

OpenAM 11 初期設定ガイド



オープンソース・ソリューション・テクノロジー(株)

作成日: 2014年1月31日

更新日: 2014年1月31日

リビジョン: 1.0

目次

1. はじめに	1
1.1 本文書の目的.....	1
1.2 略語.....	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.....	6
3.5 ユーザーデータストアの設定.....	7
3.6 サイトの設定.....	8
3.7 ポリシーエージェントのパスワード.....	9
3.8 設定の確認と反映.....	10
3.9 設定の完了.....	11
4. 改版履歴	12

1. はじめに

1.1 本文書の目的

本文書は弊社提供の OpenAM 11 パッケージ導入後の初期設定（シングルサーバー構成）に関する手順書です。OpenAM 11 パッケージのインストールについては「OpenAM 11 インストールガイド」をご参照ください。

本文書に関する記載内容について、疑問点等がある場合には、弊社サポート窓口までお問い合わせください。

1.2 略語

本文書では必要に応じて以下のような略語を用います。

- 「Red Hat Enterprise Linux」を「RHEL」と表記します。
- 「オープンソース・ソリューション・テクノロジー」を「OSSTech」と表記します。

2. 事前準備

本章では、OpenAM インストール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ドメインクッキーを発行します。そのため OpenAM サーバーに対しては、完全修飾ドメイン名(FQDN)でアクセスする必要があります(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。

Linux サーバー(RHEL 系)の場合は、以下のファイルにも FQDN を記述してください。

- /etc/sysconfig/network

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 の初期設定の手順を説明します。

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。

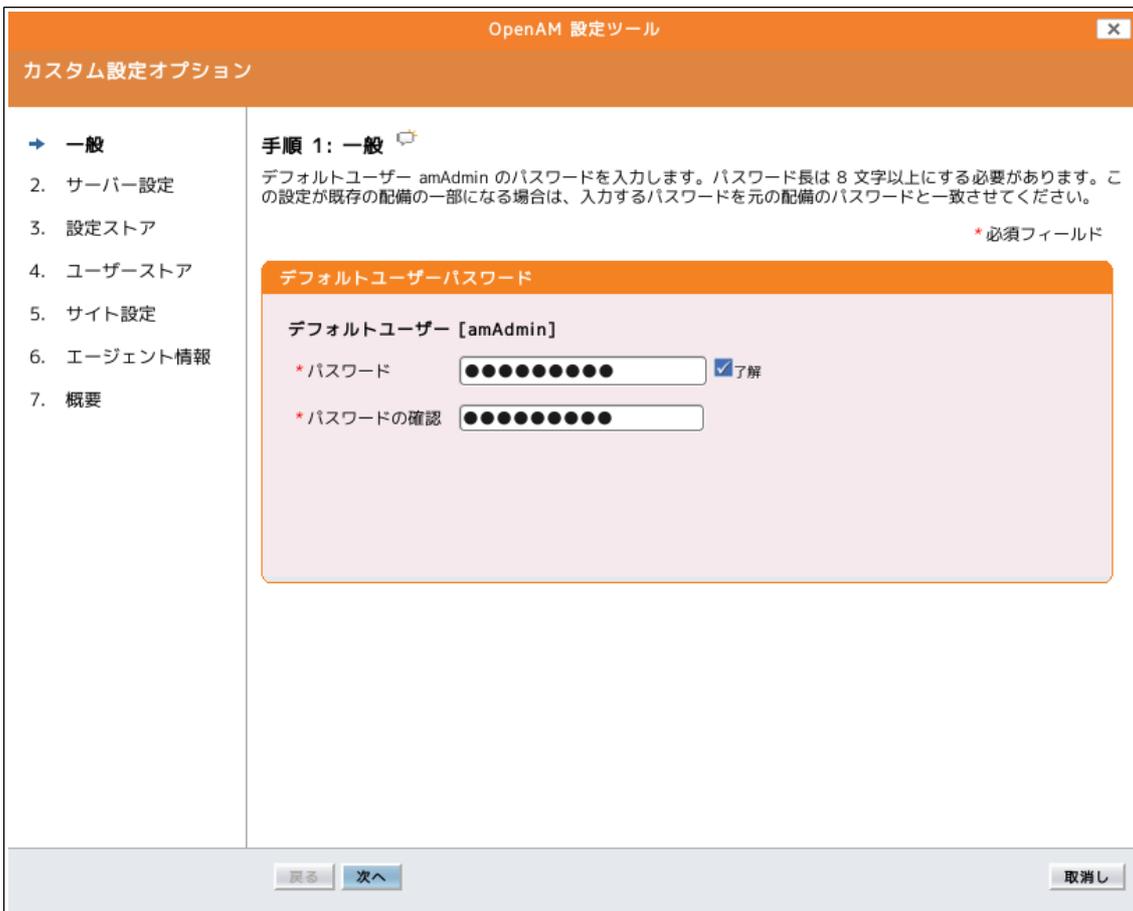
- <http://sso.example.co.jp:8080/openam>

