セキュア アプライアンス レポート

この章で説明する内容は、次のとおりです。

[概要（Overview）] ページ

[レポート（Reporting）] > [概要（Overview）] ページには、 Secure Web Applianceでのアクティビティの概要が表示されます。このページには、 Secure Web Applianceで処理される Web トラフィックに関するグラフおよびサマリー テーブルが含まれています。

表 *1*: システム概要

セクション	説明
Webプロキシ トラフィックの特徴（Web Proxy Traffic Characteristics）	過去 1 分間における 1 秒あたりの平均トランザクション数、過去 1 分間の平均帯域（bps）、過去 1 分間の平均応答時間（ms）、および現在の接続総数のリスト。
システム リソースの使用率（System Resource Utilization）	現在の全体的な CPU 負荷、RAM およびレポート/ログディスク使用率のリスト。[システムステータス（System Status）] ページに切り替えるには、[システムステータス詳細（System Status Details）] をクリックします（詳細は 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 を参照）。 （注） このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、[システムステータス（System Status）] ページに表示される CPU 値と若干異なる場合があります。

表 *2*: 時間範囲ベースのカテゴリと概要

セクション	説明
時間範囲：以下のセクションに表示されるデータの時間範囲を選択します。オプションは、[時間（Hour）]、[日（Day）]、[週（Week）]、[30日（30 Days）]、[前日（Yesterday）]、[カスタム範囲（Custom Range）] です。	
Webプロキシアクティビティ総数（Total Web Proxy Activity）	トランザクションの実際の数（縦の目盛り）、および（Webプロキシ）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）	疑わしいまたは正常な Web プロキシ アクティビティの比率を表示できます。
L4 トラフィック モニターの概要（L4 Traffic Monitor Summary）	L4 トラフィック モニターによってモニターされ、ブロックされたトラフィックをレポートします。
疑わしいトランザクション（Suspect Transactions）	さまざまなセキュリティ コンポーネントによって疑わしいトランザクションと分類された Web トランザクションを表示できます。 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表示されます。
疑わしいトランザクションの概要（Suspect Transactions Summary）	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。
上位 URL カテゴリ：総トランザクション数（Top URL Categories: Total Transactions）	ブロックされた上位 10 の URL カテゴリが表示されます。

セクション	説明
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）	AVC または ADC エンジンによってブロックされた上位アプリケーションタイプが表示されます。
上位マルウェア カテゴリ：モニターまたはブロック（Top Malware Categories: Monitored or Blocked）	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ー（Top Users Blocked or Warned Transactions）	ブロックされたトランザクションまたは警告されたトランザクションを生成しているユーザーが表示されます。認証されたユーザーはユーザー名で表示され、認証されていないユーザーは IP アドレスで表示されます。
Web トラフィック タップ ステータス	タップされていないトラフィック トランザクションおよびタップされたトラフィック トランザクションがグラフ形式で表示されます。
Web トラフィック タップ サマリ	タップされたトラフィック トランザクションおよびタップされていないトラフィック トランザクションの概要が、トラフィック トランザクションの合計とともに表示されます。
タップされた HTTP/HTTPS トラフィック	タップされた HTTP および HTTPS トラフィック トランザクションがグラフ形式で表示されます。
タップされたトラフィック サマリ	HTTP および HTTPS トラフィック トランザクションの概要が、HTTP および HTTPS トラフィック トランザクションの合計とともに表示されます。
EUP トランザクション	カプセル化された URL のトランザクションが表示されます。これらは、*translate.google.com* などの Web サイトから実行されたトランザクションです。
EUP トランザクションの概要	カプセル化された URL のトランザクションの概要が表示されます。
疑わしい EUP トランザクション	疑わしいと検出された、カプセル化された URL のトランザクションが表示されます。
疑わしい EUP トランザクションの概要	疑わしいと検出された、カプセル化された URL のトランザクションの概要が表示されます。

[ユーザ（Users）] ページ

[レポート（Reporting）]>[ユーザー（Users）]ページには、個々のユーザーの Web トラフィック情報を表示するためのリンクが提供されています。ネットワーク上のユーザーがインターネット、特定の Web サイト、または特定の URL で費やした時間と、ユーザーが使用した帯域幅の量を表示できます。

