サーバーレスアーキテクチャで構築する
統合認証基盤と顧客サービス向けの認可サーバー

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

© 2019 OGIS-RI Co., Ltd.

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

© 2019 OGIS-RI Co., Ltd.

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）

aws partner network
Advanced Consulting Partner

オージス総研

Daigas Group

© 2019 OGIS-RI Co., Ltd.

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

テミストラクト
ThemiStruct®
アイデンティティプラットフォーム
IdentityPlatform®

OAuth 2.0 に対応した
APIエコノミー時代に求められる
統合認証パッケージ

© 2019 OGIS-RI Co., Ltd.

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

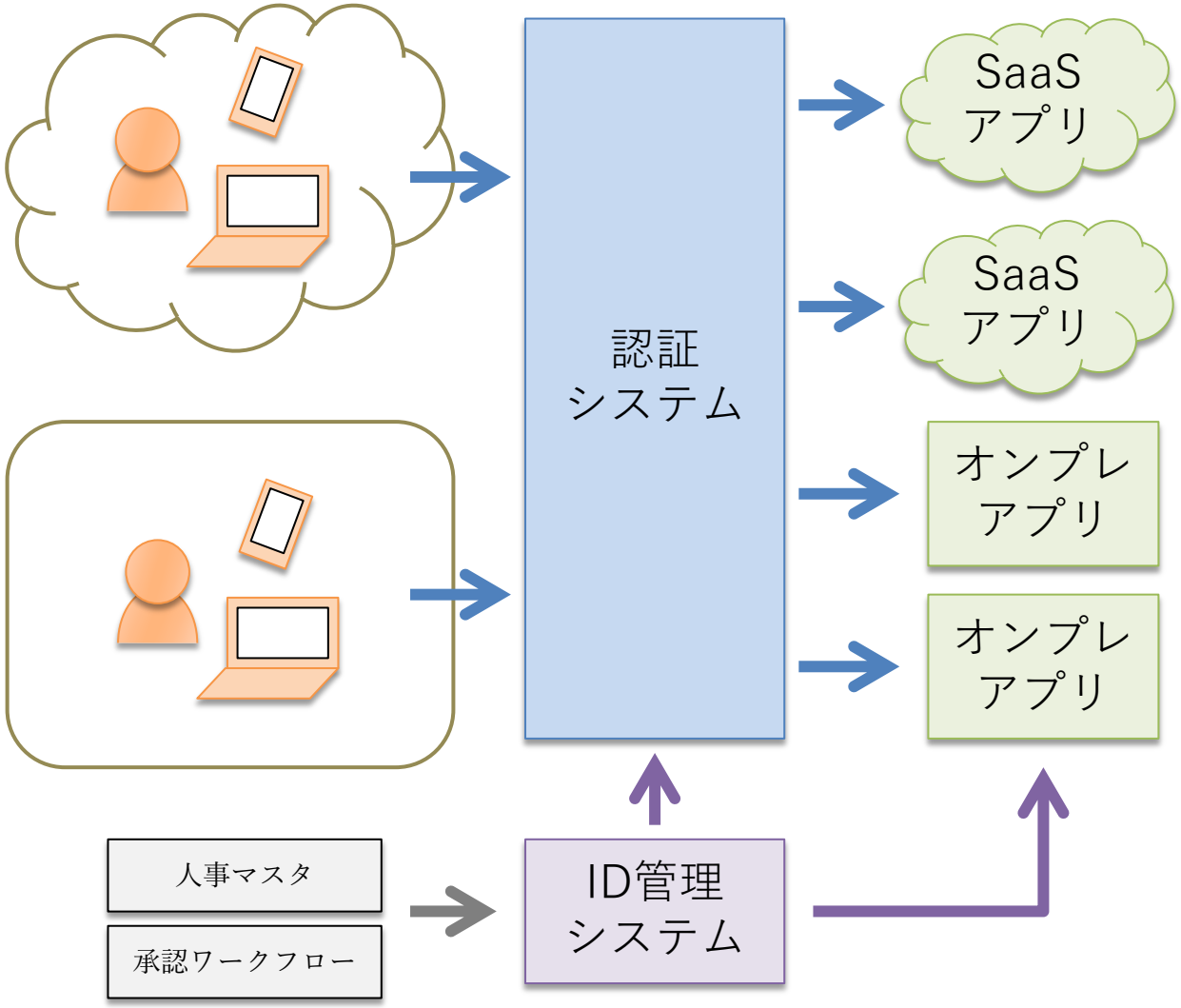
オープンAPIを提供するための「**API連携認証システム**」を構築する

© 2019 OGIS-RI Co., Ltd.

「社内統合認証基盤」

- 安全で便利な業務環境の提供
- 適正な業務処理の実現
- ID管理業務負担の軽減
- 社内業務システムと
  取引先へのシステム提供

- 異動や申請に基づくタイムリーな
  権限付与・削除
- アクセス元、利用端末を含めた認証
- 業務システムの追加のしやすさ
- SaaS、パッケージ製品との接続性

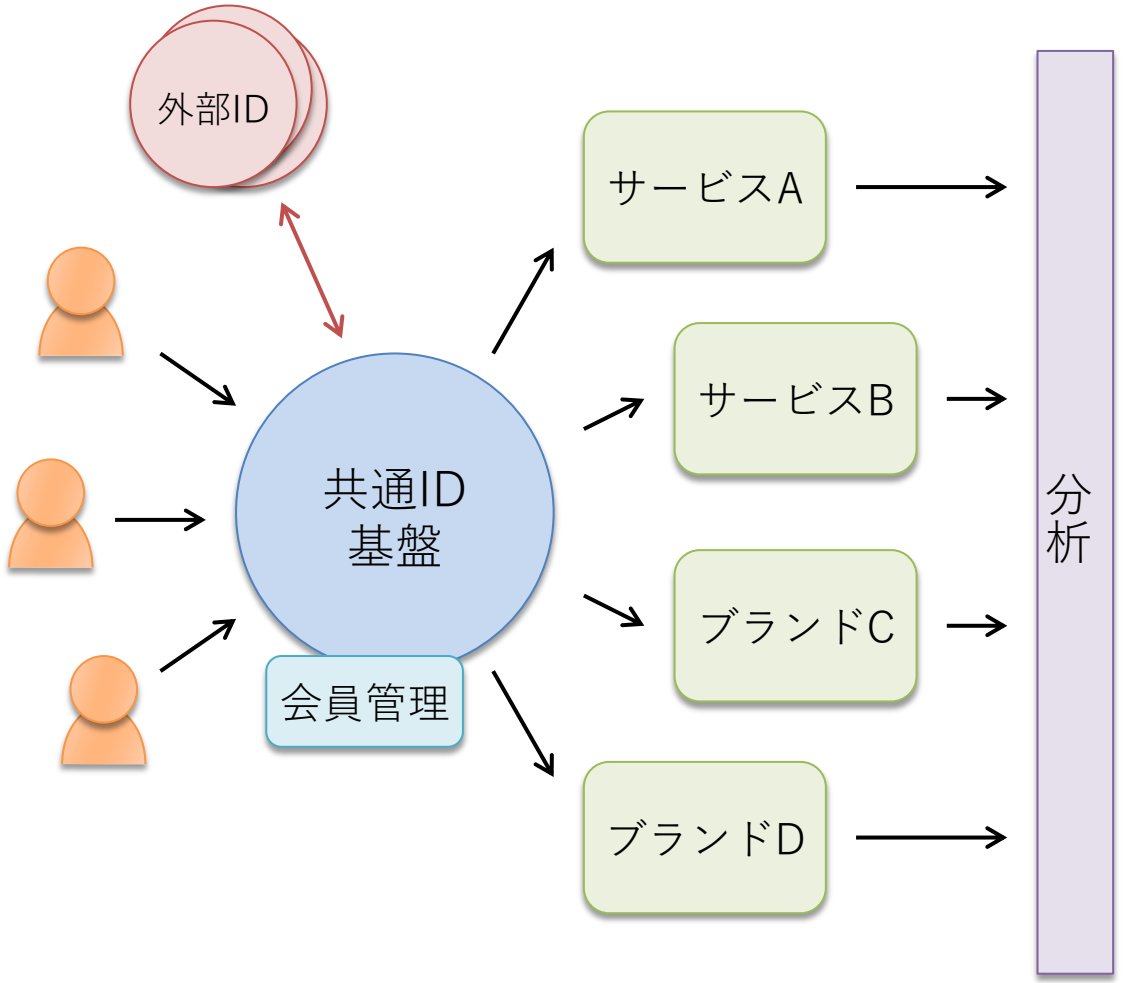


© 2019 OGIS-RI Co., Ltd.

「共通ID基盤」

- 自社サービスの会員IDを共通化
- 外部IDと連携した簡単登録の実現
- サービス利用状況の把握・分析
- 変わりゆく認証方式への対応

- 既存画面へのUI統合、デザイン変更
- ブランド毎の画面の出しわけ
- 24時間365日止めない運用の実現
- スパイクアクセスへの対応・耐性
- 既存会員管理との統合、データ移行



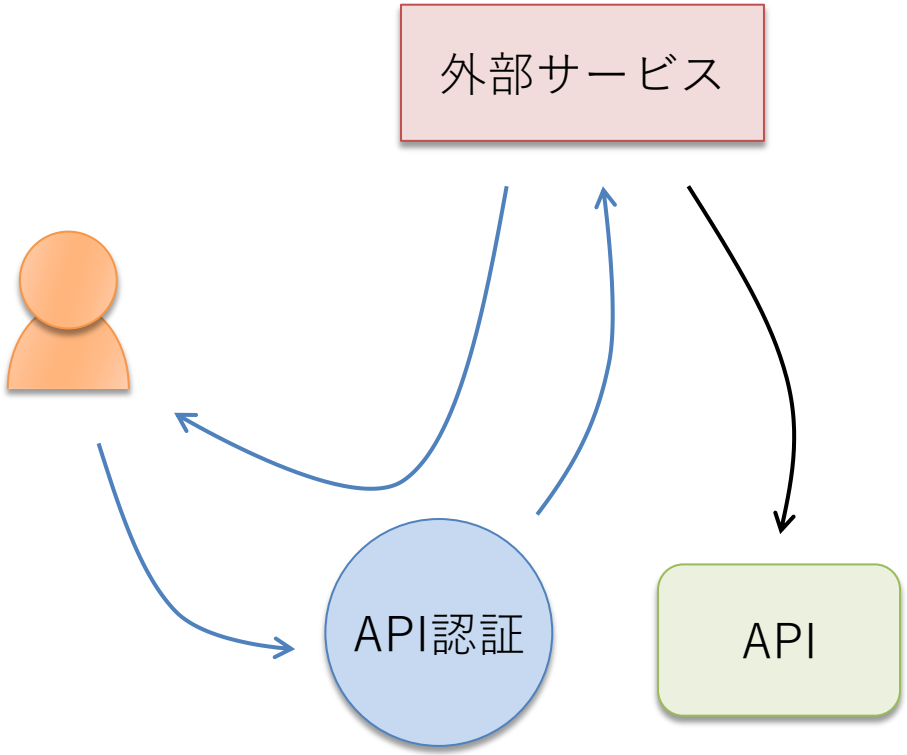
© 2019 OGIS-RI Co., Ltd.

「API連携認証システム」（OAuth認可サーバー）

- 外部サービスへのAPI提供、そのための認証機能の実現
- 利用者の同意に基づくAPI提供・アクセス許可の実現

- 技術標準仕様への適合
- 利用者が理解しやすい同意画面の提示、画面デザイン変更
- 利用機能、利用目的ごとのアクセス管理

- ＋ 共通ID基盤の特性



© 2019 OGIS-RI Co., Ltd.

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

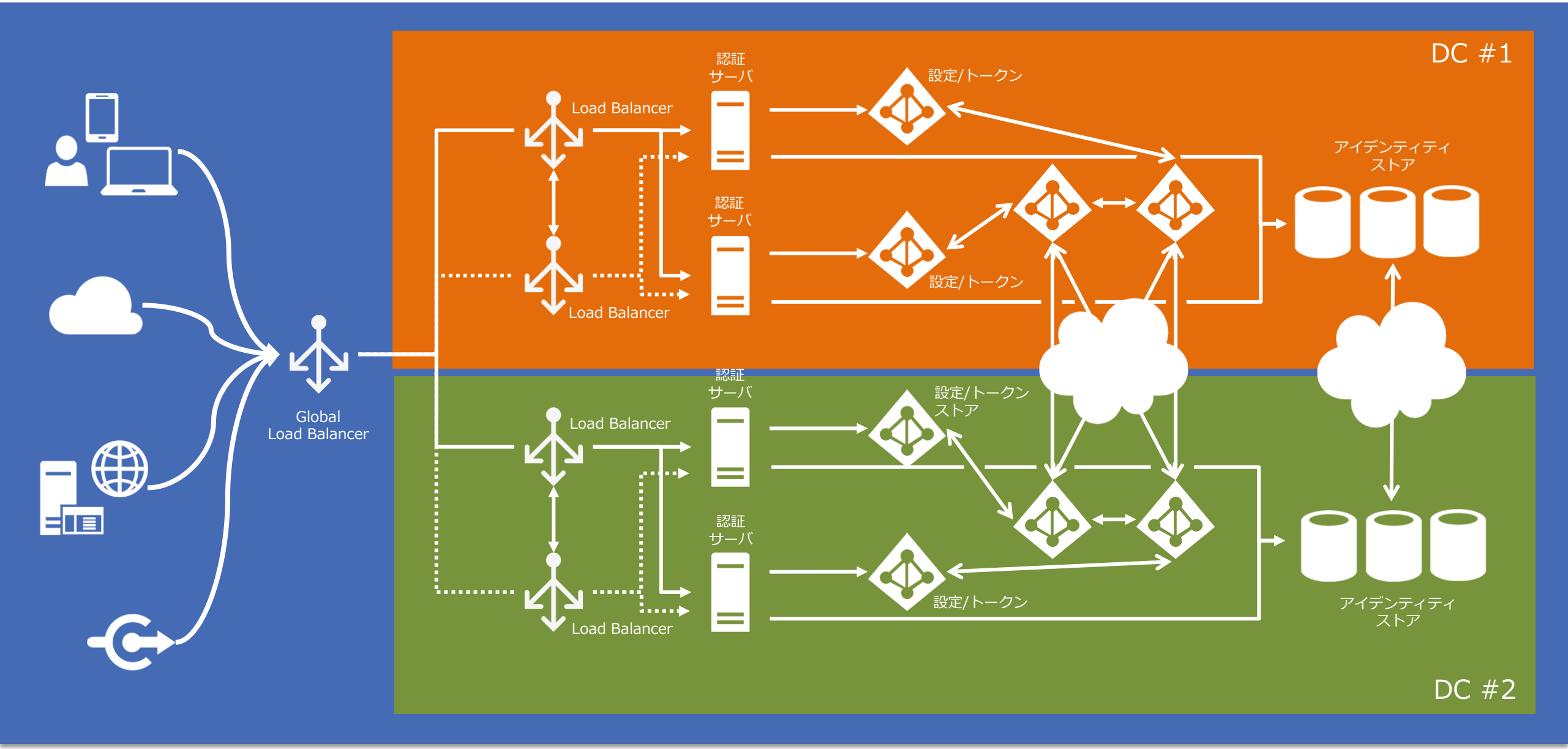
- 業務影響を抑えるため障害状態から短時間での回復が必要

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

© 2019 OGIS-RI Co., Ltd.

