OpenAM 技術 Tips

Vol.2

OpenAM SAML 設定手順

執筆者：オープンソース・ソリューション・テクノロジ株式会社

唐木　大介

監修：　OpenAM コンソーシアム

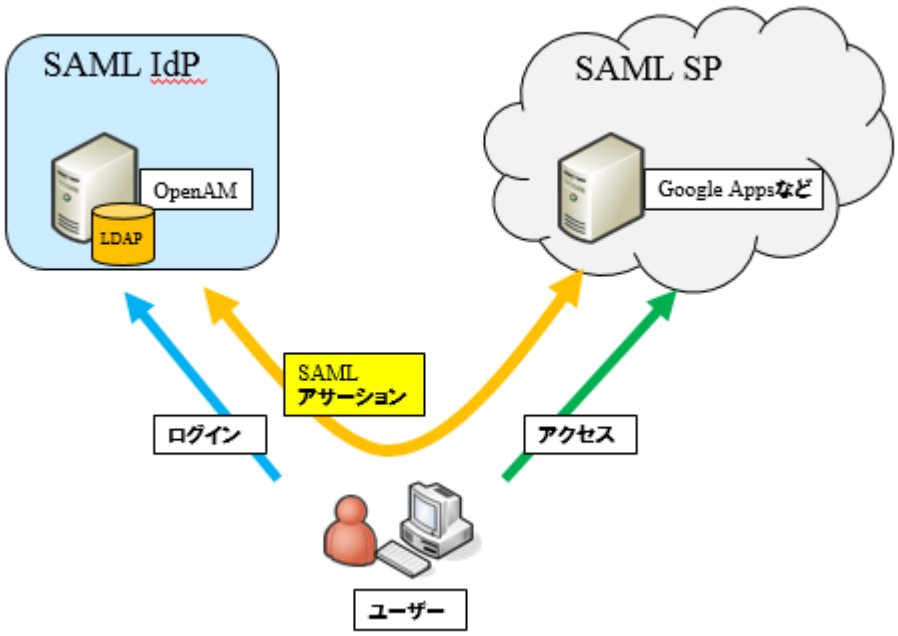
目次

1．はじめに

OpenAM は旧 Sun Microsystems 社の OpenSSO をベースに ForgeRock 社が開発を行うオープンソースソフトウェアであり、Web アプリケーションやクラウドサービスへのシングルサインオン（以降 SSO）を実現します。本資料では、この OpenAM の SAML 機能を用いて、Google Apps for Work（以降 Google Apps）を例にクラウドサービスとのシングルサインオンが可能になるまでの検証を目的とした構築手順を紹介します。

シングルサインオンに利用可能なフェデレーションのプロトコルはいくつかありますが、現時点では組織におけるシングルサインオン用途では、SAML の利用が一般的です。Google Apps のほかにも Salesforce などクラウドサービスが SAML による SSO に対応しています。

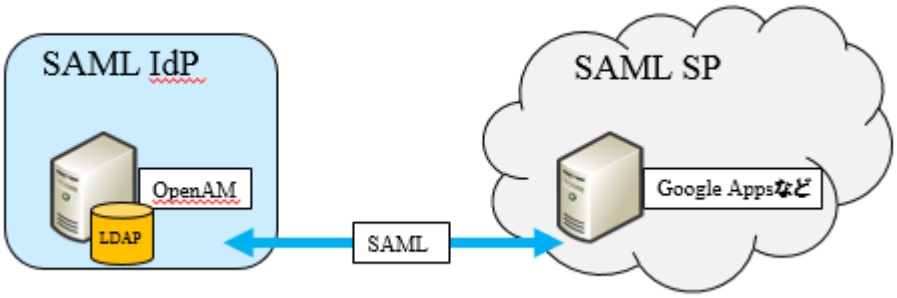
SAML とは Security Assertion Markup Language の略でサムルと発音します。
アサーションとは認証や認可の情報を表し、認証サーバーである OpenAM とサービスを提供するアプリケーションの間でこの情報を受け渡すことにより SSO を実現します。 この場合 OpenAM を IdP（アイデンティティープロバイダ、アイディピー）と呼び、アプリケーションを SP（サービスプロバイダ、エスピー）と呼びます。
IdP と SP の通信方法（バインディング）にはいくつかの方法がありますが、ブラウザを介してアサーションを渡す HTTP Redirect Binding、HTTP POST Binding と呼ばれるバインディングを用いると、IdP と SP 双方と通信できるブラウザがあれば組織内の IdP とクラウド上の SP の直接通信の必要がなく、ファイヤーウォール等に設定を追加をしなくても SSO ができます。



