新しい Web インターフェイスでのセキュア アプライアンス レポート

この章は、次の項で構成されています。

新しい Web インターフェイスの Web レポート ページの概要

次の表は、Web セキュリティアプライアンス 用 AsyncOS のサポートされている最新リリースで、Web インターフェイスの [レポート（Reports）] ドロップダウンから利用できるレポートを示します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。Web セキュリティアプライアンス でこれ以前のリリースの AsyncOS を実行している場合は、これらのレポートの一部を利用できません。

表 *1 : [Web*レポート（*Web Reports*）*]* ドロップダウンのオプション

[レポート（Reports）] ドロップダウンのオプション	操作
一般的なレポート	

[レポート（Reports）] ドロップダウンのオプション	操作
[概要（Overview）] ページ	[概要（Overview）] ページには、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および要約テーブルが含まれます。詳細については、[概要（Overview）] ページ （5 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）] 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）] ページ （7 ページ）を参照してください。
[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ	指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ （9 ページ）を参照してください。
[SOCKS プロキシ（SOCKS Proxy）] 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）] ページ （12 ページ）を参照してください。
[URLカテゴリ（URL Categories）] 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）] ページ （14 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[ユーザー（Users）] ページ	[ユーザー（Users）] ページには複数の Web トラッキング リンクが表示され、各ユーザーの Web トラッキング情報を確認できます。 [ユーザー（Users）] ページでは、システム上のユーザー（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、そのユーザーが使用している帯域幅の量を表示できます。 [ユーザー（Users）] ページのインタラクティブな [ユーザー（Users）] テーブルで個々のユーザーをクリックすると、その特定のユーザーの詳細情報が [ユーザーの詳細（User Details）] ページに表示されます。 [ユーザーの詳細（User Details）] ページでは、[ユーザー（Users）] ページの [ユーザー（Users）] テーブルで指定したユーザーに関する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、ユーザー レベルの調査を実行している場合に、ユーザーがアクセスしているサイト、ユーザーが直面しているマルウェアの脅威、ユーザー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ー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、[ユーザー（Users）] ページ （18 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）] ページ（Web レポーティング） （19 ページ）を参照してください。
[Webサイト（Web Sites）] 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）] ページ （22 ページ）を参照してください。
[HTTPS レポート（HTTPS Reports）]	[HTTPS レポート（HTTPS Reports）] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー（トランザクションまたは帯域幅の使用量）のすべてを集約しています。詳細については、[HTTPS レポート（HTTPS Reports）] ページ （16 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
脅威レポート	
[マルウェア対策（Anti-Malware）] 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）] ページ （25 ページ）を参照してください。
Advanced Malware Protection ページ	Advanced Malware Protection では、既知のファイルレピュテーションを取得し、レピュテーションサービスには未知である特定のファイルの動作を分析し、新しい情報が利用可能になったときに新たな脅威を継続的に評価し、ネットワークに侵入した後に脅威と判断されたファイルについて通知することによって、ゼロデイの脅威や標的型のファイルベースの脅威から保護します。詳細については、Advanced Malware Protection ページ （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）] 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 Risks）] ページ （29 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）] 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）] ページ （30 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 ページでユーザーが費やした時間を表します。各 URL カテゴリでユーザーが費やした時間。ユーザー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 に各ユーザーが費やした時間。

トランザクションイベントに「viewed」のタグが付けられる（ユーザーが特定の 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 ユーザーごとに、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、各ユーザーが費やした時間は、そのユーザーが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザーがアクティブな 1 分間に 4 つの異なるドメインに進んだ場合、そのユーザーは各ドメインで 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 ユーザーは、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ー名または 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、ユーザーが開始する 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ー 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。

[概要（Overview）] ページ

[概要（Overview）] レポートページには、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および要約テーブルが含まれます。

[概要（Overview）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [概要（Overview）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

[概要（Overview）] レポート 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）] レポートページの下半分は、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 : [*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）	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。

