演習 6 - OAuthセキュリティーの実装

この演習では、OAuthセキュリティーを実装してテストする方法を確認します。

演習 6 - 目的

この演習では、以下の内容を理解できます。

- ネイティブOAuthプロバイダーの定義方法
- OAuthで保護されるAPIのセキュリティー定義方法
- OAuthセキュリティーの定義方法

6.1 - ネイティブOAuthプロバイダーの作成

1. API Managerにログインしていない場合には、ログインします。

2. まず、Native OAuthプロバイダーでの認証を行うURLを `認証ユーザー・レジストリー` として設定します。左のメニューから `リソース` を選択します。

3. `ユーザー・レジストリー` の画面で、 `作成` をクリックします。

4. `認証 URL ユーザー・レジストリー` をクリックします。

5. 以下を入力して `保存` をクリックして保存します。

項目	入力値	備考
タイトル	AuthURL	認証URL名前
Display Name	AuthURL	表示名
URL	https://httpbin.org/basic-auth/user/pass	認証サービスのURL
TLSクライアント・プロファイル	TLSプロファイルなし	

6. 次に、 `OAuthプロバイダー` を設定します。 `OAuth プロバイダー` を選択し、 `追加` をクリックして `ネイティブ OAuth プロバイダー` を選択します。

7. `タイトル` に `oauthprovider` と入力して `次へ` をクリックします。

1. `サポートされている権限付与タイプ` フィールドで、 `リソース所有者 - パスワード` にチェックを入れ、 `次へ` をクリックします。

2. `スコープ` セクションで、上部の `名前` フィールドに `details` と入力し、 `説明` フィールドに `Branch details` と入力し、 `次へ` をクリックします。

3. `ID抽出` に `基本認証` が選択され、 `認証` に `AuthURL` が選択され、 `許可 設定が 認証済み` に設定されていることを確認して、 `次へ` をクリックします。

> *前の手順で作成した、 `認証URLユーザー・レジストリー` をOAuthプロバイダーの認証に利用するように設定しています。*

4. サマリーページが表示されるので、下までスクロールして、 `終了` をクリックします。

5. `デバッグ応答ヘッダーの有効化` にチェックを入れて、 `保存` をクリックします。

6. このOAuthプロバイダーを利用するに、カタログで有効化します。API Managerの左のメニューから `管理` を選択します。

7. `Sandbox` を選択します。

8. 左側のカタログの管理メニューから `設定` を選択します。

9. `OAuthプロバイダー` を選択し、 `編集` をクリックします。

10. 利用可能なOAuthプロバイダーが表示されるので、チェックを入れて `保存` をクリックします。

    ![](/lab-guide/img/lab6/add-oauth-provider.png

11. 左のメニューの `APIエンドポイント` をクリックして `ゲートウェイURL` をコピーしておきます。後続の手順で利用します。

    左上のをクリックして、管理画面に戻ります。

6.2 - APIへのOAuthセキュリティーの追加

次に既存のAPIにOAuthセキュリティーを追加します。

1. これまでの演習で作成した、FindBranchにセキュリティー定義を追加します。左のメニューから `開発` を選択し、開発メニューに進みます。

2. `FindBranch` を選択します。

3. `セキュリティー定義` をクリックして、 `追加` をクリックします。

4. 以下のように入力し、 `保存` をクリックします。

項目	入力値	備考
名前	oauth	
タイプ	OAuth2	
OAuth プロバイダー	oauthprovider	
フロー	Resource Owner	

5. 次に `セキュリティー` をクリックし、定義した `oauth` にチェックを入れ、スコープ `details` にチェックを入れて、 `保存` をクリックします。

    以上でAPIへのOAuthセキュリティー定義の追加が完了しました。

6.3 - 製品の再公開

1. APIのテストを行ってみましょう。左のメニューから `開発` を選択し、開発メニューに進みます。

2. `FindBranch` APIを選択します。

3. 上部から `アセンブル` をクリックして、アセンブル画面に移動します。

4. 画面上のボタンをクリックしてテストツールを表示します。

5. `製品の再公開` をクリックします。

6.4 - テスト用のアプリケーション作成と利用登録

1. テスト用のアプリケーションをAPI Manager画面から作成します。左のメニューから、 管理 メニューを右クリックし、新しいタブでリンクを開きます。

1. ログイン画面が表示されたら、再度ログインします。左のメニューから 管理 メニューを選択します。

2. `Sandbox` を選択します。

3. 左側のカタログの管理メニューから アプリケーション を選択します。

4. アプリケーションを新規に作成します。 `追加` ボタンをクリックし、 `作成` を選択します。

5. 以下のように入力して、 `作成` をクリックします。

項目	入力値	備考
タイトル	oauthapp	
OAuth リダイレクト URL (オプション)	https://example.com	
コンシューマー組織	`Sandbox Test Organization` にチェック	

