ID連携技術を使ったクラウド、モバイル活用実現に向けて

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
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

オージス総研です

会社情報

社　　名	株式会社オージス総研
代 表 者	代表取締役社長　西岡　信也
設　　立	1983年6月29日
資 本 金	4.4億円　（大阪ガス株式会社100%出資）
事業内容	システム開発、プラットフォームサービス、コンピュータ機器・ソフトウェアの販売、 コンサルティング、研修・トレーニング
売上実績	366.8億円（単体）　参考　669.7億円（グループ単純合計）（2017年度）
従業員数	1,423名（単体）　参考　3,371名（グループ合計）（2018年3月31日現在）

オフィス

本　　社	大阪府 大阪市西区千代崎3-南2-37 ICCビル
東京本社	東京都 品川区西品川1-1-1 住友不動産大崎ガーデンタワー20階
千　　里	大阪府 豊中市新千里西町1-2-1
うつぼ本町	大阪府 大阪市西区靭本町1-10-24 三共本町ビル10階
名 古 屋	愛知県 名古屋市中区錦1-17-13 名興ビル
豊　　田	愛知県 豊田市小阪本町1-5-10 矢作豊田ビル４階

関連会社

さくら情報システム株式会社、株式会社宇部情報システム、
株式会社アグニコンサルティング、株式会社システムアンサー、
OGIS International, Inc.、上海欧計斯軟件有限公司（中国）

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）
IdentityPlatform

APIエコノミー時代の
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。
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。

現在の認証基盤の主要なユースケース

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

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連携認証システム**」を構築する

「社内統合認証基盤」を考える

企業におけるID管理・アクセス管理の必要性

- 情報セキュリティ対策
- 法令対応
- 認証制度への適合
- 内部統制、IT統制の構築

ID管理・アクセス管理とは何か？

> “アイデンティティとアクセス管理（IAM）は、正しい人が適切なタイミングで適切なリソースに適切な理由でアクセスできるようにするセキュリティ規律です。”

Gartner社「**Gartner IT Glossary**」より

引用元: https://www.gartner.com/it-glossary/identity-and-access-management-iam/

この講演では以下の表記を使います。

アイデンティティ管理 ➡ ID管理

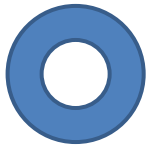
アクセス管理 ➡ アクセス管理

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）

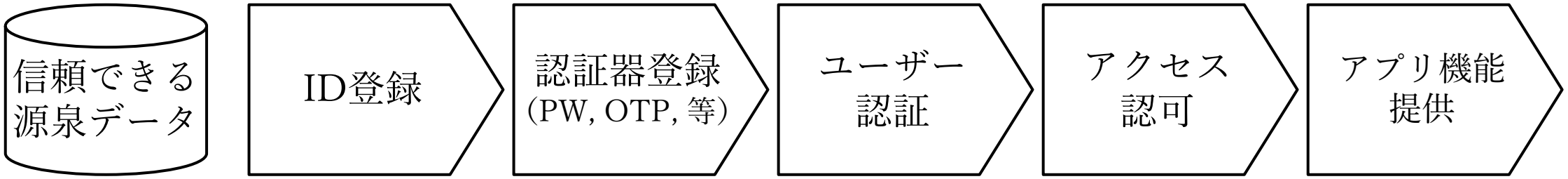
- 機密性: Confidentiality
- 完全性: Integrity
- 可用性: Availability　➡　本当は最も優先されるべき要素

