OpenAM 14 WebAuthn 認証モジュール
利用手順書

OSSTech 株式会社

更新日 2023 年 6 月 9 日
リビジョン 1.3

目次

1 はじめに

本文書は、OSSTech 版 OpenAM 14 に含まれる WebAuthn 認証モジュールの利用手順書です。

1.1 認証モジュールの構成

FIDO2 では認証デバイスの「登録」と認証デバイスを利用した「認証」の 2 つのシーケンスが存在します。

WebAuthn 認証もこれらのシーケンスに従い、WebAuthn (登録) と WebAuthn (認証) の 2 つのモジュールに分かれています。

OpenAM の認証連鎖に含めることで、「登録」と「認証」のそれぞれで異なる認証と組み合わせることが可能です。

1.2 LDAP ディレクトリ構成

従来、OpenAM では認証デバイスの情報をユーザーの属性として格納していました（FR OATH 認証など）。

しかし、WebAuthn 認証では認証デバイスをユーザーとは異なるディレクトリに格納します。

```
ou=example,ou=com
  |
  ├── ou=Users <- ユーザー格納先
  |    ├── uid=user1
  |    ├── uid=user2
  |    └── uid=user3
  |
  └── ou=Credentials <- 認証デバイス格納先
       ├── fido2CredentialID=XXXXXXXXXXX
       ├── fido2CredentialID=XXXXXXXXXXX
       └── fido2CredentialID=XXXXXXXXXXX
```

そして、ユーザーエントリーと認証デバイスエントリーの紐づけは entryUUID 属性によって行います。

以下の例では user1 が認証デバイスを 2 つ、user3 が認証デバイスを 1 つ所有していることを示しています（user2 は所有していない）。

```
ou=example,ou=com
  |
  ├── ou=Users
  |    ├── uid=user1
  |    |    └── entryUUID: 1f23ab57-8391-4d81-8799-6538fe6d06c7
  |    ├── uid=user2
  |    |    └── entryUUID: 639c7d57-ac06-3493-8faf-54650b3a383c
  |    └── uid=user3
  |         └── entryUUID: f01f029a-4908-48da-96e1-28171a98f423
  |
  └── ou=Credentials
      ├── fido2CredentialID=XXXXXXXXXXX <- user1 所有
      |    └── fido2UserID: 1f23ab57-8391-4d81-8799-6538fe6d06c7
      ├── fido2CredentialID=XXXXXXXXXXX <- user1 所有
      |    └── fido2UserID: 1f23ab57-8391-4d81-8799-6538fe6d06c7
      └── fido2CredentialID=XXXXXXXXXXX <- user3 所有
           └── fido2UserID: f01f029a-4908-48da-96e1-28171a98f423
```

1.3 ユースケース

WebAuthn 認証のユースケースを以下に示します。ユースケースによって認証モジュールの設定内容が異なります。

【ユースケース】	【説明】
パスワードレス認証	FIDO2 で ID と認証デバイスにより認証します。
二段階認証	FIDO2 を ID/パスワード認証と組み合わせて二段階認証として 利用します。
ユーザーネームレス認証	ユーザーハンドルを格納した FIDO2 認証デバイス (Resident Key) のみで認証します。

なお、ここで示すユースケースは「認証」シーケンスが対象です。本文書では「登録」シーケンスのユースケースには言及しません。WebAuthn (登録) はデータストア認証 (ID/パスワード認証) と組み合わせて利用します。

2 想定システム構成

本文書で想定するシステム構成です。

2.1 ホスト名 / URL

本文書では、ホスト名や URL を以下のように仮定しています。

【機器】	【ホスト名】
OpenAM	oam.sso.example.co.jp
OpenAM URL	https://oam.sso.example.co.jp/openam
OpenLDAP	ldap.sso.example.co.jp

3 事前準備

WebAuthn 認証を導入する前に、OpenAM サーバーでは以下の事前準備が必要です。

- OpenAM サーバーが HTTPS で動作している
- OpenAM の初期設定が完了している
- WebAuthn 認証で利用する LDAP 属性をユーザーデータストア設定で許可している
- 認証デバイス用ディレクトリサーバーを準備する

3.1 ユーザーデータストア設定

「1.2 LDAP ディレクトリ構成」で言及した通り、ユーザーエントリーと認証デバイスエントリーの紐づけは entryUUID 属性によって行います。よって、entryUUID をユーザーデータストアで許可する必要があります。

なお、検証目的でユーザーデータストアとして内蔵 OpenDJ を利用する場合、本設定は不要です。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム →「データストア」→ 対象のデータストア を開きます。
3.「LDAP ユーザー属性」に entryUUID で準備した属性を追加して「保存」ボタンをクリックします。

3.2 認証デバイス用ディレクトリサーバーを準備する

認証デバイス用ディレクトリサーバーを準備します。

認証デバイス用ディレクトリサーバーでは認証デバイス用の LDAP スキーマを導入する必要があります。また、認証デバイスの格納先のエントリーを準備しておきます。通常はユーザー用の OpenLDAP サーバーとの併用を想定しています。

なお、検証目的で認証デバイス用ディレクトリサーバーをとして内蔵 OpenDJ を利用する場合、本設定は不要です。

3.2.1 osstech-openam-ldapschema パッケージのアップデート

OpenLDAP サーバーに導入されている osstech-openam-ldapschema パッケージのバージョンが 1.5 未満の場合は必要なスキーマが含まれていないため、アップデートする必要があります。

