ThemiStruct
テミストラクト

クラウド・モバイル活用、今企業に求められる認証基盤

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
古賀　俊廣

自己紹介

名前

古賀 俊廣（こが としひろ）

所属

テミストラクトソリューション部

領域

自社開発認証基盤(Apache)、
OpenSSO、OpenAM、EJBCA、
OpenIDM、ThemiStruct

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

統合認証ソリューションの分野に携わる事10年

略歴

- 2007年から基盤部門でセキュリティソリューションの担当として
- 2009年からThemiStructブランドを立ち上げて
- 2013年からは専門部隊として
- 2015年から自社製品で

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。

クラウドサービスの認証は当り前に行なう時代

ロ 外部クラウドサービスはセキュリティを強化して使う

- ➢ 活用推進する上でセキュリティは不可欠、社内標準のセキュリティを適用出来るかで対応方針が変化する

ロ Hybridクラウドでのシングルサインオンの実現

- ➢ クラウドサービスへの認証
  - ● サービス側で対応している認証方式に合わせた対応
  - ● フェデレーションでのSSO
- ➢ 自社システムの認証
  - ● 既存の仕組みを利用して認証基盤側でフィットさせる
  - ● リバースプロキシ or エージェントを用いたSSO

モバイルの認証もパターンが見えてきた

- **モバイル端末を特定し、適切に認証する**
  - 社有端末、BYOD…etc
- **情報漏えい、シャドーIT対策**
  - 認証の組み合わせにより強固な認証を実現
    - 多要素認証、２段階認証
  - スマートデバイス、持ち歩き端末のみ認証を強化する
    - リスクの強弱に合わせて認証の強弱を変えるリスクベース認証の活用
    - B2Cの領域でも増えてきている

これから考えていかないといけない課題

- **社内ネットワークの内外にシステムや端末が増え続ける**
  - データを社外ネットワークに置くことが増えた
  - モバイル機器は社外にも社内にも多数存在
- **認証とそれに伴うユーザー登録へも要求が増している**
  - システム、デバイスに合わせた認証の提供
  - 新規サービスでも個人情報は慎重に取り扱うべき
- **モバイルアプリケーションは高度化が進む**
  - 新しいモバイル向けWebアプリケーションの技術は増えている
  - ネイティブアプリはOSの更新による仕様変更への対応