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。

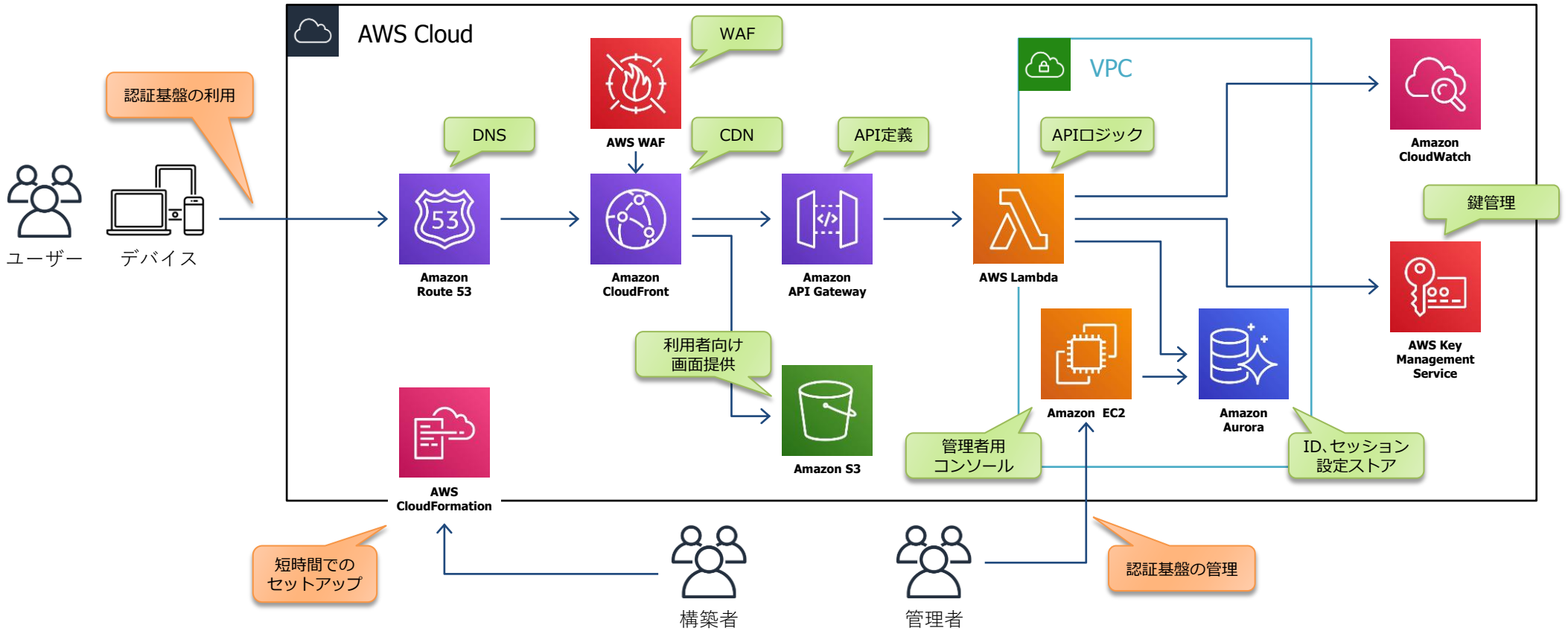


© 2019 OGIS-RI Co., Ltd.

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？

© 2019 OGIS-RI Co., Ltd.

ThemiStruct Identity Platform を開発



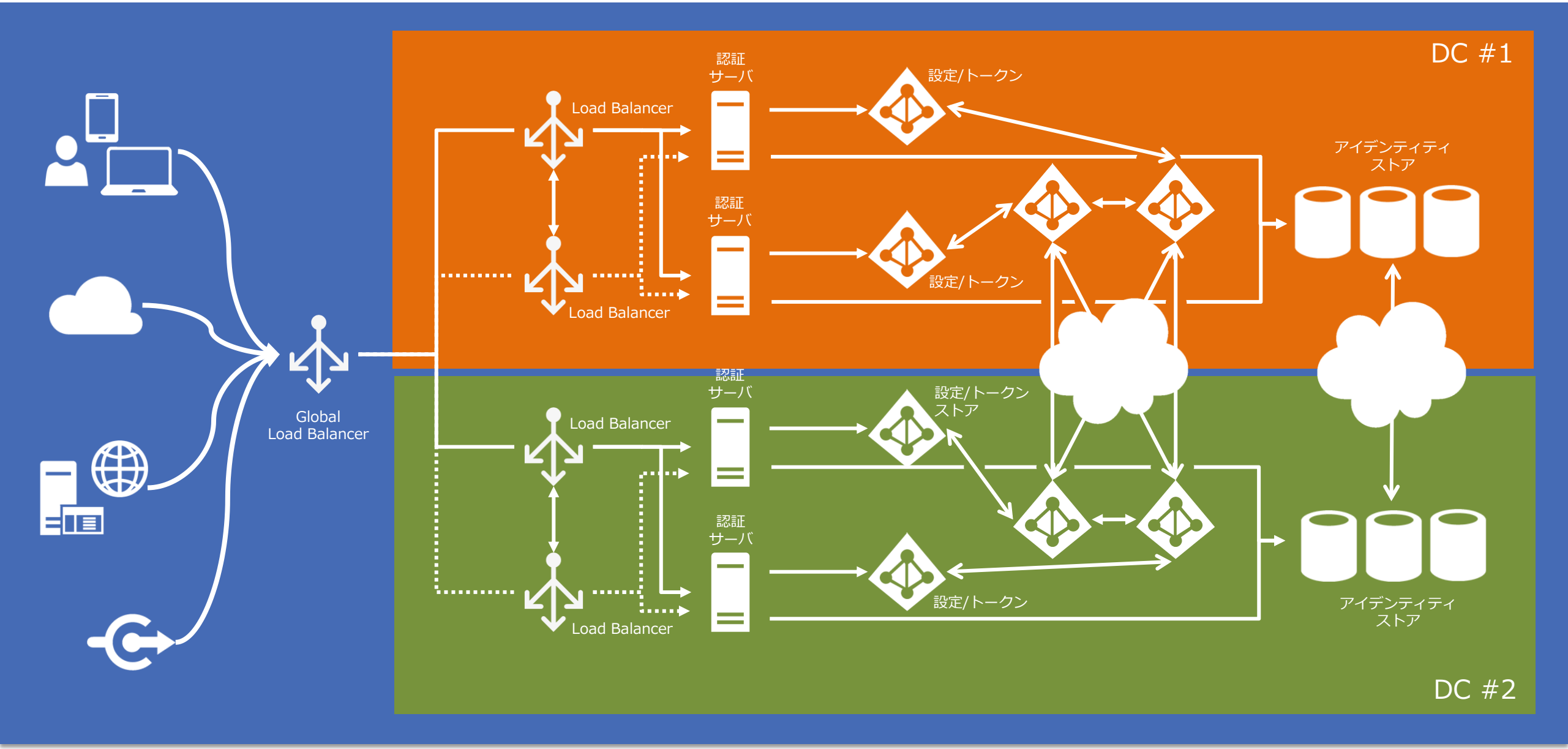
© 2019 OGIS-RI Co., Ltd.

ThemiStruct Identity Platform の特長

- Amazon API Gateway, AWS Lambda など、AWS Cloud のコンポーネントを活用。
- AWS Cloud 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。
- アマゾン ウェブ サービス (AWS) の各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。

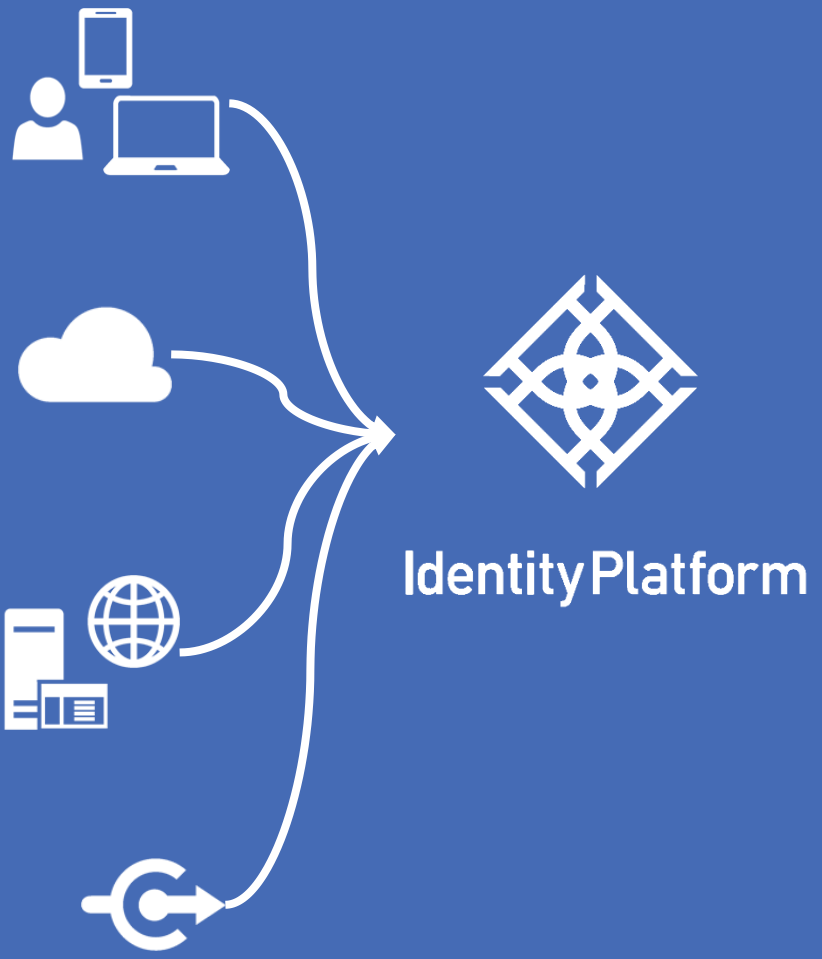
© 2019 OGIS-RI Co., Ltd.

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。



© 2019 OGIS-RI Co., Ltd.

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。



© 2019 OGIS-RI Co., Ltd.

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

© 2019 OGIS-RI Co., Ltd.

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	△

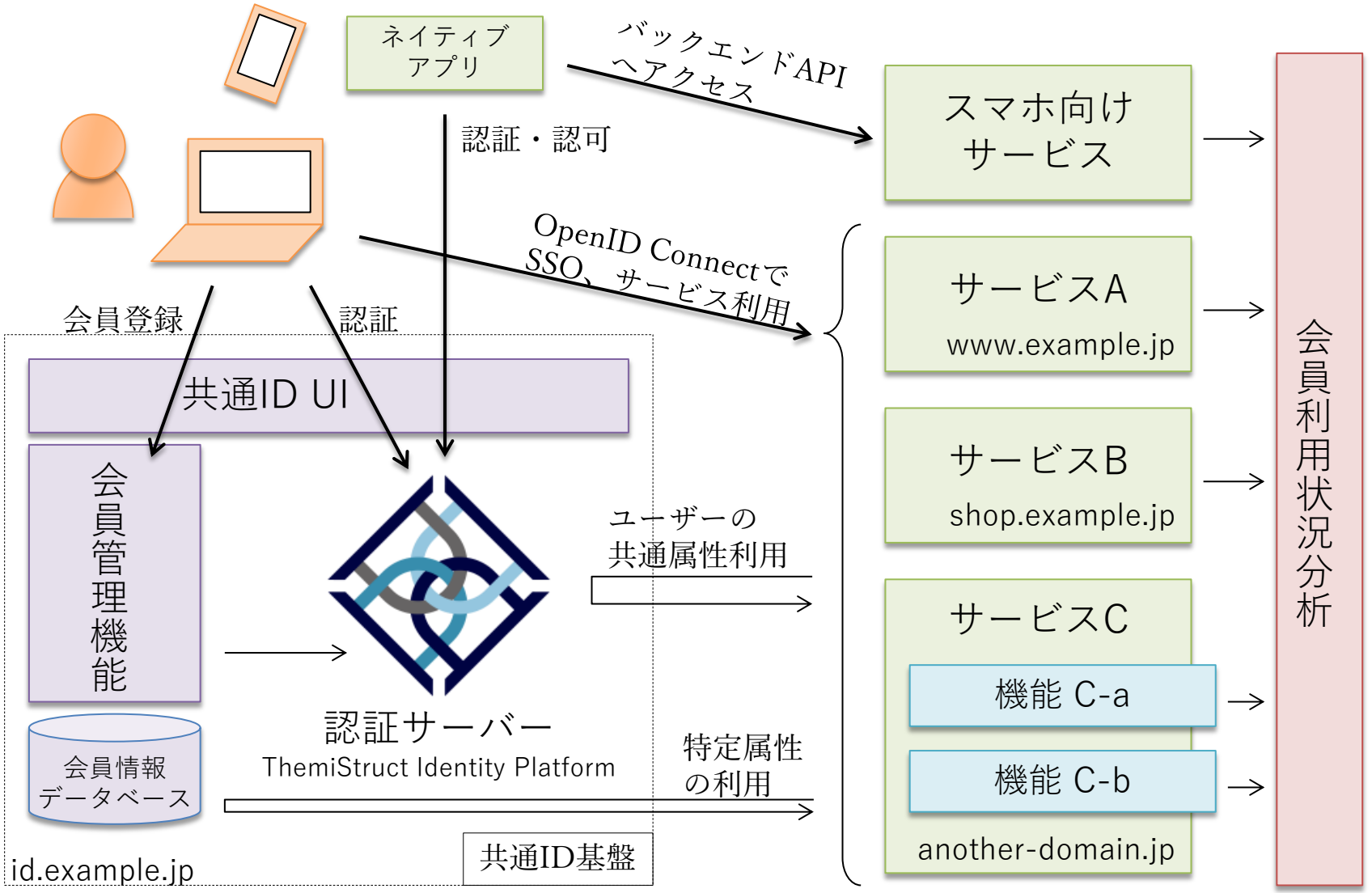
© 2019 OGIS-RI Co., Ltd.

