

OpenAM 技術 Tips

Vol.1

OpenAM インストール手順

執筆者：株式会社オージス総研 浜口 ゆう

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。

1. はじめに

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を実現します。本資料では、この OpenAM を用いて、ユーザー認証が可能になるまでの検証を目的とした 簡単な構築手順を紹介します。

はじめに、OpenAM の基本的な認証の仕組みを説明します。

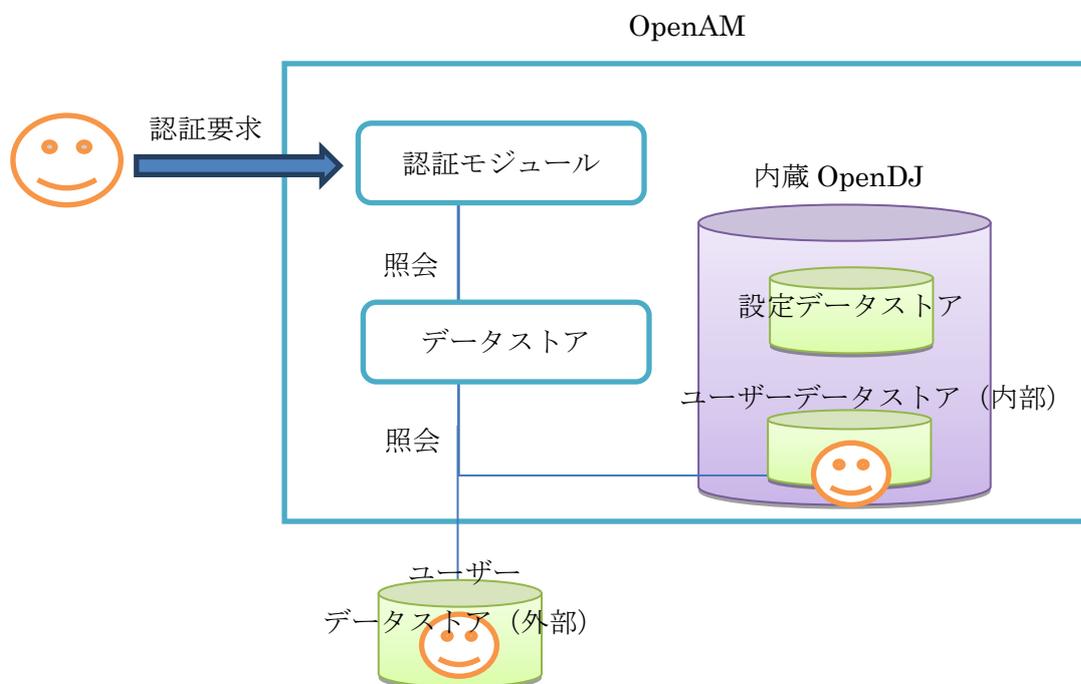
OpenAM には認証処理を担当する「認証モジュール」と、ユーザー情報の参照や保存を担当する「データストア」と呼ばれるコンポーネントがあります。

デフォルトの設定で OpenAM を構築すると、認証モジュールには「DataStore」が使用され、データストアには OpenAM の内蔵 OpenDJ をユーザーデータストアとして使用する設定が登録されています。「DataStore」認証モジュールは、設定されたデータストアを利用して認証を行うモジュールです。つまり、デフォルト構成では内蔵 OpenDJ 内に格納されたユーザーデータストアを参照して認証を行うことになります。

このように認証モジュールとデータストアが分かれているため、認証方式だけを変更することが可能です。例えば、ワンタイムパスワードを利用する認証モジュールなどが標準で用意されています。また、データストアについても汎用 LDAP や Active Directory 用の設定が用意されており、参照先のデータストアを切り替え可能になっています。

本資料では、データストアに外部のユーザーデータストアである OpenLDAP を追加し、OpenLDAP に登録されたユーザーで認証を行うための設定手順をこの後で紹介します。

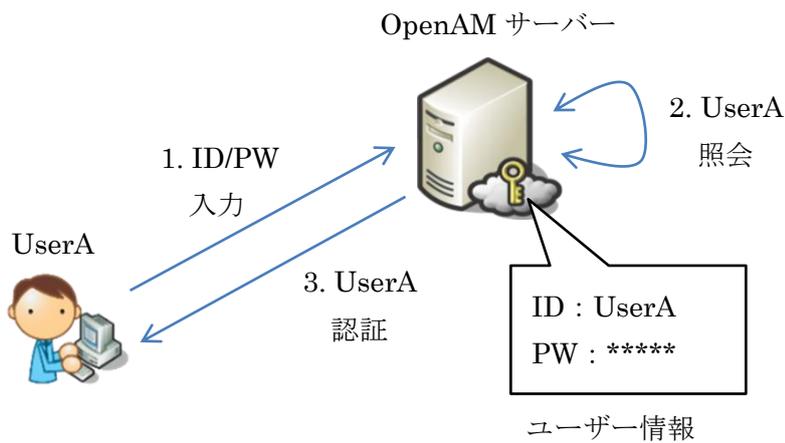
なお、OpenAM の内蔵 OpenDJ には、OpenAM の設定情報も格納されており、これを設定データストアと呼びます。



