ThemiStruct
テミストラクト

APIを保護する、認証とアクセス管理の考え方

株式会社オージス総研
サービス事業本部 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 （やはた たかし）

- 株式会社オージス総研
- テミストラクト関連サービス 東日本エリア責任者
- テミストラクト商品開発 リードアーキテクト

- OpenAMコンソーシアム 理事
- OpenIDファウンデーション・ジャパン
  Enterprise Identity WG リーダー

- twitter.com/paoneJP
- facebook.com/takashi.yahata
- https://paonejp.github.io
- OpenID, OAuth, SCIM, Python, OpenAM, OpenIDM, …

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）
Identity Platform AWS対応版

クラウド、IoT時代の
“All in one”
認証プラットフォーム

統合認証ソリューションに取り組んで15年

- 2001年ごろから基盤部門で
- セキュリティソリューションの一環として
- 2005年からはオープンソースソフトウェアをベースに開発をし
- 2009年からThemiStructブランドを立ち上げて
- 2013年からは専門部隊として

なぜ認証基盤を作るのか？

認証基盤を作るメリット

① 利用者が便利になる

- 作業効率の向上
- IT活用の促進

② セキュリティレベルのばらつきがなくなる

- 開発者に依存したばらつき
- ユーザーに依存したばらつき

③ システム開発がしやすい

- アプリ毎の認証機能開発は不要
- サブシステムに分割した開発の実現

④ 認証方式の変更がやりやすい

- ID/パスワードを使った認証
- 多要素認証への対応
- 新しい方式への対応

セキュリティのための認証基盤

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。

「ビジネスのデジタル変容」が拍車をかける

モバイル、クラウド、
ソーシャルの活用

ビジネスプロセス
の自動連携

ユーザー情報の
活用と分析

多様なデバイスの
連携、活用

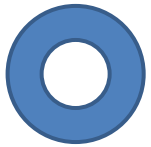
- ユーザー毎に最適化されたサービスの提供
- 業務効率の向上、提供スピードの向上

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

“Identity is the new perimeter.”

