# OpenAM 学認設定ガイド



OSSTech(株)
------------

更新日

2023年4月28日

リビジョン

1

# **OSSTech**

# 目次

1	はじめに	1
1.1	本書の目的	1
1.2	略語	1
1.3	OpenAM の学認対応	1
1.4	Shibboleth IdP サーバーからの移行 ...................	2
2	OpenAM の設定	5
2.1	Shibboleth IdP の FQDN を OpenAM に登録 .............	5
2.2	OpenAM の旧監査ログ設定............................	6
2.3	署名鍵/暗号鍵を OpenAM のキーストアヘインポート .........	7
2.4	学認メタデータの署名検証用証明書のインポート...........	9
2.5	ホスト ldP プロバイダーの作成 ..........................	10
2.6	リモート SP プロバイダー初期値の設定 ..............	11
2.7	メタデータ自動更新の設定	11
2.8	学認で利用する属性の生成	13
2.9	学認で利用する属性の送信設定	19
2.10	送信属性同意機能の設定................................	21
2.11	トラストサークルの設定.............................	24
2.12	Apache の設定	24
3	運用ガイド	26
3.1	SP の追加	26
3.2	SP の削除	40
3.3	ldP のサーバー証明書の更新	50
4	改版履歴	59

## **OSSTech**

## 1 はじめに

## 1.1 本書の目的

本書は OpenAM の環境を学術認証フェデレーションに参加し、利用するための設定に関 する手順書です。

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。

•「学術認証フェデレーション」を「学認」と表記します。

## 1.3 OpenAM の学認対応

OpenAM 14.5 より、学認との連携機能として次の機能が備わっています。

- 送信属性同意機能
- メタデータ自動更新機能
- computedID(eduPersonTargetedID) 生成機能

従来では学認との連携に Shibboleth IdP サーバーを導入し運用していたような構成に対し、OpenAM を導入して学認連携を OpenAM に任せることにより、 Shibboleth IdP サーバーを無くすことが出来ます。

#### 1.3.1 制限事項

OpenAM では、全ての Shibboleth IdP の機能が利用できるわけではありません。 例えば、 下記の機能は OpenAM には用意されておりません。これらの機能を利用する必要がある場 合は、学認との連携は Shibboleth IdP で行い OpenAM と Shibboleth IdP を連携する構成を ご検討ください。

- データベースを利用した機能
  - eduPersonTargetedID の DB 保存 (storedId)
  - 送信属性同意の情報を DB に保存
- •利用規約の表示 (terms of use)



• Shibboleth1.x の通信とバックチャネル

## 1.4 Shibboleth IdP サーバーからの移行

本書では、すでに学認に参加している Shibboleth IdP サーバーを OpenAM へ移行することを中心に説明します。

以降、OpenAM の環境は構築済みで認証やデータストアなどの設定は完了しているもの とし、学認と連携するための設定について説明します。 OpenAM の構築に関しては初期設 定ガイドや管理者マニュアル等を参照してください。OpenAM のバージョンは 14.5 以降で あることが前提となります。



• 移行前の構成

移行前の構成例として、ユーザーは Shibboleth IdP を経由して学認を利用し、学内の サービスは OpenAM を経由して利用している想定とします。ここでは、Shibboleth IdP と OpenAM でそれぞれアクセスする URL が異なります。 (図では idp.exmaple.co.jp と sso.exmaple.co.jp)



• 移行後の構成



図2 移行後の構成

移行後の構成では、ユーザーは学認も学内のサービスも OpenAM を経由して利用しま す。移行にあたっては、Shibboleth IdP の FQDN(図では idp.exmaple.co.jp) の名前解決を OpenAM サーバーに変更します。 つまり、Shibboleth IdP で利用していた SAML のエンド ポイントの URL を OpenAM がそのまま引き継いで処理する形です。これにより、学認に 登録している IdP のメタデータの変更は必要ありません。

移行の作業中の段階では、OpenAM と Shibboleth IdP の共存が可能です。Shibboleth IdP サーバーで学認を利用しつつ並行して OpenAM の学認参加の設定を行い、特定の端末 (hosts ファイルの変更)のみ OpenAM 経由で学認サービスの利用の確認が出来ます。



図3 並行稼働の構成

このような並行稼働により、テスト端末から OpenAM を経由した学認参加で問題ないことを確認してから、本格的に切り替えることが可能です。

図では示しておりませんが、Shibboleth IdP と OpenAM は同じユーザーレポジトリ (OpenLDAP)を参照している前提です。 また、Cookie を共有する必要があるため、OpenAM のアクセス FQDN と Shibboleth IdP のアクセス FQDN とでドメインが一致している必要が あります。

## **OSSTech**

## 2 OpenAM の設定

本章では Shibboleth IdP から OpenAM への移行において必要な設定を説明します。

## 2.1 Shibboleth IdP の FQDN を OpenAM に登録

OpenAM に対して Shibboleth IdP の FQDN でもアクセス出来るよう、FQDN マップの設 定を行います。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. 上部メニューの「設定」 -> 「デフォルトサーバー」-> 「詳細設定」と辿ります。
- 3. 画面の一番下より次の値を入力します。
  - ・プロパティ名に com.sun.identity.server.fqdnMap[【Shibboleth IdPのFQDN】]
  - ・プロパティ値に【Shibboleth IdPのFQDN】

Shibboleth IdP の FQDN が idp.example.co.jp の場合の設定値は次のとおりです。 プロパティ名: com.sun.identity.server.fqdnMap[idp.example.co.jp] プロパティ値: idp.example.co.jp

4. +を押して、値が追加されたことを確認し「変更の保存」を押します。

続けて、レルムの「レルムまたは DNS のエイリアス」に【Shibboleth IdP の FQDN】を 登録します。

- 1. 上部メニューのレルムから対象のレルムをクリックします。
- 2. レルムの概要の右側の「プロパティ」を押します。
- 3.「レルムまたは DNS のエイリアス」に【Shibboleth IdP の FQDN】を追加し「変更の 保存」を押します。

以上で設定完了です。この設定が完了すると【Shibboleth IdP の FQDN】で OpenAM に アクセスすることが出来るようになります。



## 2.2 OpenAM の旧監査ログ設定

SAML に関するログを記録するため、OpenAM の旧監査ログを出力します。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. 上部メニューの「設定」->「グローバルサービス」->「システム」->「ログ」と辿 ります。
- 3. 下記の設定を行います。

設定項目	設定値
ログ状態	アクティブ
ログローテーション	有効のチェックを外す

旧監査ログのログローテートを logrotate で行います。具体的には、/opt/osstech/etc/logrotate.d/openam に旧監査ログのローテート設定を追加します。

/opt/osstech/etc/logrotate.d/openam

```
/opt/osstech/var/lib/tomcat/data/openam/openam/stats/*
/opt/osstech/var/lib/tomcat/data/openam/openam/log/*.access <- 追加
/opt/osstech/var/lib/tomcat/data/openam/openam/log/*.error <- 追加
{
    rotate 100
    daily
...</pre>
```

設定の反映には Tomcat の再起動が必要ですが、再起動はこのあとの手順 (キーストアファ イルの変更) で行います。

## **OSSTech**

## 2.3 署名鍵/暗号鍵を OpenAM のキーストアヘインポート

「PEM 形式のサーバー証明書」と「秘密鍵」を OpenAM のキーストアにインポートしま す。 Shibboleth IdP では idp.properties で指定しているファイルです。 学認が公開している 手順に従って Shibboleth IdP を構築していた場合、署名鍵と暗号鍵は同じファイルを利用し ています。

```
idp.signing.key= %{idp.home}/credentials/server.key
idp.signing.cert= %{idp.home}/credentials/server.crt
idp.encryption.key= %{idp.home}/credentials/server.key
idp.encryption.cert= %{idp.home}/credentials/server.crt
```

「PEM 形式のサーバー証明書」(server.crt)と「秘密鍵」(server.key)を OpenAM サーバー 上に配置してください。(本書では/tmp に配置したと仮定します。)

これらのファイルを、keytool コマンドを利用し、OpenAM のキーストアにインポートします。 OpenAM が利用しているキーストアファイルは、下記の設定項目で指定しているファイルです。

• キーストアの設定箇所

-「設定」タブ 「デフォルトサーバー」 「セキュリティ」 「キーストア」
 「キーストアファイル」

本書ではキーストアファイルは/opt/osstech/var/lib/data/openam/private/mykeystore.jceks としますので、自身の環境に合わせて読み替えてください。

キーストアに格納するエイリアス名を決める必要があります。エイリアス名は学認用であ ると判別出来るように GakuNin の文字を入れ、証明書の更新に備えて発行した年を含める ことを推奨します。本書ではエイリアス名を gakunin-cert-2023 とします。最初に PEM 形 式のサーバー証明書と秘密鍵を PKCS#12 形式に変換します。

# openssl pkcs12 \
 -export \
 -in /tmp/server.crt \
 -inkey /tmp/server.key \
 -out /tmp/server.pkcs12 \
 -name "gakunin-cert-2023"

実行するとパスワードを聞かれるため、任意のパスワードを入力します。

## **OSSTech**

Enter Export Password: <- 任意のパスワードを入力 Verifying - Enter Export Password: <- 同じパスワードを入力

パスワード入力後、何も表示されずコマンドが終了すれば成功です。 作成した PKCS#12 形式のファイルをキーストアにインポートします。

# keytool -importkeystore \
 -srckeystore /tmp/server.pkcs12 \
 -destkeystore /opt/osstech/var/lib/data/openam/private/mykeystore.jceks \
 -srcstoretype pkcs12 \
 -srcalias "gakunin-cert-2023" \
 -deststoretype jceks \
 -destalias "gakunin-cert-2023" \
 -deststorepass "【キーストアパスワード】" \
 -destkeypass "【秘密鍵のパスワード】"

【キーストアパスワード】や【秘密鍵のパスワード】は、OpenAM キーストア作成時に設 定したパスワードです。

コマンドを実行すると Enter source keystore password: と聞かれるため、PKCS#12 形式変換時に入力した任意のパスワードを入力します。

Enter source keystore password: <- openssl pkcs12 実行時に入力したパスワード

パスワード入力後 Warning のメッセージが表示されることがありますが、問題はありま せんので無視します。インポートが完了したら、キーストアに含まれているか確認します。

# keytool -list \
 -keystore /opt/osstech/var/lib/data/openam/private/mykeystore.jceks \
 -alias "gakunin-cert-2023" \
 -storepass "【キーストアパスワード】"

コマンドを実行し、次のようにフィンガープリントなどが表示されれば成功です。

gakunin-cert-2023, Apr 20, 2023, PrivateKeyEntry, Certificate fingerprint (SHA-256): XX:XX:XX:...

インポート作業終了後、PEM 形式や PKCS#12 形式のファイルは不要なため削除します。



# rm /tmp/server.key /tmp/server.crt /tmp/server.pkcs12

## 2.4 学認メタデータの署名検証用証明書のインポート

学認が提供するメタデータは署名されているため、この署名を検証するための署名用証明 書を OpenAM のキーストアにインポートします。

まず、メタデータの署名用証明書を学認のサイトからダウンロード<sup>\*1</sup>し OpenAM サーバーに配置します。(本書では/tmp に配置したとします。)

# keytool -importcert \
 -alias gakunin-signer-2017 \
 -noprompt \
 -trustcacerts \
 -file /tmp/gakunin-signer-2017.cer \
 -keystore "/opt/osstech/var/lib/data/openam/private/mykeystore.jceks"

「Shibboleth IdP の署名鍵」と「学認メタデータの署名検証用証明書」のインポートが完 了し、かつ OpenAM を複数台構成で構築している場合は、キーストアファイルを他のサー バーにコピーしてください。全ての OpenAM サーバーで同じファイルを使用します。

# scp /opt/osstech/var/lib/data/openam/private/mykeystore.jceks \
 [OpenAM 別号機]:/opt/osstech/var/lib/data/openam/private/mykeystore.jceks

キーストアの変更を反映させるため Tomcat を再起動します。

# systemctl restart osstech-tomcat

\*<sup>1</sup> 運用フェデレーションとテストフェデレーションで署名検証用証明書が異なります。OpenAM が参加する フェデレーションの署名用証明書をダウンロードしてください。

## **OSSTech**

## 2.5 ホスト IdP プロバイダーの作成

OpenAM 管理コンソールからホスト IdP プロバイダーを作成します。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. OpenAM 管理コンソールで対象のレルムをクリックします。
- 3.「共通タスク」で「SAMLv2 プロバイダを作成」をクリックします。
- 4.「SAMLv2 プロバイダを作成」のメニューから「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。
- 5.「このプロバイダのメタデータがありますか?」は「いいえ」をチェックします。
- 6.「メタデータ」の「名前」の URL を Shibboleth IdP の EntityID に変更します。
- 7.「署名鍵」はプルダウンメニューから選択します。「署名鍵/暗号鍵を OpenAM のキー ストアヘインポート」で指定したエイリアス名を選択してください。
- 8.「新しいトラストサークル」にトラストサークルの名前を入力します。ここで は"GakuNin" と入力します。
- 9.「ベース URL」の URL を、一般ユーザーが OpenAM ヘアクセスする URL(本書では https://sso.example.co.jp/openam) に変更します。
- 10. 画面右上の「設定」ボタンをクリックして設定を保存します。属性マッピングは特に 設定しません。
- 11. 設定完了の画面が表示されます。次のアクションを求められますが、ここでは「終 了」ボタンをクリックします。

ホスト IdP プロバイダー作成が完了しました。続いて、作成したホスト IdP プロバイダー に学認に関連した設定を行います。

- 1. 画面上部のメニューから「連携」を押し、 エンティティープロバイダの一覧から 「Shibboleth IdP の EntityID」を押します。
- 2. 「表明コンテンツ」タブの「NameIDの書式リスト」から「urn:oasis:names:tc:SAML:2.0:nameidformat:persistent」を削除し、画面右上の「保存」を押します。
- 表明処理」タブのアカウントマッパーの「Disable NameID Persistence:」のチェック ボックスにチェックを入れ、画面右上の「保存」を押します。
- 4.「表明処理」タブの属性定義用スクリプトで「SAML Attribute Resolution Script」を選 択し、画面右上の「保存」を押します。
- 5. サービスタブの下記のエンドポイントの URL を Shibboleth IdP のメタデータに記載 されている URL に変更し、画面右上の「保存」を押します。



