## OpenAM 14 SMS OTP 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	12	

# 目次

1	はじめに	1
2	システム構成	2
3	事前準備	3
3.1	Amazon SNS へのアクセス設定 ..........................	3
3.2	Amazon Simple Notification Service の利用上限コストの設定	3
3.3	属性とユーザーデータストアの設定.......................	3
4	認証モジュールと認証連鎖の設定	5
4.1	認証モジュールの追加	5
4.2	認証連鎖の設定	8
5	仕様 / 注意事項	11
5.1	OTP 送信回数	11
5.2	送信先電話番号	11
5.3	送信するメッセージの長さ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	12
5.4	AWS 利用上限	12
5.5	監査ログ	12
6	認証時の操作	14
7	備考	18
7.1	メッセージの配信統計	18



## 1 はじめに

本文書は、OSSTech 版 OpenAM14 に含まれる SMS OTP 認証モジュールの利用手順書です。



## 2 システム構成

SMS OTP 認証モジュールのシステム構成について説明します。



図1 システム構成

ユーザーが OpenAM にアクセスし、端末で ID / パスワード認証を行った後 OTP を要求 します。 OpenAM が Amazon Web Services を利用してユーザーの携帯端末に SMS で OTP メッセージを送信します。ユーザーは受信した OTP コードを OpenAM の認証画面に入力 して認証を行います。



### 3 事前準備

SMS OTP 認証モジュールを使用するためには、以下の事前準備が必要です。

- Amazon SNS へのアクセス設定
- Amazon Simple Notification Service の利用上限コストの設定
- OpenAM の初期設定
- 認証で利用する属性とユーザーデータストアの設定

### 3.1 Amazon SNS へのアクセス設定

Amazon SNS へのアクセスをセットアップする (https://docs.aws.amazon.com/ja\_jp/sns/latest/dg/snssetting-up.html) を参照して AWS アカウントの作成及びユーザーの作成、Amazon SNS 用 のアクセスキーの取得を行ってください。「認証モジュールの追加」でアクセスキーのアク セスキー ID とシークレットアクセスキーが必要になりますので、控えておいてください。

### 3.2 Amazon Simple Notification Service の利用上限コス トの設定

Amazon SNS では、SMS のメッセージ送信にかかるコストに上限を設けています。 デ フォルトでは 1.00 USD / 月に設定されています。設定された上限コストに利用コストが 達すとメッセージの送信ができなくなりますので、デフォルトの上限コストを超える可能 性のある場合には Amazon SNS で SMS メッセージの引き上げをリクエストするにはどう すればよいですか?(https://aws.amazon.com/jp/premiumsupport/knowledge-center/sns-smsspending-limit-increase/)を参照して利用上限コストの引き上げを行ってください。

### 3.3 属性とユーザーデータストアの設定

SMS OTP 認証モジュールでは OTP コードの送信回数をユーザーごとに管理するため、 ユーザーデータストアのカウンタ属性に各ユーザーの送信日時と送信回数を保存します。カ ウンタ属性には任意の属性を指定することができますが、JSON 文字列を格納できる属性に 限ります。 OpenAM では、SMS OTP 認証モジュールのカウンタ属性用に OpenLDAP 用ス キーマファイル sms.schema を提供しています。 ここでは sms.schema を利用する場合の設 定方法を説明します。



#### 3.3.1 スキーマの有効化

- 1. /opt/osstech/etc/openldap/schema/以下にスキーマファイルを配置します。
- 2. /opt/osstech/etc/open1dap/slapd.conf に下記の定義を追加します。

include /opt/osstech/etc/openldap/schema/sms.schema

3. OpenLDAP を再起動します。

# systemctl restart osstech-slapd

#### 3.3.2 ユーザーデータストアの設定

sms.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.「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 am-auth-sms-otp-service、「LDAP ユー ザー属性」に am-auth-sms-otp-counter を追加して「保存」を押下します。



