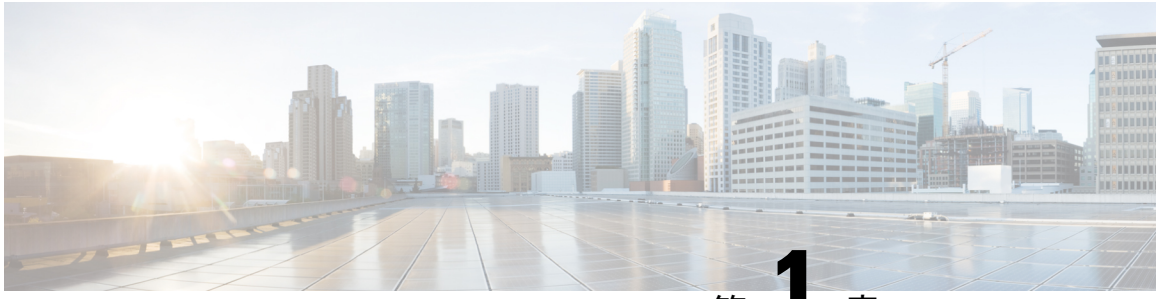
Cisco Advanced Web Security Reporting 7.5.1 のインストール、セットアップ、ユーザ ガイド

初版：2021 年 7 月 5 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。



第 1 章

インストールおよびセットアップ

この章は、次のセクションで構成されています。

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フィルタとダッシュボードは、複数の Web セキュリティアプライアンス、および Cisco Umbrella 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。Cisco Advanced Web Security Reporting アプリケーションには、データ収集と表示アプリケーション、および Web セキュリティアプライアンス（WSA）と Umbrella ホスト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。

Cisco Advanced Web Security Reporting アプリケーションはログデータを受信すると、データモジュールに保存します。これらのデータは、定義した検索または「フィルタ」を使用して表示できます。

最新情報

リリース 7.5.1 の新機能

機能	説明
Splunk エンジンのアップグレード	Splunk エンジンがバージョン 7.3.5 にアップグレードされています。
Syslog パーサーの更新	Cisco Web セキュリティアプライアンス 12.0.1-334 の Syslog パーサーの更新。

リリース 7.5 の新機能

機能	説明
Splunk エンジンのアップグレード	Splunk エンジンがバージョン 7.3.3 にアップグレードされています。
[ユーザのドリルダウン（Use Drilldown）] ページには、AD グループの詳細のレポートが表示されます。	**[ユーザ分析（User Analysis）]** > **[ユーザのドリルダウン（Use Drilldown）]**ページに、AD グループ名で検索するための新しいフィルタが追加されています。AD グループの詳細が検索結果に表示されます。[AD グループ（AD Group）]、[ユーザID（User ID）]、[宛先ドメイン（Destination Domain）]、[使用済み帯域幅（Bandwidth used）]、および [滞留時間（Time Spent）] の詳細が表示されます。

リリース 7.0 の新機能

機能	説明
AWSR プロキシサービスの検索結果に WBRS スコアのないイベントが表示される	WBRS スコアなしの新しいフィルタ（[WBRSの表示: スコアなし（Show WBRS: No Score）]）が**[Webトラッキング（Web Tracking）] > [プロキシサービス（Proxy Services）]**ダッシュボードに追加されました。このフィルタを使用すると、WBRS スコアのない AWSR プロキシサービスの検索結果を表示できます。
部門メンバーシップレポートに AD グループレポートの詳細な結果が表示される	AD グループレポートの次の結果を**[ユーザ分析（User Analysis）] > [概要（Overview）]**に表示できるようになりました。 • [ブロックされたトランザクション数の上位グループ（Top Groups by Transactions Blocked）] • [ブロックされたトランザクションのサマリー（Transactions Blocked Summary）] • [帯域幅使用量の上位グループ（Top Groups by Bandwidth Used）] • [使用帯域幅のサマリー（Bandwidth Used Summary）] • [ユーザ別の上位グループ（Top Groups by User）] • [使用帯域幅のサマリー（Bandwidth Used Summary）] • [ADグループサマリー（AD Group Summary）] • [ユーザごとのADグループの詳細（AD Group per User Details）]

リリース 6.6 の最新情報

機能	説明
カスタム ダッシュボードでの検索	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。
任意のページからのエクスポート	データ（グラフィカルデータ以外）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、任意のダッシュボードからエクスポートできます。ダウンロードするためにこのオプション  を表示するには、ダッシュボードデータの表示ペインの上にマウスカーソルを置く必要があります。

リリース 6.4 の最新情報

機能	説明
ダッシュボードの更新の Web トラッキング	• 新規フィルタ：**ユーザ、クライアント IP、WBRS** の最小および最大スコア範囲、および **SNI** が、**[Web トラッキング（Web Tracking）] > [プロキシ サービス（Proxy Services）]**ダッシュボードに追加されます。 • プロキシサービス 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。

リリース 6.3 の最新情報

機能	説明
Splunk エンジンのアップグレード	Splunk エンジンがバージョン 6.6.6 にアップグレードされています。

リリース 6.2 の最新情報

機能	説明
Cisco Umbrella レポートのサポート	Cisco Advanced Web Security Reporting アプリケーションから Umbrella によって提供されるログを含むプライベート AWS S3 バケットをポイントできます。統合 Web セキュリティ レポート ダッシュボードで、レポートを表示できます。
Splunk エンジンのアップグレード	Splunk エンジンが最新バージョンにアップグレードされています。

（注） ロールベースのレポート機能は、高速化されないデータ モデルに対してのみ機能します。高速化を無効にするとレポートの読み込み時間が長くなるため、ロールベースのレポートを使用しない場合は、データ モデルの高速化を有効にしてください。「設定のベスト プラクティス」および「職務別の部門レポートへのアクセスの制限」を参照してください。

リリース 6.1 の最新情報

機能	説明
CEF エクストラクタ	共通イベント フォーマット（CEF）エクストラクタ サービスによって、1 つまたは複数の WSA から受信したアクセス ログを CEF 形式の出力データに変換できます。
Web セキュリティ アプライアンス AsyncOS 10.1 のサポート	Web セキュリティ アプライアンスのリリースの AsyncOS 10.1 に含まれている、アーカイブ スキャン アクセス ログの変更をサポートします。

リリース 6.0 の最新情報

機能	説明
カスタム フィルタ	「フィルタリング」と呼ばれるプロセスで、利用可能なアクセス ログ、SOCKS ログ、AMP ログのデータのカスタム検索を定義します。
Web セキュリティ アプライアンス AsyncOS 10.0 の変更	AMP の機能拡張と参照元のヘッダー関連のサポート。

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	サポート対象外
サーバ	単一サーバ展開	複数サーバ展開
送信方法	FTP（ファイルおよびディレクトリ） TCP（Syslog）	
PDF	統合 PDF 生成 スケジュール済 PDF レポート	
カスタム ダッシュボード	定義済みのレポートの場合は、それぞれに [ダッシュボードとして保存（Save As Dashboard）] を使用し、時間範囲、ソースタイプ、およびホスト（制限あり）を選択してカスタムダッシュボードを作成します。カスタムフィルタの場合は、それぞれに[ダッシュボードとして保存（Save As Dashboard）] を使用し、アクセスログ、SOCKS ログ、または AMP ログのフィルタフィールドを選択してカスタムダッシュボードを作成します。	

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『*Cisco Advanced Web Security Reporting Release Notes*』で詳しく説明されています。

AWSR で使用される次のポートは開いている必要があります。これらのポートがエンタープライズ ファイアウォールでブロックされていないことを確認します。

- 8887/TCP：Python ベースのアプリケーションサーバがリッスンするポート番号。このポートは、アプリケーション サーバ ポートと呼ばれます。
- 8888/TCP：Cisco Advanced Web Security Reporting の GUI にアクセスするためのポート。このポートは、Web ポートとも呼ばれます。

- 8889/TCP：Cisco Advanced Web Security Reporting がデーモンプロセスとの通信に使用するポート。このポートは管理ポートと呼ばれます。
- 8886/TCP - mongodb：デーモンが KV ストアサーバへの接続に使用するポート。
- 22/TCP：SSH/SCP/WGET
- 514/TCP：Syslog
- 21/TCP：FTP

（注） nmap/netstat/iptables を有効にして、システム構成と Windows の RDP を制御および検証することもできます。

セットアップの概要

- Cisco Advanced Web Security Reporting を初めてインストールします。
  - Cisco Advanced Web security Reporting 7.5.1 のインストール
  - ライセンスおよび移行
  - 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
  - 履歴データのインポートおよびインデックス作成
  - 継続的なデータ転送の設定（Web セキュリティアプライアンスのセットアップを含む）
  - Umbrella のログの更新
- Cisco Advanced Web Security Reporting 7.5.1 へのアップグレード

Cisco Advanced Web security Reporting 7.5.1 のインストール

（注） インストールまたはアップグレードする前に、ブラウザの Cookie とキャッシュをクリアしてください。

（注） AWSR 7.5.1 の場合、ログイン情報はインストール中に作成されます。インストール中に作成されたログイン情報には、「管理者」のロール、および機能/特権があります。

Cisco Advanced Web Security Reporting アプリケーション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
- Windows の場合

Linux の場合

次のタスクを順序どおりに実行してください。

ステップ 1 必要な Cisco Advanced Web Security Reporting バージョンのインストーラをダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

ステップ 2 以下のコマンドを使用して、/opt にあるインストーラソフトウェアを抽出します。

```
tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-1-0-114.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 /opt/cisco_wsa_reporting./setup.sh
```

- このコマンドの結果が次の場合には、以下の操作を行います。

```
./setup.sh: Permission denied
```

1. 次のコマンドを使用して、スクリプト `setup.sh` の権限レベルを変更します。

   ```
   chmod 777 setup.sh
   ```

2. スクリプトを再実行します。

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 管理者のユーザ名とパスワードを作成し、パスワードを確認します。

```
Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/home/rtestuser/AWSR7.5/cisco_wsa_reporting/etc/openlda
```

ステップ 5 前の手順で作成したユーザ名とパスワードを入力してログインします。

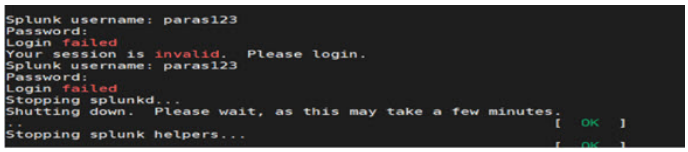
```
The Splunk web interface is at http://wsa061-client05.cs1:8888

Splunk username: admin
Password:
The licenses object has been added
```

ステップ 6 Cisco Advanced Web Security Reporting を起動し、インストール中に作成されたクレデンシャルを使用してログインします。

1. ブラウザウィンドウで `https://<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。

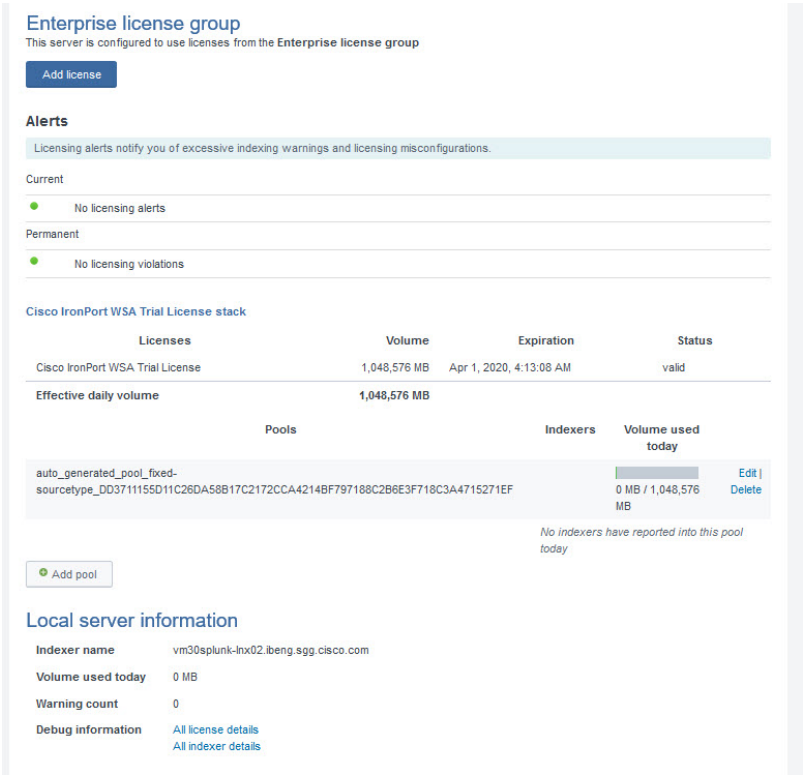
（注） Splunk へのログイン時にユーザ名とパスワードを誤って 2 回指定すると、**setup.sh** コマンドの実行中にライセンスは追加されません。