[シングルサインオンサービス] - [HTTP-REDIRECT] - [場所] -> Shibbleth IdP メタデータの SingleSignOnService Binding="urn:oasis:names:tc:SAML :2.0:bindings:HTTP-Redirect"のLocationのURL

[シングルサインオンサービス] - [POST] - [場所]

-> Shibbleth IdP メタデータの SingleSignOnService Binding="urn:oasis:names:tc:SAML :2.0:bindings:HTTP-POST" の Location の URL

以上で、ホスト IdP プロバイダーの作成は完了です。

## 2.6 リモート SP プロバイダー初期値の設定

OpenAM 管理コンソールから、リモート SP プロバイダー初期値の設定を作成します。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. OpenAM 管理コンソールで対象のレルムをクリックします。
- 3. 左のサイドメニューの「サービス」を開き、「サービスの追加」を押します。
- 4. サービスタイプに「SAMLv2 リモート SP 初期値設定」を選択し、「作成」を押します。
- 5.「属性送信の同意画面を表示する」を有効にし、「設定の保存」を押します。

## 2.7 メタデータ自動更新の設定

OpenAM 管理コンソールからメタデータ自動更新の設定を行い、学認のメタデータを取り込む設定を行います。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. OpenAM 管理コンソールで対象のレルムをクリックします。
- 3. 左のサイドメニューの「サービス」を開き、「サービスの追加」を押します。
- 4. サービスタイプに「SAMLv2 メタデータの自動更新」を選択し、「作成」を押します。
- 5. 設定画面となります。下記を設定し「変更の保存」を押します。
  - •「キー」に"学認のメタデータ取得 URL"をセットします。
  - 「値」はメタデータファイルの保存先のため、OpenAM 設定ディレクトリ配下 (例: /opt/osstech/var/lib/tomcat/data/openam/openam/gakunin-metadata.xml)を指 定します。「キー」と「値」を入力したら「+add」を押します。
  - 「実行時刻」は取得を実行する時刻です。任意の時刻で構いません。例えば 04:00:00(午前4時に実行)と指定します。
  - •「対象とするロール」は"なし"とします。



- •「対象とするエンティティ」に利用する SP の EntityID を全て登録します。\*2
- •「エンティティの新規登録を許可する」「有効期限をチェックする」「署名を検証 する」は有効とします。

#### 2.7.1 メタデータ読み込み

メタデータ自動更新の設定が終わったらメタデータの読み込みを行います。OpenAMの 管理者ログインが完了している状態で下記の URL ヘアクセスします。\*<sup>3</sup>

・https://【FQDN】/【コンテキストパス】/saml2/jsp/reload.jsp?realm=【レルム】

メタデータの読み込みに成功すると「Complete」と表示されます。もし「Complete」と 表示されない場合は、設定に誤りや不足がありますので、設定や OpenAM のデバッグログ (MetadataReloadTaskFactory)を確認してください。

メタデータの読み込みは、OpenAM 管理者による認証済み状態でアクセスする必要があ ります。OpenAM 未ログイン状態でアクセスするとログイン画面にリダイレクトされます。 一般ユーザーによる認証済み状態でアクセスすると This action is only allowed for admin user. と表示され、メタデータの読み込みは行われません。

<sup>\*&</sup>lt;sup>2</sup> OpenAM は、ここで指定した SP のみメタデータを取り込みます。 Shibboleth IdP の設定 (attribute-filter.xml) やログ (idp-audit.log) から、利用している学認 SP を確認して設定してください。

<sup>\*&</sup>lt;sup>3</sup> 例として、OpenAM セットアップガイドに従って構築した OpenAM の場合、メタデータ更新 URL は次の とおりです。https://openam01.example.co.jp/openam/saml2/jsp/reload.jsp?realm=/sso

OSSTech

### 2.8 学認で利用する属性の生成

Shibboleth IdPの attribute-resolver.xml にあたる設定を OpenAM に行います。

#### 2.8.1 データストアのユーザー属性に学認用の属性を追加

LDAP のユーザーエントリにある学認用の属性を OpenAM で参照する設定を行います。 Shibboleth IdP の設定から使用している LDAP の属性\*<sup>4</sup>を確認し、OpenAM に設定します。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. OpenAM 管理コンソールで対象のレルムをクリックします。
- 3. 左のメニューの「データストア]を押し、「(データストア名)」と辿ります。
- 4.「LDAP ユーザー属性」について、Shibboleth IdP で使用し「現在の値」のリストに含まれていない属性を追加します。
- 5.「保存」を押します。

Shibboleth IdP で phonetic が付いた属性を利用している場合は、「LDAP ユーザー属性」では phonetic を付けた属性を設定します。

例:

givenName;lang-ja を「LDAP ユーザー属性」のリストに追加する。

#### 2.8.2 SAML 属性送信のスクリプトを作成

Shibboleth IdP で LDAP の属性値をそのまま SP に送るのではなく何らかの加工をしていた場合は、 OpenAM の SAML 属性送信のスクリプトを使って生成します。

SAML 属性送信のスクリプトの編集は管理コンソールより行います。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. OpenAM 管理コンソールで対象のレルムをクリックします。
- 3. 左メニューの「スクリプト」を押し、スクリプトの一覧から「SAML Attribute Resolution Script」をクリックします。
- 4.「名前」などの設定は変更せず、「スクリプト」のコードを編集し、「変更の保存」を 押します。

「SAML Attribute Resolution Script」は初期状態でスクリプトがセットされています。初

<sup>\*&</sup>lt;sup>4</sup> 例えば attribute-resolver.xml の DataConnector id="myLDAP"の exportAttributes に記載されている属性は、 OpenAM への設定が必要です。



期状態のスクリプトの関数 (function の定義) はいくつかそのまま利用しますが、利用しない コードは削除してしまって問題ありません。

以下、attribute-resolver.xml で定義している属性の type ごとに、生成方法を説明します。

#### 2.8.2.1 type="Static" で生成した値

学認の attribute-resolver.xml テンプレートでは、oと jao などで大学名を設定しています。 全 SP で同じ値を送信するケースに使います。

・ attribute-resolver.xml の設定

OpenAM のスクリプトでは下記のように定義します。

```
setStaticData();
function setStaticData() {
    putEntry("o", "Test Organization");
    putEntry("jao", "テスト大学");
}
```



#### 2.8.2.2 type="Scoped" で生成した値

学認の attribute-resolver.xml テンプレートでは、eduPersonScopedAffiliation や eduPerson-PrincipalName を Scoped を使って生成するサンプルが記載されています。

• attribute-resolver.xml

この設定で eduPersonScopedAffiliation は、LDAP の属性 eduPersonAffiliation の値にス コープ (idp.properties で定義)を繋げた値となります。 OpenAM のスクリプトでは下記のよ うに定義します。

• OpenAM のスクリプト定義

```
var scope = "osstech.co.jp";
seteduPersonAffiliation();
function setScopeValue(name, ldap_attr) {
    var ldap_values = identity.getAttribute(ldap_attr);
    if (ldap_values) {
        var set_values = new java.util.HashSet();
        var iter = ldap_values.iterator();
        while (iter.hasNext()) {
            set_values.add(iter.next() + "@" + scope);
        }
        putEntry(name, set_values);
    }
}
function seteduPersonAffiliation() {
   setScopeValue("eduPersonScopedAffiliation", "eduPersonAffiliation");
}
```



#### 2.8.2.3 type="Mapped" で生成した値

学認の attribute-resolver.xml テンプレートでは、 isMemberOf を Mapped を使って生成するサンプルが記載されています。

• attribute-resolver.xml

<attributedefinition id="isMemberOf" xsi:type="Mapped"></attributedefinition>
<inputdataconnector attributenames="uid" ref="myLDAP"></inputdataconnector>
<valuemap></valuemap>
<returnvalue>https://voplatform1.example.ac.jp/gr/FooGroup</returnvalue>
<sourcevalue>user0001</sourcevalue>
<valuemap></valuemap>
<returnvalue>https://voplatform2.example.ac.jp/gr/FooGroup</returnvalue>
<sourcevalue>user0002</sourcevalue>
<valuemap></valuemap>
<returnvalue>https://voplatform99.example.ac.jp/gr/FooGroup</returnvalue>
<sourcevalue>user0099</sourcevalue>

この設定で isMemberOf は、LDAP の属性 uid の値によって値が変わります。uid が user0001,user0002,user0003 以外の値の場合は isMemberOf は SP に送信されません。 Ope-nAM のスクリプトでは次のように定義します。

• OpenAM のスクリプト定義

```
setisMemberOf();
function setisMemberOf(){
  var name = "isMemberOf";
  var ldap_values = identity.getAttribute("uid");
  if (ldap_values) {
    var set_values = new java.util.HashSet();
    var iter = ldap_values.iterator();
    while (iter.hasNext()) {
      var value = checkisMemberOf(iter.next());
      if (value) {
         set_values.add(value);
    }
}
```

## 0SSTech

```
}
        }
        putEntry(name, set_values);
    }
}
function checkisMemberOf(uid){
    if (uid == "user0001") {
        return "https://voplatform1.example.ac.jp/gr/FooGroup";
    }
    if (uid == "user0002") {
        return "https://voplatform2.example.ac.jp/gr/FooGroup";
    }
    if (uid == "user0099") {
        return "https://voplatform99.example.ac.jp/gr/FooGroup";
    }
}
```

### 2.8.2.4 type="SAML2NameID" で生成した値 (computedID)

学認の attribute-resolver.xml テンプレートでは、eduPersonTargetedID を type="SAML2NameID" を使い生成しています。

• attribute-resolver.xml

Shibboleth IdP では、 saml-nameid.properties でソルトやアルゴリズム等を設定します。 OpenAM では、スクリプトの初期値として computedId を生成する setComputedID 関数を



用意しています。 この関数に Shibboleth IdP の設定内容を設定します。

項目	Shibboleth IdP のプロパティの設定項目名
ソースとなる属性	idp.persistentId.sourceAttribute
ソルト文字列	idp.persistentId.salt(secrets.properties で設定)
アルゴリズム	idp.persistentId.algorithm
エンコード方式	idp.persistentId.encoding

• OpenAM のスクリプト定義

上記のスクリプト定義は「ソースとなる属性」が uid、「ソルト文字列」が VfIzEzattecXS97Obxkl、「アルゴリズム」が SHA-1、「エンコード方式」が BASE64 となります。 Shibboleth IdP の設定値に従って置き換えてください。

**OSSTech** 

## 2.9 学認で利用する属性の送信設定

学認で利用する属性の生成で準備した属性について、SP単位で属性を送信する設定を行います。Shibboleth IdPの attribute-filter.xml にあたる設定です。

基本的な設定方法は次のとおりです。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. 画面上部のメニューから「連携」を押し、エンティティープロバイダの一覧から「設 定する SP の EntityID」を押します。
- 3.「表明処理」タブの「属性マップ」<sup>\*5</sup>に、SP に送信する属性を全て定義します。「属 性マップ」に設定する形式は [SAML 属性名]=[属性名] です。
- 4. eduPersonTargetedID を SP に送信する場合のみ、「エスケープしない属性」を設定し ます。(後述)
- 5. 画面右上の「保存」を押します。
- 6. SP の数だけ繰り返します。

[SAML 属性名] について説明します。学認の属性については、運用ガイドで SAML の属 性名が定められております。 下記表に示しますので、 SP に送信する学認の属性としては、 対応した SAML の属性名を設定します。

学認の属性名	SAML の属性名
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
o(organizationName)	urn:oid:2.5.4.10
jao(jaOrganizationName)	urn:oid:1.3.6.1.4.1.32264.1.1.4
ou(organizationalUnitName)	urn:oid:2.5.4.11
jaou(jaOrganizationalUnitName)	urn:oid:1.3.6.1.4.1.32264.1.1.5
eduPersonAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7
mail	urn:oid:0.9.2342.19200300.100.1.3
givenName	urn:oid:2.5.4.42

<sup>\*&</sup>lt;sup>5</sup>「属性マップ」については、SAML 設定ガイドの「NameID や属性で連携する値について」の説明を参照く ださい。



学認の属性名	SAML の属性名
jaGivenName	urn:oid:1.3.6.1.4.1.32264.1.1.2
sn	urn:oid:2.5.4.4
jasn	urn:oid:1.3.6.1.4.1.32264.1.1.1
displayName	urn:oid:2.16.840.1.113730.3.1.241
jadisplayName	urn:oid:1.3.6.1.4.1.32264.1.1.3
gakuninScopedPersonalUniqueCode	urn:oid:1.3.6.1.4.1.32264.1.1.6
isMemberOf	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11
eduPersonUniqueId	urn:oid:1.3.6.1.4.1.5923.1.1.1.13
eduPersonOrcid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16

「属性マップ」の設定例を示します。下記の2つの「属性マップ」を設定すると、SPには givenName と jaGivenName が連携されます。

urn:oid:2.5.4.42=givenName urn:oid:1.3.6.1.4.1.32264.1.1.2=givenName;lang-ja

### 2.9.1 eduPersonTargetedID の設定について

eduPersonTargetedID はスクリプトで生成します。 スクリプトで生成した computedID の「表明処理」の設定は、次の2つが必要です。

•「属性マップ」を次のように設定する。\*6

```
urn:oasis:names:tc:SAML:2.0:attrname-format:uri|urn:oid:1.3.6.1.4.1.5923
.1.1.1.10=computedId
```

•「エスケープしない属性」に設定を追加する

urn:oid:1.3.6.1.4.1.5923.1.1.1.10

eduPersonTargetedID は SAML の NameID フォーマットの形式で送信する必要があるため、上記の 2 つの設定が必要となります。

\*6表示の都合上改行していますが、実際の設定時は改行せず1行で設定します。

**OSSTech** 

## 2.10 送信属性同意機能の設定

SAML アサーション送付前に送信属性の同意画面を表示する機能に関して、設定を行います。SAML 設定ガイドの「送信属性同意機能の設定」の章にある下記の作業を実施します。

- 組織認証用鍵ペアの作成
- 組織認証用の証明書エイリアスの変更
- 同意が必要な属性の設定
- 監査ログ

SAML 設定ガイドの「送信属性同意機能の有効化」の作業は、SP メタデータ読み込み時 に有効になるため不要です。

「同意が必要な属性の設定」に設定する文言は任意ですが、参考情報として Shibboleth IdP(v4.2.1)の属性情報同意画面で表示される文言を設定する値を示します。

