LINE OTP 認証モジュール導入手順書

OSSTech **株式会社**

更新日	2022 **年** 7 **月** 14 **日**
リビジョン	1.1

目次

1 要旨

本文書は OpenAM 用 LINE OTP 認証モジュールの導入手順を説明します。

2 システム構成/前提条件

本文書で想定するシステム構成と前提条件を説明します。

2.1 システム構成

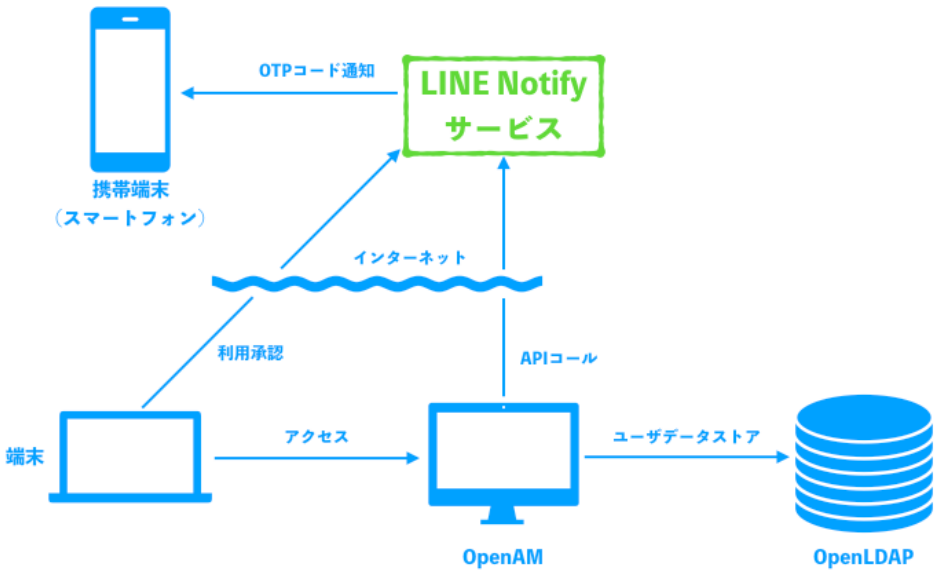

図 1　システム構成

LINE OTP 認証モジュールは LINE Notify サービスを利用します。そのためインターネット上に公開されている以下の LINE Notify API のエンドポイントに対して、 OpenAM が接続できる必要があります。またユーザ端末から LINE 利用の承認操作を行う必要があるので、ユーザ端末からも認証系エンドポイントに接続できなくてはなりません。

- 認証系エンドポイント: `https://notify-bot.line.me/`
- 通知系エンドポイント: `https://notify-api.line.me/`

ユーザデータストアはユーザのアクセストークンを保存する任意の属性が必要になります。ユーザデータストアとして OpenLDAP を利用することは必須ではありませんが、LINE OTP 認証モジュール用にこの属性を含むスキーマファイルを提供しています。詳しくはユーザデータストアの節で説明します。

2.2 その他前提条件

LINE Notify サービスの利用には事前に利用登録をします。利用登録には LINE アカウントが 1 つ必要になります。

3 LINE Notify サービスの利用登録

ここでは LINE Notify サービスの利用登録について説明します。なお利用登録はインターネットにアクセス可能であれば任意の端末で構いません。また利用登録にはサービスの管理者となる LINE アカウントが必要になります。LINE アカウントの取得方法については LINE のホームページ (https://line.me/ja/) 等を参照ください。

3.1 サービス利用登録

LINE Notify のページ (https://notify-bot.line.me/ja/) をブラウザで開きます。開いたらページ下部の「サービスを登録する」を選択します。

図 2　LINE Notify のホームページ

選択するとログイン画面に遷移するので、LINE アカウントでログインします。

図 3　LINE ログイン

ログイン後、サービス名等の必要事項を入力します。

図 4　サービス登録

必要事項を記入すると以下の画面が表示され、入力したメールアドレス宛に登録用 URL を含むメールアドレスが届きます。メールの内容を確認後、問題なければ登録用 URL を開きます。URL を開くと登録が完了し、登録されたサービスが表示されます。

