OpenAM 認証連鎖分岐モジュール
利用手順書

OSSTech **株式会社**

更新日 2022 **年** 7 **月** 14 **日**
リビジョン 1.2

目次

1 はじめに

本文書は、OSSTech 版 OpenAM 14 に含まれる認証連鎖分岐モジュールの利用手順書です。

1.1 機能概要

認証連鎖分岐モジュールの機能について説明します。

本モジュールは OpenAM で複数の認証連鎖を設定し、ユーザーの属性値によって利用する認証連鎖を変えることが出来るモジュールです。これにより、ユーザーの属性値に従ってユーザーが行う認証方式をコントロールすることが可能となります。

1.1.1 認証連鎖

OpenAM は様々な認証機能を「認証モジュール」で提供しています。例えば ID/パスワードで認証を行う「データストア」、ワンタイムパスワード (OTP) で認証を行う「HOTP」があります。「認証連鎖」はこれらの認証モジュールを組み合わせてユーザーが行う認証を設定します。

「データストア」と「HOTP」を組み合わせた認証連鎖を設定すると、ユーザーが行う認証は “ID/パスワードによる認証” → “OTP による認証” という 2 段階の認証となります。

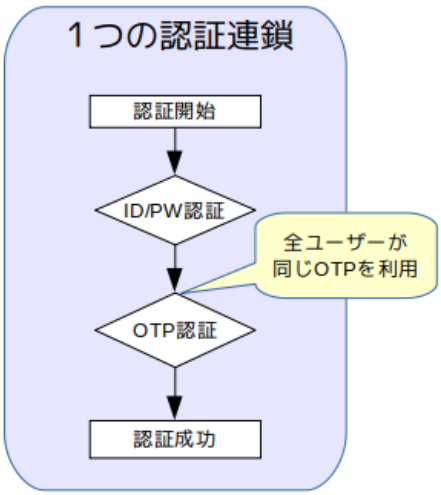

図 1　認証連鎖

一つの認証連鎖では全ユーザーが同じ認証を行うことになりますが、認証連鎖分岐モジュールを使うとユーザーの属性値によって、実行する認証連鎖を変えることができます。

1.1.2 利用イメージ

ユーザーが ID/パスワードの認証を行った後に実施する 2 要素目の認証方式を属性値から決定することが可能です。

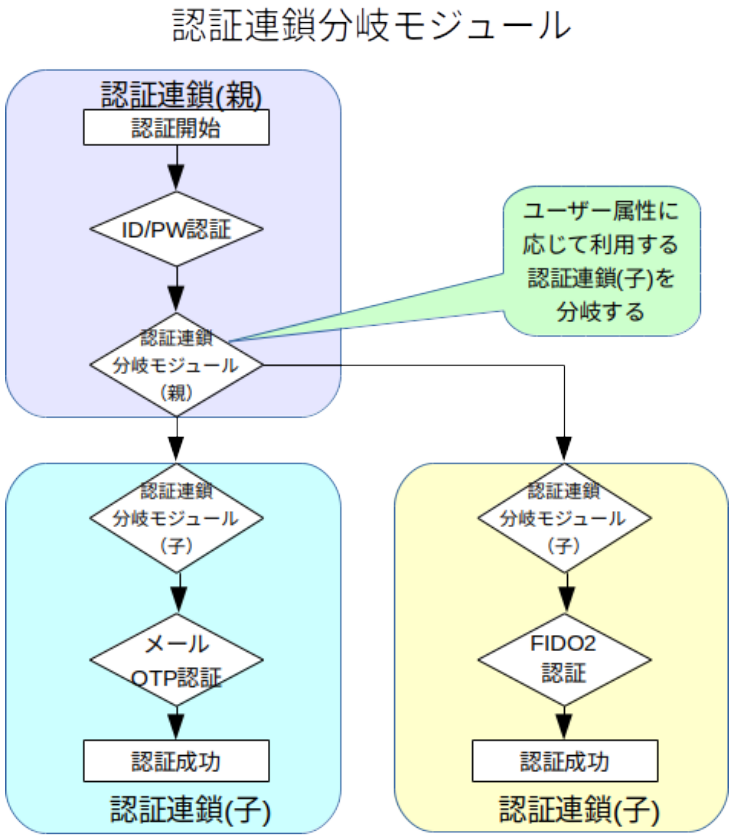

図 2　利用イメージ

- 表: ユーザーの属性値のマッピング例

【ユーザーの属性値】	【追加で行う認証方式】
HOTP	メールベースのワンタイムパスワード
