

図 5-15　[Web Reputation Filters] ページ



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

表 5-13　[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.3-18）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	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」の場合は、トランザクションがアンチマルウェア 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)	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。

上記の最初の 4 つのセクションには、印刷可能なファイルにデータをエクスポートするための [Export] ハイパーテキスト リンクが表示されています。印刷可能なファイルについては、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

[Web Reputation Actions] テーブルには、設定可能なインタラクティブ カラムがあります。インタラクティブ カラムの設定の詳細については、「レポート ページのカラムの設定」（P.5-10）および「中央集中型 Web レポーティング ページのインタラクティブ カラム」（P.E-1）を参照してください。

Web レピュテーション スコアの設定

Security Management アプライアンスおよび Web セキュリティ アプライアンスをインストールしてセットアップすると、Web セキュリティ アプライアンスで Web レピュテーション スコアのデフォルトの設定が指定されます。ただし、Web レピュテーションのスコアを付けるためのこれらのしきい値の設定は、必要に応じて変更できます。

アクセス ポリシーおよび復号化ポリシーのグループに対して、Web レピュテーション フィルタの設定を指定する必要があります。

アクセス ポリシーに対する Web レピュテーション フィルタの設定

アクセス ポリシー グループに対する Web レピュテーション フィルタの設定を編集するには、次の手順を実行します。

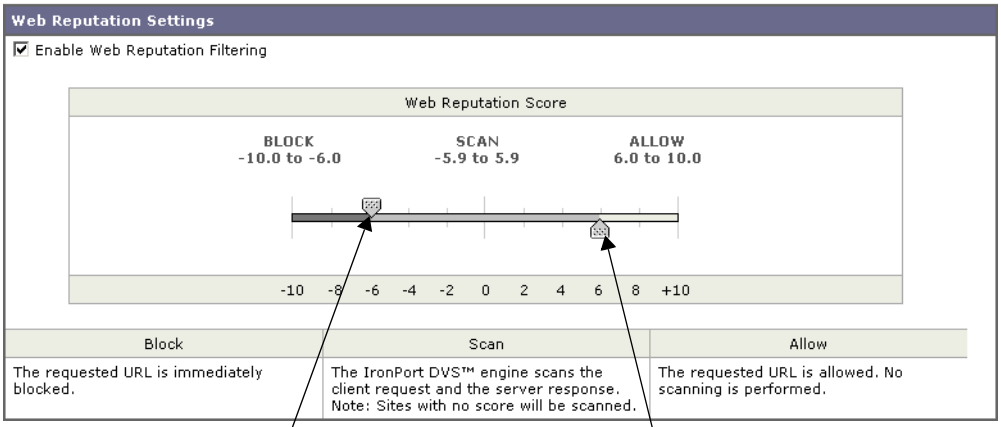
ステップ 1　Security Management アプライアンスのウィンドウで、[Configuration Master 7.1] > [Access Policies] を選択します。

ステップ 2　[Web Reputation and Anti-Malware Filtering] カラムで、編集するアクセス ポリシー グループのリンクをクリックします。

ステップ 3　[Web Reputation and Anti-Malware Settings] セクションで、[Enable Web Reputation Filters] チェックボックスをオンにします（オフになっている場合）。

[Web Reputation Score] ボックスが表示されます。

図 5-16　アクセス ポリシーに対する Web レピュテーション フィルタの設定



これにより、グローバル ポリシー グループの Web レピュテーションおよびアンチマルウェアの設定をオーバーライドできます。

ステップ 4　[Enable Web Reputation Filtering] チェックボックスがオンになっていることを確認します。

ステップ 5　マーカーを動かして、URL のブロック、スキャン、許可の各アクションの範囲を変更します。

ステップ 6　[Submit] をクリックしてページ上の変更を送信し、[Commit Changes] をクリックしてアプライアンスへの変更を確定します。

この時点で、復号化ポリシーに対して Web レピュテーションを設定する必要があります。復号化ポリシーに対する Web レピュテーション フィルタ設定の編集または指定については、『*Cisco IronPort AsyncOS for Web User Guide*』の「Web Reputation Filters」を参照してください。

[L4 Traffic Monitor Data] ページ

[Web] > [Reporting] > [L4 Traffic Monitor] ページは、指定した時間範囲内に L4 トラフィック モニタが検出したマルウェア ポートとマルウェア サイトに関する情報を表示する、セキュリティ関連のレポーティング ページです。

