ThemiStruct
テミストラクト

B2B、B2C向けWebサービスにおける認証基盤のあり方

株式会社オージス総研
事業開発本部 テミストラクトソリューション部
金井　敦

自己紹介

金井　敦

株式会社オージス総研

統合認証ソリューション担当部門　マネジャー

主戦場

金融・保険業界を中心としたB2B/B2C向けの
Identity and Access Management基盤の構築、
プロジェクトマネジメント、ソリューション開発

OpenIDファウンデーション・ジャパン　KYC WG

本日のお話し

- Part１：それって認証なの？認可なの？ 8min
- Part２：Webサービスにおける認証・認可 7min
- Part３：認証基盤が提供する認証・認可 20min
- Part４：まとめ 5min

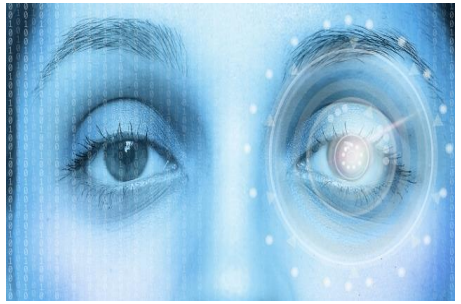
全体で40分間

Part１：
それって認証なの？認可なの？

認証について考える

◆ 認証（Authentication）

- 相手が誰であるかを確認すること。（あなた何者？）
- 相手が誰であるかを確認する手段は様々。
  - アナログでは、運転免許証、健康保険証、住民票、学生証、パスポート、名刺、知人の紹介など
  - デジタルでは、ID/パスワード、指紋、顔、ICカードなど
- 確認方法によって、本人確認の精度や確認できる情報も様々。
- Webサービスでは対面での本人確認を行うことや身分証明書の提示が（現段階では）難しいため、精度を高める方法が課題となりやすい。



認可について考える

◆ 認可（Authorization）

- 要求する権限を有しているかを確認すること。（権利ある？）
- 権限を持っているかを確認する手段は様々。
  - アナログでは、運転免許証、健康保険証、パスポート、チケット、クーポン、鍵、第三者の印鑑など
  - デジタルでは、ユーザー種別、グループ情報、ロール情報、トークンなど
- 認証と認可は異なる概念のものである。認可を行うために、認証が必要であるとは限らない。認証されたからと言って、必ず認可されるとも限らない。
  - 切符やクーポン、コインロッカーを使うのに誰であるかを名乗る必要はない
  - 取得した権限を第三者に譲渡して利用させることもあり得る
  - 相手が誰であるかを高い精度で確認できたとしても、要求を受け入れてよいかは別問題

Webサービスと認証・認可

◆ サービス利用時にユーザー登録を行いログインをして利用するWebサービスにおいて、認証と認可は必ず必要となる処理である

- Webサービスでは対面での本人確認を行うことや身分証明書の提示が（現段階では）難しいため、一般的には**ユーザー登録時に設定したパスワード情報を再提示することで認証を行う**ケースが多い。

- **認証における主な脅威は身分を偽られること（なりすまし、虚偽の申告）**であるが、パスワードを使った認証は非常に理解しやすく使いやすい反面、脅威を受けやすい。このため**認証の強度や精度を高める方法が課題となりやすい。**

- Webサービスにおいては多くの場合、誰であるかを認証してから、認証された相手に対して認可（権限）を与えたり、確認する構造であるため認証と認可が混同されやすいが、**認証されたユーザーアカウントに対して適正な権限が割り当てられ、権限の範囲でサービスを利用できる必要**がある。

- **認可における主な脅威は権限の不正取得や越権行為**であるが、他者に権限を一部委譲したくてもアカウントの単位で権限設定されているため、持っている**一部の権限やデータのみを切り出して提供することが構造的に難しい。**

Part２：
Webサービスにおける認証・認可
～モデルケースと課題～

Webサービスにおける認証・認可とは

◆ 店舗サービスの例

サービス利用者

認証

利用したいので会員登録してよ

免許証

免許証です

認可

会員証をどうぞ　会員証

会員証

会員証です、DVD貸して

DVDをどうぞ

会員登録窓口

身分証明を見せてください。

確かにご本人ですね。
会員証を発行します。

サービス利用窓口

会員様ですね。
ご利用ありがとうございます。

こちらの貸出しはプレミアム会員様のみご利用いただけます。

Webサービスにおける認証・認可とは

◆ Webサービスでは

- 会員登録時のユーザー情報・権限情報と認証情報を紐づけることで、ログイン時に認証を行い会員登録した本人であることを確認している。（と同時に会員IDの権限を確認している）