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」をクリックします。



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。



The screenshot shows the 'OpenAM 設定ツール' (OpenAM Configuration Tool) window. The title bar includes a close button (X). The main content area is titled 'カスタム設定オプション' (Custom Setting Options). On the left, a navigation menu lists: 一般 (General), 2. サーバー設定 (Server Settings), 3. 設定ストア (Settings 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 (Overview). The '一般' option is selected and highlighted with a blue arrow. The main panel displays '手順 1: 一般' (Step 1: General) with a help icon. Below this, there is a text instruction: '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 setting becomes part of an existing deployment, ensure the password matches the original deployment's password.) A red asterisk indicates a required field. Below the instruction is a section titled 'デフォルトユーザーパスワード' (Default User Password) containing two input fields: 'デフォルトユーザー [amAdmin]' (Default User [amAdmin]), '*パスワード' (Password), and '*パスワードの確認' (Confirm Password). The password field has a '了解' (I understand) checkbox. At the bottom of the window, there are three buttons: '戻る' (Back), '次へ' (Next), and '取消し' (Cancel).

3.3 サーバー設定

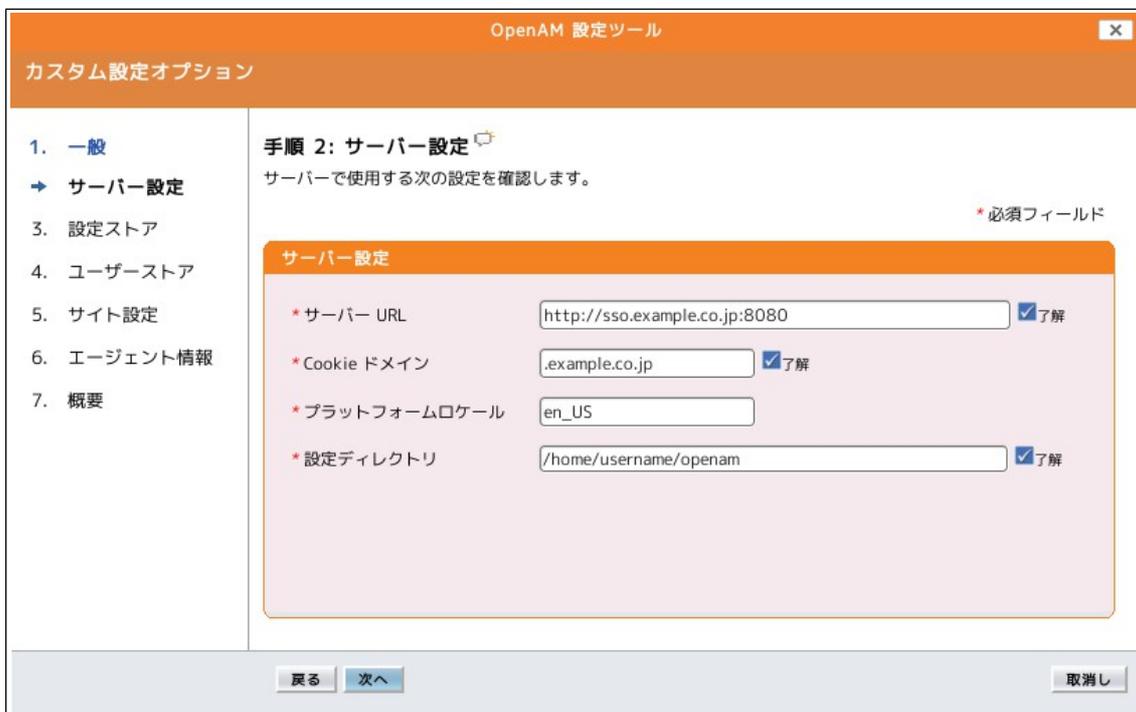
サーバー固有の情報を設定します。

項目	詳細
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問題ありません。
Cookie ドメイン(注 1)	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。
プラットフォームロケール	デフォルトの「en_US」のままとします。
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。

(注 1) Cookie ドメイン

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」の場合は「.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。

各項目を入力後、「次へ」ボタンをクリックします。



OpenAM 設定ツール

カスタム設定オプション

1. 一般
 → **サーバー設定**
 3. 設定ストア
 4. ユーザストア
 5. サイト設定
 6. エージェント情報
 7. 概要

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 了解

* Cookie ドメイン 了解

* プラットフォームロケール

* 設定ディレクトリ 了解

戻る 次へ 取消し

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 OpenDJ(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ものであるためデフォルトの設定で問題ありません。「次へ」ボタンをクリックします。



