

# OpenAM 初期設定ガイド



OSSTech

オープンソース・ソリューション・テクノロジー(株)

更新日: 2015年1月7日

リビジョン: 1.3

## 目次

1. 概要	1
2. 事前準備	2
2.1 ホスト名の名前解決.....	2
3. OpenAM の初期設定	3
3.1 設定の開始.....	3
3.2 管理者ユーザーのパスワード設定.....	4
3.3 サーバー設定.....	5
3.4 設定データストアの設定.....	7
3.5 ユーザーデータストアの設定.....	8
3.6 サイトの設定.....	9
3.7 ポリシーエージェントのパスワード.....	10
3.8 設定の確認と反映.....	11
3.9 設定の完了.....	12
4. 改版履歴	13

## 1. 概要

本書は OpenAM の初期設定ガイドです。OpenAM を単一サーバーで構築する場合の設定方法について説明します。

## 2. 事前準備

本章では、OpenAM 初期設定を開始する前の確認事項について説明します。

### 2.1 ホスト名の名前解決

OpenAM はシングルサインオンを実現するためにクッキーをドメインに対して設定します。そのため OpenAM サーバーへのアクセスは完全修飾ドメイン名(FQDN)で行う必要があります(注 1)。FQDN が DNS 等により名前解決可能であることを確認して下さい。

なお、本書では OpenAM サーバーのホスト名を「sso.example.co.jp」として説明します。

(注 1) : IP アドレス等の完全修飾ドメイン名以外でアクセスがあった場合には、OpenAM は完全修飾ドメイン名を使って自分自身にリダイレクトを行います。

## 3. OpenAM の初期設定

本章では、OpenAM の初期設定を行います。前提として、OSSTech 版 OpenAM のインストールが完了していることを条件とします。OSSTech 版 OpenAM のインストール方法については、「OpenAM インストールガイド」をご参照ください。

### 3.1 設定の開始

以下の URL にブラウザでアクセスすることにより OpenAM の設定を開始します。必ず完全修飾ドメイン名(FQDN)でアクセスして下さい。

- <http://sso.example.co.jp:8080/openam>

設定オプション選択ページが表示されます。カスタム設定の「新しい設定の作成」を選択します。



## 3.2 管理者ユーザーのパスワード設定

管理者ユーザー(amadmin)のパスワードを設定します。パスワードは8文字以上である必要があります。パスワードを入力し、「次へ」ボタンをクリックします。

### 手順 1: 一般

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。

\* 必須フィールド

#### デフォルトユーザーパスワード

##### デフォルトユーザー [amAdmin]

\*パスワード

\*パスワードの確認

### 3.3 サーバー設定

サーバー固有の設定情報を指定します。

- サーバー URL : OpenAM にアクセスするための URL です。通常はデフォルトのままです。
- Cookie ドメイン : OpenAM が発行する Cookie のドメインを指定します。ここでは、「.example.co.jp」とします。Cookie ドメインに「.co.jp」は設定できないためご注意ください。
- プラットフォームロケール : デフォルトの「en\_US」のままです。
- 設定ディレクトリ : OpenAM の設定情報を保存するディレクトリを指定します。

Cookie ドメインには、インストーラーがサーバーホスト名の FQDN の末尾から 2 番目のドットまでを抜き出したものが自動的に設定されています。ホスト名が「sso.example.co.jp」の場合「.co.jp」となりますが、「co.jp」ドメインの場合は Cookie ドメインに少なくとも 3 つのピリオドを含む必要があります (Cookie の仕様)。そのため、このような場合は適切なドメインに設定し直して下さい。例えば「sso.example.co.jp」の場合には「.example.co.jp」に設定し直します。Cookie ドメインにホスト名ではなくドメインを指定する場合は、「.example.co.jp」の様に先頭に「.(ドット)」が必要です。

設定が終わったら「次へ」ボタンをクリックします。

**手順 2: サーバー設定** 

サーバーで使用する次の設定を確認します。

\* 必須フィールド

**サーバー設定**

*サーバー URL	<input type="text" value="http://sso.example.co.jp:8080"/>	<input checked="" type="checkbox"/> 了解
*Cookie ドメイン	<input type="text" value=".example.co.jp"/>	<input checked="" type="checkbox"/> 了解
*プラットフォームロケール	<input type="text" value="en_US"/>	
*設定ディレクトリ	<input type="text" value="/home/username/openam"/>	<input checked="" type="checkbox"/> 了解



### 3.4 設定データストアの設定

OpenAM の設定情報が保存される OpenDS(OpenAM 組み込みの LDAP サーバー)の設定を行います。

「最初のインスタンス」を選択します。

「設定データストア」は「OpenAM」を選択します。ポートやルートサフィックスは変更も可能ですが、設定データストア自体は OpenAM が内部的に参照するのみであるためデフォルトの設定で問題ありません。設定が終わったら「次へ」ボタンをクリックします。

