

снарте 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。



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

#### <u>》</u> (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。

Logged in as: admin on vmw002-esa03.run Options v Help and Support v

	Management Appliance	Email	Web						
	Centralized Services	Ne	twork	System Administration					
E	Edit Centralized Web Reporting Service Settings								
W	Web Reporting Service								
	✓ Enable Centralized Web Reporting Service								
	Usernames in Reports: Anonymize usernames in reports								
	If you turn off this service you will not be able to use the Centralized Web Reporting feature.								
	Cancel					Submit	I		

**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。



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。
	<ul> <li>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。</li> </ul>
	<ul> <li>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。</li> </ul>
	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 ビ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。



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)
- $[User Details] \sim \checkmark \downarrow (P.5-20)$
- 「[Web Sites] ページ」 (P.5-24)
- $\lceil [URL Categories] \sim \vee \rfloor$  (P.5-28)
- $\lceil [Application Visibility] \sim \lor \rfloor (P.5-36)$
- [Client Malware Risk]  $\sim \Im$  (P.5-50)
- [Web Reputation Filters]  $\sim \checkmark$  (P.5-58)
- $\lceil [L4 \text{ Traffic Monitor Data}] \sim \Im (P.5-64)$
- [Reports by User Location]  $\sim \checkmark$  (P.5-67)
- [Web Tracking]  $\sim \checkmark$  (P.5-70)
- $\lceil$  [System Capacity]  $\sim \Im$  (P.5-76)
- $\lceil \text{[Data Availability]} \sim \vee \rfloor (P.5-81)$

# 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。





[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。

<u>》</u> (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。

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

### 図 5-2 [Web] > [Reporting] > [Users] ページ

#### Users



[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。

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

#### 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。

#### <u>》</u> (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。



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。



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

		-				Printable (PD
Time Range: 90 days						
23 Apr 2010 00:00 to 22 J	J 2010 01:42 (GMT	+03:00)				
JRL Categories by Tota	l Transactions			Trend by To	tal Transactions	
				200		
				180 -		
				160 -		
				140 -		
				120 -		
Search Engines and F	ortals		95	100 -		
Business and Inc	dustry 📕 7			80 -		
Computers and In	ternet 🔳 5			60 -		
Advertise	ments 4			40 -		
Initasu	score s			20-		
	0 20 4	40 60 Turnanti	80 100	25	Apr 09-May 23-May 06-Jun	20-Jun 04-Jul 18-Jul
		Transacu	Ex	port		Export.
						_
JRL Lategories Matche	a tritter	1 7				
URL Category	Bandwidth Us	ed T	ime Spent	Blocked URL Category	Transactions Completed	Total Transactions v
Search Engines and Porta	ls 44	7.4KB	00:21	0	99	9
Business and Industry	1	5.5KB	00:06	5 0	7	
Computers and Internet	8	4.4KB	00:06	i 0	5	
Advertisements	1	6.9KB	00:00	0 0	4	
Infrastructure	4	,540B	00:00	0 0	3	
Totals (all available dat	ta): 561	8.6KB	00:33	3 0	118	11
	Follow Advance					orburne Lowert
Data below is not availab Jul 2010 23:59 (GMT +	le for the full time n 03:00). Click to ch	ange sele ange the t	cted. Data fo lime range o	r this table is available for 13 f this report to reflect the dat	<i>Jul 2010 01:00 to 14</i> available.	Change Time Range
Domain or IP	Bandwidth Used	Time	Spent	Transactions Completed	Transactions Blocked	Total Transactions 🔻
google.com	464.5K	в	00:36	101	. 5	10
gmodules.com	83.1K	в	00:06	4	. 0	
google-analytics.com	8,272	B	00:00	4	0	
doubleclick.net	15.1K	в	00:00		0	
kontera.com	6,391	B	00:06	2	0	
addthis.com	1,365	8	00:00	1	. 0	
augustrania com	1,231	.D	00:00		0	
candex ru	2,021	B	00:00		0	
	Find Domain or IP	1				Columns   Export.
						Coldminster   Export
Applications Matched						
No data was found in the	selected time range	2				
Malware Threats <u>Detec</u>	ted					
No data was found in the	selected time range	2				
Policies Matched						
Policy Name	Policy Type	Bandwid	th Used	Completed Transactions	Blocked Transactions	Total Transactions 🔻
DefaultGroup	Access		568.6KB	11	8 0	11
IONE	Access		0B		0 5	
Totals (all available dat	a):		568.6KB	11	8 5	12
	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	5-4	[Web] > [Rep	orting] > [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開 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 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	き)
-------	---	----

