モバイル、オープンAPIを活用するための認証基盤

（標準技術 OpenID Connect, OAuth 適用の考え方）

株式会社オージス総研
サービス事業本部 テミストラクトソリューション部
八幡 孝

自己紹介

八幡 孝

株式会社オージス総研
統合認証ソリューション担当

OpenAMコンソーシアム
副会長

OpenIDファウンデーション・ジャパン
Enterprise Identity WG
リーダー

統合認証ソリューションを15年以上やってきました

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（テミストラクト）
Identity Platform AWS対応版

クラウド、IoT時代の
“All in one”
統合認証パッケージ

認証基盤のユースケースが拡大

ユースケース	狙い・特長
社内システム利用のガバナンス強化	認証処理の一元化、人事システム等と連動したタイムリーなIDメンテナンス。
取引先へのシステム提供	取引先ユーザーの確実な認証。IPアドレスや電子証明書の併用。
クラウドサービス利用時、スマホ・タブレット利用時の認証強化	社外からの利用の制限。社外での利用時の追加の認証の実施。社用端末の識別。 クラウドサービスのIDメンテナンス。
顧客（一般消費者）向けの情報提供、サービス提供	SSOによる顧客への利便性の提供。複数アプリへの展開。収集した属性の活用。他社サービスとの連携。

これからは モバイルアプリ と オープンAPI対応 が必要に

ユースケース	狙い・特長
社内システム利用のガバナンス強化	認証処理の一元化、人事システム等と連動したタイムリーなIDメンテナンス。
取引先へのシステム提供	取引先ユーザーの確実な認証。IPアドレスや電子証明書の併用。
クラウドサービス利用時、スマホ・タブレット利用時の認証強化	社外からの利用の制限。社外での利用時の追加の認証の実施。社用端末の識別。 クラウドサービスのIDメンテナンス。
顧客（一般消費者）向けの情報提供、サービス提供	SSOによる顧客への利便性の提供。複数アプリへの展開。収集した属性の活用。他社サービスとの連携。
モバイルアプリ化、オープンAPI活用によるアプリ機能、サービスの高度化	• アプリ内にパスワード保存不要な安全な認証方式、SSOに対応できる認証方式への対応。 • 利用者同意に基づく必要最少権限でのデータ連携を実現する認証・認可方式への対応。

どちらのサービスにも関わる話題です

従業員向け
サービス

顧客向け
サービス

なぜ認証基盤を作るのか？

（おさらい）

認証基盤を作るメリット

① 利用者が便利になる

- 作業効率の向上
- IT活用の促進

② セキュリティレベルのばらつきがなくなる

- 開発者に依存したばらつき
- ユーザーに依存したばらつき

③ システム開発がしやすい

- アプリ毎の認証機能開発は不要
- サブシステムに分割した開発の実現

④ 認証方式の変更がやりやすい

- ID/パスワードを使った認証
- 多要素認証への対応
- 新しい方式への対応

セキュリティのための認証基盤

“Identity is the new perimeter.”