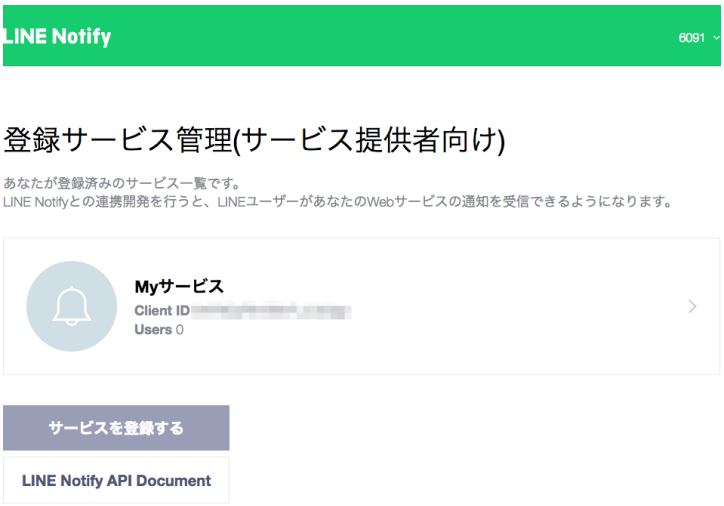

図 5　サービス一覧

登録したサービスを選択すると、サービス利用に必要な Client ID と Client Secret が確認できます。 この Client ID と Client Secret はモジュールの設定の項目で参照します。

図 6　サービス内容

3.2 Callback URL の設定

LINE OTP 認証モジュールにおいて初めてのユーザーは LINE サービス利用の承認操作を行います。 この承認操作は LINE サイト上で行う必要があるので必然的に認証の中で LINE サイトへのリダイレクトが行われます。 つまり認証は「OpenAM の画面」 →「LINE 承認画面」 →「OpenAM の画面」という画面遷移を経て実行されます。

この画面遷移の中で「LINE 承認画面」 → 「OpenAM の画面」の遷移は、LINE 側から OpenAM の画面を呼び出します。 そのためには LINE 側が遷移先 (OpenAM の画面) を知っておく必要があります。 この遷移先の URL を Callback URL と呼び、事前に LINE サービスに登録します。

サービス利用登録の節のサービス内容の画面を下にスクロールすると Callback URL 入力画面が表示されます。 ここに OpenAM のログイン画面の URL を登録してください。なお URL フラグメントは除去してかまいません。

図 7　Callback URL の設定

4 ユーザデータストア

LINE OTP 認証モジュールはユーザデータストアに各ユーザのアクセストークンを保存します。アクセストークンの保存先には任意の属性を指定することができますが、OpenAM では LINE OTP 認証モジュール用に OpenLDAP 用スキーマファイル line.schema を提供しています。 ここでは line.schema を利用する場合の設定方法を説明します。

4.1 ユーザーデータストアの設定を変更する

line.schema を利用する場合、OpenAM のユーザーデータストアの設定を変更する必要があります。

1. OpenAM にログイン後、対象のレルムを選択します。
2. レルムを選択後に「データストア」→対象のデータストアを選択します。
3. 「LDAP ユーザーオブジェクトクラス」に LineOTPObject、「LDAP ユーザー属性」に lineToken を追加して「保存」ボタンをクリックします。