ロ ネットワーク型の境界防御が効かない時代になった

- 守るべき情報資産は壁 (Firewall) の外にある
- アクセスする主体は壁の中にも外にもいる

ロ アイデンティティを用いた情報へのアクセス管理が重要に

- アイデンティティによるアクセスの制御
- アイデンティティによるアクセスの監視

アイデンティティ？

エンティティ（実体）　認証　アイデンティティ　コンテキスト

・属性の集合
・コンテキスト毎に複数

ひとりの人

アクセスする実体を
システムが認識している
アイデンティティと
紐付けること ＝ 認証

社員番号: 1234567890
名前: 八幡 孝
所属コード: 7777
…

名前: 八幡 孝
所属: オージス総研
担当セッション: AAA
…

…

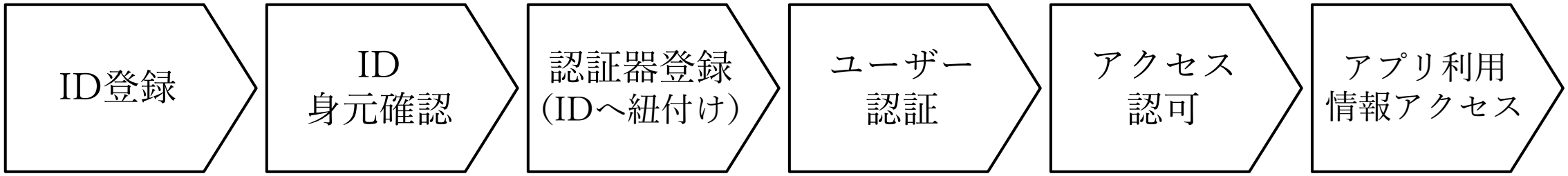
オージス総研
の社員として

講演者として

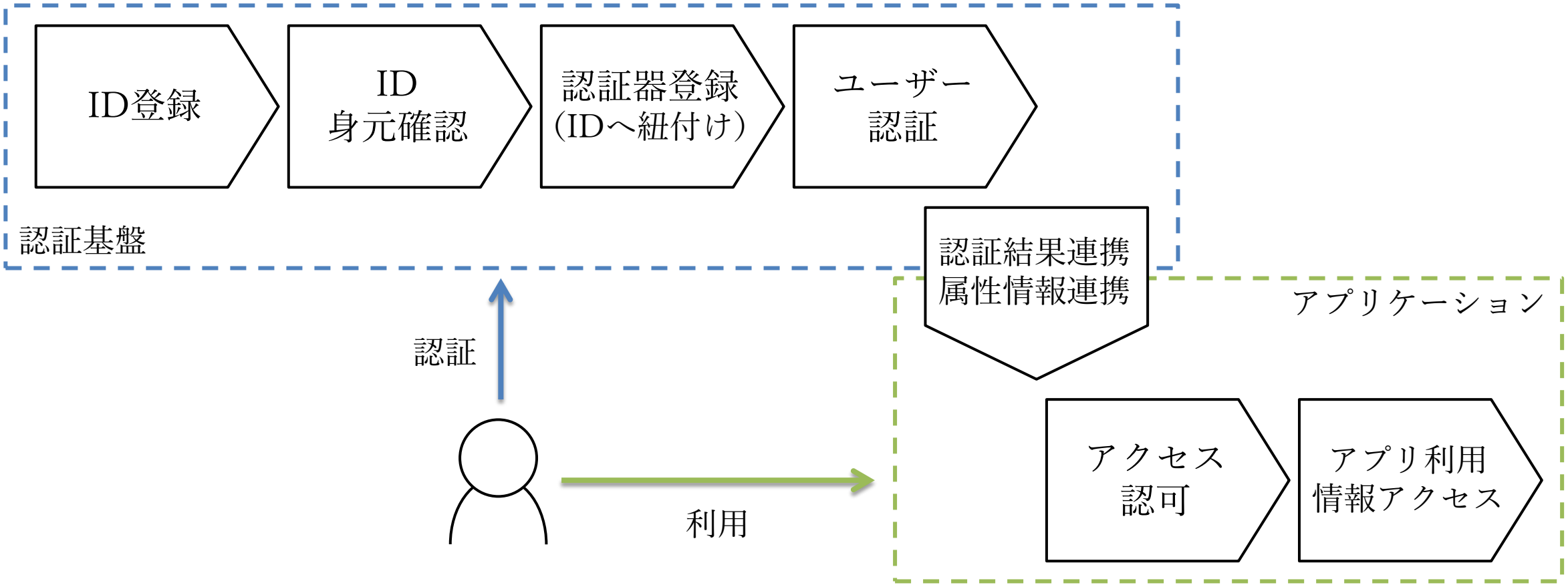
家族からみた

…

アイデンティティ＆アクセス管理のフロー



アイデンティティ＆アクセス管理のフロー



アプリケーションは何の情報を必要としているか？

□ ① ユーザーの認証状態の確認

- 識別子、認証方法、認証時刻、...

□ ② ユーザーが誰であるかの把握

- 名前、所属、役職、メール、...
- 名前、住所、電話、メール、...
- その人向けのサービス・機能を提供

□ ③ ユーザーの権限の判定

- 社員番号、組織番号、権限番号、...
- 契約中のサービスコード、
- その人がやれることを正確に確認

□ ④ 関連する情報の参照と利用

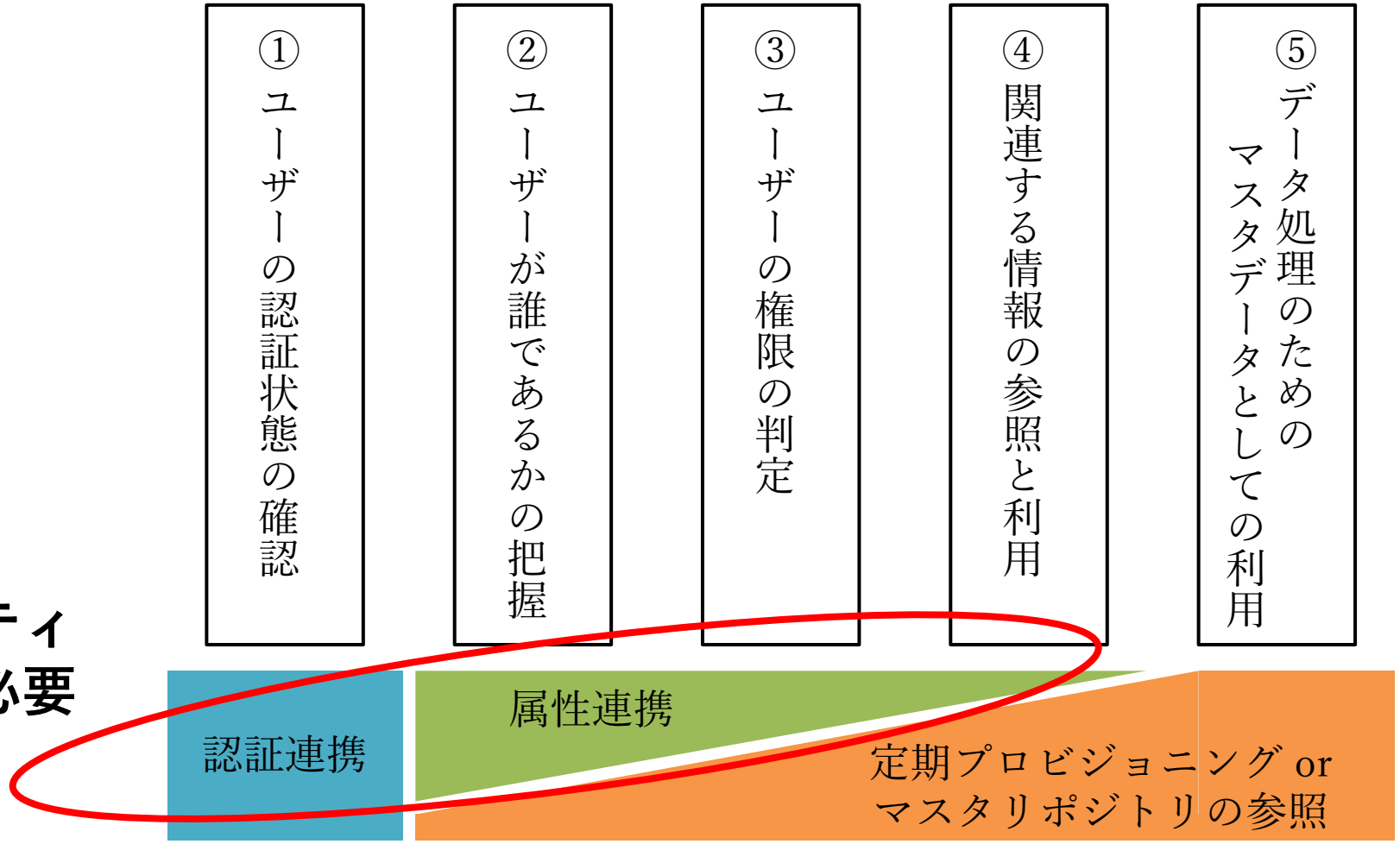
- 他ユーザーの属性、組織の属性、...