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（ 画面には表示されません ）
```

次に弊社から提供された OpenAM パッケージ一式をインストール先ホストの任意のディレクトリに展開します。

パッケージ展開先のディレクトリに弊社提供のパッケージ一式があることを確認します。

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  x86_64
# ls x86_64
...
osstech-openam-ldapschema-X.X-X.el7.noarch.rpm
...
repodata
```

rpm コマンドを使用して、RPM パッケージをアップデートします。

```
# cd x86_64
# rpm -Uvh osstech-openam-ldapschema-X.X-X.el7.noarch.rpm
```

3.2.2 スキーマの有効化

/opt/osstech/etc/openldap/slapd.conf に下記の定義を追加し、インストールした OpenAM 用のスキーマファイルを読み込むように設定します。

```
include /opt/osstech/etc/openldap/schema/fido2.schema
```

設定変更後、OpenLDAP を再起動します。

```
# systemctl restart osstech-slapd
```

3.2.3 認証デバイスの格納先の準備

認証デバイスの格納先のエントリーを準備しておきます。

本文書では ou=Credentials,dc=osstech,dc=co,dc=jp を利用します。

4 パスワードレス認証として導入する

本章では WebAuthn 認証をパスワードレス認証として導入するための手順を示します。

4.1 WebAuthn Authenticator サービスを設定する

WebAuthn 認証モジュールを動作させるためには WebAuthn Authenticator サービスを作成して認証デバイスを格納するディレクトリサーバーや LDAP オブジェクト／属性を指定する必要があります。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「サービス」を開きます。
3. 「サービスの追加」ボタンをクリックします。
4. 「サービスタイプ」に「WebAuthn Authenticator サービス」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。内蔵 OpenDJ を利用する場合も「バインドパスワード」は必ず入力してください。

【項目名】	【設定例】
Authenticator オブジェクトクラス	fido2Credential, top
Credential ID 属性	fido2CredentialID
公開鍵属性	fido2PublicKey
Credential Name 属性	fido2CredentialName
カウンター属性	fido2SignCount
ユーザーハンドル属性	fido2UserID
プライマリ LDAP サーバー	ldap.sso.example.co.jp:389
ベース DN	ou=Credentials,dc=osstech,dc=co,dc=jp
バインドユーザー DN	cn=oam,dc=osstech,dc=co,dc=jp
バインドユーザーパスワード	「バインドユーザー DN」のパスワードを入力
LDAP Connection Mode	LDAP

4.2 WebAuthn (登録) モジュールを設定する

WebAuthn (登録) モジュールのインスタンスを作成し、登録用の認証連鎖を作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンをクリックします。
4. ここでは「名前」に “registerModule” と入力し、「タイプ」は「WebAuthn (登録)」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。

【項目名】	【設定例】
RP 名	OpenAM
Origin	https://oam.sso.example.co.jp:443
Attestation 設定	none
Attachiment 設定	undefined
Resident Key 設定	false
ローカル認証設定	preferred
タイムアウト (ミリ秒)	60000
Display Name 保存属性名	cn
Authenticator の最大数	3
認証レベル	0

6. 左側のメニューより、「認証」→「認証連鎖」を開きます。
7. 「認証連鎖の追加」ボタンをクリックします。
8. ここでは「認証連鎖名」に “registerService” と入力し、「作成」ボタンをクリックします。
9. 認証連鎖の設定画面が表示されますので、「モジュールの追加」ボタンをクリックします。
10. 「モジュールの選択」のプルダウンで「DataStore」を選択し、「基準の選択」は「Requisuite」を選択して「OK」ボタンをクリックします。
11. 再度「モジュールの追加」ボタンをクリックします。
12. 「モジュールの選択」のプルダウンで「registerModule」を選択し、「基準の選択」は「Required」を選択して「OK」ボタンをクリックします。

13. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンをクリックします。

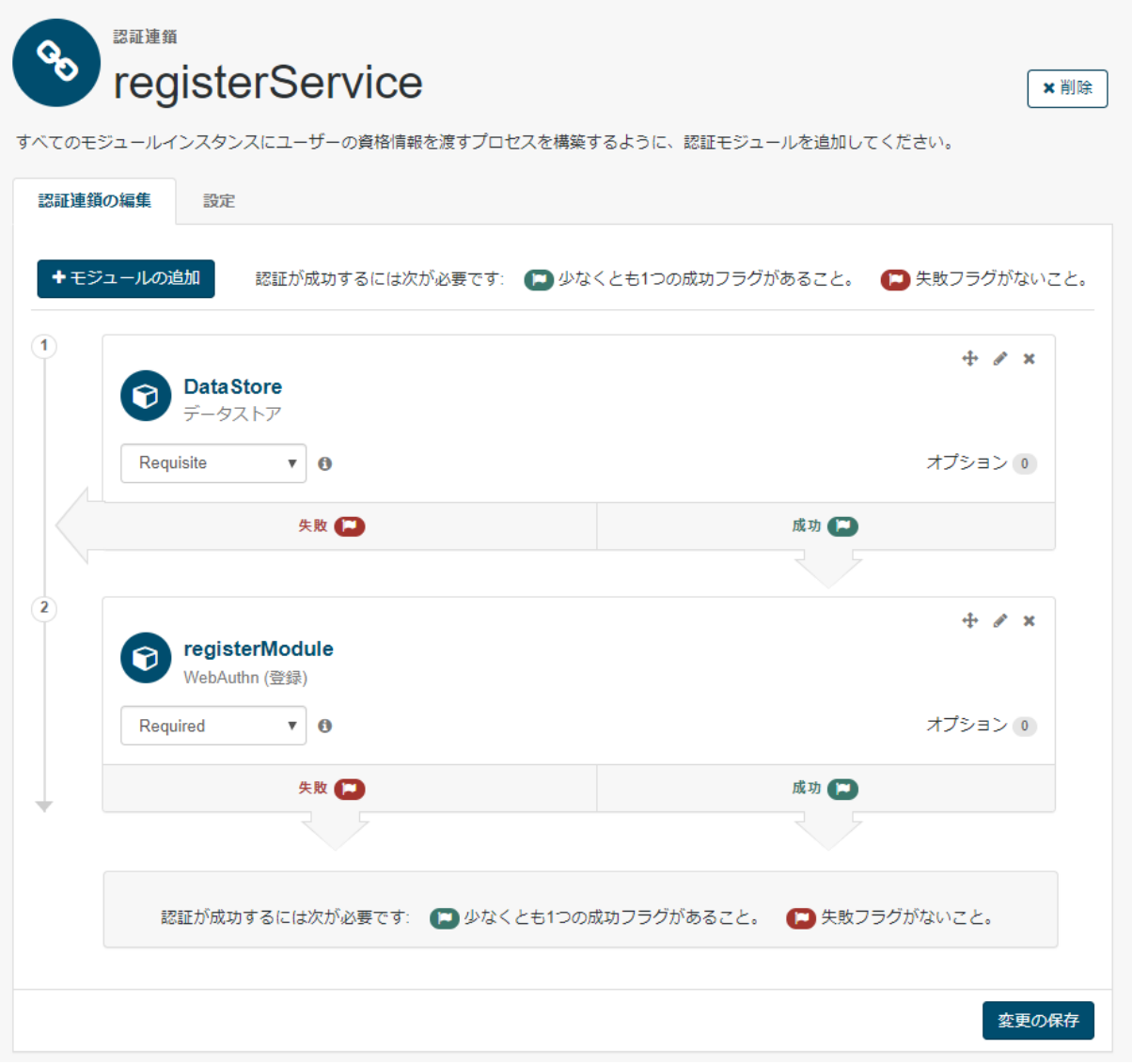

図 1　認証連鎖の設定

以上で完了です。

4.3 WebAuthn (認証) モジュールを設定する

WebAuthn (認証) モジュールのインスタンスを作成し、認証用の認証連鎖を作成します。

1. OpenAM に管理者ユーザーでログインします。

2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンをクリックします。
4. ここでは「名前」に “pwdLessModule” と入力し、「タイプ」は「WebAuthn (認証)」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。

【項目名】	【設定例】
RP 名	OpenAM
Origin	https://oam.sso.example.co.jp:443
Resident Key 認証利用	false
ローカル認証設定	preferred
Transports の送信	true
タイムアウト (ミリ秒)	60000
MFA の 2 段階目以降に利用	false
Display Name 保存属性名	cn
認証レベル	0

6. 左側のメニューより、「認証」→「認証連鎖」を開きます。
7. 「認証連鎖の追加」ボタンをクリックします。
8. ここでは「認証連鎖名」に “pwdLessService” と入力し、「作成」ボタンをクリックします。
9. 認証連鎖の設定画面が表示されますので、「モジュールの追加」ボタンをクリックします。
10. 「モジュールの選択」のプルダウンで「pwdLessModule」を選択し、「基準の選択」は「Required」を選択して「OK」ボタンをクリックします。
11. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンをクリックします。

図 2　認証連鎖の設定

以上で完了です。

4.4 動作確認 (パスワードレス認証)