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。
ブロックされたトランザクション数別上位ユーザー（Top Users by Transactions Blocked）	ブロックされたトランザクションの数（横の目盛り）が最大のユーザー（縦の目盛り）が表示されます。
使用した帯域幅別上位ユーザー（Top Users by Bandwidth Used）	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）を使用しているユーザー（縦の目盛り）が表示されます。
ユーザー テーブル（Users Table）	個々のユーザーを一覧表示し、ユーザーごとに複数の統計情報を表示します。

[ユーザーの詳細（User Details）] ページ

[ユーザーの詳細（User Details）] ページには、[レポート（Reporting）] > [ユーザー（Users）] ページの [ユーザー テーブル（Users Table）] で選択した特定のユーザーに関する情報が表示されます。

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。
総トランザクション数別 URL カテゴリ（URL Categories by Total Transactions）	特定のユーザー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。
総トランザクション数別トレンド（Trend by Total Transaction）	ユーザーが Web にいつアクセスしたかが表示されます。
一致した URL カテゴリ（URL Categories Matched）	完了したトランザクションとブロックされたトランザクションの両方について、指定した時間範囲内で一致したすべての URL カテゴリが表示されます。

セクション	説明
一致したドメイン（Domains Matched）	このユーザーがアクセスした特定のドメインまたは IP アドレスに関する情報が表示されます。 （注） このドメインのデータを CSV ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。
一致したアプリケーション（Applications Matched）	AVC または ADC エンジンによって検出された、特定のユーザーが使用している特定のアプリケーションが表示されます。
検出されたマルウェア脅威（Malware Threats Detected）	特定のユーザーによって引き起こされているマルウェアの脅威の内、上位のものが表示されます。
一致したポリシー（Policies Matched）	この特定のユーザーに適用されている特定のポリシーが表示されます。

[ユーザー数（User Count）] ページ

[レポート（Reporting）]>[ユーザー数（User Count）]ページには、アプライアンスの認証されたユーザーと認証されていないユーザーの合計に関する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 ユーザー数が表示されます。

（注） システムは、認証されたユーザーと認証されていないユーザーの合計を、1 日に 1 回計算します。

たとえば、5 月 22 日 23 時 59 分にユーザー数レポートを表示すると、システムは 5 月 22 日 0 時までの合計ユーザー数を表示します。

[Webサイト（Web Sites）] ページ

[レポート（Reporting）] > [Web サイト（Web Sites）] ページは、 Secure Web Appliance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。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	このメニューからレポートに含めるデータの時間範囲を選択できます。

セクション	説明
総トランザクション数別上位ドメイン（Top Domains by Total Transactions）	サイト上のアクセス上位ドメインがグラフ形式で表示されます。
ブロックされたトランザクション数別上位ドメイン（Top Domains by 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。
一致したドメイン（Domains Matched）	サイト上の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。 （注） このドメインのデータを CSV ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。

[URLカテゴリ（URL Categories）] ページ

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページでは、ネットワーク上のユーザーがアクセスしている URL カテゴリを表示できます。[URL カテゴリ（URL Categories）] ページを [アプリケーションの表示（Application Visibility）] ページおよび [ユーザー（Users）] ページと併用すると、特定のユーザーとそのユーザーがアクセスを試みているアプリケーションや Web サイトのタイプを調べることができます。

（注） 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。

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。
総トランザクション数別上位 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を受けたトランザクション数別上位 URL カテゴリ（Top URL Categories by 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。

セクション	説明
一致した URL カテゴリ（URL Categories Matched）	指定した時間範囲における URL カテゴリ別のトランザクションの傾向、および各カテゴリで使用された帯域幅と費やされた時間が表示されます。 未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。 • 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループ ポリシーに適用できます。 • 評価およびデータベース更新用に、未分類の URL と誤って分類された URL をシスコにレポートできます。 • Web レピュテーション フィルタリングと、アンチマルウェア フィルタリングがイネーブルになっていることを確認してください。

URL カテゴリ セットの更新とレポート

Secure Web Appliance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。

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

[レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページには、Application Visibility and Control または Application Discovery and Control エンジンで検出されたアプリケーションと、使用されているアプリケーションのタイプ、およびブロックされているアプリケーションのタイプが表示されます。

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。
[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。

