アイデンティティ連携技術を使った認証基盤の実装

株式会社 オージス総研
テミストラクトソリューション部
千野 修平

エンティティとアイデンティティ（自己紹介）

アイデンティティ（属性の集合）

名前　千野 修平（せんのしゅうへい）
所属　認証技術グループ
役割　主任アーキテクト

…
関西弁
メガネをかけている
アラサー

エンティティ（実体）

入社 — 2009

OpenSSO/OpenAMを活用した案件の遂行 — 2010

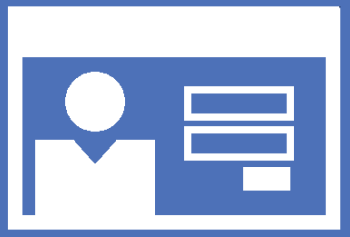
認証基盤商品の追加機能開発 — 2013

AWSを活用した認証基盤商品の新規開発 — 2015

デジタル変容

技術要求の変化

アイデンティティ連携



実際何ができるのか?

For Enterprise

For Partner

For Customer

本日のアジェンダ

CASE ＃1
　従業員のための認証基盤（社内認証基盤）

CASE #2
　顧客にサービスを提供するための認証基盤
　（BtoC認証基盤）

本日のアジェンダ

CASE ＃1
　従業員のための認証基盤（社内認証基盤）

CASE #2
　顧客にサービスを提供するための認証基盤
　（BtoC認証基盤）

当社のアプローチ ～従業員のための認証基盤～

ThemiStruct-WAM
テミストラクト
OpenAM

ThemiStruct-WAM（OpenAM）

- シングルサインオンを実現する認証基盤
- OpenAMをコアソフトウェアとしている

ThemiStruct-IDM
テミストラクト
OpenIDM

ThemiStruct-IDM（OpenIDM）

- 様々なシステムに対し、ID・属性のプロビジョニングを行い、組織のID管理を実現する
- OpenIDMをコアソフトウェアとしている

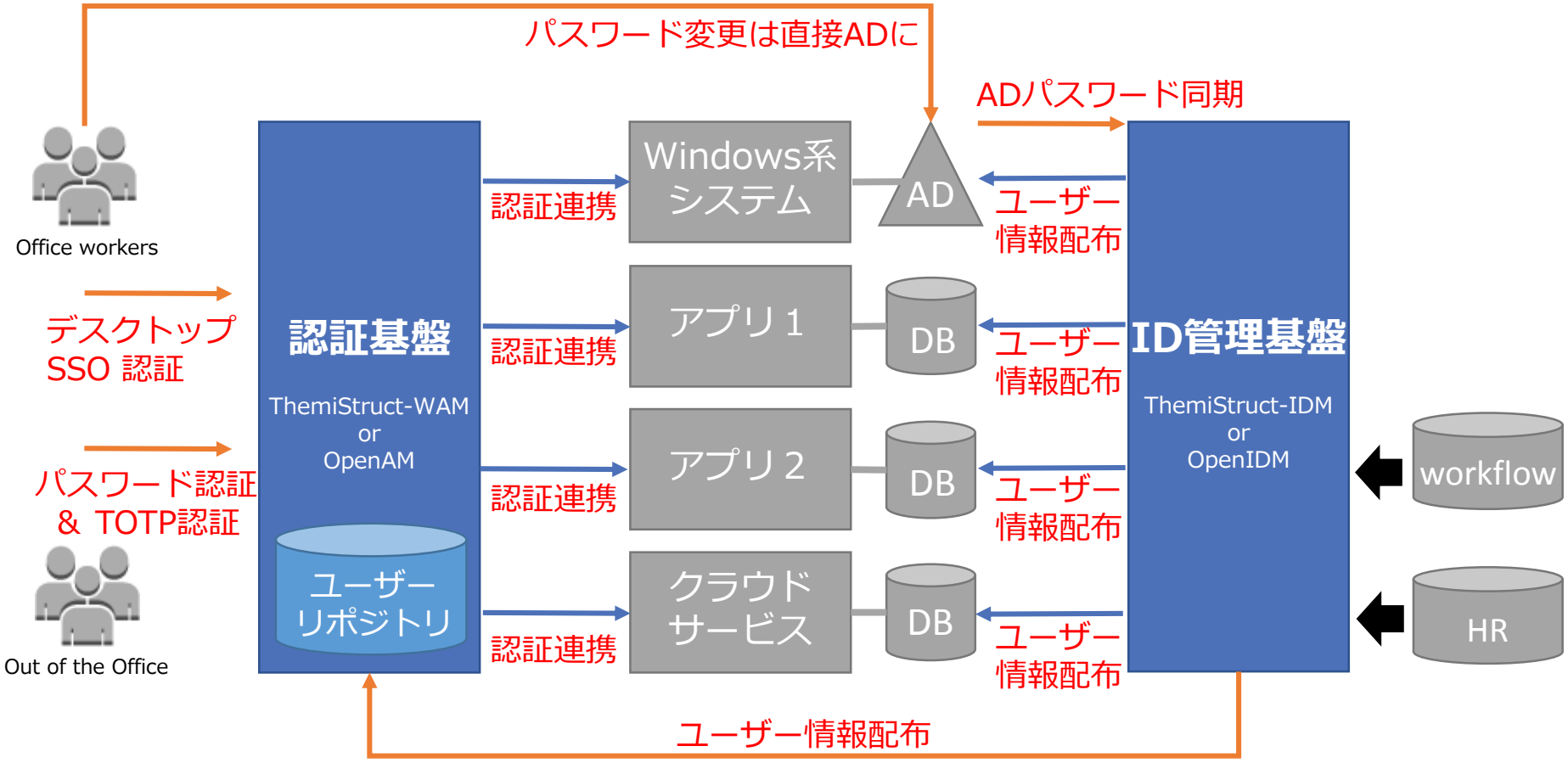
ThemiStruct-CM
テミストラクト
EJBCA
PKI BY PRIMEKEY

