

# OpenAM 技術 Tips

## Vol.4

# Apache 2.4 と Web Policy Agent の設定手順

執筆者：株式会社オージス総研 小林 融

監修：OpenAM コンソーシアム

当技術 Tips コンテンツは、OpenAM コンソーシアム監修のもと、OpenAM コンソーシアム開発ワーキンググループに属する各企業の担当者により、執筆、編集されたものであり、各記事の著作権は執筆者に帰属いたします。

また、当記事のライセンスは、Creative Commons 4.0 の BY-NC-SA (表示、非営利、継承) とし、執筆者のクレジット(氏名、作品タイトル)を表示し、かつ非営利目的に限り、また改変を行った際には元の記事と同じ組み合わせの CC ライセンスで公開することを主な条件に、改変したり再配布したりすることができるものとします。

## 目次

1.	はじめに.....	3
2.	目的.....	4
3.	推奨環境.....	5
3.1.	OpenAM サーバー.....	5
3.2.	Web サーバー.....	5
4.	事前準備.....	6
4.1.	OpenAM サーバーの準備.....	6
4.2.	Web サーバーの準備.....	6
4.3.	Web Policy Agent のダウンロード.....	6
5.	OpenAM の設定.....	8
5.1.	エージェントプロファイルの作成.....	8
6.	Web サーバーへの Web Policy Agent 導入.....	13
6.1.	Apache の停止.....	13
6.2.	Web Policy Agent の配置.....	13
6.3.	エージェントプロファイル用パスワードファイルの作成.....	13
6.4.	Web Policy Agent のインストール.....	13
6.5.	インストール後処理.....	16
6.6.	Apache の起動.....	16
7.	動作確認.....	17
8.	おわりに.....	18
	参考資料.....	19

## 1. はじめに

本書では、「OpenAM 技術 Tips」の vol.1 から vol.3 を予め参照していることを前提としています。特に vol.1 は OpenAM を構築する手順について記載していますので、必ず参照してください。ただし、vol.1 で記載している OpenAM のバージョンや推奨環境については、本書の「3.推奨環境」を参考に読み替えてください。

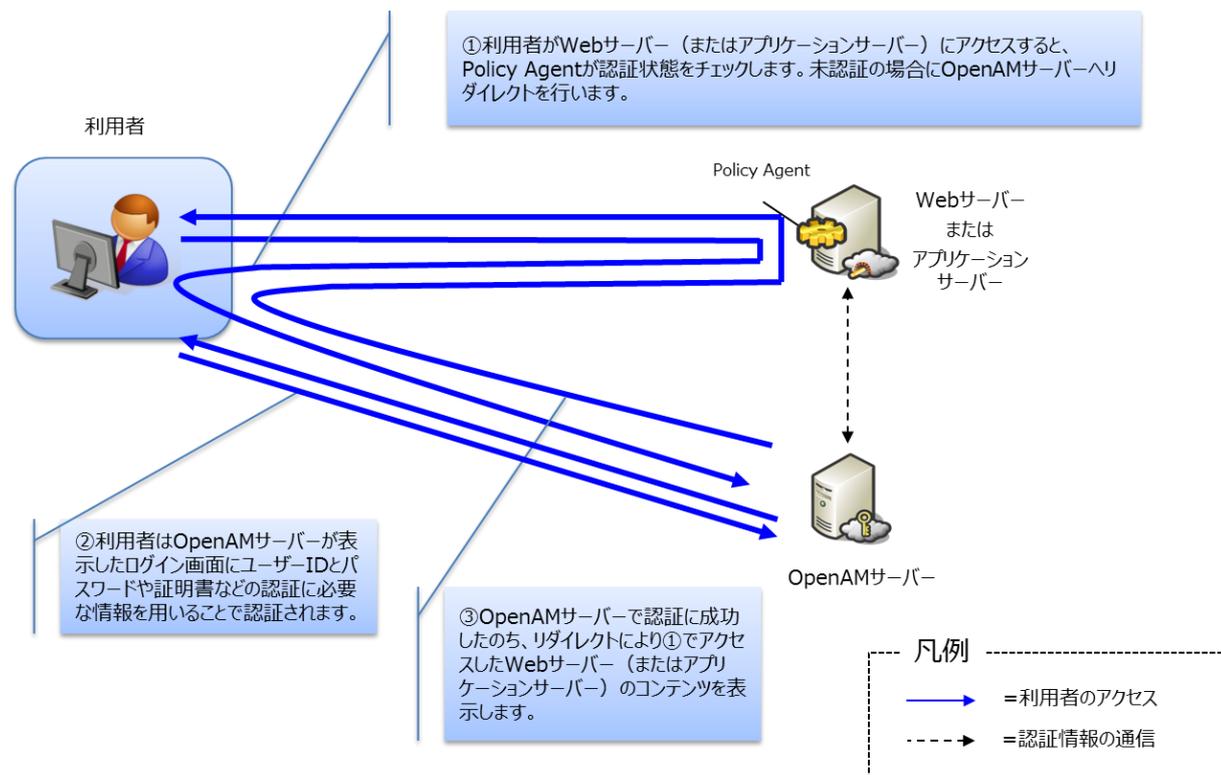
OpenAM は旧 Sun Microsystems 社の OpenSSO をベースに ForgeRock 社が開発を行うオープンソースソフトウェアであり、Web アプリケーションやクラウドサービスへのシングルサインオン(以降 SSO)を実現します。本資料では、既存の Web アプリケーションと SSO を行うための OpenAM と Web サーバーの設定について説明します。

