フィルタとダッシュボード

この章は、次のセクションで構成されています。

フィルタとダッシュ ボードの概要

Cisco Advanced Web Security Reporting では、利用可能なアクセスログ、SOCKS ログ、および AMP ログのデータのカスタム検索を定義し、各検索結果を個別に表示できます。この処理は「フィルタリング」とも呼ばれます。このフィルタリングは、Webセキュリティアプライアンスのネイティブなレポート機能との一貫性をできる限り保ちます。各カスタム検索は、独自のページまたは「パネル」に表示され、後からアクセスするために保存できます。

Cisco Advanced Web Security Reporting アプリケーションでは、定義済みの検索がいくつか提供されており、いつでも表示するように選択できます。これらの既存の検索と保存されたフィルタは、「ダッシュボード」と呼ばれます。実際に、保存されたフィルタは、[カスタムダッシュボード（Custom Dashboards）]メニューから開きます。さらに、これらの検索が表示されるページまたはパネルも、ダッシュボードと呼ばれることがあります。

（注） Cisco Advanced Web Security Reporting を使用して提示されたデータには、Web セキュリティアプライアンスだけで入手できるよりも多くの情報が表示される場合があります。

ダッシュボードの表示

始める前に

Cisco Advanced Web Security Reporting 管理者は、各種ダッシュボードに表示する Web セキュリティアプライアンス（ホスト）を制御できます。追加、削除、または名前を変更するホストがある場合は、その詳細を Cisco Advanced Web Security Reporting 管理者に知らせてください。

ステップ 1 Web ブラウザを使用して Cisco Advanced Web Security Reporting アプリケーションにサインインします。

概要情報を示した [概要（Overview）] ダッシュボードが表示されます。

ステップ 2 [カスタムダッシュボード（Custom Dashboards）] メニューなどの他のメニューから既存のダッシュボードを選択するか、[カスタムフィルタ（Custom Filter）] を選択して新しい検索を定義します。この検索は、カスタム ダッシュ ボードとして保存できます。

Cisco Advanced Web Security Reporting で提供されるダッシュボードのリストについては、「事前定義されたダッシュボード」を参照してください。[カスタムフィルタ（Custom Filter）] オプションの使用については、「カスタム フィルタの作成」で説明しています。

ステップ 3 該当する場合は、時間範囲、データ ソース、およびホストを選択します。

（注） カスタム ダッシュボードでの検索がサポートされています。[送信（Submit）] ボタンのある [メイン検索（Main Search）] フィールドを使用してデータを検索できます。結果のペインで、セカンダリ [検索（search）] フィールドを使用して検索結果をフィルタ リングできます。

事前定義されたダッシュボード

Cisco Advanced Web Security Reporting アプリケーションでは、デフォルトで次のダッシュボードが提供されています。

- 概要
- ユーザ分析
  - 概要
  - ロケーションベース
  - ユーザドリルダウン
- ブラウジング分析
  - ドメイン
    - 概要

- ロケーションベース
- ドメインドリルダウン

- URL カテゴリ
  - 概要
  - ロケーションベース
  - URL カテゴリドリルダウン

- アプリケーション分析
  - 概要
  - アプリケーション
    - ロケーションベース
    - アプリケーション ドリルダウン
  - アプリケーションタイプ
    - アプリケーション タイプ ドリルダウン

- セキュリティ分析
  - L4 トラフィックモニタ
    - 概要
    - L4 TM ドリルダウン
  - アンチ スパム
    - 概要
    - クライアント マルウェア リスク
    - ロケーションベース
    - マルウェア カテゴリ ドリルダウン
    - マルウェア脅威ドリルダウン
  - Web レピュテーションフィルタ
    - 概要
    - ロケーションベース
  - 高度なマルウェア防御

