ThemiStruct
テミストラクト

これから企業の認証基盤に求められること

～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

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

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

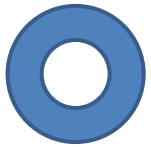
アクセス管理 ➡ アクセス管理

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）

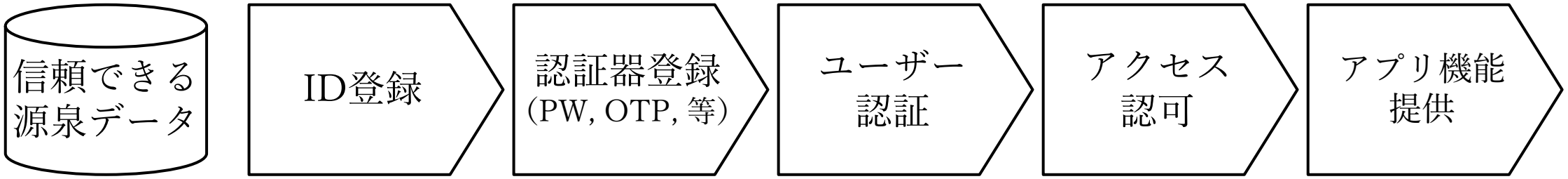
- 機密性: Confidentiality
- 完全性: Integrity
- 可用性: Availability　➡　本当は最も優先されるべき要素

