

OpenAM 14 初期設定ガイド



OSSTech

OSSTech(株)

更新日 2023年6月9日

リビジョン 2.2

目次

1	はじめに	1
1.1	本書の目的	1
1.2	略語	1
2	システム構成	2
2.1	サーバー / 機器一覧	2
2.2	アクセス URL	2
2.3	システム構成図	3
2.4	ソフトウェア構成図	4
2.5	OpenAM レルム構成	5
3	事前準備	6
3.1	ホスト名の名前解決	6
3.2	ファイアウォールの設定	6
3.3	パッケージのインストール	6
3.4	Apache の設定	6
4	OpenAM の初期設定	7
4.1	設定の開始	7
4.2	ライセンスの同意	8
4.3	管理者ユーザーのパスワード設定	9
4.4	サーバー設定	10
4.5	設定データストアの設定	11
4.6	ユーザーデータストアの設定	12
4.7	サイトの設定	13
4.8	ポリシーエージェントのパスワード	14
4.9	設定の確認と反映	15
4.10	設定の完了	16
4.11	レルムの設定	17
4.12	OpenAM サーバーの再起動	21
4.13	一般ユーザー FQDN でのアクセスの確認	21



5	SELinux の設定	22
6	改版履歴	23

1 はじめに

1.1 本書の目的

本書は弊社提供の OpenAM 14 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 14 パッケージのインストールについては「OpenAM 14 インストールガイド」をご参照ください。本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

本書では必要に応じて以下の略語を用います。

- 「Red Hat Enterprise Linux」を「RHEL」と表記します。

2 システム構成

本章では、本書が想定するシステム構成について説明します。

2.1 サーバー / 機器一覧

サーバー	ホスト名 (FQDN)
OpenAM 1 号機	openam01.example.co.jp

2.2 アクセス URL

2.2.1 管理者ログイン

OpenAM の各種設定を行う際は以下の URL にアクセスし、管理者アカウントでログインします。この URL からログインして表示される画面を「管理コンソール」と呼びます。

- <https://openam01.example.co.jp:8443/openam>

2.2.2 一般ユーザーログイン

一般ユーザーとしてログインする場合は以下の URL にアクセスします。

- <https://sso.example.co.jp/openam>

2.3 システム構成図

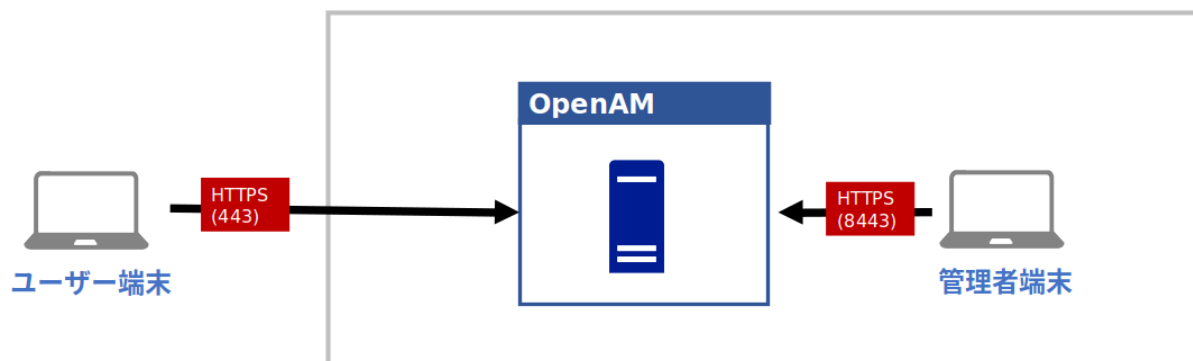


図1 システム構成図

各ノード間には下記の通信を行います。

送信元	送信先	プロトコル	ポート
ユーザー	OpenAM	HTTPS	443
管理者	OpenAM	HTTPS	8443

2.4 ソフトウェア構成図

OpenAM サーバー上で Apache HTTP Server を動かします。Apache が 8080,443,8443 ポートで Listen し HTTP リクエストを受付けます。Apache - Tomcat 間は AJP 通信を行います。