２．目的

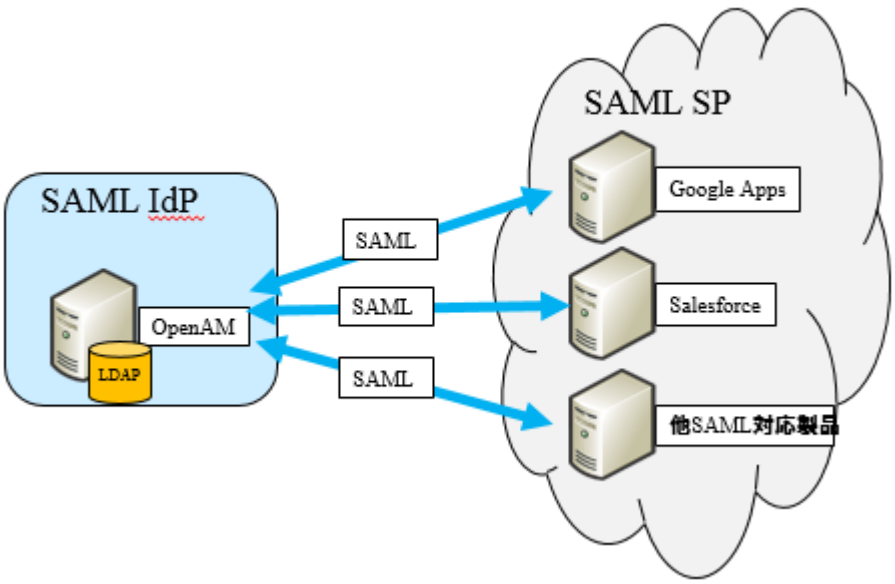
本構築手順を実施する事で、Google Apps のユーザー認証を OpenAM で行う環境を構築することを目的とします。

・Google Apps の認証に OpenAM を利用する構成



本構築手順で紹介する SAML の構成手順を応用することで、複数のアプリケーション（SAML SP）をシングルサインオンで利用できるようになります。

・複数のアプリケーションを OpenAM で SSO する構成



３．推奨環境

OpenAM をインストールするサーバー環境の推奨環境は以下の通りです。

・サーバーOS：Linux, Windows, UNIX
・メモリ：2GB 以上（JVM ヒープサイズ）
・JDK：1.6 以上
・アプリケーションコンテナ（例. Apache Tomcat, JBoss, …etc）

詳細については ForgeRock 社サイト（OpenAM Release Notes）をご参照下さい。

本構築手順では以下環境を前提としています。

・サーバーOS：CentOS 6.5
・メモリ：2GB
・JDK：OpenJDK 1.7.0_71
・アプリケーションコンテナ：Apache Tomcat 6.0.24
・OpenAM：OpenAM-13.0.0-SNAPSHOT_20150331.war

４．事前準備

Vol.1「OpenAM インストール手順」で構築された OpenAM サーバーを用意してください。

OpenAM サーバーを用意できましたら下記項目を確認してください。

項目	内容
ホスト名	ホスト名が「sso1.example.com」となっている
時刻同期	OS の時刻同期がされている
テストユーザー	openldapuser01 が登録されている ※外部ユーザーデータストアの OpenLDAP に登録済みである