利用を制限するための認証基盤

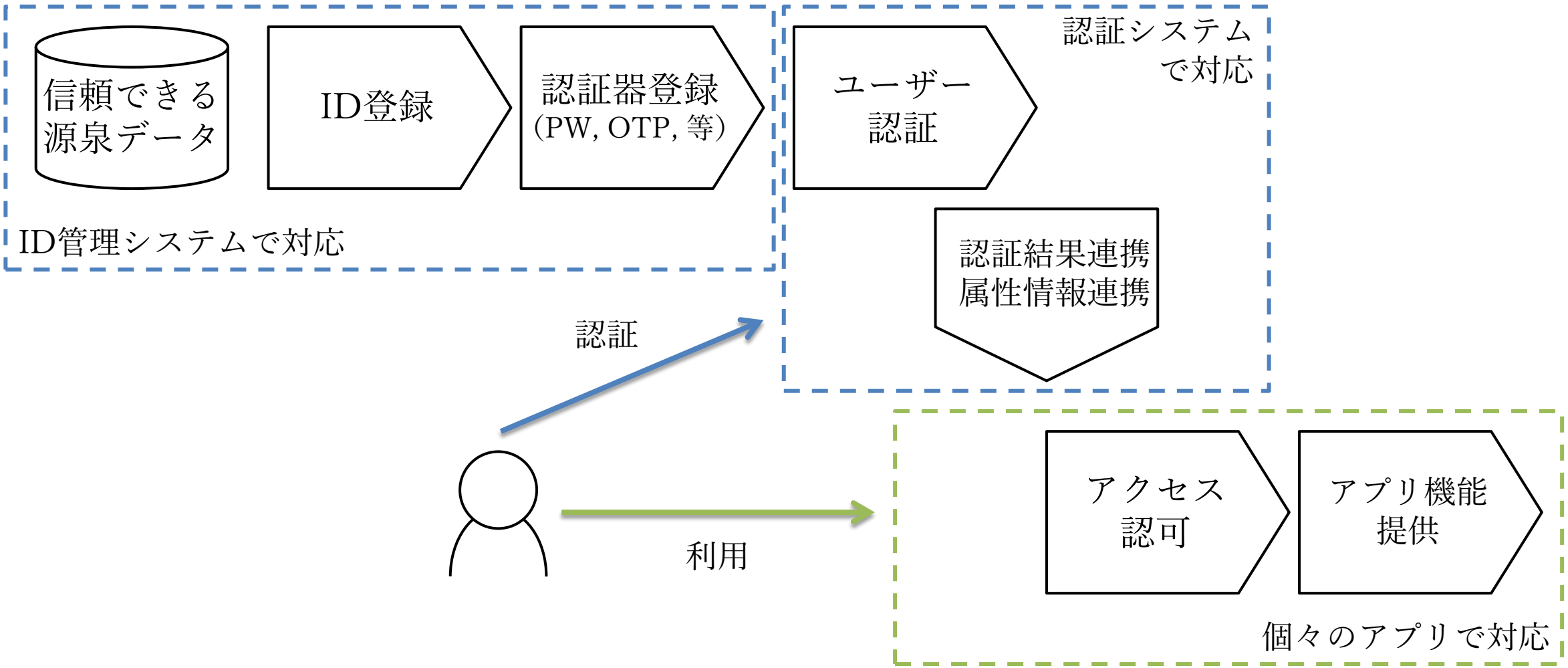


クラウド、デバイス、サービスを活用してもらうための認証基盤

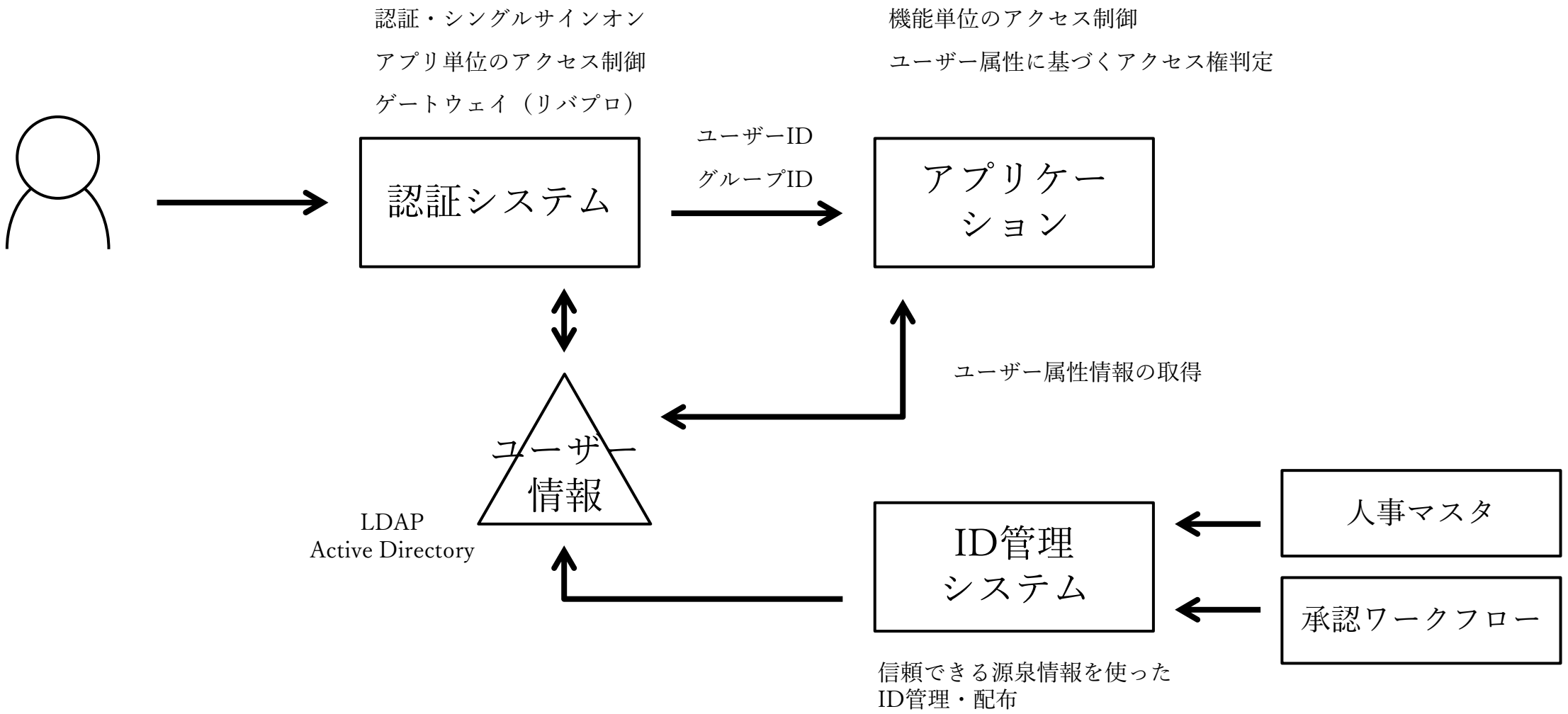
ID管理 と アクセス管理 のフロー



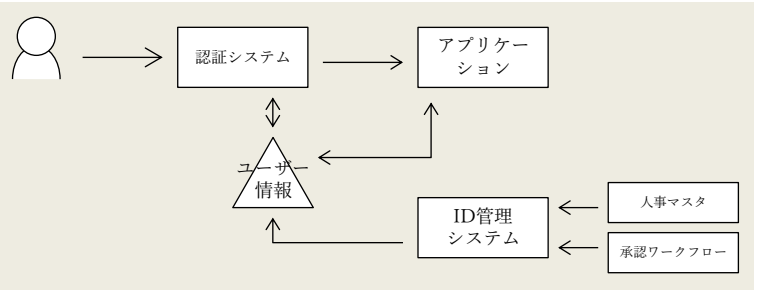
ID管理 と アクセス管理 のフロー



認証基盤の基本形



認証基盤の基本形



ロ 良い点

- ➢ 認証・アクセス制御の関所化
  - ● 退職等での利用停止を1箇所で対応
- ➢ 個別のID管理なしに最新の情報に基づいた権限を付与

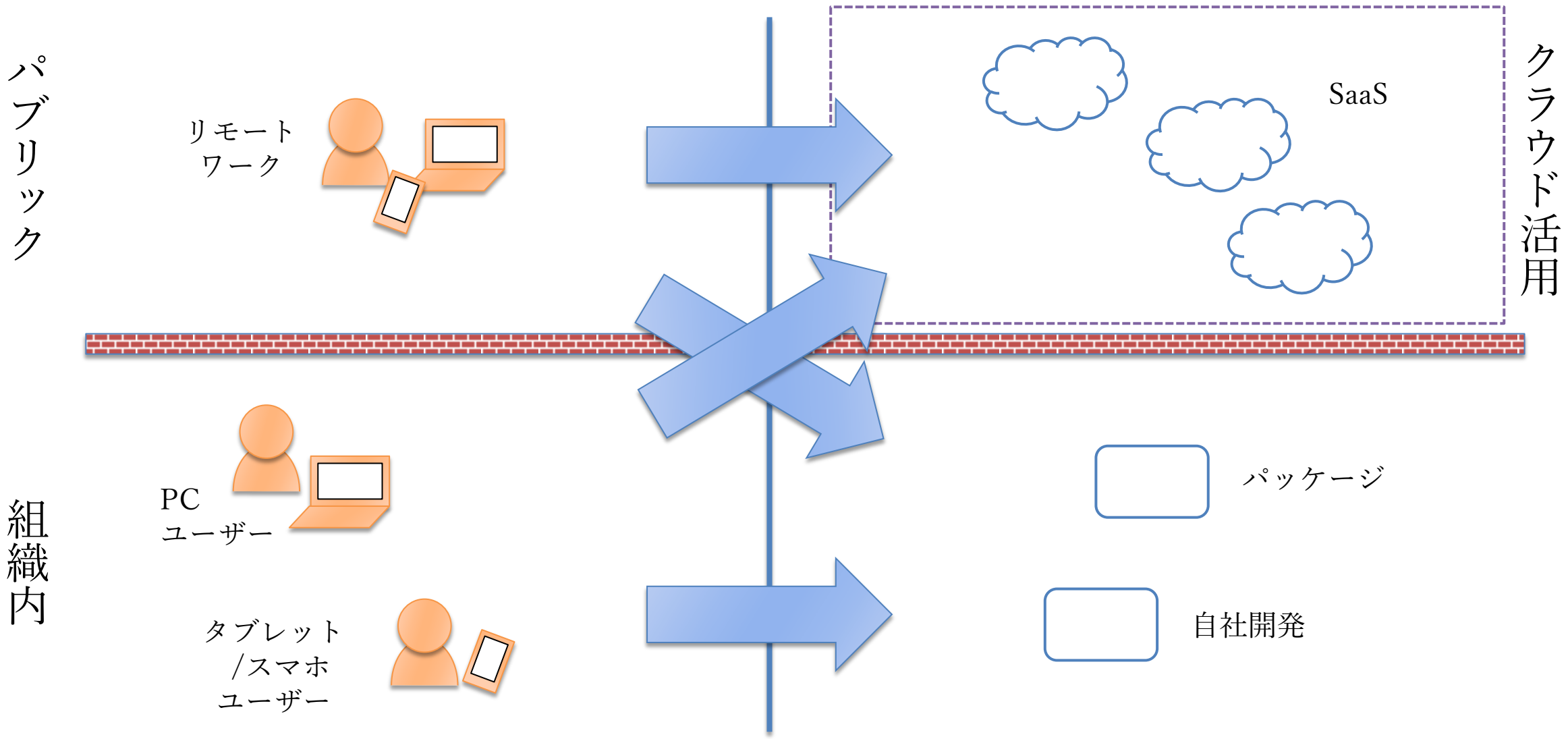
ロ 問題点

- ➢ アプリケーション開発ガイドの展開とそれに基づいた開発
- ➢ 個別にID登録が必要なアプリケーション（パッケージ、SaaS）の接続
- ➢ ゲートウェイ（リバプロ）経由アクセスにできないSaaSへの対応

