FUJITSU Hybrid IT Service FJcloud-O 認証サービス サービス仕様書

2020 年 6 月 11 日

1. サービス仕様

当社は、以下のサービスを提供します。

(1) 基本サービス

契約者が FUJITSU Hybrid IT Service FJcloud-O PaaS ポータルから認証サービスの利用を開始すると、管理テナント（注 1）が 1 つ作成されます。契約者は、管理テナントにより運用テナント（注 2）の管理を行うことができます。

① 基本機能

i. シングルサインオン機能

一度の認証で、連携する複数のシステムを利用可能にする機能を提供します。

ii. 業務サービス連携機能

（ア）OpenID 対応本サービスは OpenID Connect 1.0 に対応し、OpenID Provider (OP)として動作します。OpenID Connect 1.0 の Relying Party (RP)に対応した Web アプリケーションや外部クラウドサービスと連携することができます。

（イ）SAML2.0 対応

本サービスは SAML 2.0 に対応し、Identity Provider（IdP）として動作します。SAML 2.0 の Service Provider（SP）に対応した Web アプリケーションや外部クラウドサービスと連携することができます。

② 管理画面

下記の管理機能を提供します。

i. 利用者管理

（ア）利用者一覧

利用者一覧画面では以下の操作・情報確認が可能です。

・テナント情報の確認

認証方式ごとの最大 ID 数、登録 ID 数、残 ID 数の情報が確認できます。

・利用者検索

利用者 ID を検索することができます。

・出力結果

利用者検索の検索結果が出力されます。

本画面から利用者 ID の削除・設定変更を行うことができます。

（イ）利用者追加

利用者追加画面では利用者 ID を追加することができます。

ii. 各種設定

（ア）カスタマイズ

カスタマイズ画面では以下の操作が可能です。

・ログイン画面

ログイン画面のカスタマイズを行うことができます。

・セッション

セッション有効時間、1 人当たりの同時ログイン数を設定できます。

（イ）ドキュメント・ツール

本サービスに関するドキュメントやツールをダウンロードすることができます。

（ウ）アプリケーション登録

アプリケーション登録画面では連携アプリケーションを登録することができます。

iii. サービス内容

(ア) サービス内容確認

サービス内容確認画面では以下の操作が可能です。

・サービス内容

認証サービス ID および付加されているオプションを確認することができます。

・テナント作成

運用テナント追加画面に移動します。

・現在の利用状況

運用テナントの利用状況を確認し、削除・設定変更を行うことができます。

(イ) サービス内容変更

サービス内容変更画面では利用するオプションを選択し変更することができます。

(ウ) テナント追加

テナント追加画面では運用テナントを追加することができます。

iv. 認証設定

(ア) パスワードポリシー

入力規約(正規表現)、有効期限(日数)、ロックアウトされる連続認証失敗回数、ロックアウトの警告が表示される認証失敗回数、ロックアウト自動解除時間(秒)、パスワード世代管理数の設定が可能です。

(イ) ADFS 設定

・事前に本サービスに Active Directory の利用者 ID や業務サービスで取得する利用者情報を登録することにより、ADFS（ActiveDirectory Federation Services）と連携することができます。

・ADFS 連携を行う場合は、本サービスの以下の機能が無効となります。

- 本サービスでの認証（ID パスワード、ワンタイムパスワード、生体認証）
- アカウントの有効期間
- パスワードポリシーの設定
- IP アドレス制限

・ADFS 連携を利用するには、連携対象の ADFS サーバに連携用の設定を実施する必要があります。契約者は、自らの責任により当該設定を実施する必要があります。

・ADFS 連携を利用するには、ADFS 側のトークン署名証明書を本サービスが提供する証明書に置き換える必要があります。

(ウ) IP アドレス制限

認証を許可する IP アドレスを設定し、指定した IP アドレス以外からの管理画面や業務サービスへのアクセスを制限することができます。

v. 個人設定

個人設定画面では以下の操作が可能です。

(ア) 基本情報

利用者 ID 情報を確認および利用者のパスワードの変更ができます。

(イ) タイムゾーン

タイムゾーンを変更することができます。なお、タイムゾーンは、本サービスの管理画面内の時間表示および設定に適用されます。

(ウ) ワンタイムパスワード

ワンタイムパスワード認証方式が指定されている利用者のみ表示されます。また、ワンタイムパスワードのクライアントアプリケーションのセットアップ時に利用するワンタイムパスワード生成用のパスフレーズを確認することができます。

(エ) 生体認証

生体認証方式が指定されている利用者のみ表示されます。また、生体認証クライアントアプリケーションのセットアップ時に利用するパスワードを登録することができます。なお、生体要素としては手のひら静脈および指紋が利用可能であり、契約者は、生体センサーを別途準備する必要があります。