#### eduPersonAffiliation

urn:oid:1.3.6.1.4.1.5923.1.1.1.1|en|Affiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1|職位

#### • jao

urn:oid:1.3.6.1.4.1.32264.1.1.4|en|Organization name (written in Japanese) urn:oid:1.3.6.1.4.1.32264.1.1.4|所属機関名[日本語]

#### • jaDisplayName

urn:oid:1.3.6.1.4.1.32264.1.1.3|en|Display name (written in Japanese) urn:oid:1.3.6.1.4.1.32264.1.1.3|表示名[日本語]

#### • givenName

urn:oid:2.5.4.42|en|Given name urn:oid:2.5.4.42|名

#### • eduPersonPrincipalName



urn:oid:1.3.6.1.4.1.5923.1.1.1.6|en|Principal name urn:oid:1.3.6.1.4.1.5923.1.1.1.6|プリンシパル ID

#### eduPersonTargetedID

urn:oid:1.3.6.1.4.1.5923.1.1.1.10|en|Unique ID for each service provider urn:oid:1.3.6.1.4.1.5923.1.1.1.10|サービス毎のユニーク ID

• ou

urn:oid:2.5.4.11|en|Organizational unit urn:oid:2.5.4.11|機関内所属名

#### • jasn

urn:oid:1.3.6.1.4.1.32264.1.1.1|en|Surname (written in Japanese) urn:oid:1.3.6.1.4.1.32264.1.1.1|姓[日本語]

• 0

urn:oid:2.5.4.10|en|Organization name urn:oid:2.5.4.10|所属機関名

• displayName

urn:oid:2.16.840.1.113730.3.1.241|en|Display name urn:oid:2.16.840.1.113730.3.1.241|表示名

#### • jaGivenName

urn:oid:1.3.6.1.4.1.32264.1.1.2|en|Given name (written in Japanese) urn:oid:1.3.6.1.4.1.32264.1.1.2|名[日本語]

• eduPersonScopedAffiliation



urn:oid:1.3.6.1.4.1.5923.1.1.1.9|en|Scoped affiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9|スコープ付き職位

#### • jaou

urn:oid:1.3.6.1.4.1.32264.1.1.5|en|Organizational unit (written in Japanese) urn:oid:1.3.6.1.4.1.32264.1.1.5|機関内所属名[日本語]

#### • gakuninScopedPersonalUniqueCode

urn:oid:1.3.6.1.4.1.32264.1.1.6|en|Personal unique code urn:oid:1.3.6.1.4.1.32264.1.1.6|個人識別番号

• sn

urn:oid:2.5.4.4|en|Surname urn:oid:2.5.4.4|姓

#### • eduPersonEntitlement

urn:oid:1.3.6.1.4.1.5923.1.1.1.7|en|Entitlement urn:oid:1.3.6.1.4.1.5923.1.1.1.7|資格情報

• mail

urn:oid:0.9.2342.19200300.100.1.3|en|E-mail urn:oid:0.9.2342.19200300.100.1.3|メールアドレス

#### • isMemberOf

urn:oid:1.3.6.1.4.1.5923.1.5.1.1|en|Group identifier urn:oid:1.3.6.1.4.1.5923.1.5.1.1|所属グループ識別子

• eduPersonAssurance

## **OSSTech**

urn:oid:1.3.6.1.4.1.5923.1.1.1.11|en|Assurance level urn:oid:1.3.6.1.4.1.5923.1.1.1.11|保証レベル

#### • eduPersonUniqueId

urn:oid:1.3.6.1.4.1.5923.1.1.1.13|en|Unique ID urn:oid:1.3.6.1.4.1.5923.1.1.1.13|ユニーク ID

eduPersonOrcid

urn:oid:1.3.6.1.4.1.5923.1.1.1.16|en|ORCID urn:oid:1.3.6.1.4.1.5923.1.1.1.16|ORCID

## 2.11 トラストサークルの設定

トラストサークルに学認の SP を追加し、信頼関係を構築します。

OpenAM 管理コンソールから [連携] を押し、ホストアイデンティティプロバイダ作成時 に作ったトラストサークルに IdP や学認 SP を追加します。

- 1. OpenAM に管理者ユーザーでログインします。
- 2. 画面上部のメニューから「連携」を押します。
- 3. ホスト IdP プロバイダーの作成で作成したトラストサークル名 (本書では GakuNin) を押します。
- 4.「エンティティープロバイダ」の「選択可能」の一覧から学認の SP の EntityID を追加し、「保存」を押します。

## 2.12 Apache の設定

OpenAM サーバーにて Shibboleth IdP のエンドポイントのリクエストを受け付けるため に、 サーバー証明書の設定や OpenAM の URL に Rewrite する設定を行います。サーバー 証明書 (必要に応じて中間証明書) と秘密鍵は、Shibboleth IdP サーバーのファイルを使用し ます。

```
<VirtualHost *:443>
ServerName [Shibboleth IdP の FQDN]
SSLCertificateKeyFile /etc/pki/tls/private/server.key
```



```
SSLCertificateFile /etc/pki/tls/certs/server.crt

SSLCertificateChainFile /etc/pki/tls/certs/chain.crt

RewriteEngine on

RewriteRule ^/idp/profile/SAML2/Redirect/SSO

/openam/SSORedirect/metaAlias/【メタエイリアス】 [PT]

RewriteRule ^/idp/profile/SAML2/POST/SSO

/openam/SSOPOST/metaAlias/【メタエイリアス】 [PT]

</VirtualHost>
```

2 つの RewriteRule の設定は表示の都合上改行していますが、実際の設定時は改行せずに それぞれ1行で設定します。

【メタエイリアス】は OpenAM の管理コンソールにて確認出来ます。

• [連携] - [ホスト IdP の EntityID] - [サービス] タブ - [MetaAlias]

作業は以上で完了です。ここまでの作業を終えたら OpenAM は学認に参加出来ます。



## 3 運用ガイド

本章では、 OpenAM を学認に参加させて運用する際に必要となる作業について説明します。

### 3.1 SP の追加

利用する学認の SP を追加したい場合の手順について説明します。

作業実施前に、新しく追加する SP の「EntityID」と「送信する属性」を確認します。 情報は Shibboleth IdP の attribute-filter.xml の設定内容から判断出来ます。通常は、学認サイトの SP 一覧ページの該当 SP の「IdP 管理者向け」に記載があります。

例として attribute-filter.xml の設定内容が下記の場合、「EntityID」と「送信する属性」は 次のとおりです。

- EntityID
  - https://www.elgaronline.com/oa/metadata
- 送信する属性
  - eduPersonScopedAffiliation

```
<!-- Policy for Elgaronline -->
<AttributeFilterPolicy id="PolicyforElgaronline">
        <PolicyRequirementRule xsi:type="Requester"
            value="https://www.elgaronline.com/oa/metadata" />
            <AttributeRule attributeID="eduPersonScopedAffiliation">
                <PermitValueRule attributeID="eduPersonScopedAffiliation">
                <PermitValueRule xsi:type="ANY" />
               </AttributeRule>
</AttributeFilterPolicy>
```

次ページより、実際の手順を説明します。本書では次の SP を追加する手順を示します。

- EntityID
  - https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp
- 送信する属性
  - eduPersonTargetedID
  - mail
  - displayName



### 3.1.1 該当 SP をメタデータ更新対象に追加

追加する SP のメタデータを取り込む設定を行います。

• OpenAM に管理者ユーザーでログインします。

OpenAM
OPENAM へのサインイン
amadmin  パスワード ユーサー&を記憶する。

図4 管理ユーザ ログイン画面

• OpenAM 管理コンソールで対象のレルムをクリックします。(下図では demo レルム)

GoonAM 🌢 レルム - 🖌 I	Q定 - 品 デブロイメント - 目 連邦	↓ 替 セッション	۰
レルム			
対象および設定データを整理するためにレル。 できます。	ムを使用します。各レルム内では、データストフ	?、管理権限、認証連鎖、認可ポリシー、およびその他のレルム協有の	D股定を行うことが
◆新規レルム			
1	· · ·		
最上位のレルム	demo		
/ openam 1 more	/demo operam. demo. ossitech. co. jp 1 more		
◎アクティブ	© 70717		

図 5 レルムの選択



左のサイドメニューの「サービス」を開きます。



\*「SAMLv2 メタデータの自動更新」をクリックします。

🔒 OpenAM	レルム・ チ 設定。 赤 デブロイメント・ 🗍 連携 👹 セッション	
🌰 demo	サービス	
& ダッシュボード ▲ 認証 ♪ サービス 器 データストア & 相限	サービス OpenAM のレルム国有のプロバティを設定します。	<b>●</b> ヘルプ
Q4 認可 譬 対象 ● エージェント	サービス& 	/ x
∲ STS ゆ スクリプト	User Self Service WebAuthn Authenticator サービス	# ×
	<ul> <li></li></ul>	/ ×
	- ボリシー設定	8 X
	□ 電子メールサービス	₽ ×

図 7 SAMLv2 メタデータの自動更新



・「対象とするエンティティ」に追加する SP の EntityID を入力し

🛱 OpenAM	► LILA -	▶ 股定 -		[] 連携	替 セッション	
🌰 demo	サート	ビス > saml2M	ietadataAutoReloadServic	10		
<ul> <li>動 ダッシュボード</li> <li>単 認証</li> <li>ダ ワービス</li> <li>デニータフトマ</li> </ul>	Ç	*-EA	MLv2 メタ	デー	タの自動更新	× Rith
B 権限 4,認可 督 対象	http	メタデ- os://metadata.ga	ータのURLとバックアップ先r akunin.nii.ac.jp/gakunin- test-metadata.xml	のマッピング /opt/ossied	0 hivarilialiomcatidatalopenam/metadata.xml	<b>x</b>
🛊 エージェント 🏕 STS		+		値		+ auld
の スクリプト			実行時刻	00:00		0
			実行するサーバーのURL	http://oper	nam1.demo.ocstech.co.jp:8080/openam	~ 0
			対象とするロール	なし	•	0
			対象とするエンティティ	https://test https://test https://shit https://mel https://test https://test	1. example.co.jphestsp 3. example.com/tstsp idp4.example.com/1452/Shibboleth/ indp4.example.com/1452/Shibboleth/ sp2.gakunin.mi.ac.jphshibboleth-sp at8p1.example.co.jphmelion.text 2. example.ac.jphmelion.text	)
			除外するエンティティ			0

図 8 SPの EntityID 入力

• Add を押します。

= データストア			
2 40.00			
19 m	メタデータのURLとバックアップ先	のマッピング 😗	
● 対象	https://metadata.gakunin.nii.ac.jp/gakunin- test-metadata.xml	/opt/osstech/var/lib/tomcat/data/openam/metadata.xml	×
▶ エージェント ▶ STS	*-	値	+ add
▷ スクリプト	実行時刻	00:00	0
	実行するサーバーのURL	http://openam1.demo.osstech.co.jp:8080/openam	~ 0
	対象とするロール	なし - <b>・</b>	0
	対象とするエンティティ	https://test1.example.co.jp/testsp https://test3.example.com/testsp https://shibidp4.example.com/1452/Shibboleth/ https://mellion-test.ostisch.example.co.jp:10443/mellion-test https://test-sp2.gakumin.nil.ac.jp/shibboleth-sp https://alma9sp1.example.co.jp/mellion-test https://test-sp1.puburuo.ac.epichebelande.sp	0
	除外するエンティティ	Add https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp	>
	テレスノスノムが細胞的を強力する		

図9 SPの EntityID の追加(Add)



•「対象とするエンティティ」に SP の EntityID が追加されたことを確認し、「変更の保存」を押します。

タストア		
マタデータへいい とバックマップパ	1.07	
A37-3000LC/1997999		
https://metadata.gakunin.ni.ac.jp/gakunin- test-metadata.xml	/opt/osstech/var/lib/tomcat/data/openam/metadata.xml	×
4-	備	+ add
実行時刻	00:00	0
実行するサーバーのURL	http://openam1.demo.osstech.co.jp:8080/openam	~ 0
対象とするロール	なし	0
対象とするエンティティ	https://test1.example.co.jp/testsp	0
	https://test3.example.com/testsp	
	https://shibidp4.example.com:1452/Shibboleth/	
	https://mellon-test.osstech.example.co.jp.10443/mellon-test	
	https://test-sp2.gakunin.ni.ac.jp/shibboleth-sp	
	https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp	
除外するエンティティ		0
エンティティの新規登録を許可する		0
有効期限をチェックする		0
署名を検証する		0
	—	
		変更の保存

図 10 変更の保存

•「変更を保存しました」と表示されれば完了です。

19 - 19 - T	メタデータのいたいとバックアップな	テクシュアング 6		
• #8¤] h	ttps://metadata.gakuni 🟮 変更を保存しま	した。	am/metadata.xml	×
対象	test-metauata.xiii			
エージェント	+-	値		+ add
▶ STS				
> スクリプト	実行時刻	00:00		0
	実行するサーバーのURL	http://openam1.demo.osstech.co.	p:8080/openam	~ <b>8</b>
	対象とするロール	なし		• 0
	対象とするエンティティ	https://test1.example.co.jp/testsp https://test3.example.com/testsp https://shibidpd.example.com.145 https://mellon-test.osstech.exampl https://test-sp2.gakunin.nii.ac.jp/sh https://test-sp1.gakunin.nii.ac.jp/sh	//Shibboleth/ a.co.jp:10443/mellon-test ibboleth-sp Illon-test ibboleth-sp	0
	除外するエンティティ			0
	エンティティの新規登録を許可する			0
	有効期限をチェックする			0
	署名を検証する			0