L4 トラフィック モニタは、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。

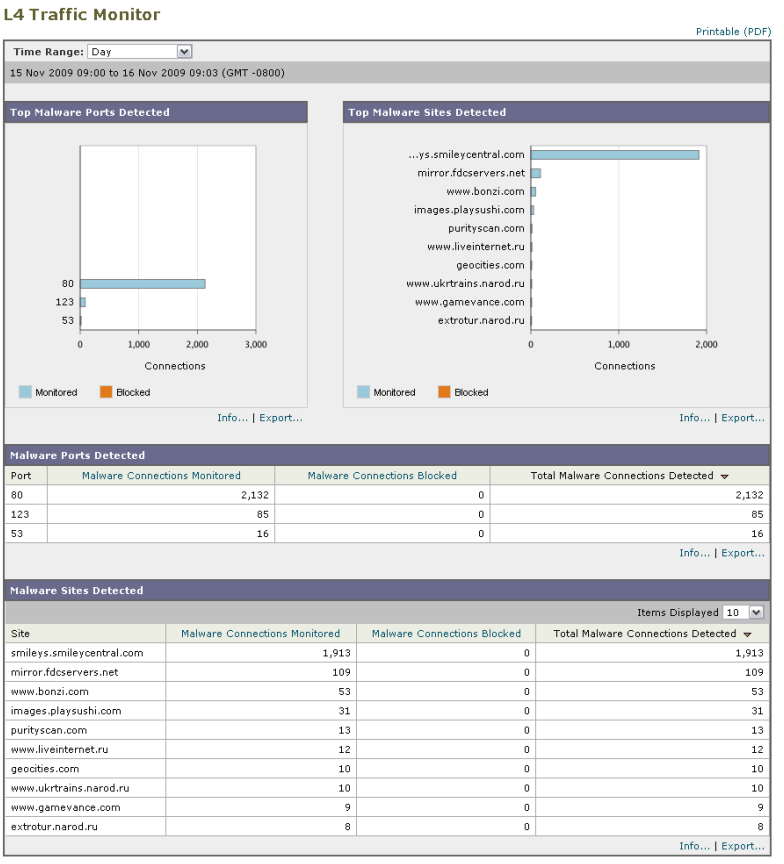
レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。

[L4 Traffic Monitor Data] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [L4 Traffic Monitor] を選択します。

[L4 Traffic Monitor] ページが表示されます。

図 5-17　[L4 Traffic Monitor] ページ



[L4 Traffic Monitor] ページには次の情報が表示されます。

表 5-14　[Web] > [Reporting] > [L4 Traffic Monitor] ページの詳細

セクション	説明
Time Range（ドロップダウン リスト）	1 ～ 90 日間またはカスタム日数範囲を指定できるドロップダウン リスト。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。
Top Malware Ports Detected	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 ポートがグラフ形式で表示されます。
Top Malware Sites Detected	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。 このビューでは、L4 トラフィック モニタによって検出された、モニタされたドメインまたはブロックされたドメインが、色分けされたグラフで表示されます。
Malware Ports Detected	[Malware Ports Detected] テーブルには、L4 トラフィック モニタによって検出されたすべてのポートが表示されます。
Malware Sites Detected	[Malware Sites Detected] テーブルには、L4 トラフィック モニタによって検出されたすべてのドメインが表示されます。

上記のすべてのセクションには、印刷可能なファイルにデータをエクスポートするための [Export] ハイパーテキスト リンクが表示されます。印刷可能なファイルについては、「レポート ページからのレポートの印刷」（P.5-11）を参照してください。

L4 トラフィック モニタの設定

L4 トラフィック モニタは、Security Management アプライアンスのシステム セットアップ ウィザード（[Management Appliance] > [System Administration] > [System Setup Wizard] を選択）を使用した初期システム セットアップの中で、イネーブルにすることができます。

デフォルトでは、L4 トラフィック モニタがイネーブルになり、すべてのポートでトラフィックをモニタするように設定されます。これには、DNS やその他のサービスが含まれます。

正しいクライアント IP アドレスをモニタするには、ネットワーク アドレス変換（NAT）が行われる前にファイアウォール内で必ず L4 トラフィック モニタを設定する必要があります。

L4 トラフィック モニタの設定の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。システム セットアップ ウィザードの詳細については、「システム セットアップ ウィザードについて」（P.2-10）を参照してください。

（注）　[L4 Traffic Monitor] 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、「レポートのスケジューリング」（P.5-83）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。

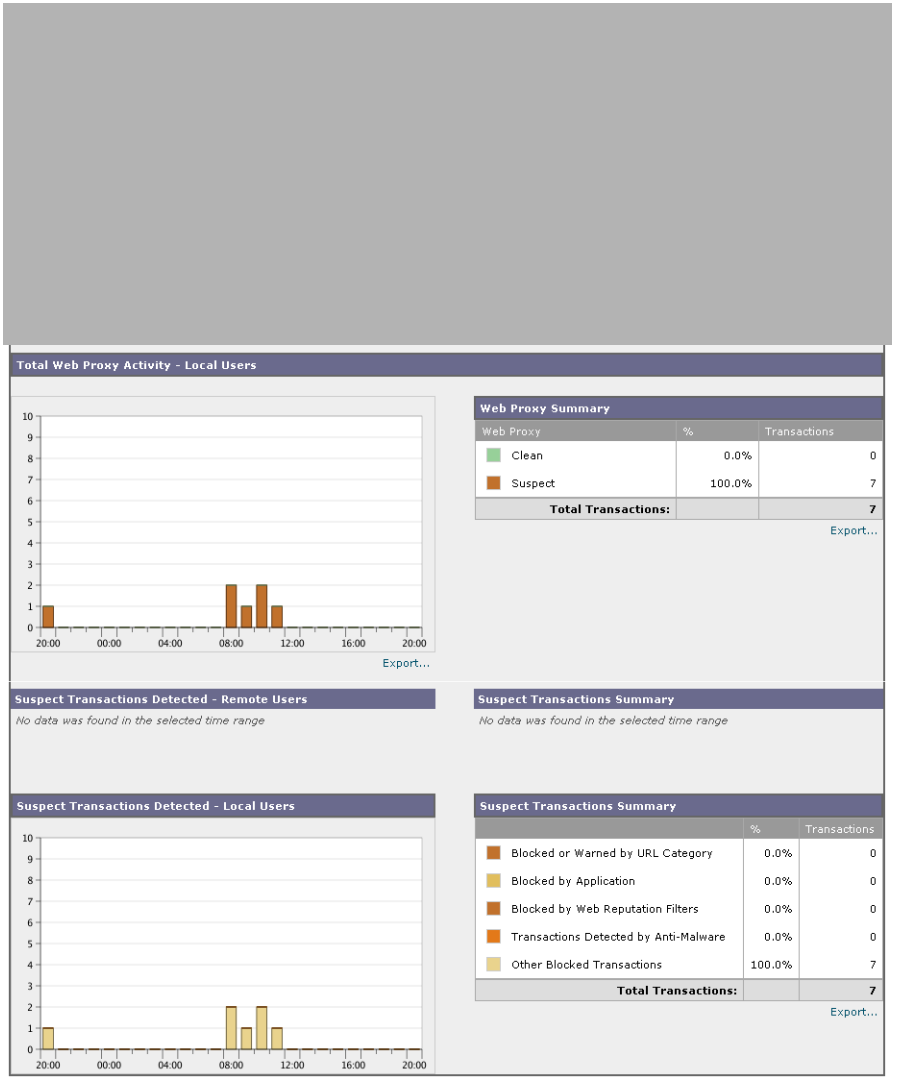
- ローカル ユーザおよびリモート ユーザがアクセスしている URL カテゴリ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザおよびリモート ユーザがアクセスしているアプリケーション。
- ユーザ（ローカルおよびリモート）。
- ローカル ユーザおよびリモート ユーザがアクセスしているドメイン。