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

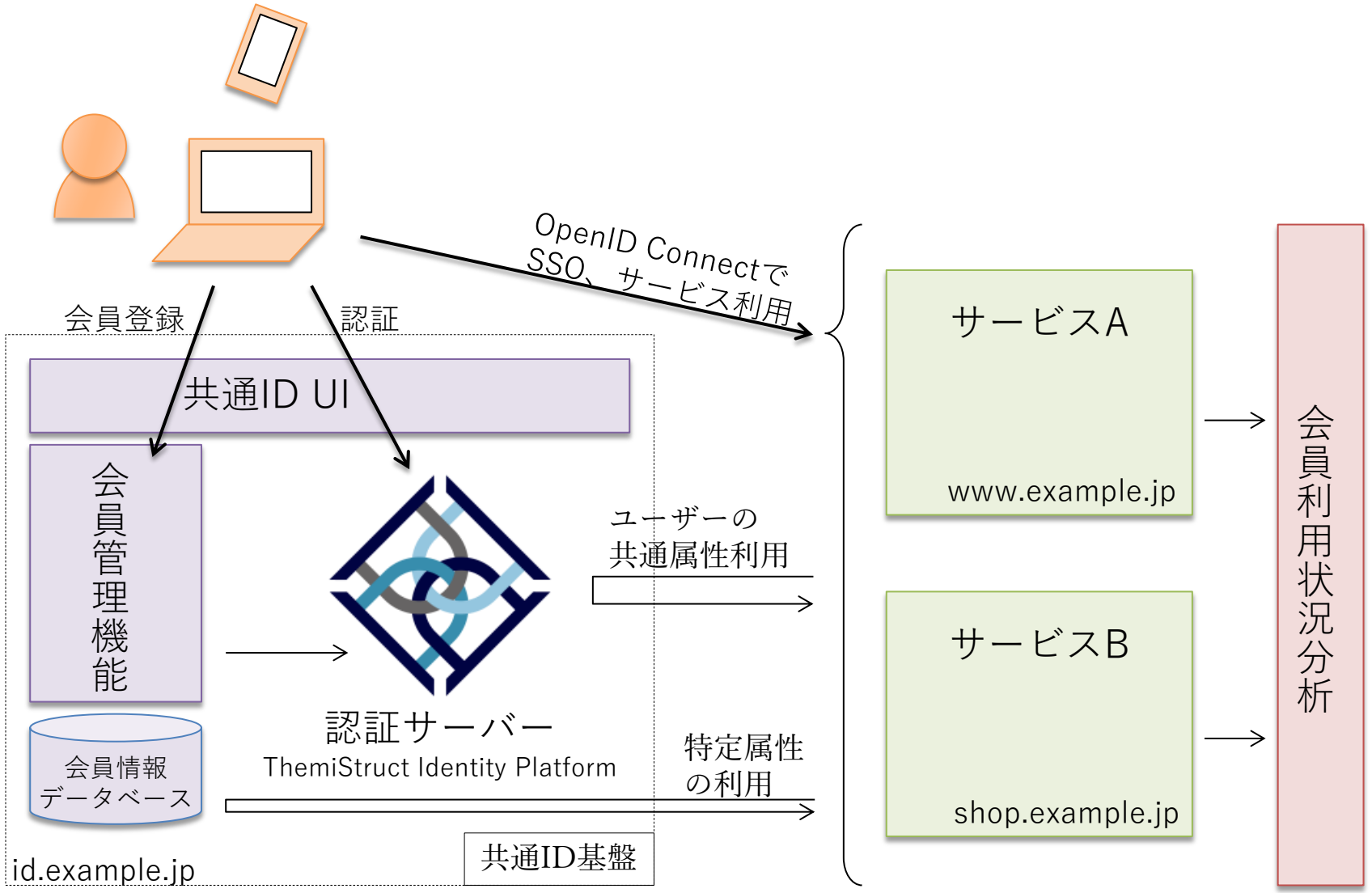
© 2019 OGIS-RI Co., Ltd.

「共通ID基盤」の構築イメージ



© 2019 OGIS-RI Co., Ltd.

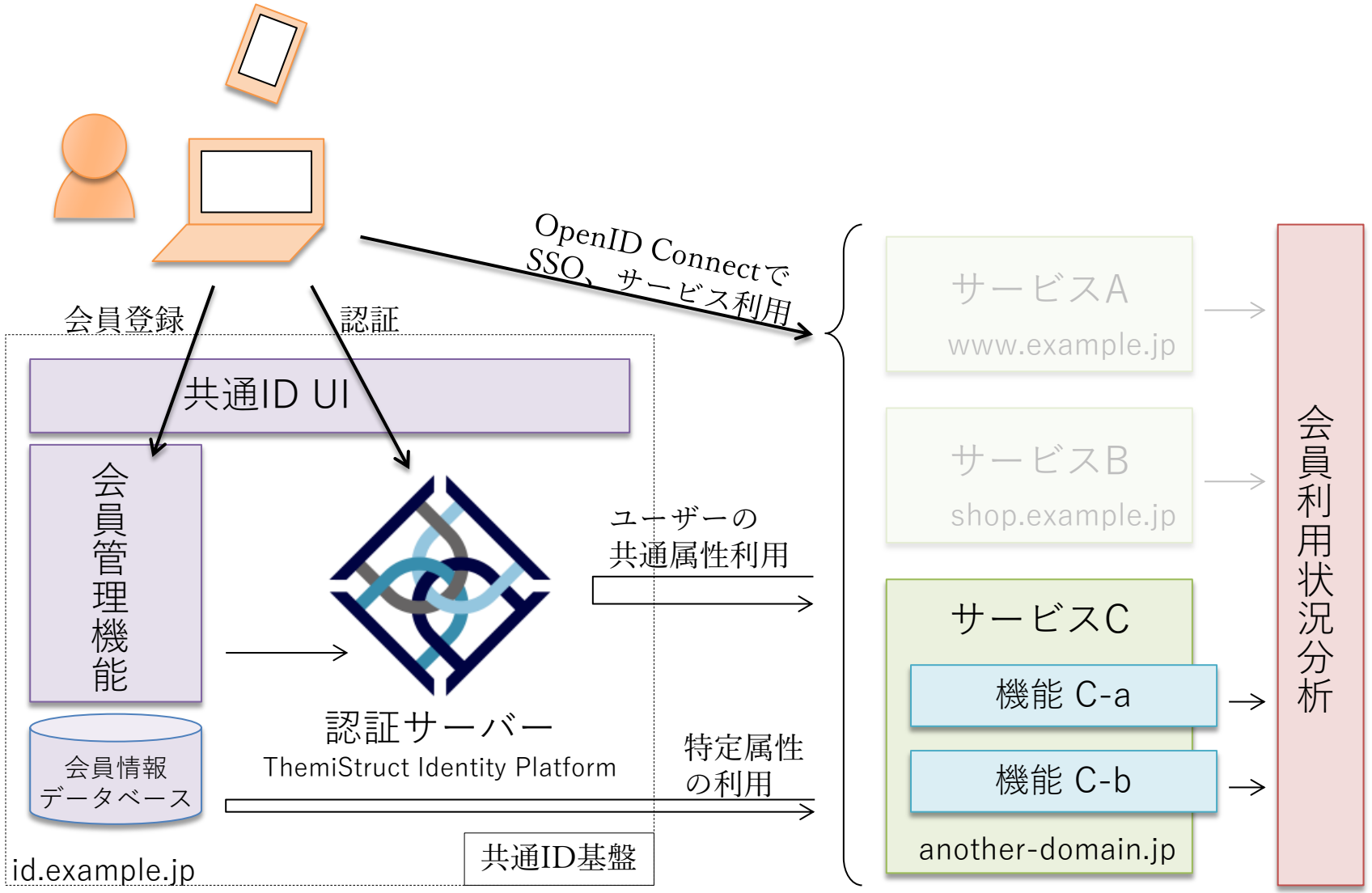
顧客向けサービスのIDを共通化する



- ✓ 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。

© 2019 OGIS-RI Co., Ltd.

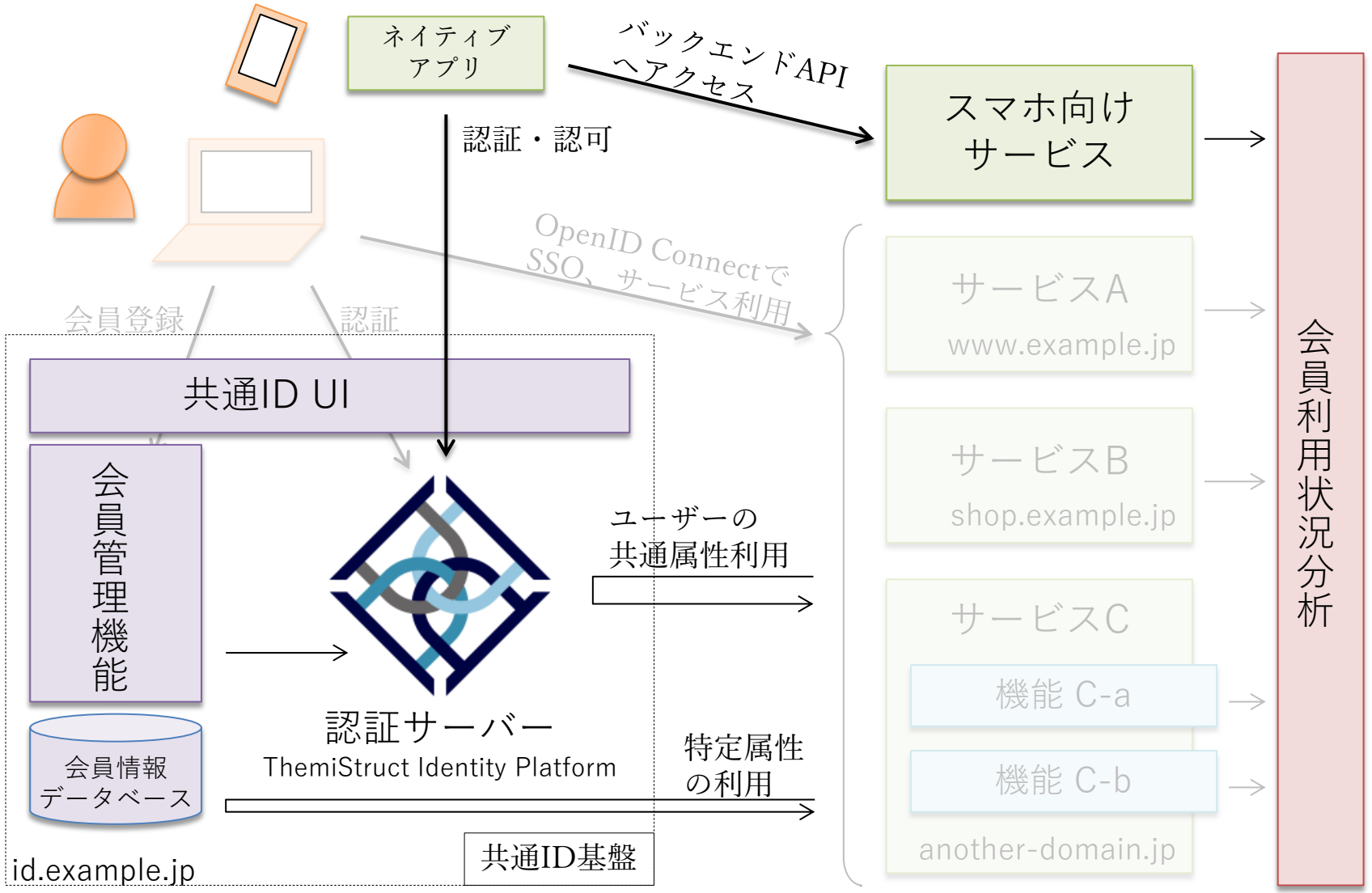
提供サービスを追加する、更新する



- ✓ 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。

© 2019 OGIS-RI Co., Ltd.

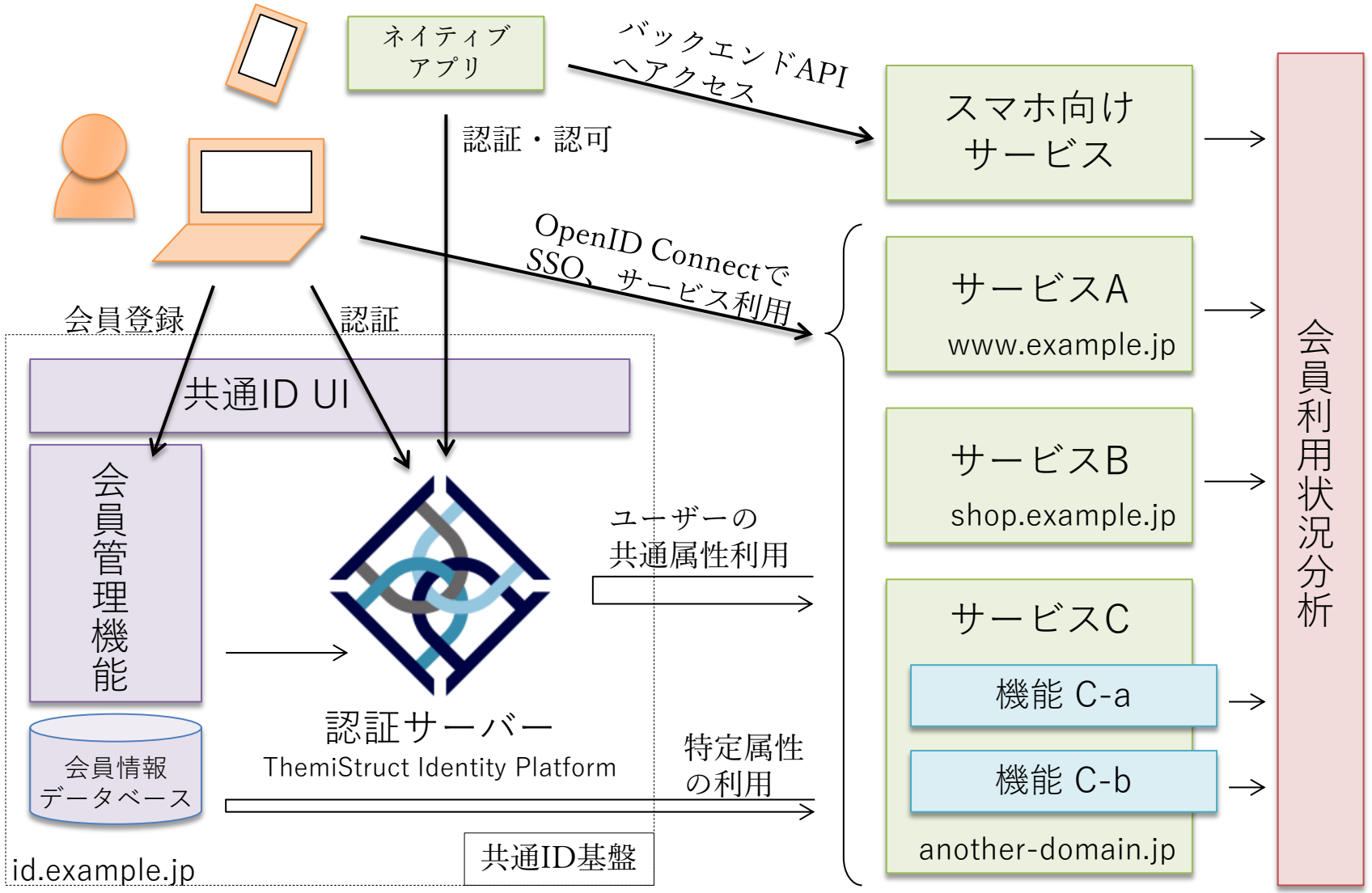
スマホ向けサービスを提供する



- ✓ 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。

© 2019 OGIS-RI Co., Ltd.