ライセンスファイルを手動で追加するには、次の手順に従います。

<INSTALL_HOME> ディレクトリ、たとえば /opt/cisco_wsa_reporting から次を実行します。

- ファイル「**Splunk-eval-120d-500GB.License**」の内容をコピーし、管理者として AWSR GUI にログインします。
- **[設定（Settings）] > [システム（SYSTEM）] > [ライセンス（Licensing）] > [ライセンスの追加（Add license）]**に移動して、**[ライセンスXMLディレクトリをコピーして直接貼り付ける（Copy & paste the license XML directly）]** をクリックし、**「Splunk-eval-120d-500GB.License」の内容の貼り付け > [インストール（Install）]**を実行して、再起動します。



- インストール後のタスク

- ライセンスおよび移行

Windows の場合

始める前に

Windows では、Advanced Web Security Reporting のインストールバージョンを 1 つだけ使用できます。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 必要な Cisco Advanced Web Security Reporting バージョンのインストーラをダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

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。

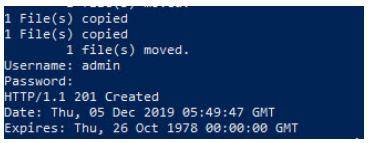
（注） デジタル署名に関連するファイルは、パッケージが抽出されたディレクトリにあります。たとえば、次のようになります。

```
C:\Users\<UserDirectory>\Downloads\CiscoAdvancedWebSecurityReporting-Windows_7-5-1-0-114.tgz
```

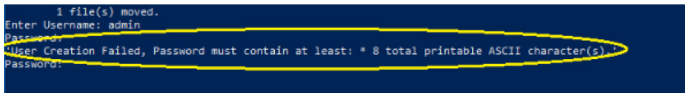
ステップ 3 コマンドライン シェル（PowerShell）を管理者として起動し、ディレクトリをインストーラの解凍先ディレクトリに変更します。

ステップ 4 インストールコマンド `./install.bat` を実行します。

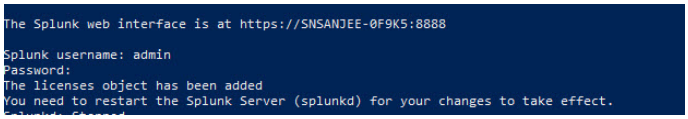
ステップ 5 管理者のユーザ名とパスワードを作成し、パスワードを確認します。



（注） パスワードの長さが無効な場合、「パスワードには少なくとも8文字の出力可能なASCII文字が含まれている必要があります（Password must contain at least 8 total printable ASCII character）」というエラーメッセージが表示される場合があります。ユーザを正常に作成するには、パスワードに少なくとも 8 文字の ASCII 文字を含めてください。



ステップ 6 前の手順で作成したユーザ名とパスワードを入力してログインします。



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 7 Cisco Advanced Web Security Reporting サーバを再起動します。

ステップ 8 次の手順で Cisco Advanced Web Security Reporting アプリケーションを起動し、ログインします。

1. ブラウザウィンドウで `https://<hostname>:8888` にアクセスします。
2. インストール中に作成したユーザ名とパスワードでログインします。

（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。

次のタスク

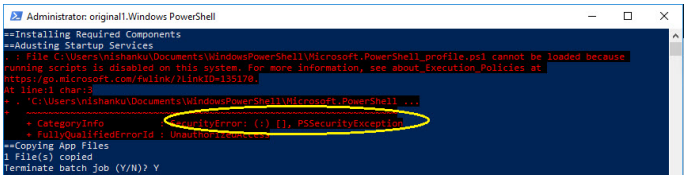
- インストール後のタスク
- ライセンスおよび移行

インストール中のエラーの処理

インストール中に次のエラーが表示される場合があります。このセクションでは、インストール中に発生する可能性のある一般的なエラーと、これらのエラーを解決するために実行する必要のある手順について説明します。

セキュリティエラー: PSSecurityException

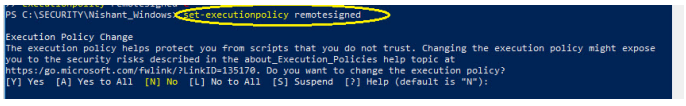
新しいアプライアンスに Cisco Advanced Web Security Reporting をインストールすると、PSSecurityException エラーが発生する場合があります。



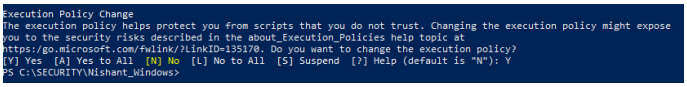
この問題を解決するには、次の手順を実行します。

ステップ 1 プロンプトで次のコマンドを実行します。

```
set-executionpolicy remotesigned
```

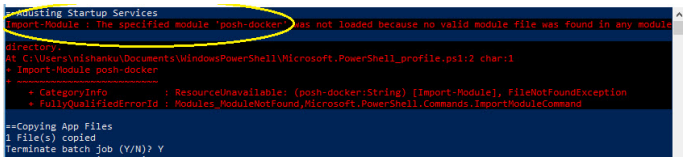


ステップ 2 表示されるプロンプトに対して [Y]（はい）を選択します。



ステップ 3 インストールコマンド `/install.bat` を再実行します。

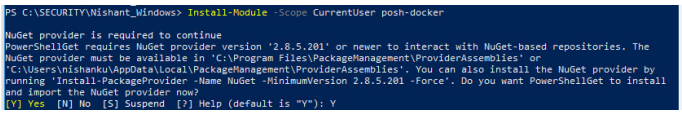
モジュールのインポートエラー：posh-docker



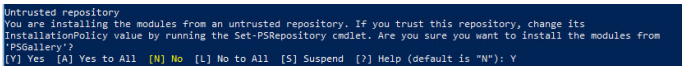
この問題を解決するには、次の手順を実行します。

ステップ 1 プロンプトで次のコマンドを実行します。

```
Install-Module -Scope CurrentUser posh-docker
```

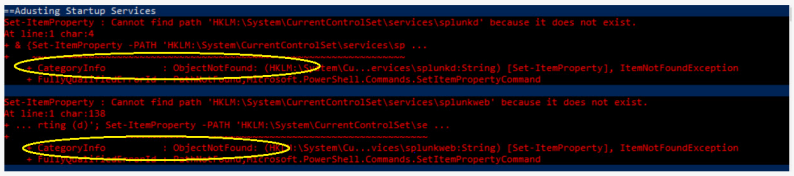


ステップ 2 表示されるプロンプトに対して **[Y]**（はい）を選択します。



ステップ 3 インストールコマンド `/install.bat` を再実行します。

ObjectNotFound：パスが見つからない



この問題を解決するには、次の手順を実行します。

ステップ 1 プロンプトで次のコマンドを実行します。

```
New-Item -Path HKLM:\System\CurrentControlSet\services\splunkd -Force | Out-Null

New-Item -Path HKLM:\System\CurrentControlSet\services\splunkweb -Force | Out-Null
```

ステップ 2 インストールコマンド `/install.bat` を再実行します。

Cisco Advanced Web Security Reporting 7.5.1 へのアップグレード

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 インストールされている Cisco Advanced Web Security Reporting の以前のバージョンのディレクトリに移動します。

ステップ 2 `chmod 777 ./shutdown` コマンドを使用して前のセッションをシャットダウンします。

ステップ 3 `https://<hostname>:8888` に移動して、AWSR が引き続きブラウザで実行されているかどうかを確認します。

ステップ 4 `/opt /` ディレクトリにあるバージョンの Cisco Advanced Web Security Reporting の新しいインストーラを次の場所からダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

ステップ 5 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、 Cisco 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、ファイルを `/opt/` ディレクトリに置きます。

ステップ 6 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 7 次のコマンドを使用してインストーラを解凍します。適切なバージョン番号を使用します。

```
tar -zxvf CiscoAdvancedWebSecurityReporting-Linux_7-5-1-0-114.tgz
cisco_wsa_reporting/SeamlessUpgrade.sh; cp -f cisco_wsa_reporting/SeamlessUpgrade.sh./
```

ステップ 8 アップグレード スクリプトを実行します。適切なバージョン番号を使用します。

```
./SeamlessUpgrade.shCiscoAdvancedWebSecurityReporting-Linux_7-5-1-0-114.tgz
```

- このコマンドの結果が次の場合には、以下の操作を行います。

  ```
  ./SeamlessUpgrade.sh: Permission denied
  ```

  1. 次のコマンドを実行して、スクリプト SeamlessUpgrade.sh の権限レベルを変更します。

     ```
     chmod 777 cisco_wsa_reporting/SeamlessUpgrade.sh
     ```

  2. スクリプトを再実行します。

ステップ 9 ブラウザで `https://<wsa_reporting_server_host_name>:8888` を開き、ユーザ名とパスワードを使用してログインします。

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 必要な Cisco Advanced Web Security Reporting バージョンのインストーラをダウンロードします。

https://software.cisco.com/download/home/286290962/type/283998384/release/7.5.1

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` を使用して、Cisco Advanced Web Security Reporting をアップグレードします。

ステップ 5 ブラウザで `https://<wsa_reporting_server_host_name>:8888` を開き、ユーザ名とパスワードを使用してログインします。

ユーザ（Users）

Cisco Advanced Web Security Reporting アプリケーションは、2 人の管理者ユーザを提供します。さらにユーザを作成し、既存のロールを割り当てるか、新しいロールを作成することができます。「職務別の部門レポートへのアクセスの制限」を参照してください。

管理ユーザ（Administrative Users）

Cisco Advanced Web Security Reporting アプリケーションには、次の 2 つの管理ユーザが用意されています。

- 「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）]**）。

新規ユーザーの作成

管理ユーザとは別に、新しいユーザを作成することもできます。

ステップ 1 **[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）]**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 [ユーザ名（Username）] に名前を入力し、ロールを割り当てます。「職務別の部門レポートへのアクセスの制限」を参照してください。

ステップ 4 パスワードを設定します。

ステップ 5 [保存（Save）] をクリックします。

設定のベスト プラクティス

- Web セキュリティアプライアンスおよび Umbrella ホスト間で一貫性のある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、Cisco 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）。
- ロールベースのレポートを使用しない場合は、データ モデルの高速化を有効にします。
  1. **[設定（Settings）] > [データ（Data）] > [データの高速化（Data Acceleration）]** を選択します。
  2. [編集（Edit）] をクリックします。
  3. [高速化の編集（Edit Acceleration）] を選択します。
  4. [高速化（Accelerate）] チェックボックスをオンにし、[サマリの範囲（Summary Range）] で [3ヵ月（3 months）] を選択します。
  5. [保存（Save）] をクリックします。

Cisco 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

Cisco Advanced Web Security Reporting アプリケーションを停止するには、次の手順に従います。

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
```

Cisco Advanced Web Security Reporting アプリケーションを起動するには、次の手順に従います。

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

Cisco Advanced Web Security Reporting アプリケーションを停止するには、次の手順に従います。

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
```

Cisco Advanced Web Security Reporting アプリケーションを起動するには、次の手順に従います。

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。

インストール後のタスク

AWSR で HTTPS を有効にする

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションで、**[設定（Settings）]** > **[システム（System）]** > **[サーバ設定（Server Settings）]**を選択します。

ステップ 2 [全般設定（General Settings）] をクリックします。

ステップ 3 [Cisco Advanced Web Security Reportingアプリケーションで SSL（HTTPS）を有効にする（Enable SSL (HTTPS) in Cisco Advanced Web Security Reporting application）] で [はい（Yes）] をクリックします。

デフォルトでは、暗号化が有効になっている場合、AWSR の導入ではデフォルトの証明書を指します。証明書に署名については、「証明書の生成と署名」を参照してください。