セクション	説明
[Webプロキシアクティビティ総数（Total Web Proxy Activity）]	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、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。 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。
[疑わしいトランザクション（Suspect Transactions）]	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グラフ形式で表示できます。 このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付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疑わしいトランザクションの比率も表示できます。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。
[L4トラフィックモニタの概要（L4 Traffic Monitor Summary）]	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 トラフィックをグラフ形式で表示できます。
上位 URL カテゴリ：総トランザクション数（Top URL Categories: Total Transactions）	ブロックされている上位の URL カテゴリが、URL カテゴリのタイプおよび特定タイプのカテゴリが実際にブロックされた回数を含め、グラフ形式で表示されます。 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 （15 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：総トランザクション数（Top Application Types: Total Transactions）	ブロックされている上位アプリケーション タイプが、実際のアプリケーション タイプ名および特定のアプリケーションがブロックされた回数を含め、グラフ形式で表示されます。
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）	検出されたすべてのマルウェア カテゴリをグラフ形式で表示できます。

セクション	説明
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）	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をグラフ形式で表示できます。ユーザは IP アドレスまたはユーザ名で表示できます。
[上位の脅威カテゴリ：WBRSによりブロック（Top Threat Categories: Blocked ）]	ブロックされたすべての脅威カテゴリを表示できます（グラフ形式）。

[アプリケーションの表示（Application Visibility）] ページ

（注） [アプリケーションの表示（Application Visibility）] の詳細については、『User Guide for AsyncOS for Cisco Web セキュリティアプライアンス』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）] レポートページでは、セキュリティ管理アプライアンスおよび Web セキュリティアプライアンス 内の特定のアプリケーションタイプに制御を適用することができます。

[アプリケーションの表示（Application Visibility）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [アプリケーションの表示（Application Visibility ）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

アプリケーション制御を使用すると、たとえば 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 タイプに対する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、『User Guide for AsyncOS for Cisco Web セキュリティ アプライアンス s』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 3 : [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）	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アプリケーションタイプ（Top Application Types by Total Transactions）]	サイト上でアクセスされた上位のアプリケーション タイプがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。 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。

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アプリケーション（Top Applications by Blocked Transactions）]	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。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。 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。
[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）] 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。
[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）] インタラクティブ テーブルには、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。 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。

[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ

[レイヤ4トラフィックモニター（Layer 4 Traffic Monitor Page）] レポートページには、指定した時間範囲内にレイヤ 4 トラフィックモニターによってお使いの 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。

[Web サイト（Web Sites）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [Web サイト（Web Sites）] を選択します。詳細に

ついては、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

レイヤ 4 トラフィックモニターは、各 Web セキュリティアプライアンス のすべてのポートに着信するネットワークトラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベーステーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

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

表 *4 : [レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] 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。
上位クライアントIP：検出されたマルウェア接続（Top Client IPs: Malware Connections Detected）	組織内で最も頻繁にマルウェア サイトに接続している上位のコンピュータの IP アドレスがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、チャート化するデータの選択を参照してください。 このグラフは、[クライアント マルウェア リスク（Client Malware Risks）] ページ（29 ページ）の [レイヤ4トラフィックモニタ：検出されたマルウェア接続（Layer 4 Traffic Monitor: Malware Connections Detected）] グラフと同じです。
上位マルウェアサイト：検出されたマルウェア接続（Top Malware Sites: Malware Connections Detected）	レイヤ 4 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。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、チャート化するデータの選択を参照してください。

セクション	説明
[クライアントソースIP（Client Source Ips）]	このインタラクティブテーブルを使用すると、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 アドレスを表示できます。 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、[クライアントIPによるフィルタ（Filter by Client IP）] 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、[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニタ（Layer 4 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、レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （39ページ）を参照してください。 このグラフは、[クライアント マルウェア リスク（Client Malware Risks）]ページ （29 ページ）の [レイヤ4トラフィックモニタ：検出されたマルウェア接続（Layer 4 Traffic Monitor: Malware Connections Detected）] グラフと同じです。
[マルウェアポート（Malware Ports）]	このインタラクティブ テーブルを使用すると、レイヤ 4 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を表示できます。 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、[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、[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニタ（Layer 4 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、レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （39 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）]	このインタラクティブ テーブルを使用すると、レイヤ 4 トラフィック モニタが最も頻繁にマルウェアを検出したドメインを表示できます。 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、[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニタ（Layer 4 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、レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （39 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