### 4 認証モジュールと認証連鎖の設定

ここでは、SMS OTP 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。

### 4.1 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」に任意のモジュール名 (ここでは SMS) を入力し、「種類」のドロップダウンリ ストから SMS OTP を選択します。

OpenAM 🌢 UNL	・ チ酸定・ 山	デプロイメント 🗸 🔋 連携	誉 セッション		•
▲ 最上位のレルム	認証 - モジュール > nev	v			
<ul><li>● ダッシュボード</li><li>▲ 認証</li></ul>	新規モジ	ュールの作成	,		
> 設定 > 認証連鎖 > モジュール ● サービス	名前	SMS SMS OTP			
■ データストア 図 権限				キャンセル	,作成
<ul> <li>4, 認可</li> <li>営 対象</li> <li>オ ニージェント</li> <li>∲ STS</li> <li>か スクリプト</li> </ul>					

#### 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遷移します。

0SSTe	ch		
<ul> <li>● ダッシュボー</li> <li>▲ 認証</li> <li>&gt; 設定</li> </ul>	SMS OTP		
> 1881世現 > モジュー ★ サービス	ル 酸亜レベル	0	
■ データスト: 2 梅限 Q 藤町	ッ アクセスキー ID シークレットアクセスキー		
譬 対象 ● エージェン1 ∲ STS	リージョン 国名コード属性	ap-northeast-1	0
ゆ スクリプト	テフォルトの国名コード 電話番号属性	JP telephoneNumber	0
	IState ID SMS のタイプ カウン伝言称	Transactional	- 0
	ディン・4日上 最大 OTP 送信回数 ワンタイムパスワードの有効調酬(分)	5 5	0 0
	ワンタイムパスワードの長さ OTP コードの自動送信	8	· 0
	最大照合回数 監査ログ	3	0
			元に戻す 変更の保存

図3 モジュールの設定

- 5. 各項目に設定を入力し、「変更の保存」を押下します。 各項目の詳細は以下の通りです。
  - 認証レベル
    - 認証成功時にセットされる認証レベルを指定します。
  - ・アクセスキー ID
    - -「事前準備」で取得したアクセスキーのアクセスキー ID を入力します。
  - シークレットアクセスキー
    - -「事前準備」で取得したアクセスキーのシークレットアクセスキーを入力し ます。
  - ・リージョン
    - AWS のリージョンを指定します。
    - 利用可能なリージョンについては、サポートされているリージョンおよび国(https://docs.aws.amazon.com/ja\_jp/sns/latest/dg/sns-supported-regions-countries.html)を参照してください。
    - 指定されていない場合はデフォルト値の ap-northeast-1 が使用されます。
  - 国名コード属性
    - ISO 3166-1 で規定されているアルファベット2文字の国名コードを属性値 に持つ属性を指定します。



- デフォルトの国名コード
  - ISO 3166-1 で規定されているアルファベット 2 文字の国名コードで国名 コードを指定します。
- 電話番号属性
  - ユーザーの携帯電話番号を属性値に持つ属性を指定します。
  - 指定されていない場合はデフォルト値の telephoneNumber が使用されます。
- 送信者 ID
  - SMS でメッセージを受信した際に送信者として表示される文字列です。
  - スペースを含まない1文字以上11文字以内の半角英数字で構成する必要が あります。
  - 指定されていない場合はデフォルト値の OpenAM が使用されます。
- SMS のタイプ
  - SMS のタイプを Promotional または Transactional から選択します。
  - OTP の送信には Transactional が推奨されています。
- カウンタ属性
  - -「事前準備」で設定したカウンタ属性を指定します。
- 最大 OTP 送信回数
  - ユーザーが1日に受信することのできる OTP メッセージの最大数を指定します。
- ワンタイムパスワードの有効期間(分)
  - ワンタイムパスワードの有効期間を指定します。
- ワンタイムパスワードの長さ
  - 送信されるワンタイムパスワードの長さを6桁または8桁から選択します。
- OTP コードの自動送信
  - 認証時に OTP コードを自動で送信するかどうかを選択します。
- 最大照合回数
  - 認証時に入力された OTP コードを照合する最大回数を指定します。
- 監査ログ

