統合認証基盤を
サーバーレスアーキテクチャで構築する
狙い、メリット、考慮点

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

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

統合認証基盤の重要性が高まる

ロ サービス時間帯の拡大

- 平日業務時間内の提供から24時間365日の提供へ
- メンテナンスに利用できる時間帯が大幅に縮小

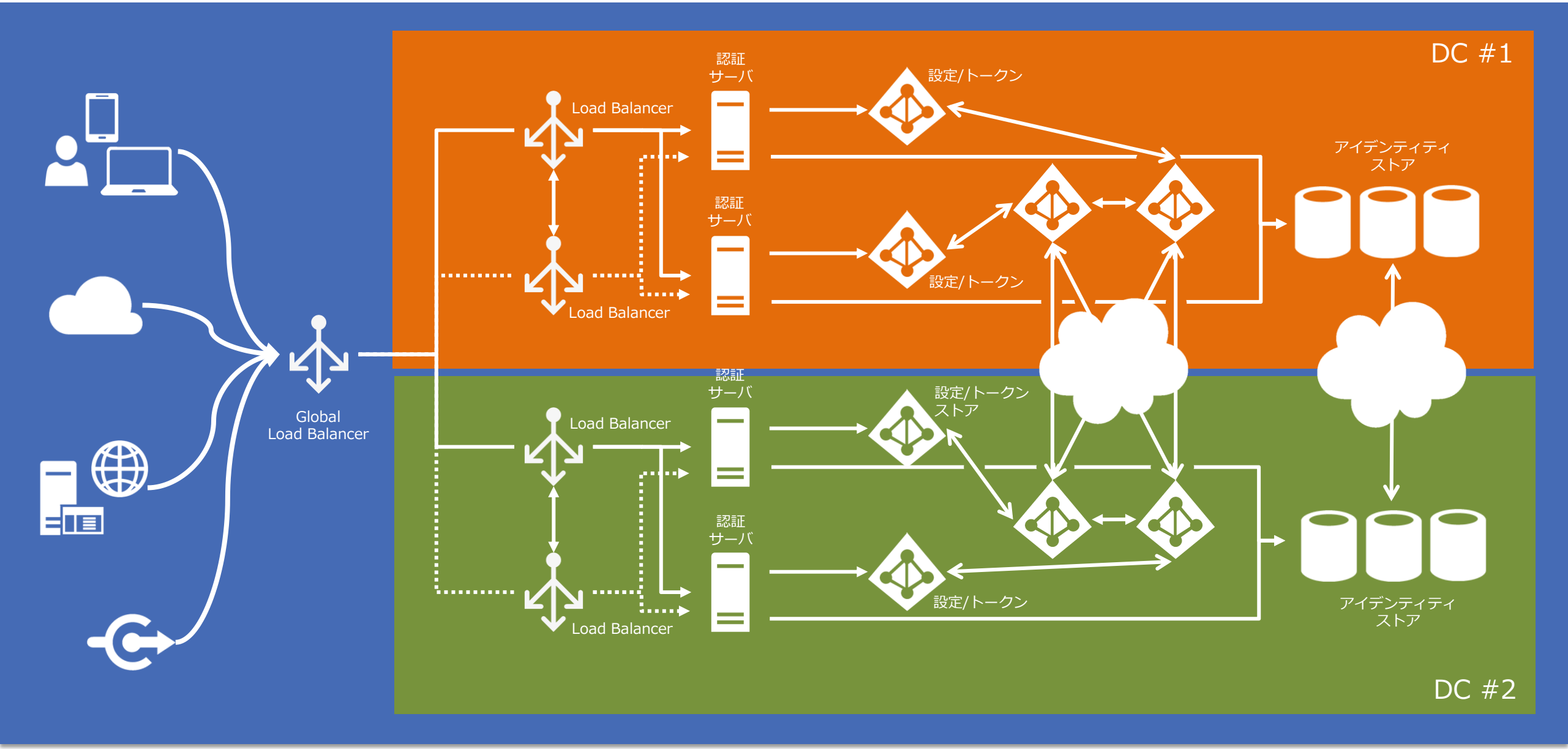
ロ 許容停止時間の短縮

- 業務影響を抑えるため障害状態から短時間での回復が必要

ロ アクセス集中時の性能確保

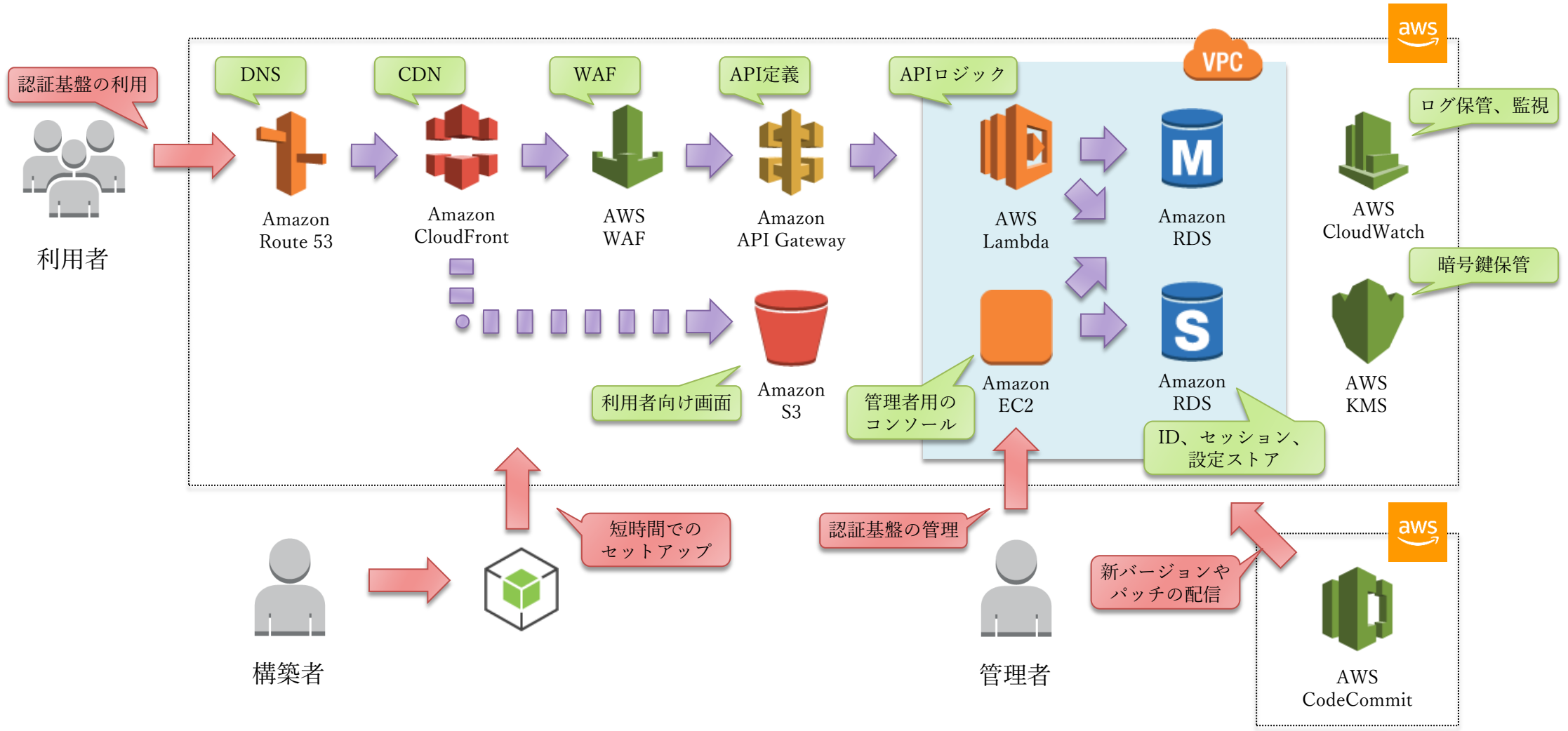
- 出勤時、特定業務の締切日・締切時間、など
- 特定イベント（キャンペーンなど）による一斉アクセス、など