[SOCKS プロキシ（SOCKS Proxy）] ページ

[SOCKSプロキシ（SOCKS Proxy）] レポート ページでは、SOCKS プロキシを通じて処理されたトランザクションを、宛先およびユーザに関する情報を含めてグラフおよび表の形式で表示できます。

[SOCKS プロキシ（SOCKS Proxy）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [SOCKS プロキシ（SOCKS Proxy）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

（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、『*User Guide for AsyncOS for Cisco Web* セキュリティアプライアンス *s*』を参照してください。

表 5 : [SOCKSプロキシ（SOCKS Proxy）] 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。
上位SOCKS宛先：トランザクション合計（Top Destinations for SOCKS: Total Transactions）	SOCKS プロキシによって検出された上位の宛先をグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。
上位SOCKSユーザ：マルウェア トランザクション（Top Users for SOCKS: Malware Transactions）	SOCKS プロキシによって検出された上位のユーザをグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。
[宛先（Destinations）]	このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理された宛先ドメインまたはIPアドレスのリストを表示できます。 特定の宛先のデータのみを含めるには、テーブルの下部のボックスにドメイン名または 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。
Users	このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理されたユーザまたはIPアドレスのリストを表示できます。 特定のユーザのデータのみを含めるには、テーブルの下部のボックスにユーザ名または IP アドレスを入力し、[ユーザID/クライアントIPアドレスの検索（Find User ID / Client IP Address）] をクリックします。

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 （39 ページ）

[URLカテゴリ（URL Categories）] ページ

[URLカテゴリ（URL Categories）] レポート 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）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [URL カテゴリ（URL Categories）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

[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 : [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。
上位 URL カテゴリ：総トランザクション数（Top URL Categories: Total Transactions）	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。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択（33 ページ）を参照してください。
上位URLカテゴリ：ブロックおよび警告されたトランザクション（Top URL Categories: Blocked and Warned Transactions）	トランザクションごとに発生するブロック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。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択（33 ページ）を参照してください。
[上位 YouTube カテゴリ（Top Youtube Categories）] : [トランザクションの合計数（Total Transactions）]	サイト上でアクセスされている上位の YouTube カテゴリを表示できます（グラフ形式）。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択（33 ページ）を参照してください。

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 セキュリティ アプライアンス 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 （16 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

Web セキュリティ 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自動更新される場合があります。

これらの更新が行われると、古いカテゴリに関連づけられたデータが古すぎてレポートに含まれなくなるまで、古いカテゴリ名は引き続きレポートに表示されます。URL 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。

[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）] ページを [アプリケーションの表示（Application Visibility）] ページ （7 ページ）、[ユーザの詳細（User Details）] ページ（Web レポーティング） （19 ページ）、および [ユーザー（Users）] ページ （18 ページ） と併用して、特定のユーザーや特定のユーザーがアクセスしようとしているアプリケーションまたは Web サイトのタイプを調査できます。

たとえば、[URLカテゴリ（URL Categories）] ページ （14 ページ） からは、サイトでアクセスしたすべての URL カテゴリの詳細を示す人事リソース向けの高レベル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、[ユーザー（Users）] インタラクティブ テーブルのユーザーをクリックすることができます。このアクションにより [ユーザー（Users）] ページ （18 ページ）が表示され、そのユーザーのトレンドを確認し、そのユーザーの 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 （34 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。

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://talosintelligence.com/tickets。

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 [送信したURLのステータス（Status on Submitted URLs）] タブをクリックします。

[HTTPS レポート（HTTPS Reports）] ページ

[HTTPS レポート（HTTPS Reports）] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー（トランザクションまたは帯域幅の使用量）のすべてを集約しています。