セクション	説明
ブロックされたトランザクション数別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。
一致したアプリケーション タイプ（Application Types Matched）	[総トランザクション数別上位アプリケーション タイプ（Top Applications Type by Total Transactions）] グラフに表示されているアプリケーション タイプについて、さらに詳しい情報を表示できます。
一致したアプリケーション（Applications Matched）	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。

[マルウェア対策（Anti-Malware）] ページ

[レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページでは、Cisco DVS エンジンによって検出されたマルウェアをモニターおよび識別することができます。

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。
検出された上位マルウェア カテゴリ（Top Malware Categories Detected）	DVS エンジンによって検出された上位のマルウェア カテゴリが表示されます。
検出された上位マルウェア脅威（Top Malware Threats Detected）	DVS エンジンによって検出された上位のマルウェア脅威が表示されます。
マルウェア カテゴリ（Malware Categories）	[検出された上位マルウェア カテゴリ（Top Malware Categories Detected）] セクションに表示されている特定のマルウェア カテゴリに関する情報が表示されます。
マルウェア脅威（Malware Threats）	[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特定のマルウェアの脅威に関する情報が表示されます。

[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。

[マルウェア脅威（Malware Threats）] 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 [マルウェア脅威（Malware Threats）] 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。

Secure Endpoint ページ

「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」を参照してください。

[ファイル分析（File Analysis）] ページ

ファイル レピュテーションおよびファイル分析のレポートとトラッキング を参照してください。

[セキュアエンドポイント判定のアップデート（Cisco Secure Endpoint Verdict Updates）] ページ

「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」を参照してください。

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

[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。

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。
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）	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：マルウェア リスク別クライアント（Web Proxy: Clients by Malware Risk）	[Webプロキシ：マルウェア リスク別クライアント（Web Proxy: Clients by Malware Risk）] 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）]	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。

[Web プロキシ：マルウェア リスク別クライアント（Web Proxy: Clients by Malware Risk）] の [クライアントの詳細（Client Detail）] ページ

[クライアントの詳細（Client Detail）] ページには、指定した時間範囲における特定クライアントの Web アクティビティとマルウェア リスクの全データが表示されます。

ステップ 1 [レポート（Reporting）] > [クライアント マルウェア リスク（Client Malware Risk）] を選択します。

ステップ 2 [Web プロキシ：クライアントマルウェアのリスク（Web Proxy - Client Malware Risk）] セクションで、[ユーザー ID/クライアント IP アドレス（User ID / Client IP Address）] 列のユーザー名をクリックします。

次のタスク

[ユーザーの詳細（User Details）] ページ （4 ページ）

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

[レポート（Reporting）] > [Web レピュテーション フィルタ（Web Reputation Filters）] ページは、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（ユーザーが設定）の結果を表示する、セキュリティ関連のレポーティング ページです。

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。
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（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。
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がトランザクション数との対比で表示されます。
ブロックされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Blocked Transactions）	レピュテーション スコアが低いためブロックされた脅威タイプが表示されます。
詳細にスキャンされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Scanned Further Transactions）	トランザクションのスキャンを指示するレピュテーション スコアが生じた、脅威タイプが表示されます。
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)）	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。

[L4 トラフィック モニター（L4 Traffic Monitor）] ページ

[レポート（Reporting）] > [L4 トラフィック モニター（L4 Traffic Monitor）] ページは、指定した時間範囲内に L4 トラフィック モニターが検出したマルウェア ポートとマルウェア サイトに関する情報を表示する、セキュリティ関連のレポーティング ページです。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 モニターは、アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベース テーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

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。
上位クライアント IP（Top Client IPs）	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。
上位マルウェア サイト（Top Malware Sites）	L4 トラフィック モニター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。
クライアント ソース IP（Client Source IPs）	頻繁にマルウェア サイトに接続している組織内のコンピュータの IP アドレスが表示されます。
マルウェア ポート（Malware Ports）	L4 トラフィック モニター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。
検出されたマルウェア サイト（Malware Sites Detected）	L4 トラフィック モニター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。

[SOCKS プロキシ（SOCKS Proxy）] ページ

[レポート（Reporting）] > [SOCKS プロキシ（SOCKS Proxy）] ページでは、上位宛先およびユーザーに関する情報を含む、SOCKS プロキシを介して処理されたトランザクションのデータとトレンドを表示できます。

[ユーザー ロケーション別のレポート（Reports by User Location）] ページ

[レポート（Reporting）] > [ユーザーの場所別レポート（Reports by User Location）] ページで、ローカルおよびリモート ユーザーが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以下のとおりです。

