

# 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

当技術 Tips コンテンツは、OpenAM コンソーシアム監修のもと、OpenAM コンソーシアム開発 ワーキンググループに属する各企業の担当者により、執筆、編集されたものであり、各記事の著 作権は執筆者に帰属いたします。

また、当記事のライセンスは、Creative Commons 4.0 の BY-NC-SA (表示、非営利、継承) とし、執筆者のクレジット(氏名、作品タイトル)を表示し、かつ非営利目的に限り、また改変を行 った際には元の記事と同じ組み合わせの CC ライセンスで公開することを主な条件に、改変し たり再配布したりすることができるものとします。



## 目次

1.	はじめに	3
2.	目的	4
3.	推奨環境	5
4.	事前準備	6
5.	環境構築の順番	7
6.	OpenAM アイデンティティープロバイダの作成	8
7.	リモートサービスプロバイダ Google Apps の設定	10
8.	Google Apps のシングルサインオンの設定	12
9.	動作確認	15
10.	おわりに	17
11.	付録	17
12.	参考資料	21



#### 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	openIdapuser01 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 <u>www.changeip.com</u>を利用しました。

HOME	WHY	US7 PR	ODUCTS	SIGN	UPI S	UPPORT	CONTA
Home	My Details	My Services	My Dom	ain Registration	s My Quotes	My Involces	i My
DNS Ma	nager						
DNS Ma	inager	uma ref					
Portal.Home	Domain Manage	ment					
Portal Home	Domain Manager Stechtest.dy	ment namic-dns.n	et				
DNS Ma Portal Home = Domain: os Total Records:3 Select At   Car	nager Domain Manage stechtest.dy	ment namic-dns.n	et				
DNS Ma Portal Home = Domain: os Total Records.3 Select At   Car Rostname	nager Domain Manage stechtest.dy	meni namic-dns.ne	et Type	Value			
DNS Ma Partal Home : Domain: os Total Records:3 Select At   Car Rostname	nager Domin Manage stechtest.dy	ment namic-dns.n	et Type A	Value 222.158.192	.45		
DONS Ma Portal Home : Domain: os Total Records 3 Select At   Car Rostname Tra	Inager Domain Manage Istechtest.dy	meni namic-dns.n	et Type A A	Value 222.158.192 222.158.192	.65		click to

・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

<6>



<7>

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。

<u>گەلە</u>	20
FORGEROCK	
通タスク アクセス制御 連携 設定 セッション	
SAMLv2 プロバイダを作成	Salesforce CRM の設定
これらのワークフローを使用して、SAMLv2 連携のホストまたはリモートのアイ デンティティーとサービスプロバイダを作成します。 ホストッイデンティープロバイがの作成	OpenAM と Salesforce CRM を統合して、シングルサインオン環境を作成しま す。最初に、SAMu2 ホストアイデンティティープロバイダとトラストサーク ルを設定する必要があります。
ホストサービスプロバイダの作成	Salesforce CRM の設定
リモートアイデンティティープロバイダを登録	
リモートサービスプロバイダを登録	Configure Social Authentication
OAuth2 の設定	Add social authentication options per reaum. Inis task configures authentication through third parties such as Facebook, Google and Microsoft.
このタスクはレルムごとに OAuth2 を設定します。レルム単位に認可サーバと	Configure Facebook Authentication
して動作することができます。	Configure Google Authentication
OAuth2 の設定	Configure Microsoft Authentication
Fed1et 友作成	Configure Other Authentication (1)
Fedlet を作成して、OpenAM のこのインスタンスでホストされているアイデン ティティープロバイダと、連携ソリューションのないりモートサービスプロバ	連携の接続性をテスト
イダ間で、連携を有効にします。最初に、ホストアイデンティティープロバイ ダを設定する必要があります。	この自動化されたテストを使用して、連携の接続が成功するかどうかを判断 し、どこに問題があるかを確認します。
Fedlet を作成	連携の接続性をテスト
Google Apps の設定	製品マニュアルを取得
OpenAM と Google Apps Web アプリケーションを統合して、シングルサインオ ン環境を作成します。最初に、ホストアイデンティティープロバイダとトラス	OpenAM 製品マニュアルのページを起動します。
トサークルを設定する必要があります。	製師イニュアルを取得 1
Google Apps の設定 i	