- 概要
- ロケーションベース
- ファイル分析：[このアプライアンスからの完了済みの分析リクエスト（Completed Analysis Requests from This Appliance）] テーブルでいずれかのエントリのファイル ID（SHA256）をクリックすると、そのファイルの [ファイル分析の詳細（File Analysis Detail）] ページが開きます。[ファイル分析の詳細（File Analysis Detail）] ページにある [ファイル分析サーバのURL（File Analysis Server URL）] テキストボックスで、データを表示する対象のファイル分析サーバを指定できます。通常この URL は、8.5 までのどの Web セキュリティ アプライアンス バージョンでも `https://intel.api.sourcefire.com` です。

  ただし、この特定のファイルの分析に別のサーバを使用する場合は（デモなど）、このファイル（このドリルダウン レポートにアクセスする際にクリックしたSHAによって決まります）の詳細を表示するサーバの URL を変更できます。
- AMP判定のアップデート

- Web トラッキング
  - プロキシサービス
  - SOCKS
  - SOCKS ドリルダウン
- 設定
  - 分散環境
  - システム
  - データ
  - ユーザと認証
  - 第三者のサービス
- ユーザー
  - アカウントの編集
- Web セキュリティの統合レポート：Cisco Umbrella および Cisco Web セキュリティアプライアンスからの統合されたレポートを以下の分類で表示できます。
  - 概要
  - アクティビティ検索
  - セキュリティアクティビティ
  - 上位ドメイン

- 上位カテゴリ
- 上位ユーザ
- 上位セキュリティカテゴリ

関連情報：

- ダッシュボードの表示

ダッシュボードとして保存

定義済みの各レポートページでは、表示されているレポートを別のダッシュボードとして保存できます。つまり、現在表示されているダッシュボードの複製を作成できます。

（注） また、「ダッシュ ボードとしてのカスタム フィルタの保存」の説明のとおり、カスタムフィルタをダッシュボードとして保存することもできます。これらのダッシュ ボードは、その他のカスタム ダッシュボードと同様に開いたり編集したりできます。

ステップ 1 現在の**レポートページ**で、必要に応じて時間、データソース、ホストパラメータなどを変更し、[ダッシュボードとして保存（Save As Dashboard）] ボタンをクリックします。

ステップ 2 [ダッシュボードパネルとして保存（Save As Dashboard Panel）] ダイアログボックスで次の情報を入力します。

- [ダッシュボードタイトル（Dashboard Title）]：新しいダッシュボードの表示名です。

  レポート ページをダッシュボードとして保存する場合は、カスタム ダッシュボードを区別するために、選択された入力を反映する適切なタイトルを指定する必要があります。

- [ダッシュボードID（Dashboard ID）]：ダッシュボードを保存するファイル名を指定します。後で変更することはできません。
- [ダッシュボードの説明（Dashboard Description）]：（任意）簡単な説明です。
- [ダッシュボードの権限（Dashboard Permissions）]：[プライベート（Private）] または [アプリで共有（Shared in App）] を選択します。プライベート ダッシュボードはユーザ本人にのみ表示され、共有ダッシュボードはすべてのユーザに表示されます。

ステップ 3 [保存（Save）] をクリックします。

新しいダッシュボードが [カスタムダッシュボード（Custom Dashboards）] メニューに追加されます。ダッシュボードを表示および編集する場合は、メニューからそのカスタム ダッシュボードを選択します。

カスタム ダッシュボードの編集

現在表示されているカスタム ダッシュボードを編集できます。個々のレポート パネルの位置変更および削除、ダッシュボードのタイトルおよび説明の変更、パネルの検索クエリーの時間範囲の変更、パネルのチャート タイプの変更などが可能です。