図 11 変更の保存の完了



#### 3.1.2 メタデータの手動更新

メタデータ読み込みの手順に従ってメタデータ更新 URL にアクセスし、メタデータを更 新します。

• OpenAM に管理者ユーザーでログインします。

OPENAM ^	<b>○</b> のサインイン
amadmin	
ハスシート	
D2	112

図 12 ログイン画面

• メタデータ更新 URL にアクセスし「Complete」と表示されるのを確認します。



#### 図 13 メタデータ更新 URL にアクセス

**OSSTech** 

### 3.1.3 該当 SP をトラストサークルへ追加

トラストサークルの設定に従って、追加する SP の EntityID をトラストサークル名 (本書 では GakuNin) に追加します。

• OpenAM に管理者ユーザーでログインします。

	OpenAM
_	OPENAM へのサインイン
amadr	un l
	- ド ・名を記憶する。
	ログイン

図 14 管理ユーザ ログイン画面

• 画面上部のメニューから「連携」を押します。

GpenAM 🌢 レルム -	♪ 股定 - ム デプロイメント 📃 連携 🔮 ひょション	
レルム		
対象および設定データを整理するため できます。	にレルムを使用します。各レルム内では、データストア、管理権限、認証達領、認可ポリ	シー、およびその他のレルム協有の設定を行うことが
+ 新規レルム		=
	•	
0		
最上位のレルム	demo	
openam 1 more	raemo openam.demo.osstech.co.lp 1.more	
◎ アクティブ	G 7294J	

図 15 連携を押す



• トラストサークルの「GakuNin」を押します。

Open	nAM	× +					
	C 🔺 保護さ	れていない通信  <del>https:</del> // <b>openam1.demo.osstech.co.jp</b> /openam/fec		\$	□ 🖨	シークレット	E
'-:am )pen/	nAdmin サーバー: a	penam1.demo.osstech.co.jp					0071
クセス	制御 連携	設定 セッション		_		_	
21-1	サークル設定	SAML 1.x の設定					
スト1 0セクシ エンテ	サークル設定 ションは、トラスト・ ティティーテーブルI	ナークルのプロパティーの設定に使用できます。エンティティーテーブルは、ブ 作成した後で、トラストリークルに追加できます。	'ロバイダのインボートやエクスボートなどエンティ!	ティープロバイダの管	理に使用で	きます。エンティ	7-
スト! シセクシ エンテ ラスト 湖	サークル設定 ションは、トラスト・ ティティーテーブルド トサークル (2 項目 削除	ワークルのプロパティーの設定に使用できます。エンティティーテーブルは、ブ 作成した後で、トラストリークルに追加できます。 ))	ロバイダのインボートやエクスボートなどエンティー	ティープロバイダの管	理に使用で	きます。エンティ	7-
スト! シセクシ エンデ 現 回 4	サークル設定 ションは、トラスト・ ティティーテーブル( トサークル(2 項目 前版 名前	ワークルのプロパティーの設定に使用できます。エンティティーテーブルは、ブ 作成した後で、トラストリークルに当然できます。 ))	ロバイダのインボートやエクスボートなどエンティー	Fィーブロバイダの管 レルム	理に使用で	きます。エンティ 大阪	÷7-
スト! シセクら エンラ ラスト 通 4 日 6	サークル設定 ションは、トラスト ティティーテーブル トサークル (2 項目 ) () () 名前 demo-cot	・クルのプロパティーの設定に使用できます、エンティティーテーブルは、ブ 作成した後で、トラストサークルに追加できます。           ))           ▲           エンティティー           https://htts.pl.gakunin.nil.ac.jp/thlbboleth-splcaml2 https://bit.godemo.stateCh.co.jp/45/lopenamlcaml2 https://bit.godemo.stateCh.co.jp/45/lopenaml2aml2 https://bit.godemo.stateCh.co.jp/saml2 https://bit.godemo.stateCh.co.jp/saml2 https://bit.godemo.stateCh.co.jp/saml2 https://bit.godemo.stateCh.co.jp/saml2 https://bit.godemo.stateCh.co.jp/saml2	ロバイダのインボートやエクスボートなどエンティ	ティーブロバイダの管 レルム /demo	環に使用で <u>へ</u> え	きます。エンティ 伏服 アクティブ	÷74-

図 16 GakuNin を押す

• エンティティプロバイダの選択可能から「SPのEntityID」を選択し、「追加」を押し ます。

👕 OpenAM	x +	<b>•</b> -	• 😣
← → C ▲ 保護され	ていない通信   https://openam1.demo.osstech.co.jp/openam/federation/Federation/Federation.cotNameHref=GakuN 🗴 🔲	🍮 シークレット	(更新 ;)
		-	
トラストサークルの編集		保存 リセット	戻る
名前:	GakuNin		
說明:			
IDFF ライターサービス URL:			
	共通ドメインに Cookie を書き込む IDFF ライターサービスの場所。		
IDFF リーダーサービス URL:			
	共通ドメインから Cookie を読み取る IDFF リーダーサービスの場所。		
SAML2 949-7-6X URL:	共通ドメインに(weble を集合込む Samt) ライターサービスの場所。		
SAML2 リーダーサービス URL:	AND A TAK COME CHICKLE TAKEN CARENT		
	共通ドメインから Cookie を読み取る SAML2 リーダーサービスの場所。		
秋態:	● アクティブ ○ #アクティブ		
L/1L/L:	/demo		
エンティティープロバイダ トラストサークルの最小要件は、1	つのアイデンティティープロバイダと1つのサービスプロバイダです。プロバイダが、上で指定したレルムに割り当てられます。		
(	Wei (E)     Bit (E)	*	

図 17 SPの EntityID を追加



エンティティプロバイダの選択欄に SP の EntityID が追加されたことを確認し、「保存」を押します。

👚 OpenAM	× +	🕑 – 🔍 😫
← → C ▲ 保護され	र । रहे । 🔐 🖓 र र प्रत्ये प्	🍮 シークレット 🛛 更新 🚦
トラストサークルの編集		保存 セット 戻る
名前:	GakuNin	$\smile$
說明:		
IDFF ライターサービス URL:		
	共通ドメインに Cookie を書き込む IDFF ライターサービスの場所。	
IDFF リーダーサービス URL:		
SAMI2 5 / Q-#-FZ UP	共通ドメインから Cookie を説み取る IDFF リーダーサービスの場所。	
30012 7 1 7 - 7 - 6 7 00L.	共通ドメインに Cookie を書き込む SAML2 ライターサービスの場所。	
SAML2 リーダーサービス URL:		
	共通ドメインから Cookie を読み取る SAML2 リーダーサービスの場所。	
状態:	● アクティブ ○ 林アクティブ	
L11.4:	/demo	
エンティティープロバイダ トラストサークルの最小要件は、1	つのアイデンティティープロバイダと1つのサービスプロバイダです。プロバイダが、上で指定したレルムに削り当てられます。	
	選挙可能 SSD-uniCorn SAMLy2 * 「記址 > 「また」」 「また」でも認知 >> 「また」」 「「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」 「」」」」」 「」」」」 「」」」」 「」」」」」 「」」」」」 「」」」」」 「」」」」」 「」」」」」 「」」」 「」」」 「」」」 「」」」」 「」」」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 「」 「	

図18 追加を確認し保存

• "トラストサークルプロファイルが更新されました。"と表示されれば完了です。

🔐 OpenAM	× +			🗸 – 🗉 😣
← → C ▲ 保護され	ていない通信   https://openam1.demo.os	stech.co.jp/openam/federation/FSAuthDo		☆ □ 👶 シークレット (更新 🔅)
ユーザー:amAdmin サーバー:ope	nam1.demo.osstech.co.jp			
		🔒 情報		
		トラストサークルプロファイルが更新されまし	.t.	
トラストサークルの編集				保存 リセット 戻る
名前:	GakuNin			
說明:				
IDFF ライターサービス URL:				
	共通ドメインに Cookie を書き込む IDFF ライターサ・	ービスの場所。		
IDFF リーダーサービス URL:	+ 達 ビメインから Cookie を詰ま 取る IDEE リーガー	サービスの温裕		
SAML2 ライターサービス URL:	70217X177775 COOKE 2 2079105 1077 5 - 3 -	9 - C X0/48/710		
	l 共通ドメインに Cookie を書き込む SAML2 ライター	サービスの場所。		
SAML2 リーダーサービス URL:				
	, 共通ドメインから Cookie を読み取る SAML2 リーダ	ーサービスの場所。		
状態:	<ul> <li>● アクティブ</li> <li>○ 非アクティブ</li> </ul>			
レルム:	/demo			
エンティティープロバイダ トラストサークルの最小要件は、1	つのアイデンティティープロバイダと1つのサービス	プロバイダです。プロバイダが、上で指定したレルムに	こ割り当てられます。	
	選択可能: sso-unicorn SAMLv2 1 すべてを追加 すべてを追加	選択: google.com/a/g000.osstech.co.jp SAMU https://openam.demo.osstech.co.jp:44	.v2 I3/openam SAMLv2	
		図 19 保存の確	呈認	



### 3.1.4 属性の設定

学認で利用する属性の送信設定に従って、追加する SP の送信属性の設定を行います。

• OpenAM に管理者ユーザーでログインします。

OpenAM
OPENAM へのサインイン
amadmin
パスワード
□ ユーザー名を記憶する。
<u>ログイン</u>

#### 図 20 ログイン画面

• 画面上部のメニューから「連携」を押します。



#### 図 21 連携を押す



• エンティティプロバイダから「追加した SP の EntityID(本書では https://testsp1.gakunin.nii.ac.jp/shibboleth-sp)」を押します。

	Sensorcox	https://www.spii.gov/more.meac.gov/movemv.spipma/ https://www.spii.gov/movemv.spipma/ https://www.spii.gov/movemv.spipma/ spipma/ spipma/ https://tess.sex.spip.cov/movemv.spipma/ spipma/ spipma/ https://tess.sex.spip.cov/ https://tess.spip.cov/ https://tess.sex.spip.cov/ https://tess.spip.		prent		19747	
G	GakuNin	https://test-sp1.gakumin.mi.ac.jp/shibboieth-sp[saml2 https://pensam.demo.ostech.co.jp-sk1/pensamjasml2 https://shib-idp_gakumin.mi.ac.jp/shibboieth-sp[saml2 https://shib-idp.demo.ostech.co.jp/dp1/shibboiethjsaml2 google.com/sp(2000.ostech.co.jp/aml2 https://ibsts.example.ac.in/ibsbeith-spisaml2 https://ibsts.example.ac.in/ibboieth-spisaml2		/demo	2	アクティブ	
ロンティ	ィティープロバイ	(夕(8項目)					
Eンティ 新規	ィティープロバイ 削除 エン?	イダ(8項目) ₩7≠−のインボート				_	
Eンティ 新規 名国 ま	イティープロバイ 削除 エン5 名前	(ダ(8項目) マティーのインボート	<u>م الدام (</u>	\$17 △	場所	△ <b>₩</b> 4	4
=ンティ 新規 2 国 名 □ g	イティーブロバイ 削除 エン5 名前 google.com/a/g00	<b>(ダ(3)項目)</b> マティーのインボート	▲ プロトコル ▲ SAMLy2	<b>홍1가 쇼</b> 5위	場所 /	≤ <b>1-7-L</b> /demo	4
にンティ 新規 日日 和 日 日 日	イティーブロバイ 削除 エン5 名前 google.com/a/g00 https://openam.d	(ダ (8 項目)  - (7 のインボート) 0.osstech.co.jp mo.osstech.co.jp.443/openam	プロトコル     SAMLv2     SAMLv2	<b>\$17</b> △ SP IDP	場所 ノ リモート ホスト	△ I-JI-IA /demo /demo	4
:>ティ ñ# 0 8 0 h 0 h	イティーフロバイ 削除 正とう 名前 google.com/a/g00 https://shib-idp.do https://shib-idp.do	ダ(8月目) オティーのインポート 0.osslech.co.jp emo.osslech.co.jp.443/openam omo.osslech.co.jp.443/openam	▲ プロトコル △ SAMU2 SAMU2 SAMU2	<b>\$417</b> △ SP IDP IDP	場所 ノ リモート ホスト ホスト	I UIU /demo /demo /demo /demo	4
	イティーブロバイ 用JM エン5 名射 google.com/a/g00 https://shib-idp.di https://shib-sp.exx https://shib-sp.exx	ダ(8 13日) マティーのインボート… のastechco.jp emo astechco.jp/dbj/bibboleth mpia ac.jp/bibboleth-sp mpia ac.jp/bibboleth-sp mpia ac.jp/bibboleth-sp mpia ac.jp/bibboleth-sp mpia ac.jp/bibboleth-sp	<ul> <li>Хату</li>     &lt;</ul>	\$4.7 △ SP IDP IDP SP SP	場所 リモート ホスト ホスト リモート	I UIU /demo	4
Eンティ 新規 2回 和 0 h 0 h	イティープロバイ 削除 エン3 名部 google.com/a/g00 https://shib.idp.do https://shib.idp.do https://shib.exp.ex. https://settp.exp.ex.	ダ(3項目) マティーのインボート… 0 osstech.co.jp mo.osstech.co.jp/ddy/hibboleth umple.co.jp/ddy/hibboleth umple.co.jp/ddy/hibboleth umple.co.jp/ddy/hibboleth sp totals.com.twellow.	x <b>201-31/ △</b> SAMU2 SAMU2 SAMU2 SAMU2 SAMU2 SAMU2	\$17 SP IDP SP SP SP SP	場所 リモート ホスト ホスト リモート リモート リモート	✓      ✓	4
Eンティ 新規 2回 名 0 h 0 h 0 h	イティープロバイ 削除 エン3 名解 google.com/a/g00 https://shib.idp.do https://shib.idp.do https://test.p.ex. h	ダ (8 均目) マティーの・インボート  Coastech.co.jp Coastech.co.jp/AdJ/openam Coastech.co.jp/Coastec	<ul> <li>Хотъзи</li> <li>Ханцу2</li> </ul>	\$477         \$           \$59         \$           \$10P         \$           \$0P         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$           \$\$9         \$	場所 ノ リモート ホスト リモート リモート リモート リモート リモート	L/JL/A /demo	4

図 22 追加した SPの EntityID を押す

•「表明処理」を押します。

🕆 OpenAM 🛛	+	🔷 – 🔍 😫
	😭   https://openam1.demo.osstech.co.jp/openam/federation/Federation/Federation.entityNameHref=htt 🛧	🛯 🎯 シークレット 👿新 👔
ユーザー: amAdmin サーバー: openam1.dem	norstech ca.jp	0070 b
SP		
表明コンテン! 表明処理 サー	ビス 高度	
https://test-sp1.gakunin.nii.ac.j	p/shibboleth-sp	保存 リセット 戻る
⇒ 署名と暗号化 ⇒ 基本認証		
¥ NamelD の書式		
署名と暗号化		
要求/応答署名 署名する要求/応答のチェックボックスを選択		
認証要求が署名されました:		
表明が署名されました:		
POST 応答が著名されました:		
アーティファクト応答が署名されまし;		
ログアウト要求が署名されました:		
ロッアット総合が著名されました:		
名前1D応答の管理が署名されました:		
暗号化		
属性:		
表明:		
NameID:		

