OpenAM 13 インストールガイド

オープンソース・ソリューション・テクノロジ (株)

更新日	2020 年 6 月 15 日
リビジョン	2.7

目次

1 はじめに

1.1 本書の目的

本文書は、弊社提供の OpenAM 13 パッケージのインストールを実施するための手順書です。 OpenAM 13 パッケージのインストールやアップデートの際には、必ず本文書の内容を確認してから作業を実施してください。

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 前提条件

本書は、特に指示がない限り、以下のような条件を前提に記述しています。これと異なる場合は、適宜内容を読み替えるか、必要な作業を別途実施してください。

- 作業者が OS と関連ソフトウェアの管理や操作手順についての一般的な知識を有すること。
- OS と関連ソフトウェアの基本設定が適切になされていること。
- OS のセキュア OS 機能 (SELinux 等) やファイアウォール機能を無効にすること。
  - ファイアウォールを有効化した状態で OpenAM を運用することも可能です。手順の簡略化のために、本書ではファイアウォールが無効化されていることを前提とします。
  - 現状、OpenAM は SELinux が 有効な状態では動作しないため、SELinux を無効化してください。
- 管理ユーザー root のシェル端末で作業すること。(作業ユーザーを指定している場合を除く)
- 製品パッケージファイル群をインストール対象環境の`/srv/osstech-work/software/RPMS`ディレクトリ以下にコピーしておくこと。

1.3 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」を「OSSTech」と表記します。

2 事前準備

本章では、OpenAM の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。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。

3 システム要件

3.1 ソフトウェア要件

以下のいずれかの OS 環境が必要です。

- Red Hat Enterprise Linux 7 (x86_64)
- CentOS 7 (x86_64)

また、以下のソフトウェアが必要です。

- OS 標準 OpenJDK 8
- OS 標準 Tomcat 7 (RHEL7/CentOS7)

4 パッケージ構成

弊社が提供する Linux 版ソフトウェアは以下のパッケージにより構成されています。

1. OSSTech ソフトウェア製品基本パッケージ

- osstech-base
- osstech-support
- osstech-daemontools(RHEL7/CentOS7)

2. OSSTech Tomcat パッケージ

- osstech-tomcat(RHEL7/CentOS7)

3. OSSTech OpenAM 13 パッケージ

- osstech-openam13

5 RPM パッケージのインストール

各パッケージのインストールは、OS 付属の rpm コマンドを用いて行います。以下の手順にしたがってパッケージのインストールを実施してください。

5.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（ 画面には表示されません ）
```

次に弊社から提供されたパッケージ一式をインストール先ホストの任意のディレクトリに展開します。

以降は /srv/osstech-work/software/RPMS に展開したことを前提として記述します。

5.2 依存パッケージのインストール

5.2.1 ksh

OSSTech 版製品の動作には ksh が必要です。ksh がインストールされていない場合はインストールしてください。

```
# yum install ksh
```

5.2.2 OpenJDK 8

OpenAM の動作には OpenJDK 8 が必要です。OpenJDK 8 がインストールされていない場合はインストールしてください。

```
# yum install java-1.8.0-openjdk
```

5.2.3 Tomcat(RHEL7/CentOS7)

RHEL7 または CentOS7 環境の場合、OS 標準 Tomcat のバイナリを利用して動作を行います。Tomcat がインストールされていない場合はインストールしてください。

```
# yum install tomcat
```

5.3 パッケージの確認

パッケージ展開先のディレクトリに弊社提供のパッケージ一式があることを確認します。

- RHEL7/CentOS7 の場合

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  x86_64
# ls x86_64
osstech-base-X.X-X.el7.x86_64.rpm
osstech-daemontools-X.X-X.el7.x86_64.rpm
osstech-openam13-13.0.0-X.el7.noarch.rpm
osstech-openam13-configtools-13.0.0-X.el7.noarch.rpm
osstech-openam13-tools-13.0.0-X.el7.noarch.rpm
osstech-support-X.X-X.el7.x86_64.rpm
osstech-tomcat-7.instanceX.X.X-X.el7_7.X.X.rX_X.noarch.rpm
repodata
```