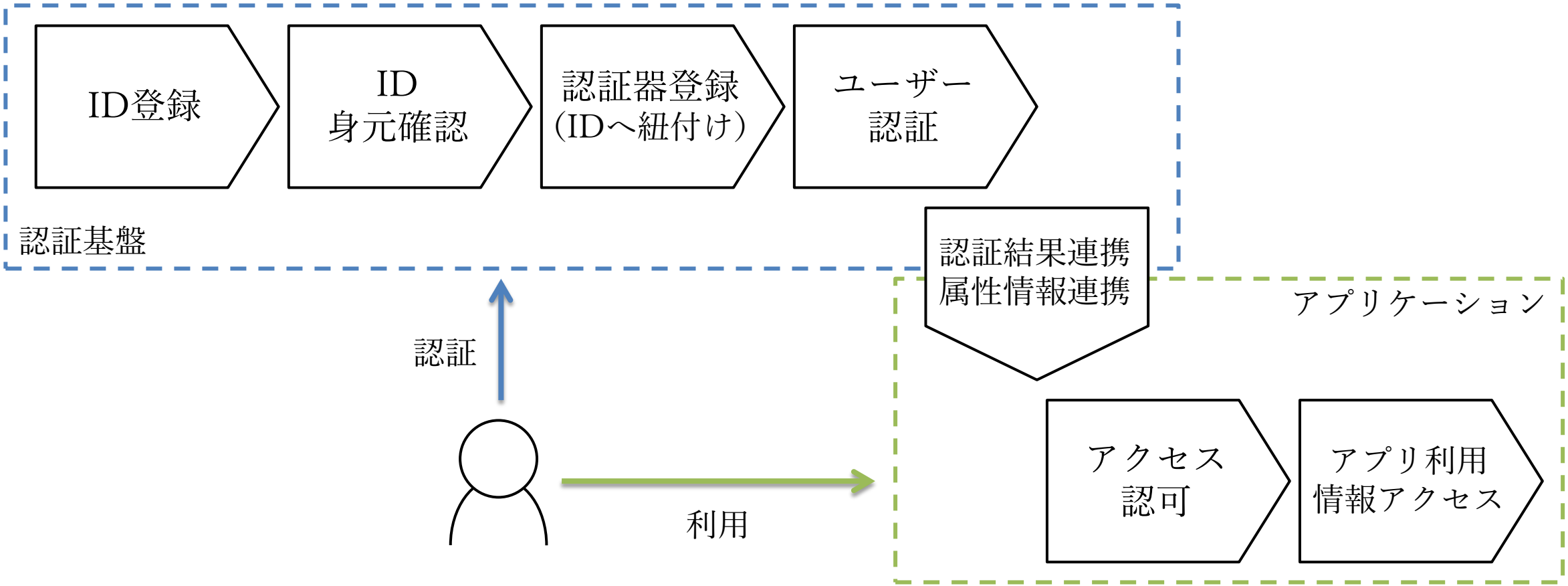
ロ ネットワーク型の境界防御が効かない時代になった

- 守るべき情報資産は壁 (Firewall) の外にある
- アクセスする主体は壁の中にも外にもいる

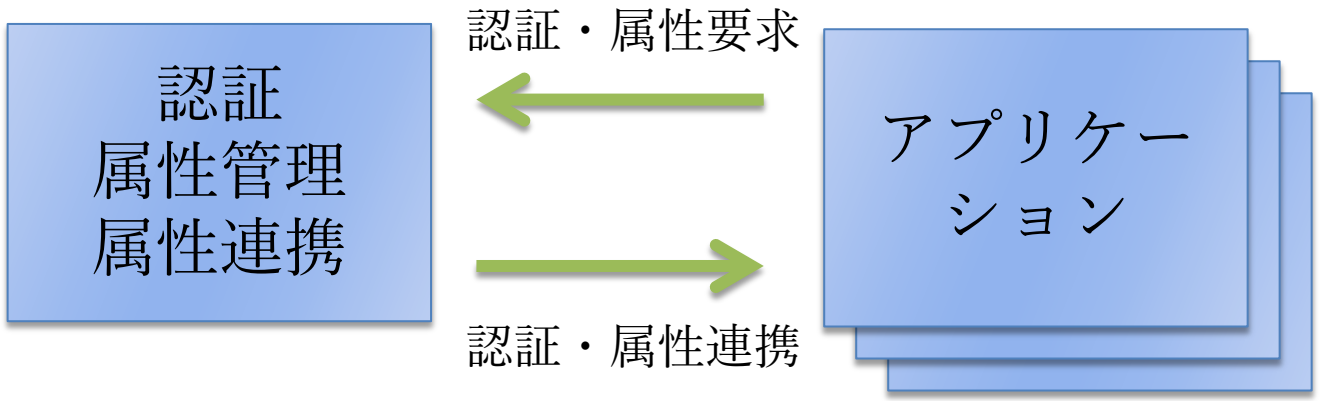
ロ アイデンティティを用いた情報へのアクセス管理が重要に

- アイデンティティによるアクセスの制御
- アイデンティティによるアクセスの監視

アイデンティティ＆アクセス管理のフロー



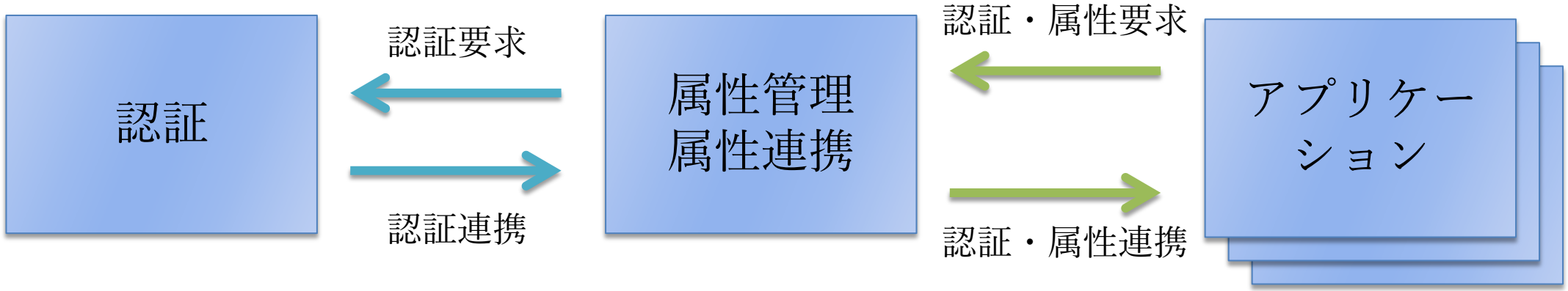
認証基盤を作る・サービスを展開する



ユーザーの認証
アプリが必要とする
属性の管理、提供、記録

ユーザーごとに
最適化された
サービスを提供

外部IdP活用で、より使いやすく、より管理しやすく



外部の信頼できる
認証システム(IdP)を利用

ドメインログオン、
Google, Facebook, Yahoo! JAPAN, ...

アプリが必要とする
属性の管理、提供、記録

ユーザーごとに
最適化された
サービスを提供

アイデンティティ連携を実現する標準技術たち

これらの技術は標準化が進み、製品・サービスへの実装も浸透している。

モバイル向けアプリの認証を考える

モバイル向けアプリの分類

ロ モバイルアプリ（ネイティブアプリ）

- iOS, Android, ...
- ストア or モバイルアプリ管理(MAM) を通じた配布

ロ モバイルウェブ

- ウェブブラウザ + JavaScript
- SPA (Single Page Application)
- PWA (Progressive Web Application)
- 配布不要、ブラウザアクセスで利用

モバイル向けアプリの導入・提供の形態

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

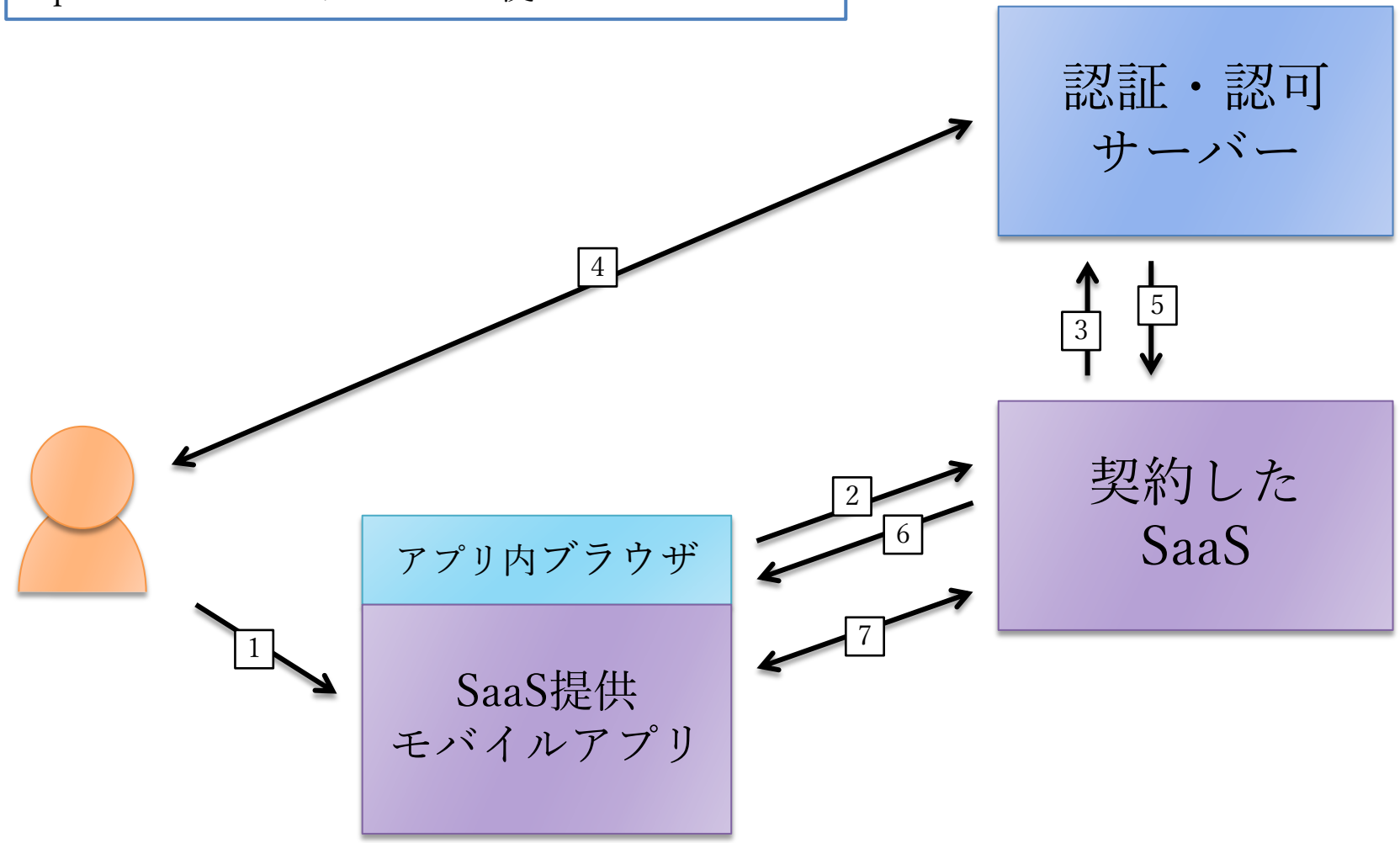
認証・アクセス認可の実装の考え方

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	OpenID Connect や SAML を使ったSaaSへのSSO	—
モバイルウェブの開発と提供	OAuth 2.0 Implicit Grant を用いたバックエンドAPIへのアクセス認可	
ネイティブアプリの開発・提供	OAuth 2.0 for Native Apps のプラクティスを用いたバックエンドAPIへのアクセス認可	
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	OAuth 2.0 を用いたAPI連携時認証・アクセス認可 Implicit, Authz Code, Authz Code+PKCE （OIDF FAPI WGの動向の考慮も必要）