図 23 表明処理を押す



• 属性マップの「新しい値」に "[SAML 属性名]=[属性名]" を入力し、「追加」を押し ます。

OpenAM × +	🕑 - 🔍 😫
🗧 🔶 🖸 🔺 保護されていない通信   https://openam1.demo.osstech.co.jp/openam/federation/SAMLvZSPAssertionContent/SAMLvZSPAsser 🛧	🔲 💩 シークレット 👿新 👔
⊥−∀-: amAdmin 'サ−r(-: openam).demo.osstech.co.jp	GØ79⊧ -
SP	
表明コンテンツ 表明処理 サービス 高度	
https://test-spl.gakunin.nii.ac.jp/shibboleth-sp	保存 リセット 戻る
⇒ 属性マッパー ⇒ アーティファクトメッセージのエンコーディング	
2 送信する属性の同意	
属性マッパー	
属性マップ	
STLUM BIL	
このマッピングは、異性マッパーで使用される設定です。マッピングは、表明内で SAML ATTRIBUTE NAME-PROFILE ATTRIBUTE NAME として定義してください。例: EmailAddress-mail	l, Address=postaladdress
エスケーブしない腐性	

図 24 属性マップへ追加

• 現在の値に"[SAML 属性名]=[属性名]"が追加されていることを確認します。

🕆 OpenAM x +	💌 – 🔍 😣
🗧 🔶 C 🔺 保護されていない通信   https://openam1.demo.osstech.co.jp/openam/Federation/SAMLvZSPAssertionContent/SAMLvZSPAssertion	🗟 シークレット 🛛 更新 👔
⊥−∀−: anAdmin ∀−≀(−: openam1.demo.osstech.co.jp Sopen-AM	GØ79⊁.
59	
表明コンテンツ 表明処理 サービス 高度	
https://test-spl.gakunin.nii.ac.jp/shibboleth-sp	保存 リセット 戻る
<ul> <li></li></ul>	
属性マッパー	
展性マップ 現在の I um coasis names to SAMI-2.0 attmame format unitum cirid 1.3.6.1.4.15993111110=computed() - 新議	
新LL14個 調加	
このマッピングは、異性マッパーで使用される設定です。マッピングは、表明的で SAML ATTRIBUTE NAME-PROFILE ATTRIBUTE NAME として定義してください。例: EmailAddress-mail, Addr	ess=postaladdress
エスケープしない展性	

図 25 属性マップへ追加



•送信する属性の数だけ設定を繰り返します。

_		
° OpenAM	и х +	
$\ \  \   \leftrightarrow \  \   \sigma$	A 保護されていない運信   https://openam1.demo.osstech.co.jp/openam/federation/SAMLvZSPAssertionContent7SAMLv2	ZSPAsser ☆ 🔲 💩 シークレット (更新 i)
그—サー:amAdn 浴 OpenAN	min 9−1(-:spenam1.dema.osstech.ca.jp N	<u>277)</u>
SP		
表明コンテン、	ツ 表明処理 サービス 高度	
https://test-		保存 リセット 戻る
<ul> <li>※ 属性マッパー</li> <li>※ 詳信する開始(</li> </ul>	<ul> <li>マーティファクトメッセージのエンコーディング</li> <li>の用意</li> </ul>	
屋体フッパー	-	
MILE & 971		
属性マップ 現在の	0   wmcasic.ramest.cSML20.atmame.format.wijum.oid13.61.41.99211.11.0*computedid *	
新しい	.vm	
このマ	?ッピングは、属性マッパーで使用される設定です。マッピングは、表明内で SAMLATTRIBUTE NAME=PROFILE ATTRIBUTE NAME として定義してください。例	EmailAddress=mail, Address=postaladdress
エスケーブしる	ない N 開 性	

図 26 属性マップへ追加

エスケープしない属性の「新しい値」に urn:oid:1.3.6.1.4.1.5923.1.1.1.10 を入力し、
 「追加」を押します。\*7

OpenAM	x +	▼ = □ (
← → C ▲ @##	れていない通信   http://openami.demo.osstech.co.jp/openam//ederation/SAMLvZSPAssertionProcessing	🖈 🔲 💩 シークレット (更新
https://test-sp1.gaku	nin.nii.ac.jp/shibboleth-sp	保存 リセット 戻る
※ 歴性マッパー ※ ※ 送信する属性の同意	アーティファクトメッセージのエンコーディング	
属性マッパー		
属性マップ		
現在の値 unroadis unroid:2 unroid:0	manests:CMU2.0 attrivanes formati unifurnoid:1.3.6.1.4.1.5923.1.1.1.10+computedid ~ [1039] [3.2342.159203300.106.1.3-mail	
新しい値	36.htt	
このマッピングは、屋	住マッパーで使用される設定です。マッピングは、表明内で SAML ATTRIBUTE NAME-PROFILE ATTRIBUTE NAME として定義してください。	91: EmailAddress-mail, Address-postaladdress
エスケープしない屋性		
364の48		
新しいS urn:oid:1	3.6.1.4.1.5973 išm	
値をエスケープしない	SANL 属性名を施定してください。ここで施定した SANL 属性は AttributeStatement に値をエスケーブせずに追加されます。SP 街で設定され	1ている場合、IdP 側の設定は無視されます。

#### 図 27 エスケープしない属性へ追加

<sup>\*&</sup>lt;sup>7</sup> エスケープしない属性の設定は、SP に eduPersonTargetedID を送信する場合のみ必要です。属性マップへ追 加で eduPersonTargetedID を設定していない場合は、エスケープしない属性の設定は不要です。



 現在の値に urn:oid:1.3.6.1.4.1.5923.1.1.1.10 が追加されていることを確認し、「保存」 を押します。

OpenAM	x + v - 1	• 🙁
← → C	🔺 保護されていない通信   https://openam1.demo.osstech.co.jp/openam/federation/SAMLVZSPAssertionProcessing 🔬 🗈 🙆 シークレット 🤅	更新
https://test-sp × 届性マッパー × 法信言る属性の同	sp1.gakunin.nii.ac.jp/shibboleth-sp	<u>戻る</u> ^
属性マッパー		
屋住フップ		- 1
現在の値	umodd:0.5340.1203tmame-formatsurjumodd:1.3.6.1.4.1.5923.1.1.1.10+computedid = IIII - IIIII - IIIII - IIIIII - IIIIII - IIIIII	
新しい彼		- 1
エスケープしない	ビンジは、実後マジバーで使用される認定です。マツビンジは、使用用で SAMLATTRIBUTE NAME *PROFILE ATTRIBUTE NAME として定義してください。例: EmainAddress-mail, Address-postaladdress い歴性	
現在の値	a unrodd136141502311110 * ANN	
新しい値	a iôtu	
値をエスケ	ウーブしない SAML 展落名を転定してください、ここで転定した SAML 展発は AttributeStatement に勝をエスクーブサザに追加されます。SP 数で放定されている場合、MP 数の設定は物格されます。	

図 28 保存を押す

 "SAMLv2 サービスプロバイダプロパティーが更新されました。"と表示されれば完 了です。

🖀 OpenAM	× (+)				· -	٥	8
$\leftrightarrow \rightarrow G$	▲ 保護されていない通信   https://openam1.demo.osstech.co.jp/openam/Federation/SAMLv2SPAssertionProcessing	\$		🔒 >	ークレット		•
ユーザー: amAdmin	'Ψ−/',−; openami demo osstech co.jp					ログアウト	
SP		-		-	_	-	
表明コンテンツ	表明処理 サービス 高度						
	⑥ 情報 SAMU/2サービスプロバイダブロバティーが更新されました。						
https://test-sp	<b>51.gakunin.nii.ac.jp/shibboleth-sp</b>			保存	リセット	戻る	
※ 送信する属性の同							
属性マッパー							
属性マップ							
現在の値	umoasiscamests: SMU:2.0 attraume.formaturijumodi 3.6.1.4.1.5923.1.1.110-computed d * BIR umodi 2.6.844.1.1303.1.241-tigita/stame umodi 0.9.2342.19200380.100.1.3+mail						
新しい値	júc, htt						
このマッヒ エスケープしない	シングは、誕往マッパーで使用される設定です。マッピングは、表明内で SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME として定義してください。 例: Email/ddre 編性	ss=mail,	Addres	s=postalad	dress		

#### 図 29 設定の更新確認

以上の作業で SP の追加作業は完了です。 追加した SP ヘアクセスし、サービスが利用可能なことを確認してください。



## 3.2 SP の削除

サービスを利用しなくなった等の理由により、SP を利用不可にする手順を説明します。 本章では次の SP を削除する手順を示します。

• EntityID

- https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp

### 3.2.1 該当 SP をトラストサークルから除外

利用しない SP をトラストサークルの一覧から削除することで、OpenAM の連携対象から 外れます。

• OpenAM に管理者ユーザーでログインします。

	OpenAM
	OPENAM へのサインイン
amadmin	
パスワード	
□ ユーザー名を記憶	72.
	ログイン

図 30 ログイン画面



• 画面上部のメニューから「連携」を押します。



図 31 連携を押す

• トラストサークルの「GakuNin」を押します。

Ор	enAM			+															) -	۰
	C 🔺	保護され		通信   <del>https</del> ://	орепал	m1.dem	o.osstech	h.co.jp/op									0		レット	E
	amAdmin # mAM	†−/{−:ope	enam1.der	no.osstech.co.jp															1	<b>□</b> Ø70
アクセ	ス制御	連携	設定	セッション				_	_	_		_	_							
721	サークル	1072	SPANE 1.8 V	V BBCAL																
このセク お、エン トラフ	クションは、 ンティティー: ストサークバ	トラストサ- テーブルに作 レ (2 項目)	ークルのプ 1度した後	ロバティーの設定 だ、トラストサー	に使用で クルに追	できます。 R 加できま	、エンティ ます。	71-7-	ブルは、ブ	าตการตา	インボートや	エクスボート	などエンテ	<₹ <b>1</b> −7	ロバイダの	管理に	史用で	3# <b>7</b> , :	エンティ	₹ <b>-</b> -
このセク は、エン トラフ 新規 (3)[3]	クションは、 >ティティー: ストサークル ・ 州除 本館	トラストサ- テーブルに作 レ (2 項目)	- クルのブ は成した後*	ロバティーの設定 で、トラストサー イティー	に使用で クルに追	できます。 Bカロできま	, エンティ ます。	7-1-7-	ブルは、ブ	10//40/	インボートや	エクスボート	などエンテ	<₹	ロバイダの	管理に	使用で	きます。: : : : :	エンティ	P
このセク ま、エン トラス 新規 日日	クションは、 ンティティー ストサークル 、 例除 を解 demo-cot	トラストサ- テーブルに作 レ (2 項目)	- クルのブ 域した後 * エンティ https:// https:// https:// sougle, https://	ロバティーの設定 で、トラストサー test-sp1.gakunin openam.demo.or shib-idp.demo.or shib-idp.demo.or shib-idp.demo.or shib-sp.example.c com/a/g000.osst	に使用で クルに追 unil.ac.jp sstech.co sstech.co ech.co.jp com/mel .ac.jp/sh	できます。 B加できま p/shibbc co.jp:443 co.jp:443 co.jp:443 elionjsam	、エンティ ます。 aleth-sp[sa l/openam] /shibbolet 12 h-sp[sam]	ティーテー: aml2  saml2 th saml2	ブルは、ブ	7ロバイダのイ	インボートや	エクスボート	などエンテ	イティーブ レ /d	⊔ <i>⊼-1\$0</i> №А	管理に	使用で <u>へ</u> 1	きます。: 快騰 アクティ:	エンティ	Ē.4−

#### 図 32 GakuNin を押す



•エンティティプロバイダの選択:から「SPのEntityID」を選択し、「削除」を押します。

OpenAM	and a second	
トラストサークルの編集		保存 リヒット 戻る
名前:	GakuNin	
說明:		
IDFF ライターサービス URL:		
	共通ドメインに Cookie を書き込む IDFF ライターサービスの場所。	
IDFF リーダーサービス URL:		
	共通ドメインから Cookie を読み取る IUFF リーダーサービスの場所。	
SAML2 ライターサービス URL:		
	共通ドメインに Cookie を書き込む SAML2 ライターサービスの場所。	
SAML2 リーダーサービス URL:	AND DE CAMPA CAMPA AND DE CAMPA DE MARKE	
状態:	● プラティブ ● プラティブ ○ (声ブララィブ	
LILA:	/demo	
エンティティープロバイダ トラストサークルの最小要件は、1	つのアイデンティープロバイダと1つのサービスプロバイダです。プロバイダが、上で指定したレルムに割り当てられます。	
	選択で利比 sse-unicorn SAMLv2 「アイズを追加 >> ドリンパ(byensum demo asster tv. co. jp SAMLv2 ドリンパ(byensum SAMLv2 ・ のかかいのでは、のかいのでは、のかいのでは、のないのい。のいいいい。のいいいいいい。のいいいいいいいいいいいいい。のいいいいいい	

図 33 SPの EntityID を削除

エンティティプロバイダの選択可能欄に SP の EntityID が追加されたことを確認し、
 「保存」を押します。

CpenAM		
トラストサークルの編集		R4 1271 R6
名前:	GakuNin	
説明:		
IDFF ライターサービス URL:		
	共通ドメインに Cookie を書き込む IDFF ライターサービスの場所。	
IDFF リーダーサービス URL:		
	共通ドメインから Cookie を読み取る IDTF リーダーサービスの場所。	
SAML2 549-7-CX URL:	共通ドメインに Cookie を来き込む SLMI 2 ライターサービスの爆発。	
SAML2 リーダーサービス URL:		
	共通ドメインから Cookie を読み取る SAML2 リーダーサービスの場所。	
祝服:	© 79717 ○ ₩79717	
LILL:	/demo	
エンティティープロバイダ		
トラストサークルの最小要件は、1	つのアイテンティティープロバイダと1つのサービスプロバイダです。プロバイダが、上で指定したレルムに割り捨てられます。	
	astrovie: 地域で https://test-spl.gakunin.nii.ac.jp/shibboleth-sp SAMLv2 ・ 道知 > google.com/a/g000.osstech.co.jp SAMLv2 ・	
	soc-unicom onecvz すべてを遺版 >>> https://openam.demo.osstech.co.jp:443/openam SAMLv2 https://openam.demo.osstech.co.jp:443/openam SAMLv2	
	< #JRR https://shib-sp.example.ac.jp/shibboleth-sp.SAMLv2	
	オペてを削除 https://testsp.example.com/mellon SAMLv2 https://testsp.example.com/mellon SAMLv2	
	Ec	
	기국	
	v v	