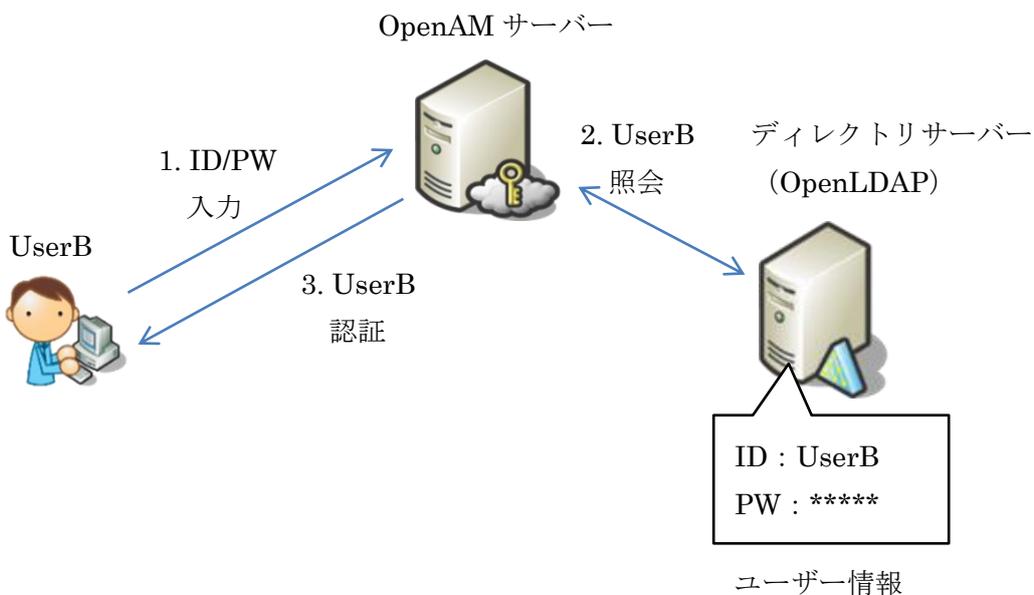
2. 目的

本構築手順を実施する事で、ディレクトリサーバーに登録されたユーザーで OpenAM サーバーにユーザー認証する事が可能になる事を目的とします。ディレクトリサーバーとして、内部ユーザーデータストアを用いる場合と、外部ユーザーデータストアを用いる場合の 2 種類の方法を紹介します。

・内部ユーザーデータストアを用いる場合



・外部ユーザーデータストア (OpenLDAP) を用いる場合



3. 推奨環境

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: 1.6 以上
- ・アプリケーションコンテナ (例. Apache Tomcat, JBoss, …etc)

詳細については ForgeRock 社サイト (OpenAM Release Notes) をご参照下さい。

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: CentOS 6.5
- ・メモリ: 2GB
- ・JDK: OpenJDK 1.7.0_71
- ・アプリケーションコンテナ: Apache Tomcat 6.0.24
- ・OpenAM: OpenAM-13.0.0-SNAPSHOT_20141202.war

4. 事前準備

OpenAM をインストールするために、サーバー環境のセットアップを行います。また、本構築手順では OpenAM サーバーを以下の環境で構築します。

項目	値
ホスト名	sso1.example.com
IP アドレス	192.168.0.11

・ホスト名の確認

OpenAM サーバーのホスト名が上記 FQDN であるかどうかを確認し、必要であれば変更します。

(下記#はプロンプトを意味し、コマンドを root 権限で実行する事を意味します。以降同様の意です。)

```
# vi /etc/sysconfig/network
```

(下記内容で編集)

```
HOSTNAME=sso1.example.com
```

・hosts ファイルの編集

OpenAM サーバーのローカル hosts ファイルを編集します。

```
# vi /etc/hosts
```

(下記内容で編集)

```
127.0.0.1 localhost
192.168.0.11 sso1.example.com sso1
```

・ファイアウォール、SELinux の無効化

本構築手順の簡略化のために、ファイアウォール、及び SELinux を無効化します。設定変更後、OpenAM サーバーの再起動が必要です。

```
# service iptables stop
```

```
# service ip6tables stop
```

```
# chkconfig iptables off
```

```
# chkconfig ip6tables off
```

```
# vi /etc/sysconfig/selinux
```

(下記内容で編集)

```
SELINUX=disabled
```

・OS の時刻同期

OS の時刻同期設定をしておく事を推奨します。時刻同期は今後 OpenAM にて SAML 構成を行う場合に必須になります。

・OpenAM サーバーの再起動

上記設定を実施後、OpenAM サーバーの再起動を実施して下さい。

```
# shutdown -r now
```

・JDK インストール

OpenAM がデプロイされる Apache Tomcat を起動するために Java をインストールします。

```
# yum -y install java-1.7.0-openjdk
```

Java のバージョン情報が正しく表示される事を確認して下さい。

```
# java -version
```

```
java version "1.7.0_71"
```

5. Apache Tomcat セットアップ

・Apache Tomcat インストール

Apache Tomcat を yum コマンドでインストールします。

```
# yum -y install tomcat6
```

・ファイルディスクリプタの設定

ファイルディスクリプタの最大値を上げて置く事を推奨します

```
# vi /etc/security/limits.conf
```

(下記内容を追加)

```
tomcat soft nofile 65536
tomcat hard nofile 131072
```

同様に、OS のファイルディスクリプタ最大値も確認して下さい。

```
# cat /proc/sys/fs/file-max
```

(例)165648

もし、上記最大値が低すぎる場合は、/etc/sysctl.conf を編集し、カーネルのパラメーターである fs.file-max を、より高い最大値に設定して下さい。(設定の反映には sysctl -p コマンドを実行します。)

・URL 文字化け対策

Apache Tomcat のリクエスト URL 文字化け対策として server.xml を編集します。

```
# vi /etc/tomcat6/server.xml
```

(Connector タグに下記内容を追加)

```
<Connector port="8080" protocol="HTTP/1.1"
  ... (設定略)
  URIEncoding="UTF-8" />
```