OpenAM は Policy Agent と呼ばれる「エージェント」ソフトウェアを Web サーバーや Java アプリケーションサーバーへインストールすることで、Web アプリケーションへのアクセス時に、一元管理された認証、アクセス制御の機能を提供し、SSO を実現します。

Policy Agent には、Web サーバー用の Web Policy Agent とアプリケーションサーバー用の Java EE Policy Agent が存在します。

さらに Web Policy Agent には Microsoft Internet Information Services 向けと Apache HTTP Server(以降 Apache)向けが存在します。本書で扱う Web Policy Agent は Apache 向けとなります。

以下の図では、利用者が Web サーバー(またはアプリケーションサーバー)にアクセスした場合に、OpenAM サーバーと Policy Agent がどのような認証処理を行うかについて概要を記載しています。

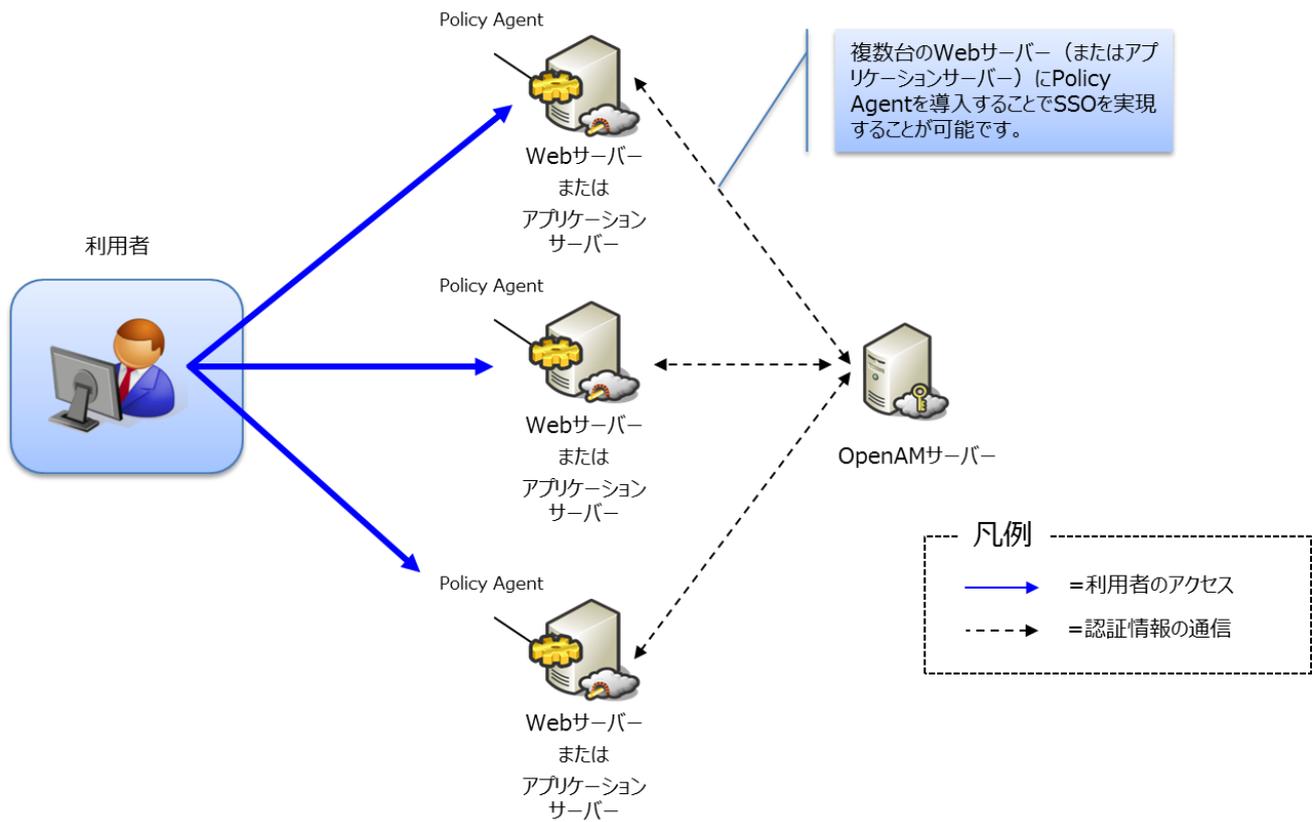


## 2. 目的

本構築手順を実施することで、Web アプリケーションへのアクセス時に認証を行うことができます。さらにアクセス時には認証のほかにアクセス制御を行うことができます。アクセス制御については、別の技術 Tips で取り扱います。

また、本構築手順を応用することで複数のアプリケーションでの SSO を実現することもできます。

以下の図では、複数の Web サーバー（またはアプリケーションサーバー）に Policy Agent を導入し SSO を実現している例を記載しています。



### 3. 推奨環境

本構築手順では、OpenAM サーバーと Web サーバーを使用します。

#### 3.1. OpenAM サーバー

OpenAM をインストールするサーバー環境の推奨環境は以下の通りです。

- ・サーバーOS: Linux, Windows, UNIX
- ・メモリ: 2GB 以上 (JVM ヒープサイズ)
- ・JDK: 1.7 以上 (OpenAM-13 の場合)
- ・アプリケーションコンテナ (例. Apache Tomcat, JBoss Application Server, ...etc)