図 34 確認して保存



• "トラストサークルプロファイルが更新されました。"と表示されれば完了です。

ユーザー:amAdmin サーバー:op	enam1.demo.oxstech.co.jp			ログアウト
		<b>1 情報</b> トラストサークルプロファイルが更新されました。		
トラストサークルの編集				保存 リセット 戻る
名前:	GakuNin			
說明:				
IDFF ライターサービス URL:				
	共通ドメインに Cookie を書き込む IDFF ライターサービス	の場所。		
IDFF リーダーサービス URL:				
	共通ドメインから Cookie を読み取る IDFF リーダーサービ	スの場所。		
SAML2 ライターサービス URL:				
	共通ドメインに Cookie を書き込む SAML2 ライターサービ	スの場所。		
SAMLZ リーターサービス URL:	十字ビスノンから クール・を読え物 えぐかり スリーゲーキー	ビュル地震		
状態:	<ul> <li>アクティブ</li> <li>非アクティブ</li> </ul>			
レルム:	/demo			
エンティティープロバイダ			- * *	
トラストサージルの最小要任は、1	3051772777777777000173215005-ビスプロハ 選択可能・	イダです。フロハイダか、上で指定したレルムに割り当てら 週4日。	(LI 9.	
	https://text-spl.gakunin.nii.ac.jp/shibboleth-sp S https://text-spl.gakunin.nii.ac.jp/shibboleth-sp S sso-unicorn SAMLv2	AMLV2 適加 > すべてを追加 >> すべてを追加 >> く 削除 https://shib-idp.d https://shib-idp.d	0.osstech.co.jp SAMLv2 * emo.osstech.co.jp/443/openam SAMLv2 emo.osstech.co.jp/idp/shibboleth SAMLv2 ample.ac.jp/SIMboleth SAMLv2 mple.ac.jp/SIMboleth.sp SAMLv2	

図 35 保存の確認

SP を利用不可にする際は、トラストサークルからの除外のみを実施することを推奨しま す。利用者がトラストサークルの一覧に存在しない SP を利用しようとすると、OpenAM の エラー画面が表示されます。このように SP の設定自体は残しておくことで、今後改めて該 当 SP の利用を再開する場合はトラストサークルの追加を実施することにより簡単に利用を 再開できます。

もし今後利用する予定はなく SP 設定自体を削除したい場合は、メタデータ更新対象から 除外と SP の設定の削除を実施します。



#### 3.2.2 メタデータ更新対象から除外

利用しない SP について、メタデータを取り込まない設定を行います。

• OpenAM に管理者ユーザーでログインします。

	OpenAM
OPE	NAM へのサインイン
amadmin]	
□ ユーザー名を記憶する。	ログイン

図 36 管理ユーザ ログイン画面

• OpenAM 管理コンソールで対象のレルムをクリックします。(下図では demo レルム)

OpenAM	▲ レルム -	▶ 設定 -	▲ デプロイメント・	日連携	警 セッション		۰ (	
レルム								
****	ークを放得すストル	にしまんを使用し	ます みししんのでは	データフトア	第1946月 1917年6月	伊司ポリシー、およびその前	のしまん回右の時実を行うことが	
できます。	V CART VICE	10 P 7 P 20 C (0.71) C	a si go mari ciat	/ ////	BARTERAL BURLENIS	10-9-1-9-1-0-0-0-0-0-0	O P PARA O MALEN J C CD	
+新規レルム								
	2		0					
最上位	ないしょ		demo /demo					
0 1	penam more		openam.demo.osstech.co.jp 1 more					
• 7	クティブ		◎ アクティブ					

図 37 レルムの選択



左のサイドメニューの「サービス」を開きます。



\*「SAMLv2 メタデータの自動更新」をクリックします。

	▶ レルム - ♪ 設定 - 品 デプロイメント - □ 連携 替 セッション	
🏝 demo	サービス	
<ul> <li>会 ダッシュボード</li> <li>▲ 認証</li> <li>少 サービス</li> </ul>	サービス OpenAM のレルム国有のプロバティを設定します。	<b>●</b> ヘルプ
<ul> <li>データストア</li> <li>増限</li> <li>4、認可</li> <li>H all</li> </ul>	+サービスの治加 ▲ 前日:	
雪 対象 ● エージェント	サービス名 コーSAMLv2 メタザータの自動更新	/ ×
# STS	User Self Service	# x
ゆ スタリプト	□ WebAuthn Authenticator サービス	<i>₽</i> ×
	□ ダッシュボード	1 ×
	□ パスワードリセット	Ø X
	□ ポリシー設定	<i>₽</i> ×

図 39 SAMLv2 メタデータの自動更新



•「対象とするエンティティ」から対象 SP の EntityID を選択し、Del キーを押して削除 します。

- タストア			
179			
<b>同</b>	メタテータのURLとバックアップ先	のマッピング 😝	
康	https://metadata.gakunin.nii.ac.jp/gakunin- test-metadata.xml	/opt/osstech/var/lib/tomcat/data/openam/metadata.xml	×
:ージェント TS	*-	領	+ add
マリプト	実行時刻	00:00	0
	実行するサーバーのURL	http://openam1.demo.asstech.co.jp:8080/apenam	~ 0
	対象とするロール	<u>なし</u>	0
	対象とするエンティティ	https://test1.example.co.jp/testsp https://test3.example.com/testsp https://shibidip4.example.com:1452/ShibboletH/ https://mellon-test.osstech.example.co.jp:10443/mellon-test https://test-sp2.gakunin.in.ac.jp/shibboletH-sp	0
		парылекершурканалагасурыноосеоныр	-

図 40 SAMLv2 メタデータの自動更新設定

•「対象とするエンティティ」のリストから SP が削除されていることを確認し、「変更の保存」を押します。

<b>譬</b> 対象	test-metadata.xml	тори оконолия таки контиска како организация на положители и н	. <b>.</b> .
∲ エージェント ≉ STS	*-	値	+ add
ゆ スクリプト	実行時刻	00:00	0
	実行するサーバーのURL	http://openam1.demo.osstech.co.jp:8080/openam	0
	対象とするロール	なし -	0
	対象とするエンティティ	https://test1.example.co.jp/iestsp https://test3.example.com/testsp https://shibidid4.example.com/t452/shibbidieth/ https://meilon-test.ostech.example.co.jp.10443/meilon-test https://test-seg_gakuincin.ita.gi/shibbidiethy- https://test-seg_gakuincin.ita.gi/shibbidiethy-	0
	除外するエンティティ		0
	エンティティの新規登録を許可する		0
	有効期限をチェックする		0
	署名を検証する		0
			変更の保存

図 41 確認して保存



•「変更を保存しました」と表示されれば完了です。

THE ALL REAL	test-metadata.xml		
♦ エージェント	+-	値	+ add
🏘 STS	<ul> <li>変更を保存しまし</li> </ul>	- <i>t</i> <sub>c</sub>	
<♪ スクリプト	夫仃阿刘	00:00	0
	実行するサーバーのURL	http://openam1.demo.osstech.co.jp:8080/openam	~ <b>0</b>
	対象とするロール	なし	• 0
	対象とするエンティティ	https://test1.example.co.jp/testsp https://test3.example.com/testsp https://test3.example.com/t452/Shibboleth/ https://testset2.gakunin.nii.ac.jps/thbboleth-sp https://testse2.gakunin.nii.ac.jps/thbboleth-sp https://testse2.gakunin.nii.ac.jps/thbboleth-sp	0
	除外するエンティティ		0
	エンティティの新規登録を許可する		0
	有効期限をチェックする		0
	署名を検証する		θ
			変更の保存

図 42 保存の完了



### 3.2.3 SP の設定の削除

利用しない SP の設定を削除します。

• OpenAM に管理者ユーザーでログインします。

openAM
OPENAM へのサインイン
amadminj
パスワード
□ ユーザー名を記憶する。

#### 図 43 管理ユーザ ログイン画面

• 画面上部のメニューから「連携」を押します。



#### 図 44 連携を押す



エンティティプロバイダから「削除したい SP の EntityID(本書では https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp)」をチェックし、「削除」を押します。

القال	名詞	▲ エンティティー		L11.1	h	状態
	demo-cot	https://set-spi_gakimin mi.ac_ip/shibboleth-spisami2 https://set-spi_gakimin.mi.ac_ip/shibboleth-spisami2 https://shib-set.ac_ip/sami2 google.com/a/g000/assterk-to.gip/sami2 https://setspi_gakimi2 https://setspi_gakimi2 saso-unicom/sami2 https://shibboleth-spisami2		/dem	0	アクティブ
0	GakuNin	https://seenam.demo.oszlech.co.jp.443/openamijaami2 https://seta-oglawinnin/ais_pi/hihboleth-sgi.sgi.ami3 https://seta-oglawinnin/ais_pi/sgi.hihboleth-sgi.sgi.ami3 https://seta-oglawinnin/ais_pi/sgi.hihboleth-sgi.ami3 https://setap.aarepia.com/meil/opiami2 https://setap.aarepia.com/meil/opiami2 https://setap.aarepia.com/meil/opiami2		/dem	0	アクティブ
ンテ	・イティープロバイダ(	(8 項目)				
ンテ 11月 11月	・イティープロバイダ (別称 ユ)アイア	8項目) イーのインボート			_	
ンテ 	イティープロバイダ ( 創業 ユ ティテ 名言	0ਸ਼ੑੑੑ <u>ਗ਼</u> ੑੑੑੑੑੑੑੑੑੑੑੑੑੑਗ਼ੑੑੑੑੑੑੑਗ਼ੑੑੑੑੑੑੑੑੑੑ	▲ 701-31k	917	、	< D.L.L
ンテ 規 [1]	イティープロバイダ( 創際 アイデ 名音 google.com/a/g000.oss	8 ЛВ) іч—012#- F Лесћсо јр	х 701-3/4 ∧ SAMUv2	<b>917</b>	<ul> <li></li></ul>	л UJLL /demo
ンテー	イティープロバイダ( 創際 アイデ 名音 google.com/a/g000.oss https://openam.demo.	8 第日) マールインボート tech.co.jp ossied:co.jp.443/openam	<ul> <li>ХОРЭЛ ∧</li> <li>SANU2</li> <li>SANU2</li> </ul>	<b>917</b> SP IDP	<ul> <li>場所</li> <li>リモート</li> <li>ホスト</li> </ul>	л UJLL /demo /demo
	イティーブロバイダ( 削除 アイテ を回 google.com/a/g000.oss https://openam.demo. https://chib-idp.demo.	Ø 7/E) ≺−Øf ≥/F−ト_ Mechca jp osstech ca jp 443/openam osstech ca jp 443/openam	х 70 № Ли № SAMU2 SAMU2 SAMU2	<b>9-17</b> SP IDP IDP	<ul> <li>場所</li> <li>リモート</li> <li>ホスト</li> <li>ホスト</li> </ul>	<ul> <li>العلاما</li> <li>/demo</li> <li>/demo</li> <li>/demo</li> </ul>
	イティーフロバイダ(	8 7(B) y==0:f2:y==b=	ХОТЕЛИ ▲ 544Lv2 544Lv2 544Lv2 544Lv2 544Lv2 544Lv2	<b>9-17</b> SP IDP IDP SP	<ul> <li></li></ul>	►ILL /demo /demo /demo /demo
	イティーフロバイタ () 1) 1) 1) 1) 1) 1) 1) 1) 1) 1	37E)     (→ D 1 2 K − k − k     dechca jp     ostachca jp     ostachca jp joldgr/hibboleth     ca jp/hibboleth sp     can/mellon	▲ 70 1-37 A	<b>9-17</b> SP IDP IDH SP SP	場所 リモート ホスト ホスト リモート リモート	LILL     /demo     /demo     /demo     /demo     /demo     /demo     /demo
	イティープロバイダ ( ) ) ) ) ) ) ) ) ) ) ) ) )	87(2) →	x 701131 ↔ SMU2 SMU2 SMU2 SMU2 SMU2 SMU2 SMU2	9477 SP IDP DP SP SP SP	場所 リモート ホスト ホスト リモート リモート リモート リモート リモート	
	イティープロバイダ ( 単原 ユ アイア なの google com/a/g000 oss https://bihi-idp.demo. https://bihi-idp.demo. https://bihi-idp.demo. https://bihi-sp.campi ntps://testsp.campi ntps://testsp.campi ntps://testsp.campi	8 JHEI)       Image: Control of the second sec		<b>9-17</b> SP IDP SP SP SP SP SP	場所 リモート ホスト リモート リモート リモート リモート リモート リモート	L/b.2.      /demo     /demo     /demo     /demo     /demo     /demo     /demo     /demo

図 45 SP の EntityID を削除

・"【SPのEntityID】が削除されました。"と表示されれば完了です。

z=#=;anAdmin #==/(=;openam1.demio.osstech.co.jp							
アクセン	ス制御 連携	設定 セッション					
			● 情報 https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp が別除されました。				
トラスト	サークル設定 × S	AML 1.x の設定					
このセク ィティー トラス 新規	ションは、トラストサー テーブルに作成した後で トサークル (2 項目) 削除	クルのプロパティーの設定に 、トラストサークルに追加で	復用できます。エンティティーテーブルは、プロバイダのインボートやエクスボートなどエンティティープロバイダの管理に使用できます。エンティティーは、エンテ きます。				
28	名前 ⊿	エンティティー	レルム 状態				
	demo-cot	https://test-sp1.gakunin. https://openam.demo.os https://shib-idp.demo.os google.com/a/g000.osste https://testsp.example.os sso-unicorn[saml2 https://shib-sp.example.	nilac.jp/shibboleth.spjsami2 //demo アクティブ stehc.ac.jp/shibboleth/splsami2 stehc.ac.jp/shibboleth/sami2 stehc.ac.jp/shibboleth/sami2 stehc.ac.jp/shibboleth/sami2 ac.jp/shibboleth-splsami2				
	GakuNin	https://openam.demo.os https://test-sp2.gakunin. https://shib-idp.demo.os google.com/a/g000.osste https://testsp.example.o	またたた。				