利用を制限するための認証基盤

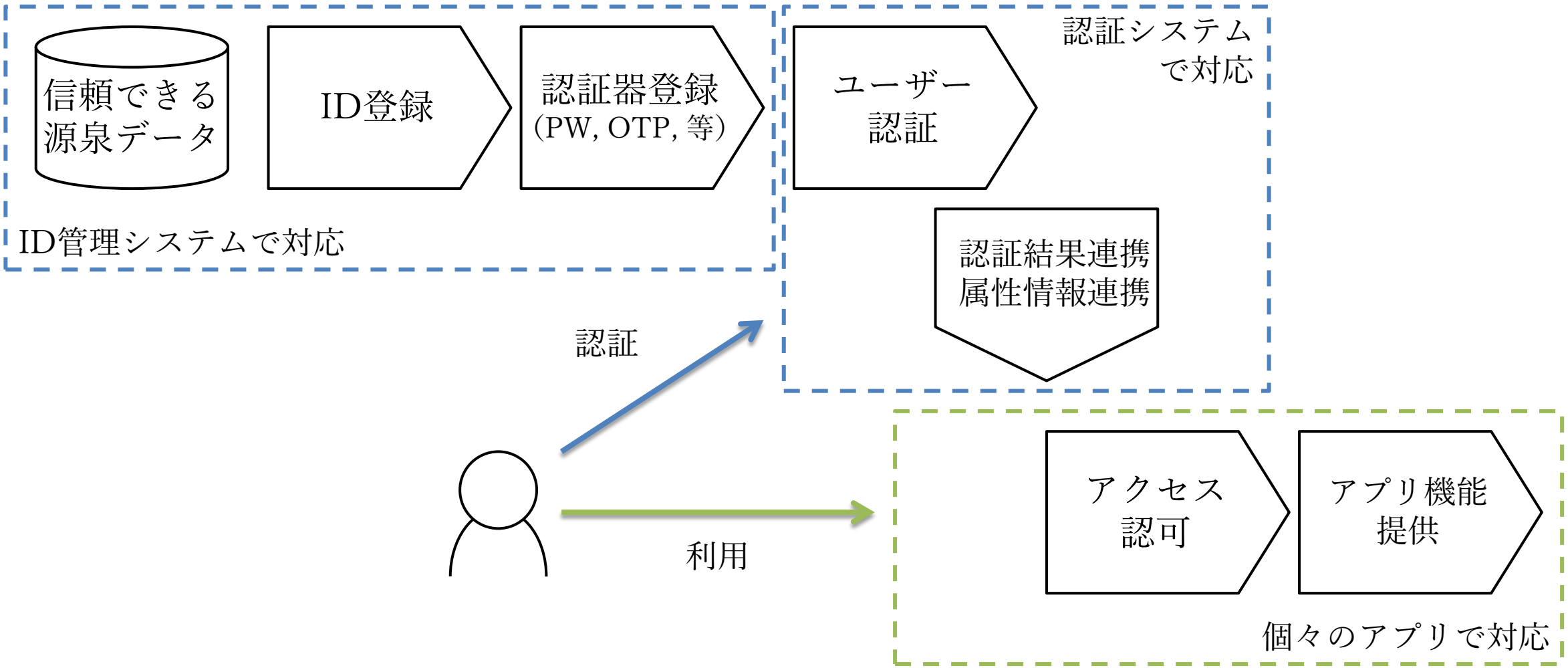


クラウド、デバイス、サービスを活用してもらうための認証基盤

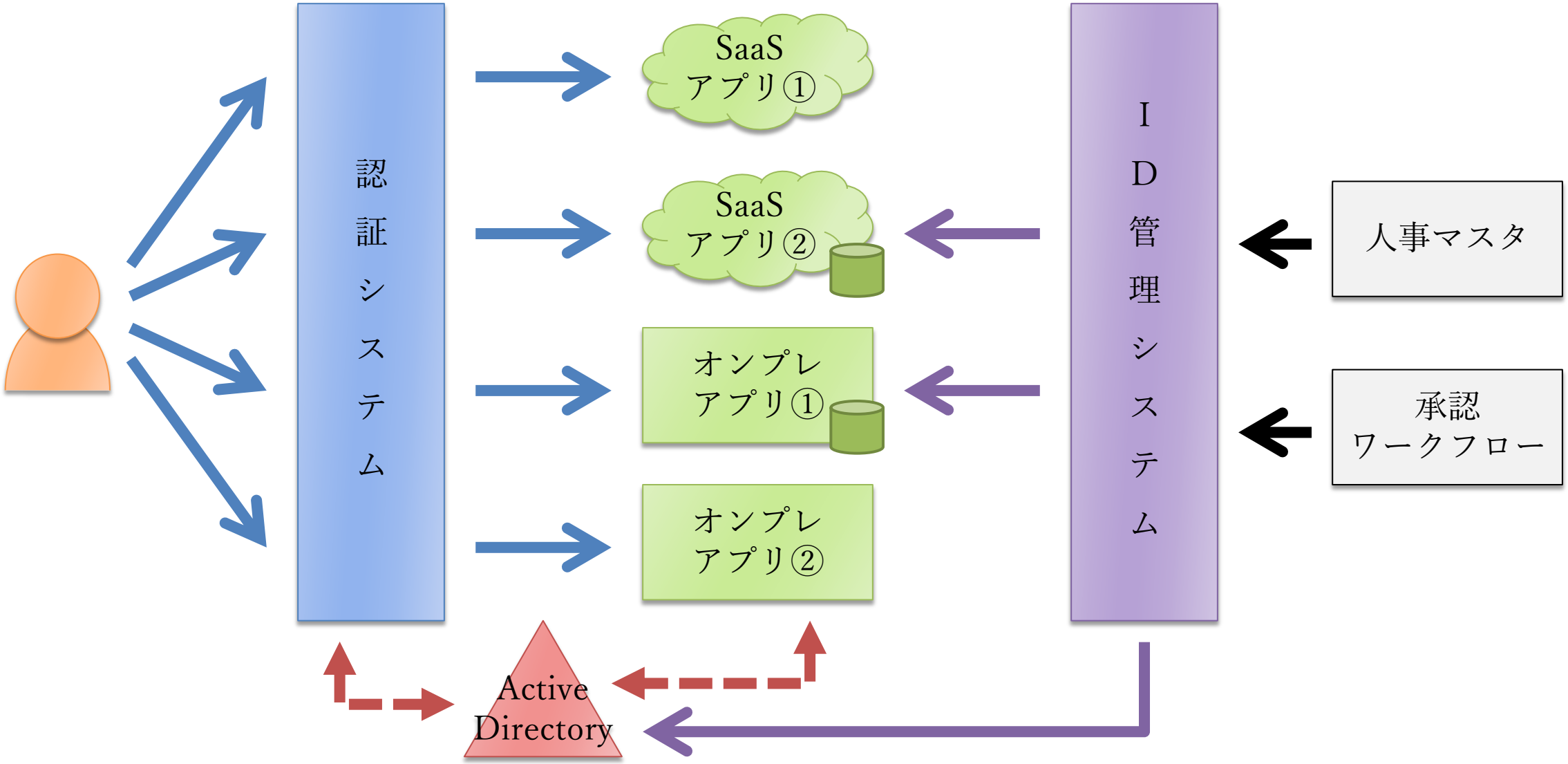
ID管理 と アクセス管理 のフロー



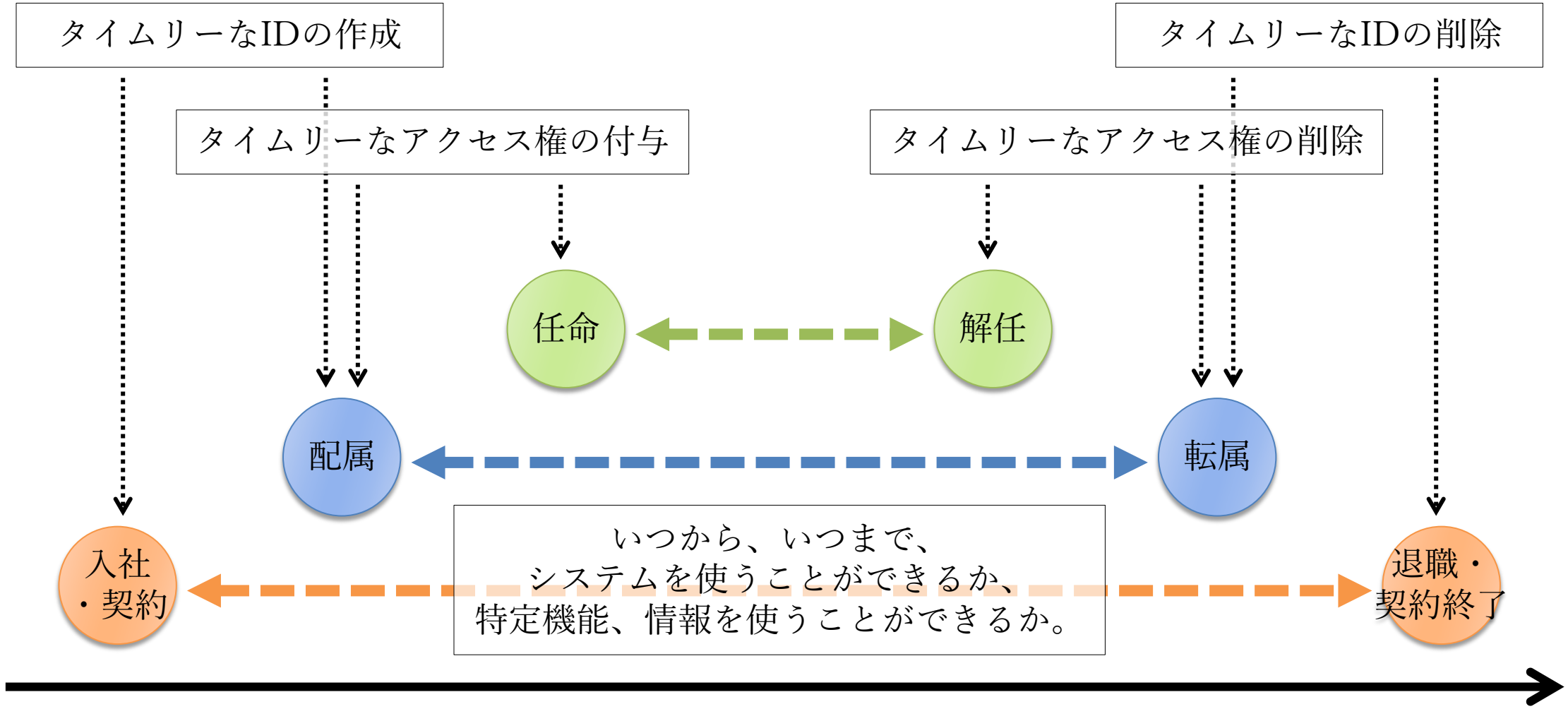
ID管理 と アクセス管理 のフロー



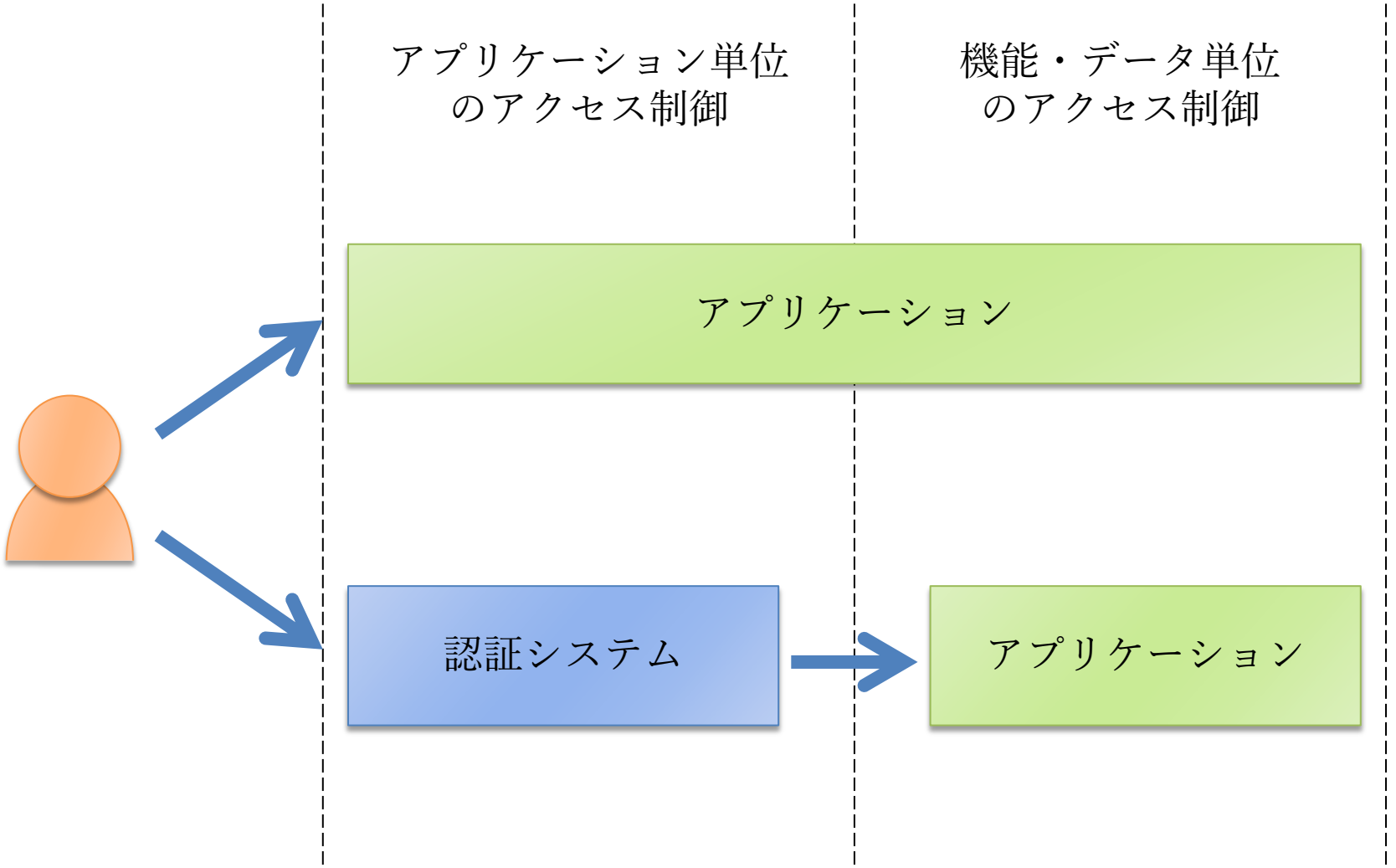
認証基盤の基本形



企業内のIDライフサイクル



アクセス制御をどこで実装するか



- 認証方式・強度の統一
- SSO利便性の提供
- アプリへのID管理対応必要性の低減

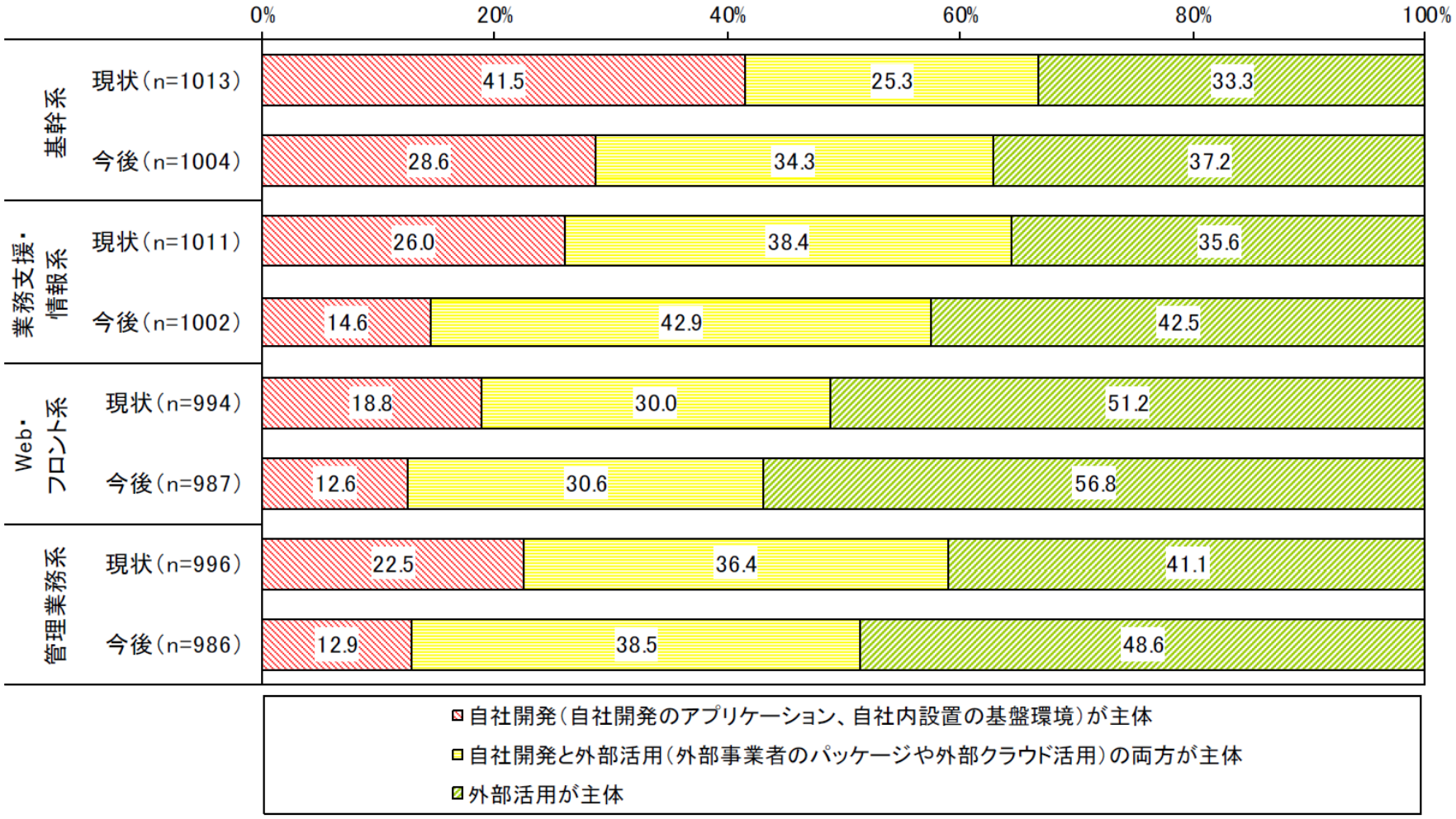
認証システム から アプリ へ認証結果を連携する（SSOする）

方式	クラウド対応	アプリ改修	モバイル対応	備考
ID連携技術 (SAML, OpenID Connect)	○	—	○	アプリ側での実装が必要である。標準化された技術であり、SaaS、パッケージでの対応が徐々に広がっている。
エージェント、リバースプロキシ ＋HTTPヘッダ連携	×	必要	○	アプリの認証画面の廃止、セッション生成機構部分の修正が必要。 認証システムから受け取るID情報だけでアプリを動かす、ID管理システム不要の構成も検討できる。
エージェント、リバースプロキシ ＋代理認証	×	不要	○	アプリの認証画面にID、パスワードをユーザーの代わりに入力する方式。 アプリごとに代理認証用のスクリプトを開発する必要がある。 ブラウザとアプリの間にリクエストを中継する機構が必要なため、SaaSには適用できない。
ブラウザ拡張	○	不要	×	ブラウザ拡張で、アプリの認証画面にID、パスワードをユーザーの代わりに入力する方式。 ブラウザ拡張が必要なため、対応ブラウザが制限される点、ブラウザ拡張の配布、設定方法の検討が必要。

