FUJITSU
Hybrid IT Service FJcloud-O
「認証サービス」
ご紹介資料

富士通株式会社

2021年6月

Version 2.10

目次

はじめに　～認証統合の要は「4つのA」～

FUJITSU

認証統合は「4A」を軸にした検討が必要です

■認証(Authentication)
人間・機器・プログラム等のものが**想定通りのもの**である
ことを、他のものが**確認する**こと、またはその**機能**。

■認可(Authorization)
認証を受けた人間・機器・プログラム等のものに対して、
機器・**プログラム・データに対するアクセスを許可する**こと、
またはその**機能**。

4A

■管理(Administration)
認証や認可を行うための利用者情報、機器情報等や
アクセス制御情報を保有し**利用・変更を可能にする**こと、
またはその**機能**。

■監査＆監査証跡
(Audit & Audit Trail)
機器・プログラム・データに対して**アクセスした記録や履歴**を
保存し、そのアクセスの**正当性をチェック**や監査すること、
またはその**機能**。

認証（Authentication）

人や機器の真正性を確認

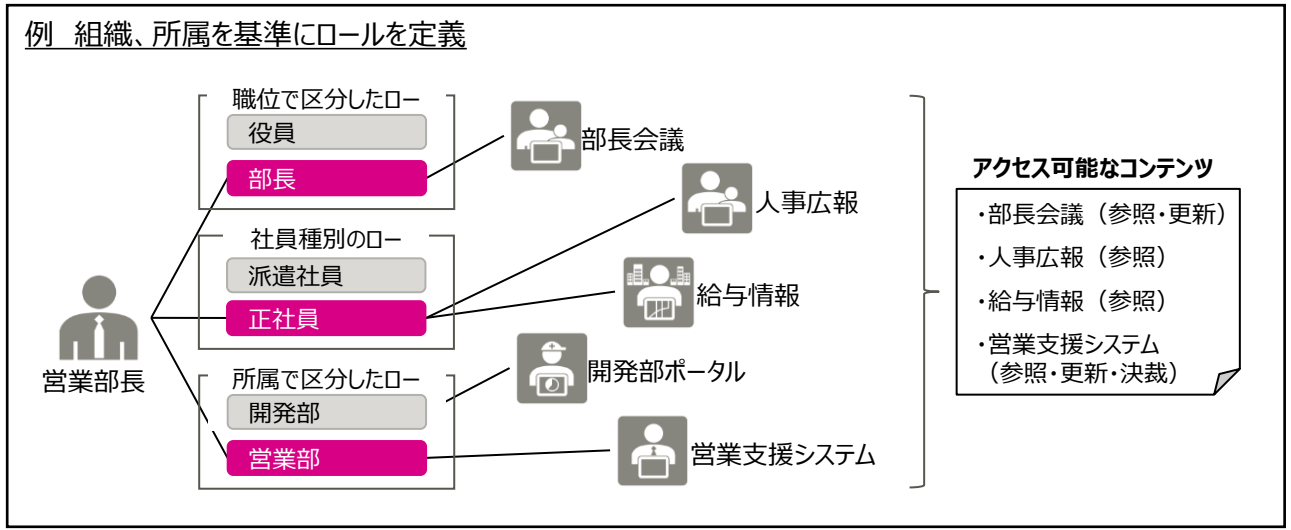
○ 認証方式の識別特性とメリット・デメリット

識別特性	認証方式の具体例	メリット	デメリット
1．記憶	・文字列パスワード ・PIN(暗証番号) 	○導入・運用コストが安価 ○わかりやすい	●紛失・盗難に気づきにくい ●簡単だと推測しやすい ●複雑だと覚えにくい （忘却しやすい）
2．所持品	・ICカード ・証明書 ・トークン ・機器に組み込まれたデータ 	○悪用が困難 ○紛失・盗難に気づきやすい ○モノを持っている安心感	●導入・運用コストが高価 ●紛失・盗難しやすい ●壊れる
3．身体的特徴	・静脈 ・指紋 ・虹彩 	○紛失・盗難されない ○なりすましが困難	●高価 ●プライバシー ●人によっては利用できない ●誤検知の場合もある ●ケガ等により損なわれる