ステップ 4 root ユーザとして CLI にログインし、$AWSR_Home/etc/system/local/ に移動します。

ステップ 5 **web.conf** ファイルを編集し、エントリ enableSplunkWebSSL = 1 がそのファイルに存在することを確認します。

ステップ 6 $AWSR_HOME ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 7 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

ステップ 8 ここで、Cisco Advanced Web Security Reporting アプリケーションへのアクセスに使用する URL の前に `https://` を追加する必要があります。

クライアントが開始した再ネゴシエーションの無効化

ステップ 1 `root` ユーザとして CLI にログインし、`$AWSR_Home/etc/system/local/` に移動します。

ステップ 2 **web.conf** ファイルを開き、最後に `allowSslRenegotiation = false` というテキストを追加します。

ステップ 3 `$AWSR_HOME` ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 4 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

証明書の生成と署名

詳細については、「証明書の生成と署名」を参照してください。

Strict Transport Security ヘッダーの送信

ステップ 1 `root` ユーザとして CLI にログインし、`$AWSR_Home/etc/system/local/` に移動します。

ステップ 2 **server.conf** ファイルを開き、次のテキストを追加します。

```
[httpServer]
replyHeader.X-XSS-Protection= 1; mode=block
replyHeader.Content-Security-Policy = script-src 'self'; object-src 'self'
[sslConfig]
sendStrictTransportSecurityHeader = true
```

ステップ 3 **web.conf** ファイルを開き、次のテキストを追加します。

```
sendStrictTransportSecurityHeader = true
replyHeader.X-XSS-Protection= 1; mode=block
```

ステップ 4 `$AWSR_HOME` ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 5 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

パスワードの長さの制限

このトピックでは、パスワードを設定または変更するときに、許可する最小パスワードの長を文字数で設定する方法について説明します。

ステップ 1 root ユーザとして CLI にログインし、$AWSR_Home/etc/system/local/ に移動します。

ステップ 2 **authentication.conf** ファイルを開き、最後に次のテキストを追加します。

```
[splunk_auth]
minPasswordLength = <positive integer>
```

ここで、positive integer には 12、127、256 などの正の数を指定できます。

（注） **authentication.conf** ファイルが $AWSR_HOME/etc/system/local パスに存在しない場合、$AWSR_HOME/etc/system/default パスから $AWSR_HOME/etc/system/local パスにファイルをコピーして、上記手順 2 で指定した変更を行います。

ステップ 3 $AWSR_HOME ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 4 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

圧縮アルゴリズムの無効化

次の手順では、SSL/TLS 圧縮アルゴリズムの情報漏えいに関する脆弱性に対処します。

ステップ 1 root ユーザとして CLI にログインし、$AWSR_Home/etc/system/local/ に移動します。

ステップ 2 **server.conf** ファイルを開き、**[sslConfig]** セクションの下に allowSslCompression = false を追加します。

ステップ 3 $AWSR_HOME ディレクトリに移動し、**shutdown.sh** コマンドを実行して AWSR プロセスを停止します。

ステップ 4 **startup.sh** コマンドを実行して、AWSR プロセスを開始します。

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、Web セキュリティ アプライアンス 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 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 Web セキュリティアプライアンス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（Web セキュリティ アプライアンス）から v4.0（Web セキュリティ アプライアンスのみ）レポートへの移行
- v3.0（Web セキュリティ アプライアンス専用）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（Webセキュリティアプライアンス）からv4.0（Webセキュリティアプライアンスのみ）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 Web セキュリティ アプライアンス 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（Web セキュリティ アプライアンス専用）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 Web セキュリティ アプライアンス 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できます。

Web セキュリティアプライアンス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（`ciscoumbrella` 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 Web セキュリティアプライアンス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 Cisco 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、Web セキュリティアプライアンス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、適切な Umbrella パッケージを購入していることを確認します。

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、および wsa_amplogs **のみ**であることを確認します。

シスコの Cisco 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、Cisco Advanced Web Security Reporting の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 Cisco 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 Cisco 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。
    1. **[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。
    2. [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。
    3. 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。次の手順に従って、Cisco Advanced Web Security Reportingライセンスをインストールします。

ステップ 1 Cisco 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 [インストール（Install）] 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/	$Input_base=path of root FTP folder host_name=Web Security appliance
アクセス	/$Input_base/wsa_hostname/accesslogs/	$Input_base=deployment host_name=Web Security appliance
AMP	/$Input_base/wsa_hostname/amplogs/	$Input_base=deployment host_name=Web Security appliance

履歴データのインポートおよびインデックス作成

始める前に

- 「Cisco Advanced Web Security Reporting 7.5.1 へのアップグレード」にリストされている構成タスクを実行します。
- 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」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 Cisco 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。

1. **[設定（Settings）] > [データ（Data）] > [インデックス（Indexes）]**を選択します。
2. サマリー行までスクロールします。
3. [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（次のセクション「（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）。

次のタスク

- Web セキュリティ アプライアンス ログのデータ入力の設定

（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

始める前に

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、以下のファイルを開きます。

```
<install_home>/cisco_wsa_reporting/etc/apps/cisco_wsa_reporting/local/inputs.conf
```

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、Web セキュリティ アプライアンス 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 Cisco 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
- 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」）。
- Cisco Advanced Web Security Reporting アプリケーションに `admin` としてログインします。

Web セキュリティ アプライアンス 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 Cisco 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 Web セキュリティ アプライアンス ログを送信する FTP ディレクトリへのフル パスを入力します。

このパスと Web セキュリティ アプライアンスの [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 [新規（New）] をクリックします。

ステップ 7 [ソースタイプ（Source Type）] にタイプを入力し、[ソースタイプのカテゴリ（Source Type Category）] でカテゴリを選択して、[ソースタイプの説明（Source Type Description）] に説明を入力します。

`wsa_accesslogs`：レイヤ 4 トラフィックモニタおよび高度なマルウェア防御レポートを除くすべてのレポートに使用します。

`wsa_trafmonlogs`：レイヤ 4 トラフィックモニタレポートで使用します。

`wsa_amplogs`：高度なマルウェア防御レポートで使用します。

ステップ 8 [アプリコンテキスト（App context）] ドロップダウン リストから [Advanced Web Security Reporting 6.2.0] を選択します。

ステップ 9 [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 Web セキュリティアプライアンスのホスト名を入力します。

ステップ 10 宛先**インデックス**として [メイン（Main）] を選択します。

ステップ 11 [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 12 [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できます。

Web セキュリティ アプライアンス Syslog のデータ入力の設定

ステップ 1 Cisco 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 [新規（New）] をクリックします。

ステップ 6 [ソースタイプ（Source Type）] フィールドで `wsa_syslog` を入力します。

ステップ 7 [アプリコンテキスト（App Context）] で [Advanced Web Security 6.2.0] を選択します。

ステップ 8 [ホスト（Host）] セクションの [方法（Method）] 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 Web セキュリティ アプライアンス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 [メイン（Main）] 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。

ステップ 12 **[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 Cisco 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。2 つの異なるデータ入力に同じポートを使用することはできません。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

始める前に

- 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」）。
- 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。
- Cisco 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 Cisco 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（Access）	accesslogs
	トラフィックモニタ（Traffic Monitor）	trafmonlogs
	AMPエンジン（AMP Engine）	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。
（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（Access）	**Squid**
	トラフィックモニタ（Traffic Monitor）	該当なし
	AMPエンジン（AMP Engine）	該当なし

設定	ログ タイプ	値
ログ レベル（Log Level）	アクセス（Access）	該当なし
	トラフィックモニタ（Traffic Monitor）	該当なし
	AMPエンジン（AMP Engine）	[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（Access）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（FTP on Remote Server）**	いずれか	[ホスト名（Hostname）] : Cisco 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）] : Cisco Advanced Web Security Reporting 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） Cisco Advanced Web Security Reporting と Web セキュリティアプライアンス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。

設定	ログ タイプ	値
取得方法（Retrieval Method） **Syslog 送信（Syslog Push）**	どちらか	[ホスト名（Hostname）]：Cisco 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） Cisco Advanced Web Security Reporting と Web セキュリティアプライアンス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。

Umbrella のログの更新

始める前に

- Cisco Advanced Web Security Reporting アプリケーションに `admin` としてログインします。
- プライベート AWS S3 バケットが必要です。プライベート S3 バケットを設定するには、https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-your-own-s3-bucket を参照してください。

ステップ 1 Cisco 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/Umbrellaログ（Cisco CWS/Umbrella 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 このデータ入力の**名前**を入力します。

ステップ 4 Umbrella から提供された **client_id**、**s3_key**、および **s3_secret** を入力します。**client_id** は、Umbrella のAWS バケット名です。

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、Umbrella 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 [sourcetypeの設定（Set sourcetype）] ドロップダウン リストで [手動（Manual）] を選択します。

ステップ 7 [ソースタイプ（Source Type）] を入力します。`ciscoumbrella`（Umbrella レポートの場合）を入力します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 成功したことを示す画面が表示されます。

（注） シスコが管理する AWS S3 バケットではサポートされていません。

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。

- Cisco Advanced Web Security Reporting アプリケーションでロールにバンドルされた AD/LDAP グループを使用します。
- 組織の役割に基づくデータのレポートを実行する。

関連情報：

- 職務別の部門レポートへのアクセスの制限

部門メンバーシップ レポートのセットアップ

始める前に

- 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 **[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）]（グループ DN を指定）

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、メンバーシップの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。

`departments.csv` ファイルはロールベースのレポート機能で使用されます。このファイルには、次の記述が含まれています。

- 最初の列に user（cs ユーザ名：認証されたユーザ名）。
- 後続の列に displayname、groupname（スクリプトを使用して Active Directory または LDAPサーバから取得）。アクセス ログ（user_id フィールド）に存在するユーザに対して、対応する表示名とグループが displayname と department フィールドに表示されます。

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できます。Linux と Windows 用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。

（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。

職務別の部門レポートへのアクセスの制限

始める前に

- 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。
- Cisco 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 **[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。

ステップ 5 **[設定（Settings）] > [データ（Data）] > [データの高速化（Data Acceleration）]** を選択します。

ステップ 6 [編集（Edit）] をクリックします。

ステップ 7 [高速化の編集（Edit Acceleration）] を選択します。

ステップ 8 [高速化（Accelerate）] チェック ボックスをオフにして、[保存（Save）] をクリックします。

新しい役割の検索の制限を確認するには、新しいユーザを作成して検索を実行します。「新規ユーザーの作成」を参照してください。手順 4 で作成した役割に割り当てられたユーザの検索結果には、役割で指定された検索文字列に一致するイベントのみが表示されます。

（注） ロールベースのレポートを使用しない場合は、データ モデルの高速化を有効にします。これにより、レポートのパフォーマンスが強化されます。「設定のベストプラクティス」を参照してください。

関連情報：

- ユーザ（Users）

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 Cisco 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）

Cisco 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
- PDF レポート生成のスケジュール

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 Cisco Advanced Web Security Reporting アプリケーションを設定できます。

始める前に

- Cisco 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 Cisco 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。

1. [メールホスト（Mail host）]：SMTP サーバのホスト名を入力します。
2. [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 を使用できます。
3. [ユーザ名（Username）]：SMTP サーバ認証で使用する名前を入力します。
4. [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。
5. [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。

1. [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。
2. [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。
3. [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」を参照してください。

始める前に

- Cisco 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。

ユーザの作成または変更

新規ユーザを作成します。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションに admin ユーザとしてログインします。

ステップ 2 **[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）] > [新規追加（Add New）]**を選択します。

ステップ 3 次の詳細を入力します。

1. [ユーザ名（Username）] : 一意のユーザ名を入力します（必須）。
2. [フルネーム（Full Name）] : 姓名を入力します。
3. [電子メールアドレス（Email Address）] : 電子メールアドレスを入力します。
4. [タイムゾーン（Time Zone）] : タイム ゾーンを選択します。
5. [デフォルトアプリ（Default app）] : **cisco_wsa_reporting**（Advanced Web Security Reporting 7.0）
6. [ロールに割り当てるまたはこのユーザのロールを作成する（Assign to roles or Create a role for this use）] : ユーザロールを新規作成するには、「ロールの作成または変更」を参照してください（必須）。
7. [パスワード（Password）]（必須） : パスワードを入力します。
8. [パスワードの確認（Confirm Password）]（必須） : パスワードを再入力します。

