OpenAM 11 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)

作成日: 2013 年 12 月 26 日

更新日： 2021 年 9 月 10 日

リビジョン: 1.8

目次

1. はじめに

1.1 本文書の目的

本文書は OpenAM 11 パッケージを導入するための手順書です。OpenAM 11 パッケージのインストールの際に、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

本文書は、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化すること。
    - 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。
- root ユーザーで作業すること。(作業ユーザーを指定している場合を除く)
- OSSTech 製品パッケージファイル群をインストール対象 OS 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(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. Linux 版パッケージ

本章では弊社が提供する Linux 版 OpenAM 11 パッケージのインストール手順を説明します。

3.1 システム要件

3.1.1 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 6 (x86/x86_64)
- Red Hat Enterprise Linux 7 (x86_64)
- CentOS 6(x86/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
    - osstech-openam11-11.0.0-120 から利用する Java のバージョンが 8 に変更になりました
- OS 標準 Tomcat (RHEL7/CentOS7)

3.2 パッケージ構成

弊社が提供する OpenAM 11 は以下のパッケージにより構成されています。

- OSSTech ソフトウェア製品基本パッケージ
    - osstech-base
    - osstech-support
    - osstech-daemontools(RHEL7/CentOS7)
- OSSTech Tomcat パッケージ
    - osstech-tomcat7(RHEL6/CentOS6)
    - osstech-tomcat(RHEL7/CentOS7)
- OSSTech OpenAM 11 パッケージ
    - osstech-openam11

3.3 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。

3.3.1 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。

下記の例では/srv/osstech-work/software/RPMS に展開したことを前提とて記述します。

3.3.2 依存パッケージのインストール

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
```

OpenJDK8

OpenAM の動作には OpenJDK8 が必要です。OpenJDK8 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
```

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
```

3.3.3 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。

RHEL6/CentOS6 の場合

```
# cd /srv/osstech-work/software/RPMS/openam11
# ls base
osstech-base-3.0-XX.el6.noarch.rpm
osstech-support-3.0-XX.el6.noarch.rpm
# ls openam
```

```
osstech-openam11-11.X.X-X.el6.noarch.rpm
osstech-openam11-tools-11.X.X-X.el6.noarch.rpm
osstech-tomcat7-7.0.X-X.el6.noarch.rpm
```

RHEL7/CentOS7 の場合

```
# cd /srv/osstech-work/software/RPMS/openam11
# ls base
osstech-base-3.0-XX.el7.noarch.rpm
osstech-support-3.0-XX.el7.noarch.rpm
osstech-daemontools-1.03-X.x86_64.rpm
# ls openam
osstech-openam11-11.X.X-X.el7.noarch.rpm
osstech-openam11-tools-11.X.X-X.el7.noarch.rpm
osstech-tomcat-7-instance1.0.0-X.el7_X.X.X.X.noarch.rpm
```

3.3.4 パッケージのインストール

rpm コマンドを使用して、RPM パッケージをインストールします。

```
# rpm -ivh base/*.rpm
# rpm -ivh openam/*.rpm
```

3.3.5 Tomcat の起動

Tomcat を起動します。

RHEL6/CentOS6 の場合