認可（Authorization）

認証された人や機器にアクセス権限（ロール）を付与

○ ロール
職位、資格、所属する組織や職責を示すものです。
組織内における仕事や役割を表す用語を定義します。
ロールの定義にしたがって必要な認可が割り当てられます。

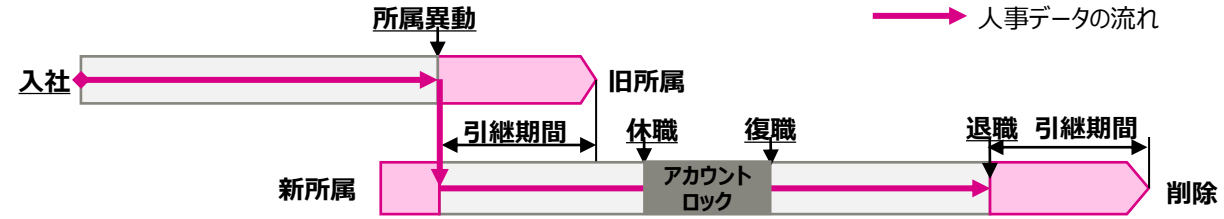


管理（Administration）

人や機器のライフサイクルを正しく管理

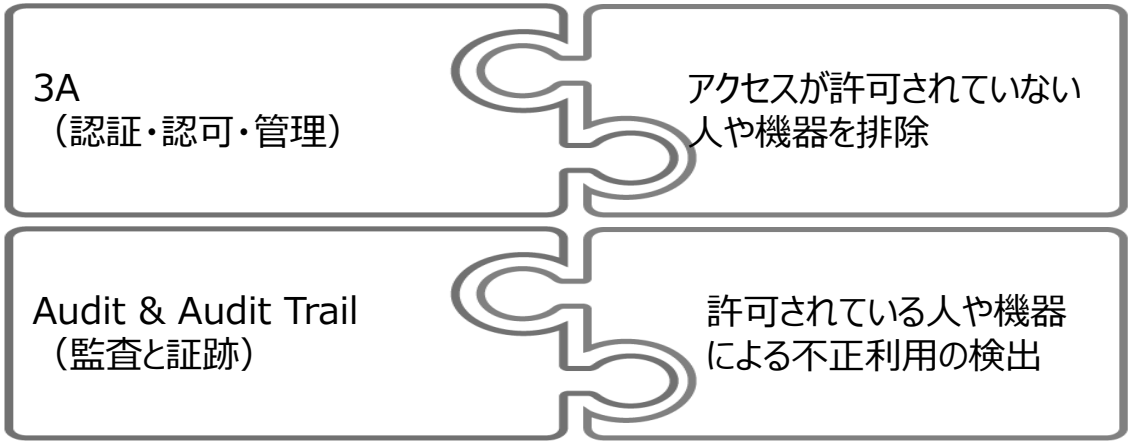
- ライフサイクル管理
  社員の**入社、退職、所属異動、休職、復職**など、アカウント情報の**登録から削除**までの管理機能です。
- 非正規従業員の管理
  人事情報に登録されない、現場裁量にて採用される**非正規従業員などのアカウント情報管理**も適切に運用できる必要があります。
- 大規模異動処理への対応
  国内企業に特有の年度初めの**大規模人事異動**などにおいて、アカウント情報を**迅速に対応**させる必要があります。

アカウント情報のライフサイクル管理の一例



監査と証跡（Audit & Audit Trail）

「監査と証跡」により、3Aがより一層効果的に機能



セキュリティ管理者など

記録される情報例

- ✓ いつ、だれが、だれの情報を操作したか
- ✓ いつ、だれが、どの端末にログインしたか
- ✓ いつ、だれが、どの端末でログインに失敗したか

認証サービスでの機能提供範囲

FUJITSU

認証要素4つのうち、3要素を提供

■認証(Authentication)
・シングルサインオン
・ワンタイムパスワード
・生体認証

■認可(Authorization)