サービス利用者

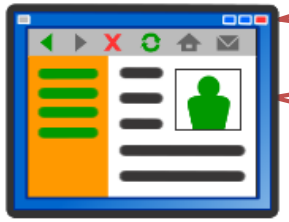
利用したいので会員登録してよ

会員登録用URLです

ユーザー情報とパスワードです

プレミアム会員でID発行されました

会員登録画面



メールアドレスを登録してください。確認メールを送付します。

確かにメールアドレスの利用者ですね。会員IDを発行します。

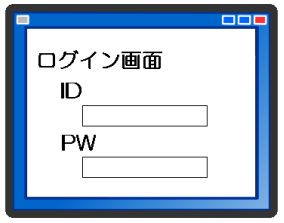
ユーザー情報とパスワードを登録してください。

認証・認可

会員IDはMe、パスワードは1234です

動画を再生します

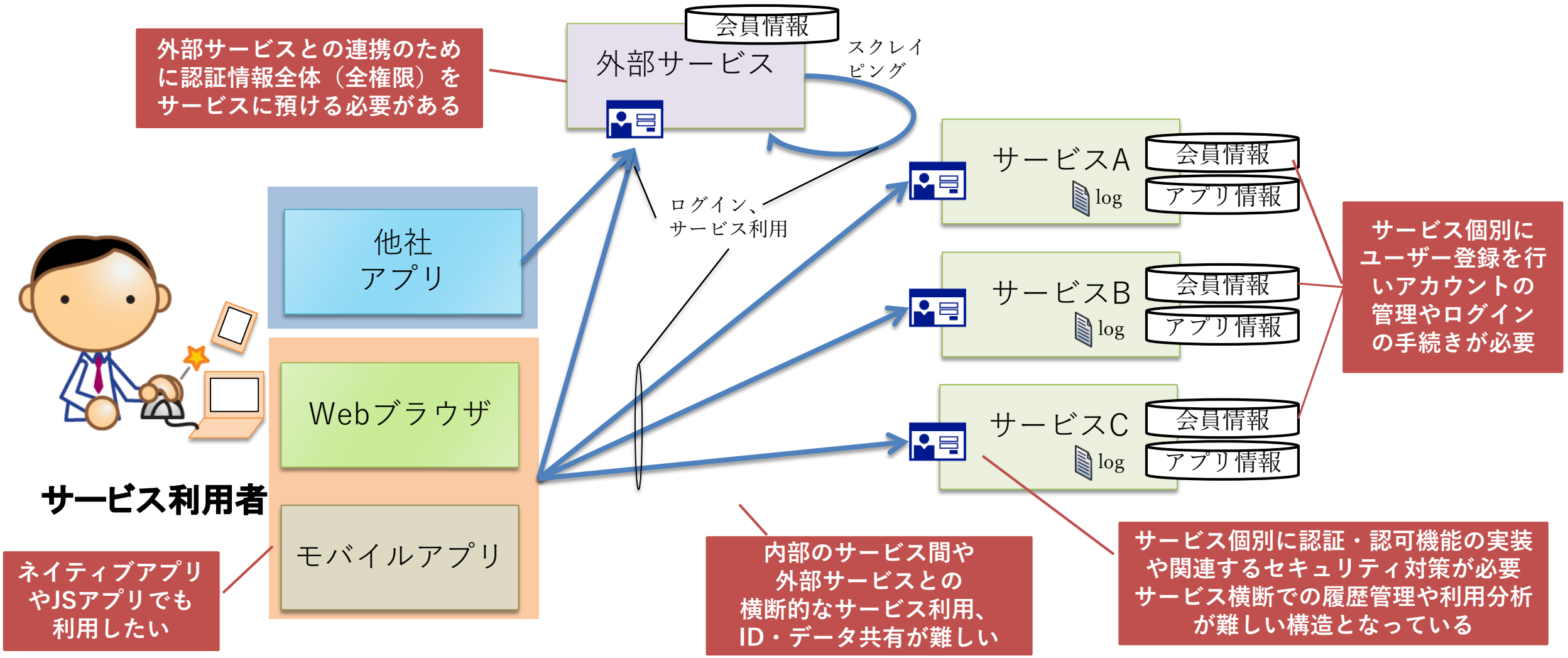
ログイン画面



会員様ですね。
ご利用ありがとうございます。

こちらの視聴はプレミアム会員様のみご利用いただけます。

従来型のWebサービスのモデルケースと課題



従来型Webサービスにおける課題のまとめ

サービス毎に似たようなユーザー情報を登録して、１つ１つログインするなんて面倒！
パスワードを使いまわさないようにするなんて無理！いちいち覚えてられない！

これスマートフォンアプリで使えないの？使いにくいんだけど・・・
毎回ログインとか勘弁して。

このサービスに預けたデータ、別のサービスからも使いたいな～。ログイン情報を設定すれば出来そう。なんとなく信用できそうなサービスだし大丈夫だろ。

不正利用の被害からはしっかり守ってよね。

リスト型攻撃が流行っているから認証を強化しろ？
全部のサービスに対応したら物凄い工数と予算がかかりますよ？

サービスの利用情報をマーケティングに活用したい？ユーザーID
もデータもサービスによってバラバラだし何日かかるやら・・・

外部サービスと連携できるようにしたい？
仕様の調査や技術習得も必要だし個別に対応してられないよ。

不正利用されないようサービスの安全性は確保しなきゃなぁ・・・

そんなときに必要なのが認証基盤

その課題、認証基盤で解決します！

- 独自仕様や個別実装は脆弱性を生みやすい
- サービスを安全に安心して利用いただくために不可欠となる認証・認可の機能を専門的なシステムやエンジニアのノウハウを活用して実現
- 認証・認可の共通化、標準化の実現に必要な機能の開発や最新技術動向への追従は認証基盤で
- 様々な認証方式、認証連携方式を適用できる
- ユーザーやサービス運営者の負担を軽減し、UXの向上や効率的なサービス運営に寄与できる

