Full SLO(Single Logout)の設定方法

本稿でSLOの設定方法を説明していますが、学認のIdP/SPに対してSLOの実装を強制もしくは推奨するものではありません。

2016年9月時点で学認が把握している範囲においてSLOを実装しているIdP/SPは少数であり、対向のIdPもしくはSPが全てSLOに対応していることを期待することはできません。すなわち、仮に自組織の学認参加IdPでSLO対応したとしても、それにより学認の全てのSPからログアウトできるかのような説明は避けてください。

ひとまず、学内サービスと学内IdPのように限られた範囲でSLOを有効化する際の参考として、ご利用いただければと思います。

なお、学認のスタンスとは異なりますが、SLOについてShibboleth開発元では以下のように表現しております。短期的に何かあるというわけではございませんがご留意のほどお願いいたします。詳細はリンク先をご確認ください。
https://wiki.shibboleth.net/confluence/display/IDP4/LogoutConfiguration

> *It has no future.*

以下の手順でメタデータにフロントチャネルのエンドポイントのみを記載していますが、これはユーザにSLOを実行するか否かの選択肢を残すためです。もしかしたら「IdPからもログアウトしたくない」という要望があるかもしれませんが、それは今後の検討課題です。

なお、IdPがSPからのリクエストをバックチャネルを用いて受けることは可能ですが、IdPからSPへバックチャネルリクエストを送る機能は3.xでは実装されていません。IdPv4からの新機能となります（IDP-964）。また、前者を使う際にはIdPのセッションストレージがサーバ側のものを用いていることを確認してください。

ShibbolethにおけるSLO (Single Logout) の設定方法を記載します。

前提

IdP/SPはそれぞれ以下のバージョンであることを前提とします。

- IdP: 3.2.1
- SP : 2.6.0

IdPの設定

メタデータへ<SingleLogoutService>を追加

IdPのメタデータに <IDPSSODescriptor> の子要素として <SingleLogoutService> を追加します。LocationのIdPのホスト名部分は適宜読み替え適切に設定して下さい。IdPが特殊な設定でなければ、ホスト名部分のみ合わせれば問題ありません。

```
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://IdPのホスト名/idp/profile/SAML2
/POST/SLO"
                         xmlns:aslo="urn:oasis:names:tc:SAML:2.0:protocol:ext:async-slo" aslo:supportsAsynchronous="true"/>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://IdPのホスト名/idp/profile
/SAML2/Redirect/SLO"
                         xmlns:aslo="urn:oasis:names:tc:SAML:2.0:protocol:ext:async-slo" aslo:supportsAsynchronous="true"/>
        ↑上記4行を追加
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
    <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://IdPのホスト名/idp/profile
/Shibboleth/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://IdPのホスト名/profile/SAML2/POST
/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://IdPのホスト名/idp/profile
/SAML2/Redirect/SSO"/>
  </IDPSSODescriptor>
```

⚠ メタデータ内の要素は並び順が決まっているものがありますので注意してください。特に<IDPSSODescriptor>の子要素については下記の順番となるように<SingleLogoutService>を挿入してください。

- <KeyDescriptor>
- <ArtifactResolutionService>
- <SingleLogoutService>
- <NameIDFormat>
- <SingleSignOnService>

- (ds:Signature)
- md:Extensions
- md:KeyDescriptor
- (md:Organization)
- (md:ContactPerson)
- md:ArtifactResolutionService
- md:SingleLogoutService
- md:ManageNameIDService
- md:NameIDFormat
- md:SingleSignOnService
- md:NameIDMappingService
- md:AssertionIDRequestService
- md:AttributeProfile
- saml:Attribute

idp.propertiesの変更

idp.propertiesの以下の箇所を変更します。

/opt/shibboleth-idp/conf/idp.properties の設定

```
# Configuration of client- and server-side storage plugins
#idp.storage.cleanupInterval = PT10M
idp.storage.htmlLocalStorage = true ← アンコメントして変更

# Set to true to expose more detailed errors in responses to SPs
(省略)
# Track information about SPs logged into
idp.session.trackSPSessions = true ← アンコメントして変更
# Support lookup by SP for SAML logout
idp.session.secondaryServiceIndex = true ← アンコメントして変更
# Length of time to track SP sessions
#idp.session.defaultSPlifetime = PT2H
```