□ ⑤ データ処理のためのマスタデータとしての利用

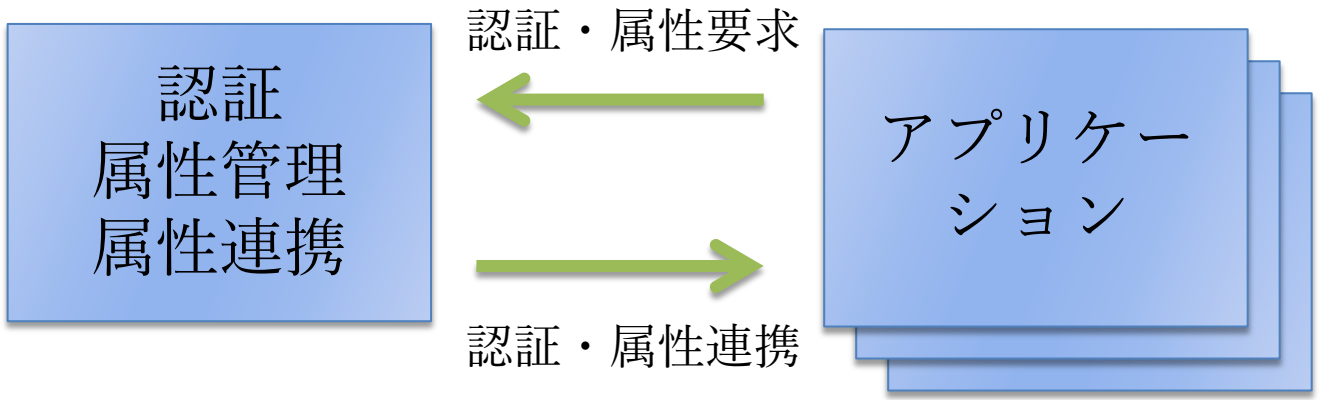
- 社員マスタ、組織マスタ、権限マスタ、...

アプリケーションに必要な情報を提供する方法

アイデンティティ連携の技術が必要



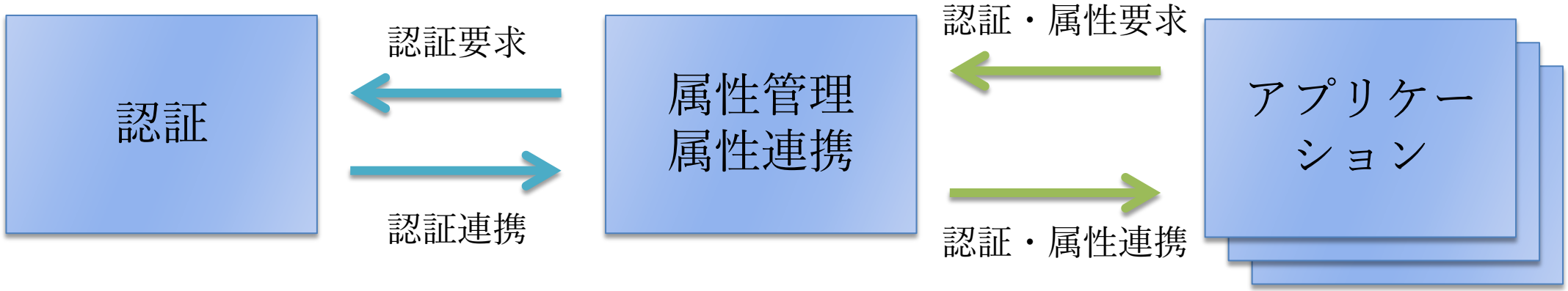
認証基盤を作る・サービスを展開する



ユーザーの認証
アプリが必要とする
属性の管理、提供、記録

ユーザーごとに
最適化された
サービスを提供

外部IdP活用で、より使いやすく、より管理しやすく



外部の信頼できる
認証システム(IdP)を利用

ドメインログオン、
Google, Facebook, ...