セクション	<ul> <li>説明</li> <li>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。</li> </ul>	
Domains Matched		
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



[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。

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

#### 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。



[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 た ゴリがグラフ形式で表示されます。	

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

### 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。
	<ul> <li>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。</li> </ul>

[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

#### Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

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。



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

#### **Custom URL Categories**

Custom URL Categories	
Add Custom Category	
No Custom URL Categories are defined.	

**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

Custom URL Categories: Add Category

Edit Custom URL Category		
Category Name:		
List Order:	1	
Sites: ①	(e.g. example.com, .example.com, 10.1.1.1, 10.1.1.0/24)	Sort URLS Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
≂ Advanced	Regular Expressions (Access Policies Only); (?)  Enter one regular expression per line.	

- **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



.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



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。



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

		-	_				Printable (PDF
Time Range: Week			~				
20 Aug 2010 00:00 to 27	Aug 20:	10 21:19 (GM	4T +03:00)				
Top Application Tupos	bu Tot	tal Transasi	tions		Т	an Applications by Blocked Trans	actions
Top Application Types	Dy TO	tai iraiisati	lions		N	o data was found in the selected time	range
Instant Mess Social Netwo	saging Media orking	0 2	2,655 2,420 2,000 4,000	229			
			Transactions				
				Export			
Application Types Mate	ched						
Application Type	E	3andwidth Us	ed Transact	ions Completed	Transa	actions Blocked by Application	Total Transactions 🔻
Instant Messaging			3.7MB	3,929		0	3,929
Media		49	1.6MB	2,655		0	2,655
Social Networking		1	4.8MB	2,420		0	2,420
Totals (all available dat	ta):	51	0.1MB	9,004		0	9,004
							Columns   Export
Applications Matched							
Applications	Applic	cation Type	Bandwidth Used	Transaction Completed	s	Transactions Blocked by Application	Total Transactions <del>▼</del>
MSN Messenger	Instar Messa	nt aging	3.0ME	5	3,314	(	3,314
Facebook	Social Netwo	l orking	14.8ME	5	2,420	(	2,420
YouTube	Media		357.0ME	5	1,387	(	1,387
Flash Video	Flash Video Media		85.7ME	1,251		(	1,251
Yahoo Messenger	Instar Messa	nt aging	595.3KE		574	(	574
Google Talk	Instar Messa	nt aging	103.1KE		41		41
ASF	Media		25.5KE	3	12	(	12
MPEG	Media		48.9ME	3	5	(	5
Totals (all available data):			510.1ME	8	9,004	(	9,004
	Find A	pplications					Columns   Export

### Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

[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。				

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。				

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



[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。

#### Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

[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
```

Time Range: Month (30	days) 🛩								
7 Oct 2009 00:00 to 16 N	ov 2009 10:15 (GMT -	-0800)							
op Malware Categorie:	s Detected		т	op Malware 1	hreats D	etected			
Adware Phishing UR. Trojan Downloader Trojan Horse	0 100 200 Trensact	300 400 tions		• "Trojan-	"Unl "Virtun "Ult Adware Sa " Other Ma Trojan Bla Downloade	nown" rasurf" Altnet" Iware" ckmal" r.Gen" 0 100	200 Trans-	0 300 actions	400
Monitored Blocks	rd .	Info   Eve		Monitored	Blocke	d		Info	LEvport
Monitored Blocks	ed .	Info   Exp	port	Monitored	Blocke	d		Info.	Export
Montored Blocks	ed	Info   Exp	port	Monitored	Blocke	d		Info.	Export
Monitored Blocks	411	Info   Exp	port	Monitored	Blocke	d		Info.	Export
Monitored Blocks	All Bandwidth Savad I	Info   Exp	port	Monitored	Blocke	d	Tran	Info.	Export
Montored Blocks	all Bandwidth Saved b	Info   Exp by Blocking 3.9MB	port Transactions	Monitored s Monitored	Blocke	d ctions Blocked 331	Tran	Info. sactions De	Expor tected <del></del> 3
Montored Blocks	all Bandwidth Saved b	Info   Exp by Blocking 3.9MB 12.0KB	port Transactions	Monitored s Monitored 0 0	Biocke	d ctions Blocked 331 1	Tran	Info. sactions De	Expor tected <del></del> 3
Montored Block alware Categories alware Category dware hishing URL rojan Downloader	All Bandwidth Saved b	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB	port	Monitored s Monitored 0 0	Blocke	d ctions Blocked 331 1 1	Tran	Info. Isactions De	Export tected <del>v</del> 3
Montored Elocke alware Categories Summary alware Category dware chishing URL rojan Downloader rojan Horse	All Bandwidth Saved b	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB 12.0KB	oort Transactions	Monitored S Monitored 0 0 0 0 0 0	Blocke	d ctions Blocked 331 1 1 1 1	Tran	Info. sactions De	Exportected v
Montored Blocks Summary alware Categories dware Category dware dware ojan Downloader ojan Horse	All Bendwidth Saved I	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB 12.0KB	port Transactions	Monitored s Monitored 0 0 0 0 0	Blocke	d ctions Blocked 331 1 1 1 1	Tran	Info. sactions De Info.	Expor
Montored Blocks slware Categories Summary alware Category Ware vishing URL rojan Downloader ojan Harse alware Threats	All Bandwidth Saved L	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB 12.0KB	port Transactions	Monitored s Monitored 0 0 0	Transa	d ctions Blocked 331 1 1 1	Tran	Info. sactions De Info.	Expor
Markord Book Summary Summary alware Category alware Category dware was alware Category nishing URL crojan Horse alware Threats alware Threat	All Bandwidth Saved b	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB 12.0KB	port Transactions red by Blocking	Monitored Monitored 0 0 0 0 0 0 0 0 0 0 0 0 0	Transa	d ctions Blocked 331 1 1 1 1 Transactions Blo	Tran	Info. sactions De Info.	Expor tected - 3   Expor
Markord Bocker Sammary data almare Category dware mshing ULL rojan Downloader rojan Horse almare Threats Joknown	All Bandwidth Saved I Malware Category Adware	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB 12.0KB 12.0KB	Transactions	Monitored Monitored 0 0 0 0 1 Transactions	Transa Monitored 0	d ctions Blocked 331 1 1 1 1 1 1 7 Transactions Blo	Tran cked T 308	Info.	Expor tected - 3   Expor Detected 3
Interior Categories Summary alware Category dware cojan Downloader ojan Downloader ojan Horse alware Threats Jakare Threats	All Bandwidth Saved L Bandwidth Saved L Malware Category Adware Adware	Info   Exp by Blocking 3.948 12.068 12.068 12.068 Bandwidth Sav	Port Transactions ved by Blocking 3.648 216.0KB	Monitored Monitored 0 0 0 Transactions	Blocke     Transa     Monitored     0 0	d ctions Blocked 331 1 1 1 Transactions Blo	Tran cked T 308 18	Info sactions De Info	Expor tected - 3   Expor Detected 3