「ビジネスのデジタル変容」が拍車をかける

モバイル、クラウド、
ソーシャルの活用

ビジネスプロセス
の自動連携

ユーザー情報の
活用と分析

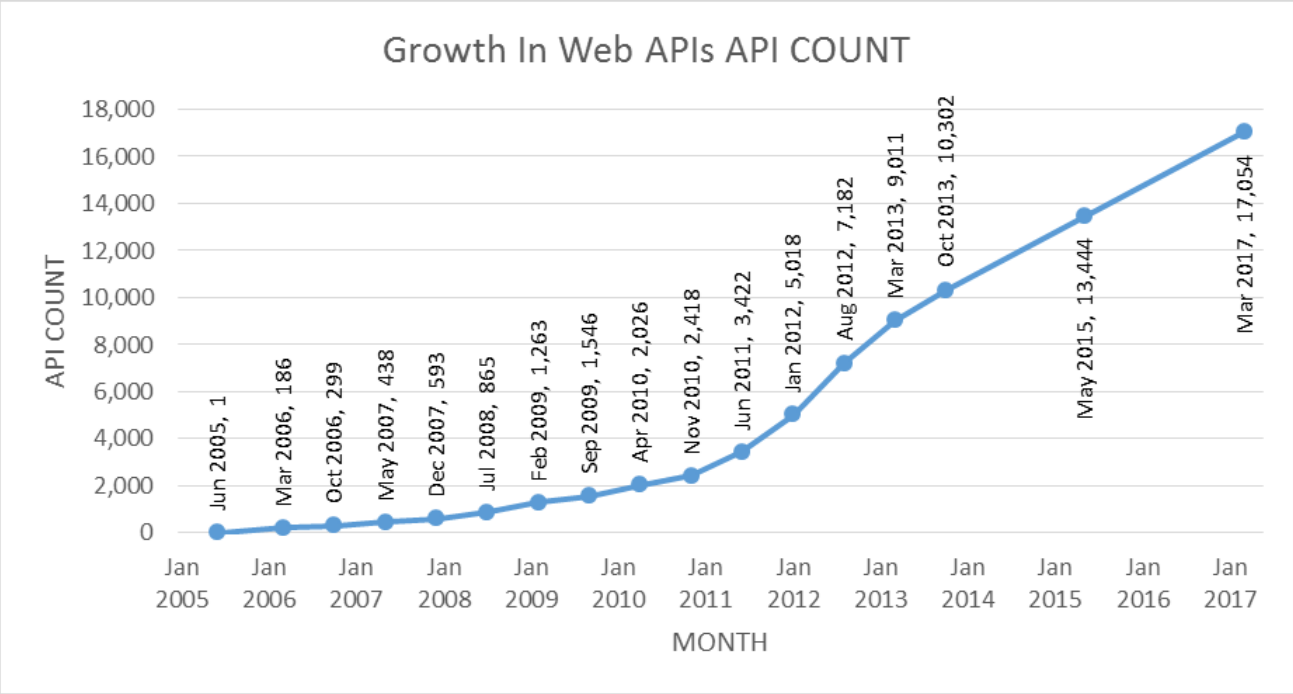
多様なデバイスの
連携、活用

- ユーザー毎に最適化されたサービスの提供
- 業務効率の向上、提供スピードの向上

Web API の利用はこれから広がっていく

増加を続ける Web API（公開型）

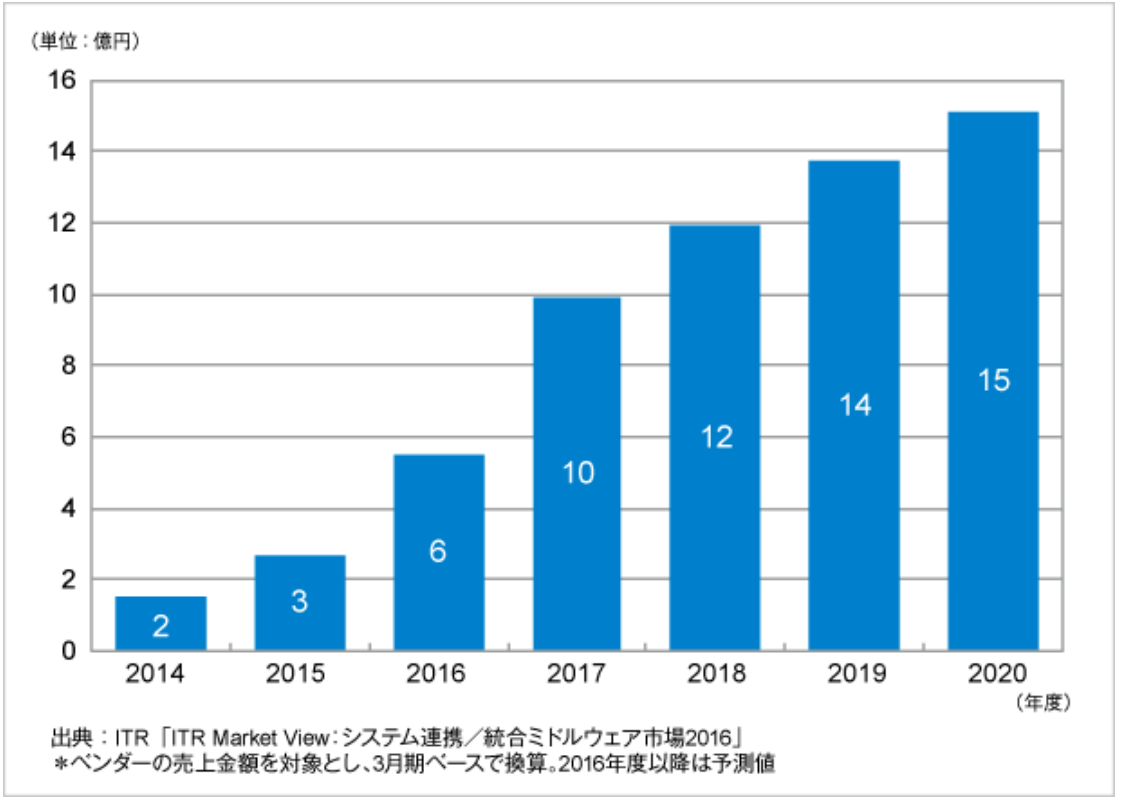
ProgrammableWebの情報を基に当社で加筆・グラフ化



引用元: https://www.programmableweb.com/api-research

「API管理市場売上金額推移および予測」

ITR社プレスリリースより



引用元: https://www.itr.co.jp/company/press/161213PR.html

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

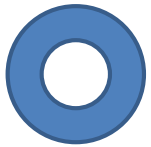
セキュリティのための認証基盤

セキュリティのための認証基盤

ロ 情報セキュリティの3要素（CIA）

- 機密性: Confidentiality
- 完全性: Integrity
- 可用性: Availability　➡　本当は最も優先されるべき要素

利用を制限するための認証基盤



クラウド、デバイス、サービスを活用してもらうための認証基盤

“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？

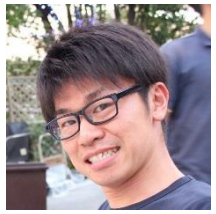
エンティティ（実体）

認証

アイデンティティ

コンテキスト

・属性の集合
・コンテキスト毎に複数



ひとりの人

