集約 Web レポーティングおよびトラッキングの使用

この章は、次の項で構成されています。

中央集中型Webレポーティングおよびトラッキングの概要

Cisco コンテンツ セキュリティ管理アプライアンスは、複数の Web セキュリティ アプライアンスのセキュリティ機能から情報を収集し、Web トラフィック パターンとセキュリティ リスクのモニタに使用できるデータを記録します。リアルタイムで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、レポートをスケジュール設定して、定期的に実行することもできます。また、レポーティング機能を使用して、rawデータをファイルにエクスポートすることもできます。

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

ドメイン

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

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

ユーザ

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

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

URL カテゴリ

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

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

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

一般

ロギング ページとレポーティング ページの詳細については、ロギングとレポーティングを参照してください。

（注） アクセスされた特定の URL だけでなく、ユーザが利用するすべてのドメイン情報を取得することができます。ユーザがアクセスしている特定の URL、その URL にアクセスした時刻、その URL が許可されているかどうかなどの情報を入手するには、[Webトラッキング（Web Tracking）] ページの Web プロキシ サービスによって処理されたトランザクションの検索 （52 ページ）を使用します。

（注） Web セキュリティ アプライアンスは、ローカル レポートが使用されている場合にのみデータを保存します。集約管理レポートが Web セキュリティ アプライアンスで有効な場合、Web セキュリティ アプライアンスはシステム容量とシステム ステータス データのみを保持します。中央集中型 Web レポーティングがイネーブルになっていない場合、生成されるレポートはシステム キャパシティとシステム ステータスだけです。

セキュリティ管理アプライアンスで Web レポーティング データを表示する方法は複数あります。

- インタラクティブ レポート ページを表示する場合は、[Web レポート（Web Reporting）] ページの説明 （6 ページ）を参照してください。
- レポートをオンデマンドで生成するには、オンデマンドでの Web レポートの生成 （49 ページ）を参照してください。
- レポートが定期的に繰り返し作成されるようにスケジュールを設定する場合は、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。
- 以前に実行されたレポート（スケジュール設定されたレポートとオンデマンドで生成されたレポートの両方）のアーカイブ版を表示する方法については、アーカイブ済みの Web レポートの表示と管理 （51 ページ）を参照してください。
- 個々のトランザクションに関する情報を表示するには、Web トラッキング（Web Tracking）（51 ページ）を参照してください。

中央集中型Webレポーティングおよびトラッキングの設定

中央集中型 Web レポーティングおよびトラッキングを設定するには、次の手順を順序どおりに実行します。

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

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

ステップ 2 セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）]>[ウェブ（Web）]>[集約管理レポート（Centralized Reporting）] を選択します。

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

a) [有効化（Enable）] をクリックします。

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

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

a) [設定の編集（Edit Settings）] をクリックします。
b) [中央集中型Webレポーティングサービスを有効にする（Enable Centralized Web Report Services）] チェックボックスを選択します。
c) Web レポートでのユーザ名の匿名化 （5 ページ）はここで実行することも、後で実行することもできます。

ステップ 5 変更を送信し、保存します。

Webセキュリティアプライアンスでの中央集中型レポーティングのイネーブル化

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

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

『AsyncOS for Cisco Web Security Appliances User Guide』の「Enabling Centralized Reporting」セクションを参照してください。

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

他の中央集中型管理機能を設定する際、すでにアプライアンスを追加したかどうかによって、ここでの手順は異なります。

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

ステップ 2 リストに、すでに Web セキュリティ アプライアンスを追加している場合は、次の手順を実行します。

a) Web Security Appliances の名前をクリックします。
b) [集約管理レポート（Centralized Reporting）] サービスを選択します。

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

a) [Webアプライアンスの追加（Add Web Appliance）] をクリックします。
b) [アプライアンス名（Appliance Name）] および [IP アドレス（IP Address）] テキスト フィールドに、Web セキュリティ アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注） [IP アドレス（IP Address）] フィールドに DNS 名を入力した場合でも、[送信（Submit）] をクリックすると、IP アドレスに変換されます。

c) [集約管理レポート（Centralized Reporting）] サービスがすでに選択されています。
d) [接続の確立（Establish Connection）] をクリックします。
e) 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[接続の確立（Establish Connection）] をクリックします。

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

f) 「Success」 メッセージがページのテーブルの上に表示されるまで待機します。
g) [テスト接続（Test Connection）] をクリックします。
h) テーブルの上のテスト結果を確認します。

ステップ 4 [送信（Submit）] をクリックします。

ステップ 5 中央集中型レポーティングをイネーブルにする各 Web Security Appliances に対してこの手順を繰り返します。

ステップ 6 変更を保存します。

Web レポートでのユーザ名の匿名化

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

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

ステップ 1 [管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [ウェブ（Web）] > [集約管理レポート（Centralized Reporting）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [レポートでユーザ名を匿名にする（Anonymize usernames in reports）] チェックボックスをオンにします。

ステップ 4 変更を送信し、保存します。

Web セキュリティ レポートの使用

Web レポーティング ページでは、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 アプライアンスに関する情報をモニタできます。

目的	参照先
レポートデータのアクセスおよび表示オプションを確認する	レポート データの表示方法
インタラクティブ レポート ページのビューをカスタマイズする	レポート データのビューのカスタマイズ
データ内の特定のトランザクションに関する情報を検索する	Web トラッキング（Web Tracking） （51 ページ）
レポート情報を印刷またはエクスポートする	レポーティング データおよびトラッキング データの印刷およびエクスポート
さまざまなインタラクティブ レポート ページについて理解する	[Web レポート（Web Reporting）] ページの説明 （6 ページ）
レポートをオンデマンドで生成する	オンデマンドでの Web レポートの生成 （49 ページ）
レポートが指定した間隔で所定の時刻に自動的に実行されるようスケジュールを設定する	スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）
アーカイブ済みのオンデマンド レポートとスケジュールされたレポートを表示する	アーカイブ済みの Web レポートの表示と管理（51 ページ）
データの収集方法を理解する	セキュリティ管理アプライアンスによるレポート用データの収集方法

[Web レポート（Web Reporting）] ページの説明

（注） [Webレポート（Web Reporting）] タブのどのオプションをオンデマンドまたはスケジュール済みレポートとして使用できるかについては、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。

表 *1 : [Web*レポート（*Web Reporting*）*]* タブの詳細

[Webレポート（Web Reporting）] メニュー	アクション
Web レポートの概要 （11 ページ）	[概要（Overview）] ページには、お使いの Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。詳細については、Web レポートの概要 （11 ページ）を参照してください。
[ユーザ（Users）] レポート（Web） （13 ページ）	[ユーザ（Users）] ページには複数の Web トラッキング リンクが表示され、各ユーザの Web トラッキング情報を確認できます。 [ユーザ（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。 [ユーザ（Users）]ページのインタラクティブな[ユーザ（Users）] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [ユーザの詳細（User Details）] ページに表示されます。 [ユーザの詳細（User Details）] ページでは、[ウェブ（Web）] > [レポート（Reporting）] > [ユーザ（Users）] ページのインタラクティブな [ユーザ（Users）] テーブルで指定したユーザについて具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。 詳細については、[ユーザ（Users）] レポート（Web） （13 ページ）を参照してください。システムにおける各ユーザの情報については、[ユーザの詳細（User Details）]（Web レポーティング）（15 ページ）
[ユーザ数レポート（User Count Report）]（Web）	[ユーザ数（User Count）] ページは、中央集中型レポーティングが有効な Web セキュリティ アプライアンスの認証されたユーザと認証されていないユーザの合計数に関する集約情報を提供します。このページには、直近の過去 30 日間、90 日間、および 180 日間のユニーク ユーザ数が表示されます。 （注） システムは、1 時間ごとに、認証されたユーザと認証されていないユーザの合計ユーザ数を計算します。

[Webレポート（Web Reporting）] メニュー	アクション
[Web サイト（Web Sites）] レポート （17 ページ）	[Webサイト（Web Sites）] ページでは、管理対象アプライアンスで発生しているアクティビティ全体を集約して表示できます。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。詳細については、[Web サイト（Web Sites）] レポート （17 ページ）を参照してください。
[URLカテゴリ（URL Categories）] レポート （18 ページ）	[URLカテゴリ（URL Categories）] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。 • トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL。 • 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブな列見出しのあるインタラクティブテーブルとなっていて、必要に応じてデータをソートできます。 詳細については、[URLカテゴリ（URL Categories）] レポート （18 ページ）を参照してください。
[アプリケーションの表示（Application Visibility）] レポート （21 ページ）	[アプリケーションの表示（Application Visibility）] ページでは、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンス内で特定のアプリケーション タイプに適用されているコントロールを適用し、表示できます。詳細については、[アプリケーションの表示（Application Visibility）] レポート （21 ページ）を参照してください。
[マルウェア対策（Anti-Malware）] レポート （23 ページ）	[マルウェア対策（Anti-Malware）] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、[マルウェア対策（Anti-Malware）] レポート （23 ページ）を参照してください。