また、管理対象のアプライアンスを通過する個々の HTTP/HTTPS Web トラフィックの場合、クライアント側接続またはサーバ側接続のいずれかに基づいてサポート対象の暗号のサマリーを確認することもできます。

[HTTPS レポート（HTTPS Reports）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [HTTPS レポート（HTTPS Reports）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

表 *7 : [HTTPS レポート（HTTPS Reports）] 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、時間範囲の変更を参照してください。

セクション	説明
[Web トラフィック サマリー（Web Traffic Summary）]	アプライアンスの Web トラフィック サマリーは、次のいずれかの方法で表示できます。 • **トランザクション**：グラフ形式の HTTP または HTTPS Web トランザクションの数と表形式の HTTP または HTTPS Web トランザクションの割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。 • **帯域幅の使用量**：グラフ形式の HTTP または HTTPS Web トラフィックで消費される帯域幅の大きさと表形式の HTTP または HTTPS 帯域幅の使用量の割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。
トレンド：Web トラフィック	次のいずれかの方法で必要な時間範囲に基づいてアプライアンスの Web トラフィックのトレンド グラフを表示することができます。 • **Web トラフィック トレンド**：トランザクションまたは帯域幅の使用量に基づいて HTTP と HTTPS Web トラフィックの累積トレンドを表示するには、ドロップダウン リストからこのオプションを選択します。 • **HTTPS トレンド**：トランザクションまたは帯域幅の使用量に基づいて HTTPS Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。 • **HTTP トレンド**：トランザクションまたは帯域幅の使用量に基づいて HTTP Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。
暗号	暗号のサマリーは、次のいずれかの方法で表示できます。 • クライアント側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのクライアント側で使用される暗号のサマリーを表示するには、ドロップダウン リストからこのオプションを選択します。 • サーバ側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのサーバ側で使用される暗号のサマリーを表示するには、ドロップダウン リストからこのオプションを選択します。

[ユーザー（Users）] ページ

[ユーザー（Users）] レポート ページには、各ユーザーの 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。

[ユーザー（Users）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [ユーザー（Users）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

[ユーザー（Users）] ページでは、システム上のユーザー（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、そのユーザー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 上のユーザーの最大数は 500 です。

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

表 *8 : [ユーザー（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）	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。
上位ユーザ：ブロックされたトランザクション（Top Users: Transactions Blocked）	上位ユーザ（IP アドレスまたはユーザ名で表示）と、そのユーザがブロックされたトランザクションの数がグラフ形式で表示されます。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。このページやスケジュール済みのレポートでユーザー名を認識できないようにする方法の詳細については、『*User Guide for AsyncOS for Cisco Content Security Management Appliances*』を参照してください。デフォルト設定では、すべてのユーザー名が表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。

セクション	説明
上位ユーザ：使用帯域幅（Top Users: Bandwidth Used）	システム上で最も多くの帯域幅を使用している上位ユーザ（IP アドレスまたはユーザ名で表示）がグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。
ユーザー（Users）	このインタラクティブテーブルを使用すると、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。[ユーザー（User）] テーブル下部のテキスト フィールドに特定のユーザー ID またはクライアント IP アドレスを入力し、[ユーザーID/クライアントIPアドレスの検索（Find User ID / 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。 特定のユーザをクリックすると、さらに具体的な情報を得ることができます。詳細については、[ユーザの詳細（User Details）] ページ（Web レポーティング） （19 ページ）を参照してください。

（注） クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。

[ユーザの詳細（User Details）] ページ（Web レポーティング）

[ユーザーの詳細（User Details）] ページでは、[ユーザー（Users）] レポート ページのインタラクティブ テーブルで指定したユーザー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、ユーザー レベルの調査を実行している場合に、ユーザーがアクセスしているサイト、ユーザーが直面しているマルウェアの脅威、ユーザー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ー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。

特定のユーザーの [ユーザーの詳細（User Details）] ページを表示するには、[ユーザー（Users）] レポート ページの [ユーザー（Users）] インタラクティブ テーブルでそのユーザーをクリックします。