業務向けIT活用の変化

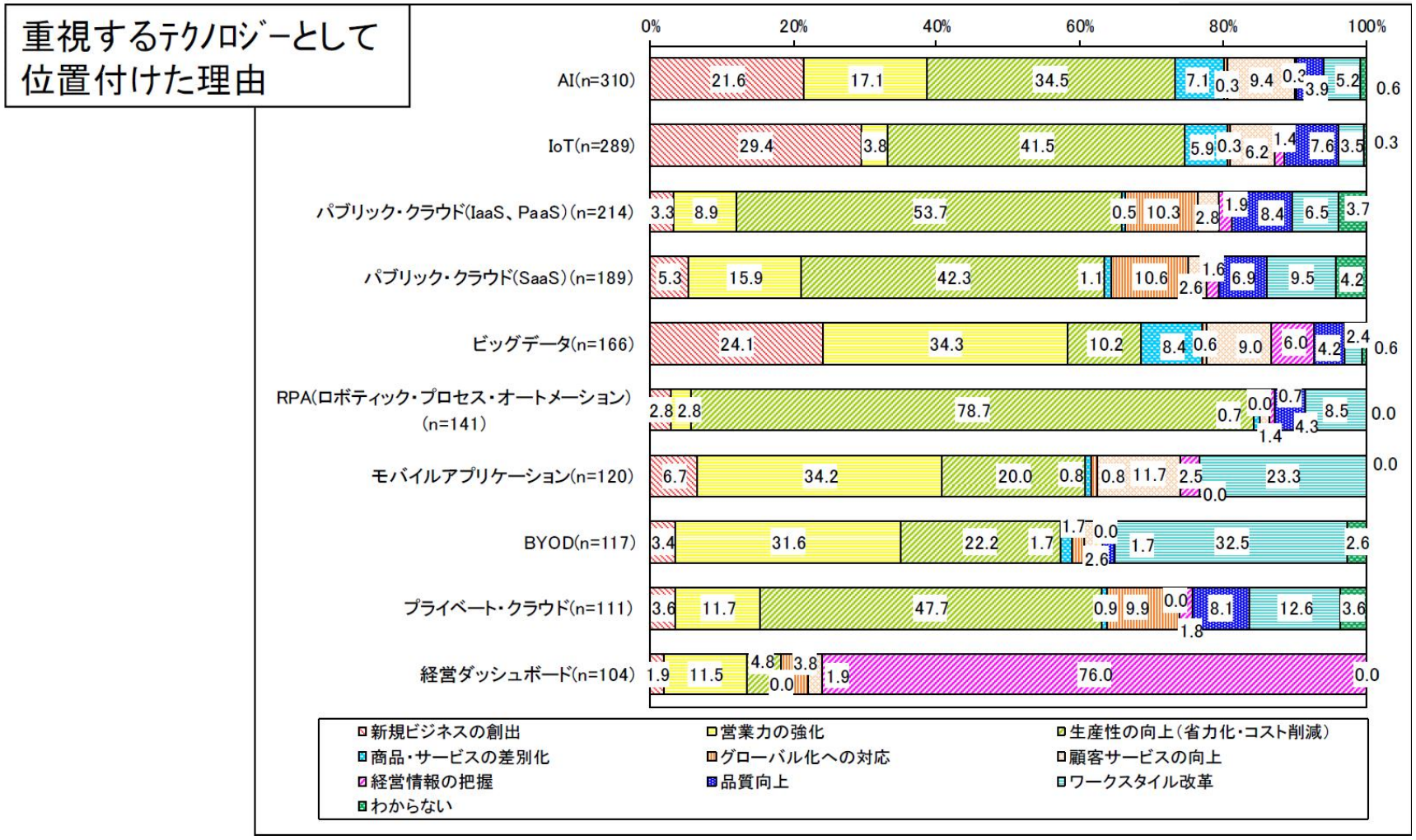
- **クラウド活用の拡大（SaaS）**
  - 自社開発 よりも パッケージ利用、パッケージ利用 よりも SaaS活用
- **デバイスが多様化**
  - PC から スマホ/タブレット の活用へ
- **利用時間、利用場所の拡大**
  - オフィス内、移動中、在宅勤務
- **クラウド活用したシステム開発への対応（PaaS）**
  - PaaSの認証機能との連携の必要性

【参考】パッケージ、SaaS活用 志向が高まってきている



出典: 一般社団法人日本情報システム・ユーザー協会「企業IT動向調査報告書2018」報告発表資料, p79
<http://www.juas.or.jp/cms/media/2017/02/it18_ppt.pdf>

【参考】営業力強化、ワークスタイル改革にモバイルアプリとBYODを重視



出典: 一般社団法人日本情報システム・ユーザー協会「企業IT動向調査報告書2018」報告発表資料, p45
<http://www.juas.or.jp/cms/media/2017/02/it18_ppt.pdf>

業務向けIT活用の変化

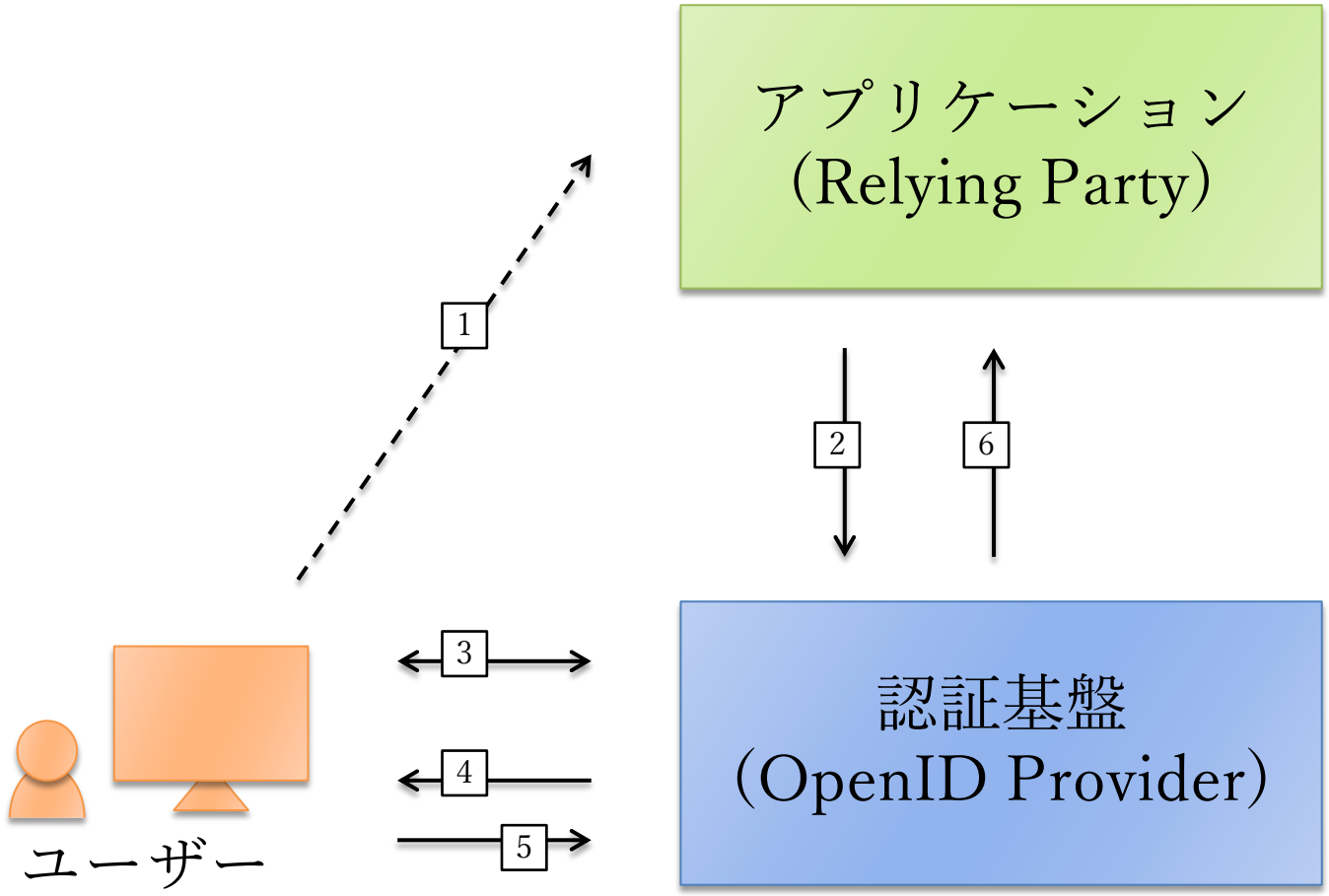
- **クラウド活用の拡大（SaaS）**
  - 自社開発 よりも パッケージ利用、パッケージ利用 よりも SaaS活用
- **デバイスが多様化**
  - PC から スマホ/タブレット の活用へ
- **利用時間、利用場所の拡大**
  - オフィス内、移動中、在宅勤務
- **クラウド活用したシステム開発への対応（PaaS）**
  - PaaSの認証機能との連携の必要性

認証基盤で対応しておくべきこと、など

- ID連携技術への対応
- 状況に応じた認証方式の選択
- 認証状態の管理、アプリセッション管理の考え方の見直し
- プロビジョニング方式の選択

ID連携技術への対応

OpenID Connect を使ったID連携の例



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。

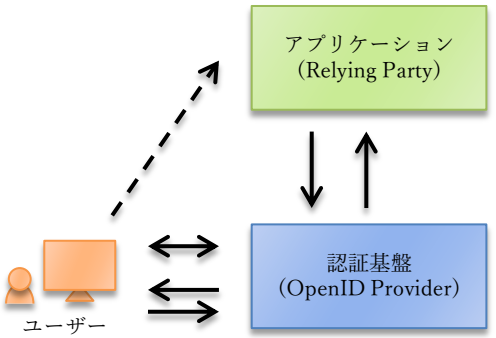
※ 概念を図示するため、実際のリクエスト・レスポンスの方法、回数等を簡略化しています。

状況に応じた認証方式の選択

- パスワード認証
- ワンタイムパスワード（OTP）
- FIDO U2F
- クライアント証明書の利用
- 統合Windows認証（デスクトップSSO）
- 認証方式を選択して、あるいは組合せて使用する
  - 認証連鎖、認証ツリー、リスクベース認証、…