・JVM ヒープサイズの変更

Apache Tomcat の JVM ヒープサイズを確保します。

```
# vi /etc/sysconfig/tomcat6
```

(下記内容で編集)

```
JAVA_OPTS="-server -Xmx2048m -XX:MaxPermSize=256m"
```

・OpenAM デプロイ

ForgeRock 社サイトより Nightly Build の OpenAM ファイルをダウンロードします。
詳細については ForgeRock 社サイト (OpenAM Nightly Builds) をご参照下さい。

本構築手順ではファイル名を下記のとおり表記します。

OpenAM-13.0.0-SNAPSHOT_20141202.war

ダウンロードした OpenAM ファイルを Apache Tomcat のデプロイ用ディレクトリ配下にファイル名を”openam.war”
として配置します。

```
# cp OpenAM-13.0.0-SNAPSHOT_20141202.war /var/lib/tomcat6/webapps/openam.war  
# chown .tomcat /usr/share/tomcat6/
```

・Apache Tomcat 起動

Apache Tomcat のサービスを起動します。

```
# service tomcat6 start
```

```
Starting tomcat6: [ OK ]
```

Apache Tomcat の起動が成功すると、Apache Tomcat の /var/log/tomcat6/catalina.out ログに下記行のよう
なログが出力されます。

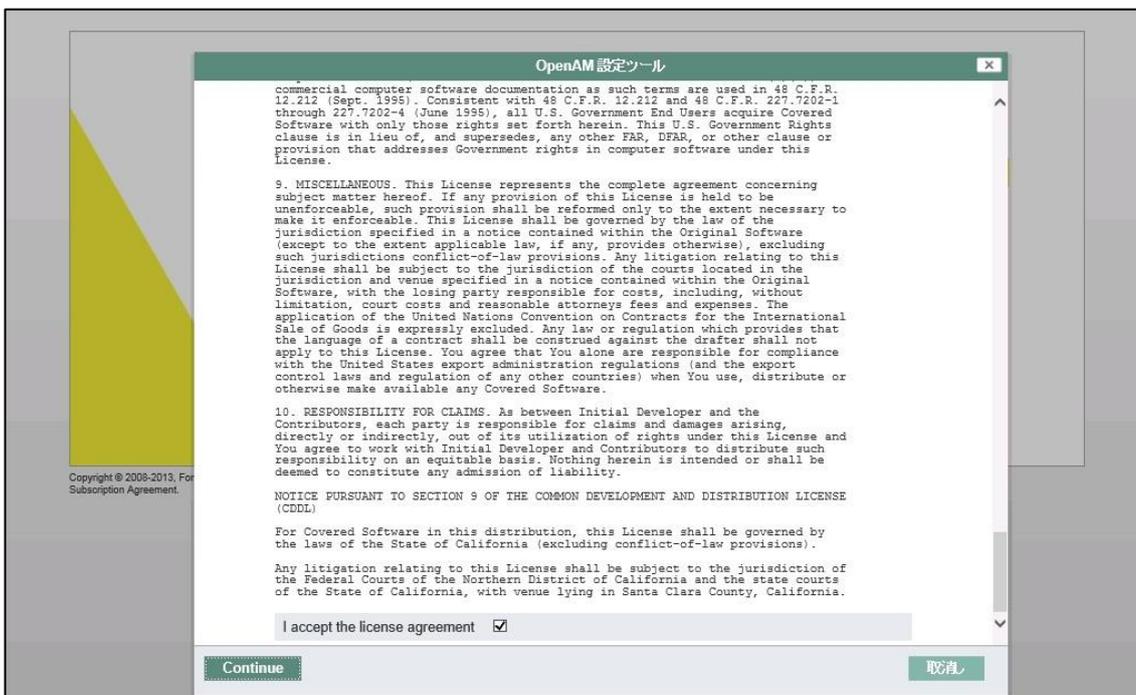
```
Dec 04, 2014 7:00:30 AM org.apache.catalina.startup.Catalina start  
INFO: Server startup in 35537 ms
```

6. OpenAM セットアップ

クライアントブラウザから <http://sso1.example.com:8080/openam/> にアクセスすると、以下画面が表示されるので、「新しい設定の作成」をクリックします。



ソフトウェアライセンス同意画面が表示されるので、同意する場合は、「I accept the license agreement」にチェックして「Continue」をクリックします。



デフォルトの管理者アカウント(amAdmin)のパスワードを入力します。パスワード長は 8 文字以上必要です。



The screenshot shows the 'OpenAM 設定ツール' (OpenAM Configuration Tool) window. The main title is 'カスタム設定オプション' (Custom Configuration Options). On the left, there is a navigation menu with the following items: 1. 一般 (General), 2. サーバー設定 (Server Settings), 3. 設定ストア (Configuration Store), 4. ユーザーストア (User Store), 5. サイト設定 (Site Settings), 6. エージェント情報 (Agent Information), and 7. 概要 (Summary). The '一般' (General) option is selected and highlighted in yellow. The main content area is titled '手順 1: 一般' (Step 1: General) and contains the following text: 'デフォルトユーザー amAdmin のパスワードを入力します。パスワード長は 8 文字以上にする必要があります。この設定が既存の配備の一部になる場合は、入力するパスワードを元の配備のパスワードと一致させてください。' (Enter the password for the default user amAdmin. The password length must be 8 characters or more. If this configuration becomes part of an existing deployment, please ensure the password matches the original deployment password.) Below this text, there is a section titled 'デフォルトユーザーパスワード' (Default User Password) with the following fields: 'デフォルトユーザー [amAdmin]' (Default User [amAdmin]), '*パスワード' (Password) with a text input field and a '7 桁' (7 characters) indicator, and '*パスワードの確認' (Confirm Password) with a text input field. At the bottom of the window, there are three buttons: '戻る' (Back), '次へ' (Next), and '取消し' (Cancel).