#### 図 46 削除の完了

以上で、SP の削除は完了です。

**OSSTech** 

## 3.3 IdP のサーバー証明書の更新

サーバー証明書の更新手順について説明します。作業の流れは学認の手順 (IdP Key Rollover) と同様で、メタデータ伝播中に IdP が利用できない期間が発生しないようにします。手元に更新用のサーバー証明書および秘密鍵が準備されているものとします。

#### 3.3.1 1日目

#### 3.3.1.1 Apache に対して証明書の更新

OpenAM サーバーの Apache の証明書を新しいものに差し替え、Apache の再起動を実施 します。

#### 3.3.1.2 学認申請システムにて証明書を追加

学認申請システム上で、予備の欄に更新用のサーバー証明書を登録します。すでに予備の 欄に証明書が登録済みの場合、古いサーバー証明書が学認申請システム上に残っている状態 です。今回のタイミングで整理し、学認申請システム上では、現在利用中のサーバー証明書 と予備の欄での更新用のサーバー証明書を登録した状態としてください。

#### 3.3.1.3 OpenAM にサーバー証明書の追加

更新用のサーバー証明書を OpenAM に追加します。更新用のサーバー証明書と秘密鍵を、 署名鍵/暗号鍵を OpenAM のキーストアヘインポートの手順を実施してキーストアにイン ポートします。

- 本書では、現在利用中の鍵ペアのエイリアス名を gakunin-cert-2023、更新用のもの を gakunin-cert-2024 とします。エイリアス名はご利用の環境に合わせて読み替えて ください。
- OpenAM が冗長化構成の場合は、1 台の OpenAM でインポートを実施し、作業後に他のサーバーへキーストアファイルをコピーしてください。全ての OpenAM サーバーが同じキーストアファイルを利用する必要があります。

キーストアファイルの更新後、Tomcatの再起動を行います。

# systemctl restart osstech-tomcat



OpenAM のホスト IdP の設定を変更します。

• OpenAM に管理者ユーザーでログインします。

OpenAM
OPENAM へのサインイン
amadmin    パスワード   ユーザー金を取得する。
DØ4>

図 47 管理ユーザ ログイン画面

• 画面上部のメニューから「連携」を押します。



図 48 連携を押す



・エンティティプロバイダから、「ホスト IdP の EntityID(本書では https://shibidp.demo.osstech.co.jp/idp/shibboleth)」をクリックします。

	м	× +				
→ c	▲ 保護され	ていない通信  <del>https:</del> // <b>openam1.demo.osstech.co.jp</b> /openam/federatio			🖈 🗆 🖨	シークレット (更
	110-00	mporytes sprzakamen macjpyrnoboteni sppomia https://pemaid.emo.ostech.co.gip/dog/htmlaml2 https://pitub-dg.demo.ostech.co.gip/dg.htmlaml2 google.com/alg500 anstech.co.gip/dg.html2 https://totspc.sample.com/mellonjaml2 sos unicom/saml2 https://totspc.asmple.com/mellonjaml2		paene		79717
Galo	kuNin	https://test.spl.gakumin.mia.c.jp/hibboleth-splpaml2 https://pers.ade.mo.ststk-fo.gioH3.poenumisaml2 https://test.spl_gakumin.mi.ac.jp/hibboleth-splpaml2 https://thib.getemo.ststk-fo.gio/pdg/hibboleth[saml2 google.com/a/g000.aststeft.oo_jplpaml2 https://test.spample.com/mid0ml01jaml2		/demo	,	79717
		https://shib-sp.example.ac.jp/shibboleth-sp]saml2				
ロンティテ	ティープロバイダ	https://shib-sp.example.ac.jp/shibboleth-sp(saml2	_	_	_	
Eンティテ 新規 「 月日 本村	ティープロバイダ 削除 <u>エンティ</u>	https://shib-sp.example.ac.jp/shibboleth-sp(saml2 (8 項目) アイーのインボート	70 k 11 k	411	道所	
ンティテ 所規 1 画 名組	ティーフロバイダ 削除 エンティ N N nele com/a/v000 g	https://shib-sp.example.ac.jp/shibboleth-sp(saml2 (9 項目) ディーのインボート		<b>317</b> ▲	<u>場所</u> リモート	A VALA A
ンティテ 5編 2 国 名前 0 goog	Fィープロバイダ 削除 ユンティ N Digle.com/a/g000.o ps://openam.dem	https://shib-sp.example.ac.jp/shibboleth-sp(sam12 (まれ日) アイージインボート	<b>7⊡⊁⊐Л</b>	<b>9417</b> ▲ SP IDP	場所 4 リモート ホスト	△ <b>レルム</b> △ /demo /demo
ンティテ 1線 1回 名前 1回 名前 10 goog 10 http	Fィーフロバイダ NJM エンティ H ogle.com/a/g000.o ps://openam.dem ps://shib-idp.demw	https://thib-sp.example.ac.jp/thibboleth-sp(sml2 (各項目) アモーのインポート astech.co.jp	プロトコル ム SAMIV2 SAMIV2 SAMIV2	<b>\$17</b> ▲ SP IDP	場所 4 リモート ホスト ホスト	△ <b>レルム</b> △ /demo /demo
ンティテ 観… 「 こ 名和 」 gooj http 」 http	ディーフロバイダ 削除 ロジティー pgle.com/a/g000.o ps://openam.demy ps://shib.idp.dems ps://shib.idp.dems ps://shib.sp.examy	https://shib-sp.example.ac.jp/shibboleth-spisaml2 (8 項目) アイージインボート astech.co.jp astech.co.jp/dpi/shibboleth osotech.co.jp/dpi/shibboleth osotech.co.jp/dpi/s	701≻⊐Ли	\$17 ▲ SP IDP IDP SP	場所 2 リモート ホスト ホスト リモート	LINA A
ンティテ 新規 「夏」名前 「東ooy 」 http 」 http 」 http	ディーフロバイダ 削除 エンティ・ 時 ge.com/a/g000.0 ps://openam.dem ps://shib-idp.dem ps://shib-jop.enam ps://testsp.enamp	https://shib-sp.example.ac.jp/shibboleth-sp(saml2 (9 項目) アイーのインボート astech.co.jp astech.co.jp astech.co.jp/dd/shibboleth aste	701-⊐ли SMUs2 SMUs2 SMUs2 SMUs2 SMUs2	<b>\$17</b> ▲ SP IDP IDP SP SP	場所 2 リモート ホスト リモート リモート リモート	Links a
ンティテ 新規 「 日日 名前 日日 2001 日本 日日 100 日本 日日 100 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	Fイーフロバイダ MIN エンティ Bigle.com/a/g00.o. ps://openam.dem ps://shib.idp.dem ps://shib.sq.exampl ps://testsp.exampl ps://testsp.exampl	https://thib-sp.example.ac.p/thibboleth-sp(sml2 (8 72 =) 77 = -07 = 2 # - 1	プロトコル A SAMLv2 SAMLv2 SAMLv2 SAMLv2 SAMLv2 SAMLv2	<b>\$17</b> ▲ SP IDP IDP SP SP SP	場所 / リモート ホスト ホスト リモート リモート	► LPLA ▲ /demo /demo /demo /demo /demo
ンティテ 新規 日日 名納 日日 2000 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本		https://bib-sp.example.ac.jp/bibboleth-sp(saml2  (8 HE)  70-1-2-H  astech.co.jp  astech.co.jp  astech.co.jp/dp/bboleth-sp  astech.co.jp/dp/bboleth-sp  astech.co.jp/dp/bboleth-sp  astech.co.jp  boostech.co.jp/dp/bboleth-sp  astech.co.jp  boostech.co.jp/dp/bboleth-sp  bo	プロトコル         △           SAMLy2         SAMLy2           SAMLy2         SAMLy2           SAMLy2         SAMLy2           SAMLy2         SAMLy2           SAMLy2         SAMLy2	<b>317</b> ▲ SP IDP IDP SP SP SP SP SP SP	場所 / リモート ホスト リモート リモート リモート リモート	A DRL A /demo /demo /demo /demo /demo /demo /demo /demo

図 49 ホスト IdP の EntityID を選択

 証明書エイリアスの署名の「新しい値」に更新用のエイリアス名を入力し、「追加」を 押します。

IDP	
主動 シュンジ 主動 田 サービュ 宝奈	
009337777 0093506 7 °C A 1608	
https://shib-idp.demo.osstech.co.jp/idp/shibboleth	保存 リセット 戻る
※ 署名と地号化 ※ 認証コンテキスト ※ 基本認証	
≈ NamelD の書式 ≈ 表明時間 ≈ 表明キャッシュ	
	*必須入力フィールド
署名と暗号化	
要求/応答署名	
<b>楽乞する要求/応答のチェックボックスを通</b> 例	
認証要求:	
アーティファクト解決処理:	
ログアウト要求: □	
11/27/21-10台: 0 名前の男性の問題: 0	
2.前の資源の管理: □	
NamelD 接号化: □	
証明書エイリアス	
著名: 現在の個 gakunin-cert-2023 ^ NUR	
#LUA	

図 50 証明書の追加



・証明書エイリアスの署名の現在の値のリストの1番目が「gakunin-cert-2023(現在利用中のエイリアス名)」2番目が「gakunin-cert-2024(更新用のエイリアス名)」であることを確認し、「保存」を押します。

IDP	
表明コンテンツ 表明処理 サービス 真変	
https://shib-idp.demo.osstech.co.jp/idp/shibboleth	保存しりセット 戻る
※ 署名と陽号化 ※ 認知コンテキスト ※ 基本認証	
8 NameiD の第二 8 政府時間 8 政府キャッシュ	■必須入力フィールド
署名と暗号化	

図 51 確認と保存

 "SAMLv2 アイデンティティープロバイダプロパティーが更新されました。"と表示 されることを確認します。

IDP	
表明コンテンツ 表明処理 サービス 高度	
	<b>• • •</b>
	SAMEVZフィナンティティーノロハイダノロハナイーが更新されました。
https://shib-idp.demo.osstech.co.jp/idp/shibboleth	
※ 署名と暗号化 ※ 認証コンテキスト ※ 基本認証	
× <u>NamelDの書式</u> × 表明時間 × 表明キャッシュ	
署名と暗号化	
要求/応答署名	
署名する要求/応答のチェックボックスを選択	
認証要求:	
アーティファクト解決処理:	
ログアウト要求:	
ログアウト応答:	
名前 ID 要求の管理:	
名前10応告の管理:	
NameiD 暗号化: □	
証明書エイリアス	
著名: 現在の値 gakunin-cert-2023 ^ 削除 gakunin-cert-2024	





 IdP のメタデータを表示します。メタデータの表示 URL は次のとおりです。\*<sup>8</sup>
 https://【FQDN】/【コンテキストパス】/saml2/jsp/exportmetadata.jsp?entityid= 【IdP の EntityID】&realm=【レルム名】