ステップ 1 現在のカスタム ダッシュボードで [編集（Edit）] ボタンをクリックして、次のいずれかのオプションを選択します。

- [パネルの編集（Edit Panel）]：パネルの編集を有効にします。パネルの位置を変更する場合はタイトル バーをドラッグし、パネルを削除する場合は [閉じる（close）] ボタンをクリックします。パネルのタイトルの上にラベルを追加することもできます。該当するボタンをクリックすると次の操作を実行できます。
  - パネルのチャート タイプを変更する。
  - チャートのパラメータを変更する。
- [タイトルまたは説明の編集（Edit Title or Description）]：ダッシュボード全体のタイトルおよび説明を変更します。
- [権限の編集（Edit Permissions）]：ダッシュボード全体の表示権限を変更します。
- [PDF配信のスケジュール（Schedule PDF Delivery）]：このダッシュボードからのレポート PDF の定期的な生成をスケジュールします。生成された PDF は指定したアドレスに電子メールで送信されます。
- [削除（Delete）]：ダッシュボード全体を削除します。

ステップ 2 [パネルの追加（Add Panel）] をクリックして、類似したカスタム ダッシュボードのパネルをこのダッシュボードに追加することもできます。

このボタンは、カスタム ダッシュボードの [編集（Edit）] ボタンをクリックすると表示されます。

ステップ 3 ダッシュボードの編集作業が終わったら、[完了（Done）] をクリックします。

カスタム フィルタの作成

カスタムフィルタを設定すると、選択した「データモデル」が Cisco Advanced Web Security Reporting によって検索されます。さらに、「データオブジェクト」や「属性」を選択することで、これらを基準にモデルのデータ セットをフィルタリングして表示できます。使用可能なデータ モデルはそれぞれ、特定の種類の一連のログを表します。一方、データ オブジェクトはそれぞれ、特定のログの種類か、場合によっては現在のデータ モデルの子コンポーネントであるデータ セットを表します。

以下の手順に従って、特定のログ データの集合をフィルタし、表示します。

ステップ 1 Cisco Advanced Web Security Reporting のメニューバーで [カスタムフィルタ（Custom Filter）] をクリックします。

ステップ 2 [データモデルの選択（Select a Data Model）] ページで、検索するデータ モデルを選択します。

- [AMPアクセスモデル（AMP Access Model）]：すべての使用可能な Advanced Malware Protection ログ。
- [SOCKSアクセスモデル（SOCKS Access Model）]：すべての使用可能な SOCKS ログ。
- [Webアクセスデータ（Web Access Data）]：その他すべての使用可能な Web 関連ログ（たとえば、ユーザやドメインに関連するアクセス ログ）。
  - 次に示すこのデータ モデルのフィールドは、Cisco Umbrella ログから値を格納できます。これらのフィールドは、Umbrella ログのカスタム ダッシュ ボードを作成するために使用できます。これには、フィルタのドロップダウンリストで *sourcetype* に *ciscoumbrella* を選択します。

フィールド	Umbrella のログ データ
user_id_fixed	外部または内部IP。存在する場合には、最も詳細なアイデンティティも含みます。
dest_domain	要求されたドメイン。
odnsaction	DNS 要求に対して行われたアクション。
x_wbrs_threat_type_fixed	悪意のあるドメインに対して DNS 要求があった場合のマルウェアのカテゴリ。
x_webcat_code_full	要求されたドメインの URL カテゴリ。
dnsquery_fixed	実行された DNS 要求のタイプ。
dnsresp_fixed	要求に対する DNS 戻りコード。

各データ モデルは、指定されたタイプの収集されたログを表します。

ステップ 3 [データセットを選択（Select a Dataset）] ページで、以下の操作を行います。

1. 選択したデータ モデルで使用可能なデータ オブジェクトの一覧を展開します。これには、データ モデルのイベント名（たとえば、「Web アクセス イベント」）の前にある右矢印をクリックします。
2. データ オブジェクト（[イベント（Event）] または [属性（Attribute）]）をクリックし、[上位値（Top Values）] または [時間帯別の上位値（Top Values by Time）] のいずれかを選択します。

   [上位値（Top Values）] を選択した場合、行に選択した属性データが表示されます。各行には 2 番目の列が表示され、その特定の属性エントリについてのイベント カウントが表示されます。

