OpenAM 14 ID 認証モジュール 利用手順書

OSSTech 株式会社

更新日 2022 年 7 月 14 日
リビジョン 1.3

目次

1 はじめに

本文書は、OSSTech 版 OpenAM14 に含まれる ID 認証モジュールの利用手順書です。

1.1 機能概要

ID 認証モジュールの機能について説明します。

従来の認証方法では、ユーザーを特定するためにデータストア認証モジュールや OpenLDAP 認証モジュールのような ID とパスワードを用いる認証が必要でした。 そのため、ID とワンタイムパスワードを組み合わせた認証連鎖はできませんでした。

本モジュールは ID のみを用いてユーザーを特定するため、上記のような認証連鎖も実現できるようになりました。更に認証連鎖分岐モジュールと組み合わせることによって柔軟な認証を実現可能です。

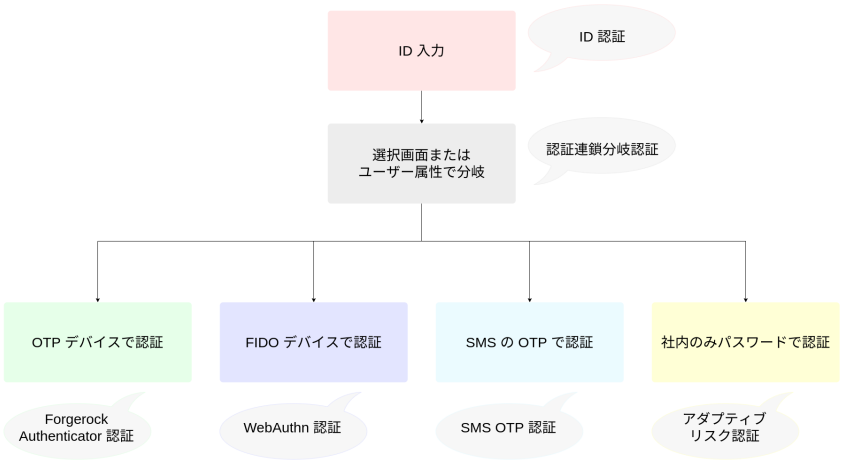

図 1　認証連鎖分岐モジュールとの組み合わせ例

2 認証モジュールと認証連鎖の設定

ここでは、ID 認証モジュールを利用するための設定方法を説明します。事前準備として以下の設定が完了しているものとします。

- OpenAM の初期設定
- ID 認証モジュールと組み合わせて利用する認証モジュールの設定

2.1 認証モジュールの追加

1. OpenAM にログイン後、対象のレルムを選択します。
2.「認証」→「モジュール」に移動し、「モジュールの追加」を押下します。
3.「名前」に認証モジュール名 (ここでは ID) を入力し、「種類」のドロップダウンリストから ID を選択します。

