

# OpenAM 14 初期設定ガイド（冗長構成）



OSSTech

OSSTech(株)

更新日 2023年6月9日

リビジョン 2.3

## 目次

1	はじめに	1
1.1	本書の目的	1
1.2	略語	1
2	サイト構成（冗長構成）の特徴	2
2.1	設定の同期	2
2.2	セッションフォワーディング	2
3	システム構成	3
3.1	サーバー / 機器一覧	3
3.2	アクセス URL	3
3.3	システム構成図	4
3.4	ソフトウェア構成図	5
3.5	OpenAM レルム構成	5
4	設定手順	7
5	事前準備	8
5.1	ホスト名の名前解決	8
5.2	ファイアウォールの設定	8
5.3	パッケージのインストール	8
5.4	Apache の設定	8
6	OpenAM サーバー 1 号機の初期設定	9
6.1	設定の開始	9
6.2	ライセンスの同意	10
6.3	管理者ユーザーのパスワード設定	11
6.4	サーバー設定	12
6.5	設定データストアの設定	13
6.6	ユーザーデータストアの設定	14
6.7	サイトの設定	14
6.8	ポリシーエージェントのパスワード	16

6.9	設定の確認と反映	17
6.10	設定の完了	18
6.11	レルムの設定	19
7	OpenAM サーバー 2 号機の初期設定	23
7.1	設定の開始	23
7.2	ライセンスの同意	24
7.3	管理者ユーザーのパスワード設定	25
7.4	サーバー設定	26
7.5	設定データストアの設定	27
7.6	サイトの設定	28
7.7	設定の確認と反映	29
7.8	設定の完了	30
8	冗長構成の確認	31
8.1	Tomcat の設定変更	31
8.2	OpenAM サーバーの再起動	31
8.3	サイト構成の確認	32
8.4	ロードバランサー経由のアクセスの確認	33
9	SELinux の設定	34
9.1	事前準備	34
9.2	SELinux の設定	34
10	改版履歴	37

# 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（冗長構成）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 サイト構成（冗長構成）の特徴

OpenAM ではロードバランサー (LB) の背後に配置された複数の OpenAM サーバー群を「サイト」として設定することで各 OpenAM サーバーがロードバランサーの URL を持つ 1 つの OpenAM として動作します。そのため、OpenAM では冗長構成を「サイト構成」と呼びます。

本章では、サイト構成の特徴について説明します。

### 2.1 設定の同期

サイト構成では OpenAM の設定変更を 1 台のサーバーに対して実施します。設定変更は他のサーバーに同期されます。

OpenAM では設定情報を OpenDJ (OpenAM 組み込みの LDAP サーバー) に保存します。サイト構成では OpenDJ のレプリケーションが動作しており、1 台に実施した変更は他の号機にレプリケーションされます。

2 台間で設定データを同期しているため、原則として OpenAM の設定変更は 2 台の OpenAM サーバーが稼働中に行います。

#### 2.1.1 片系を停止した場合の設定変更

片系のサーバーを停止していた場合の設定データも 3 日以内であれば同期されます。例として 1 号機を停止中に 2 号機の管理コンソールにアクセスし OpenAM の設定を変更した場合、2 号機での変更から 3 日以内に 1 号機を起動すればデータは自動的に同期されます。変更から 3 日以上経過してから 1 号機を起動すると 2 号機での設定内容が反映されない場合があります。このため原則として OpenAM の設定変更は 2 台の OpenAM サーバーが稼働中に行います。

### 2.2 セッションフォワーディング

サイト構成では、あるサーバーが発行した認証セッション (Cookie) を別の号機に対して問い合わせても正常に動作します。そのため、ロードバランサーは認証後のアクセスを同一のサーバーに振り分ける必要はありません。

サイト構成の場合、問い合わせを受けたサーバーはセッションを発行したサーバーに認証セッションが有効かどうかを問い合わせることができます。

ただし、認証中は同一サーバーへの振り分けが必要です。

## 3 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。

### 3.1 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
OpenAM 2 号機	openam02.example.co.jp
ロードバランサー	sso.example.co.jp

### 3.2 アクセス URL

#### 3.2.1 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。

- 1 号機 : <https://openam01.example.co.jp/openam>
- 2 号機 : <https://openam02.example.co.jp/openam>