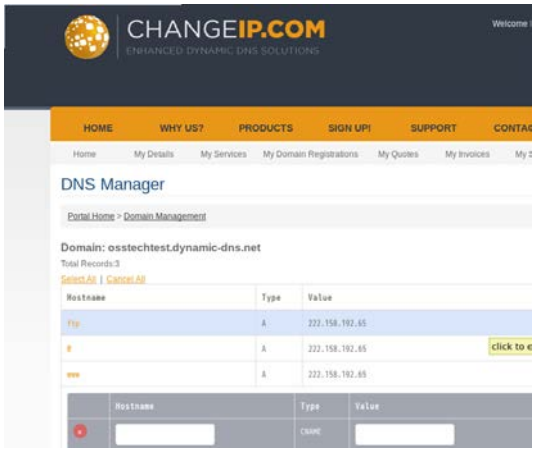
事前準備には以下に説明する3つの準備が必要です。

・Google Apps で利用するドメインの取得

Google Apps ではユーザー組織の識別名としてドメイン名を利用するため、あらかじめ Google Apps で利用するドメイン名を所有している必要があります。ただし、このドメイン名はダイナミック DNS を利用した無償のものでも対応可能です。本書では「ko.my03.com」という名前で用意しました。

TXT レコードまたは CNAME を自分で変更できるダイナミック DNS サービスを利用すると便利です。

今回は www.changeip.com を利用しました。



・Google Apps 30 日試用の申し込み

無償で 30 日間の試用が可能です。　SAML による SSO 機能も試用できます。

無料試用については以下の URL を参照ください。管理者としてログインできるところまで準備しておく必要があります。

https://www.google.co.jp/intx/ja/work/apps/business/faq/free-trial.html

・SAML 署名鍵と証明書の生成（※今回の環境を、継続し実運用に利用する場合必須）

実運用では OpenAM 付属のテスト用の鍵とは別に、組織固有の鍵と証明書を使う必要があります。OpenAM 付属のテスト用の鍵と証明書をそのまま利用すると簡単に IdP のなりすましをされる恐れがあり危険です。

実際の手順は「10. 本番運用における署名鍵の作成方法」に記載しています。検証のみの場合は設定を行わなくても

動作可能です。

５．構築手順の概要

SAML の IdP と SP の設定は、OpenAM と Google Apps の両方に登録する必要があります。

以下の順番で構築を行います。

・OpenAM でのアイデンティティープロバイダの作成

OpenAM に SAML の認証サーバーとして IdP を構築します。

※IdP の構築は一度だけ行えば、複数の SP に対応できます。

・OpenAM への Google Apps の接続登録

OpenAM に構築した IdP に Google Apps を SP として登録します。

・Google Apps でのシングルサインオンの設定

Google Apps の SSO 設定に OpenAM を SAML IdP として登録し、SSO を有効にします。

6．OpenAM でのアイデンティティープロバイダの作成

クライアント上のブラウザから http://sso1.example.com:8080/openam/にアクセスし、トップ画面の「ホストアイデンティティープロバイダの作成」をクリックします。