[Reports by User Location] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Reports by User Location] を選択します。

[Reports by User Location] ページが表示されます。

図 5-18　[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 5-15　[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.3-18）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。

（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、「レポートのスケジューリング」（P.5-83）を参照してください。

[Web Tracking] ページ

[Web] > [Reporting] > [Web Tracking] ページでは、基本的な Web 関連情報（Web セキュリティ 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）をトラッキングし、表示することができます。これには、時間範囲やユーザ ID とクライアント IP アドレスなどの情報が含まれ、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。

マルウェア情報のフィルタリング、および WBRS のスコア範囲またはレピュテーション脅威による Web サイトのトラッキングも、Web トラッキングの重要な要素です。[Web Tracking] ページでは、これらすべての基準を検索し、モニタすることができます。Web トラッキングの結果からデータを除外する方法はありませんが、トラッキングする基準を決定した後に、基準をさらに追加して結果セットを絞り込むことができます。

[Web Tracking] ページでは、管理者がデフォルトの Web トラッキング結果ビューを使用してユーザに関する簡単な情報を確認したり、詳細な Web トラッキング結果ビューを使用してより詳細な情報を確認したりできるように設計されています。

[Web Tracking] ページを他の Web レポーティング ページと組み合わせて使用する例については、「[URL Categories] ページとその他のレポーティング ページの併用」（P.5-32）を参照してください。

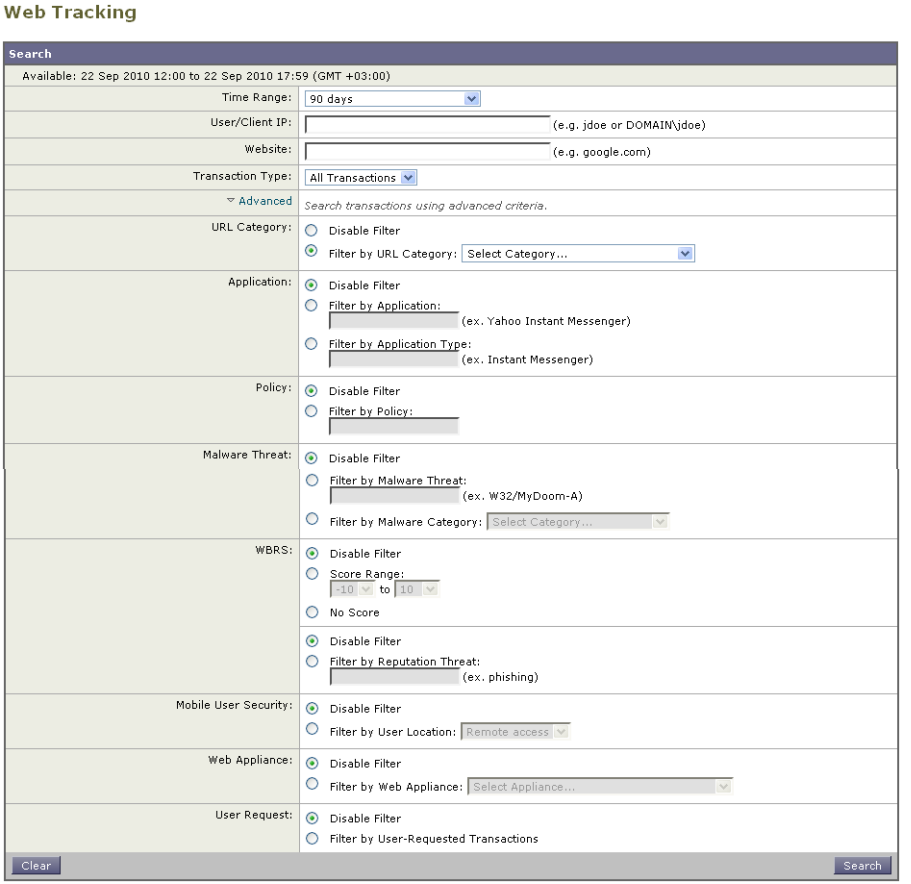
（注）　Web レポーティングでは、アクセスされる特定の URL に限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Web Tracking] ページを使用します。