サーバー設定画面にて、サーバーURL、Cookie ドメイン、プラットフォームロケール、設定ディレクトリの設定を行います。サーバーURL は”localhost”や IP アドレスではなく、必ず FQDN を指定するようにして下さい。設定ディレクトリは、指定したパス配下に OpenAM の設定が保存されていきます。本構築手順では以下のように設定します。

- ・Server URL: http://sso1.example.com:8080
- ・Cookie Domain: .example.com
- ・Platform Locale: en_US
- ・Configuration Directory: /usr/share/tomcat6/openam



設定データストア設定を行います。本構築手順では変更の必要はありません。



ユーザーデータストア設定は、内部データストアである「OpenAM ユーザーデータストア」を選択します。(※外部ユーザーデータストアと接続する場合は、インストール後に別途行う事を推奨します。)



サイト設定を行います。本構築手順では変更の必要はありません。



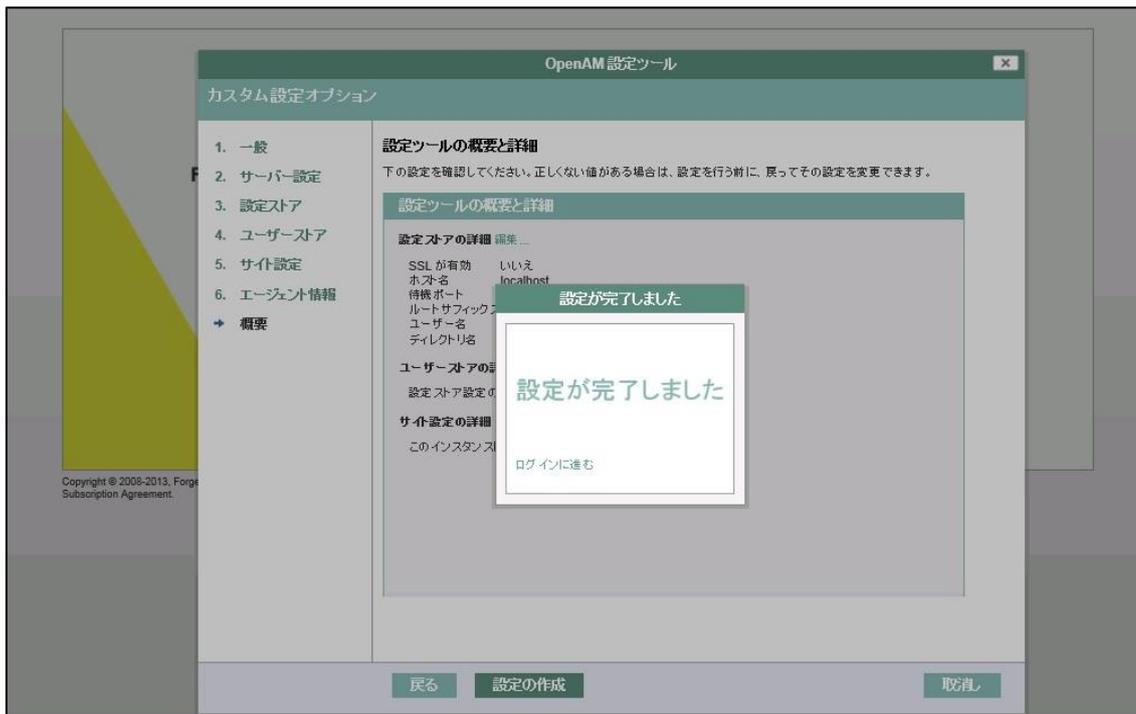
ポリシーエージェントユーザーのパスワードを入力します。パスワード長は 8 文字以上で、且つ管理者アカウント (amAdmin)のパスワードと異なる必要があります。