- OTP コード送信後、監査ログに送信記録を出力するかどうかを指定します。 以下が設定例です。

【項目名】

【設定例】

認証レベル

0

【項目名】	【設定例】
アクセスキー ID	AKIAIOSFODNN7EXAMPLE
シークレットアクセスキー	jbfhf9 jhmHzTQZJiElGPAkLPgck5rTkuExample
リージョン	ap-northeast-1
国名コード属性	(空欄)
デフォルトの国名コード	JP
電話番号属性	telephoneNumber
送信者 ID	OSSTech
SMS のタイプ	Transactional
カウンタ属性	am-auth-sms-otp-counter
最大 OTP 送信回数	5
ワンタイムパスワードの有効期間 (分)	5
ワンタイムパスワードの長さ	8
OTP コードの自動送信	無効
最大照合回数	3
監査ログ	有効

### 4.2 認証連鎖の設定

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 smsService) を入力し、「作成」を押下します。

055	Tec	ih	
	OpenAM 🔺 U	レム 🗸 チ 設定 🖌 ボデブロイメント 🔹 道携 🍯 セッション	<ul> <li>•</li> </ul>
	▲ 最上位のレルム	認証 - 認証達與 > new	
	<b>ぬ</b> ダッシュボード	認証連鎖の追加	
	▲ 認証 > 設定 > 認証連鎖 > モジュール	名前 smsService	
	∲ サービス		キャンセル 作成
	言 データストア 19 権限		
	4. 認可		
	雪 対版 ● エージェント		
	# STS		
	い スクリプト		

図4 認証連鎖の作成

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。

OpenAM 🌢 Dul - 🗡	設定 ▼ 山 デプロイメント ▼ □ 連携  替 1		
▲ 最上位のレルム 認証 - 認	証連鎖 > smsService		
<ul> <li>● ダッシュボード</li> <li>● 認定 <ul> <li>&gt; 設定</li> <li>&gt; 設定</li> <li>&gt; 受ジュルル</li> <li>ダ サービス</li> <li>ビ データストア</li> <li>ビ 情限</li> <li>ヘ 誤可</li> <li>営 対象</li> <li>キ ニージェント</li> <li>※ STS</li> <li>の スクリプト</li> </ul></li></ul>	SEE 要用 SEE #  SmasService  Eジュールインスタンスにユーゲーの資格情報を選すプロセス  (の)  E  D  C  C  C  C  C  C  C  C  C  C  C  C	を構築するように、認証モジュールを通加してください。 ● 少なくとも1つの成功フラグがあること。 ● 大阪フラグが ★ ↓ オプション 成功 ● は1つの成功フラグがあること。 ● 大阪フラグがないこと。	

図 5 データストア認証モジュールの追加

5. 4. と同様にして「モジュールの選択」で SMS を選択し、「基準の選択」で Required を選択します。

OpenAM 🌢 UNG -	▶ 設定 ▼ 山 デプロイメント ▼ □ 連携 曽		•
▲ 最上位のレルム	8証 - 認証連鎖 > smsService		
<ul> <li>● ダッシュボード</li> <li>▲ 認証</li> <li>&gt; 設定</li> <li>&gt; 認正</li> <li>&gt; モジュール</li> <li>● サービス</li> </ul>	部正連載           SmsService           されてのモジュールインスタンスにユーザーの資格情報を渡すプロセ           原匠連載の編集         設定	× えを構築するように、認証モジュールを追加してください。	• MURR
<ul> <li>データストア</li> <li>2 権限</li> <li>4 取</li> <li>4 取</li> <li>4 対象</li> <li>              エージェント</li></ul>	<ul> <li>◆モジュールの追加 認証が成功するには次が必要です:</li> <li>1</li> <li>○ DataStore データストア</li> <li>Requisite</li> </ul>	●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・ + メ × オブション ◎	ε <b>ε.</b>
ゆ スクリプト	\$\$ <b>\$</b>	成功 💌	
	SMS SMS SMS OTP	+ / × オプション ()	
	失敗 〇	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。 <b>〇</b> 朱阪フラグがないこと。 変更の	保存