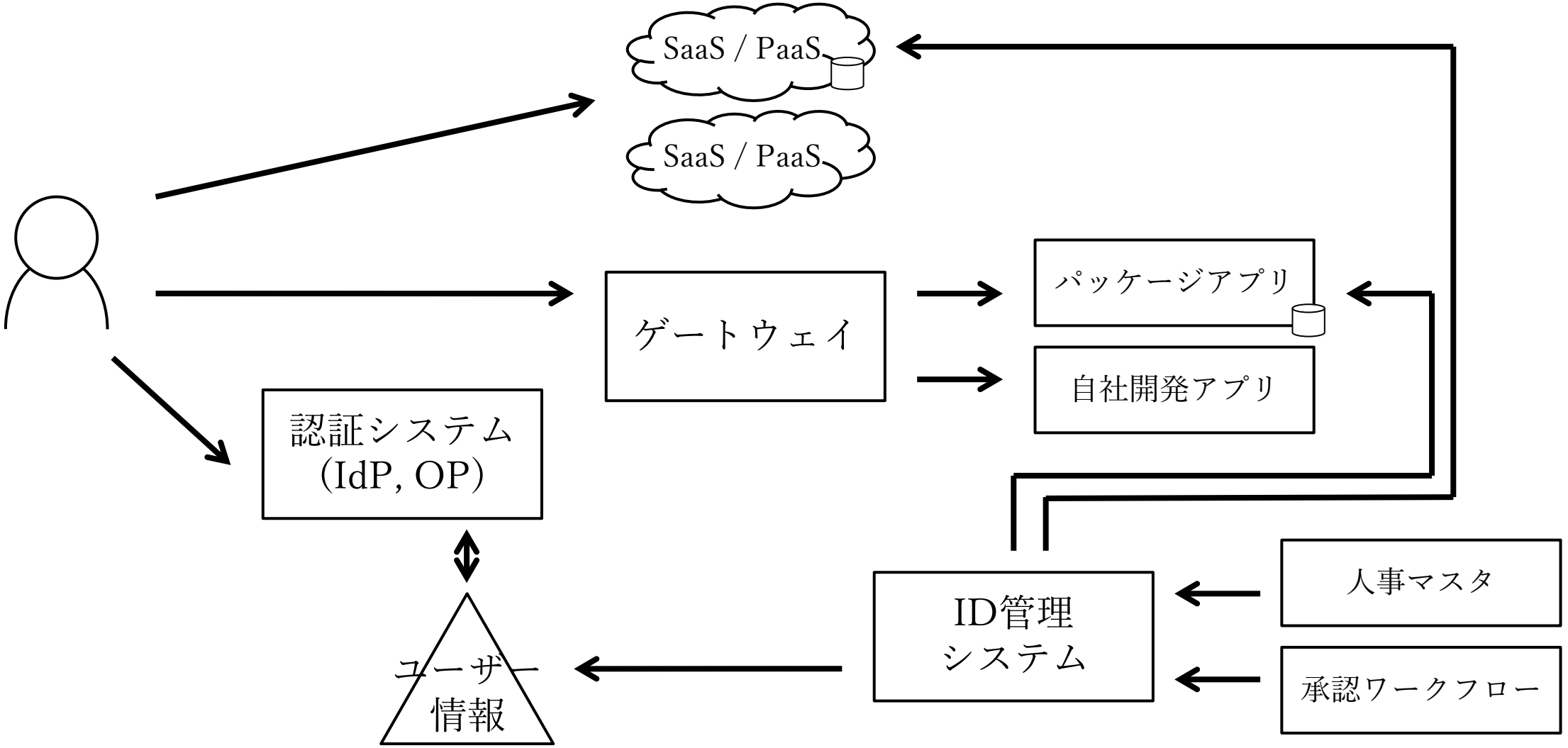
業務向けIT活用の変化

- **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

業務向けIT活用の世界観



認証基盤の基本形

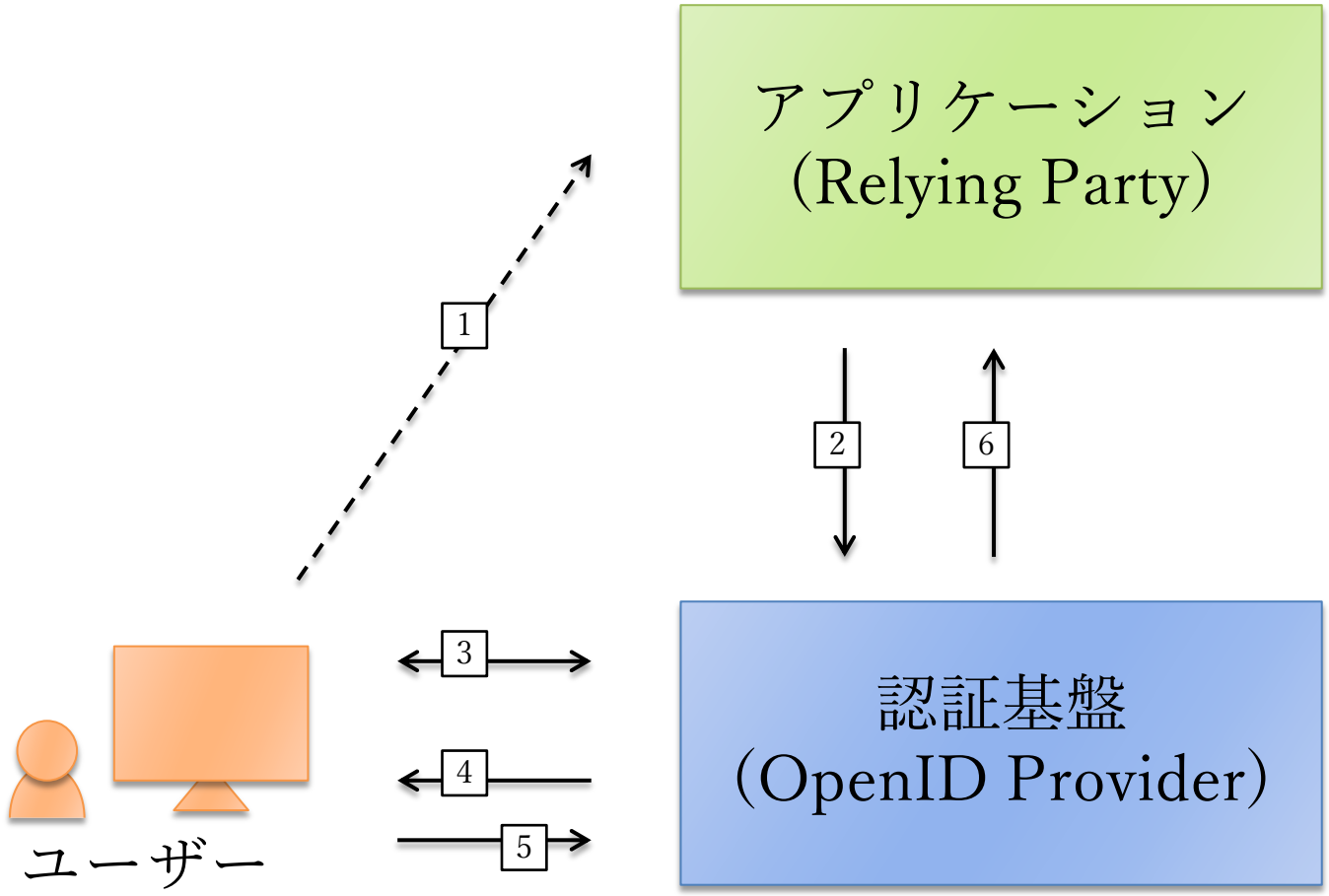


認証基盤で対応しておくべきこと、など

- 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

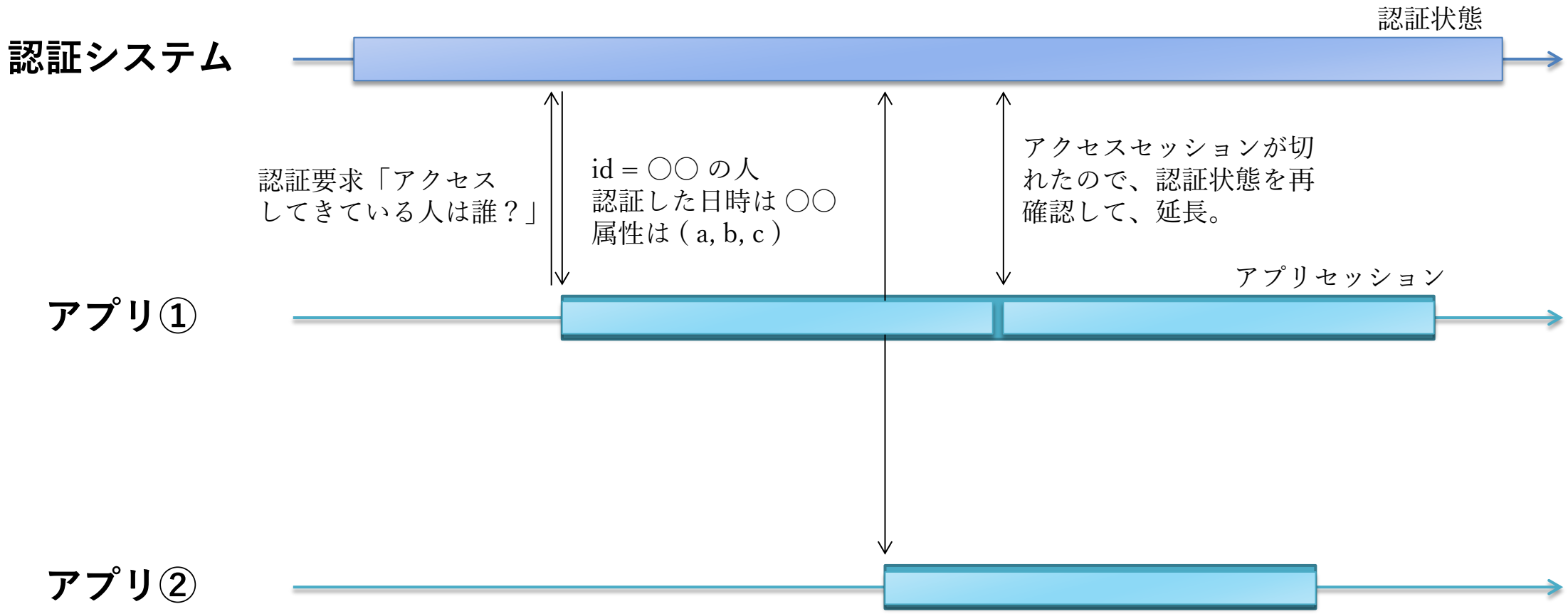
認証状態の管理、アプリセッション管理の考え方の見直し

- **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

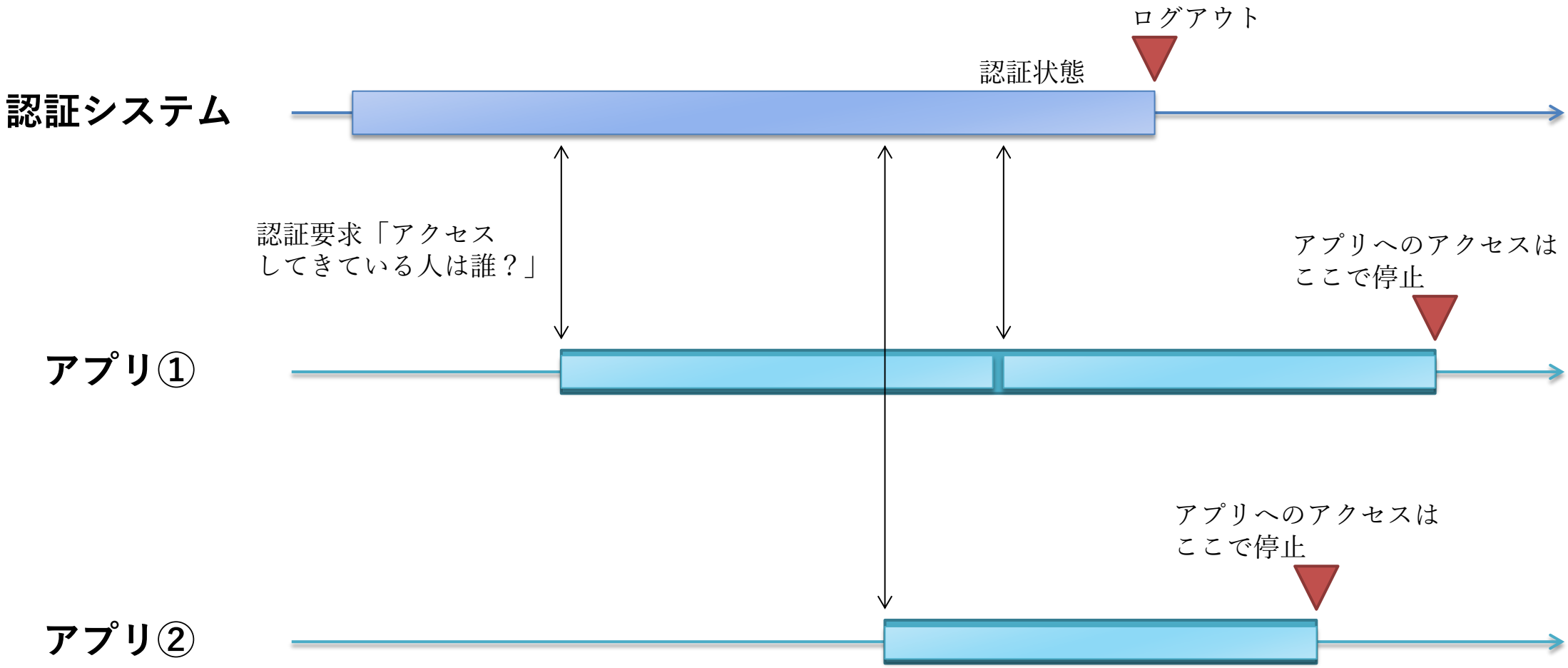
- **異動等に伴うシステムの利用停止をどう実現するか？**
  - セッション管理の考え方で対応
  - リスクが高いシステムは、即時プロビジョニングで対応

