OpenAM 14 ForgeRock Authenticator (OATH) 認証モジュール利用手順書

OSSTech 株式会社

更新日 2023 年 5 月 2 日
リビジョン 1.1

目次

1 はじめに

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

1.1 機能概要

ForgeRock Authenticator (OATH) 認証モジュールは OATH 標準アルゴリズムとして定義されている HOTP (RFC 4226) および TOTP (RFC 6238) の 仕組みを使用した認証機能を提供します。 「OpenAM サーバー」と「ユーザーの保持する OATH 準拠のデバイス (スマートフォン等)」に共通の鍵 (秘密鍵) を保持し、両者が秘密鍵からワンタイムパスワードを生成します。ユーザーはデバイスで生成されたワンタイムパスワードを送信し、OpenAM はユーザーから送信されたワンタイムパスワードが自身の生成したものと一致するかどうか確認することで認証を行います。

秘密鍵を含むデバイスの情報は、データストアのユーザーエントリの属性にユーザー毎に保持します。デバイスの登録機能 (秘密鍵の生成) が本モジュールに含まれており、初回認証時にデバイス登録したり、アダプティブリスク等の他の認証モジュールと組み合わせて安全に登録処理を行うことが可能です。

1.1.1 「デバイスの登録」と「ワンタイムパスワードによる認証」

ForgeRock Authenticator (OATH) 認証モジュールは一つのモジュールで「デバイスの登録」と「ワンタイムパスワードによる認証」が行えます。認証モジュール動作時にデータストアのユーザーエントリの属性にデバイスの情報がない場合は「デバイスの登録処理」となります。デバイスの情報が存在する場合は「ワンタイムパスワードによる認証処理」となります。

ForgeRock Authenticator (OATH) 認証モジュールは、単独 (この認証モジュールだけ) では動作しません。認証連鎖を構成しその前段でデータストア認証モジュールなどで認証済み (ユーザー名が判別済み) である必要があります。

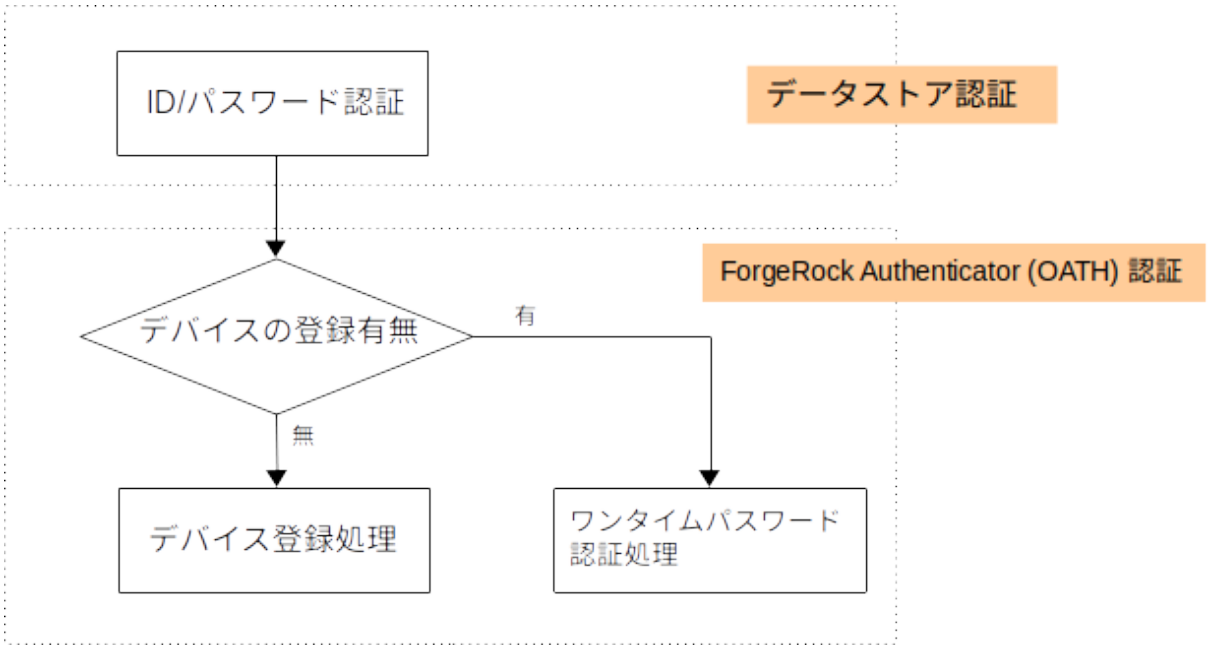

図 1　認証の構成

1.1.2 OATH 準拠の生成デバイス (スマートフォン等)

ForgeRock Authenticator (OATH) 認証モジュールを使うために、ユーザーはワンタイムパスワードを生成するためのデバイス (YubiKey 等の物理デバイスやワンタイムパスワードを生成するアプリをインストールしたスマートフォン) を用意する必要があります。ワンタイムパスワードを生成するスマートフォンのアプリとして下記が利用できます。