Motived Booke Summary  Alvare Category Avare Avare Summary Son Downloader Opan Downloader Opan Horse Alvare Threat Alvare Threat Alvare Threat Hohown	All Bandwidth Saved I Bandwidth Saved I Malware Category Adware Adware Adware	Info   Exp by Blocking 3.948 12.0KB 12.0KB 12.0KB	ved by Blocking 3.64B 26.0KB 36.0KB	Monitored Monitored 0 0 0 0 0 0 0 0 0 0 0 0 0	Blocke     Transa     Monitored     0     0	d ctions Blocked 331 1 1 1 1 1 1 1	Tran Cked T 308 18 3	Info. sactions De Info.	Expor tected v 3   Expor
Interest of the second	All Bandwidth Saved L Bandwidth Saved L Adware Adware Adware Adware	Info   Exp 3.9/HB 12.0/KB 12.0/KB 12.0/KB	Anticipation of the second sec	Monitored o O O O Transactions	Monitored 0 0 0	d ctions Blocked 331 1 1 1 Transactions Blo	Tran cked T 308 18 3 1	Info. Info.	Exper tected - 3   Exper Detected 3
Motived Booke	All Bandwidth Saved b Bandwidth Saved b Malware Category Adware Adware Adware Adware	Info   Exp by Blocking 3.949 12.008 12.008 12.008 12.008	ved by Blocking 3.648 216.0KB 36.0KB 12.0KB 12.0KB	Monitored 0 0 0 0 0 0 0 0 0 0 0 0 0	Monitored 0 0 0 0	d ctons Blocked 331 1 1 1 1 Transactions Blo	Tran (ked T 308 18 3 1 1 1 1	Info. sactions De Info.	Exper tected - 3   Exper Detected 3
Mattored Bookers	All Bandwidth Saved L Bandwidth Saved L Adware Adware Adware Adware Adware	Info   Exp by Blocking 3.9MB 12.0KB 12.0KB 12.0KB 12.0KB	And the second s	Monitored  Monitored  Monitored  Transactions	Monitored 0 0 0 0 0 0	d ctions Blocked 331 1 1 1 1 1 1	Tren Cked T 308 3 1 1 1 1	Info. sactions De Info.	Exper tected - 3   Exper Detected 3
Motored Booke	Mainer Category Advare Advare Advare Advare Advare Advare Advare	Info   Exp by Blocking 3.949 12.048 12.048 12.048 12.048	2001 Transactions 3.648 216.045 36.046 12.046 12.046 22.046 12.046 12.046	Monitored	Monitored 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	d ctions Blocked 331 1 1 1 1 1 1 1 1 1 1	Tren Cked T 18 3 1 1 1 1 1 1	Info. sactions De Info.	Expor
Matored Booker Summary alware Category dware Category dware Category organ Downloader rojan Downloader rojan Downloader rojan Andre Threats indenom? 'intumonde' 'intumode' 'intumode' 'intumode' 'intumode' 'intervent	Malware Category Adware Adware Adware Adware Adware Adware Adware Phining URL Trojan Downloader	Info   Exp by Blocking 3.948 12.0KB 12.0KB 12.0KB	Transactions           Transactions           216 0/kB           3.6 MB           216 0/kB           12 0/kB	Monitored  Monitored  Monitored  Transactions	Monitored 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	d ctons Blocked 331 1 1 1 1 1 Transactions Blo	Tran Cked T 308 18 3 1 1 1 1 1 1 1 1 1 1 1 1 1	Info. sactions De Info.	Exper

[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 Category**

Adware



## [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

#### **Malware Threat**

Adware > "Ultrasurf"

Printable (PDF)



E) [Anti-Malware] ヘーンの [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
<b>アドウェア</b>	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



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)。

Web Access Policies: Reputation and Anti-Malware Settings: groupAuthPolicy

Web Reputation and Anti-Malware Settings
Define Web Reputation and Anti-Malware Custom Settings

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。

IronPort DVS Anti-Malware Settings	
🔽 Enable Suspect User Agent Scanning 🔽 Enable Webroot 🔽 Sophos 🗸	
	Monitor <del>()</del>
Malware Categories	Select all
le Adware	$\checkmark$
😝 Browser Helper Object	$\checkmark$
\varTheta Commercial System Monitor	1
\varTheta Dialer	<b>v</b>
\varTheta Hijacker	<b>V</b>
O Phishing URL	1
\varTheta PUA	<b>V</b>
\varTheta System Monitor	$\checkmark$
😝 Trojan Downloader	$\checkmark$
\varTheta Trojan Horse	<b>V</b>
😝 Trojan Phisher	$\checkmark$
\varTheta Virus	$\checkmark$
\varTheta Worm	$\checkmark$
Other Malware (May include Worms, Trojans and other dangerous forms of malware.)	~