- ローカル ユーザーおよびリモート ユーザー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。

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。
Web プロキシ アクティビティ総数：リモート ユーザー（Total Web Proxy Activity: Remote Users）	指定した時間（横方向）におけるリモート ユーザーのアクティビティ（縦方向）が表示されます。
Web プロキシの概要（Web Proxy Summary）	ネットワーク上のローカル ユーザーとリモート ユーザー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 ユーザー（Total Web Proxy Activity: Local Users）	指定した時間（横方向）におけるリモート ユーザーのアクティビティ（縦方向）が表示されます。
検出された疑わしいトランザクション：リモート ユーザー（Suspect Transactions Detected: Remote Users）	指定した時間内（横方向）に、リモート ユーザー向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション（縦方向）が表示されます。
疑わしいトランザクションの要約（Suspect Transactions Summary）	ネットワーク上のリモート ユーザーの疑わしいトランザクションの要約が表示されます。
検出された疑わしいトランザクション：ローカル ユーザー（Suspect Transactions Detected: Local Users）	指定した時間内（横方向）に、リモート ユーザー向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション（縦方向）が表示されます。
疑わしいトランザクションの要約（Suspect Transactions Summary）	ネットワーク上のローカル ユーザーの疑わしいトランザクションの要約が表示されます。

[Web トラッキング（Web Tracking）] ページ

[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、その詳細を取得します。必要に応じて、以下のタブのいずれかで検索を行います。

[Web トラッキング（Web Tracking）] ページ	タスクへのリンク
Web プロキシによって処理されたトランザクション（Transactions processed by the Web Proxy）	Web プロキシによって処理されるトランザクションの検索 （14 ページ）
L4 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（Transactions processed by the L4 Traffic Monitor）	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 （17 ページ）
SOCKS プロキシによって処理されたトランザクション（Transactions processed by the SOCKS Proxy）	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 （17 ページ）

または、透過的なパススルーなどの場合に、FQDN を使用して [Web トラッキング（Web Tracking）] ページで Web サイトデータを検索します。

（注） 透過的なリクエストでは、ドメインまたはサーバーの名前がトラッキングページに表示されます。ただし、透過的なパススルーを含む透過的な要求が SNI なしで送信されると、IP アドレスが表示されます。

Web プロキシによって処理されるトランザクションの検索

[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、特定のユーザーまたはすべてのユーザーの Web の使用状況を追跡し、レポートできます。

所定の期間内に記録されたトランザクションのタイプ（ブロック、モニターリング、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。

ステップ 1 [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 設定項目を設定します。

設定	説明
時間範囲（Time Range）	レポート対象の時間範囲を選択します。
ユーザー/クライアント IP（User/Client IP）	（任意）レポートに表示される認証ユーザー名、または追跡対象のクライアント IP アドレスを入力します。IP 範囲を 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）	（任意）追跡対象の Web サイトを入力します。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。 （注） SNI（サーバー名指定）で検索できます。SNI、TLS プロトコルの拡張子を使用して、クライアントは Web トランザクションの実行中に安全にホスト名を指定できます。単語全体を指定する必要があります。 SNI を有効にするには、セキュアエンドポイント 、およびレピュテーションサービスを有効にする必要があります。
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。

ステップ 4 （任意）[詳細設定（Advanced）] セクションを展開してフィールドを設定し、より詳細な条件で Web トラッキングの結果をフィルタリングします。

設定	説明
URL カテゴリ（URL Category）	URL カテゴリでフィルタリングするには、[URL カテゴリ別フィルタ（Filter by URL Category）] を選択し、フィルタリング対象とする 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。
アプリケーション（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	このトランザクションに対して最終決定を行うポリシーの名前でフィルタするには、[アクション ポリシーによってフィルタ（Filter by Action 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（アクセス ポリシー、復号化ポリシー、またはデータ セキュリティ ポリシー）を入力します。詳細については、アクセス ログ ファイル内の Web プロキシ情報の PolicyGroupName に関する説明を参照してください。