5.4 パッケージのインストール

yum でパッケージインストールができる環境の場合、以下のコマンドを実行しインストールを実施します。

```
# ./install.sh
```

コマンドを実行すると「Is this ok [y/N]:」という出力があります。ここで「y」を入力すると、依存パッケージも含めてパッケージ一式がインストールされます。

この「install」コマンドは「yum」に依存しています。したがって、これまで yum コマンドを実行したことがない場合はもう一度「Is this ok [y/N]:」という出力があります。問いかけの意味については yum のマニュアルをご覧ください。

以下の出力が得られれば完了です。

```
完了しました!（もしくは Complete!）
```

yum でパッケージインストールができない環境の場合、依存パッケージインストール後、

以下のように rpm コマンドを使用してパッケージインストールを実施します。

```
# cd x86_64
# rpm -ivh osstech-base*.rpm \
> osstech-support*.rpm \
> osstech-daemontools*.rpm \
> osstech-tomcat*.rpm \
> osstech-openam13-13.0.0-*.rpm \
> osstech-openam13-tools-*.rpm
```

以下の出力が得られれば完了です。

```
...(省略) [100%]
```

5.5 Tomcat の起動

RPM パッケージをインストール後、Tomcat を起動します。

```
# /sbin/service osstech-tomcat start
```

5.6 初期設定の開始

Tomcat が起動したら、ブラウザで以下の URL にアクセスします。

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

「設定オプション画面」が表示されます。この画面から OpenAM の初期設定を行います。コンテキスト名 (/openam/) は変更可能です。コンテキスト名を変更する場合は Tomcat を起動する前に「コンテキスト名の変更」を実施ください。

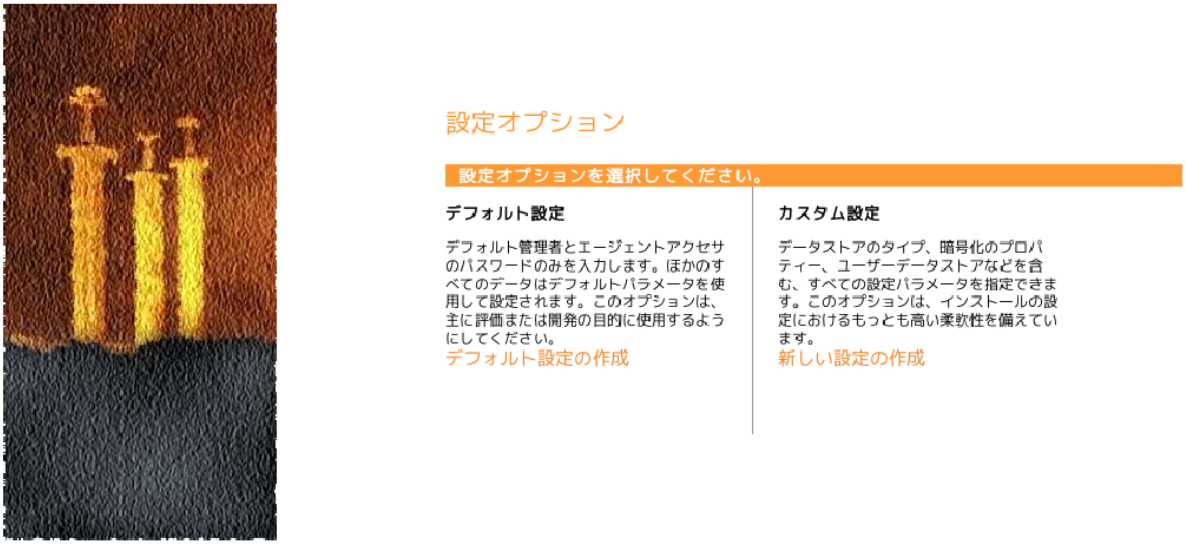

図 1　設定オプション画面

6 RPM パッケージのアップデート

弊社提供のパッケージをアップデートする際は、以下の手順にしたがって実施してください。2 台構成の場合は「OpenAM 2 台構成のアップデート」をご覧ください。

6.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（ 画面には表示されません ）
```

次に弊社から提供されたパッケージ一式をインストール先ホストの任意のディレクトリに展開します。

以降は /srv/osstech-work/software/RPMS に展開したことを前提として記述します。

6.2 Tomcat の停止

Tomcat を停止します。