- Google Authenticator
- Microsoft Authenticator

スマートフォンのアプリに限らず、上記以外でも OATH に準拠しているアプリケーションであれば利用可能です。

2 事前準備

ForgeRock Authenticator (OATH) 認証モジュールを利用するために、実施すべき内容を説明します。

2.1 OpenLDAP の準備

OpenAM のデータストアとして OSSTech 版 OpenLDAP を利用している場合に必要な手順です。 OpenAM は OATH の秘密鍵などをデータストアのユーザーの属性に書き込みます。事前準備として OpenAM が利用する属性の拡張スキーマの定義と書き込み権限の付与 (アクセス制御) の設定を行います。作業はすべて OpenLDAP サーバー上で行います。

2.1.1 LDAP スキーマの導入

OpenAM 拡張スキーマパッケージを入手し[*1]、rpm コマンドでインストールを行います。

```
# rpm -ivh osstech-openam-ldapschema-*.rpm
```

slapd.conf に下記の定義を追加します。

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

設定を反映させるため再起動を行います。

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

2.1.2 アクセス制御の設定

OpenAM が書き込む属性のアクセス制御の設定が必要です。下記に設定例を示します。OpenAM のデータストアの LDAP バインド DN は `cn=openam,dc=example,dc=com` であると想定していますので環境によって読み替えて下さい。

```
access to attrs=oath2faEnabled,oathDeviceProfiles
        by dn="cn=openam,dc=example,dc=com" write
        by * none
```

[*1] OpenAM 拡張スキーマパッケージがお手元にない場合は、OSSTech サポートまでサポート ID を添えてお問い合わせ下さい。

oath2faEnabled と oathDeviceProfiles の属性が OpenAM が接続するバインド DN で書き込める必要があります。 秘密鍵が入る属性のため、他の LDAP アカウントで読み書き出来ないように none を設定しています。[*2]

2.2 OpenAM の準備

2.2.1 持続検索制御 (Persistent search) の有効化

OpenLDAP 上でのユーザーの属性の変更内容を即座に OpenAM に通知するため持続検索制御 (Persistent search) を有効にします。 設定手順は OpenAM 管理者ガイドを参照してください。

[*2] LDAP のレプリケーション用のアカウントなどは読める必要があるため、管理系アカウントのアクセス制御の定義より下に記載する必要があります。

3 認証モジュールと認証連鎖の設定

ForgeRock Authenticator (OATH) 認証モジュールを利用するための設定内容について説明します。

3.1 認証モジュールの追加

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」ボタンを押下します。
4. 「名前」に任意の名称 (ここでは otp) を入力し、「タイプ」は「ForgeRock Authenticator (OATH)」を選択して、「作成」ボタンを押下します。
5. 各パラメーターを入力し、「変更の保存」を押下します。以下はパラメータの例です。

【項目】	【設定値】	【備考】
ワンタイムパスワードの長さ	6	
秘密鍵の最小桁数	40	10 の倍数を設定してください。
使用する OATH アルゴリズム	TOTP	HOTP は対応していないアプリがあるため通常は TOTP を利用します。
TOTP タイムステップ期間	30	
発行者の名前	OSSTech	デバイス上で表示される名称となります。
リカバリーコードの発行	無効	リカバリーコードを使用する場合は有効します。リカバリーコードについてはこちら

下記の項目は原則としてデフォルトから変更しないで下さい。

- ワンタイムパスワードの長さ
- チェックサム数字の追加
- トランケーションオフセット
- TOTP タイムステップ期間

3.2 認証連鎖の設定

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」 →「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 otpService) を入力し、「作成」を押下します。
4. 「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 パスワード認証を行う認証モジュール (ここでは DataStore) を選択し、「基準の選択」のドロップダウンリストから Requisite を選択します。
5. 同様に「モジュールの選択」で otp を選択し、「基準の選択」で Required を選択します。
6. 「変更の保存」を押下します。

3.3 動作確認

手元に Google Authenticator をインストールしたスマートフォンを準備しておきます。設定例の設定を行った場合は下記のような動作となります。

3.3.1 初回アクセス (デバイスの登録)

1. OpenAM の ログイン URL に `?service=otpService` を付けてアクセスします。
2. ログイン画面が表示されるため、ID/パスワードを入力し、ログインを押下します。

図 2　ID/パスワード画面

3. デバイスの登録開始画面が表示されます。「デバイスの登録」を押下します。

図 3　デバイスの登録画面 1

4. QR コードが表示されます。手元のスマートフォンで読み込みます。[*3]スマートフォン上でワンタイムパスワードが表示されることを確認したら「次へ進む」を押下します。

図 4　デバイスの登録画面 2

5. スマートフォン上で表示されるワンタイムパスワードを入力し、「送信」を押下します。

図 5　デバイスの登録画面 3

[*3] スマートフォンで OpenAM にアクセスしている場合は「スマートデバイスはこちら」を押下することで Google Authenticator が起動しデバイスの登録が可能です。