4.4.1 認証デバイスを登録する

登録用の認証連鎖を動作させて認証デバイスを登録します。

1. WebAuthn をサポートするブラウザーで次の URL にアクセスします。

- https://oam.sso.example.co.jp/openam/UI/Login?service=registerService

2. ログイン画面が表示されますので、ユーザー名/パスワードを入力して「ログイン」ボタンをクリックします。

図 3　データストア認証

3. ブラウザでポップアップが表示されます。ブラウザの指示に従って認証デバイスを操作します。

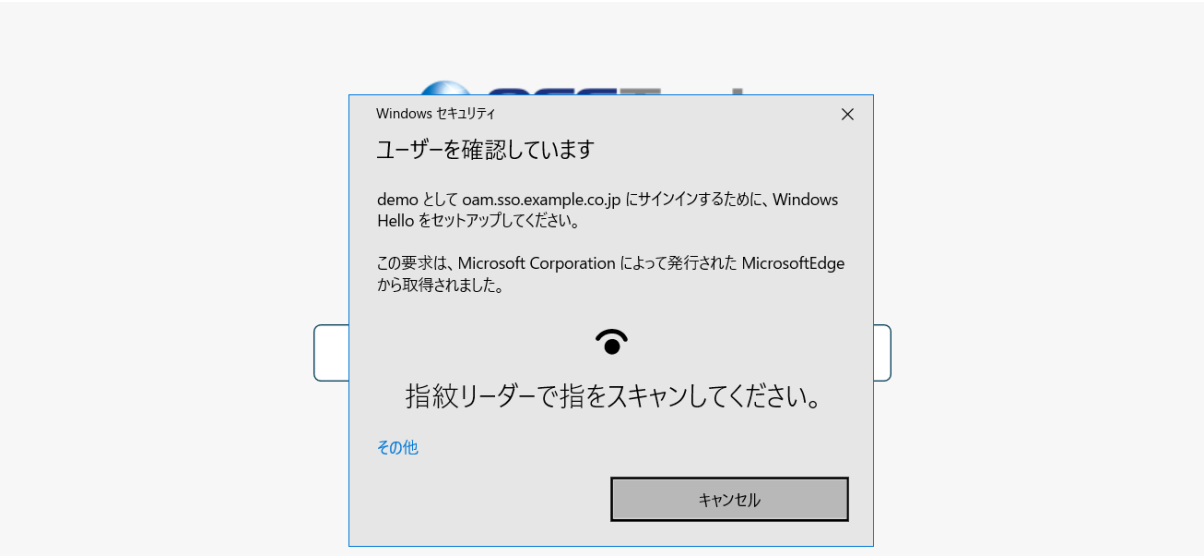

図 4　認証デバイスの登録

4. 登録処理が成功すると「認証デバイスが登録されました識別名を入力してください(任意)」と表示されますので、認証デバイスの識別名を入力して「次へ」ボタンをク

リックします。

図 5　認証デバイスの識別名の入力

5. 認証セッションが発行されてユーザープロファイル画面が表示されます。

以上で完了です。

4.4.2 認証デバイスで認証する

認証用の認証連鎖を動作させて認証デバイスで認証します。

1. WebAuthn をサポートするブラウザーで次の URL にアクセスします。

- https://oam.sso.example.co.jp/openam/UI/Login?service=pwdLessService

2. ログイン画面が表示されますので、ユーザー名を入力して「ログイン」ボタンをクリックします。

図 6　WebAuthn 開始

3. ブラウザでポップアップが表示されます。ブラウザの指示に従って認証デバイスを操作します。

図 7　WebAuthn

4. 認証が成功すると認証セッションが発行されてユーザープロファイル画面が表示されます。

以上で完了です。

5 二段階認証として導入する

本章では WebAuthn 認証を二段階認証として導入するための手順を示します。

5.1 WebAuthn Authenticator サービスを設定する

WebAuthn 認証モジュールを動作させるためには WebAuthn Authenticator サービスを作成して認証デバイスを格納するディレクトリサーバーや LDAP オブジェクト／属性を指定する必要があります。

手順及び設定内容は「4.1 WebAuthn Authenticator サービスを設定する」と同様です。既に実施している場合は「5.2 WebAuthn (登録) モジュールを設定する」に進みます。

5.2 WebAuthn (登録) モジュールを設定する

WebAuthn (登録) モジュールのインスタンスを作成し、登録用の認証連鎖を作成します。手順及び設定内容は「4.2 WebAuthn (登録) モジュールを設定する」と同様です。既に実施している場合は「5.3 WebAuthn (認証) モジュールを設定する」に進みます。

5.3 WebAuthn (認証) モジュールを設定する

WebAuthn (認証) モジュールのインスタンスを作成し、認証用の認証連鎖を作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンをクリックします。
4. ここでは「名前」に “mfaModule” と入力し、「タイプ」は「WebAuthn (認証)」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。

【項目名】	【設定例】
RP 名	OpenAM
Origin	https://oam.sso.example.co.jp:443
Resident Key 認証利用	false
ローカル認証設定	preferred
Transports の送信	true

【項目名】	【設定例】
タイムアウト (ミリ秒)	60000
MFA の 2 段階目以降に利用	true
Display Name 保存属性名	cn
認証レベル	0

6. 左側のメニューより、「認証」→「認証連鎖」を開きます。
7. 「認証連鎖の追加」ボタンをクリックします。
8. ここでは「認証連鎖名」に “mfaService” と入力し、「作成」ボタンをクリックします。
9. 認証連鎖の設定画面が表示されますので、「モジュールの追加」ボタンをクリックします。
10. 「モジュールの選択」のプルダウンで「DataStore」を選択し、「基準の選択」は「Requisuite」を選択して「OK」ボタンをクリックします。
11. 再度「モジュールの追加」ボタンをクリックします。
12. 「モジュールの選択」のプルダウンで「mfaModule」を選択し、「基準の選択」は「Required」を選択して「OK」ボタンをクリックします。
13. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンをクリックします。