[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 *9 : [*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。
URLカテゴリ：トランザクション合計（URL Categories: Total Transactions）	特定のユーザが使用している特定の URL カテゴリがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。 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を参照してください。
トレンド：トランザクション合計（Trend: Total Transactions）	このトレンド グラフを使用すると、特定のユーザのすべての Web トランザクションを表示できます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。 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。
[一致したURLカテゴリ（URL Categories Matched）]	[一致したURLカテゴリ（URL Categories Matched）] インタラクティブ テーブルは、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。 テーブル下部のテキスト フィールドに入力して [URLカテゴリの検索（Find URL Category）] をクリックすると、特定の URL カテゴリを検索できます。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を参照してください。

セクション	説明
[一致したドメイン（Domains Matched）]	[一致したドメイン（Domains Matched）] インタラクティブ テーブルは、ユーザがアクセスしたドメインまたは IP アドレスを示します。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。 テーブル下部のテキスト フィールドに入力して [ドメインまたはIPの検索（Find Domain or IP）] をクリックすると、特定のドメインまたは IP アドレスを検索できます。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）]	[一致したアプリケーション（Applications Matched）] インタラクティブ テーブルには、特定のユーザが使用しているアプリケーションが表示されます。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。 テーブル下部のテキスト フィールドに入力して [アプリケーションの検索（Find Application）] をクリックすると、特定のアプリケーション名を検索できます。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。
Advanced Malware Protection 検出された脅威	[セキュアエンドポイントで検出された脅威（Advanced Malware Protection Threats Detected）] インタラクティブ テーブルには、Advanced Malware Protectionエンジンによって検出されたマルウェア脅威ファイルが表示されます。 テーブル下部のテキスト フィールドに入力して [マルウェア脅威ファイルSHA 256の検索（Find malware Threat File SHA 256）] をクリックすると、マルウェア脅威ファイルの特定の SHA 値に関するデータを検索できます。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）]	[検出されたマルウェア脅威（Malware Threats Detected）] インタラクティブ テーブルには、特定のユーザによってトリガーされた上位のマルウェア脅威が表示されます。 テーブル下部のテキスト フィールドに入力して [マルウェア脅威の検索（Find Malware Threat）] をクリックすると、特定のマルウェア脅威名に関するデータを検索できます。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。

セクション	説明
[一致したポリシー（Policies Matched）]	[一致したポリシー（Policies Matched）] インタラクティブ テーブルには、Web へのアクセス時にこのユーザに適用されたポリシー グループが表示されます。 テーブル下部のテキスト フィールドに入力して [ポリシー検索（Find Policy）] をクリックすると、特定のポリシー名を検索できます。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。

[Webサイト（Web Sites）] ページ

[Webサイト（Web Sites）] レポート ページは、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。このレポート ページを使用すると、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタすることができます。

[Web サイト（Web Sites）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [Web サイト（Web Sites）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

[Webサイト（Web Sites）] ページには次の情報が表示されます。

表 *10 : [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）	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。

セクション	説明
上位ドメイン：トランザクション合計（Top Domains: Total Transactions）	Web サイト上でアクセスされた上位のドメインがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。
上位ドメイン：ブロックされたトランザクション（Top Domains: Transactions Blocked）	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。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。 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）]	このインタラクティブ テーブルでは、Web サイト上でアクセスされたドメインを検索できます。特定のドメインをクリックすると、より詳細な情報を得ることができます。[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。

Advanced Malware Protection ページ

Advanced Malware Protection は、次によりゼロデイやファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザーガイドまたは *Web* セキュリティアプライアンス の *AsyncOS* のオンラインヘルプを参照してください。

Advanced Malware Protection レポートページには、次のレポートビューが表示されます。

- Advanced Malware Protection – [セキュアエンドポイントサマリー（AMP Summary）] ページ
- Advanced Malware Protection – [ファイル分析（File Analysis）] ページ

Advanced Malware Protection レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > Advanced Malware Protection を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

Advanced Malware Protection – [セキュアエンドポイントサマリー（AMP Summary）] ページ

[セキュアエンドポイント（Advanced Malware Protection）] レポートページの [セキュアエンドポイントサマリー（AMP Summary）] セクションには、ファイル レピュテーション サービスによって識別された、ファイルベースの脅威が表示されます。

