Cisco Advanced Web Security Reporting 5.0 のインストールとセットアップのユーザ ガイド

バージョン 5.0

2016 年 5 月 13 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Advanced Web Security Reporting 5.0 のインストールとセットアップのユーザ ガイド

CONTENTS

はじめに 1-1
- 5.0 の新機能 1-2
- サポートされる機能と、サポートされない機能 1-2

システム要件およびサイズ変更とスケーリングの推奨事項 1-3

セットアップの概要 1-3

Advanced Web Security Reporting アプリケーションのバージョン 5.0 のインストール 1-4
- Linux の場合 1-4
- Windows の場合 1-5

Advanced Web Security Reporting アプリケーションのバージョン 5.0 へのアップグレード 1-5
- バージョン 4.0 以降からのアップグレード 1-5
  - Linux の場合 1-6
  - Windows の場合 1-6
- バージョン 3.0 からバージョン 5.0 へのアップグレード 1-6
- 管理ユーザ（Administrative Users） 1-7
- コンフィギュレーションのベスト プラクティス 1-8
- Advanced Web Security Reporting アプリケーションを起動および停止するコマンド 1-8
  - Linux の場合 1-8
  - Windows の場合 1-8

ライセンスおよび移行 1-9
- v3.0 WSA レポートから v4.0 WSA 専用レポートへの移行 1-9
- v3.0 WSA 専用レポートから v4.0 ハイブリッド レポートへの移行 1-9
- 新しいハイブリッド レポート ライセンス 1-9
- ハイブリッド レポート ライセンスの問題 1-10
- バージョン 4.0 以降のアップグレードに関するライセンスの考慮事項 1-10
- ライセンスのインストール 1-10

アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成 1-11

履歴データのインポートおよびインデックス作成 1-11
- （任意）インデックス生成後にログ ファイルを削除するようアプリケーションを設定する 1-12

継続的なデータ転送の設定 1-12
- WSA ログのデータ入力の設定 1-13
- WSA Syslog のデータ入力の設定 1-13

Web セキュリティ アプライアンスからのログ転送の確立 1-14
CWS ログのアップデートの設定 1-16
部門メンバーシップ クエリーのセットアップ（任意） 1-16
部門メンバーシップ レポートのセットアップ 1-17
職務別の部門レポートへのアクセスの制限 1-18
部門メンバーシップ レポートのトラブルシューティング 1-18
スケジュール済 PDF レポートのセットアップ（任意） 1-18
電子メール アラートの設定 1-19
PDF レポート生成のスケジュール 1-19
レポートの概要 2-1
レポートへのアクセス 2-1
ダッシュボードとして保存（Save As Dashboard） 2-2
カスタム ダッシュボードの編集 2-2
データの書式 2-3
時間範囲 2-3
データ可用性のタイミング 2-4
エクスポート 2-4
.CSV ファイルにエクスポート 2-4
PDF ファイルにエクスポート 2-4
汎用データと特定データ 2-5
詳細を表示 2-5
検索 2-5
検索のヒント 2-5
検索のトラブルシューティング 2-5
定義済みレポート 2-6
使用シナリオ 2-7
ユーザの調査 2-7
Web 使用トレンドの閲覧 2-8
トランザクション履歴の閲覧 2-8
アクセスした URL 2-8
最もアクセス数の高い Web サイトの閲覧 2-8
アクセス数の高かった URL カテゴリ 2-9
最も一般的な URL カテゴリの閲覧 2-9

インストールおよびセットアップ

- はじめに（1-1 ページ）
- システム要件およびサイズ変更とスケーリングの推奨事項（1-3 ページ）
- セットアップの概要（1-3 ページ）
- Advanced Web Security Reporting アプリケーションのバージョン 5.0 のインストール（1-4 ページ）
- Advanced Web Security Reporting アプリケーションのバージョン 5.0 へのアップグレード（1-5 ページ）
- ライセンスおよび移行（1-9 ページ）
- アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成（1-11 ページ）
- 履歴データのインポートおよびインデックス作成（1-11 ページ）
- 継続的なデータ転送の設定（1-12 ページ）
- CWS ログのアップデートの設定（1-16 ページ）
- 部門メンバーシップ クエリーのセットアップ（任意）（1-16 ページ）
- スケジュール済 PDF レポートのセットアップ（任意）（1-18 ページ）

はじめに

Cisco Advanced Web Security Reporting アプリケーションに用意されているレポートとダッシュボードは、複数の Cisco Web セキュリティ アプライアンスおよびシスコのクラウド Web セキュリティ（CWS）ゲートウェイから送られる大量のデータを分析できるように設計されています。Advanced Web Security Reporting アプリケーションには、データ収集とレポート作成アプリケーション、および Web セキュリティ アプライアンス（WSA）と CWS サービスから収集したログ データを転送する関連サーバが含まれます。

（注） クラウド Web セキュリティは「ScanSafe」とも呼ばれます。

Advanced Web Security Reporting アプリケーションはログ データを受信してデフォルトまたはメイン インデックスに保存します。これらのデータは、定義済みレポートを使用することで表示できます。

図 1-1　Advanced Web Security Reporting システムの汎用アーキテクチャ

5.0 の新機能

機能	説明
以前のバージョンからのシームレス アップグレード	
CWS の AMP レポート	
レポート全体のメール配信のスケジュール	
カスタム ダッシュボードのサポート	既存のパネルの追加/削除 グラフ形式の選択 独自のダッシュボードの作成
更新されたインターフェイス	アプリケーションの「ルックアンドフィール」が更新されました。

サポートされる機能と、サポートされない機能

コンポーネント	サポート対象	未サポート
レポート	Advanced Web Security Reporting アプリケーションに含まれるレポート	カスタム レポート
サーバ	単一サーバ展開	複数サーバ展開