   [時間帯別の上位値（Top Values by Time）] を選択した場合、`_time` が [行を分割（Split Rows）] のフィルタになり、選択した属性が [列を分割（Split Columns）] のフィルタになります。つまり、各行がイベント時間を表し、各列が特定の属性のエントリを表します。したがって、各テーブル セルには、特定の時間における特定の属性の出現回数が表示されます。

（注）　各属性エントリの前にある記号はその種類を表し、たとえば英数字値や数値などがあります。

ステップ 4　前の手順で [上位値（Top Values）] を選択した場合、[列を分割（Split Columns）] メニューから別の属性を選択することで、表示されるデータをさらにフィルタできます。

ステップ 5　必要に応じて、カスタム フィルタダッシュボードで表示される情報とそのプレゼンテーションをさらに調整できます。詳細については、「カスタム フィルタの表示の変更と保存」を参照してください。

ステップ 6　このカスタム フィルタ ダッシュボードを保存するには、**[名前を付けて保存（Save As）] > [ダッシュボードパネル（Dashboard Panel）]** を選択します。すると、このダッシュボードパネルが、指定した名前の下の [カスタムダッシュボード（Custom Dashboards）] メニューに表示されます。

（注）　現在のフィルタのテーブルまたはグラフが読み込まれるか更新されるときには、[一時停止（Pause）] または [停止（Stop）] ボタンをクリックできます。[リロード（Reload）] をクリックすることで、いつでもフィルタ処理されたデータをリロードできます。

カスタム フィルタの表示の変更と保存

カスタムフィルタを作成した後、[新規カスタムフィルタ（New Custom Filter）] ページに表示されるオプションを使用して、追加のフィルタ処理を順次適用し、表示する情報をさらに絞り込むことができます。たとえば、[行を分割（Split Rows）] 機能を使用して現在のデータセットをデータ入力ごとに 1 つの行に分割し、次に [列を分割（Split Columns）] を使用して各行に列を追加し、各行のエントリから抽出された情報を示すことに加えて、[フィルタ（Filters）] と [列値（Column Values）] メニューを使用してパラメータと属性を適用することもできます。

さらに、別のデータモデルや別のデータオブジェクトを選択することもできます。書式設定を変更したり、ページ上のデータをエクスポートおよび印刷したりできます。グラフの種類を変更できます。また、このカスタムフィルタをダッシュボードとして保存することもできます。[新規カスタムフィルタ（New Custom Filter）] パネルのオプションは次のとおりです。

- [グラフの種類（Chart type）]：アプリケーションウィンドウの左側にあるデータ表示タイプストリップのボタンをクリックして、カスタムフィルタデータの表示方法を変更します。たとえば、棒グラフや円グラフを選択できます。
- [名前を付けて保存（Save As）]：現在のフィルタをダッシュボードとして保存します。このダッシュボードは、[カスタムダッシュボード（Custom Dashboards）] メニューに追加されます。詳細については、「ダッシュ ボードとしてのカスタム フィルタの保存」を参照してください。
- [クリア（Clear）]：現在のカスタムフィルタパラメータとデータの表示をクリアします。
- **Web アクセス イベント**
  - 「カスタムフィルタの作成」で説明されているように、別のデータモデルを選択できます。
  - 「カスタムフィルタの作成」で説明されているように、現在選択されているデータモデルから別のデータオブジェクトを選択できます。

- 現在表示されているデータ セットについての情報も表示されます。

- [フィルタ（Filters）]：表示されているフィルタについては、編集ボタン（鉛筆アイコン）をクリックして、フィルタに適用されているパラメータを変更するか、または表示されているフィルタを削除します。追加（+）ボタンをクリックすると、現在のフィルタの集合に別のデータ オブジェクトを選択できます。
- [行を分割（Split Rows）]：現在の行オブジェクトパラメータの編集、行オブジェクトの削除、およびスプリット行へのオブジェクト追加（フィルタの説明に準拠）を行うことができます。
- [列を分割（Split Columns）]：同様に、現在の列オブジェクトパラメータの編集、列オブジェクトの削除、および [列を分割（Split Columns）] へのオブジェクトの追加を行うことができます。
- [列値（Column Values）]：さらに、列値を編集および削除できます。