認証状態の管理、アプリセッション管理の考え方の見直し

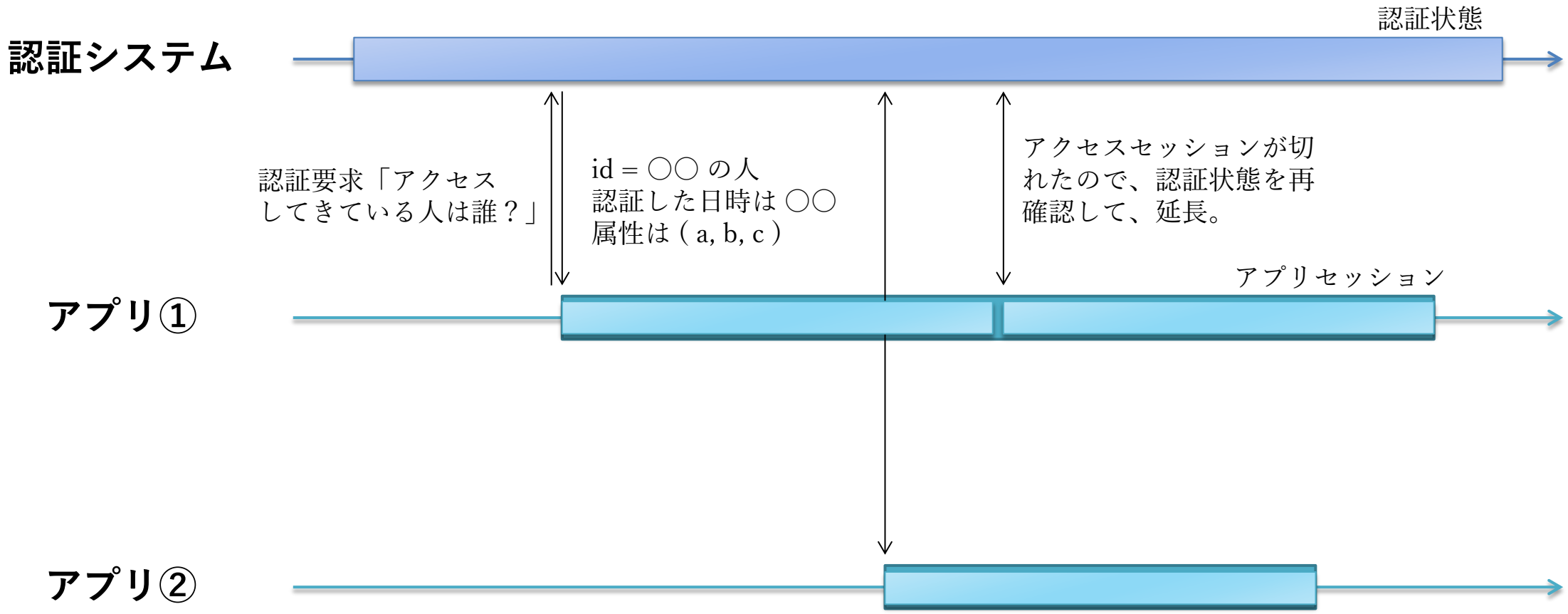
- **認証システム と アプリケーション で管理主体が異なる。**
  - 認証システム上の認証状態
  - アプリケーションのセッション状態　はそれぞれが管理



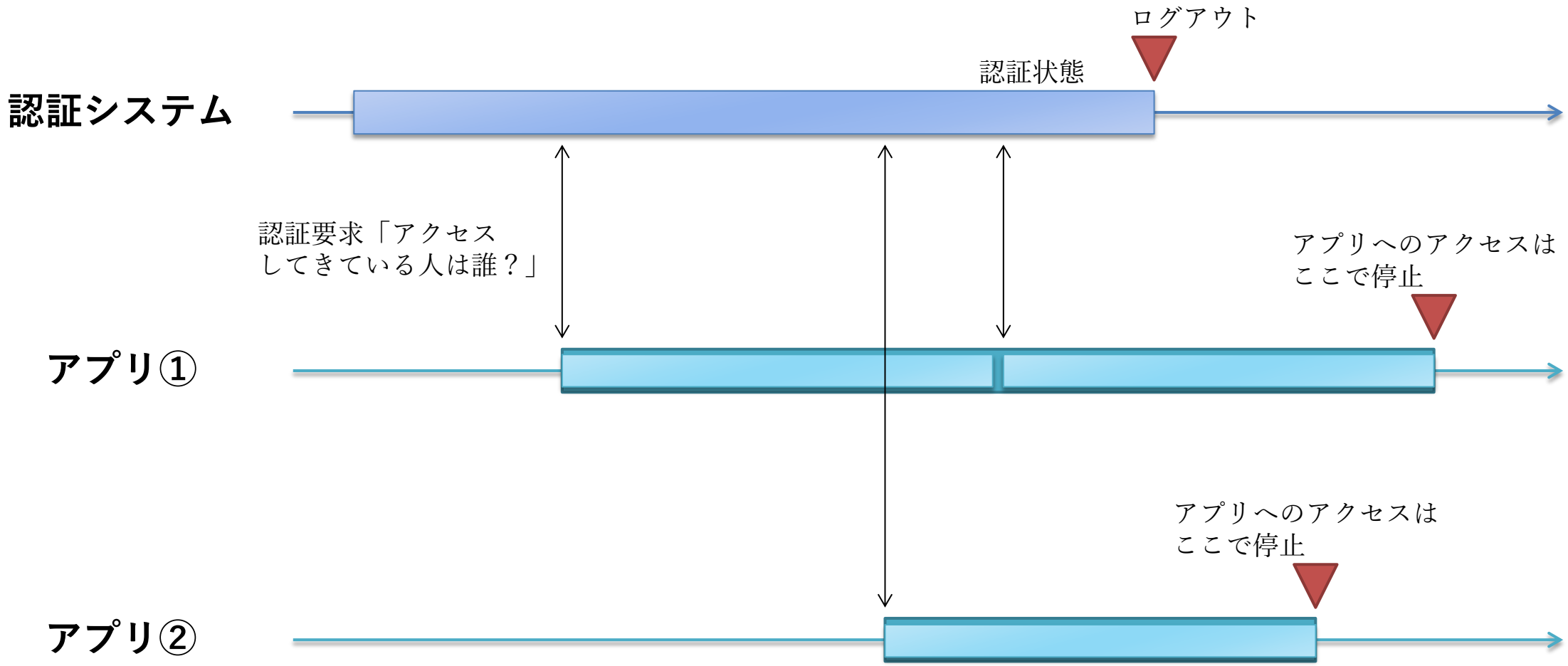
- **異動等に伴うシステムの利用停止をどう実現するか？**
  - セッション管理の考え方で対応
  - リスクが高いシステムは、即時プロビジョニングで対応

- **権限に関わる属性変更された時の反映をどう実現するか？**
  - 現在はプロビジョニングによる方式が唯一の選択肢か

セッション管理の考え方 ①



セッション管理の考え方 ②



プロビジョニング方式の選択

ID連携時の属性連携

- 比較的運用がしやすい
- 対応可能なSaaSが限られる

事前プロビジョニング

- 標準技術 SCIM を使う
- アプリケーション（パッケージ、SaaS）独自のインタフェースを使う
- ID管理システムで連携開発を頑張る

Just-in-time プロビジョニング

- アプリケーション利用開始時、SCIM、独自インタフェースを使って

モバイル向けアプリに
どう対応していくか

モバイル向けアプリの分類

- **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
- **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	—	○