コンポーネント	サポート対象	未サポート
送信方法	FTP（ファイルおよびディレクトリ） TCP（Syslog）	該当なし
PDF	統合 PDF 生成 スケジュール済 PDF レポート	該当なし
カスタム ダッシュボード	選択した時間範囲、ソース タイプおよびホスト（制限あり）のカスタム ダッシュボードを作成する、各レポートの [ダッシュボードとして保存（Save As Dashboard）]。	

システム要件およびサイズ変更とスケーリングの推奨事項

システム要件およびサイズ変更とスケーリングの推奨事項については、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html から入手できる『*Advanced Web Security Reporting Release Notes*』で詳しく説明されています。

セットアップの概要

次のいずれか

- Advanced Web Security Reporting アプリケーションの新規インストール
  - Advanced Web Security Reporting アプリケーションのバージョン 5.0 のインストール（1-4 ページ）
  - ライセンスおよび移行（1-9 ページ）
  - アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成（1-11 ページ）
  - 履歴データのインポートおよびインデックス作成（1-11 ページ）
  - 継続的なデータ転送の設定（1-12 ページ）（Web セキュリティ アプライアンスのセットアップを含む）
  - CWS ログのアップデートの設定（1-16 ページ）

または

- Advanced Web Security Reporting アプリケーションのバージョン 5.0 へのアップグレード（1-5 ページ）

Advanced Web Security Reporting アプリケーションのバージョン 5.0 のインストール

Advanced Web Security Reporting アプリケーションのバージョン 5.0 をインストールするには、この項の手順を実行します。

- Linux の場合（1-4 ページ）
- Windows の場合（1-5 ページ）

Linux の場合

次のタスクを順番どおりに実行してください。

ステップ 1　Advanced Web Security Reporting 5.0 ソフトウェアのインストーラをダウンロードします。

https://software.cisco.com/download/release.html?mdfid=282803425&softwareid=283998384&release=5.0&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　インストーラ ソフトウェアを解凍します。

現在の作業ディレクトリにインストールするには、次のコマンドを実行します。

```
tar zxvf cisco_wsa_reporting-5.0.0.tgz.
```

`/opt/cisco-wsa_reporting/` ディレクトリにインストールするには、次のコマンドを使用します。

```
tar zxvf cisco_wsa_reporting-5.0.0.tgz -C /opt
```

ステップ 3　ディレクトリを `/cisco_wsa_reporting/` に変更してセットアップ スクリプトを実行します。

```
cd cisco_wsa_reporting
./setup.sh
```

セットアップ時に、進行状況およびマイルストーン ステートメントが表示されます。

ステップ 4　次の手順で Advanced Web Security Reporting アプリケーションを起動してログインします。

a. ブラウザ ウィンドウで `http://<hostname>:8888` にアクセスします。

（注）　以前のバージョンではポート 8000 が使用されていましたが、バージョン 4.0 以降で使用するポートは 8888 です。

b. ユーザ名を `admin`、パスワードを `Cisco@dmin` としてログインします。

c. `admin` パスワードを変更します。

次の手順

- ライセンスおよび移行（1-9 ページ）

Windows の場合

はじめる前に

Windows でインストールできる Advanced Web Security Reporting ソフトウェアのバージョンは 1 つのみです。したがって以前のバージョンがインストールされている場合は、既存のデータをバックアップして以前のバージョンをアンインストールしてから、新しいバージョンをインストールする必要があります。

ステップ 1　Advanced Web Security Reporting 5.0 ソフトウェアのインストーラをダウンロードします。

https://software.cisco.com/download/release.html?mdfid=282803425&softwareid=283998384&release=5.0&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　インストーラを解凍します。7-Zip や WinZip などのアプリケーションを使用できます。

ステップ 3　コマンドライン シェル（PowerShell）を管理者として起動し、ディレクトリをインストーラの解凍先ディレクトリに変更します。

ステップ 4　`install.bat` を実行します。

アプリケーションが `C:\Program Files\Cisco\CiscoWSAReporting` フォルダにインストールされます。

ステップ 5　Advanced Web Security Reporting サーバを再起動します。

ステップ 6　次の手順で Advanced Web Security Reporting アプリケーションを起動してログインします。

a. ブラウザ ウィンドウで `http://<hostname>:8888` にアクセスします。

（注）　以前のバージョンではポート 8000 が使用されていましたが、バージョン 4.0 以降で使用するポートは 8888 です。

b. ユーザ名を `admin`、パスワードを `Cisco@dmin` としてログインします。

c. `admin` パスワードを変更します。

次の手順

- ライセンスおよび移行（1-9 ページ）

Advanced Web Security Reporting アプリケーションのバージョン 5.0 へのアップグレード

- バージョン 4.0 以降からのアップグレード（1-5 ページ）
- バージョン 3.0 からバージョン 5.0 へのアップグレード（1-6 ページ）

バージョン 4.0 以降からのアップグレード

バージョン 4.0 またはバージョン 4.5 からバージョン 5.0 にアップグレードするには、この項の手順を実行します。

- Linux の場合（1-6 ページ）
- Windows の場合（1-6 ページ）

Linux の場合

次のタスクを順番どおりに実行してください。

ステップ 1　Advanced Web Security Reporting 5.0 ソフトウェアのインストーラ（CiscoAdvancedWebSecurityReporting_Linux_5_0_0.tgz）をダウンロードします。

https://software.cisco.com/download/release.html?mdfid=282803425&softwareid=283998384&release=5.0&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　ダウンロードしたインストーラ ファイルを cisco_wsa_reporting ディレクトリのベース ディレクトリにコピーします。

たとえば、Advanced Web Security Reporting の以前のバージョンが /opt/cisco_wsa_reporting/ にインストールされている場合は、.tgz ファイルを /opt/ ディレクトリに置きます。

ステップ 3　ディレクトリをインストールのベース ディレクトリ（/opt/ など）に変更します。

ステップ 4　次のコマンドを実行してインストーラを解凍します。

```
tar -zxvf CiscoAdvancedWebSecurityReporting_Linux_5_0_0-002.tgz
cisco_wsa_reporting/SeamlessUpgrade.sh; cp -f cisco_wsa_reporting/SeamlessUpgrade.sh .
```