6. 認証に成功するとユーザープロファイル画面が表示されます。「ダッシュボード」をクリックします。

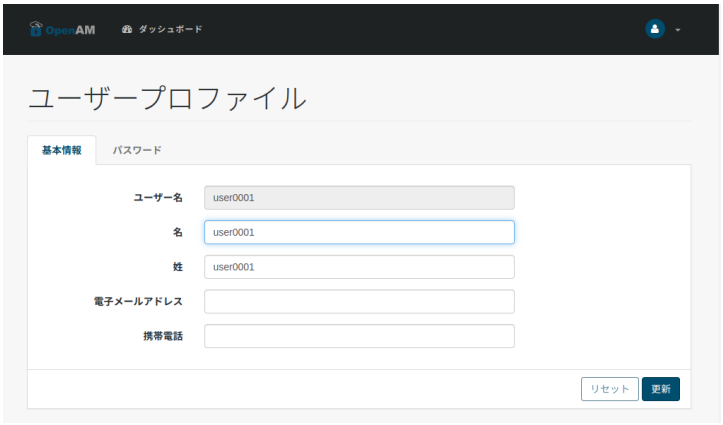

図 6　ユーザープロファイル画面

7. ダッシュボードの認証デバイスに OATH Device が存在することを確認します。

図 7　ダッシュボード

8. 確認が終わったらログアウトを行います。

図 8　ダッシュボード

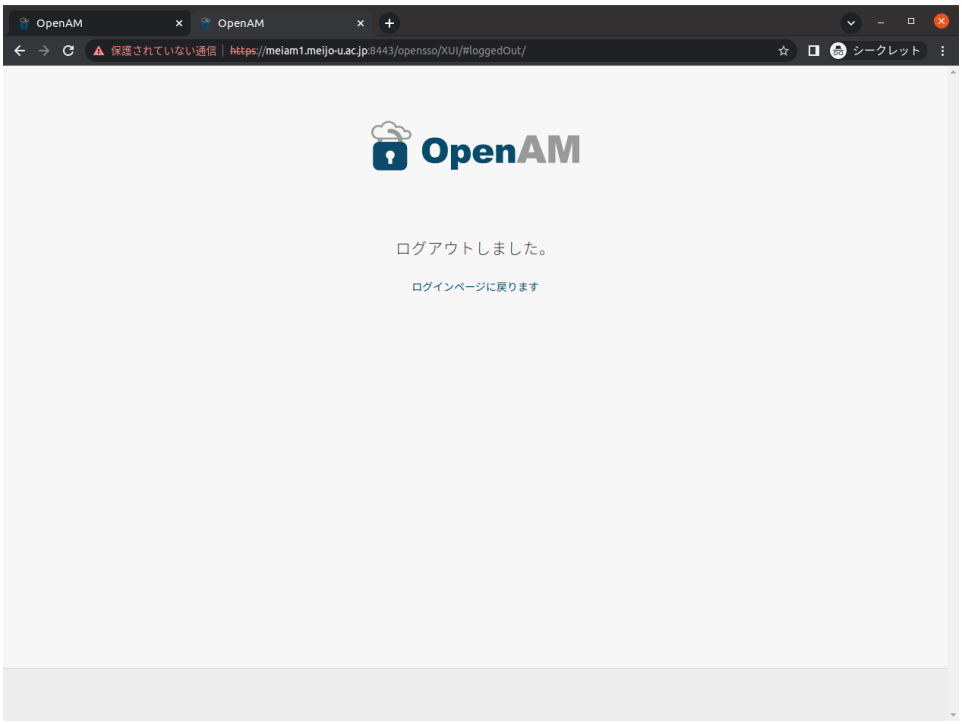

図 9　ログアウト成功

3.3.1.1 「QR コードを読めない方はこちら」について

秘密鍵は QR コードの表示画面でスマートフォンのカメラを使って読み込みますが、カメラが壊れている等の理由で QR コードを読めないデバイスには手動で入力可能です。QR コード表示の画面で「手動で入力 (QR コードを読めない方はこちら)」を押下します。

図 10　QR コードの表示

秘密鍵の文字列が表示されますので、デバイスに鍵文字列を直接入力して登録します。

図 11　デバイスの手動登録

3.3.2 デバイス登録済みの状態でアクセス (ワンタイムパスワードによる認証)

1. もう一度 OpenAM へログイン URL に `?service=otpService` を付けてアクセスします。
2. ログイン画面が表示されるため、デバイス登録したユーザーの ID/パスワードを入力し、ログインを押下します。