設定ツールの概要と詳細を確認して、問題なければ「設定の作成」ボタンをクリックして下さい。OpenAM 設定の作成が開始されます。



OpenAM 設定の作成が完了すると、以下画面が表示されます。

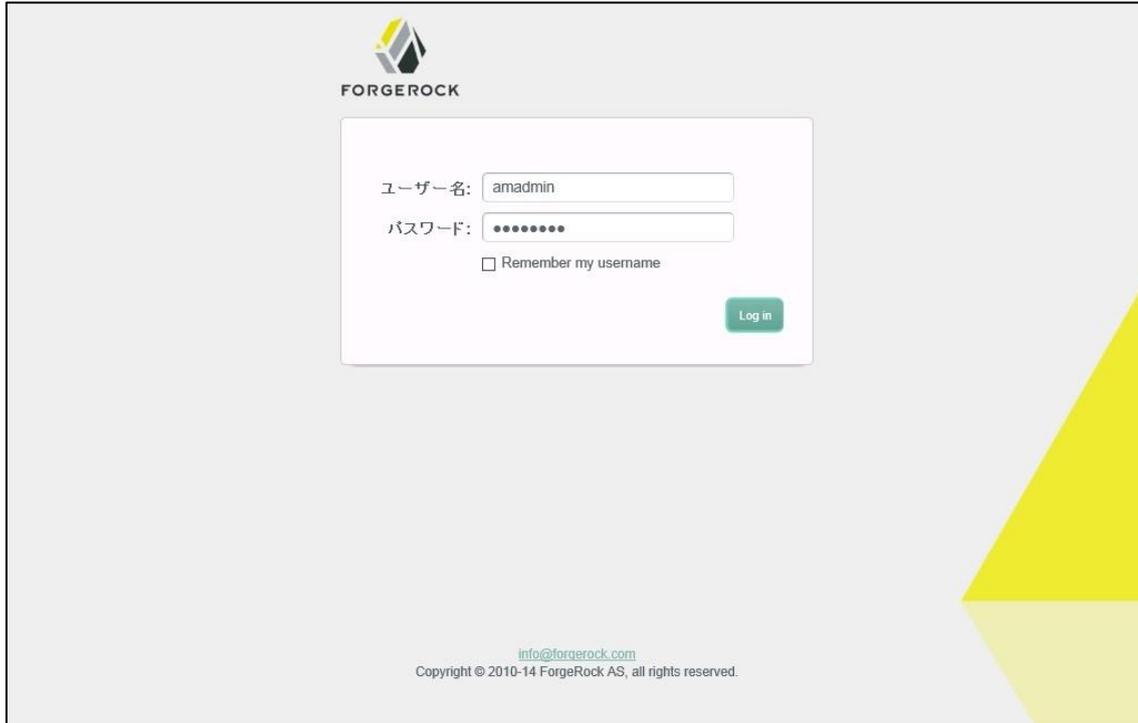


上記インストールに失敗し、再インストールを行いたい場合は、下記ディレクトリを削除する必要があります。

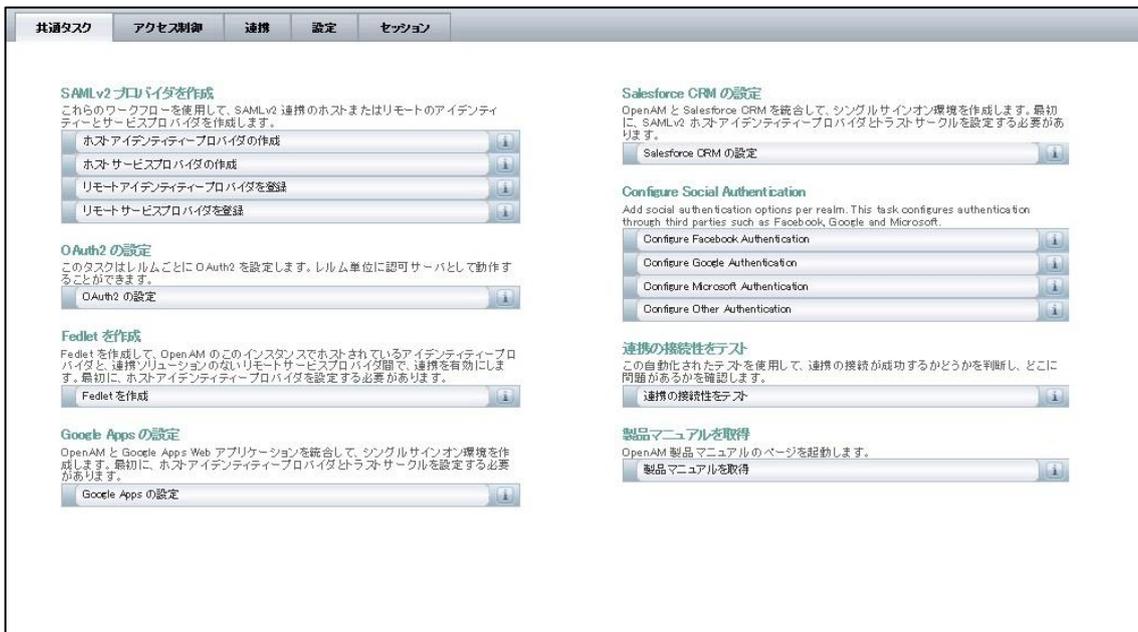
```
# service tomcat6 stop
```

```
# rm -rf /usr/share/tomcat6/openam/ /usr/share/tomcat6/.openamcfg/
```

http://sso1.example.com:8080/openam/にアクセスすると、OpenAM ログインページにアクセスする事ができます。管理者アカウント(amAdmin)でログインする事で、OpenAM 管理トップ画面にログインする事ができます。



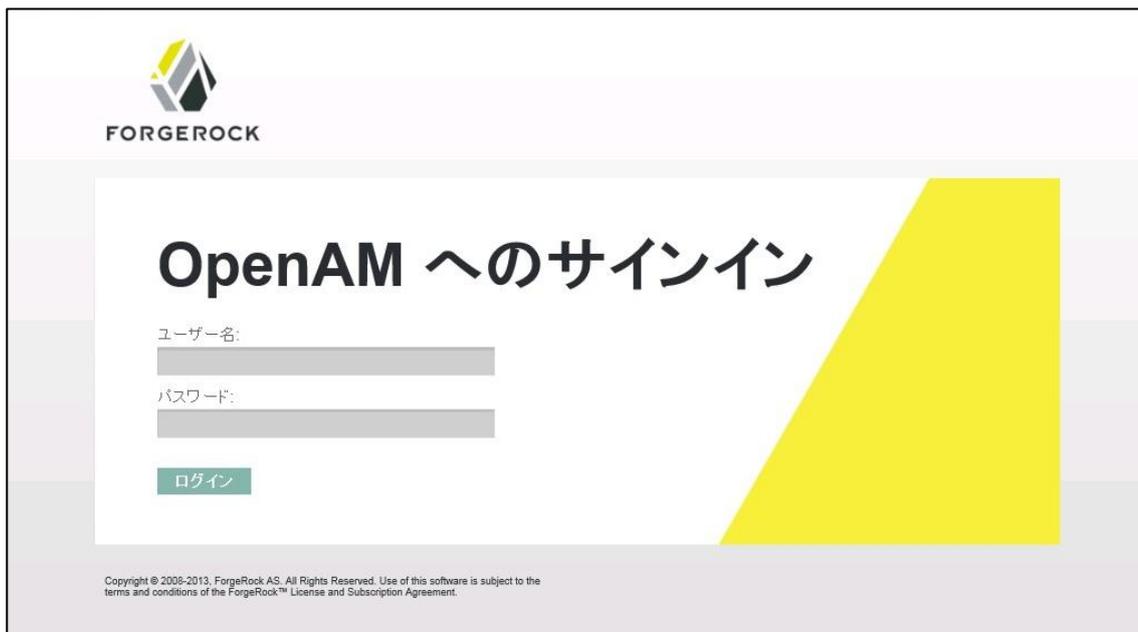
管理トップ画面



また、OpenAM の Nightly Build 版を利用する場合は、XUI 機能を無効化する事を推奨します。XUI を無効化するには、OpenAM 管理トップ画面より、「設定」>「認証」>「コア」に遷移して、「XUI インターフェイス」を無効にして下さい。