```
# /sbin/service osstech-tomcat7 start
```

RHEL7/CentOS7 の場合

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

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「5 コンテキスト名の変更」を実施ください。

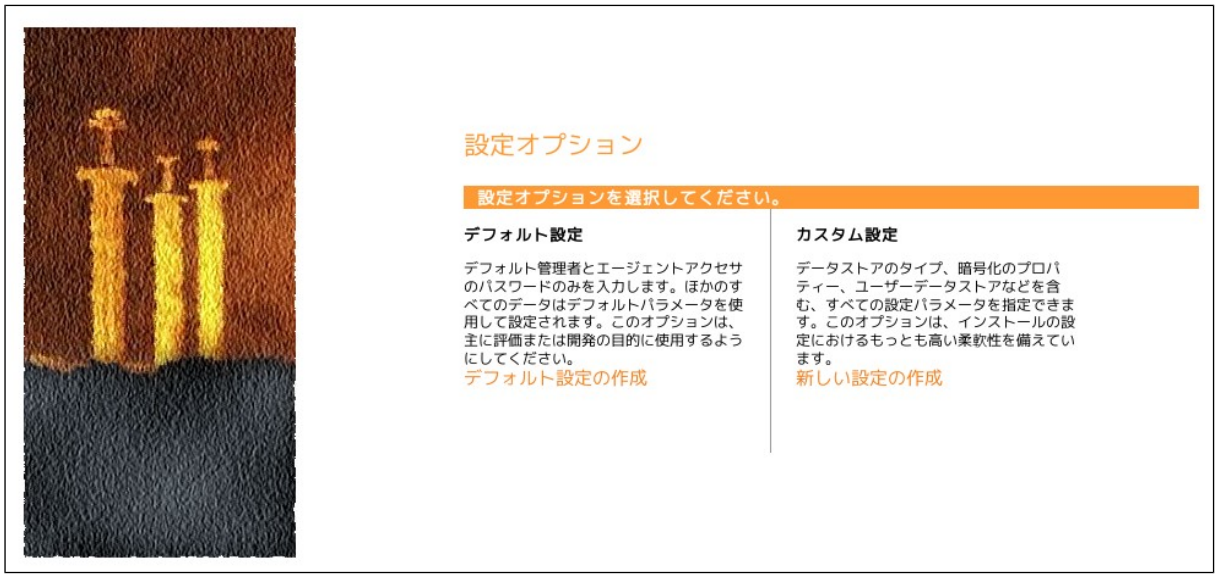

図 1:設定オプション画面

以上でパッケージのインストールは完了です。

3.4 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。

3.4.1 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、最初に 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。

下記の例では/srv/osstech-work/software/RPMS に展開したことを前提とて記述します。

3.4.2 依存パッケージのインストール

OpenJDK8

osstech-openam11-11.0.0-120 から利用する Java のバージョンが 8 に変更になりました。動作には OpenJDK8 が必要です。OpenJDK8 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
```

3.4.3 Tomcat の停止

Tomcat を停止します。

RHEL6/CentOS6 の場合

```
# /sbin/service osstech-tomcat7 stop
```

RHEL7/CentOS7 の場合

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

3.4.4 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/tomcat7/openam」、バックアップ先は「/root/backup/conf」です。

```
# mkdir -p /root/backup/conf
# cd /opt/osstech/var/lib/tomcat7
# cp -pir openam /root/backup/conf
```

3.4.5 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/tomcat7/work/Catalina/localhost/openam
```

3.4.6 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。

RHEL6/CentOS6 の場合

```
# cd /srv/osstech-work/software/RPMS/openam11
# ls base
osstech-base-3.0-XX.el6.noarch.rpm
osstech-support-3.0-XX.el6.noarch.rpm
# ls openam
osstech-openam11-11.X.X-X.el6.noarch.rpm
osstech-openam11-tools-11.X.X-X.el6.noarch.rpm
osstech-tomcat7-7.0.X-X.el6.noarch.rpm
```

RHEL7/CentOS7 の場合

```
# cd /srv/osstech-work/software/RPMS/openam11
# ls base
osstech-base-3.0-XX.el7.noarch.rpm
osstech-support-3.0-XX.el7.noarch.rpm
osstech-daemontools-1.03-X.x86_64.rpm
# ls openam
osstech-openam11-11.X.X-X.el7.noarch.rpm
```

```
osstech-openam11-tools-11.X.X-X.el7.noarch.rpm
osstech-tomcat-7-instance1.0.0-X.el7_X.X.X.X.noarch.rpm
```

3.4.7 パッケージのアップデート

最初に base ディレクトリに含まれるパッケージのアップデートを rpm コマンドで行います。