Part３：
認証基盤が提供する認証・認可

認証基盤の主要なユースケース

エンタープライズ向け

企業/企業グループ内の業務向けの「**社内統合認証基盤**」を構築する

B2B・B2C 向け

顧客向けサービスサイトの「**共通ID基盤**」を構築する

オープンAPIを提供するための「**API連携認証基盤**」を構築する

顧客向けサービスサイトの

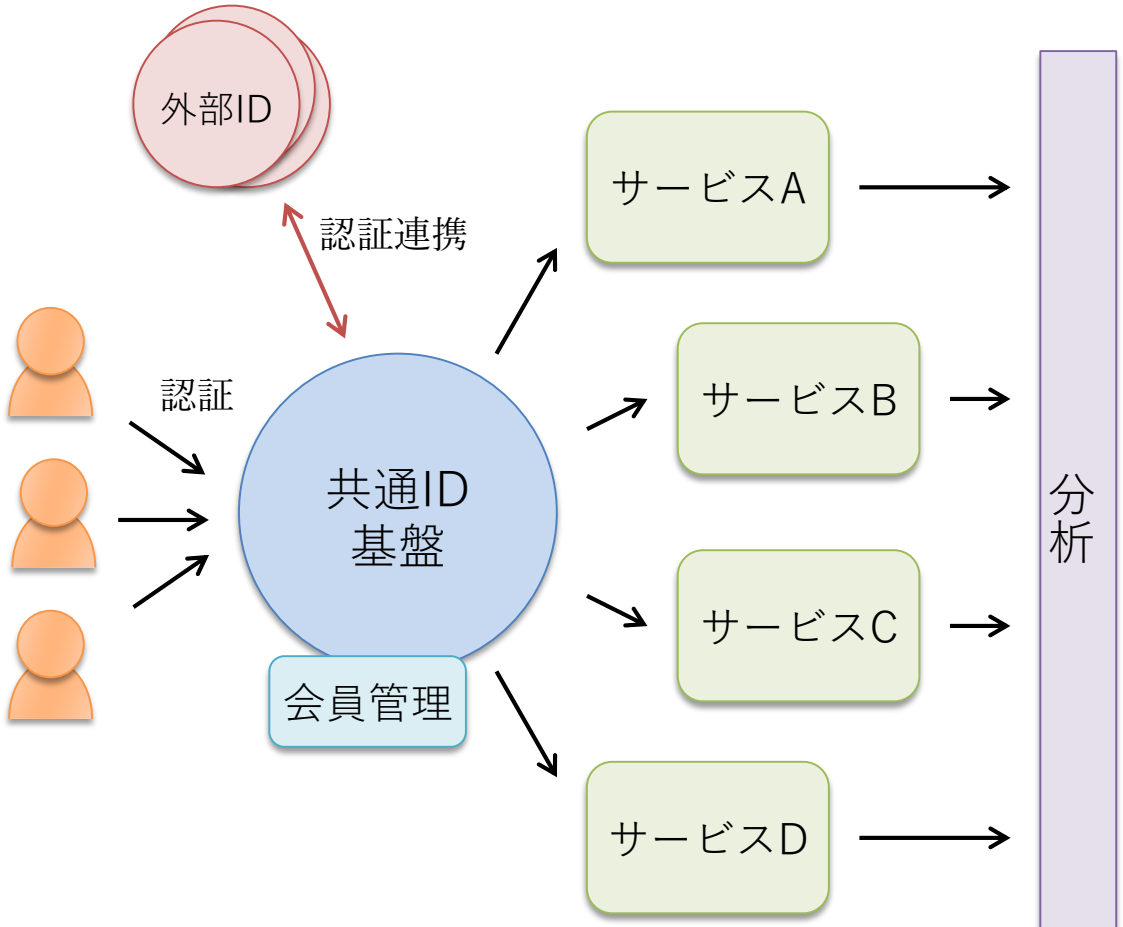
「共通ID基盤」の構築を考える

「共通ID基盤」の役割

認証統合
- ◆ 自社サービスの会員IDを共通化
- ◆ 自社サービスのログインを共通化
- ◆ サービス横断での利用状況の把握・分析

安全策
- ◆ 変わりゆく認証方式への対応
- ◆ 多要素認証による認証強化

認証連携
- ◆ 外部IDと連携した会員登録の実現
- ◆ 外部IDと連携したログインの実現
- ◆ 標準技術仕様に適合したシステム間連携の実現



認証基盤を導入することで機能分離・共通化を実現

Webサービスで用いられる認証要素とは

□ 認証要素とは以下の三種類で構成される

- What You Know（知っている）
  - ユーザーが記憶している情報による認証
    - パスワード、生年月日、PIN、秘密の質問…
  - ユーザーの記憶できる範囲であることが多く推測・漏洩のリスクが高い