OATH	Authenticator によるワンタイムパスワード
LINE	LINE によるワンタイムパスワード
WebAuthn	FIDO2 による認証
OK	なし (追加で認証を必要とせず、認証成功として扱う)

1.2 認証モジュールの構成

認証連鎖分岐モジュールは２つの認証モジュールで構成されます。

1. 認証連鎖分岐モジュール (親)
2. 認証連鎖分岐モジュール (子)

それぞれの認証モジュールについて説明します。

1.2.1 認証連鎖分岐モジュール (親)

ユーザーの属性値より実行する認証連鎖を判定するモジュールです。

- ユーザーの属性値に従い認証連鎖を呼び出します。
- 呼び出した認証連鎖の結果の認証レベルで認証成功とします。
- このモジュールの前にデータストア認証等の何らかの認証モジュールを用いてユーザーを特定済み (認証済み) であることが必要です。

1.2.2 認証連鎖分岐モジュール (子)

認証連鎖分岐モジュールから呼び出され、ユーザー名を取り出し後続の認証モジュールに渡すモジュールです。

- 「認証連鎖分岐モジュール (親)」で呼び出す認証連鎖の最初に組み込む認証モジュールとなります。

1.2.3 モジュールの構成図

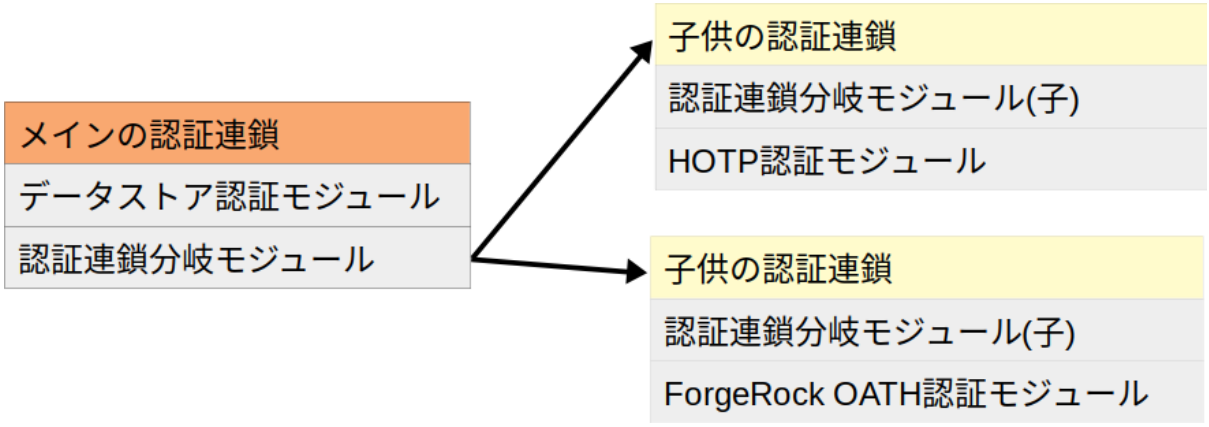

図 3　認証モジュール構成

本書では “認証連鎖分岐モジュール (親)” が動作する認証連鎖のことを「メインの認証連鎖」、認証連鎖分岐モジュールから呼び出される “認証連鎖分岐モジュール (子)” が含まれる認証連鎖のことを「子供の認証連鎖」と表記します。

2 導入

本章では認証連鎖分岐モジュールの導入方法を設定例を交えて説明します。これから示す設定例は、ユーザーの属性値で「HOTP 認証モジュール」か「ForgeRock Authenticator (OATH) モジュール」に 分岐される構成を設定します。前提として OpenAM サーバーでは以下の事前準備が必要です。