（システムに依存するため業務アプリ側での対応）

4A

■管理(Administration)
・ID管理機能連携（API提供）

■監査＆監査証跡
(Audit & Audit Trail)
・監査ログ取得機能連携
（API提供）

認証サービスとは –認証統合の課題-

FUJITSU

認証サービスの導入により、認証統合に関する様々な課題を解決します。

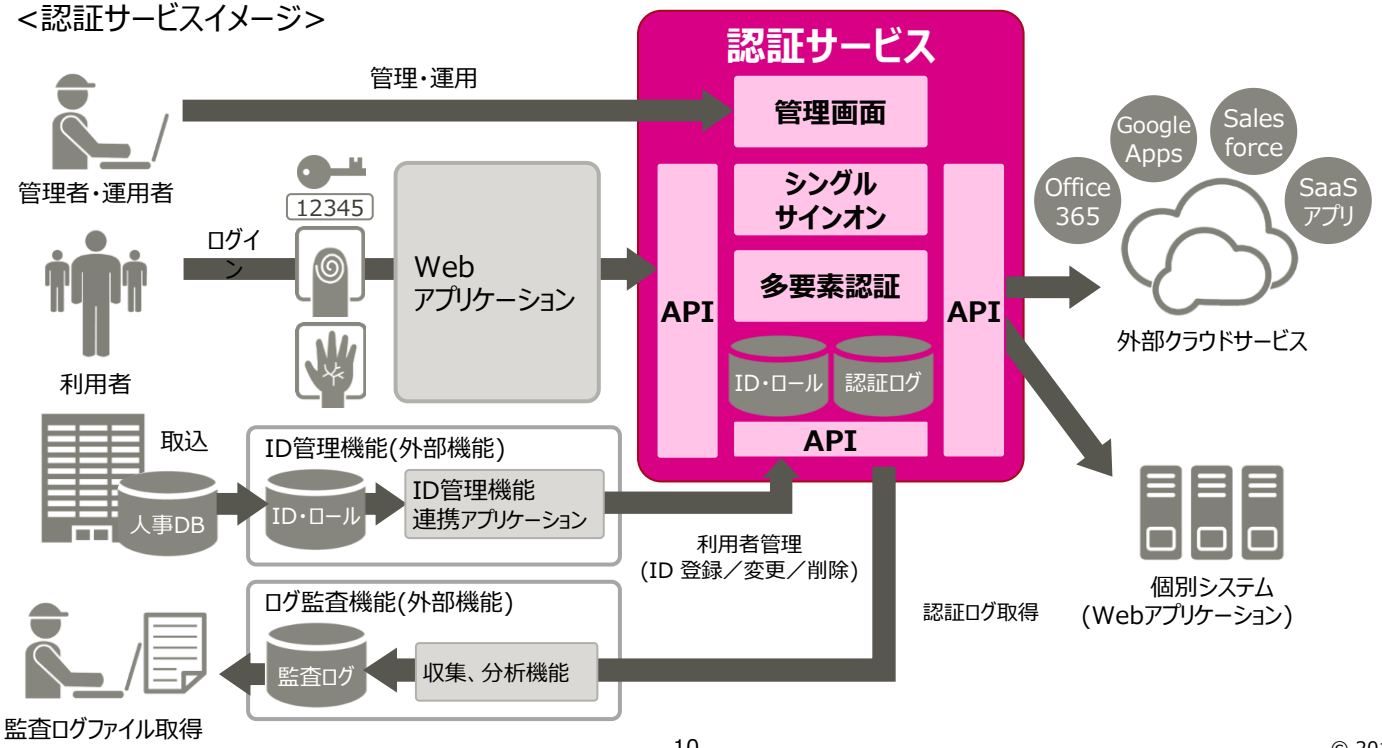
認証サービスで課題解決！

クラウド時代において、利便性を損なわずに本人と証明できる
パブリッククラウドサービスが必要となっている

認証サービスとは –サービス概要-

Webアプリケーションに対して多様な認証機能をスピーディーに組み込みできるサービスです。