[Web Tracking] 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　Security Management アプライアンスのウィンドウで、[Web] > [Reporting] > [Web Tracking] を選択します。

[Web Tracking] ページが表示されます。

図 5-19　[Web Tracking] ページ



（注）　上に示す [Web Tracking] ページは、[Advanced] の各フィールドが表示された状態のものです。

[Web Tracking] ページには次の情報が表示されます。

デフォルトの Web トラッキング結果

- 時間範囲
- ユーザ/クライアント IP

- Web サイト
- トランザクション タイプ

詳細な基準の Web トラッキング結果

- URL カテゴリ
- アプリケーション
- ポリシー
- マルウェアの脅威
- Web ベースのレポーティング システム（WBRS）
- モバイル ユーザのセキュリティ
- Web アプライアンス
- ユーザ要求

Web トラッキングの設定

Web トラッキング結果は、次の 2 つのビューで表示できます。

- デフォルトの Web トラッキング結果
- 詳細な Web トラッキング結果

デフォルトの Web トラッキング結果

デフォルトの Web トラッキング ビューでは、Web トラッキングの結果を、ユーザ名または IP アドレス、トランザクション タイプなどの基本的な基準でフィルタリングできます。

デフォルトの Web トラッキングの結果を収集するには、次の手順を実行します。

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

[Web Tracking] ページが表示されます。

ステップ 2　[Time Range] ドロップダウン リストで、トラッキングする時間範囲を選択します。

時間範囲および Security Management アプライアンスでの時間範囲の機能については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

ステップ 3　[User/Client IP] にユーザまたはクライアント IP アドレスを入力し [Website] フィールドに入力します。

これらの Web サイトおよびユーザまたはクライアント IP アドレスに関して、情報がトラッキングされます。

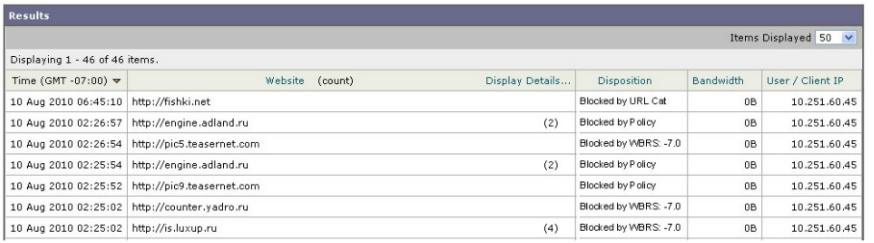
ステップ 4　[Transaction Type] ドロップダウン リストで、トラッキングするトランザクションのタイプを選択します。

選択肢は、[All Transactions]、[Completed]、[Blocked]、[Monitored]、[Warned] です。

ステップ 5　[Search] をクリックします。

デフォルト ビューの結果は、カラムで設定できません。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。デフォルト ビューの結果は、次のページのようになります。

図 5-20　デフォルトの Web トラッキング ビューの [Results] ページ


Results

Items Displayed 50

Displaying 1 - 46 of 46 items.

Time (GMT -07:00)	Website (count)	Display Details...	Disposition	Bandwidth	User / Client IP
10 Aug 2010 06:45:10	http://fishki.net		Blocked by URL Cat	0B	10.251.60.45
10 Aug 2010 02:26:57	http://engine.adland.ru	(2)	Blocked by Policy	0B	10.251.60.45
10 Aug 2010 02:26:54	http://pic5.teasernet.com		Blocked by WBRS: -7.0	0B	10.251.60.45
10 Aug 2010 02:25:54	http://engine.adland.ru	(2)	Blocked by Policy	0B	10.251.60.45
10 Aug 2010 02:25:52	http://pic9.teasernet.com		Blocked by Policy	0B	10.251.60.45
10 Aug 2010 02:25:02	http://counter.yadro.ru		Blocked by WBRS: -7.0	0B	10.251.60.45
10 Aug 2010 02:25:02	http://is.luxup.ru	(4)	Blocked by WBRS: -7.0	0B	10.251.60.45

[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 Web サイト

  [Transaction] カラムで [Display Details] をクリックすると、トランザクションに関する詳細情報が表示されます。
- Disposition

[Disposition] カラムには、トランザクションがブロックされた理由、つまりポリシーによってブロックされたのか、WBRS スコアによってブロックされたのかなどが表示されます。

- Bandwidth
- User ID/Client IP

詳細な Web トラッキング結果

詳細な Web トラッキング ビューでは、より詳細な基準を使用して Web トラッキングの結果をフィルタリングできます。たとえば、WBRS レピュテーション スコア、URL カテゴリ、Web レピュテーションの脅威などによってフィルタリングできます。