#### 3.2.2 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>

### 3.3 システム構成図

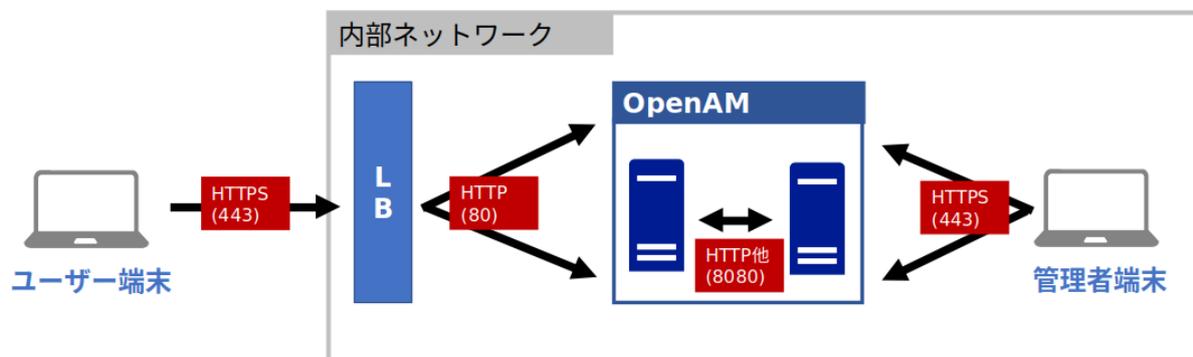


図1 システム構成図

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	ロードバランサー	HTTPS	443
ロードバランサー	OpenAM	HTTP	80
OpenAM	OpenAM	HTTP, LDAP	8080, 4444, 50389, 50889, 58989
管理者	OpenAM	HTTPS	443

## 3.4 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 80,8080,443 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。

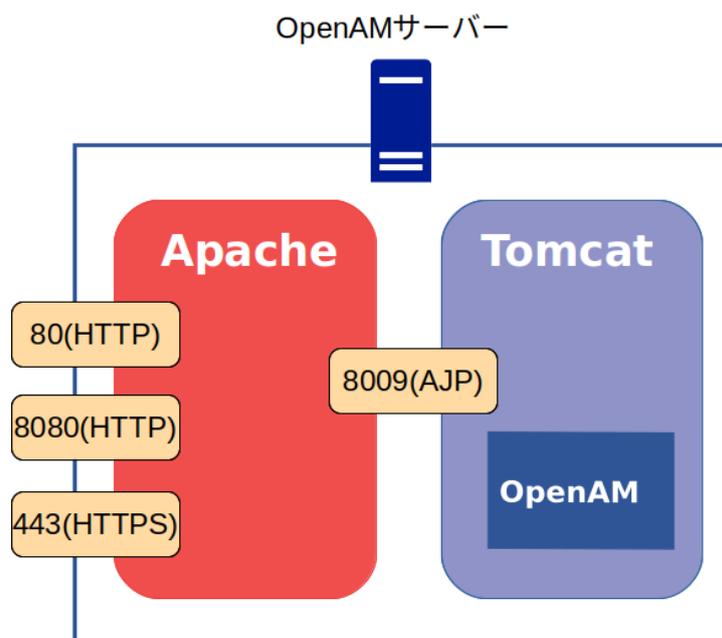


図2 ソフトウェア構成図

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
80	一般ユーザーからのアクセスを処理します。
8080	OpenAM サーバー間のアクセスを処理します。
443	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。

## 3.5 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。 各サーバーのホスト名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。

## 4 設定手順

OpenAM の初期設定（冗長構成）は以下の流れで実施します。

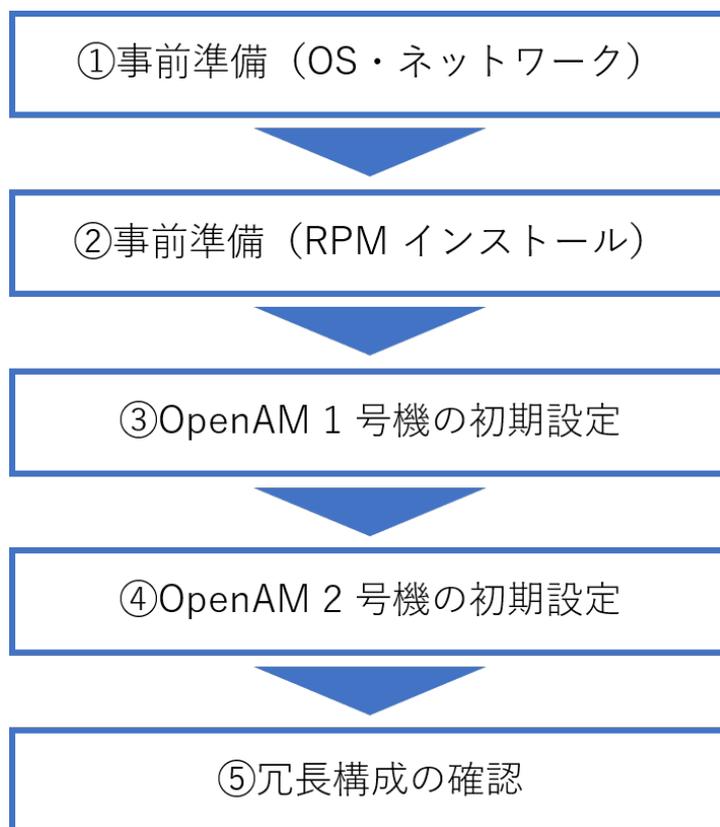


図3 初期設定の流れ

- については「5 事前準備」を確認 / 実施して下さい
- については「6 OpenAM サーバー 1号機の初期設定」を実施して下さい
- については「7 OpenAM サーバー 2号機の初期設定」を実施して下さい
- については「8 冗長構成の確認」を実施して下さい