スケーラブル、ハイアベイラブルな共通ID基盤に



- ✓ AWS Cloud が持つスケーラビリティにより、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。

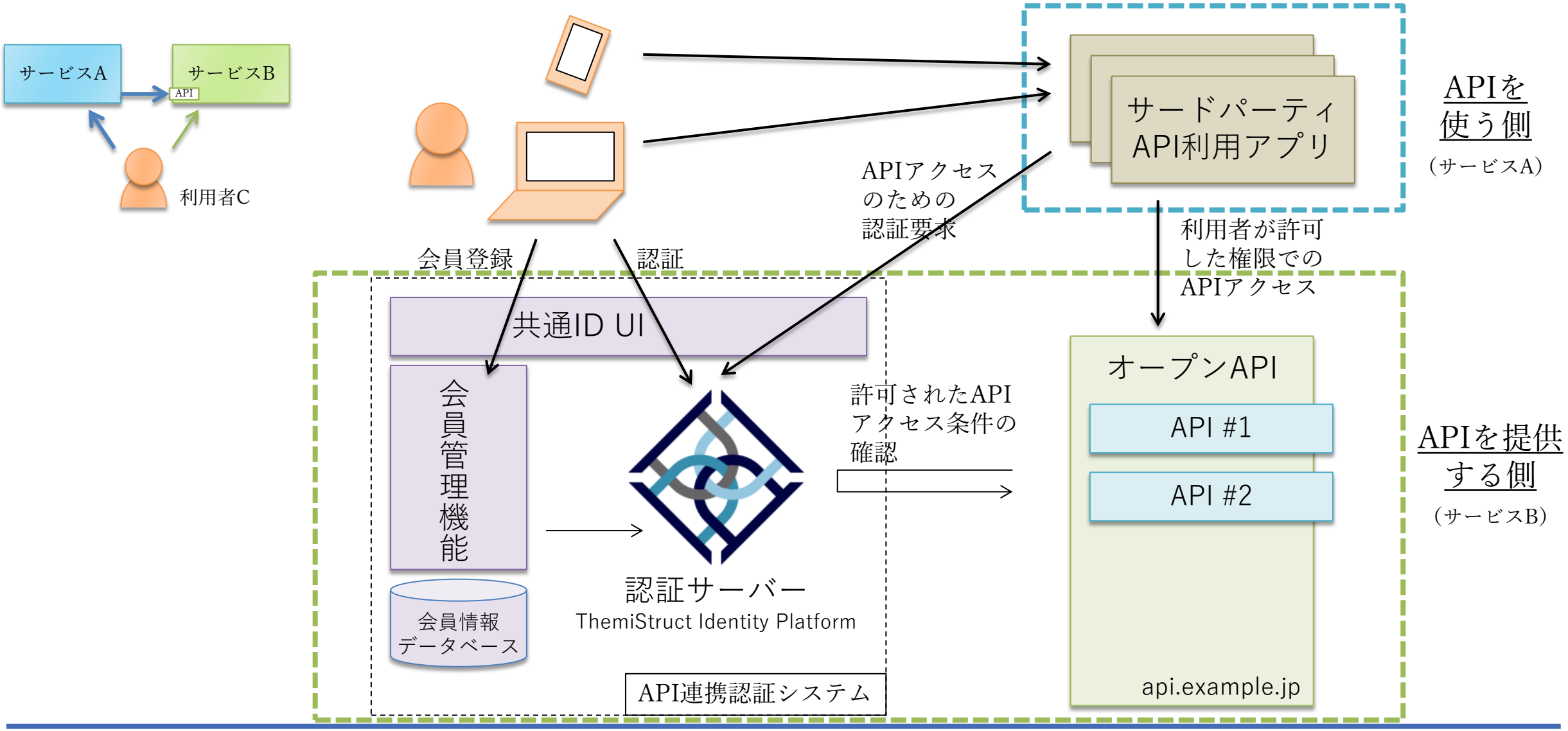
© 2019 OGIS-RI Co., Ltd.

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

© 2019 OGIS-RI Co., Ltd.

「API連携認証システム」の構築イメージ

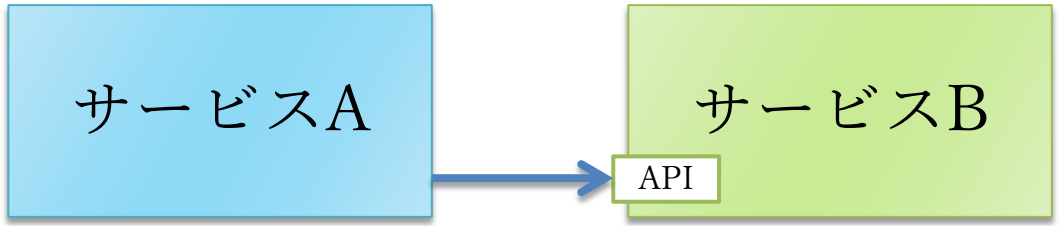


© 2019 OGIS-RI Co., Ltd.

Web API 利用の形態

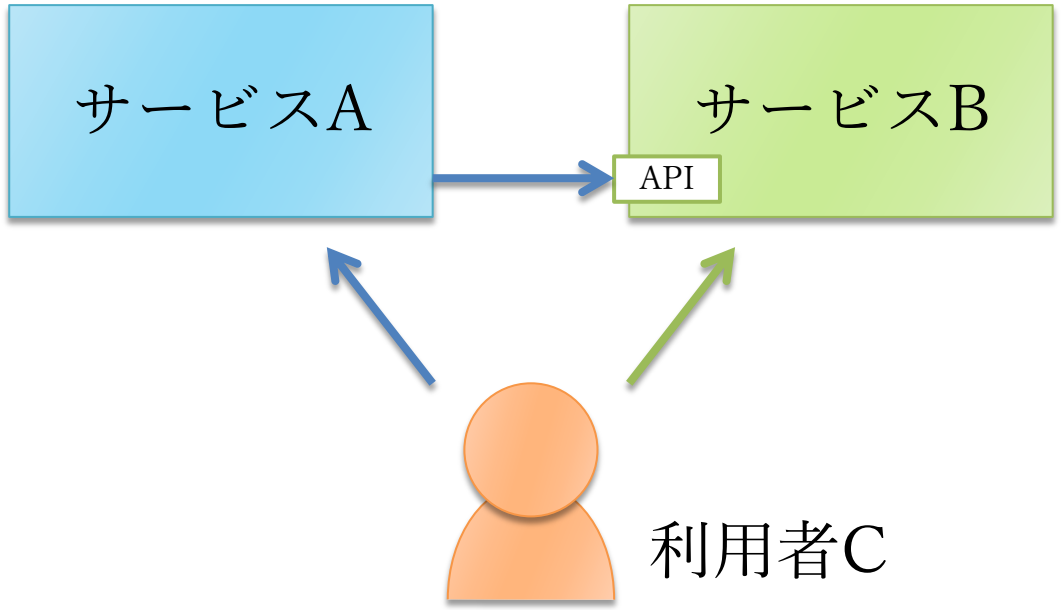
2者間でのAPI利用

- サービスA が サービスB の機能を利用するために API にアクセスする。
- サービスB は サービスA 向けの機能・データを提供する。



3者間でのAPI利用

- 利用者C は サービスA、サービスB の利用者である。
- サービスA は、利用者Cの意図により、利用者C に代わり サービスB の API にアクセスする。
- サービスB は 利用者C 向けの機能・データーを提供する。



© 2019 OGIS-RI Co., Ltd.

2者間でのAPI利用時の認証

- **API のアクセス元を認証する。**
  - APIキー
  - BASIC認証（IDとパスワード）
  - クライアント証明書
  - OAuth 2.0 Client Credentials Grant
  - …
- **アクセス元が認証できれば、API はアクセス権を判断できる。**

© 2019 OGIS-RI Co., Ltd.

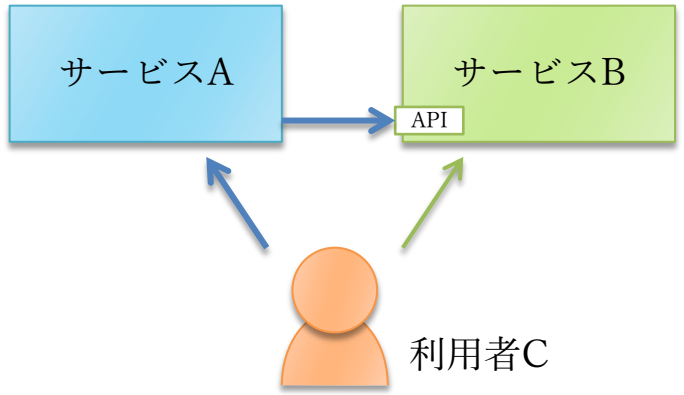
3者間でのAPI利用時の認証

ロ 利用者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

- 利用者C の同意に基づき、利用者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



© 2019 OGIS-RI Co., Ltd.

OAuth 2.0 仕様の概略（最小限）

© 2019 OGIS-RI Co., Ltd.

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]	—	—	○

© 2019 OGIS-RI Co., Ltd.

API利用時の構成パターン

ロ バックエンドあり（Confidential Client）

ロ バックエンドなし（Public Client）

© 2019 OGIS-RI Co., Ltd.

アプリ形態別、対応すべき OAuth の方式

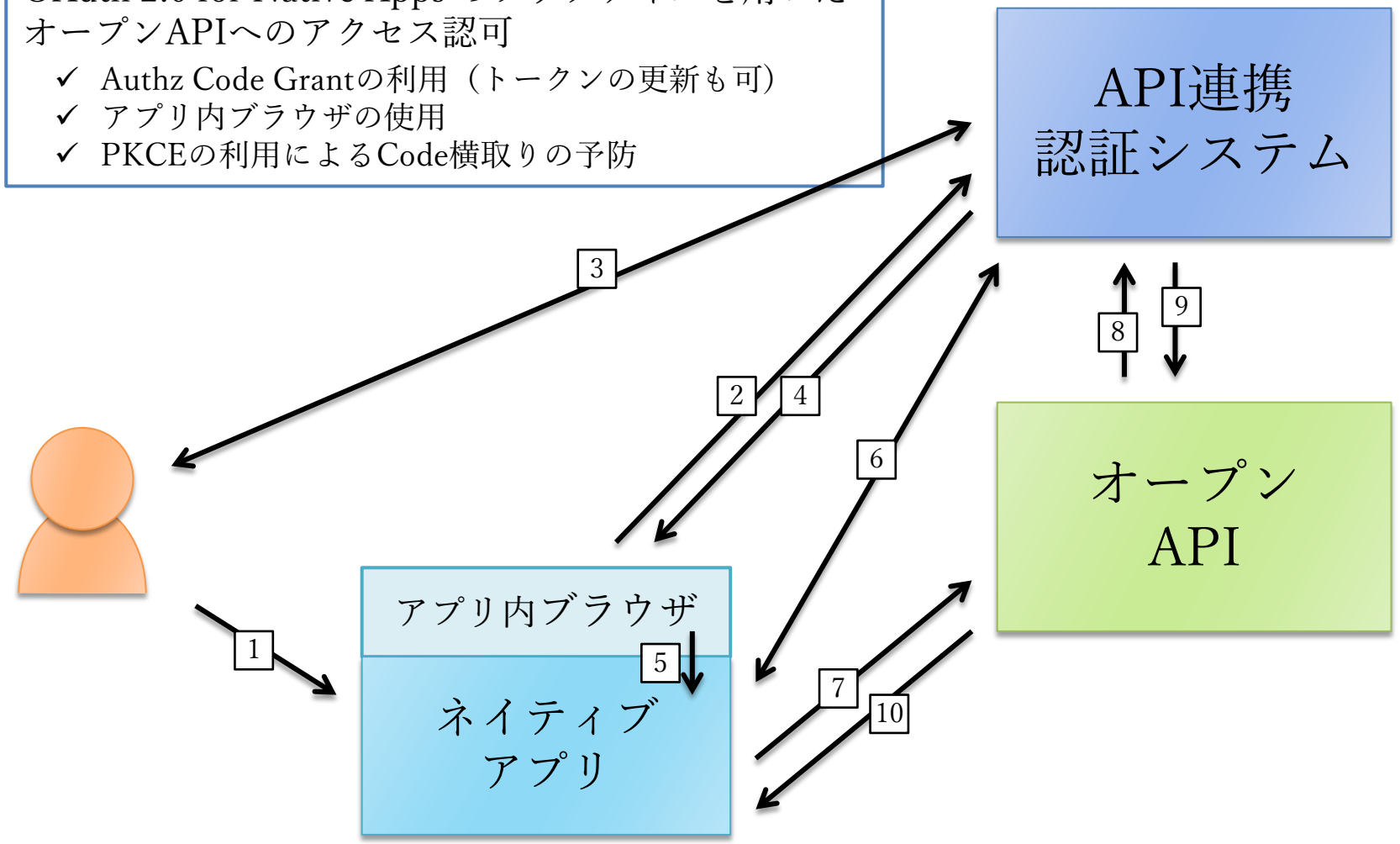
#	利用者への提供形態	バックエンド	OAuthの方式	ポイント
①	**ブラウザで動作するJavaScriptアプリ** (モバイルウェブ、SPA、など)	あり	Authz Code Grant	バックエンドがオープンAPIへアクセス。バックグラウンドでのAPIアクセスのため、トークン自動更新が必要な場合も。
②		なし	Implicit Grant ➡ Authz Code Grant w/ PKCE に向かう	JSアプリがオープンAPIへアクセス。トークン更新が必要な場合はブラウザを介して行なえる。
③	**ネイティブアプリ**	あり	Authz Code Grant	（① と同じ）
④		なし	Authz Code Grant 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 Grant	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。

© 2019 OGIS-RI Co., Ltd.

ネイティブアプリでのAPIアクセス認可

OAuth 2.0 for Native Apps のプラクティスを用いた
オープン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、ログイン開始
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. アクセストークンを取得するためのCodeを返却
5. アプリ内ブラウザからネイティブアプリにCodeを返却
6. Codeをアクセストークンに交換（PKCEを併用）
7. アクセストークンをつけてオープンAPIにアクセス
8. ~9. 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）
10. オープンAPIが情報を使ってネイティブアプリが動作

オープンAPIの振る舞いは、JSアプリ、ネイティブアプリで共通。

© 2019 OGIS-RI Co., Ltd.

対応が必要となってくる追加仕様
（OAuth 2.0, OpenID Connect 関連）

© 2019 OGIS-RI Co., Ltd.

金融API向けにOAuth実装仕様の策定が進行中

- **OpenID Foundation (Global) の Financial-grade 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 2).
  - Part 2: Read & Write API Security Profile (Implementer's Draft 2).
  - JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

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

© 2019 OGIS-RI Co., Ltd.

Part 1: Read-Only API Security Profile ①

Draft-06の内容を抜粋

#	Authorization Server への要求事項
1	コンフィデンシャルクライアントをサポートする。(SHALL)
2	パブリッククライアントをサポートすることが望ましい。(SHOULD)
3	（署名や暗号化に）対象鍵を使う場合は [OIDC] の 16.19節 の要件に準拠した client_secret を提供する。(SHALL)
4	トークンエンドポイントでは以下のいずれかの方法を用いてコンフィデンシャルクライアントを認証する。(SHALL) 1. [MTLS] の 2章 で指定されている OAuthクライアント認証のためのTLS相互認証 2. [OIDC] の 9章 で指定されている client_secret_jwt もしくは private_key_jwt
5	クライアント認証にRSA暗号アルゴリズムを用いる場合は 2048ビット 以上の長さの鍵を用いる。(SHALL)
6	クライアント認証に楕円曲線暗号アルゴリズムを用いる場合は 160ビット 以上の長さの鍵を用いる。(SHALL)
7	[RFC7636] の S256コードチャレンジ方式 を使用する。(SHALL)
8	リダイレクトURIは事前登録する。(SHALL)
9	認可要求のパラメータに redirect_uri を必要とする。(SHALL)
10	（認可要求の）redirect_uri の値は、事前に登録されたリダイレクトURIの一つに完全一致しなければならない。(SHALL)

- **OAuth 2.0 [RFC6749] の基本仕様に加え、OAuthシリーズの追加仕様、OpenID Connectで定義された仕様などを併用するように整理されている。**
- **鍵やトークンの長さ、パラメータの使い方、リクエストやデータの検証方法など、より具体的な指定がなされている。**
- **PKCEへの対応が必須に。ネイティブアプリはカスタムスキームではなく App Links, Universal Links への対応が必要に。**

© 2019 OGIS-RI Co., Ltd.