5 モジュールを認証連鎖に追加する

ここでは LINE OTP 認証モジュールを認証連鎖に追加する方法を説明します。

5.1 モジュールの追加とモジュールの設定

OpenAM にログイン後、対象のレルムを選択します。

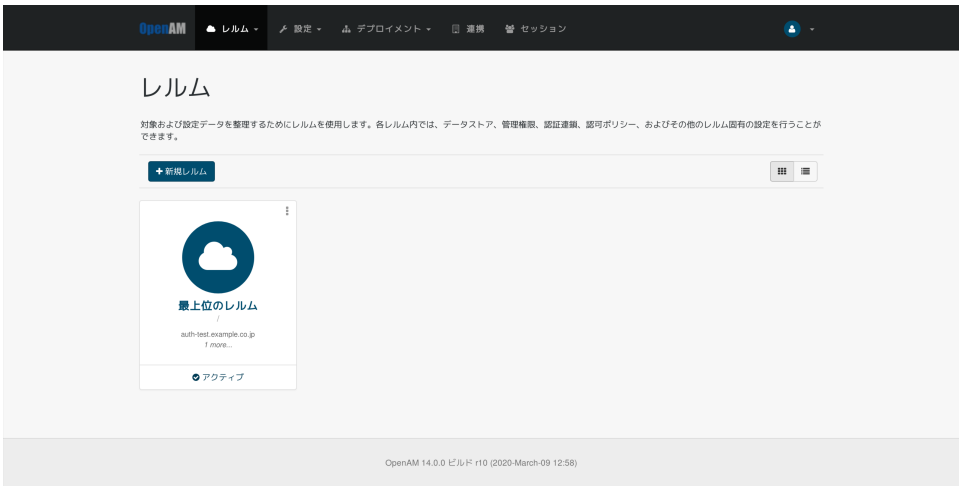

図 8　レルムの選択

レルムを選択後に「認証」→「モジュール」→「モジュールの追加」を選択します。

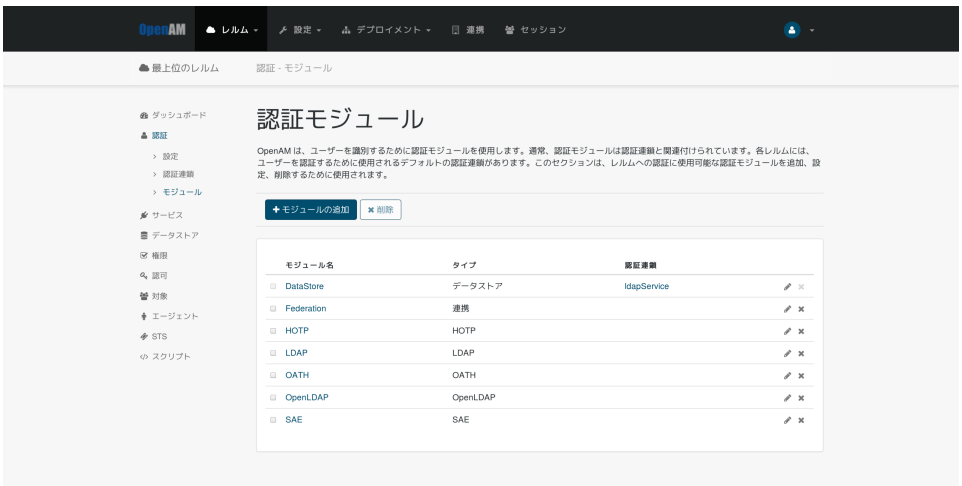

図 9　モジュールの追加

モジュールのタイプは「 LINE OTP 」を選択し、モジュール名は任意の値 (図では LINE)

を入力します。入力が済んだら「作成」を選択します。

図 10　モジュールの作成

LINE OTP 認証モジュールの設定画面になります。

図 11　モジュールの作成

各設定項目は以下のように決定してください。

- 認証レベル
  - モジュールの認証レベルを設定します
  - 必要に応じて入力してください
- LINE 認証 API 共通 URL
  - 変更する必要はありません。

- LINE 通知 API 共通 URL
  - 変更する必要はありません。
- Client ID
  - サービス利用登録の節で確認した値を入力します (後述)。
- Client Secret
  - サービス利用登録の節で確認した値を入力します (後述)。
- アクセストークン属性名
  - アクセストークンを保存するデータストアの属性名です。
  - データストアの節を参考に適切な値を入力してください。
  - 添付のスキーマファイルを OpenLDAP に適用している場合はデフォルトのままで構いません。
- API コネクションタイムアウト
  - Line Notify API をコールする際ののコネクションタイムアウトです。
  - 必要に応じて変更してください。
- API リードタイムアウト
  - Line Notify API をコールする際ののリードタイムアウトです。
  - 必要に応じて変更してください。
- ワンタイムパスワードの有効期間
  - 必要に応じて変更してください。
- ワンタイムパスワードの長さ
  - 必要に応じて変更してください。
- OTP コードの自動送信
  - 自動的に OTP を送信する場合に有効にします。
  - 必要に応じて変更してください。