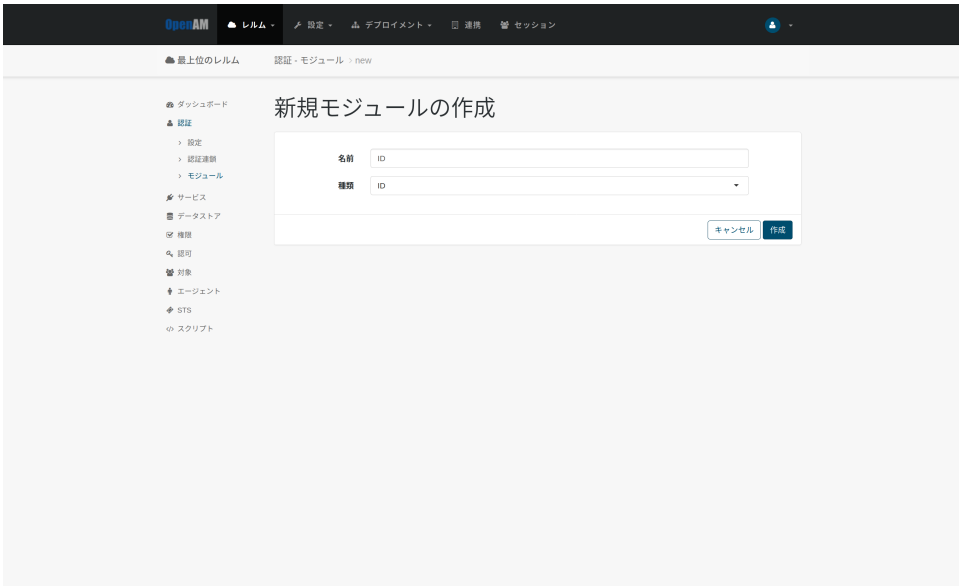

図 2　認証モジュールの作成

4.「作成」を押下し、認証モジュールの設定画面に移動します。

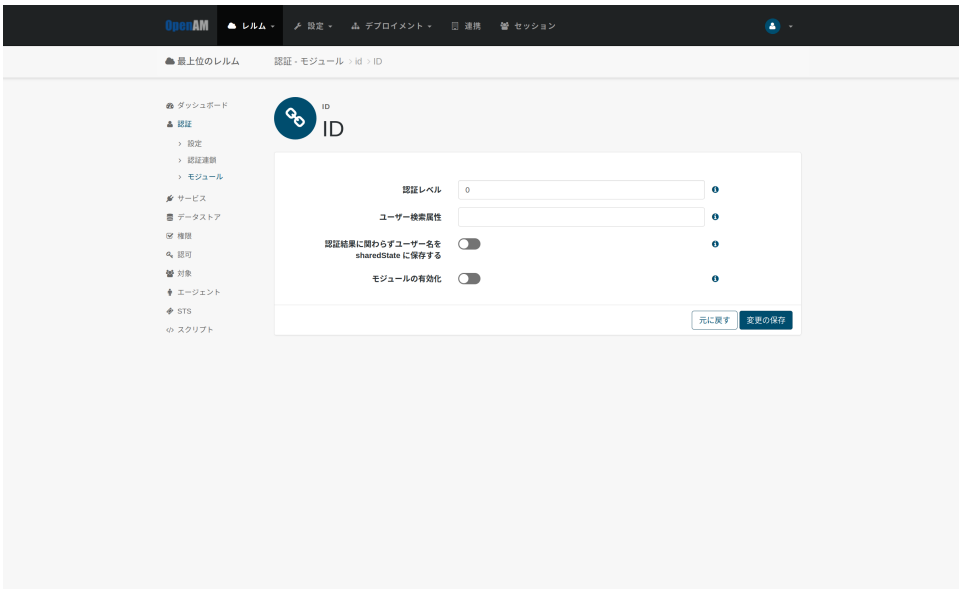

図 3　認証モジュールの設定

5. 各項目の設定をし、「変更の保存」を押下します。
   各項目の詳細は下記を参照してください。

項目名	設定内容
認証レベル	認証成功時にセットされる認証レベル
ユーザー検索属性	ユーザー検索に使用する属性名
認証結果に関わらずユーザー名を sharedState に保存する	認証に失敗してもユーザー名を sharedState に保存するかどうか
モジュールの有効化	モジュールを利用可能にするかどうか
エラーメッセージコード	ユーザーの特定に失敗したときに表示されるエラーメッセージに対応するコード 設定方法は「認証失敗時のエラーメッセージ」へ

以下が設定例です。

【項目名】	【設定例】
認証レベル	0

【項目名】	【設定例】
ユーザー検索属性	`uid　mail`
認証結果に関わらずユーザー名を sharedState に保存する	有効
モジュールの有効化	有効
エラーメッセージコード	（空欄）