## 5 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。

### 5.1 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。

### 5.2 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。

### 5.3 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。

### 5.4 Apache の設定

Apache はソフトウェア構成図で示すとおり、80,8080,443 番ポートを Listen し、443 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。)

## 6 OpenAM サーバー 1 号機の初期設定

本章では、OpenAM サーバー 1 号機の初期設定の手順を説明します。

### 6.1 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 4 1 号機の初期設定 - 設定オプション

## 6.2 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。

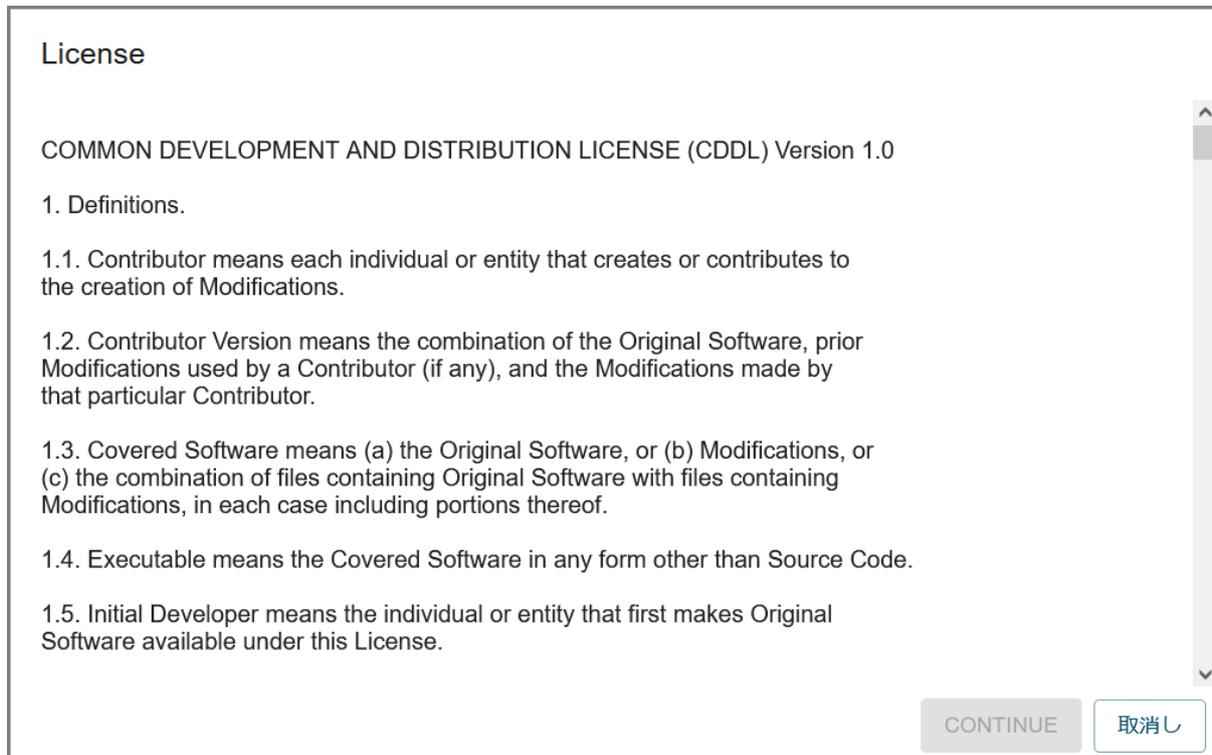


図5 1号機の初期設定 - ライセンス

## 6.3 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 6 1 号機の初期設定 - 一般

## 6.4 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。

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 7 1 号機の初期設定 - サーバー設定

## 6.5 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。



図 8 1 号機の初期設定 - 設定ストア

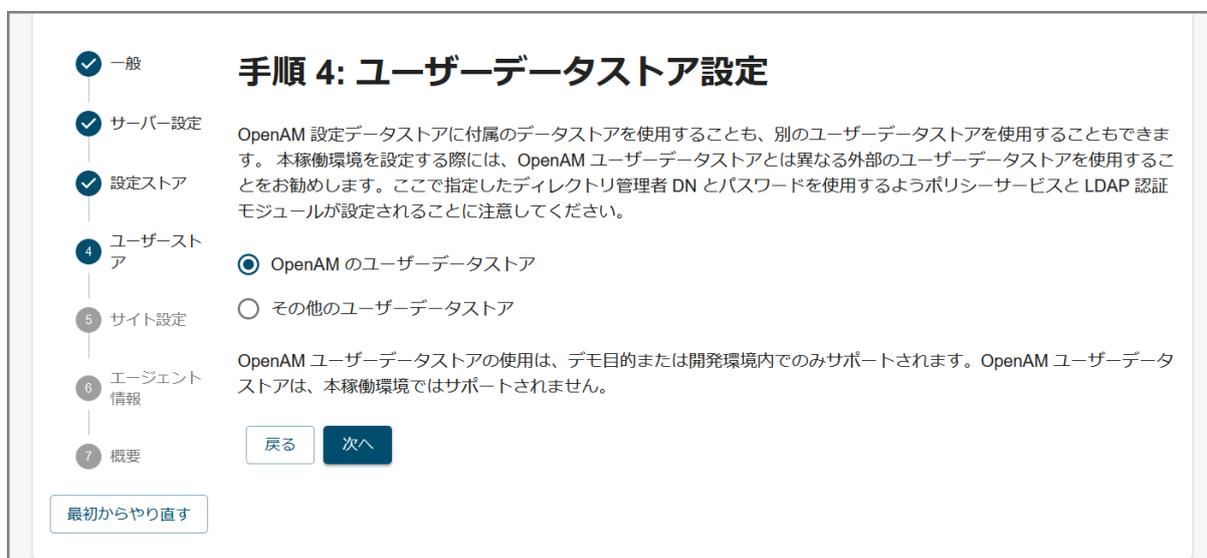
ホスト名を正しく設定していない場合、ポート番号がすべて「-1」に設定されます。  
正しいホスト名を設定してください。

## 6.6 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, a vertical list of steps is shown: 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) - currently selected, 5. サイト設定 (Site Settings), 6. エージェント情報 (Agent Information), and 7. 概要 (Summary). Below the list are buttons for "戻る" (Back), "次へ" (Next), and "最初からやり直す" (Restart from beginning). The main content area contains the following text:

**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

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。