ステップ 5　アップグレード スクリプトを実行します。

```
./SeamlessUpgrade.sh CiscoAdvancedWebSecurityReporting_Linux_5_0_0-002.tgz
```

Windows の場合

次のタスクを順番どおりに実行してください。

ステップ 1　Advanced Web Security Reporting 5.0 ソフトウェアのインストーラ（CiscoAdvancedWebSecurityReporting_Windows_5_0_0.tgz）をダウンロードします。

https://software.cisco.com/download/release.html?mdfid=282803425&softwareid=283998384&release=5.0&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　インストーラを解凍します。7-Zip や WinZip などのアプリケーションを使用できます。

ステップ 3　コマンドライン シェル（PowerShell）を管理者として起動し、ディレクトリをインストーラの解凍先ディレクトリに変更します。

ステップ 4　コマンド .\WinSeamlessUpgrade.ps1 を実行して Advanced Web Security Reporting アプリケーションをアップグレードします。

バージョン 3.0 からバージョン 5.0 へのアップグレード

バージョン 3.0 インストールをバージョン 5.0 にアップグレードするには、この項の手順を実行します。バージョン 3.0 インストールからのアップグレードでは、次の基本的な手順が必要です。

- 既存のバージョン 3.0 インデックス データのバックアップ コピーを作成する。
- 新しくインストールしたバージョン 5.0 アプリケーションをシャットダウンする。
- バージョン 3.0 のバックアップ データを新しいデータ ディレクトリにコピーする。

- バージョン 5.0 アプリケーションを再起動する。

詳細な手順は次のとおりです。

この手順では、バージョン 3.0 が `/opt/splunk` で動作していて、新しいバージョンが `/opt/cisco_wsa_reporting` にあると想定します。状況に応じてパスを調整します。

ステップ 1　古いバージョンを停止します。

```
/opt/splunk/bin/splunk stop
```

ステップ 2　古い `inputs.conf` ファイル（`/opt/splunk/etc/apps/SplunkforCiscoIronportWSA/local/inputs.conf`）を編集して、すべての入力を無効にします。

ステップ 3　古いバージョンを再起動します。

```
/opt/splunk/bin/splunk start
```

ステップ 4　メイン インデックスにホット バケットが残っていないことを確認します。

```
cd /opt/splunk/var/lib/splunk/defaultdb/db
ls -la hot*（結果がないことを確認する）
```

ステップ 5　古いバージョンを再度停止します。

```
/opt/splunk/bin/splunk stop
```

ステップ 6　新しいバージョンが実行されていないことを確認します。

```
/opt/cisco_wsa_reporting/shutdown.sh
```

ステップ 7　新しいバージョンのインデックス フォルダを削除します。

```
cd /opt/cisco_wsa_reporting/var/lib/splunk
rm -rf *
```

ステップ 8　古いバージョンから新しいバージョンにインデックスをコピーします。

```
cd /opt/cisco_wsa_reporting/var/lib/splunk
cp -r /opt/splunk/var/lib/splunk/defaultdb .
cp -r /opt/splunk/var/lib/splunk/fishbucket .
```

ステップ 9　Advanced Web Security Reporting の新しいバージョンを起動します。

```
/opt/cisco_wsa_reporting/startup.sh
```

ステップ 10　ブラウザで `http://<wsa_reporting_server_host_name>:8888` を開いて、ユーザ名 `admin` とパスワード `Cisco@dmin` を使ってログインします。

管理ユーザ（Administrative Users）

Advanced Web Security Reporting アプリケーションの管理ユーザは 2 人です。

- 「デフォルトの管理者」（ユーザ名：`admin`、パスワード：`Cisco@dmin`）はすべての管理機能にアクセスできます。

  `admin` ユーザはライセンスをインストールして分散環境を設定できます。設定、テスト、トラブルシューティングを行うためにこのアカウントを使用します。
- 2 人目の管理ユーザ（名前：`wsa_admin`、パスワード：`Ironp0rt`）には管理機能のサブセットへのアクセス権があります。

インストール後すぐに両方のパスワードを変更することを推奨します（[設定（Settings）] > [ユーザと認証（Users and Authentication）] > [アクセスコントロール（Access Controls）] > [ユーザ（Users）]）。

コンフィギュレーションのベスト プラクティス

- WSA および CWS アプライアンスに一貫したタイムゾーンを設定します。
  検索結果に表示される時間は、Advanced Web Security Reporting インスタンスの「ローカルの」時間を表しています。デフォルトでは、アプライアン ログへの入力はすべて TZ = GMT に設定されます。
- ローカル `admin` アカウントのパスワードを記録します（選択した認証方法に関係なく）。

Advanced Web Security Reporting アプリケーションを起動および停止するコマンド

Linux の場合

Advanced Web Security Reporting アプリケーションを停止する手順は次のとおりです。

ディレクトリを `/cisco_wsa_reporting/` に変更し、次のコマンドを実行します。

```
./shutdown.sh
```

Advanced Web Security Reporting アプリケーションを起動する手順は次のとおりです。

ディレクトリを `/cisco_wsa_reporting/` に変更し、次のコマンドを実行します。

```
/startup.sh
```

Windows の場合

Advanced Web Security Reporting アプリケーションを停止する手順は次のとおりです。

ディレクトリを *<install_home>*\ に変更し、次のコマンドを実行します。

```
shutdown.bat
```

Advanced Web Security Reporting アプリケーションを起動する手順は次のとおりです。

ディレクトリを *<install_home>*\ に変更し、次のコマンドを実行します。

```
startup.bat
```

（注）　Windows では、*<install_home>*\ は `C:\Program Files\Cisco\CiscoWSAReporting` です。