アクセスする実体を
システムが認識している
アイデンティティと
紐付けること ＝ 認証

社員番号: 1234567890
名前: 古賀　俊廣
所属コード: 7777
…

名前: 古賀　俊廣
所属: オージス総研
担当セッション: AAA
…

名：俊廣
誕生日：YYYY.MM.DD
…

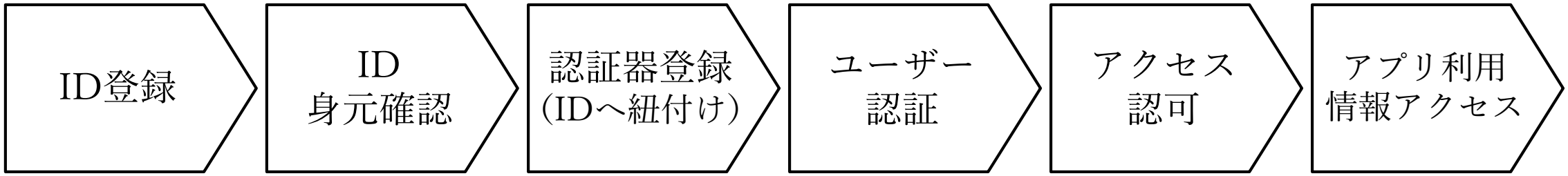
オージス総研
の社員として

講演者として

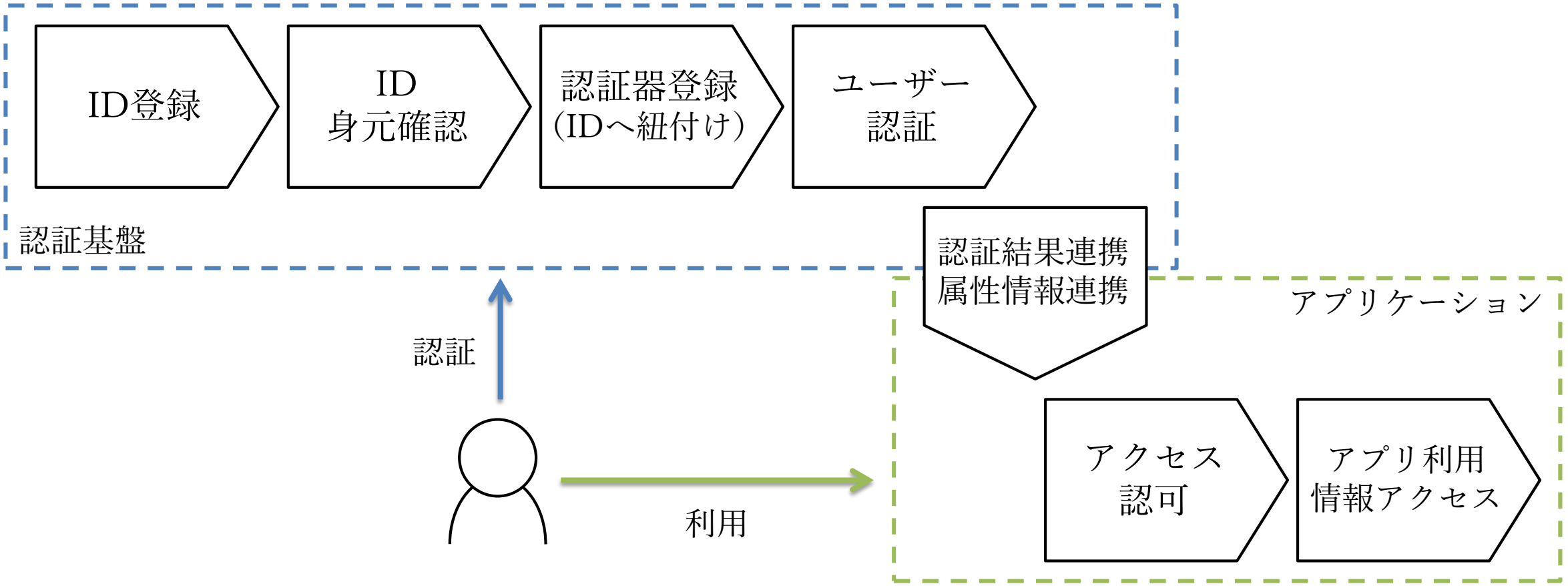
家族からみた

…

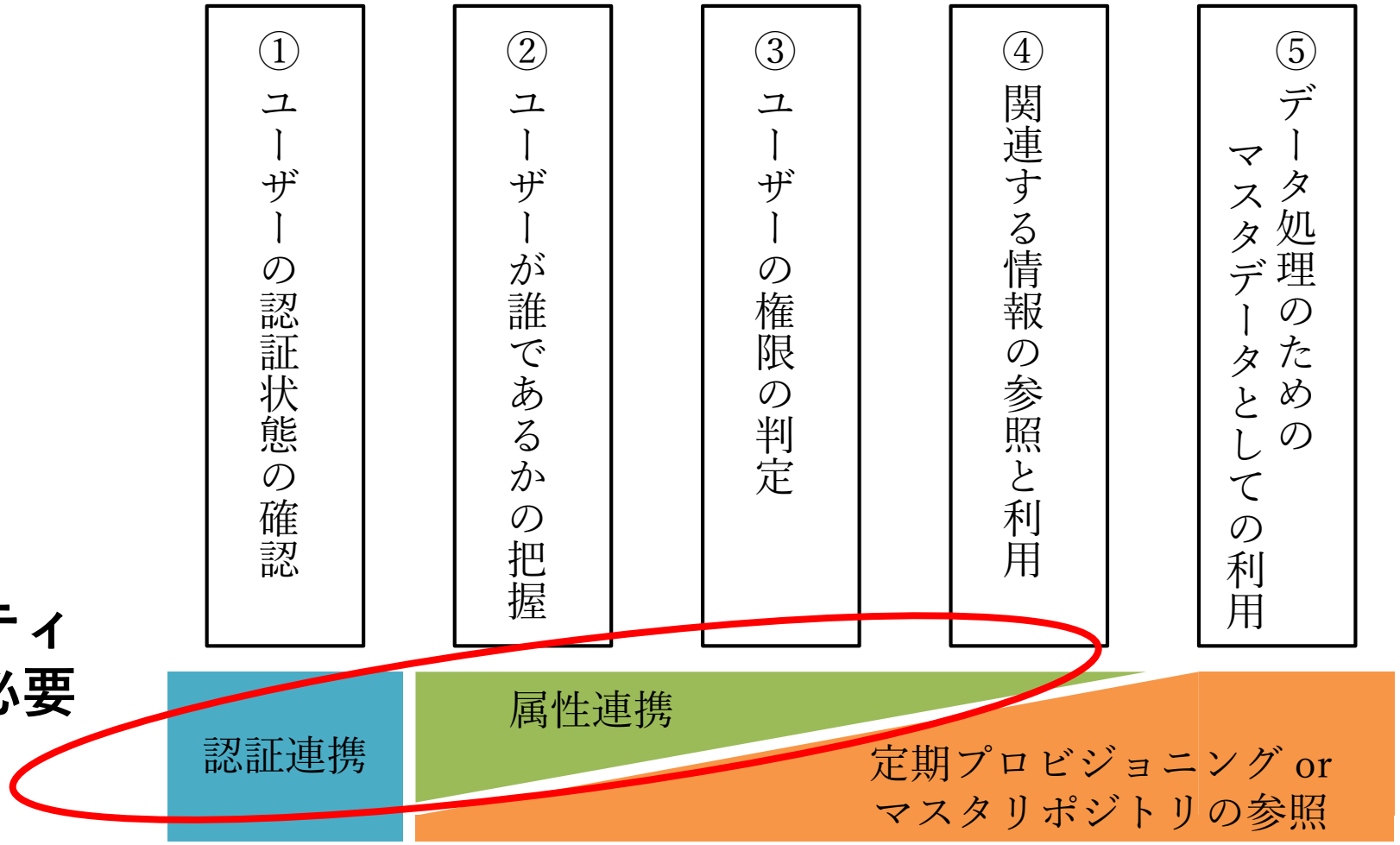
アイデンティティ＆アクセス管理のフロー



アイデンティティ＆アクセス管理のフロー

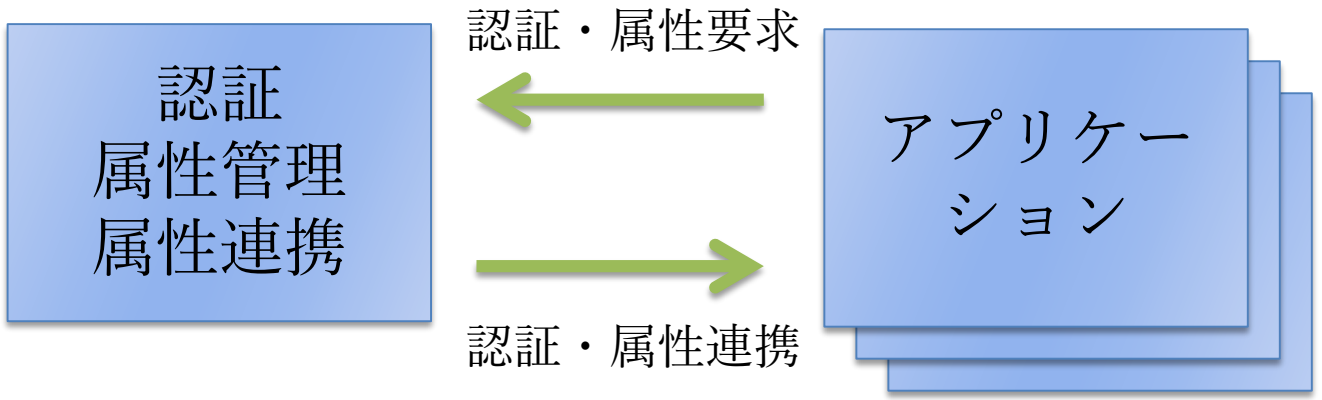


アプリケーションに必要な情報を提供する方法



アイデンティティ連携の技術が必要

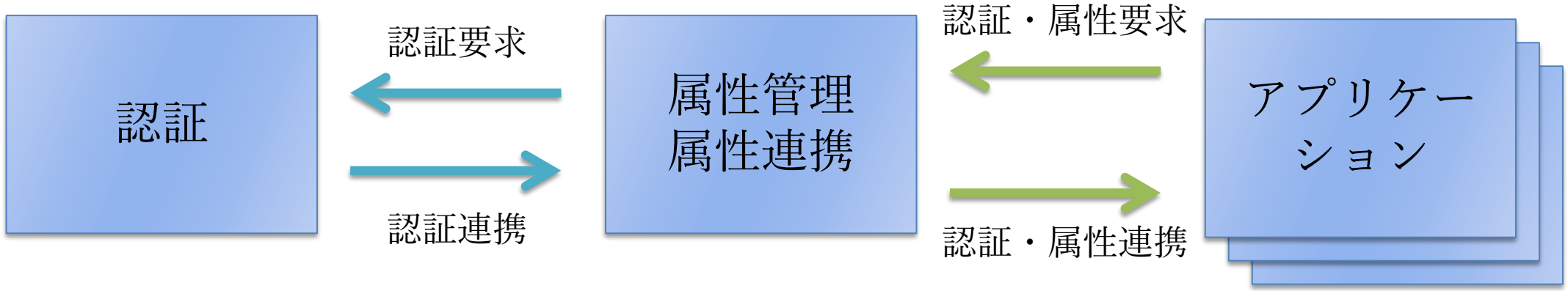
認証基盤を作る・サービスを展開する



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, ...

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

アイデンティティ技術の標準化動向

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。

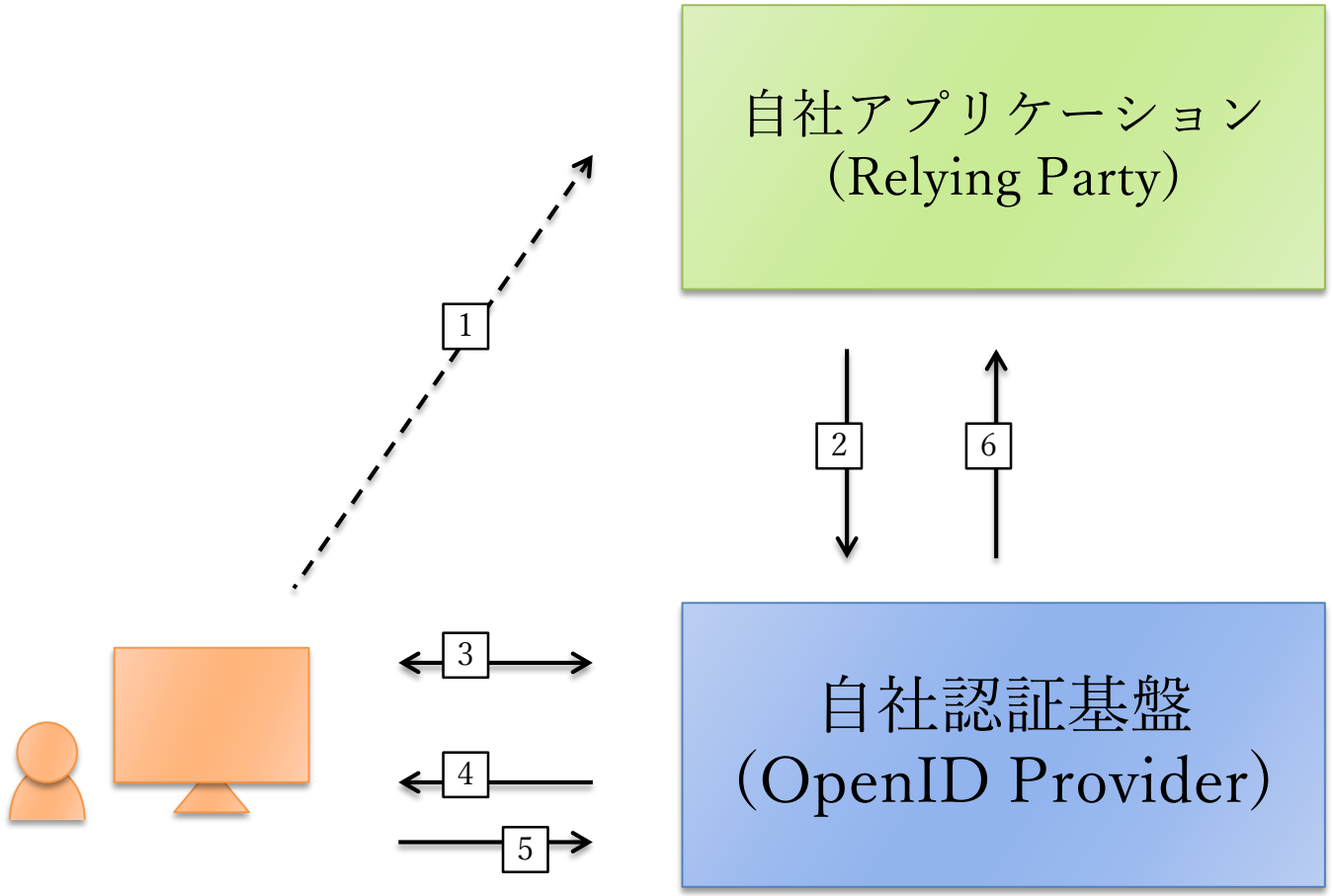
アイデンティティ連携を実現する標準技術たち

標準技術	概要
OpenID Connect	認証されたユーザーの情報（認証状態）を、サイト間、アプリケーション間で安全に伝達する仕組み。
OAuth	ユーザーの情報への特定のアクセス・操作を、情報を所有するユーザーの同意に基づき、アプリケーションに対して許可する仕組み。