	Monitor 😝
Other Categories	Select all
😝 Encrypted File	$\checkmark$
⊖ Suspect User Agents	$\checkmark$
😝 Unscannable	$\checkmark$

#### 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。

夜 5-10 ノンビベ ハリン―に対するアンナマルウェア設定(前	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
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**

										Printable (PDF
Time Range: Da	ay	V								
15 Nov 2009 09:00	0 to 16 Nov 2	009 09:30 (GMT -0800)								
Web Proxy: Top	Clients by M	talware Risk			L4 Traffic Moni	itor: To	op Client:	s by Malwa	are Risk	
173.37	10 103				173.33	7 8 1 5 3				
173.37	7 10 45				173.3	37 8 46				_
173.37	7 10 99				173.	37 8 21				
173.37.	11,230				173.3	37.8.47				
173.37.	10.118	-			173.3	37.8.41				
173.37	7.10.76				173.33	7.8.128				
10.21.1	26.102				173.33	7.8.146				
10.21.1	48.253				173.3	37.9.38				
10.21.	69.104				173	.37.9.5				
10.251	L.60.15				173	.37.9.6				
	0	2 4 6 8 1	0				0	200	400	
	Ū	Transactions						Contra	tions	
		Transactions						Conhei	aons	
Monitored	Blocked				Monitored	E Blo	ocked			
		Info	Export.						In	fo   Export
Web Proxy: Clier	nts by Malwa	are Risk								
									Items Disp	layed 10 💌
Summary	AШ									
Samary [										
User ID / Client IF	P Address	Malware Transactions Mon	itored	Malwar	e Transactions Blo	ocked	Total	Malware Tr	ansactions	Detected 👻
173.37.10.103			0			2				2
173.37.10.45			-			- 2				2
173.37.10.99			0			- 2				- 2
173.37.11.230			- 0			- 2				2
173.37.10.118			-			1				1
173 37 10 76			1							1
10 21 126 102			- 0							-
10.21.148.253			0			0				0
10.21.69.104			0			0				0
10.251.60.15			0			0				0
10.201.00.10		I	U			0			To	fo LExport
									10	ioni Fexportini
14 Traffic Monite	or: Clients-b	v Malware Risk								
2. Hunterroma	on-enencs D								Items Di	laved to feel
									Trems Disp	ayed to
Client IP Address	Suspect Mal	ware Connections Monitored	Suspect	Malware	Connections Block	ked T	otal Suspe	ect Malware	Connectio	ns Detected 🔻
173.37.8.153		490				0				490
173.37.8.46		422				0				422
173.37.8.21		364				0				364
173.37.8.47		356				0				356
173.37.8.41		276				0				276
173.37.8.128		102				0				102
173.37.8.146		86				0				86
173.37.9.38		25				0				25
173.37.9.5		25				0				25
173.37.9.6		25				0				25
									In	fo   Export

[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。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。



[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

#### Users > 173.37.10.190

Printable (PDF)						
Ilme Range: Day	2010 21,46 (CMT	· ·				
09 Mar 2010 21:00 to 10 Ma	F 2010 21:46 (GM)	)				
URL Categories by Total	Fransactions		Trend by Tot	al Transactions		
			No data was fo	ound in the selected time range	÷	
Refer	ence	393				
Uncategorized I	JRLs 114					
Computers and Inte	rnet 71					
Search Engines and Po	rtals 59					
Business and Indu	istry 🔜 41					
Advertisem	ents 28					
Health and Nutr	ntion 24					
Social Networ	king 13					
Arts and Entertainr	nent 9					
	0	200 400	-			
		Transactions				
		Fr	nort			
URL Categories Matched						
				Ib	ems Displayed 10 💌	
				<under< td=""><td>fined 1-10 undefined»</td></under<>	fined 1-10 undefined»	
URL Category	Bandwidth Use	d Time Spent	Blocked URL Category	Transactions Completed	Total Transactions 🔻	
Reference	3.	1MB 393	0	393	390	
Uncategorized URLs	14.	3MB 114	0	114	114	
Computers and Internet		0B 0	71	0	7:	
Search Engines and Portals	192.	2KB 65	0	65	65	
Business and Industry	314.	6KB 41	0	41	4:	
Advertisements		0B 0	28	0	28	
Health and Nutrition	26.	1KB 24	0	24	24	
News	469.	8KB 19	0	19	19	
Social Networking	80.	9KB 13	0	13	10	
Arts and Entertainment	355.	7КВ 9	0	9		
Totals (all available data):	18.	9MB 697	104	697	80:	
Find URL Category Columns   Export						
Domains Matched						
Loading.						
Applications Matched						
Application	Application Type	Bandwidth Used	Transactions Completed	Other Blocked Transactions	Total Transactions 🔻	
Google Search	Search Engine	45.9KB	20	0	20	