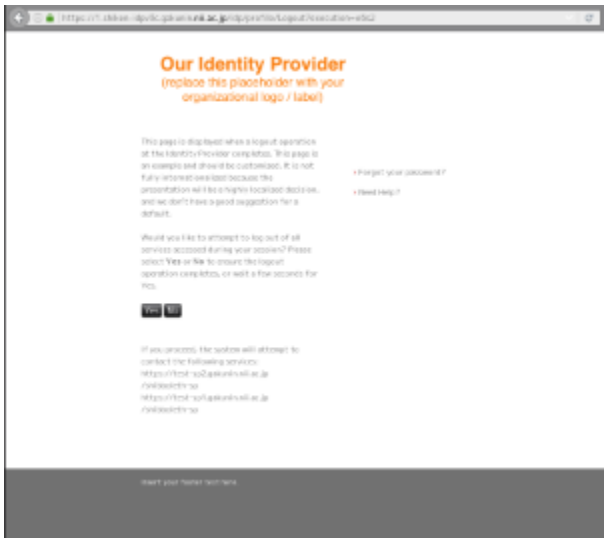
また、SLOとして必須ではありませんが、以下の箇所を変更することでSLO実行時に画面に表示されるSPの情報がURLからメタデータ由来のDisplayNameに変化します。

/opt/shibboleth-idp/conf/idp.properties の変更

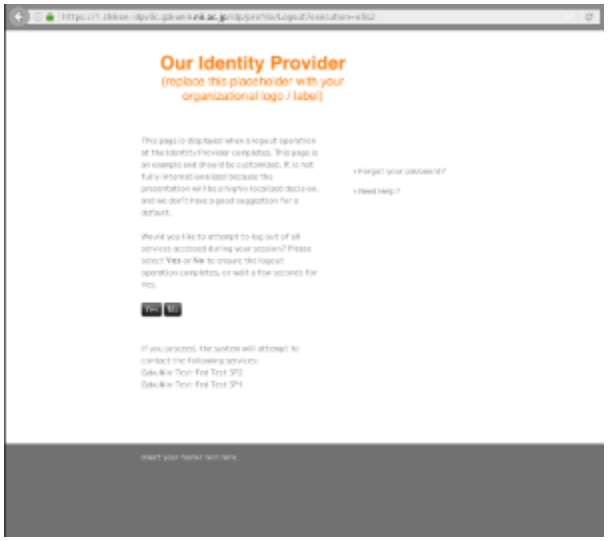
```
# Whether to lookup metadata, etc. for every SP involved in a logout
# for use by user interface logic; adds overhead so off by default.
idp.logout.elaboration = true ← アンコメントして変更
```

idp.logout.elaboration の影響

idp.logout.elaboration=false の場合



idp.logout.elaboration=true の場合



SPの設定

shibboleth2.xmlの設定

SPでのログアウトをトリガーとしてSLOを駆動するためには、shibboleth2.xmlのSessions要素内のLogout要素に以下のように"SAML2"が設定されている必要があります。デフォルト設定ですので、変更していない場合は追加設定は不要ですが、"SAML2"の部分が削除されている場合は追加してください。

```
            <!-- SAML and local-only logout. -->
            <Logout>SAML2 Local</Logout>
```