- What You Have（持っている）
  - ユーザーが保持しているものによる認証
    - OTP、ICカード、クライアント証明書、公開鍵認証…
  - 推測による不正認証は難しいが、紛失時のリスクが高い

- What You Are（あなたである）
  - ユーザー自身の情報による認証
    - 生体認証
  - 利用する機器により認証精度が異なり、他人受け入れ・本人拒否の可能性がある

多要素認証と多段階認証

- **各認証要素には前述の特徴があり、複数の要素を組み合わせることで欠点を補いセキュリティレベルを高めることができる**
  - PWと秘密の質問で多段階認証にしても、ユーザーが他サイトと同一の組み合わせを利用していたら他サイト側での漏洩により突破される可能性も
  - PWとクライアント証明書による多要素認証であれば一方が漏洩、紛失してももう一方を攻撃者が取得・推測することは難しい
- **これらの内複数の要素を満たす認証を「多要素認証」と呼ぶ**
  - パスワード＋生年月日やパスワード＋秘密の質問では「多要素認証」ではなく同一要素の「多段階認証」である

認証方式の強化

多段階認証

認証強度の問題

多段階だが多要素ではない

生体認証

ユーザーの心理的抵抗感

ユーザーへの展開負担

ワンタイムパスワード認証

カバレッジや手間の問題

ユーザーへの展開負担

リスクベース認証

精度や環境制約の問題

誤認証の可能性

クライアント証明書認証

証明書発行管理の負担

クライアントへの展開負担

ICカード認証

ICカード発行管理の負担

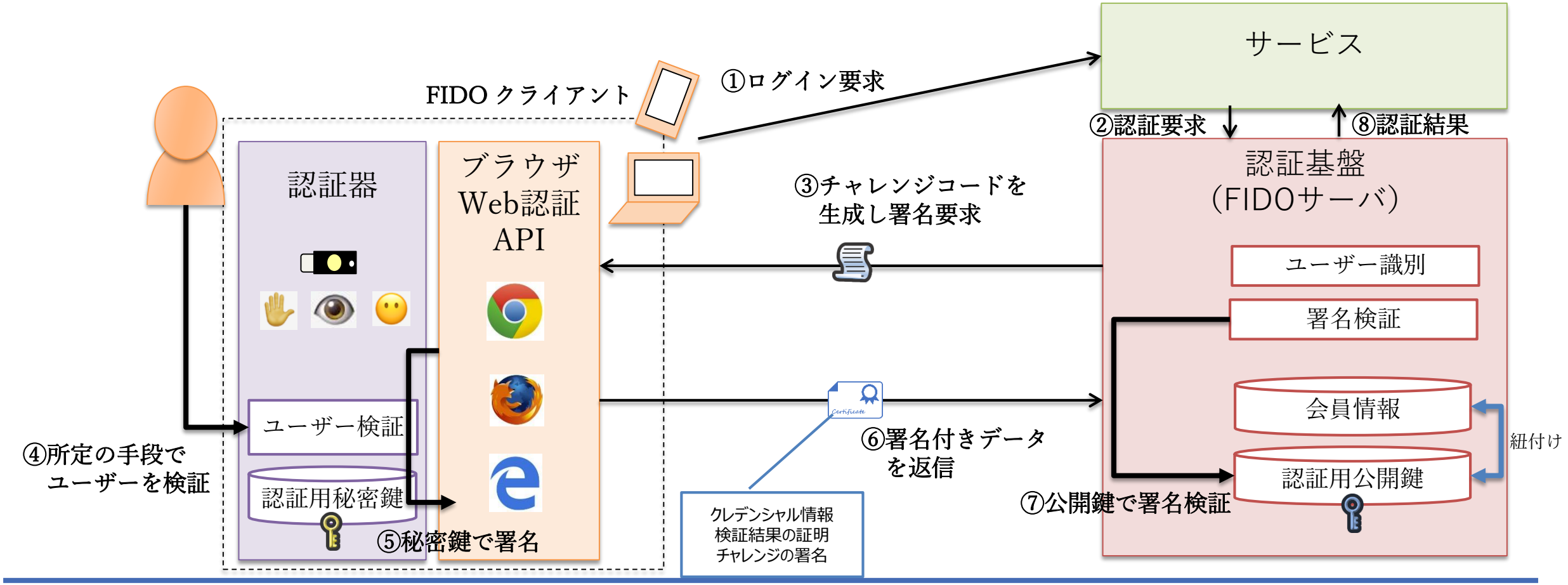
ユーザーへの展開負担

負担増やコスト増の懸念から特定業種以外では積極的には採用が進んでこなかった
ユーザーの意思に応じて利用可能な環境を整えてあげることがまずは必要

変わりゆく認証方式　～FIDO2～

◆ FIDO2の登場

➢ 公開鍵認証方式を応用してオンライン経由で認証を行う仕組み



変わりゆく認証方式　～FIDO2～

◆ 認証器とは

- 公開鍵認証を実施するために**秘密鍵をもとに署名の生成を行う機器**で認証機能を持つものがある
- Windows HelloやスマートフォンのFIDO2対応の指紋認証など**デバイス内蔵の認証器を利用できる**
- FIDO2対応のUSBやBluetooth、NFCの**外部認証器を利用することもできる**

出典：Google
[https://cloud.google.com/titan-security-key/]

◆ FIDO2のメリット

- 認証サーバに**パスワード情報や生体情報を保持する必要がない**
- パスワード情報や生体情報が**ネットワーク上を流れない**
- 上記情報がないため、認証サーバが**狙われない、不正ログインできない**