[Webレポート（Web Reporting）] メニュー	アクション
[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート （27 ページ）	ファイル レピュテーションおよび分析データは3 つのレポーティング ページに表示されます。 詳細については、[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート （27 ページ）を参照してください。
[クライアント マルウェア リスク（Client Malware Risk）] レポート （33 ページ）	[クライアントマルウェアリスク（Client Malware Risk）] ページは、セキュリティ関連のレポーティングページです。このページを使用して、著しく頻繁にマルウェア サイトへ接続している可能性がある個々のクライアント コンピュータを特定できます。 詳細については、[クライアントマルウェアリスク（Client Malware Risk）] レポート （33 ページ）を参照してください。
[Web レピュテーション フィルタ（Web Reputation Filters）] レポート （34 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 レピュテーションフィルタ（Web Reputation Filters）] レポート （34 ページ）を参照してください。
[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 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 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 ページ）を参照してください。
[SOCKS プロキシ（SOCKS Proxy）] レポート （39 ページ）	宛先、ユーザなど、SOCKS プロキシ トランザクションのデータを表示できます。 詳細については、[SOCKS プロキシ（SOCKS Proxy）] レポート （39 ページ）を参照してください。
ユーザの場所別レポート（Reports by User Location） （40 ページ）	[ユーザの場所別のレポート（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、ユーザの場所別レポート（Reports by User Location） （40 ページ）を参照してください。

[Webレポート（Web Reporting）] メニュー	アクション
Web トラッキング（Web Tracking） （51 ページ）	[Web トラッキング（Web Tracking）] ページでは、次のタイプの情報を検索できます。 • Webプロキシサービスによって処理されたトランザクションの検索 （52 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）を追跡して表示できます。 これには、時間範囲、ユーザ ID、クライアント IP アドレスなどの情報が含まれるほか、特定のタイプの URL、各接続が占有している帯域幅の量、特定のユーザの Web 使用状況のトラッキングなどの情報も含まれます。 • L4 トラフィック モニタによって処理されたトランザクションの検索 （56 ページ） では、マルウェアの転送アクティビティに関与しているサイト、ポート、およびクライアント IP アドレスの L4TM データを検索できます。 • SOCKS プロキシによって処理されるトランザクションの検索 （57 ページ） では、SOCKS プロキシによって処理されたトランザクションを検索できます。 詳細については、Web トラッキング（Web Tracking） （51 ページ）を参照してください。
[システム容量（System Capacity）] ページ （41 ページ）	レポーティングデータをセキュリティ管理アプライアンスに送信する、全体的なワークロードを表示できます。 詳細については、[システム容量（System Capacity）] ページ （41 ページ）を参照してください。
[使用可能なデータ（Data Availability）] ページ （43 ページ）	各アプライアンスのセキュリティ管理アプライアンス上のレポーティング データの影響を把握できます。詳細については、[使用可能なデータ（Data Availability）] ページ （43 ページ）を参照してください。
[スケジュール設定されたレポート（Scheduled Reports）]	指定した時間範囲のレポートのスケジュールを設定できます。詳細については、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。
[アーカイブレポート（Archived Reports）]	指定した時間範囲のレポートをアーカイブできます。詳細については、アーカイブ済みの Web レポートの表示と管理 （51 ページ）を参照してください。

（注） ほとんどの Web レポーティング カテゴリでレポートをスケジュール設定できます。これには、拡張された上位 URL カテゴリおよび上位アプリケーション タイプに関する追加のレポートが含まれます。レポートのスケジュール設定の詳細については、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。

[滞留時間（Time Spent）] について

さまざまなテーブルの [滞留時間（Time Spent）] 列は、Web ページでユーザが費やした時間を表します。各URLカテゴリでユーザが費やした時間。ユーザを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザが費やした時間。

トランザクション イベントに「viewed」のタグが付けられる（ユーザが特定の URL に進む）と、[滞留時間（Time Spent）] の値の計算が開始され、Web レポーティング テーブルのフィールドとして追加されます。

費やされた時間を計算するため、AsyncOS はアクティブ ユーザごとに、1 分間のアクティビティに対して 60 秒という時間を割り当てます。この 1 分間の終わりに、各ユーザが費やした時間は、そのユーザが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザは各ドメインで 15 分ずつ費やしたと見なされます。

経過時間の値に関して、以下の注意事項を考慮してください。

- アクティブ ユーザは、アプライアンスを介して HTTP トラフィックを送信し、Web サイトにアクセスした、すなわち AsyncOS が「ページ ビュー」と見なす動作を行ったユーザ名または IP アドレスとして定義されています。
- AsyncOS では、クライアント アプリケーションが開始する要求とは逆に、ユーザが開始する HTTP 要求としてページ ビューを定義します。AsyncOS はヒューリスティック アルゴリズムを使用して、可能な限り効果的にユーザ ページ ビューを識別します。

単位は時間：分形式で表示されます。

Web レポートの概要

[ウェブ（Web）] > [レポート（Reporting）] > [概要（Overview）] ページでは、お使いの Web セキュリティ アプライアンスでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフやサマリー テーブルも含まれます。

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

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

表 2 : [ウェブ（*Web*）] > [レポート（*Reporting*）] > [概要（*Overview*）] ページの詳細

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。
[次のデータを参照（View Data for）]	概要データを表示する Web セキュリティ アプライアンスを選択するか、[すべての Web アプライアンス（All Web Appliances）] を選択します。 アプライアンスまたはレポーティング グループのレポート データの表示も参照してください。
[Webプロキシアクティビティ総数（Total Web Proxy Activity）]	このセクションでは、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される Web プロキシ アクティビティを表示できます。 このセクションには、トランザクションの実際の数（縦の目盛り）、およびアクティビティが発生したおよその日付（横の時間軸）が表示されます。
[Webプロキシの概要（Web Proxy Summary）]	このセクションでは、疑わしい Web プロキシ アクティビティまたは正常なプロキシアクティビティの比率を、トランザクションの総数も含めて表示できます。
[L4トラフィックモニタの概要（L4 Traffic Monitor Summary）]	このセクションでは、現在セキュリティ管理アプライアンスで管理されている Web セキュリティ アプライアンスによって報告される L4 トラフィックを報告します。
[疑わしいトランザクション（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。
[疑わしいトランザクションの概要（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。

セクション	説明
[総トランザクション数の上位URLカテゴリ（Top URL Categories by Total Transactions）]	このセクションには、ブロックされている上位 10 の URL カテゴリが表示されます。URL カテゴリのタイプ（縦の目盛り）、特定タイプのカテゴリが実際にブロックされた回数（横の目盛り）などがあります。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート （20 ページ）を参照してください。
[総トランザクション数の上位アプリケーションタイプ（Top Application Types by Total Transactions）]	このセクションには、ブロックされている上位アプリケーション タイプが表示されます。これには、実際のアプリケーション タイプ名（縦の目盛り）、特定のアプリケーションがブロックされた回数（横の目盛り）が含まれます。
[検出された上位マルウェアカテゴリ（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。
[ブロックまたは警告されたトランザクション数の上位ユーザ（Top Users Blocked or Warned Transactions）]	このセクションには、ブロックされたトランザクションまたは警告が発行されたトランザクションを生成している実際のユーザが表示されます。ユーザは IP アドレスまたはユーザ名で表示できます。ユーザ名を識別できないようにするには、Web レポートでのユーザ名の匿名化 （5 ページ）を参照してください。

[ユーザ（Users）] レポート（Web）

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

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

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

[ユーザ（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 3 : [ウェブ（*Web*）] > [レポート（*Reporting*）] > [ユーザ（*Users*）] ページの詳細

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。

セクション	説明
[ブロックされたトランザクション数の上位ユーザ（Top Users by Transactions Blocked）]	このセクションには、IP アドレスまたはユーザ名で示された上位ユーザ（縦の目盛り）、そのユーザがブロックされたトランザクションの数（横の目盛り）が表示されます。レポーティングを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページまたはスケジュール設定されたレポートでユーザ名を認識不可能にする方法の詳細については、セキュリティ管理アプライアンスでの中央集中型 Web レポーティングのイネーブル化 （3 ページ）を参照してください。デフォルト設定では、すべてのユーザ名が表示されます。ユーザ名を非表示にするには、Web レポートでのユーザ名の匿名化 （5 ページ）を参照してください。
[帯域幅使用量の上位ユーザ（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。
[ユーザテーブル（Users Table）]	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。[ユーザ（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、[ユーザIDまたはクライアントIPアドレスの検索（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。 [ユーザテーブル（Users Table）] 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、[ユーザの詳細（User Details）] ページに表示されます。[ユーザの詳細（User Details）] ページの詳細については、 [ユーザの詳細（User Details）]（Web レポーティング） （15 ページ）

（注） クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。詳細は、LDAP との統合の章のLDAP サーバ プロファイルの作成を参照してください。

ヒント このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

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

（注） [ユーザ（Users）]ページについて、レポートを生成またはスケジュールすることができます。詳細については、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。

[ユーザの詳細（User Details）]（Web レポーティング）

[ユーザの詳細（User Details）] ページでは、[ウェブ（Web）] > [レポート（Reporting）] > [ユーザ（Users）] ページのインタラクティブな [ユーザ（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。

[ユーザの詳細（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 [ユーザの詳細（User Details）] ページを表示するには、[ウェブ（Web）] > [ユーザ（Users）] ページの [ユーザ（User）] テーブルでそのユーザをクリックします。

[ユーザの詳細（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 *4 : [ウェブ（Web）] > [レポート（Reporting）] > [ユーザの詳細（User Details）] ページの詳細*

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。時間範囲の詳細と実際のニーズに合わせたカスタマイズについては、レポートの時間範囲の選択を参照してください。
[総トランザクション数別のURL カテゴリ（URL Categories by Total Transactions）]	このセクションには、特定のユーザが使用している特定の URL カテゴリのリストが表示されます。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート （20 ページ）を参照してください。
[総トランザクション数別のトレンド（Trend by Total Transactions）]	このグラフには、ユーザが Web にいつアクセスしたかが表示されます。 たとえば、1 日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。[時間範囲（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。