図 12　ID/パスワード画面

3. 今度はワンタイムパスワードの入力を求められます。スマートフォン上で表示されるワンタイムパスワードを入力し、「送信」を押下します。

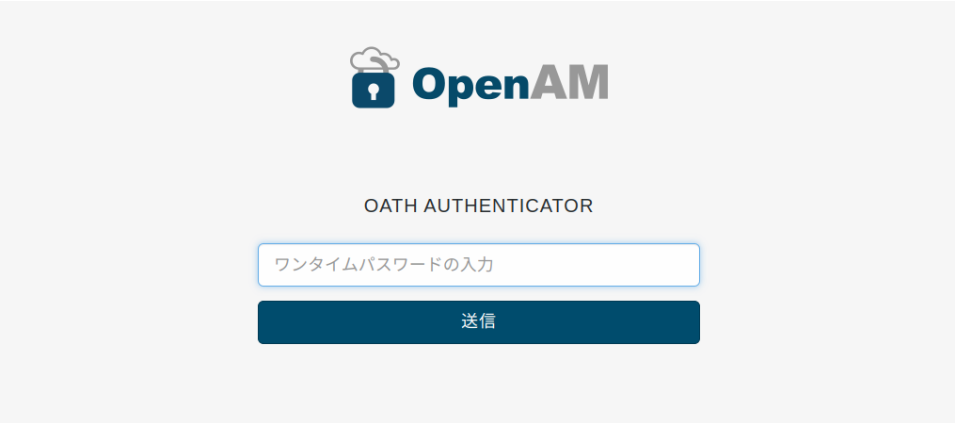

図 13　ワンタイムパスワードの入力

4. 認証に成功するとユーザープロファイル画面が表示されます。

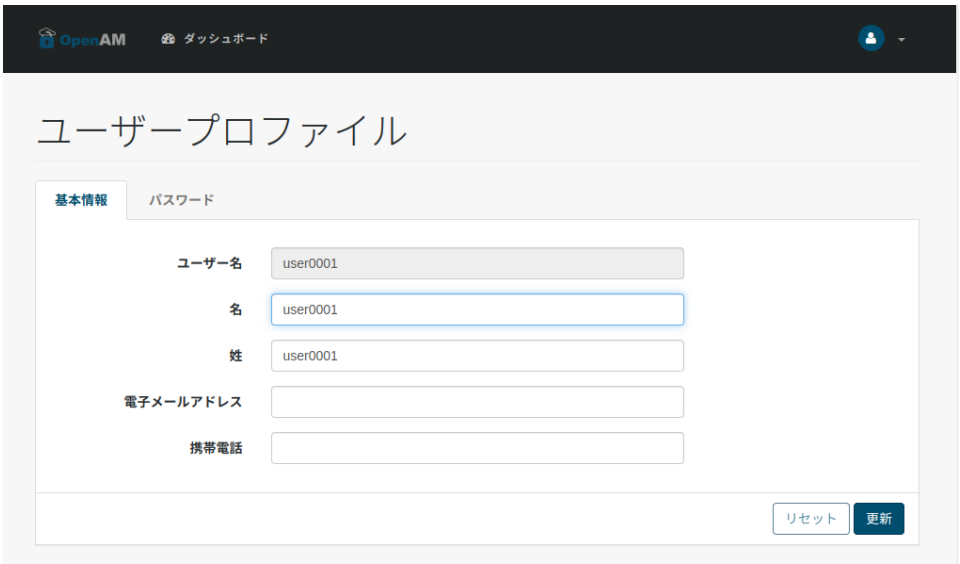

図 14　ユーザープロファイル画面

機能概要で説明したとおり ForgeRock Authenticator (OATH) 認証モジュールはデバイスの登録がないユーザーがアクセスすると、デバイスの登録処理となります。デバイス登録済みのユーザーがアクセスするとワンタイムパスワードによる認証 (ワンタイムパスワードの入力を求める画面) となります。

3.4 データストアに保存される情報

ここではデバイス登録時に保存される属性について説明します。

3.4.1 oathDeviceProfiles のデータ構造

OpenAM がデバイス登録時にユーザーのエントリに保存する oathDeviceProfiles のデータ構造を説明します。 値は json で保持しています。下記が値の例となります。(見やすいよう整形しています。)

```
{
    "uuid": "f640de52-595c-437b-865c-ebe15f468f38",
    "recoveryCodes": ["4bHeXxicG3", "9ZYEVhypew", "ufe7bc3qum"],
    "sharedSecret": "B0AFAEEC665BAEF588CE8B610C1A575532AD3844",
    "deviceName": "OATH Device",
    "lastLogin": 1670551080,
    "counter": 0,
    "checksumDigit": false,
    "truncationOffset": 0,
    "clockDriftSeconds": 0
}
```

各項目について説明します。

【項目】	【説明】
uuid	OpenAM が生成した一意な識別子
recoveryCodes	リカバリーコード。配列で複数の値を持つ。 リカバリーコードを発行しなかった場合は空配列となる
sharedSecret	秘密鍵。鍵のデータを 16 進数表記した文字列 (デフォルト: 40 桁)
deviceName	ダッシュボードで表示される名称。常に “OATH Device”
lastLogin	最後にユーザーがログインした時刻。TOTP を設定した場合に利用
counter	HOTP のカウンタ値。HOTP を設定した場合に利用
checksumDigit	現在使用していません。常に false
truncationOffset	現在使用していません。常に 0
clockDriftSeconds	サーバーとデバイスの時刻の差分。TOTP を設定した場合に利用

3.4.1.1 OpenAM 以外から鍵情報を登録する

現行環境で OATH 準拠のワンタイムパスワードを利用し OpenAM に移行する場合等、oathDeviceProfiles の json を生成し OpenLDAP に登録することで ForgeRock Authenticator (OATH) 認証モジュールを利用可能です。