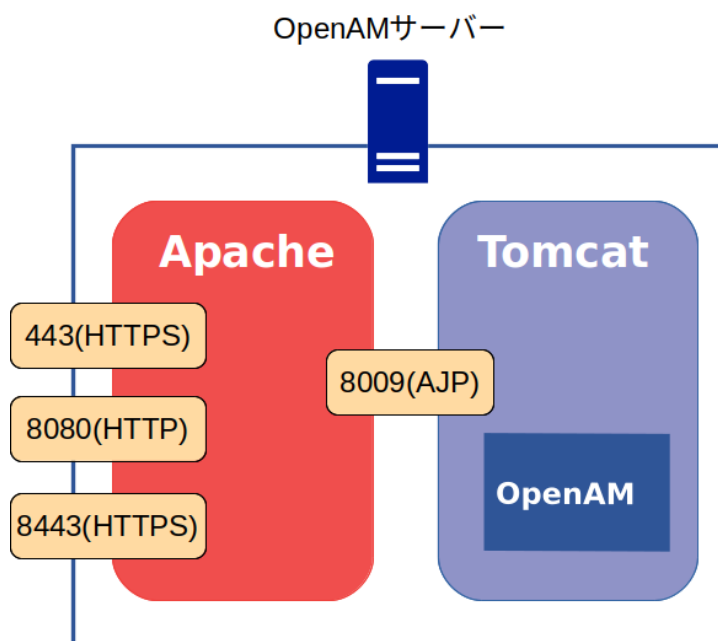


図2 ソフトウェア構成図

Apache で Listen する各ポート番号では以下のリクエストを取り扱います。

ポート番号	説明
443	一般ユーザーからのアクセスを処理します。
8080	初期設定時に利用します。 OpenAM2 台目を構築した場合や Policy Agent を導入した場合に使用します。
8443	管理コンソールのアクセスを処理します。

各ポート毎の VirtualHost を設定することでアクセスの種類で Apache のログを分けたり Require ディレクティブでアクセス制御を行うことができます。

2.5 OpenAM レルム構成

OpenAM のレルムとは、認証設定を構成する管理単位を示します。本書では以下のように構成します。

レルム	説明
/ (最上位のレルム)	OpenAM 管理者用の設定を行います。 openam01.example.co.jp でアクセスされた場合に適用されます。
/sso	一般ユーザー用の設定を行います。 sso.example.co.jp でアクセスされた場合に適用されます。

3 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。

3.1 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。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。

3.2 ファイアウォールの設定

OpenAM はシステム構成図で示す通信を行います。ファイアウォールを適切に設定するか、無効化して下さい。

3.3 パッケージのインストール

「OpenAM 14 インストールガイド」に従って RPM パッケージをインストールして下さい。

3.4 Apache の設定

Apache はソフトウェア構成図で示すとおり、8080,443,8443 番ポートを Listen し、443,8443 番ポートでは HTTPS 通信を利用できるようサーバー証明書等を設定します。Apache - Tomcat 間は AJP 通信を行うよう設定します。(本書では Apache の設定は割愛致します。)

4 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。

4.1 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://openam01.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。



図 3 初期設定 - 設定オプション

4.2 ライセンスの同意

ライセンスの同意を行います。内容を確認し、末尾の「I accept the license agreement」をチェックして、「CONTINUE」ボタンをクリックします。