#### ・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。



OpenAM コンソーシアム

< 8 >



#### 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。

	umile.com	<u>סאַדאַס</u>
シングルサインオン用の Gool メタデータを設定する前に、アイデンラ Apps はサービスプロバイダとして機能	g <b>le Apps の設定</b> イティープロバイダとリモートサービスプロバイダの情報を指定する必要があります。OpenAM はアイデンティティー こます。SAMLV2 は、アイデンティティープロバイダでトラストサークルを作成するためのシングルサインオンプロト:	作成 取消し プロバイダとして機能し、Google コルです。
* トラストサークル: * アイデンティティープロバイダ: リモート SP の設定 * ドメイン名: 現在の細	メタデータは正常に設定されました。「了解」をクリックして、サービスプロバイダを設定するための パラメータを取得します。 了解	* 必須入力フィールド
新しい毎 これま Google Google Apps アカウントがまだない緒 http://www.google.com/apps/int/en/	i的D e Apps に登録したプライマリドメインです。例: domain.com 白は、すぐに作成する必要があります。 Dusiness/index.html に移動し、Premier Edition アカウントの作成手順に従います。	

<10>



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 フォームヘ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 ヘログインしてください。

パージョン ユーザー: amAdmi	n サーバー::	ssol.example.com	ログアウト
🚷 fo	RGER	оск	
Google App:	5 のシングル	ルサインオンの設定	終了
Google Apps の 情報を保存しま	)シングルサイン tす。	パンを設定するときは、次の情報を Google Apps に指定する必要があります。Google Apps のシングルサインオンの設定に進む前に、次の URL とŧ	検証証明書
URL			
サインインペ	ージの URL:	http://ssol.example.com:8888/openam/SSORedirect/metaAlias/idp OpenAM および Google Apps にサインインするための URL	
サインアウト	ページの URL:	http://ssol.example.com:8888/openam/UI/Logout?goto=http://ssol.example.com:8888/openam サインアウト勝のユーザーのリダイレワト先 URL	
パスワード変	更の URL:	http://ssol.example.com:8080/openam/idm/EndUser ユーザーが OpenAM のバスフードを変更できる URL	
検証証明書			
<b>校証証明書</b> :	BEGIN CEF MIICQDCCAakCB bGmb3JuwREXFL ZW5TU08xDTALBg CQY0YQQGEwJVUJ BgWVBAOTAIN1 AQEFAA0BjQAwg) RkDsaVigkAV JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxuE/ JsØVo5+IgjxUE	RTIFICATE EHBBBWQYIXGZTHvc:MAQEEBQAwZ2ELMAKGAIUEBHACVVMkEpARDgVIXbagTCklh DeBBBWQYIXGZTHvc:MAQEEBQAwZ2ELMAKGAIUEBHACVVMkEpARDgQVVBagTCklh QWBARTBBL:SQmHcnWBQaHTEIMTicoTMSinc.dWITgWHTEyHTkxOTDSHJBBWB QWBARTBBL:SQmHcnWBQaHTEIMTicoTMSinc.dWITgWHTEyHTkxOTDSHJBBWB VKVGFLMSGLUCIMSGTSAWZ.cmg/SPCHABCHABCHABCHABCHABCHABCHABCHABCHABCHAB	
	このテキストをテ	ー テキストファイルにコピーし、新しいテキストファイルを Google Apps の検証証明書にアップロードします。	ます。

#### 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.exa
	mple.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 管理コンソールヘログインし、「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。



OpenAM コンソーシアム

「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。

OpenAM コンソーシアム

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。

ログイン ページの URL	http://sso1.example.com:8080/openam/SSORedirect/metaAlias/idp		
	システムと Google Apps へのログイン用 URL		
ログアウト ページ URL	n:8080/openam/UI/Logout?goto=http://sso1.sso1.example.com:80800,		
	ユーザーがログアウトするときにリダイレクトする URL		
パスワード変更 URL	http://sso1.example.com:8080/openam/idm/EndUser		
認証の確認	認証ファイルをアップロードしました。 証明書を更新		
	認証ファイルには、ログイン リクエストを確認するための Google 公開キーが含まれている必要があります。		
🔽 ドメイン固有の発行	元を使用 🚱		
ネットワーク マスク			
	ネットワーク マスクは、シングル サインオンで有効にできるアドレスを決定します。マスクが指定されない場合 トワーク全体に対して SSO 機能が適用されます。マスクの区切りにはセミコロンを使用します(例: 64.233.187 72 14.0.0/16)、範囲を指定する場合はダッシュを使用します(例: 64.233.167-204.99/32)、すべてのネットワ		