登録する json は下記のような内容となります。[*4]

```
{
    "uuid": "【新しく uuid を生成】",
    "recoveryCodes": [],
    "sharedSecret": "【現行の秘密鍵をセット】",
    "deviceName": "OATH Device",
    "lastLogin": 0,
    "counter": 0,
    "checksumDigit": false,
    "truncationOffset": 0,
    "clockDriftSeconds": 0
}
```

[*4] 「使用する OATH アルゴリズム」で HOTP の環境を移行する場合はカウンター値の移行が必要です。

3.4.1.2 リカバリーコード

oathDeviceProfiles 内のリカバリーコードについて説明します。リカバリーコードは、ワンタイムパスワード入力欄に一度だけ使える文字列 (コード) です。デバイスを紛失した状況で OpenAM にログインする場合に用いることを想定しています。

認証モジュールの設定の「リカバリーコードの発行」を有効にすることで、ユーザーのデバイス登録時に生成され、oathDeviceProfiles に保存されます。

リカバリーコードはダッシュボードから確認できます。ユーザーは事前に自身に発行されたリカバリーコードを緊急時に備えて保持しておき利用します。[*5]

図 15　ダッシュボード

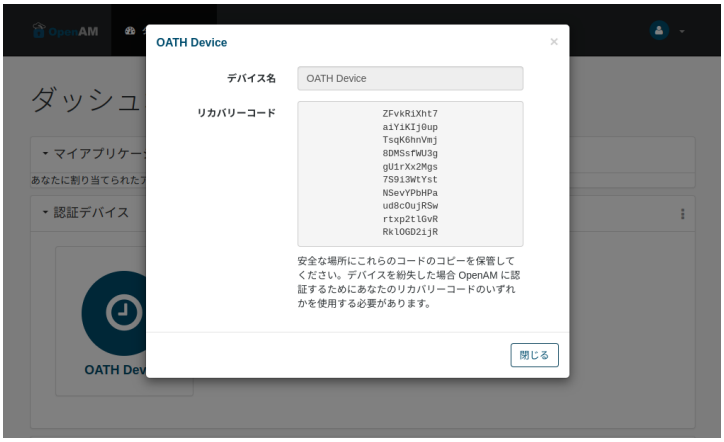

図 16　リカバリーコード

各コードは 1 度だけ使用可能です。使用するとそのコードは一覧から削除されます。

[*5] リカバリーコードが漏洩すると ForgeRock Authenticator (OATH) 認証を突破出来てしまうのでコードの取扱いには注意するよう周知してください。

3.4.2 oath2faEnabled

OpenAM がデバイス登録時にユーザーのエントリに保存する oath2faEnabled を説明します。 oath2faEnabled は「二段階認証を必須にする」を「無効」に設定した場合に使用します。設定が「有効」の場合は使用しません。

oath2faEnabled は 0,1,2 のいずれかの数値が入り、それぞれ次の意味となります。

【設定値】	【説明】
0	未設定状態を意味する。(oath2faEnabled 属性が存在しない場合も同様)
1	ワンタイムパスワードによる認証をスキップする。 ForgeRock Authenticator (OATH) 認証モジュールは常に認証成功となります。
2	ワンタイムパスワードによる認証をスキップしない。 ワンタイムパスワードの入力画面となります。

4 ユースケース

ForgeRock Authenticator (OATH) 認証のユースケースを以下に示します。

【ユースケース】	【説明】
認証モジュール単体の利用（登録→認証）	一つの認証連鎖でデバイスの登録、認証を行います。
アダプティブリスクと組み合わせた利用	デバイス登録用の認証連鎖、ワンタイムパスワード認証用の認証連鎖を用意します。 登録時の IP アドレス制限、鍵の無いユーザーは認証失敗させる等を行います。

4.1 認証モジュール単体の利用（登録→認証）

認証連鎖の設定で作成した otpService 認証連鎖をデフォルトの認証連鎖とします。ID/パスワード認証後にデバイス未登録ユーザーはデバイス登録画面となり、デバイス登録済みユーザーはワンタイムパスワードによる認証を行う構成です。

4.2 アダプティブリスクと組み合わせた利用

デバイス登録用の認証連鎖、ワンタイムパスワード認証用の認証連鎖を用意しアダプティブリスク認証モジュールを組み込んでデバイスの登録に制限をかける構成です。

- デバイス登録用の認証連鎖 (registerotpService)

【認証モジュール】	【条件】
データストア	Requisite
アダプティブリスク	Required
ForgeRock Authenticator (OATH)	Required

登録用の認証連鎖に組み込むアダプティブリスクでは IP アドレスのチェックを行います。これにより、アダプティブリスクで設定した特定の場所 (IP アドレス) からのみデバイスの登録を行う構成とします。

- 認証用の認証連鎖 (oathService)

【認証モジュール】	【条件】
データストア	Requisite
アダプティブリスク	Required
ForgeRock Authenticator (OATH)	Required

認証用の認証連鎖に組み込むアダプティブリスクで oathDeviceProfiles の存在チェックを行います。 デバイス未登録ユーザー (oathDeviceProfiles が存在しないユーザー) の認証を失敗させます。

2 つの認証連鎖を作成したら、oathService をデフォルトの認証連鎖とします。ユーザーにデバイス登録用の URL として `service=registerotpService` の Query パラメーターを付けた URL を周知します。