詳細な Web トラッキングの結果を収集するには、次の手順を実行します。

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

[Web Tracking] ページが表示されます。

ステップ 2　[Time Range] ドロップダウン リストで、トラッキングする時間範囲を選択します。

時間範囲および Security Management アプライアンスでの時間範囲の機能については、「インタラクティブ レポートの時間範囲の選択」（P.3-18）を参照してください。

ステップ 3　[User/Client IP] にユーザまたはクライアント IP アドレスを入力し [Website] フィールドに入力します。

これらの Web サイトおよびユーザまたはクライアント IP アドレスに関して、情報がトラッキングされます。

ステップ 4　[Transaction Type] ドロップダウン リストで、トラッキングするトランザクションのタイプを選択します。

選択肢は、[All]、[Completed]、[Blocked]、[Monitored]、[Warned] です。

ステップ 5　[Advanced] の矢印をクリックしてページを展開し、詳細な基準を表示します。

ステップ 6　[Filter by URL Category] の横のオプション ボタンをクリックして、URL カテゴリをディセーブルまたはイネーブルにします。

URL カテゴリによるフィルタリングをイネーブルにすると、[Filter By URL Category] ドロップダウン リストの選択肢を選択して、イネーブルにするカテゴリを選択できます。

ステップ 7　特定のポリシーでフィルタリングするには、[Filter by Policy] の横のオプション ボタンをクリックし、テキスト フィールドにポリシー名を入力します。

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。

ステップ 8　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] の横のオプション ボタンをクリックし、テキスト フィールドに脅威の名前を入力します。

ステップ 9　WBRS のスコア範囲を指定するには、[Score Range] の横のオプション ボタンをクリックします。

このフィルタをディセーブルにするには、[WBRS] セクションの [Disable Filter] オプション ボタンをクリックします。WBRS スコア範囲情報の詳細については、『*Cisco IronPort AsyncOS for Web User Guide*』を参照してください。

ステップ 10　レピュテーションの脅威で Web トラッキングをフィルタリングするには、[WBRS] セクションで [Filter by Reputation Threat] オプション ボタンをクリックします。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 11　特定のモバイル ユーザ セキュリティでフィルタリングするには、[Filter by User Location] の横のオプション ボタンをクリックし、テキスト フィールドに位置を入力します。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 12　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。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 13　特定のユーザ要求でフィルタリングするには、[Filter by User-Requested Transaction] 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。このフィルタをディセーブルにするには、このセクションの [Disable Filter] オプション ボタンをクリックします。

ステップ 14　ページ ビューの結果をイネーブルにするには、[Enable Page] ビューの結果の横にあるチェックボックスをオンにします。

ステップ 15　[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。

ステップ 16　[Transaction] カラムで [Display Details] をクリックすると、トランザクションに関する詳細情報が表示されます。

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-2）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 Security Management 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たものになっ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。これによって、設定の最適化または追加アプライアンスが、いつ必要になったかがわかります。
- 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。

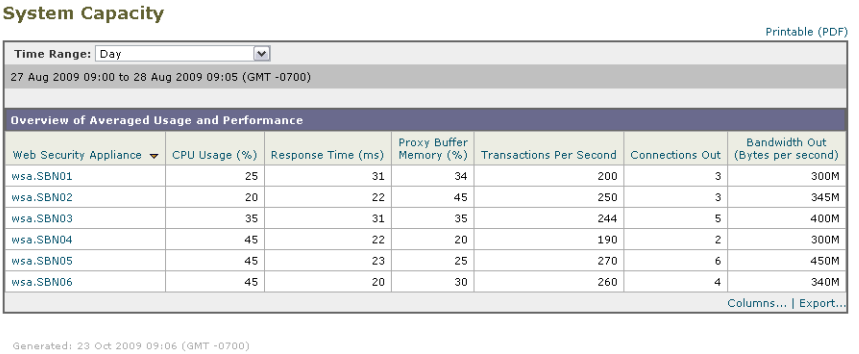
（注） 他のレポートで時間範囲に [Year] を選択した場合は、最も大きな時間範囲である 90 日を選択することを推奨します。

[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　Security Management 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 5-21　[System Capacity] ページ


System Capacity

Printable (PDF)

Time Range: Day

27 Aug 2009 09:00 to 28 Aug 2009 09:05 (GMT -0700)

Overview of Averaged Usage and Performance

Web Security Appliance	CPU Usage (%)	Response Time (ms)	Proxy Buffer Memory (%)	Transactions Per Second	Connections Out	Bandwidth Out (Bytes per second)
wsa.SBN01	25	31	34	200	3	300M
wsa.SBN02	20	22	45	250	3	345M
wsa.SBN03	35	31	35	244	5	400M
wsa.SBN04	45	22	20	190	2	300M
wsa.SBN05	45	23	25	270	6	450M
wsa.SBN06	45	20	30	260	4	340M

Columns... | Export...