外部サービスのモバイル向けアプリの利用

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

OpenID Connect や SAML を使ったSaaSへのSSO

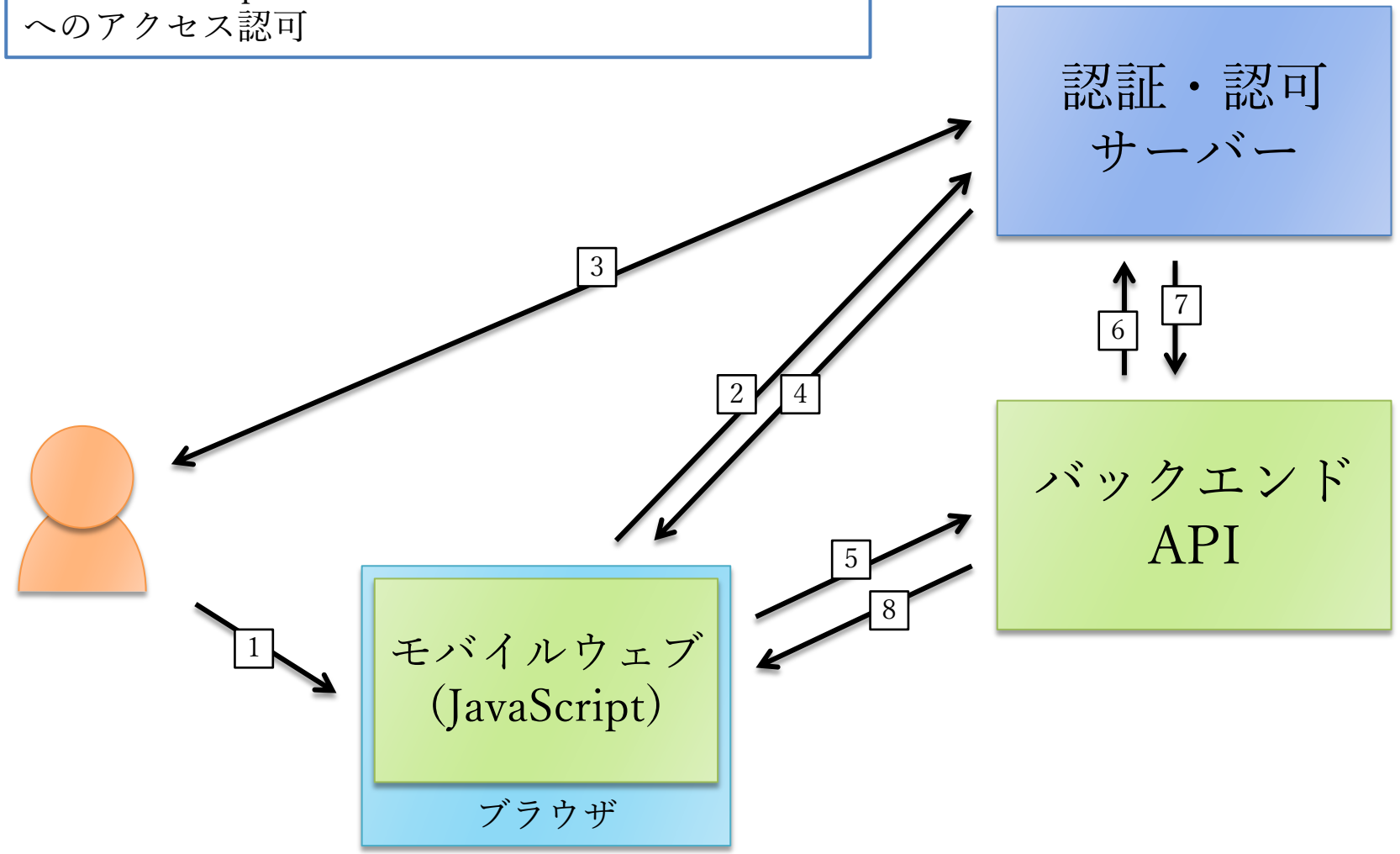


1. SaaSのモバイルアプリを起動、ログイン
2. モバイルアプリが**ブラウザベースのUI**でSaaSの認証画面へ
3. SSOの設定により自社の認証サーバーへ認証要求 (SAML or OpenID Connect を使用)
4. ユーザー認証を実行
5. 認証結果を連携
6. ログイン完了
7. モバイルアプリでSaaSを利用

モバイルウェブでのバックエンドAPIアクセス認可

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

OAuth 2.0 Implicit Grant を用いたバックエンドAPIへのアクセス認可



1. ブラウザでモバイルウェブを起動、ログイン
2. リダイレクトによりOAuth認可を要求
3. ユーザー認証を実行
4. バックエンドAPIアクセス用のアクセストークンを返却
5. アクセストークンをつけてバックエンドAPIにアクセス
6. ~7. アクセストークンの情報を確認（ユーザー、Scope、有効期限、など）
8. バックエンドAPIが情報を使ってモバイルウェブが動作

Implicit Grant か RO Passwd Creds Grant か?

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

- 1st Party のリソース (API) アクセス。
  Resource Owner Password Credentials Grant でも良いケース。
- Implicit Grant を使い、ブラウザレベルでログインしておくことで、他のアプリのSSOが可能に。（ログイン状態を保っていれば）
- ブラウザベースのUIのため、認証サーバーが提供する多要素認証方式、外部IdPと連携したログインなどに対応できる。