- **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

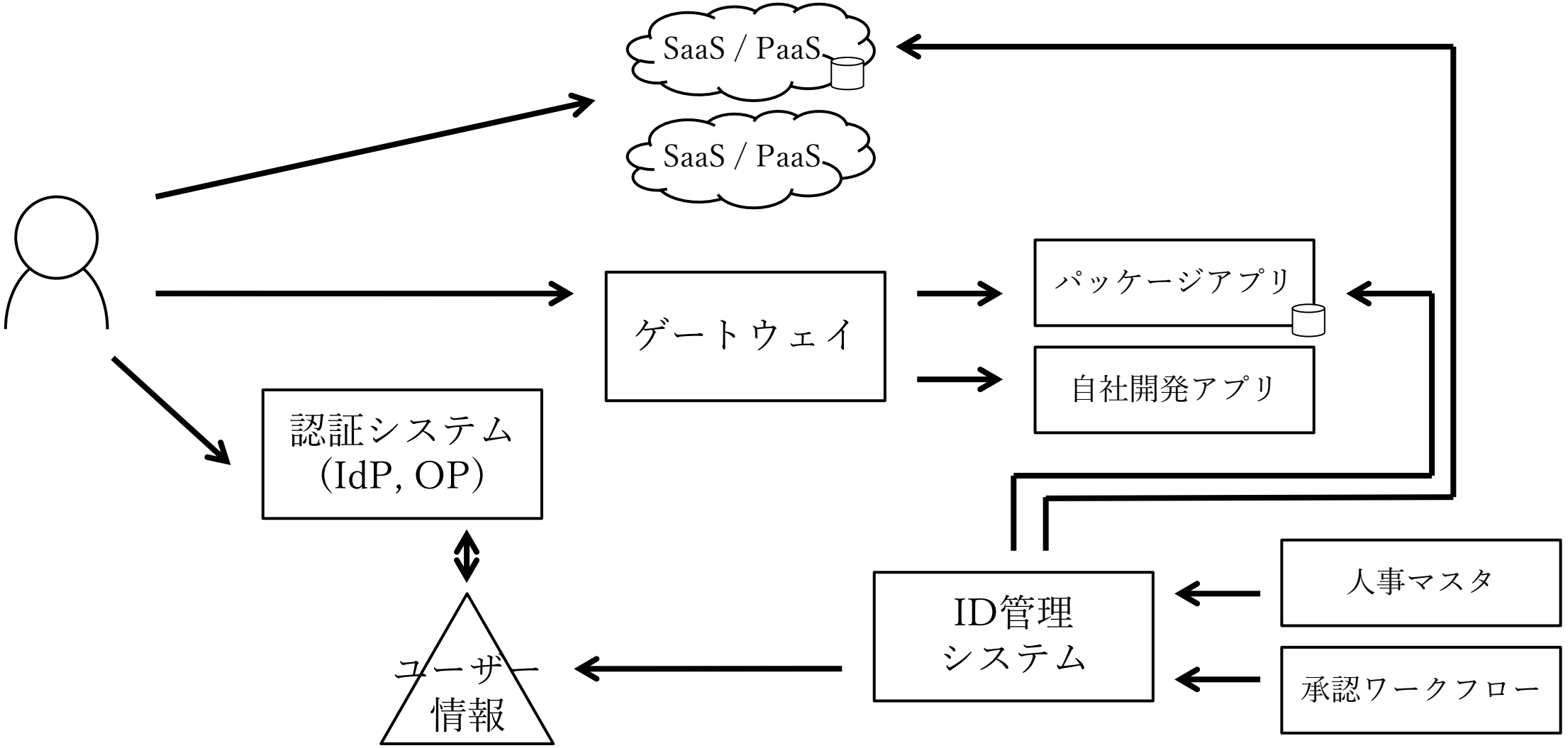
ID連携時の属性連携

- 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

認証基盤の基本形



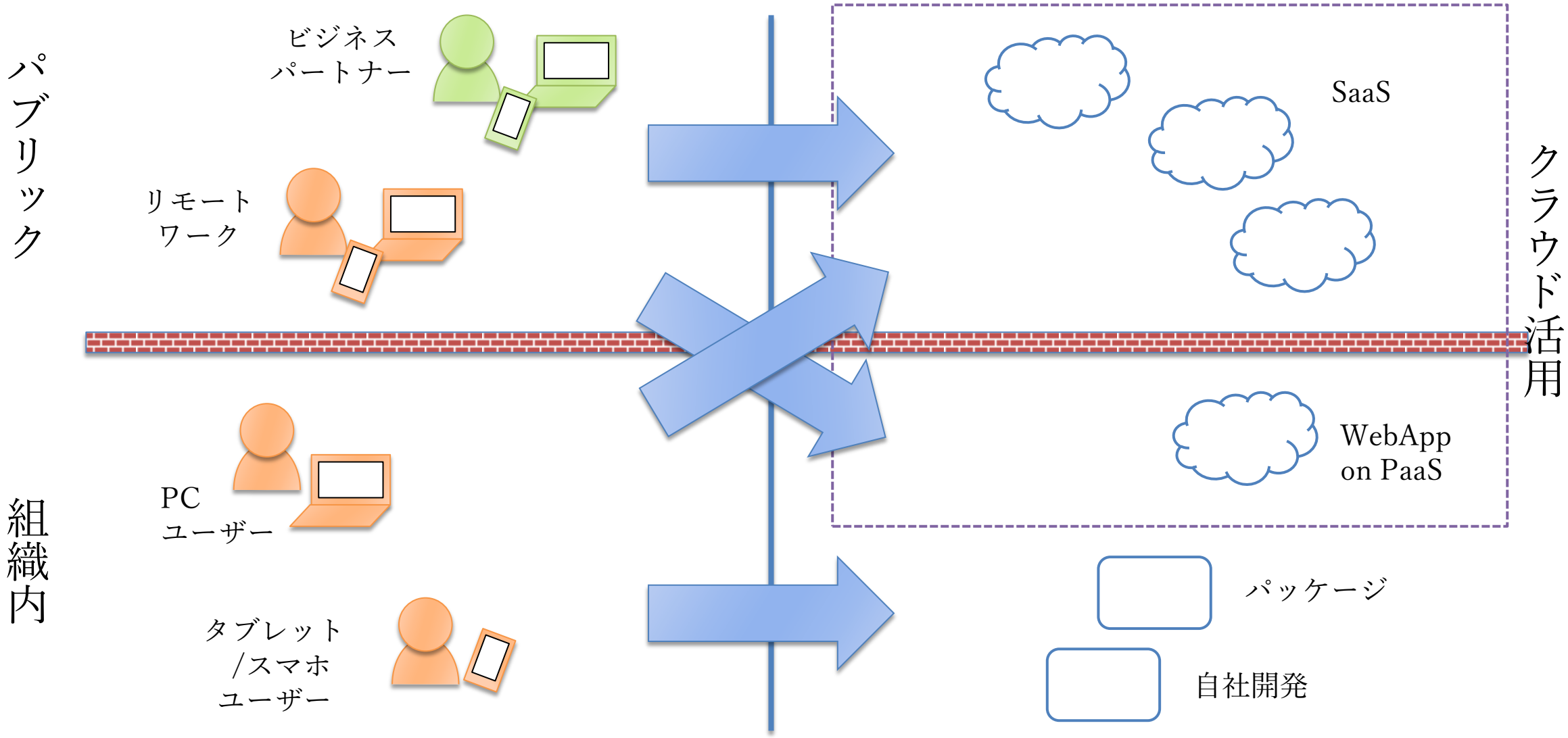
モバイル向けアプリの導入・提供の形態

	企業内業務向け	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	—	○

モバイル向けアプリの導入・提供の形態

	企業内業務向け	考慮点
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	○	利用停止が必要な際の処理方法。何をトリガーにアクセストークンを失効させるか。
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	○	OAuth認可サーバー機能への対応も必要になる。
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	—	—