各 SHA にアクセスしようとしたユーザー、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（Malware Threat File）] インタラクティブ テーブルのリンクをクリックすると、レポートに対して選択された時間範囲に関係なく、設定可能な最大時間範囲内で検出されたそのファイルのすべてのインスタンスが [Web トラッキング（Web Tracking）] に表示されます。

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。

[セキュアエンドポイント（Advanced Malware Protection）] ページの [セキュアエンドポイントサマリー（AMP Summary）] セクションには、次の情報を表示できます。

- Advanced Malware Protection エンジンのファイル レピュテーション サービスによって識別されたファイルの概要（グラフ形式）。
- 上位のマルウェア脅威ファイル（グラフ形式）。
- ファイル タイプに基づいた上位の脅威ファイル（グラフ形式）。
- 選択した時間範囲のすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位のマルウェア脅威ファイルを一覧表示する [マルウェア脅威ファイル（Malware Threat Files）] インタラクティブ テーブル。
- 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を一覧表示する [レトロスペクティブ判定変更（Retrospective Verdict Change）] インタラク

ティブテーブルを含むファイル。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。

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。

同一ファイルの複数の Web セキュリティアプライアンス で判定のアップデートが異なる場合は、最も新しいタイムスタンプの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。

Advanced Malware Protection – [ファイル分析（File Analysis）] ページ

[セキュアエンドポイント（Advanced Malware Protection）] レポートページの [ファイル分析（File Analysis）] セクションには、分析のために送信された各ファイルについて、時刻と判定（または中間判定）が表示されます。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。

オンプレミスの AMP Malware Analytics アプライアンスでの導入の場合： AMP Malware Analytics アプライアンスで許可リストに含まれているファイルは、「クリーン」として表示されます。許可リストについては、 AMP Malware Analytics 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ーで 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 AMP Malware Analytics リンクをクリックします。

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。

[セキュアエンドポイント（Advanced Malware Protection）] レポートページの [ファイル分析（File Analysis）] セクションを使用すると、次の情報を表示できます。

- Advanced Malware Protection エンジンのファイル分析サービスによってファイル分析のためにアップロードされたファイルの数。
- ファイル分析要求が完了しているファイルのリスト。
- ファイル分析要求の処理待ちとなっているファイルのリスト。

[マルウェア対策（Anti-Malware）] ページ

[マルウェア対策（Anti-Malware）] レポート 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。

[マルウェア対策（Anti-Malware）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）]>[マルウェア対策（Anti-Malware）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

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、次を参照してください。 [レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ （9 ページ）

[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 *11 : [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）	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。
上位マルウェアカテゴリ（Top Malware Categories）	特定のカテゴリ タイプによって検出された上位のマルウェア カテゴリをグラフ形式で表示できます。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（28 ページ）を参照してください。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。
上位マルウェア脅威（Top Malware Threats）	上位のマルウェア脅威をグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。

セクション	説明
[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 （28 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。

[マルウェア カテゴリ（Malware Category）] レポート ページ

ステップ 1 [レポート（Reports）] > [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 カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

[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ー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ー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。

マルウェアのタイプ	説明
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。

[クライアント マルウェア リスク（Client Malware Risks）] ページ

[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ー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）] ページには、L4 トラフィック モニター（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。

表 *12 : [クライアント マルウェア リスク（Client Malware Risks）] ページの詳細情報*

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。
[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コンピュータの IP アドレスが表示されます。
[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）] インタラクティブ テーブルには、[Webプロキシ：マルウェアリスク別上位クライアント（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。
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）	[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）] インタラクティブ 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。

[Web レピュテーション フィルタ（Web Reputation Filters）] ページ

[Webレピュテーションフィルタ（Web Reputation Filters）] レポート ページでは、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（Web Reputation Filters）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから、[モニターリング（Monitoring）] > [Web レピュテーションフィルタ（Web Reputation Filters）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用を参照してください。