```
# /sbin/service osstech-tomcat stop
```

6.3 OpenAM 設定ディレクトリのバックアップ

現在の OpenAM の設定をバックアップします。

下の例では OpenAM の設定の保存先は「/opt/osstech/var/lib/tomcat/openam」、バックアップ先は「/root/backup/conf」です。

```
# mkdir -p /root/backup/conf
# cd /opt/osstech/var/lib/tomcat
# cp -pir openam /root/backup/conf
```

6.4 Tomcat の work ディレクトリの削除

Tomcat の work ディレクトリを削除します。

```
# rm -rf /opt/osstech/share/tomcat/work/Catalina/localhost/openam
```

6.5 パッケージの確認

パッケージ展開先のディレクトリに弊社提供のパッケージ一式があることを確認します。

- RHEL7/CentOS7 の場合

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  x86_64
# ls x86_64
osstech-base-X.X-X.el7.x86_64.rpm
osstech-daemontools-X.X-X.el7.x86_64.rpm
osstech-openam13-13.0.0-X.el7.noarch.rpm
osstech-openam13-configtools-13.0.0-X.el7.noarch.rpm
osstech-openam13-tools-13.0.0-X.el7.noarch.rpm
osstech-support-X.X-X.el7.x86_64.rpm
osstech-tomcat-7.instanceX.X.X-X.el7_7.X.X.rX_X.noarch.rpm
repodata
```

6.6 パッケージのアップデート

パッケージのアップデートを rpm コマンドで行います。

```
# cd x86_64
# rpm -Uvh osstech-base*.rpm \
> osstech-support*.rpm \
> osstech-daemontools*.rpm \
> osstech-tomcat*.rpm \
> osstech-openam13-13.0.0-*.rpm \
> osstech-openam13-tools-*.rpm
```

既に最新のパッケージがインストール済みの場合、次のエラーが表示されます。この場合はインストール済みのパッケージをアップデートする必要はありませんので、アップデート不要なパッケージを rpm コマンドの引数から取り除き、再度アップデートを試みます。

```
準備中...    ########################################### [100%]
      パッケージ osstech-base-3.0-115.el7.x86_64 は既にインストールされています。
```

```
      パッケージ osstech-support-3.0-115.el7.x86_64 は既にインストールされています。
```

上記の例の場合、osstech-base パッケージと osstech-support パッケージのアップデートが不要なことを表しています。

openam13-13.0.0-91 より python-requests パッケージが必要 となります。

```
エラー: 依存性の欠如:
 python-requests は osstech-openam13-tools-13.0.0-94.el7.noarch に必要とされています
```

rpm コマンド実行時上記のエラーが表示された場合は python-requests パッケージのインストールを行ってから rpm コマンドを実行してください。

```
# yum install python-requests
```

6.6.1 index.html の警告が表示された場合

画面カスタマイズで/opt/osstech/share/tomcat/webapps/openam/XUI/index.html ファイルを変更している場合、アップデート時に以下の警告が表示されます。

```
更新中 / インストール中...
   1:osstech-openam13-13.0.0-94.el7    警告: /opt/osstech/share/tomcat7/webapps/
       openam/XUI/index.html は /opt/osstech/share/tomcat7/webapps/openam/
       XUI/index.html.rpmnew として作成されました。
```