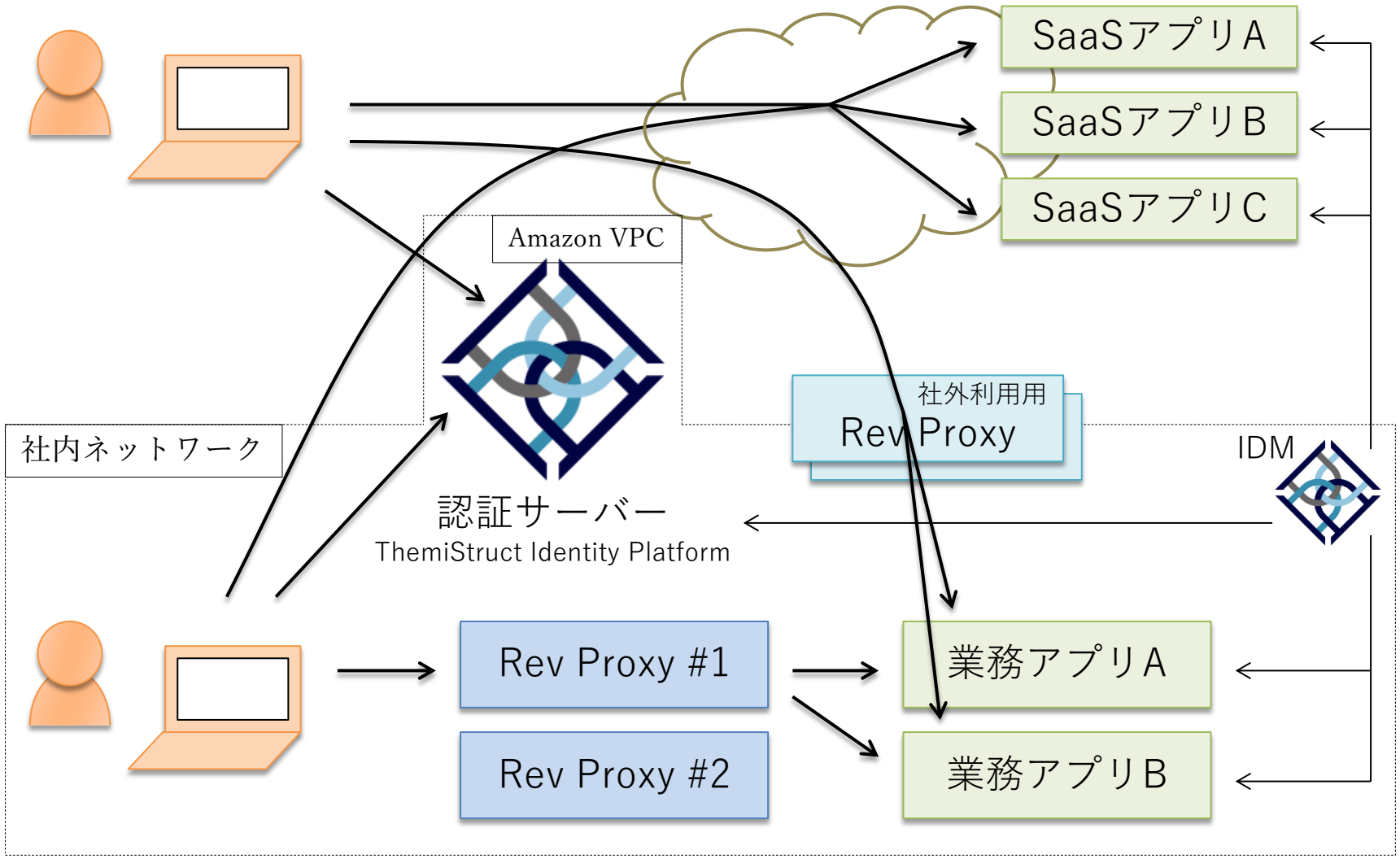
業務向けIT活用の世界観（さらに先へ）



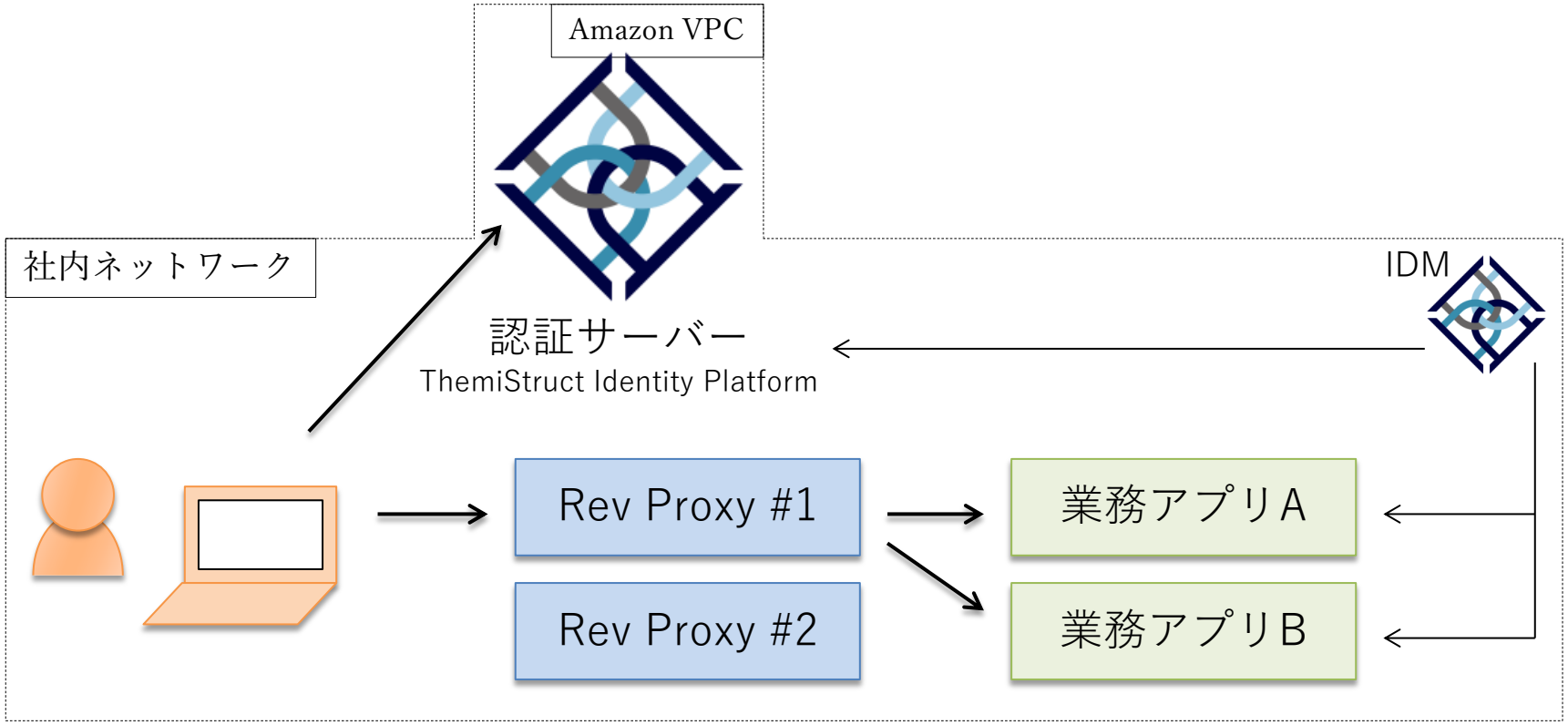
ThemiStruct Identity Platform で
企業/企業グループ内の業務向けの