ステップ 4 [保存（Save）] をクリックします。

Delete Users

既存のユーザを削除するには、次の手順を実行します。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションに admin ユーザとしてログインします。

ステップ 2 **[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）]**を選択します。

ステップ 3 各ユーザーの横にある [削除（Delete）] をクリックして、そのユーザを削除します。

（注） admin ユーザは削除できません。

ロールの作成または変更

ユーザロールを作成または変更します。

ステップ 1 Cisco Advanced Web Security Reporting アプリケーションに admin ユーザとしてログインします。

ステップ 2 **[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）] > [新規追加（Add New）]**を選択します。

ステップ 3 次の詳細を入力して、新しいロールを作成します。

1. [ロール名（Role Name）]：ロールの一意の名前を入力します。
2. [デフォルトアプリ（Default app）]：cisco_wsa_reporting
3. [検索の制限（Search Restrictions）]：このロールによって実行される検索の範囲を制限します。このロールの検索結果には、この検索文字列に一致するイベントのみが表示されます。

   – [検索条件の制限（Restrict search terms）]（source、host、index（以下で設定可能）、eventtype、sourcetype、search フィールド、*、OR および AND を含めることができます）。たとえば、「host=web* OR source=/var/log/*」となります。

   –[検索時間範囲の制限（Restrict search time range）]（このロールの検索の最大時間枠（秒単位）を設定します。たとえば、これを「60」に設定すると、このロールの検索は、検索で指定された最新の時刻の 1 分前に制限されます。これを「0」に設定して時間枠を明示的に無限にすることも、「-1」に設定してこのロールの時間枠の設定を解除することもできます（インポートされたロールによってオーバーライドできます））。

   –[ユーザレベルの同時検索ジョブの制限（User-level concurrent search jobs limit）]（このロールの各ユーザの同時検索ジョブの最大数を入力します）。

   – [このロールの各ユーザーのリアルタイム検索ジョブ（Real-time search jobs for each user of this role）]（この数は、通常の検索ジョブの制限とは無関係です）。

   – [ロールレベルの同時検索ジョブの制限（Role-level concurrent search jobs limit）]（このロールの累積同時検索ジョブの最大数を入力します）。

   –[ロールレベルの同時リアルタイム検索ジョブの制限（Role-level concurrent real-time search jobs limit）]（このロールの累積同時リアルタイム検索ジョブの最大数を入力します。この数は、通常の検索ジョブの制限とは無関係です）。

   – [合計ジョブディスククォータの制限（Limit total jobs disk quota）]（ユーザの検索ジョブで使用できる合計ディスク容量を MB 単位で入力します。たとえば、「100」の場合はこのロールは合計 100 MB に制限されます）。

4. [継承（Inheritance）]：機能とインデックスを継承するロールを指定します。継承された機能とインデックスを無効にすることはできません。複数のロールが指定されている場合、このロールは最も範囲の広い権限を持つ親から機能を継承します。以下は、機能によって異なる事前定義ロールのリストです。

   – admin

   – can_delete

– power

– splunk_system_role

– user

– wsa_admin

5. [機能（Capabilities）]：使用可能な機能名のリストについては、以下の「機能のリスト」の表を参照してください。
6. [デフォルトで検索されるインデックス（Indexes searched by default）]：インデックスが指定されていない場合にデフォルトで検索されるインデックスを設定します。このロールを持つユーザは、index= を使用して他のインデックスを検索できます（たとえば「index=special_index」）。
7. [インデックス（Indexes）]：このロールの検索を指定されたインデックスに制限します。
8. [保存（Save）] をクリックします。

機能のリスト

機能名	実行できる機能
accelerate_datamodel	データモデルのアクセラレーションを有効または無効にします。このデータモデルの自動アクセラレーションを有効にするにはアクセラレーションを true に設定します。データ内のイベント、フィールド、および個別のフィールド値の数に応じて、追加のスペースが必要です。詳細については、『Knowledge Manager Manual』を参照してください。
accelerate_search	レポートのアクセラレーションを有効または無効にできます。ユーザには schedule_search 機能も割り当てる必要があります。変換コマンドを使用する検索で機能します。詳細については、『Knowledge Manager Manual』を参照してください。
admin_all_objects	オブジェクトに設定されている制限に関係なく、システム内の任意のオブジェクトにアクセスして変更できます。ユーザオブジェクト、検索ジョブ、レポート、ナレッジオブジェクトなどです。Linux 環境でのルートへのアクセスと同じように、ACL 制限をバイパスできます。
change_authentication	認証設定を変更し、認証をリロードできます。認証の詳細については、『Securing Splunk Enterprise Manual』を参照してください。

機能名	実行できる機能
change_own_password	自身のパスワードを変更できます。
delete_by_keyword	「delete」演算子を使用できます。「delete」コマンドは、検索によって返されたすべてのイベントを削除済みとしてマークします。これによりデータが検索結果に表示されないようにマスクされますが、実際にはディスク上のrawデータは削除されません。詳細については、『Search Manual』を参照してください。
dispatch_rest_to_indexers	REST検索コマンドをインデクサにディスパッチできます。
edit_deployment_client	導入クライアントの設定を変更できます。導入クライアントの詳細については、『Managing Indexers and Clusters of Indexers Manual』を参照してください。
edit_deployment_server	導入サーバの設定を変更できます。フォワーダや他の導入クライアントにプッシュされるリモート入力を変更または作成できます。導入サーバの詳細については、『Managing Indexers and Clusters of Indexers Manual』を参照してください。
edit_dist_peer	分散検索用のピアを追加および編集できます。詳細については、『Managing Indexers and Clusters of Indexers Manual』マニュアルを参照してください。
edit_forwarders	SSL、バックオフスキームなどの設定を含む、フォワーダ設定を変更できます。TCPおよびSyslog出力管理ハンドラでも使用されます。
edit_httpauths	httpauth-tokensエンドポイントを介してユーザセッションを編集および終了できます。
edit_indexer_cluster	インデクサクラスタを編集できます。インデクサの詳細については、『Managing Indexers and Clusters of Indexers Manual』を参照してください。
edit_input_defaults	サーバ設定エンドポイントを使用して、入力データのデフォルトのホスト名を変更できます。
edit_monitor	ファイルのモニタリングに関する入力を追加し、設定を編集できます。標準入力エンドポイントおよびワンショット入力エンドポイントでも使用されます。

機能名	実行できる機能
edit_roles	ロールを編集し、ユーザ/ロールのマッピングを変更できます。ユーザとロールエンドポイントの両方で使用されます。
edit_roles_grantable	ロールを編集し、限られたロールセットのユーザ/ロールのマッピングを変更できます。他のユーザに任意のロールを割り当てることができます。この機能を制限するには、authorize.conf で grantableRoles を設定します。例：grantableRoles = role1;role2;role3
edit_scripted	スクリプト入力を作成および編集できます。
edit_search_head_clustering	検索ヘッドのクラスタリング設定を編集できます。
edit_search_schedule_priority	通常よりも高いスケジュール優先度を検索に割り当てることができます。検索スケジューラの詳細については、『Knowledge Manager Manual』を参照してください。
edit_search_schedule_window	スケジュールウィンドウをスケジュールされたレポートに割り当てることができます。schedule_search 機能が必要です。検索スケジューラの詳細については、『Knowledge Manager Manual』を参照してください。
edit_search_scheduler	検索スケジューラを有効または無効にできます。『Knowledge Manager Manual』を参照してください。
edit_search_server	タイムアウト、ハートビート、ブラックリストなどの一般的な分散検索設定を編集できます。
edit_server	サーバ名、ログレベルなどの一般的なサーバ設定を編集できます。
edit_server_crl	サーバ名、ログレベルなどの一般的なサーバ設定を編集できます。一般的なサーバとイントロスペクトの設定を読み取る機能を継承します。
edit_sourcetypes	ソースタイプを編集できます。ソースタイプの詳細については、『Knowledge Manager Manual』を参照してください。
edit_splunktcp	別の Splunk インスタンスから TCP 入力を受信するための設定を変更できます。
edit_splunktcp_ssl	Splunk TCP 入力の SSL 固有の設定を表示または編集できます。

機能名	実行できる機能
edit_splunktcp_token	Splunktcp トークンを編集できます。
edit_tcp	一般的な TCP 入力を受信するための設定を変更できます。
edit_tcp_token	TCP トークンを変更できます。これは管理機能であり、システム管理者にのみ割り当てる必要があります。
edit_telemetry_settings	製品インストルメンテーションをオプトインまたはオプトアウトします。
edit_token_http	HTTP トークン入力の設定を作成、編集、表示、および削除できます。HTTP イベントコレクタ機能も有効にします。
edit_udp	UDP 入力の設定を変更できます。
edit_user	ユーザを作成、編集、または削除できます。edit_user 機能を持つロールは、他のユーザに任意のロールを割り当てることができます。この機能を制限するには、authorize.conf で grantableRoles を設定します。たとえば、grantableRoles = role1;role2;role3 とします。また、分散検索用の証明書を管理できます。
edit_view_html	HTML ベースのビューを作成、編集、または変更できます。
edit_web_settings	システム設定エンドポイントを介して web.conf の設定を変更できます。
embed_report	レポートを埋め込んだり、埋め込まれたレポートの埋め込みを無効にできます。
export_results_is_visible	Splunk Web の [結果のエクスポート（Export Results）] ボタンを表示または非表示にできます。デフォルト値はボタンを表示することです。
extra_x509_validation	x509 検証を追加できます。
get_diag	/streams/diag エンドポイントを使用して Splunk インスタンスからリモート診断を取得できます。
get_metadata	「メタデータ」検索プロセッサを使用できます。
get_typeahead	エンドポイントと先行入力検索フィールドで先行入力を使用できます。

機能名	実行できる機能
indexs_edit	ファイルサイズやメモリ制限などのインデックス設定を変更できます。
input_file	inputcsv（dispatch=t モードを除く）および inputlookup を介してファイルを入力として追加できます。
license_edit	ライセンスを編集できます。
license_tab	ライセンスにアクセスして変更できます。この属性は非推奨です。
license_view_warnings	データ制限を超えている場合、またはライセンスの有効期限に達した場合に、警告メッセージを表示できます。これらの警告は、システムバナーに表示されます。
list_accelerate_search	アクセラレーションレポートを表示できます。ユーザはレポートを高速化できません。
list_deployment_client	導入クライアントの設定を表示できます。
list_deployment_server	導入サーバの設定を表示します。
list_forwarders	データ転送の設定を一覧表示して表示できます。TCP および Syslog 出力管理ハンドラーで使用できます。
list_httpauths	httpauth-tokens エンドポイントを介してユーザセッションを表示できます。
list_indexer_cluster	インデクサクラスタのリストと、バケット、ピアなどのインデクサクラスタオブジェクトを表示できます。
list_indexerdiscovery	インデクサ検出の設定を表示できます。インデクサ検出ハンドラでも使用されます。
list_inputs	ファイル、TCP、UDP、スクリプトなどからの入力を含む、さまざまな入力のリストを表示できます。
list_introspection	インデクサ、検索、プロセッサ、キューなどのイントロスペクション設定と統計を読み取ることができます。
list_search_head_clustering	アーティファクト、委任されたジョブ、メンバー、キャプテンなどの検索ヘッドクラスタリングオブジェクトを一覧表示して表示できます。
list_search_scheduler	検索スケジューラジョブのリストを表示できます。