（注） 特定のオプションに対して複数のオブジェクトが表示されている場合、オブジェクトボックスをドラッグして順番を変更できます。たとえば、現在選択されているフィルタが左から右に `All timecategory is *`、`dest_url` の場合、`dest_url` を他の 2 つの間にドラッグでき、それによって順番が `All time`、`dest_url`、`category is *` になります。

ダッシュ ボードとしてのカスタム フィルタの保存

各 [カスタムフィルタ（Custom Filter）] ページでは、表示されたフィルタをカスタムダッシュボードとして保存することで、今後の表示にすぐに使用できます。

ステップ 1 現在の [カスタムフィルタ（Custom Filter）] ページで、必要に応じて検索パラメータを変更し、[名前を付けて保存（Save As）] ボタンをクリックして、[ダッシュボードパネル（Dashboard Panel）] を選択します。

ステップ 2 [ダッシュボードパネルとして保存（Save As Dashboard Panel）] ダイアログボックスで、このダッシュボードの種類として [新規（New）] または [既存（Existing）] のいずれかを指定します。

1. [新規（New）] を選択した場合は、次の情報を入力します。
   - [ダッシュボードタイトル（Dashboard Title）]：（任意）新しいダッシュボードの表示名です。

     レポート ページをダッシュボードとして保存する場合は、カスタム ダッシュボードを区別するために、選択された入力を反映する適切なタイトルを指定する必要があります。
   - [ダッシュボードID（Dashboard ID）]：ダッシュボードを保存するファイル名を指定します。後で変更することはできません。
   - [ダッシュボードの説明（Dashboard Description）]：（任意）簡単な説明です。

- [ダッシュボードの権限（Dashboard Permissions）]：[プライベート（Private）] または [アプリで共有（Shared in App）] を選択します。プライベート ダッシュボードはユーザ本人にのみ表示され、共有ダッシュボードはすべてのユーザに表示されます。
- [パネルのタイトル（Panel Title）]：（任意）これは、このカスタムダッシュボードを表示するときに、パネルの上部に表示されるタイトルです。
- [パネルの付加機能（Panel Powered By）]：これは常に [インライン検索（Inline Search）] です。
- [パネルの内容（Panel Content）]：[統計情報（Statistics）] または <グラフの種類> を選択して、このフィルタの情報を表形式のデータまたは現在表示に使用されているグラフの種類で表示します。

2. [既存（Existing）] を選択した場合は、次の情報を入力します。
   - [選択（Select）]：このフィルタデータを追加する既存のカスタムダッシュボードの名前を選択します。
   - [パネルのタイトル（Panel Title）]：（任意）これは、このカスタムダッシュボードを表示するときに、パネルの上部に表示されるタイトルです。
   - [パネルの付加機能（Panel Powered By）]：これは常に [インライン検索（Inline Search）] です。
   - [パネルの内容（Panel Content）]：[統計情報（Statistics）] または <グラフの種類> を選択して、このフィルタの情報を表形式のデータまたは現在表示に使用されているグラフの種類で表示します。

ステップ 3 [保存（Save）] をクリックします。

新しいダッシュボードが [カスタムダッシュボード（Custom Dashboards）] メニューに追加されます。ダッシュボードを表示および編集する場合は、メニューからそのカスタム ダッシュボードを選択します。

データのエクスポート

現在のカスタム フィルタ パネルのエクスポート

現在表示されているカスタムフィルタデータは、カンマ区切り値（csv）ファイル、XMLファイル、または JavaScript Object Notation（json）ファイルとしてエクスポートできます。