Part 1: Read-Only API Security Profile ②

Draft-06の内容を抜粋

#	Authorization Server への要求事項
11	[X.1254] に定義された LoA 2 以上のユーザー認証を要求する。(SHALL)
12	以前に承認されていない scope の要求を承認する場合には、ユーザーの明示的な同意を必要する。(SHALL)
13	認可コード ([RFC6749] 1.3.1節) が以前に使用されてないことを検証することが望ましい。(SHOULD)
14	[RFC6749] 4.1.4節に沿ったトークンレスポンスを返す。(SHALL)
15	発行されたアクセストークンとともに許可されたスコープのリストを返す。(SHALL)
16	[RFC6749] の 10.10節 にあるように、攻撃者が生成されたトークンを推測する確率が 2^(-160) 以下となるよう、 エントロピーが最低128ビットである不透明な推測できないアクセストークンを発行する。(SHALL)
17	[OIDC] 16.18節にあるとおり認可中に長期間の許可を与えようとしていることユーザーに明示することが望ましい。(SHOULD)
18	[OIDC] 16.18節にあるとおりエンドユーザーがクライアントに付与されたアクセストークンやリフレッシュトークンを失効する仕組みを提供することが望ましい。(SHOULD)
19	2つ以上の方法でクライアント識別子を送信することを許可するクライアント認証方法では、提供されたクライアント識別子が一致していない場合、[RFC6749] の 5.2節 で定義された invalid_client エラーを返す。(SHALL)
20	httpsスキームを使うリダイレクトURIを使用する。(SHALL)

- **OAuth 2.0 [RFC6749] の基本仕様に加え、OAuthシリーズの追加仕様、OpenID Connectで定義された仕様などを併用するように整理されている。**
- **鍵やトークンの長さ、パラメータの使い方、リクエストやデータの検証方法など、より具体的な指定がなされている。**
- **PKCEへの対応が必須に。ネイティブアプリはカスタムスキームではなく App Links, Universal Links への対応が必要に。**

© 2019 OGIS-RI Co., Ltd.

Part 1: Read-Only API Security Profile ③

Draft-06の内容を抜粋

#	Authorization Server への要求事項（認証されたユーザーの識別子を応答するときの追加要求事項）
1	[OIDC] 3.1.2.1節にあるとおりの認証要求をサポートする。(SHALL)
2	[OIDC] 3.1.2.2節にあるとおりの認証要求の検証を行なう。(SHALL)
3	[OIDC] 3.1.2.2節および3.1.2.3節にあるとおりユーザーを認証する。(SHALL)
4	[OIDC] 3.1.2.4節および3.1.2.5節にあるとおり認証結果に応じて認証応答を行なう。(SHALL)
5	[OIDC] 3.1.3.2節にあるとおりトークン要求を検証する。(SHALL)
6	要求された scope に openid が含まれている場合は、[OIDC] 3.1.3.3節にあるとおり、トークン応答の中で認証されたユーザーに対応するsub値を持つ（オプションでacr値も含めた）IDトークンを発行して応答する。(SHALL)

- **OAuth 2.0 [RFC6749] の基本仕様に加え、OAuthシリーズの追加仕様、OpenID Connectで定義された仕様などを併用するように整理されている。**
- **鍵やトークンの長さ、パラメータの使い方、リクエストやデータの検証方法など、より具体的な指定がなされている。**
- **PKCEへの対応が必須に。ネイティブアプリはカスタムスキームではなく App Links, Universal Links への対応が必要に。**

© 2019 OGIS-RI Co., Ltd.

Part 2: Read and Write API Security Profile ①

Draft-06の内容を抜粋

#	Authorization Server への要求事項
1	[OIDC] 6章にあるとおり、request あるいは request_uri パラメータにJWS署名のJWTを使用する。(SHALL)
2	response_type の値には、code id_token もしくは code id_token token を使用する。(SHALL)
3	認可リクエストに対するレスポンスの分離署名として IDトークンを応答する。(SHALL)
4	クライアントが（認可要求の中で）state 値を提供した場合は、state 値を保護するため、IDトークンに state 値のハッシュである s_hash を含める。(SHALL) 認可エンドポイントから返される IDトークン に s_hash が存在する場合は、トークンエンドポイントから返されるIDトークンでは (s_hashを) 省略できる。
5	記名式 (Holder of Key) の認可コード、アクセストークン、リフレッシュトークンのみを発行する。(SHALL)
6	記名式 (Holder of Key) の仕組みには [OAUTB] あるいは [MTLS] を用いる。(SHALL)
7	[X.1254] に定義された LoA 3 以上のユーザー認証を要求する。(SHALL)
8	署名付きのIDトークンをサポートする。(SHALL)
9	署名付きかつ暗号化されたIDトークンをサポートすることが望ましい。(SHOULD)

- **OpenID Connectへの対応、オプションとして定義されている高度な仕様への対応**
- **IDトークンを使った認可レスポンスへの署名（at_hash, c_hash, s_hashへの対応）**
- **策定中のOAuth追加仕様 (OAUTB, MTLS) の実装**
- **多要素認証の対応**

© 2019 OGIS-RI Co., Ltd.

Part 2: Read and Write API Security Profile ②

Draft-06の内容を抜粋

#	Authorization Server への要求事項
10	リクエストもしくは request_uri を通じて渡された全てのパラメータは、署名されたリクエストオブジェクト中に存在しなければならない。(SHALL)
11	7章で説明する リクエストオブジェクトエンドポイント をサポートしても良い。(MAY)
12	パブリッククライアントをサポートするときは、[RFC7636] の S256コードチャレンジ方式 はパブリッククライアントのみで使用する。(SHALL)
13	リクエストオブジェクトは exp クレームを含んでいなければならない。(SHALL)
14	トークンエンドポイントでは以下のいずれかの方法を用いてコンフィデンシャルクライアントを認証する。(SHALL)（この項目は FAPI Part 1 の 5.2.2.4節 の内容を上書きしている） 1. [MTLS] の 2章 で指定されている OAuthクライアント認証のためのTLS相互認証 2. [OIDC] の 9章 で指定されている private_key_jwt

- **OpenID Connectへの対応、オプションとして定義されている高度な仕様への対応**
- **IDトークンを使った認可レスポンスへの署名（at_hash, c_hash, s_hashへの対応）**
- **策定中のOAuth追加仕様 (OAUTB, MTLS) の実装**
- **多要素認証の対応**

© 2019 OGIS-RI Co., Ltd.

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-07]	○	○	○
⑥	OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens [MTLS] [draft-ietf-oauth-mtls-11]	○	○	○
⑦	JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)	○	—	○

© 2019 OGIS-RI Co., Ltd.

すべてのAPIが金融向けのグレードである必要はない

- FAPI の Profile は主に金融API向け
- APIが提供する機能、情報のリスクを評価してどこまで対応するかを決める
- 対応策は、FAPI Profile が参考になる

R/O Prof. LoA 2

R/W Prof. LoA 3

- 不便, 苦痛, または社会的地位やレピュテーションの毀損
- 経済的損失または機関の負債
- 組織や組織のプログラム、公共の利益への損害
- 許可されていないセンシティブ情報の公開
- 個人の安全
- 民事または刑事上の違反

Table 6-2 – Potential impact at each level of assurance

Possible consequences of authentication failure	Potential impact of authentication failure by LoA			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min*	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the organization, its programs or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High

* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High.

引用元: ITU-T Recommendation X.1254 Entity authentication assurance framework, p7 (2012年9月)

© 2019 OGIS-RI Co., Ltd.

利用者の意思に基づき
データー・機能を提供するための

同意取得・同意画面のあり方

© 2019 OGIS-RI Co., Ltd.

サービスを選ぶときの利用者の心理

便利そう!

お得そう!

みんな使ってるから自分も!

何の情報が渡される？

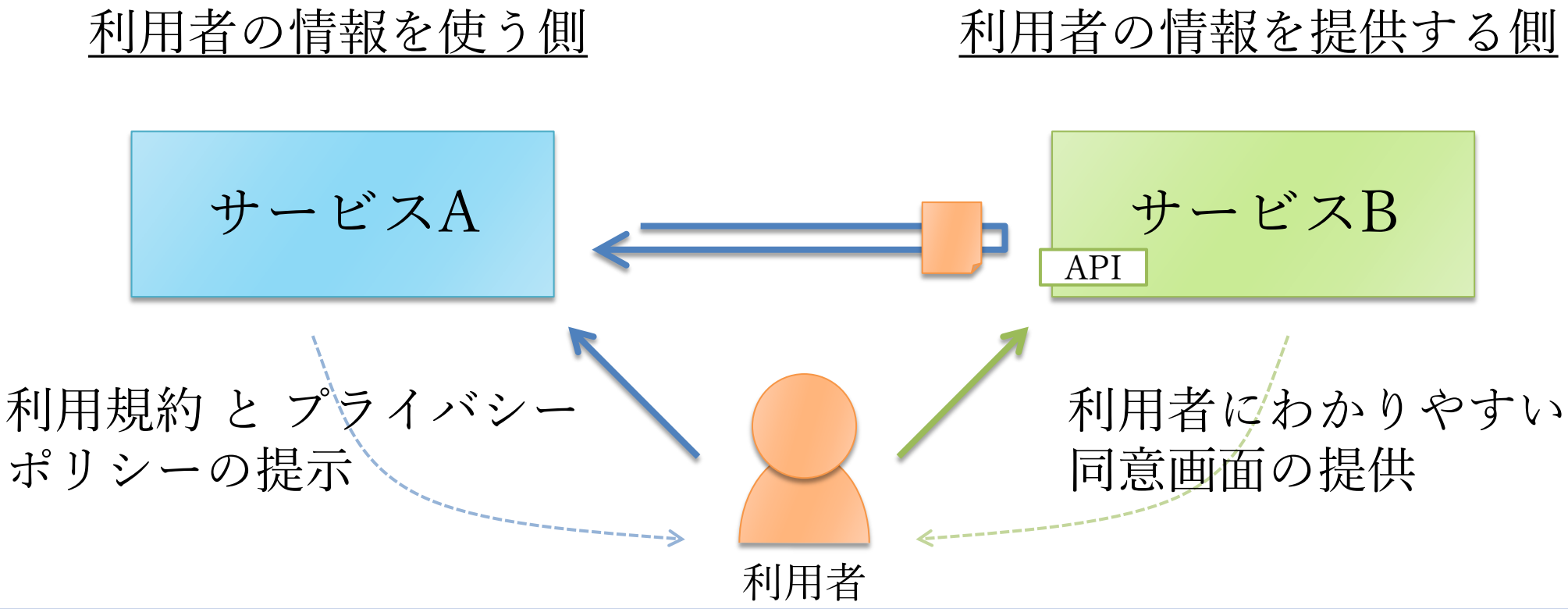
その情報は何に使うの？

情報は安全に管理される？

© 2019 OGIS-RI Co., Ltd.

情報の使用と管理について適切に利用者に伝える

- 利用規約 と プライバシーポリシー
- 情報取得時点での利用者への提示と確認（同意）



© 2019 OGIS-RI Co., Ltd.

利用者に何を伝えるか

ロ 法令・ガイドライン、業界団体等での検討結果、などを踏まえ、デザインしていく。

（例）「オープン API のあり方に関する検討会報告書」
3.4 利用者保護原則　3.4.2 説明・表示、同意取得

c 銀行は、トークン発行に当たって、少なくとも以下の点について、わかりやすく画面表示のうえ、利用者の同意を求めることが必要である。

- アクセス権限を付与するAPI接続先の名称
- API 連携するサービス等の名称
- 付与する権限の内容・範囲
- 付与する権限の有効期限
- 付与した権限の削除、解除方法
- その他注意喚起が必要な事項

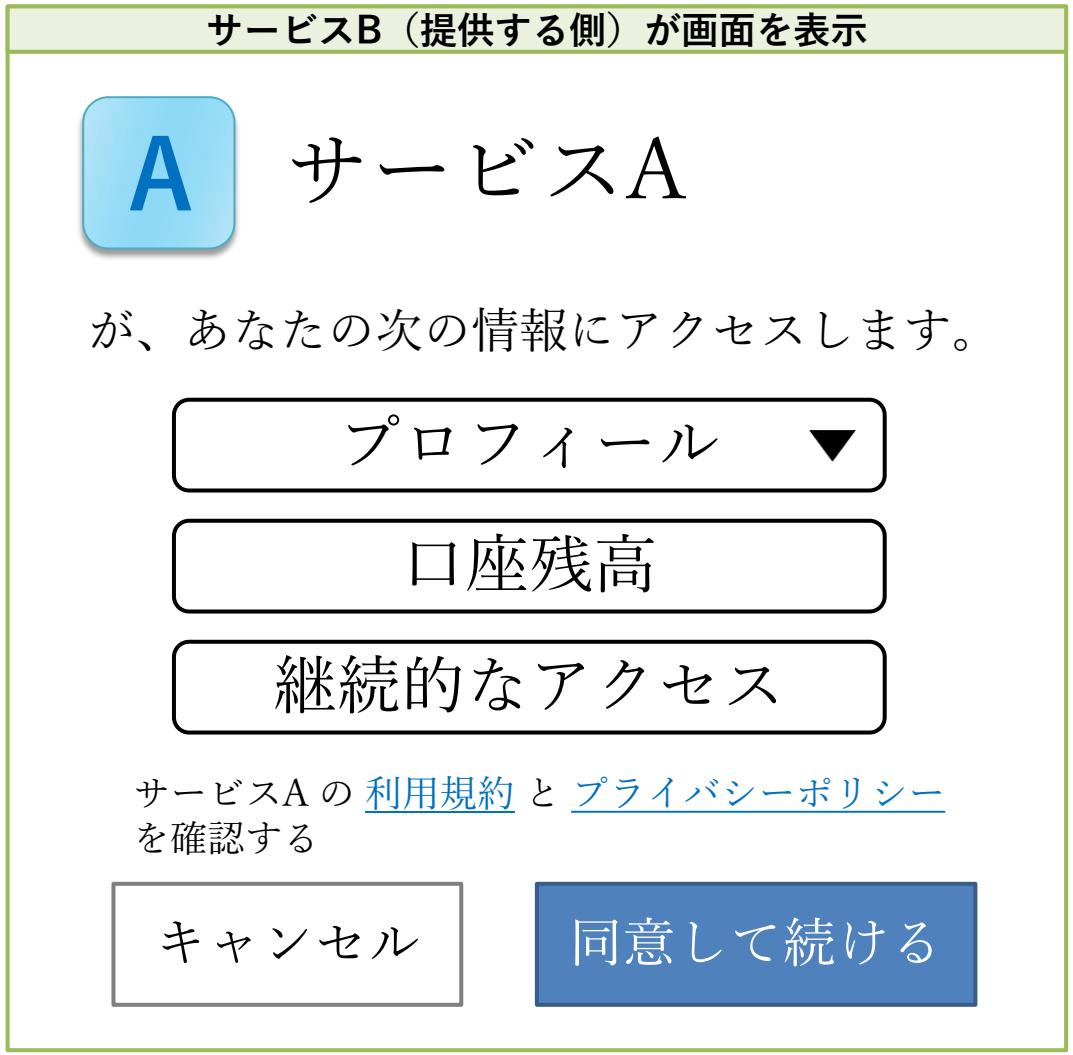
d API 接続先は、サービス提供に当たって、少なくとも以下の点について、わかりやすく画面表示のうえ、利用者の同意を求めることが必要である。

- 個人情報保護法にもとづく取得情報の利用目的、共有範囲（第三者提供の有無）
- 取得した情報の削除に関する事項
- サービス利用上の制限
- その他注意喚起が必要な事項

引用元: https://www.zenginkyo.or.jp/fileadmin/res/abstract/council/openapi/openapi_report_1.pdf

© 2019 OGIS-RI Co., Ltd.

同意画面の構成例



どのサービスに情報を提供するか が視覚的に確認できる。

何の情報を提供するかを、利用者が理解しやすい表現で提示する。

1回だけの提供か、継続的な提供かを確認できる。

サービスA の利用規約とプライバシーポリシーへの導線を作り、利用者が確認しやすい環境を提供する。

情報提供を拒否することができる。

© 2019 OGIS-RI Co., Ltd.