```
# rpm -Uvh base/*.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ディレクトリから除いておき、再度アップデートを試みます。

```
# rpm -Uvh base/*.rpm
準備中...    ########################################### [100%]
        パッケージ osstech-base-3.0-81.el6 は既にインストールされています。
        パッケージ osstech-support-3.0-81.el6 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。

続いて OpenAM パッケージをアップデートします。

```
# rpm -Uvh openam/*.rpm
```

3.4.8 Tomcat の起動

Tomcat を起動します。

RHEL6/CentOS6 の場合

```
# /sbin/service osstech-tomcat7 start
```

RHEL7/CentOS7 の場合

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

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/

以下の「アップグレード画面」が表示された場合は、「OpenAM11 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

以下の確認画面で「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。

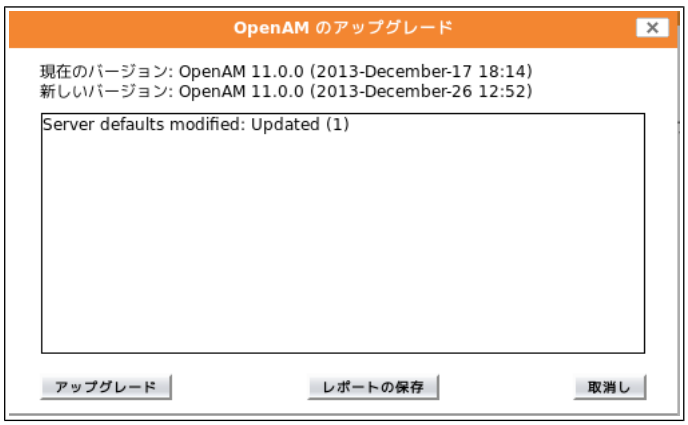

図 3: アップグレード確認画面

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。

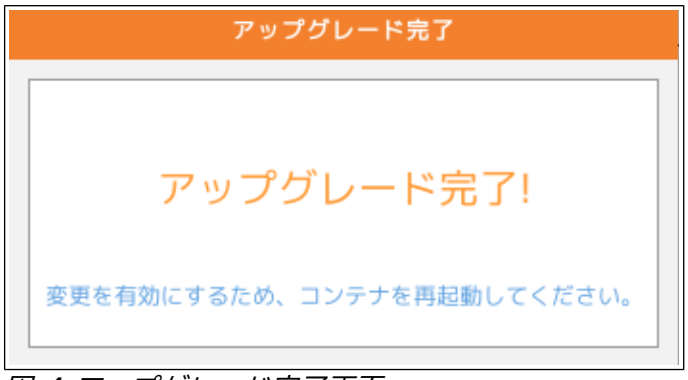

図 4:アップグレード完了画面

3.4.9 Tomcat の設定変更 1

最新の Tomcat 7 では URL のクエリーに “[“ や “]” を利用できない仕様となりました。

OpenAM11 の管理コンソールの一部では “[“ や “]” をクエリーとして利用しているため、デフォルトの設定では当該の画面を表示させると HTTP ステータスコード 400（Bad Request）が返却されます。

これを回避するためには、server.xml で管理コンソールへのアクセスで利用する HTTP コネクターに対して relaxedQueryChars を設定してください。

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" relaxedQueryChars="[]" />
```

relaxedQueryChars の詳細は Tomcat 7 のリファレンスをご覧ください。

https://tomcat.apache.org/tomcat-7.0-doc/config/http.html

3.4.10 Tomcat の設定変更 2 (RHEL6/CentOS6)

RHEL6/CentOS6 向けパッケージ同梱の osstech-tomcat7 はバージョン 7.0.0-100 のリリースより AJP コネクターにシークレット（共通鍵）がデフォルトで必須となりました。