ThemiStruct-CM（EJBCA）

- クライアント向け電子証明書の発行・管理を実現する電子証明書運用管理基盤
- EJBCAをコアソフトウェアとしている

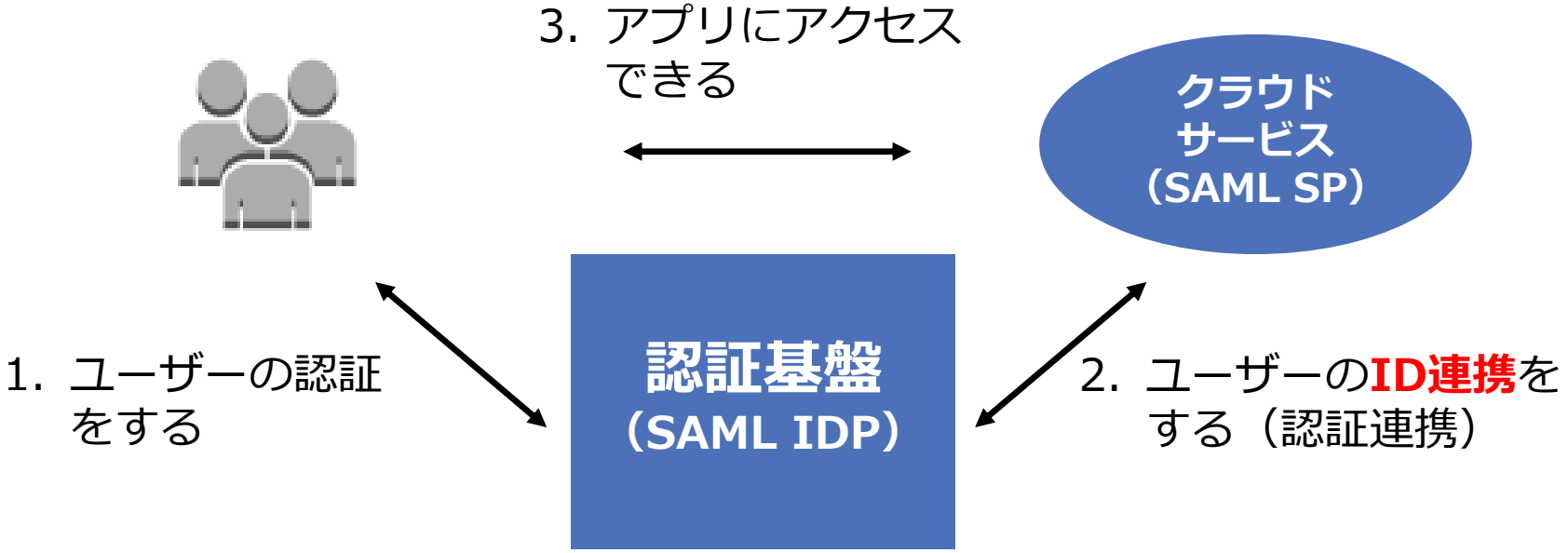
アーキテクチャパターン #1 一般的な社内利用パターン

社内で利用する認証基盤に求められる要件事項
1. 非常に多様なシステムとの認証連携（パッケージ、クラウド、Windows系）
2. スマデバ活用、リモート活用に対応
3. Active Directoryとの連携



ID連携技術（SAML）を使ったクラウドサービスへのSSO

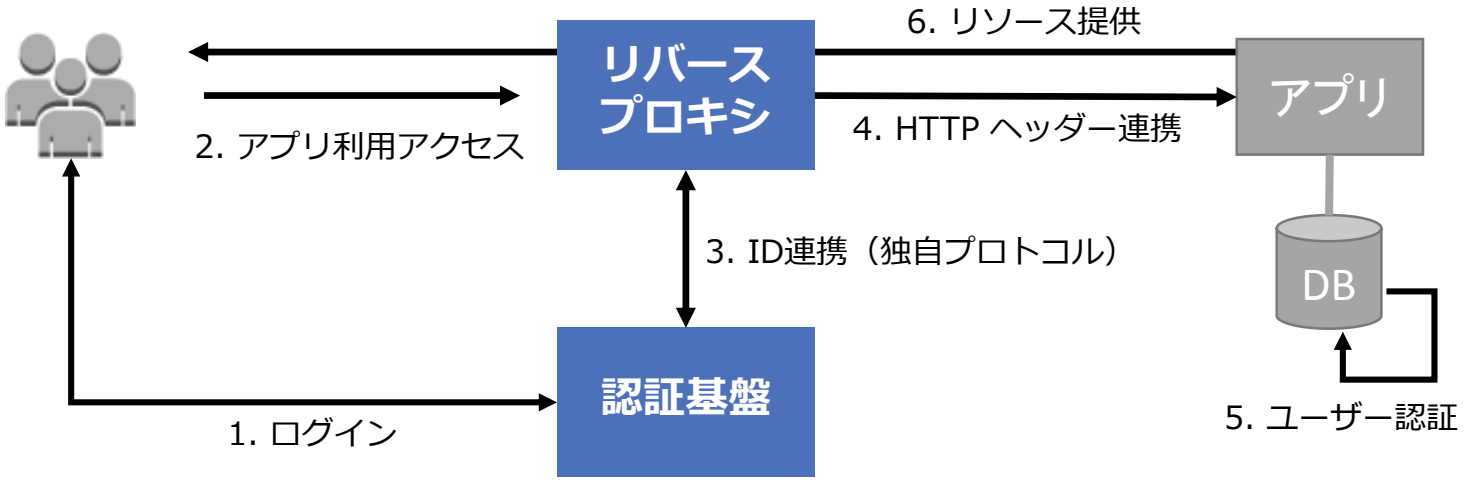
- 企業の情報システムとして一般的となったクラウドサービスの多くはSAML SPとして動作し、組織の認証基盤とID連携（認証連携）を行い、SSOをすることが可能
- クラウドサービスの利用選択にあたって、組織の認証基盤と統合できる機能を有することを指標とするケースもでてきている。



ThemiStruct-WAM/OpenAMで実現可能

Agent/Reverse Proxy 型のSSO

- ID連携を受けるためのシステム変更が困難なシステム（パッケージやレガシー）、厳密なアクセス制御が必要なシステムの場合は、エージェントやリバースプロキシを用いたSSO実装する