- OpenAM の初期設定が完了している
- 追加で実施したい認証方式の認証モジュールの設定が完了している
  - 「HOTP 認証モジュール」
  - 「ForgeRock Authenticator (OATH) モジュール」

2.1 ユーザー毎の挙動

これからユーザーの属性値に従って、下記図の動作となるような設定を行います。

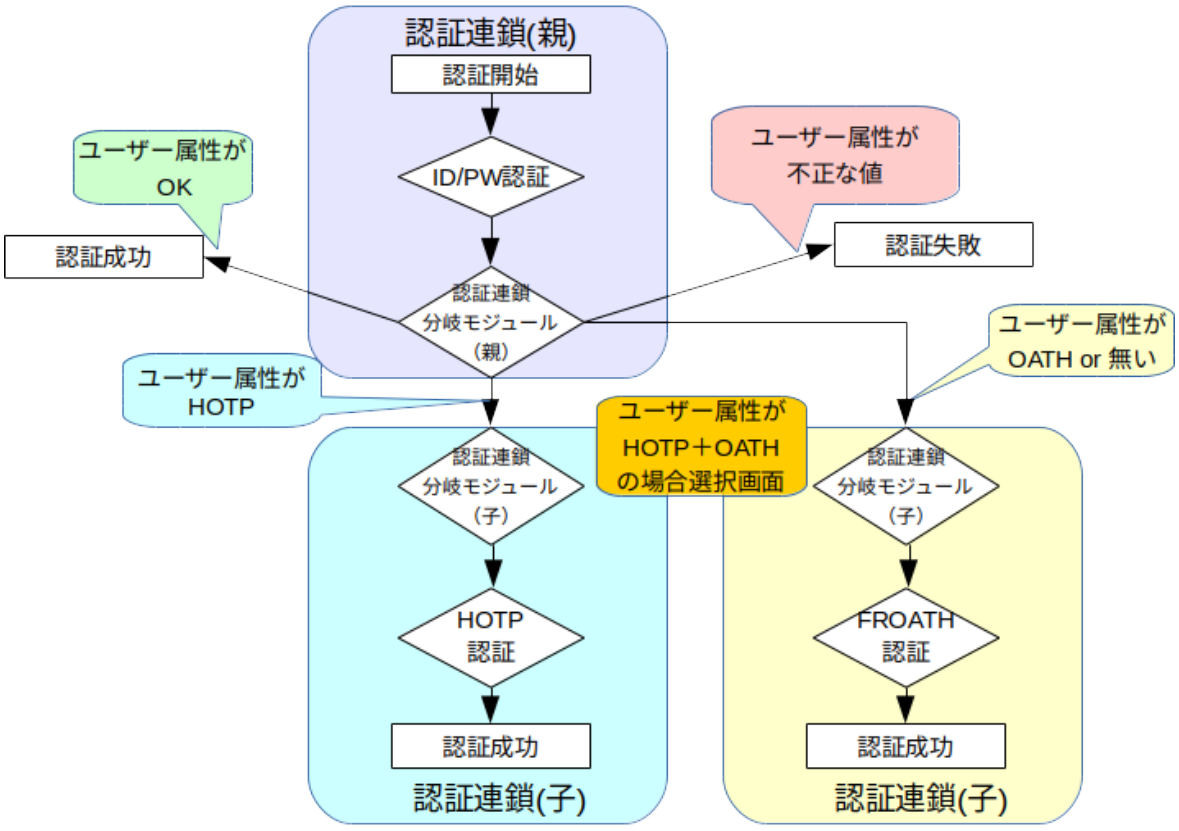

図 4　属性値に従った振る舞い

本書の通りに設定するとログインするユーザー名によって下記表の挙動となります。

【ユーザー名】	【動作】	【説明】
user01	HOTPService	認証連鎖 HOTPService が実行され、メールベースをワンタイムパスワード画面になります。
user02	OATHService	認証連鎖 OATHService が実行され、Authenticator を使ったワンタイムパスワード画面となります。
user03	認証成功	追加の認証連鎖を実行せず認証成功と扱われます。
user04	選択画面	属性値を複数持つユーザーで示すユーザーに選択させる画面となります。選択した方式の認証連鎖が実行されます。
user05	認証エラー	属性値が認証連鎖分岐モジュールの「属性値と認証連鎖のマップ」に設定されていない値のため認証エラーとなります。