この警告が表示された場合の対応について説明します。アップデート時にこの警告が表示されなければ本項の対応は不要です。

警告が表示された場合は現在の index.html の「urlArgs の値」の修正が必要です。新しい index.html ファイルが/opt/osstech/share/tomcat/webapps/openam/XUI/index.html.rpmnew として保存されています。このファイルを確認します。

```
# view /opt/osstech/share/tomcat/webapps/openam/XUI/index.html.rpmnew
```

ファイル内の下記の記述にあるの urlArgs の値 (下記例では v=3fe9843) をコピーします。

```
            var require = {
                urlArgs : "v=3fe9843",
                deps : ['main'],
```

次に現在の index.html を開きます。

```
# vi /opt/osstech/share/tomcat/webapps/openam/XUI/index.html
```

ファイル内の urlArgs の値をコピーした値に変更してください。 現在の index.html の urlArgs の値を index.html.rpmnew ファイルと同じ値とします。

```
変更前:   urlArgs : "v=8173efa",
変更後:   urlArgs : "v=3fe9843",
```

以上で index.html の警告が表示された場合の対応は完了です。

6.7 Tomcat の起動

```
# /sbin/service osstech-tomcat start
```

6.8 アップグレードの実行

1. Tomcat が起動したら、ブラウザで OpenAM 管理者でログインする際の URL にアクセスします。

- 本書の場合は以下の URL です。
  - http://sso.example.co.jp:8080/openam/

2. 「アップグレード画面」の「OpenAM13 へのアップグレード」のリンクをクリックします。

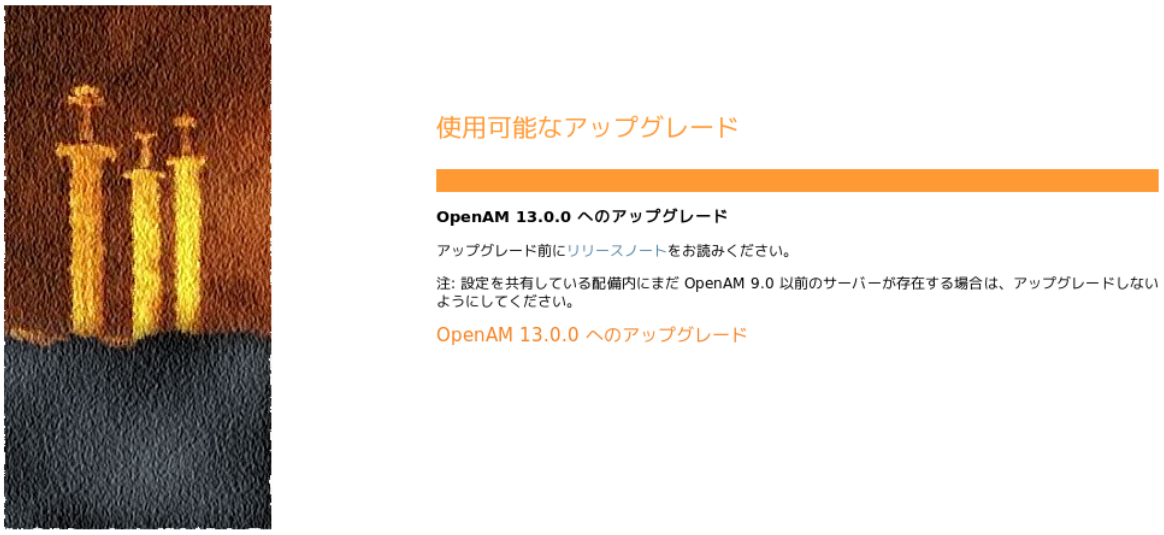

図 2　アップグレード画面

3.「ライセンス同意画面」をスクロールし、「I accept the license agreement」にチェックして「Continue」ボタンをクリックします。