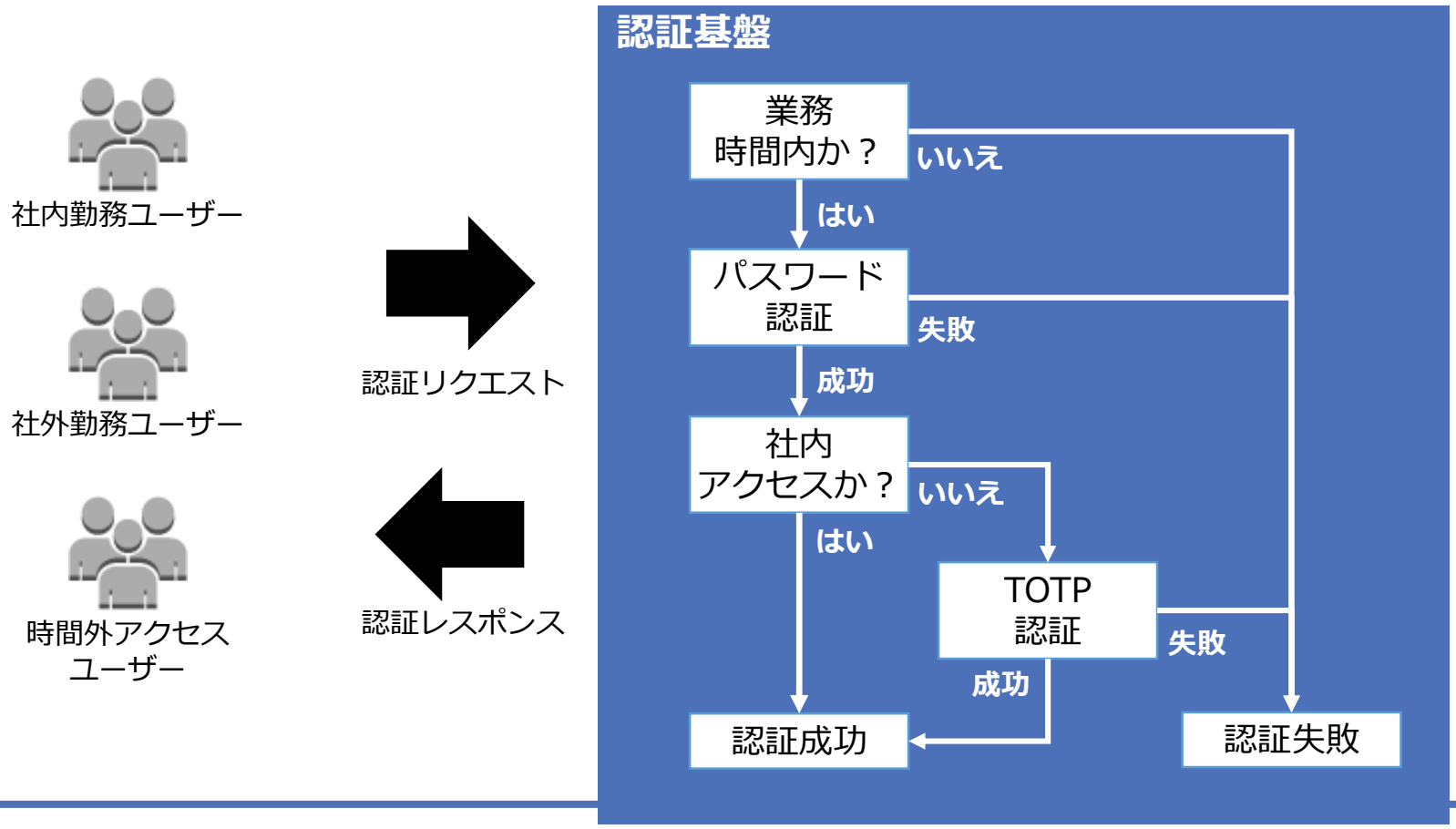


リバースプロキシ型 SSO

ThemiStruct-WAM/OpenAM で実現可能

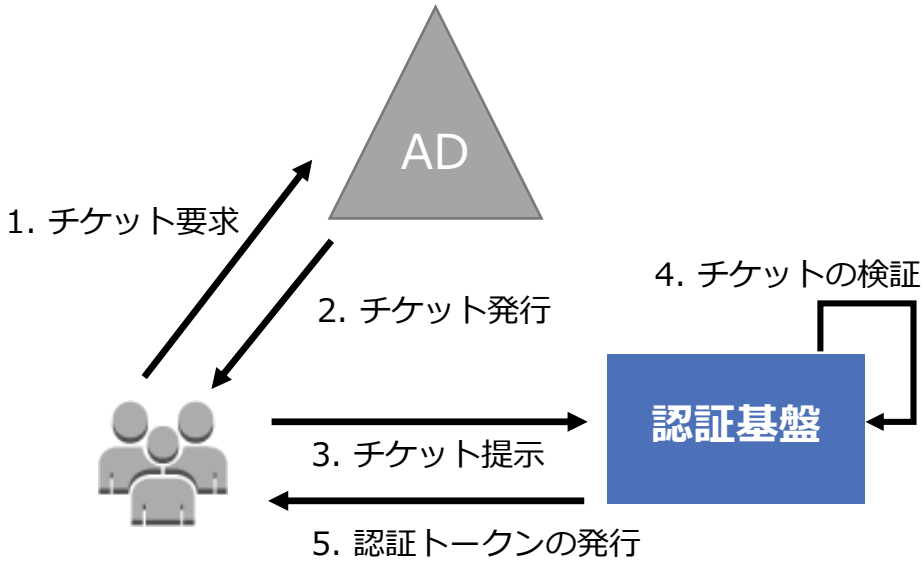
多要素認証・認証連鎖

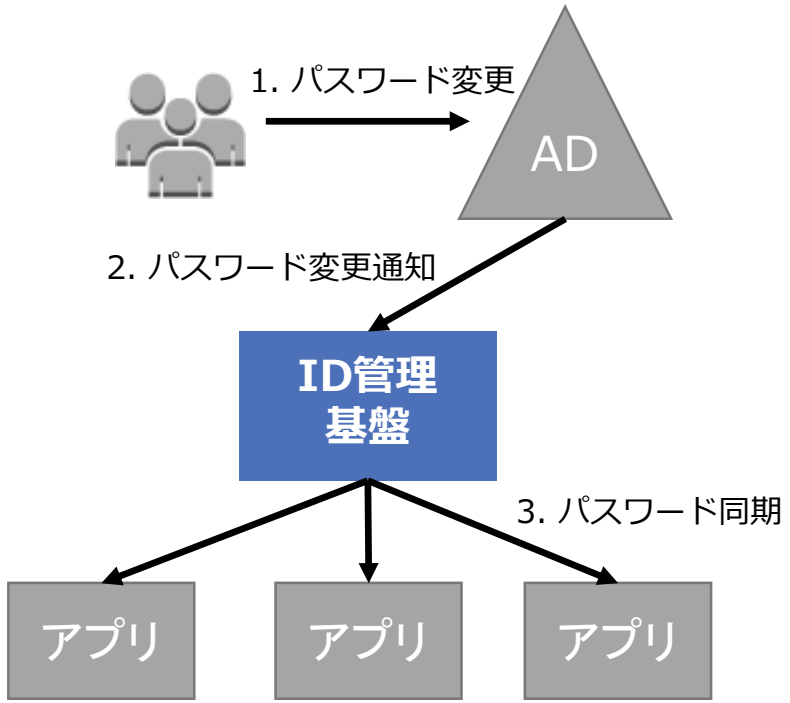
- 社用デバイスの利用シーンの増加に伴い、多要素認証は必須要件となりつつあり、また、ユーザーの利用シーンに合わせた認証手段の提供が求められる。