- FIDO対応のブラウザと認証器を持つデバイスがあれば**多要素認証が簡単に実現できる（例：公開鍵認証＋認証器による生体認証）**
- パスワードを使わず認証することもでき、**パスワード管理から解放される**

変わりゆく認証方式　～CIBA～

◆ CIBAとは

- OpenID Foundationという団体が策定を進めるドラフト仕様の一つ
- アプリケーションを操作している人ではなく第三者の認証情報を確認する際に利用する

◆ CIBAが想定するユースケースの例

- コールセンターへの架電を行ったユーザーが本人であることを認証する
- 窓口対応しているユーザーが身分証明書を出さずとも本人であることを認証する
- クレジットカード決済時に決済端末にPIN入力せず、利用者のスマートフォンで認証する

◆ CIBAのメリット

- ユーザーが他者の端末に認証情報を入力する必要がない（情報の漏洩や傍受のリスクを低減）
- 遠隔地のユーザー認証を認証する際のセキュリティレベル向上（WYKである個人情報を確認する以外の方法や多要素でユーザーを認証できる）

変わりゆく認証方式　～CIBA～

◆ CIBAの利用イメージ（概要）　コールセンターでの利用モデル

エンドユーザー

認証

ユーザー端末

④

⑤

認証基盤

①

③

⑥

オペレータ

オペレータ端末

②

アプリケーション

CIBAを使った認証の流れ（例）

① ユーザーがコールセンターへ電話

② ユーザーの電話番号入力

③ 認証要求

④ ログインURLをメール送信

⑤ ユーザー認証

⑥ 認証情報の返却

外部IDを利用した会員登録やログインの実現

◆ 外部IDとの認証連携によるメリット

- 外部サービスのIDを使ってログインができ、サービス利用時に**サービス毎のID/パスワードを思い出す必要がなく、アカウントロックやパスワード忘れの発生頻度も削減**される
- **外部サービスが提供する多要素認証の仕組み**をユーザーが利用できる
- **新規会員登録の際に外部サービスから**取得できる氏名やメールアドレスなどの**情報を入力フォームに自動補完**できる

「共通ID基盤」構築による効果

◆ サービス利用時のUX向上に寄与できる基盤

- 会員IDやログイン処理の**統合によるユーザー負担の軽減、UXの向上**
- 外部IDとの連携による**集客効果、心理的ハードルの抑制、パスワード管理負担の軽減**

◆ 安全にサービスを利用・提供できる基盤

- **認証方式の強化**や**新たな技術仕様への追従**が容易
- 高い安全性が認められている**標準技術仕様に適合したサービス提供**が可能

◆ サービスの開発や運営に貢献できる基盤

- 開発要員やコストを認証部分に割くことなく、**サービス自体の機能開発に注力**
- ユーザー管理、システム監査、サービス利用分析などの**運用業務の負担軽減や効率化**