ライセンスおよび移行

バージョン 4.5 で追加された 3 つの AMP レポートは、WSA AMP ログでのみサポートされます。

バージョン 4.0 以降の Advanced Web Security Reporting アプリケーションは、WSA と CWS の両方のログ レポートをサポートします。これは「ハイブリッド レポート」と呼ばれます。ハイブリッド レポートを使用するには、新しいライセンスをインストールする必要があります。既存のライセンスで WSA 専用レポートを引き続き使用できます。次のようにライセンスと移行のさまざまな状況が考えられます。

- v3.0 WSA レポートから v4.0 WSA 専用レポートへの移行
- v3.0 WSA 専用レポートから v4.0 ハイブリッド レポートへの移行
- 新しいハイブリッド レポート ライセンス

v3.0 WSA レポートから v4.0 WSA 専用レポートへの移行

バージョン 4.0 以降のソフトウェアをインストールし、以前にインストール済みのライセンスで引き続き WSA レポートを使用できます。さらに、バージョン 4.0 以降のソフトウェアには評価ライセンスが組み込まれています。このライセンスにはハイブリッド レポートを評価できるレポート ソース タイプが追加されています。

v3.0 WSA 専用レポートから v4.0 ハイブリッド レポートへの移行

前の項で説明したように、バージョン 4.0 以降のソフトウェアをインストールしても、以前にインストール済みのライセンスで引き続き WSA レポートを使用できます。また、組み込みの評価ライセンスを使用してハイブリッド レポート機能を評価することができます。

WSA 専用レポートからハイブリッド レポートに移行するには、Cisco Technical Assistance Center (TAC) のサポート ケースを開いて既存のライセンスを削除し、ソース タイプの完全なリストを含む (`ciscocws` ソース タイプが https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case に含まれています) 新しいハイブリッド レポート ライセンスをインストールする必要があります。

（注） バージョン 3.0 WSA 専用レポートからバージョン 4.0 以降のハイブリッド レポートにアップグレードする場合にのみ TAC への連絡が必要です。

新しいハイブリッド レポート ライセンス

新規の Advanced Web Security Reporting ユーザとしてバージョン 4.0 以降のソフトウェアをインストールした後に、WSA およびハイブリッド Web セキュリティ レポートを利用する場合は、評価期間中に無制限で組み込みの評価ライセンスを使用できます。評価期間後も継続する場合や、評価の制限を超えてレポートを提供する場合は、マスター ハイブリッド ライセンスを取得する必要があります。新規インストールでは、注文時に提供される infodoc を使用して、ライセンスを要求します。

ハイブリッド レポート ライセンスの問題

ハイブリッド レポート ライセンスに関する問題が発生した場合は、シスコに問い合わせる前に、CWS ログ抽出ライセンス（L-CWS-LOG-LIC=）を購入済みであること、および CWS ログをインポートするように環境が設定されていることを確認してください。

また、レポート アプリケーション ライセンス（SMA-WSPL-LIC=、SMA-WSPL-LOW-LIC=、または SMA-WSPL-HIGH-LIC= を購入した場合に発行されます）に含まれているソース タイプが、`wsa_trafmonlogs`、`wsa_accesslogs`、`wsa_w3clogs`、`wsa_syslog`、`wsa_amplogs`、および `ciscocws` **のみ**であることを確認します。

シスコの Advanced Web Security Reporting アプリケーションを使用してこれ以外のソース タイプ（`ps` など）のログを処理すると、ライセンス違反エラーが発生します。このようなエラーは、別のソース タイプのログを生成する他のアプリケーションをインストールした場合に発生することがあります。

バージョン 4.0 以降のアップグレードに関するライセンスの考慮事項

履歴データ転送を処理するためには、最初に大量のデータに適した評価ライセンスが最低限必要になります。その後、Advanced Web Security Reporting ライセンスが必要になります。

1. 履歴データの初回アップロード時と毎日の継続的な運用時の両方でインデックスが作成されるデータ量を考慮します。
2. 履歴データ転送に十分な評価ライセンスを取得してアップロードします。
3. インデックスが作成される該当ソース タイプの予想データに対して十分な Advanced Web Security Reporting ライセンスを取得およびアップロードします。
4. ライセンスのタイプを、トライアルから評価または Advanced Web Security Reporting に変更します。
5. インデックスが正しいプールにレポートされることを確認します。

a. [設定（Settings）] > [システム（System）] > [ライセンス（Licensing）] に移動して、該当するライセンス スタックで [今日使用されたプールインデクサボリューム（Pools Indexers Volume used today）] 行を探します。

b. [編集（Edit）] をクリックすると、必要に応じて日単位の最大ボリューム割り当ておよび割り当てられたインデクサを変更できます。

c. 変更を行わなかった場合は [キャンセル（Cancel）]、変更した場合は [送信（Submit）] をクリックします。

ライセンスのインストール

ライセンスを取得するには、注文時に提供された情報を参照してください。以下の手順に従って、Advanced Web Security Reporting ライセンスをインストールします。

ステップ 1　Advanced Web Security Reporting アプリケーションを起動（ブラウザ ウィンドウで `http://<hostname>:8888` と入力）して、デフォルト `admin` ユーザとしてログインします。

ステップ 2　[設定（Settings）] > [システム（System）] > [ライセンス（Licensing）] に移動します。

ステップ 3　[ライセンスの追加（Add License）] をクリックします。

ステップ 4　XML ライセンス ファイルを参照します。

ステップ 5　[Install（インストール）] をクリックします。

アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成

ログ	デフォルト パス	変数
トラフィック モニタ	/$Input_base/wsa_hostname/trafmonlogs/	$Input_base = ルート FTP フォルダのパス host_name = WSA デバイス
アクセス	/$Input_base/wsa_hostname/accesslogs/	$Input_base = 展開先 host_name = WSA デバイス
AMP	/$Input_base/wsa_hostname/amplogs/	$Input_base = 展開先 host_name = WSA デバイス

