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	र	
1	要旨	1
2 2.1 2.2	システム構成/前提条件 システム構成	2 2 3
3 3.1 3.2	LINE Notify サービスの利用登録 サービス利用登録 Callback URL の設定	4 4 6
4 4.1	ユーザデータストア ユーザーデータストアの設定を変更する	8 8
5 5.1 5.2	モジュールを認証連鎖に追加する モジュールの追加とモジュールの設定................ 認証連鎖の設定	9 9 12
6 6.1 6.2	認証操作 初回時	16 16 18
7	変更履歴	20



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。

OSSTech

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 <u>LINE</u> 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。

サービス提供者様へ	
LINE Notifyと連携を行うことで、LINEユーザーが簡単にサービスの通知を受f	言できるようになります。
サービスを登録する >	
LINE Notify API Document >	
● LINEで送る	
プライバシーポリシー – ヘルプ – お問い合わせ	日本語 ^
© LINE Corporation	

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。



LINE	
メールアドレス	?
パスワード	
ログイン	
LINEについて © LINE Corporation	

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。

LINE Notify		6091 ~
サービス? LINE Notifyと連携する	を登録する るには、下記の項目を入力しメール認証を完了してください。	
サービスロゴ		
サービス名・		
サービス概要 •		
サービスURL・		

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。

LINE Notify		6091 ~
Myサービ ^{Client ID} Client Secret	ス また また 数示 リセット また の ます。	
Users	0	
サービスロゴ https://colly-bot_line.me/my/s	ervices/edit/celentid=EKF9Cy/R/m08vFLJLlb3go	

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。

サービス概要・	サービス試用
サービスURL •	https://www.osstech.co.jp/
企業/事業者名•	オープンソース・ソリューション・テクノロジ株式会社
担当者名 •	
メールアドレス・	and the second
Callback URL •	http://www.sample.com:8080/openam http://www.sample.com:8080/openam/Ul/Login
	e改行することで、Calibaok URLを5つまで登録できます。
	• 必須
更新す	る 削除する

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。

レルム 対象もよび設定データを整理するためにしルムを使用します。各レルム内では、データストア、管理権限、認証連編、認可ポリシー、およびその他のレルム既有の設定を行うことが
● 新聞したム 田 ■
またでは、 auth-test example co.jp ? nove のアクティブ
DeenAM 14 00 12 /105 /10 /2003/March-00 12 580

図8 レルムの選択

OpenAM 🏊 レルム	▼ ♪ 設定 ▼ 品 デプロイメント	▼ 目 連携 曾 セッショ		
▲ 最上位のレルム	認証 - モジュール			
 ● ダッシュボード ● 第三 > 第2 > 第2 > 第2 > 第230 ダ ワービス ● データストア 2 極限 4 第四 4 第四 4 第四 4 第四 4 第一 5 第5 (75) <li< th=""><th> 認証モジュール OpenAM IA. ユーザーを選加するために認知 ユーザーを提加するために使用されるデンタ は、期間するために使用されるデンタ ま、期間するために使用されるデンタ ま、期間するために使用されるデンタ ま、期間 モジュールを DataSlore Federation HOTP LDAP OATH </th><th>モジュールを使用します。還常、1 いトの認識運動があります。このセ タイプ データストア 道路 HOTP LDAP OATH</th><th>旅歴モジュールは旅歴漫画と間違付けられて クジョンは、レルムへの旅艇に使用可能な 実成漫画 IdapService</th><th>COURT 9、各レルムには、 認証モジュールを通知、設</th></li<>	 認証モジュール OpenAM IA. ユーザーを選加するために認知 ユーザーを提加するために使用されるデンタ は、期間するために使用されるデンタ ま、期間するために使用されるデンタ ま、期間するために使用されるデンタ ま、期間 モジュールを DataSlore Federation HOTP LDAP OATH 	モジュールを使用します。還常、1 いトの認識運動があります。このセ タイプ データストア 道路 HOTP LDAP OATH	旅歴モジュールは旅歴漫画と間違付けられて クジョンは、レルムへの旅艇に使用可能な 実成漫画 IdapService	COURT 9、各レルムには、 認証モジュールを通知、設
	OpenLDAP	OpenLDAP		# ×
	© SAE	SAE		1 ×