図 9 1 号機の初期設定 - ユーザーストア

## 6.7 サイトの設定

本書では冗長構成を採るため「サイト」を利用します。「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	サイトの名称です。 ここでは「site1」とします。

項目	詳細
ロードバランサの URL	一般ユーザーがアクセスするロードバランサの URL です。 ここでは「https://sso.example.co.jp:443/openam」とします。
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	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。



図 10 1号機の初期設定 - サイト設定

## 6.8 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ます、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。



**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。

デフォルトポリシーエージェント [UriAccessAgent]

パスワード\*

パスワードの確認\*

戻る 次へ

最初からやり直す

図 11 1号機の初期設定 - エージェント情報

## 6.9 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 12 1号機の初期設定 - 概要

## 6.10 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 13 1号機の初期設定 - 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 14 ログイン画面

続けて、管理者でログインしレルムの設定を行います。

## 6.11 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 15 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 16 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。

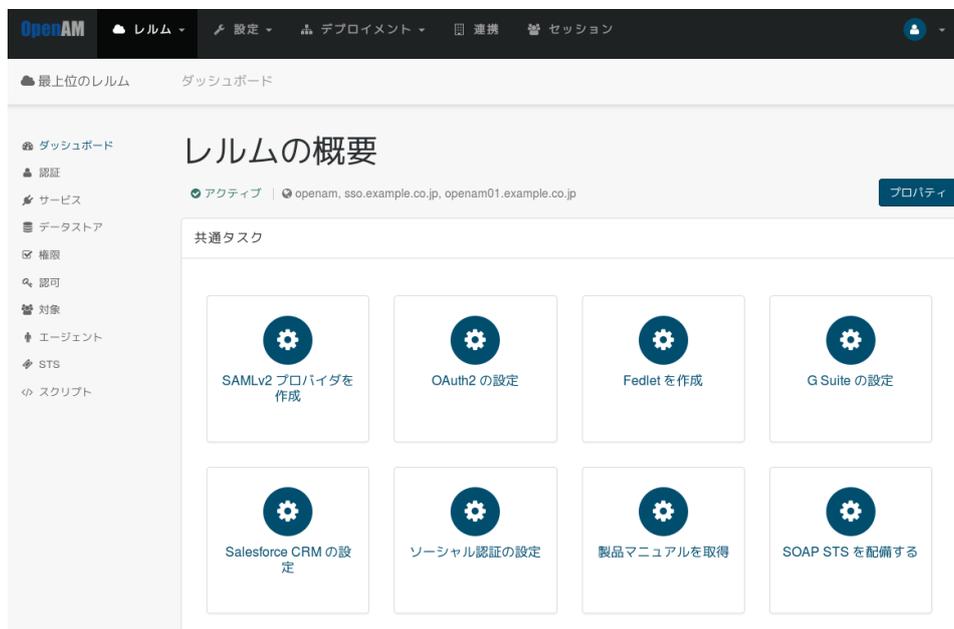


図 17 最上位のレルム

「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 18 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 19 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 20 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。