アプリが必要とする
属性の管理、提供、記録

ユーザーごとに
最適化された
サービスを提供

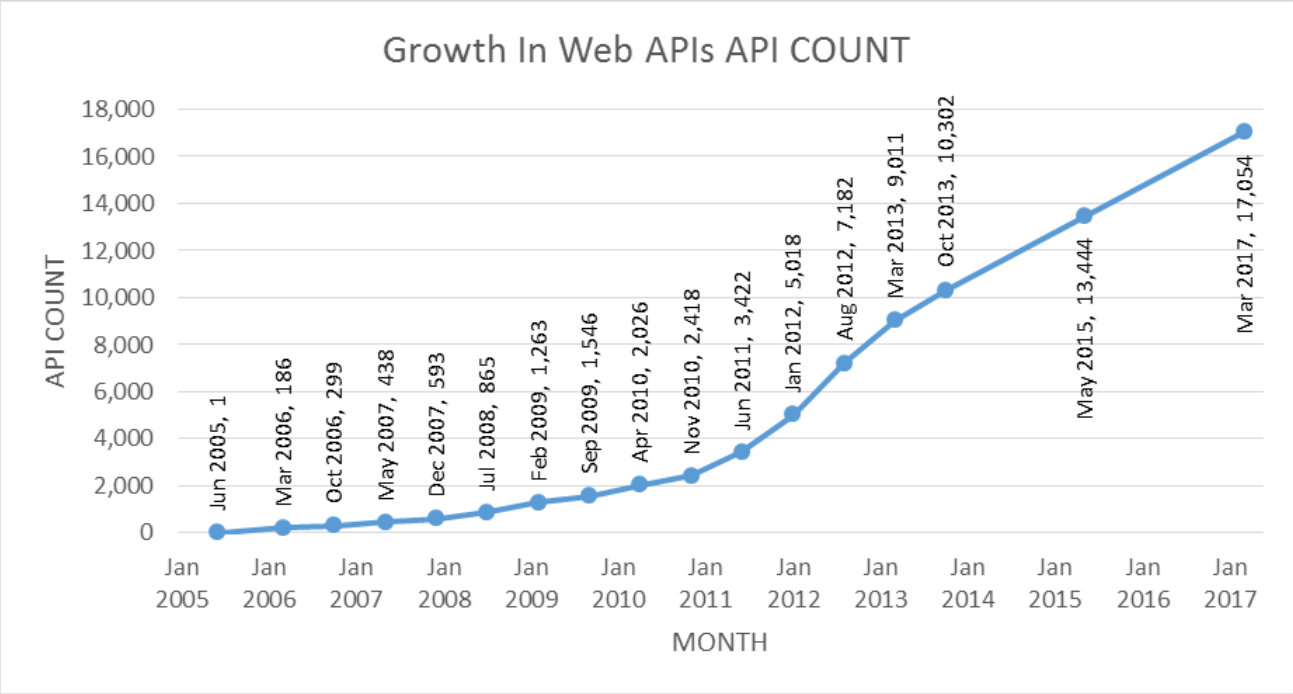
認証基盤 にとどまらず
アイデンティティプラットフォーム が
必要になっている

Web API のアクセス管理への展開

Web API の利用が広がっている

増加を続ける Web API（公開型）

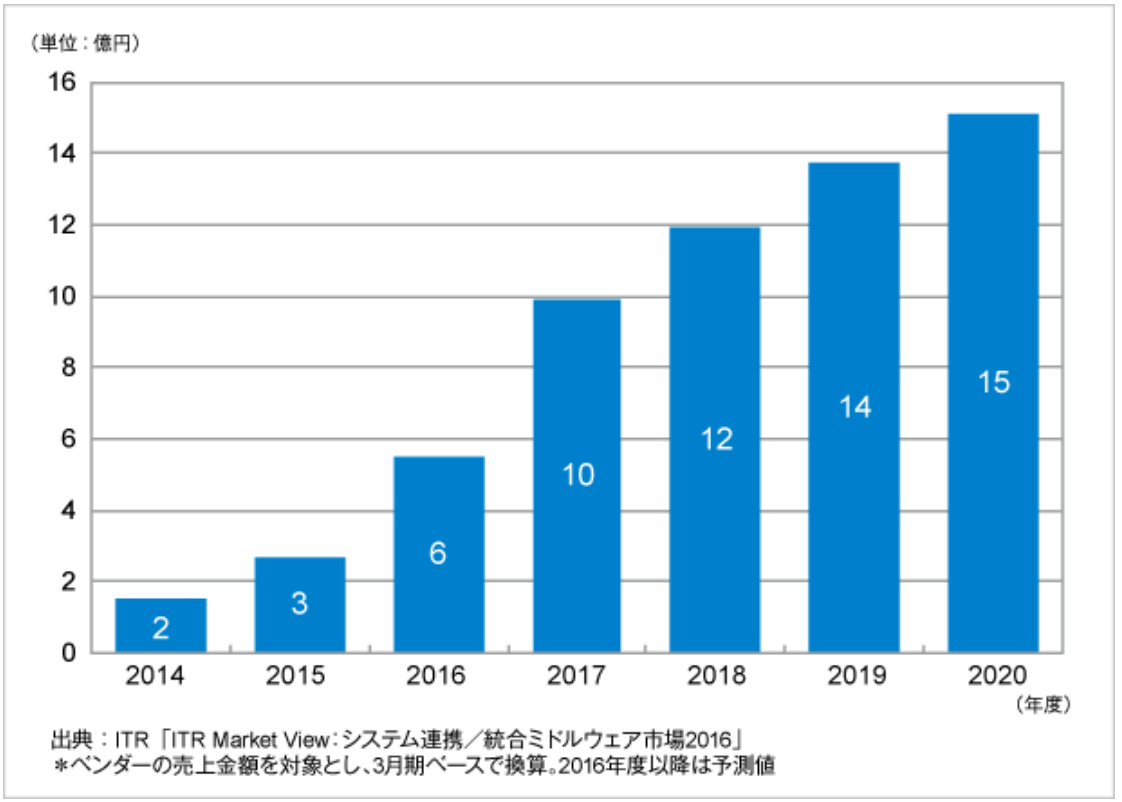
ProgrammableWebの情報を基に当社で加筆・グラフ化



引用元: https://www.programmableweb.com/api-research

「API管理市場売上金額推移および予測」

ITR社プレスリリースより



引用元: https://www.itr.co.jp/company/press/161213PR.html

Web API はデジタルビジネスの中核技術と言われている

> “デジタルイノベーションやデジタルトランスフォーメーションを実現するコア技術のひとつとして導入が進む”