モバイルウェブ アクセス前の認証とAPIアクセス

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

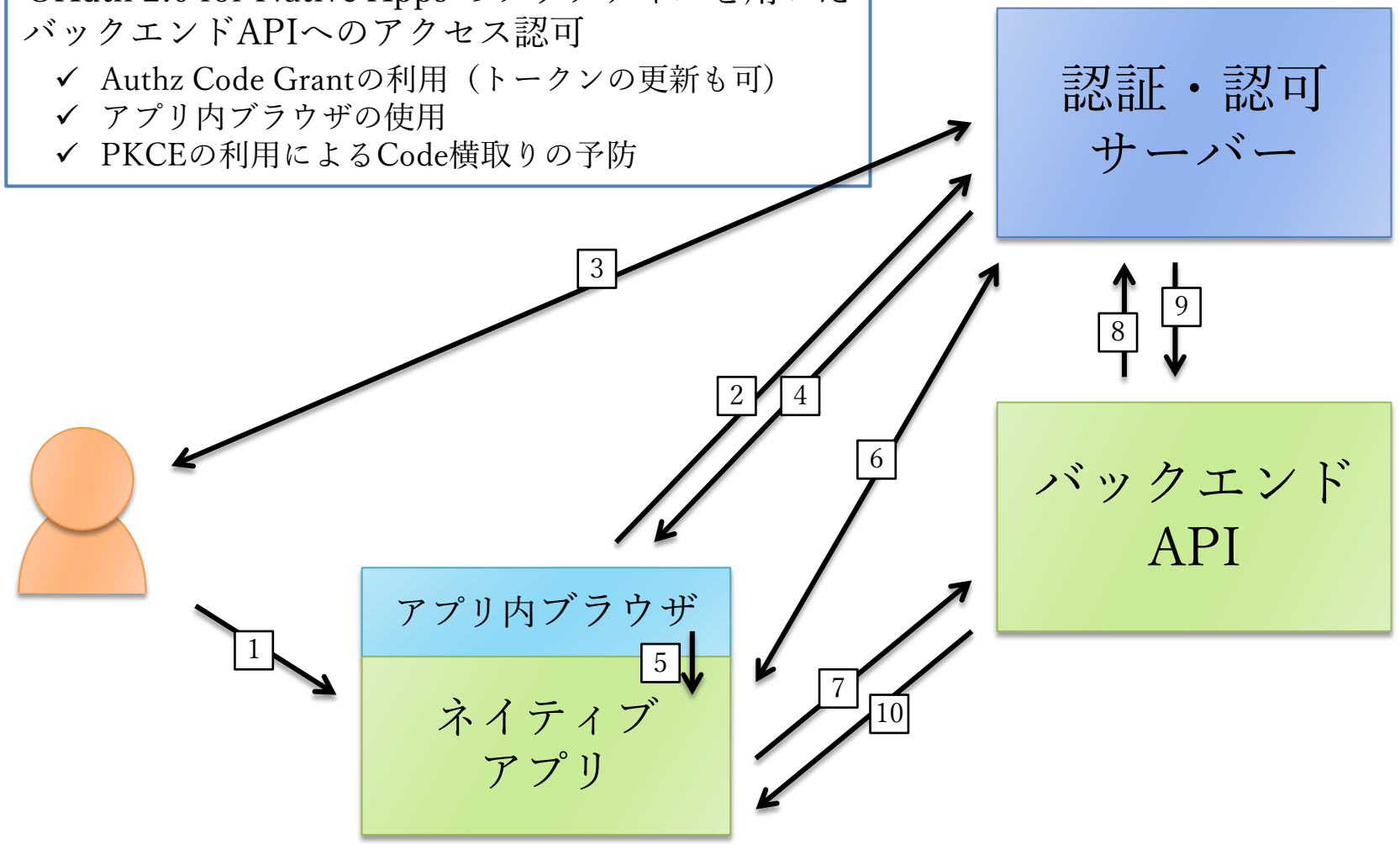
- 企業利用の場合、モバイルウェブ（HTML+JS）へのアクセス時点で認証サーバーでの認証を要求する構成とすることも多い。
- ブラウザレベルで認証済みとなっているため、p20, Step 3 の認証はインタラクション無しで完了して、モバイルウェブの利用ができる。（SSOされる）

ネイティブアプリでのバックエンドAPIアクセス認可

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

OAuth 2.0 for Native Apps のプラクティスを用いたバックエンドAPIへのアクセス認可

- ✓ Authz Code Grantの利用（トークンの更新も可）
- ✓ アプリ内ブラウザの使用
- ✓ PKCEの利用によるCode横取りの予防

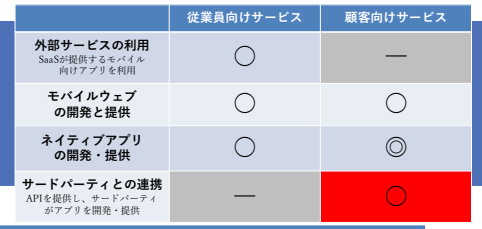


1. ネイティブアプリを起動、ログイン
2. アプリ内ブラウザを使いOAuth認可を要求（PKCEを併用）
3. ユーザー認証を実行
4. アクセストークンを取得するためのCodeを返却
5. アプリ内ブラウザからネイティブアプリにCodeを返却
6. Codeをアクセストークンに交換（PKCEを併用）
7. アクセストークンをつけてバックエンドAPIにアクセス
8. ~9. アクセストークンの情報を確認（ユーザー、Scope、有効期限、など）
10. バックエンドAPIが情報を使ってネイティブアプリが動作

バックエンドAPIの振る舞いは、モバイルウェブ、ネイティブアプリで共通。

オープンAPIでのアクセス認可の考慮点

対応しておくべき OIDC/OAuth のフロー



	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

#	ユーザーへの提供形態	バックエンド	OIDC/OAuthのフロー	ポイント
①	**ブラウザで動作するJavaScriptアプリ** (モバイルウェブ、SPA、など)	あり	Authz Code Flow	バックエンドがオープンAPIへアクセス。バックグラウンドでのAPIアクセスのため、トークン自動更新が必要な場合も。
②		なし	Implicit Flow	JSアプリがオープンAPIへアクセス。トークン更新が必要な場合はブラウザを介して行なえる。
③	**ネイティブアプリ**	あり	Authz Code Flow	（①と同じ）
④		なし	Authz Code Flow w/ PKCE	ネイティブアプリがオープンAPIへアクセス。バックグラウンドでのAPIアクセスのため、トークン自動更新が必要な場合も。
⑤	**Webアプリ**	あり (Webアプリサーバー)	Authz Code Flow	WebアプリケーションサーバーがオープンAPIへアクセス。バックグラウンドでのAPIアクセスのため、トークン自動更新が必要な場合も。

異なるレベルのAPI提供に対応できる API連携認証システム機能の必要性

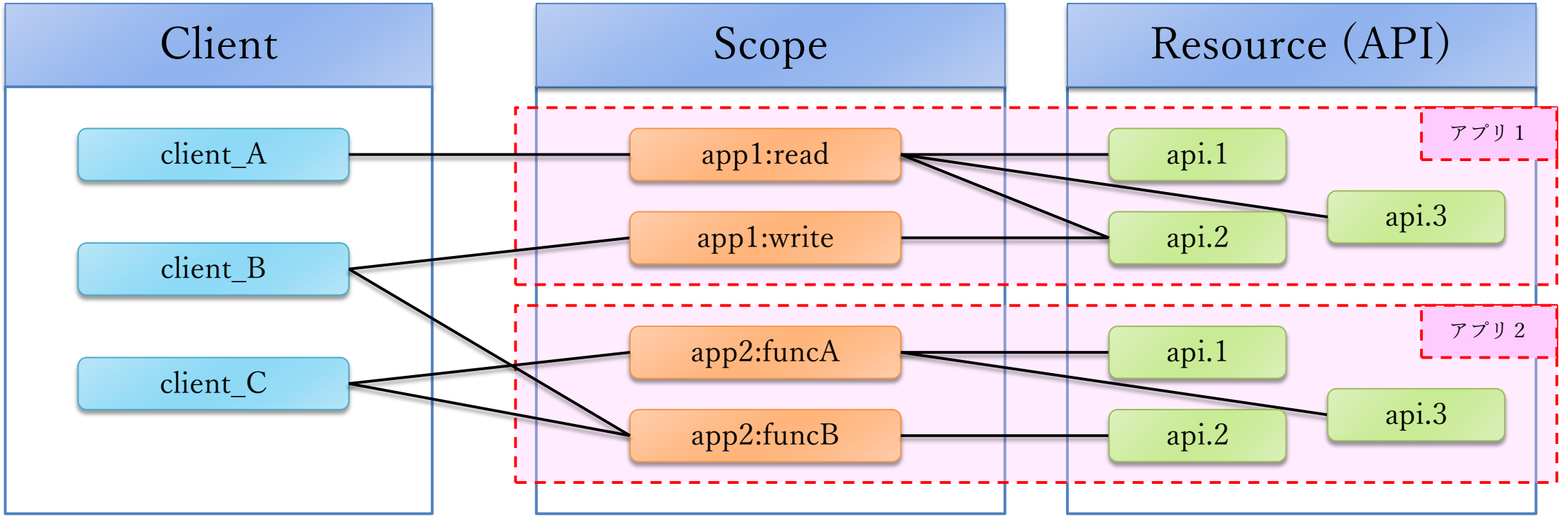
	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○