高度な基盤設計が必要に ➡ 入念な可用性、性能のテスト。プロジェクトの巨大化。



サーバーレスアーキテクチャで
アプローチすることで
解決できないか？

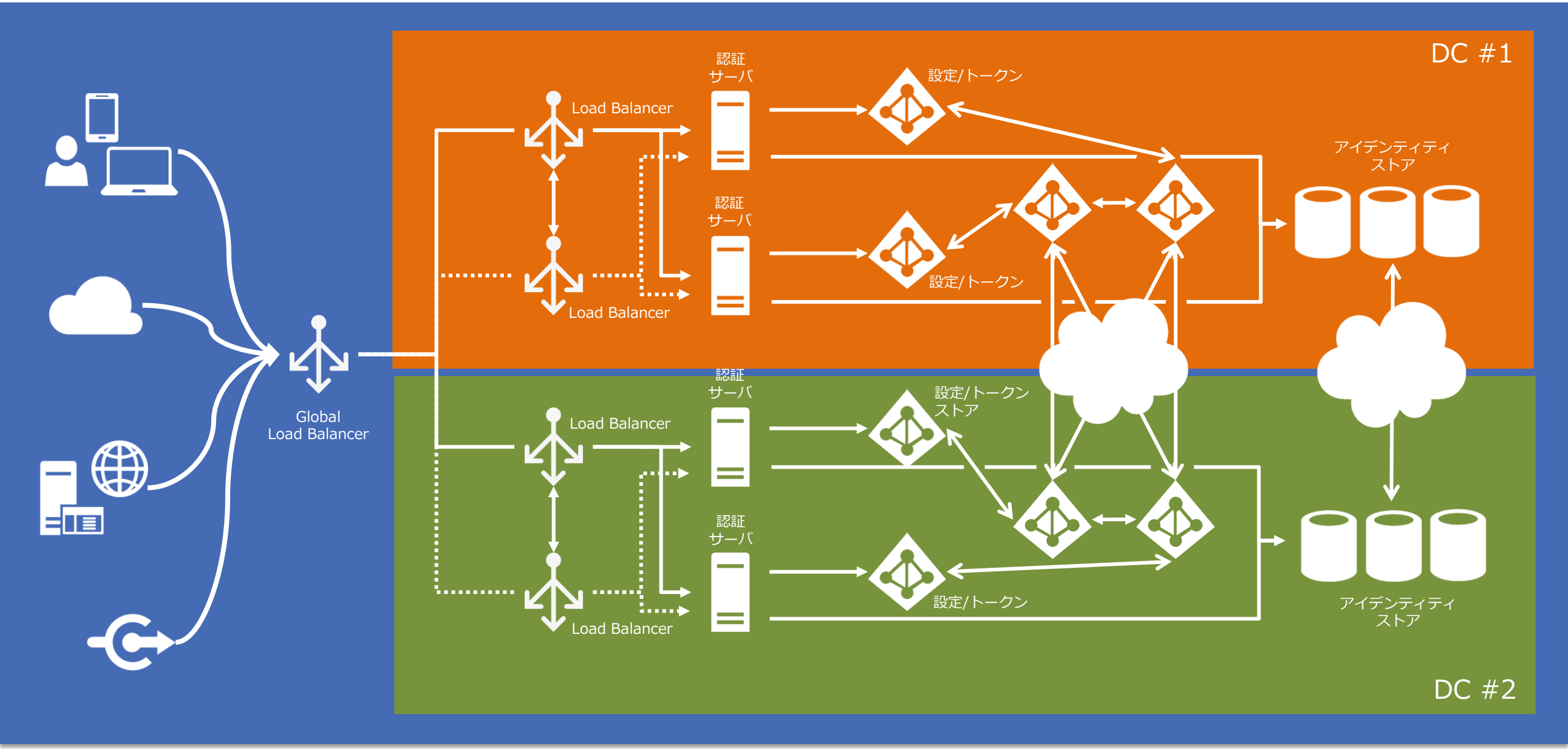
ThemiStruct Identity Platform を開発



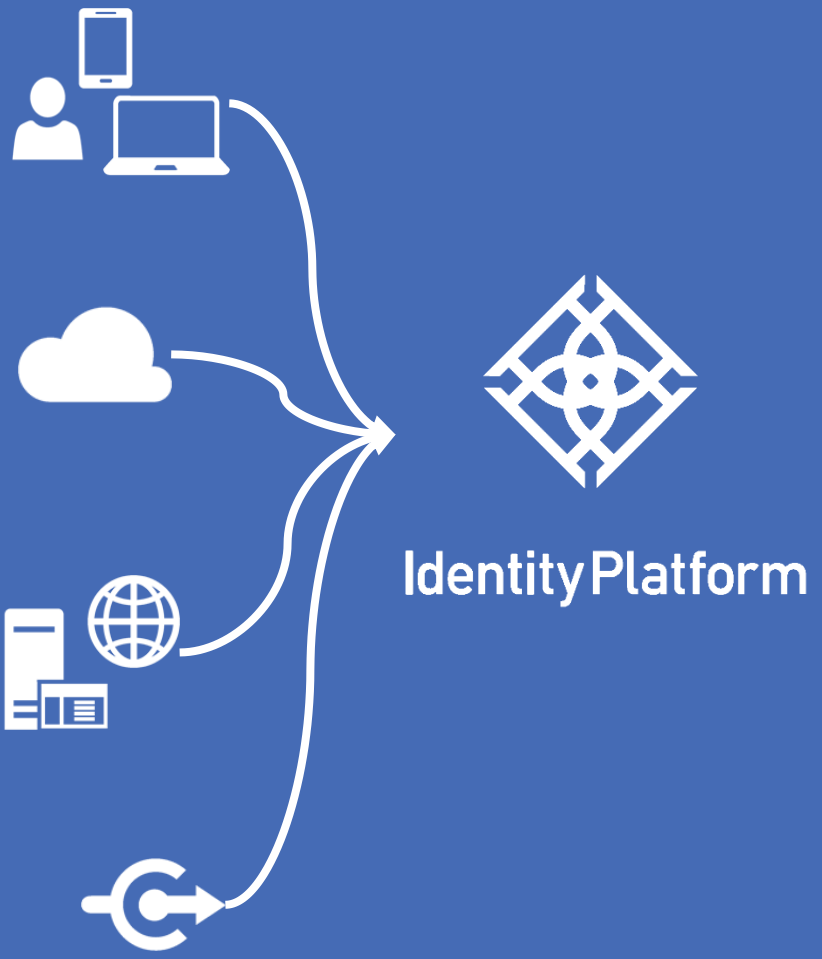
ThemiStruct Identity Platform の特長

- Amazon API Gateway, AWS Lambda など、AWSのマネージドサービスのコンポーネントを活用。
- AWSマネージドサービスで提供される可用性、スケーラビリティのメリットを享受。
- ユーザー情報などのデータは、自社VPC内で保持。
- AWSの各サービスコンポーネントの設定、コードの配置を自動化する専用のインストーラーを提供。

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。



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。



統合認証基盤を自社に構築するかIDaaSを利用するか

#	要件・ニーズ	自社内に構築 (オンプレ、IaaS)	IDaaS利用
1	短期間での導入・設定完了	× 設計・テストが必要	◎ サインアップだけで利用可能
2	サーバー管理（パッチ適用、バックアップ等）の負担軽減	× 個々のサーバーの管理が必要	◎ IDaaS側で管理される
3	外部からアクセス可能な環境の実現	△ 専用設備の設計導入が必要	◎ 外部からアクセスして利用する前提
4	自社ネットワーク内でのサービス提供	○ 自社ネットワークで動かすことが前提	× IDaaSのネットワークでの提供となる
5	ユーザー情報等データの自社ネットワーク内への留保	○ データは自社のサーバー上に格納	？ IDaaS側でテナント毎に管理される
6	自社運用スケジュールにあわせたメンテナンス等の運用	○ 運用スケジュールを自社で決められる	× IDaaS側で運用スケジュールが決まる
7	カスタマイズ対応のしやすさ	○ 製品機能、周辺開発で対応可能	△ IDaaS提供の仕組みの範囲内で対応可能

ThemiStruct Identity Platform は第３の選択になる

#	要件・ニーズ	自社内に構築 (オンプレ、IaaS)	ThemiStruct Identity Platform	IDaaS利用
1	短期間での導入・設定完了	×	○ 約2時間で導入可 リバースプロキシ構成の場合はサーバー構築が必要。	◎
2	サーバー管理（パッチ適用、バックアップ等）の負担軽減	×	○ サーバー管理不要 Identity Platform ソフトウェアのアップデート作業は必要。 リバースプロキシサーバーがある場合はその管理は必要。	◎
3	外部からアクセス可能な環境の実現	△	○ 外部からアクセスして利用する前提の設計	◎
4	自社ネットワーク内でのサービス提供	○	○ 自社のVPC内で動作させる	×
5	ユーザー情報等データの自社ネットワーク内への留保	○	○ データはVPC内のDBに格納	？
6	自社運用スケジュールにあわせたメンテナンス等の運用	○	○ 運用スケジュールを自社で決められる	×
7	カスタマイズ対応のしやすさ	○	○ カスタムモジュールの開発が可能	△