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。

סעע אעע איז	▶ 設定 - 击 デブロイメント - □ 連携 替 セッション	a •
▲ 最上位のレルム	電証 - モジュール > new	
 ▲ 認知 ▲ 認知 > 認定 > 認定通知 > モジュール ダ リービス ● デタストア ※ 植物 	新規モジュールの作成	・ (手やンセル) 作成
4、前町 營 括数 ∲ エージェント ∲ 5TS の スクリプト		
	OpenAM 14.0.0 ピルド r10 (2020-March-09 12:58)	

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。

OpenAM	▲ レルム × チ 設定 × 击 デプロイメント ×	目 連携 曽 セッション	▲ •
▲ 最上位のレル	レム 認証 - モジュール > lineotp > LINE		
● ダッシュボード ▲ 認証 > 設定			
> 認証連鎖 > モジュール ✔ サービス 書 データストア	認証レベル LINE既証API共選URL	0 https://notlly-bot.line.me/	0
G 権限 4、認可 譬 対象	LINE遗知API共遭URL Client ID	https://notify-api.line.me/) o
≢ エージェント 伊 STS Φ スクリプト	Client Secret アクセストークン属性名	lineToken]] o
	APIリードタイムアウト(ミリ参) APIリードタイムアウト(ミリ参) ワンタイムパスワードの有効期間(分)	5000 5]] 0
	ワンタイムパスワードの長さ	8 -	0

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。



LINE Notify		小田切耕司
OSSTecl	1	
Client ID	Second and the second	
Client Secret	表示 リセット	
Users	1	
サービスロゴ		
サービス名・	OSSTech	

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、<u>必ず LINE OTP 認証モジュールの前に OpenAM の ID</u> 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。

OpenAM 🍝 v.v.	ム・ チ 設定 ・ 击 デプロイメント ・ 目 連携 曽 セッション	
▲ 最上位のレルム	認証 - 認証連鎖	
 会 ダッシュボード 歳 第22 第23 モジュール ダ リービス データストア ダ 相限 4 第5 	 RE工業員会 Maxe #WE 生業者 きるために、 繊維連絡を使用してください。 線延達制は連絡 する1つ以上の 郷廷モジュールで構成: Maxeのモジュールインスタンスに受け進がれます。 Maxe #WE #WE #WE #WE #WE #WE #WE #WE #WE #WE	され、資格情報は認証連
 登 対象 す エージェント ∲ STS Φ スクリプト 		

 \bigcirc

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。

<mark>OpenAM</mark> 📥 UILA -	▼ ▶ 設定 - 本 デプロイメント - 『] 連携 督 セッション		
▲ 最上位のレルム	認証 - 認証連鎖 > new			
 タッシュボード 総証 	認証連鎖の追加			
> 認定 > 認定連續 > モジュール	名前 lineService			
∲ サービス 書 データストア			キャンセル	
87 権限 44 医可				
響 対象 ∳ エージェント ∲ STS				
ゆ スクリプト				
	OpenAM 14.0.0 E	Jレド r10 (2020-March-10 12:00)		

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。

OSSTech

OpenAM 🍝 UNI	A → → B	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 DataStore - データストア	基準の選択 Requisite マ	
 ● グリジュボード ● 設定 >> 設定 >> 設定 >> 設定 >> 認定 ● 設定 >> 認定 ● 設定 >> 認定 ● 認定 ● ジェール Ø ジェール Ø ジェール Ø ジェール ● ジェール ●	54004 54004 1000	オブション キー 値 年一の泊加 「 少なくとも一つの服匪モジ	aの必加 (まャンセル) (* ユールを追加する必要があります。 (+ モン	 11日本 <
		OpenAM 14.0.0 년ルド r	10 (2020-March-09 12:58)	