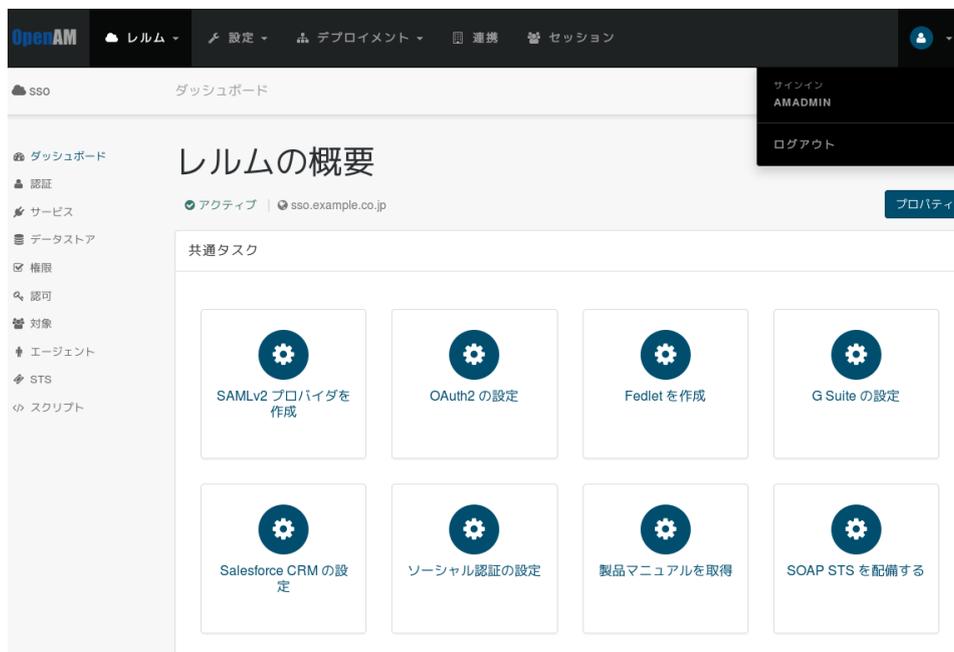


図 21 sso レルム

ログアウト成功を示すメッセージが表示されます。



図 22 ログアウト成功

以上で OpenAM 1 号機の初期設定およびレルムの設定は完了です。

## 7 OpenAM サーバー 2 号機の初期設定

本章では、OpenAM サーバー 2 号機の初期設定の手順を説明します。

### 7.1 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://openam02.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 23 2 号機の初期設定 - 設定オプション