2.2 ユーザーエントリ

OpenAM が参照する LDAP のエントリには以下のユーザーを作成します。
今回は description の属性値によってユーザーの認証方式を判定します。

- ユーザーのエントリ (関連する属性のみ記載)

```
dn: uid=user01,ou=people,dc=openam,dc=osstech,dc=co,dc=jp
uid: user01
description: HOTP

dn: uid=user02,ou=people,dc=openam,dc=osstech,dc=co,dc=jp
uid: user02

dn: uid=user03,ou=people,dc=openam,dc=osstech,dc=co,dc=jp
uid: user03
description: OK

dn: uid=user04,ou=people,dc=openam,dc=osstech,dc=co,dc=jp
uid: user04
description: HOTP
```

```
description: OATH
description: OK

dn: uid=user05,ou=people,dc=openam,dc=osstech,dc=co,dc=jp
uid: user05
description: notfound
```

2.2.1 データストアの属性設定

ユーザーの認証方式の判定に使用する属性は、データストアのユーザー属性設定に定義されている必要が有ります。OpenAM 管理コンソールで下記の設定を確認してください。

1. 対象レルム →「認証」 →「データストア」 → データストア名 を開きます。
2.「ユーザーの属性」の「現在の値」の一覧

一覧の中に認証方式の判定に使用する属性名が含まれていることが必要です。description の場合は、デフォルトでは存在しないためここに追加しておきます。

3.「新しい値」に “description” と入力し、「追加」を押す
4. 画面右上の「保存」を押す

2.3 作業の流れ

認証連鎖分岐モジュール (親) 設定時に「子供の認証連鎖」が作成されている必要が有ります。そのため以下の順序で設定を行います。

1. 認証モジュール「認証連鎖分岐モジュール (子)」を作成する
2. 準備する認証方式の数だけ「子供の認証連鎖」を作成する
3. 認証モジュール「認証連鎖分岐モジュール (親)」を作成する
4.「メインの認証連鎖」を作成する

2.4 認証連鎖分岐モジュール (子) を設定する

認証連鎖分岐モジュール (子) のインスタンスを作成します。

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 “authchainswitchchild” と入力し、「タイプ」は「認証連鎖分岐モ

ジュール (子)」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】
認証レベル	0

2.5 子供の認証連鎖を作成する

1. 対象レルム → 「認証」 → 「認証連鎖」を開きます。
2. 「認証連鎖の追加」ボタンをクリックします。
3. ここでは「認証連鎖」に「HOTPService」を入力し、「作成」ボタンをクリックします。
4. 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。
5. 「モジュールの選択」のプルダウンで「authchainswitchchild」を選択し、「基準の選択」は「Requisite」を選択して「OK」ボタンをクリックします。
6. 再度「モジュールの追加」ボタンをクリックします。
7. 「モジュールの選択」のプルダウンで「HOTP 認証モジュール」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。
8. 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。

同様の手順で認証方式の認証モジュールの数だけ子供の認証連鎖を作成します。本書では上記の他に ForgeRock Authenticator (OATH) を認証連鎖「OATHService」として作成します。

2.6 認証連鎖分岐モジュール (親) を設定する

認証連鎖分岐モジュール (親) のインスタンスを作成します。

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 “authchainswitch” と入力し、「タイプ」は「認証連鎖分岐モジュール (親)」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】	
認証連鎖を判定する値が入る属性名	description	
属性値と認証連鎖のマップ	キー: HOTP	値: HOTPService
	キー: OK	値: [Empty]
	キー: OATH	値: OATHService
属性が存在しない場合に動作する認証連鎖	OATHService	
セッションアップグレート時 [Empty] でも認証成功とする	無効	
Cookie 名	authchainswitchchoice	
Cookie の有効期限	30	
認証レベル	0	