図 6 SMS OTP 認証モジュールの追加

6.「変更の保存」を押下します。

7.「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 smsService を選択し、「変更の保存」を押下します。

נאנע 🍝 <mark>OpenAM</mark>	✔ ▶ 設定 ▼ 山 デプロイメント ▼	① 連携  著 セッション	۰ -
▲ 最上位のレルム	認証 - 設定		
金 ダッシュボード ▲ 認証	認証設定		
> 設定 > 認証連鎖	<b>コア</b> ユーザープロファイル アカ・	ウントロック 一般 セキュリティ ポスト員	8証プロセス
→ モジュール # サービス	管理者認証股定組織認証股定	IdapService	· 0
<ul> <li>データストア</li> <li>図 権限</li> <li>0 期期</li> </ul>			元に戻す 参更の保存
≪ 回川 · · · · · · · · · · · · · · · · · · ·			
♥ エージェント			

図7 設定



### 5 仕様 / 注意事項

ここでは SMS OTP 認証モジュールの仕様と利用上の注意事項について説明します。

#### 5.1 OTP 送信回数

OTPの最終送信日時と送信回数が「カウンタ属性」に保存されます。記録される送信日時 はサーバーの設定に依存します。送信回数はユーザーごとにカウントされ、日付が変わると リセットされます。

#### 5.2 送信先電話番号

AWS で SMS メッセージを送信するためには、ITU-T が勧告した E.164 フォーマットの携 帯電話番号が必要です。送信先電話番号は、以下のように生成されます。

- ユーザーの電話番号属性値が+から始まる場合は国番号付きの電話番号として扱われ、「国名コード属性」と「デフォルトの国名コード」の設定は無効となります。
- ユーザーの電話番号属性値が + から始まらず、ユーザーが「国名コード属性」に指定 された属性を持っている場合はその属性値が国名コードとして使用され、国番号付き の電話番号が生成されます。
- ユーザーの電話番号属性値が + から始まらず、「国名コード属性」が指定されていない又はユーザーが「国名コード属性」に指定された属性を持っていない場合は、「デフォルトの国名コード」に指定された値が国名コードとして使用され、国番号付きの電話番号が生成されます。

		【デフォルトの国名		
【電話番号属性値】	【国名コード属性】	コード】	【送信先電話番号】	
+818012345678		GB	+818012345678	
+8108012345678		GB	+818012345678	
+81-80-1234-5678		GB	+818012345678	
+81 80 1234 5678		GB	+818012345678	
08012345678	US		+108012345678	
08012345678	US	GB	+108012345678	
08012345678		GB	+448012345678	

また、「電話番号属性」と「国名コード属性」として参照される属性値は1つです。その

OSS Tech

ため、属性値として複数の値が登録されている場合、どの値が利用されるかは保証されま せん。

#### 5.3 送信するメッセージの長さ

送信するメッセージが規定の長さを超える場合、分割して送信される又はメッセージの送 信に失敗する可能性があります。SMS メッセージの送信(https://docs.aws.amazon.com/ja\_jp/ sns/latest/dg/sms\_publish-to-phone.html)を参照してください。

#### 5.4 AWS 利用上限

利用コストが「事前準備」で設定した Amazon Simple Notification Service の利用上限コ ストに達すと SMS でのメッセージの送信ができなくなります。認証モジュールでは、利用 上限コストに達したことによるメッセージの送信失敗を検知することができません。

### 5.5 監査ログ

「認証モジュールの追加」で「監査ログ」の設定を有効にした場合は、/var/opt/osstech/lib/ tomcat/data/openam/openam/log/activity.csv に OTP コードの送信履歴が出力されま す。出力されない場合は、「設定」 「グローバルサービス」 「Audit Logging」に移動し、 「Audit logging」が有効になっているか確認してください。無効になっている場合は出力さ れません。