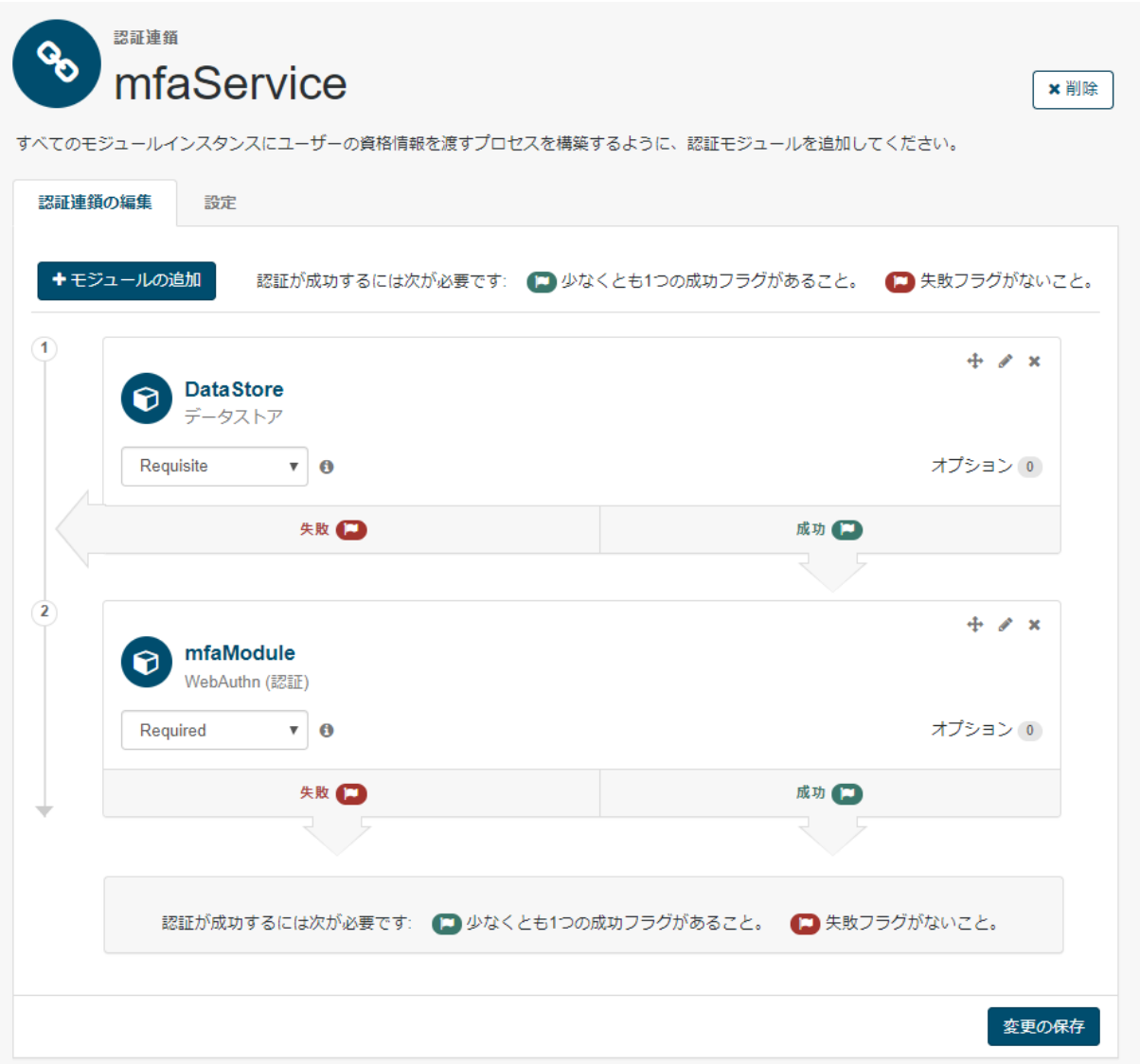

図 8　認証連鎖の設定

以上で完了です。

5.4 動作確認 (二段階認証)

5.4.1 認証デバイスを登録する

登録用の認証連鎖を動作させて認証デバイスを登録します。手順は「4.4.1 認証デバイスを登録する」と同様です。既に実施している場合は「5.4.2 認証デバイスで認証する」に進みます。

5.4.2 認証デバイスで認証する

認証用の認証連鎖を動作させて認証デバイスで認証します。

1. WebAuthn をサポートするブラウザーで次の URL にアクセスします。

- https://oam.sso.example.co.jp/openam/UI/Login?service=mfaService

2. ログイン画面が表示されますので、ユーザー名/パスワードを入力して「ログイン」ボタンをクリックします。

図 9　データストア認証

3. ブラウザでポップアップが表示されます。ブラウザの指示に従って認証デバイスを操作します。

図 10　WebAuthn

4. 認証が成功すると認証セッションが発行されてユーザープロファイル画面が表示されます。

以上で完了です。

6 ユーザーネームレス認証として導入する

本章では WebAuthn 認証をユーザーネームレス認証として導入するための手順を示します。

6.1 WebAuthn Authenticator サービスを設定する

WebAuthn 認証モジュールを動作させるためには WebAuthn Authenticator サービスを作成して認証デバイスを格納するディレクトリサーバーや LDAP オブジェクト／属性を指定する必要があります。

手順及び設定内容はは「4.1 WebAuthn Authenticator サービスを設定する」と同様です。既に実施している場合は「6.2 WebAuthn (登録) モジュールを設定する」に進みます。

6.2 WebAuthn (登録) モジュールを設定する

WebAuthn (登録) モジュールのインスタンスを作成し、登録用の認証連鎖を作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンをクリックします。
4. ここでは「名前」に “residentRegisterModule” と入力し、「タイプ」は「WebAuthn (登録)」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。

【項目名】	【設定例】
RP 名	OpenAM
Origin	https://oam.sso.example.co.jp:443
Attestation 設定	none
Attachiment 設定	undefined
Resident Key 設定	true
ローカル認証設定	preferred
タイムアウト (ミリ秒)	60000
Display Name 保存属性名	cn
Authenticator の最大数	3

【項目名】	【設定例】
認証レベル	0

6. 左側のメニューより、「認証」→「認証連鎖」を開きます。
7. 「認証連鎖の追加」ボタンをクリックします。
8. ここでは「認証連鎖名」に “residentRegisterService” と入力し、「作成」ボタンをクリックします。
9. 認証連鎖の設定画面が表示されますので、「モジュールの追加」ボタンをクリックします。
10. 「モジュールの選択」のプルダウンで「DataStore」を選択し、「基準の選択」は「Requisuite」を選択して「OK」ボタンをクリックします。
11. 再度「モジュールの追加」ボタンをクリックします。
12. 「モジュールの選択」のプルダウンで「residentRegisterModule」を選択し、「基準の選択」は「Required」を選択して「OK」ボタンをクリックします。
13. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンをクリックします。