認証基盤におけるOpenID Connectへの適用

ネットワークSSO	アイデンティティ技術でのSSO
画一的な自前の認証	3rdパーティーの認証の選択と活用
自社サービスのみの利用	外部サービスとの高度な接続

OpenID Connect を使ったSSO

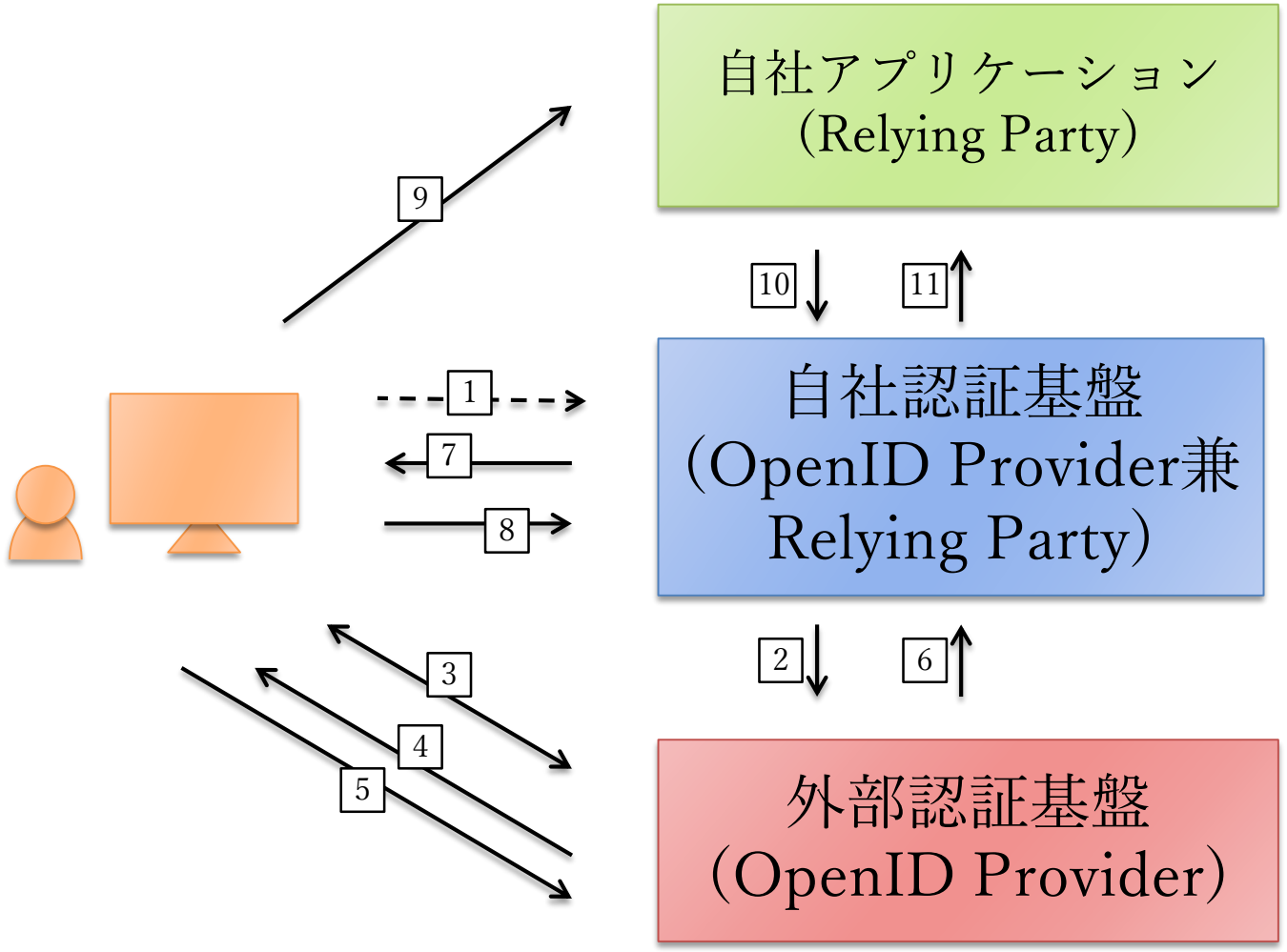


1. ユーザーがアプリケーションにアクセス
2. このユーザーは誰？
3. ユーザーを認証
4. このアプリにログインしようとしているけど良い？ユーザー名とメールアドレスを求めているけど渡しても良い？
5. いいよ
6. このユーザーは、○○さん。メールアドレスは△△。最後に認証したのはこの時刻。認証方法は□□。

ユーザー属性の連携は OpenID Connect UserInfo End Point による方法のほか、SCIM を併用した方法も採れる。

※ 概念を図示するため、実際のリクエスト・レスポンスの方法、回数等を簡略化しています。

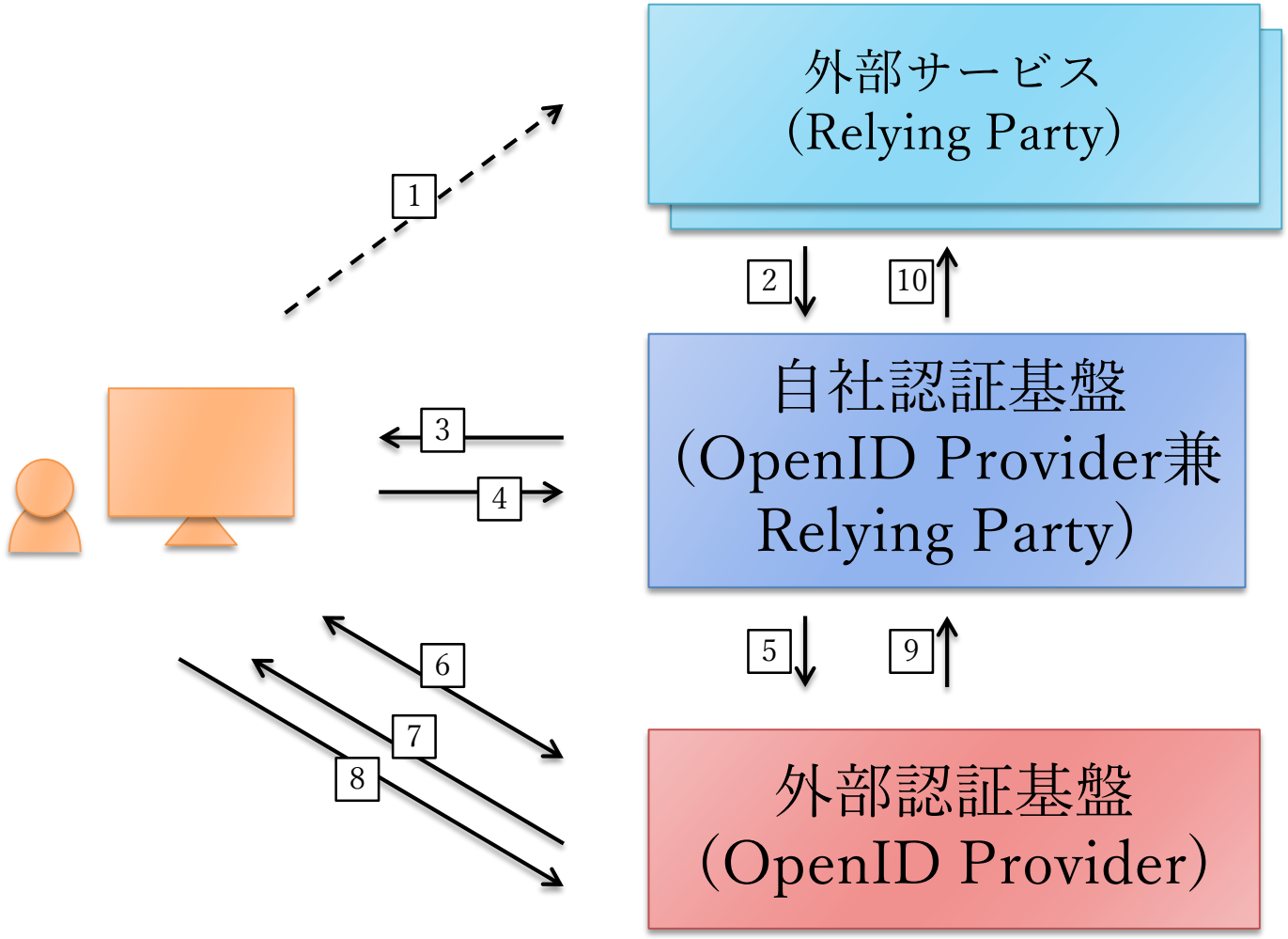
3rdパーティーの認証を使ったユーザー登録～アプリ利用



1. サービス利用したい
2. このユーザーは誰？
3. ユーザー認証
4. このサービスにユーザー情報渡しても良い？
5. いいよ
6. このユーザーは、○○さん。メールアドレスは△△。
7. この情報でアカウント作成しても良い？
8. いいよ
9～11. 外部認証基盤の結果を元に自社認証基盤の認証情報を連携し、ユーザー利用に持ち込む

※ 概念を図示するため、実際のリクエスト・レスポンスの方法、回数等を簡略化しています。

外部サービスとの相互接続



1. 外部サービス使いたい
2. このユーザー誰？
3. どの認証使う？
4. 外部認証基盤のアカウント使う
5. 外部認証基盤にユーザーの認証を要求
6. ～9. 外部認証基盤が認証結果を連携
6. ～9. 外部認証基盤が認証結果を連携
10. このユーザーは、○○さん。メールアドレスは△△。最後に認証したのはこの時刻。認証方法は□□。