2.7 メインの認証連鎖を作成する

1. 対象レルム → 「認証」 → 「認証連鎖」を開きます。
2. 「認証連鎖の追加」ボタンをクリックします。
3. ここでは「認証連鎖」に “authchainswitchService” を入力し、「作成」ボタンをクリックします。
4. 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。
5. 「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。
6. 再度「モジュールの追加」ボタンをクリックします。
7. 「モジュールの選択」のプルダウンで「authchainswitch」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。
8. 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。

以上で完了です。

2.8 動作確認

1. ブラウザで次の URL にアクセスします。

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

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 5　データストア認証

ユーザーエントリの各ユーザーでログインするとユーザー毎の挙動となります。

2.8.1 属性値を複数持つユーザー

「属性値と認証連鎖のマップ」で設定されている属性値を複数持つ場合は選択画面を表示します。user04 は「HOTP」「OATH」と 2 つの属性値を持つため、ID/パスワードを入力後は以下のような認証連鎖をユーザーに選択させる画面となります。

図 6　選択画面

リストの一覧から認証方式を選択し、「決定」を押すとその認証連鎖が実行されます。

選択した認証方式を `Cookie` に保存します。次に選択画面が表示された際は
前回選択した認証方式がデフォルトで選択された状態となります。

2.8.2 「属性値と認証連鎖のマップ」に無い属性を持つユーザー

「属性値と認証連鎖のマップ」に無い属性を持つユーザー (user05) は認証エラーとなります。ユーザーには下記のメッセージが表示されます。

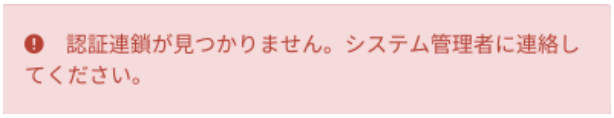

図 7　エラーメッセージ

「ユーザーの属性値」と「属性値と認証連鎖のマップ」の “キー” は大文字小文字を**区別します。**

ユーザーの属性値が複数値の場合は，一つでも「属性値と認証連鎖のマップ」に
定義されていない属性値が存在すると「認証エラー」となります。

2.8.3 ユーザーが実施した認証連鎖の取得

認証連鎖分岐モジュールは、実行した子供の認証連鎖をセッション属性にセットします。下記のセッション属性の値を参照することで、ユーザーが何の認証を行ったか取得することが出来ます。

【セッション属性名】
AuthChainSwitchService

本書の構成では、ユーザーは下記のセッション属性値がセットされます。

【ユーザー名】	【セッション属性値】
user01	HOTPService
user02	OATHService
user03	[Empty]

3 本番環境で使用する場合の留意点

3.1 レルムの構成

本モジュールを本番環境で使用する場合は、サブレルムで設定する構成にすることが推奨されます。

- /(トップレルム) は管理コンソールへのアクセス用とする
- サブレルムをサービス提供用のレルムとする（本認証モジュールを設定する）
- サブレルムでは認証連鎖分岐モジュールに関連する認証連鎖以外を削除する

OpenAM **はログイン** URL **に** Query String **で** service=[**認証連鎖**] **と指定することで**
任意の認証連鎖を動作させることが可能です。
そのため認証連鎖分岐モジュールに関連する認証連鎖以外を削除します。
service=[**子供の認証連鎖**] **としてログインを試みた場合は**
「認証連鎖分岐モジュール（子)」が認証エラーにします。

3.2 ワンタイムパスワードのパスワード失敗試行回数の設定

認証連鎖分岐モジュールを使った場合「子供の認証連鎖」で認証失敗すると「メインの認証連鎖」も失敗し、結果としてユーザーは ID/パスワード認証（メインの認証連鎖の最初から）からやり直しとなります。

「子供の認証連鎖」でワンタイムパスワードを入力する認証モジュールを使用した際、設定によっては 1 回のワンタイムパスワードの入力ミスで、ID/パスワードからのやり直しとなります。