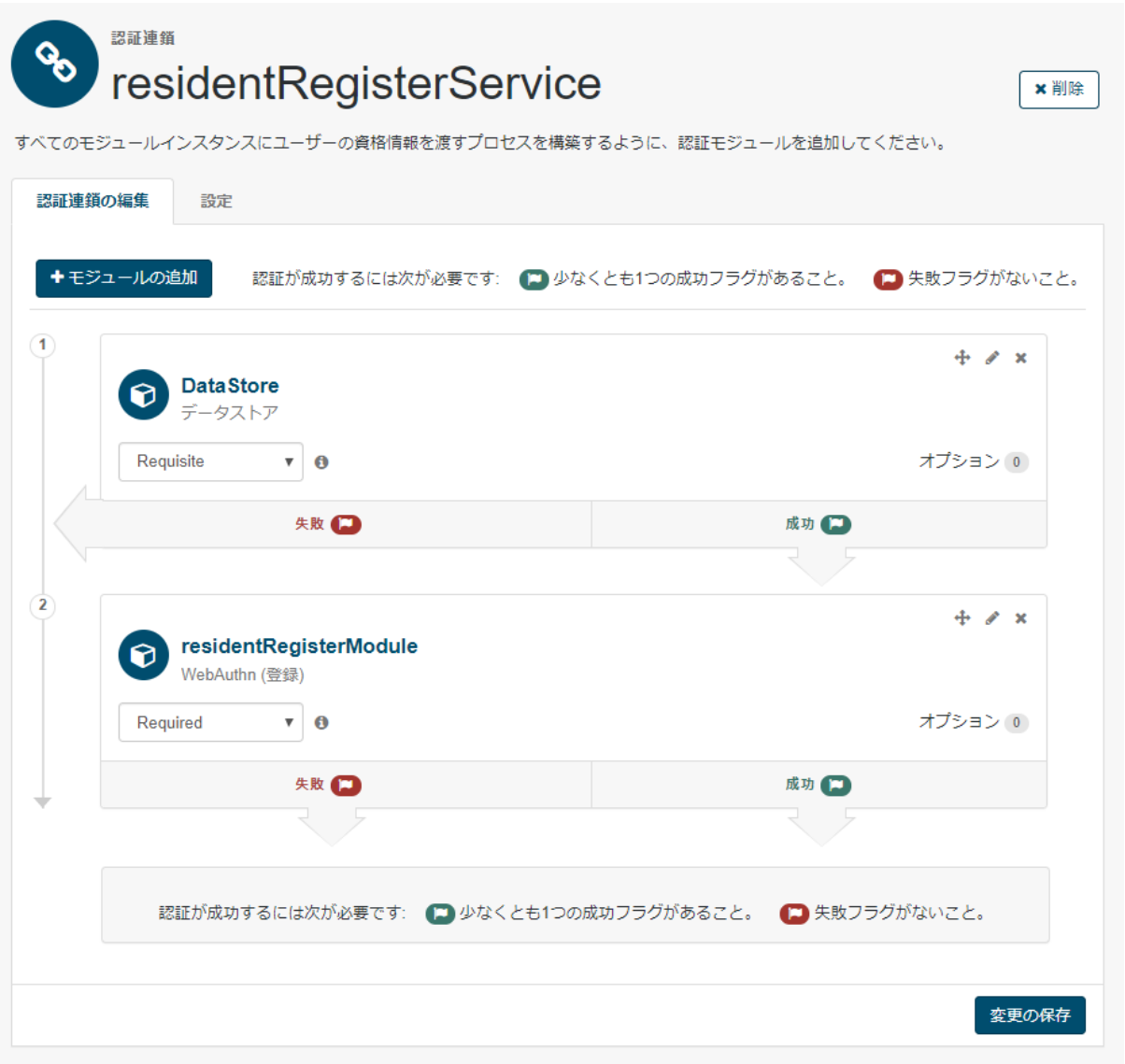

図 11　認証連鎖の設定

以上で完了です。

6.3 WebAuthn (認証) モジュールを設定する

WebAuthn (認証) モジュールのインスタンスを作成し、認証用の認証連鎖を作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンをクリックします。

4. ここでは「名前」に “residentModule” と入力し、「タイプ」は「WebAuthn (認証)」を選択して、「作成」ボタンをクリックします。
5. 各パラメーターを入力し、「変更の保存」をクリックします。以下はパラメータの例です。

【項目名】	【設定例】
RP 名	OpenAM
Origin	https://oam.sso.example.co.jp:443
Resident Key 認証利用	true
ローカル認証設定	preferred
Transports の送信	true
タイムアウト (ミリ秒)	60000
MFA の 2 段階目以降に利用	false
Display Name 保存属性名	cn
認証レベル	0

6. 左側のメニューより、「認証」→「認証連鎖」を開きます。
7. 「認証連鎖の追加」ボタンをクリックします。
8. ここでは「認証連鎖名」に “residentService” と入力し、「作成」ボタンをクリックします。
9. 認証連鎖の設定画面が表示されますので、「モジュールの追加」ボタンをクリックします。
10. 「モジュールの選択」のプルダウンで「residentModule」を選択し、「基準の選択」は「Required」を選択して「OK」ボタンをクリックします。
11. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンをクリックします。

図 12　認証連鎖の設定

以上で完了です。

6.4 動作確認 (ユーザーネームレス認証)