Generated: 23 Oct 2009 09:06 (GMT -0700)

ステップ 2　[Overview of Averaged Usage and Performance] インタラクティブ テーブルの Web Security Appliance カラムで特定のアプライアンスをクリックし、そのアプライアンスのシステム キャパシティを表示します。

このユーザに関する [System Capacity] グラフが表示されます。[System Capacity] ページでは、次の 2 種類の情報を表示できます。

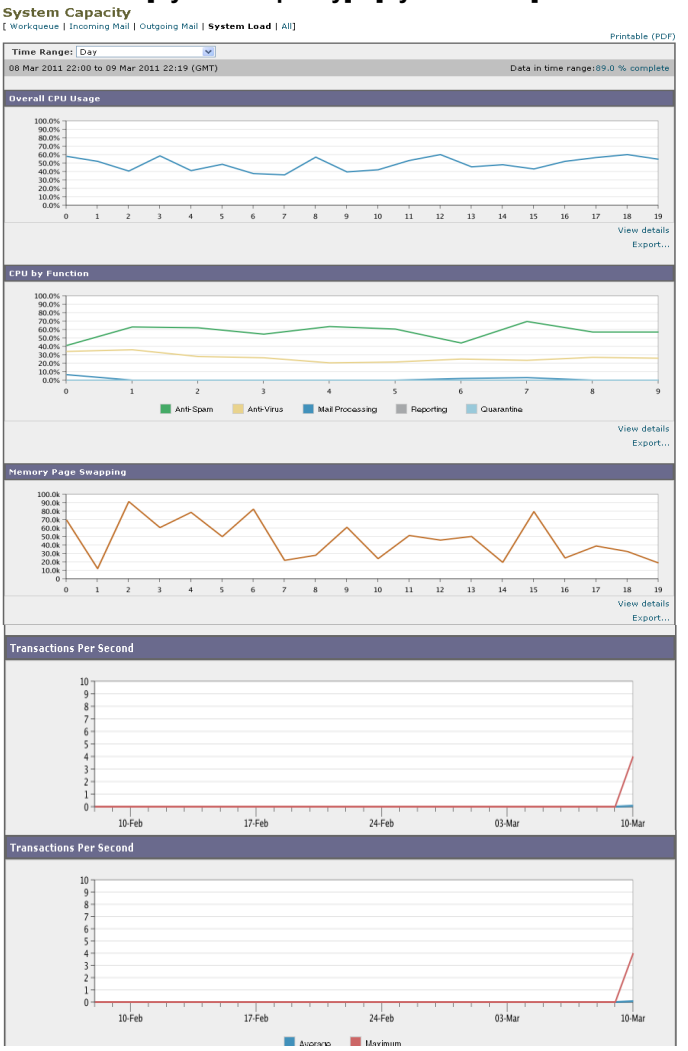
- [System Capacity] : [System Load]
- [System Capacity] : [Network Load]

[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 5-22　[System Capacity] : [System Load]

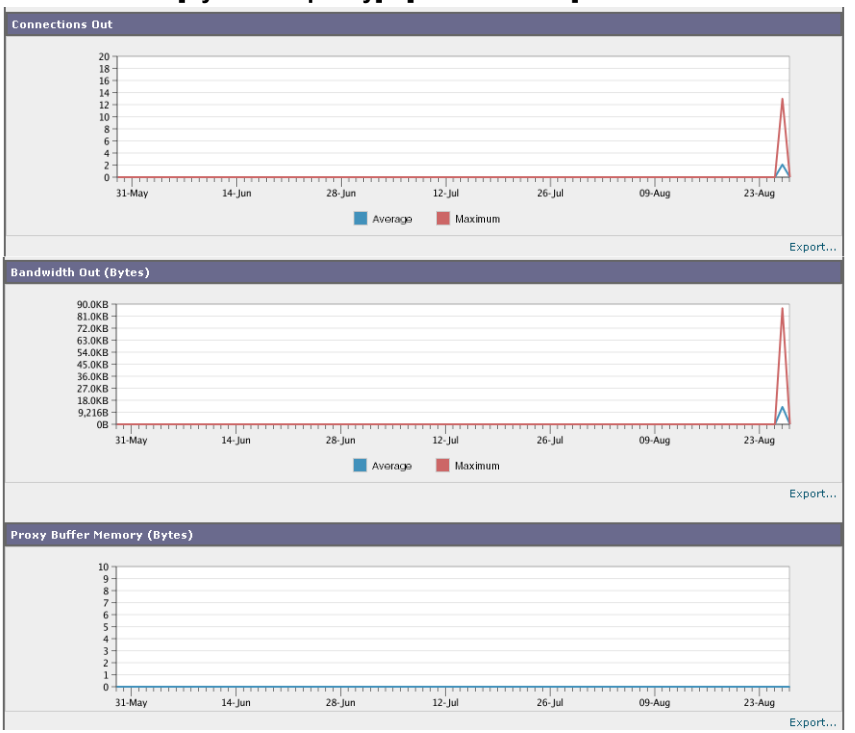


[System Capacity] : [Network Load]

[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。

図 5-23　[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 *常に* 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以外は、プロキシ バッファ メモリ スワッピングは正常であり、起こり得る挙動です。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。

[System Capacity] のカラム設定は、[System Capacity] ページの [Overview of Averaged Usage and Performance] セクションで指定できます。インタラクティブ カラムの設定の詳細については、「レポート ページのカラムの設定」（P.5-10）および「中央集中型 Web レポーティング ページのインタラクティブ カラム」（P.E-1）を参照してください。

[Data Availability] ページ

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

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

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

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

図 5-24　[Web Reporting Data Availability] ページ

Web Reporting Data Availability

Printable (PDF)