履歴データのインポートおよびインデックス作成

はじめる前に

- Advanced Web Security Reporting アプリケーションのバージョン 5.0 へのアップグレード（1-5 ページ）に記載された設定のタスクを完了します。
- フォルダ構造を理解します。アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成（1-11 ページ）を参照してください。

ステップ 1　ログ ファイルのフォルダ構造に、履歴ログ ファイルをコピーします。

ステップ 2　Advanced Web Security Reporting アプリケーションで `admin` としてログインします。

ステップ 3　データがインポートされていることを確認します。

a. [設定（Settings）] > [データ（Data）] > [インデックス（Indexes）] を選択します。

b. サマリー行までスクロールします。

c. [最も古いイベント（Earliest event）] および [最新のイベント（Latest event）] カラムに適切な日付が表示されることを確認します。履歴データのインポートを評価ライセンスで実行した場合は、アカウント用にダウンロードしたデフォルト ライセンスをインストールし、非プロダクション ライセンスをすべて削除してください。

ヒント　チェックサム エラーにより、アプリケーションで設定された入力タイプのファイルにインデックスが生成されない場合は、`inputs.conf` ファイルの各入力スタンザに `crcSalt = <source>` 行を追加します（次の「（任意）インデックス生成後にログ ファイルを削除するようアプリケーションを設定する」で `inputs.conf` ファイルの編集について説明します）。

次の作業

- WSA ログのデータ入力の設定（1-13 ページ）。

（任意）インデックス生成後にログ ファイルを削除するようアプリケーションを設定する

はじめる前に

inputs.conf ファイルが <*install_home*>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/ ディレクトリに存在しない場合は、入力コンフィギュレーション ファイル（<*install_home*>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf）を作成します。

ステップ 1　テキスト エディタを使用して、<*install_home*>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf を開きます。

ステップ 2　次のようにセグメントを追加します。

```
[batch:///home/logger/incoming/wsa176.wga/accesslogs/*]
host_segment = 4
disabled = false
sourcetype = wsa_accesslogs
move_policy = sinkhole
```

ここでの最初の行は、WSA ログが送信される FTP ディレクトリ パスです。2 行目はホスト名を含む FTP パスの一部です。3 行目はこの FTP 入力を有効にします。4 行目でこの入力のソースを指定します。最後の行（move_policy = sinkhole）は、インデックス生成後の元のデータの削除を有効にします。

ステップ 3　inputs.conf ファイルを保存して、[設定（Settings）] > [システム（System）] > [サーバコントロール（Server controls）] に移動し、[リスタート（Restart）] をクリックして Advanced Web Security Reporting アプリケーションを再起動します。

継続的なデータ転送の設定

はじめる前に

- 履歴データのインポートおよびインデックス作成（1-11 ページ）
- ログ ファイルへのパスを把握します（アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成（1-11 ページ））。
- Advanced Web Security Reporting アプリケーションに admin としてログインします。

WSA ログのデータ入力の設定

（注）　複数の WSA からのデータ入力を設定するには、ホストごとに次の手順を繰り返してください。

ステップ 1　Advanced Web Security Reporting アプリケーションで次の手順を実行します。

- [設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [ファイルとディレクトリ（Files & directories）] を選択します。

ステップ 2　`CiscoWSA` とラベル付けされた入力をすべて無効にします。

ステップ 3　[新規（New）]をクリックします。

ステップ 4　[継続的なモニタ（Continuously Monitor）] をクリックし、WSA ログの送信先となる FTP ディレクトリへのフル パスを入力します。

このパスと WSA の [ログ設定（Log Subscription）] ページで指定した FTP パスが一致する必要があります。

ステップ 5　[次へ（Next）]をクリックします。

ステップ 6　[ソースタイプ（Sourcetype）] で [手動（Manual）] をクリックし、[ソースタイプ（Sourcetype）] ラベル（`wsa_accesslogs`、`wsa_trafmonlogs`、または `wsa_amplogs`）を指定します。

ステップ 7　[アプリコンテキスト（App Context）] メニューから [Advanced Web Security 5.0.0] を選択します。

ステップ 8　[定数値（Constant value）] をクリックし、[ホストフィールド値（Host field value）] フィールドに WSA のホスト名を入力します。

ステップ 9　宛先インデックスとして [デフォルト（Default）] を選択します。

ステップ 10　[レビュー（Review）] をクリックして指定した値を確認します。

ステップ 11　[送信（Submit）] をクリックします。

（注）　[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [ファイルとディレクトリ（Files & directories）] で、新しいデータ入力エントリを確認することができます。

WSA Syslog のデータ入力の設定

ステップ 1　Advanced Web Security Reporting アプリケーションで次の手順を実行します。

- [設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [TCP] を選択します。

ステップ 2　[新規（New）]をクリックします。

ステップ 3　[TCP] ボタンをクリックして [ポート（Port）] フィールドに `514` と入力します。残りのフィールドは空白のままにします。

ステップ 4　[次へ（Next）] をクリックします。

ステップ 5　[手動（Manual）] をクリックして、[ソースタイプ（Sourcetype）] フィールドに `wsa_syslog` と入力します。

ステップ 6　[アプリコンテキスト（App Context）] で [Advanced Web Security 5.0.0] を選択します。

ステップ 7　[ホスト（Host）] セクションの [方法（Method）] フィールドで [カスタム（Custom）] をクリックし、[ホストフィールド値（Host field value）] に WSA のホスト名を入力します。

ステップ 8　宛先インデックスとして [デフォルト（Default）] を選択します。

ステップ 9　[レビュー（Review）] をクリックして指定した値を確認します。

ステップ 10　[送信（Submit）] をクリックします。

ステップ 11　[設定（Settings）] > [データ入力（Data inputs）] > [TCP] に移動して新しい入力エントリを確認します。

（注）　複数アプライアンス設定を使用して、各アプライアンスの Advanced Web Security Reporting アプリケーションでこれらの手順を繰り返す必要があります。ただし、`inputs.conf` ファイルを編集して複数のアプライアンスを設定することもできます。