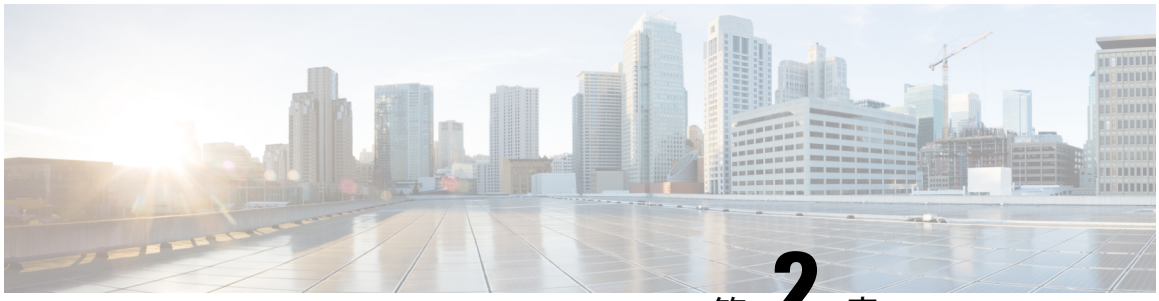
機能名	実行できる機能
list_settings	サーバ名やログレベルなどのサーバとイントロスペクションの設定を一覧表示して表示できます。
list_storage_passwords	/storage/passwords エンドポイントを一覧表示して表示したり、GET を実行したりできます。/storage/passwords エンドポイントに対して POST を実行するには、admin_all_objects 機能をロールに追加する必要があります。
output_file	outputcsv（dispatch=t モードを除く）や outputlookup などのファイル出力を作成できます。
pattern_detect	[検索（Search）] ビューの [パターン（Patterns）] タブを表示して使用できます。
request_remote_tok	リモート認証トークンを取得できます。これにより、分散ピア管理を実行し、レプリケーションをバンドルして、古い 4.0.x Splunk インスタンスに検索を分散できます。
rest_apps_management	Python リモートアプリハンドラーのエントリとカテゴリの設定を編集できます。詳細については、restmap.conf を参照してください。
rest_apps_view	Python リモートアプリハンドラーでさまざまなプロパティを一覧表示して表示できます。詳細については、restmap.conf を参照してください。
rest_properties_get	サービス/プロパティエンドポイントから情報を取得できます。
rest_properties_set	サービス/プロパティエンドポイントを編集できます。
restart_splunkd	サーバ制御ハンドラを介して Splunk Enterprise を再起動できます。
rtsearch	リアルタイム検索を実行できます。
run_debug_commands	debug コマンドを実行できます。たとえば、「Summarize」を実行できます。
run_multi_phased_searches	redistribute コマンドを使用して検索を実行できます。このコマンドは、分散検索環境で並列削減検索処理を呼び出します。この機能は、デフォルトではどのロールにも割り当てられていません。

機能名	実行できる機能
schedule_search	保存された検索をスケジュールして、アラートを作成および更新し、トリガーされたアラート情報を確認できます。
search	検索を実行できます。詳細については、『Search Manual』を参照してください。
search_process_config_refresh	「refresh search-process-config」CLI コマンドを使用して、アイドル状態の検索プロセスを手動でフラッシュできます。
srchFilter	検索フィルタを管理できます。詳細については、『Search Manual』を参照してください。
srchIndexesAllowed	検索インデックスを実行できます。詳細については、『Search Manual』を参照してください。
srchIndexesDefault	デフォルトの検索インデックスを設定できます。
srchJobsQuota	検索ジョブのクォータを設定できます。
srchMaxTime	検索の最大時間を設定できます。
use_file_operator	「file」検索演算子を使用できます。「file」検索演算子は非推奨です。
web_debug	Web ファイルをデバッグできます。

表 *1 : Windows* 固有の機能

機能名	実行できる機能
edit_modinput_admon	admon.conf のモジュラ入力を編集します。
edit_modinput_perfmon	perfmon.conf でモジュラ入力を編集します。
edit_modinput_winhostmon	Windows ホストデータをモニタリングするための入力を追加および編集します。
edit_modinput_winnetmon	Windows ネットワークデータをモニタリングするための入力を追加および編集します。
edit_modinput_winprintmon	Windowsプリンタデータをモニタリングするための入力を追加および編集するために必要です。
edit_win_admon	（非推奨）

機能名	実行できる機能
edit_win_eventlogs	Windows のイベントログを編集します。
edit_win_perfmon	（非推奨）
edit_win_regmon	（非推奨）
edit_win_wmiconf	wmi.conf を編集します。
list_pdfserver	PDF サーバファイルを表示します。
list_win_localavailablelogs	すべてのローカル Windows イベントログを一覧表示します。
srchTimeWin	検索時間制限を設定します。
write_pdfserver	PDF サーバファイルに書き込みます。



第 2 章

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。

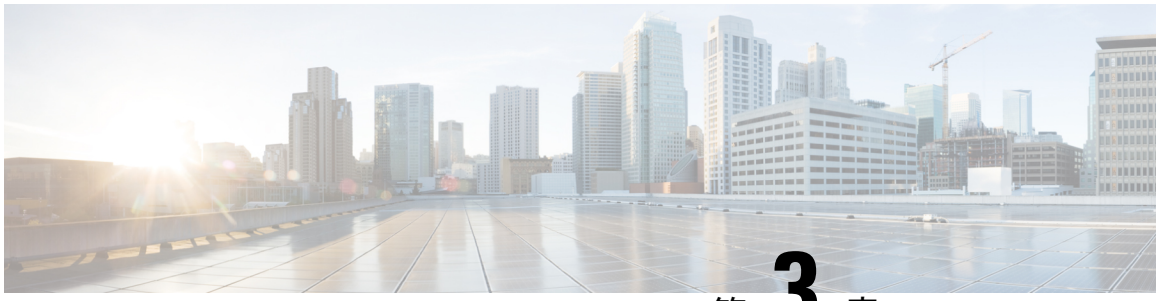
ステップ 2 トータル トランザクションのグラフでは、上位 10 の URL カテゴリを表示します。

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。



第 3 章

CEF エクストラクタ

この章は、次のセクションで構成されています。

CEF エクストラクタ サービスについて

Advanced Web Security Reporting（AWSR）アプリケーションで実行される共通イベント フォーマット（CEF）エクストラクタ サービスによって、1 つまたは複数の WSA から受信したアクセス ログを CEF 形式の出力データに変換して、ArcSight アプリケーションなど、他のサードパーティ製セキュリティ情報管理（SIM）システムに転送できます。

（注） CEF エクストラクタ サービスは分散環境のみで動作するため、少なくとも 2 つの個別の AWSR インスタンスを異なるホストで実行する必要があります。一方の AWSR インスタンスが「マスター」または「検索ヘッド」として機能し、専用の検索機能やライセンス共有機能を提供します。さらに、他方の「リスナー」または「ピア」インスタンスはインデクサとして機能し、AWSR データベースに変換後の Syslog データを送信します。

CEF エクストラクタ サービスの設定

Advanced Web Security Reporting の CEF エクストラクタ サービスは、次の手順で設定します。

- 1 つまたは複数のピア インスタンスを「リスナー」として設定し、リンクした Web セキュリティ アプライアンスからの syslog データの受信と変換、および syslog データへのインデックス作成を行えるようにします。詳細については、「CEF ピアの設定」を参照してください。
- マスター AWSR インスタンスまたは「検索ヘッド」を設定します。「AWSR マスターの設定」を参照してください。

- すべてのマスターおよびピア システムでライセンスを設定します。「ライセンスの設定」を参照してください。
- マスター システムで CEF サービスを設定します。「CEF エクストラクタの初期設定」を参照してください。
- マスター システムの再起動
- CEF 出力フィールドへのアクセス ログのマッピング設定
- CEF サービスのデータ入力を設定します。「CEF エクストラクタ サービスのデータ入力の設定」を参照してください。

はじめる前に

- 必要なすべてのホストで、AWSR ソフトウェアをインストールし、基本的な稼働と通信に関する設定を行います。

CEF ピアの設定

以下の手順に従って、インデックス ピアのホスト サーバで、インデックス ピアを「リスナー」として設定します。これには、受信側の新しいエントリを作成し、Web セキュリティ アプライアンスの syslog データをリッスンするポートを指定します。

始める前に

- AWSR ピアを起動し、管理者ユーザとしてログインします。

ステップ 1 **[設定（Settings）] > [データ（Data）] > [転送と受信（Forwarding and Receiving）]**を選択します。

ステップ 2 [転送と受信（Forwarding and Receiving）] ページで、[データを受信（Receive data）] セクションの [受信を設定（Configure receiving）] 行の [新規追加（Add new）] リンクをクリックします。

目的のリスナー ポートがすでに設定されている場合、[受信を設定（Configure receiving）] リンクをクリックして、[データを受信（Receive data）] ページに直接移動し、ポートを有効化できます。

ステップ 3 [新規追加（Add new）] > [受信を設定（Configure receiving）] ページで、リッスンするポートの番号を入力します。

ステップ 4 [保存（Save）] をクリックします。

[データを受信（Receive data）] ページに戻り、リッスンする利用可能なポートが表示されます。ここでは、個々のポートの有効化/無効化および削除を行えます。このページから新しいポートを追加することもできます。

AWSR マスターの設定

マスター（または検索ヘッド）システムで分散検索を有効にして、1 つまたは複数の検索ピアをピアのリストに追加する必要があります。

始める前に

- AWSR マスターを起動し、管理者ユーザとしてログインします。

ステップ 1 分散検索を有効にするには、次のコマンドを実行します。

1. **[設定（Settings）] > [分散環境（Distributed Environment）] > [分散検索（Distributed Search）]**を選択します。
2. [分散検索（Distributed search）] ページで、[分散検索の設定（Distributed search setup）] をクリックします。
3. **[分散検索の設定（Distributed search setup）]** ページで、[分散型の検索を有効にしますか（Turn on distributed search?）] オプションに対して [はい（Yes）] を選択します。
4. [保存（Save）] をクリックします。

[分散検索（Distributed search）] ページに戻ります。

ステップ 2 検索ピア（インデクサ）を追加するには、以下の手順を実行します。

1. [分散検索（Distributed search）] ページの [検索ピア（Search peers）] 行にある [新規追加（Add new）] をクリックします。
2. [新規追加（Add new）] ページの [検索ピアを追加（Add search peers）] で、[ピアID（Peer ID）] に *server_name:management_port* または *IP_address:management_port* のいずれかの形式で入力します。
3. ピアに接続するために、以下の分散検索認証パラメータを指定します。
   - [リモートユーザ名（Remote username）]：リモート検索ピアの管理者ユーザのユーザ名を指定します。
   - [リモートパスワード（Remote Password）]：そのユーザの接続パスワードを入力します。
   - [パスワードの確認（Confirm password）]：パスワードを再入力します。
4. [保存（Save）] をクリックします。

[検索ピア（Search peers）] ページに戻ります。

[検索ピア（Search peers）] ページに、現在設定されているすべてのピアが一覧表示されます。個々の検索ピアを有効化/無効化および削除できます。このページから新しい**検索ピア**を追加することもできます。**[設**

定（**Settings**）] > **[分散環境（Distributed Environment）]** > **[分散検索（Distributed Search）]** を選択し、[検索ピア（Search peers）] をクリックして、このページにいつでもアクセスできます。

ライセンスの設定

マスターシステムでは、1つのライセンスを各インデクサで使用できます。つまり、インデクサピアごとに個別のライセンスは必要ありません。次の項では、すべての AWSR インスタンスにライセンスを設定する方法について説明します。

- ピアのライセンス
- マスター ライセンス

ピアのライセンス

各インデクサは、マスター システムによって維持されるライセンス プールのライセンスにアクセスするように設定します。

ステップ 1 インデクサシステムで**[設定（Settings）]** > **[システム（System）]** > **[ライセンス（Licensing）]**を選択し、[ライセンス（Licensing）] ページを開きます。

このページの上部に、このサーバのライセンスのロールに関する通知が表示されます。サーバのロールは、[リモートマスターライセンスサーバへ関連付け（associated with a remote master license server）] または [マスターライセンスサーバとして動作（acting as a master license server）] のいずれかになります。

ステップ 2 このピアについて表示されているロールが [マスターライセンスサーバとして動作（acting as a master license server）] の場合は、[スレーブへ変更（Change to slave）] ボタンをクリックします。

ステップ 3 [マスターの関連付けを変更（Change master association）] ページで、[マスターライセンスサーバとして異なるAWSRインスタンスを指定（Designate a different AWSR instance as the master license server）] を選択します。

ステップ 4 マスターのライセンスサーバのアクセス情報として、目的のサーバの *server_name :management_port* または *IP_address:management_port* を入力します。

ステップ 5 [保存（Save）] をクリックします。

マスター ライセンス

マスターシステムでは、1つのライセンスを各インデクサで使用できます。以下の手順に従って、すべての設定済みインデクサ システムで共有するライセンス プールを指定します。

ステップ 1 検索ヘッドで **[設定（Settings）]** > **[システム（System）]** > **[ライセンス（Licensing）]**を選択し、[ライセンス（Licensing）] ページを開きます。