オープンAPIを提供するための

「API連携認証基盤」の構築を考える

Web API を公開する際の課題

◆ クローズドAPI

- 組織内での Web API の利用
- 組織の境界内からのみアクセス可能

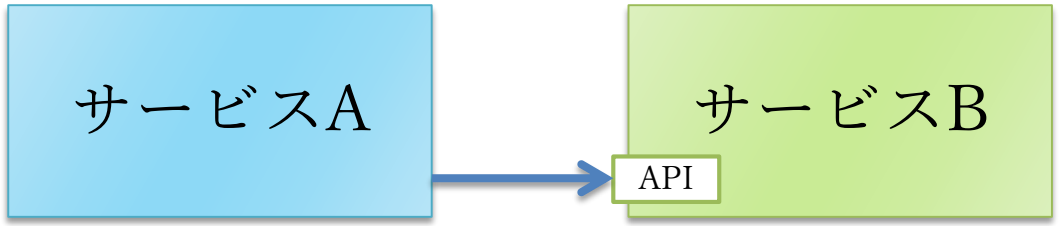
◆ オープンAPI

- 組織の境界の外側の**第三者へ積極的に公開**する Web API
- Web API 利用者の**認証**、機能やデータへの**アクセス権管理**が不可欠

Web API 利用の形態

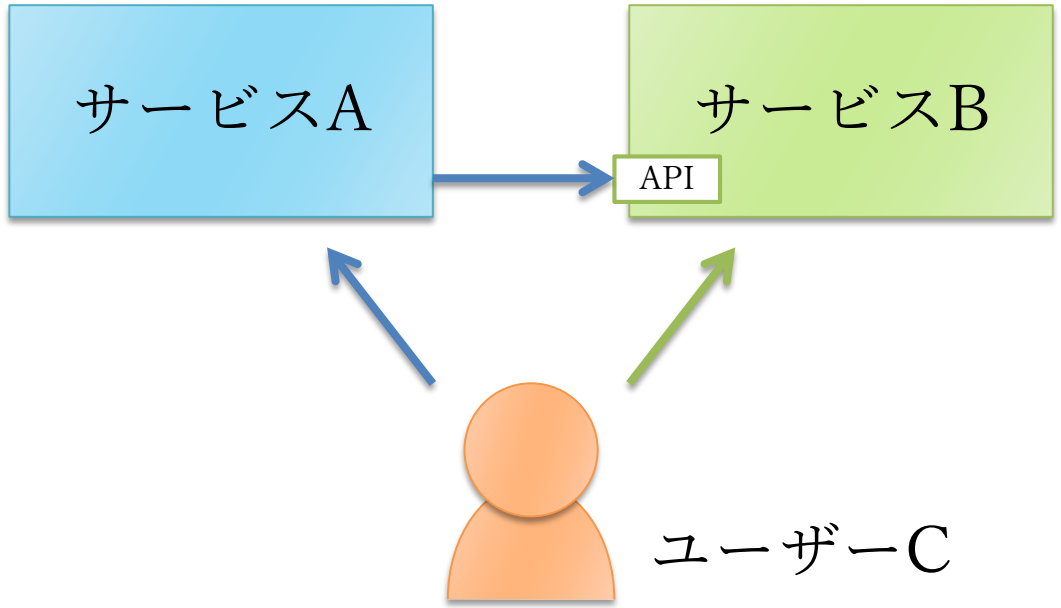
2者間でのAPI利用

- サービスA が サービスB の機能を利用するために API にアクセスする。
- サービスB は サービスA 向けの機能・データを提供する。



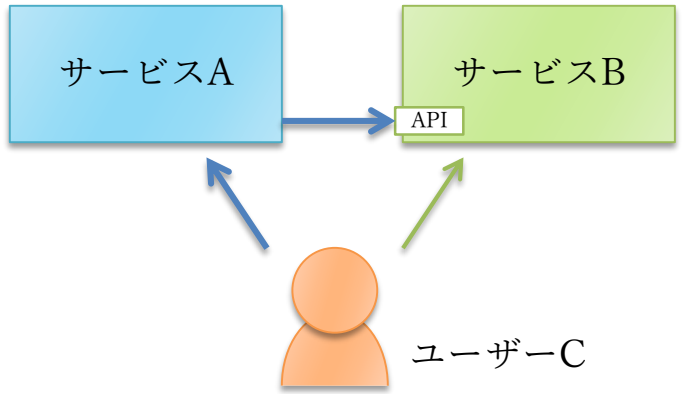
3者間でのAPI利用

- ユーザーC は サービスA、サービスB の利用者である。
- サービスA は、ユーザCの意図により、ユーザーC に代わり サービスB の API にアクセスする。
- サービスB は ユーザーC 向けの機能・データを提供する。



3者間でのAPI利用時の認証

- **ユーザーC は サービスA に、アクセスできるデータや操作を限定して、サービスB の API へアクセスさせたい**
  - ユーザーIDとパスワードなど、クレデンシャル情報を渡す方式では、全権限をサービスAに与えてしまう。
- **3者間でのAPI利用を実現するために必要な認可手続きをオンライン上で安全に行うための標準仕様がOAuth 2.0**
- **現時点では認可情報連携のための標準仕様であるOAuth2.0の利用が唯一の選択肢**
  - ユーザーC の同意に基づき、ユーザーC が意図した範囲の限定された権限で API へのアクセスを許可する方式
  - OAuth 2.0 Authorization Code Grant
  - OAuth 2.0 Implicit Grant　など



オープンAPIの提供には「API連携認証基盤」が不可欠

- **OAuth 2.0を利用するには「認可サーバ」の機能が必要**
- **認可（アクセス権の委譲）の前提としてユーザーが適切な方法で認証されている必要がある**

- **オープンAPIを提供するためには、API利用者の認証・認可ができる仕組みを構築しないといけない**
  - ユーザーを認証する機能（この機能には認証情報連携のための標準仕様であるOpenID Connectなどの利用が別途必要）
  - OAuth2.0 認可サーバの機能

