独自属性の送信/受信方法

1. はじめに

本メニューでは、IdPとSPを共にカスタマイズします。
また、ユーザ情報（LDAP）も操作します。
内容としては、独自の属性をSPに送信し、SPのWebアプリケーション側で受信した属性値を使った制御を行います。
実習セミナーでは、属性受信の確認ページをWebアプリケーションとし、独自に追加したshadowExpire属性で制御します。
（有効期限を使った制御）

---

2. 実習セミナーでは

「3. 手順書」に記載の手順書に沿って作業を進めてください。ただし、参照する手順書の中では「displayName」を使って説明していますが、本実習セミナーでは「shadowExpire」に置き換えて実施します。以下の項目についてはこちらで読み替えてください。

＜IdP側の設定＞

手順書内の実施する作業としては、LDAPのユーザ情報に属性を追加する「属性の追加方法」と
IdPの送信属性に追加する「属性のリリース方法」となります。

・属性の追加方法（shadowExpire）

実習セミナーでは、以下のldifファイルを作成して、ユーザ情報に属性を追加してください。

以下は、test001ユーザに3日前の日付、test002ユーザに3日後の日付を設定するldifファイルです。
※参考までに本日() は、となります。

```
dn: uid=test001,ou=Test Unit1,o=test_o,dc=ac,c=JP
changetype: modify
add: objectClass
objectClass: shadowAccount
-
add: shadowExpire
shadowExpire:

#              ↑1970年1月1日からの日数（）


dn: uid=test002,ou=Test Unit2,o=test_o,dc=ac,c=JP
changetype: modify
add: objectClass
objectClass: shadowAccount
-
add: shadowExpire
shadowExpire:

#              ↑1970年1月1日からの日数（）
```

・独自属性としてshadowExpireを使用

「shadowExpire」のoidは、以下のように確認してください。（今回はファイルより確認）
・/etc/openldap/slapd.d/cn¥=config/cn¥=schema配下にcn={4}nis.ldifがあるか確認します。（数字部分は異なる可能性があります）
・cn={4}nis.ldif に以下のような定義が設定されていることを確認してください。

```
Scheme :  nis.schema
objectClass :  shadowAccount

olcAttributeTypes: {8}( 1.3.6.1.1.1.1.10 NAME 'shadowExpire' EQUALITY intege

rMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

もし当該ファイルが見つからなければ、まず下記コマンドでNISスキーマをインストールしてください。そしてもう一度ファイルを確認してください。

```
# ldapadd -Y EXTERNAL -H ldapi:// -f /etc/openldap/schema/nis.ldif
```

＜SP側の設定＞

手順書内で実施する作業としては、IdPより受信した属性値を参照できるように「shadowExpire」の
マッピング設定を行います。（/etc/shibboleth/attribute-map.xml）
また以下の手順に従って、作業を進めてください。（サンプルコードを使用する）

・属性受信の確認ページのサンプルコード

SP：/var/www/html/secure/index.phpに2つのPHP文を追加してください。

```
<html>
<head>
↓ヘッダに下のphp部分を追加する
<?php
header("Expires: Dec, 20 Jul 2010 05:00:00 GMT");
header("Last-Modified: " . gmdate("D, d M Y H:i:s") . " GMT");
header("Cache-Control: no-store, no-cache, must-revalidate");
header("Cache-Control: post-check=0, pre-check=0", false);
header("Pragma: no-cache");
?>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>属性受信の確認ページ</title>
<style type="text/css"> body {

（省略）
```

```
（省略）

  <div id="maincenter">
  <strong id="logintitle">属性受信の確認ページ</strong><br>
<?php
//error_reporting(E_ERROR | E_WARNING | E_PARSE);
error_reporting(E_ALL ^ E_NOTICE);
print "      <b id='loginname'>あなたのIdPは、&lt;". htmlspecialchars($_SERVER['Shib-Identity-Provider']). "&gt;です。</strong>";
?>
    <br>
  </div>
<?php
$nowt = time();
$strNow = date("Y年m月d日", $nowt);
if (!empty($_SERVER['shadowExpire'])) {
    $expt = intval($_SERVER['shadowExpire'])*60*60*24;
    $strExp = date("Y年m月d日", $expt);
    $zant = $expt - $nowt;
    $zand = floor($zant/60/60/24);
    print "<div style=¥"position: relative; top: 85px;¥">";
    print "<h1>現在：$strNow ,";
    print "期限：$strExp ,";
    print "残日数：".intval($zand+2)."日間</h1>";
    print "</div>";
    if ($zand < 0) {
        $errmsg = "有効期限を".intval(($zand+1)*-1)."日過ぎています。";
        header("HTTP/1.1 301 Moved Permanently");
        header("Location: https://ex-sp-testXX.gakunin.nii.ac.jp/secure/error.php?exp=".$strExp."&errmsg=".$errmsg);
                                  //↑各自SPのホスト名
        exit();
    }
}
?>
↑mainテーブルの前に上のphp部分を追加する
  <table id="main" cellspacing="0">
    <colgroup>
      <col width="280">
      <col width="420" valign="top">
    </colgroup>
    <thead>
    <tr>
      <th scope="col" class="chart">属性</th>
      <th scope="col" class="chart">属性値</th>
    </tr>

（省略）
```

※端末のサイズによっては表記がずれる可能性がございます。画面を広くしてご覧ください。

・有効期限切れエラーページのサンプルコード

SP：/var/www/html/secure/error.phpを作成します。
※有効期限が切れたユーザでアクセスすると、このエラーページが表示されます。

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>有効期限切れエラー</title>
</head>
<body>
<h1>有効期限切れエラー</h1>
<br>
有効期限　：<?php echo htmlspecialchars($_GET[exp]) ?><br>
メッセージ：<?php echo htmlspecialchars($_GET[errmsg]) ?><br>
</body>
</html>
```

3. 手順書

下記の手順書に沿って作業を行います。
※上述の通りshadowExpire属性を対象とし、各種設定値に置き換える事を忘れないようにしてください。

- IdP：独自属性送信設定
  「属性の追加方法」および「属性のリリース方法」参照
- SP：独自属性受信設定

4. 動作確認

① 設定後、IdPはJetty、SPはApacheやshibdの再起動を行ってない場合は行なってください。

```
・IdP
 systemctl restart jetty

・SP
 systemctl restart httpd
 systemctl restart shibd
```

② 各自が使用するSPの接続確認用ページにアクセスします。

```
例）1番を割り振られた場合 https://ex-sp-test01.gakunin.nii.ac.jp/
```

③ ログインボタンをクリックします。

④ DSの所属機関の選択画面が表示されるので、各自が使用するIdPを選択します。

⑤ IdPのログイン画面が表示されるので、Username/Passwordを入力して認証を行います。
※test001：有効期限切れ、test002：有効期限内、test003：有効期限なし
※本実習のアクセス権限課題を設定している場合、test002以外での動作確認ができなくなっている可能性があります。一時的にrelying-party.xmlの設定を解除するか、当該SPをアクセス制限の対象外にしてください。設定変更したらjettyを再起動してください。

⑥ ユーザ情報（有効期限）で正しく制御されることを確認します。
test001の場合：有効期限切れエラーのページが表示されます。
test002の場合：属性受信の確認ページが表示され、有効期限や残り日数などが表示されます。
test003の場合：通常の属性受信の確認ページが表示されます。