監査ログは以下のように出力されます。

```
"9575740d-9fd8-4fd9-b92c-65416df2b8f2-218","2020-06-11T12:58:53.457+09:00",
"AM-SMSOTP-SENT","9575740d-9fd8-4fd9-b92c-65416df2b8f2-216",
"id=test1,ou=user,dc=openam,dc=osstech,dc=co,dc=jp","[""a62081fd37ce14b001""]",
"id=dsameuser,ou=user,dc=openam,dc=osstech,dc=co,dc=jp","a62081fd37ce14b001",
"SEND","{""date"":""2020-06-07T14:13:58+09:00"",""numberOfTimes"":3}",
"{""date"":""2020-06-11T12:58:53+09:00"",""numberOfTimes"":1}",,,"SmsOTP","/"
```

主な項目と格納内容は以下の通りです。

#### 【項目】

timestamp 監査ログ出力日時 eventName イベント名 userId ユーザーの ID 【格納内容】

2020-06-11T12:58:53.457+09:00 AM-SMSOTP-SENT id=test1,ou=user, dc=openam,dc=osstech,dc=co,dc=jp



#### 【項目】

【項目】		【格納内容】
operation	操作	SEND
before	更新前のカウンタ属性	{"date":"2020-06-07T14:13:58+09:00",
		"numberOfTimes":3}
after	更新後のカウンタ属性	{"date":"2020-06-11T12:58:53+09:00",
		"numberOfTimes":1}
component	コンポーネント	SmsOTP
realm	レルム	/



### 6 認証時の操作

ここでは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. DataStore 認証の画面で ID とパスワードを入力し、「ログイン」を押下します。

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 8 データストア認証でログイン

3.「認証モジュールの追加」で設定した「OTP コードの自動送信」が無効になっている 場合は「OTP コードを送信」を押下し、OTP コードを要求します。

00	0SSTech					
	0SSTech					
	OTPコードを送信ボタンを押下するとSMSでOTPコードが通知されます					
	OTP-F					
	ログイン					
	OTPコードを送信					

図9 OTP コードの要求

4. OTP コードが送信されると画面が切り替わります。

<b>0</b> SSTech	
SMS で通知された OTP コードを入力してください	
OTP コードの送信可能回数はあと 4 回です。	
OTP⊐−ド	
ログイン	
OTPコードを送信	

図 10 OTP コード送信後

5. ユーザーの携帯端末に送信された OTP コードを確認します。



図 11 OTP コードの確認

6. SMS 認証画面の OTP コード入力欄に正しく入力し、「ログイン」を押下するとログインに成功します。



<b>OSS</b> Tech	
SMS で通知された OTP コードを入力してください	
OTP コードの送信可能回数はあと 4 回です。	
•••••	
ログイン	
OTPコードを送信	)

図 12 OTP コードの入力

ユーザープロフ 基本情報 パスワード	ァイル	
ユーザー名	test1	
名	КОЈІ	
姓	ODAGIRI	
電子メールアドレス		
携带電話		
		リゼット 更新

図 13 ログイン成功

### 7 備考

### 7.1 メッセージの配信統計

メッセージの配信統計を AWS コンソールで確認することができます。「サービス」 「Simple Notification Service」 「Mobile」 「テキストメッセージング(SMS)」に移動し、 上部のリージョン切り替え部分を「認証モジュールの追加」の「リージョン」に設定したも のに合わせてください。「認証モジュールの追加」で「SMS のタイプ」を Promotional に 設定した場合は「プロモーションテキストメッセージ」、Transactional に設定した場合は 「トランザクションテキストメッセージ」から確認できます。



### 8 改版履歴

- 2020年6月19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6月9日リビジョン1.2
  - ldap 再起動コマンドを systemctl に変更