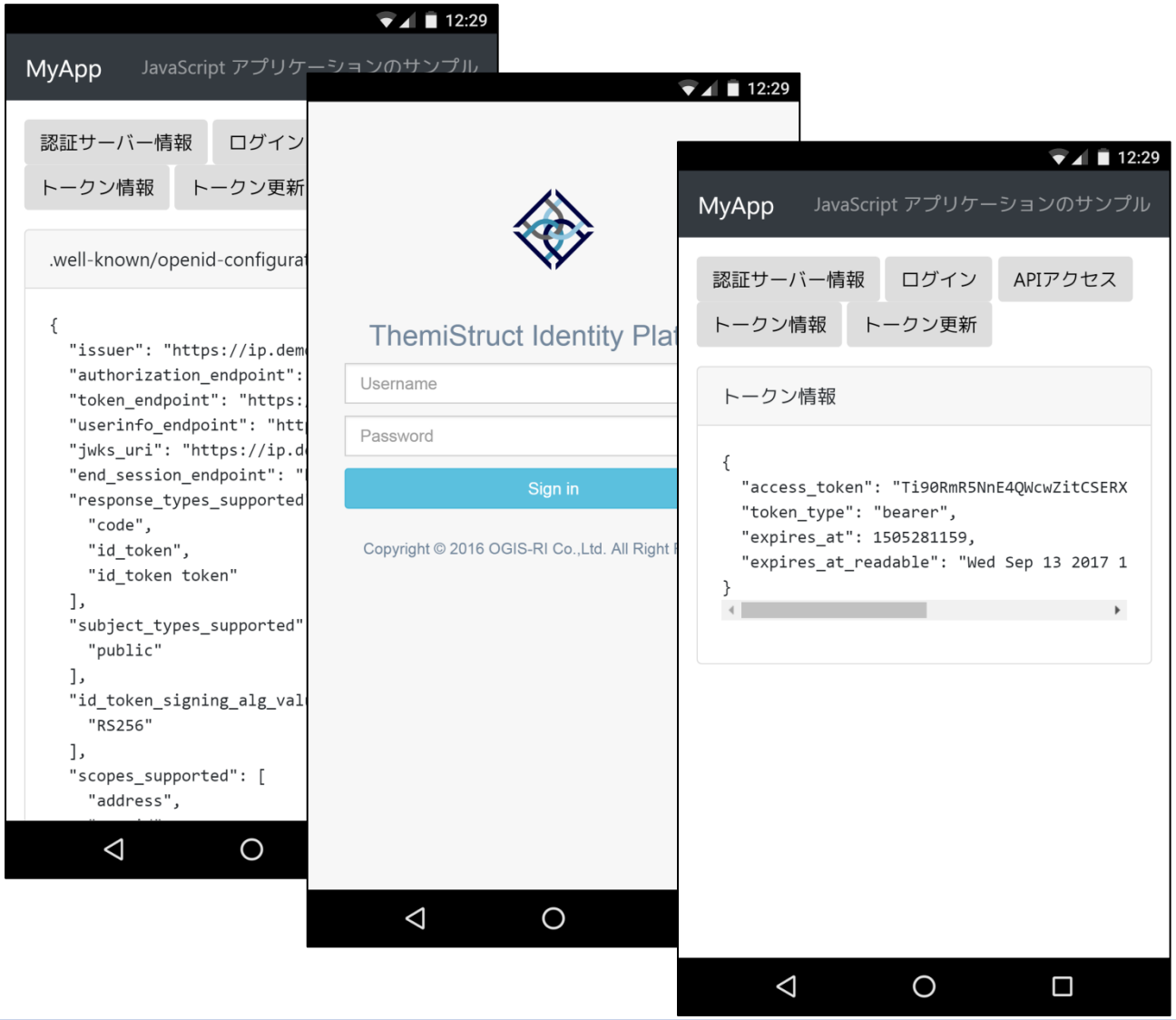
認証・アクセス認可の実装の考え方

	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 Authorization Code Grant + PKCE を用いたバックエンドAPIへのアクセス認可 （OAuth 2.0 Security Best Current Practice（draft）の動向の考慮も必要）	
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 Authz Code, Authz Code+PKCE （OIDF FAPI WGの動向の考慮も必要）