セクション	説明
[一致したURLカテゴリ（URL Categories Matched）]	[一致したURLカテゴリ（URL Categories Matched）] セクションには、完了したトランザクションとブロックされたトランザクションの両方について、一致したカテゴリが表示されます。 このセクションでは、特定の URL カテゴリを検索することもできます。セクション下部のテキスト フィールドに URL カテゴリを入力し、[URLカテゴリの検索（Find URL Category）] をクリックします。カテゴリは正確に一致している必要はありません。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート （20 ページ）を参照してください。
[一致したドメイン（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、および列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、[ドメインまたはIPの検索（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。
[一致したアプリケーション（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、[アプリケーション（Application）]列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、[アプリケーションの検索（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。
[検出されたマルウェア脅威（Malware Threats Detected）]	このテーブルでは、特定のユーザがトリガーしている上位のマルウェア脅威を確認できます。 特定のマルウェア脅威の名前に関するデータを[マルウェア脅威の検索（Find Malware Threat）] フィールドで検索できます。マルウェア脅威の名前を入力し、[マルウェア脅威の検索（Find Malware Threat）] をクリックしてください。マルウェア脅威の名前は正確に一致している必要はありません。
[一致したポリシー（Policies Matched）]	このセクションでは、Web にアクセスする際にこのユーザに適用されるポリシー グループを検索できます。 セクション下部のテキストフィールドにポリシー名を入力し、[ポリシーの検索（Find Policy）] をクリックします。ポリシーの名前は正確に一致している必要はありません。

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

[ユーザの詳細（Users Details）] ページの使用例については、例 1：ユーザの調査を参照してください。

[ユーザ数レポート（User Count Report）]（Web）

[Web] > [レポート（Reporting）] > [ユーザ数（User Count）] ページには、中央集中型レポーティングが有効な Web セキュリティ アプライアンスの認証されたユーザと認証されていないユーザの合計数に関する集約情報が表示されます。このページには、直近の過去 30 日間、90 日間、および 180 日間のユニーク ユーザ数が表示されます。

（注） システムは、1 時間ごとに、認証されたユーザと認証されていないユーザの合計ユーザ数を計算します。

[Web サイト（Web Sites）] レポート

[ウェブ（Web）] > [レポート（Reporting）] > [Webサイト（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 サイト（Web Sites）] ページには次の情報が表示されます。

表 5 : [ウェブ（Web）] > [レポート（Reporting）] > [Web サイト（Web Sites）] ページの詳細

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。
[総トランザクション数の上位ドメイン（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。

セクション	説明
[ブロックされたトランザクション数の上位ドメイン（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。
[一致したドメイン（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トラッキング（Web Tracking）] ページに [プロキシサービス（Proxy Services）] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。 特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。 Web トラッキングの使用例については、例 2：URL のトラッキングを参照してください。 （注） このデータを .csv ファイルにエクスポートすると、最初の 300,000 エントリのみがエクスポートされます。

ヒント このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

（注） [Webサイト（Web Sites）] ページの情報について、レポートを生成またはスケジュールすることができます。詳細については、スケジュール設定されたレポートとオンデマンドWeb レポートについて （44 ページ）を参照してください。

[URLカテゴリ（URL Categories）] レポート

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

[URL カテゴリ（URL Categories）] ページには次の情報が表示されます。

表 *6 : [*ウェブ（*Web*）*] > [*レポート（*Reporting*）*] > [URL* カテゴリ（*URL Categories*）*]* ページの詳細

セクション	説明
時間範囲（Time Range）（ドロップダウンリスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択を参照してください。
[総トランザクション数の上位URLカテゴリ（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。
[ブロックまたは警告されたトランザクション数別の上位URLカテゴリ（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。
[一致したURLカテゴリ（URL Categories Matched）]	[一致したURLカテゴリ（URL Categories Matched）] セクションには、指定した時間範囲内におけるURLカテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。 未分類の URL が多数ある場合は、未分類の URL の削減 （19 ページ）を参照してください。
[URLフィルタリングのバイパス（URL Filtering Bypassed）]	URL フィルタリングの前に実行されるポリシー、ポートおよび管理ユーザ エージェントのブロッキングを示します。

ヒント このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

（注） このページよりもさらに詳細なレポートを生成するには、上位URLカテゴリ - 拡張（Top URL Categories — Extended） （47 ページ）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でデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「この時間範囲の一部のデータは使用不可でした。（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。

未分類の URL の削減

未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。

- 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。これらのトランザクションは、代わりに[URL フィルタリングバイパス（URL Filtering Bypassed）]統計情報に含まれるようになります。これを行うには、『AsyncOS for Cisco Web Security Appliances User Guide』でカスタム URL カテゴリについて参照してください。
- 既存またはその他のカテゴリに含めるべきサイトについては、誤って分類された URL と未分類の URL のレポート （21 ページ）を参照してください。

URL カテゴリ セットの更新とレポート

URL カテゴリ セットの更新の準備および管理で説明されているように、セキュリティ管理アプライアンスでは一連の定義済み URL カテゴリが定期的に更新される場合があります。

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

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

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

[URLカテゴリ（URL Categories）]ページと[アプリケーションの表示（Application Visibility）]レポート （21 ページ）および[ユーザ（Users）] レポート（Web） （13 ページ）を併用すると、特定のユーザと、特定のユーザがアクセスしようとしているアプリケーションタイプまたは Web サイトを調査できます。

たとえば、[URLカテゴリ（URL Categories）] レポート （18 ページ）で、サイトからアクセスされたすべての URL カテゴリの詳細を表示する、人事部門向けの概要レポートを生成できます。同じページの[URLカテゴリ（URL Categories）]インタラクティブ テーブルでは、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[ストリーミングメディア（Streaming Media）] カテゴリ リンクをクリックすると、特定の [URLカテゴリ（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（[カテゴリ別の総トランザクション上位ユーザ（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（[一致したドメイン（Domains Matched）] インタラクティブ テーブル）。

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているので、そのユーザのアクセス先を正確に確認する必要があるとします。ここから、[ユーザ（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 [ユーザの詳細（User Details）]（Web レポーティング）（15 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 [完了したトランザクション（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 トラッキング（Web Tracking）] ページに Web プロキシ サービスによって処理されたトランザクションの検索（52 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ついて、実際の詳細情報を確認できます。

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

誤って分類された URL と未分類の URL のレポート

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

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

送信内容は評価され、今後のルール更新への組み込みに活用されます。

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

[アプリケーションの表示（Application Visibility）] レポート

（注） [アプリケーションの表示（Application Visibility）] の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding Application Visibility and Control」の章を参照してください。

[ウェブ（Web）]>[レポート（Reporting）]>[アプリケーションの可視性（Application Visibility）] ページでは、セキュリティ管理アプライアンスと 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することができます。

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、『AsyncOS for Cisco Web Security Appliances User Guide』の「Understanding Application Visibility and Control」の章を参照してください。

[アプリケーションの表示（Application Visibility）] ページには次の情報が表示されます。

表 7 : [ウェブ（*Web*）] > [レポート（*Reporting*）] > [アプリケーションの表示（*Application Visibility*）] ページの詳細

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。
[総トランザクション数の上位アプリケーションタイプ（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。
[ブロックされたトランザクション数の上位アプリケーション（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
[一致したアプリケーションタイプ（Application Types Matched）]	[一致したアプリケーションタイプ（Application Types Matched）] インタラクティブ テーブルでは、[総トランザクション数の上位アプリケーションタイプ（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。[アプリケーション（Applications）] 列で、詳細を表示するアプリケーションをクリックできます。
[一致したアプリケーション（Applications Matched）]	[一致したアプリケーション（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列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。 [一致したアプリケーション（Applications Matched）] セクションに表示する列を設定することができます。このセクションの列の設定については、Web セキュリティ レポートの使用 （6 ページ）を参照してください。 [アプリケーション（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 [表示された項目（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、[一致したアプリケーション（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、[アプリケーションの検索（Find Application）] をクリックします。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

（注）　[アプリケーションの表示（Application Visibility）] ページの情報に関して、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。

[マルウェア対策（Anti-Malware）] レポート

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

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

（注） L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 ページ）を参照してください。

[マルウェア対策（Anti-Malware）] ページには次の情報が表示されます。

表 8 : [ウェブ（*Web*）] > [レポート（*Reporting*）] > [マルウェア対策（*Anti-Malware*）] ページの詳細

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。
[上位マルウェアカテゴリ：モニタまたはブロック済み（Top Malware Categories: Monitored or Blocked）]	このセクションには、所定のカテゴリ タイプによって検出された上位マルウェア カテゴリが表示されます。この情報はグラフ形式で表示されます。有効なマルウェア カテゴリの詳細については、マルウェアのカテゴリについて （25 ページ）を参照してください。
[上位マルウェアの脅威：モニタまたはブロック済み（Top Malware Threats: Monitored or Blocked）]	このセクションには、上位のマルウェアの脅威が表示されます。この情報はグラフ形式で表示されます。
[マルウェアカテゴリ（Malware Categories）]	[マルウェアカテゴリ（Malware Categories）] インタラクティブ テーブルには、[上位マルウェアカテゴリ（Top Malware Categories）] チャートに表示されている個々のマルウェア カテゴリに関する詳細情報が表示されます。 [マルウェアカテゴリ（Malware Categories）] インタラクティブ テーブル内のリンクをクリックすると、個々のマルウェア カテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。 例外：このテーブルの [アウトブレイクヒューリスティック（Outbreak Heuristics）] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。 有効なマルウェア カテゴリの詳細については、マルウェアのカテゴリについて （25 ページ）を参照してください。
[マルウェア脅威（Malware Threats）]	[マルウェアの脅威（Malware Threats）] インタラクティブ テーブルには、[上位マルウェア脅威（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。 「アウトブレイク（Outbreak）」のラベルと番号が付いている脅威は、他のスキャン エンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