ITR社「**ITRがAPI管理市場規模推移および予測を発表**」より

引用元: https://www.itr.co.jp/company/press/161213PR.html

> “まさしく、ハイブリッドクラウド環境におけるAPIエコノミーが、DXを実現しているのである。”

IDC Japan社「**～ デジタルトランスフォーメーション・エコノミーの萌芽 ～ 2017年 国内IT市場の主要10項目を発表**」より

引用元: http://www.idcjapan.co.jp/Press/Current/20161213Apr.html

Web API をどう保護するか？

□ Web API 利活用が広がる

- ➢ 内部での Web API 技術の利用
- ➢ 外部の Web API の活用
  - ● Closed Network での提供
  - ● Open Network での提供
- ➢ 外部への Web API の公開

□ ネットワーク型の境界防御だけでは保護できない

Web API でもアイデンティティを用いたアクセス管理が必要

Web API アクセス管理を考える切り口

□ クライアント（Web APIへのアクセス元）の認証

- ネットワーク、電子証明書、ベーシック認証、APIキー、…

OAuth の Client Authentication

□ 適切なアクセス権限の提供

- アクセスできる情報の範囲、行なえる操作の内容

OAuth の SCOPE へマッピング

□ 情報の所有者によるアクセスの許可

OAuth による認可（と OpenID Connect による認証）

外部の Web API を活用するには？

- **Web API でアクセスするリソースが企業に帰属するなら**
  - クライアント認証をしてアクセス
- **個人（従業員など）に帰属するなら**
  - 企業がアクセスを許可すればよい場合
    - クライアント認証をしてアクセス
  - 個人がアクセスを許可するべきものの場合
    - OAuthによる認可、個人の認証への対応が必要
    - 個人の認証は、自社の認証基盤からのSSOに対応することも検討

外部へ Web API を公開するには？

- Web API で提供するリソースが誰に帰属するかを分析する
- リソース毎に付与する権限を整理する
- リソース x 権限 を SCOPE にマッピングする
- OAuth による認可を実装する
- ユーザーを認証する機能を実装する
- ユーザーが使用している認証基盤とのSSOに対応する