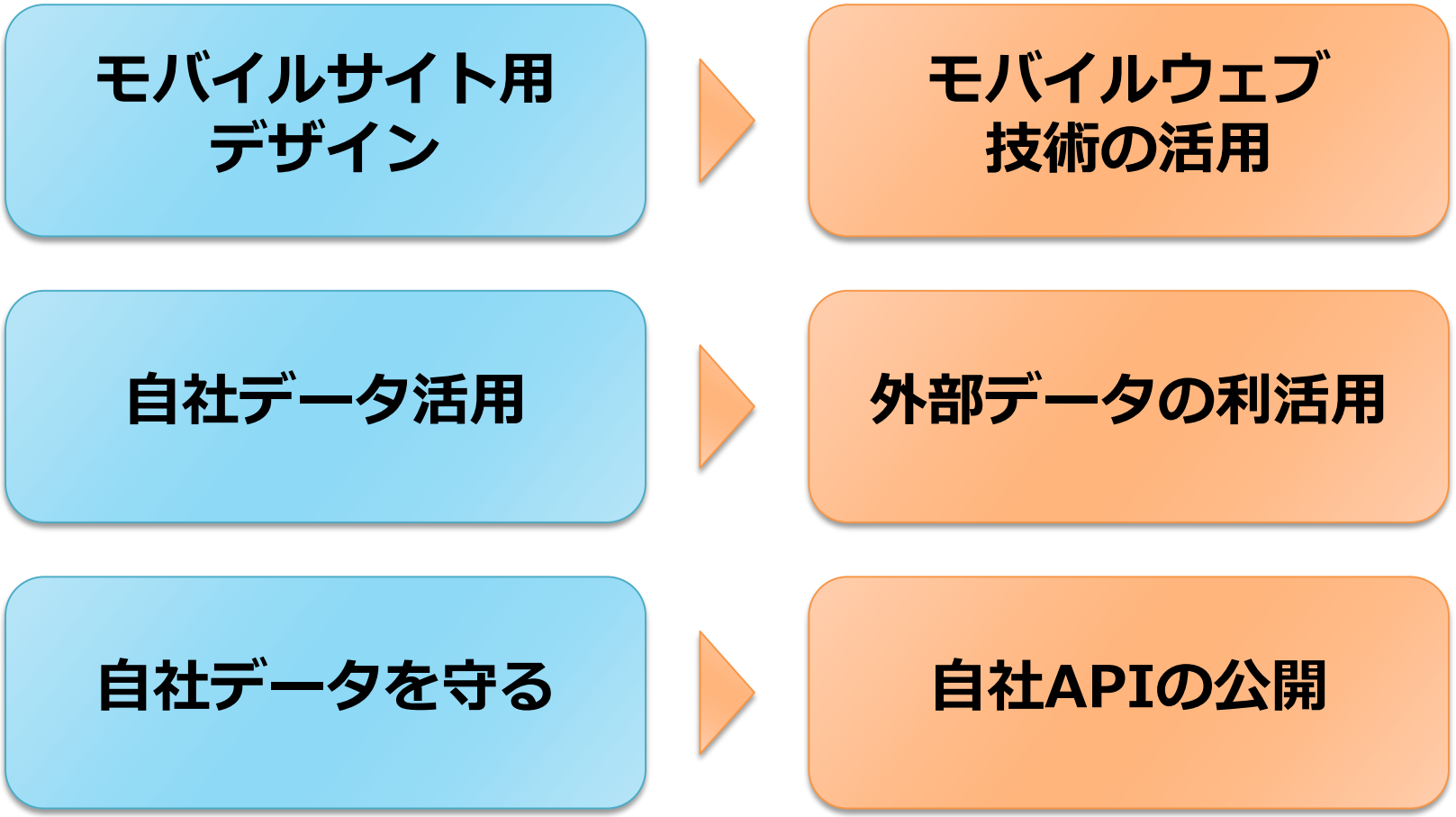
※ 概念を図示するため、実際のリクエスト・レスポンスの方法、回数等を簡略化しています。

モバイル向けアプリへの適用

モバイルアプリ は 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。

認証基盤におけるOAuthへの適用メリット



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）

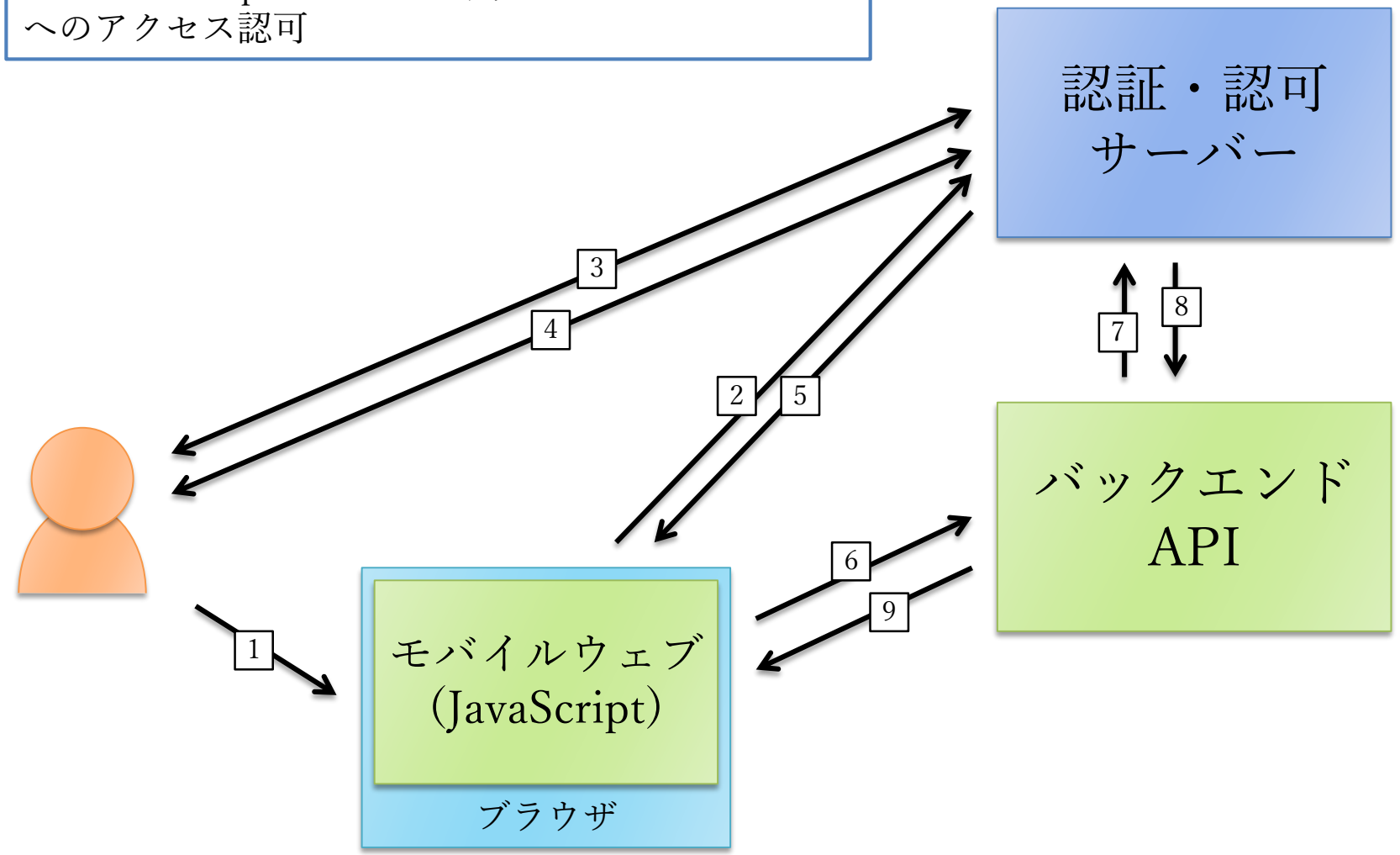
- iOS, Android, ...
- ストア or モバイルアプリ管理(MAM) を通じた配布