Web セキュリティ アプライアンスからのログ転送の確立

はじめる前に

- ログ ファイルへのパスを把握します（アクセスおよびトラフィック モニタ ログ ファイルのフォルダ構造の作成（1-11 ページ））。
- 転送の頻度を決定します。60 分単位以下には設定できません。
- Web セキュリティ アプライアンスの Web インターフェイスを開きます。

ステップ 1　Web セキュリティ アプライアンスの Web インターフェイスで、[システム管理（System Administration）] > [ログ設定（Log Subscription）] に移動します。

ステップ 2　[ログ設定を追加（Add Log Subscription）] をクリックするか、既存のサブスクリプションの名前をクリックして編集します。

ステップ 3　サブスクリプションを設定します（この例では、アクセス、AMP エンジン、およびトラフィック モニタ ログを扱います）。

設定	ログ タイプ	値
ログ タイプ（Log Type）	アクセス	accesslogs
	トラフィック モニタ	trafmonlogs
	AMPエンジン	amp_logs
ログ名（Log Name）	いずれか	ログ ディレクトリの名前。
（AsyncOS のリリースによって異なります） **ファイルサイズ別ロールオーバー（Rollover by File Size）** **最大ファイル サイズ（Maximum File Size）**	いずれか	500 MB 以下を推奨します。

設定	ログ タイプ	値
（このオプションを利用できるかどうかは AsyncOS のリリースによって異なります） 時刻によりロールオーバー（Rollover by Time）	いずれか	1 時間（1h）またはそれ以上頻繁なカスタム ロール オーバー間隔を推奨します。AMP ログの場合は 1 分（1m）を推奨します。
ログ スタイル（Log Style）	アクセス	**Squid**
	トラフィック モニタ	該当なし
	AMPエンジン	該当なし
ログ レベル（Log Level）	アクセス	該当なし
	トラフィック モニタ	該当なし
	AMPエンジン	[デバッグ（Debug）] を選択します。 **（注）** AMP レポートの場合は、[ログレベル（Log Level）] を [デバッグ（Debug）] に変更しないと、情報がほとんどレポートされないので注意してください。
（任意）カスタム フィールド	アクセスのみ	%XK（ウエブ レピュテーション脅威の理由を追加します）。
取得方法（Retrieval Method） **リモート サーバ上の FTP**	いずれか	[ホスト名（Hostname）]：Advanced Web Security Reporting ホストの IP アドレスまたはホスト名。 [ディレクトリ（Directory）]：Advanced Web Security Reporting のインスタンス ディレクトリの名前。 [ユーザ名/パスワード（Username/Password）]：アプリケーションにアクセスするための FTP ユーザ名とパスワード。 **（注）** Advanced Web Security Reporting と WSA 間の接続が失われると、接続が復旧するまで、その期間のログは使用できません。
取得方法（Retrieval Method） **Syslog 送信（Syslog Push）**	どちらか	[ホスト名（Hostname）]：Advanced Web Security Reporting ホストの IP アドレスまたはホスト名。 [プロトコル（Protocol）]：TCP。 [ファシリティ（Facility）]：[auth] を選択します。 **（注）** Advanced Web Security Reporting と WSA 間の接続が失われると、接続が復旧するまで、その期間のログは使用できません。

（注）　[ログ設定を追加（Add Log Subscription）] ページからオンライン ヘルプにアクセスすると、すべての設定に関する詳細情報が表示されます。

CWS ログのアップデートの設定

はじめる前に

- Advanced Web Security Reporting アプリケーションに `admin` としてログインします。

ステップ 1　Advanced Web Security Reporting アプリケーションで次の手順を実行します。

- [設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [Cisco CWS ログ（Cisco CWS Logs）] を選択します。

ステップ 2　[新規（New）]をクリックします。

ステップ 3　このデータ入力にわかりやすい**名前**を指定します。

ステップ 4　CWS から提供された **client_id**、**s3_key**、および **s3_secret** を指定します。**client_id** は CWS で使用されるバケット ID です。

ステップ 5　[詳細設定（More settings）] チェックボックスをオンにして、CWS ログを取得できる [間隔（Interval）] を秒単位で指定します。デフォルトは 3600 です。

ステップ 6　[次へ（Next）] をクリックします。

ステップ 7　成功したことを示す画面が表示されます。

（注）　[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [Cisco CWS ログ（Cisco CWS Logs）] で、新しいデータ入力エントリを確認することができます。

部門メンバーシップ クエリーのセットアップ（任意）

次の条件で部門メンバーシップ要件のセットアップ手順を実行します。

- Advanced Web Security Reporting アプリケーションの役割にバインドされた AD/LDAP グループを使用する。
- 組織の役割に基づくデータのレポートを実行する。

関連項目

- 職務別の部門レポートへのアクセスの制限（1-18 ページ）

部門メンバーシップ レポートのセットアップ

はじめる前に

- Linux ユーザ：次のコマンドを使用して、`ldapsearch` ツールをインストールします。

  ```
  sudo yum install openldap-clients
  ```

ステップ 1　Advanced Web Security Reporting アプリケーションで次の手順を実行します。

- [設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [AD/LDAPサーバの詳細（AD/LDAP Server Details）] を選択します。

ステップ 2　[LDAP ADサーバの詳細（LDAP AD Server Details）] をクリックします。

ステップ 3　[LDAP ADサーバの詳細（LDAP AD Server Details）] ページで、次のサーバ情報を入力して [保存（Save）] をクリックします。

- [AD/LDAPサーバ名（AD/LDAP Server Name）]
- [AD/LDAPユーザ名（AD/LDAP User Name）]
- [AD/LDAPユーザパスワード（AD/LDAP User Password）] と [確認（Confirm）]
- [AD/LDAPグループ名（AD/LDAP Group Name）]

ステップ 4　[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [スクリプト（scripts）] を選択して、メンバーシップ スクリプトを有効にします。