Office 365 モバイルアプリ + ThemiStruct

Office 365 モバイルアプリ利用時はThemiStruct Identity Platform を使って認証

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




```
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

モバイル向けアプリを展開する上での課題

- **SaaSを利用する場合は、SAML or OpenID Connect に対応していることが必要。**

- **SaaSがネイティブアプリを提供しているケースでは、認証にWeb画面を使用する方式になっていることが必要。**
  - こちらは、まだまだ対応できているSaaSは少ない。

認証基盤の運用事例

私の部門で使用しているシステム類

- スケジューラー
- ディスカッションボード

Daigas グループ共通認証システムで管理

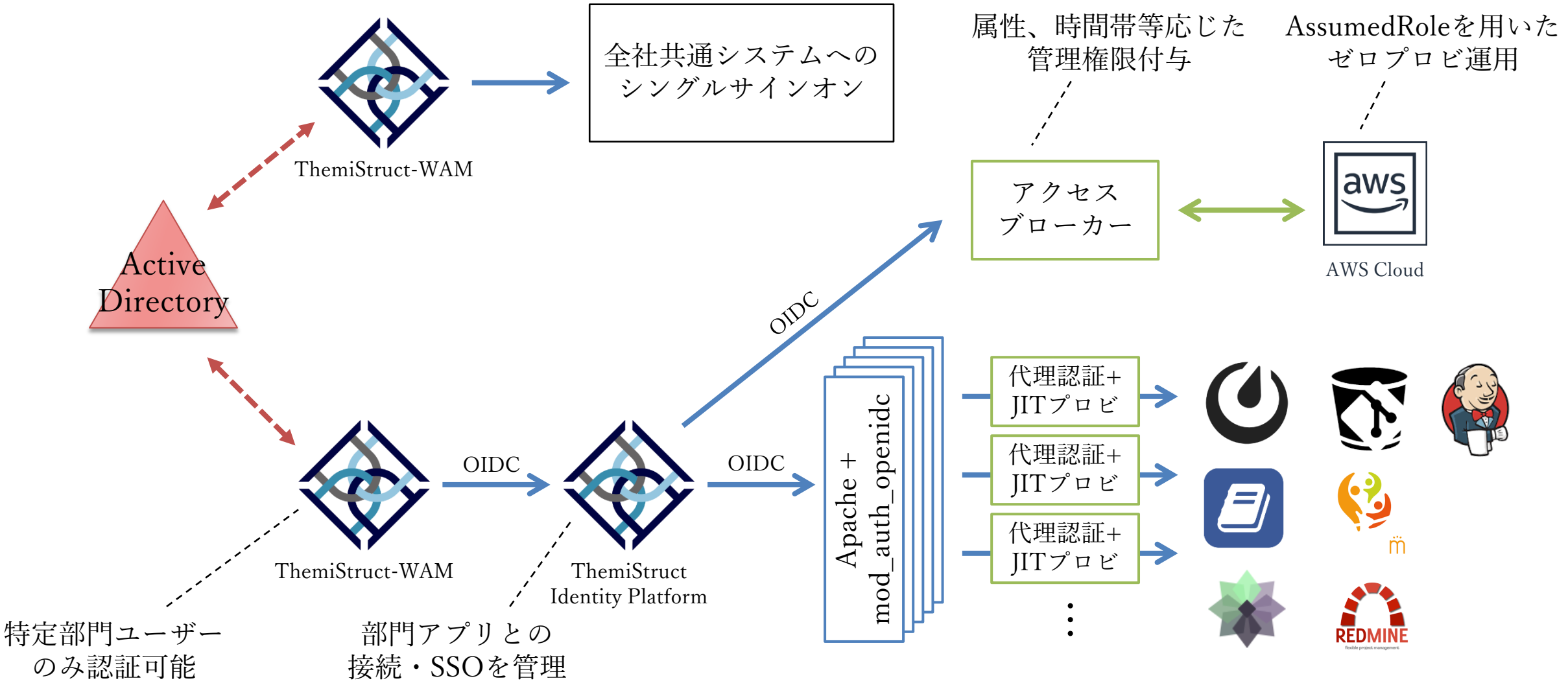
- ドメインログオン
- メール
- ポータル
- ワークフロー
- 経費/人事セルフサービス
- リモートアクセス

当社 全社共通の認証基盤で管理

- **チャット (Mattermost)**
- **リポジトリ (GitBucket)**
- **CI (Jenkins)**
- **ナレッジ管理 (Knowledge)**
- **プロジェクト管理 (Taiga, Pleasanter, Redmine)**
- **AWS管理コンソール**

部門の認証基盤で管理
ユーザーリポジトリに全社 Active Directory を使うことで、異動情報反映の運用の手間を削減

全社リポジトリと連携した部門認証基盤を構成



メリットと課題

ロ　メリット

- 部門の業務で活用するシステムが多数あるが、メンバーの増減にともなうIDメンテナンスの作業は不要。
- アカウントがないことでツールが使われない問題が改善されて、ナレッジ文書の共有、チャットによる情報共有やディスカッションが進む。

ロ　課題

- 新しいソフトウェアを投入するときに、ちょっとした開発が必要。
  - JITプロビジョニングの実現、代理認証の実現
- 離任時にはタイムリーにシステムが使えない状態になるが、アプリ毎のアカウント棚卸と、不要アカウントに削除運用は、定期的に手作業で必要あり。

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

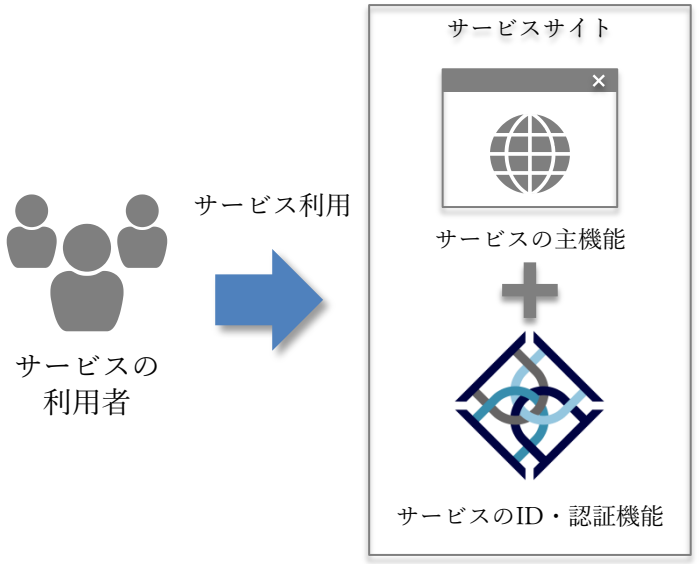
ThemiStruct（テミストラクト）
IdentityPlatform

APIエコノミー時代の
統合認証パッケージ

統合認証パッケージ ThemiStruct Identity Platform

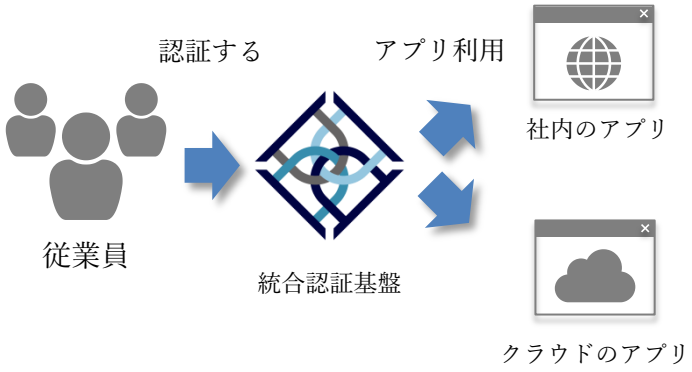
ThemiStruct Identity Platform は、ITシステム利用者のアイデンティティ管理と認証の機能を提供します。顧客向けにサービスを展開したり、従業員向けにアプリケーションを展開する際に必要となる、共通ID基盤の構築に活用いただけます。

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

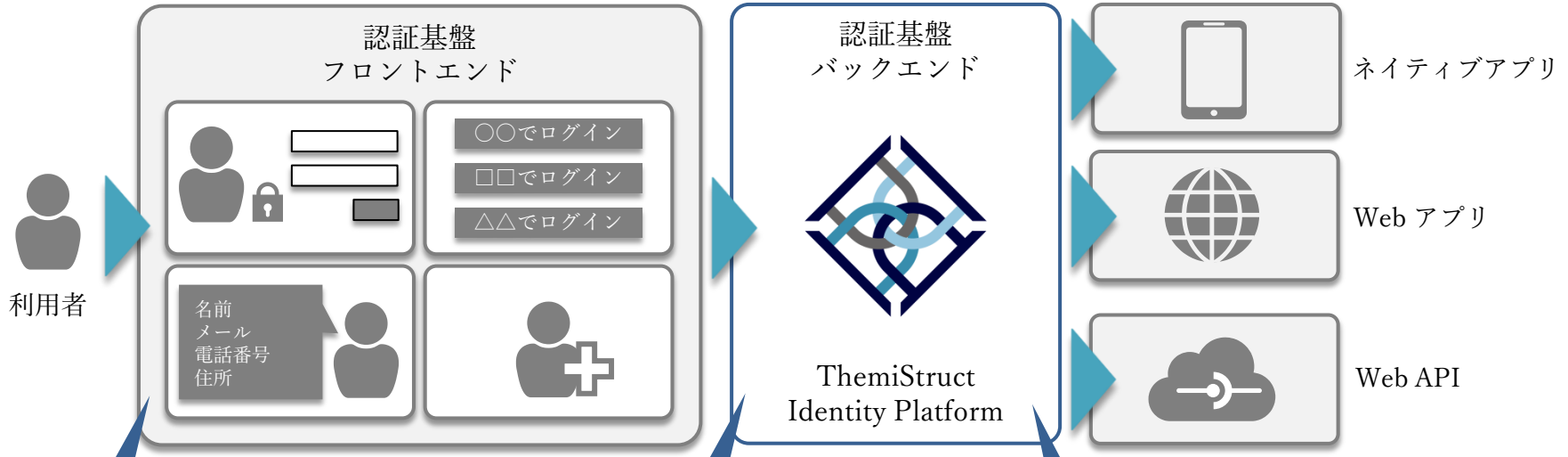
エンタープライズ領域に活用



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、サービスの利用者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、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、アクセス認可の機能をアプリに組み込む

利用者のID情報の管理や認証などの共通機能を、サイトの統一されたデザインで組み込むことができます。