同意画面の構成例

APIを提供するサービスサイトの特性・デザインに合わせてUIを作る必要がある。

どのサービスに情報を提供するか
が視覚的に確認できる。

何の情報を提供するかを、利用者が
理解しやすい表現で提示する。

1回だけの提供か、継続的な提供か
を確認できる。

サービスA の利用規約とプライバシーポリシーへの
導線を作り、利用者が確認しやすい環境を提供する。

情報提供を拒否することができる。

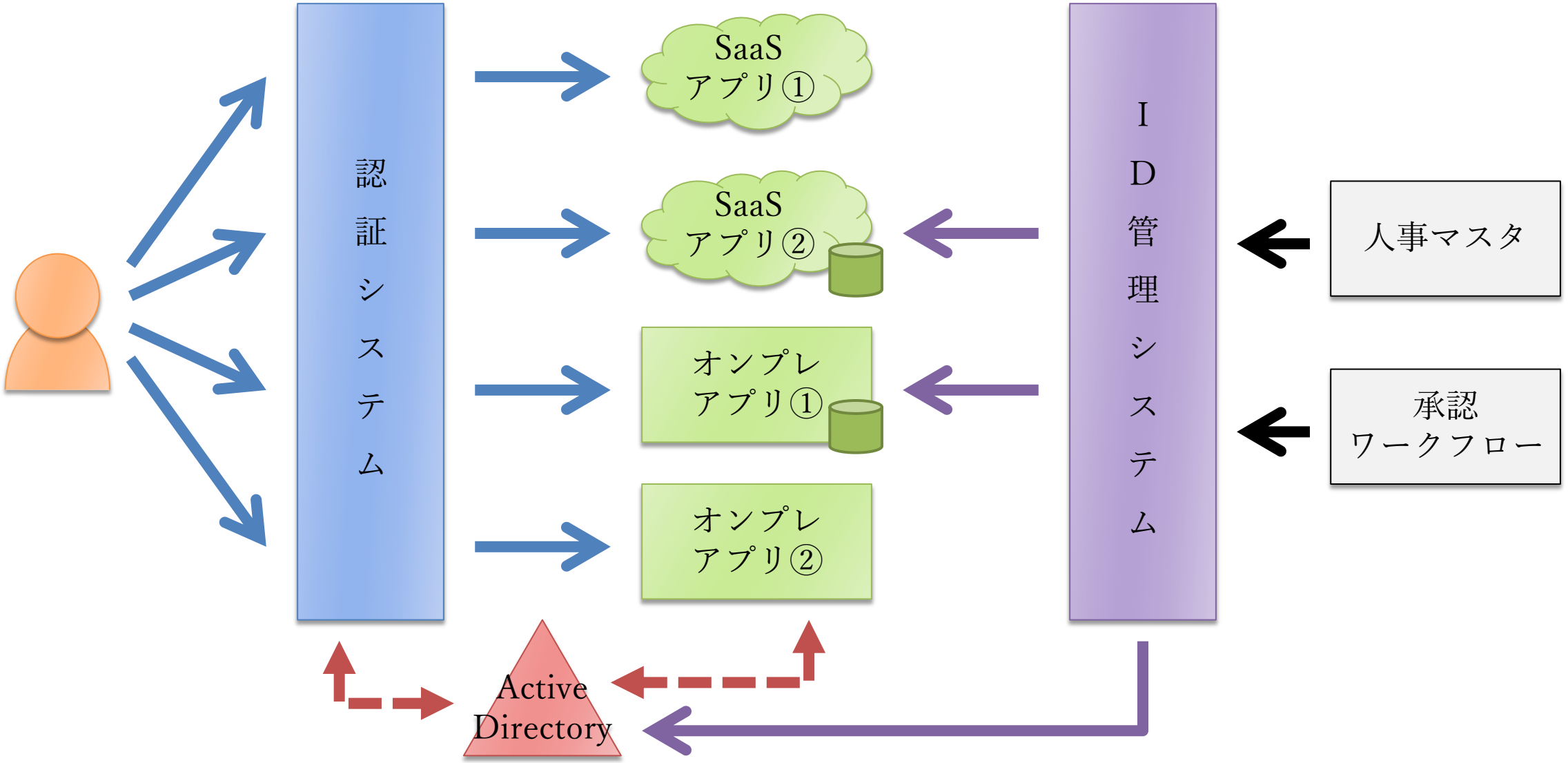
© 2019 OGIS-RI Co., Ltd.

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

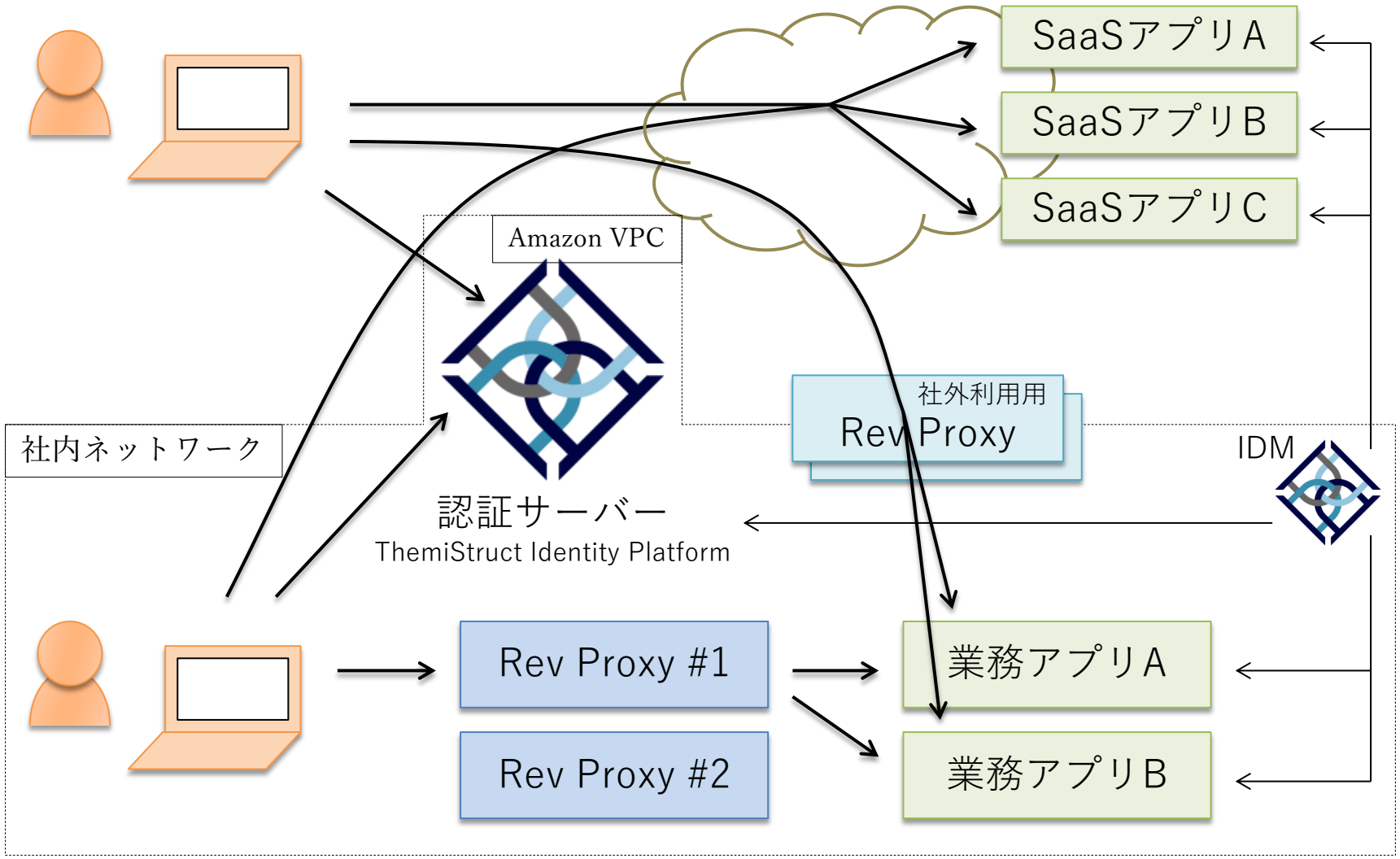
© 2019 OGIS-RI Co., Ltd.

認証基盤の基本形



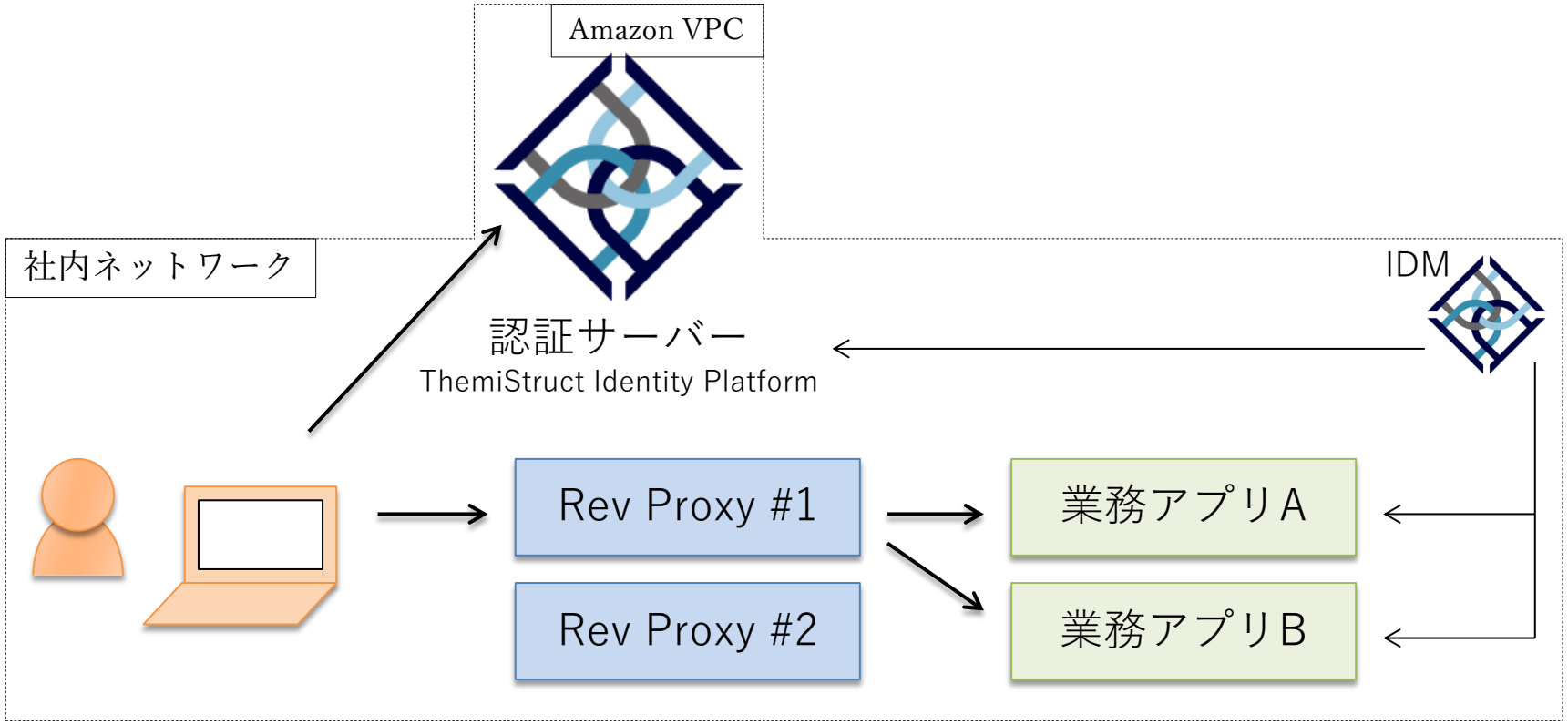
© 2019 OGIS-RI Co., Ltd.

「社内統合認証基盤」の構築イメージ



© 2019 OGIS-RI Co., Ltd.

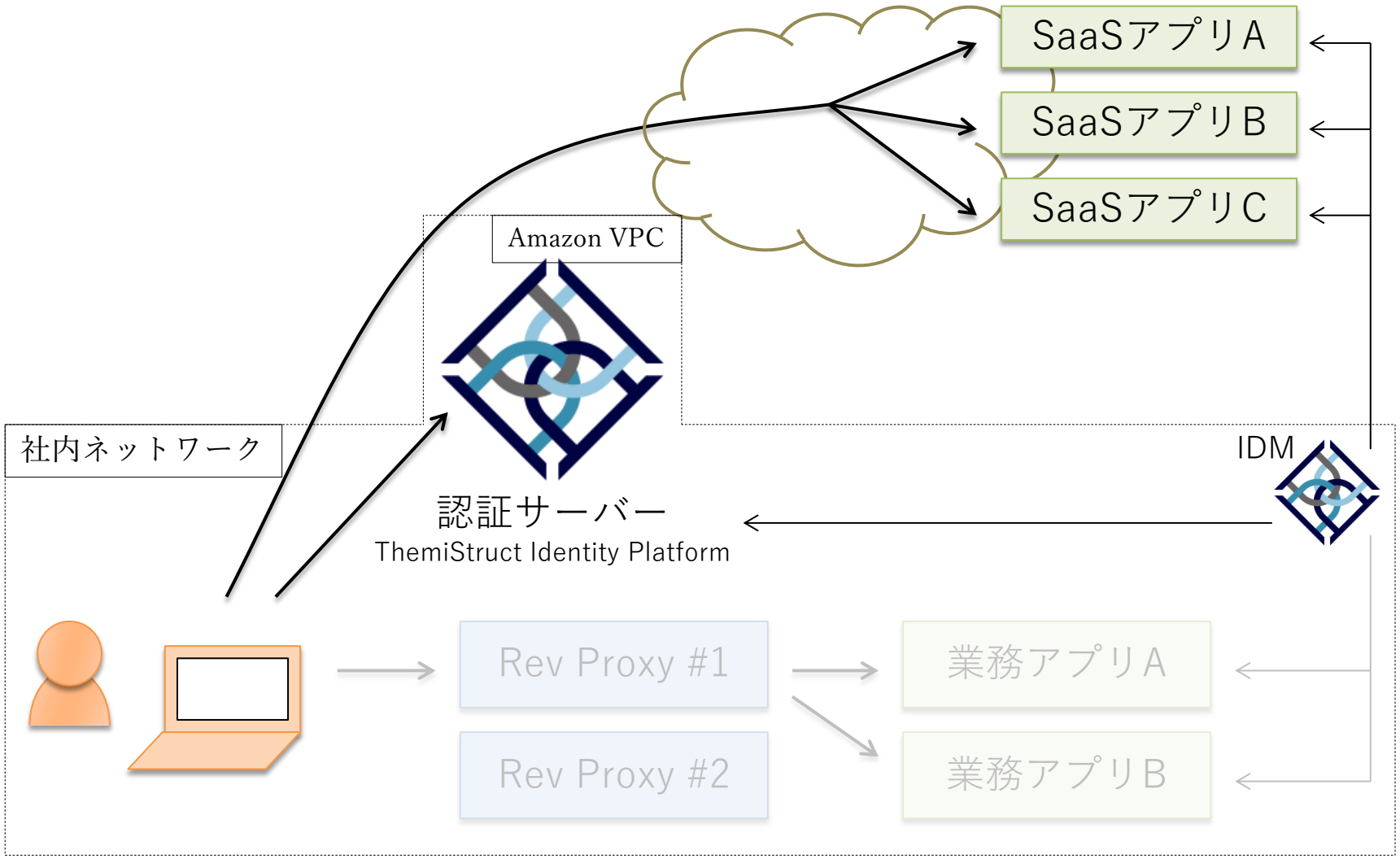
社内に配置されたシステムへのSSOを実現する



- ✓ 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。

© 2019 OGIS-RI Co., Ltd.