Web Reporting Data Range

	Web Reporting		Web Tracking and Reporting Detail			
Web Security Appliance	From	To	From	To	Missing Data	Status
wsa.SBN01	22 May 2009 10:20	06 Nov 2009 09:01	07 Aug 2009 10:01	06 Nov 2009 09:01	No	OK
wsa.SBN02	22 May 2009 10:20	06 Nov 2009 08:48	07 Aug 2009 10:01	06 Nov 2009 08:48	No	Not updated in 12 minutes
wsa.SBN03	22 May 2009 10:20	06 Nov 2009 08:57	07 Aug 2009 10:01	06 Nov 2009 08:57	No	OK
wsa.SBN04	22 May 2009 10:20	06 Nov 2009 08:57	07 Aug 2009 10:01	06 Nov 2009 08:57	No	OK
wsa.SBN05	22 May 2009 10:20	06 Nov 2009 08:57	07 Aug 2009 10:01	06 Nov 2009 08:57	Yes	OK
wsa.SBN06	22 May 2009 10:20	06 Nov 2009 08:59	07 Aug 2009 10:01	06 Nov 2009 08:59	No	OK
Overall:	**22 May 2009 10:20 (GMT -07:00)**	**06 Nov 2009 09:01 (GMT -08:00)**	**07 Nov 2009 10:20 (GMT -07:00)**	**07 Nov 2009 09:01 (GMT -08:00)**		

このページから、すべてのデータ リソース使用率および Web トラフィックの問題箇所を表示できます。

（注）　[Web Reporting Data Availability] ページでは、個々の Web アプライアンスおよび電子メール アプライアンス上で Web レポーティングと電子メール レポーティングの両方がディセーブルになっている場合にのみ、Web レポーティングがディセーブルと報告されます。Web レポーティングがディセーブルになると、Security Management 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 Security Management 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.12-123）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。

さらに、Web レポーティングまたは Web トラッキングのいずれかで設定された範囲全体にギャップがある場合は、[Missing Data] カラムに「Yes」が表示されます。

ステップ 2　Web Security Appliance カラムで、データ アベイラビリティ情報が必要な特定のアプライアンスをクリックします。

そのアプライアンスの [Web Reporting Data Availability] が表示されます。このウィンドウには次の情報が表示されます。

- 受信したデータ
- この特定のアプライアンスの有効な日付範囲。
  この情報は [Overview] ページにも反映されます。[Web Reporting] セクションと [Web Tracking and Reporting Details] セクションの [From] および [To] の各見出しはハイパーリンクになっており、特定のユーザの特定の Web 詳細情報を表示することができます。

  データは、特定の期間における時間間隔についてのみ表示されます。

ステップ 3　[Items Displayed] ドロップダウン メニューから、表示するレコード数を選択できます。

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

（注） 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。

レポートのスケジューリング

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。

レポートをスケジュール設定できるレポート タイプは次のとおりです。

- [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.5-12）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.5-16）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.5-28）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.5-87）を参照してください。
- [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.5-36）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.5-88）を参照してください。
- [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.5-40）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.5-50）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.5-58）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 Data] ページ」（P.5-64）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.5-67）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.5-76）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管理

ここでは、次の内容について説明します。

- 「スケジュール設定されたレポートの追加」（P.5-85）
- 「スケジュール設定されたレポートの編集」（P.5-86）
- 「スケジュール設定されたレポートの削除」（P.5-86）
- 「追加の拡張レポート」（P.5-86）

（注）　スケジュール設定されたレポートでは、すべてのユーザ情報を認識できないようにすることができます。レポートでユーザ名が認識できない状態でレポートを生成するには、[Anonymize usernames in reports] チェックボックスをオンにします。デフォルト設定では、すべてのレポートにすべてのユーザ名が表示されます。

Security Management 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「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

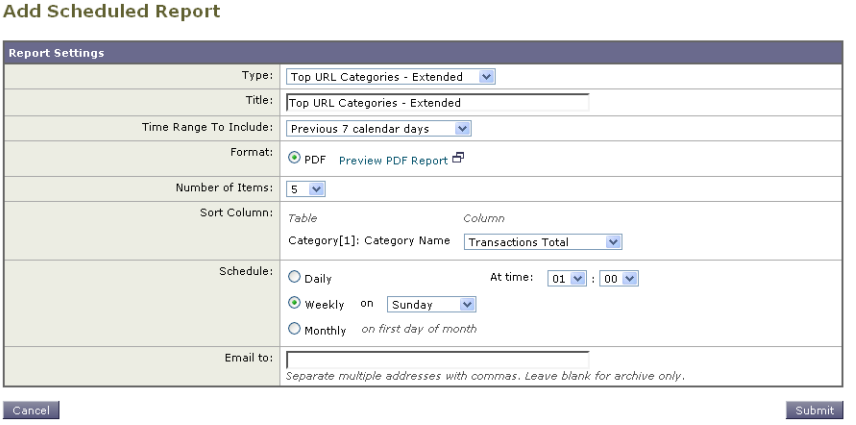
スケジュール設定された Web レポートを追加するには、次の手順を実行します。

ステップ 1　Security Management 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] ページが表示されます。

図 5-25　[Add Scheduled Reports] ページ



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

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。大部分のレポートでは、CSV のスケジューリングを行うことができます。

ステップ 7　[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　[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　[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 10　[Email] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

電子メール 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 11　[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

Security Management アプライアンスの [Web] > [Reporting] セクションでは、追加で 2 種類の拡張レポートを生成できます。次のものがあります。