RHEL6/CentOS6 の OS 標準 Apache HTTP Server には AJP 接続にシークレットを設定する機能がありません。AJP を利用している場合、Tomcat の設定でシークレットを無効化する必要があります。

server.xml で AJP コネクターに対して secretRequired="false" を設定してください。

```
    <Connector protocol="AJP/1.3"
               secretRequired="false"
               port="8009"
               redirectPort="8443" />
```

secretRequired の詳細は Tomcat 7 のリファレンスをご覧ください。

https://tomcat.apache.org/tomcat-7.0-doc/config/ajp.html

3.4.11 Tomcat の再起動

Tomcat を再起動します。

RHEL6/CentOS6 の場合

```
# /sbin/service osstech-tomcat7 restart
```

RHEL7/CentOS7 の場合

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

以上でアップデートは完了です。

4. 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<TOMCATDIR>と記載します)

4.1 事前準備

4.1.1 OpenJDK のインストール

OpenAM の動作には OpenJDK8 が必要です。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。

下記のコマンドは RHEL 環境で OS 標準の OpenJDK8 をインストールする例です。

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

4.1.2 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。

4.1.3 JAVA ヒープサイズ

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。

4.1.4 OpenAM war ファイルの取得

OpenAM の war ファイルは OSSTech 版 OpenAM 11 パッケージの RPM(osstech-openam11)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/openam11/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. 「3.3 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、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、「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」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-openam11-11.X.X-X.el6.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/openam11/openam.war
opt/osstech/share/openam11/openam.war
```

4.2 インストール

4.2.1 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/
```

4.2.2 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。

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(図 1:設定オプション画面)。この画面から OpenAM の初期設定を行います。

以上でインストールは完了です。

5. 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「3.3.5 Tomcat の起動」の前に本章の作業を実施ください。

5.1 Sever.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/

弊社ドキュメントばデフォルトの openam を想定して書かれておりますので適宜読み替えてください。

6. 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。

6.1 システム要件

6.1.1 ソフトウェア要件

以下のソフトウェアが必要です。

- OSSTech 版 OpenLDAP

6.2 パッケージ構成

弊社が提供する OpenAM 用 LDAP スキーマは以下のパッケージにより提供されています。

- OpenAM 用 LDAP スキーマパッケージ
  - osstech-openam-ldapschema

6.3 スキーマファイルパッケージのインストール

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。

6.3.1 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、最初に 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。

下記の例では/srv/osstech-work/software/RPMS に展開したことを前提とて記述します。

6.3.2 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。

```
# cd /srv/osstech-work/software/RPMS
# ls ldapschema
```

```
osstech-openam-ldapschema-1.X-X.el6.noarch.rpm
```

6.3.3 RPM パッケージのインストール

rpm コマンドを使用して、RPM パッケージをインストールします。

```
# cd ldapschema
# rpm -ivh osstech-openam-ldapschema-1.X-X.el6.noarch.rpm
```

6.3.4 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
```

以上で完了です。

7. 改版履歴

- 2013年12月26日　リビジョン 1.0
  - 初版作成
- 2014年3月24日　リビジョン 1.1
  - 「3.3.2 依存パッケージのインストール」に ksh のインストール手順を追記。
- 2014年4月16日　リビジョン 1.2
  - 「3.1.1 ソフトウェア要件」の対象 OS を修正。
- 2014年8月25日　リビジョン 1.3
  - RPM パッケージのアップデート手順に「3.4.4 OpenAM 設定ディレクトリのバックアップ」を追加。
- 2015年1月13日　リビジョン 1.4
  - 「5 コンテキスト名の変更」を追加。
- 2015年7月10日　リビジョン 1.5
  - RHEL7/CentOS7 に対応。
- 2018年2月1日　リビジョン 1.6
  - 依存パッケージを OpenJDK7 から OpenJDK8 に変更。
- 2018年10月15日　リビジョン 1.7
  - RPM パッケージのアップデート手順に「3.4.9 Tomcat の設定変更 1」を追加。
- 2021年9月10日　リビジョン 1.8
  - RPM パッケージのアップデート手順に「3.4.10 Tomcat の設定変更 2 (RHEL6/CentOS6)」を追加。