## 7.2 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。

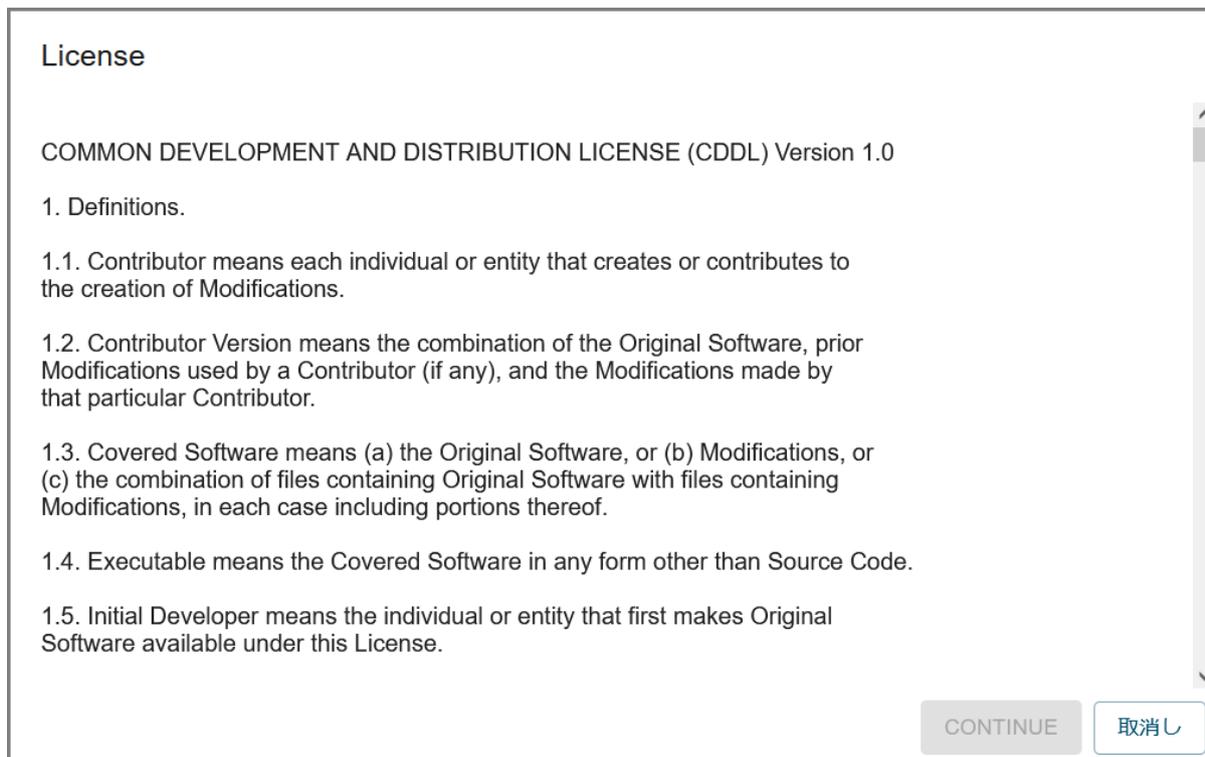


図 24 2号機の初期設定 - ライセンス

## 7.3 管理者ユーザーのパスワード設定

管理者ユーザー (amAdmin) のパスワードを入力します。1号機と同じパスワードを入力し、「次へ」ボタンをクリックします。



図 25 2号機の初期設定 - 一般

## 7.4 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。

各項目を入力後、「次へ」ボタンをクリックします。



図 26 2号機の初期設定 - サーバー設定

## 7.5 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。「既存の配備に追加しますか。」を選択します。

サーバー URL に 1 号機の URL である「http://openam01.example.co.jp:8080/openam」を入力します。自動的に画面が更新され、各種ポート番号が表示されます。



**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。

サーバー URL\*

http://openam01.example.co.jp:8080/openam

**新しい OpenAM インスタンスのポート設定**

待機ポート\*

50389

管理者ポート\*

4444

レプリケーションポート\*

58989

JMX ポート\*

1689

既存の OpenAM インスタンスのポート設定

戻る 次へ

図 27 2 号機の初期設定 - 設定ストア

## 7.6 サイトの設定

「はい」を選択し、1号機と同じ値を入力後、「次へ」ボタンをクリックします。

項目	詳細
サイト名	サイトの名称です。 ここでは「site1」とします。
ロードバランサの URL	一般ユーザーがアクセスするロードバランサの URL です。 ここでは「https://sso.example.co.jp:443/openam」とします。
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	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。



The screenshot shows the '手順 5: サイト設定' (Step 5: Site Settings) 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 Settings - 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:

- 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？
- Radio buttons for 'いいえ' (No) and 'はい' (Yes), with 'はい' selected.
- Text: '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'
- Form fields:
  - サイト名\*: site1
  - ロードバランサの 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' (unchecked)
- Buttons: '戻る' (Back) and '次へ' (Next)

図 28 2号機の初期設定 - サイト設定

## 7.7 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

**サイト設定の詳細** [編集...](#)

[最初からやり直す](#) [戻る](#) [設定の作成](#)

図 29 2号機の初期設定 - 概要

## 7.8 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 30 2号機の初期設定 - 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 31 ログイン画面

以上で OpenAM 2号機の初期設定は完了です。1号機の設定が自動的に反映されるため、2号機でのレルムの設定作業は不要です。

## 8 冗長構成の確認

### 8.1 Tomcat の設定変更

ブラウザ（一般ユーザーおよび管理者）は HTTPS 通信でしかアクセスしないため/opt/osstech/etc/tomcat ディレクトリにある server.xml を変更します。OpenAM サーバー 1 号機、2 号機共に変更作業が必要です。

```
<Connector protocol="AJP/1.3"
  secretRequired="false"
  address="127.0.0.1"
  port="8009"
  scheme="https"      <- 追加
  secure="true"      <- 追加
  redirectPort="8443" />
```

### 8.2 OpenAM サーバーの再起動

初期設定で指定したサイトの設定を反映するためには OpenAM の再起動が必要です。OpenAM サーバー 1 号機、2 号機共に下記のコマンドを実行して再起動を行います。

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

## 8.3 サイト構成の確認

管理コンソールでサイトの設定を確認します。管理者用 URL にアクセスし、管理者アカウントでログインします。

- 1号機 : <http://openam01.example.co.jp:8080/openam>
- 2号機 : <http://openam02.example.co.jp:8080/openam>

管理コンソールの「デプロイメント」「サーバー」を開きます。画面に1号機と2号機のURLが表示されることを確認します。また、URLの下にサイト名(ここではsite1)が表示されることを確認して下さい。