新しい値 <input type="text"/> <input type="button" value="追加"/>	
↑ 認証に使用されるLDAP 接続プールのサイズを制御します。	
LDAP デフォルトの接続プールサイズ:	<input type="text" value="1:10"/> デフォルトの接続プールサイズ、形式: 最小値:最大値
リモート認証セキュリティ:	<input type="checkbox"/> 有効 ↑ 各要求とともにアプリケーション SSO トークンを送信するにはリモート認証クライアントが必要です。
ログアウト処理のポストプロセスオブジェクトを保持:	<input type="checkbox"/> 有効 ↑ セッションの持続のためポストプロセスクラスを格納します。
ログアウト処理の認証モジュールオブジェクトを保持:	<input type="checkbox"/> 有効 ↑ 認証モジュールインスタンスは、ユーザーのセッションに格納されます。
XUI インターフェイス:	<input type="checkbox"/> 有効 ↑ XUI を OpenAM のデフォルト インターフェイスにするかどうかを決定します。

XUI 無効化後のログイン画面



7. 内部ユーザーデータストア認証

OpenAM の内部ユーザーデータストアを利用して認証する場合の手順を記述します。

OpenAM 管理トップ画面よりアクセス制御タブに遷移すると、OpenAM のレルム選択画面が表示されます。OpenAM はレルムを複数作成する事で、リソースやユーザーデータストアをレルム単位で管理する事が可能ですが、本構築手順ではデフォルトの「最上位のレルム」を選択します。

レルムは、OpenAM が設定情報の整理に使用する単位です。レルム内では、認証プロパティ、承認ポリシー、データストア、対象、その他のデータを定義できます。最上位のレルムは、OpenAM の配備時に作成されます。最上位のレルムは、OpenAM インスタンスの root で OpenAM 設定データを含んでいます。

レルム

*

レルム (1 項目)

<input checked="" type="checkbox"/>	レルム名	場所
<input checked="" type="checkbox"/>	/ (最上位のレルム)	/

次画面にて、対象タブに遷移し、ユーザーの「新規」ボタンをクリックします。

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

ユーザー グループ

/ (最上位のレルム)

ユーザー

*

ユーザー (3ユーザー)

<input checked="" type="checkbox"/>	名前	汎用 ID
<input checked="" type="checkbox"/>	amAdmin	amAdmin
<input type="checkbox"/>	anonymous	anonymous
<input type="checkbox"/>	demo	demo

次画面にて、認証を行いたいユーザーを作成します。本構築手順書では以下のユーザーアカウントを作成します。

属性名	属性値	説明
ID	testuser01	ユーザーID
userPassword	(※任意のパスワード文字列)	パスワード
フルネーム	testuser01	氏名
姓	test	姓
名	user01	名
ユーザー状態	アクティブ	有効/無効フラグ

新しいユーザー 了解 取消し

* 必須入力フィールド

* ID:

名:

* 姓:

* フルネーム:

* パスワード:

* パスワード(確認):

* ユーザー状態: アクティブ 非アクティブ

対象タブに遷移し、作成したユーザーアカウントが表示されている事を確認します。

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

ユーザー グループ

(最上位のレルム)

ユーザー アクセス制御へ戻る

*

ユーザー (4ユーザー)

<input checked="" type="checkbox"/>	名前	汎用 ID
<input checked="" type="checkbox"/>	amAdmin	amAdmin
<input type="checkbox"/>	anonymous	anonymous
<input type="checkbox"/>	demo	demo
<input type="checkbox"/>	testuser01	testuser01

最後に、OpenAM に作成したユーザーアカウントでログインできる事を確認して下さい。



FORGEROCK

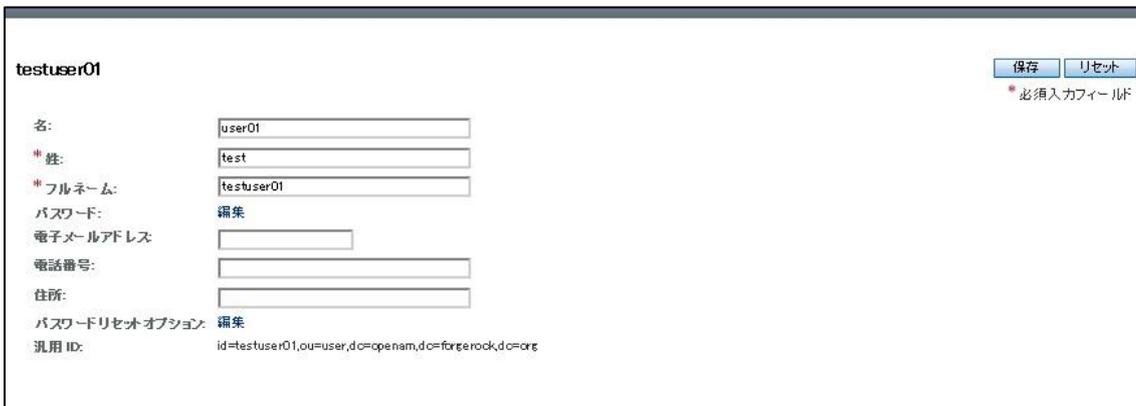
OpenAM へのサインイン

ユーザー名:
testuser01

パスワード:
●●●●●●

ログイン

ログインが成功するとユーザープロフィール画面が表示されます。



testuser01

保存 リセット
* 必須入力フィールド

名: user01

* 姓: test

* フルネーム: testuser01

パスワード: 編集

電子メールアドレス:

電話番号:

住所:

パスワードリセットオプション: 編集

汎用 ID: id=testuser01,ou=user,dc=openam,dc=forgerock,dc=ore

8. 外部ユーザーデータストア認証

OpenLDAP サーバーを OpenAM の外部ユーザーデータストアとして利用して認証する場合の手順を記述します。

OpenLDAP サーバーは以下の環境で構築済みである事を前提とします。

項目	値
ホスト名	openldap1.example.com
IP アドレス	192.168.0.12
ポート番号	389
バインドユーザーDN (※OpenLDAP に接続するためのユーザーDN)	cn=Manager,dc=example,dc=com
認証対象ユーザーアカウントが存在する OU	ou=People,dc=example,dc=com

OpenAM で認証を行うためのユーザーアカウントを OpenLDAP サーバーに作成します。本構築手順では、以下ユーザーアカウントを作成します。

属性名	属性値	説明
objectClass	inetOrgPerson	オブジェクトクラス
objectClass	organizationalPerson	オブジェクトクラス
objectClass	Person	オブジェクトクラス
objectClass	Top	オブジェクトクラス
dn	uid=openldapuser01, ou=People,dc=example,dc=com	ユーザーDN
uid	openldapuser01	ユーザーID
userPassword	(※任意のパスワード文字列)	パスワード
cn	openldapuser01	氏名
sn	openldap	姓
givenName	user01	名
mail	openldapuser01@example.com	メールアドレス

上記 OpenLDAP サーバー及びユーザーアカウントが準備できた後に、OpenAM のデータストア設定を行います。OpenAM 管理トップ画面よりアクセス制御タブに遷移し、「最上位のレルム」を選択します。

共通タスク **アクセス制御** 連携 設定 セッション

レルムは、OpenAM が設定情報の整理に使用する単位です。レルム内では、認証プロバイダー、承認ポリシー、データストア、対象、その他のデータを定義できます。最上位のレルムは、OpenAM の配備時に作成されます。最上位のレルムは、OpenAM インスタンスの root で OpenAM 設定データを含んでいます。

レルム

*

レルム (1 項目)

<input checked="" type="checkbox"/>	レルム名	場所
<input checked="" type="checkbox"/>	/ (最上位のレルム)	/

次画面にて、データストアタブに遷移し、データストアの「新規」ボタンをクリックします。

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

/ (最上位のレルム)

(最上位のレルム) - データストア

データストア (1 項目)

<input checked="" type="checkbox"/>	名前	タイプ
<input type="checkbox"/>	embedded	OpenDJ

次画面にて、名前とタイプを指定します。タイプは「汎用 LDAPv3」を選択します。

ステップ 1/2: データストアのタイプを選択

* 必須入力フィールド

* 名前:

* タイプ:

- Active Directory
- Active Directory アプリケーションモード (ADAM)
- OpenAM スキーマを含んだ Sun Directory Server
- OpenDJ
- Tivoli Directory Server
- データベースリポジトリ (アーリーアクセス)
- 汎用 LDAPv3

次画面にて、OpenLDAP サーバーへの接続設定を行います。この画面にて必要な設定を行った後、「終了」ボタンをクリックします。

ステップ 2/2: 新規データストア - 汎用 LDAPv3 戻る 終了 取消し

* 必須入力フィールド

* 名前:

完了時にスキーマを読み込み:

サーバー設定

* LDAP サーバー

現在の値: 削除

新しい値: 追加

形式: LDAP サーバーのホスト名:ポート |server_ID |site_ID

LDAP バインド DN:
サポートされる操作を実行できる適切なアクセス権を持つユーザーまたは管理者。

LDAP バインドパスワード:

LDAP バインドパスワード (確認):

* LDAP 組織 DN:

本構築手順では、デフォルトの設定から以下の属性を変更しています。

設定名	設定値	説明
LDAP サーバー	openldap1.example.com:389	OpenLDAP サーバーと合わせます。
LDAP バインド DN	cn=Manager,dc=example,dc=com	
LDAP バインドパスワード	(※LDAP バインド DN のパスワード文字列)	
LDAP 組織 DN	dc=example,dc=com	ou=People,dc=example,dc=com 下のユーザーアカウントを検索対象とします。
LDAP ピープルコンテナネーミング属性	ou	
LDAP ピープルコンテナ値	People	
LDAP グループコンテナネーミング属性	-(※空にする)	本構築手順ではグループは参照しないので、空にします。
LDAP グループコンテナ値	-(※空にする)	

設定変更後データストアタブに戻ると、作成したデータストア設定が追加されています。

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

/ (最上位のレルム)
 (最上位のレルム) - データストア [アクセス制御へ戻る](#)

データストア (2 項目)

新規... 削除

<input checked="" type="checkbox"/>	名前	タイプ
<input type="checkbox"/>	embedded	OpenDJ
<input type="checkbox"/>	openldap	汎用 LDAPv3

対象タブに遷移し、OpenLDAP 上のユーザーアカウントが表示されている事を確認します。

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

ユーザー グループ

/ (最上位のレルム)
 ユーザー [アクセス制御へ戻る](#)