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

モバイルウェブでのバックエンドAPIアクセス認可

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

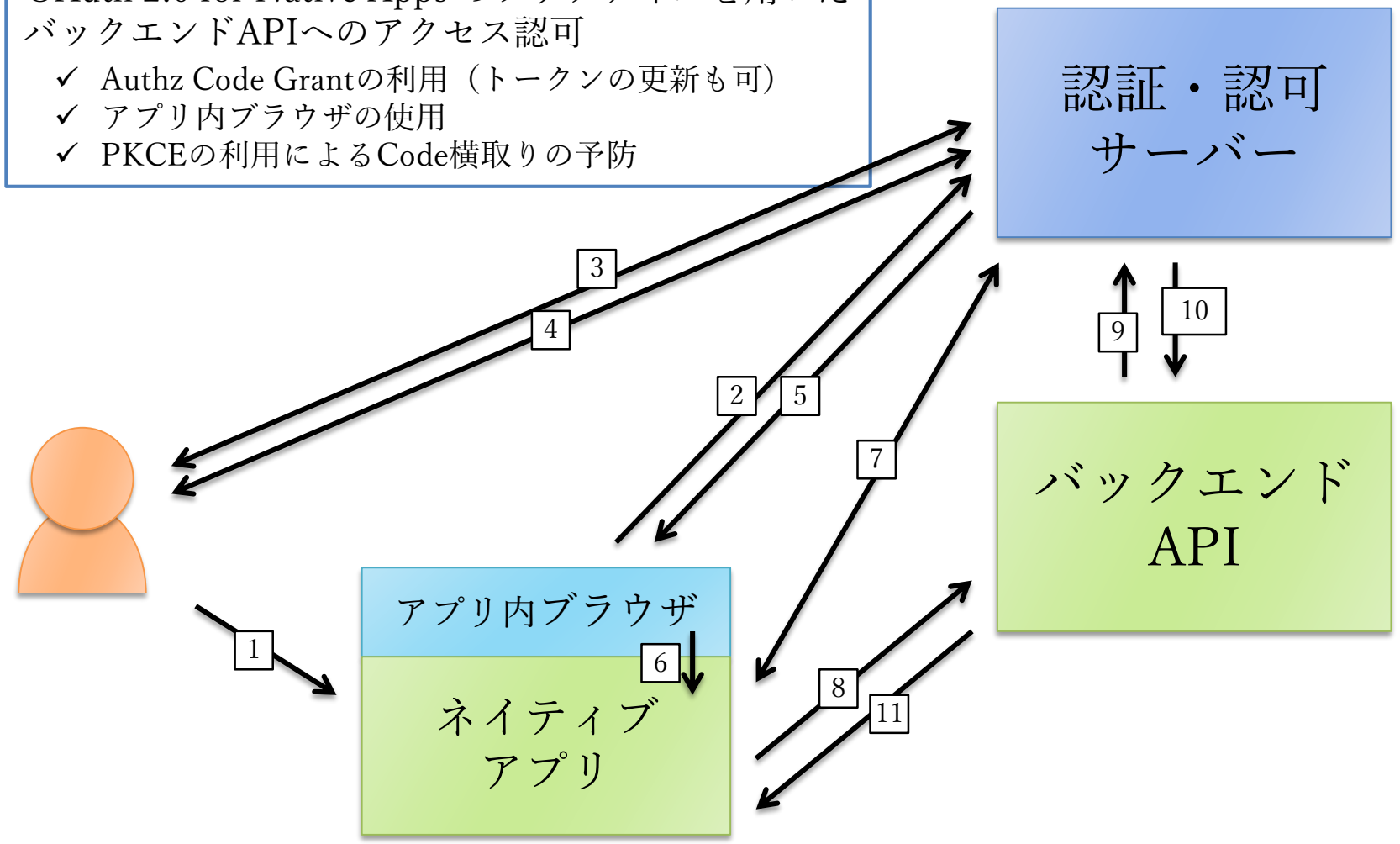


1. ブラウザでモバイルウェブを起動、ログイン開始
2. リダイレクトによりOAuth認可を要求
3. ユーザー認証を実行
4. （リソースアクセス許可）
5. バックエンドAPIアクセス用のアクセストークンを返却
6. アクセストークンをつけてバックエンドAPIにアクセス
7. ~8. アクセストークンの情報を確認（ユーザー、Scope、有効期限、など）
9. バックエンドAPIが情報を使ってモバイルウェブが動作

ネイティブアプリでのバックエンドAPIアクセス認可

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. （リソースアクセス許可）
5. アクセストークンを取得するためのCodeを返却
6. アプリ内ブラウザからネイティブアプリにCodeを返却
7. Codeをアクセストークンに交換（PKCEを併用）
8. アクセストークンをつけてバックエンドAPIにアクセス
9. ~10. 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）
11. 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。

外部の Web API を活用するには？

- **Web API でアクセスするリソースが企業に帰属するなら**
  - クライアント認証をしてアクセス
- **個人（従業員など）に帰属するなら**
  - 企業がアクセスを許可すればよい場合
    - クライアント認証をしてアクセス
  - 個人がアクセスを許可するべきものの場合
    - OAuthによる認可、個人の認証への対応が必要
    - 個人の認証は、自社の認証基盤からのSSOに対応することも検討

外部へ Web API を公開するには？

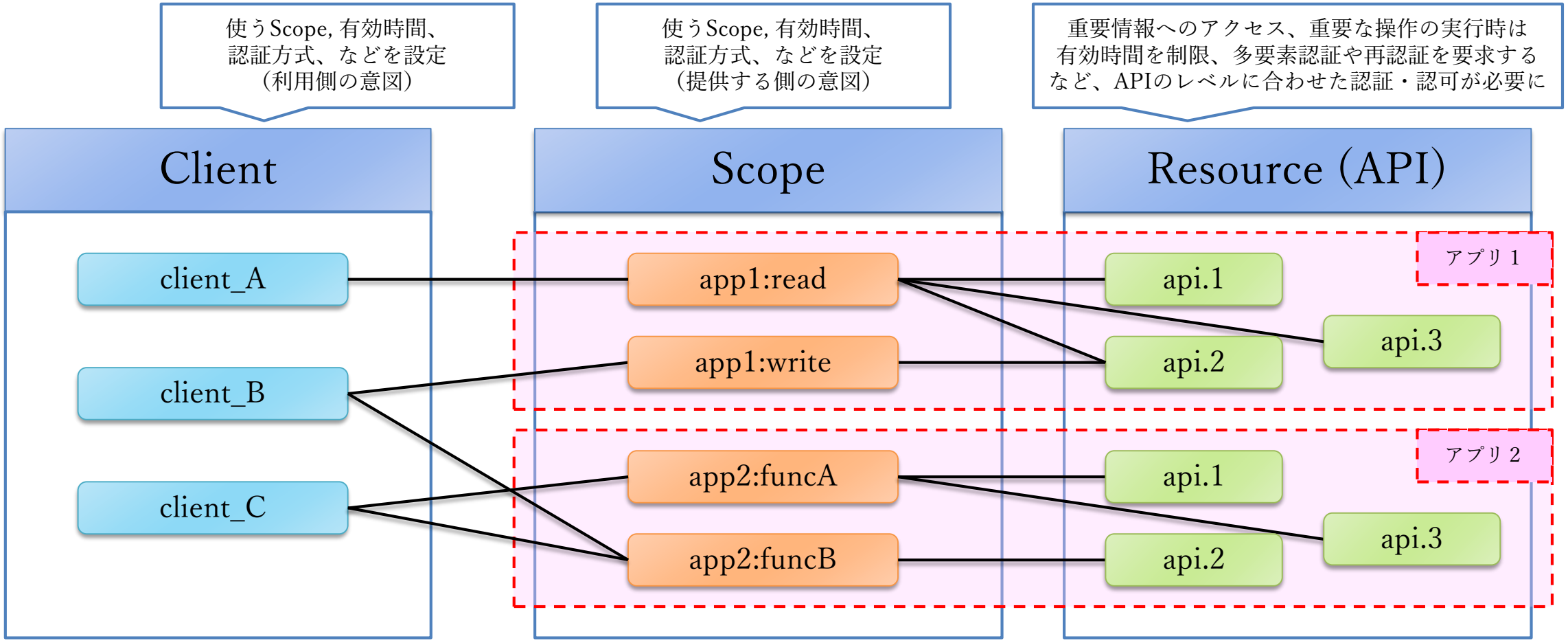
- Web API で提供するリソースが誰に帰属するかを分析する
- リソース毎に付与する権限を整理する
- リソース x 権限 を SCOPE にマッピングする
- OAuth による認可を実装する
- ユーザーを認証する機能を実装する
- ユーザーが使用している認証基盤とのSSOに対応する