API提供が進むと提供側の意図と矛盾が生じない認証・認可が課題となる

使うScope, 有効時間、認証方式、などを設定（利用側の意図）

使うScope, 有効時間、認証方式、などを設定（提供する側の意図）

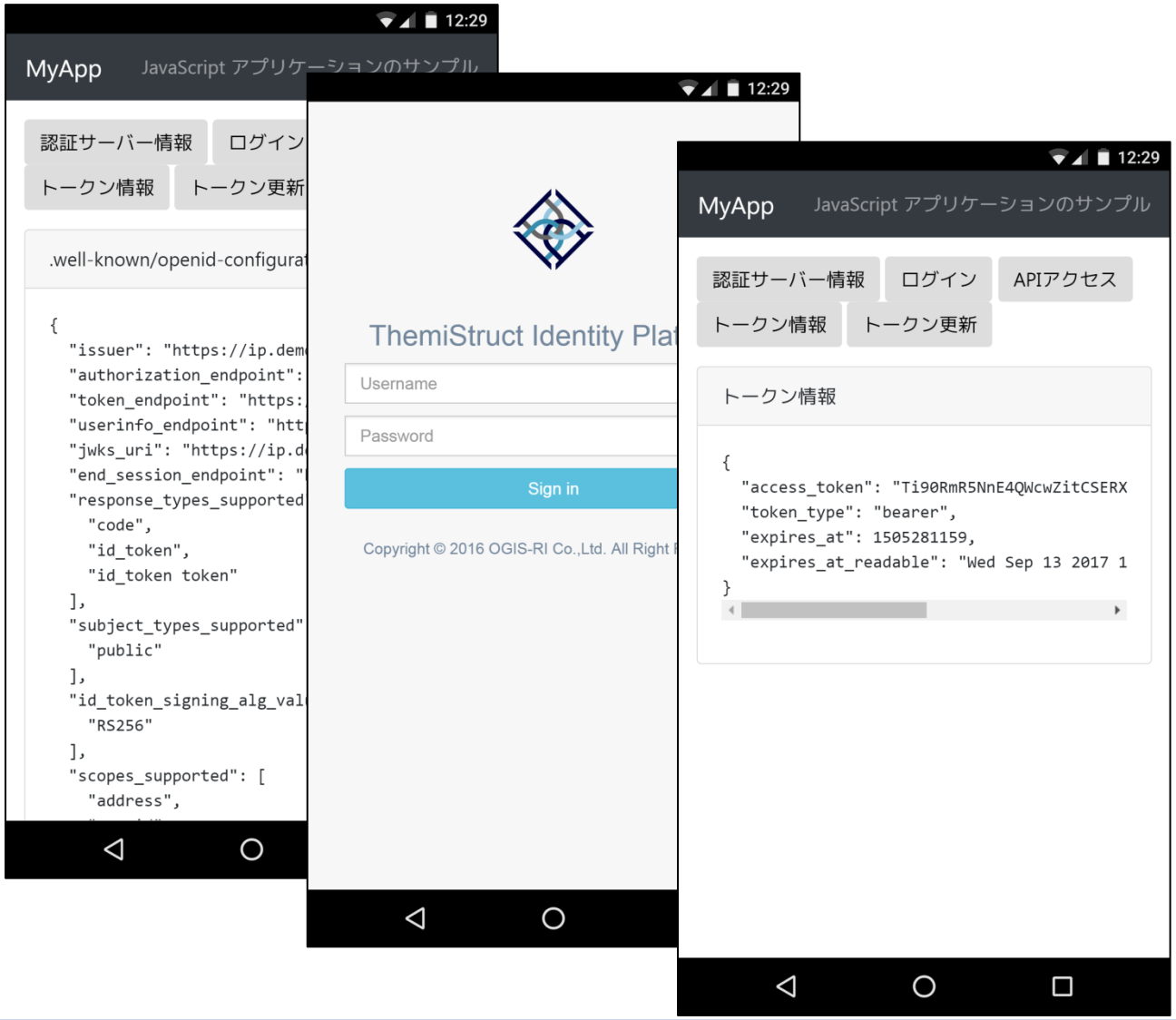
重要情報へのアクセス、重要な操作の実行時は有効時間を制限、多要素認証や再認証を要求するなど、APIのレベルに合わせた認証・認可が必要に



ThemiStruct Identity Platform を使った実装例

oidc-client-js [1] + ThemiStruct でモバイルウェブ

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○




```
var settings = {
    authority: 'https://ip.demo.example.com/oauth/v2',
    client_id: 'xxxxxxxxxxxxxxxxxxxxxxxxxxxx',
    redirect_uri: 'https://app.example.com/',
```

```
var manager = new Oidc.UserManager(settings) ;
manager.signinRedirect() ;
```

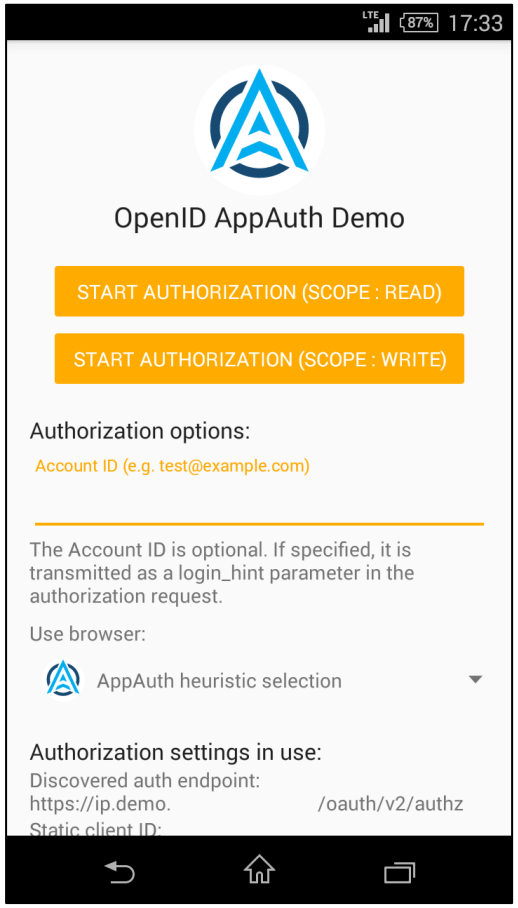
```
manager.signinRedirectCallback().then(function (u) {
    // ログイン成功
}).catch(function (e) {
    // ログイン失敗
}) ;
```