[マルウェアのカテゴリ（Malware Category）] レポート

[マルウェアのカテゴリ（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。

[マルウェアのカテゴリ（Malware Category）] レポート ページにアクセスするには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンスで、[ウェブ（Web）] > [レポート（Reporting）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2　[マルウェアカテゴリ（Malware Categories）]インタラクティブテーブルで、[マルウェアのカテゴリ（Malware Category）] 列内のカテゴリをクリックします。

ステップ 3　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

[マルウェアの脅威（Malware Threat）] レポート

[マルウェア脅威（Malware Threats）] 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、[クライアントの詳細（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。

このレポートを表示するには、[マルウェア対策（Anti-Malware）] レポート ページの [マルウェアのカテゴリ（Malware Category）] 列でカテゴリをクリックします。

詳細については、テーブルの下の [サポートポータルマルウェア詳細（Support Portal Malware Details）] リンクをクリックしてください。

マルウェアのカテゴリについて

Web セキュリティ アプライアンスは次のタイプのマルウェアをブロックできます。

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

マルウェアのタイプ	説明
システム モニタ	システムモニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモート ホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
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。

[高度なマルウェア防御（ファイルレピュテーション）（Advanced Malware Protection (File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート

ファイル分析レポートの詳細の要件

（クラウド ファイル分析）管理アプライアンスがファイル分析サーバに到達できることを確認する

ファイル分析レポートの詳細を取得するには、アプライアンスがポート443経由でファイル分析サーバに接続できる必要があります。詳細については、ファイアウォール情報を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスがインターネットに直接接続していない場合は、このトラフィック用にプロキシサーバを設定します（アップグレードとアップデートの設定（Upgrade and Update Settings）を参照）。プロキシを使用してアップグレードおよびサービスアップデートを入手するようにアプライアンスを設定済みの場合は、既存の設定が使用されます。

HTTPS プロキシを使用する場合は、そのプロキシでトラフィックを復号化しません。パススルー機能を使用してファイル分析サーバと通信するようにしてください。プロキシ サーバはファイル分析サーバからの証明書を信頼する必要がありますが、ファイル分析サーバに自身の証明書を提供する必要はありません。

（クラウド ファイル分析）詳細なファイル分析結果が表示されるように管理アプライアンスを設定する

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の Cisco E メール セキュリティ アプライアンスまたは Cisco Web セキュリティ アプライアンスから分析用に送信されるファイルに関するクラウド内の詳細な結果が表示されるようにするには、すべてのアプライアンスを同じアプライアンス グループに結合する必要があります。

ステップ 1 [管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] を選択します。

ステップ 2 [ファイル分析（File Analysis）] セクションにスクロールします。

ステップ 3 管理対象アプライアンスが別のファイル分析クラウドサーバを指している場合は、結果の詳細の表示元となるサーバを選択します。

結果の詳細は、その他のクラウド サーバによって処理されたファイルでは使用できません。

ステップ 4 分析グループ ID を入力します。

- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- この値に CCOID を使用することを推奨します。
- この値は大文字と小文字が区別されます。
- この値は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。
- アプライアンスは 1 つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

ステップ 5 [今すぐグループ化（Group Now）] をクリックします。

ステップ 6 このアプライアンスとデータを共有する各 Web セキュリティ アプライアンスで、同じグループを設定します。

次のタスク

関連項目

クラウドで詳細なファイル分析結果が表示されるファイル （32 ページ）

（オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する

オンプレミス（プライベート クラウド）の Cisco AMP Threat Grid Appliance を導入した場合、Threat Grid Appliance で使用可能なレポート詳細を表示するために、Cisco コンテンツ セキュリティ管理アプライアンスのファイル分析アカウントをアクティブ化する必要があります。通常、これは 1 回のみ必要です。

始める前に

重大レベルでシステム アラートを受信していることを確認します。

ステップ 1 Threat Grid Appliance からファイル分析レポート詳細に最初にアクセスしようとするときに、数分待ってから、リンクを含むアラートを受信します。

このアラートを受信しなかった場合は、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] に移動し、[上位アラートを表示（View Top Alerts）] をクリックします。

ステップ 2 アラート メッセージ内のリンクをクリックします。

ステップ 3 必要に応じて、Cisco AMP Threat Grid Appliance にサインインします。

ステップ 4 管理アプライアンスのアカウントをアクティブ化します。

追加の要件

追加の要件については、お使いのセキュリティ管理アプライアンス リリースのリリース ノート（次の場所で入手可能）を参照してください http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して、各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイルを処理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルがその SHA-256 値（短縮形式）別に表示されます。組織のマルウェア インスタンスに関連付けられたファイル名を特定するには、[レポート（Reporting）] > [高度なマルウェア防御（Advanced Malware Protection）] を選択し、テーブルの SHA-256 リンクをクリックします。関連付けられたファイル名が詳細ページに表示されます。

[高度なマルウェア防御（ファイルレピュテーション）（AdvancedMalwareProtection(File Reputation)）] および [高度なマルウェア防御（ファイル分析）（Advanced Malware Protection (File Analysis)）] レポート ページ

レポート	説明
[高度なマルウェア防御（Advanced Malware Protection）]	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 各 SHA にアクセスしようとしたユーザ、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。 [マルウェア脅威ファイルの詳細（Malware Threat File Details）] レポートページの下部にあるリンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内に検出された、Web トラッキング内のファイルのすべてのインスタンスが表示されます。 判定が変更されたファイルについては、[AMP判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。 圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。 [カテゴリ別マルウェアファイル（Malware Files by Category）] セクションは、[カスタム検出（Custom Detection）] に分類される、AMP for Endpoints コンソールから受信したブラックリスト ファイル SHA の割合を示しています。 AMP for Endpoints コンソールから取得されるブラックリストに追加されたファイル SHA の脅威名は、レポートの [マルウェア脅威ファイル（Malware Threat Files）] セクションで [シンプルカスタム検出（Simple Custom Detection）] として表示されます。 AMP for Endpoints コンソールでブラックリストに登録されたファイル SHA のファイル トラジェクトリの詳細を表示するには、次の手順を実行します。 **1.** [レポート（Reporting）] > [高度なマルウェア防御（Advanced Malware Protection）] を選択します。 **2.** トラジェクトリの詳細を表示するファイル SHA のリンクをクリックします。 **3.** [詳細の表示（More Details）] セクションで [AMPコンソール（AMP Console）] リンクをクリックします。

レポート	説明
ファイル分析（File Analysis）	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。 1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。 オンプレミスの Cisco AMP Threat Grid Appliance での導入の場合：Cisco AMP Threat Grid Appliance でホワイトリストに登録されているファイルは、「クリーン」として表示されます。ホワイトリストについては、AMP Threat Grid のオンライン ヘルプを参照してください。 ドリル ダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。 また、分析を実行したサーバでSHAに関する追加の詳細を直接表示するには、SHA を検索するか、またはファイル分析の詳細ページ下部にある Cisco AMP Threat Grid リンクをクリックします。 ファイルを分析したサーバに関する詳細を表示するには、ファイル分析レポートの詳細の要件 （27 ページ）を参照してください。 圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析（File Analysis）] レポートに含まれます。
AMP判定のアップデート（AMP Verdict Updates）	このアプライアンスで処理され、トランザクションの処理後に判定が変わったファイルの一覧を示します。この状況の詳細については、お使いのWebセキュリティ アプライアンスのマニュアルを参照してください。 1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。 1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。 複数の Web Security Appliances で同じファイルの判定アップデートが異なる場合、最新のタイム スタンプが付いた結果が表示されます。 SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内にこの SHA-256 が含まれた、すべてのトランザクションの Web トラッキング結果が表示されます。 使用可能な最大時間範囲内（レポート用に選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けたすべてのトランザクションを表示するには、[マルウェアの脅威ファイル（Malware Threat Files）] ページの下部にあるリンクをクリックします。

その他のレポートでのファイル レピュテーション フィルタ データの表示

該当する場合は、ファイル レピュテーションおよびファイル分析のデータを他のレポートでも使用できます。レポートによっては、[高度なマルウェア防御でブロック（Blocked by Advanced Malware Protection）] 列がデフォルトで非表示になっている場合があります。追加列を表示するには、テーブルの下の [列（Columns）] リンクをクリックします。

[ユーザの場所別のレポート（Report by User Location）] に [高度なマルウェア防御（Advanced Malware Protection）] タブが含まれています。

クラウドで詳細なファイル分析結果が表示されるファイル

パブリック クラウドのファイル分析を導入した場合は、ファイル分析のためにアプライアンス グループに追加された、任意の管理対象アプライアンスからアップロードされたすべてのファイルの詳細な結果を表示できます。

グループに管理アプライアンスを追加した場合は、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] ページにあるボタンをクリックして、グループの管理対象アプライアンスのリストを表示できます。

分析グループのアプライアンスはファイル分析クライアント ID で識別されます。特定のアプライアンスのこの ID を判別するには、次の場所を参照してください。

アプライアンス	ファイル分析クライアント ID の場所
E メール セキュリティ アプライアンス	[セキュリティ サービス（Security Services）] > [ファイル レピュテーションと分析（File Reputation and Analysis）] ページの [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション
Web セキュリティ アプライアンス	[セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページの [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション。
Cisco コンテンツ セキュリティ管理アプライアンス	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] ページの下部

関連項目

- （クラウドファイル分析）詳細なファイル分析結果が表示されるように管理アプライアンスを設定する （28 ページ）

[クライアント マルウェア リスク（Client Malware Risk）] レポート

[ウェブ（Web）] > [レポート（Reporting）] > [クライアントマルウェアリスク（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。

