OpenAM 14 ID 認証モジュール 利用手順書



更新日

2022年7月14日

リビジョン

1.3



目次	5	
1 1.1	はじめに 機能概要	1 1
2 2.1 2.2	認証モジュールと認証連鎖の設定 認証モジュールの追加	2 2 4
3	認証時の操作	8
4 4.1 4.2 4.3	注意事項 ユーザーの存在有無の漏洩 ID のみで認証可能 「モジュールベースの認証」の無効化................	10 10 10 10
5 5.1 5.2	備考 認証連鎖作成時のオプション	11 11 11
6	改版履歴	15



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 OpenL-DAP 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。

OpenAM 🌢 UILA			警 セッション		•
▲ 最上位のレルム	認証・モジュール > n	ew			
@ ダッシュボード ▲ 認証	新規モジ	ュールの作成	Ż		
 > 設定 > 認証連鎖 > モジュール 	名前種類	ID ID			
書 データストア G 権限 G 複限				(キャンセル	作成
 					
\$\$ X797F					

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。

	OpenAM • LILL	▼ ▶ 段定 ▼ ▲ デブロイメント ▼	目 連携 替 セッション		•
	▲ 最上位のレルム	認証 - モジュール > id > ID			
) 設定 10) 設定書 モジョーン) モジョーン 第正レベル 0 ダ ウービス 第正レベル 0 를 データストア ユーケー焼素度 ロ 短 調 第正記書座(前する) ロ 細 調 第正記書座(前する) ウ ニッシュトレーク モジュールの有効化 ① キ ゴージェントト モジュールの有効化 ① ウ 515 第二人友育 数化 ①	● ダッシュボード▲ 認証	⊗ □			
・ モジュール び ひ い い い い い い い い い い い い い い	 設定 設定連續 				
レージーと入 コーダー検索風性 0 ビージーストア コーダー検索風性 0 ビージョント ボニージョールの有效化 0 ・・ジョーレの有效化 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	 ・ モジュール 	認証レベル	0		0
○ 相談 詳認は第に図からアニーソー会会 ● Q 認可 AnaccEntant (気俗する) ● ● 対加 モジュールの有効化 ● + エージェント モジュールの有効化 ● + 513 東北政策) 変更的体子 東北政策) 変更的体子	が ワーヒス 書 データストア	ユーザー検索属性			0
	2 権限 4 認可	認証結果に関わらずユーザー名を sharedState に保存する			0
		モジュールの有効化			0
(0 X27)/F	∲ STS			元1	戻す 変更の保存
	\$\$ \$\$U\$F				

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。

【設定例】
0



【項目名】	【設気	ミ例】
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	
	有効	
エラーメッセージコード	(空桐	剿)

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。

OpenAM 🔺 un	ム・ チ 設定 ・ 击 デブロイメント・ 回 連携 🔮 セッション	۵.
📤 最上位のレルム	認証-認証連鎖 > new	
	認証連鎖の追加	
> 設定 > 認定連動 > モジュール	名前 idService	
★ サービス 書 データストア		ギャンセル 作成
양 権限 요. 認可		
留 対象 ● エージェント 会 CTS		
ゆ スクリプト		

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。

OpenAM 🌢 VILL	- チ 段定 - 本 デブロイメント - 団 連携 曽 セッション	
▲ 最上位のレルム	認証 - 認証連鎖 > idService	
 ▲ ダンシュボード ▲ 第三 ⇒ 改正 ⇒ 初辺(第) ⇒ モンコール ダ リービス 第 データス入び ※ 相相 へ 相助 ● 対応 ● ゴント ● 打ち ● ボン ● ボン		★ 前座 転換フラグがないこと、 + ★ ★ × オブション ⑧ ないこと、
		変更の保存

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。
- 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。

OpenAM 🌰 UILL	- × 1	新規モジュール		۵
🚔 最上位のレルム	1212 - 121	モジュールの選択	基準の選択	
		DataStore - $\overline{\tau} - g \chi \vdash \overline{\tau}$ -	Required •	
 タッシュボード 認証 	90	オプション キー	셜	利用 ×
> 認証連鎖	すべてのモ	iplanet-am-auth-shared-state-enabled	true #	を追加してください。
> モジュール ∲ サービス	1212101	キーの追加	値の追加 ◆	
■ データストア 図 検照	+ च		キャンセル のK	うること。 😰 失敗フラグがないこと。
a, 認可	1			+ / ×
營 対象				
♥ エージェント		Required • 0		オプション (0)
		朱欣 🔁		成功 🛄
		認証が成功するには次が必要です:	● 少なくとも1つの成功フラグがあること。	● 失敗フラグがないこと。
				変更の保存

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。

OpenAM - UNL	- ノ 設定		誉 セッション		÷
▲ 最上位のレルム	121E - 121E)	Ē鍵 > idService			
 参 ダッシュボード 認証 > 認定 > 認証達録 > モジュール サービス 	 ゆう すべてのモジ 認証連鎖の 	認証連結 idService ュールインスタンスにユーザーの資格情報を渡すフ 協定	プロセスを構築するように、認証モジュールイ	▲剤してください。	1RR
 ボータストア 2 検照 4 認可 4 初永 	+ €93	-ルの通加 認証が成功するには次が必要で の 10	*す: 💽 少なくとも1つの成功フラグがあ	ること。 🔁 失敗フラグがないこと 中 🥒 🗶	5.
 ■ エージェント 		Required • •	Я	オブション 0 835 🖸	
	2	DataStore $\overline{\tau} - g_{\overline{\lambda}} \models \overline{\tau}$		+ # x	
	÷		Ā	x) 2 1 2 1	
		認証が成功するには次が必要です: 🌘 少	なくとも1つの成功フラグがあること。 🌘	🎦 失敗フラグがないこと。	
				変更の保存	Ŧ

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。



<mark>OpenAM</mark> 🔺 ил.	ム ・ チ 設定 ・ 本 デプロイメント・	□ 連携 曽 セッション	٠ -
▲ 最上位のレルム	1812 - 1972		
 あ ダッシュボード 構築) 時間 	認証設定	ントロック 一般 かたっリティ	ポット時にブロナッ
→ 認識額 > 認識額 > モジュール ● サービス 書 データストア	管理者認証設定 編編認証設定	klapService kdService	· 0 · 0
G 権限 4、認可 留:対象			元に戻す」 変更の保存
∳ エージェント ∲ STS ゆ スクリプト			

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。

	059	Tech
	OPENAM ^	のサインイン
tes	st1	
	04	ブイン

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。



055Tech
test1 のパスワードを入力してください
•••••
ログイン

図 10 データストア認証モジュール

OpenAM & Yvya	ж- F	
ユーザープ	ロファイル	
基本情報 パスワード		
	⊐-ザ-% testi	
	* KOJI	
電子メー	敗 COAGIRI ルアドレス	
	携带電話	
		Utar Es

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て認証するこ 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。

 愛証に失敗しました。
0SSTech
OPENAM へのサインイン
non-existentUser
□ ユーザー名を記憶する。
ログイン

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。

05	STech		
		 ユーザー ゆが間違っています。 OSSTech 	
		OPENAM へのサインイン	
		non-existentUser ローザー名を記憶する。	
		ログイン	

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