メタデータへ<SingleLogoutService>を追加

SPのメタデータに <SPSSODescriptor> の子要素として <SingleLogoutService> を追加します。LocationのSPのホスト名部分は適宜読み替え適切に設定して下さい。SPが特殊な設定でなければ、ホスト名部分のみ合わせれば問題ありません。

```
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://SPのホスト名/Shibboleth.sso/SLO/POST"/> ← 追加
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://SPのホスト名/Shibboleth.sso/SLO/Redirect"/> ← 追加
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://SPのホスト名/Shibboleth.sso/SAML2/POST" index="1" isDefault="true"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://SPのホスト名/Shibboleth.sso/SAML2/POST-SimpleSign" index="2"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://SPのホスト名/Shibboleth.sso/SAML2/Artifact" index="3"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post" Location="https://SPのホスト名/Shibboleth.sso/SAML/POST" index="4"/>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01" Location="https://SPのホスト名/Shibboleth.sso/SAML/Artifact" index="5"/>
    <AttributeConsumingService index="1" isDefault="true">
(省略)
  </SPSSODescriptor>
```

⚠ メタデータ内の要素は並び順が決まっているものがありますので注意してください。特に<SPSSODescriptor>の子要素については下記の順番となるように<SingleLogoutService>を挿入してください。

- <KeyDescriptor>
- <SingleLogoutService>
- <NameIDFormat>
- <AssertionConsumerService>
- <AttributeConsumingService>

- (ds:Signature)
- md:Extensions
- md:KeyDescriptor
- (md:Organization)
- (md:ContactPerson)
- md:ArtifactResolutionService
- md:SingleLogoutService
- md:ManageNameIDService
- md:NameIDFormat
- md:AssertionConsumerService
- md:AttributeConsumingService

SLOの実行

SP-initiatedのSLO

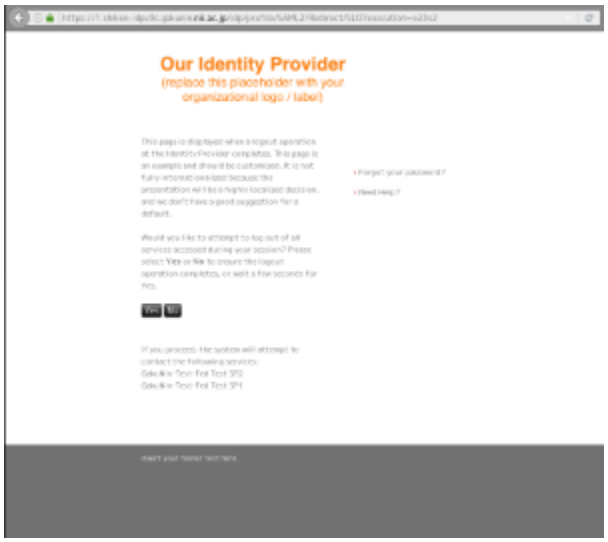
上記設定を行ったSPにおいて、ログインしている状態であれば次のURLにアクセスすることで、接続しているIdP、及びIdPとの間に認証セッションが確立している全てのSPからログアウトしようとします。

```
https://SPのホスト名/Shibboleth.sso/Logout
```

この操作によりIdPからログアウトするためには、前述したIdPのメタデータへの<SingleLogoutService>の追加が必要です。

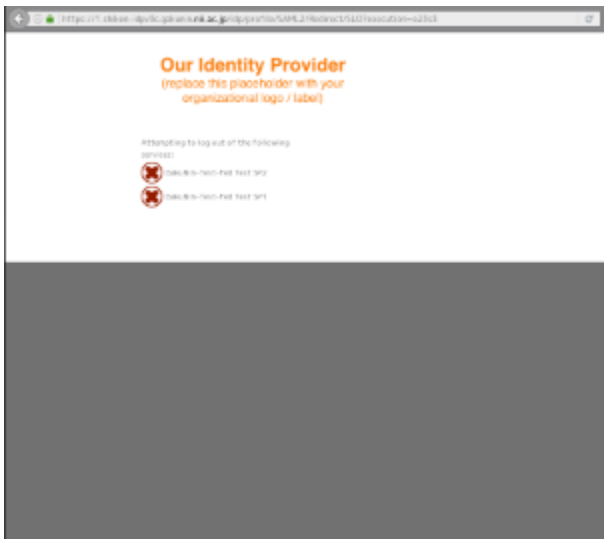
また、他のSPからログアウトするためには、そのSP側で、前述したSPのメタデータへの<SingleLogoutService>の追加が実施されている必要があります。