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

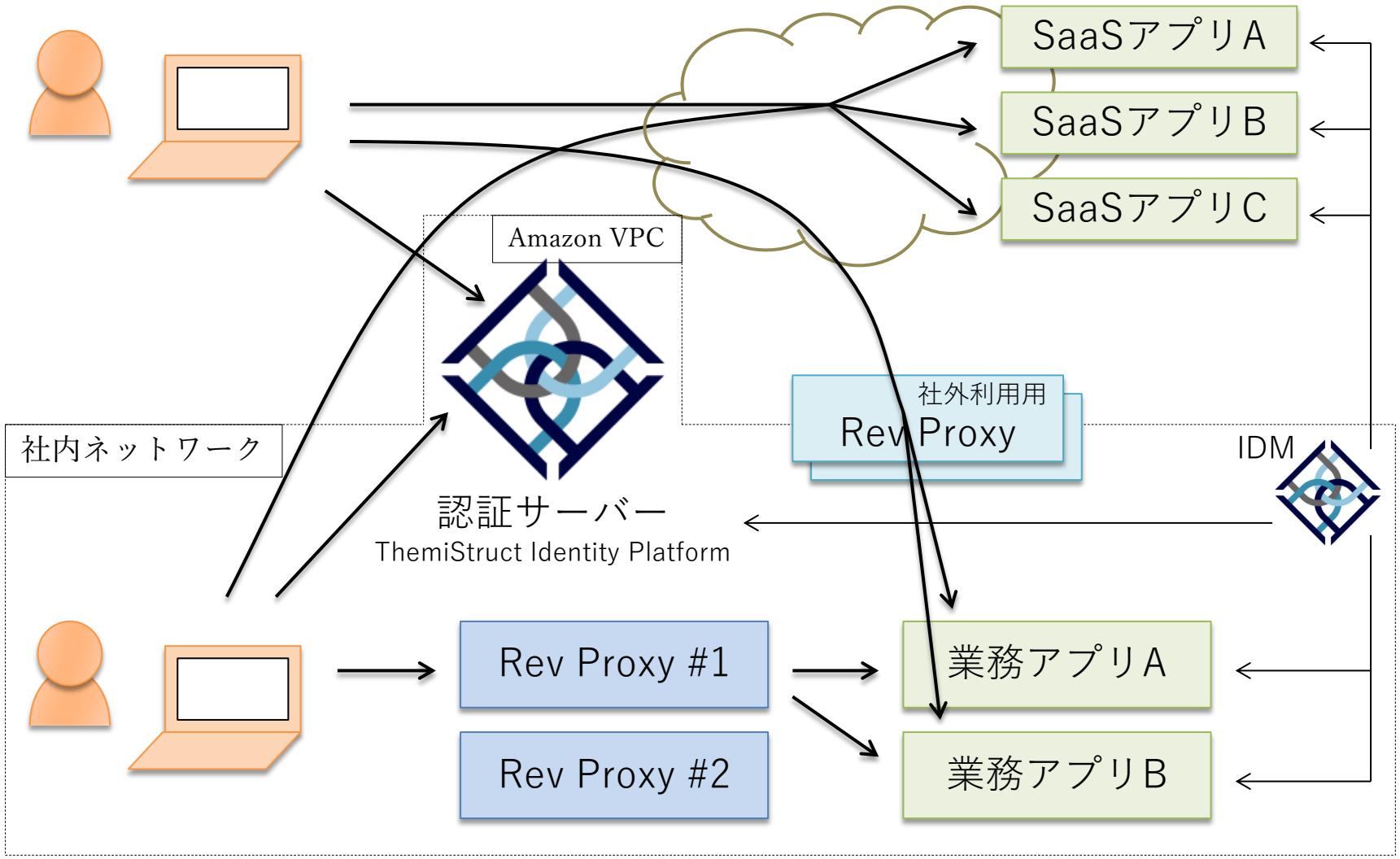
顧客向けサービスサイトの「**共通ID基盤**」を構築する

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

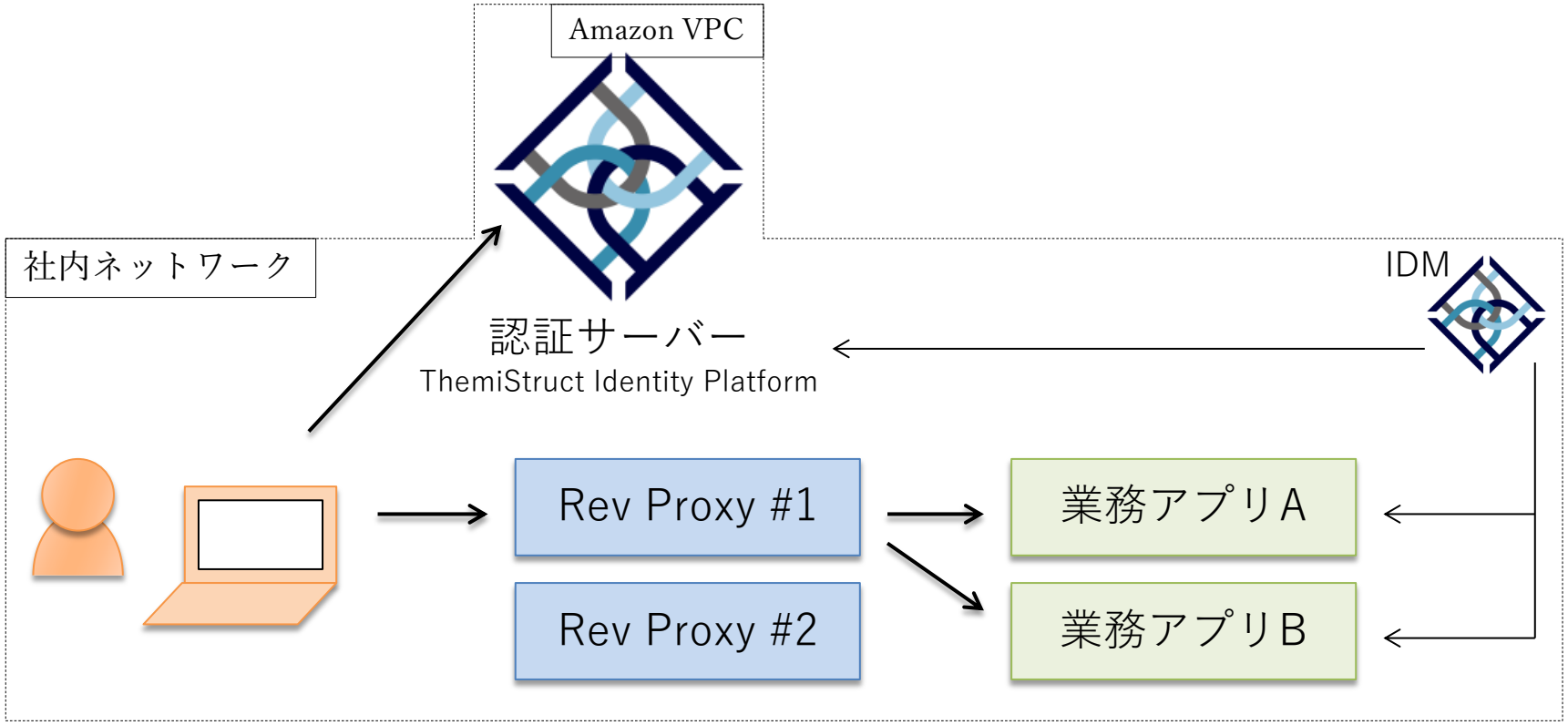
ThemiStruct Identity Platform で
企業/企業グループ内の業務向けの