・アイデンティティープロバイダの作成

署名鍵はプルダウンより「test」または、組織固有のものを選択し、トラストサークルは「新しいトラストサークル」に任意の名前を入れ「設定」をクリックします。

※組織固有のものを選択するには、キーストアに署名鍵を先に入れておく必要があります。キーストアに署名鍵を入れる手順は付録を参照してください。

アイデンティティープロバイダの作成完了

この画面にある「Google Apps の設定」から引き続き Google Apps を SP として追加する手順へ進めます。

または、OpenAM ログイン直後の画面より「Google Apps の設定」を選ぶことにより設定作業を開始できます。

7．OpenAM への Google Apps の接続登録

リモート SP のドメイン名に Google Apps 申し込み時に利用したドメイン名を入力し、「作成」を押します。

メタデータは正確に設定された旨の表示がでますので、「了解」を押します。

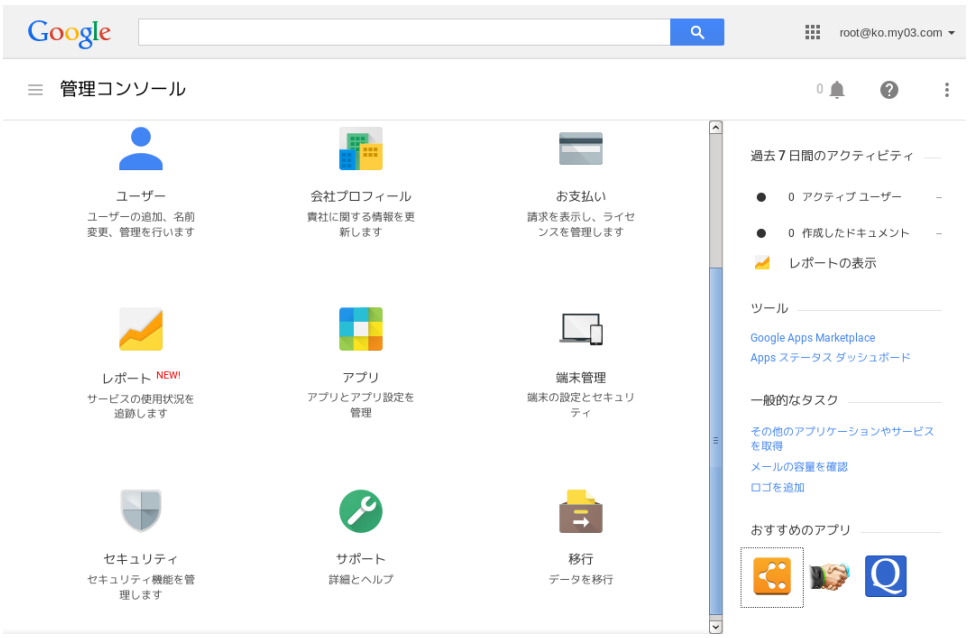
以上で、OpenAM サーバー側の設定は完了です。
検証証明書は Google Apps の設定画面へアップロードするため、ダウンロードしておきます。
「ダウンロードするには、ここをクリックします。」をクリックすると、OpenSSOCert.txt というファイル名でダウンロードできます。
この後の手順で、OpenAM 画面に表示された3つの設定値を、Google Apps シングルサインオン設定画面の所定のフォームへコピー入力するので、このウィンドウは閉じずに、ブラウザの別ウィンドウで Google Apps の管理コンソールへログインしてください。