https://SPのホスト名/Shibboleth.sso/Logout にアクセス後の画面遷移



SP-initiatedのSLO実行時でもIdPの画面に遷移します。
認証セッションが確立しているSPがログアウト対象として一覧に表示されますがアクセスしたSPは表示されません。
メタデータに<SingleLogoutService>が追加されていない(Full SLOに対応していない)SPも表示されますがログアウトは実施されません。

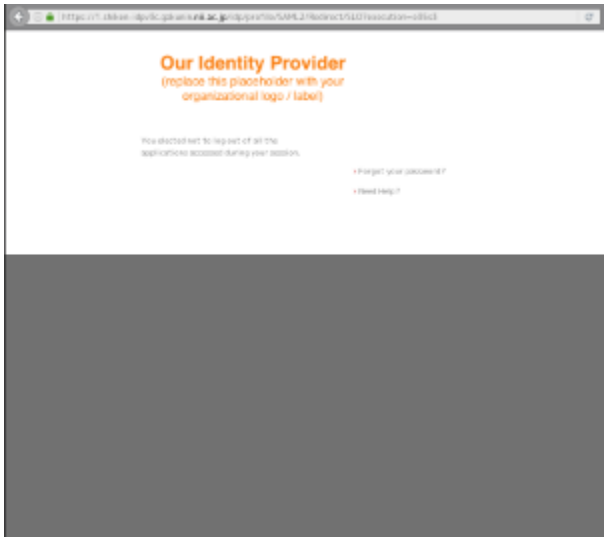
a) 上記画面で Yes を選択、或いは規定の秒数経過後の画面遷移



Full SLOに対応しているSPには  が表示され、対応していないSPには  が表示されます。

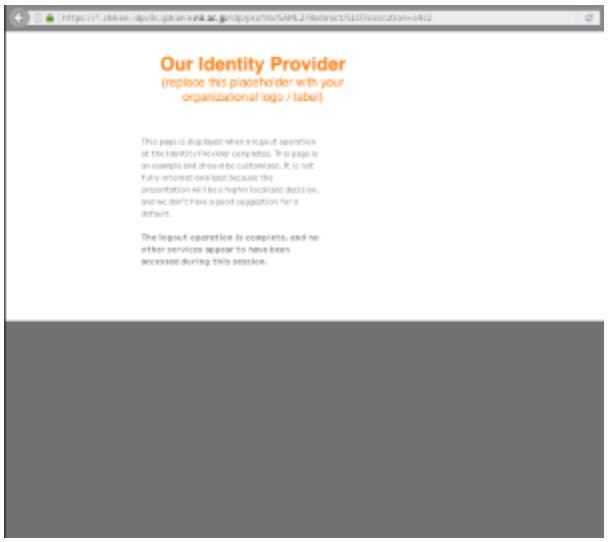
上の画面例で  が表示されているSPは、SP側で保持しているIdPメタデータに<SingleLogoutService>が存在しないためSP-initiatedのSLOが実行できない環境でした。

b) 上記画面で No を選択後の画面遷移



アクセスしたSP及びIdPからはログアウトされますが他のSPからはログアウトされません。

https://SPのホスト名/Shibboleth.sso/Logout にアクセスした際に他のSPにログインしていない場合の画面遷移



アクセスしたSP及びIdPからのログアウトが実施されSLOが完了します。IdPの画面で完了するのは Async SLOの挙動であり、SPの設定で大元のSPの画面への遷移を強制することも可能です。