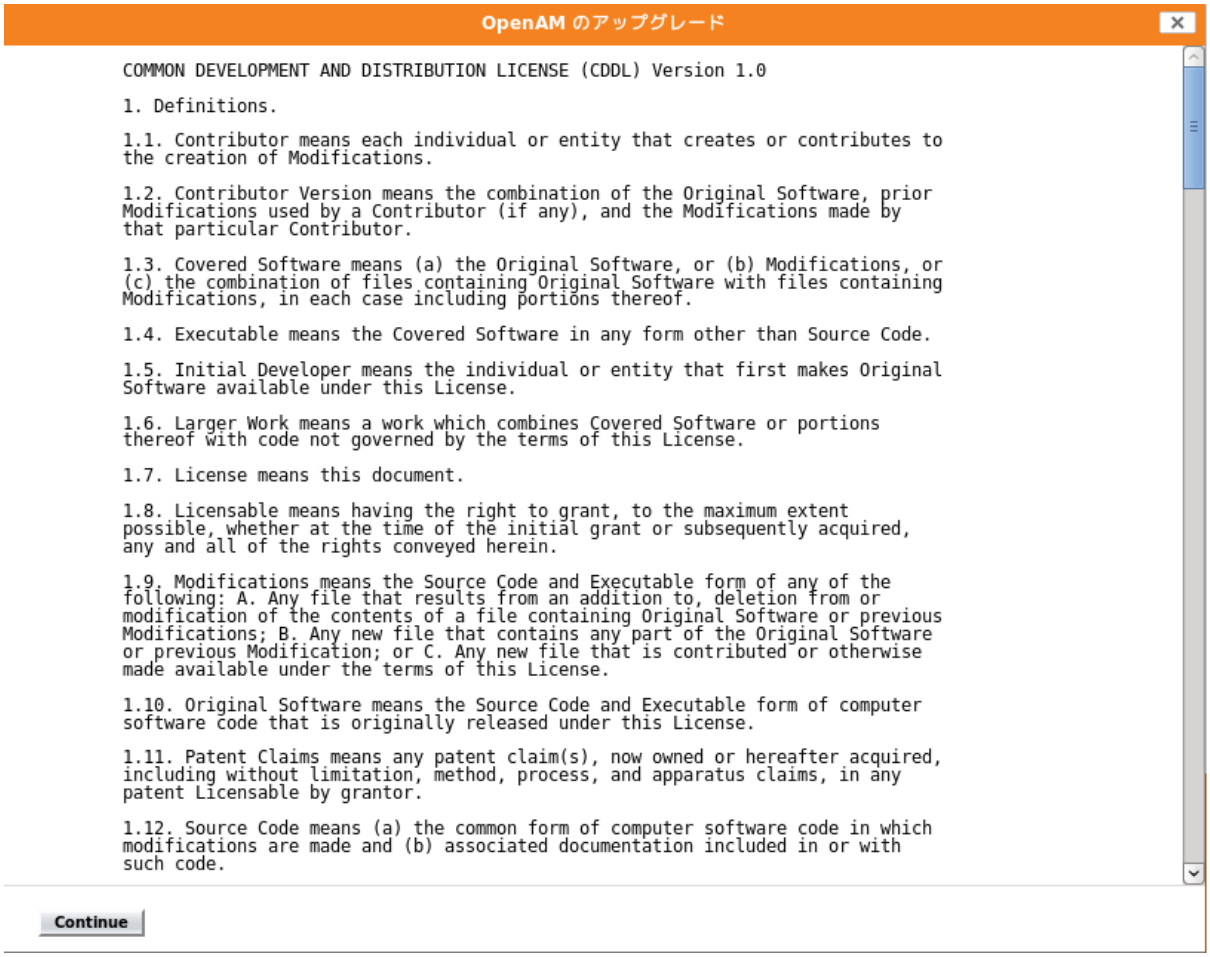

図 3　ライセンス同意画面

4. 確認画面で「アップグレード」ボタンをクリックして OpenAM をアップグレードします。

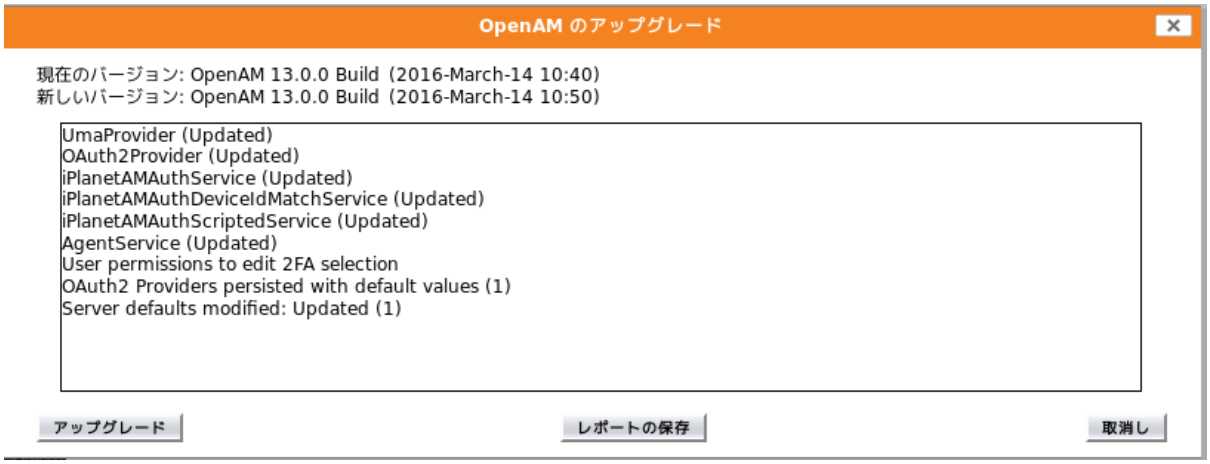

図 4　アップグレード確認画面

5. OpenAM のアップグレードが完了すると以下の画面が表示されます。

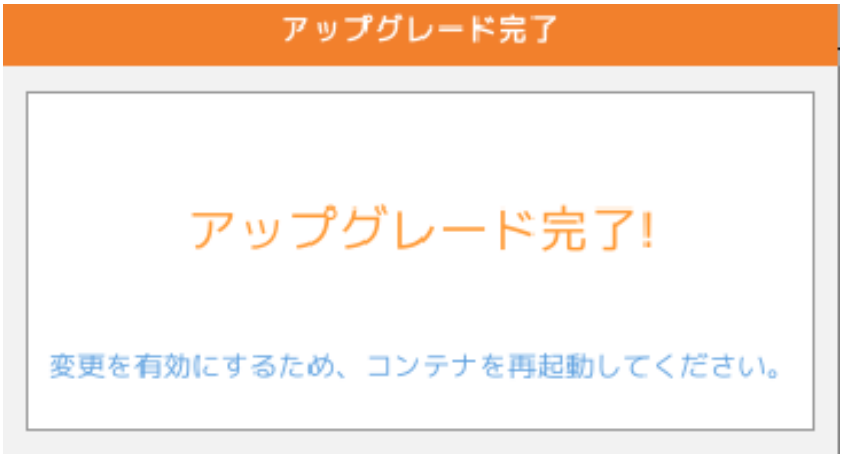

図 5　アップグレード完了画面

6.9 Tomcat 再起動

Tomcat を再起動します。

```
# /sbin/service osstech-tomcat restart
```

以上で、アップデート作業は完了です。

6.10 OpenAM2 台構成のアップデート

本節では OpenAM が 2 台で構成される場合のアップデート手順について説明します。

1. 「準備」と「Tomcat の停止」と「OpenAM 設定ディレクトリのバックアップ」を行います。
   - OpenAM1 号機,2 号機でそれぞれの号機で実行し、バックアップを取得します。
   - 本作業は片系ずつ実施可能です。片系ずつ実施する場合はもう一方を起動させた状態で取得します。
2. サービス提供を継続する場合は 2 号機のみ Tomcat を起動しておきます。
   - 負荷分散装置の振り分け設定を行い、利用者のアクセスを OpenAM2 号機のみへ振り分けます。
   - OpenAM1 号機にはアクセスが届かないようにします。
   - サービス提供の継続が不要な場合は 2 台とも Tomcat を停止しておきます。
3. OpenAM1 号機で「Tomcat の work ディレクトリの削除」と「パッケージの確認」と「パッケージのアップデート」を行います。
4. 続けて OpenAM1 号機で「Tomcat の起動」と「アップグレードの実行」と「Tomcat 再起動」を行います。
   - 「アップグレードの実行」では 1 号機のサーバーホスト名 (FQDN) でアクセスします。