Active Directoryとの連携

- Active Directoryとの連携に関する機能要求は以下の２つが存在する





デスクトップSSO認証

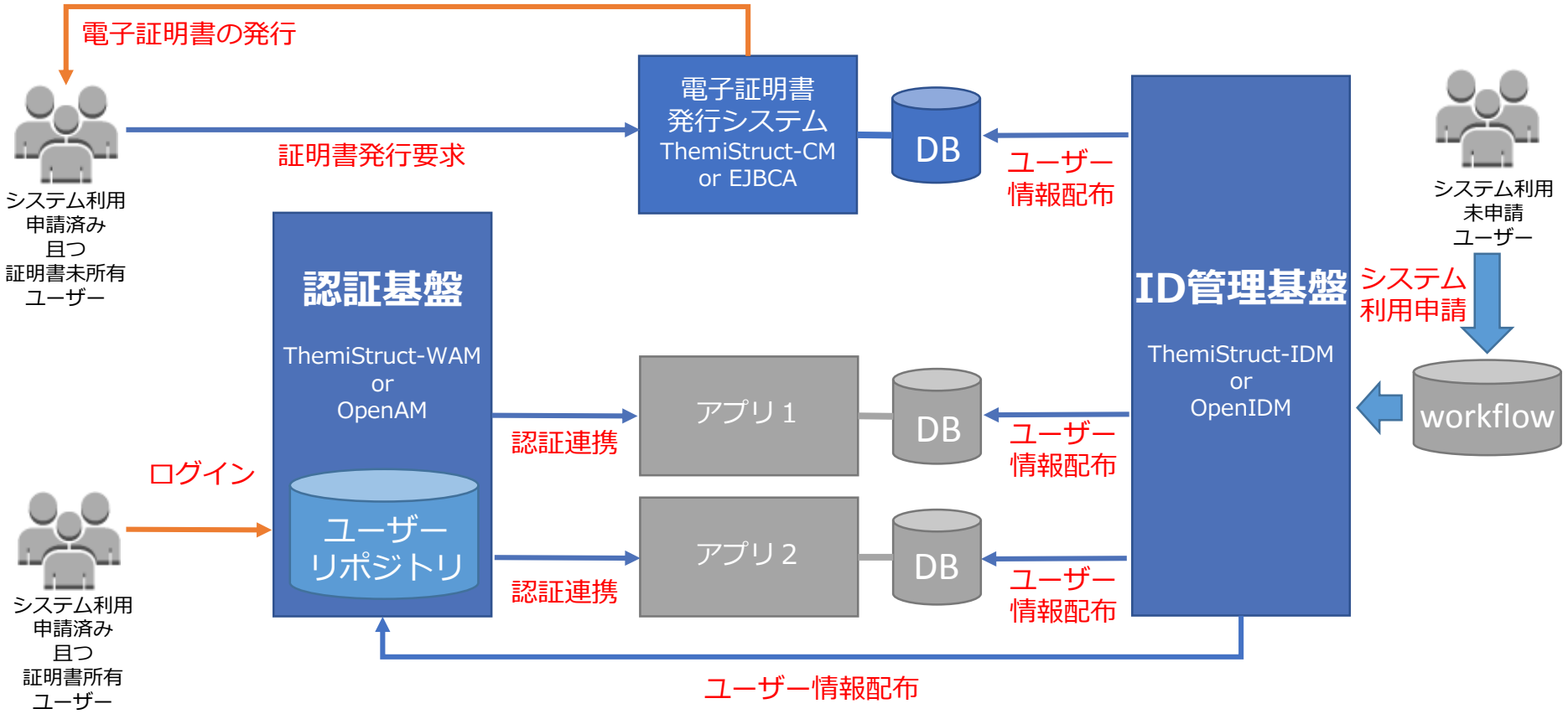
ThemiStruct-WAM/OpenAM
で実現可能

AD パスワード同期

ThemiStruct-IDM/OpenIDM
で実現可能

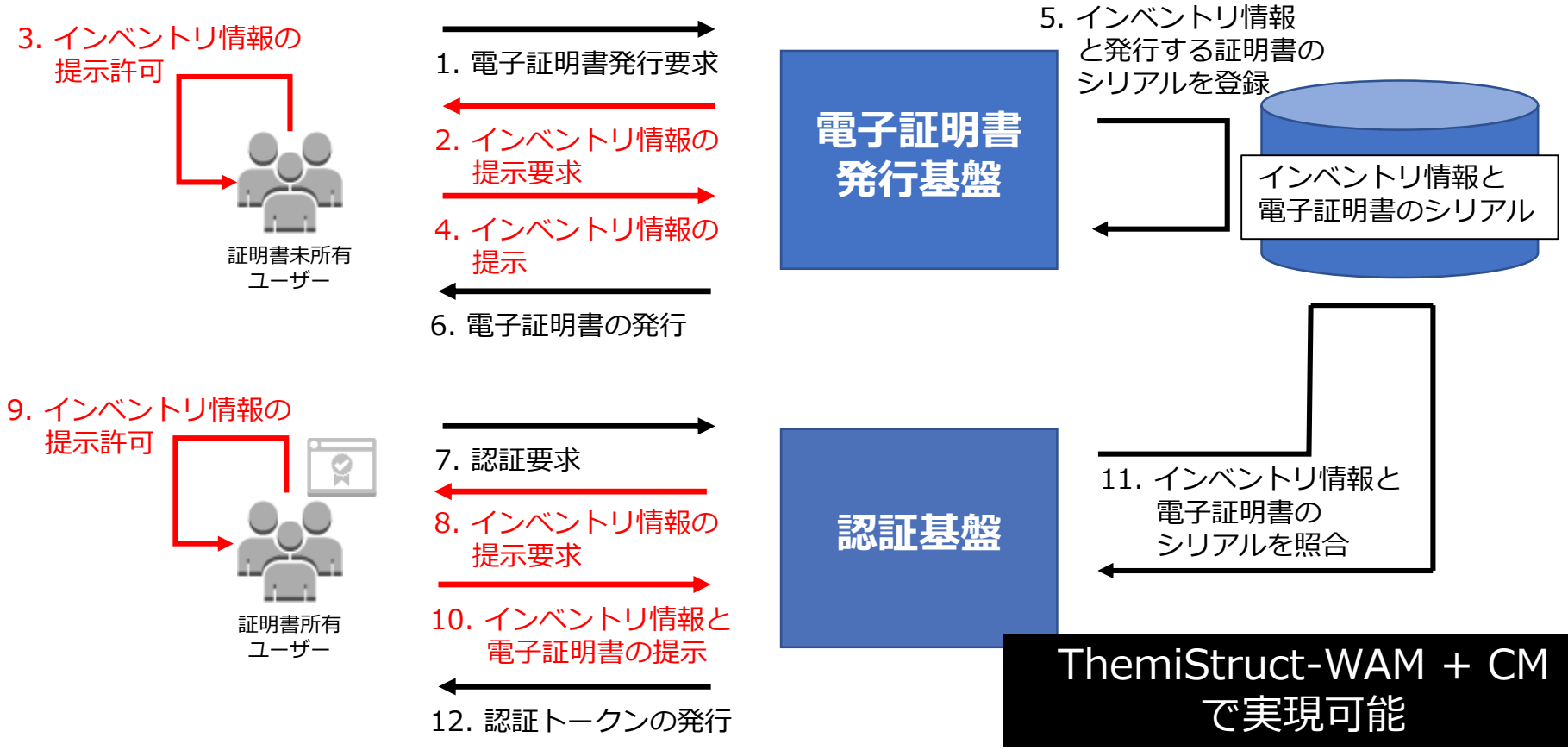
アーキテクチャパターン #2 BtoB利用パターン

ビジネスパートナーに提供するサービスの認証基盤に求められる要件事項
1. 利用端末の調達はビジネスパートナーが行なうが、利用端末の制限が必要
2. 利用端末の制限には電子証明書を活用する



ID連携技術(OpenID Connect)を使った端末認証

- ビジネス・パートナーに対し、サービスを提供する際、電子証明書を用いた端末認証を行なうのは一般的である
- 加えて、電子証明書がコピーされて利用されるリスクを軽減するために、 **ID連携技術を用いて**端末情報を収集し、管理をしている



まとめ ～従業員のための認証基盤～

ロ 特徴

- 大前提として、企業が所有する様々な情報システムとの連携が必須要件である
- それ故、従業員のための認証基盤では、多くの認証連携方式の認証方式のサポートが求められる

  →認証連携方式：SAML、OpenID Connect、Agent/RP 型

  →認証方式：TOTP、電子証明書認証、生体認証デバイスとの連携

ロ アプローチ

- 機能が充実しているOSSを用いて、複雑な機能要件を実現する。
- ID管理基盤や電子証明書発行基盤と組み合せて、機能要求を実現する必要もある

本日のアジェンダ

CASE ＃1
　従業員のための認証基盤（社内認証基盤）

CASE #2
　顧客にサービスを提供するための認証基盤
　（BtoC認証基盤）

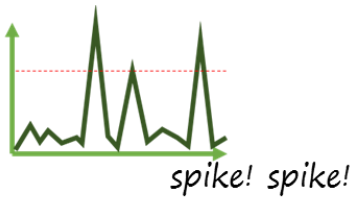
当社のアプローチ ～顧客にサービスを提供するための認証基盤～

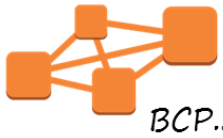
ThemiStruct
Identity Platform

- ✓ AWSネイティブなアイデンティティ連携基盤
- ✓ ≠OpenAM
- ✓ ≠OpenIDM
- ✓ オージス総研自社製品

なぜ独自で実装を行ったか？

- **認証基盤が捌くトラフィック量が増大した**
  - 認証ユーザーや、認証クライアントが増大する傾向にある
- **認証基盤へのアクセスがスパイクする**
  - 定常的なアクセスと比較し、数十倍のアクセスが発生するケースがある
- **認証基盤に求められる可用性要件の高難度化**
  - 事業継続性や機会損失回避などの要求が増え、認証基盤における可用性要求のレベルが格段に上った
- **プロジェクトの短期間化**
  - 短期間でビジネスをスタートさせたり、情報システム戦略の実行をするケースが増えた