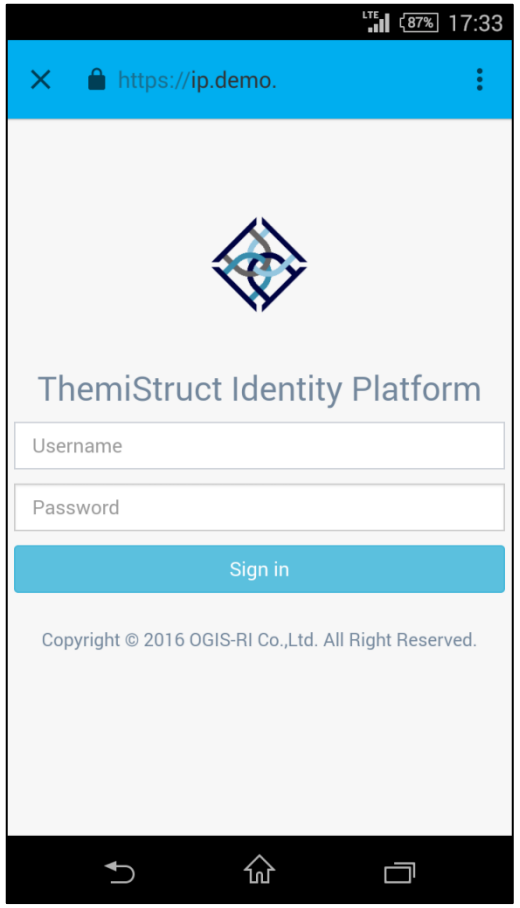
```
manager.getUser().then(function (u) {
    if (!u || u.expired) {
        return Promise.reject(new Error('invalid token')) ;
    }
    var token = u.access_token ;
```

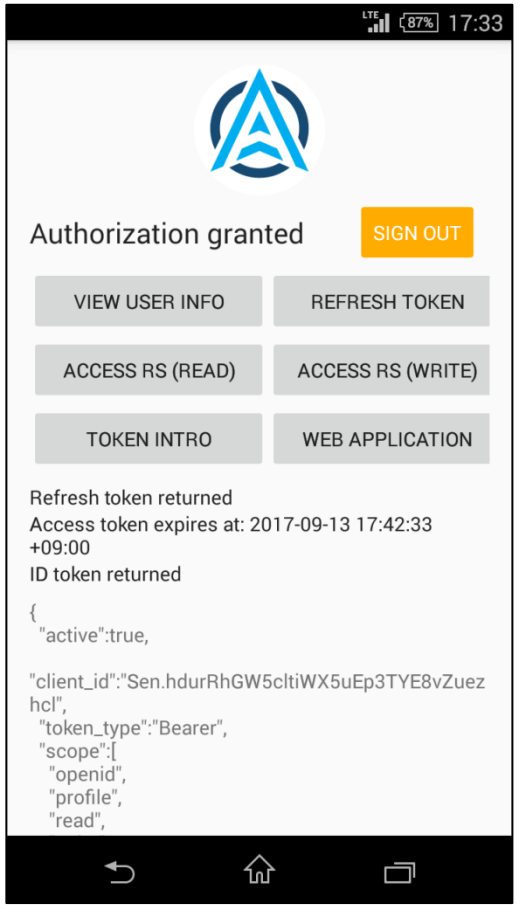
[1] https://github.com/IdentityModel/oidc-client-js

AppAuth for Android [2] + ThemiStruct でネイティブアプリ

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○







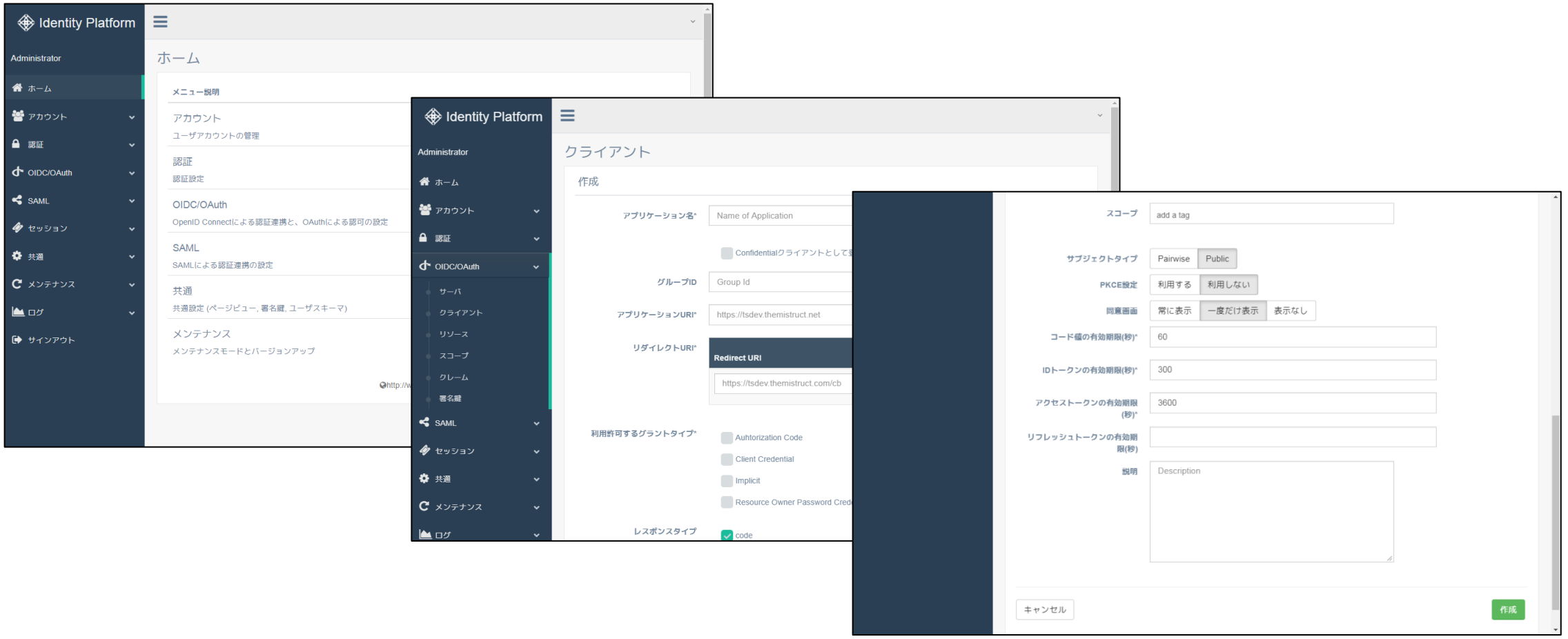
- Authz Code Grant
- PKCE
- Chrome Custom Tabs
- Token Introspection (Server Side)

AppAuthに含まれるデモアプリにパッチしてテスト中...

[2] https://appauth.io/

APIの提供のための OAuth Client と Scope の定義

	従業員向けサービス	顧客向けサービス
外部サービスの利用 SaaSが提供するモバイル向けアプリを利用	○	—
モバイルウェブの開発と提供	○	○
ネイティブアプリの開発・提供	○	◎
サードパーティとの連携 APIを提供し、サードパーティがアプリを開発・提供	—	○



ただいま開発中...