Flash Video	Media	536.4KB	11	0	1:	
YouTube	Media	6,579B	3	0	3	
Totals (all available data):		588.8KB	34	0	34	
Fi	nd Application				Columns   Export	
Malware Threats Detecte	d					
No data was found in the se	lected time range					
Policies Matched						
Policy Name	Policy Type	Bandwidth Used	Completed Transactions	Blocked Transactions	Total Transactions =	
Defenition	A	10 010	compressed in an auditoria	2		
DeraultGroup	ACCESS	18.9MB	69	/  104	801	

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

[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。

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。

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

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 Printable (PDF) Time Range: Day ¥ 09 Mar 2010 22:00 to 10 Mar 2010 22:38 (GMT) Web Reputation Actions (Trend) No data was found in the selected time range Block 0.0% 0 Scan Further: Malware Detected 0.0% 0 Scan Further: Clean 98.0% 684 Allow 2.0% 14 698 Total Export.. Web Reputation Threat Types by Blocked Transactions Web Reputation Threat Types by Scanned Further Transactions adware adware trojan trojan 📃 2 4 6 10 ż â 6 8 10 0 8 Transactions Transactions Export. Export. Web Reputation Actions (Breakdown by Score) Items Displayed 10 🗸 «undefined 1-10 11-20 21-21 undefined» Score Block 🔻 Scan Further: Malware Detected Scan Further: Clean Allow -10.0 ... -9.1 0 0 0 -9.0 ... -8.1 0 0 0 0 -8.0 ... -7.1 0 0 0 0 -7.0 ... -6.1 n 0 0 n -6.0 ... -5.1 0 0 9 -5.0 ... -4.1 0 0 0 0 -4.0 ... -3.1 0 0 0 -3.0 ... -2.1 0 15 0 0 -2.0 ... -1.1 0 0 0 0 -1.0 ... -0.1 0 0 14 0 0.0 ... 0.9 0 0 30 0 1.0 ... 1.9 0 0 0 0 2.0 ... 2.9 17 0 0 0 3.0 ... 3.9 0 0 398 0 4.0 ... 4.9 0 58 0 0 5.0 ... 5.9 0 0 47 0 6.0 ... 6.9 0 0 0 12 7.0 ... 7.9 0 0 0 1 8.0 ... 8.9 n 0 0 1 9.0 ... 10.0 0 0 0 0 No score 0 0 96 0 Export..

[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

							Printable (	PDF)
Time	Range: Day	~						
15 Nov	2009 09:00 to 16 Nov 2	009 09:03 (GMT -080	D)					
Тор Ма	alware Ports Detecte	d	Т	op Malware S	ites Detec	ted		
				VS	.smilevcentr	al.com		
				mi	rror.fdcserv	ers.net		
					www.bor	nzi.com		
				ima	ges.playsus	hi.com		
					puritysci	an.com		
					www.liveinte	rnet.ru		
					geociti	es.com		
	80			www	.ukrtrains.n	arod.ru		
	123			WW	w.gamevan	ce.com		
	53				extrotur.na	arod.ru		
	0 1,000	2,000 3,000				0	1,000 2,000	
	Con	nections					Connections	
Ma	nitored Blocked			Monitored	Blocked			
inter inter	Biocica Elocica			Monitorea	DIOCROU			_
		Info   Exp	iort				Info   Expor	t
maiwa	re Ports Detected							
Port	Malware Connec	tions monitored	Maiware C	Johnections Bi	оскеа		otal Malware Connections Detected	
80		2,132			U		2,3	05
123		85			U			00
53		16			U		Tefa I Furan	16
							Intel., J Expor	·
Malmar	re Sites Detected							
Turinu	ie sites beteeteu			_	_	_	Theme Discloyed 10	
0.14		Not see the				la al a d	Telefis Displayed 10	-
Site		maiware Connectio	ns monitored	Malware Co	nnections B	юскеа	Total Malware Connections Detected	110
mirror	Hereiters net		1,913			0	1,9	-13
mirror.	racservers.net		109			0		E9
	alaususki asas	53		0		0		33
nnayes	.praysusm.com	31		0		0		31
puricysi mana 6	ainternet ru	13		0		0		12
neocitic	encerneerd		10			0		10
geocide	ertraine pared ru		10			0		10
			10			0		10
extroty	r parod ru		9			0		7
670,000	rateroea e		0			0	Info   Even	• •
							ind   expor	Sec. 1

[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 <sup>-</sup>	Traffic I	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

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

[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。



[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。



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

Web Tracking

Search	
Available: 22 Sep 2010 12:00 to 22 Sep 2010 17:5	59 (GMT +03:00)
Time Range:	90 days 💌
User/Client IP:	(e.g. jdoe or DOMAIN\jdoe)
Website:	(e.g. google.com)
Transaction Type:	All Transactions 💌
	Search transactions using advanced criteria.
URL Category:	O Disable Filter