この構成はデバイス登録を社内などの安全な IP アドレスの環境からのみ行えるように制限し、OpenAM には必ずワンタイムパスワードによる認証が必要となります。

5 その他の設定

5.1 認証設定の「二段階認証を必須にする」

OpenAM の認証設定の「二段階認証を必須にする」について説明します。この設定は ForgeRock Authenticator (OATH) 認証モジュールの動作に影響があります。 設定箇所は下記のとおりです。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「設定」 → 「一般」と辿ります。

この設定を「無効」 (デフォルト: 「有効」) にすると ForgeRock Authenticator (OATH) 認証モジュールのデバイス登録の画面に「登録しないでログインする」が表示されるようになります。

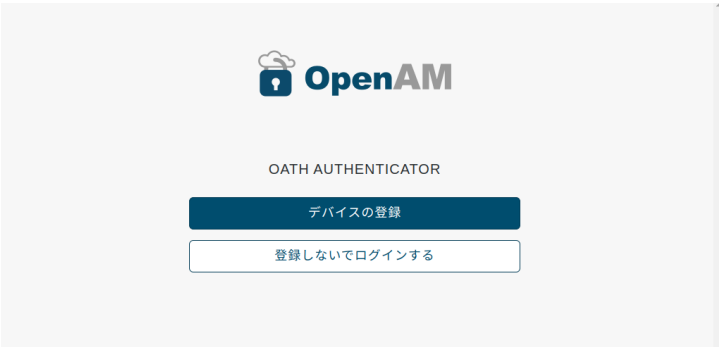

図 17　デバイス登録時に「登録しないでログインする」が表示

ユーザーが「登録しないでログインする」を選択するとデバイス登録せずに (QR コード画面に遷移せずに) 認証成功となります。これ以降 ForgeRock Authenticator (OATH) で認証する際は、ワンタイムパスワードの入力画面は表示されずに認証が成功します。ユーザーにワンタイムパスワードによる認証を行うかを選択させることが出来る機能です。

デバイス登録時にユーザーが選択した内容はデータストアのユーザー属性 oath2faEnabled に保存されます。「二段階認証を必須にする」が無効な場合のフローは下記のとおりです。

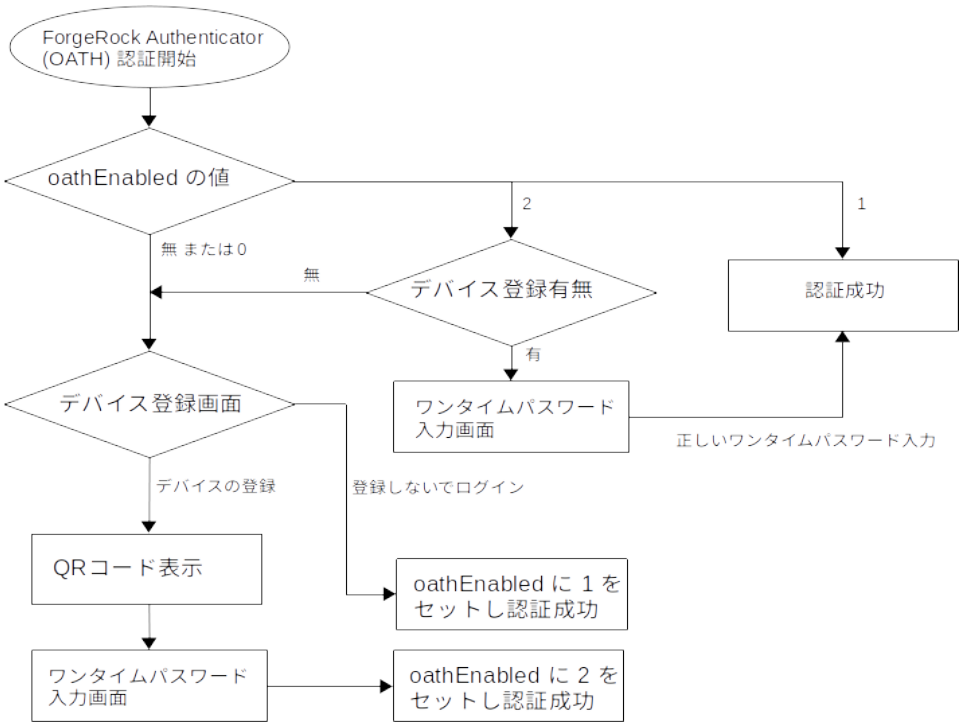

図 18　「二段階認証を必須にする」が無効な場合のフロー

ユーザーが選択した内容はダッシュボードから確認/変更が可能です。ダッシュボードの「認証デバイス」の「設定アイコン」 →「設定」をクリックします。

図 19　ダッシュボード

デバイス登録時に「登録しないでログインする」を選択していると、二段階認証が無効な状態です。

図 20　二段階認証が無効な状態

二段階認証が有効な状態は下記のように表示されます。この設定はこの画面でユーザー自身で変更可能です。

図 21　二段階認証が有効な状態

「二段階認証を必須にする」を「無効」は、ワンタイムパスワードによる認証の利用有無をユーザー自身に選べるようにするシステムで設定します。システムとしてワンタイムパスワードの利用を必須にする場合は「無効」にしないでください。