「最大バリデーション試行回数」の設定項目が存在する認証モジュールではパスワードミスによる試行回数の設定が可能です。この設定が存在する認証モジュールでは設計してシステムに合った値を設定することを推奨します。

HOTP **認証モジュールの場合、初期値は** 1 **です。**
LINE **認証モジュールの場合、初期値は** 3 **です。**
ForgeRock Authenticator (OATH) **モジュールは設定変更できず、失敗試行回数は** 3 **回です。**

4 設定項目

本章では「認証連鎖分岐モジュール」の設定項目について説明します。

4.1 認証連鎖分岐モジュール

【項目名】	【必須】	【説明】
認証連鎖を判定する値が入る属性名	○	認証連鎖の判定に用いるユーザーの属性名を設定
属性値と認証連鎖のマップ	○	“キー” に [属性値]、“値” に認証連鎖を設定。認証連鎖に [Empty] と指定した場合は、認証連鎖を呼び出さずに認証成功となる。
属性が存在しない場合に動作する認証連鎖	○	ユーザーのエントリに属性が存在しない場合に動作する認証連鎖を設定。認証連鎖に [Empty] と指定した場合は、認証連鎖を呼び出さずに認証成功となる。
セッションアップグレード時 [Empty] でも認証成功とする	○	セッションアップグレード時に [Empty] の使用有無を設定
Cookie 名	-	選択画面で選んだ認証方式を保存する Cookie の名前を設定
Cookie の有効期限	○	保存する Cookie の有効期限を設定 (単位: 日)
認証レベル	○	認証が成功した際にセットされる認証レベル

4.1.1 選択画面のリスト内のメッセージについて

属性値を複数持つユーザーは選択画面が表示されます。選択画面のリスト内に表示される文言は properties ファイルで設定可能です。

properties ファイルは jar ファイル内に存在します。jar ファイルを展開し properties ファイルを取り出して編集し以下のディレクトリに配置してください。properties ファイルの編集方法は OpenAM の標準の方法と同等です。詳細は OpenAM 画面カスタマイズを参照してください。

- jar ファイル
  - /opt/osstech/share/tomcat/webapps/openam/WEB-INF/lib/authchainswitch-authentication-module-X.X.X.jar
- properties ファイル配置場所
  - /opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes
- properties ファイル名
  - amAuthAuthChainSwitch.properties
  - amAuthAuthChainSwitch_ja.properties

properties ファイルには「属性値」=「文言」の形式で定義します。初期値としては以下の属性値に対応した文言が登録されています。これらの値をユーザーの属性値に利用すると下記表の文言がリスト内に表示されます。

【属性値】	【表示される文言】
OK	追加の認証をしない
HOTP	登録メールアドレスにワンタイムパスワードを通知
DATASTORE	ID/パスワード
LDAP	ID/パスワード
LINE	LINE にワンタイムパスワードを通知
OATH	Authenticator のワンタイムパスワード

properties ファイルに「属性値」=「文言」が定義されていない場合は、選択画面内のリストには属性値がそのまま表示されます。

4.2 認証連鎖分岐モジュール (子)

【項目名】	【必須】	【説明】
認証レベル	○	認証が成功した際にセットされる認証レベル

5 制限事項

本章では「認証連鎖分岐モジュール」の制限事項について説明します。

5.1 新規レルム作成時のエラー

新規のレルム作成時に指定する親レルムに「認証連鎖分岐モジュール」が存在すると以下のエラーとなり正しくレルムが作成されません。

図 8　表示されるエラー

新しくレルムを作成する際の親レルムに「認証連鎖分岐モジュール」が存在する場合、一度「認証連鎖分岐モジュール」を削除してからレルムを作成してください。

6 改版履歴

- 2020 年 3 月 5 日 リビジョン 1.0
  - 初版作成
- 2020 年 8 月 7 日 リビジョン 1.1
  - 制限事項追加
- 2022 年 7 月 14 日 リビジョン 1.2
  - 表紙の社名を OSSTech 株式会社に変更