Client ID および Client Secret はサービス利用登録の節で説明した LINE Notify サイトで確認します。

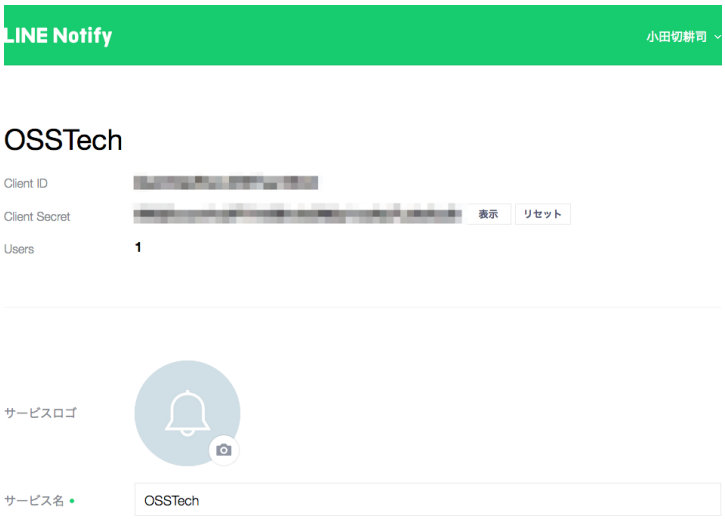

図 12　トークンを確認

5.2 認証連鎖の設定

認証連鎖に組み込むことで LINE OTP 認証モジュールによる認証を実現できます。 なお LINE OTP 認証モジュールは単独で認証連鎖を構成できません。 Data Store 認証など、必ず LINE OTP 認証モジュールの前に OpenAM の ID を認証するモジュールを指定してください。

ここでは Data Store 認証モジュール → LINE OTP 認証モジュールの 2 段階の認証連鎖の新規作成について説明します。既存の認証連鎖に LINE OTP 認証モジュールを追加する場合は本設を参考に設定してください。

OpenAM にログイン後、対象のレルムを選択、「認証」→「認証連鎖」→「認証連鎖の追加」を選択します。

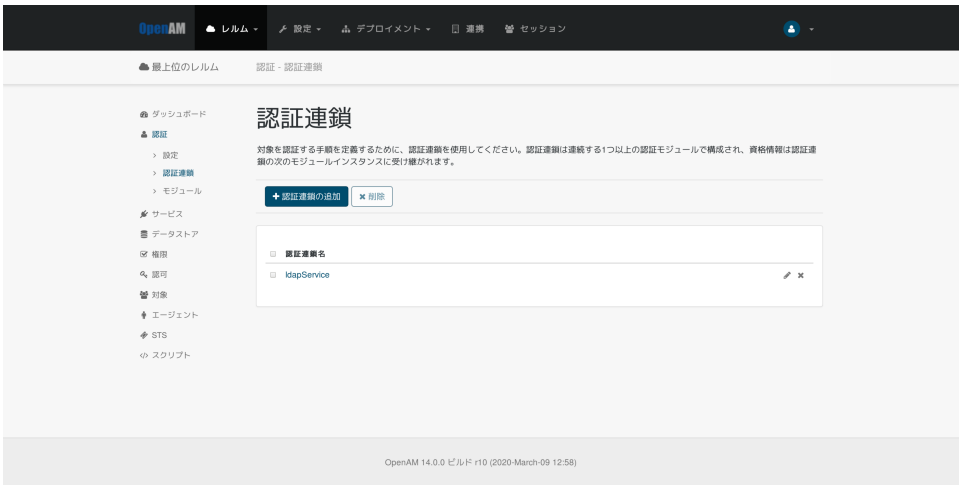

図 13　認証連鎖の追加

「認証連鎖名」に適当な値を設定して (下図では “lineService”)、「作成」を選択します。

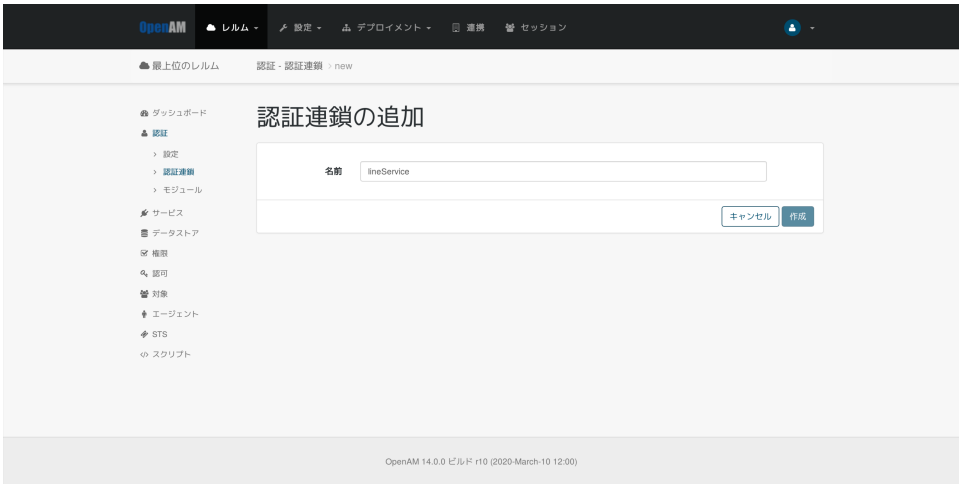

図 14　認証連鎖の作成

認証連鎖が作成されたので、認証モジュールを追加します。 前段に Data Store 認証モジュールを追加するので「モジュールの追加」を選択後、「モジュールの選択」から「Data Store」を選択します。「基準の選択」についてはここでは「Requisite」とします。