本サービスの利用により、セキュリティ強化と利便性向上を実現します。

<認証サービスイメージ>



認証サービスの特長

FUJITSU

利便性の向上（シングルサインオン（SSO））

標準規約に沿った認証方式(SAML,OpenID Connect 1.0)の採用により、他のクラウドサービスと連携、シングルサインオンシステムの構築が可能になります。

セキュリティリスクの低減（多要素認証）

富士通の生体認証（手のひら静脈・指紋）の利用により、安全な認証システムの構築が可能になります。

ID管理連携（APIを提供）

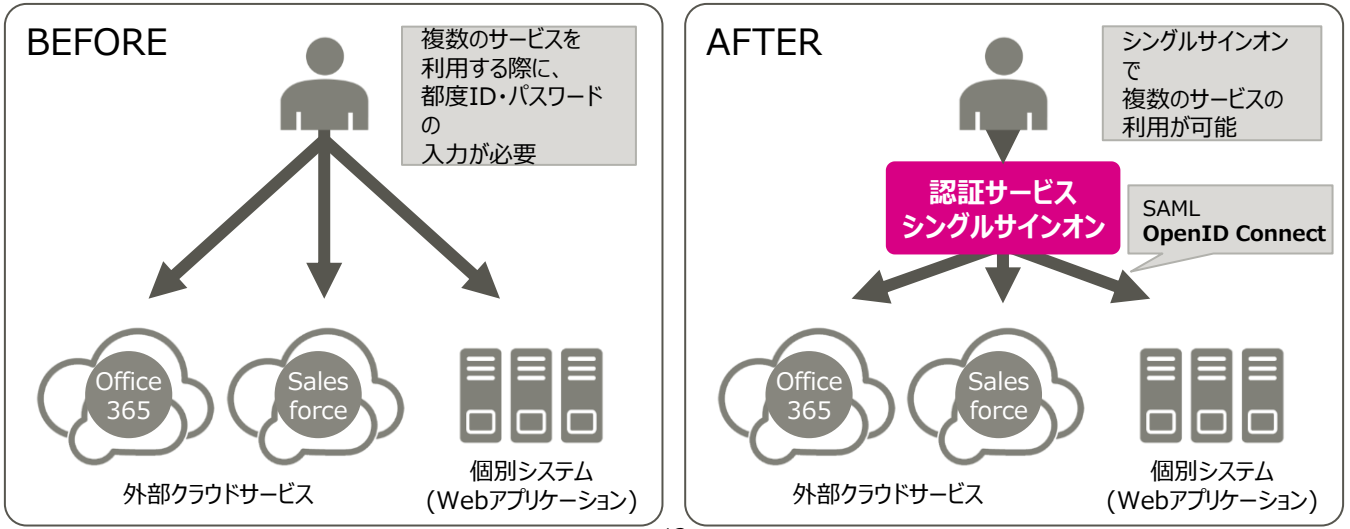
認証用のID情報に関して、ID管理元からのAPIの利用により連携可能になります。