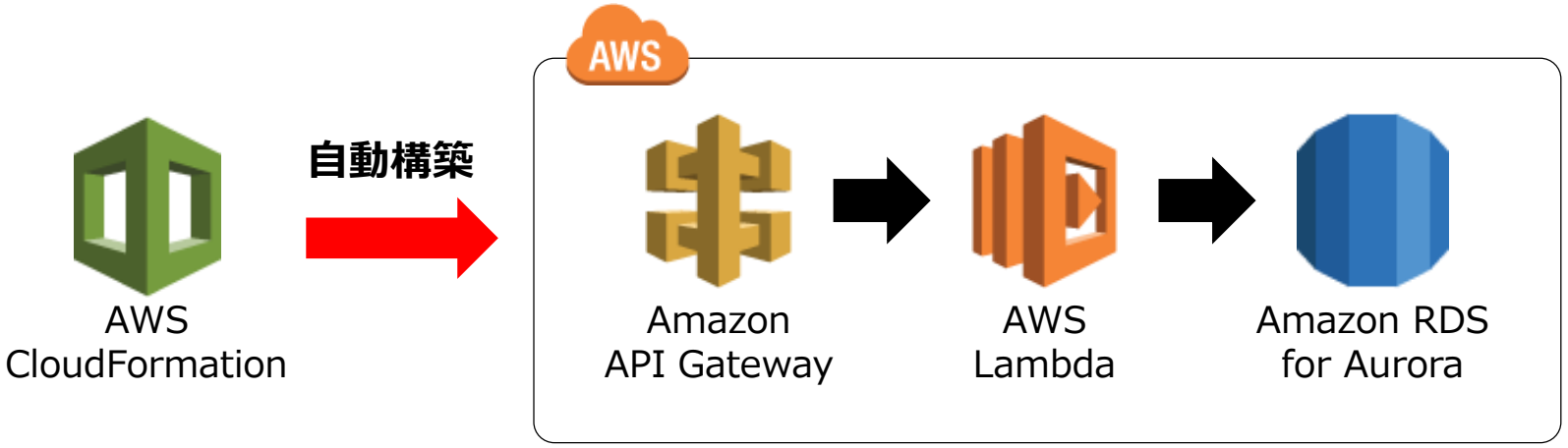




個別に設計して、実装するのは大変・・・
クラウドリソース（AWS）と組み合わせて、これらの課題を解決したい

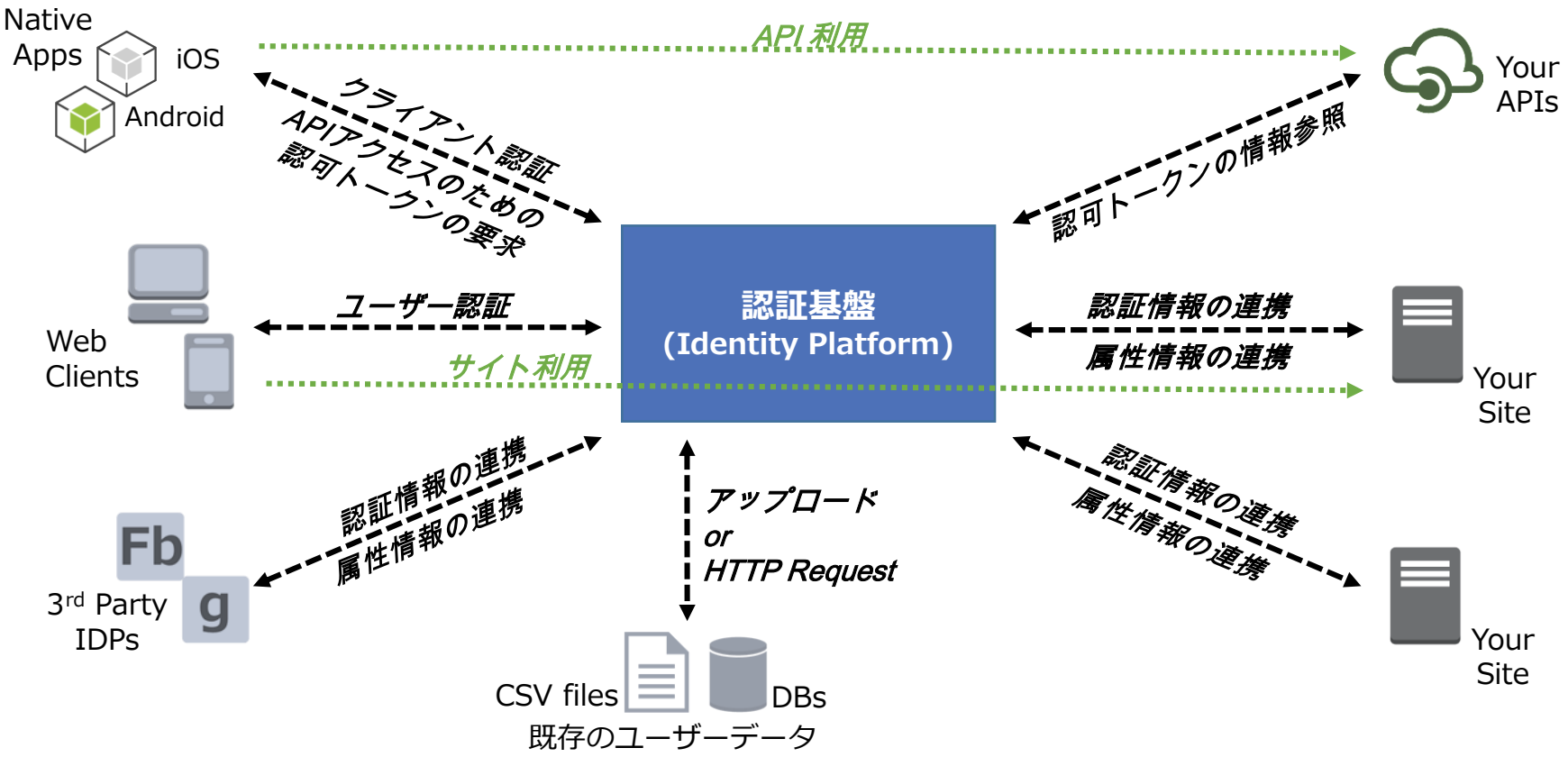
AWSネイティブなアーキテクチャを採用し、アベイラビリティ、成長と共に拡張するスケーラビリティを確保

- 仮想サーバーを極力使用しないアーキテクチャで実装している
  - Amazon API Gateway
  - AWS Lambda
  - Amazon RDS for Aurora
- AWSネイティブなアーキテクチャにより下記の恩恵を享受できる
  - リクエストに応じて自動でスケーリングする（トラフィック量の増大、スパイクアクセスへの対応）
  - 一定の可用性確保と自動復旧の実現（可用性要件の高度化）
  - デプロイメントのスピードアップ（プロジェクトの短期間化）