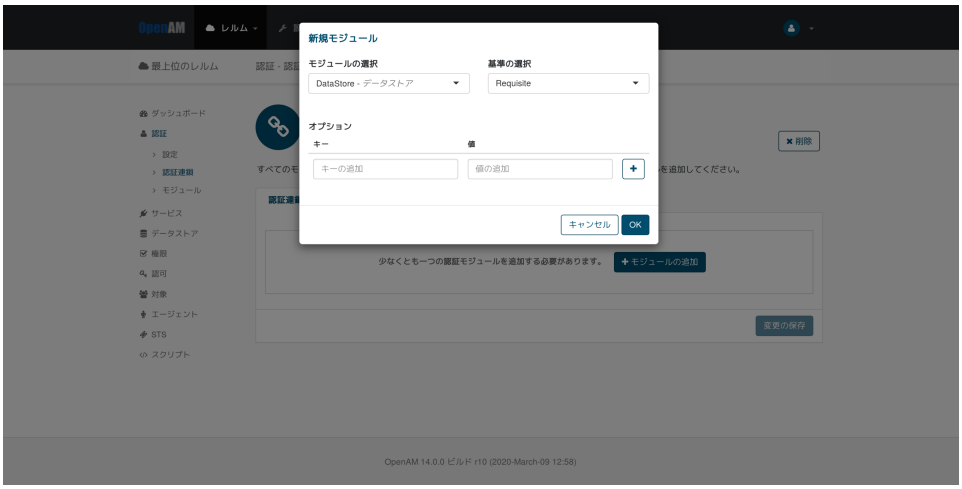

図 15　Data Store 認証モジュールを追加

「OK」を選択してください。Data Store 認証モジュールが認証連鎖に追加されます。 次に LINE OTP 認証モジュールを追加します。再度「モジュールの追加」を選択し、モジュールの追加とモジュールの設定の節で設定した LINE OTP 認証モジュール (下図では “LINE”) を選択します。「基準の選択」についてはここでは「Required」とします。

図 16　LineOTP 認証モジュールを追加

「OK」を選択します。これで認証連鎖下図のように設定されます。

図 17　認証連鎖

最後に認証設定で今回作成した認証連鎖を指定します。「認証」→「設定」を選択し、「組織認証設定」から作成した認証連鎖 (下図では “lineService”) を選択してください。

図 18　LINE 認証連鎖を指定

「変更の保存」を選択することで、次回以降の認証から設定した認証連鎖による認証が有効になります。

6 認証操作

ここではユーザによる認証操作について説明します。 LINE OTP 認証モジュールは初回時と 2 回目以降で認証操作が変わります。 初回時は LINE サービス利用の承認操作が必要になります。なお認証連鎖は認証連鎖の設定の節で設定したとおり、Data Store 認証モジュール→ LINE OTP 認証モジュールの 2 段階の認証を指定しています。

6.1 初回時

認証開始画面です。設定通り Data Store 認証モジュールの画面になります。

図 19　認証開始画面

ユーザ ID とパスワードを入力して「ログイン」を選択すると、LINE サイトへの転送確認画面になります。内容を確認したら「確認」を選択します。

図 20　LINE サイトへの転送確認

LINE サイトへ転送されて、 LINE ログイン画面が表示されるので通知先となるユーザの LINE アカウントのメールアドレスとパスワードを入力してログインします。

図 21　LINE ログイン

LINE Notify サービス連携の同意画面になるのでトークルームを「1:1 で LINE Notify から通知を受け取る」を選択して、「同意して連携する」を選択します。

図 22　LINE Notify サービス連携の同意

再び OpenAM に転送されて、OTP コード入力画面になります。 ここで「OTP コードを送信」を選択すると、 先程ログインした LINE アカウント宛に OTP コードが送信されます。

図 23　OTP コード入力

受信した OTP コードを入力して「ログイン」するとログインに成功します。

6.2 2 回目以降

認証開始画面です。初回時同様に Data Store 認証モジュールの画面になります。

図 24　認証開始画面

ユーザ ID とパスワードを入力して「ログイン」を選択すると、OTP コード入力画面になります。 ここで「OTP コードを送信」を選択すると、初回時にログインした LINE アカウント宛に OTP コードが送信されます。

図 25　OTP コード入力

受信した OTP コードを入力して「ログイン」するとログインに成功します。

7 変更履歴

- 2020 年 3 月 12 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