このページの上部に、このサーバのライセンスのロールに関する通知が表示されます。サーバのロールは、[リモートマスターライセンスサーバへ関連付け（associated with a remote master license server）] または [マスターライセンスサーバとして動作（acting as a master license server）] のいずれかになります。

ステップ 2 このピアについて表示された権限が [リモートマスターライセンスサーバへ関連付け（associated with a remote master license server）] の場合は、[マスターへ変更（Change to master）] ボタンをクリックし、[マスターの関連付けを変更（Change master association）] ダイアログ ボックスでこのサーバをマスター ライセンス サーバとして指定します。このダイアログ ボックスで [保存（Save）] をクリックして、[ライセンス（Licensing）] ページに戻ります。

ステップ 3 [ライセンスのスタック（License stack）] セクションで、インデクサ ピアと共有するライセンス プールを表す行の [編集（Edit）] をクリックします。

ステップ 4 [ライセンスプールの管理（Manage license pool）] ページで、[このプールから取得できるインデクサを指定（Which indexers are eligible to draw from this pool?）] オプションの [特定のインデクサ（Specific indexers）] を選択します。

使用可能なインデクサの一覧が表示されます。

ステップ 5 [関連付けられたインデクサ（Associated indexers）] リストに追加するために、目的のインデクサの前に表示された緑色の [追加（Add）] ボタンをクリックします。必要に応じてこの手順を繰り返します。

ステップ 6 [送信（Submit）] をクリックします。

ステップ 7 [更新（Update）] の通知で [OK] をクリックします。

[ライセンス（Licensing）] ページに戻ります。このページで、ライセンスを追加したり、ライセンス プールを追加、編集、および削除したりできます。

CEF エクストラクタの初期設定

AWSR CEF エクストラクタ マスターおよびインデクサ システムを設定したら、CEF エクストラクタ サービスを設定する必要があります。

始める前に

- AWSR マスター システムを起動し、管理者ユーザとしてログインします。

ステップ 1 **[設定（Settings）] > [サードパーティサービス（Third Party Services）] > [CEFエクストラクタ（CEF Extractor）]**を選択し、[CEFエクストラクタ（CEF Extractor）] ページを開きます。

CEF アプリケーションがまだ完全に構成されていないことが通知されます。

ステップ 2 [アプリの設定ページに進む（Continue to app setup page）] ボタンをクリックして、AWSR CEF の設定ページに進みます。

ステップ 3 [リアルタイムのインデックス作成を有効にする（Enable Indexed Realtime）] をオンにして、リアルタイムでインデックスの作成と検索ができるようにします。

パフォーマンスを向上させるには、このオプションを有効にすることをお勧めします。

ステップ 4 [インデクサの設定（Indexer Setup）] セクションの [インデクサ（Indexers）] フィールドに、各ピアのアクセス ID 情報を *server_name:listener_port* または *Ip_address:istener_port* のいずれかの形式で入力します。

（注） インデクサエントリごとに、「CEF ピアの設定」で説明されているように、そのインデクサシステム用に設定されたリスナーポートの番号を使用してください。

ステップ 5 [保存（Save）] をクリックします。

マスター システムの再起動

Advanced Web Security Reporting マスター システム、ピア ライセンス共有、および CEF エクストラクタ サービスを構成したら、マスター サーバを再起動する必要があります。

ステップ 1 **[設定（Settings）] > [システム（System）] > [サーバコントロール（Server Controls）]** を選択し、[サーバコントロール（Server controls）] ページを開きます。

ステップ 2 [AWSRを再起動（Restart AWSR）] ボタンをクリックし、指示に従ってシステムを再起動します。

ステップ 3 再起動が完了したら、再度ログインします。

CEF 出力フィールドへのアクセス ログのマッピング設定

次のタスクでは、Web セキュリティ アプライアンスのアクセス ログのマッピングを CEF エクストラクタ サービスの CEF 出力フィールドに設定し、この情報の出力先を定義します。

ステップ 1 **[設定（Settings）] > [サードパーティサービス（Third Party Services）] > [CEFエクストラクタ（CEF Extractor）]**を選択し、[CEFエクストラクタ（CEF Extractor）] ページを開きます。

ステップ 2 [新規（New）] をクリックして、**CEF エクストラクタデータ検索設定**ウィザードを起動します。

ステップ 3 データを取得する [データモデル（Data Model）] を選択します。この場合は、[Web_Access_Data] を選択します。

ステップ 4 [オブジェクト（Object）] ドロップダウン リストから [Web_Access_Event] を選択することにより、Web セキュリティ アプライアンスの Web アクセス ログからデータ フィールドを取得するように指定します。

ステップ 5 [次へ（Next）] をクリックして、ウィザードの [マップフィールド（Map Fields）] ページに進みます。

このページには、[CEF出力フィールド（CEF Output Fields）] と [データモデル属性（Data-model attributes）] の 2 つの列が表示されます。各行の [出力フィールド（Output Fields）] 列は、すべての CEF 出力形式を含むドロップダウンリストです。また、[データモデル属性（Data-model attributes）] 列にはデータモデルで使用できる属性のハードコードされたリストが表示されます。

ステップ 6 必要に応じて、**CEF 出力**フィールドを Web Access のデータモデル属性にマップします。

一部のフィールドは自動的にマッピングされます（たとえば、データモデルの属性 `host` は自動的に CEF フィールドの `syslog_host` にマッピングされます）。このページには、自動的なマッピングとデフォルトのマッピングの両方が表示され、それぞれを変更できます。

マッピングを追加または変更するには、更新対象の出力フィールドから属性へのマッピングを表す行のドロップダウンリストを開き、このデータモデル属性にマッピングする **CEF 出力**フィールドを選択します。

ステップ 7 [次へ（Next）] をクリックして、ウィザードの [静的フィールドの作成（Create Static Fields）] ページに進みます。

このページのフィールドを使用して、対応するデータモデル属性がない CEF 出力フィールドに、状況依存の静的値を指定します。

ステップ 8 一覧表示された **CEF 出力**フィールドに対する静的なフィールド値を入力します。

たとえば、CEF 出力フィールド `dvc_vendor` にフィールド値の CISCO を入力し、`dvc_product` に `AWSR_CEF` を入力できます。

ステップ 9 [次へ（Next）] をクリックして、ウィザードの [出力を定義（Define Outputs）] ページに進みます。

このページでは、CEF データの送信先の出力グループを作成または選択します。

ステップ 10 [新規出力グループの作成（Create new output group）] をクリックします。

ステップ 11 [新規出力グループ（New Output Group）] ダイアログボックスで、以下の新しい出力グループパラメータを指定します。

- [名前（Name）]：この出力グループの識別子。
- [データの出力先のホスト（Hosts to output data to）]：CEF 出力データを送信する出力サーバ。*server_namereceive_port* または *IP_address:receive_port* のいずれかの形式で入力します

（注） syslog データを出力する予定がある場合は、TCP ポート 514 はすでに使用されているため使用できません。「Web セキュリティ アプライアンス Syslog のデータ入力の設定」を参照してください。

ステップ 12 [保存（Save）] をクリックして、[新規出力グループ（New Output Group）] ダイアログボックスを閉じます。

ステップ 13 [次へ（Next）] をクリックして、ウィザードの [検索を保存（Save Search）] ページに進みます。

ステップ 14 このマッピングまたは検索の設定を指定します。

- [検索名（Search Name）]：この CEF 情報の検索設定の識別子またはマッピング名。
- [検索の説明（Search Description）]（任意）：この CEF 情報検索の簡単な説明。

ステップ 15 [保存（Save）] をクリックして、ウィザードを終了します。

[CEFエクストラクタ（CEF Extractor）]ページに、定義済みのデータセットのマッピングが一覧表示されます。新しいデータセットを追加したり、既存のデータセットを有効化、無効化、または削除したりできます。

CEF エクストラクタ サービスのデータ入力の設定

次のタスクでは、CEF エクストラクタ サービスのデータ フィールドを設定します。

（注） この項では、CEF エクストラクタ サービスのデータ入力として Web セキュリティ アプライアンスのアクセス ログを設定する方法について説明します。また、FTP プッシュおよび syslog プッシュをサービスのデータ入力として設定することもできます。詳細については、「継続的なデータ転送の設定」と「Umbrella のログの更新」を参照してください。

ステップ 1 **[設定（Settings）]** > **[データ（Data）]** > **[データ入力（Data inputs）]**を選択して、[データ入力（Data inputs）] ページを開きます。

ステップ 2 [データ入力（Data inputs）]ページの [ファイルとディレクトリ（Files & directories）]行の [新規追加（Add new）]をクリックして、新しいデータ フォルダのフィールドのマッピングと監視を設定するウィザードを起動します。

ステップ 3 [ファイルまたはディレクトリ（File or Directory）] フィールドの横にある [参照（Browse）] ボタンをクリックします。

ステップ 4 [ソースの選択（Select source）] ダイアログ ボックスで、目的の Web セキュリティ アプライアンスのアクセス ログ フォルダを参照して選択します（たとえば、`home/logger/incoming/wsa_test/accesslogs`）。

ステップ 5 [選択（Select）] をクリックして [ソースの選択（Select source）] ダイアログ ボックスを閉じます。

ステップ 6 [ソースの選択（Select Source）] ウィザード ページで [次へ（Next）] をクリックして [入力設定（Input Setting）]ページに移動します。

ステップ 7 ソースの種類については、[選択（Select）] をクリックし、[ソースの種類を選択（Select Source Type）] をクリックして `wsa_accesslogs` を選択します（[ソースの種類の選択（Select Source Type）] ドロップダウン リストの一番上にあるフィルタ フィールドに `wsa_accesslogs` を 1 文字ずつ入力することで、エントリをすばやく見つけることができます）。

ステップ 8 アプリ コンテキストについては、[アプリコンテキスト（App context）] ドロップダウンリストから [Advanced Web Security Reporting 6.1.0] を選択します。

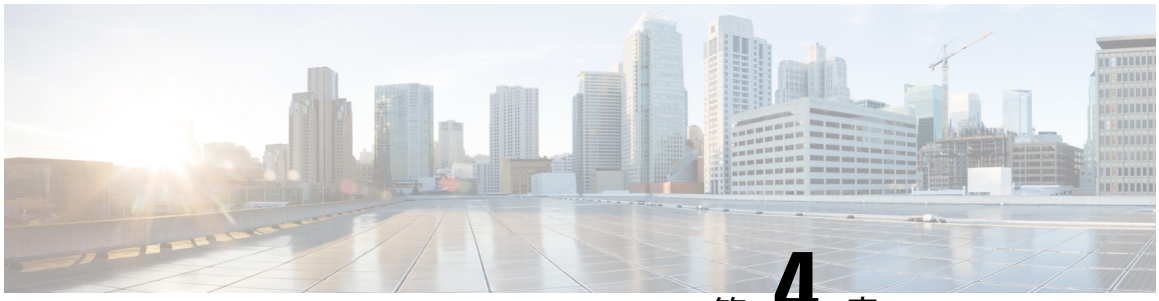
ステップ 9 [ホスト（Host）] エントリまで下にスクロールして、[パス内のセグメント（Segment in path）] をクリックし、[セグメント番号（Segment number）] に入力します。

[ホスト（Host）] エントリは、ソースのイベントに対してホスト フィールドの値を決定する方法を指定します。[パス内のセグメント（Segment in path）] オプションは、先に指定した [ソースパス（Source path）] のセグメントから決定されることを意味します。セグメント番号は、パスのどのセグメントがホスト値であるかを示します。たとえば、前のサンプルのソース パス

`home/logger/incoming/wsa_test/accesslogs` の場合、ホスト名 `wsa_test` はパスの 4 番目のセグメントなので、ここに入力するセグメント番号は 4 になります。