詳細については ForgeRock 社サイト (OpenAM Release Notes) をご参照ください。[\[\\*1\]](#)

本構築手順では以下環境を前提としています。

- ・サーバーOS: Red Hat Enterprise Linux 7.2 (AWS 上)
- ・AWS サーバタイプ: t2.medium
- ・メモリ: 4GB
- ・CPU: 2vCPU
- ・JDK: OpenJDK 1.8.0
- ・アプリケーションコンテナ: Apache Tomcat 8.0.39

※OpenAM-13 は、Tomcat 8.5 系ではセッション Cookie の動作仕様が変更されたため、正常に動作しないことを確認していますので、Tomcat 8.0 系を使用してください。

- ・OpenAM: OpenAM-13.0.0.war

#### 3.2. Web サーバー

- ・サーバーOS: Red Hat Enterprise Linux 7.2 (AWS 上)
- ・AWS サーバタイプ: t2.small
- ・メモリ: 2GB
- ・CPU: 2vCPU
- ・Apache: Apache HTTP Server 2.4
- ・Web Policy Agent: Apache\_v24\_Linux\_64bit\_4.0.0

## 4. 事前準備

### 4.1. OpenAM サーバーの準備

Vol.1「OpenAM インストール手順」で構築された OpenAM サーバーを用意してください。

OpenAM サーバーを用意できましたら下記項目を確認してください。

項目	内容
ホスト名	ホスト名が「sso1.example.com」となっている
テストユーザー	testuser01 が登録されている

### 4.2. Web サーバーの準備

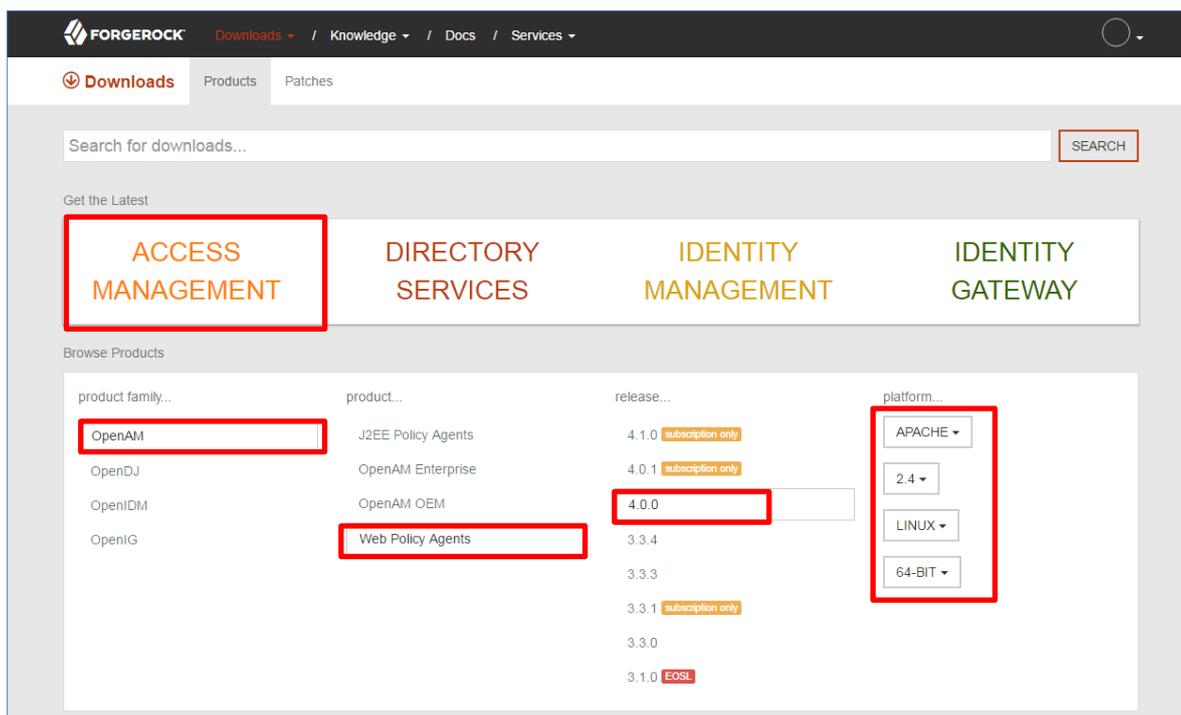
エージェントを導入する Web サーバーを用意していただき、OS および Apache のインストールまで準備してください。

項目	内容
ホスト名	ホスト名が「apl1.example.com」となっている
Apache	yum コマンドを使用して Apache をインストールしている
SELinux	OFF であること

### 4.3. Web Policy Agent のダウンロード

Web Policy Agent を OpenAM のサイトからダウンロードします。

OpenAM Download 画面 [\[\\*2\]](#) から [ACCESS MANAGEMENT]-[OpenAM]-[Web Policy Agents]-[4.0.0]-[APACHE]-[2.4]-[LINUX]-[64-BIT]と選択します。