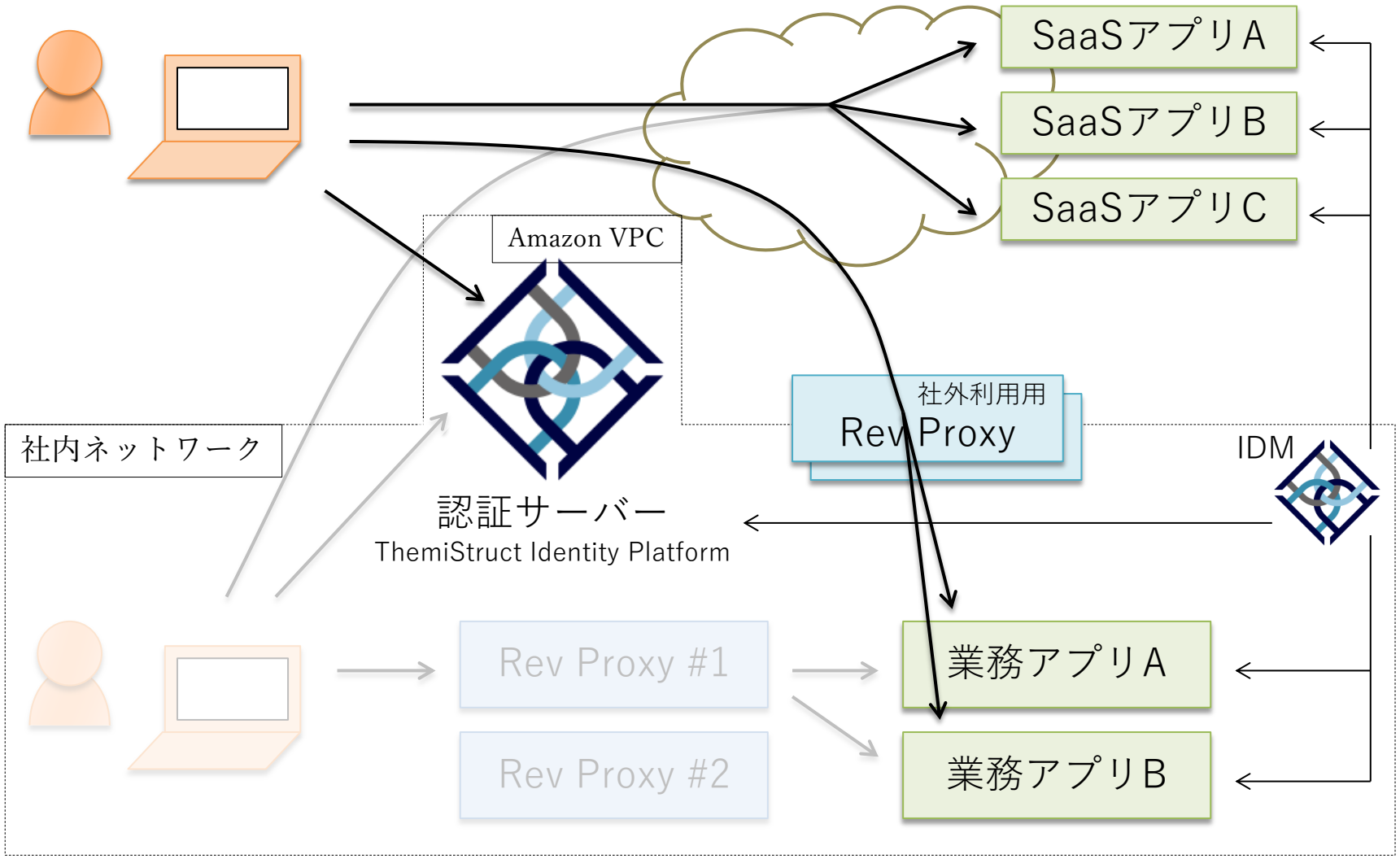
クラウドサービスへのアクセスを管理する



- ✓ 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。

© 2019 OGIS-RI Co., Ltd.

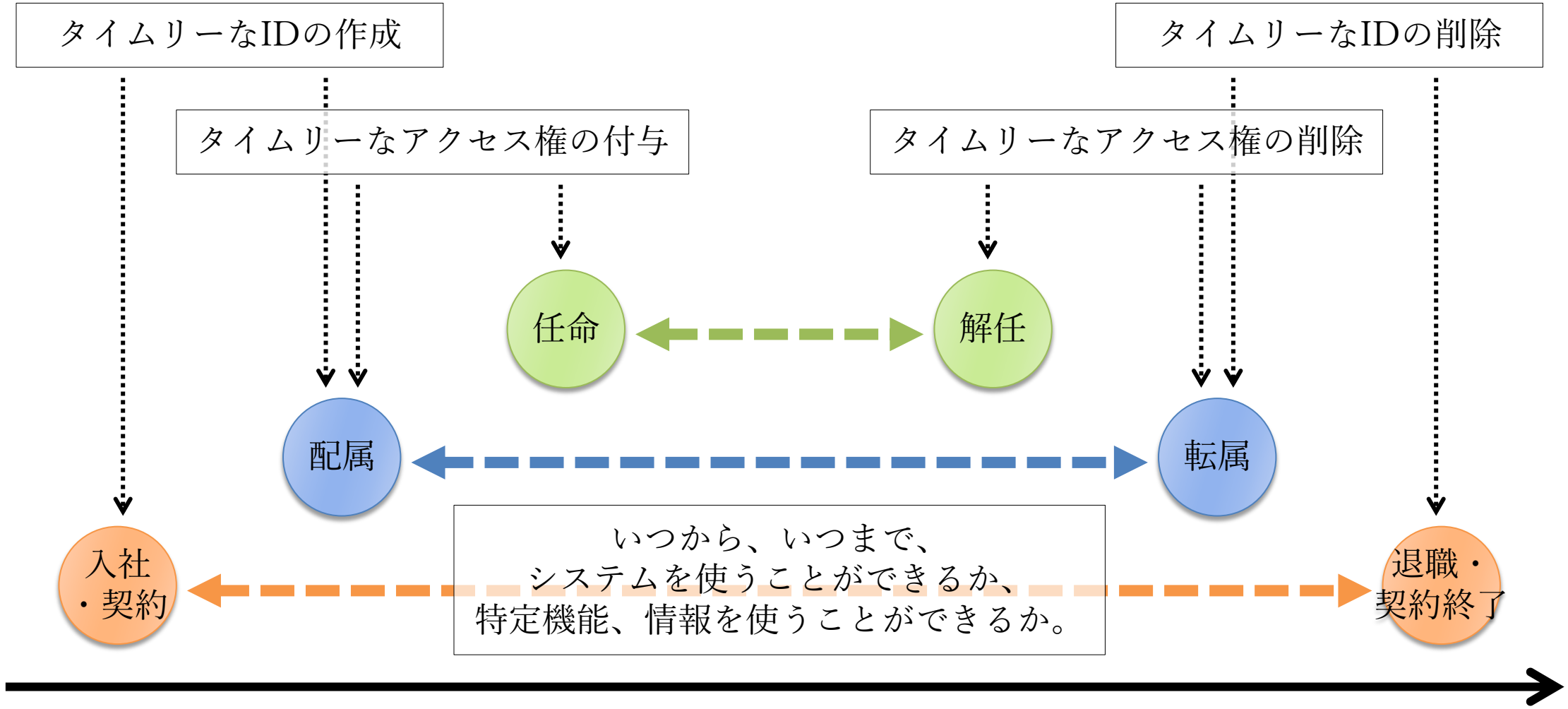
社外からのシステム利用を実現する



- ✓ 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。

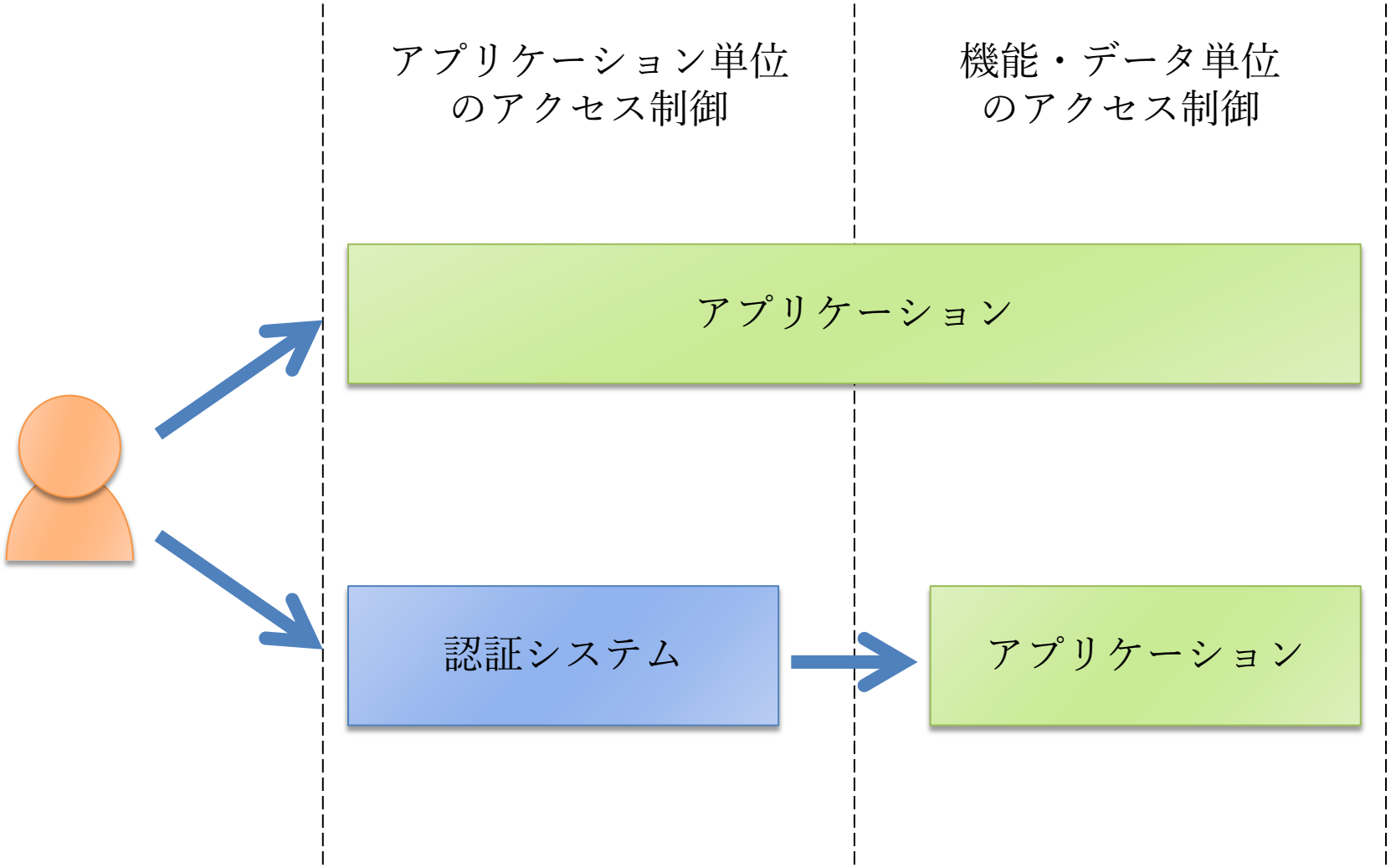
© 2019 OGIS-RI Co., Ltd.

企業内のIDライフサイクル



© 2019 OGIS-RI Co., Ltd.

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

© 2019 OGIS-RI Co., Ltd.

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。

© 2019 OGIS-RI Co., Ltd.

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

© 2019 OGIS-RI Co., Ltd.

部門認証基盤を構築して運用する

© 2019 OGIS-RI Co., Ltd.

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

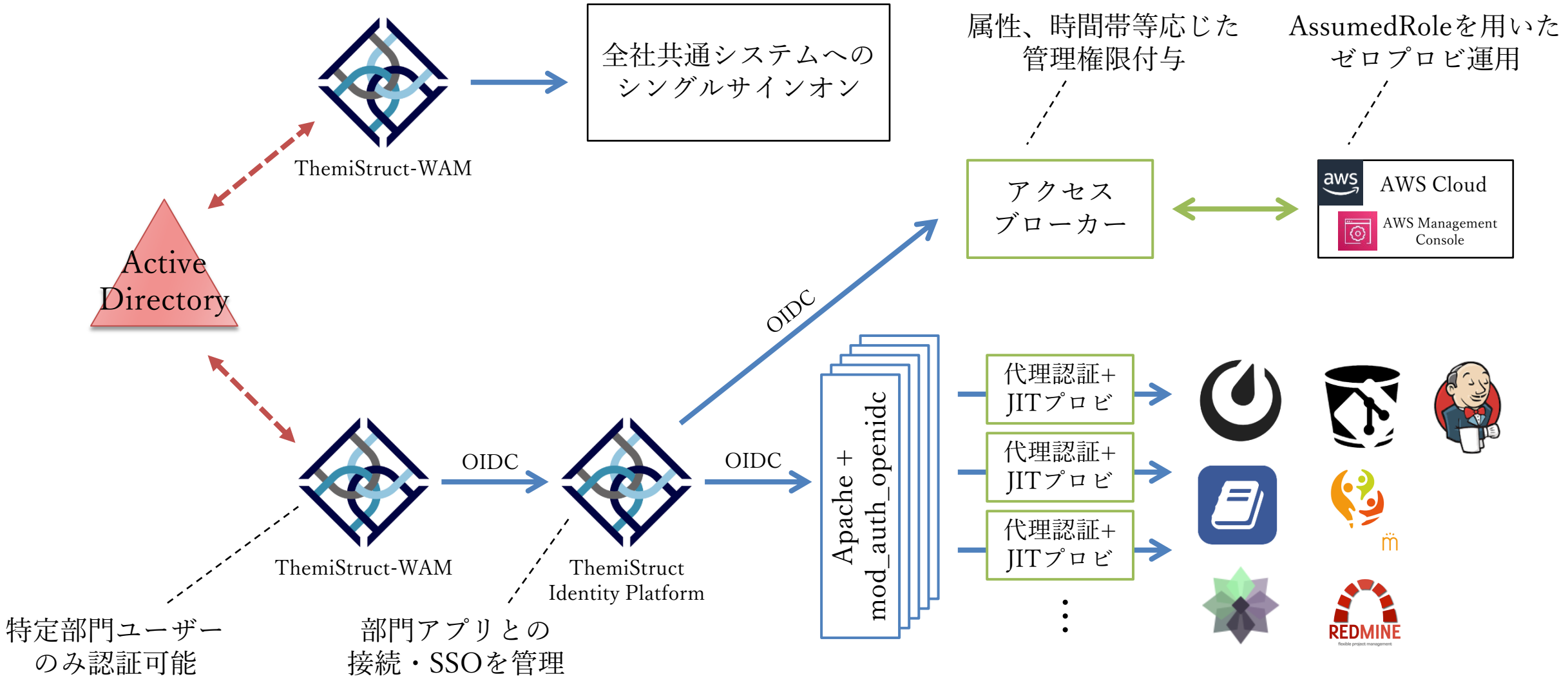
当社 全社共通の認証基盤で管理

- **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

© 2019 OGIS-RI Co., Ltd.