#### 手順 3: 設定データストア設定

環境にほかの既存の OpenAM インスタンスがなければ、「最初のインスタンス」を選択します。環境に 1 つ以上の既存の OpenAM インスタンスがあれば、「既存の配備に追加しますか。」を選択します。

最初のインスタンス  既存の配備に追加しますか。

\* 必須フィールド

#### 設定ストアの詳細

設定データストア  OpenAM  Sun Java System Directory Server

\* SSL が有効

\* ホスト名

\* ポート

\* Admin Port

\* JMX Port

\* 暗号化鍵

\* ルートサフィックス

### 3.5 ユーザーデータストアの設定

ユーザーデータストアとは、ユーザー情報を保存・参照するためのデータベースです。

OpenAM はユーザーデータストアとして Active Directory や OpenLDAP 等の外部データベースを使用することが可能です。これらは初期設定完了後に必要に応じて追加することが出来ます。

ここでは初期設定として「OpenAM のユーザーデータストア」を選択します。初期設定の段階では管理者ユーザーやデモユーザーが OpenAM のユーザーデータストアに保存されます。

設定が終わったら「次へ」ボタンをクリックします。

#### 手順 4: ユーザーデータストア設定

OpenAM 設定データストアに付属のデータストアを使用することも、別のユーザーデータストアを使用することもできます。本稼働環境を設定する際には、OpenAM ユーザーデータストアとは異なる外部のユーザーデータストアを使用することをお勧めします。ここで指定したディレクトリ管理者 DN とパスワードを使用するようポリシーサービスと LDAP 認証モジュールが設定されることに注意してください。

- OpenAM のユーザーデータストア
- その他のユーザーデータストア

\* 必須フィールド

#### ユーザーストアの詳細

 OpenAM ユーザーデータストアの使用は、デモ目的または開発環境内でのみサポートされます。OpenAM ユーザーデータストアは、本稼働環境ではサポートされません。

### 3.6 サイトの設定

サイトとは OpenAM を 2 台以上構築する構成です。ロードバランサの背後に配置された複数の OpenAM サーバー群をサイトと呼びます。本書では単一サーバー構成を採るため「サイト」は利用しません。「いいえ」を選択し「次へ」ボタンをクリックします。

**手順 5: サイト設定** 

このインスタンスは、サイト設定の一部としてロードバランサの背後に配備されますか？

いいえ  
 はい

\* 必須フィールド

**サイト設定の詳細**

これは OpenAM の最初のインスタンスで、現在、サイト設定は存在しません。新しいサイト設定を作成するには、次の情報を入力します

\* サイト名

\* ロードバランサの URL

### 3.7 ポリシーエージェントのパスワード

デフォルトのポリシーエージェントのパスワードを設定します。本システムでは未使用ですが、インストールウィザードでは入力が必要となっているため、パスワードを入力します。

ここでもパスワードは8文字以上にする必要があり、かつ管理者ユーザー(amadmin)のパスワードとは異なるものにする必要があります。設定が完了したら「次へ」ボタンをクリックします。

#### 手順 6: デフォルトのポリシーエージェントユーザー

これらの設定は、ポリシーエージェントのプロパティを取得するために OpenAM ポリシーエージェントで使用されます。

\*必須フィールド

##### ポリシーエージェントユーザー

##### デフォルトポリシーエージェント [UrlAccessAgent]

- \*パスワード   了解
- \*パスワードの確認

### 3.8 設定の確認と反映

これまでの設定項目の一覧が表示されます。確認が済んだら「設定の作成」ボタンをクリックします。これにより設定がサーバーおよびデータストアに反映されます。

#### 設定ツールの概要と詳細

下の設定を確認してください。正しくない値がある場合は、設定を行う前に、戻ってその設定を変更できます。

##### 設定ツールの概要と詳細

##### 設定ストアの詳細 [編集...](#)

SSLが有効	いいえ
ホスト名	localhost
待機ポート	50389
ルートサフィックス	dc=opensso,dc=java,dc=net
ユーザー名	cn=Directory Manager
ディレクトリ名	/home/username/openam

##### ユーザーストアの詳細 [編集...](#)

設定ストア設定の使用

##### サイト設定の詳細 [編集...](#)

このインスタンスは、ロードバランサの背後には設定されません。

### 3.9 設定の完了

設定の作成が完了すると以下のような画面が表示されます。



以上で初期設定は完了です。「ログインに進む」をクリックし、表示される以下のログイン画面から管理者ユーザー amadmin でログインします。



以上で OpenAM のインストールは完了です。

## 4. 改版履歴

- 2010年11月21日 リビジョン1.0
  - 初版作成
- 2011年7月28日 リビジョン1.1
  - インストール条件を修正(OSバージョン明記、JDK 6バージョンから Update 20 以前を削除)
- 2012年3月1日 リビジョン1.2
  - OpenAM のインストール手順(Tomcat、OpenAM RPM のインストール)を削除
- 2015年1月7日 リビジョン1.3
  - 表紙及び改版履歴を修正