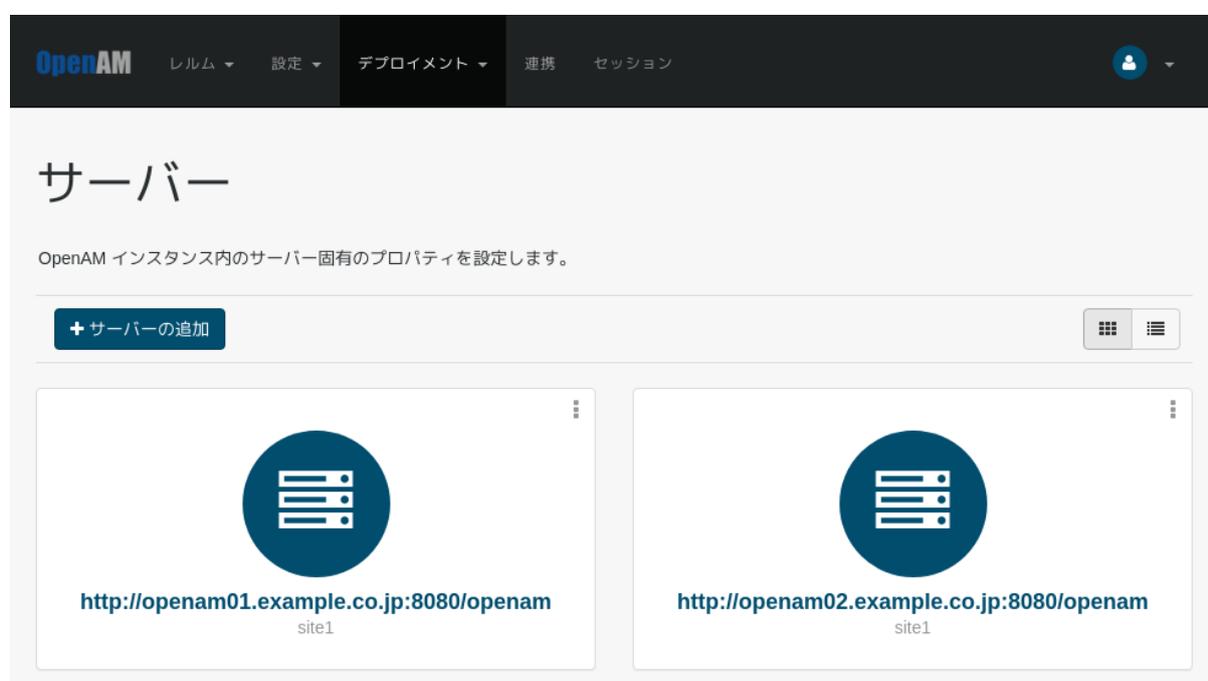


図 32 管理コンソール - サーバー一覧

## 8.4 ロードバランサー経由のアクセスの確認

ロードバランサー経由した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。



The screenshot shows the OpenAM user profile page. At the top, there is a navigation bar with the OpenAM logo and a 'ダッシュボード' (Dashboard) link. The main heading is 'ユーザープロフィール' (User Profile). Below this, there are two tabs: '基本情報' (Basic Information) and 'パスワード' (Password). The '基本情報' tab is active, showing a form with the following fields: 'ユーザー名' (Username) with the value 'demo', '名' (First Name) with an empty field, '姓' (Last Name) with the value 'demo', '電子メールアドレス' (Email Address) with an empty field, and '携帯電話' (Mobile Phone) with an empty field. At the bottom right of the form, there are two buttons: 'リセット' (Reset) and '更新' (Update).

図 33 demo ユーザー - プロファイル画面

## 9 SELinux の設定

本章は SELinux が有効な環境で必要な手順を説明します。SELinux が無効な環境では本章の内容を実施する必要はありません。

この SELinux の設定は、OpenAM のログに関する内容を含みます。OpenAM の各種ログの出力先は、「設定ディレクトリ (初期設定のサーバー設定で指定)」/「コンテキスト名」です。本章で示すログの出力先は、デフォルトの場所である `/opt/osstech/var/lib/tomcat/data/openam/openam` で表記します。もしデフォルトから変更している場合は、全て読み替えてください。

### 9.1 事前準備

#### 9.1.1 必要パッケージのインストール

SELinux の設定を行うために必要なパッケージをインストールします。

```
# dnf install -y policycoreutils-python-utils
```

#### 9.1.2 debug ディレクトリの確認

OpenAM の debug ディレクトリが存在することを確認します。

```
# ls -d /opt/osstech/var/lib/tomcat/data/openam/openam/debug  
/opt/osstech/var/lib/tomcat/data/openam/openam/debug/
```