ステップ 10 [レビュー（Review）] をクリックして、ウィザードの [レビュー（Review）] ページに進みます。

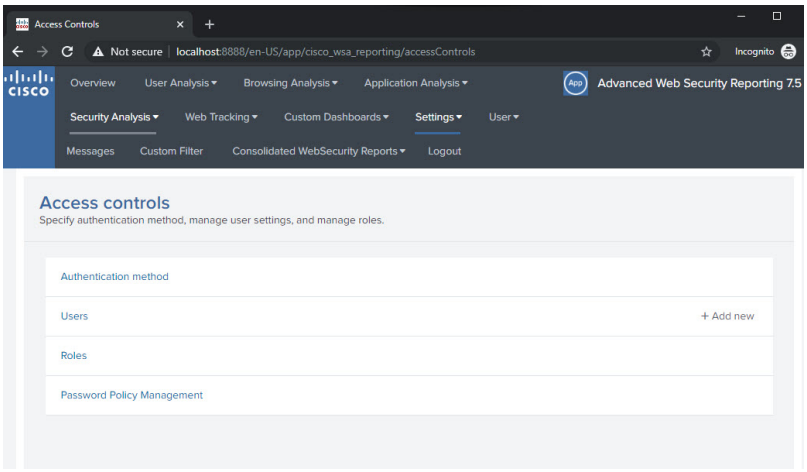
ステップ 11 入力した情報を確認し、[送信（Submit）] をクリックして新しいデータ入力インスタンスを作成します。



第 4 章

パスワードポリシー管理

この章では、Cisco Advanced Web Security Reporting アプリケーションの Web GUI で実行できるパスワード関連の設定について説明します。これらの操作を実行するには、管理者権限が必要です。**[設定（Settings）] > [ユーザーと認証（USERS AND AUTHENTICATION）] > [アクセス制御（Access Controls）] > [パスワードポリシー管理（Password Policy Management）]** に移動して、[パスワードポリシー管理（Password Policy Management）] ページに移動します。



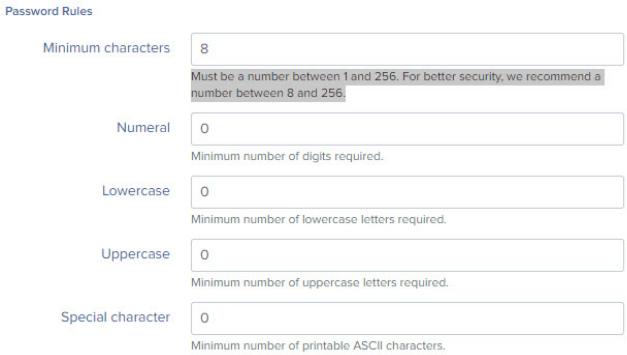
パスワードの規則

パスワードは数字、小文字、大文字、英数字の組み合わせにする必要があります。パスワードを設定するには次のフィールドを指定できます。

- [最小文字数（Minimum Characters）]：パスワードで使用される最小文字数を設定します。

（注） 1 ～ 256 の範囲内の数を指定してください。8 を超える数を使用することをお勧めします。

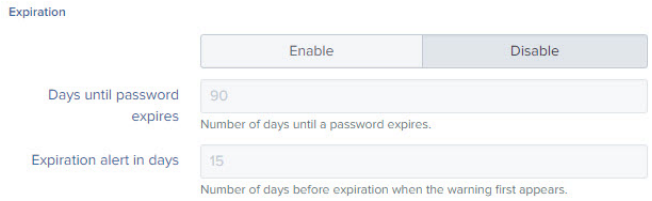
- [数字（Numerals）]：パスワードの数字の最小文字数を設定します。
- [小文字（Lowercase）]：パスワードの小文字の最小文字数を設定します。
- [大文字（Uppercase）]：大文字の最小文字数を設定します。
- [特殊文字（Special character）]：特殊文字または英数字の最小文字数を設定します。



パスワードの期限

パスワードの期限の期間を有効または無効にできます。次のフィールドを設定できます。

- [パスワードの期限までの日数（Date until password expires）]：パスワードの期限が切れるまでの日数を設定します。
- [有効期限アラート（日数）（Expiration alert in days）]：ユーザにアラートが表示される有効期限までの日数を設定します。



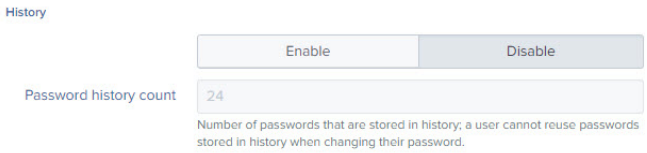
アラートの例を以下に示します。

パスワード履歴

[パスワード履歴（Password History）] オプションを有効または無効にできます。

- [パスワード履歴カウント（Password History Count）]：履歴に保存されているパスワードの数。

（注） ユーザは、パスワードを変更するときに、履歴に保存されているパスワードを再利用できません。



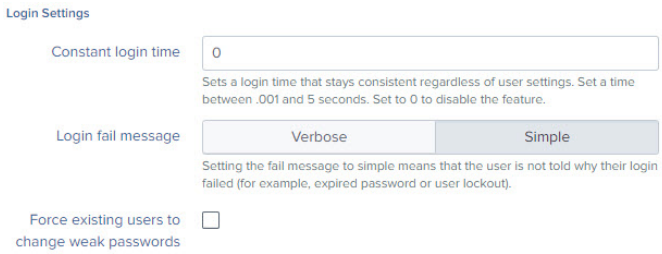
ログイン設定

- [一定のログイン時間（Constant Login Time）]：ユーザ設定に関係なく一貫性を保つログイン時間を設定します。

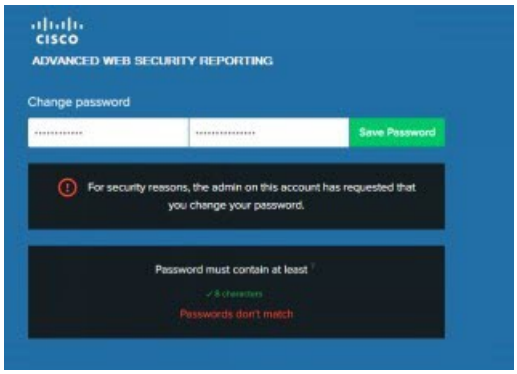
（注） この機能を無効にするには、0 に設定します。

- [ログイン失敗メッセージ（Login fail message）]：ユーザに示す失敗メッセージを設定します。[シンプル（Simple）] を選択した場合、ユーザには

ログインが失敗した理由（期限切れのパスワードやユーザのロックアウトなど）が通知されません。



パスワードの変更中にエラーが発生した場合は、エラーの理由が表示されます。次に例を示します。



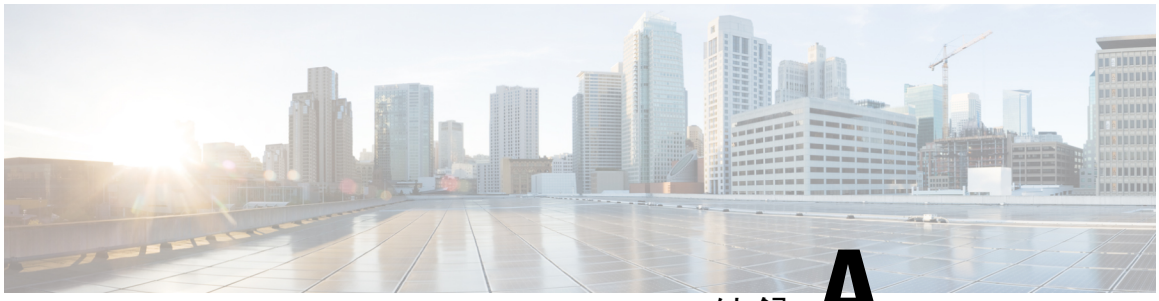
パスワード ロックアウト

この機能では、ブルートフォースログイン攻撃を防ぐために、単位時間あたりの各送信元のクレデンシャル試行回数を制限します。

次のフィールドを設定できます。

- [ログイン試行失敗回数（Failed login attempts:）]：ユーザがロックアウトされるまでに実行できるログイン試行回数。
- [ロックアウトしきい値（分単位）（Lockout threshold in minutes）]：最初のログイン失敗後、カウンタがリセットされるまでに必要な時間。
- [ロックアウト期間（分単位）（Lockout duration in minutes）]：ユーザが再度ログインを試行できるようになるまでのロックアウト期間。

ログインに失敗すると、管理者が指定したロックアウト期間中はユーザアカウントがロックされます。



付録 A

証明書の生成と署名

この章は、次のセクションで構成されています。

Cisco Advanced Web Security Reporting アプリケーションの自己署名証明書

このトピックでは、Cisco Advanced Web Security Reporting アプリケーションに含まれているバージョンの OpenSSL を使用して、コマンドラインで自己署名証明書を作成するための基本的な例を示します。

自己署名証明書は組織によって署名されるため、ブラウザの証明書ストアには含まれていません。その結果、Webブラウザは、自己署名証明書を「信頼できない」と見なします。これによってユーザへの警告ページが生成され、ユーザのアクセスが妨げられる場合もあります。

自己署名証明書は、Cisco Advanced Web Security Reporting アプリケーションに接続するすべてのブラウザストアに独自の CA を追加できる組織内または既知のエンティティ間での、ブラウザから Cisco Advanced Web Security Reporting アプリケーションへの通信に最適です。その他のシナリオでは、CA 署名付き証明書をお勧めします。詳細については、「Cisco Advanced Web Security Reporting アプリケーション用のサードパーティにより署名された証明書の取得」を参照してください。

はじめる前に

この説明では、`$AWSR_HOME` は AWSR Enterprise のインストールディレクトリを指します。この表記法に従うことをお勧めしますが、この表記法を使用しない場合は、これらの例を使うときに `$AWSR_HOME` をインストールディレクトリに置き換える必要があります。

Windows の場合、コマンドラインまたは [システムのプロパティ（System Properties）] ダイアログの [環境（Environment）] タブで、この変数の設定が必要になる場合があります。デフォルトのホームディレクトリは、プラットフォームによって異なります。

- Windows の場合、AWSR Enterprise ディレクトリはデフォルトで `C:\Program Files\Cisco\` です。
- ほとんどの Linux プラットフォームでは、デフォルトのインストールディレクトリは `/opt/` です。

認証局となる新しいルート証明書の生成

ステップ 1 証明書とキーをホストする新しいディレクトリを作成します。この例では、`$AWSR_HOME/etc/auth/mycerts` を使用します。

ステップ 2 新しい RSA 秘密キーを生成します。Cisco Advanced Web Security Reporting アプリケーションは 2048 ビットのキーをサポートしていますが、ブラウザでサポートされている場合は、より大きなキーを指定できます。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

Windows の場合：

Windows では、openssl.cnf ファイルの場所の追加が必要な場合があることに注意してください。

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

Cisco Advanced Web Security Reporting アプリケーションは 2048 ビットのキーをサポートしていますが、ブラウザでサポートされている場合は、より大きなキーを指定できます。

ステップ 3 プロンプトが表示されたら、パスワードを作成します。

秘密キー `myCAPrivateKey.key` がディレクトリに表示されます。これはルート証明書の秘密キーです。

ステップ 4 ルート証明書の秘密キー `myCAPrivateKey.key` を使用して証明書署名要求を生成します。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr
```

ステップ 5 秘密キー `myCAPrivateKey.key` にパスワードを入力します。

新しい CSR myCACertificate.csr がディレクトリに表示されます。

ステップ 6 CSR を使用して、新しいルート証明書を生成し、秘密キーで署名します。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl x509 -req -in myCACertificate.csr -signkey myCAPrivateKey.key -out
myCACertificate.pem -days 3650
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl x509 -req -in myCACertificate.csr -signkey myCAPrivateKey.key -out
myCACertificate.pem -days 3650
```

ステップ 7 プロンプトが表示されたら、秘密キー `myCAPrivateKey.key` にパスワードを入力します。

新しい証明書 `myCACertificate.pem` がディレクトリに表示されます。これが自身のパブリック証明書です。

Cisco Advanced Web Security Reporting アプリケーションの新しい秘密キーの作成

ステップ 1 新しい秘密キーを生成します。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048 -config
```

ステップ 2 プロンプトが表示されたら、パスワードを作成します。

新しいキー `myAWSRWebPrivateKey.key` がディレクトリに表示されます。

ステップ 3 キーからパスワードを削除します（Cisco Advanced Web Security Reporting アプリケーションは、パスワードで保護された秘密キーをサポートしていません）。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
```