ステップ 1 [エクスポート（Export）] ボタンをクリックします。

ステップ 2 [結果をエクスポート（Export Results）] ダイアログボックスで、次の手順を実行します。

1. [形式（Format）] で目的の形式を [CSV]、[XML]、または [JSON] から選択します。
2. （任意）必要に応じて [ファイル名（File Name）] を指定します。

   ファイル名を入力しない場合は、ランダムな番号の名前が生成されます。
3. [結果の数（Number of Results）] で保存する結果の数を指定します。[制限なし（Unlimited）] または [制限あり（Limited）] をクリックします。

   [制限なし（Unlimited）] を選択した場合、現在のフィルタ パラメータによって返されるすべてのデータが保存されます。[制限あり（Limited）] を選択した場合、[最大の結果数（Max Results）] に表示する値の最大数を指定します。この値の数だけ保存されます。

ステップ 3 [エクスポート（Export）] をクリックし、ダイアログ ボックスを閉じて、エクスポート ファイルを作成します。

ステップ 4 [開く/保存（Open/Save）] ダイアログボックスが表示されます。[形式（Format）] で選択した形式のファイルについて、システムで定義されているアプリケーションを使用してエクスポートファイルを開くか、または指定した場所にファイルを保存するように選択できます。

現在のダッシュボードを PDF ファイルとしてエクスポート

現在のダッシュボード データを PDF ファイルとしてエクスポートできます。

始める前に

- Cisco Advanced Web Security Reporting 管理者が DF 出力を有効化していることを確認します。

ステップ 1 [PDFへエクスポート（Export PDF）] ボタンをクリックします。

ステップ 2 [開く/保存（Open/Save）] ダイアログボックスが表示されます。システムで PDF に対して定義されているアプリケーションを使用して PDF ファイルを開くか、または指定した場所にファイルを保存するように選択できます。

現在のダッシュボードを別のファイル フォーマットにエクスポート

現在表示されているダッシュボードデータは、カンマ区切り値（csv）ファイル、XML ファイル、または JavaScript Object Notation（json）ファイルとしてエクスポートできます。

ステップ 1 ダッシュボード データの表示ペインにカーソルを移動します。

ステップ 2 [ダウンロード（Download）] アイコン をクリックします。

1. [形式（Format）] で目的の形式を [CSV]、[XML]、または [JSON] から選択します。

2. （任意）必要に応じて [ファイル名（File Name）] を指定します。

   ファイル名を入力しない場合は、ランダムな番号の名前が生成されます。

3. [結果の数（Number of Results）] で保存する結果の数を指定します。[制限なし（Unlimited）] または [制限あり（Limited）] をクリックします。

   [制限なし（Unlimited）] を選択した場合、現在のフィルタ パラメータによって返されるすべてのデータが保存されます。[制限あり（Limited）] を選択した場合、[最大の結果数（Max Results）] に表示する値の最大数を指定します。この値の数だけ保存されます。

ステップ 3 [エクスポート（Export）] をクリックし、ダイアログ ボックスを閉じて、エクスポート ファイルを作成します。

ステップ 4 [開く/保存（Open/Save）] ダイアログボックスが表示されます。[形式（Format）] で選択した形式のファイルについて、システムで定義されているアプリケーションを使用してエクスポートファイルを開くか、または指定した場所にファイルを保存するように選択できます。

関連情報：

- スケジュール済 PDF レポートのセットアップ（任意）

データの書式

場合によっては、Cisco Advanced Web Security Reporting でのデータのプレゼンテーションが、ソースアプリケーションのネイティブなレポート機能によって提供されるデータのプレゼンテーションと異なります。

データ	書式例
大きな数値（8 桁以上）	`2E11` は 2 x 1011 を表します。
時刻（Time）	`d+hh:mm:ss.ms` は、経過した日数、時間数、分数、秒数、およびミリ秒数を示します。たとえば `1+03:22:36.00` は、1 日と 3 時間 22 分 36 秒 0 ミリ秒を表します。