アイデンティティ技術の標準化動向

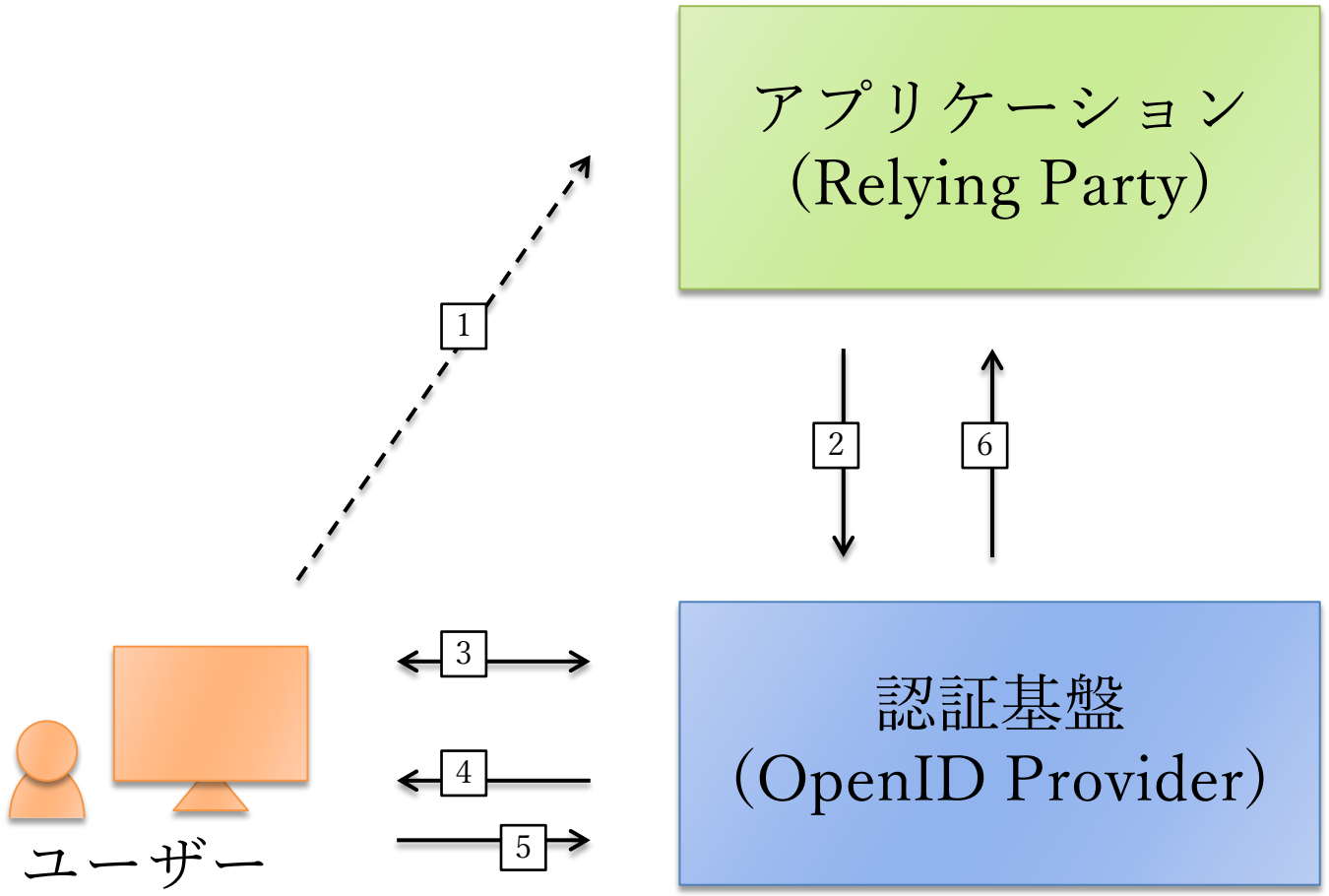
アイデンティティ連携を実現する標準技術たち

これらの技術は標準化が進み、製品・サービスへの実装も浸透している。

アイデンティティ連携を実現する標準技術たち

標準技術	概要
OpenID Connect	認証されたユーザーの情報（認証状態）を、サイト間、アプリケーション間で安全に伝達する仕組み。
SCIM	ユーザーに関する各種属性情報へのアクセス・操作をする仕組み。（属性情報の閲覧、検索、登録、更新、削除など）
OAuth	ユーザーの情報への特定のアクセス・操作を、情報を所有するユーザーの同意に基づき、アプリケーションに対して許可する仕組み。

OpenID Connect を使った認証連携（SSO）

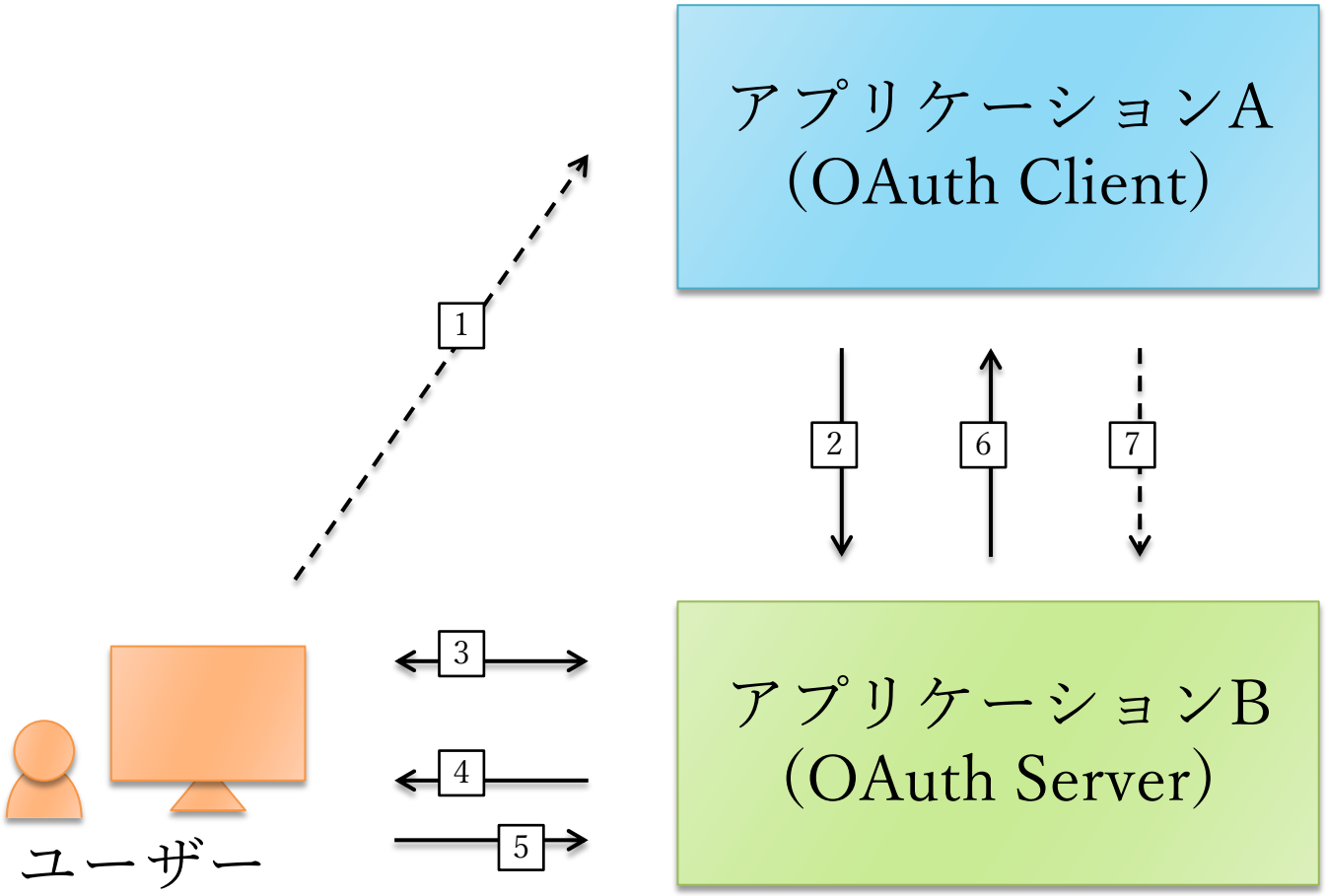


1. ユーザーがアプリケーションにアクセス
2. このユーザーは誰？
3. ユーザーを認証
4. このアプリにログインしようとしているけど良い？ユーザー名とメールアドレスを求めているけど渡しても良い？
5. いいよ
6. このユーザーは、○○さん。メールアドレスは△△。最後に認証したのはこの時刻。認証方法は□□。