次のコマンドを使用して、パスワードが削除されたことを確認できます。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -text
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -text
```

パスワードを入力しなくても、証明書の内容を読み取ることができます。

サーバ証明書の作成と署名

ステップ 1 秘密キー `myAWSRWebPrivateKey.key` を使用して新しい証明書署名要求を作成します。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

Windows の場合：

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

CSR `myAWSRWebCert.csr` がディレクトリに表示されます。

ステップ 2 ルート証明書の秘密キー `myCAPrivateKey.key` を使用して CSR に自己署名します。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl x509 -req -in myAWSRWebCert.csr -CA myCACertificate.pem -CAkey
myCAPrivateKey.key -CAcreateserial -out myAWSRWebCert.pem -days 1095
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl x509 -req -in myAWSRWebCert.csr -CA myCACertificate.pem -CAkey
myCAPrivateKey.key -CAcreateserial -out myAWSRWebCert.pem -days 1095
```

ステップ 3 プロンプトが表示されたら、ルート証明書の秘密キー `myCAPrivateKey.key` にパスワードを入力します。

証明書 `myAWSRWebCert.pem` がディレクトリに追加されます。これはサーバ証明書です。

単一の PEM ファイルの作成

サーバ証明書とパブリック証明書をこの順序で 1 つの PEM ファイルに結合します。

Linux でこれを行う例を次に示します。

```
# cat myAWSRWebCert.pem myCACertificate.pem > myAWSRWebCertificate.pem
```

Windows の例を次に示します。

```
# type myAWSRWebCert.pem myCACertificate.pem > myAWSRWebCertificate.pem
```

証明書チェーンの設定

複数の証明書を使用するには、次の順序でサーバの証明書ファイルの最後に中間証明書を追加します。

```
<div class=samplecode
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
</div>
```

たとえば、証明書チェーンは次のようになります。

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

Cisco Advanced Web Security Reporting アプリケーション用のサードパーティにより署名された証明書の取得

このトピックでは、SSL 認証および暗号化用に Cisco Advanced Web SecurityReporting アプリケーションを構成するために必要な第三者の署名付き証明書を作成するための基本的な例を示します。

Cisco Advanced Web Security Reporting アプリケーションの新しい秘密キーの作成

ステップ 1 独自の証明書とキーをホストするための新しいディレクトリを作成します。この例では、`$AWSR_HOME/etc/auth/mycerts` を使用します。

既存の証明書を上書きしないように、新しい証明書を `$AWSR_HOME/etc/auth/splunkweb` とは別のディレクトリに保存することをお勧めします。これにより、必要に応じて AWSR に付属の証明書を他の AWSR コンポーネントに使用できます。

ステップ 2 新しい秘密キーを生成します。Cisco Advanced Web Security Reporting アプリケーションは、2048 ビット以上のキーをサポートします。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl genrsa -des3 -out myAWSRWebPrivateKey.key 2048
```

ステップ 3 元のキーのパスフレーズを入力するように求められたら、パスワードを作成します。

新しい秘密キー `myAWSRWebPrivateKey.key` がディレクトリに追加されます。このキーを使用して、CSR に署名できます。

ステップ 4 秘密キーからパスワードを削除します。Cisco Advanced Web Security Reporting アプリケーションは、秘密キーのパスワードをサポートしていません。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl rsa -in myAWSRWebPrivateKey.key -out myAWSRWebPrivateKey.key
-config $AWSR_HOME\openssl.cnf
```

次のコマンドを使用して、パスワードが正常に削除されたことを確認できます。

```
# openssl rsa -in myAWSRWebPrivateKey.key -text
```

パスワードが正常に削除された場合は、パスワードを入力しなくても証明書の内容を表示できます。

認証局（CA）要求の作成とサーバ証明書の取得

ステップ 1 秘密キー `myAWSRWebPrivateKey.key` を使用して新しい証明書署名要求を作成します。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

Windows の場合：

```
$AWSR_HOME/bin/splunk cmd openssl req -new -key myAWSRWebPrivateKey.key -out myAWSRWebCert.csr
```

Windows プラットフォームに関する注意：次のようなエラーが表示された場合

```
Unable to load config info from

c:\\build-amd64-5.0.2-20130120-1800\\AWSR/ssl/openssl.cnf
```

コマンドプロンプトに次のように入力してから、openssl コマンドを再度実行してください。

```
set OPENSSL_CONF=c:/Program Files/AWSR/openssl.cnf
```

ステップ 2 CSR `myAWSRWebCert.csr` を使用して、認証局（CA）に新しい署名証明書を要求します。署名証明書を要求するプロセスは、認証局が証明書署名要求を処理する方法によって異なります。詳細については、CA に問い合わせてください。

ステップ 3 認証局から返されたサーバ証明書をダウンロードします。この例では、この証明書を「`myAWSRWebCert.pem`」とします。

ステップ 4 認証局の公開 CA 証明書をダウンロードします。この例では、この証明書を「`myCAcert.pem`」とします。

ステップ 5 サーバ証明書とパブリック CA 証明書の両方が PEM 形式であることを確認してください。証明書が PEM 形式でない場合は、既存のファイルタイプに適した `openssl` コマンドを使用して証明書を変換します。DER 形式に使用できるコマンドの例を次に示します。

```
$ AWSR_HOME / bin / splunk cmd openssl x509 -in myAWSRWebCert.crt -inform DER -out myAWSRWebCert.pem
-outform PEM
```

```
$AWSR_HOME/bin/splunk cmd openssl x509 -in myAWSRWebCert.crt -inform DER -out myAWSRWebCert.pem
-outform PEM
```

ステップ 6 両方の証明書をチェックして、必要な情報が記載されていて、パスワードで保護されていないことを確認してください。

Linux の場合：

```
$AWSR_HOME/bin/splunk cmd openssl x509 -in myCACert.pem -text
```

```
$AWSR_HOME/bin/splunk cmd openssl x509 -in myAWSRWebCert.pem -text
```

Windows の場合：

```
$AWSR_HOME\bin\splunk cmd openssl x509 -in myCACert.pem -text
```

```
$AWSR_HOME\bin\splunk cmd openssl x509 -in myAWSRWebCert.pem -text
```

`myAWSRWebCert.pem` の発行者情報は、`myCACert.pem` のサブジェクト情報である必要があります（中間証明書を使用している場合を除く）。

証明書とキーを 1 つのファイルに結合

サーバ証明書とパブリック証明書をこの順序で 1 つの PEM ファイルに結合します。

証明書チェーンの設定

複数の証明書を使用するには、次の順序でサーバの証明書ファイルの最後に中間証明書を追加します。

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

たとえば、証明書チェーンは次のようになります。

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

中間証明書に署名したルート CA とすべての中間証明書はブラウザの証明書ストアに存在する必要があることに注意してください。

Cisco Advanced Web Security Reporting 認証用に署名証明書を準備する方法

証明書を取得したら、サーバ証明書とキーを 1 つのファイルにまとめて、Cisco Advanced Web Security Reporting ソフトウェアで使用できるようにする必要があります。

（注） 証明書と公開キーが x509 形式であること、および秘密キーが RSA 形式であることを確認します。

単一の PEM ファイルの作成

サーバ証明書とパブリック証明書をこの順序で 1 つの PEM ファイルに結合します。この例では、「Cisco Advanced Web Security Reporting アプリケーションの自己署名証明書」および「Cisco Advanced Web Security Reporting アプリケーション用のサードパーティにより署名された証明書の取得」で説明されているファイル名を使用しています。

以下は Linux の例です。

```
cat myServerCertificate.pem myServerPrivateKey.key myCACertificate.pem >

myNewServerCertificate.pem
```

以下は Windows の例です。

```
type myServerCertificate.pem myServerPrivateKey.key myCACertificate.pem >

myNewServerCertificate.pem
```

作成したら、ファイル `myNewServerCertificate.pem` の内容に以下をこの順序で含める必要があります。

- サーバー証明書（`myServerCertificate.pem`）
- 秘密キー（`myServerPrivateKey.key`）
- 認証局の公開キー（`myCACertificate.pem`）

適切に連結された証明書の例を次に示します。

```
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCscBkn/xey1TANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
...
<Server Certificate>
...
8/PZr3EuXYk1c+N5hgIQys5a/HIn
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CFCECC7976725DE5
S+DPcQ0l2Z1bk71N3cBqr/nwEXPNDQ4uqtecCd3iGMV3B/WSOWAQxcWzhe9JnIsl
...
<Server Private Key - Passphrase protected>
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCscBkn/xey1TANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
...
<Certificate Authority Public Key>
...
8/PZr3EuXYk1c+N5hgIQys5a/HIn
-----END CERTIFICATE-----
```

証明書チェーンの設定方法

複数の証明書を使用するには、サーバの証明書ファイルの最後に中間証明書を追加します。ルートまで、階層の降順で必要な数の証明書を追加できます。

証明書は次の順序で連結されます。

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

たとえば、証明書チェーンは次のようになります。

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

もう 1 つの例では、秘密キーを含む AWSR フォワーダからインデクサへの証明書を使用すると、完成した証明書ファイルは次のようになります。

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...<Server Private Key – Passphrase protected>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

証明書認証を使用した導入サーバとクライアントの保護

導入サーバからクライアントにプッシュされた構成データは不正利用可能な情報を提供しないため、導入サーバとクライアント間で署名付き証明書を使用した認証はお勧めしません。導入サーバとクライアントの証明書認証を構成すると、他の構成に次のような影響があります。

- Cisco Advanced Web Security Reporting アプリケーションは、証明書を使用するように設定しない限り、認証に失敗します。
- CLI は導入サーバと通信できなくなります。

非常に機密性の高いサーバ構成データがファイアウォールの外側のさまざまな場所に送信される可能性のある特定の分散構成では、証明書認証が必要になる場合があります。導入サーバと通信するように各インデクサを手動で設定できます。

証明書の生成と署名

（注） 導入サーバは、証明書をピアに正しくプッシュできません。各メンバーを個別に設定する必要があります。

ステップ 1 同じルート CA を使用して 1 つ以上の証明書を作成します。

ステップ 2 証明書を導入サーバとクライアントに配布します。

ステップ 3 **server.conf** を編集して、証明書の場所を指定します。

```
[sslConfig]

enableSplunkdSSL = true

sslVersions = Defaults to "*,-ssl2" (anything newer than SSLv2). This is the recommended
setting.

serverCert = The full path to the PEM format server certificate file. Default
certificates

($SPLUNK_HOME/etc/auth/server.pem) are generated by Splunk at start. To secure Splunk,
you should replace the default cert with your own PEM file.

sslPassword = password

sslRootCAPath = absolute path to the operating system's root CA (Certificate Authority)
PEM

format file containing one or more root CA. Do not configure this attribute on Windows.
```

ステップ 4 前の手順の [sslConfig] スタンザに次の属性を追加して、server.conf を編集して証明書に対して認証します。

```
requireClientCert = true
```

（注） この `requireClientCert` は、デフォルトで「false」に設定されています。これを true に変更して Splunk にクライアントの証明書を強制的にチェックさせると、Cisco Advanced Web Security Reporting アプリケーションと CLI でも証明書がチェックされます。CLI では証明書をクライアントとして提示できないため、CLI 接続は機能しなくなります。

ステップ 5 web.conf を編集して同じルート CA で署名された証明書を提示して、Cisco Advanced Web Security Reporting アプリケーションがサーバに接続できるようにします。

以下は編集された設定スタンザの例です。

```
[settings]
enableSplunkWebSSL = true
privKeyPath = etc/auth/splunkweb/mySplunkWebPrivateKey.key
serverCert = etc/auth/splunkweb/mySplunkWebCertificate.pem
cipherSuite = <your chosen cipher suite (optional)>
```

（注） Cisco Advanced Web Security Reporting アプリケーションはパスワードをサポートしていないため、秘密キーからパスワードを削除する必要があります。

Cisco Advanced Web Security Reporting 認証のトラブルシューティング

証明書の構成を確認できない場合は、`$AWSR_HOME/var/log/splunk` の **web_service.log** を使用して、再起動時に発生するエラーを表示およびトラブルシューティングできます。

SSL構成の警告を探します。たとえば、`serverCert` で宣言されたサーバ証明書への誤ったパスを指定すると、Cisco Advanced Web Security Reporting アプリケーションの起動に失敗し、次のエラーが表示されます。

```
2010-12-21 16:25:02,804 ERROR [4d11455df3182e6710] root:442 - [Errno 2] No such file or directory: '/opt/splunk/share/splunk/mycerts/mySplunkWebCertificate.pem'
```

（注） `privKeyPath` で提供されている秘密キーがパスワードで保護されている場合、エラーは発生しませんが、ブラウザでは Cisco Advanced Web SecurityReporting アプリケーションがロードされません。