	Filter by URL Category: Select Category
Application:	Disable Filter
	Filter by Application:     (or Yahao Instant Mossenger)
	Eiter by Application Type:
	(ex. Instant Messenger)
Policy:	Disable Filter
	Filter by Policy:
Malware Threat:	Disable Filter
	(ex. W32/MyDoom-A)
	Filter by Malware Category: Select Category
WBRS:	<ul> <li>Disable Filter</li> </ul>
	Score Range:
	O No Score
	Disable Filter     Silter by Desutation Thready
	(ex. phishing)
Mobile User Security:	Oisable Filter
	O Filter by User Location: Remote access
Web Appliance:	Oisable Filter
	O Filter by Web Appliance: Select Appliance
User Request:	Oisable Filter
	O Filter by User-Requested Transactions
Clear	Search



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。

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド
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	~	1				
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。



[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

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 οк 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 οк wsa.SBN04 22 May 2009 10:20 06 Nov 2009 08:57 07 Aug 2009 10:01 06 Nov 2009 08:57 No ок wsa.SBN05 22 May 2009 10:20 06 Nov 2009 08:57 07 Aug 2009 10:01 06 Nov 2009 08:57 Yes ОK ок wsa.SBN06 22 May 2009 10:20 06 Nov 2009 08:59 07 Aug 2009 10:01 06 Nov 2009 08:59 No Overall: 22 May 2009 10:20 06 Nov 2009 09:01 (GMT -07:00) (GMT -08:00) 07 Nov 2009 10:20 07 Nov 2009 09:01 (GMT -07:00) (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。



[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

Printable (PDF)

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)



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

Report Settings	
Туре:	Top URL Categories - Extended 💙
Title:	Top URL Categories - Extended
Time Range To Include:	Previous 7 calendar days 💌
Format:	◎ PDF Preview PDF Report &
Number of Items:	5 🔍
Sort Column:	Table Column
	Category[1]: Category Name Transactions Total
Schedule:	○ Daily At time: 01 🕶 : 00 🕶
	📀 Weekly on Sunday 💌
	O Monthly on first day of month
Email to:	
	Separate multiple addresses with commas. Leave blank for archive only.
Cancel	Subm

Add Scheduled Report

- **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。 Add Scheduled Report

Report Settings	
Туре:	Top URL Categories - Extended 💌
Title:	Top URL Categories - Extended
Time Range To Include:	Previous 7 calendar days 🛛 💌
Format:	◎ PDF Preview PDF Report &
Number of Items:	5 🗸
Sort Column:	Table     Column       Category[1]: Category Name     Transactions Total
Schedule:	Daily         At time:         01 v :         00 v           Weekly on Sunday v   <
Email to:	Separate multiple addresses with commas. Leave blank for archive only.
Cancel	Submit

- **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。

Cisco IronPort AsyncOS 7.7 for Security Management ユーザ ガイド

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。 Add Scheduled Report

Report Settings		
Туре:	Top Application Types - Extended 💌	
Title:	Top Application Types - Extended	
Time Range To Include:	Previous 7 calendar days	
Format:	© PDF Preview PDF Report      □     CSV ⑦	
Number of Items:	5 💌	
Sort Column:	Table     Column       Type: Application Name     Transactions Total	
Schedule:	○ Daily         At time:         01 ♥ : 00 ♥           ⑨ Weekly         on         Sunday         ♥           ○ Monthly         on first day of month         ♥	
Email to:	Separate multiple addresses with commas. Leave blank for archive only.	
Cancel	Submit	

- **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

Generate Report

Generate Report	
Report Type:	Select report type 💌
Title:	
Time Range To Include:	Previous 7 calendar days 💌
Format:	© PDF ○ CSV ⑦
Delivery Options:	Archive Final now to recipients: Separate multiple addresses with commas.
Back to Archived Reports     Deliver This Report	

- **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。



- 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。