[DOWNLOAD]ボタンが表示されるので、Web Policy Agent をダウンロードします。  
本手順書では “Apache\_v24\_Linux\_64bit\_4.0.0” がダウンロードされます。  
ダウンロードされたファイルを Web サーバーの「/tmp」に保存してください。

ACCESS MANAGEMENT

Web Policy Agents 4.0.0 › Apache 2.4 Linux (64-bit)

zip

Apache 2.4 Linux (64-bit) › **zip**

File name: Apache\_v24\_Linux\_64bit\_4.0.0.zip  
File size: 1.6 MB  
MD5 checksum: 7bf703c25c3039671a01ab90e71c1bd6

Accept Software License Agreement terms

**DOWNLOAD** • Release Notes • Documentation

FORGEROCK Copyright © 2010-2016 ForgeRock, all rights reserved. @fr\_backstage Report a problem Privacy Policy About Help

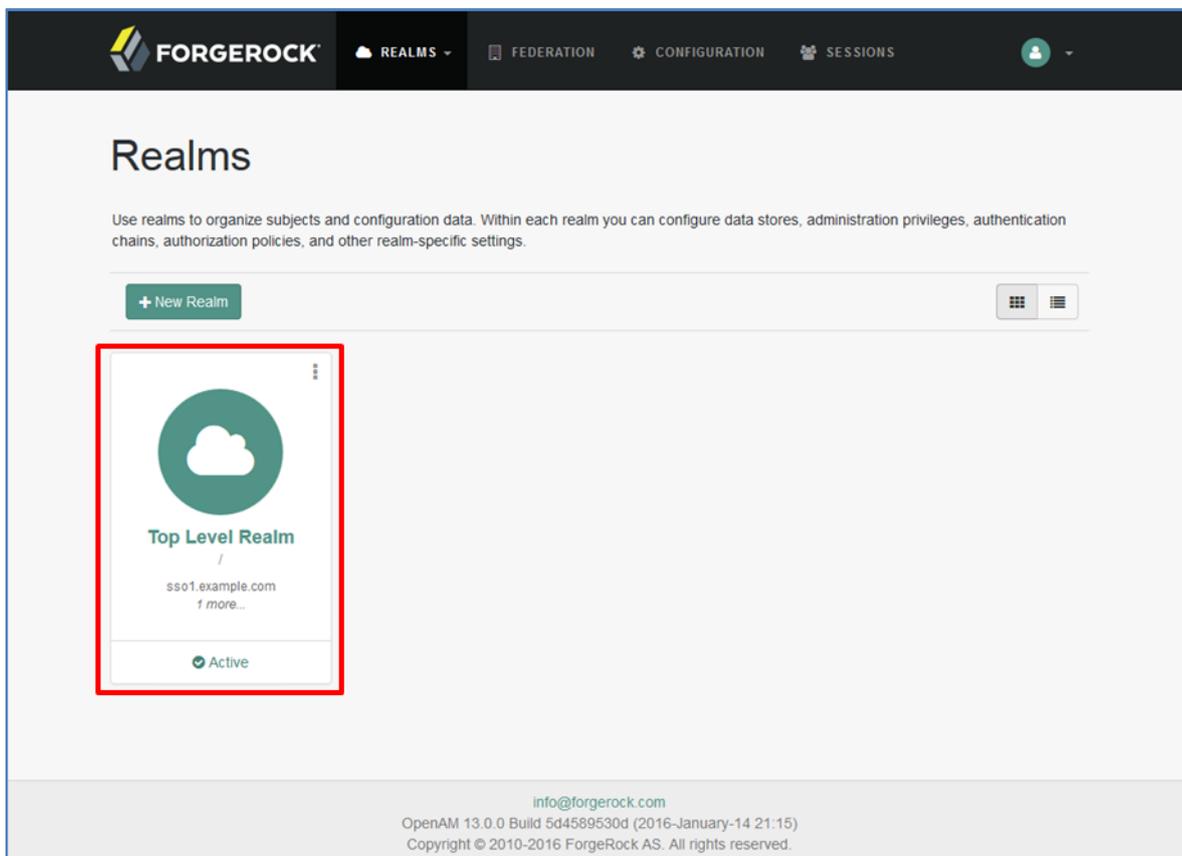
## 5. OpenAM の設定

OpenAM では、Web Policy Agent の設定を OpenAM サーバーで集中的に管理することができます。本手順では、OpenAM の設定画面で、Web Policy Agent の設定であるエージェントプロファイルを作成します。また、「SSO のみモード」と呼ばれるモードも設定します。このモードを設定することでアクセス制御を行わずに認証を行います。動作としては、認証された全てのユーザーが Web アプリケーションへアクセスすることができるようになります。