全社リポジトリと連携した部門認証基盤を構成



© 2019 OGIS-RI Co., Ltd.

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。

© 2019 OGIS-RI Co., Ltd.

当社ソリューションのご紹介

© 2019 OGIS-RI Co., Ltd.

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® アイデンティティプラットフォーム

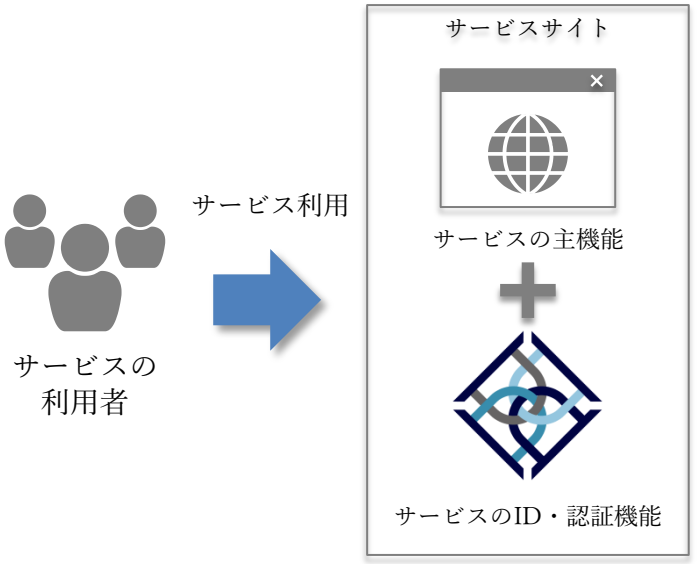
OAuth 2.0 に対応した
APIエコノミー時代に求められる
統合認証パッケージ

© 2019 OGIS-RI Co., Ltd.

統合認証パッケージ ThemiStruct Identity Platform

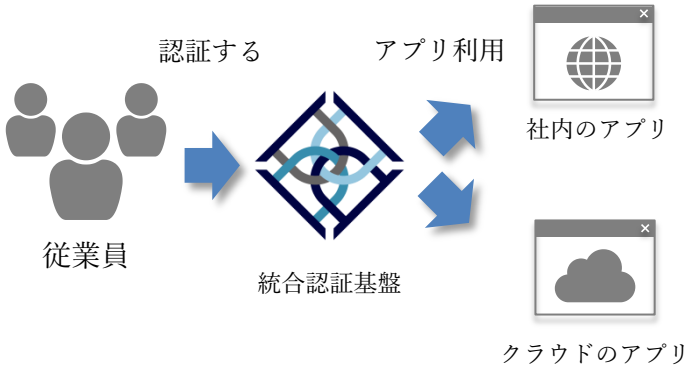
ThemiStruct Identity Platform は、ITシステム利用者のアイデンティティ管理と認証の機能を提供します。顧客向けにサービスを展開したり、従業員向けにアプリケーションを展開する際に必要となる、共通ID基盤の構築に活用いただけます。

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

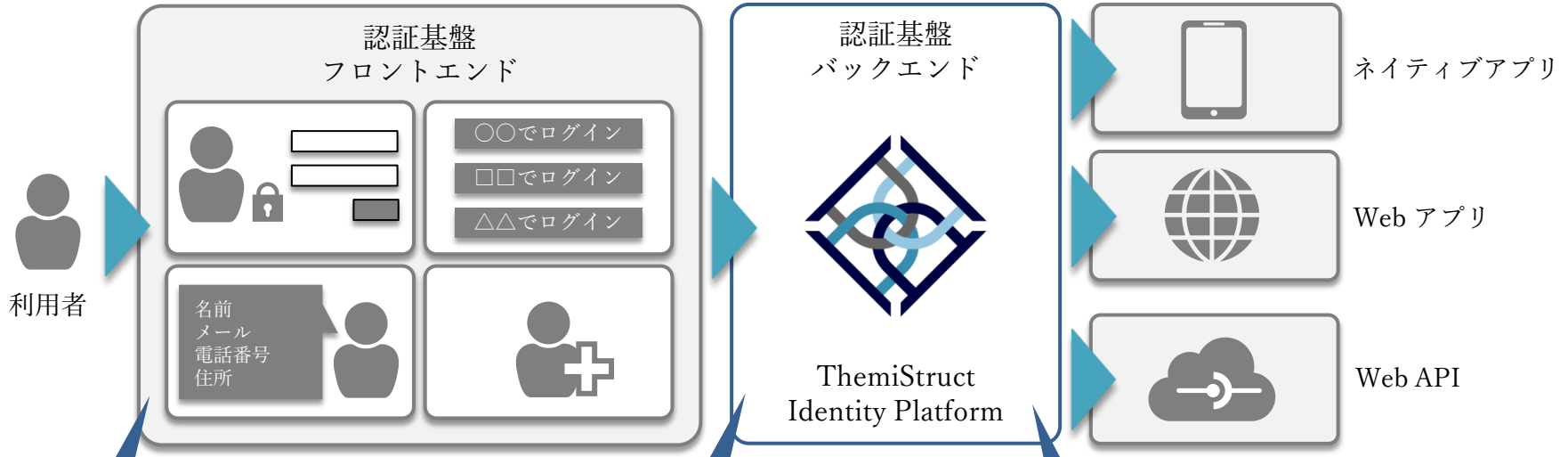


エンタープライズアプリ群の
SSOやアクセス制御の基盤として利用

© 2019 OGIS-RI Co., Ltd.

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。

© 2019 OGIS-RI Co., Ltd.

『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。

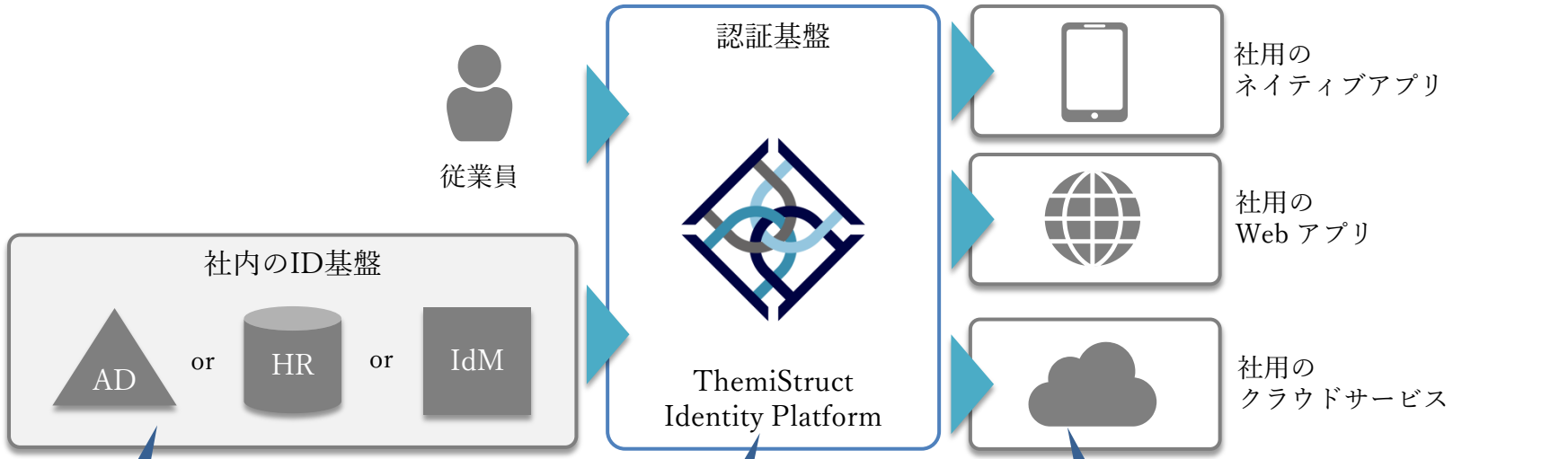
ロ　短期間での導入が可能

- 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。

© 2019 OGIS-RI Co., Ltd.

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。

© 2019 OGIS-RI Co., Ltd.

『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。

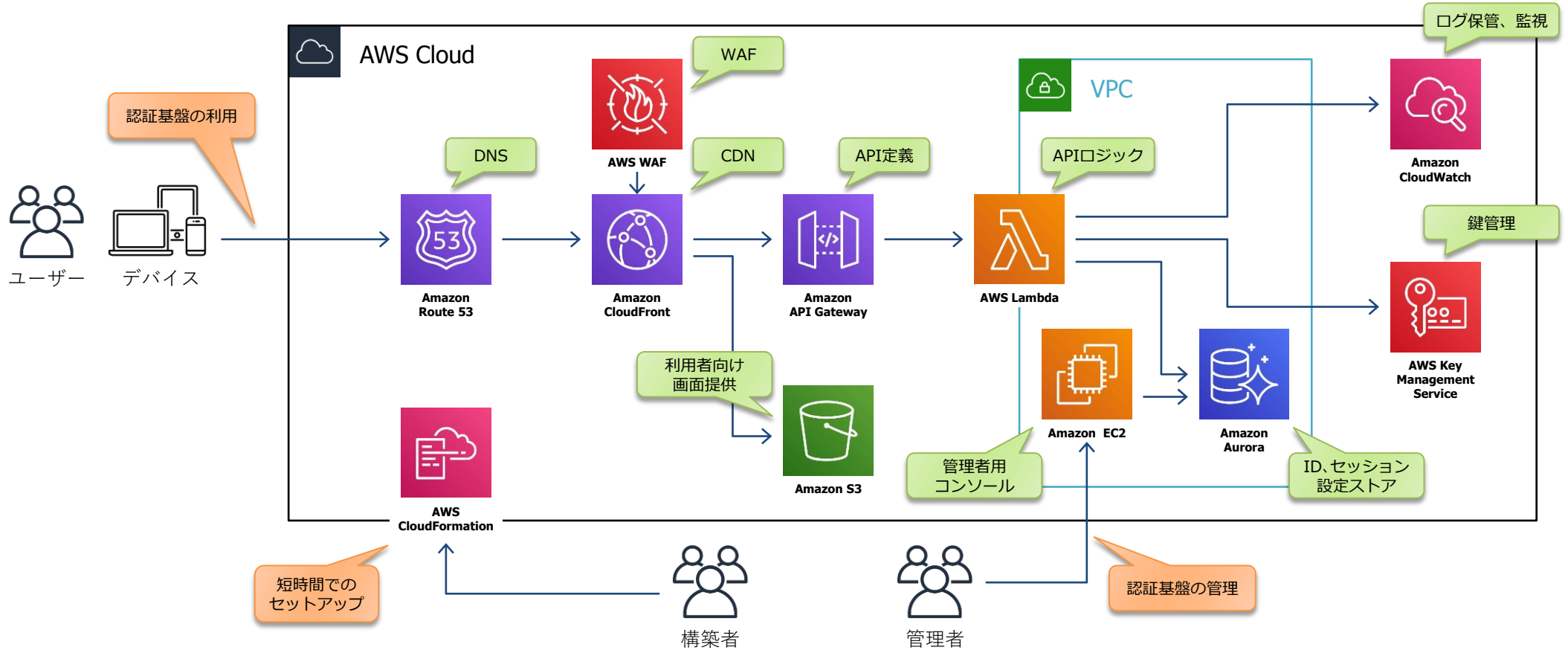
ロ　既存のID基盤と統合

- 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。

© 2019 OGIS-RI Co., Ltd.

サーバーレスアーキテクチャを採用

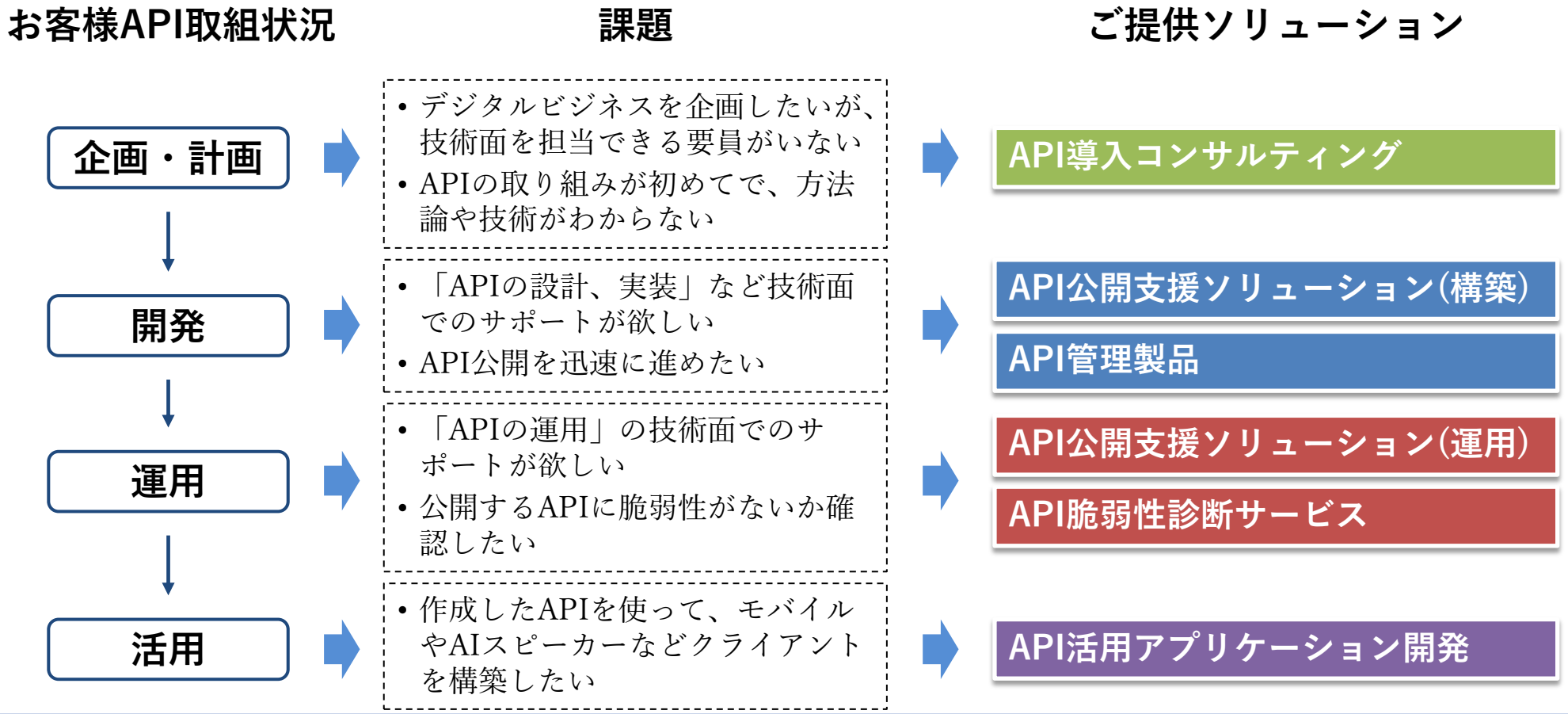
ThemiStruct Identity Platform は AWS Cloud 上で稼働し、高可用・スケーラブルな認証基盤を実現することができます。また、以下の構成のセットアップを約2時間で完了できるインストーラを提供しています。



© 2019 OGIS-RI Co., Ltd.

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



© 2019 OGIS-RI Co., Ltd.

まとめ

© 2019 OGIS-RI Co., Ltd.

まとめ

- 認証基盤のユースケースは、社内統合認証にとどまらず、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。
- OpenID Connect, SAMLといったID連携の標準技術に加え、OAuth 2.0 の標準仕様群に継続的に対応していく必要がある。
- 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 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。

© 2019 OGIS-RI Co., Ltd.

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

© 2019 OGIS-RI Co., Ltd.