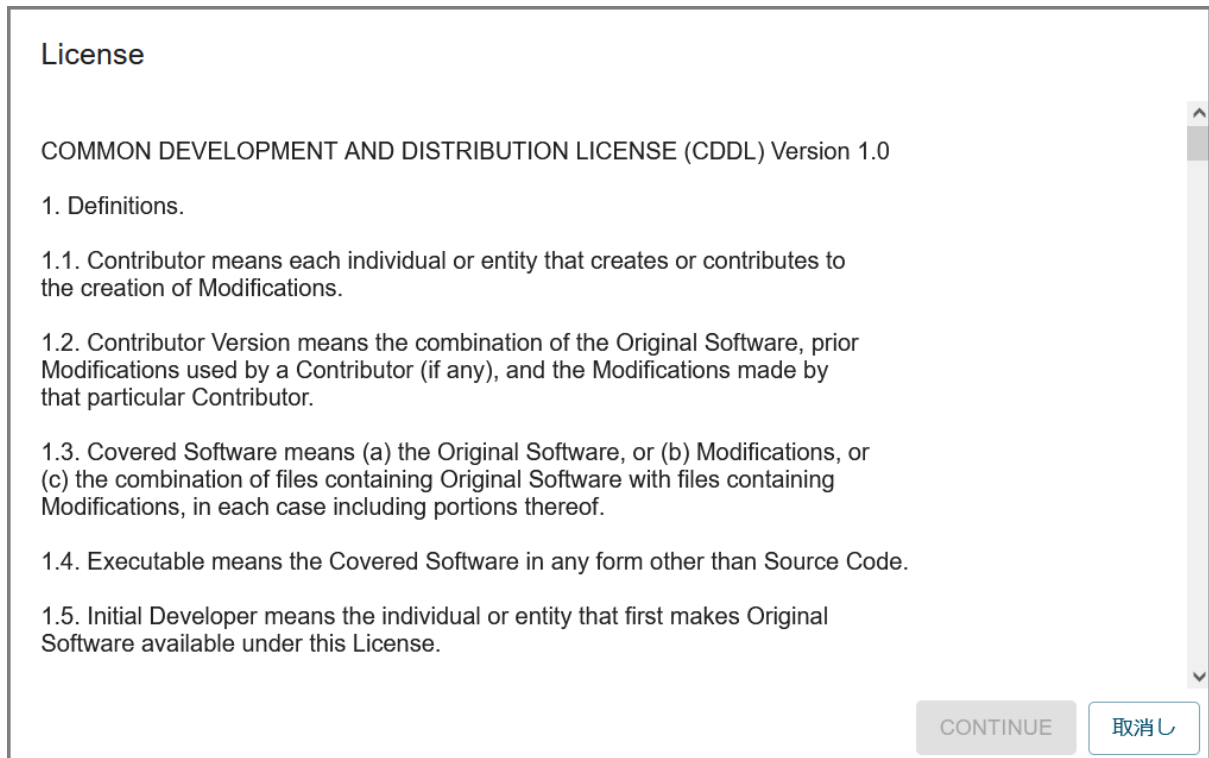


図 4 初期設定 - ライセンス

4.3 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。

デフォルトユーザー [amAdmin]

パスワード*

パスワードの確認*

次へ

最初からやり直す

図 5 初期設定 - 一般

4.4 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。
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。

各項目を入力後、「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。

サーバー設定

サーバー URL*
http://openam01.example.co.jp:8080

Cookie ドメイン
example.co.jp

プラットフォームロケール*
en_US

設定ディレクトリ*
/opt/osstech/var/lib/tomcat/data/openam

最初からやり直す

戻る 次へ

図 6 初期設定 - サーバー設定

4.5 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。



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。

SSL が有効

ホスト名*
localhost

ポート*
50389

管理者ポート*
4444

JMX ポート*
1689

暗号化鍵*
+ZaTprzMespdXTjilMmtEoo9cs0VIMeF

ルートサフィックス*
dc=openam,dc=osstech,dc=co,dc=jp

[最初からやり直す](#)

[戻る](#) [次へ](#)

図 7 初期設定 - 設定ストア

ホスト名を正しく設定していない場合、ポート番号がすべて「-1」に設定されます。
正しいホスト名を設定してください。

4.6 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。



The screenshot shows a configuration wizard titled "手順 4: ユーザーデータストア設定" (Step 4: User Data Store Configuration). On the left is a vertical navigation menu with steps 1 through 7: 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). Step 4 is currently selected. The main content area contains the following text: "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。" Below this text are two radio button options: "OpenAM のユーザーデータストア" (selected) and "その他のユーザーデータストア". At the bottom of the main area are two buttons: "戻る" (Back) and "次へ" (Next). At the bottom left of the wizard frame is a button labeled "最初からやり直す" (Reset).

図 8 初期設定 - ユーザーストア

4.7 サイトの設定

一般ユーザーと管理者の FQDN を分けるためサイトを設定します。「はい」を選択し、各項目を入力後、「次へ」ボタンをクリックします。

項目	詳細
サイト名	<p>サイトの名称です。</p> <p>ここでは「site1」とします。</p>
ロードバランサの URL	<p>一般ユーザーがアクセスするロードバランサの URL です。</p> <p>ここでは「https://sso.example.co.jp:443/openam」とします。</p>
セッション HA 永続化とフェイルオーバーを有効にします	<p>セッションフェイルオーバーを有効にする場合はチェックします。</p>



The screenshot shows the '手順 5: サイト設定' (Step 5: Site Configuration) screen. On the left is a navigation menu with steps: 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 Configuration - active), 6. エージェント情報 (Agent Information), 7. 概要 (Summary). Below the menu is a '最初からやり直す' (Reset from start) button.