- Linux の場合、スクリプト名は `discovery.py` です。
- Windows の場合、スクリプト名は `discovery.vbs` です。

メンバーシップのスクリプトは、毎日実行するように初期設定されます。間隔は秒単位で設定されます。変更するには、[設定（Settings）] > [データ（Data）] > [データ入力（Data inputs）] > [スクリプト（scripts）] に移動して、`discovery` ファイル内の間隔を編集します。

<install_home>`/etc/apps/cisco_wsa_reporting/lookups/departments.csv` ファイルを調べることで、`departments.csv` ファイルにユーザ データを含むスクリプトが入力されていることを確認できます。

（注）　Windows では、この時点で `departments.csv` ファイルにデータが入力されていない場合、ディレクトリを *<install_home>*`\etc\apps\cisco_wsa_reporting\bin`（*<install_home>* は `C:\Program Files\Cisco\CiscoWSAReporting` です）に変更して、`cscript discovery.vbs` を実行します。

メンバーシップのスクリプトは、毎日実行するように初期設定されます。秒間隔にセットされ、配置要件に合わせて変更できます。

職務別の部門レポートへのアクセスの制限

はじめる前に

- ユーザのデータ閲覧が特定の部門またはグループからのデータに制限されている場合、レイヤ 4 トランスポート モニタ（L4TM）データを利用できるのは管理者のみに限られることを理解します。これは、L4TM データが部門または役割にリンクされていないためです。
- Advanced Web Security Reporting アプリケーションに `admin` としてログインします。

ステップ 1　Advanced Web Security Reporting アプリケーションで以下を実行します。

- [設定（Settings）] > [ユーザと認証（Users and authentication）] > [アクセスコントロール（Access Controls）] > [役割（Roles）] を選択します。

ステップ 2　[新規（New）] をクリックするか、既存の役割を編集します。

ステップ 3　役割の検索制限を定義します。

例：営業部門データの閲覧だけに役割を限定する場合は、[検索条件の制限（Restrict search terms）] フィールドに `department=sales` と入力します。

ステップ 4　[保存（Save）] をクリックします。

部門メンバーシップ レポートのトラブルシューティング

ヒント

- Linux ユーザ：ldapsearch ツールが Advanced Web Security Reporting ユーザのパスにあることを確認します。
- departments.csv ファイルがアプリケーションの参照フォルダに存在することを確認します。
- Windows ユーザ：`option explicit` をコメントアウトし、エラーの発生と原因についてより具体的な情報を示します。
- LDAP パスの構文が正しいことを確認します。
- バインド サービスのアカウント名が正しいことを確認します。
- 正しいバインド パスワードが入力されていることを確認します。
- ポート 389 経由でリモート マシンにテスト接続します。
- 正しい属性がメンバー名に設定されていることを確認します。
- 正しい属性がグループ メンバーシップに使用されたことを確認します。
- 正しい属性がグループ名に設定されていることを確認します。

スケジュール済 PDF レポートのセットアップ（任意）

Advanced Web Security Reporting アプリケーション ユーザは、ダッシュボード、ビュー、検索またはレポートからの PDF 出力の生成をスケジュールできます。次の設定手順に従って、スケジュール済 PDF レポートをセットアップします。

- 電子メール アラートの設定（1-19 ページ）
- PDF レポート生成のスケジュール（1-19 ページ）

電子メール アラートの設定

PDF レポートの生成後に電子メール アラートを送信するように Advanced Web Security Reporting アプリケーションを設定できます。

はじめる前に

- Advanced Web Security Reporting アプリケーションに admin としてログインします。

ステップ 1　Advanced Web Security Reporting アプリケーションで次の手順を実行します。

- [設定（Settings）] > [システム（System）] > [サーバ設定（Server Settings）] > [電子メール設定（Email Settings）] を選択します。

ステップ 2　電子メール アラートの送信に必要なメール サーバ設定を入力または更新します。

a. [メールホスト（Mail host）]：SMTP サーバのホスト名を入力します。

b. [Eメールセキュリティ（Email security）]（任意）：電子メール セキュリティ オプションを選択します。アプリケーションでは SMTP サーバとの通信に SSL または TLS を使用することができます。

c. [ユーザ名（Username）]：SMTP サーバ認証で使用する名前を入力します。

d. [パスワード（Password）]：指定したユーザ名に設定するパスワードです。

e. [パスワードの確認（Confirm password）]：パスワードを再入力します。

ステップ 3　必要な電子メールの形式情報を入力します。

a. [リンクのホスト名（Link hostname）]：出力結果の作成に使用するサーバのホスト名です。

b. [送信元（Send email as）]：電子メールの送信元として表示される送信者名です。

c. [電子メールのフッター（Email footer）]：送信電子メールのフッターに表示されるメモです。

ステップ 4　必要に応じて、[レポート用紙サイズ（Report Paper Size）] および [レポート用紙の向き（Report Paper Orientation）] を選択して、PDF レポート設定を変更します。

ステップ 5　[保存（Save）] をクリックします。

PDF レポート生成のスケジュール

カスタム ダッシュボードに対して PDF レポートの定期的な生成および電子メール送信をスケジュールできます。カスタム ダッシュボードの作成については、ダッシュボードとして保存（Save As Dashboard）（2-2 ページ）を参照してください。

はじめる前に

- Advanced Web Security Reporting アプリケーションに admin としてログインします。

ステップ 1　[カスタムダッシュボード（Custom Dashboards）] メニューから目的のダッシュボードを選択します。

ステップ 2　[編集（Edit）] > [PDF配信のスケジュール（Schedule PDF Delivery）] を選択します。

ステップ 3　[PDFスケジュールの編集（Edit PDF Schedule）] ダイアログボックスで、[PDFのスケジュール（Schedule PDF）] をオンにして、スケジュール、電子メール、およびページのオプションを指定します。

ステップ 4　（任意）[テスト メールの送信（Send Test Email）] をクリックして、生成された PDF が指定した電子メール アドレスに添付ファイルとして送信されることを確認します。