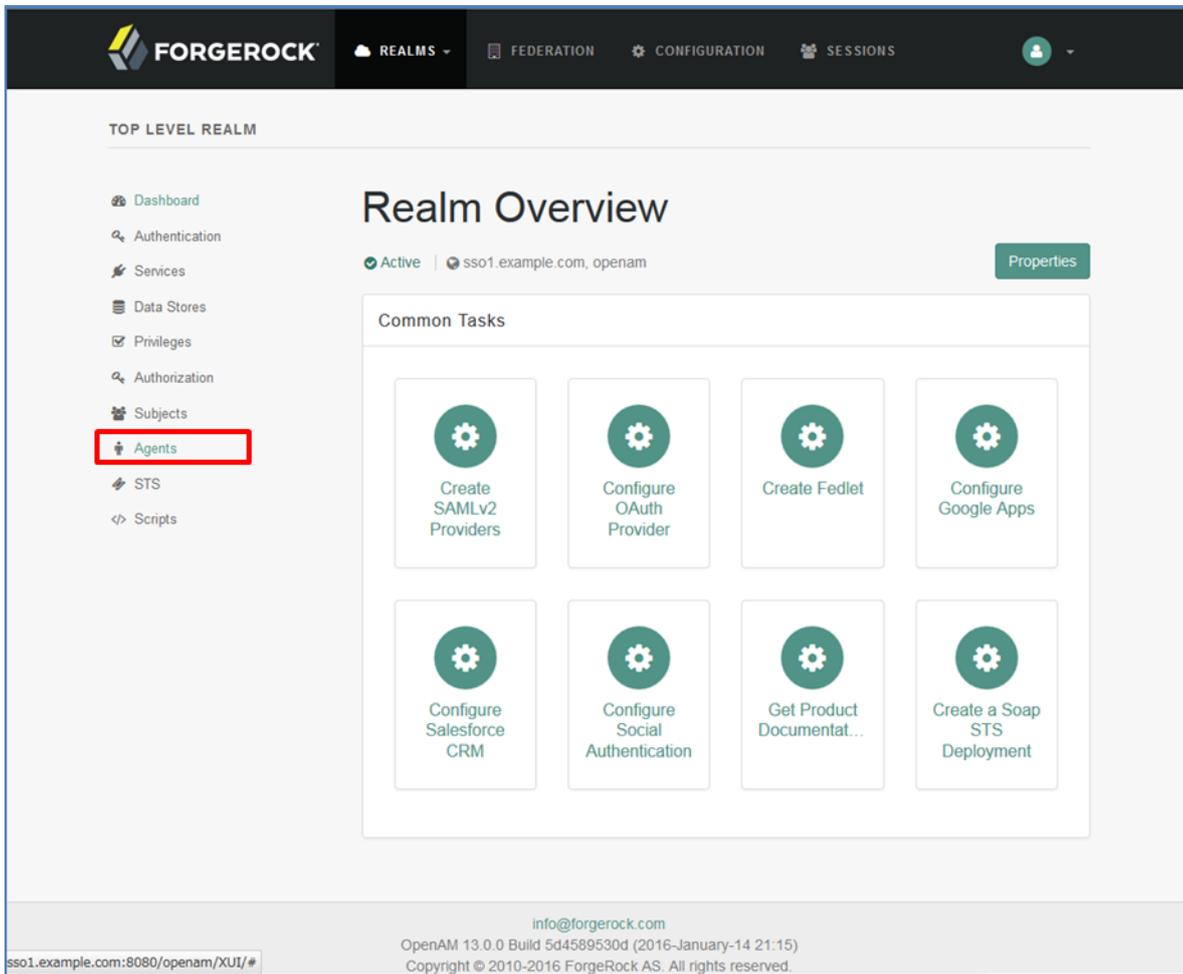
### 5.1. エージェントプロファイルの作成

クライアント上のブラウザから <http://sso1.example.com:8080/openam/> にアクセスし、管理者ユーザーである「amadmin」でログインを行い、トップ画面を表示します。

トップ画面で、[Top Level Realm] を選択します。



Realm Overview 画面の画面左にある[Agents]を選択します。



エージェント一覧のエージェントの [新規...] をクリックします。



Web Policy Agent の登録画面で、下表の設定のとおりに入力を行い、[作成] をクリックします。

項目	内容
名前	Web Policy Agent の名前です。本手順書では Web Policy Agent をインストールするサーバー名にします。ここでは、「agent01」とします。
パスワード	Web Policy Agent が OpenAM サーバーにアクセスするときのパスワード。本手順書では、パスワードに「kaE9%aow」を用います。セキュリティを考慮し 8 文字以上ランダム文字列としています。
パスワードの再入力	パスワードを再入力します。
設定	Web Policy Agent の設定を OpenAM サーバーで管理する場合は「集中」、Web サーバーのローカルファイルで管理する場合は「ローカル」を選択します。ここでは「集中」を選択します。
サーバー URL	OpenAM サーバーの URL を入力します。ポート番号を明示的に入力する必要があります。ここでは「http://sso1.example.com:8080/openam」とします。
エージェント URL	Web Policy Agent をインストールするサーバーの URL を入力します。OpenAM サーバーから Web Policy Agent に設定やポリシーの更新を通知し、即時に反映するために使われます。ここでは、「http://apl1.example.com:80」とします。

先ほど作成したエージェントをエージェント一覧から選択します。

The screenshot shows the OpenAM console interface. At the top, there is a navigation bar with tabs for '一般', '認証', 'サービス', 'データストア', '権限', 'ポリシー', '対象', 'エージェント', 'STS', and 'Scripts'. The 'エージェント' tab is selected. Below the navigation bar, there is a sub-menu with tabs for 'Web', 'J2EE', '2.2 エージェント', 'OAuth 2.0 クライアント', 'エージェント認証', and 'SOAP STS Agent'. The 'Web' tab is selected. The main content area shows the 'Web' agent configuration page. It includes a search bar, a section for 'エージェント (1 エージェント)' with a table listing the 'agent01' agent, and a section for 'グループ (0 グループ)'. The 'agent01' agent is highlighted with a red box.