5.2 ダッシュボードへリンクの追加

ダッシュボードに「OATH デバイスの登録」、「OATH デバイスの再登録」のリンクを表示する機能について説明します。

5.2.1 OATH デバイスの登録

ダッシュボードにデバイスの登録のリンクを表示する設定方法を説明します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム →「サービス」と辿ります。サービス名の一覧から「ダッシュボード」をクリックします。一覧に「ダッシュボード」が存在しない場合は「サービスの追加」を押下し、「ダッシュボード」を作成します。
3.「OATH デバイス 登録用 URL」にデバイスを登録するための URL を入力し「変更の保存」を押下します。

「OATH デバイス登録用 URL」が設定されていると、ダッシュボードの「認証デバイス」の設定アイコンをクリックした際に「OATH Device の登録」のリンクが表示されます。 ユーザーが「OATH Device の登録」をクリックすると、「OATH デバイス 登録用 URL」で設定した URL へ遷移します。

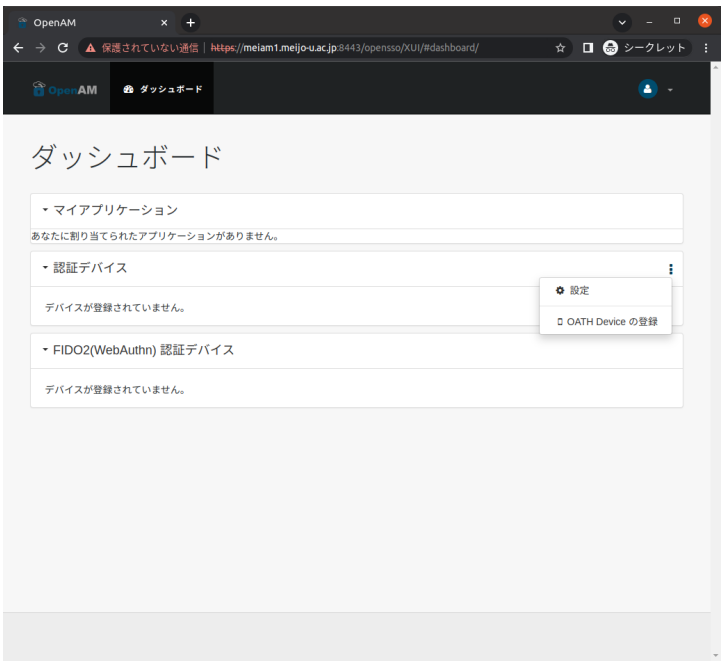

図 22　OATH Device 登録用リンク

5.2.2 OATH デバイスの再登録

ダッシュボードにデバイスの再登録のリンクを表示する設定方法を説明します。

事前準備としてデバイスの再登録用の認証連鎖を準備してください。「OATH デバイス再登録用 URL」には専用に用意した認証連鎖を指定する必要があります。

ここでは認証連鎖の設定と同じ構成の reOtpService という認証連鎖を準備したと想定します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム →「サービス」と辿ります。サービス名の一覧から「ダッシュボード」をクリックします。一覧に「ダッシュボード」が存在しない場合は「サービスの追加」を押下し、「ダッシュボード」を作成します。
3. 「OATH デバイス再登録用 URL」に OpenAM ログイン URL に`?service=reOtpService`を付けた URL を入力し「変更の保存」を押下します。

「OATH デバイス再登録用 URL」が設定されていると、ダッシュボードの OATH Device の設定アイコンをクリックした際に「再登録」のリンクが表示されます。