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。

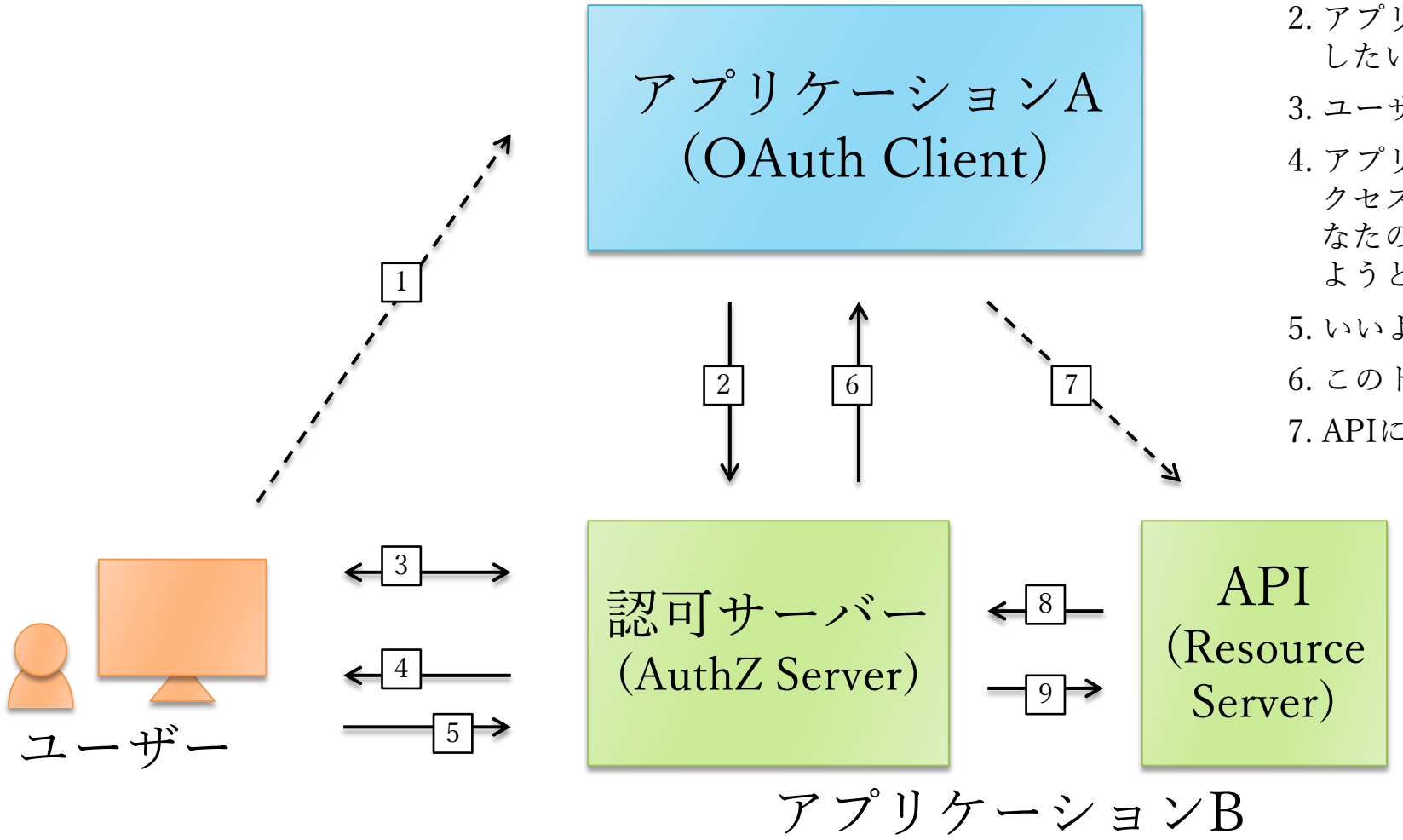
OAuth を使ったアプリケーション間API連携の許可 ①



1. ユーザーがアプリAにアクセス
2. アプリBのユーザー情報のAPIにアクセスしたい
3. ユーザーを認証
4. アプリAが、アプリBのあなたの情報にアクセスしようとしているけどいい？（あなたの代わりにアプリBでこんな操作しようとしているけどいい？）
5. いいよ
6. このトークンでAPIにアクセスして
7. APIにアクセス