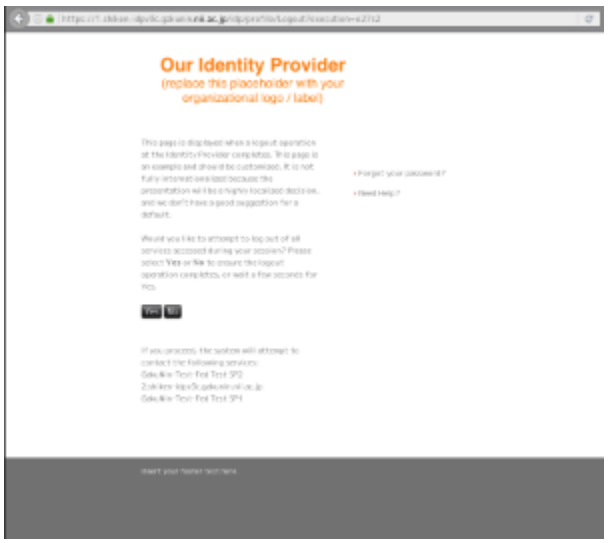
IdP-initiatedのSLO

ログインしているIdPの次のURLにアクセスすることで、アクセスしたIdP、及びIdPとの間に認証セッションが確立している全てのSPからログアウトしようとします。

```
https://IdPのホスト名/idp/profile/Logout
```

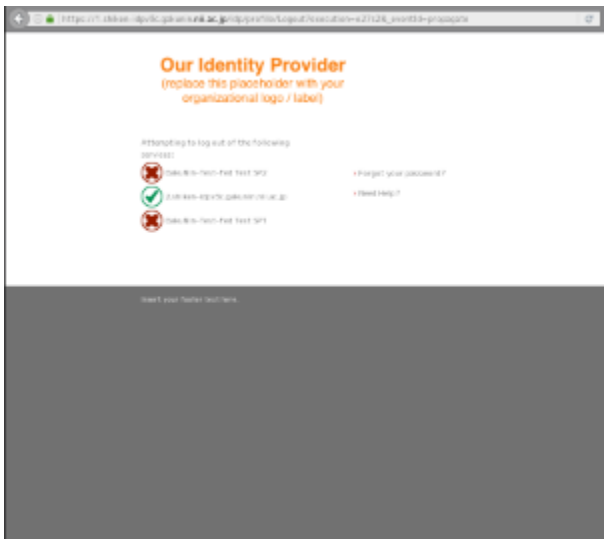
この操作によりSPからログアウトするためには、SP側で、前述の通りSPメタデータへ <SingleLogoutService> が追加されている必要があります。

https://IdPのホスト名/idp/profile/Logout にアクセス後の画面遷移



認証セッションが確立している全てのSPがログアウト対象として一覧に表示されます。
メタデータに<SingleLogoutService>が追加されていない(Full SLOに対応していない)SPも表示されますがログアウトは実施されません。

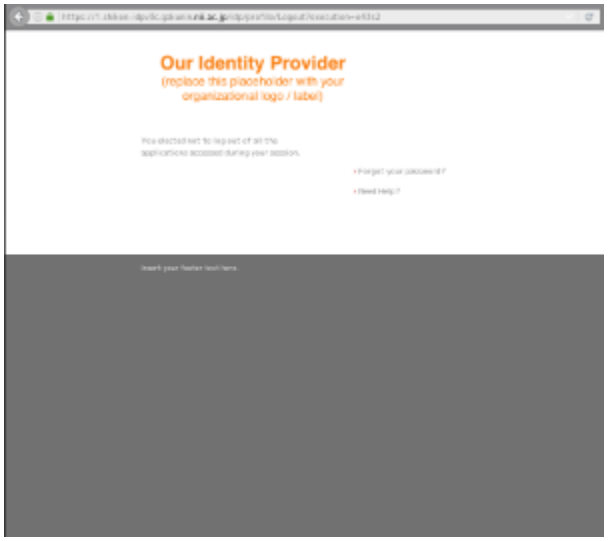
a) 上記画面で Yes を選択、或いは規定の秒数経過後の画面遷移



Full SLOに対応しているSPには  が表示され、対応していないSPには  が表示されます。

上の画面例で  が表示されているSPは、SP側で保持しているIdPメタデータに<SingleLogoutService>が存在しないためFull SLOが実行できない環境でした。