API連携認証基盤を構築することに他ならない

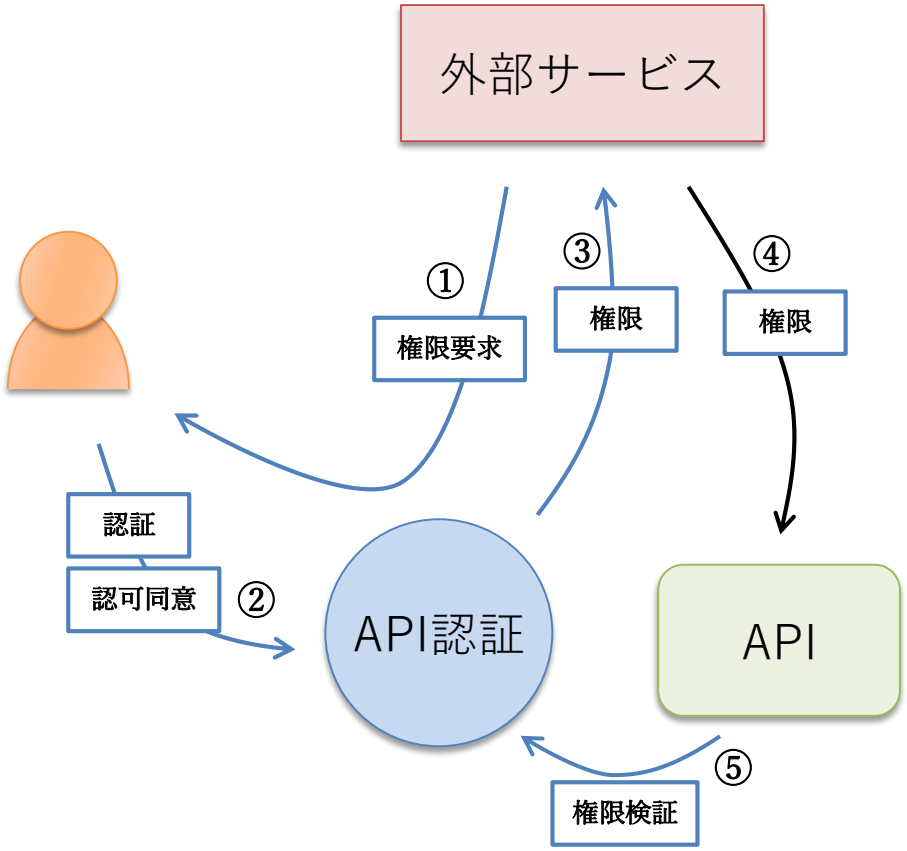
「API連携認証基盤」（OAuth認可サーバ）の役割

API認証

- 外部サービスへのAPI提供、そのための安全な認証機能の実現
- 再ログインを伴わない安全なサービス利用継続の実現
- サービス利用可能なプラットフォームの拡充

権限管理

- 利用者の同意に基づくAPI提供・アクセス許可の実現
- APIアクセス可能なクライアントの制限、アクセス権の適用
- ＋ 共通ID基盤の特性



認証基盤を導入することで API認証に必要な機能を実現

「API連携認証基盤」構築による効果

◆ サービス利用時のUX向上に寄与できる基盤

- **再認証を伴わないサービス利用継続**による利便性向上
- **様々なプラットフォーム上**で同じサービスをユーザーの状況に応じて利用できる

◆ 安全にサービスを利用・提供できる基盤

- 公開APIに対する**認証や範囲を限定した認可、権限設定が可能**
- **認証情報**自体をクライアント側に**保持させることなく期限を限定**し公開APIを利用許可
- 公開APIを通じたサービス連携に対して**利用者自身による同意や失効手続きが可能**

◆ サービスの開発や運営に貢献できる基盤

- 外部サービスへの連携により**新たな価値、新しいサービス領域を創造できる可能性**

Part４：
まとめ

まとめ

- Webサービスの提供や安全性の確保には認証・認可の機能が欠かせないが、サービス個別に新しい認証方式や標準仕様に継続的に追従していくには限界があり、認証や認可に関わる様々な課題を抱えやすい。
- 認証基盤を導入することでそれらの課題が解決しやすくなり、合わせてWebサービスに対するUX向上や安全かつ効率的なサービス運営に役立てることができる。
- 認証基盤のユースケースは顧客向けサービス、オープンAPI向けへと広がり、重要性がより高まっていく。外部サービスとの連携やID/パスワード認証以外の認証方法の利用も今後更なる拡大が見込まれる。