The main content area contains the following text and form elements:

- Question: 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？ (Is this instance deployed behind a load balancer as part of the site configuration?)
- Options: いいえ (No), はい (Yes)
- Message: 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 (This is the first instance of OpenAM, and currently, no site configuration exists. To create a new site configuration, enter the following information).
- Form fields:
 - サイト名* (Site Name): site1
 - ロードバランサの URL* (Load Balancer URL): https://sso.example.co.jp:443/openam
- Checkbox: セッション HA 永続化とフェイルオーバーを有効にします (Enable session HA persistence and failover)
- Buttons: 戻る (Back) and 次へ (Next)

図 9 初期設定 - サイト設定

4.8 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 a configuration window 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). On the left is a vertical navigation menu with steps: 一般 (checked), サーバー設定 (checked), 設定ストア (checked), ユーザーストア (checked), サイト設定 (checked), エージェント情報 (6, selected), and 概要 (7). Below the menu is a "最初からやり直す" button. The main area contains a note: "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。" Below this is a form for "デフォルトポリシーエージェント [UriAccessAgent]" with two password fields: "パスワード*" and "パスワードの確認*", both masked with dots. At the bottom are "戻る" and "次へ" buttons.

図 10 初期設定 - エージェント情報

4.9 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。確認の後「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。



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
管理者ポート	4444
JMX ポート	1689
ルートサフィックス	dc=openam,dc=osstech,dc=co,dc=jp
ユーザー名	cn=Directory Manager
ディレクトリ名	/opt/osstech/var/lib/tomcat/data/openam

ユーザーストアの詳細 [編集...](#)

設定ストア設定の使用

[戻る](#) [設定の作成](#)

図 11 初期設定 - 概要

4.10 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。

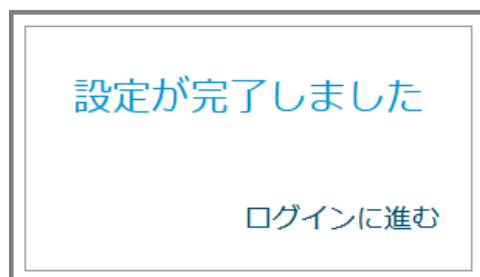


図 12 初期設定 - 完了

「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。



図 13 ログイン画面

4.11 レルムの設定

管理者ユーザー (amAdmin) でログインを行います。パスワードは**管理者パスワード**で設定した値です。



図 14 管理者ログイン

ログインすると以下の画面となりますので「最上位のレルム」を押します。



図 15 管理者ログイン後の画面

最上位のレルムの設定画面となります。画面右の「プロパティ」を押します。

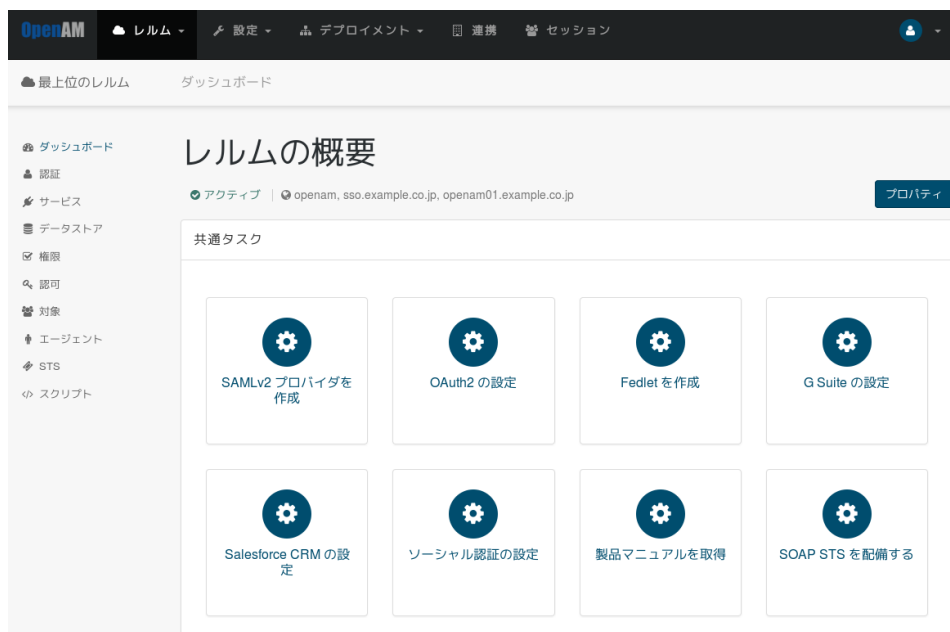


図 16 最上位のレルム

「レルムまたは DNS のエイリアス」に sso.example.co.jp(サイト構成で定義した FQDN) が存在するため削除し、画面右下の「変更の保存」を押します。