Web APIの認証・アクセス認可に対応

OAuth 2.0 を使ったAPI連携認証システムが実現でき、モバイルアプリ、オープンAPIを安全に公開できます。

短期間での導入が可能

スモールスタート、突発的アクセス集中に対応できる伸縮可能かつ事業継続性を考慮した認証基盤が、2時間でセットアップできます。

『顧客向けサイト』に向けた3大特長

ロ　IDとユーザー認証、アクセス認可の機能をアプリに組み込む

- 利用者のID情報の管理や認証など利用者IDに関連する共通機能の実装を支援する『フレームワーク』と『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に認証機能やパスワード変更機能、アプリケーションへのID連携機能などを組み込むことができます。

ロ　Web APIの認証・アクセス認可に対応

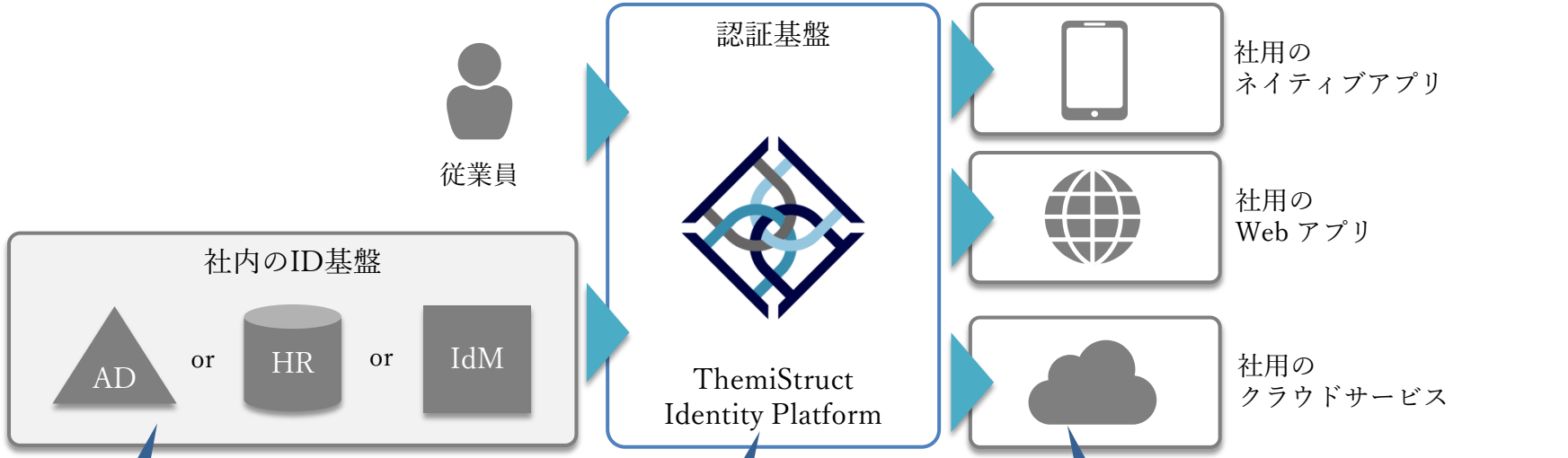
- OAuth 2.0 の技術仕様に基づいた認証・アクセス認可機能を提供します。OAuth 2.0 を使ったAPI連携認証システムが実現でき、モバイルアプリ、オープンAPIを安全に公開できます。

ロ　短期間での導入が可能

- AWSマネージドサービスのコンポーネントを活用し、導入時におけるキャパシティやアベイラビリティプラニングから解放します。スモールスタート、突発的アクセス集中に対応できる伸縮可能かつ事業継続性を考慮した認証基盤が、2時間でセットアップできます。

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

多要素、多段階認証に対応し多様なセキュリティ要件に応じた認証機能を提供します。

シングルサインオン

社内、社外問わず、様々なアプリケーション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。社内、社外問わず、様々なアプリケーションにシングルサインオンできます。

ロ　企業ポリシーの適用

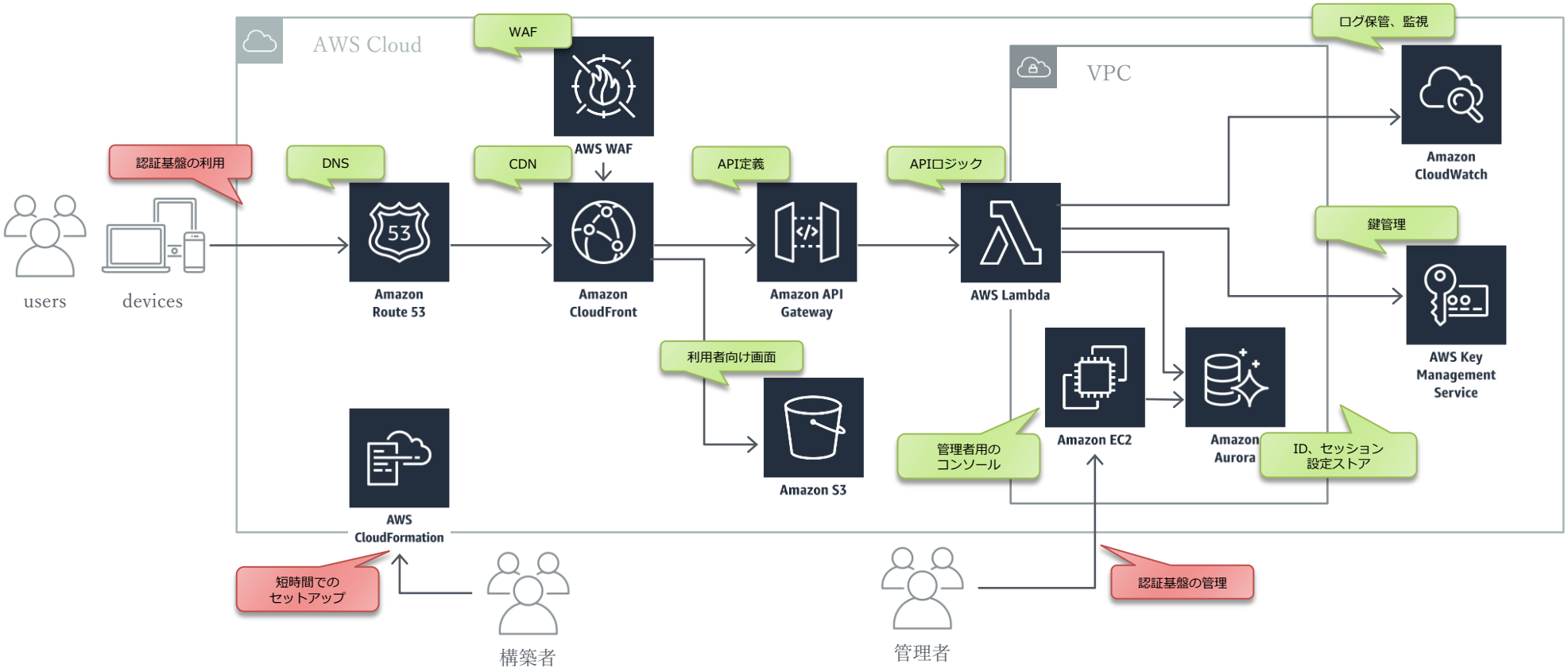
- ユーザーの属性や状態、利用するアプリケーションに応じて、柔軟な認証ポリシーをデザインすることができます。例えば、社内ネットワークからのアクセスの場合、IDとパスワードの認証を提供し、外出先からのアクセスの場合、追加でワンタイムパスワード認証を提供するといったポリシーを展開することができます。

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APIを提供しています。これにより、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。

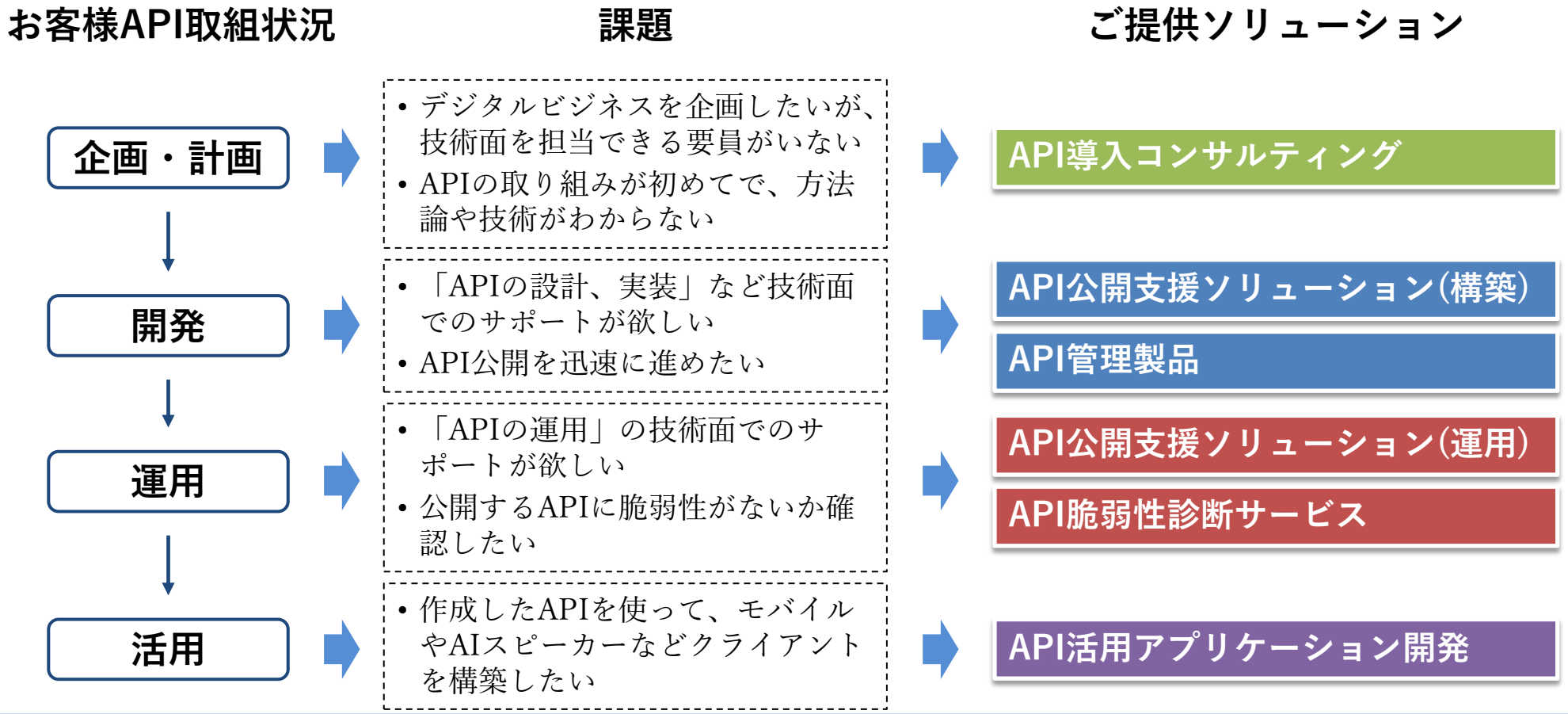
サーバーレスアーキテクチャを採用

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。



オージス総研のAPIソリューション

- APIの技術調査・検討から運用までのフルカバー
- API利用者のニーズを捉えたビジネスの継続的な進化を実現



まとめ

まとめ

- 企業でのIT活用と情報アクセス管理には認証基盤が不可欠である。
- 企業の業務のためのIT活用方法は、時代とともに変化している。
- クラウド、パッケージとの接続性を高めるためのID連携技術に対応、利用環境に応じて多彩な認証方式に対応できるよう、認証基盤でも対応をしていく必要がある。
- 部門、プロジェクトなどドメイン特化の認証基盤を構築する、JITプロビジョニングを活用するなどで、認証基盤の導入・維持の障壁を下げる検討も有効である。
- 当社では ThemiStruct シリーズを提供。それらを組み合わせて社内統合認証基盤、共通ID基盤、API連携認証システム の構築ニーズに対応する。

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 / 06-6871-8054
mail: info@ogis-ri.co.jp

OGIS-RI