監査と証跡のログ取得（APIを提供）

セキュリティ監査に必要となるアクセスログ（証跡ログ）をAPIの利用により取得可能になります。

利便性の向上（シングルサインオン（SSO））

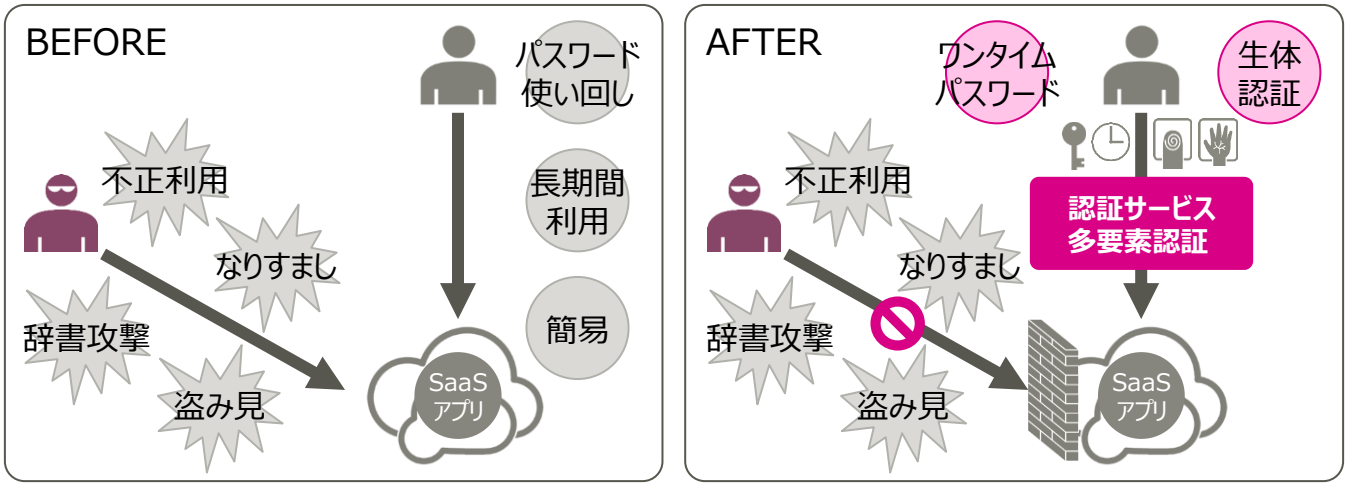
- 複数の業務サービス（Webアプリケーションや外部クラウドサービス）を利用する際に、都度ID・パスワードの入力を行うことなく1回の認証でアクセスすることができます。
- 標準規約に沿った認証方式(SAML,OpenID Connect 1.0)の採用により様々なクラウドサービスを一元してシングルサインオンシステムで利用が可能になります。
- ID／パスワードを一元管理することにより利便性が向上します。



セキュリティリスクの低減（多要素認証）

「ワンタイムパスワード」や「生体認証」による認証を行うことにより、確実な本人特定で、ルール厳格化では防げない「なりすまし」、「不正利用」による情報漏えいのリスクを大幅に軽減することができます。

- ワンタイムパスワード
  1回限りの使い捨てパスワードを用いることにより、高い安全性を確保します。
- 生体認証
  生体情報を利用し、確実に本人であることを証明しアプリケーションにアクセスできます。



機能概要

FUJITSU

○ 基本サービス

機　能		概　要
認証機能	シングルサインオン	標準規約に沿った認証方式(SAML,OpenID Connect 1.0)の採用により様々な業務サービスと連携することによりシングルサインオン環境を提供します。
	多要素認証	一般的なID、パスワードだけでなく、手のひら静脈認証、指紋認証、ワンタイムパスワードの多要素認証の提供によるセキュアな認証システムを提供します。

○ 管理画面

機　能	概　要
利用者管理	Webアプリケーションの利用者の管理を行います。運用テナントごとの最大ID数(申請ID数)、登録ID数、残ID数の確認や利用者の検索・追加・変更・削除が可能です。
各種設定	ログイン画面やセッションの設定、ドキュメント・ツールのダウンロード、認証連携を行うアプリケーションの登録を行います。
サービス内容	運用テナントの追加や利用状況の確認を行います。認証方式オプションの設定変更（ワンタイムパスワードオプション／生体認証オプションの設定／解除）が可能です。
認証設定	パスワードポリシーの設定、ADFS設定、IPアドレス制限の設定を行います。
個人設定	利用者のパスワード変更やタイムゾーンの設定を行います。ワンタイムパスワードや生体認証のオプションが設定されている利用者は、パスフレーズの確認や生体認証登録時のパスワードを設定することができます。