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

次の表で、[クライアント マルウェア リスク（Client Malware Risk）] ページの情報について説明します。

表 *9 : [クライアント マルウェア リスク（Client Malware Risk）] レポート ページの内容*

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。詳細については、レポートの時間範囲の選択を参照してください。
[Webプロキシ:モニタまたはブロックされた上位クライアント（Web Proxy: Top Clients Monitored or Blocked）]	このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。
[L4トラフィックモニタ:検出されたマルウェア接続（L4 Traffic Monitor: Malware Connections Detected）]	このチャートには、組織内で最も頻繁にマルウェア サイトに接続している 10 台のコンピュータの IP アドレスが表示されます。 このチャートは[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 ページ）の [上位クライアントIP（Top Client IPs）] チャートと同じです。詳細およびチャート オプションについてはこの項を参照してください。

セクション	説明
[Webプロキシ:クライアントマルウェアリスク（Web Proxy: Client Malware Risk）]	[Webプロキシ：クライアントマルウェアリスク（Web Proxy: Client Malware Risk）] テーブルには、[Webプロキシ:マルウェアリスクによる上位クライアント（Web Proxy: Top Clients by Malware Risk）] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。 このテーブルで各ユーザをクリックすると、そのクライアントに関連する [ユーザの詳細（User Details）] ページが表示されます。このページの詳細については、[ユーザの詳細（User Details）]（Web レポーティング） （15 ページ）を参照してください。 テーブルで任意のリンクをクリックすると、個々のユーザと、マルウェアのリスクをトリガーしているそのユーザのアクティビティをさらに詳しく表示できます。たとえば [ユーザID/クライアントIPアドレス（User ID / Client IP Address）] 列のリンクをクリックすると、そのユーザの [ユーザ（User）] ページに移動します。
[L4トラフィックモニタ:マルウェアリスク別クライアント（L4 Traffic Monitor: Clients by Malware Risk）]	このテーブルには、組織内でマルウェア サイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。 このテーブルは[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 ページ）の [クライアントソースIP（Client Source IPs）] テーブルと同じです。テーブルの操作についてはこの項を参照してください。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

[Web レピュテーションフィルタ（Web Reputation Filters）] レポート

[ウェブ（Web）] > [レポート（Reporting）] > [Web レピュテーションフィルタ（Web Reputation Filters）] では、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）の結果を確認できます。

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、たとえば以下のものがあります。

- 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 フィルタの詳細については、『IronPort AsyncOS for Web User Guide』の「Web Reputation Filters」を参照してください。

[Web レピュテーションフィルタ（Web Reputation Filters）] ページには次の情報が表示されます。

表 *10 : [ウェブ（Web）] > [レポート（Reporting）] > [Web レピュテーションフィルタ（Web Reputation Filters）] ページの詳細*

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。
[Webレピュテーションアクション(トレンド)（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レピュテーションアクション(ボリューム)（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。

セクション	説明
[WBRSによってブロックされるWebレピュテーションの脅威タイプ（Web Reputation Threat Types Blocked by WBRS）]	このセクションには、Web レピュテーション フィルタリングによってブロックされたトランザクションで発生した脅威タイプが表示されます。 注：WBRS では、常に、脅威のタイプを識別できるわけではありません。
[他のトランザクションで脅威タイプが検知されました（Threat Types Detected in Other Transactions）]	このセクションには、Web レピュテーション フィルタリングによってブロックされないトランザクションで発生した脅威タイプが表示されます。 これらの脅威がブロックされなかった理由には、次のようなものがあります。 • すべての脅威に、ブロッキングのしきい値を満たすスコアがあるわけではありません。ただし、アプライアンスのその他の機能は、これらの脅威を検出する可能性があります。 • ポリシーが、脅威を許可するよう設定されている可能性があります。 注：WBRS では、常に、脅威のタイプを識別できるわけではありません。
Web レピュテーションアクション（スコアによる内訳）（Web Reputation Actions (Breakdown by Score)）	Adaptive Scanning がイネーブルでない場合、このインタラクティブ テーブルには各アクションの Web レピュテーション スコアの内訳が表示されます。

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーション設定の詳細については、『AsyncOS for Cisco Web Security Appliances User Guide』を参照してください。

[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート

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

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

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

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

表 *11 : [L4* トラフィック モニタ（*L4 Traffic Monitor*）*]* レポート ページの内容

セクション	説明
時間範囲（Time Range）（ドロップダウン リスト）	レポート対象の時間範囲を選択できるメニュー。詳細については、レポートの時間範囲の選択を参照してください。
[上位クライアント IP（Top Client Ips）]	このセクションには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。 チャートの下の [チャートオプション（Chart Options）] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続（Malware Connections Detected）] から [モニタされたマルウェア接続（Malware Connections Monitored）] または [ブロックされたマルウェア接続（Malware Connections Blocked）] に変更できます。 このチャートは、[クライアント マルウェア リスク（Client Malware Risk）] レポート （33 ページ）の [L4 トラフィック モニタ：検出されたマルウェア接続（L4 Traffic Monitor: Malware Connections Detected）] チャートと同じです。
[上位マルウェア サイト（Top Malware Sites）]	このセクションには、L4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。 チャートの下の [チャートオプション（Chart Options）] リンクをクリックすると、表示を総合的な [検出されたマルウェア接続（Malware Connections Detected）] から [モニタされたマルウェア接続（Malware Connections Monitored）] または [ブロックされたマルウェア接続（Malware Connections Blocked）] に変更できます。

セクション	説明
[クライアントソースIP（Client Source Ips）]	このテーブルには、組織内でマルウェア サイトに頻繁に接続しているコンピュータの IP アドレスが表示されます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ（Filter by Port）] をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェア サイトへ「誘導」しているかを判断できます。 各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリをクリックします。たとえば、ある特定のクライアント IP アドレスの [ブロックされたマルウェア接続（Malware Connections Blocked）] が高い数値を示している場合、その列の数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[ウェブ（Web）] > [レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページの [L4 トラフィック モニタ（L4 Traffic Monitor）] タブに検索結果として表示されます。リストの詳細については、L4 トラフィック モニタによって処理されたトランザクションの検索 （56 ページ）を参照してください。 このテーブルは、[クライアント マルウェア リスク（Client Malware Risk）] レポート （33 ページ）の [L4 トラフィック モニタ - マルウェア リスク別クライアント（L4 Traffic Monitor - Clients by Malware Risk）] テーブルと同じです。
[マルウェア ポート（Malware Ports）]	このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたポートが表示されます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[検出されたマルウェア接続の総数（Total Malware Connections Detected）] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[ウェブ（Web）] > [レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページの [L4 トラフィック モニタ（L4 Traffic Monitor）] タブに検索結果として表示されます。リストの詳細については、L4 トラフィック モニタによって処理されたトランザクションの検索 （56 ページ）を参照してください。

セクション	説明
[検出されたマルウェアサイト（Malware Sites Detected）]	このテーブルには、L4 トラフィック モニタによって最も頻繁にマルウェアが検出されたドメインが表示されます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ（Filter by Port）] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続（Malware Connections Blocked）] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[ウェブ（Web）] > [レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページの [L4 トラフィック モニタ（L4 Traffic Monitor）] タブに検索結果として表示されます。リストの詳細については、L4 トラフィック モニタによって処理されたトランザクションの検索 （56 ページ）を参照してください。

ヒント このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

関連項目

- L4 トラフィック モニタ レポートのトラブルシューティング （62 ページ）

[SOCKS プロキシ（SOCKS Proxy）] レポート

[ウェブ（Web）] > [レポート（Reporting）] > [SOCKS プロキシ（SOCKS Proxy）] ページでは、宛先、ユーザなど、SOCKS プロキシを通じて処理されたトランザクションのデータおよびトレンドを表示できます。

（注） レポートに表示される宛先は、SOCKS クライアント（通常はブラウザ）が SOCKS プロキシに送信するアドレスです。

SOCKS ポリシー設定を変更するには、『Cisco Web Security Appliances User Guide』の「AsyncOS」を参照してください。

関連項目

- SOCKS プロキシによって処理されるトランザクションの検索 （57 ページ）

ユーザの場所別レポート（Reports by User Location）

[ウェブ（Web）] > [レポート（Reporting）] > [ユーザの場所別のレポート（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。

[ユーザの場所別のレポート（Reports by User Location）] ページには次の情報が表示されます。

表 *12 : [ウェブ（Web）] > [レポート（Reporting）] > [ユーザの場所別のレポート（Reports by User Location）] ページの詳細*

セクション	説明
[時間範囲（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、レポートの時間範囲の選択を参照してください。
[Webプロキシアクティビティ総数:リモートユーザ（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プロキシの概要（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。
[Webプロキシアクティビティ総数:ローカルユーザ（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。
[検出された疑がわしいトランザクション:リモートユーザ（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。
[疑わしいトランザクションの概要（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。
[検出された疑がわしいトランザクション:ローカルユーザ（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。

セクション	説明
[疑わしいトランザクションの概要（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。

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

ヒント　このレポートのビューをカスタマイズするには、Web セキュリティ レポートの使用 （6 ページ）を参照してください。

（注）　[ユーザの場所別のレポート（Reports by User Location）] ページの情報について、スケジュール設定されたレポートを生成することができます。レポートのスケジュール設定については、スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）を参照してください。

[システム容量（System Capacity）] ページ

[ウェブ（Web）] > [レポート（Reporting）] > [システム容量（System Capacity）] ページでは、Web セキュリティ アプライアンスによってセキュリティ管理アプライアンスで発生する作業負荷全体を表示できます。重要な点は、[システム容量（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 Security Appliances をモニタすると、キャパシティが実際の量に適しているかを確認できます。量は、時間の経過に伴って必ず増加しますが、適切にモニタリングしていれば、追加キャパシティまたは設定変更を予防的に適用できます。