* [検索](#)

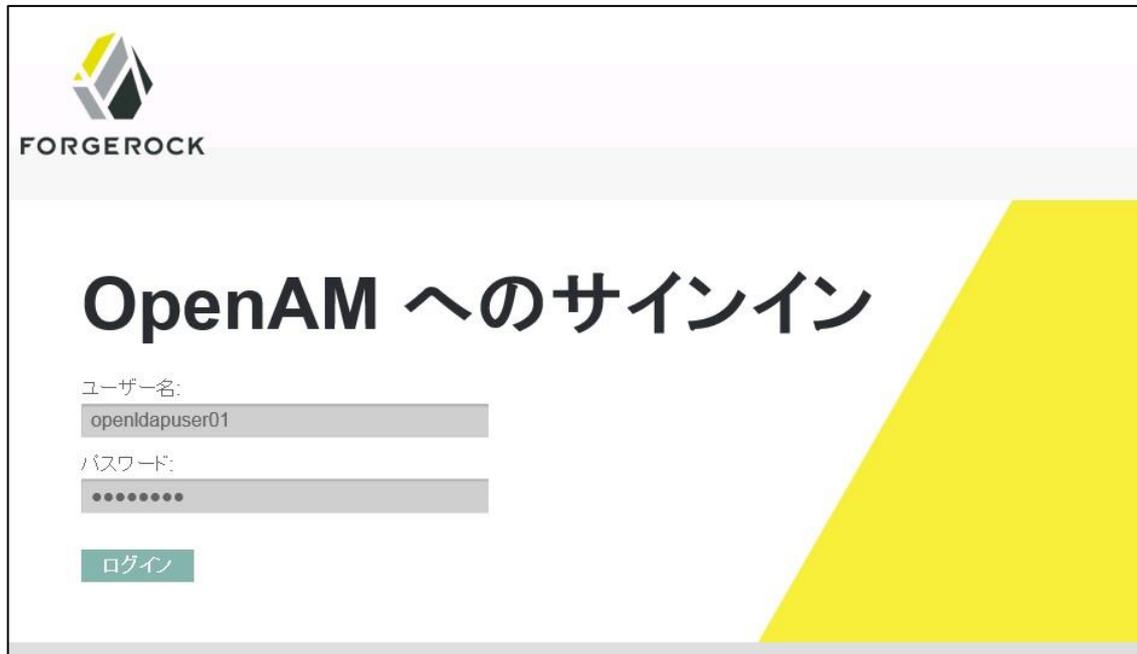
ユーザー (5 ユーザー)

新規... 削除

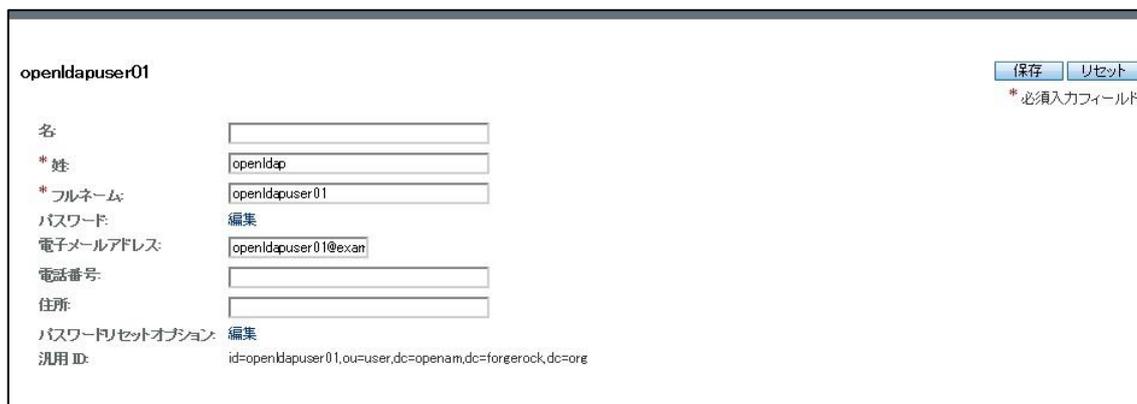
<input checked="" type="checkbox"/>	名前	汎用 ID
<input type="checkbox"/>	amAdmin	amAdmin
<input type="checkbox"/>	anonymous	anonymous
<input type="checkbox"/>	demo	demo
<input type="checkbox"/>	openldapuser01	openldapuser01
<input type="checkbox"/>	testuser01	testuser01

また、今回はデータストアのタイプとして「汎用 LDAPv3」を指定していますが、OpenAM で定義している LDAP スキーマを用いて OpenLDAP をスキーマ拡張する事で別のタイプを指定する事が可能です。スキーマ拡張を行う事で、そのままでは利用できない OpenAM の各種機能が利用可能になります。(例. ログイン失敗回数によるアカウントロックアウト)

最後に、OpenAM に OpenLDAP 上のユーザーアカウントでログインできる事を確認して下さい。



ログインが成功するとユーザープロフィール画面が表示されます。



9. おわりに

今回は、OpenLDAP サーバーを利用したユーザー認証が可能になるまでの OpenAM の構築手順を紹介しましたが、OpenAM には他にもたくさんの機能があります。以降、Web アプリケーションへのエージェント導入や、クラウドサービスとのフェデレーション設定を行う事でシングルサインオンが実現できます。他にも OpenAM の認証モジュールを設定する事で、ID/PW 入力以外の認証方法も設定可能です。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をご参照下さい。

参考資料

OpenAM Release Notes

<http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/release-notes/index/index.html>

OpenAM Installation Guide

<http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/install-guide/index.html>

OpenAM Nightly Builds

<http://forgerock.org/downloads/openam-builds/>