時間範囲

ヒント より迅速に結果を返すには、より小さな時間範囲を選択します。

データ可用性のタイミング

範囲	インデックス生成開始	データのレポート表示
時間（Hour）	1 時間経過後	インデックス生成開始後 60 ～ 90 分
日（Day）	午前 0 時過ぎ	インデックス生成開始後 1 日
Week	土曜日の午前 0 時過ぎ（日曜日の早朝）	インデックス生成開始後 1 週間
90 日間	90 日目の午前 0 時過ぎ	インデックス生成後 90 日
カスタム：1 時間未満	1 時間経過後	インデックス生成開始後 60 ～ 90 分
カスタム：1 日未満	午前 0 時過ぎ	インデックス生成開始後 1 日
カスタム：1 週間未満	土曜日の午前 0 時過ぎ（日曜日の早朝）	インデックス生成開始後 1 週間

トラブルシューティング

- Cisco Advanced Web Security Reporting は、一連のファイルを使用してメニューにデータを入力します。メニューで問題が発生した場合は、アプリケーションの参照フォルダに、次のファイルを含むすべての必要なファイルが含まれていることを確認します。

  — `malware_categories.csv`

  — `transaction_types.csv`

  — `url_categories.csv`

  — `malware_categories_opendns.csv`

  — `url_categories_opendns.csv`

- 管理者は、アプリケーション内に表示される URL カテゴリのリストを編集できます。カテゴリがアクセスログに表示されるが参照ファイルにはない場合、Cisco Advanced Web Security Reporting に [カスタムカテゴリ（Custom Category）] が表示されます。
- 管理者は、Web トラッキングフォームのドロップダウンフィールドに使用できるオプションを制御できます。

使用シナリオ

ユーザの調査

ここでは、システム管理者がどのように社内の特定ユーザを調査するかについて例を挙げます。このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。システム管理者は、この問題を調査するにあたり、従業員の Web 使用状況のトレンドおよびトランザクション履歴を見る必要があります。

- 総トランザクション数別 URL カテゴリ（URL Categories by Total Transactions）
- 総トランザクション数別傾向（Trend by Total Transactions）
- 一致した URL カテゴリ（URL Categories Matched）
- 一致したドメイン（Domains Matched）
- 一致したアプリケーション（Applications Matched）
- 検出されたマルウェア脅威（Malware Threats Detected）
- 特定のユーザ ID またはクライアント IP の [一致したポリシー（Policies Matched）]
- AD グループの詳細

システム管理者は、これらのレポートを使用することにより、たとえば、ユーザの「johndoe」がブロックされた URL（[ドメイン（Domains）] セクションにある [ブロックされたトランザクション（Transactions Blocked）] 列に表示）にアクセスしようとしていたかどうかを特定できます。

Web 使用トレンドの閲覧

ステップ 1 [Cisco Advanced Web Security Reporting] ドロップダウンメニューから [ユーザ（Users）] を選択します。

ステップ 2 **ユーザ ID** または**クライアント IP アドレス**をクリックします。

（注） [ユーザ（Users）] テーブルに調査対象の**ユーザ ID** または**クライアント IP アドレス**が見つからない場合は、いずれかのユーザ ID またはクライアント IP をクリックします。ユーザ ID またはクライアント IP アドレスのすべてまたは一部を検索します。

ステップ 3 （任意）**[アクション（Actions）]** > **[印刷（Print）]**を選択します。

トランザクション履歴の閲覧

ステップ 1 [Cisco Advanced Web Security Reporting] ドロップダウンメニューから [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）] を選択します。