③ REST API

以下の機能について REST API で提供します。

i. 認証・ログアウト

ii. 利用者管理（利用者の取得・一覧取得・変更、一括追加・変更・削除、ロック一括解除）

iii. パスワードポリシー管理（パスワードポリシーの取得／変更）

iv. IP アドレスによる認証制御（IP アドレスによる認証制御情報の取得／変更）

v. 認証ログ取得（認証結果ログ・認証サービス REST API 操作ログ）

(2) オプション機能

① ワンタイムパスワード

i. ワンタイムパスワードに対応するクライアントアプリケーションで生成されるワンタイムパスワードを使用できる機能を提供します。

ii. 本サービスにおけるワンタイムパスワードとは、30 秒に一度自動生成され、次のパスワードが生成された時点で無効になるパスワードを指します。

iii. ワンタイムパスワードの利用には TOTP（Time-based One Time Password）準拠のクライアントアプリケーションが必要です。

※動作確認済推奨アプリケーション

スマートフォン対応：Google Authenticator

PC 対応：WinAuth

② 生体認証

i. 利用者の端末内で管理されている生体情報でログインを可能にする機能を提供します。

ii. 生体認証クライアントアプリケーションを本サービスの管理画面からダウンロード、インストールする必要があります。この際、契約者は、当該生体認証クライアントアプリケーションを、本サービスを利用するために必要な範囲でのみ使用するものとします。

2. 提供リージョン

本サービスは、以下のリージョンで提供されます。

・東日本リージョン 1

3. 制限事項・注意事項

(1) 本サービスを利用できるクライアント環境は以下のとおりです。

OS	Web ブラウザ
Windows 8.1, 10	Internet Explorer　11
iOS 10,11	Safari ※ただし、生体認証機能は未対応
Android 7,7.1	Google Chrome ※ただし、生体認証機能は未対応

※なお、動作保証がなされる OS は、ハードウェアの仕様に従います。

(2) 生体認証機能で利用できる生体認証センサーは以下のとおりです。

生体認証センサー (手のひら静脈)	・当社製端末に内蔵の手のひら静脈センサー ・PalmSecure-SL センサー ・PalmSecure-F Light センサー
生体認証センサー (指紋)	・当社製端末に内蔵の指紋センサー（Validity 指紋センサー搭載機のみ） ・指紋認識装置 FS-400U ・指紋認識装置 FS-410U

(3) 本サービスを利用するには、連携対象の Web アプリケーション、外部クラウドサービスなどに連携用の機能を実装する必要があります。契約者は、自らの責任により当該実装を実施する必要があります。

(4) 本サービスと連携する Web アプリケーションの実行環境については、本サービスからアクセス制限を実施することができません。連携対象 Web アプリケーションのセキュリティについては、契約者が単独で責任を負うものとします。

(5) 当社は、本サービスの認証性能について、いかなる保証も行いません。また、本サービスの認証性能は、利用者の通信環境やアクセスの集中などの影響を受けます。

(6) FUJITSU Hybrid IT Service FJcloud-O PaaS の HTTPS(TLS)仕様として、SSL/TLS 通信暗号化強度が高くない方式を使用する事が可能となっています。PaaS が提供する HTTPS に対するアクセスについて、新しいブラウザを使用するなどして、暗号化強度が高い方式で通信されるようにしてください。

注釈

注1. 「管理テナント」とは、１契約番号につき１つ作成される、本サービスを利用する単位を指します。

注2. 「運用テナント」とは、契約者が管理テナントにより作成する、業務サービス（Web アプリケーションや外部クラウドサービス）と連携する、本サービスを利用する単位を指します。運用者（注 3）および利用者（注 4）は、運用テナントごとに管理されます。

注3. 「運用者」とは、運用テナントに帰属し、運用テナントの運用者権限が設定されている担当者を指します。主に運用テナントの利用者を管理し、パスワードポリシーの変更や ADFS 設定などを行います。

注4. 「利用者」とは、運用テナントに帰属し、運用テナントと連携した Web アプリケーション、外部クラウドサービスを利用するユーザーを指します。

以　上

附則（2016 年 10 月 7 日）

本サービス仕様書は、2016 年 10 月 7 日から適用されます。

附則（2016 年 10 月 28 日）

本サービス仕様書は、2016 年 10 月 28 日から適用されます。

附則（2017 年 6 月 27 日）

本サービス仕様書は、2017 年 6 月 27 日から適用されます。

附則（2018 年 3 月 1 日）

本サービス仕様書は、2018 年 3 月 1 日から適用されます。

附則（2018 年 6 月 22 日）

本サービス仕様書は、2018 年 6 月 22 日から適用されます。

附則（2018 年 8 月 30 日）

本サービス仕様書は、2018 年 8 月 30 日から適用されます。

附則（2020 年 3 月 2 日）

本サービス仕様書は、2020 年 3 月 2 日から適用されます。

附則（2020 年 6 月 11 日）

本サービス仕様書は、2020 年 6 月 11 日から適用されます。