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、『*User Guide for AsyncOS for Web* セキュリティアプライアンス *s*』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 *13 : [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）	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。

セクション	説明
[Webレピュテーションアクション(トレンド)（Web Reputation Actions (Trend)）]	指定した時間における Web レピュテーション アクションの合計数をグラフ形式で表示できます。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)）]	Web レピュテーションアクションのボリュームをトランザクション数の比率で表示できます。
[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）]	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のタイプをグラフ形式で表示できます。 （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）]	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かったトランザクションで発生した脅威のタイプをグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （33 ページ）を参照してください。 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。
一致した脅威カテゴリ	一致した脅威カテゴリを表示できます（グラフ形式）。

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、『*User Guide for AsyncOS for Cisco Web* セキュリティアプライアンス *s*』を参照してください。

（Web レポートのみ）チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できない列もあります。

チャートには、関連付けられたテーブルに表示するように選択した項目（行）数に関係なく、テーブルの列の使用可能なすべてのデータが反映されます。

ステップ 1 特定のチャートで をクリックします。

ステップ 2 表示する必要があるデータを選択します。チャートのプレビューは、選択したオプションに従って表示されます。

ステップ 3 [Apply] をクリックします。

新しい Web インターフェイスでの Web トラッキング

[Webトラッキング検索（Web Tracking Search）] ページでは、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、その詳細を表示することができます。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 （34 ページ）
- レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （39 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 （39 ページ）
- Web トラッキングの検索結果の使用 （40 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 （41 ページ）

Web プロキシと レイヤ 4 トラフィックモニターの違いについては、『*User Guide for AsyncOS for Cisco Web* セキュリティアプライアンス *s*』の「Understanding How the Web セキュリティアプライアンス Works」セクションを参照してください。

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

[Webトラッキング検索（Web Tracking Search）]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 データを検索できます。このデータには、レイヤ4 トラフィック モニタリング データまたは 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。

[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、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、ドロップダウン リストから [Web] を選択します。

ステップ 2 [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 （15 ページ）[トラッキング（Tracking）] > [プロキシサービス（Proxy Services）] を選択します。

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 *14 : [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	
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。

オプション	説明
ユーザー/クライアントIPv4または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（Website）	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。 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。
マルウェアの脅威	特定のマルウェアの脅威でフィルタリングするには、[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 （28 ページ）を参照してください。
アプリケーション	アプリケーションでフィルタ処理するには、[アプリケーション（Application）] を選択し、フィルタ処理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処理するには、[アプリケーションタイプ（Application Type）] を選択し、フィルタ処理するアプリケーションタイプを選択します。

オプション	説明
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。
脅威カテゴリ	特定の脅威カテゴリでフィルタ処理するには、[脅威カテゴリ（Threat Category）] セクションを展開し、必要な脅威カテゴリを選択します。 使用可能なすべての脅威カテゴリを選択するには、[すべて選択（Select All）] をクリックします。
ポリシー	ポリシーグループでフィルタ処理するには、[ポリシー（Policy）] を選択し、フィルタ処理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。
AnyConnect セキュア モビリティ（AnyConnect Secure Mobility）	リモートアクセスまたはローカルアクセスでフィルタ処理するには、[ユーザーの場所（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。）

オプション	説明
Advanced Malware Protection	ファイル レピュテーション サービスで識別されたファイルベースの脅威をフィルタ処理するには、[ファイル名（Filename）]ボックスにファイル名を入力します。 SHA-256ハッシュを使用してファイルをフィルタ処理するには、SHA-256ハッシュ値を [ファイル SHA-256（File SHA-256）] ボックスに入力します。 ファイル判定に基づいてファイルをフィルタ処理するには、[セキュアエンドポイントファイル判定（ AMP File Verdict）] を選択し、判定タイプを選択します。使用可能なファイル判定タイプは、[クリーン（Clean）]、[悪意のある（Malicious）]、[不明（Unknown）]、[スキャン不可（UnScannable）]、および[低リスク（Lowrisk）]です。 判定タイプの [悪意のある（Malicious）] には、次の 3 つのサブカテゴリがあります。 • [マルウェア（Malware）] : [カスタム検出（Custom Detection）] や [カスタムしきい値（Custom Threshold）] 以外の理由によりブロックされたファイル。 • [カスタム検出（Custom Detection）] : AMP for Endpoints コンソールから受信したブロックリストに登録されているファイル SHA の割合。 • [カスタムしきい値（Custom Threshold）] : AMP の設定中にしきい値設定が原因でブロックされたファイル。
ユーザー リクエスト	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。