ここで表示された URL は下記のとおりです。

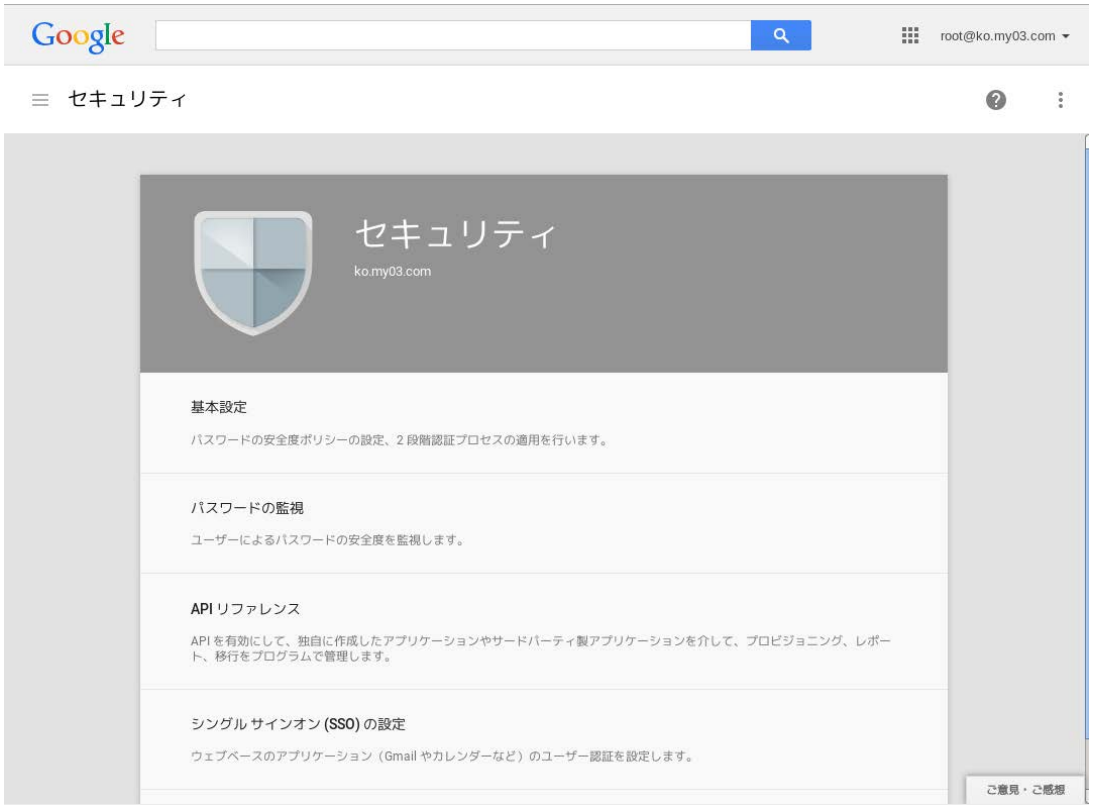
項目	URL
サインインページの URL	http://sso1.example.com:8080/openam/SSORedirect/metaAlias/idp
サインアウトページの URL	http://sso1.example.com:8080/openam/UI/Logout?goto=http://sso1.example.com:8080/openam/
パスワード変更の URL	http://sso1.example.com:8080/openam/idm/EndUser

8．Google Apps でのシングルサインオンの設定

Google Apps 管理コンソールへログインし、「セキュリティ」アイコンを選択します。



セキュリティ設定画面の一番下、「シングルサインオン（SSO）の設定」を選択します。



「サードパーティの ID プロバイダで SSO を設定するにチェック」を入れます。
「ログインページの URL」「ログアウトページ URL」「パスワード変更 URL」にはそれぞれ、
先ほど OpenAM に表示された「サインインページの URL」「サインアウトページの URL」「パスワード変更の URL」をコピーペーストします。
証明書は OpenAM 画面からダウンロードしたものをアップロードします。
「ドメイン固有の発行元を使用」にチェックを入れ「変更を保存」を押します。

念のため設定で意図した動作がうまくいかなかったときのために SSO が適用される範囲を限定しておいたほうが安全です。画面下部にあるネットワークマスクの設定をよく読み適用範囲のアドレスを設定してください。

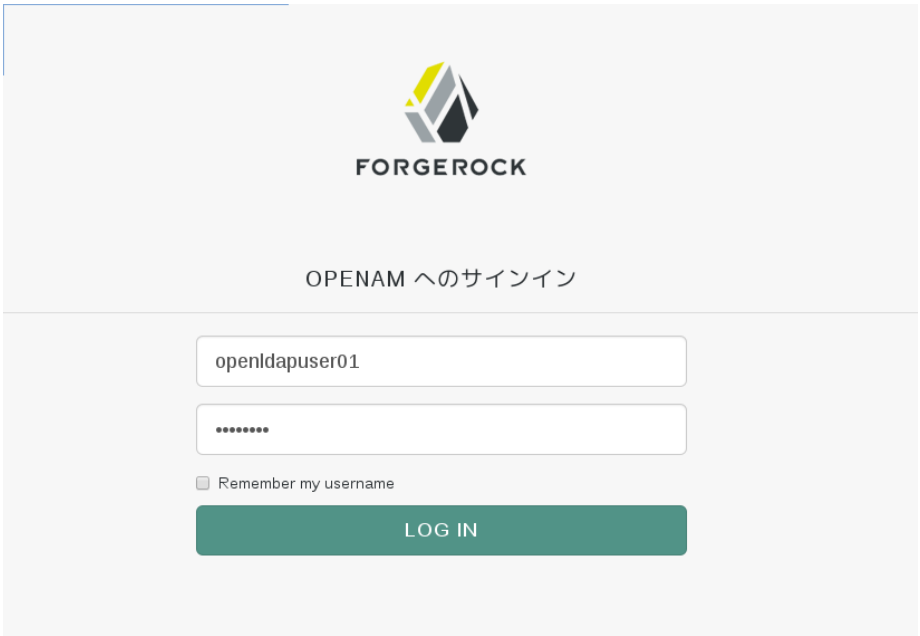
シングルサインオンには Google Apps 側にもアカウント登録が必要なので、OpenAM にログインできるユーザーと同じログイン ID になるよう作成しておきます。