「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

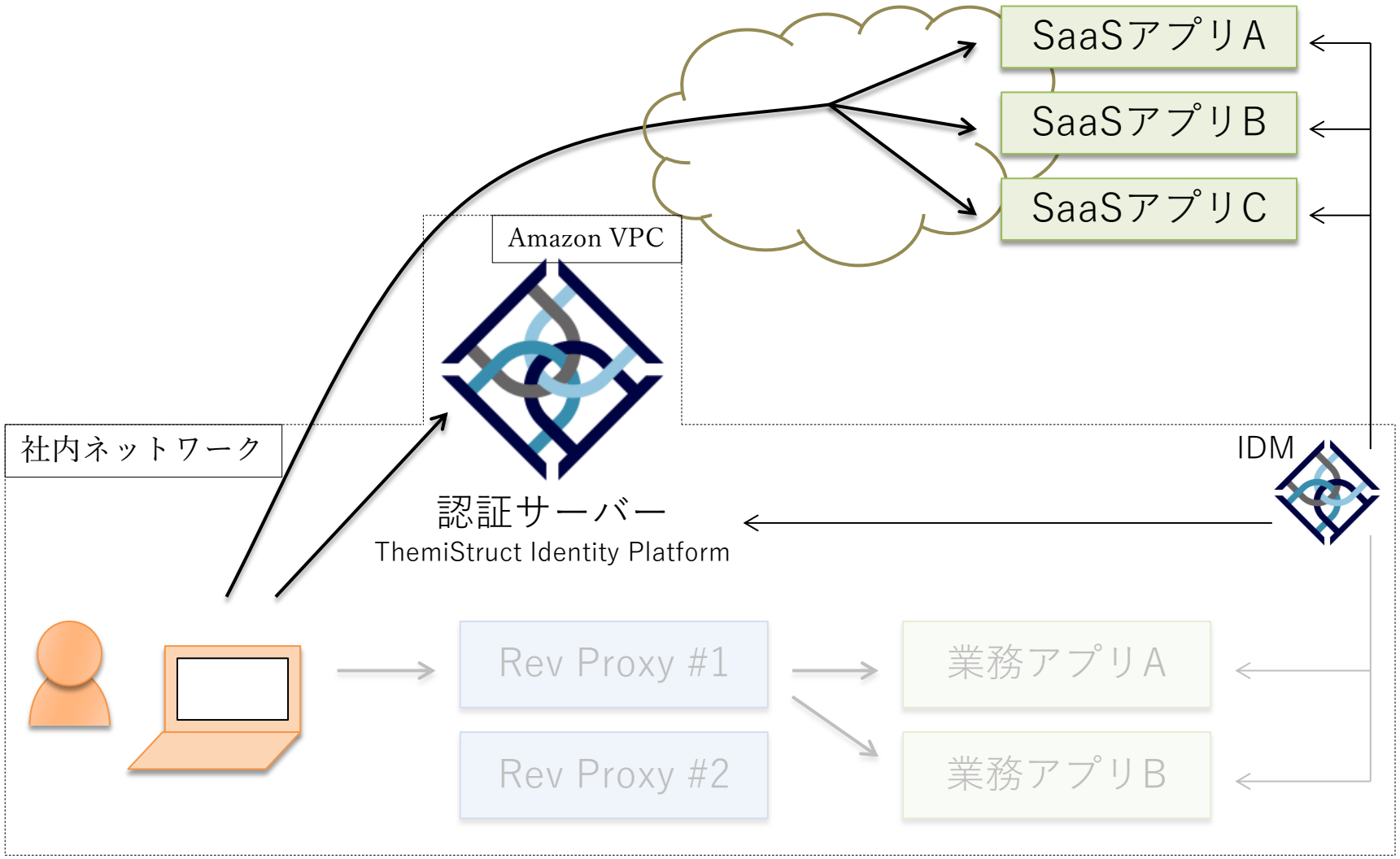


社内に配置されたシステムへのSSOを実現する



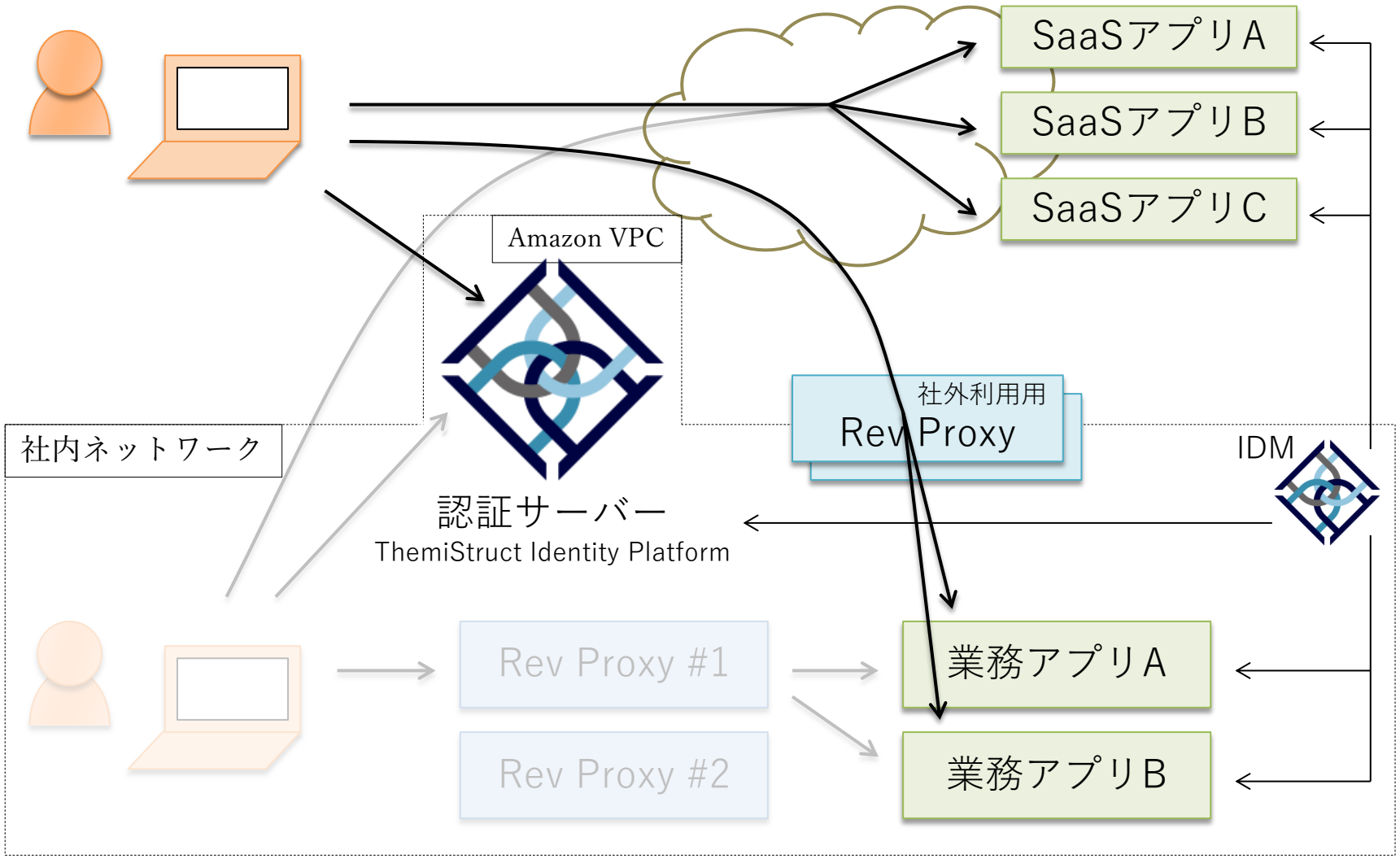
- ✓ Amazon VPC に認証サーバーを構築。標準インストールで高可用性を確保。
- ✓ 業務アプリにはリバプロ経由でアクセス。
- ✓ ユーザーが使えるアプリのアクセス制御が可能。
- ✓ 業務アプリに認証されたユーザーを連携する方式は、HTTPヘッダ連携、代理認証方式などで対応。
- ✓ リバプロの可用性確保は、レベルにより、①単一サーバー、②LBで冗長化、③冗長化+状態同期あり、から選択。

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

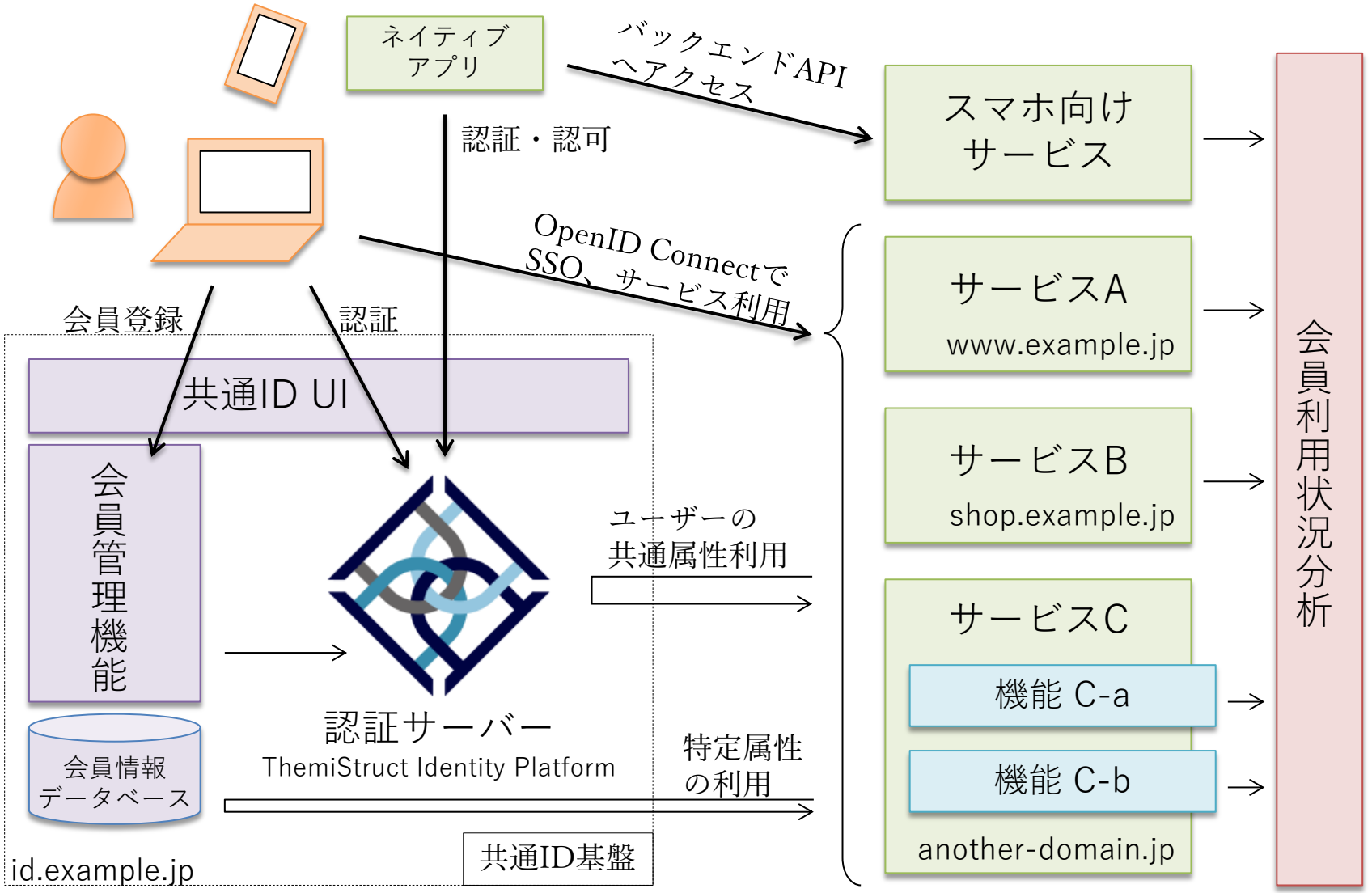


- ✓ 認証サーバーはインターネットからアクセスが可能。社外の端末で認証を利用可能。
- ✓ 社外端末からのアクセスの場合には、ワンタイムパスワードを要求するなど、認証方式の強化、使い分けが可能。
- ✓ 社内にある業務アプリも、リバプロをDMZに配置することで社外から利用可能とすることが可能。
- ✓ 特定ユーザーのみが社外から業務アプリを利用できるよう、属性ベースのアクセス制御が設定可能。

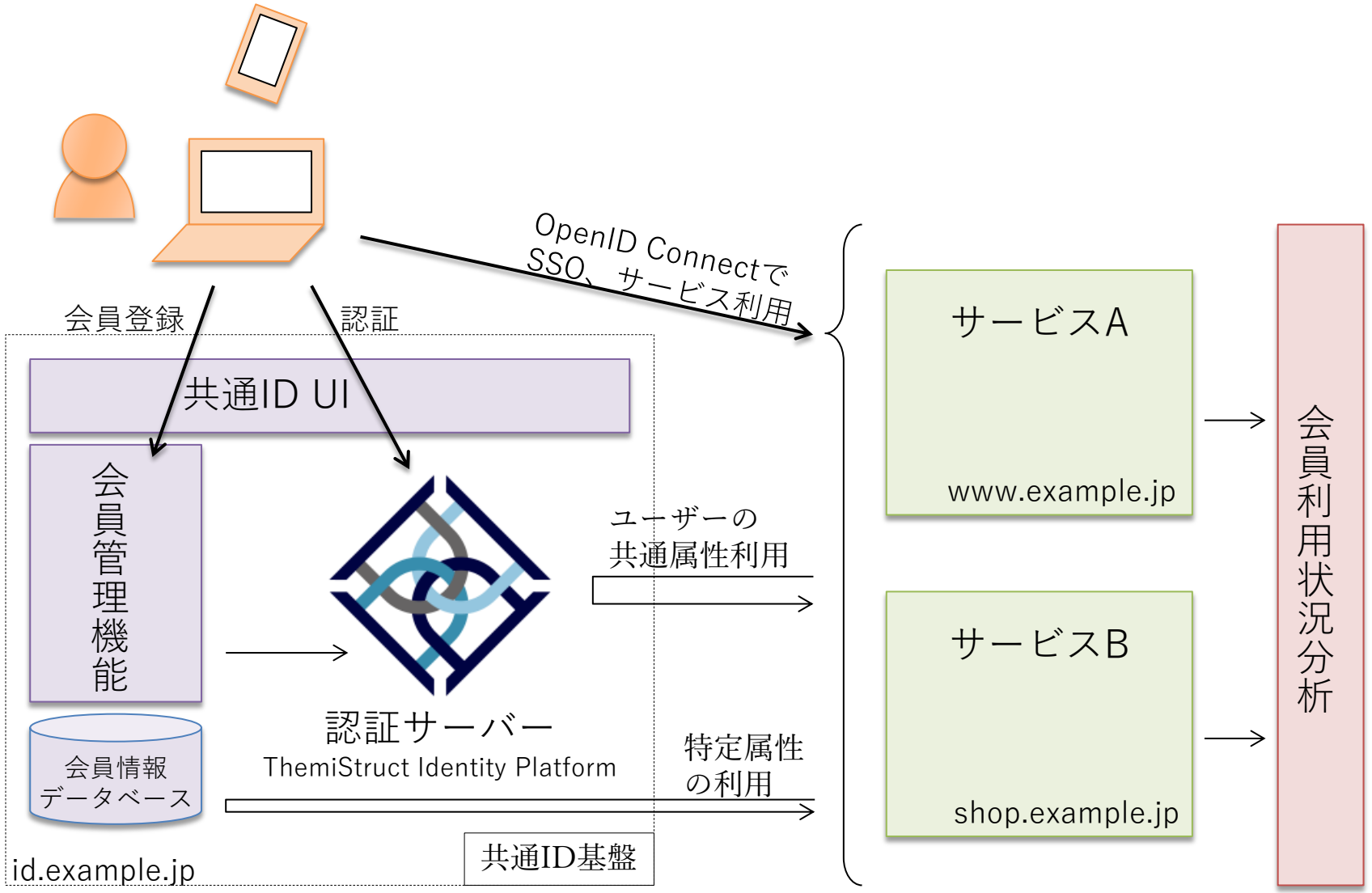
ThemiStruct Identity Platform で
顧客向けサービスサイトの