5. 2. で OpenAM2 号機のみにアクセスを振り分けている場合、負荷分散装置の設定を変更し、利用者のアクセスを OpenAM1 号機のみに振り分けます。OpenAM2 号機の「Tomcat の停止」を行い、Tomcat を停止します。
6. OpenAM2 号機で「Tomcat の work ディレクトリの削除」と「パッケージの確認」と「パッケージのアップデート」を行います。
7. OpenAM2 号機で「Tomcat の起動」を行い、Tomcat を起動します。
   - OpenAM2 号機では「アップグレードの実行」の作業は不要です。
   - 4. の 1 号機アップグレードの実行を行った際に 2 号機の Tomcat が停止状態であった場合は Tomcat 起動後再度 2 号機の Tomcat 再起動を実施します。
8. 5. で OpenAM1 号機のみにアクセスを振り分けている場合、負荷分散装置の設定を元の状態 (OpenAM1,2 号機の 2 台に振り分けられる状態) に戻します。

以上で 2 台構成のアップデート作業は完了です。

7 war ファイルのデプロイ

OpenAM の war ファイルをアプリケーションサーバーにデプロイすることも可能です。本章では Tomcat にディプロイする手順を説明します。

Tomcat は事前にインストールされているものとします。(Tomcat がインストールされているディレクトリを と記載します)

7.1 OpenJDK のインストール

OpenAM の動作には OpenJDK 8 が必要です。OpenJDK 8 がインストールされていない場合はインストールしてください。

```
# yum install java-1.8.0-openjdk
```

7.2 環境変数 JAVA_HOME の設定

OpenJDK がインストールされ、環境変数「JAVA_HOME」が正しく設定されていることを確認して下さい。

なお、OSSTech Tomcat パッケージでは、設定ファイルで JAVA_HOME を指定しているため、この設定は不要です。

7.3 Java ヒープサイズの設定