設定	説明
Secure Endpoint	Web トラッキング機能と Secure Endpoint 機能についてを参照してください。
マルウェアの脅威	特定のマルウェアの脅威でフィルタリングするには、[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。
WBRS	[WBRS] セクションでは、Web 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。
AnyConnect セキュア モビリティ	ユーザーの場所（リモートまたはローカル）によってフィルタリングするには、[ユーザーの場所でフィルタ（Filter by User Location）] を選択し、フィルタリングするユーザー タイプを選択します。
ユーザー リクエスト	クライアントによって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、[ユーザーが要求したトランザクションによるフィルタ（Filter by User-Requested Transactions）] を選択します。 （注） このフィルタをイネーブルにすると、検索結果に「最も想定される」トランザクションが含まれることがあります。
カプセル化された URL の保護	カプセル化された URL トランザクションでこのフィルタを有効にします。 （注） • HTTPS プロキシを有効にする必要があります。HTTPS プロキシのイネーブル化を参照してください • https://translate.google.com の Web レピュテーション スコアの範囲が復号する設定になっていることを確認します。復号化ポリシー グループの Web レピュテーション フィルタの設定を参照してください

ステップ 5 [検索（Search）] をクリックします。

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。

[詳細の表示（Display Details）] リンクの下のカッコ内の数値は、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、ユーザー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を示します。

ステップ 6 （任意）[トランザクション（Transactions）] 列の [詳細の表示（Display Details）] をクリックし、各トランザクションに関する詳細情報を表示します。

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

ヒント 結果内の URL が切り詰められている場合、アクセス ログで完全な URL を確認できます。

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

次のタスク

- URL カテゴリ セットの更新とレポート （7 ページ）
- マルウェアのカテゴリについて
- Web トラッキング機能と Secure Endpoint 機能について

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

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

- 時間範囲
- サイト、使用された IP アドレスまたはドメイン
- [ポート（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

一致した検索結果のうち最初の 1000 件が表示されます。

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

ブロックまたは完了したトランザクション、ユーザー、および宛先ドメイン、IP アドレス、またはポートなど含む、さまざまな基準を満たすトランザクションを検索できます。

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

[SOCKS プロキシ（SOCKS Proxy）] ページ （12 ページ）

[システム容量（System Capacity）] ページ

[レポート（Reporting）] > [システム容量（System Capacity）] ページには、 Secure Web Appliance のリソース使用率に関する現在および履歴情報が表示されます。

[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、以下のことに留意することが重要です。

- **Hour レポート。** Hour レポートは、分テーブルに照会して、60 分間を超える分単位で、1 分間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。
- **Day レポート。** Day レポートは、時間テーブルに照会して、24 分間を超える時間単位で、1 時間にアプライアンスに記録されたアイテム（バイトや接続など）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。

Week レポートおよび 30 Days レポートは、Hour レポートおよび Day レポートと同じように動作します。

[システムステータス（System Status）] ページ

システム ステータスをモニターするには、[レポート（Reporting）] > [システム ステータス（System Status）] ページを使用します。このページは、 Secure Web Applianceの現在のステータスと設定を表示します。

セクション	表示内容
Secure Web Appliance 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。 このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、システムの [概要（Overview）] ページ（[概要（Overview）] ページ （1 ページ））に表示される CPU 値と若干異なる場合があります。 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。
プロキシトラフィックの特性（Proxy Traffic Characteristics）	• 1 秒あたりのトランザクション • 帯域幅 • 応答時間 • キャッシュ ヒット率 • 接続
Web トラフィック タップ（Web Traffic Tap）	Web トラフィック タップ CPU 使用率。
高可用性	高可用性サービスのステータス。
外部サービス（External Services）	• Identity Services Engine

セクション	表示内容
現在の設定（Current Configuration）	Web プロキシ設定： • Web プロキシのステータス：イネーブルまたはディセーブル。 • 展開トポロジ • Web プロキシ モード：フォワードまたは透過。 • IP スプーフィング：イネーブルまたはディセーブル。 L4 トラフィック モニター設定： • L4 トラフィック モニターのステータス：イネーブルまたはディセーブル。 • L4 トラフィック モニターの配線。 • L4 トラフィック モニターのアクション：モニターまたはブロック。 Web トラフィック タップ設定： • Web トラフィック タップのステータス：イネーブルまたはディセーブル。 • Web トラフィック タップ インターフェイス：P1、P2、TI、T2 Secure Web Appliance バージョン情報 ハードウェア情報

関連項目

[システム容量（System Capacity）] ページ （18 ページ）

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。