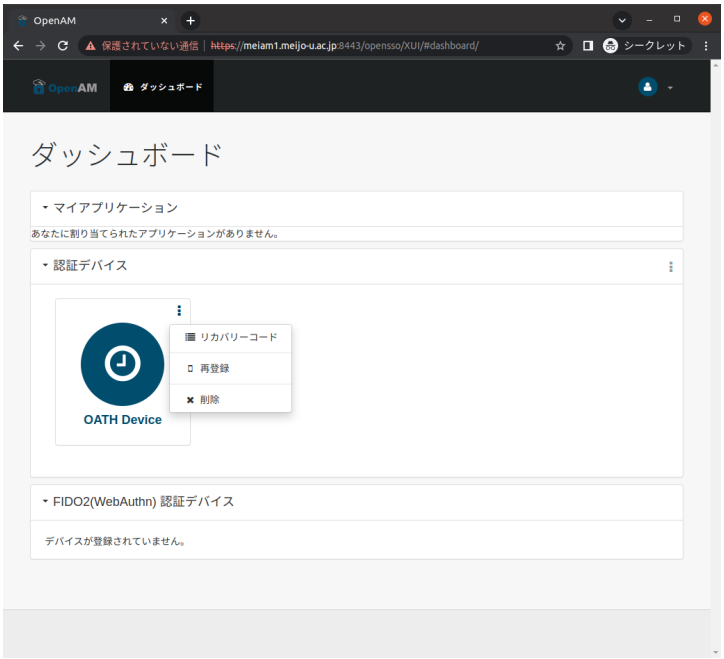

図 23　OATH Device 再登録用リンク

ユーザーが「再登録」をクリックすると、確認のメッセージが表示されます。

「開始」を押下します。

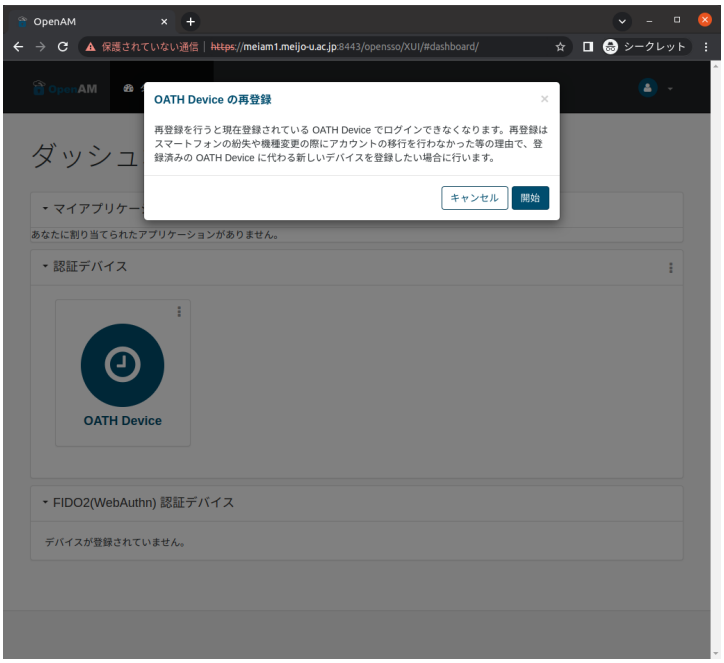

図 24　OATH Device 再登録確認画面

ID/パスワード入力画面となります。正しい ID/パスワードを入力してログインします。

図 25　ID/パスワード画面

デバイス登録の QR コードの表示画面となります。[*6]スマートフォンで QR コードを読み込んで新しくデバイスを登録します。「次へ進む」を押下します。

図 26　デバイスの再登録画面 1

スマートフォン上で表示されるワンタイムパスワードを入力し、「送信」を押下します。

図 27　デバイスの再登録画面 2

[*6] 「OATH デバイス再登録用 URL」で service=xxx と指定した認証連鎖で動作した場合はデバイス登録の開始画面は表示されず、いきなり QR コードの表示画面となります。

完了画面が表示されます。この画面が表示されると oathDeviceProfiles 内の秘密鍵は新しい値となっています。

図 28　デバイスの再登録画面 3

5.3 oathDeviceProfiles の暗号化機能

OpenAM がデバイス登録時にユーザーのエントリに書き込む oathDeviceProfiles のデータを暗号化する機能について説明します。この機能を利用するとデータストアに保存されるデータが暗号化され、秘密鍵やリカバリーコードを OpenAM 以外からは読み取れない値とすることが出来ます。

- LDAP に格納される暗号化データの例

```
oathDeviceProfiles: eyAidHlwIjogIkpXVCIsICJlbmMiOiAiQTI1NkNCQy1IUzUxMi〜
```

データの暗号化機能を設定するための手順です。暗号化にはキーストアファイルが必要です。 事前に keytool コマンドで作成しておきます。[*7]

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」 →「サービスの追加」のボタンを押下します。
3. サービスタイプを選択から「ForgeRock Authenticator (OATH) Service」を選び、「作成」ボタンを押下します。
4. 各パラメーターを入力し、「変更の保存」を押下します。以下はパラメータの例です。

【項目】	【設定例】
Device Profile Encryption Scheme	AES-256/HMAC-SHA-512 with RSAKey Wrapping
Encryption Key Store	/opt/osstech/var/lib/tomcat/data/openam/oath.jceks
Key Store Type	Java Cryptography Extension Key Store (JCEKS)
Key Store Password	[キーストアのパスワード]
Key-Pair Alias	[キーストアのエイリアス]
Private Key Password	[キーストアのキーパスワード]

設定するとデバイス登録時に oathDeviceProfiles のデータが暗号化され、認証時には oathDeviceProfiles のデータを復号して使用します。

本機能は、すでに ForgeRock Authenticator (OATH) 認証モジュールを利用中のシステムで

[*7] keytool コマンドでのキーストア作成方法に注意すべき点はありません。一般的な手順や SAML 設定ガイドの「キーストアと鍵ペアの生成」などを参照して作成してください。

は有効に出来ません。[*8]ユーザーのデータストアの oathDeviceProfiles が暗号化されている状態と暗号化されていない状態を混在した環境で利用できないためです。

本機能を使用するには ForgeRock Authenticator (OATH) 認証モジュール利用開始前に設定にしておく必要があります。

[*8] 利用中に有効に変更する場合は全ユーザーの oathDeviceProfiles の削除 (デバイス登録のやり直し) が必要です。

6 改版履歴

- 2022 年 12 月 20 日 リビジョン 1.0
  - 初版作成
- 2023 年 5 月 2 日 リビジョン 1.1
  - 文言の誤りを修正