「共通ID基盤」を構築する

「共通ID基盤」の構築イメージ

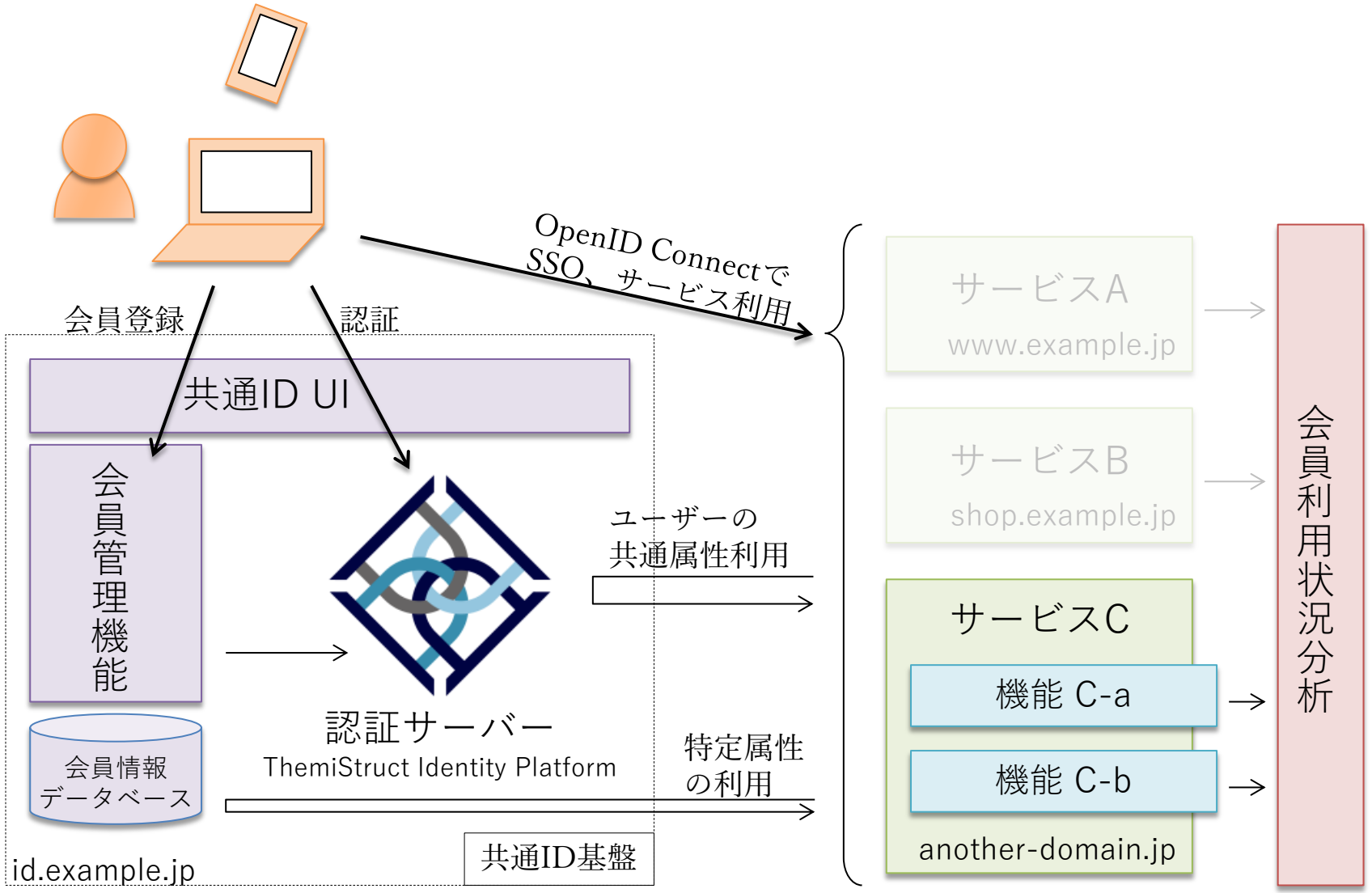


顧客向けサービスのIDを共通化する



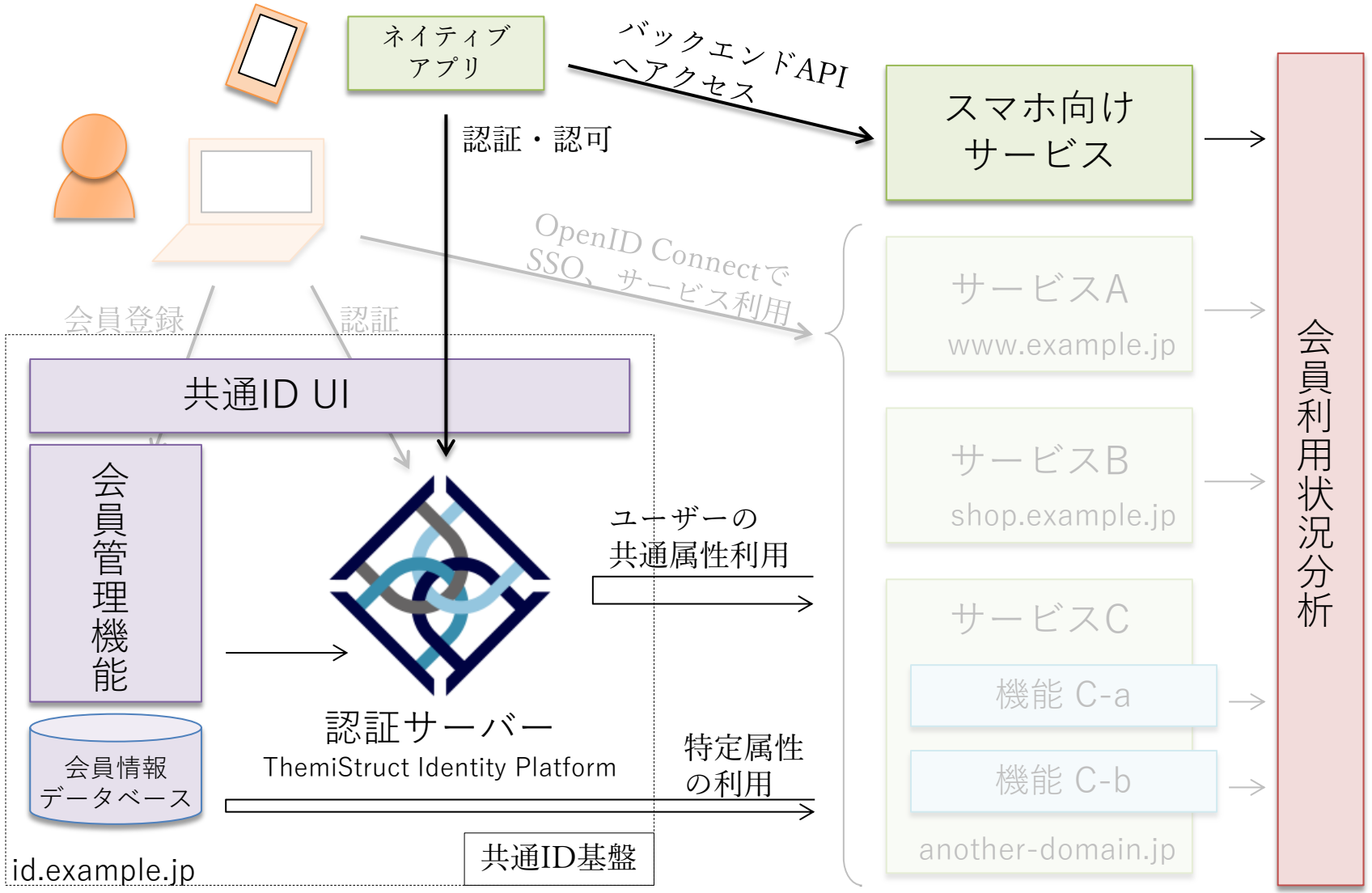
- ✓ 既存サイトに、ThemiStruct Identity Platform の認証機能を組み込む。
- ✓ 会員管理機能で登録・更新される情報をThemiStruct Identity Platformに連携。
- ✓ ユーザーは一回の会員登録、サインインで、全サービスを横断的に利用可能に。
- ✓ 各サービスが共通的に利用する属性は、認証サーバーからサービス利用時に連携することで、会員管理機能への負担を軽減。
- ✓ 全サービスを横断して会員の利用分析が可能に。