ThemiStruct テミストラクト

Identity Platform AWS対応版

プロミネンスⅢ 展示会場 にて
次期バージョンの先行展示しています。
ぜひお立ち寄りください。

当社ソリューションのご紹介

統合認証ソリューション ThemiStruct を提供しています

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

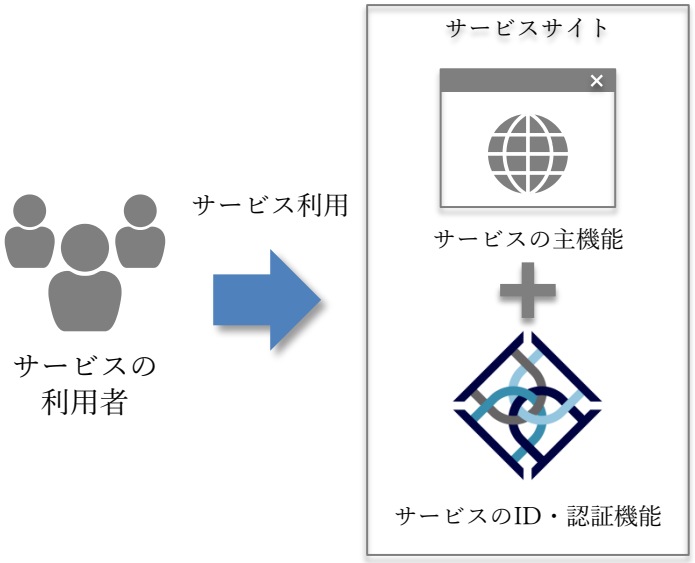
ThemiStruct（テミストラクト）
Identity Platform AWS対応版

クラウド、IoT時代の
“All in one”
統合認証パッケージ

統合認証パッケージ ThemiStruct Identity Platform

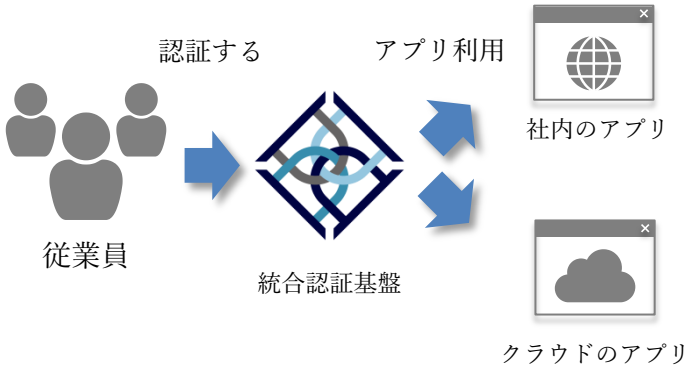
ThemiStruct Identity Platform は、ITシステム利用者のアイデンティティ管理と認証の機能を提供します。顧客向けにサービスを展開したり、従業員向けにアプリケーションを展開する際に必要となる、共通ID基盤の構築に活用いただけます。

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

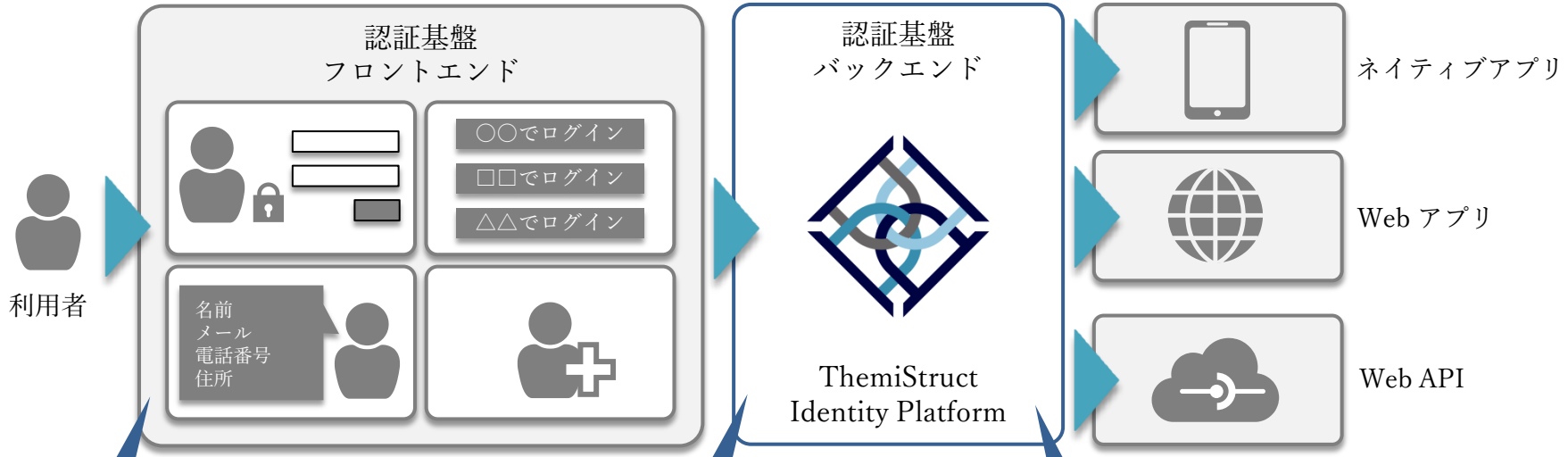
エンタープライズ領域に活用



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 を『顧客向けサイト』に活用

ThemiStruct Identity Platform を『顧客向けサイト』環境に適用した場合、サービスの顧客IDの管理と認証の機能を担うバックエンドサービスとして稼働します。これらの機能のUIにあたるアプリケーションの実装を支援し、また、実際のサービスアプリと接続するためのインタフェースを提供します。



IDと認証の機能をアプリに組み込む

ユーザ認証機能やアカウント機能を統一された見た目で提供することができます。

伸縮自在にスケール

突発的なアクセス集中やスモールスタートが可能なプラットフォームです。

短期間での導入が可能

約2時間の構築作業で、性能や可用性が担保された認証プラットフォームが誕生します。

『顧客向けサイト』に向けた3大特長

ロ　IDと認証の機能をアプリに組み込む

- IDと認証に関連する画面の実装を支援する『フレームワーク』や『Web API』　を提供します。これらを活用し、貴社のサービスサイト対し、認証画面やパスワード変更画面を組み込むことができます。

ロ　伸縮自在にスケール

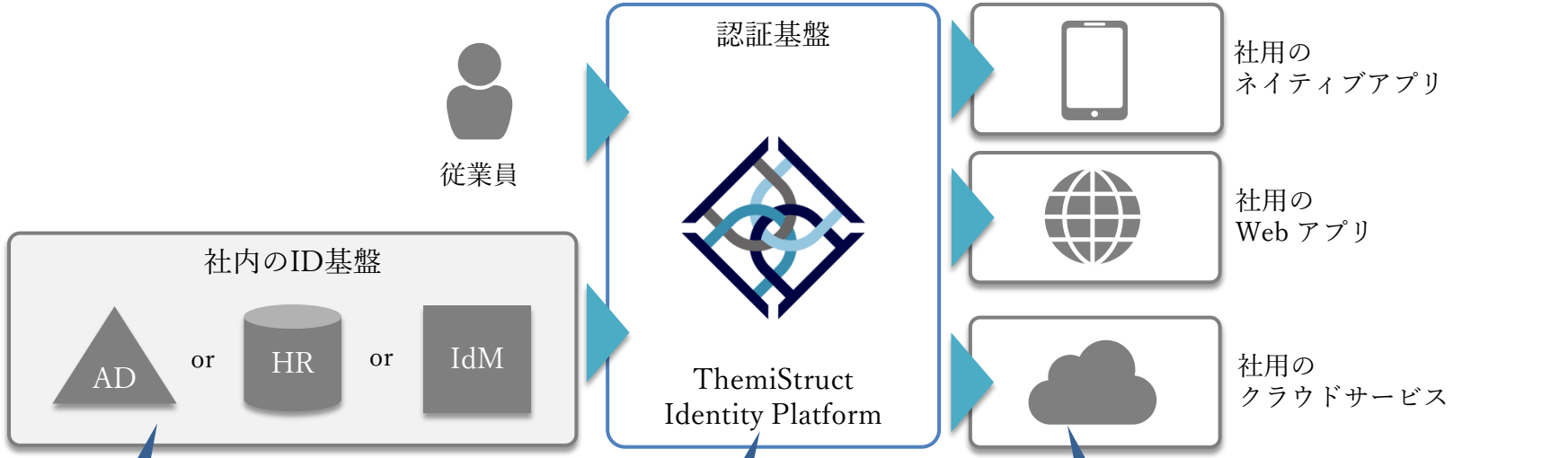
- AWS　が提供するマネージドサービスを主要コンポーネントとして活用しています。これにより、スモールスタートから大規模利用まで『自動的に伸縮』する認証プラットフォームを実現しています。