2.2 認証連鎖の追加

1. OpenAM にログイン後、対象のレルムを選択します。
2. 「認証」→「認証連鎖」に移動し、「認証連鎖の追加」を押下します。
3. 「名前」に任意の認証連鎖名 (ここでは `idService`) を入力し、「作成」を押下します。

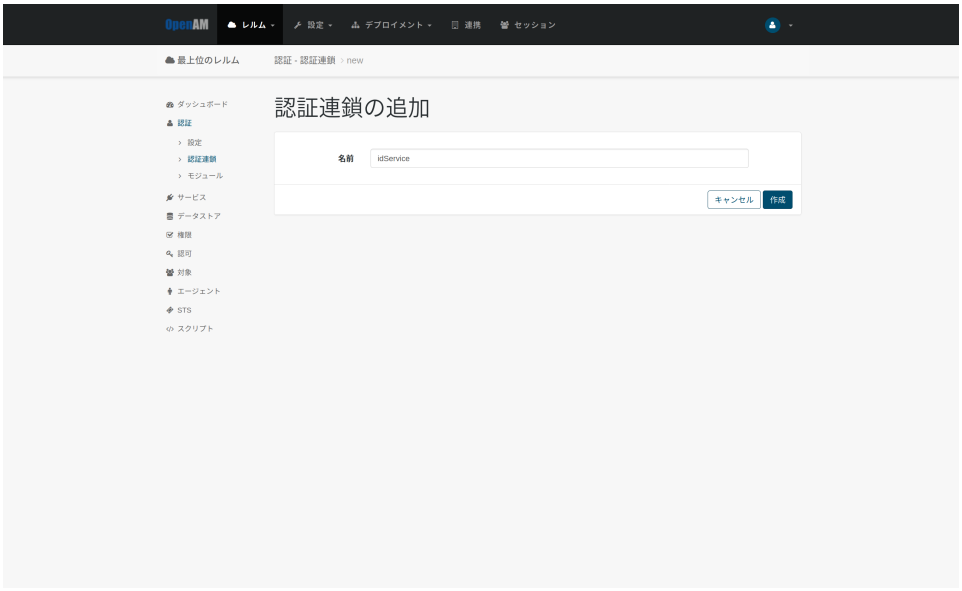

図 4　認証連鎖の追加

4. 「認証モジュールの追加」を押下し、「モジュールの選択」のドロップダウンリストから ID 認証モジュール (ここでは `ID`) を選択し、「基準の選択」のドロップダウンリストから `Required` または `Requisite` を選択して「OK」を押下します。「基準の選択」では、後続の認証モジュールがデータストア認証モジュールや OpenLDAP 認証モジュールなどの存在しない ID を渡しても問題のない認証モジュールの場合は `Required` を選択し、ForgeRock Authenticator (OATH) などのワンタイムパスワード