ステップ 3 次の条件で検索できます。

- [日（Day）]
- [データソース（Data Source）]
- [ユーザーIDまたはクライアントIP（Uer ID or Client IP）]
- [ユーザー（User）]（レポートに表示される認証ユーザー名を入力します。）
- [クライアントIP（Client IP）]（追跡するクライアント IP アドレス。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）]
- トランザクション タイプ（[すべてのトランザクション（All Transactions）]、[完了したもの（Completed）]、[ブロック対象（Blocked）]、[モニタ対象（Monitored）]、または [警告対象（Warned）]）
- [ホストネーム（Hostname）]
- [SNI]（階層の取得）
- [WBRS: 最小スコア範囲（WBRS: Min Score Range）]（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（フィルタ処理する WBRS スコア範囲の下限値を選択します）。
- [WBRS: 最大スコア範囲（WBRS: Max Score Rang）]（フィルタ処理する WBRS スコア範囲の上限値を選択します）
- （任意）[詳細設定（Advanced）]（追加のフィルタオプションを表示するには、このチェックボックスを選択します）
- [WBRSの表示: スコアなし（Show WBRS: No Score）]（フィルタ処理して、Web レピュテーションスコアのない結果を表示できます。WBRS スコアのないトランザクションを表示するには、[WBRSの表示: スコアなし（Show WBRS: No Score）] を「True」として選択します。WBRS スコアがないトランザクションのみを表示するには、[WBRS: 最小スコア範囲（WBRS: Min Score Range）] および [WBRS: 最大スコア範囲（WBRS: Max Score Range）] を「NA」として選択し、[WBRSの表示: スコアなし（Show WBRS: No Score）] を「True」として選択します）
- [URLカテゴリ（URL Category）]
- [アプリケーション（Application）]
- [アプリケーションタイプ（Application Type）]

- [ポリシー（Policy）]
- [マルウェアの脅威（Malware Threat）]
- [マルウェア カテゴリ（Malware Category）]
- [レピュテーションの脅威（Reputation Threat）]
- [ユーザの場所（User Location）]
- [AMPファイル判定（AMP File Verdict）]
- [ファイル名（Filename）]
- [ファイルSHA256（File SHA256）]

ステップ 4 （任意）CSV ファイルにデータをエクスポートするには、[エクスポート（Export）] をクリックします。[プロキシサービス（Proxy Services）] ダッシュボードから、10,000 個のトランザクションを表示し、エクスポートすることができます。

アクセスした URL

このシナリオでは、セールス マネージャが、自社で先週のアクセス数が多かった上位 5 つの Web サイトを知りたいと考えています。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

最もアクセス数の高い Web サイトの閲覧

ステップ 1 [Cisco Advanced Web Security Reporting]ドロップダウンメニューから [Webサイト（Web Sites）] を選択します。

ステップ 2 [時間範囲（Time Range）] のドロップダウン リストから[週（Week）] を選択します。

ステップ 3 ドメインと一致する表で、上位 25 のドメインが表示されます。

ステップ 4 ドメインをクリックすると、そのドメインにアクセスしたユーザが頻度の高い順に表示されます。

アクセス数の高かった URL カテゴリ

このシナリオでは、人事部マネージャが、過去30日間で社内において最もアクセス数の高かった上位 3 つの URL カテゴリを知りたいと考えています。さらに、ネットワーク管理者が、同様の情報を使って帯域幅の使用状況をモニタし、最も帯域幅を使用している URL がどれかを知りたいと考えています。以下の例は、複数の人の関心事に対応するデータを1つのレポートで提供する方法を示します。

最も一般的な URL カテゴリの閲覧

ステップ 1 [Cisco Advanced Web Security Reporting] ドロップダウンメニューから [URLカテゴリ（URL Categories）] を選択します。

ステップ 2 トータル トランザクションのグラフでは、上位 10 の URL カテゴリを表示します。

ステップ 3 （任意）[PDFへエクスポート（Export PDF）] ボタンをクリックします。PDF を保存して担当者に送信します。

ステップ 4 URL カテゴリの照合表で [許容バイト数（Bytes Allowed）] コラムを参照します。

ステップ 5 （任意）[PDFへエクスポート（Export PDF）] ボタンをクリックします。PDF を保存して担当者に送信します。

ステップ 6 より詳細に調べる場合は、特定の URL カテゴリを選択します。