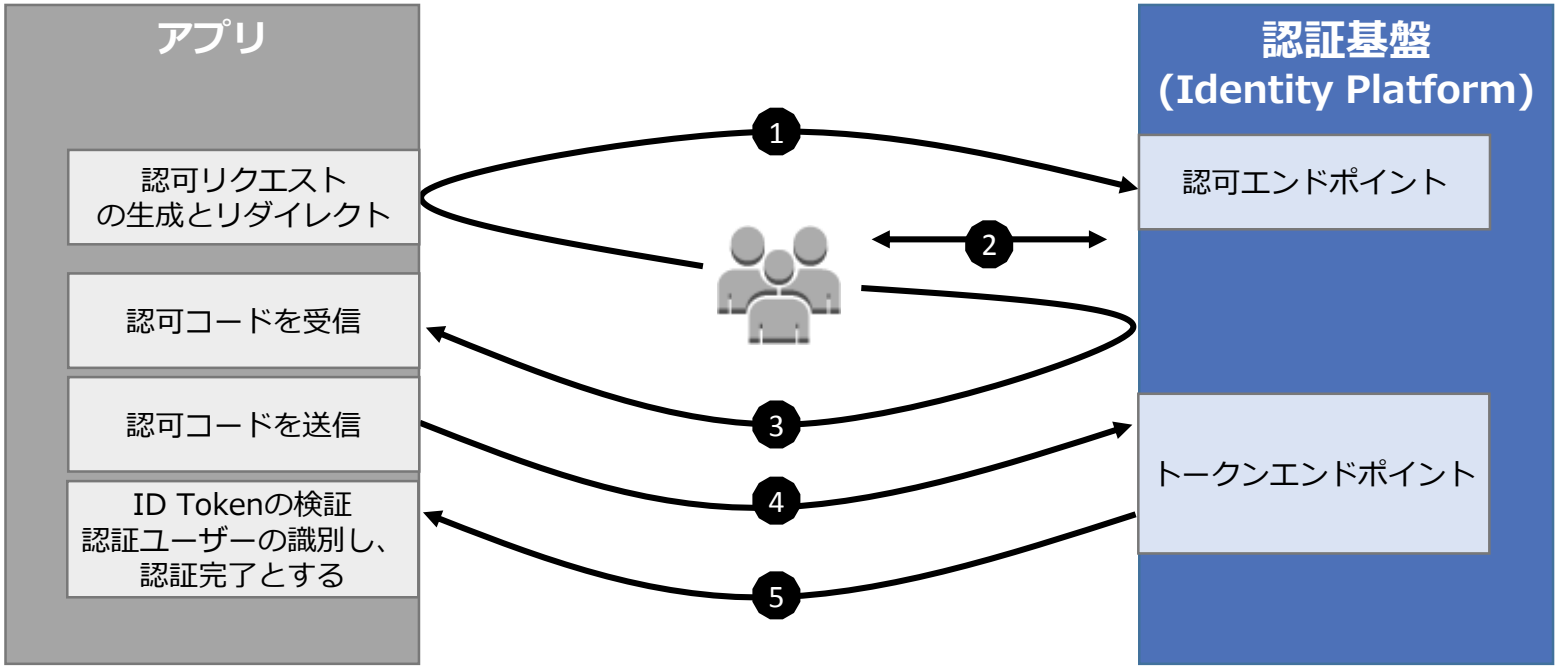
アーキテクチャパターン #3 BtoC利用

カスタマー、コンシューマに提供するサービスの認証基盤に求められる要件事項
1. Webクライアントだけではなく、ネイティブアプリもある
2. サードパーティのIDP（FacebookやGoogle）との連携が必要
3. APIへのアクセスを認可する基盤が必要



ID連携技術をつかったアプリへのシングルサインオン

- エージェントやリバースプロキシでSSOを行うと、外部プログラムの性能や可用性を考慮する必要が有るため、ID連携技術を用いたSSOを推奨する

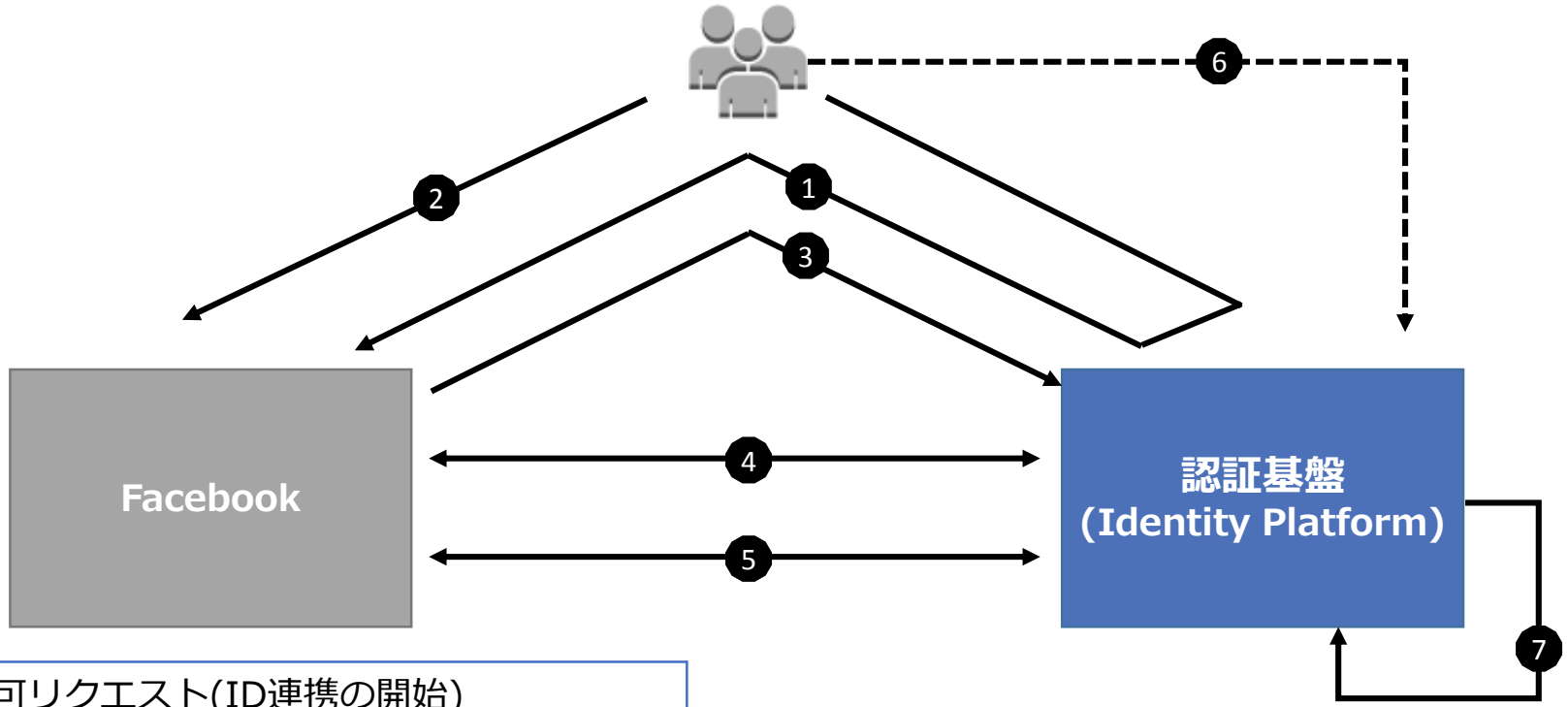


① 認可リクエスト(ID連携の開始)
② サインイン/ID連携の同意
③ 認可コードを含んだ認可レスポンス
④ 認可コードを送信
⑤ ID Token(認証連携) と Access Tokenを受信

