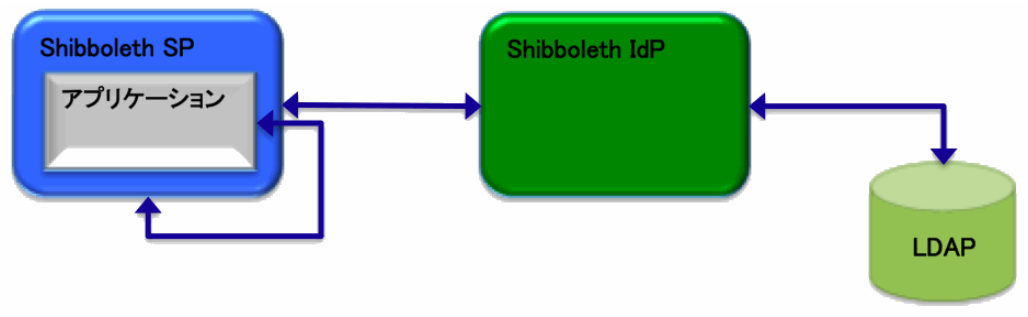
特定のリソースをShibboleth認証されたユーザにのみ見せる

特定のリソースをShibboleth認証されたユーザにのみ見せる

Shibbolethの導入のみで実現するパターンであり、特別にユーザ管理機能の構築は必要としません。

概要図



Shibboleth認証の対象となるリソースにアクセスするとShibboleth SPからShibboleth IdPの認証画面にリダイレクトされるため、Shibboleth SP側で認証の実装や属性情報を持つ必要はありません。

対象となるアプリケーションをShibboleth SPの配下に配備することでアプリケーションは、Shibbolethに保護されます。

Shibboleth SP側の設定

Apacheの設定ファイルhttpd.conf、.htaccessあるいは、shib.conf（rpmでインストールした場合のみ）のいずれかにLocationを追加することで行います。

※/etc/shibboleth/shibboleth2.xmlファイルのRequestMapper要素にtype="Native"が設定されている場合に有効です。

設定例） 「App」をShibboleth化するための設定例

```
<Location /App>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession true
  Require shib-session
</Location>
```

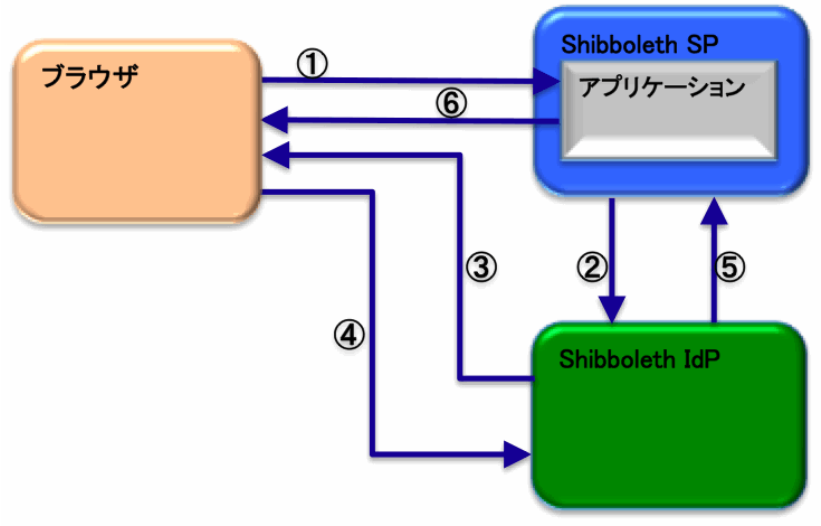
この設定ではシボレス認証により認証された全てのユーザがアプリケーションを実行する権限があるものとみなされます（Require shib-session）。
属性によりさらに制限したい場合は以下のようなRequire宣言で Require shib-session を置き換えてください。
例（学生に限定）：

```
Require shib-attr unscoped-affiliation student
```

もちろん、IdPが当該属性を送信している場合のみ有効です。（IdPが属性を送信していない場合は属性がない（=権限がない）とみなされます）

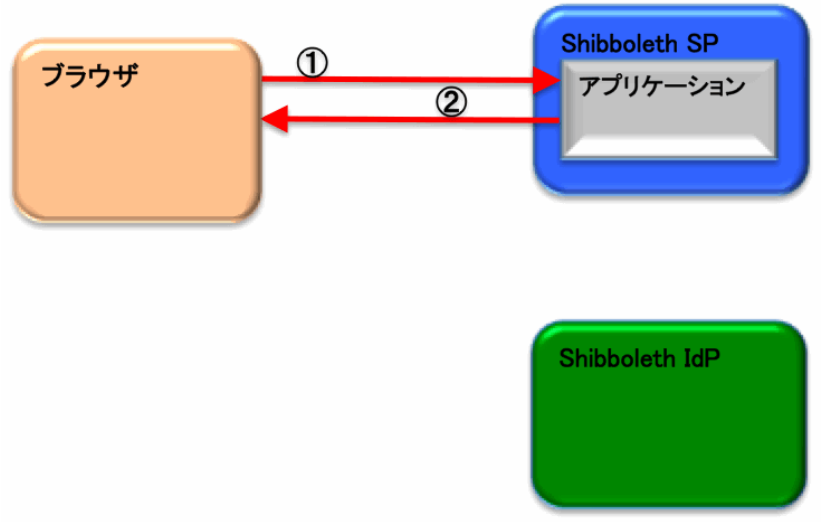
この設定により、App下の全リソースは、Shibbolethにより認証されます。

処理イメージ図：初回起動時



①ブラウザからアプリケーションのURLをアクセスします。
②Shibbolethのセッション情報がないため、Shibboleth SPからShibboleth IdPの認証画面にリダイレクトされます。
③ブラウザに認証画面を表示します。
④認証画面にユーザ／パスワードを入力し、Shibboleth IdPで認証を行います。
⑤認証結果をShibboleth SPに返します。
⑥認証が成功した場合は、アプリケーションを実行し、結果をブラウザに返します。
　ブラウザには、Shibbolethのセッション情報を含むcookieが返されます。
　認証が失敗した場合は、認証失敗画面を表示します。

処理イメージ図：SSO認証セッションが存在する場合



①ブラウザからアプリケーションのURLをアクセスします。
②既にShibboleth認証されているユーザからのアクセスであるため、アプリケーションを実行し、
　結果をブラウザに返します。