OpenAM を動作させる環境では、Java のヒープサイズを 1024MB 以上に設定することを推奨します。ヒープサイズは環境変数 JAVA_OPTS により指定できます。

以下はコマンドラインで指定する例です。

```
$ export JAVA_OPTS="-Xmx1024m -XX:MaxPermSize=256m"
```

その他、OS 起動時に実行されるスクリプト内や、Tomcat の起動スクリプト内などで JAVA_OPTS を指定することもできます。なお、OSSTech Tomcat パッケージでは、設定ファイルで Java ヒープサイズを 1024MB に指定しているため、この設定は不要です。

7.4 OpenAM war ファイルの取得

OpenAM の war ファイルは OSSTech 版 OpenAM 13 パッケージの RPM(osstech-openam13) に含まれており、以下のパスにインストールされます。

- /opt/osstech/share/openam13/openam.war

war ファイルは以下の 2 通りの方法で取得可能です。

1. 「RPM パッケージのインストール」の手順で RPM をインストールし、上記のパスにインストールされた war ファイルを利用する。
2. RPM ファイルをインストールせずに展開し、war ファイルを取得する。

ここでは、後者の方法を説明します。
まず、rpm2cpio コマンドと cpio コマンドを利用して RPM ファイルを展開します。

```
$ rpm2cpio osstech-openam13-13.X.X-X.el7.noarch.rpm | cpio -id
```

上記コマンドを実行すると、RPM に含まれるファイルがカレントディレクトリに展開されます。展開されたディレクトリの中に OpenAM の war ファイルが含まれているため、この war ファイルを利用します。

```
$ ls opt/osstech/share/openam13/openam.war
opt/osstech/share/openam13/openam.war
```