6.4.1 認証デバイスを登録する

登録用の認証連鎖を動作させて認証デバイスを登録します。 アクセスする URL 以外は「4.4.1 認証デバイスを登録する」と同様です。

- https://oam.sso.example.co.jp/openam/UI/Login?service=residentRegisterService

6.4.2 認証デバイスで認証する

認証用の認証連鎖を動作させて認証デバイスで認証します。

1. WebAuthn をサポートするブラウザーで次の URL にアクセスします。

- https://oam.sso.example.co.jp/openam/UI/Login?service=residentService

2.「認証デバイスでログイン」の画面が表示されます。「ログイン」ボタンをクリックします。

図 13　認証デバイスでログイン

3. ブラウザでポップアップが表示されます。認証するユーザーまたは利用する認証デバイスを選択します。

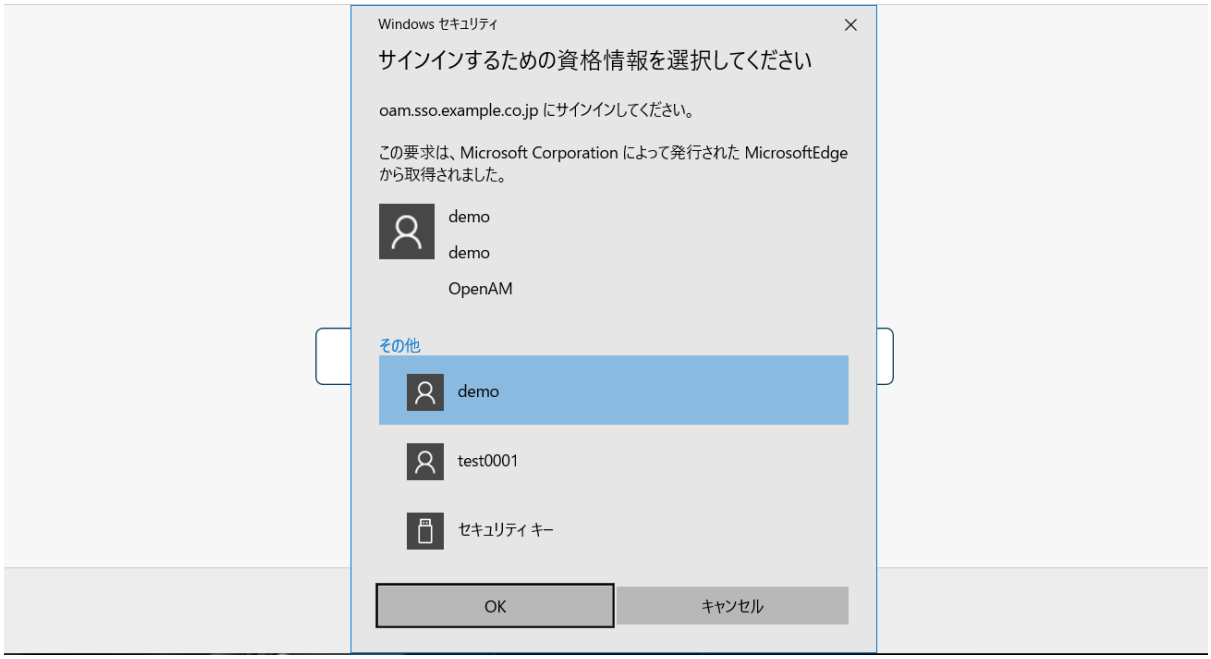

図 14　選択画面

4. ブラウザの指示に従って認証デバイスを操作します。

図 15　WebAuthn

5. 認証が成功すると認証セッションが発行されてユーザープロファイル画面が表示されます。

以上で完了です。

7 認証デバイスを管理する

本章では認証デバイスの管理方法について記載します。

7.1 認証デバイスを表示する

認証デバイスはユーザーのダッシュボード画面で表示が可能です。

1. OpenAM で認証してユーザープロファイル画面を表示します。

図 16　ユーザープロファイル画面

2. 画面左上のダッシュボードをクリックします。
3. ダッシュボード画面をスクロールすると「FIDO2(WebAuthn) 認証デバイス」というセクションがあり、登録した認証デバイスを確認できます。