[システム容量（System Capacity）] ページを使用すると、次の情報を確認できます。

- Web Security Appliances が推奨される CPU キャパシティをいつ超えたかを特定します。これによって、設定の最適化や追加アプライアンスがいつ必要になったかがわかります。
- トラブルシューティングのために、システムが最もリソースを使用している部分を識別します。
- 応答時間とプロキシ バッファ メモリを確認します。
- 1 秒あたりのトランザクション、および顕著な接続を確認します。

[システム容量（System Capacity）] レポートの表示

ステップ 1　セキュリティ管理アプライアンスで、[ウェブ（Web）] > [レポート（Reporting）] > [システム容量（System Capacity）] を選択します。

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

ステップ 3 単一のアプライアンスのシステム容量を表示するには、[平均使用率およびパフォーマンスの概要（Overview of Averaged Usage and Performance）] テーブルの [Web セキュリティ アプライアンス（Web Security appliance）] 列で目的のアプライアンスをクリックします。

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

- [システム容量（System Capacity）] : [システムの負荷（System Load）] （42 ページ）
- [システム容量（System Capacity）] : [ネットワーク負荷（Network Load）] （43 ページ）

[システム容量（System Capacity）] ページに表示されるデータの解釈方法

[システム容量（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数を表示します。これも正確な数値です。

[システム容量（System Capacity）] ページの [最大（Maximum）] 値インジケータは、指定された期間内の最大値を示します。[平均（Average）] 値は指定された期間内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 [平均（Average）] 値と [最大（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 [年（Year）] を選択した場合は、最大の時間範囲である 90 日を選択することを推奨します。

[システム容量（System Capacity）] : [システムの負荷（System Load）]

[システム容量（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 Security Appliances 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 [時間範囲（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。

[システム容量（System Capacity）]：[ネットワーク負荷（Network Load）]

[システム容量（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。

[プロキシ バッファ メモリ（Proxy Buffer Memory）] では、通常動作中にネットワーク トラフィックのスパイクが表れることがあります。しかし、グラフが最大値に向かって着実に上昇している場合は、アプライアンスが最大キャパシティに達しつつある可能性があり、キャパシティの追加を検討する必要があります。

次のチャートは、[システム容量（System Capacity）]：[システムの負荷（System Load）]（42 ページ）で説明されているチャートと同じページで、それらのチャートの下に表示されます。

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 Web セキュリティ 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。

[使用可能なデータ（Data Availability）] ページ

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

（注） Web レポーティングがディセーブルになると、セキュリティ管理アプライアンスは Web セキュリティ アプライアンスから新しいデータを取得しなくなりますが、以前に取得したデータはセキュリティ管理アプライアンスに残っています。

[Webレポート（Web Reporting）] の [開始（From）] 列と [終了（To）] 列、および [Webレポートとトラッキング（Web Reporting and Tracking）] の [開始（From）] 列と [終了（To）] 列でステータスが異なる場合は、[ステータス（Status）] 列に最も深刻な結果が示されます。

データの消去の詳細については、ディスク領域の管理を参照してください。

（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でデータ アベイラビリティが使用されている場合、いずれかのアプライアンスのデータにギャップがあると、ページの下部に「この時間範囲の一部のデータは使用不可でした。（Some data in this time range was unavailable.）」というメッセージが表示されます。ギャップが存在しない場合は何も表示されません。

スケジュール設定されたレポートとオンデマンドWebレポートについて

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

- [Web レポーティングの概要（Web Reporting Overview）]：このページに表示される情報については、Web レポートの概要 （11 ページ）を参照してください。
- [ユーザ（Users）]：このページに表示される情報については、[ユーザ（Users）] レポート（Web） （13 ページ）を参照してください。
- [Webサイト（Web Sites）]：このページに表示される情報については、[Web サイト（Web Sites）] レポート （17 ページ）を参照してください。
- [URLカテゴリ（URL Categories）]：このページに表示される情報については、[URLカテゴリ（URL Categories）] レポート （18 ページ）を参照してください。
- [上位URLカテゴリ - 拡張（Top URL Categories — Extended）]：[上位URLカテゴリ - 拡張（Top URL Categories — Extended）] のレポートを生成する方法については、上位URLカテゴリ - 拡張（Top URL Categories — Extended） （47 ページ）を参照してください。

このレポートをオンデマンド レポートとして使用することはできません。

- [アプリケーションの表示（Application Visibility）]：このページに表示される情報については、[アプリケーションの表示（Application Visibility）] レポート （21 ページ）を参照してください。
- [上位アプリケーションタイプ - 拡張（Top Application Types — Extended）]：[上位アプリケーションタイプ - 拡張（Top Application Types — Extended）] のレポートを生成する方法については、上位アプリケーションタイプ - 拡張（Top Application Types — Extended） （48 ページ）を参照してください。

このレポートをオンデマンド レポートとして使用することはできません。

- [マルウェア対策（Anti-Malware）]：このページに表示される情報については、[マルウェア対策（Anti-Malware）] レポート （23 ページ）を参照してください。

- [クライアントマルウェアリスク（Client Malware Risk）]：このページに表示される情報については、[クライアント マルウェア リスク（Client Malware Risk）] レポート （33 ページ）を参照してください。
- [Webレピュテーションフィルタ（Web Reputation Filters）]：このページに表示される情報については、[Web レピュテーションフィルタ（Web Reputation Filters）] レポート （34 ページ）を参照してください。
- [L4トラフィックモニタ（L4 Traffic Monitor）]：このページに表示される情報については、[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 ページ）を参照してください。
- [モバイルセキュアソリューション（Mobile Secure Solution）]：このページに表示される情報については、ユーザの場所別レポート（Reports by User Location） （40 ページ）を参照してください。
- [システム容量（System Capacity）]：このページに表示される情報については、[システム容量（System Capacity）] ページ （41 ページ）を参照してください。

Web レポートのスケジュール設定

このセクションの内容は次のとおりです。

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

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、過去の月（最大 12 ヵ月）のデータを含めるように設定できます。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヵ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

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。

スケジュール設定された Web レポートの保存

セキュリティ管理アプライアンスでは、スケジュール設定された各レポートの最大 30 の最新インスタンスで、生成された最新のレポートをすべてのレポートに対して、合計 1000 バージョンまで保持します。

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。30 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。

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。（詳細については、IP インターフェイスおよびアプライアンスへのアクセスを参照してください）。

関連項目

- アーカイブ済みの Web レポートの表示と管理 （51 ページ）

スケジュール設定された Web レポートの追加

ステップ 1 セキュリティ管理アプライアンスで、[Web]>[レポート（Reporting）]>[スケジュール設定されたレポート（Scheduled Reports）] を選択します。

ステップ 2 [定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 3 [タイプ（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 [タイトル（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 [時間範囲（Time Range）] ドロップダウン メニューから、レポートの時間範囲を選択します。

ステップ 6 生成されるレポートの形式を選択します。

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

ステップ 7 [アイテム数（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 [チャート（Charts）] では、[表示するデータ（Data to display）] の下のデフォルト チャートをクリックし、レポートの各チャートに表示するデータを選択します。

ステップ 9 [ソート列（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列を選択します。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列を基準とする上位「N」個の項目のレポートを作成できます。

ステップ 10 [スケジュール（Schedule）]領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 11 [メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

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

ステップ 12 [送信（Submit）] をクリックします。

スケジュール設定された Web レポートの編集

レポートを編集するには、[ウェブ（Web）] > [レポート（Reporting）] > [スケジュール設定されたレポート（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、[送信（Submit）] をクリックしてページでの変更を送信し、[変更を確定（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 Web レポートの削除

レポートを削除するには、[ウェブ（Web）] > [レポート（Reporting）] > [スケジュール設定されたレポート（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、[すべて（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 Web レポート

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

上位URLカテゴリ - 拡張（Top URL Categories — Extended）

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

（注） このタイプのレポートで生成できる最大レポート数は 20 です。

- 定義済みのURLカテゴリ リストは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート （20 ページ）を参照してください。

[上位URLカテゴリ - 拡張（Top URL Categories — Extended）] レポートを生成するには、次の手順を実行します。

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ（Web）]>[レポート（Reporting）]>[スケジュール設定されたレポート（Scheduled Reports）] を選択します。

ステップ 2 [定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 3 [タイプ（Type）] の横のドロップダウン メニューから、[上位URLカテゴリ - 拡張（Top URL categories — Extended）] を選択します。

ステップ 4 [タイトル（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 [時間範囲（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 [アイテム数（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 [ソート列（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列を選択します。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列を基準とする上位「N」個の項目のレポートを作成できます。

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

ステップ 10 [スケジュール（Schedule）]領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 11 [メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

ステップ 12 [送信（Submit）] をクリックします。

上位アプリケーションタイプ - 拡張（Top Application Types — Extended）

[上位アプリケーションタイプ - 拡張（Top Application Type — Extended）] レポートを生成するには、次の手順を実行します。

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ（Web）]>[レポート（Reporting）]>[スケジュール設定されたレポート（Scheduled Reports）] を選択します。

ステップ 2 [定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 3 [タイプ（Type）] の横のドロップダウン メニューから、[上位アプリケーションタイプ - 拡張（Top Application Types — Extended）] を選択します。

このページのオプションは変更される場合があります。

ステップ 4 [タイトル（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 [時間範囲（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 [アイテム数（Number of Items）] の横のドロップダウン リストから、生成されたレポートに出力するアプリケーション タイプの数を選択します。