Identity Platform
で実現可能

ID連携技術をつかった会員登録

- シームレスな会員登録フローの実現のために、ソーシャルアカウントを用いた会員登録機能を実装

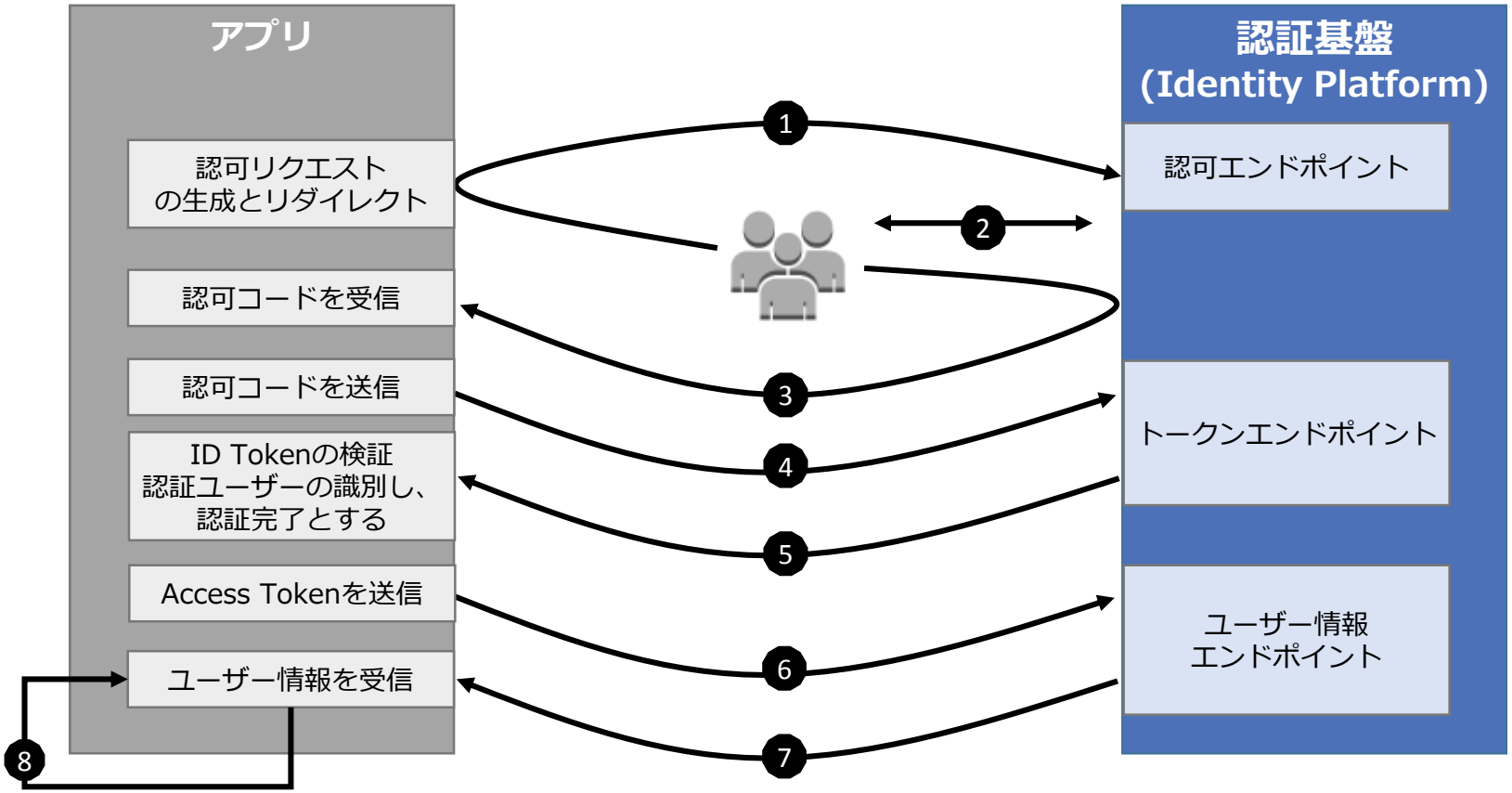


① 認可リクエスト(ID連携の開始)
② サインイン/ID連携の同意
③ 認可コードを含んだ認可レスポンス
④ 認可コードを送信し、Access Tokenを受信
⑤ Access Tokenを送信し、属性情報を受信
⑥ （必要に応じて、不足情報を入力）
⑦ 会員登録完了