以上で、Google Apps 側の設定は完了です。

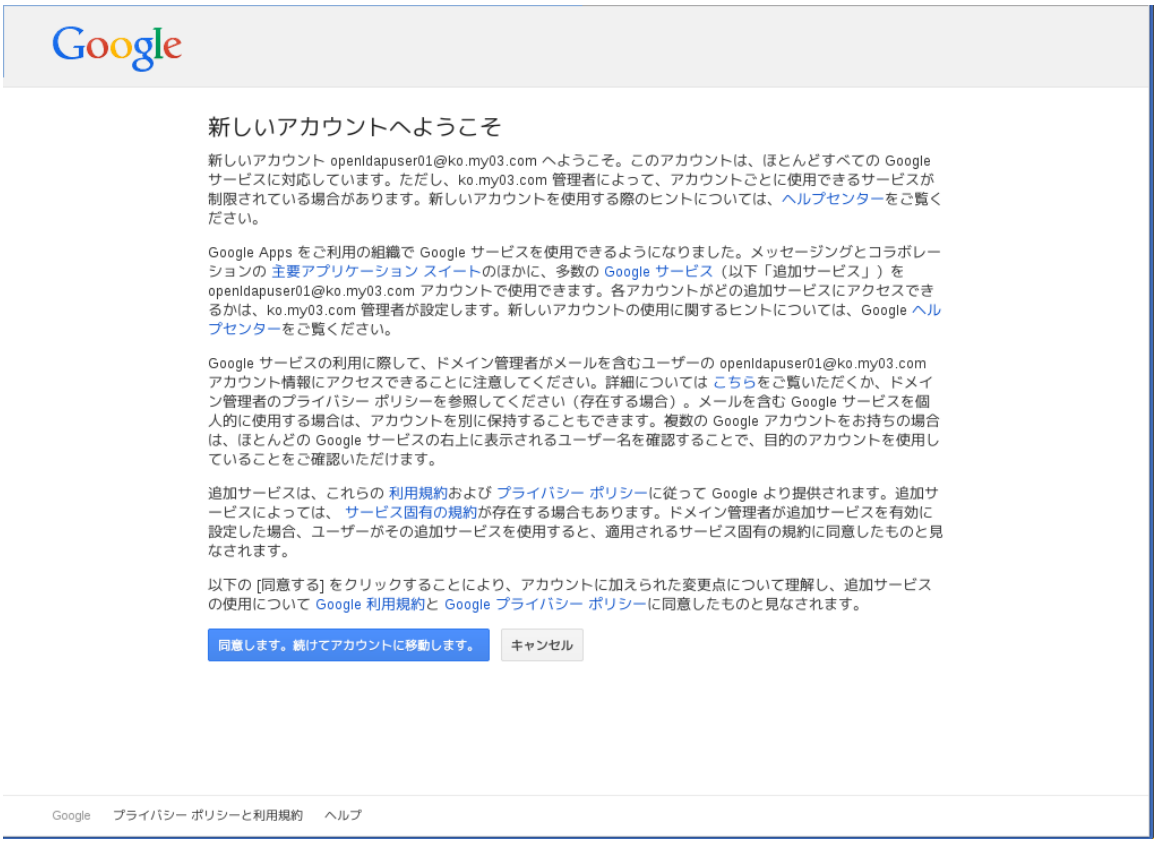
９．動作確認

SAML の設定完了後、Google Apps へアクセスし SSO の動作を確認します。
組織の Google Apps URL(例 https://mail.google.com/a/組織ドメイン名)へアクセスします。

OpenAM ログイン画面が表示されるので、openldapuser01 でログインします。



Google Apps へログインしたことが無いユーザーの場合はアカウントの確認等が必要になりますので、画面の指示に従います。



openlpdauser01 の Gmail 画面が表示されれば SAML の SSO は成功です。

１０．　本番運用における署名鍵の作成方法

本章では組織固有の SAML 用署名鍵の作成と OpenAM での利用設定について説明します。
SAML メッセージに対して署名を行なうための署名鍵を作成し、OpenAM で利用できるように設定します。
OpenAM にはデフォルトで「test」という署名鍵が登録されていますが、これは全ての OpenAM に含まれる共通の鍵であるため、IdP のなりすましなどの脆弱性につながります。そのため、署名鍵を新規に作成し OpenAM にインポートします。

- キーストアと鍵ペアの生成

JDK の keytool コマンドを利用して、鍵ペアを作成します。

```
$ keytool -genkeypair ¥
-keyalg rsa ¥
-alias openam-idp ¥
-dname "CN=sso1.example.com,OU=development,O=EXAMPLE,L=Shinagawa-ku,ST=Tokyo,C=JP" ¥
-keypass    R8g%kWg3 ¥              # 署名鍵のパスワードを指定
-keystore mykeystore.jks ¥      # キーストアファイル名を指定
-storepass changeit ¥            # キーストアのパスワードを指定
-validity 3650 ¥                 # 鍵の有効期限を指定(例:10 年)