最後に少しだけ当社の取り組みについて

当社では統合認証ソリューションを提供しており

共通ID認証基盤、API連携認証基盤の

構築ニーズに対応できます

統合認証ソリューションを15年以上やってまいりました

自社オリジナル商品
（主に大規模サービス、B2B/B2C向け）

ThemiStruct（テミストラクト）
Identity Platform

OAuth 2.0 に対応した
APIエコノミー時代に求められる
統合認証パッケージ

オープンソース
ベース商品
（主に社内・グループ内でのエンプラ利用向け）

ThemiStruct-WAM
シングルサインオン
認証基盤ソリューション

ThemiStruct-IDM
ID管理ソリューション

ThemiStruct-CM
電子証明書発行・管理
ソリューション

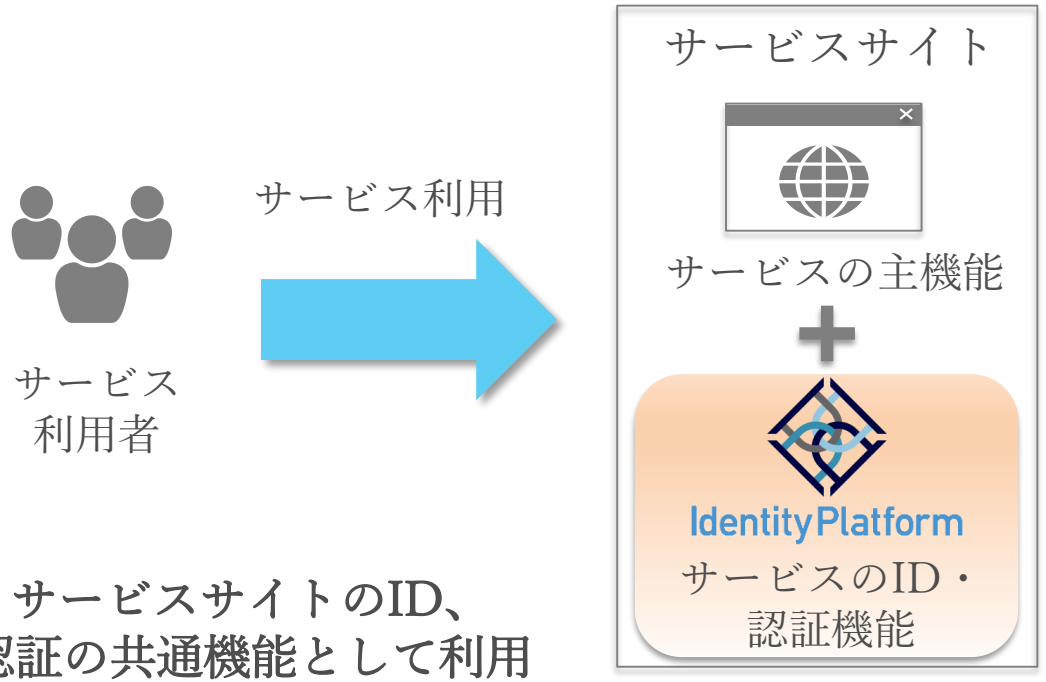
ワンタイムパスワードソリューション
ThemiStruct-OTP

システム監視ソリューション
ThemiStruct-MONITOR

ThemiStruct Identity Platform とは？

『ThemiStruct Identity Platform』は、ITシステム利用者のアイデンティティ管理と認証機能を提供します。**顧客向けにサービスを展開**したり、**従業員向けにアプリケーションを展開**する際に必要となる、共通ID基盤の構築に活用いただけます。

顧客向けサイト領域に活用



サービスサイトのID、認証の共通機能として利用

従業員向けサイト領域に活用

エンタープライズアプリ群の SSOやアクセス制御の基盤として利用

ThemiStruct Identity Platform 機能概要

シングルサインオン

シングルサインオンの機能を提供します。ユーザーは複数のサイトにわたるシームレスなアクセスが可能です。

ソーシャルログイン

ソーシャルログインの機能を提供します。ユーザーはSNS*などのサードパーティが提供しているアカウントを用いて、認証することが可能です。
* Google, Yahoo! Japan, LINE, Facebook

多要素認証

認証の強度を高めることができます。
任意で多要素認証の機能*を有効化することが可能です。
* ワンタイムパスワード（TOTP/HOTP），FIDO（U2F），リスクベース

フェデレーション

ユーザー情報を連携します。あなたのサイトでは、ユーザー情報を保持する必要はなくなり、必要なタイミングでユーザー情報の供給を受けることが可能です。

API連携

APIにアクセスする際に必要となる認可トークンの発行・管理を行なうことが可能です。

セルフレジストレーション

会員登録の機能を提供します。ユーザはサードパーティが提供しているアカウントを用い、ストレスレスな会員登録を行なうことが可能です。

セルフサービス

ユーザ情報の変更機能を提供します。ユーザ自身による登録情報のメンテナンスが可能です。

ユーザー管理

マネジメントコンソールによるユーザー情報の一元管理が可能です。

※ThemiStruct Identity Platformご紹介サイトURL
https://www.ogis-ri.co.jp/pickup/themistruct/themi_ip.html

ご清聴ありがとうございました

【お問い合わせ先】
株式会社オージス総研
TEL: 03-6712-1201 / 06-6871-8054
mail: info@ogis-ri.co.jp