系の認証モジュールでは Requisite を選択してください。ここでは後続の認証モジュールがデータストア認証モジュールのため、Required を選択します。

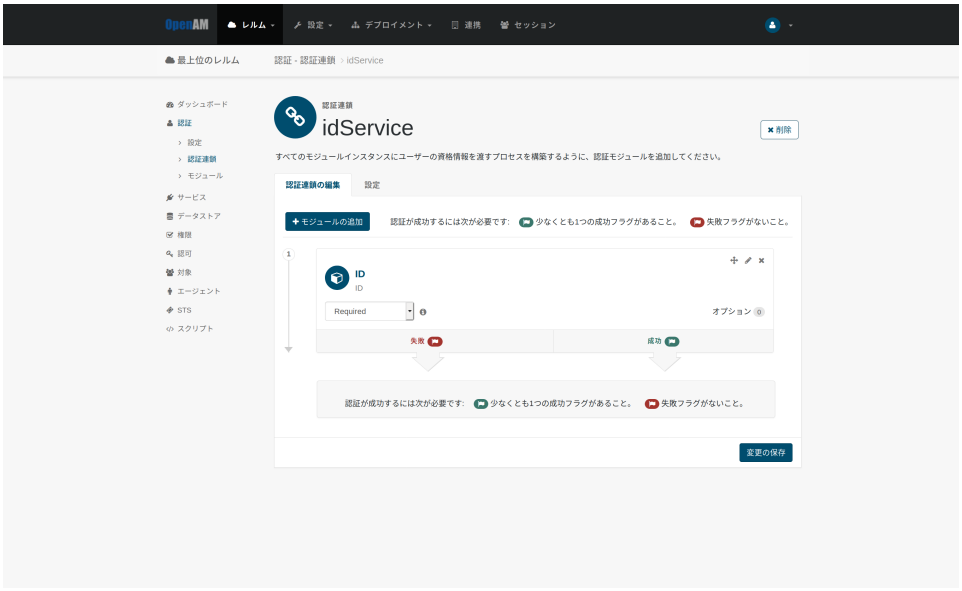

図 5　ID 認証モジュールの追加

5. 4. と同様にして、設定済みの ID 認証モジュールと組み合わせて利用する認証モジュール (ここでは DataStore) を選択し、「基準の選択」で Required を選択します。
6. ID 認証モジュールと組み合わせて利用する認証モジュールが ‘データストア’ または ‘OpenLDAP’ の場合にのみ 5. の設定欄の下にある「オプション」の「キー」に iplanet-am-auth-shared-state-enabled 、「値」に true を入力し、「+」を押下した後に「OK」を押下します。そうでない場合には、4. の設定後「OK」を押下します。