-keysize 2048                      # 鍵の長さを指定
```

「¥(バックスラッシュ)」はコマンドラインの途中で改行を行うために入力しています。「¥」を入れずに、全ての オプションを一行で指定することも可能です。「#」以降の文字列はコメントであるため、実際にはコマンドラインに入力する必要はありません。

各オプションについて説明します。

-genkeypair
　　鍵ペアを新規に作成するオプションです。

-keyalg アルゴリズム名
　　鍵ペアを生成するのに使うアルゴリズムを指定します。

-alias エイリアス名
　　証明書の別名を指定します。任意の名前を指定可能です。

-dname 識別名
　　識別名を指定します。

-keypass パスワード
　　署名鍵のパスワードを指定します。

-keystore　キーストアファイル名
　　キーストアファイル名を指定します。

-storepass パスワード

キーストアのパスワードを指定します。

-validity 日数

署名鍵の有効期限を日数で指定します。

-keysize ビット数

署名鍵の長さをビットで指定します。

➢ キーストアと鍵ペアの配置

作成した鍵ペアを OpenAM で利用できるように設定します。
まず、作成したキーストアファイルを任意のパスに配置します。このとき、キーストアファイルを Tomcat プロセスの実行ユーザーである”tomcat”が読み取れるようにパーミッションを設定します。キーストアファイルを「mykeystore.jks」と仮定して説明します。

```
# mkdir -p /usr/share/tomcat/openam/openam/private
# cp    mykeystore.jks /usr/share/tomcat/openam/openam/private
# chown -R root:tomcat /usr/share/tomcat/openam/openam/private
# chmod 750 /usr/share/tomcat/openam/openam/private
# chmod 640 /usr/share/tomcat/openam/openam/private/mykeystore.jks
```