7.5 OpenAM war ファイルのディプロイ

OpenAM の war ファイルを Tomcat の webapps ディレクトリにコピーします。

```
$ cp openam.war <TOMCATDIR>/webapps/
```

7.6 Tomcat の起動

Tomcat を起動します。

```
$ export LANG="en_US.UTF-8"
$ <TOMCATDIR>/bin/startup.sh
```

OSSTech Tomcat 以外のアプリケーションサーバーを利用する場合は、文字化けを防ぐために環境変数 LANG に “en_US.UTF-8” を設定してください。

7.7 初期設定の開始

Tomcat が起動したら、ブラウザで以下の URL にアクセスします。

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

「設定オプション画面」が表示されます。この画面から OpenAM の初期設定を行います。

8 コンテキスト名の変更

本章では OpenAM のコンテキスト名（デフォルト: openam）を変更する方法を説明します。デフォルトの名称から変更したい場合は「Tomcat の起動」の前に本章の作業を実施ください。

8.1 Server.xml の変更

コンテキスト名の変更は、server.xml にて行います。

```
<Host name="localhost"  appBase="webapps"
       unpackWARs="true" autoDeploy="true"
       deployIgnore="openam">

        <Context path="/[変更したい名称]]" docBase="openam"/>
</Host>
```

下記に example に変更する場合を示します。

```
<Host name="localhost"  appBase="webapps"
       unpackWARs="true" autoDeploy="true"
       deployIgnore="openam">

        <!-- openam から example に変える場合 -->
        <Context path="/example" docBase="openam"/>
</Host>
```

この設定を行うと、OpenAM のアクセスは全て下記の通りとなります。

- http://sso.example.co.jp:8080/example/

弊社ドキュメントはデフォルトの openam を想定しておりますので適宜読み替えてください

9 OpenLDAP スキーマ拡張

本章では OpenAM のデータストアとして OSSTech 版 OpenLDAP を利用する場合に必要なスキーマファイルのインストール手順について説明します。作業は OSSTech 版 OpenLDAP がインストールされているサーバーで行います。

9.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（ 画面には表示されません ）
```

9.2 RPM パッケージのインストール

rpm コマンドを使用して、別途提供された osstech-openam-ldapschema パッケージをインストールします。

```
# rpm -ivh osstech-openam-ldapschema-X.X-X.el7.noarch.rpm
```

9.3 スキーマの有効化

/opt/osstech/etc/openldap/slapd.conf に下記の定義を追加し、インストールした OpenAM 用のスキーマファイルを読み込むように設定します。

```
include /opt/osstech/etc/openldap/schema/openam.schema
include /opt/osstech/etc/openldap/schema/saml2.schema
```

設定変更後、OpenLDAP を再起動します。

```
# /sbin/service osstech-ldap restart
```

10 改版履歴

- 2016 年 3 月 14 日 リビジョン 1.0
  - 初版作成
- 2016 年 8 月 25 日 リビジョン 2.0
  - テンプレート変更
- 2016 年 10 月 18 日 リビジョン 2.1
  - OpenJDK のバージョンを 8 に変更
- 2017 年 03 月 23 日 リビジョン 2.2
  - OpenAM2 台構成のアップデートを追加
- 2017 年 12 月 22 日 リビジョン 2.3
  - アップデート手順に python-requests パッケージの依存エラー対応を追加
- 2018 年 03 月 13 日 リビジョン 2.4
  - アップデート手順に index.html の警告表示の対応を追加
- 2019 年 03 月 12 日 リビジョン 2.5
  - アップデート手順に 1 号機アップデート時に 2 号機を停止していた場合 2 号機 Tomcat の再起動手順を追加
- 2020 年 01 月 21 日 リビジョン 2.6
  - osstech-openam-ldapschema パッケージに関する記載を変更
- 2020 年 06 月 15 日 リビジョン 2.7
  - アップグレードの実行の分かり辛い URL の記載を変更