Identity Platform
で実現可能

ID連携技術をつかったアプリへのユーザーの登録・更新

- ユーザーの属性情報を保持する必要があるアプリケーションは、認証基盤から供給されたアイデンティティ情報を元に、ユーザーの初期登録が実装できる

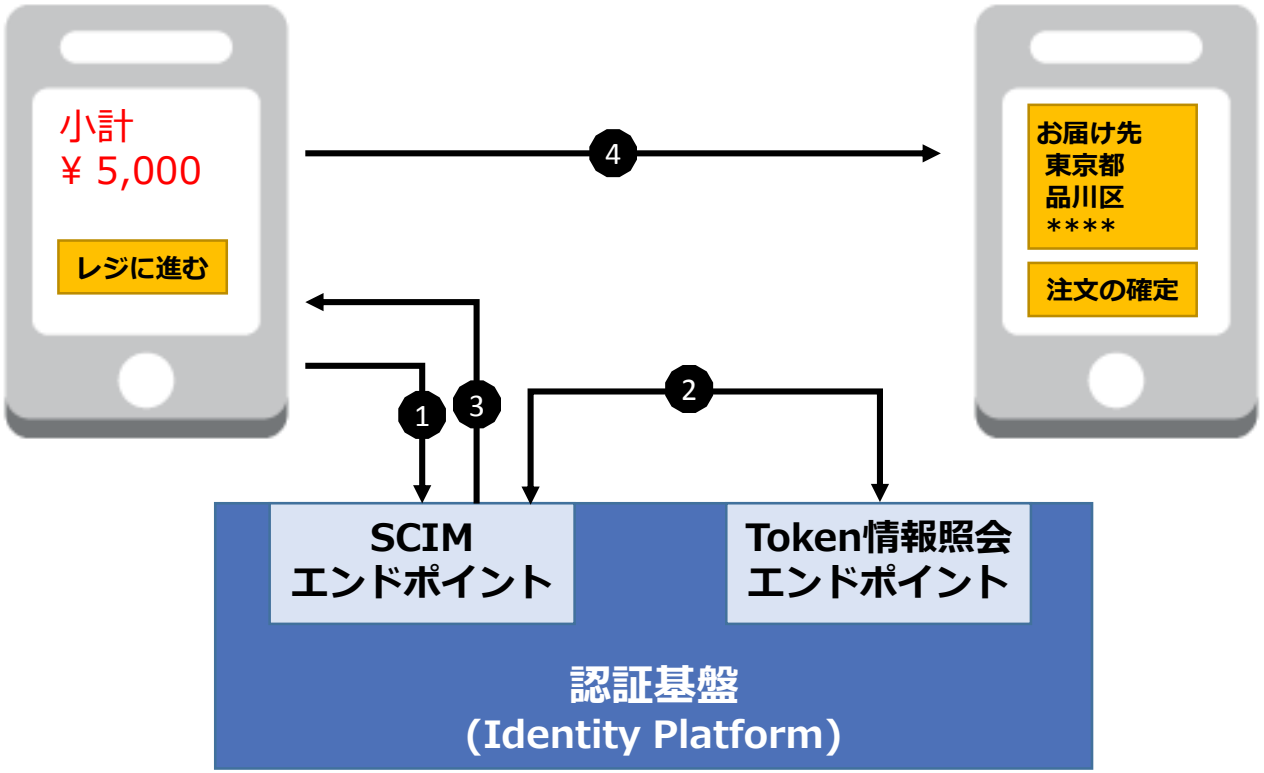


Identity Platform で実現可能

⑥ Access Tokenをユーザー情報エンドポイントに送信
⑦ ユーザー情報（属性連携）を受信
⑧ 受信したユーザー情報を使い、ユーザーの登録・更新を行う

ID連携技術を使ったユーザー属性の追加参照

- 認証基盤にユーザー属性情報の操作API(SCIM エンドポイント)を併せて実装することで、追加のユーザーの属性情報がアプリの任意のタイミングで取得できる。

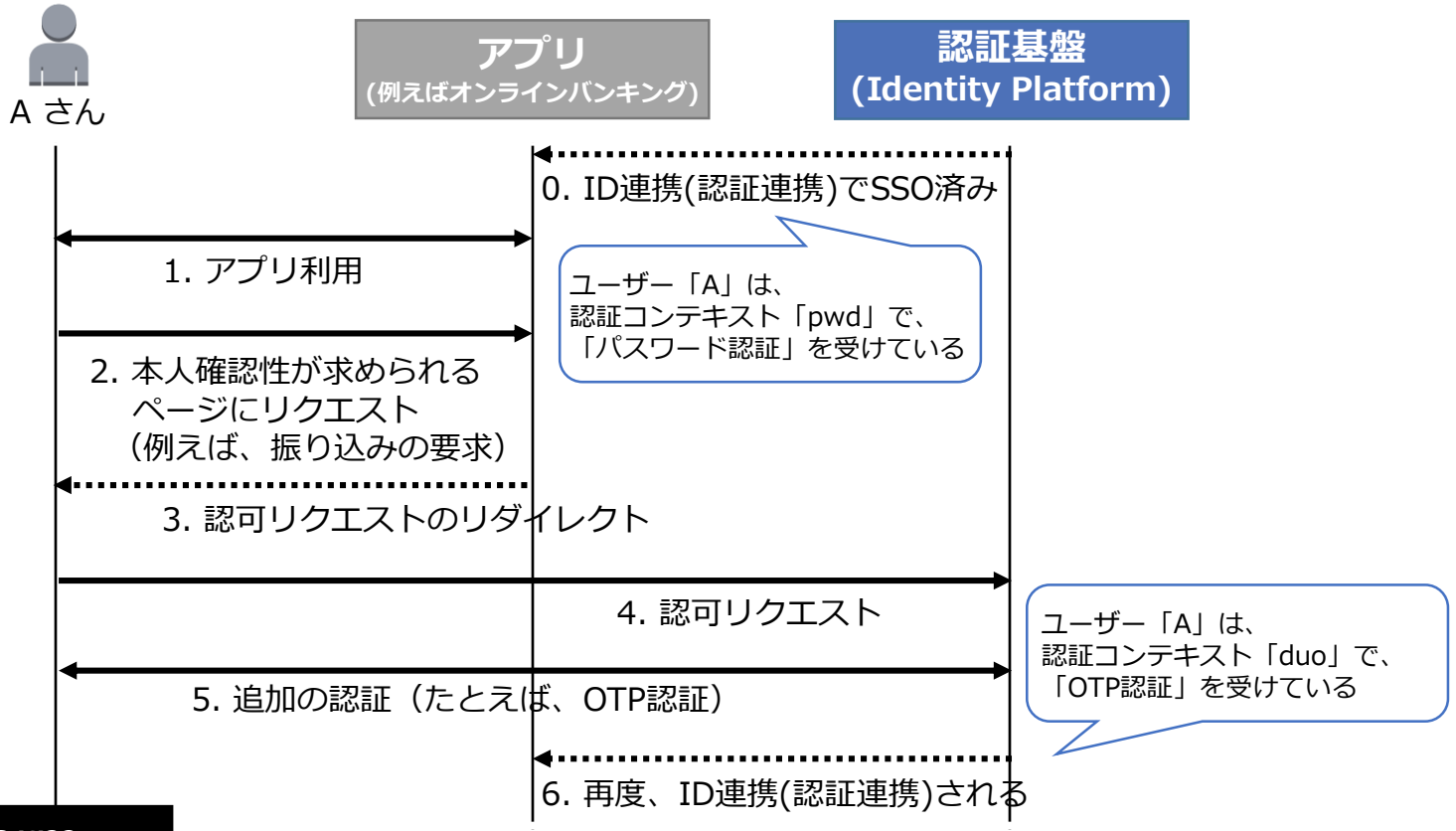


① Access TokenをSCIMエンドポイントに送信
② Access Tokenの有効性や所有者を確認
③ Access Tokenに紐付いたユーザーの属性（ここでは住所）を応答する
④ お届け先画面を生成する

Identity Platform
で実現可能

ID連携技術を使った認証連鎖の切り替え

- 認証基盤からID連携（認証情報の連携）を受けた場合、ユーザーが「どの認証連鎖」で、「どういった認証手段を用いた」のかの情報がアプリに連携される。アプリはこの情報を活用して、ユーザーに追加の認証を要求することが可能。



Identity Platform
で実現可能(v1.1.0予定)

まとめ ～顧客にサービスを提供するための認証基盤～

ロ 特徴

- 膨大なトラフィック、スパイクアクセス、機会損失などリスクに対応するために、高度な非機能設計が必要である
- 従来型の認証基盤のアーキテクチャを用いた構築では、サービス・インまでに時間がかかりすぎる傾向にある
- 従業員向けの認証基盤ほど機能要求は多く無い。ID連携技術を中心に機能実現が可能である

ロ アプローチ

- オージス総研では、認証基盤を作りなおした
- 従来のサーバーを用いたアーキテクチャではなく、AWSネイティブに作りなおすことで、一定の非機能を有する認証基盤を早く、簡単に構築できるようになった

２つのソリューションでアプローチ

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

- ✓**大規模な会員サイト向け**に特化した認証とID・属性連携のためのプラットフォーム
- ✓機会損失を回避するために**クラウドネイティブなアーキテクチャ**を採用

ThemiStruct-WAM（テミストラクト）
ThemiStruct-IDM（テミストラクト）
ThemiStruct-CM（テミストラクト）

- ✓ **エンタープライズ向け**や**ビジネスパートナー向け**に特化したのための統合認証プラットフォーム
- ✓ コアのソフトウェアに**OSS**を採用

ThemiStructで提供する３つのサービス

テクニカルサポートサービス

- 利用方法などの問合せへの回答
- 障害時の調査、回避策や代替案の提示、復旧の技術支援

プロフェッショナルサービス

- 要件実現方法の相談、回答
- 技術検証の支援
- 自社で実施する開発、構築の技術支援

システムインテグレーションサービス

- お客様の要望に応じたシステムを構築

AWS Summit Tokyo 2016 に出展します

株式会社オージス総研

Amazon API Gateway、AWS Lambda などのサービス上で直接稼動し、ピーク性のある大量アクセスに対応する高いレベルの可用性を実現した統合認証プラットフォーム「ThemiStruct (テミストラクト) Identity Platform」をご紹介します。

ThemiStruct (テミストラクト) Identity Platform »

■ 詳細情報・お申し込みは
http://www.ogis-ri.co.jp/pickup/themistruct/lineup/1250612_7683.html

本日のまとめ

1. 認証基盤、または、付帯技術（ID連携技術）の適用分野は広がっているし、適用分野によって要求事項が大きく異なる

2. 社内やBtoBにおける認証基盤は、多くの既存システムとの連携に複数の機能・技術仕様を以って連携する必要がある

3. BtoCにおける認証基盤はビジネスに直結するシーンで活用されるため、レベルの高い非機能を要求されるが、機能要求は多くなく、ID連携技術を中心に構成できる

4. オージス総研では双方のリクエストにお応えできるよう、商品ラインナップの拡充を実施
「ThemiStruct Identity Platform」をリリース

ご清聴ありがとうございました

ThemiStruct
テミストラクト

【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

OGIS-RI