機能概要

FUJITSU

○ REST API

機　能	概　　要
認証	認証／ログアウト機能を提供します。
利用者管理	利用者情報について以下の機能を提供します。 ・利用者の取得 ・利用者の一覧取得 ・利用者の一括追加 ・利用者の変更 ・利用者の一括変更 ・利用者の一括削除 ・利用者の一括ロック解除
パスワードポリシー管理	パスワードポリシーの取得／変更機能を提供します。
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／変更機能を提供します。
認証ログ取得	内部統制報告制度（J-SOX）、金融情報システムセンター（FISC）の監査に対応した認証ログを取得するAPIを提供します。 認証ログについて以下の機能を提供します。 ・認証結果ログ取得 ・認証サービスのREST API操作ログ取得

機能概要

FUJITSU

○ テナントの考え方

テナントとは、認証サービスを利用する単位です。本サービスでは、以下のテナント単位にアカウント（ID）の認証の設定を行い、管理・運用します。

名称	概　要
管理テナント	運用テナントの管理を行うためのテナントです。
運用テナント	Webアプリケーションや外部クラウドサービスとの認証連携を実現するためのテナントです。運用テナントごとに最大ID数を設定します。

○ アカウント（ID）

サービスのアカウントは、以下の4つに分類されます。

名称(権限)	概　要
契約者	FUJITSU Hybrid IT Service FJcloud-O と契約を結んでいるお客様です。認証サービスとして管理テナントを配備し、サービスを管理します。運用テナントの作成／運用者の作成、管理者の作成を行います。
管理者	管理テナントに所属し、テナントの管理者権限が設定されている担当者です。運用テナントを管理します。新たに管理者を作成することもできます。
運用者	運用テナントに所属し、テナントの運用者権限が設定されている担当者です。運用テナントに所属する利用者を作成し管理します。新たに運用者を作成することもできます。
利用者	Webアプリケーションや外部クラウドサービスの利用者です。運用テナントに所属します。

アカウント作成権限　○:作成可能／×:作成不可

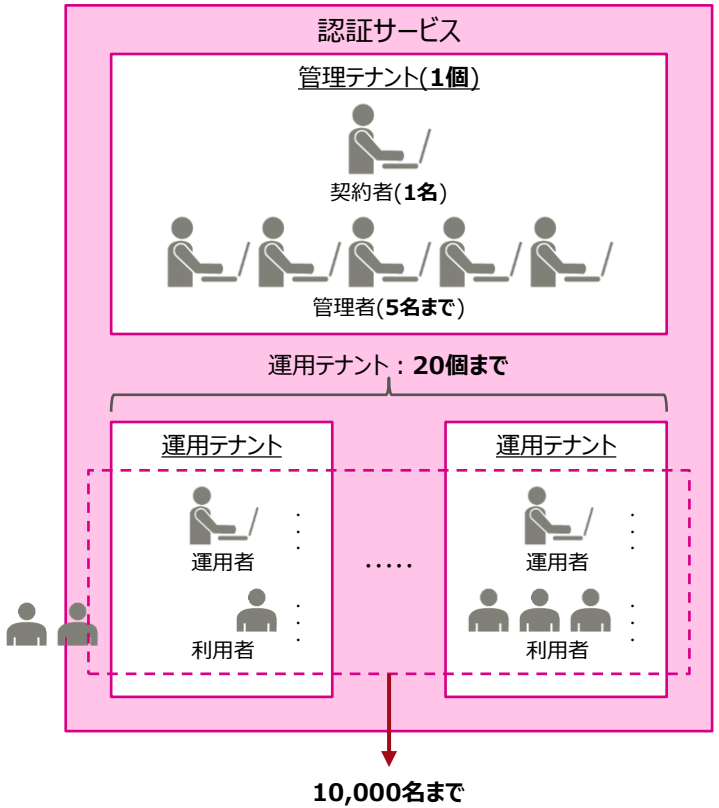
		作成者自身のアカウント権限			
		契約者	管理者	運用者	利用者
作成対象	契約者	×	×	×	×
	管理者	○	○	×	×
	運用者	○	×	○	×
	利用者	×	×	○	×