バージョン ログアウト  
ユーザー: amAdmin サーバー: sso1.example.com

**FORGEROCK**

一般 認証 サービス データストア 権限 ポリシー 対象 エージェント STS Scripts

Web J2EE 2.2 エージェント OAuth 2.0 クライアント エージェント認証 SOAP STS Agent

/ (最上位のレルム)

**Web** [アクセス制御へ戻る](#)

Web エージェントは、Apache Web Server や Microsoft IIS などの Web サーバーを保護します。

\*

**エージェント (1 エージェント)**

<input checked="" type="checkbox"/>	名前	リポジトリの場所
<input checked="" type="checkbox"/>	agent01	集中

\*

**グループ (0 グループ)**

名前

エンティティがありません。

エージェントプロファイルの編集画面が表示されるので、「SSOのみモード」の「有効」にチェックを行い、[保存] をクリックします。

バージョン
ログアウト

ユーザー: amAdmin
サーバー: sso1.example.com

グローバル
アプリケーション
SSO
OpenAM サービス
その他
高度

### agent01 の編集

[保存](#)
[リセット](#)
[メインページに戻る](#)

継承設定値
設定ダンプ

✖ プロファイル
✖ 監査

✖ 一般
✖ 完全修飾ドメイン名の確認

\* 必須入力フィールド

#### プロファイル

グループ:

\* パスワード:

\* パスワード (確認):

#### 一般

SSO のみモード:  有効  
エージェントはポリシーの認証 (SSO) のみを実施し、承認を実施しません。(プロパティ名: com.sun.identity.agents.config.sso.only)  
 ホットスワップ: 有効

リソースアクセス拒否 URL:   
カスタマイズされたアクセスが拒否されるページの URL。(プロパティ名: com.sun.identity.agents.config.access.denied.uri)  
 ホットスワップ: 有効

エージェントデバッグレベル:   
 すべて  
 エラー  
 メッセージ  
 情報  
 警告  
エージェントのデバッグレベル。(プロパティ名: com.sun.identity.agents.config.debug.level)  
 ホットスワップ: 有効

エージェントのデバッグファイルローテーション:  有効  
デバッグファイルは指定されたサイズに基づいてローテーションされます。(プロパティ名: com.sun.identity.agents.config.debug.file.rotate)  
 ホットスワップ: 有効

エージェントのデバッグファイルサイズ:   
エージェントのデバッグファイルサイズ (バイト単位)。(プロパティ名: com.sun.identity.agents.config.debug.file.size)  
 ホットスワップ: 有効

✧ 先頭に戻る

## 6. Web サーバーへの Web Policy Agent 導入

Web Policy Agent のインストールを行います。

Web Policy Agent の詳細を確認したい場合は、OpenAM Web Policy Agent User's Guide [\[\\*3\]](#)を参照ください。

### 6.1. Apache の停止

Apache が起動していると、Web Policy Agent 本体インストールが途中で止まってしまうため、予め Apache を停止します。

Apache を停止します。

```
$ sudo systemctl stop httpd
```

Apache が停止したことを確認します。「Active: inactive (dead)」という表示があるか確認してください。

```
$ sudo systemctl status httpd
```

### 6.2. Web Policy Agent の配置

ダウンロードした zip ファイルを展開します。zip ファイルを展開した場所が、インストール先になるため、先にインストール先のディレクトリを作ってから 展開します。

以下のコマンドを実行し、「/opt」の下に「openam」ディレクトリを作成します。

```
$ sudo mkdir /opt/openam
```

「/tmp」に保存した Apache\_v24\_Linux\_64bit\_4.0.0.zip を展開します。

```
$ sudo unzip /tmp/ Apache_v24_Linux_64bit_4.0.0.zip -d /tmp/
```

「/tmp/web\_agents」配下のディレクトリ「apache24\_agent」を「/opt/openam」配下にコピーします。

```
$ sudo cp -r /tmp/web_agents/apache24_agent /opt/openam
```

### 6.3. エージェントプロファイル用パスワードファイルの作成

Web Policy Agent のインストールで使用するパスワードファイルを作成します。

エージェントプロファイル作成時に設定したパスワードと同じ値を利用してください。本手順書では、例としてパスワードに「kaE9%aow」を用います。

```
$ sudo echo kaE9%aow > /tmp/pwd.txt
```

```
$ sudo chmod 400 /tmp/pwd.txt
```

### 6.4. Web Policy Agent のインストール

「/opt/openam/apache24\_agent」配下のディレクトリ「bin」に移動します。

```
$ cd /opt/openam/apache24_agent/bin
```

agentadmin コマンドを使用し、Web Policy Agent のインストールを開始します。

```
$ sudo ./agentadmin --i
```

インストール開始前にライセンスを確認し、「yes」を入力します。

Please read the following License Agreement carefully:

```
READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING
THE FORGEROCK SOFTWARE, YOU, ON BEHALF OF YOURSELF AND YOUR COMPANY, AGREE TO
. . .
```

```
Do you completely agree with all the terms and conditions
of this License Agreement (yes/no): [no]: yes
```