「社内統合認証基盤」を構築する

「社内統合認証基盤」の構築イメージ

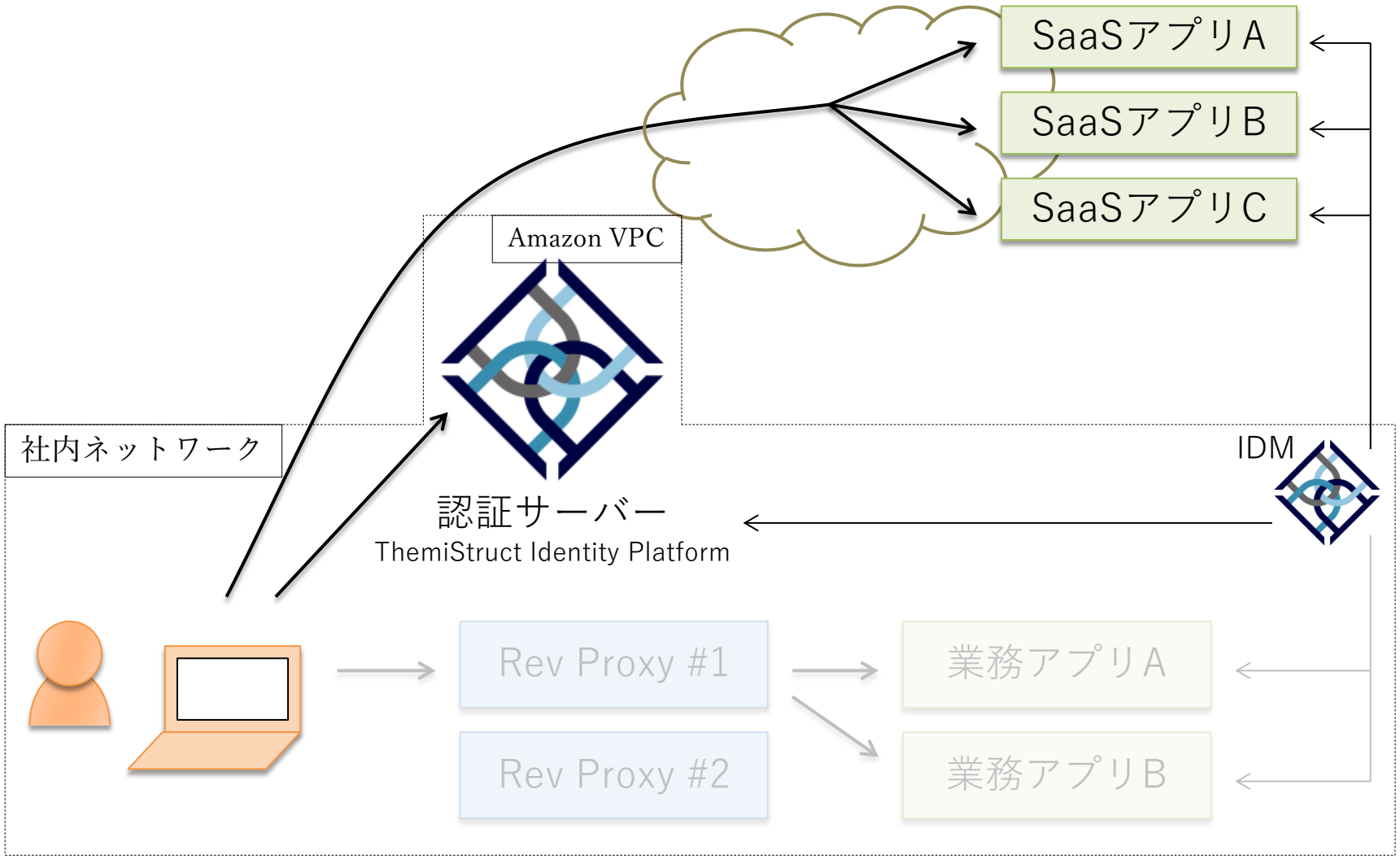


社内に配置されたシステムへのSSOを実現する



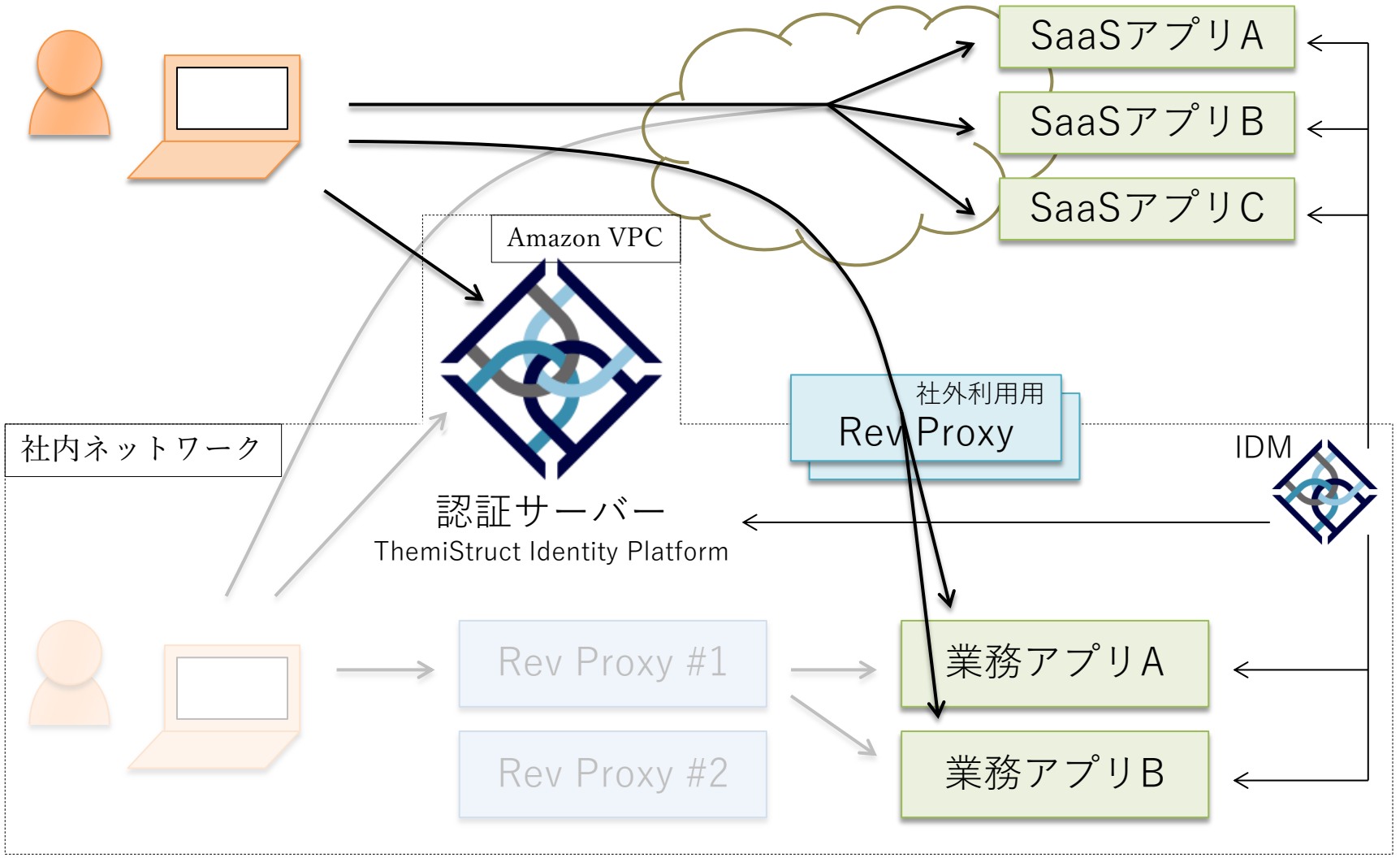
- ✓ Amazon VPC に認証サーバーを構築。標準インストールで高可用性を確保。
- ✓ 業務アプリにはリバプロ経由でアクセス。
- ✓ ユーザーが使えるアプリのアクセス制御が可能。
- ✓ 業務アプリに認証されたユーザーを連携する方式は、HTTPヘッダ連携、代理認証方式などで対応。
- ✓ リバプロの可用性確保は、レベルにより、①単一サーバー、②LBで冗長化、③冗長化+状態同期あり、から選択。

クラウドサービスへのアクセスを管理する



- ✓ クラウドサービスの認証、SSOには SAML, OpenID Connect といった標準技術を使用。
- ✓ ユーザーが使えるクラウドサービスのアクセス制御が可能。