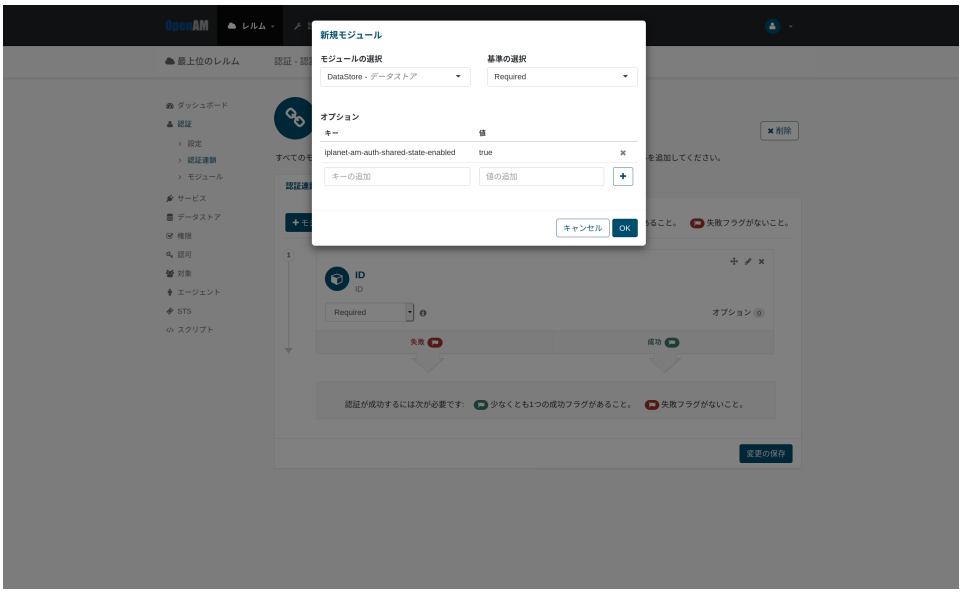

図 6　DataStore 認証モジュールの設定

7. 6. でオプションを設定した場合は、その認証モジュールのオプションの数が 1 になっていることを確認します。「変更の保存」を押下します。

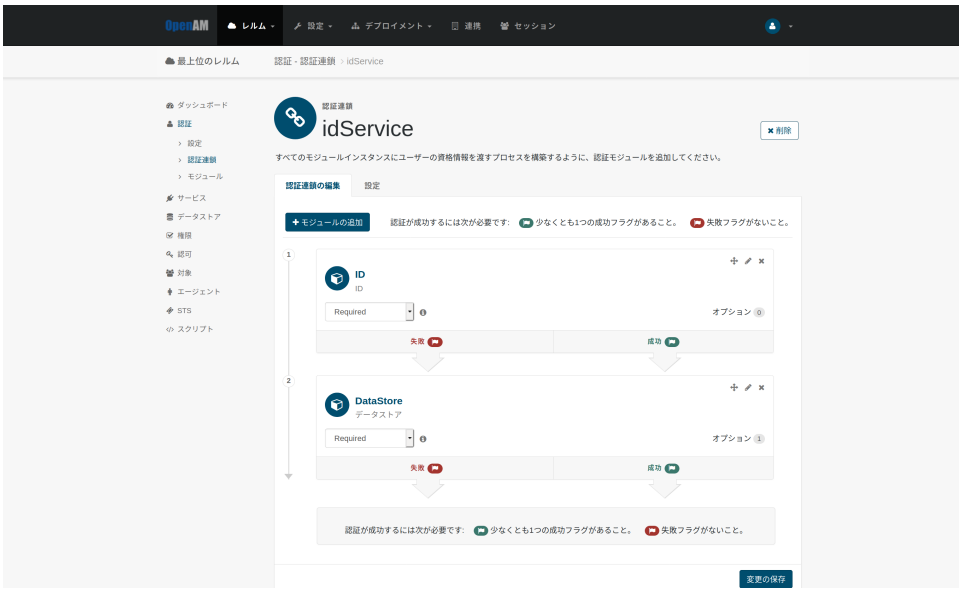

図 7　認証連鎖の保存

8.「認証」→「設定」に移動し、「組織認証設定」のドロップダウンリストから作成した認証連鎖 (ここでは `idService`) を選択し、「変更の保存」を押下します。

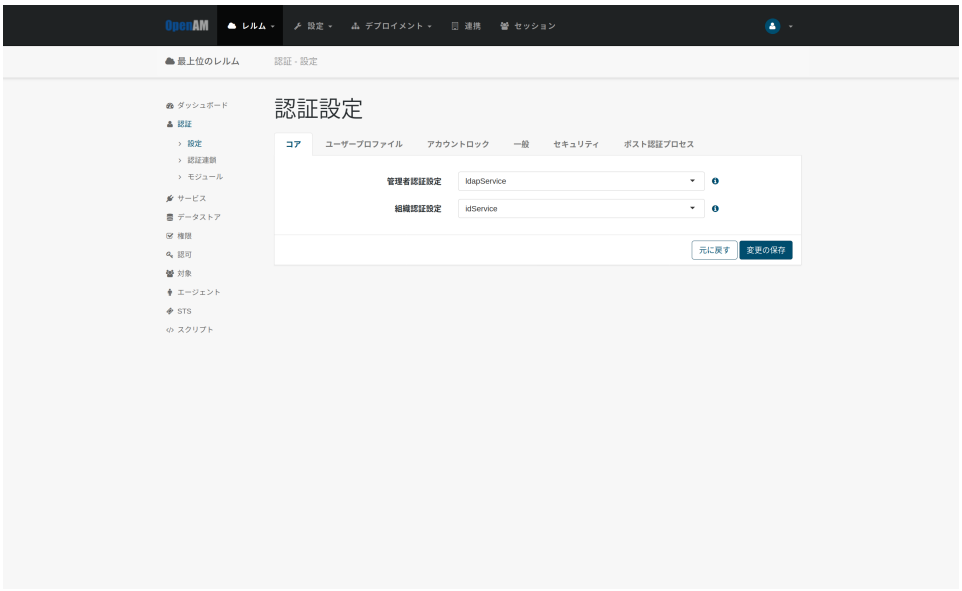
OpenAM
レルム
設定
デプロイメント
連携
セッション
最上位のレルム
認証 - 設定
ダッシュボード
認証
設定
認証連鎖
モジュール
サービス
データストア
権限
認可
対象
エージェント
STS
スクリプト
認証設定
コア
ユーザープロファイル
アカウントロック
一般
セキュリティ
ポスト認証プロセス
管理者認証設定
ldapService
組織認証設定
idService
元に戻す
変更の保存

図 8　認証設定

3 認証時の操作

ここでは「認証連鎖の追加」の例のように設定した場合のユーザーによる認証時の操作について説明します。

1. OpenAM にアクセスします。
2. ID 認証モジュールの画面で「認証モジュールの追加」の「ユーザー検索属性」に設定された属性名に対応する属性値を入力し、「ログイン」を押下します。

図 9　ID 認証モジュール

3. データストア認証モジュールの画面で正しいパスワードを入力し、「ログイン」を押下するとログインに成功します。

図 10　データストア認証モジュール

図 11　プロファイル画面

4 注意事項

ここでは ID 認証モジュールを利用する上での注意事項について説明します。

4.1 ユーザーの存在有無の漏洩

「認証連鎖の追加」の 4. で「基準の選択」を Requisite に設定した場合、ユーザー ID の存在有無によって認証連鎖の挙動が変わるため、ユーザーの存在有無が漏洩するリスクがあります。Requisite に設定する場合はリスクを考慮した上で採用してください。