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。

Google		٩			oot@ko.my	03.com 👻
≡ ユーザー			0	₹	0	0 0
フィルタ	名前 🔺	最終ログイン		メールの	使用量	
ユーザーの種類別	openidap user01	15:12 GMT+9		0 GB		
アクティブユーザー -	Test Admin	15:07 GMT+9		0 GB		
組織別						
ko.my03.com						

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 ヘアクセスし 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)ヘアクセスします。

OpenAM ログイン画面が表示されるので、openIdapuser01 でログインします。

FORGEROCK	
OPENAM へのサインイン	
openIdapuser01	
••••••	
Remember my username	
LOG IN	

Google Apps ヘ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。

Google		
	新しいアカウントへようこそ	
	新しいアカウント openIdapuser01@ko.my03.com へようこそ。このアカウントは、ほとんどすべての Google サービスに対応しています。ただし、ko.my03.com 管理者によって、アカウントごとに使用できるサービスが 制限されている場合があります。新しいアカウントを使用する際のヒントについては、ヘルプセンターをご覧く ださい。	
Google Apps をご利用の組織で Google サービスを使用できるようになりました。メッセージングとコラボレー ションの 主要アプリケーション スイートのほかに、多数の Google サービス(以下「追加サービス」)を openIdapuser01@ko.my03.com アカウントで使用できます。各アカウントがどの追加サービスにアクセスでき るかは、ko.my03.com 管理者が設定します。新しいアカウントの使用に関するヒントについては、Google ヘル プセンターをご覧くだいし		
	Google サービスの利用に際して、ドメイン管理者がメールを含むユーザーの openIdapuser01@ko.my03.com アカウント情報にアクセスできることに注意してください。詳細については こちらをご覧いただくか、ドメイ ン管理者のプライバシー ポリシーを参照してください(存在する場合)。メールを含む Google サービスを個 人的に使用する場合は、アカウントを別に保持することもできます。複数の Google アカウントをお持ちの場合 は、ほとんどの Google サービスの右上に表示されるユーザー名を確認することで、目的のアカウントを使用し ていることをご確認いただけます。	
	追加サービスは、これらの 利用規約および プライバシー ポリシーに従って Google より提供されます。追加サ ービスによっては、 サービス固有の規約が存在する場合もあります。ドメイン管理者が追加サービスを有効に 設定した場合、ユーザーがその追加サービスを使用すると、適用されるサービス固有の規約に同意したものと見 なされます。	
	以下の [同意する] をクリックすることにより、アカウントに加えられた変更点について理解し、追加サービス の使用について Google 利用規約と Google プライバシー ポリシーに同意したものと見なされます。	
同意します。続けてアカウントに移動します。 キャンセル		

OpenAM コンソーシアム

openIpdauser01の Gmail 画面が表示されれば SAMLの SSO は成功です。

	Google			· 🤉 🏢	openidapuser01	@ko.my03
	x-1.	□· C ₹	の他 -	1-3/3 <	> & *	¢٠
	1510	🖂 🚖 Gmail チーム	新しい受信トレイを使用	目するためのヒント・さん。	こんにちは。	4月3日
	193	📋 🚖 Gmail チーム	どこでも Gmail を最大	殿に活用 - さん、こんにち	は。 公式 Gm	4月3日
		Gmail チーム	Google Apps で Gmai	を使用する方法・さん。)	こんにちは。 (	4月3日
	送信済みメール 下書き 聞く・ ニ ・- <i>C</i>	10%	アカウントが作成され (ました	アカウントが作成され (金) Gmail の使い方		×
	ユーザーを検索			_		
	まだチャット相手が いないようです。使 用を開始するには、 連絡先を招待してく ださい。 詳細	セットアップの 進行状況	署名を設定	プロフィール画像を 更	変	
		0 GB(0%)/30 GB を使用中 登型	20356 WY Powered by Go	ogle-		



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。

OpenAM コンソージ

▶ 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

OpenAM コンソーシアム

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。

OpenAM JV

# 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.ht ml

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/

ChangelP.com http://www.changeip.com