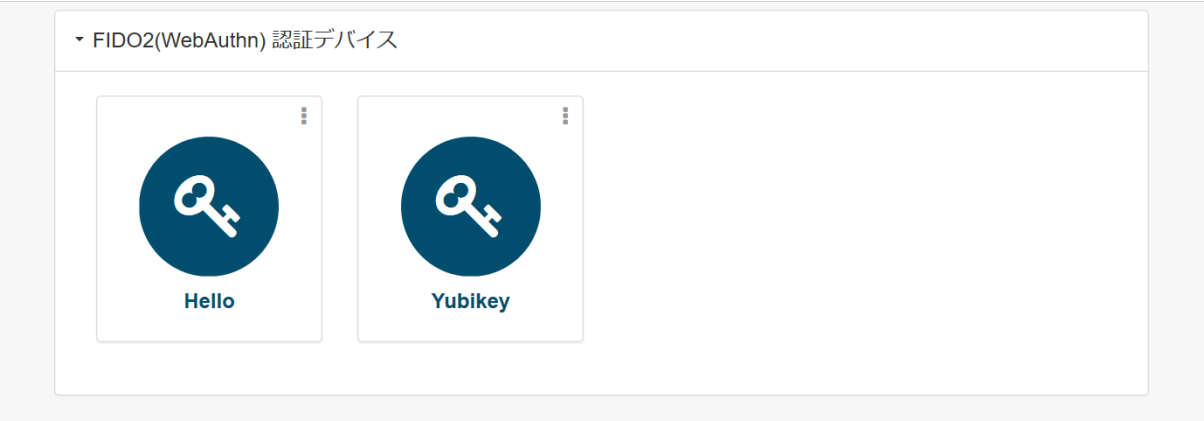

図 17　認証デバイスの表示

7.2 認証デバイス情報を確認する

認証デバイスは名前の他に登録日時を確認することができます。認証デバイスを削除する際に参考にしてください。

1. 「7.1 認証デバイスを表示する」で認証デバイスを表示します。
2. デバイスのアイコンをクリックすると、デバイス名と登録日時が表示されます。

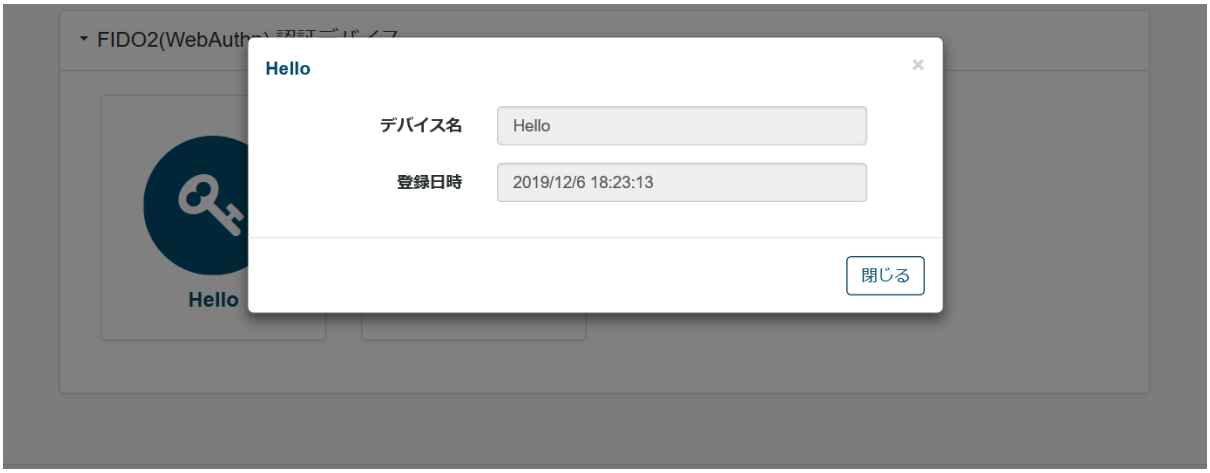

図 18　認証デバイスの詳細表示

7.3 認証デバイスを削除する

認証デバイスはユーザーのダッシュボード画面で削除が可能です。

1. 「7.1 認証デバイスを表示する」で認証デバイスを表示します。
2. デバイスのアイコンの右上をクリックして、削除メニューをクリックします。

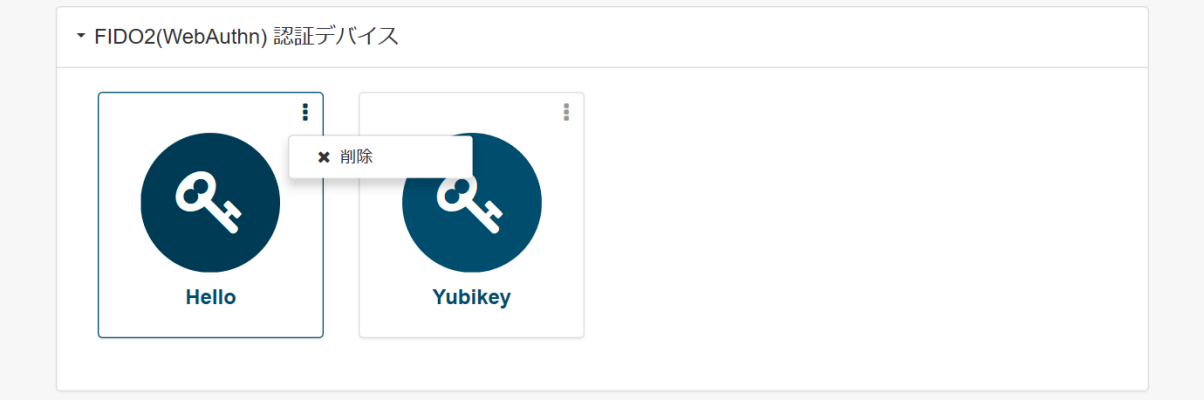

図 19　認証デバイスの削除

8 留意事項

8.1 Transports 送信設定について

WebAuthn 認証時に RP サーバー (OpenAM) が送信する Transports オプションは認証デバイスの選択を容易にするためのオプションです。

W3C による Web Authentication: An API for accessing Public Key Credentials Level 3 (Editor's Draft 17 May 2023) では hybrid が追加になる想定ですが、Draft 仕様であることと、ブラウザによっては cable を利用するなど挙動が統一されていないため、認証時に Transports オプションを送信することにより意図した認証デバイスが使えない可能性があります。

このため、osstech-openam14-14.2.0-43 以降のバージョンでは互換性を確保するために、認証時の Transports オプション送信の有無を選択できる設定を追加しました。

WebAuthn Level 3 に含まれる QR コードを利用した hybrid Transport で認証動作に問題がある場合は、本オプションを false に設定してください。

9 改版履歴

- 2019 年 12 月 6 日 リビジョン 1.0
  - 初版作成
- 2022 年 7 月 14 日 リビジョン 1.1
  - 表紙の社名を OSSTech 株式会社に変更
- 2023 年 5 月 31 日 リビジョン 1.2
  - Transports 送信設定について追加
  - ユーザーネームレス認証の画面遷移を修正
- 2023 年 6 月 9 日 リビジョン 1.3
  - ldap 再起動コマンドを systemctl に変更