まだ一度も OpenAM がログを出力していない場合は debug ディレクトリが存在しません。debug ディレクトリが存在しない場合は、ディレクトリの作成と権限設定を行います。

```
# mkdir /opt/osstech/var/lib/tomcat/data/openam/openam/debug  
# chown tomcat:tomcat /opt/osstech/var/lib/tomcat/data/openam/openam/debug  
# chmod 750 /opt/osstech/var/lib/tomcat/data/openam/openam/debug
```

## 9.2 SELinux の設定

### 9.2.1 Tomcat のログに対して設定

Tomcat が出力するログに必要なセキュリティコンテキストのタイプを設定します。

```
# semanage fcontext -a -t tomcat_log_t "/opt/osstech/var/log/tomcat(/.*)?"
# semanage fcontext -a -t tomcat_log_t "/var/opt/osstech/log/tomcat(/.*)?"
# restorecon -R /opt/osstech/var/log/tomcat
```

Tomcat ディレクトリと配下のファイルのセキュリティコンテキストのタイプが `tomcat_log_t` であることを確認します。

```
# ls -Zd /opt/osstech/var/log/tomcat
system_u:object_r:tomcat_log_t:s0 /opt/osstech/var/log/tomcat

# ls -Z /opt/osstech/var/log/tomcat
system_u:object_r:tomcat_log_t:s0 catalina.out
system_u:object_r:tomcat_log_t:s0 localhost.log
system_u:object_r:tomcat_log_t:s0 old
```

## 9.2.2 OpenAM のログに対して設定

OpenAM が出力するログに必要なセキュリティコンテキストのタイプを設定します。

```
# semanage fcontext -a -t tomcat_log_t \
    "/var/opt/osstech/lib/tomcat/data/openam/openam/log(/.*)?"
# semanage fcontext -a -t tomcat_log_t \
    "/var/opt/osstech/lib/tomcat/data/openam/openam/stats(/.*)?"
# semanage fcontext -a -t tomcat_log_t \
    "/var/opt/osstech/lib/tomcat/data/openam/openam/debug(/.*)?"
# semanage fcontext -a -t tomcat_log_t \
    "/var/opt/osstech/lib/tomcat/data/openam/opends/logs(/.*)?"

# restorecon -R /var/opt/osstech/lib/tomcat/data/openam/openam/log
# restorecon -R /var/opt/osstech/lib/tomcat/data/openam/openam/stats
# restorecon -R /var/opt/osstech/lib/tomcat/data/openam/openam/debug
# restorecon -R /var/opt/osstech/lib/tomcat/data/openam/opends/logs
```

OpenAM のログディレクトリと配下のファイルのセキュリティコンテキストのタイプが `tomcat_log_t` であることを確認します。

```
# ls -Zd /var/opt/osstech/lib/tomcat/data/openam/openam/{log,stats,debug}
system_u:object_r:tomcat_log_t:s0 /var/opt/osstech/lib/tomcat/data/openam/openam/
debug
system_u:object_r:tomcat_log_t:s0 /var/opt/osstech/lib/tomcat/data/openam/openam/
stats
```

```
system_u:object_r:tomcat_log_t:s0 /var/opt/osstech/lib/tomcat/data/openam/openam/
log

# ls -Z /var/opt/osstech/lib/tomcat/data/openam/openam/log
system_u:object_r:tomcat_log_t:s0 access.csv
system_u:object_r:tomcat_log_t:s0 authentication.csv
system_u:object_r:tomcat_log_t:s0 activity.csv
system_u:object_r:tomcat_log_t:s0 config.csv

# ls -Z /var/opt/osstech/lib/tomcat/data/openam/openam/debug
system_u:object_r:tomcat_log_t:s0 Configuration
system_u:object_r:tomcat_log_t:s0 IdRepo
system_u:object_r:tomcat_log_t:s0 old
system_u:object_r:tomcat_log_t:s0 CoreSystem
system_u:object_r:tomcat_log_t:s0 Session

# # ls -Z /var/opt/osstech/lib/tomcat/data/openam/openam/stats
system_u:object_r:tomcat_log_t:s0 amMasterSessionTableStats
system_u:object_r:tomcat_log_t:s0 idRepoCacheStat
system_u:object_r:tomcat_log_t:s0 old

# ls -dZ /var/opt/osstech/lib/tomcat/data/openam/opends/logs
system_u:object_r:tomcat_log_t:s0 /var/opt/osstech/lib/tomcat/data/openam/opends/
logs

# ls -Z /var/opt/osstech/lib/tomcat/data/openam/opends/logs
system_u:object_r:tomcat_log_t:s0 access
system_u:object_r:tomcat_log_t:s0 errors
system_u:object_r:tomcat_log_t:s0 replication
```

## 10 改版履歴

- 2020年10月8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
  - 片系を停止した場合の設定変更を追加
- 2021年11月18日 リビジョン 2.1
  - OpenDJ のレプリケーションポートを修正
- 2022年5月9日 リビジョン 2.2
  - 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 2.3
  - 「SELinux の設定」を追加