機能概要

○ テナント数、アカウント(ID)数の考え方

名称	数	説明
管理テナント	1	認証サービスの利用を開始すると1つ作成されます。
運用テナント	～20	1つの管理テナントに対し20個まで作成可能です。
契約者	1	FUJITSU Hybrid IT Service FJcloud-Oの契約者です。
管理者	～5	5名まで作成可能です。
運用者 利用者	※	管理テナントにひも付くすべての運用テナントの最大ID数（運用者＋利用者の上限数）を合算した値の上限は10,000です。

※10,000ID以上のご利用をご希望の際は、ヘルプデスクまでお問合せください。ヘルプデスクよりプラン変更方法をご案内いたします。詳細はFUJITSU Hybrid IT Service公開ホームページのFAQをご確認ください。



課金の考え方について

FUJITSU

- 課金方法
  申請ID数に応じた月額固定料金で課金されます。
  - 月額単価×申請ID数で課金されます。月額単価は申請ID数に応じて異なります。
    - 申請ID数
      すべての運用テナントの「最大ID数」を合計した数です。
    - 最大ID数
      お客様が運用テナントごとに任意に設定する項目です。
      該当の運用テナントに登録できる運用者ID＋利用者IDの上限数です。
    - 申請ID数の集計の考え方
      ①日次で運用テナントごとに「最大ID数」を集計します。（集計時刻：UTC0時※）
      ②該当料金月の中で、もっとも大きな「最大ID数」が集計対象となります。
      毎月1日のUTC0時にすべての運用テナントの「最大ID数」を合計し、
      「申請ID数」とします。

    ※JST（日本時間）の9時
  - オプションを設定している運用テナントがある場合は別途オプション料金がかかります。
    ※ワンタイムパスワードオプションは無料です。

課金計算例は次ページをご参照ください。

課金の考え方について

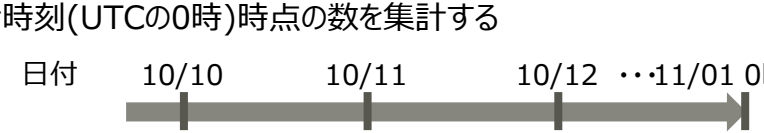
FUJITSU

○ 課金メニュー例

認証方式	1IDの単価（円）					
	～1,000ID	1,001～5,000ID	5,001～10,000ID	10,001～50,000ID	50,001～100,000ID	100,001ID～
基本料金	480	390	300	220	210	200
オプション料金(ワンタイムパスワード)	無料					
オプション料金(生体認証)	710	570	460	370	320	260

○ 課金計算例

- ○ 登録ID数ではなく最大ID数を申請ID数とする
- ○ 集計日前月の最大ID数に設定された値のうち、最大値を集計対象とする
- ○ 日々の最大ID数は集計時刻(UTCの0時)時点の数を集計する



テナント		ID数		
管理テナント		（課金計算対象外）	変更	
運用テナント1 生体認証オプション**なし**	**最大ID数**	**800**	**800→1500 →1000(最大値)**	**1000→500**
	登録ID数	0	300	400
運用テナント2 生体認証オプション**あり**	**最大ID数**	**800(最大値)**		
	登録ID数	700		

課金対象

基本料金 申請ID数　：1800
オプション料金 申請ID数：800

【基本料金】
1,800ID×390円=702,000円

【オプション料金】
800ID×710円=568,000円

【合計】
1,270,000円

制限事項・注意事項

FUJITSU

○ 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。

○ 本サービスの提供リージョンについては、FUJITSU Hybrid IT Service公開ホームページのサービス仕様書をご参照ください。

FUJITSU

Thank you