表示されたメタデータにおいて、署名用 (<KeyDescriptor use="signing">) のサーバー 証明書が新/旧2つあることを確認します。

This XML file does not appear to have any style information associated with it. The document tree is shown below.			
<pre>etnityOescriptor nutos="urn:coasis:numes:tc:SURL2.0:metadata" entityID="https://shib-idp.dem.osstech.co.jp/idp/shibdoteth"&gt;</pre>			
v=c.bi000025 v=cbc000025 ulpcEX008ptTitficate RIID02CCAupAiBaEU2/rtudfn32aLcdHnKsk2d0TCShdQFURA2DivcRdQEB8QAYTEUAAG ALBEBNCSLAd_JAMB_WBAgHBVh2aLvMDLeATV0QHALTaCLuNahG2EdTALBgVPA HF6F ulpcEX008ptTithAu809TUB1CYgDfTALBgVPAMBHBHAMHJHAD1100ce0D2DavBHeA N020HC2CAUpAIBABUAGEAUDCAUACLUALAD_AVBAGHBVPA2LvMT5AcAU DipcEX008ptTithAu809TUB1CYgDfTALBgVPAMBHBHAMHJHAD1100ce0D2DavBHeA N020HC2CAUpAIBABUAGEAUDCAUACLUALAD_AVBAGHBVPA2LvMT5AcAU ZF97TFMURAAUECg4CFFTMUT0BAHABLCGAUCLUALBGACTEAUDCAUCLUALBGAUERDJgTAFACAUCLUALBGAUERDJgTAFACAUACLUALBGAUERDJgTAFACAU p=c5d51jSaLltAtvaLdJMHABLCGAUEDGAUERDJgTABUBGAUECKUCKLUALBGAUERDJgTAFACAUACLUALBGAUERDJgTAFACAUALBGAUERDJgTAFACAUALBGAUERDJgTAFACAU p=c5d51jSaLltAtvaLdJMHABLCGAUERDJgTABUBGAUERDJgTAFAUERDJgTABUBGAUERDJgTAFAUERDJgTABUBGAUERDJgTAFAUERDJgTABUBGAUERDJgTAFAUERDJgTABUBGAUERDJgTABUBGAUERDJgTABUBGAUERDJgTAFAUERDJgTABUBGAUER			
<			
v≺Key0escriptor use="signing">			
w=ds:ReyInfo xmlms:ds="http://www.ws.org/2000/09/xmlds:g#">			
<pre>vertextBitIonsexter(); eds:SID0Cert1F1ctere=NtIDqTCCApEghaIBxgTUTZAAILbFC2y(XF4KBaLqsT/bdQVHAcIbacH0QM22CLMAG_ALUEDHCSLAb)JMQVUAgHBVva3LvRBwCQVVQQHApTaCLWAGHAC2yWpAdAYDBVHAAU BYNRH;BBMAGAILCearT1HYVQYJACDXFLB;WYAAHBHHAAMHAH,MI;MHADTBACAUJUAGHUNGA,WIQUAJUMA;BUNQGZ=NUCCBHACAUGEGHAV4;AAFEAFEAFBAUVBACKU BYNRH;BBMAGAILCearT1HYVQYJACDXFLB;WYAAHBHHAAMHAH,MI;MHADTBACAUJUAGHUNGA,WIQUAJUMA;BUNQGZ=NUCCBHACAUGEGHAV4;AAFEAFBAUVBACKU BYNRH;BBMAGAILCearT1HYVQYJACDXFLB;WYAAHBHHAAMHAH,MI;MHADTBACAUJUAGHUNGA,WIQUAJUMA;BUNQGZ=NUCCBHACAUGEGHAV4;AAFEAFBAUVBACKU BYNRH;BBMAGAILCearT1HYVQYJACDXFLB;WSHLSYNT)LISSUEGHAUHATDZHracky]THSWMAJISS MINU#750Ucd06000HEETZIBAU +05)32AFFZC(TMvv2XH4)+f122xdg;RBHCLSSTD1;LISSUEGHAUHATDZHracky]THSMMAJISS MINU#750Ucd060HEETZIBAU(SHCCGZHAV4)AFEAFBAUFBACGHATDFACHGEGHAV +05)32AFFZC(TMvv2XH4)+f122xdg;RBHCLSSTD1;LISSUEGHAUHATDZHracky]THSMMAJISS MINU#750Ucd060HEETZIBAU(SHCCGZHAV4)AFEAFBAUFBACGHATDFACHGEGHAV +05)32AFFZC(TMvv2XH4)+f122xdg;RBHCLSSTD1;LISSUEGHAUHATDZHracky]THSMMAJISS MINU#750Ucd060HEETZIBAU(SHCTGHVCGHATDFACHGEGHAV4) +05)32AFFZC(TMVv2XH4)+f124xdg;RBHCLSSTD1;LISSUEGHAUHATDZHracky]THSMMAJISS MINU#750Ucd060HEETZIBAU(SHCTGHVCGHATDFACHGEGHAV4) +05)32AFFZC(TMVv2XH4)+f124xdg;RBHCLSSTD1;LISSUEGHAUHATDZHracky]THSMMAJISS MINU#750Ucd060HEETZIBAU(SHCTGHVCGHATDFACHGEGHAV4) +125;29114560HT12HULFFFRHFFFRHRBFC;596HBHZ1EJGFTGHABBALHIALMYNCHGZFUXUJNBISTY44+v2TUUSJBHSTG4CSG2HAV4AFFMQV7NCHCHGABBAUGHAUFFX 593dayYT(R0QPUGHAUX)/WXMIXTBBBHBHBHAFFRBACHBACGHYNCGHATCHZYVYYU(MBISTY44+v2TUUSJBHSTG4CSG2HAV4AFFMQV7NCHCHGABBAU 593dayYT(R0QPUGHAUX)/WXMIXTBBBHBHBHFFRBACHTBC4CHXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</pre>			
<pre>&gt;/ds:ReyInfor </pre> /bipdescriptor> /bipdescriptor> dwf:ifictEestolitionFervice_index="0"_isBefault="true"_Binding="urn:oosis:names:tc:SML:2.0:bindings:SAMP" Location="https://genum.dems.ostech.co.jp/opman/Ltfick.Rboolver/mtalkia/dems/idpl"/= <singtelogoutservice_binding="urn:oosis:names:tc:sml:2.0:bindings:rhtp_redirect" <br="" location="https://penam.demo.osstech.co.jp/openam/IDPSLoRedirect/metalLias/dems/idpl">ResponseLocation="https://openam.demo.osstech.co.jp/openam/IDDSLoRedirect/metalLias/dems/idpl" ResponseLocation="https://openam.demo.osstech.co.jp/openam/IDDSLoRedirect/metalLias/dems/idpl"</singtelogoutservice_binding="urn:oosis:names:tc:sml:2.0:bindings:rhtp_redirect">			

図 53 OpenAM IdP メタデータ

作業は以上で完了です。設定を終えたら、任意の学認 SP が使えることを確認します。

\*<sup>8</sup> 例として、OpenAM セットアップガイドに従って構築した OpenAM の場合、メタデータ表示 URL は 次のとおりです。https://openam01.example.co.jp/openam/saml2/jsp/exportmetadata.jsp?entityid=https://shibidp.demo.osstech.co.jp/idp/shibboleth&realm=/sso



#### 3.3.2 X 日目

学認申請システムにて予備の欄に証明書を追加した申請が承認され、学認メタデータに反 映された日を X 日目とします。

### 3.3.3 X + 15 日目

新しい証明書が含まれたメタデータが伝播されたため、OpenAM による SAML の署名として新しい証明書が利用されるよう設定します。

• OpenAM に管理者ユーザーでログインします。

OpenAM		
OPENAM へのサインイン		
amadmin    パスワード   ユーザー&を記述する。		
D74V		

図 54 管理ユーザ ログイン画面

• 画面上部のメニューから「連携」を押します。

GenAM CULL - F	設定・ 山 デプロイメント 🛛 連携 🔮 🦁 ッショ	v <u>۵</u> +
レルム		
対象および設定データを整理するためにレ. できます。	レムを使用します。各レルム内では、データストア、管理権限、認証連	額、認可ポリシー、およびその他のレルム協有の設定を行うことが
+ 新規レルム		
最上位のレルム	demo /demo	
openam 1 more	openam. demo. oostech. co.]p 1 more	
◎ アクティブ	◎ アクティブ	

図 55 連携を押す



・エンティティプロバイダから「ホスト IdP の EntityID(本書では https://shibidp.demo.osstech.co.jp/idp/shibboleth)」をクリックします。

Ope	nAM	× (+)				
>		れていないない場合。 Https://openam1.demo.osstech.co ingosystes.spr.gedmintmac.gystmotoren oppame https://openamidemo.osstech.co.gipt43/openamidam https://openamidam.osstech.co.giptam12 https://otisto.posample.com/inelionjam12 soo unicom/gam12 soo unicom/gam2	j <b>p</b> /openam/řederation/ř-SAuthDomainsEdit 12 mlz		☆ C	1 @ ⊅-⊅レット (E
	GakuNin	https://test-sp1.gakunin.nii.ac.jp/shibboleth-sp]saml2 https://openam.demo.osstech.co.jp>443/openamijsam https://test-sp2.gakunin.nii.ac.jp/shibboleth-sp]saml2 https://shib-idp.demo.osstech.co.jp/idp/shibboleth[sa google.com/a/g000.osstech.co.jp]saml2	I2 mlz		/demo	アクティブ
		https://testsp.example.com/mellonjsami2 https://shib-sp.example.ac.jp/shibboleth-sp[saml2				
こンテ・ 新規	ィティープロバイ 削除 エンテ	https://whitsp.axample.com/melionjiami2 https://whitsp.example.ac.jp/shibboleth-spisami2 ダ (8 項目) イディーのインポート		_	_	_
:ンテ· 新規 日国	ィティープロバイ 創株 エンテ 名前	https://ekits.p.example.com/melionjami2 https://ekits.p.example.ac.jp/shibboleth-spisami2 ダ(8項目) ペディーのインボート	۸۲۵۲۵۲ م	ム タイブ	△ 場所	۵ ۵،۳۷۹ ۵
ンテ・ 新規… 日日	イティープロバイ ● 所除 エンテ 名前 google.com/a/g001	https://while.go.example.com/melionjami2 https://while.go.example.ac.jp/shileboleth-epizami2 ダ(8月日) イディーのインボート	▲ プロトコル 5.Mit2	△ <b>\$17</b> SP	△ 場所 リモート	∠ I+Jk-IA ▲ /dema
:ンテ· 観… 日日 日日	ィティープロバイ 原語 支約 google.com/a/g001 https://openam.de	https://whits.p.axample.com/melionjiami2 https://whits.p.axample.ac.jp/shibboleth-spizami2 ダ(3項目) イティーのインボート bostech.co.jp ma_sutech.co.jp	▲ プロトコル SANLV2 SANLV2	ム <b>タイブ</b> 5.P IDP	△ 場所 リモート ホスト	∆ <mark>I-/I-La</mark> ∆ /demo /demo
:ンテ· (線 ) 目 	イティーブロバイ 原語 z>テ 名前 google.com/a/g000 https://openam.de https://shib.idp.de	https://whits.example.ac.jp/shibboleth-spisami2 https://shib-sp.example.ac.jp/shibboleth-spisami2 ダ(8項目) イディージィンボート Josstech.co.jp mp.osstech.co.jp/dg/shibboleth	له <mark>کتاب کاله</mark> ۲۵۲۲ کیل ۲۵۸۲ کی ۲۵۸۲ کی	▲ <b>タイブ</b> SP IDP IDP	△ 場所 リモート ホスト ホスト	△ L/b/La △ /dema /demo /demo
:ンテ· 観… 1日 日 日	イティーブロバイ 同様 エンデ 名前 google.com/a/g000 https://openam.de https://shib.idp.de https://shib.idp.de	https://doibg.example.com/melionjami2 https://doib.g.example.cc/p/bibboleth-spizami2 # (3 IRE) #	▲ プロトコル SAMiv2 SAMiv2 SAMiv2 SAMiv2 SAMiv2	▲ <b>タイブ</b> SP IDP IDP SP	△ 場所 リモート ホスト ホスト リモート	∆ <b>1-78-La</b> △ /demo /demo /demo
:ンテ・ 新規 日日 日日 日日 日日 日日 日日 日日 日日 日日 日日 日日 日日	イティープロバイ BIN エンア 名前 gogle.com/a/g00 https://bloidp.dom https://bloidp.dom https://bloidp.dom https://bestsp.exan	https://white.arxingle.com/melionjiami2 https://white.go.example.ac.jp/shibboleth-spicami2 ダ(3項目) イティーのインポート Losstech.co.jp mo.osstech.co.jp/ indextech.co.jp/shibboleth mpdir.ac.jp/shibboleth mpdir.ac.jp/shibboleth mpdir.ac.jp/shibboleth mpdir.ac.jp/shibboleth	▲ プロトコル SANLv2 SANLv2 SANLv2 SANLv2 SANLv2	▲ タイプ     SP     IDP     IDP     SP     SP     SP	▲ 場所 リモート ホスト ホスト リモート リモート	LINA A /demo /demo /demo /demo
	イティーフロバイ 周期 エンテ 名前 google.com/a/g00 https://openam.de https://shb 3cp 02 https://shb 3cp 02 https://stbs.pe.org	https://whits.p=acample.ac.on/melion(jami2 https://whits.p=acample.ac.jp/shibboleth-sp[sami2 ダ(8項目) ペアイーのインパート Josstech.co.jp mp.astach.co.inist&Jopenam mo.osstech.co.jp/dp/shibboleth mp.astach.co.inist&Jopenam mo.osstech.co.jp/dp/shibboleth mp.astach.co.jp/shibboleth mp.astach.co.jp/shibboleth-sp	کتاب عالی           SAMLv2         SAMLv2           SAMLv2         SAMLv2           SAMLv2         SAMLv2           SAMLv2         SAMLv2           SAMLv2         SAMLv2	▲ <b>タイブ</b> 5P IDP IDP 5P 5P 5P	△ 場所 リモート ホスト ホスト リモート リモート	△ 1/8/L △ /dema /dema /dema /dema /dema
:ンテ· 紙規 日日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	イティープロバイ NH体 エンテ 名称 bttps://openan.de https://btb.idp.dc https://btb.sp.res https://bts/sp1ga https://bts/sp1ga	https://debsp.acample.com/melion(sam2 https://debsp.acample.com/melion(sam2 # (3 HE) # 7 - D - 2 H - F bastech.co.jp mo astech.co.jp mo astech.co.jp/dobbo/mb mpacs.cjp/dobbo/mb mpacs.cjp/dobboleth.sp umin.mi.ac.jp/shibboleth.sp	▲ プロトコル SAMIv2 SAMIv2 SAMIv2 SAMIv2 SAMIv2 SAMIv2 SAMIv2 SAMIv2	△ <b>\$477</b> SP IDP SP SP SP SP SP	△ 場所 リモート ホスト リモート リモート リモート リモート	∠ UBL △ (demo /demo /demo /demo /demo /demo

図 56 ホスト IdP の EntityID を選択

• 証明書エイリアスの署名の現在の値のリストの1番目の"gakunin-cert-2023(現在利用 中のエイリアス名)"を選択し、「削除」を押します。





• 証明書エイリアスの署名の現在の値のリストが「gakunin-cert-2024(更新用のエイリ アス名)」だけであることを確認し、「保存」を押します。

IDP	
表明コンテンツ 表明処理 リービス 高度	
https://shib-idp.demo.osstech.co.jp/idp/shibboleth	保存 リセット 戻る
◎ 署名と暗号化   ◎ 認証コンテキスト   ◎ 基本認証	$\mathbf{O}$
× NamelD の書式 × 表明時間 × 表明キャッシュ	
	* 必須入力フィールト
署名と暗号化	
要求/店苦萄名	
著名す◎便水(k)音のチェックホックスを追訳 認証要素:	
アーティファクト解決処理:	
ログアウト要求:	
ログアウト応答:	
名前 臣 要求の管理:	
名前 ID 応答の管理:	
暗号化	
NamelD 暗号化: □	
証明書エイリアス	
署名: 現在のf gakunin-cert-2024 ^ 刻印	

図 58 署名用エイリアスの更新

 "SAMLv2 アイデンティティープロバイダプロパティーが更新されました。"と表示 されることを確認します。

IDP		
表明コンテンツ 表明処理 サービス 高度		
	<b>() 情報</b> SAMLv2 アイデンティティープロバイダプロパティーが更新されました。	
https://shib-idp.demo.osstech.co.jp/idp/shibboleth		保存 リセット 戻る
≥ 署名と暗号化 ※ 認証コンテキスト ※ 基本認証		
× NamelD の書式 × 表明時間 × 表明キャッシュ		*必須入力フィールド
署名と暗号化		
■実式な客電名: ■名する東大次第のチェックボックスを選択 応証要求:		

図 59 更新の完了

作業は以上で完了です。設定を終えたら、任意の学認 SP が使えることを確認します。問題がなければ、学認申請システムから古い証明書を削除し、新しい証明書を予備の欄から移



動してください。



## 4 改版履歴

- 2023年04月28日リビジョン1.0
  - 初版作成