有効な値は 2 ～ 20 です。デフォルト値は **5** です。

ステップ 8 [列をソート（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列のタイプを選択します。選択肢は、[完了したトランザクション（Transactions Completed）]、[ブロックされたトランザクション（Transactions Blocked）]、[トランザクション合計（Transaction Totals）] です。

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

ステップ 10 [スケジュール（Schedule）] 領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 11 [メール（Email）] テキスト フィールドに、生成されたレポートが送信される電子メール アドレスを入力します。

ステップ 12 [送信（Submit）] をクリックします。

オンデマンドでの Web レポートの生成

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

（注） 一部のレポートは、オンデマンドではなくスケジュール設定されたレポートとしてのみ使用できます。追加の拡張 Web レポート （47 ページ）を参照してください。

レポートをオンデマンドで生成するには、次の手順を実行します

ステップ 1 セキュリティ管理アプライアンスで、[Web] > [レポート（Reporting）] > [アーカイブレポート（Archived Reports）] を選択します。

ステップ 2 [今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 3 [レポートタイプ（Report Type）] セクションで、ドロップダウン リストからレポート タイプを選択します。

このページのオプションは変更される場合があります。

ステップ 4 [タイトル（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 [時間範囲（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 [フォーマット（Format）] セクションで、レポートの形式を選択します。

次のオプションがあります。

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

ステップ 7 レポートで使用可能なオプションに応じて次の項目を選択します。

- [行数（Number of rows）]：テーブルに表示するデータの行数。
- [チャート（Charts）]：レポートのチャートに表示するデータ。
- [表示するデータ（Data to display）] の下のデフォルト オプションを選択します。
- [列をソート（Sort Column）]：各テーブルのソート基準となる列。

ステップ 8 [配信オプション（Delivery Option）] セクションから、次のオプションを選択します。

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

（注） [ドメイン毎のエグゼクティブサマリー（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、[今すぐ受信者にメールを送る（Email now to recipients）] チェックボックスをオンにします。
- テキスト フィールドに、レポートの受信者の電子メールアドレスを入力します。

ステップ 9 [このレポートを配信（Deliver This Report）] をクリックして、レポートを生成します。

[アーカイブ Web レポート（Archived Web Reports）] ページ

- スケジュール設定されたレポートとオンデマンド Web レポートについて （44 ページ）

- オンデマンドでの Web レポートの生成 （49 ページ）
- アーカイブ済みの Web レポートの表示と管理 （51 ページ）

アーカイブ済みの Web レポートの表示と管理

ここでは、スケジュール設定されたレポートとして生成されたレポートの使用方法について説明します。

ステップ 1 [ウェブ（Web）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] に移動します。

ステップ 2 レポートを表示するには、[レポートタイトル（Report Title）] 列でレポート名をクリックします。[表示（Show）] ドロップダウン メニューでは、[アーカイブレポート（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。

ステップ 3 リストが長い場合に特定のレポートを見つけるには、[表示（Show）] メニューからレポート タイプを選択してリストをフィルタリングするか、または列のヘッダーをクリックし、その列でソートします。

次のタスク

関連項目

- スケジュール設定された Web レポートの保存 （46 ページ）
- スケジュール設定された Web レポートの追加 （46 ページ）
- オンデマンドでの Web レポートの生成 （49 ページ）

Web トラッキング（Web Tracking）

[Webトラッキング（Web Tracking）] ページを使用して、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を表示します。展開で使用するサービスに基づき、関連するタブで検索を行います。

- Web プロキシ サービスによって処理されたトランザクションの検索 （52 ページ）
- L4 トラフィック モニタによって処理されたトランザクションの検索 （56 ページ）
- SOCKS プロキシによって処理されるトランザクションの検索 （57 ページ）
- Web トラッキングの検索結果の使用 （57 ページ）
- Web トラッキング検索結果のトランザクションの詳細の表示 （58 ページ）

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

関連項目

- Web トラッキングおよびアップグレードについて （60 ページ）

Web プロキシ サービスによって処理されたトランザクションの検索

[ウェブ（Web）] > [レポート（Reporting）] > [Webトラッキング（Web Tracking）] ページの [プロキシサービス（Proxy Services）] タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブル ユース適用コンポーネントから収集された Web トラッキング データを検索します。このデータには、L4 トラフィック モニタリング データ、および SOCKS プロキシによって処理されたトランザクションは含まれません。

このデータを使用して、次の役割を補助することができます。

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

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

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

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

（注） Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

Web トラッキングの使用例については、例 1：ユーザの調査を参照してください。

[プロキシサービス（Proxy Services）] タブと他の Web レポーティング ページの併用例については、[URL カテゴリ（URL Categories）] ページとその他のレポーティング ページの併用 （20 ページ）を参照してください。

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ（Web）] > [レポート（Reporting）] > [Web トラッキング（Web Tracking）] を選択します。

ステップ 2 [プロキシサービス（Proxy Services）] タブをクリックします。

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

ステップ 4 検索条件を入力します。

表 13 : [プロキシサービス（Proxy Services）] タブの Web トラッキング検索条件

オプション	説明
デフォルトの検索条件	

オプション	説明
時間範囲	レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで使用できる時間範囲については、レポートの時間範囲の選択を参照してください。
ユーザ/クライアント IPv4またはIPv6（User/Client IPv4 or IPv6）	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。
Web サイト	追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクション タイプ（Transaction Type）	追跡対象のトランザクションのタイプを [すべてのトランザクション（All Transactions）]、[完了（Completed）]、[ブロックされた（Blocked）]、[モニタ対象（Monitored）]、または [警告対象（Warned）] から選択します。
高度な検索条件	
URL カテゴリ	URL カテゴリでフィルタリングするには、[URLカテゴリによるフィルタ（Filter by URL Category）] を選択し、フィルタリング対象とするカスタムまたは定義済み URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。。 一連のURLカテゴリが更新されると、一部のカテゴリに「廃止予定（Deprecated）」のラベルが付けられる場合があります。廃止予定のカテゴリは、新しいトランザクションに使用されなくなります。ただし、そのカテゴリが有効な間に発生した最近のトランザクションについては、引き続き検索を実行できます。URL カテゴリ セットの更新については、URL カテゴリ セットの更新とレポート （20 ページ）を参照してください。 ドロップダウン リストに表示されるエンジン名に関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。
Application	アプリケーションでフィルタリングするには、[アプリケーションによるフィルタ（Filter by Application）] を選択し、フィルタリングに使用するアプリケーションを選択します。 アプリケーションタイプでフィルタリングするには、[アプリケーションタイプによるフィルタ（Filter by Application Type）] を選択し、フィルタリングに使用するアプリケーション タイプを選択します。
ポリシー	ポリシー グループでフィルタリングするには、[ポリシーによるフィルタ（Filter by Policy）] を選択し、フィルタリングに使用するポリシー グループ名を入力します。 このポリシーが Web セキュリティ アプライアンスで宣言済みであることを確認してください。

オプション	説明
マルウェアの脅威（Malware Threat）	特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ（Filter by Malware Threat）] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ（Filter by Malware Category）] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。説明については、マルウェアのカテゴリについて（25 ページ）を参照してください。
WBRS	[WBRS] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。 • Web レピュテーション スコアでフィルタリングするには、[スコア範囲（Score Range）] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし（No Score）] を選択すると、スコアがない Web サイトをフィルタリングできます。 • Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ（Filter by Reputation Threat）] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。 WBRS スコアの詳細は、『IronPort AsyncOS for Web User Guide』を参照してください。
AnyConnect セキュア モビリティ	リモートまたはローカルアクセスでフィルタリングするには、[ユーザの場所によるフィルタ（Filter by User Location）] を選択し、アクセス タイプを選択します。すべてのアクセス タイプを含めるには、[フィルタを無効にする（Disable Filter）] を選択します （旧リリースでは、このオプションは Mobile User Security と呼ばれていました。）
Web アプライアンス	特定の Web アプライアンスでフィルタリングするには、[Web アプライアンスによるフィルタ（Filter by Web Appliance）] の横のラジオ 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。 [フィルタを無効にする（Disable Filter）] を選択すると、検索にはセキュリティ管理アプライアンスに関連付けられている Web セキュリティ アプライアンスがすべて含まれます。
ユーザ リクエスト（User Request）	ユーザによって実際に開始されたトランザクションでフィルタリングするには、[Web ユーザが要求したトランザクションによるフィルタ（Filter by Web User-Requested Transactions）] を選択します。 **注**：このフィルタを有効にすると、検索結果には「最良の推測」トランザクションが含まれます。

ステップ 5 [検索（Search）] をクリックします。

次のタスク

関連項目

- 詳細な Web トラッキング検索結果の表示 （57 ページ）
- Web トラッキング検索結果について （58 ページ）
- Web トラッキング検索結果のトランザクションの詳細の表示 （58 ページ）
- Web トラッキング機能および高度なマルウェア防御機能について （59 ページ）

マルウェアのカテゴリについて

Web セキュリティ アプライアンスは次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。

マルウェアのタイプ	説明
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
フィッシング URL	フィッシングURLは、ブラウザのアドレスバーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャル エンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。
システム モニタ	システムモニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモートホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモート ホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
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。

L4 トラフィック モニタによって処理されたトランザクションの検索

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

- 時間範囲
- トランザクションを開始したマシンの IP アドレス（IPv4 または IPv6）
- 接続先 Web サイトのドメインまたは IP アドレス（IPv4 または IPv6）
- [ポート（Port）]
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ
- 接続を処理する Web セキュリティ アプライアンス