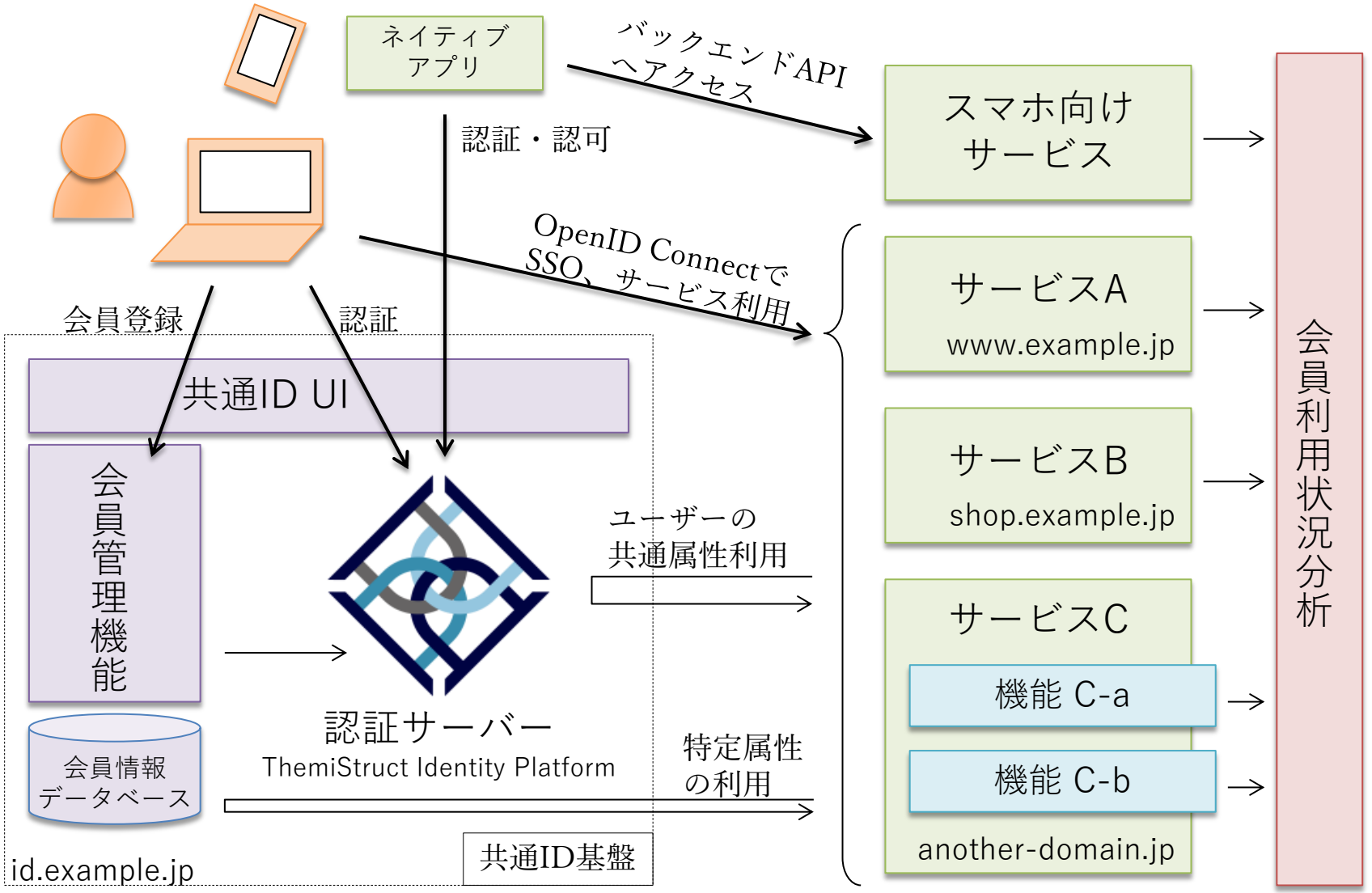
社外からのシステム利用を実現する



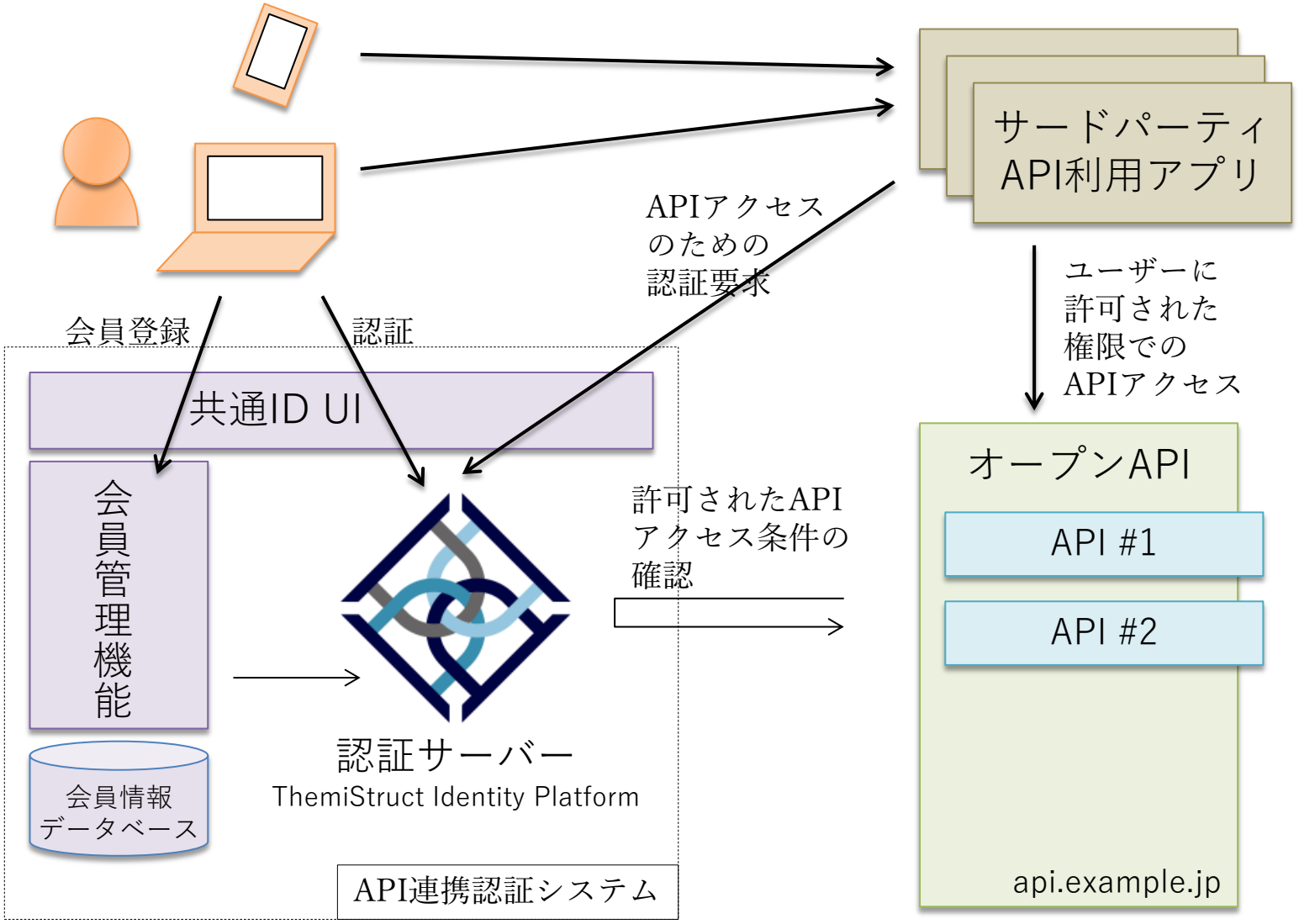
- ✓ 認証サーバーはインターネットからアクセスが可能。社外の端末で認証を利用可能。
- ✓ 社外端末からのアクセスの場合には、ワンタイムパスワードを要求するなど、認証方式の強化、使い分けが可能。
- ✓ 社内にある業務アプリも、リバプロをDMZに配置することで社外から利用可能とすることが可能。
- ✓ 特定ユーザーのみが社外から業務アプリを利用できるよう、属性ベースのアクセス制御が設定可能。

デジタルトランスフォーメーションに対応していくために

「共通ID基盤」の構築イメージ



「API連携認証システム」の構築イメージ



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

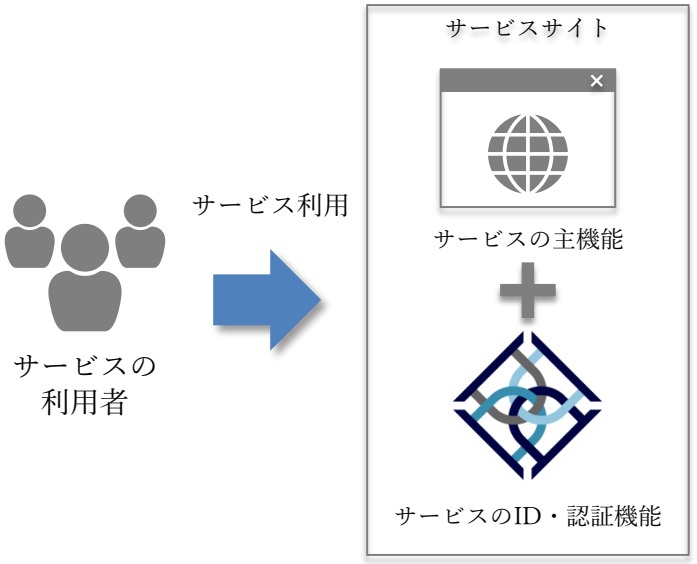
ThemiStruct（テミストラクト）
IdentityPlatform

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

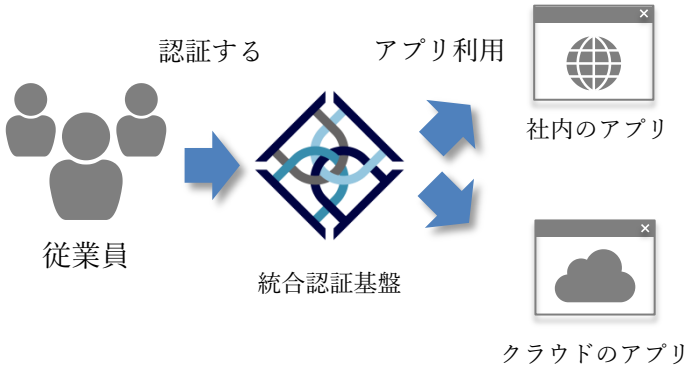
ThemiStruct Identity Platform は、ITシステム利用者のアイデンティティ管理と認証の機能を提供します。顧客向けにサービスを展開したり、従業員向けにアプリケーションを展開する際に必要となる、共通ID基盤の構築に活用いただけます。