提供サービスを追加する、更新する



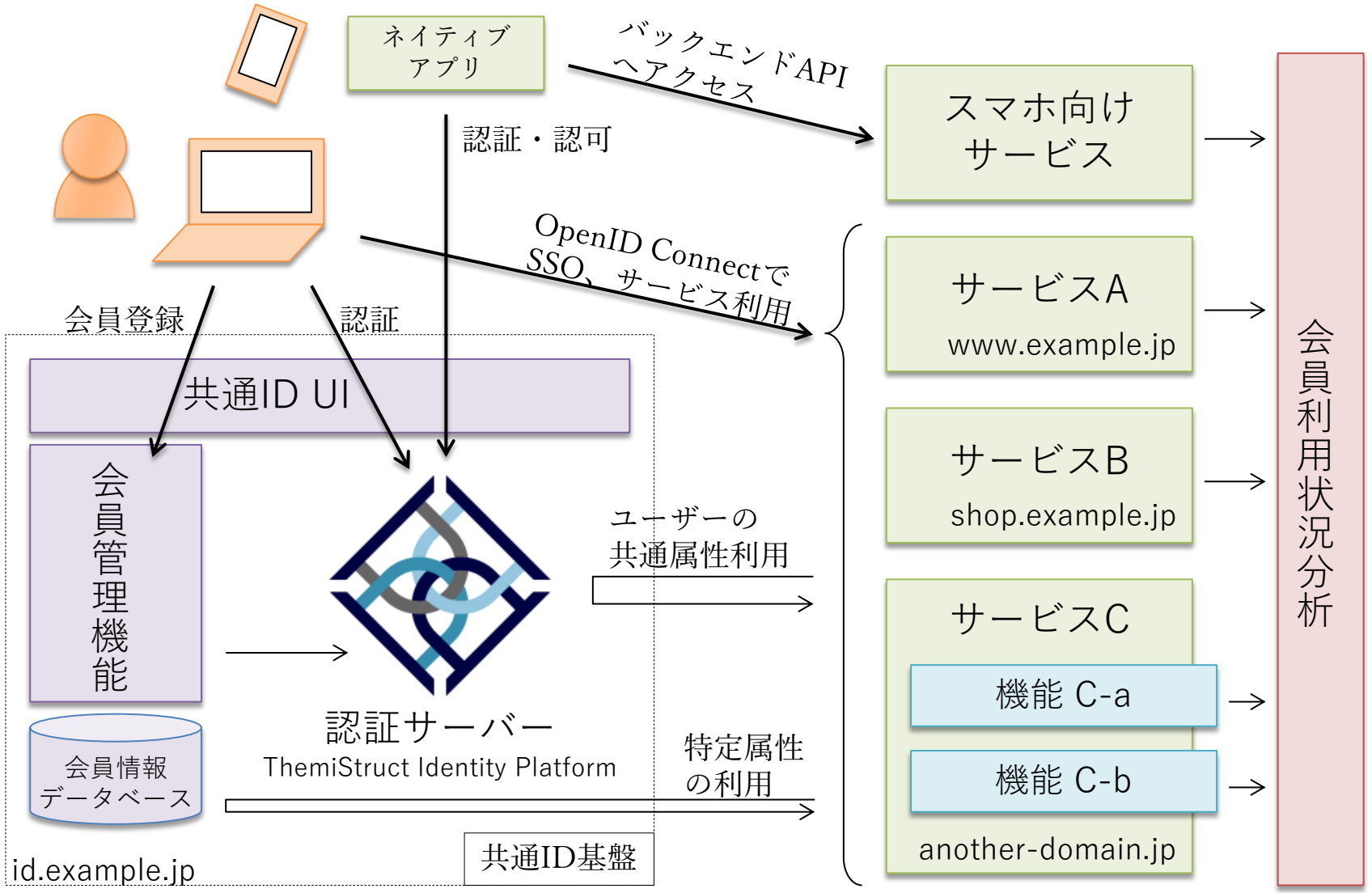
- ✓ 提供するサービスを追加する場合は、共通IDを利用するアプリとして開発するだけでSSO利用が可能に。
- ✓ サービス内の機能を増やすときも、サブシステム毎に開発してSSO接続することで、ユーザーは一つのサービスとして利用可能。
- ✓ サービス、機能の入れ替えが行ないやすい構造に。

スマホ向けサービスを提供する



- ✓ スマホ向けネイティブアプリの提供では、バックエンドAPIアクセスのための認証・認可の処理が必要に。
- ✓ ThemiStruct Identity PlatformのOAuth認可サーバーの機能でネイティブアプリの利用にも対応。

スケーラブル、ハイアベイラブルな共通ID基盤に

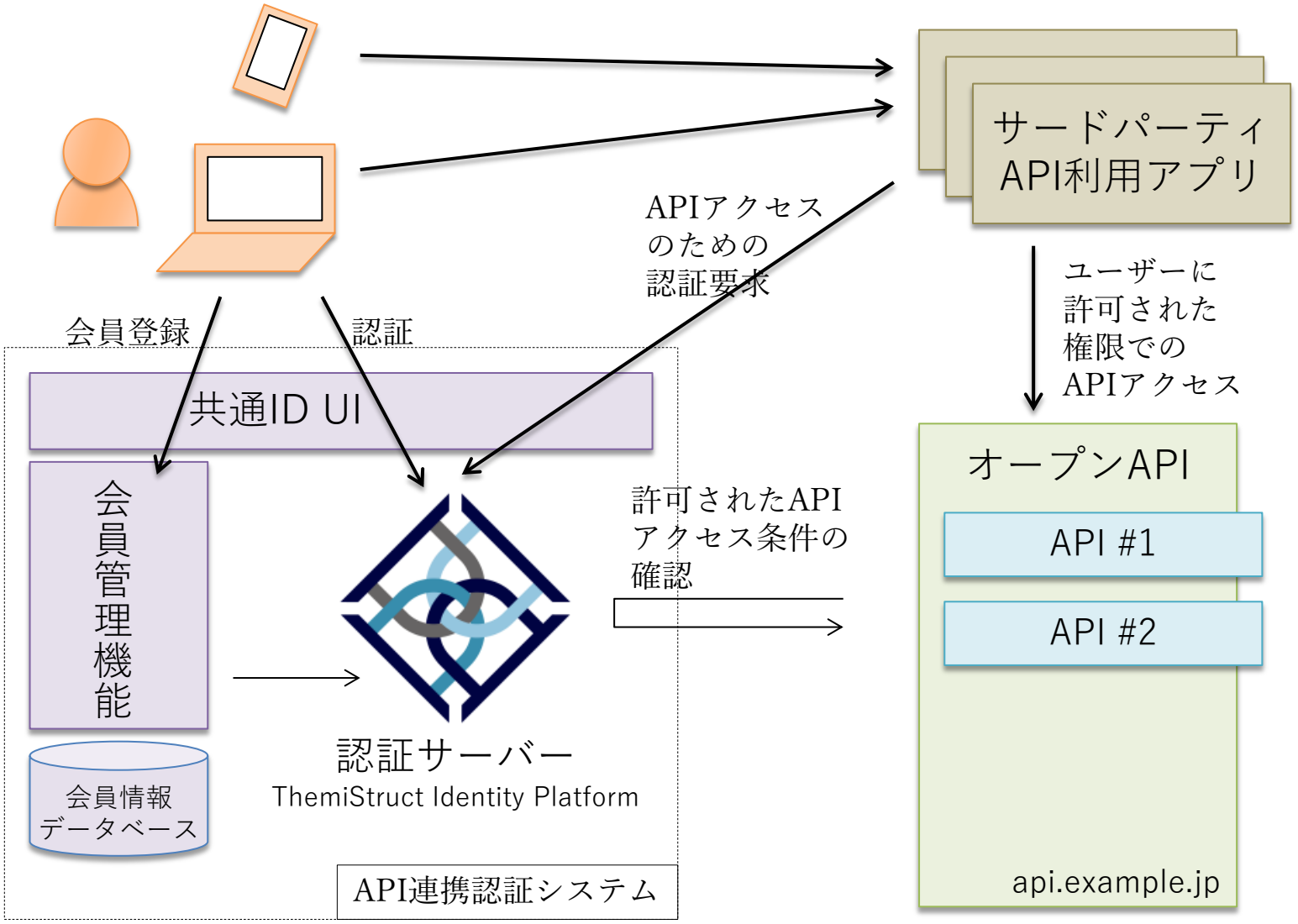


- ✓ AWSマネージドサービスにより、アクセスの繁閑にも柔軟に対応が可能。
- ✓ 無停止アップデート機能により、利用者にサービス提供を続けながらThemiStruct Identity Platformのソフトウェアを更新可能。

ThemiStruct Identity Platform で
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

「API連携認証システム」の構築イメージ



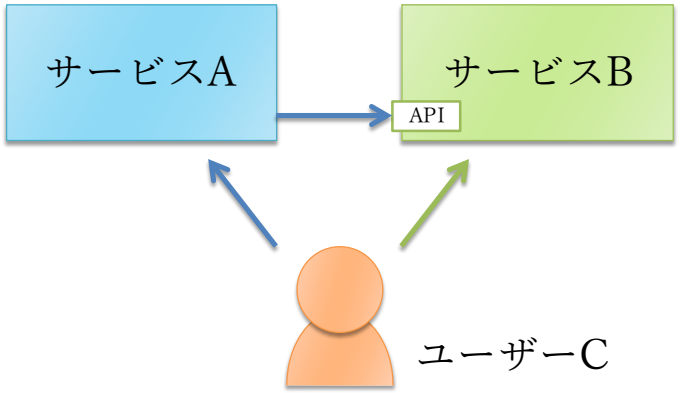
3者間でのAPI利用時の認証方式

ロ ユーザーC は サービスA に、アクセスできるデーターや操作を限定して、サービスB の API へアクセスさせたい。

- ユーザーIDとパスワードなど、クレデンシャル情報を渡す方式では、全権限をサービスAに与えてしまう。

ロ 現時点では OAuth 2.0 の利用が唯一の選択肢

- ユーザーC の同意に基づき、ユーザーC が意図した範囲の限定された権限で API へのアクセスを許可する方式。
- OAuth 2.0 Authorization Code Grant
- OAuth 2.0 Implicit Grant



対応が必要となる OAuth の仕様類

#	仕様	AS 実装者	API 開発者	API利用者 アプリ開発者
①	The OAuth 2.0 Authorization Framework [RFC 6749]	○	—	○
.1	Authorization Code Grant	○	—	○
.2	Implicit Grant	○	—	○
.3	Client Credentials Grant	○	—	○
②	The OAuth 2.0 Authorization Framework: Bearer Token Usage [RFC 6750]	—	○	○
③	OAuth 2.0 Token Revocation [RFC 7009]	○	○	○
④	Proof Key for Code Exchange by OAuth Public Clients [RFC 7636]	○	—	○
⑤	OAuth 2.0 Token Introspection [RFC 7662]	○	○	—
⑥	OAuth 2.0 for Native Apps [RFC 8252]	—	—	○

金融API向けにOAuth実装仕様の策定が進行中

- **OpenID Foundation (Global) の Financial API WG が策定**
  - https://openid.net/wg/fapi/

- **OAuthの実装仕様について、以下の2つがすでに Implementer's Draft となり、公開されている。**
  - Part 1: Read Only API Security Profile (Implementer's Draft).
  - Part 2: Read & Write API Security Profile (Implementer's Draft).