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。

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

マルウェアのタイプ	説明
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。

レイヤ4 トラフィック モニターによって処理されたトランザクションの検索

[Webトラッキング検索（Web Tracking Search）]ページの[レイヤ4トラフィックモニター（Layer 4 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

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、[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）]ページ （9 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 **[トラッキング（Tracking）] > [SOCKSプロキシ（SOCKS Proxy）]** を選択します。

ステップ 2 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 3 検索条件を入力します。

ステップ 4 **[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）] ページ （12 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

目的	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。

新しい Web インターフェイスの [システムステータス（System Status）] ページ

Web セキュリティアプライアンス で、[モニタリング（Monitoring）] > [システムステータス（System Status）] を選択して、システムステータスをモニターします。このページは、Web セキュリティアプライアンスの現在のステータスと設定を表示します。ブラウザの時刻は、右上隅の [システムステータス（System Status）] ページに表示されます。

[システムステータス（System Status）] ページには次のタブがあります。

デフォルトでは、[ステータス（Status）] タブが表示されます。

ステータス（Status）

[ステータス（Status）] ページには、次の情報が表示されます。

セクション	説明
Webセキュリティアプライアンス のステータス	• システムの動作期間 • システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。 システムによって使用されないRAMはWebオブジェクトキャッシュによって使用されるので、効率的に動作するRAM使用率は90%を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が100％に固定されない場合、システムは正常に動作しています。 （注） プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。
アラート（Alerts）	発生したアラートの名前と日付と時刻が表示されます。右上隅の上部にある [詳細（More）] またはアラート名をクリックすると、[すべてのアラート（All Alerts）] ポップアップが表示されます。[すべてのアラート（All Alerts）] ポップアップで、選択したアラート行が強調表示されます。 [すべてのアラート（All Alerts）] ポップアップには次の情報が表示されます。 • アラートの日付と時刻（Date and Time of Alert） • アラートレベル（Alert Level ）：[情報（Info）]、[警告（Warning）]、または [クリティカル（Critical）] • アラートクラス（Alert Class） • 問題（Problem）：アラートの簡単な説明 • 受信者（Recipient）：アラートの詳細が送信される電子メールアドレス

セクション	説明
ディスク使用率（Disk Usage）	ディスク使用率の値と RAID ストレージのステータスが表示されます。 RAID ストレージのステータスは、アプライアンスの設定によって異なります。仮想アプライアンスの場合、RAID ストレージのステータスには [不明（Unknown）] と表示され、物理アプライアンスには [Optimal（最適）] と表示されます。
プロキシステータス（Proxy Status）	プロキシの CPU 使用率とプロキシディスクの I/O 使用率を表示します。 また、プロキシ接続のバックログもポート番号と接続数とともに表示されます。
高可用性	フェールオーバーグループの名前、優先順位、およびステータスを表示します。 また、有効になっている高可用性フェールオーバーグループの数も表示されます。フェールオーバーグループが存在しない場合は、[設定されていません（Not Configured）] というサービスステータスが表示されます。
プロキシトラフィックの特性（Proxy Traffic Characteristics）	次のプロキシトラフィックの特性が表示されます。 • 1 秒あたりの要求数（Request Per Second） • 帯域幅 • 応答時間（Response Time） • キャッシュヒット率（Cache Hit Rate） これらのデータの平均値と最大値が表示されます。最後の 1 分間、最後の 1 時間、およびプロキシの再起動以降についての平均値が表示されます。最大値は、最後の 1 時間とプロキシの再起動以降について表示されます。

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