対応しておくべき OIDC/OAuth のフロー

#	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

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



ThemiStruct ソリューションでの対応

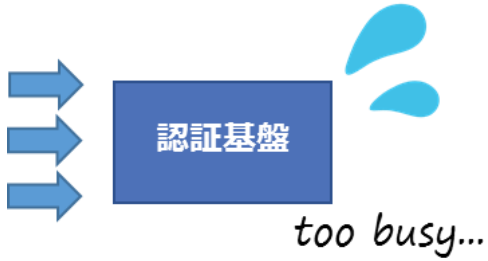
認証基盤 から
アイデンティティプラットフォーム へ

広がるユースケース
増えるアクセス
高まる重要性

おのずと「非機能要求」のレベルもアップ

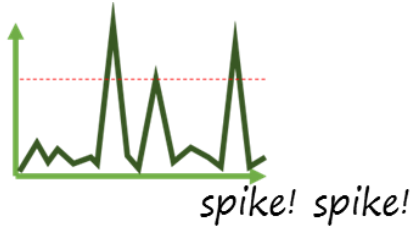
膨大なトラフィック

- 認証基盤の役割増加
- 提供するサービス・システムの増加
- ユーザー数・デバイス数の増加
- API利用の増加



スパイクアクセス

- キャンペーンやニュースサイト掲載などにより定常的なアクセスと比較し、予想不可な大量のアクセスが発生する



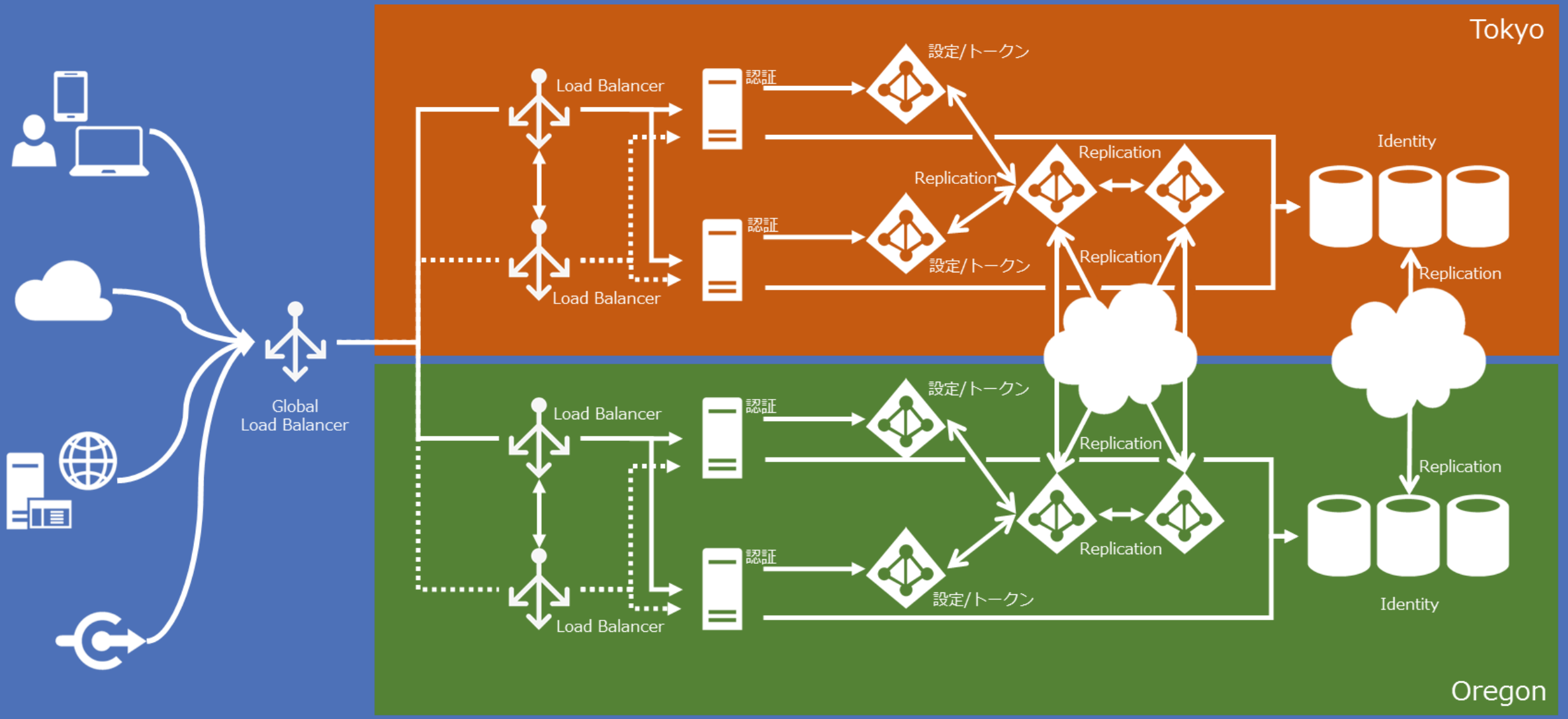
システム停止を回避

- 認証基盤役割の増加に伴い、システム停止や遅延による機会損失が大きくなり、事業継続性や機会損失回避など可用性要求のレベルが格段にUPした

スピードスタート・スモールスタート

- 短期間でビジネスをスタートさせたり、事業規模に応じてスタート、柔軟にスケールできる必要がある

これまで： 高度な基盤設計。入念な可用性、性能のテスト。プロジェクトの巨大化。



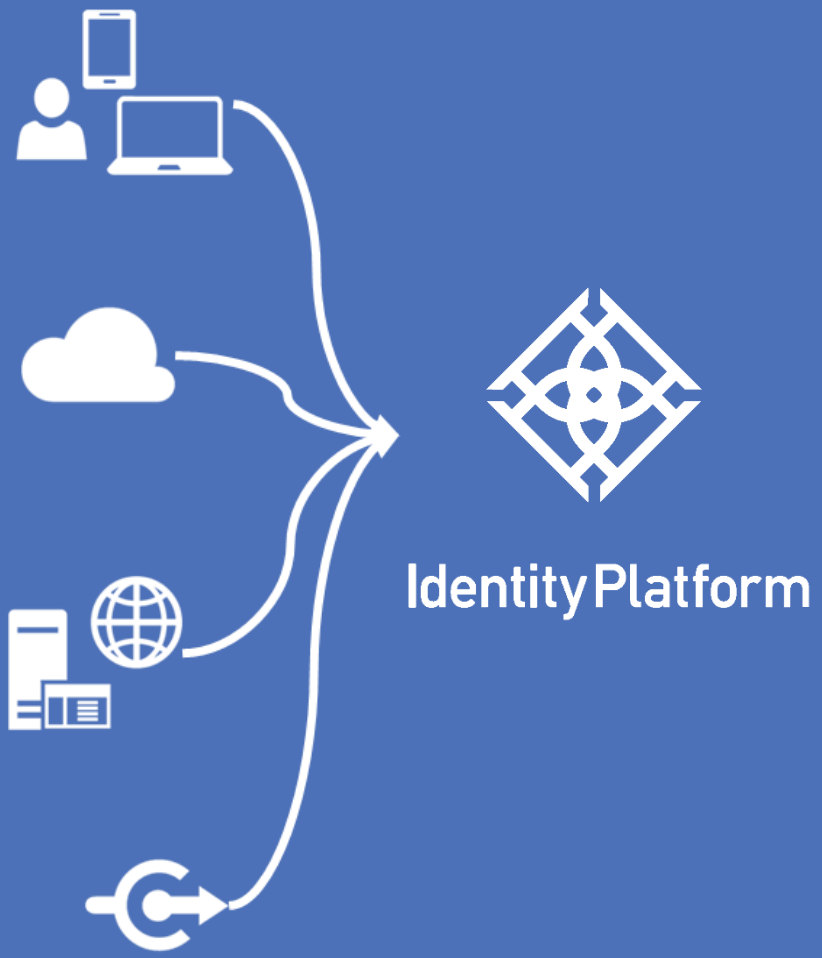
当社のアプローチ

ThemiStruct テミストラクト

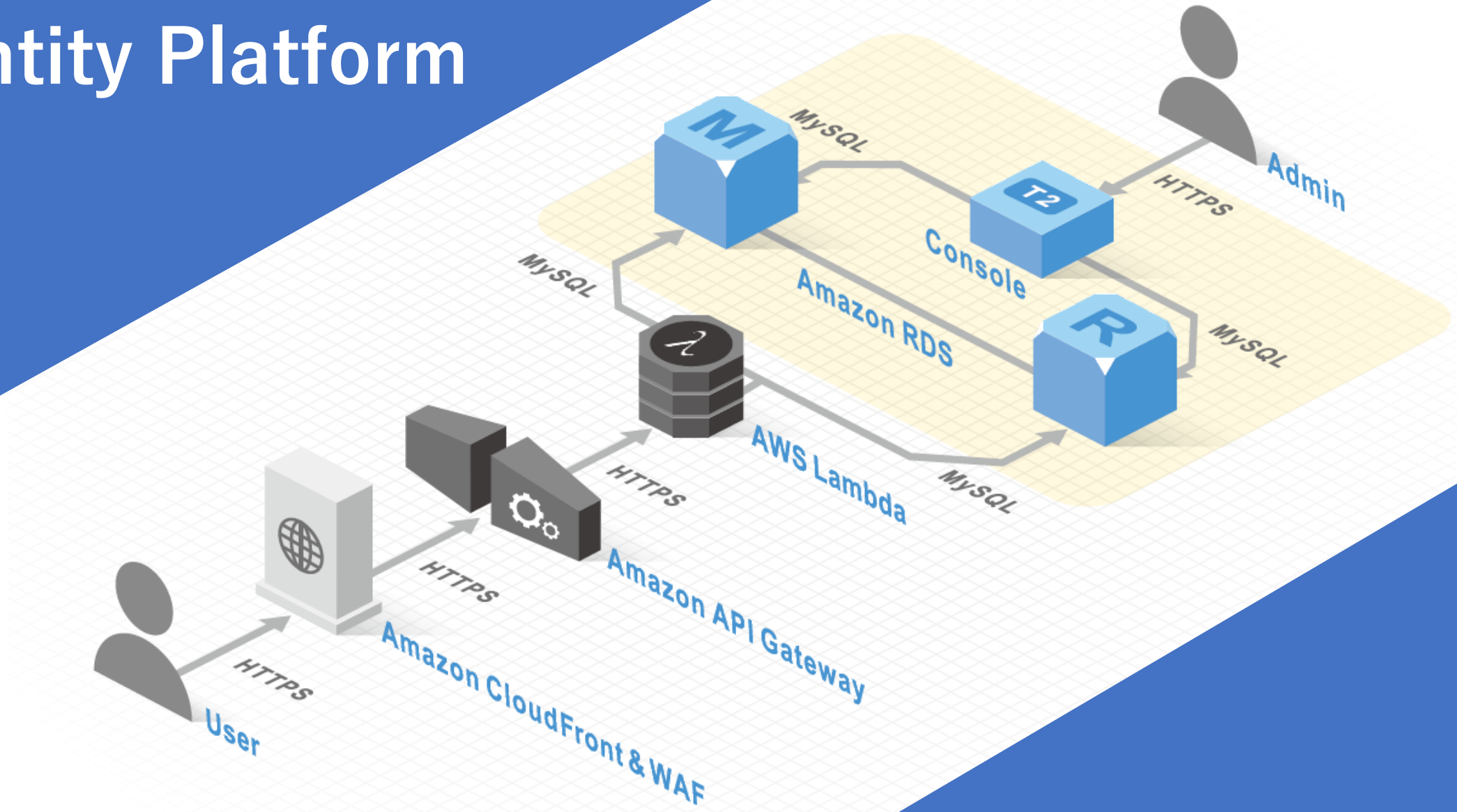
Identity Platform AWS対応版

- ✓ AWSのPaaS上で動く
  アイデンティティ連携基盤
- ✓ ≠OpenAM、OpenIDM
- ✓ ≠IDaaS
- ✓ オージス総研自社商品

これから： 基盤の設計、テストは不要。プロジェクトの迅速なスタートアップ。



ThemiStruct Identity Platform



AWSマネージドサービスを使い安全な認証基盤を短時間で

CloudFront, API Gateway, Lambda, RDS, CloudWatch, …

✓ **サーバーレス**	個々のサーバーの管理が不要
✓ **高いスケーラビリティ**	アクセス量予測、事前リソース確保、 事前の設備投資が不要
✓ **十分な可用性**	複雑な設計、膨大なテストからの開放
✓ **豊富なセキュリティオプション**	AWS WAF, AWS Shield, … などを 組み合わせて安全対策を強化
✓ **使えるモニタリング機能**	ダッシュボード、ログ管理、通知の 仕組みを簡単に構築

統合認証ソリューション ThemiStruct

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

まとめ

まとめ