4.2 ID のみで認証可能

認証連鎖の設定が正しく行われていない場合、ID のみで認証できる経路ができてしまう可能性があります。認証連鎖や設定を確認した後に「認証モジュールの追加」の「モジュールの有効化」を有効にするようにしてください。「認証連鎖の追加」の 4. で「基準の選択」を Sufficient にしたり、ID 認証モジュール単体の認証連鎖を作成したりしないようにしてください。

4.3 「モジュールベースの認証」の無効化

認証設定の「モジュールベースの認証」は必ず “無効” と設定してください。“有効” では認証モジュール名を指定することで ID のみで認証が可能な状態です。「モジュールベースの認証」については OpenAM 管理者マニュアルを参照ください。

5 備考

5.1 認証連鎖作成時のオプション

「認証連鎖の追加」の 6. のように、データストア認証モジュールや OpenLDAP 認証モジュールのオプションに `iplanet-am-auth-shared-state-enabled=true` を設定するとその前の認証モジュールから `sharedState` に保存されたユーザー名を引き継いで認証することができます。この機能と「認証モジュールの追加」の「認証結果に関わらずユーザー名を sharedState に保存する」を組み合わせて利用すると、ID 認証モジュールでの認証に失敗した場合でも認証時の画面遷移や動作を見た目上成功時と変えることなく認証することができます。

5.2 認証失敗時のエラーメッセージ

ID 認証モジュールを `Requisite` 条件で利用する場合や、「機能概要」にあるように認証連鎖分岐モジュールと組み合わせて利用する場合、ID 認証失敗時に表示されるエラーメッセージをカスタマイズすることができます。「認証モジュールの追加」の設定例のように「エラーメッセージコード」設定を空欄にしている場合、認証失敗すると「認証に失敗しました。」と表示されます。

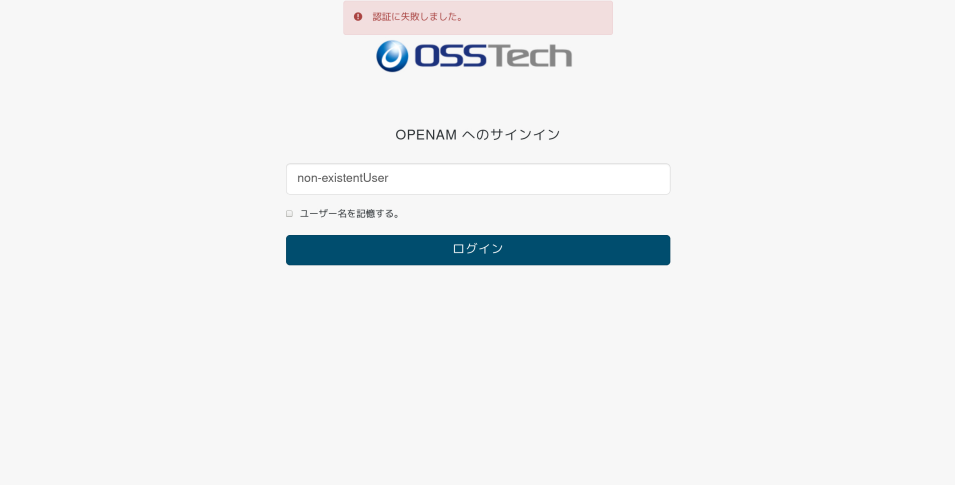

図 12　デフォルトのエラーメッセージ

このエラーメッセージをカスタマイズするには、表示したいメッセージをプロパティファイルに定義し、定義したキーを「エラーメッセージコード」に設定します。ただし、「ユーザー検索属性」設定が空欄の場合と「モジュールの有効化」設定が無効になっている場合の