ステップ 5　（任意）[PDFのプレビュー（Preview PDF）] をクリックして生成された PDF をプレビューします。

レポート

- レポートの概要（2-1 ページ）
- レポートへのアクセス（2-1 ページ）
- ダッシュボードとして保存（Save As Dashboard）（2-2 ページ）
- データの書式（2-3 ページ）
- 時間範囲（2-3 ページ）
- エクスポート（2-4 ページ）
- 汎用データと特定データ（2-5 ページ）
- 定義済みレポート（2-6 ページ）
- 使用シナリオ（2-7 ページ）

レポートの概要

Advanced Web Security Reporting には、一連の定義済みレポートが含まれます。レポート機能は、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。

（注） Advanced Web Security Reporting を使用して生成したレポートには、Web セキュリティ アプライアンスのみで使用可能なデータよりも多くのデータが表示されます。

レポートへのアクセス

はじめる前に

Advanced Web Security Reporting 管理者は、概要レポートおよび Web トラッキング レポートに表示する 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、または名前を変更したいホストがある場合は、その詳細を 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 Advanced Web Security Reporting アプリケーションにログインします。

サマリー情報が表示されます。

ステップ 2　他のメニューからレポートを選択します。定義済みレポート（2-6 ページ）を参照してください。

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。

ヒント　短い時間範囲を指定して可能な限り正確に検索を構成することによって、パフォーマンスが向上します。

ダッシュボードとして保存（Save As Dashboard）

各レポート ページでは、時間範囲、ソース タイプ、およびホストを選択してカスタム レポート ページまたは「ダッシュボード」を作成できます。

ステップ 1　現在のレポート ページで、必要に応じてレポートの検索パラメータを変更し、[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することができます。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。

データの書式

Advanced Web Security Reporting を通じて取得できるデータの表記は、ネイティブなレポート作成機能で利用できるデータ表記とは異なる場合があります。

データ	書式例
大きな数値（8 桁以上）	`2E11` は 2×10^{11} を表します。
時刻	`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 時すぎ	インデックス生成開始後 1 日
Week	土曜日の午前 0 時すぎ（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 時すぎ	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 時すぎ	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 時すぎ（日曜日の早朝）	インデックス生成開始後 1 週間

エクスポート

.CSV ファイルにエクスポート

このオプションはトラッキングタイプのレポートに適しています。

ステップ 1　レポートを生成します。

ステップ 2　[エクスポート（Export）] を選択します。

PDF ファイルにエクスポート

はじめる前に

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

ステップ 1　レポートを生成します。

ステップ 2　[PDF として保存（Save as PDF）] を選択します。

関連項目

- スケジュール済 PDF レポートのセットアップ（任意）（1-18 ページ）

汎用データと特定データ

事前定義された汎用レポートには、事前定義された特定レポートへのハイパーリンクがあります。

詳細を表示

ステップ 1　最適な定義済み汎用レポートを選択します。

たとえば、ユーザに関する特定の情報を表示する場合は、事前に定義されたユーザ レポートから開始します。

ステップ 2　詳細を知りたいサブジェクトのハイパーリンクをクリックします。

たとえば個々のユーザのユーザ ID をクリックします。

関連項目

- エクスポート (2-4 ページ)

検索

ほとんどのレポート ページで簡易検索および詳細検索オプションを利用できます。

検索のヒント

- 検索対象をできるだけ特定し、時間範囲を狭めてください。
- Advanced Web Security Reporting では、一連のファイルを使用してメニューを表示します。メニューに問題が発生した場合は、次を含む必要なファイルがアプリケーションの参照フォルダ内にあることを確認してください。
  - `malware_categories.csv`
  - `transaction_types.csv`
  - `url_categories.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、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。

検索のトラブルシューティング

`departments.csv` は、役割ベースのセキュリティ機能の一部として使用されるファイルです。このファイルは、手動でも、ロールディスカバリ スクリプト (アプリケーションの `bin` フォルダで使用可能) をスクリプト入力として設定する方法でも編集することができます。Linux と Windows、両方のスクリプトがあります。

- ファイルがアプリケーションの参照フォルダにあることを確認します。
- Linux バージョンを使用している場合は、CLI コマンド `ldapsearch` がインストールされ、アプリケーション ユーザのパスにあることを確認します。
- Windows バージョンを使用している場合は、エラーの原因と発生場所についての特定情報を明示するため、「option explicit」がコメントアウトされる可能性があります。
- LDAP パスの構文が正しいことを確認します。
- バインド サービスのアカウント名が正しいことを確認します。
- 正しいバインド パスワードが入力されていることを確認します。
- ポート 389 経由でリモート マシンにテスト接続します。
- 正しい属性がメンバー名に設定されていることを確認します。
- 正しい属性がグループ メンバーシップに使用されたことを確認します。
- 正しい属性がグループ名に設定されていることを確認します。

定義済みレポート

- 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
  - URL Category
- アプリケーション分析
  - 概要
  - Application

    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（Application Type）

    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（Client Malware Risk）

    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（Web Reputation Filters）

  概要

  ロケーション ベース

- 高度なマルウェア防御（Advanced Malware Protection）

  概要

  AMP ドリルダウン

  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 WSA 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（AMP Verdict Updates）

- Web トラッキング（Web Tracking）
  - プロキシ サービス
  - SOCKS
  - SOCKS ドリルダウン

関連項目

- レポートへのアクセス（2-1 ページ）
- 検索（2-5 ページ）

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）]

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することができます。

Web 使用トレンドの閲覧

ステップ 1　Cisco Advanced Web Security Reporting のドロップダウン 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）　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、適当なユーザ 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 のドロップダウン 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　ユーザ ID またはクライアント IP アドレスを [検索（Search）] します。

ステップ 3　トランザクションごとに表示される情報を変更するには、トランザクション リスト上部の [選択フィールド（Pick fields）] をクリックします。

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。

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 のドロップダウン 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 のドロップダウン 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。