b) 上記画面で No を選択後の画面遷移



IdPからはログアウトされますがSPからはログアウトされません。

SPのSLO対応について、Shibbolethセッションを使ってWebアプリケーションを構成している場合はこの手順で完了ですが、Webアプリケーションで独自のセッションを管理している場合、Shibbolethセッションと連動させるために以下に挙げた改修が必要です。

1. アプリケーションセッション中でもShibbolethセッションがなくなっていればセッションを終了させる。
   （チェックせずに利用している部分があるとそこが抜け穴となりますので、全てのアプリケーションセッション利用でShibbolethセッションの存在をチェックするようご注意ください）
2. Webアプリケーションにおけるログアウトのタイミングで/Shibboleth.sso/Logoutを呼ぶ。
   参考: GakuNinShare - 設定・運用・カスタマイズ - WebアプリケーションのログアウトフローへのShibbolethログアウト処理の挿入
3. （SLOの通知を受けセッションを破棄する）
   参考: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPNotify
   ※これがなくても次回アクセス時に1.の処理でセッションは破棄されるはずです。厳密なセッション管理を行うなら。

参考(SP2): https://wiki.shibboleth.net/confluence/display/SHIB2/SLOWebappAdaptation
参考(SP3): https://wiki.shibboleth.net/confluence/display/SP3/Notify

なお、SLOに対応したIdP/SPを運用している場合、SP証明書が署名用途で用いられる、およびIdP証明書が暗号化用途で用いられる可能性があるため、証明書の更新時にはより一層の注意を払っていただく必要があります。

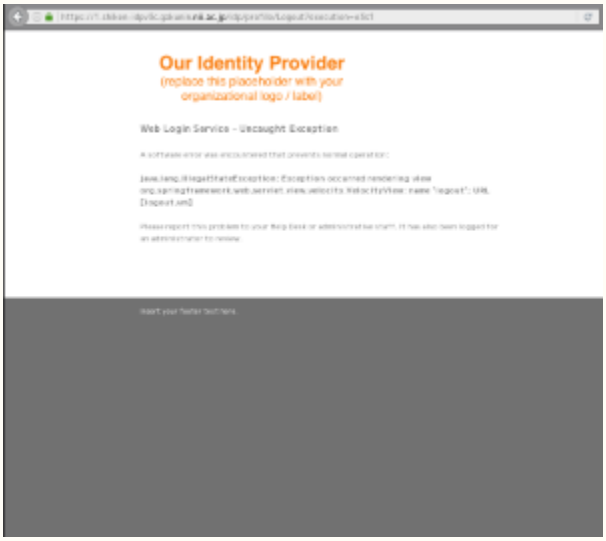
IdP 3.3.1より前のバージョンではIE / EdgeでのSLOに問題があることが分かっています。最新バージョンをお使いください。
参照: IdPv3アップデートに関する情報

IdP 3.2.1時点では上記操作実行後Webブラウザが次のようなエラーメッセージを表示する画面へ遷移し、SPからのログアウトが実施されません。（IdPからはログアウトされています）

本件はIdP 3.3.0で修正されています。

参考: IDP-892、IDP-956

--



参考:

- Shibboleth Wiki: LogoutConfiguration
- SAML v2.0 Metadata Guide
- Shibboleth Wiki: SecurityConfiguration
- Shibboleth Wiki: SLOIssues
- SWITCHaai: Enable an SP for Single Logout with the SWITCH edu-ID IdP