➢ キーストアと鍵ペアのパスワードファイルを作成

キーストアと鍵ペアファイルに設定されているパスワードをそれぞれ符号化して、テキストファイルに保存します。このテキストファイルは OpenAM がキーストアと鍵ペアを読み込む際に使用します。パスワードの符号化は OpenAM の管理者コンソール(ブラウザ)から、以下の手順で行ないます。
なお、テキストファイルはキーストア用ファイルと鍵ペア用ファイルに分けて保存します。ここでは、キーストア用の符号化パスワードファイルの作成方法のみ説明します。鍵ペアにおいても、同様の手順で符号化パスワードをファイルに保存してください。ファイル名は任意です。

OpenAM に管理者ユーザーでログインします。
ブラウザのアドレスバーに以下の URL を入力し、Enter を押下します。
http://sso1.example.com:8080/openam/encode.jsp
「符号化するパスワードを入力してください」のテキストエリアにキーストアのパスワードを入力し、「符号化」ボタンを押下します。キーストアのパスワードとは、「0」で、keytool コマンドの「-storepass」オプションで指定したパスワードです。
ブラウザ画面に表示された符号化されたパスワードを、以下のコマンドを実行して任意のファイルに保存します。ここでは、/usr/share/tomcat/openam/openam/private/.storepass に保存したと仮定します。符号化パスワードの末尾に改行コード(¥n)が入ると OpenAM からの読み込みに失敗するため、tr コマンドを利用してファイル末尾の改行コードを削除しています。

```
# cd /usr/share/tomcat/openam/openam/private/
# vim .storepass
```

エンコードされたキーストアのパスワードを入力して保存

```
# tr -d '¥n' < .storepass    > tmp && mv tmp .storepass
```

ファイルパーミッションを設定します。

```
# chown root:tomcat /usr/share/tomcat/openam/openam/private/.storepass
# chmod 640 /usr/share/tomcat/openam/openam/private/.storepass
```

以上で完了です。

鍵ペアについても、同様の手順で符号化後のパスワードをファイルに保存します
(/usr/share/tomcat/openam/openam/private/.keypass として保存したと仮定します)。

➢ OpenAM のキーストア設定を変更

OpenAM の管理コンソールから、新規に作成したキーストアと鍵ペアを使用するように設定を変更します。
OpenAM に管理者ユーザーでログインします。
「設定」→「サーバーおよびサイト」→「デフォルトのサーバー設定値」→「セキュリティ」を開きます。
「キーストア」セクションの各項目に以下の値を入力します。

※注意:OpenAM を冗長化構成(サイト構成)で構築している場合、この設定を変更すると全ての OpenAM サーバーのキーストア設定が変更されます。そのため、全ての OpenAM サーバーに新しい SAML 用署名鍵を配置してから、設定を変更してください。

「キーストアファイル」:/usr/share/tomcat/openam/openam/private/mykeystore.jks
「キーストアパスワードファイル」:/usr/share/tomcat/openam/openam/private/.storepass
「非公開鍵パスワードファイル」:/usr/share/tomcat/openam/openam/private/.keypass
「証明書エイリアス」:openam-idp

画面右上の「保存」ボタンを押下します。
設定を反映させるため OpenAM サーバーの Tomcat を再起動してください。

以上で完了です。

１１．　おわりに

今回は、Google Apps を例に手順を説明しましたが、同様の手順で他のアプリケーション(SAML SP)をシングルサインオンで利用することができますので、本書を参考にお試しいただければ幸いです。

また、引き続き OpenAM の検証を行う場合は、公開されたマニュアル等をご参照下さい。

参考資料

OpenAM Release Notes
http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/release-notes/index/index.html

OpenAM Installation Guide
http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/install-guide/index.html

OpenAM Nightly Builds
http://forgerock.org/downloads/openam-builds/

OpenAM コンソーシアム　OpenAM インストール手順
http://www.openam.jp/category/member/techtips

Google Apps for Work
https://www.google.co.jp/intx/ja/work/apps/business/

ChangeIP.com
http://www.changeip.com