

AES-GCMテストIdPシステム利用マニュアル

AES-GCMテストIdPについて

AES-GCMテストIdPは、テストフェデレーション参加SPに対してShibboleth IdP V4にてデフォルトとなったAES-GCM暗号アルゴリズムで暗号化したSAMLアサーションを送信するテストIdPです。

また、AES-GCMテストIdPには**TiqrShibプラグイン**がインストールされており、TiqrShib認証が利用できます。

利用方法

AES-GCMテストIdPを利用するには事前にテストフェデレーションに参加する必要があります。テストフェデレーションの参加方法は[テストフェデレーション参加手続き](#)を参照してください。

1. 最初に管理しているSPにアクセスして、ログインを開始してください。

図1: SPの画面



2. DSでIdPとして「GakuNin テスト IdP 2 (AES-GCM)」を選択します。

図2: DSの画面



3. IdPのログイン画面でユーザー名とパスワードを入力してください。

図3: IdPのログイン画面



AES-GCMテストIdPでは下記アカウントが利用できます。

ユーザ名	パスワード
test001	test001
test002	test002
test003	test003

- 送信属性同意画面に遷移しますので、属性送信に同意してください。

図4: IdPの送信属性同意画面



- SPがAES-GCM暗号アルゴリズムをサポートしていれば、SPのログインに成功します。

図5: ログイン後のSP画面



TiqrShibの利用方法

- SPのApache HTTP Server設定に、認証をTiqrShibに制限したいLocationに下記の設定を追加してください(設定例では/shibtqir_protected)。

```
<Location /shibtqir_protected>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  ShibRequestSetting authContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
  Require valid-user
</Location>
```

2. AES-GCMテストIdPの <https://test-idp2.gakunin.nii.ac.jp/tiqr/shib/enroll> にアクセスして使用するスマートフォンを登録してください。登録方法はTiqrShibの[How To UseのEnrollment Process](#)を参照してください。

図6: TiqrShibの登録画面



3. SPのTiqrShib認証に制限したLocationにアクセスしてログインを開始してください。
4. DSからIdPとして「GakuNin テスト IdP 2 (AES-GCM)」を選択します。
5. TiqrShibでのログイン画面に遷移しますので、登録したスマートフォンでログインしてください。ログイン方法はTiqrShibの[How To UseのLogin Process](#)を参照してください。

図7: TiqrShibのログイン画面



TiqrShibの詳細は、[TiqrShibプラグイン](#)を参照してください。