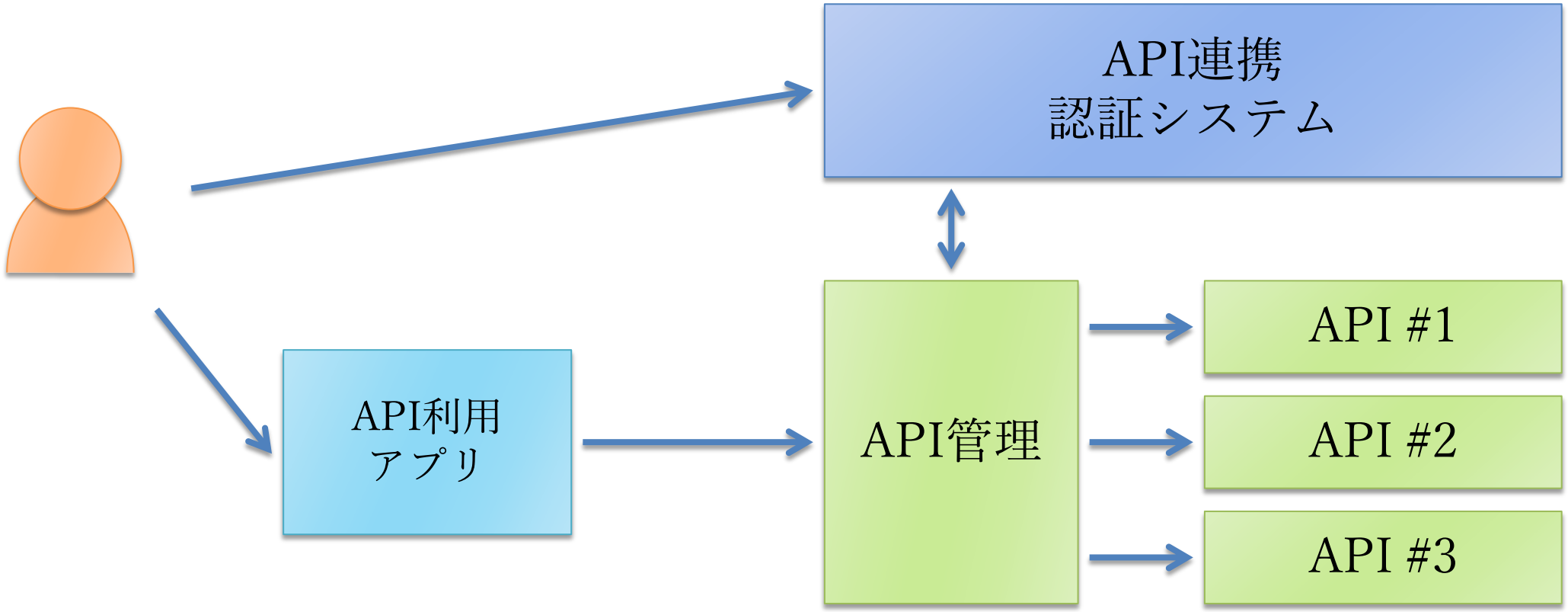
- **以下の仕様についても検討が進行中。**
  - Client Initiated Backchannel Authentication Profile.

現時点で対応を検討しておくべき仕様

#	仕様	AS 実装者	API 開発者	API利用者 アプリ開発者
①	OpenID Connect Core 1.0	○	—	○
.1	[OAUTB], [MTLS] を使った記名式トークン、認可コード発行への対応	○	○	○
.2	署名、暗号化されたIDトークンのサポート [Sec.2][Sec.16.14]	○	○	○
.3	長期間有効なトークン発行時の適切な同意画面の表示	○	—	—
②	OAuth 2.0 トークン発行時の scope クレームの応答への対応	○	—	○
③	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants [RFC 7521]	○	—	○
④	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants [RFC 7523]	○	—	○
⑤	OAuth 2.0 Token Binding [OAUTB] [draft-ietf-oauth-token-binding-05]	○	○	○
⑥	OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens [MTLS] [draft-ietf-oauth-mtls-07]	○	○	○

最新の技術標準仕様に追従する

- 策定される新しい仕様への追従を個々の API で進めるのは困難
- API管理ソリューションを使った集中管理が必要になっていく



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

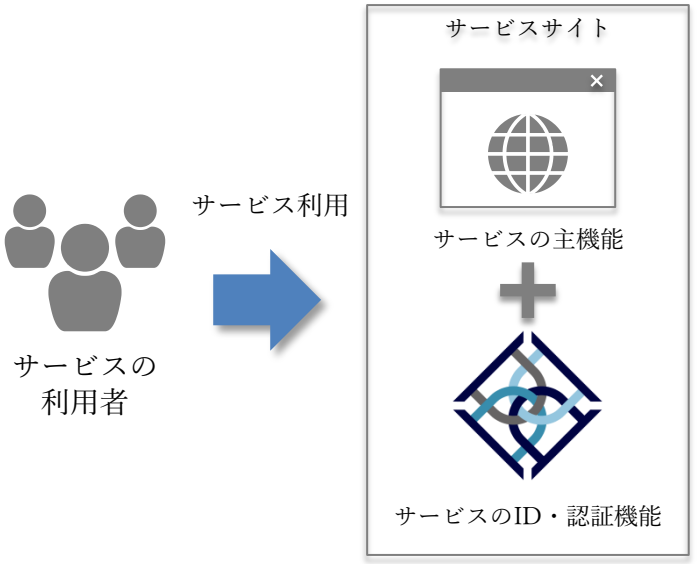
ThemiStruct（テミストラクト）
IdentityPlatform

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

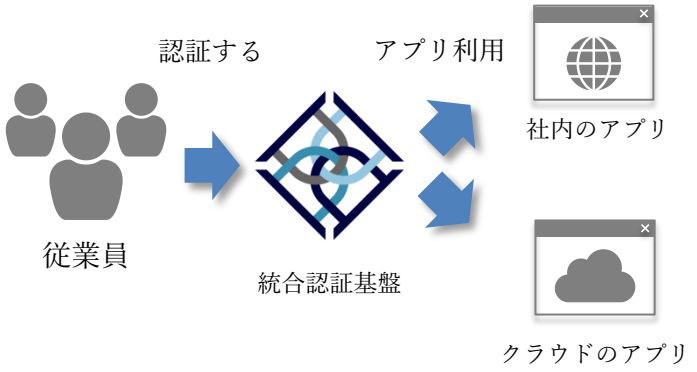
ThemiStruct Identity Platform は、ITシステム利用者のアイデンティティ管理と認証の機能を提供します。顧客向けにサービスを展開したり、従業員向けにアプリケーションを展開する際に必要となる、共通ID基盤の構築に活用いただけます。