6. アプリケーションの資格情報が表示されるので、 `クライアント ID` 、 `クライアント・シークレット` をそれぞれコピーして、保存しておきます。後続の演習で利用します。 `OK` をクリックします。

7. 作成したテスト用アプリケーションで、製品プランにサブスクライブします。 `oauthapp` の右のメニューをクリックして、 `サブスクリプションの作成` を選択します。

8. `FindBranch auto product:2.0.0/Default Plan` にチェックを入れて `作成` をクリックします。

1. 演習5で登録したアプリケーションをテストする製品に利用登録(サブスクライブ)する必要があります。左のメニューから、 `管理` メニューを右クリックし、新しいタブでリンクを開きます。

1. ログイン画面が表示されたら、再度ログインします。左のメニューから `管理` メニューを選択します。

2. `Sandbox` を選択します。

3. 左側のカタログの管理メニューから `アプリケーション` を選択します。

```
![](/lab-guide/img/lab6/sandbox-application.png)
```

4. このカタログで利用可能なアプリケーションの一覧が表示されます。 `SampleApp` の右のメニューをクリックして、 `サブスクリプションの作成` を選択します。

5. `FindBranch auto product:2.0.0/Default Plan` にチェックを入れて `作成` をクリックします。

6. ここで、先ほどのAPIのテスト画面のタブに戻ります。操作フィールドで `get /details` を選択し、 `clientId` 、 `clientSecret` フィールドに、演習5でコピーしておいた `API`キー と 秘密鍵(シークレット) を入力します。 `ユーザー名` フィールドに user と入力し、 `パスワード` フィールドに pass と入力します。

項目	入力値	備考
操作	get /details	
clientId	前の演習でコピーした `API`キー	

clientSecret	前の演習でコピーした 秘密鍵（シークレット）	
ユーザー名	user	
パスワード	pass	

7. OAuth トークンを取得します。ここでは、cURL で以下のコマンドを使用してトークンを取得します。

<APIエンドポイント>/oauthprovider/oauth2/token

curl -k <APIエンドポイント>/oauthprovider/oauth2/token -d "grant_type=password&scope=details&username=user&password=pass&client_id=<APIキー>&client_secret=<秘密鍵(シークレット)>"

curl -k https://apicgw.mycluster-843612-98d9bd8ec23489ff9abfa33c8924325c-0001.jp-tok.containers.appdomain.cloud/potorg-101/sandbox/oauthprovider/oauth2/token -d "grant_type=password&scope=details&username=user&password=pass&client_id=dc3b629792c46f2737f905292ced177a&client_secret=8eb16496599d38e8eb5

```
![](/lab-guide/img/lab6/.png)
```

1. a
2. a
3. a
4. a
5. a
6. a
7. a
8. a
9. a

ここで、再公開された API のテストに戻る必要があります。現在開いているブラウザー・タブを閉じて、再公開した API のテストに戻ります。

「操作」フィールドで、「get /details」を選択します。

「clientId」フィールドに、以前に作成したクライアント ID を入力します。「clientSecret」フィールドに、以前に作成したクライアント・シークレットを入力します。

「ユーザー名」フィールドに user と入力します。「パスワード」フィールドに pass と入力します。

OAuth トークンを取得します。ここでは、cURL で以下のコマンドを使用してトークンを取得します。

curl -k https://gateway_url/org_name/sandbox/mainprovideroa/oauth2/token -d "grant_type=password&scope=details&username=user&password=pass&client_id=app_client_id&client_secret=app_client_secret"

「explorer_access_token」フィールドにアクセス・トークンを入力するか貼り付けます。以下にトークンの例を示します。

AAIgMzU4MjRmMjY0NmY3OTllZjRjM2Y3OWU1ZDQwZGYwYWOxkwNYTnlxWaHu8Htf1OUAQUEGl3TLJVHayXjPJE5Rxd7clNdBEYRAEkuHIWX8hR2KF4AA9_SuOCNx

「呼び出し」をクリックします。URL が組み込まれている黄色いエラー・ボックスが表示される場合があります。この URL をクリックして、ブラウザー証明書エラーをオーバーライドします。

呼び出し」を再度クリックします。応答にはブランチ・データが含まれています。

以上で、演習6は終了です。

続いて、 演習 7 - に進んでください。