OpenAM 設定ツール

カスタム設定オプション

- 1. 一般
- 2. サーバー設定
- 設定ストア
- 4. ユーザストア
- 5. サイト設定
- 6. エージェント情報
- 7. 概要

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 OpenDJ or Oracle Directory Server Enterprise Edition

* 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

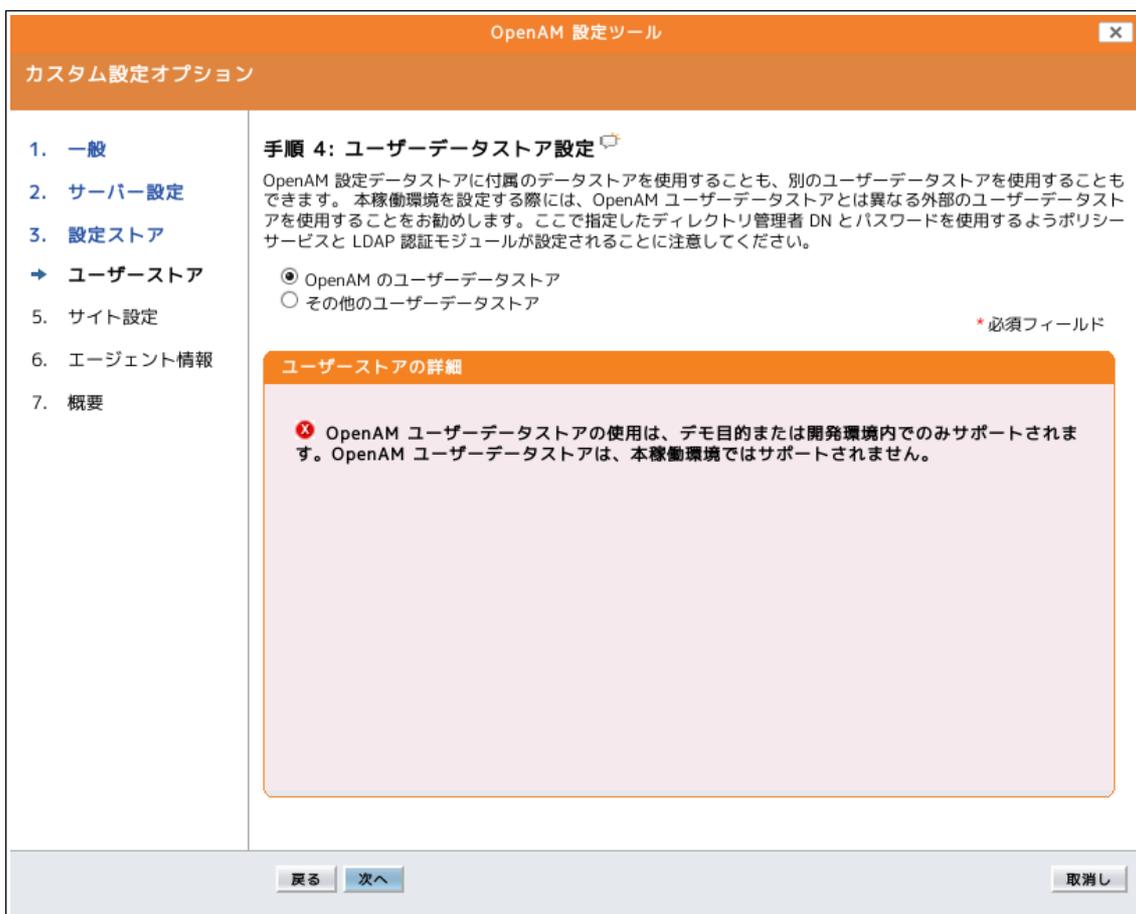
戻る 次へ 取消し

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、OpenAM の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 OpenLDAP 等の外部データベースを使用することが可能です。これらは初期設定の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。選択後、「次へ」ボタンをクリックします。