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

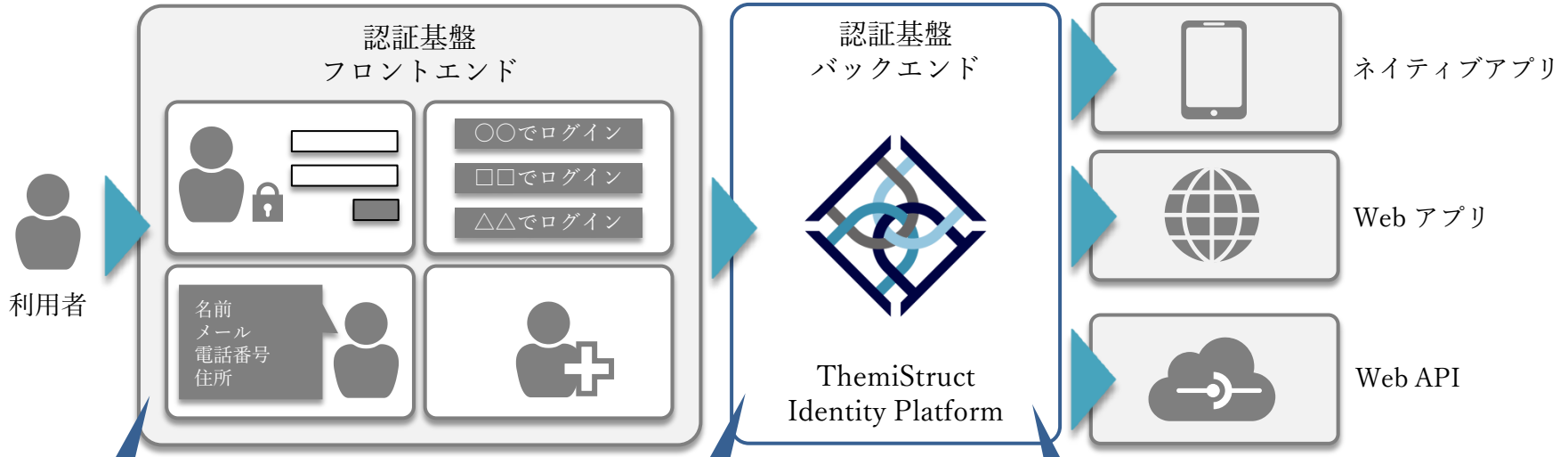
エンタープライズ領域に活用



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

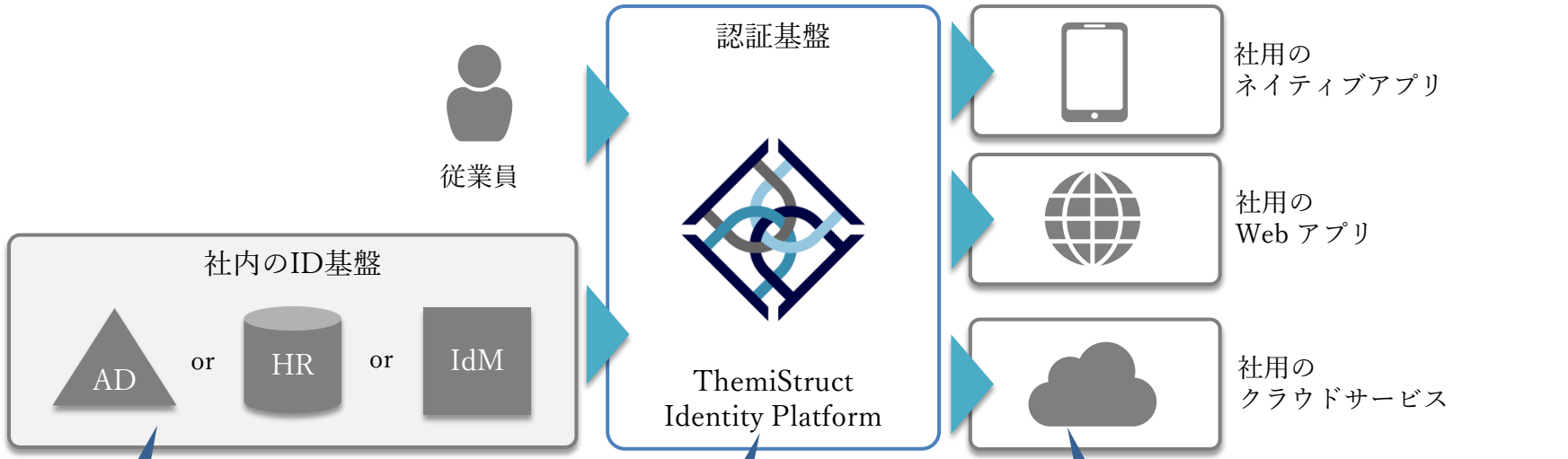
- OAuth 2.0 の技術仕様に基づいた認証・アクセス認可機能を提供します。OAuth 2.0 を使ったAPI連携認証システムが実現でき、モバイルアプリ、オープンAPIを安全に公開できます。

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

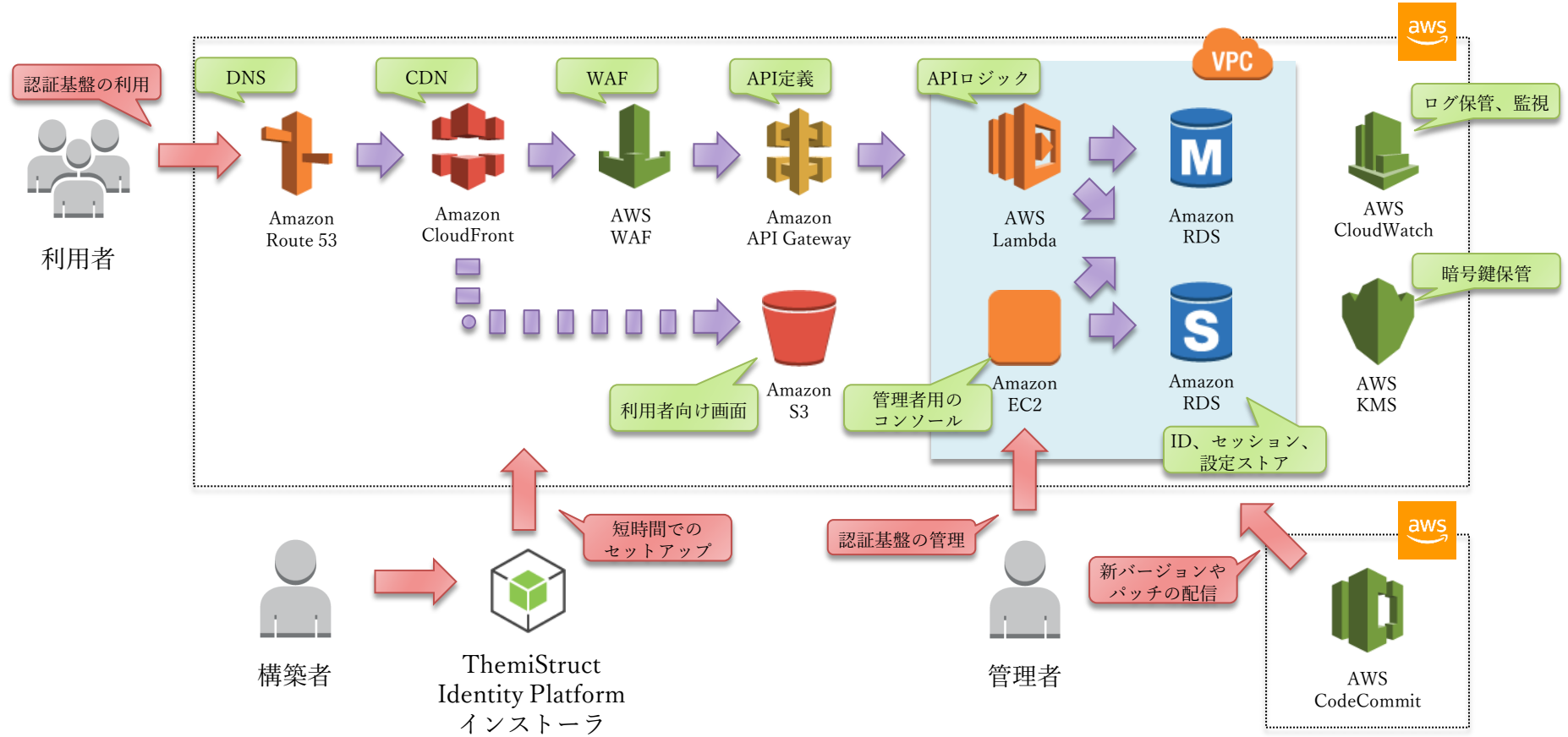
- ユーザーの属性や状態、利用するアプリケーションに応じて、柔軟な認証ポリシーをデザインすることができます。例えば、社内ネットワークからのアクセスの場合、IDとパスワードの認証を提供し、外出先からのアクセスの場合、追加でワンタイムパスワード認証を提供するといったポリシーを展開することができます。

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

- オージス総研のクラウドとAPI開発・運用の知見を集めたサービス
  - FintechやIoTなどのデジテルビジネスに必要不可欠なAPI公開を実現
  - API導入のための技術調査・検討からAPIの公開・運用までフルカバー

■API導入コンサルティングサービス

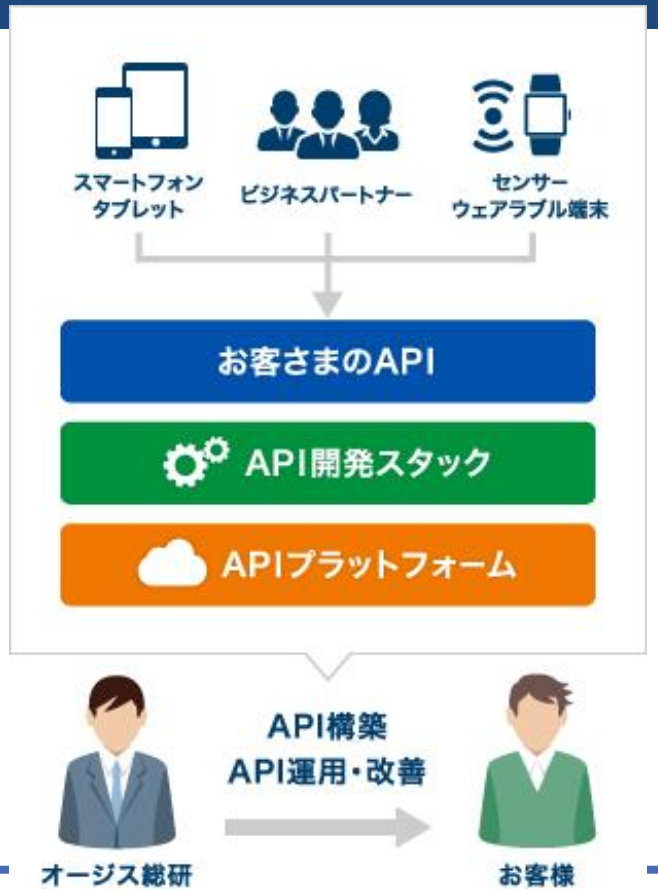
✓ ロードマップの策定援や、初期システムアーキテクチャ策定、API導入PoC等によりAPI導入を支援

■API構築サービス

✓ ベストプラクティスを組み込んだAPI開発スタックを使い、お客様の環境に合ったAPIプラットフォーム、APIを迅速かつ効率的に開発

■API運用サービス

✓ 継続的なAPIの改善・バージョンアップ
✓ 安定稼働のためのAPIプラットフォームの監視・障害対応
✓ API利用者向けサポートサービス



まとめ

まとめ

- 認証基盤のユースケースは、顧客向けサービス向け、オープンAPI向けへと広がり、重要性がより高まっている。
- 高い可用性、アクセスの増減、繁閑に対応できる認証基盤の実現が求められている。
- 認証基盤をサーバーレスアーキテクチャで構築することで要求に応えていく。
- 当社では ThemiStruct Identity Platform を、サーバーレスアーキテクチャの認証基盤を実現するパッケージとして提供している。

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