- 「レルムまたは DNS のエイリアス」は下記画面のとおり openam,openam01.example.co.jp だけとなります。



図 17 変更後の最上位のレルムのプロパティ画面

保存を終えたら、画面上のメニューから「レルム」->「新規レルム」を押します。



図 18 最上位のレルムのプロパティ画面から新規レルム作成

「名前」に sso 「レルムまたは DNS のエイリアス」に sso.example.co.jp を設定し「作成」を押します。



図 19 新規レルム作成画面

作成に成功すると sso レルムの設定画面となります。画面左上に sso と表示されます。管理者の作業は以上で終わりのため、画面右上のアイコンをクリックしログアウトを行います。

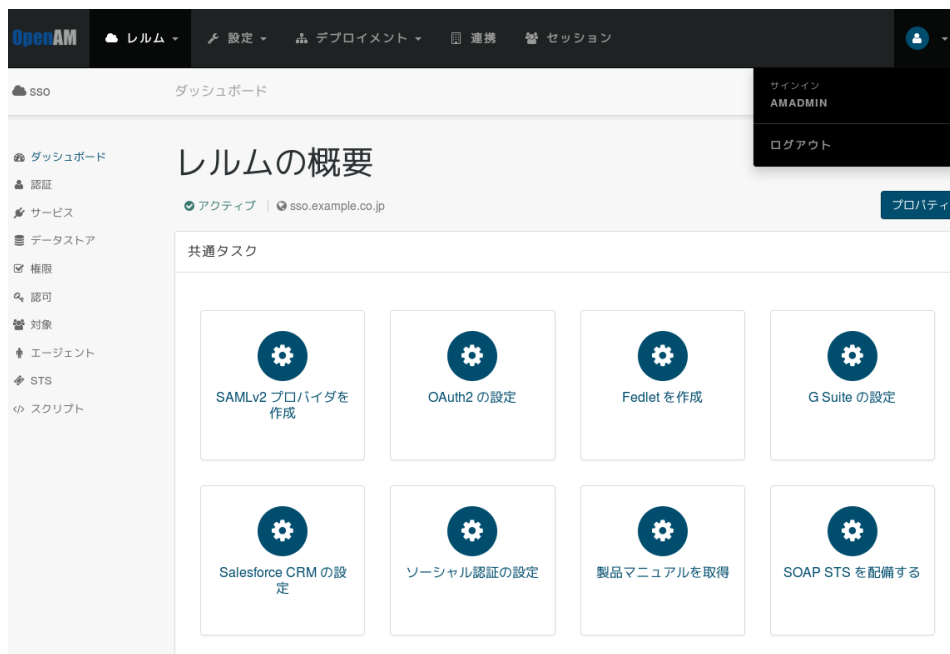


図 20 sso レルム

ログアウト成功を示すメッセージが表示されます。



図 21 ログアウト成功

4.12 OpenAM サーバーの再起動

設定を反映するためには OpenAM の再起動を行います。

```
# systemctl restart osstech-tomcat
```

以上で初期設定作業は完了です。

4.13 一般ユーザー FQDN でのアクセスの確認

一般ユーザー向けの URL にアクセスしてログイン画面が表示されることを確認します。初期設定後は demo ユーザーが存在しますのでログインして確かめることが可能です。

- アクセス URL
 - `https://sso.example.co.jp/openam`
 - ユーザー名: demo
 - パスワード: changeit

ログインに成功すると OpenAM のプロフィール画面となります。



OpenAM ダッシュボード

ユーザープロフィール

基本情報 | パスワード

ユーザー名 demo

名

姓 demo

電子メールアドレス

携帯電話

リセット 更新

図 22 demo ユーザー - プロファイル画面

5 SELinux の設定

SELinux が有効な環境では、OpenAM 初期設定後にコマンドを実行する必要があります。具体的な手順は「OpenAM 14 初期設定ガイド（冗長構成）」のドキュメントを参照してください。

6 改版履歴

- 2019年12月2日 リビジョン 1.0
 - 初版作成
- 2020年10月16日 リビジョン 2.0
 - Apache を経由する構成に変更
 - レルムの設定を追加
- 2022年5月9日 リビジョン 2.1
 - 社名変更に伴う修正
 - 初期設定画面を更新
- 2023年6月9日 リビジョン 2.2
 - SELinux の設定を追加