OpenAM 設定ツール

カスタム設定オプション

- 1. 一般
- 2. サーバー設定
- 3. 設定ストア
- ユーザーストア
- 5. サイト設定
- 6. エージェント情報
- 7. 概要

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

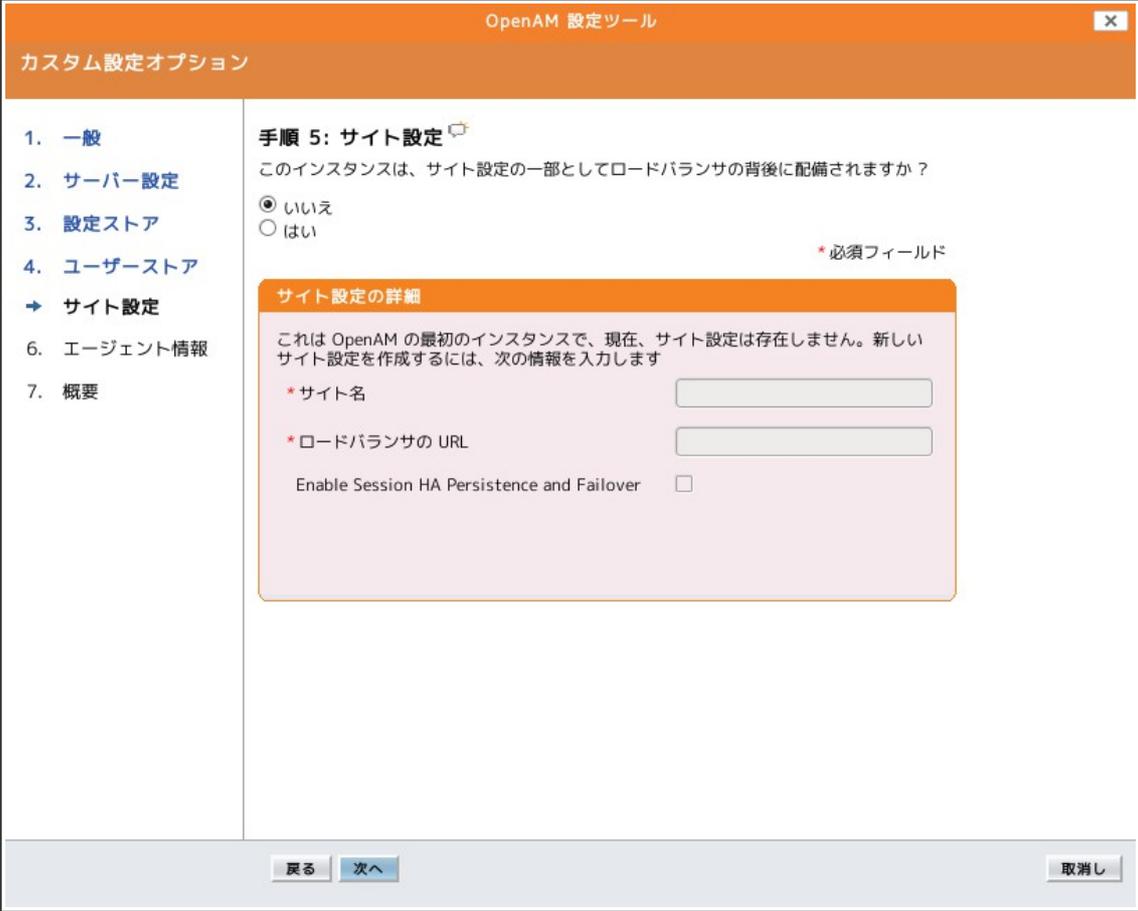
ユーザーストアの詳細

❌ 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。

戻る 次へ 取消し

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。本書ではシングル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。



OpenAM 設定ツール

カスタム設定オプション

- 1. 一般
- 2. サーバー設定
- 3. 設定ストア
- 4. ユーザストア
- **サイト設定**
- 6. エージェント情報
- 7. 概要

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

Enable Session HA Persistence and Failover

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。ポリシーエージェントを利用しない場合でも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。入力後、「次へ」ボタンをクリックします。



The screenshot shows the 'OpenAM 設定ツール' (OpenAM Configuration Tool) window. The title bar is orange with the text 'OpenAM 設定ツール' and a close button. Below the title bar is a header 'カスタム設定オプション' (Custom Setting Options). On the left is a navigation menu with items: 1. 一般 (General), 2. サーバー設定 (Server Settings), 3. 設定ストア (Settings 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) - selected with a blue arrow, 7. 概要 (Summary). The main content area is titled '手順 6: デフォルトのポリシーエージェントユーザー' (Step 6: Default Policy Agent User) and includes a warning icon. Below the title is explanatory text: '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。' (These settings are used by OpenAM Policy Agent to retrieve the properties of the policy agent). A red asterisk indicates a required field. The main form area is titled 'ポリシーエージェントユーザー' (Policy Agent User) and contains a sub-section 'デフォルトポリシーエージェント [UrlAccessAgent]' (Default Policy Agent [UrlAccessAgent]). It has two password fields: '* パスワード' (Password) and '* パスワードの確認' (Confirm Password), both with masked input and a '了解' (I understand) checkbox. At the bottom are buttons: '戻る' (Back), '次へ' (Next), and '取消し' (Cancel).

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。これにより設定が反映されます。



3.9 設定の完了

設定の作成が完了すると以下の画面が表示されます。



「ログインに進む」をクリックすると、以下のログイン画面が表示されます。



管理者ユーザー amadmin でログインすることで詳細な設定を行うことができます。

以上で初期設定は完了です。

4. 改版履歴

- 2014年1月31日 リビジョン 1.0
 - 初版作成