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。

C	DDENAM • DRA	- × 18	新規モジュール		(<u>a</u>) -
4	▶最上位のレルム	izie - izi	モジュールの選択	基準の選択	
			LINE - LINE OTP	Hequired	
a	∎ ダッシュボード	0			
4	a iziz	6	オブジョン キー 値		× HIR
	> 設定	-			
	> 認証連續 > デジュール	9~200-	+-03800	•	
	/ 0/1-//	認証連集			
	F リービス F データストア			キャンセル OK	
-	2 植限	+ E5	_	_	ること。 😰 失敗フラグがないこと。
a	、 認可	1			
	1 对象		DataStore		+ / ×
4	エージェント		データストア		
4	∲ STS		Requisite		オプション (0)
		+	×		
			認証が成功するには次が必要です: 0	●少なくとも1つの成功フラグがあること。	(二) 矢坂フラクかないこと。

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。

ダ ワービス 第 テークストア 皮 細胞 ④ 頭肉 ● ガジ ● オニージェント ● STS ゆ スクリプト ● スクリプト ● 工ージェント ● STS ゆ スクリプト ● Call Call And		r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
■ F	 データストア ● モジュールの波旋 認証が成功す ペ 認可 1 	†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
W HII 9, 301 9 398 1, 1 - 91 201- # STS 0, 20197- Max 0 20197- 1 0 2 1	受権限	
4 BFT	a, 201 (1	
		+ & ×
	量対象 テーロストロ	
• als		
2 4 4 4 2 2 1 1 1 1 2 1 1 1 1 2 1 1 1 1 2 1 1 1 1 2 1 1 1 1 2 1 1 1 1	(P Z 2 U Z 1-	0 VEVER
	朱故	D 成功 💌
((()) ()) ())) ()) ()) ())) ())) ())) ()))) ())) ()))) ())) ())))) ()))) ())))) ())))) ())))))))) ())))))))))))))))))))		
CIP LINE OTP LINE OTP Required の オブション ()) 代記 ()	2	+ # *
Line OIP Required の オブジョン () 代記 ()		
	Required	オプション 0
	失敗 🕻	🗅 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。	認証が成功するには次が過	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。

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。

סעט 🍝 ראע א	▼ ▶ 設定 ▼ 赤 デプロイメント ▼ □	連携 曽 セッション	
▲ 最上位のレルム	認証 - 設定		
 ● ダッシュボード ■ 原田 > NUE 	認証設定 ユーザーブロファイル アカウン	トロック 一般 ゼキュリティ ポスト際証プロ	セス
→ 除品連載的 → モジュール ダ サービス 豊 データストア	管理者認証設定 組織認証設定	IdapService	• 0 • 0
図 極祖 4 認可 2 対象 ∳ エージェント			元に関す 変更の保存
∲ STS ゆ スクリプト			
	OpenAM 14.0.0 ビ	レド r10 (2020-March-10 12:00)	

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。

0SSTech
OPENAM へのサインイン
test1
••••••
- ユーザー名を記憶する。
ログイン

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。

OSSTec	h
	0SSTech
	- Africa 192
	ここから先はLINEのサイトに遷移します。問題ない場合は下の"確認"ポタンを押してくだ さい。
	詳細について知りたい場合は以下のリンク先を参照してください。 About LINE Authentication
	確認

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。



E Notify		小田切耕司 ~
	OSSTech オープンソース・ソリューション・テクノロジ株式会 社	
	通知を送信するトークルームを選択してください	
	1:1でLINE Notifyから通知を受け取る	

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。

OSS Tech				
あなたのLINEに通知されたOTPコードを入力してください				
OTPK				
ロダイン				
OTPコードを送信				

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。

OSSTech		
	055Tech	
	OPENAM へのサインイン	
	test1	
	•••••	
	□ ユーザー名を記憶する。	
	ログイン	

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。

055Tech
あなたのLINEに通知されたOTPコードを入力してください
OTP⊐-H
ログイン
OTPコードを送信

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