- 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。しかし、ネットワーク管理者は、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 人のユーザの帯域幅使用状況をモニタする、詳細なレポートを必要としているとします。この場合管理者は、[Top URL Categories — Extend] レポートを使用します。

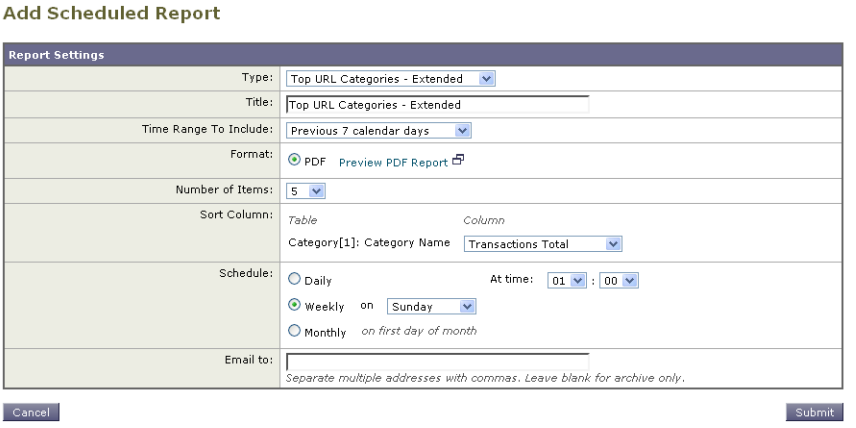
（注）　このタイプのレポートで生成できる最大レポート数は 20 です。

[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　Security Management 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 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　[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 10　[Email] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

ステップ 11　[Submit] をクリックします。

Top Application Types — Extended

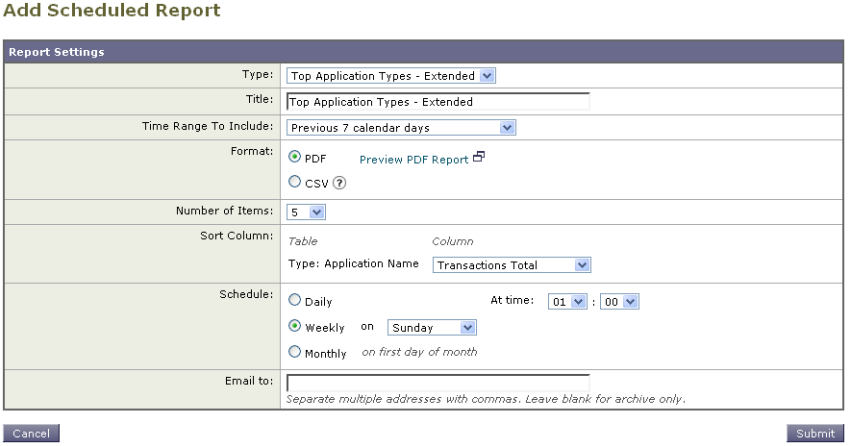
[Top Application Type — Extended] レポートを生成するには、次の手順を実行します。

ステップ 1　Security Management 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。



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、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　[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 10　[Email] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

ステップ 11　[Submit] をクリックします。

レポートのアーカイブ

[Web] > [Reporting] > [Archived Reports] ページには、使用可能なアーカイブ済みのレポートのリストが表示されます。[Report Title] カラムのレポート名はインタラクティブとなっていて、各レポートのビューにリンクしています。[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。

（注）　[Report Type] カラムに表示される各レポートは、ハイパーテキスト リンクになっています。このハイパーテキスト リンクをクリックすると、そのレポートに関する情報にアクセスできます。

また、インタラクティブなカラム見出しを使用して、各カラムのデータをニーズに合わせて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 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。

[Generate Report Now] オプション

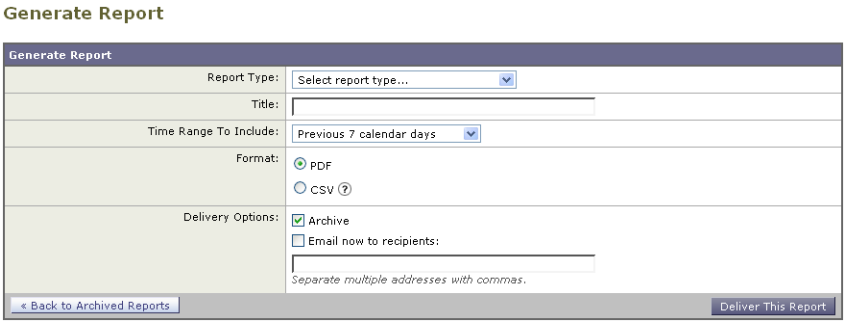
[Web] > [Archived Reports] ページの [Generate Report Now] オプションを使用すると、各レポート タイプのオンデマンド データ表示を生成できます。この機能を使用してレポートを生成するには、次の手順を実行します。

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

[Archived Reports] ページが表示されます。

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

図 5-26　オンデマンド レポートの生成



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。

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。

選択肢は次のとおりです。

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

ステップ 7　[Delivery Option] セクションから、次のオプションを選択します。

- [Archive Report] チェックボックスをオンにして、レポートをアーカイブします。

  このオプションを選択すると、レポートが [Archived Reports] ページに表示されます。

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

- 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 8　[Deliver This Report] をクリックして、レポートを生成します。