エラーメッセージは、カスタマイズを行ってもデフォルトメッセージの「認証に失敗しました。」から変更されません。

認証を行うユーザーがブラウザの言語を日本語に設定している場合、メッセージを取得するために参照されるプロパティファイルは amAuthId_ja.properties ファイルです。日本語以外の言語に設定している場合、amAuthId.properties ファイルです。OpenAM のインストールディレクトリのパス[*1]を{OPENAM_INSTALL} とすると、プロパティファイルは{OPENAM_INSTALL}/WEB-INF/lib/openam-auth-id-x.x.x.jar の中にあります。プロパティファイルを編集する際は、この jar ファイルを展開し、編集したいプロパティファイルを{OPENAM_INSTALL}/WEB-INF/classes/ ディレクトリにコピーして編集します。

ここでは、ブラウザの言語を日本語に設定している場合に表示されるエラーメッセージを変更します。

以下にインストールディレクトリがデフォルトパスの場合の展開方法と配置方法を示します。適宜パスと ID 認証モジュールのバージョン x.x.x を置き替えて実行してください。

```
# cd /opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes/
# jar -xvf ../lib/openam-auth-id-x.x.x.jar amAuthId_ja.properties
```

日本語は Unicode エスケープされてプロパティファイルに定義されているため、編集する際は一度ネイティブコードに変換し、編集後 Unicode に戻します。[*2]

```
# native2ascii -reverse amAuthId_ja.properties amAuthId_ja.properties.utf8
# vi amAuthId_ja.properties.utf8
（プロパティファイルの編集）
# native2ascii amAuthId_ja.properties.utf8 amAuthId_ja.properties
```

プロパティファイルには予め以下の設定例が定義されています。

```
errorMessage=ユーザーの特定に失敗しました。
```

上記のプロパティ値のみを変更するか、または新しくプロパティキーとプロパティ値を追加します。新しく定義する場合は、同じファイル内に定義されている既存のプロパティキーと重複しない文字列をプロパティキーとして使用する必要があります。ここでは、例としてプロパティキーを「wrongUserID」、プロパティ値を「ユーザー ID が間違っています。」と

[*1] デフォルトでは/opt/osstech/share/tomcat/webapps/openam です

[*2] この作業は ISO-8859-1 文字セットに含まれていない文字がプロパティファイル内に存在する場合にのみ必要です

定義します。

```
wrongUserID=ユーザー ID が間違っています。
```

上記のように、「基底名.properties」（ID 認証モジュールでは amAuthId.properties）以外のプロパティファイルに新しくプロパティを追加した場合、「基底名.properties」ファイルにも同様のプロパティキーを持つプロパティを追加する必要があります。amAuthId_ja.properties ファイルと同様にして展開と配置を行い、編集します。

```
# cd /opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes/
# jar -xvf ../lib/openam-auth-id-x.x.x.jar amAuthId.properties
# vi amAuthId.properties
（プロパティファイルの編集）
```

以下のように同じキーのプロパティを追加します。

```
wrongUserID=Your user ID is incorrect.
```

設定を反映するために OpenAM を再起動します。

```
# systemctl restart osstech-tomcat
```

OpenAM の再起動後、ID 認証モジュールの設定の「エラーメッセージコード」欄に使用するプロパティのキーを入力し、「変更の保存」を押下します。プロパティファイルに定義されていた設定例のプロパティ値のみ変更した場合は「errorMessage」を、新しくプロパティを追加した場合はそのキー（例では「wrongUserID」）を設定します。

例のように設定を変更すると、ID 認証失敗時に以下のように表示されます。

図 13　カスタマイズされたエラーメッセージ

6 改版履歴

- 2020 年 8 月 6 日 リビジョン 1.0
  - 初版作成
- 2021 年 3 月 25 日 リビジョン 1.1
  - 「モジュールベースの認証」について追記
- 2021 年 4 月 1 日 リビジョン 1.2
  - 「認証失敗時のエラーメッセージ」を追加
- 2022 年 7 月 14 日 リビジョン 1.3
  - 表紙の社名を OSSTech 株式会社に変更