- クラウド上のシステムは物理的なセキュリティが難しくなっている。アイデンティティを意識したセキュリティ対策が必要となってきている。
- アイデンティティを用いた認証、認可技術は標準化が進んでいる。標準技術に適合し他サービスとの相互接続性を高めることが重要である。
- モバイル、APIの利活用はこれからも進む。より良いサービス提供を目指し認証基盤の役割も高度化して行くべきである。
- 認証基盤は柔軟性と立ち上げのスピードが重要である。ThemiStructソリューションは皆さまのニーズに応えていきます。

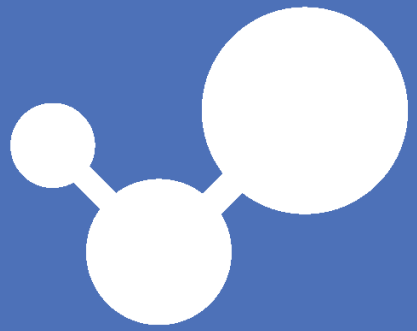
ご清聴ありがとうございました

【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

参考資料

あなたの Identity Platform が
すぐ構築可能

アイデンティティ連携



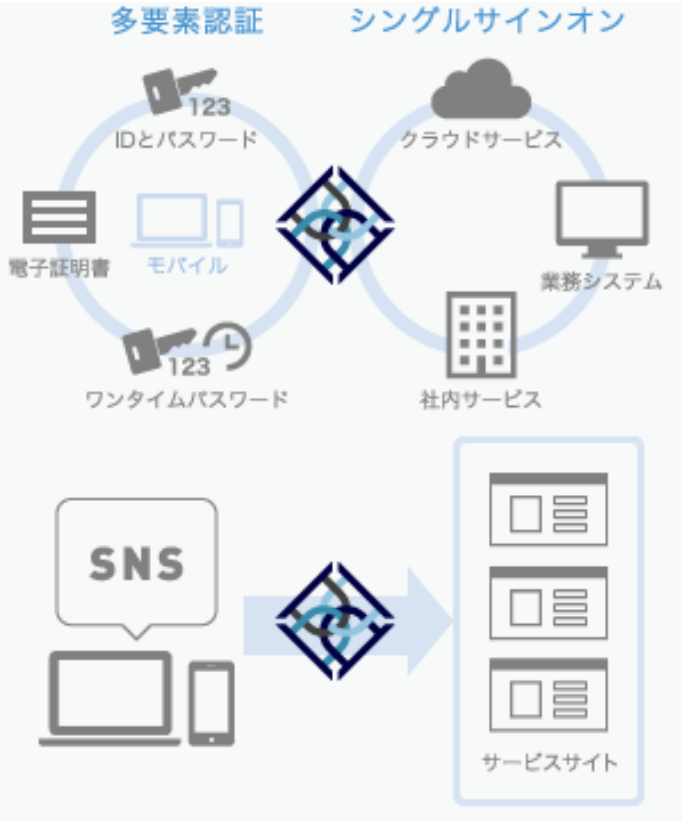
事業成長や突発的アクセスに
合わせたスケーリング

アクセスセキュリティ強化

ThemiStruct Identity Platform の特徴 (1)

認証システムの短期導入が可能

ThemiStruct Identity Platform はクラウド上に設置され、短期間で従業員、カスタマー、ビジネスパートナーに認証サービスを提供できます。また、APIを利用し既設サイトへの組み込みも容易です。



ログインを1回に、認証方法も組合せ自由

ThemiStruct Identity Platform に一度ログインを行うことで、ユーザーが利用したい各サイトへシングルサインオンすることができます。 その際のログインではIDとパスワードによる認証だけでなく、ワンタイムパスワード・電子証明書、指静脈情報などを利用することができます。また利用システムごとの設定により、各サイトやコンテンツのセキュリティ、ユーザビリティ要件に応じた認証を行うことができます。

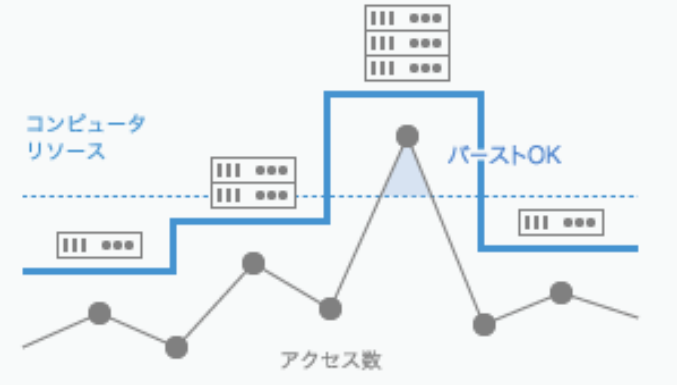
ユーザー登録のハードルを下げ、新規ユーザー登録率をアップ

FacebookやGoogleなどのユーザーが普段使っているSNSやWebサービスのアカウントを利用して、気軽にユーザー登録が可能です。サイトへの新規ユーザー登録率、ユーザビリティ、コンバージョン率を向上させます。ユーザー自身による登録や、管理者による一括登録も可能です。

ThemiStruct Identity Platform の特徴 (2)

各システムへ必要なときに、必要な情報を連携できます

ThemiStruct Identity Platform から各システムへ必要なタイミングで、必要なユーザー情報を連携することができます。各システムでユーザー情報の管理が不要になります。



事業成長に合わせたスケーリング、突発的アクセス集中への対応

サーバレスアーキテクチャにより、事業環境の変化や突発的アクセス集中に合わせて、自由にかつ自動でコンピュータリソースの拡張・縮小を行えます。