一致した検索結果のうち最初の 1000 件が表示されます。

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

この情報の詳細な使用方法については、[L4 トラフィック モニタ（L4 Traffic Monitor）] レポート （36 ページ）を参照してください。

SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、トランザクションを開始したクライアントマシンの IP アドレス、および宛先ドメイン、IP アドレス、またはポートなど、さまざまな条件に一致するトランザクションを検索できます。カスタム URL カテゴリ、一致ポリシー、およびユーザ ロケーション（ローカルまたはリモート）により、結果をフィルタリングすることもできます。IPv4 および IPv6 アドレスがサポートされます。

ステップ 1 [ウェブ（Web）] > [レポート（Reporting）] > [Web トラッキング（Web Tracking）] を選択します。
ステップ 2 [SOCKSプロキシ（SOCKS Proxy）] タブをクリックします。
ステップ 3 結果をフィルタリングするには、[詳細設定（Advanced）] をクリックします。
ステップ 4 検索条件を入力します。
ステップ 5 [検索（Search）] をクリックします。

次のタスク

関連項目

[SOCKS プロキシ（SOCKS Proxy）] レポート （39 ページ）

Web トラッキングの検索結果の使用

詳細な Web トラッキング検索結果の表示

ステップ 1 返された結果のページをすべて確認してください。

ステップ 2 現在表示されている数よりも多くの結果を各ページに表示するには、[表示された項目（Items Displayed）] メニューからオプションを選択します。

ステップ 3 条件に一致するトランザクションが、[表示された項目（Items Displayed）] メニューで選択できる最大トランザクション数より多い場合は、[印刷可能なダウンロード（Printable Download）] リンクをクリックし、一致するすべてのトランザクションを含む CSV ファイルを取得すると、完全な結果を確認できます。

この CSV ファイルには、関連トランザクションの詳細を除く、raw データ一式が含まれます。

Web トラッキング検索結果について

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

検索結果に表示される情報：

- URL がアクセスされた時刻。
- ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数。関連トランザクションの数は、列見出しの [すべての詳細を表示(Display All Details)] リンクの下の各行に表示されます。
- 処理（トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます）。

Web トラッキング検索結果のトランザクションの詳細の表示

内容	操作手順
リスト内の短縮 URL の完全な URL	トランザクションを処理したホスト Web セキュリティ アプライアンスをメモして、そのアプライアンスのアクセス ログを確認します。
個々のトランザクションの詳細	[Webサイト（Website）] 列の URL をクリックします。
すべてのトランザクションの詳細	[Webサイト（Website）] 列見出しの [すべての詳細を表示...(Display All Details...)] リンクをクリックします。
500 件までの関連トランザクションのリスト	関連トランザクションの数は、検索結果リストの列見出しにある [詳細を表示（Display Details）] リンクの下のカッコ内に表示されます。 トランザクションの [詳細（Details）] ビューで [関連トランザクション（Related Transactions）] リンクをクリックします。

Web トラッキング機能および高度なマルウェア防御機能について

Web トラッキングでファイルの脅威情報を検索する場合は、次の点に注意してください。

- ファイル レピュテーション サービスで検出された悪意のあるファイルを検索するには、Web トラッキングの [詳細設定（Advanced）] セクションにある [マルウェアの脅威（Malware Threat）] 領域で、[マルウェアカテゴリ別フィルタ（Filter by Malware Category）] オプションの [悪意のある既知の高リスクファイル（Known Malicious and High-Risk Files）] を選択します。
- Web トラッキングには、ファイル レピュテーション処理についての情報と、トランザクションが処理されたときに返された元のファイル レピュテーションの判定のみが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

  検索結果の [ブロック - AMP（Block - AMP）] は、ファイルのレピュテーション判定が原因でトランザクションがブロックされたことを意味します。

  トラッキングの詳細に表示される [AMP脅威スコア（AMP Threat Score）] は、ファイルを明確に判定できないときにクラウドレピュテーションサービスが提示するベストエフォート型のスコアです。この場合のスコアは 1 ～ 100 です（AMP 判定が返された場合、またはスコアがゼロの場合は [AMP脅威スコア（AMP Threat Score）] を無視してください）。アプライアンスはこのスコアをしきい値スコア（[セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページで設定）と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60 ～ 100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアを変更することはお勧めしません。WBRS スコアはファイルのダウンロード元となったサイトのレピュテーションです。このスコアはファイル レピュテーションとは関係ありません。
- 判定のアップデートは [AMP判定のアップデート（AMP Verdict Updates）] レポートでのみ使用できます。Web トラッキングの元のトランザクションの詳細は、判定が変更されても更新されません。特定のファイルが関係するトランザクションを表示するには、判定アップデート レポートで SHA-256 をクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

  分析済みファイルのその他の情報は、クラウドから入手できます。ファイルの使用可能なファイル分析情報を表示するには、[レポート（Reporting）]>[ファイル分析（File Analysis）] を選択して、ファイルを検索する SHA-256 を入力するか、Web トラッキングの詳細で SHA-256 リンクをクリックします。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

  分析用に送信されたファイルの後続インスタンスをアプライアンスが処理すると、そのインスタンスは Web トラッキングの検索結果に表示されるようになります。

関連項目

- SHA-256 ハッシュによるファイルの識別 （29 ページ）

Web トラッキングおよびアップグレードについて

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

Webポーティングおよびトラッキングのトラブルシューティング

すべてのレポートのトラブルシューティングも参照してください。

中央集中型レポーティングが適切に有効化されているのに機能しない

問題

指示どおりに中央集中型 Web レポーティングを有効にしても機能しません。

ソリューション

レポーティング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 レポーティングは機能しません。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、ディスク領域の管理を参照してください。

[高度なマルウェア保護判定のアップデート（Advanced Malware Protection Verdict Updates）] レポートの結果が異なる

問題

Web セキュリティ アプライアンスおよび E メール セキュリティ アプライアンスが同じファイルを分析用に送信し、Web および電子メールの [AMP 判定のアップデート（AMP Verdict Updates）] レポートに、そのファイルの異なる判定が表示されます。

ソリューション

これは一時的な違いです。すべての判定アップデートがダウンロードされると、結果は一致します。一致するまでに最大で 30 分かかります。

ファイル分析レポートの詳細の表示に関する問題

ファイル分析レポートの詳細を使用できない

問題

ファイル分析レポートの詳細を使用できません。

ソリューション

ファイル分析レポートの詳細の要件 （27 ページ）を参照してください。

ファイル分析レポートの詳細を表示する際のエラー

問題

ファイル分析レポートの詳細を表示しようとすると、「使用可能なクラウドサーバ構成がありません（No cloud server configuration is available）」エラーが表示されます。

ソリューション

[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティ アプライアンス（Security Appliances）] に移動して、ファイル分析機能が有効になっている Web セキュリティ アプライアンスを少なくとも 1 つ追加します。

ファイル分析レポートの詳細をプライベート クラウドの Cisco AMP Threat Grid Appliance に表示する際のエラー

問題

ファイル分析レポートの詳細を表示しようとすると、API キー エラー、登録エラー、またはアクティベーション エラーが表示されます。

ソリューション

プライベート クラウド（オンプレミス）の Cisco AMP Threat Grid Appliance を使用している場合は、（オンプレミスのファイル分析）ファイル分析アカウントをアクティブ化する （29 ページ）を参照してください。

Threat Grid Appliance のホスト名が変更される場合は、参照先の手順のプロセスを繰り返す必要があります。

予想されるデータがレポーティングまたはトラッキングの結果に表示されない

問題

予想されるデータがレポーティングまたはトラッキングの結果に表示されません。

ソリューション

考えられる原因：

- 目的の時間範囲を選択したことを確認します。
- トラッキング結果の場合は、一致したすべての結果が表示されていることを確認します。詳細な Web トラッキング検索結果の表示 （57 ページ）を参照してください。
- Web セキュリティ アプライアンスおよび Cisco コンテンツ セキュリティ管理アプライアンス間のデータ転送が中断されたか、データが消去された可能性があります。[使用可能なデータ（Data Availability）] ページ （43 ページ）を参照してください。
- アップグレードによって情報のレポート方法または追跡方法が変更された場合は、アップグレード前に発生したトランザクションが想定どおりに表示されないことがあります。お使いのリリースでこのような変更が行われたかどうかを確認するには、資料に示された場所で該当するリリース ノートを参照してください。
- Web プロキシ サービスのトラッキング検索結果に表示されない結果については、Web プロキシ サービスによって処理されたトランザクションの検索 （52 ページ）を参照してください。
- ユーザがリクエストしたトランザクションによるフィルタリング時の予期しない結果については、Web プロキシ サービスによって処理されたトランザクションの検索 （52 ページ）の表の「ユーザ要求（User Request）」行を参照してください。

PDF に Web トラッキング データのサブセットのみが表示される

問題

PDF に [Webトラッキング（Web Tracking）] ページに表示されるデータの一部だけが表示されます。

ソリューション

PDF および CSV ファイルで表示されるデータと除外されるデータについては、レポーティング データおよびトラッキング データの印刷およびエクスポートの表で Web トラッキングの情報を参照してください。

L4 トラフィック モニタ レポートのトラブルシューティング

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

関連項目

- [クライアント マルウェア リスク（Client Malware Risk）] レポート （33 ページ）
- L4 トラフィック モニタによって処理されたトランザクションの検索 （56 ページ）

エクスポートされた .CSV ファイルが Web インターフェイスのデータと異なる

問題

.csv ファイルにエクスポートされた [一致したドメイン（Domains Matched）] データが、Web インターフェイスに表示されているデータと異なります。

ソリューション

パフォーマンス上の理由から、最初の 300,000 エントリのみが .csv としてエクスポートされます。

エクスポートされた .CSV ファイルが Web インターフェイスのデータと異なる