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

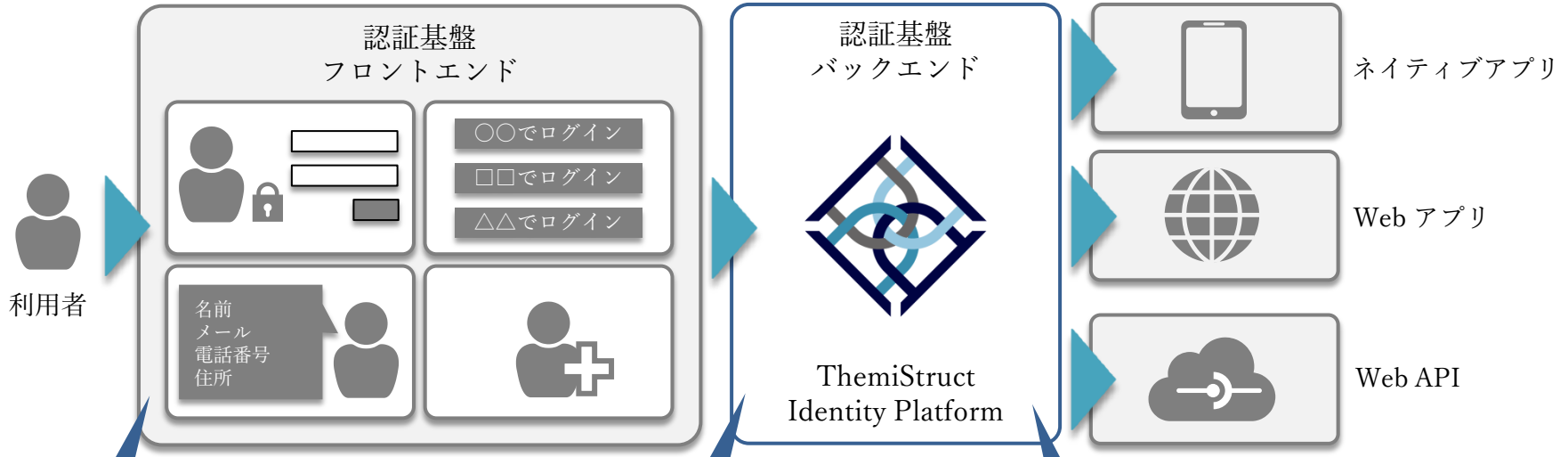
エンタープライズ領域に活用



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

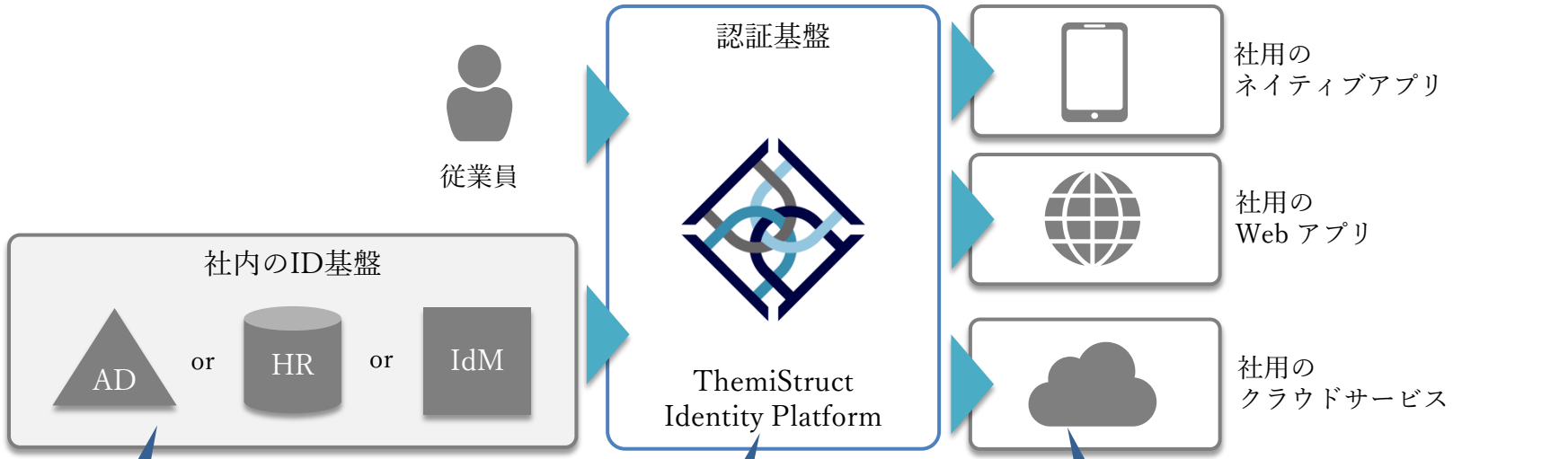
- OAuth 2.0 の技術仕様に基づいた認証・アクセス認可機能を提供します。OAuth 2.0 を使ったAPI連携認証システムが実現でき、モバイルアプリ、オープンAPIを安全に公開できます。

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

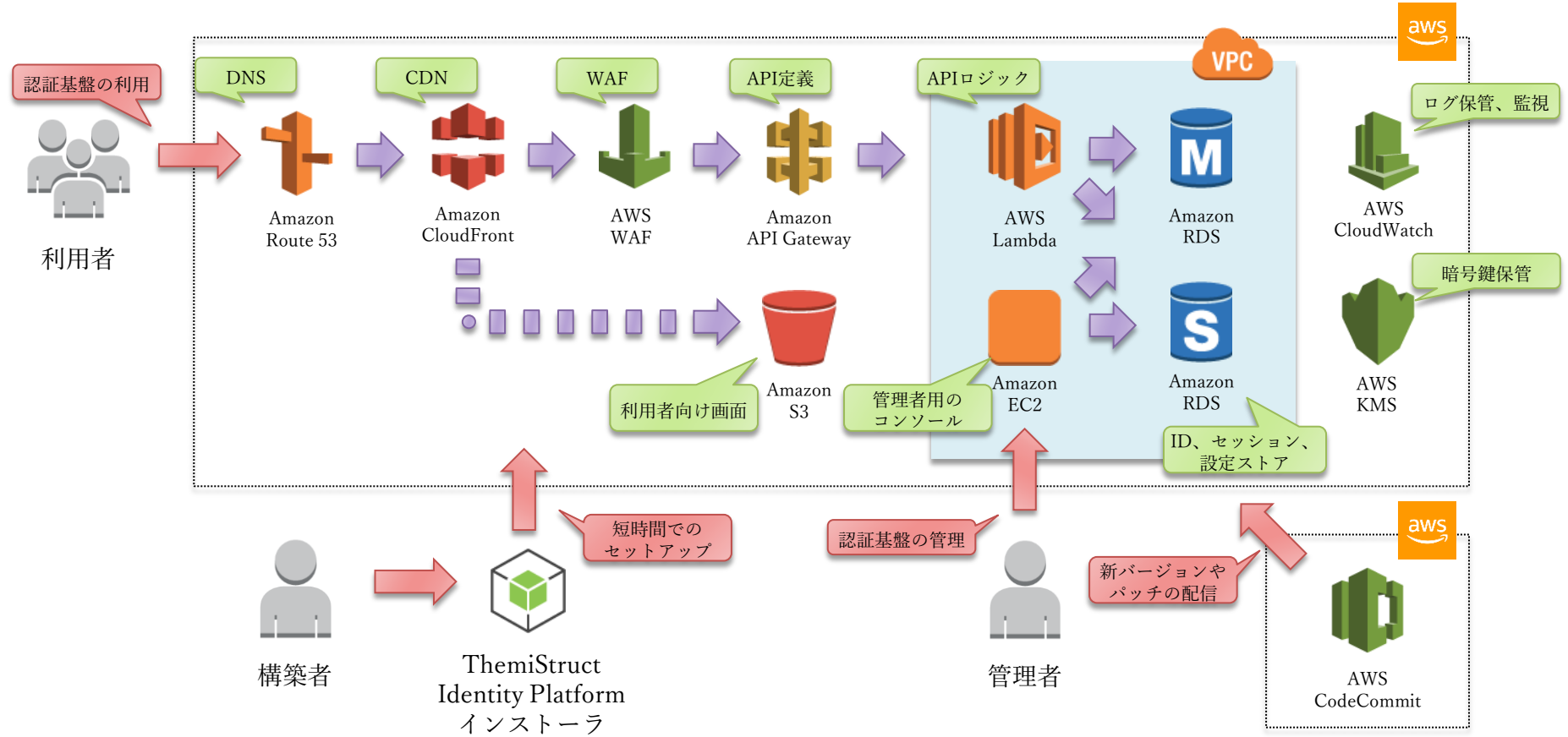
- ユーザーの属性や状態、利用するアプリケーションに応じて、柔軟な認証ポリシーをデザインすることができます。例えば、社内ネットワークからのアクセスの場合、IDとパスワードの認証を提供し、外出先からのアクセスの場合、追加でワンタイムパスワード認証を提供するといったポリシーを展開することができます。

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。

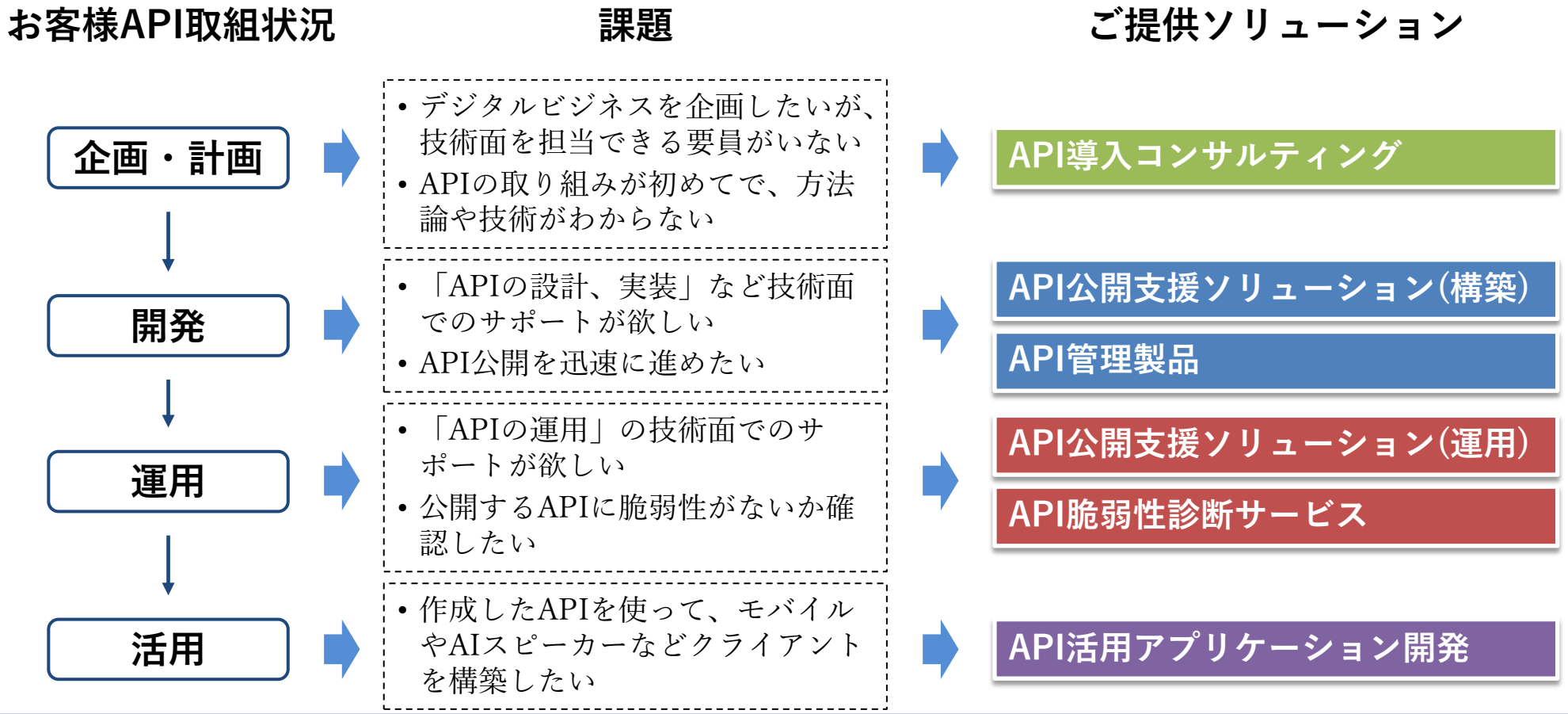
サーバーレスアーキテクチャを採用

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。
- IT活用に合わせて企業内の認証基盤も新しい方式、技術への対応が求められている。
- 企業のデジタルトランスフォーメーション実現のため、自社の顧客向けサービス、API提供のための認証基盤の検討・構築も必要である。
- 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

【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