ロ　短期間での導入が可能

- AWS 上にIdentity Platform を構築するインストーラの提供を行っています。約2時間の構築作業で性能と可用性が担保された認証プラットフォームをセットアップできます。これにより、サービスの提供開始までの期間を大幅に短縮することができます。

ThemiStruct Identity Platform を『エンタープライズ』に活用

ThemiStruct Identity Platform を『エンタープライズ』環境に適用した場合、社内外のアプリケーションにシングルサインオン可能な認証基盤を提供できます。また、企業のポリシーにあった認証機能の設定や既存のIDとの統合をすることができます。



既存のID基盤と統合

社内で既に展開されたIDに関連する仕組みとの統合を実現できます。

企業ポリシーの適用

認証のポリシーを一元管理し、柔軟な認証機能の提供ができます。

シングルサインオン

社内、社外問わず、様々なアプリにシングルサインオンできます。

『エンタープライズ』に向けた3大特長

ロ　シングルサインオン

- OpenID Connectなどの標準技術仕様を用いたシングルサインオンに対応しています。ThemiStruct Identity Platform に一度サインインすることで、ユーザが利用したい各サイトへシングルサインオンできます。

ロ　企業ポリシーの適用

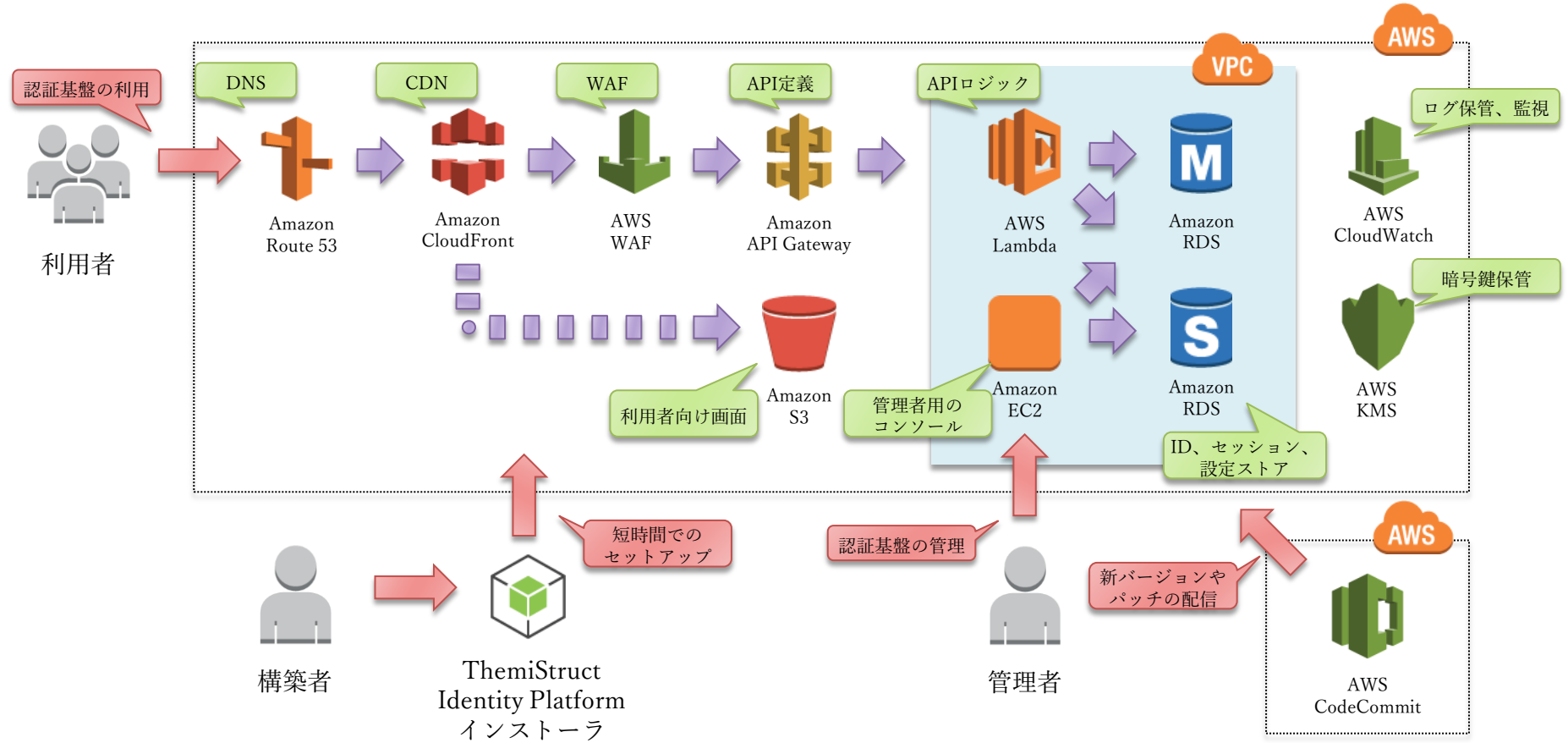
- ユーザの属性や状態、利用するアプリに応じて、柔軟な認証ポリシーをデザインすることができます。例えば、社内ネットワークからのアクセスの場合、IDとパスワードの認証を提供し、外出先からのアクセスの場合、追加でワンタイムパスワード認証を提供するといったポリシーを展開することができます。

ロ　既存のID基盤と統合

- 既存のID基盤と統合に向けたアカウント管理用のAPIを提供しています。これにより、企業のIDストアの情報を用いた認証や属性情報の連携を行うことができます。

サーバーレスアーキテクチャを採用

ThemiStruct Identity Platform は Amazon Web Services のマネージドサービス上で稼働するため、一定のアベイラビリティ、スケーラビリティを実現することができます。また、以下の構成のセットアップを約2時間で完了できるインストーラを提供しています。



まとめ

まとめ

- 従業員向けサービス、顧客向けサービスともに、今後はモバイル向けアプリの提供が不可欠に。
- オープンAPIの活用が進むことで異なるレベルのAPIに対応できるAPI連携認証システムの実現が必要となる。
- OpenID Connect, SAMLといったID連携の標準技術に加え、OAuth 2.0 の標準仕様群に対応できる認証基盤が必要となる。
- ThemiStruct Identity Platform 次期バージョンでは、これらの機能を強化し、さらに重要性を増す認証基盤の実現に対応。

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 / 06-6871-7998
mail: info@ogis-ri.co.jp