以下のように表示されるので、<Apache の設定ファイルのパス>として「/etc/httpd/conf/httpd.conf」を入力します。

```
Enter the complete path to the httpd.conf file which is used by Apache HTTP
Server to store its configuration.
[ q or 'ctrl+c' to exit ]
Configuration file [/opt/apache/conf/httpd.conf]: /etc/httpd/conf/httpd.conf
```

Web サーバーのユーザーおよびグループで関連ディレクトリを作成するように設定します。ここでは「yes」を入力します。

```
Change ownership of created directories using User and Group settings in httpd.conf
[ q or 'ctrl+c' to exit ]
(yes/no): [no]:yes
```

OpenSSOAgentBootstrap.properties ファイルの上書き確認です。初期導入時にはファイルが存在しないため、ここでは何も入力せず、[Enter]キーを押下します。

```
To set properties from an existing configuration enter path to file
[ q or 'ctrl+c' to exit, return to ignore ]
Existing OpenSSOAgentBootstrap.properties file: [Enter]
```

以下のように表示されるので、OpenAM サーバーの情報 (http<s>://<OpenAM サーバーの FQDN>:<ポート番号>/<パス>)として「http://sso1.example.com:8080/openam」を入力します。

```
Enter the URL where the OpenAM server is running. Please include the
deployment URI also as shown below:
(http://openam.example.com:58080/openam)
[ q or 'ctrl+c' to exit ]
OpenAM server URL: http://sso1.example.com:8080/openam
```

以下のように表示されるので、Web サーバーの情報 (http<s>://<Web サーバーの FQDN>:<ポート番号>)として「http://apl1.example.com:80」を入力します。

```
Enter the Agent URL as shown below:
```

```
(http://agent.example.com:1234)
```

```
[ q or 'ctrl+c' to exit ]
```

```
Agent URL: http://apl1.example.com:80
```

以下のように表示されるので、OpenAM サーバーに登録したエージェントの名前と同じ「agent01」を入力します。

```
Enter the Agent profile name
```

```
[ q or 'ctrl+c' to exit ]
```

```
Agent Profile name: agent01
```

エージェントプロファイルを設定した Realm を選択します。本手順書では Top Level Realm を使用しているため「/」を入力します。

```
Enter the Agent realm/organization
```

```
[ q or 'ctrl+c' to exit ]
```

```
Agent realm/organization name: [/]:/
```

以下のように表示されるので、事前に作成したエージェントプロファイル用パスワードファイルのパス「/tmp/pwd.txt」を入力します。

```
Enter the path to a file that contains the password to be used
```

```
for identifying the Agent
```

```
[ q or 'ctrl+c' to exit ]
```

```
The path and name of the password file: /tmp/pwd.txt
```

以下のように表示されるので、入力内容を確認し、インストールを継続するため「yes」と入力します。

```
Installation parameters:
```

```
OpenAM URL: http://sso1.example.com:8080/openam
```

```
Agent URL: http://apl1.example.com:80
```

```
Agent Profile name: agent01
```

```
Agent realm/organization name: /
```

```
Agent Profile password source: /tmp/pwd.txt
```

```
Confirm configuration (yes/no): [no]: yes
```

「Installation complete.」が表示されることを確認します。

```
Validating...
```

```
Validating... Success.
```

```
Cleaning up validation data...
```

```
Creating configuration...
```

```
Installation complete.
```

## 6.5. インストール後処理

Web Policy Agent のパスワードファイルを削除します。

```
$ sudo rm -f /tmp/pwd.txt
```

Web Policy Agent のパッケージを削除します

```
$ sudo rm -rf /root/web_agents
```

コマンドライン履歴にパスワードが残っているので、削除しておきます。

```
$ history -c
```

## 6.6. Apache の起動

Apache を起動します。

```
$ sudo systemctl start httpd
```

Apache が起動したことを確認します。「Active: active (running)」という表示があるか確認してください。

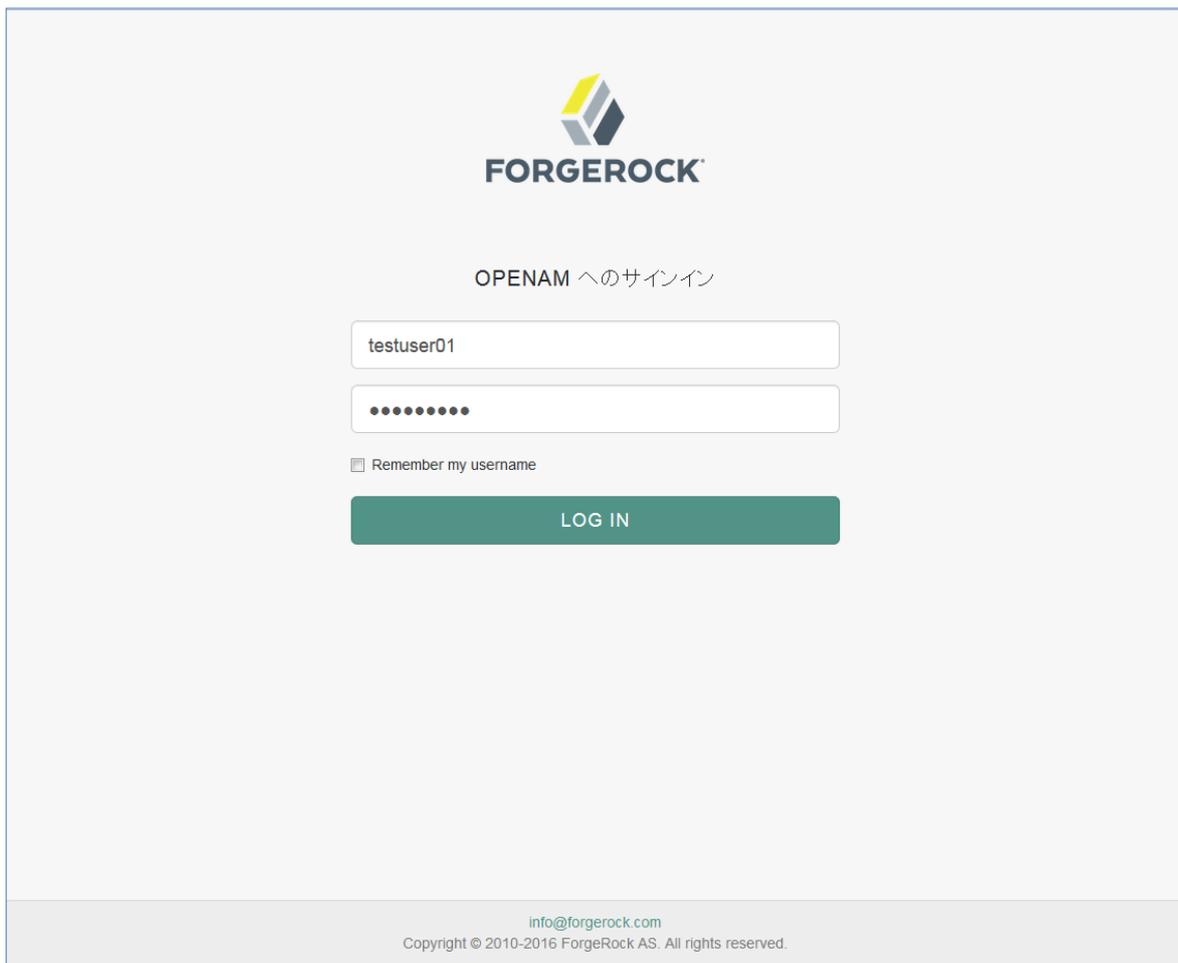
```
$ sudo systemctl status httpd
```

## 7. 動作確認

クライアント上のブラウザから <http://apl1.example.com> にアクセスします。



Web サーバーの画面が表示されるのではなく、OpenAM の認証画面が表示されます。ユーザー「testuser01」でログインします。

A screenshot of the OpenAM login page. At the top center is the FORGEROCK logo, which consists of a stylized 'F' made of three overlapping shapes in yellow, grey, and blue. Below the logo is the text "FORGEROCK". Underneath that is the heading "OPENAM へのサインイン". There are two input fields: the first contains the username "testuser01", and the second contains a password represented by ten dots. Below the password field is a checkbox labeled "Remember my username". At the bottom of the form is a green button with the text "LOG IN". At the very bottom of the page, there is a footer with the email address "info@forgerock.com" and the copyright notice "Copyright © 2010-2016 ForgeRock AS. All rights reserved."

ログイン後、Web サーバーの画面が表示されます。

**Red Hat Enterprise Linux Test Page**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

<p><b>If you are a member of the general public:</b></p> <p>The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.</p> <p>If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.</p> <p>For example, if you experienced problems while visiting <code>www.example.com</code>, you should send e-mail to "<code>webmaster@example.com</code>".</p> <p>For information on Red Hat Enterprise Linux, please visit the <a href="#">Red Hat, Inc. website</a>. The documentation for Red Hat Enterprise Linux is <a href="#">available on the Red Hat, Inc. website</a>.</p>	<p><b>If you are the website administrator:</b></p> <p>You may now add content to the directory <code>/var/www/html/</code>. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file <code>/etc/httpd/conf.d/welcome.conf</code>.</p> <p>You are free to use the image below on web sites powered by the Apache HTTP Server:</p> <div style="text-align: center;"></div>
--	---

## 8. おわりに

・今回は、Web Policy Agent を利用した認証が可能になるまでの OpenAM の設定手順を紹介しましたが、OpenAM の Policy Agent には Microsoft Internet Information Services 向けの「Web Policy Agent」や、Apache Tomcat や JBoss Application Server など Java EE 準拠のアプリケーションサーバー向けの「Java EE Policy Agent」があります。引き続き OpenAM の検証を行う場合は、公開されたマニュアル等[\*4]をご参照ください。

参考資料

[\*1]

OpenAM 13 Release Notes

<https://backstage.forgerock.com/docs/openam/13/release-notes>

[\*2]

OpenAM Download

<https://backstage.forgerock.com/downloads/OpenAM>

[\*3]

OpenAM Web Policy Agent v4 User's Guide

<https://backstage.forgerock.com/docs/openam-web-policy-agents/4/web-users-guide>

[\*4]

OpenAM 13 Installation Guide

<https://backstage.forgerock.com/docs/openam/13/install-guide>