※ 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。

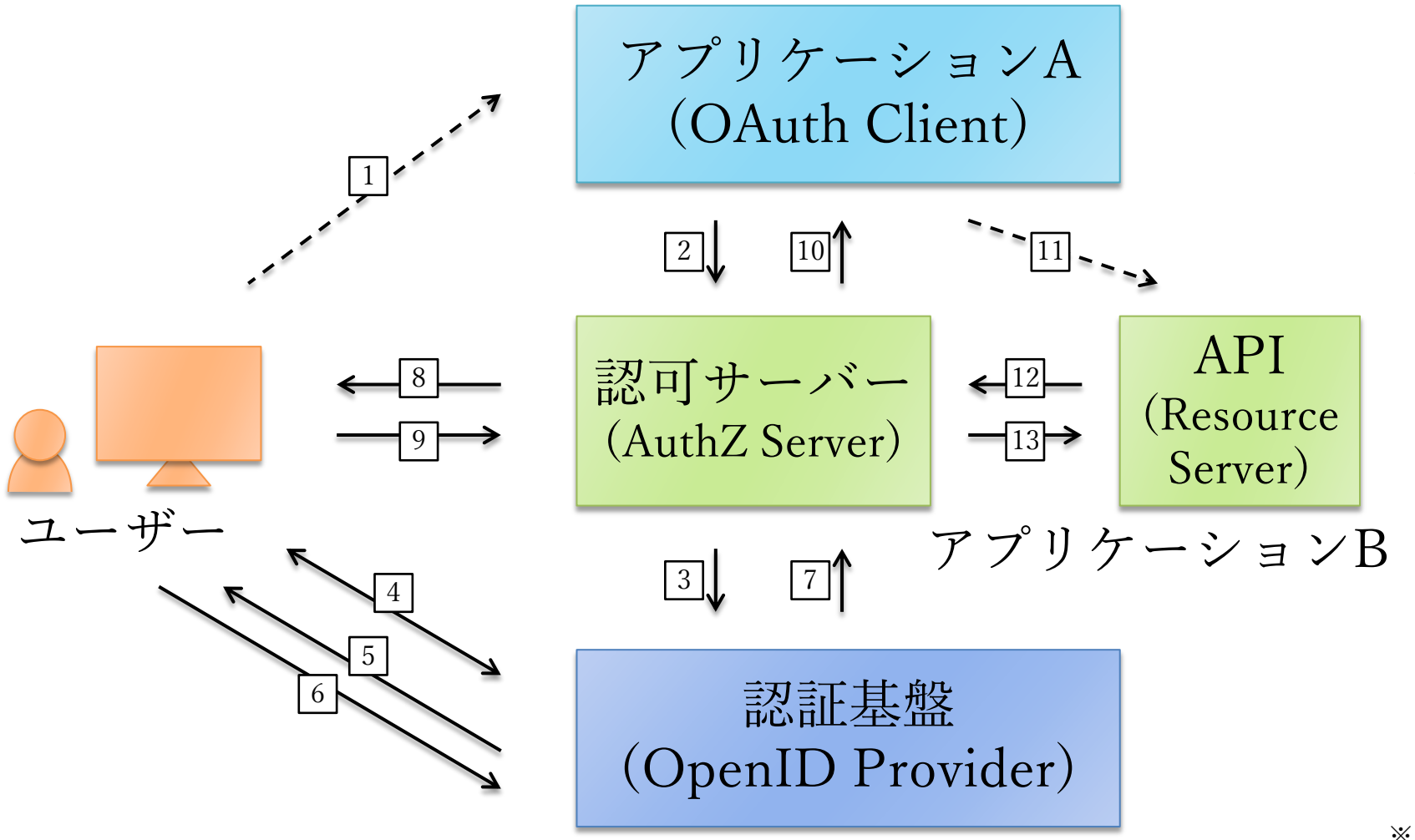
OAuth を使ったアプリケーション間API連携の許可 ②



1. ユーザーがアプリAにアクセス
2. アプリBのユーザー情報のAPIにアクセスしたい
3. ユーザーを認証
4. アプリAが、アプリBのあなたの情報にアクセスしようとしているけどいい？（あなたの代わりにアプリBでこんな操作しようとしているけどいい？）
5. いいよ
6. このトークンでAPIにアクセスして
7. APIにアクセス
8. このトークンは何を許可したもの？
9. ○○さんが、アプリAがアプリBで△△することを許可したもの。

※ 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。

認証基盤と連動したAPI連携の認可



1. アプリAにアクセス
2. APIへのアクセス許可を要求
3. ユーザーの認証を要求
4.～7. 認証結果を連携
8.～10. アクセストークンを応答
11. APIへアクセス
12.～13. アクセストークンを確認してAPIを実行

※ 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。

ThemiStruct ソリューション での対応

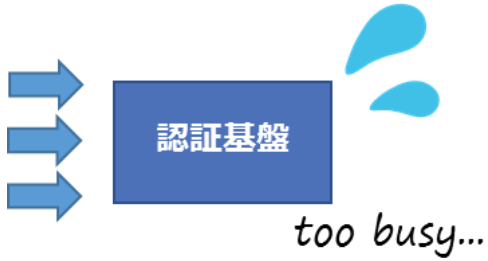
認証基盤 から
アイデンティティプラットフォーム へ

広がるユースケース
増えるアクセス
高まる重要性

おのずと「非機能要求」のレベルもアップ

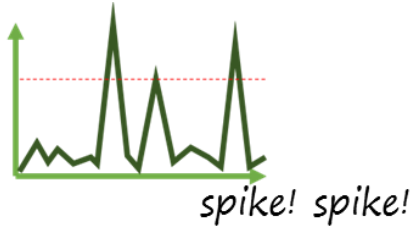
膨大なトラフィック

- 認証基盤の役割増加
- 提供するサービス・システムの増加
- ユーザー数・デバイス数の増加
- API利用の増加



スパイクアクセス

- キャンペーンやニュースサイト掲載などにより定常的なアクセスと比較し、予想不可な大量のアクセスが発生する



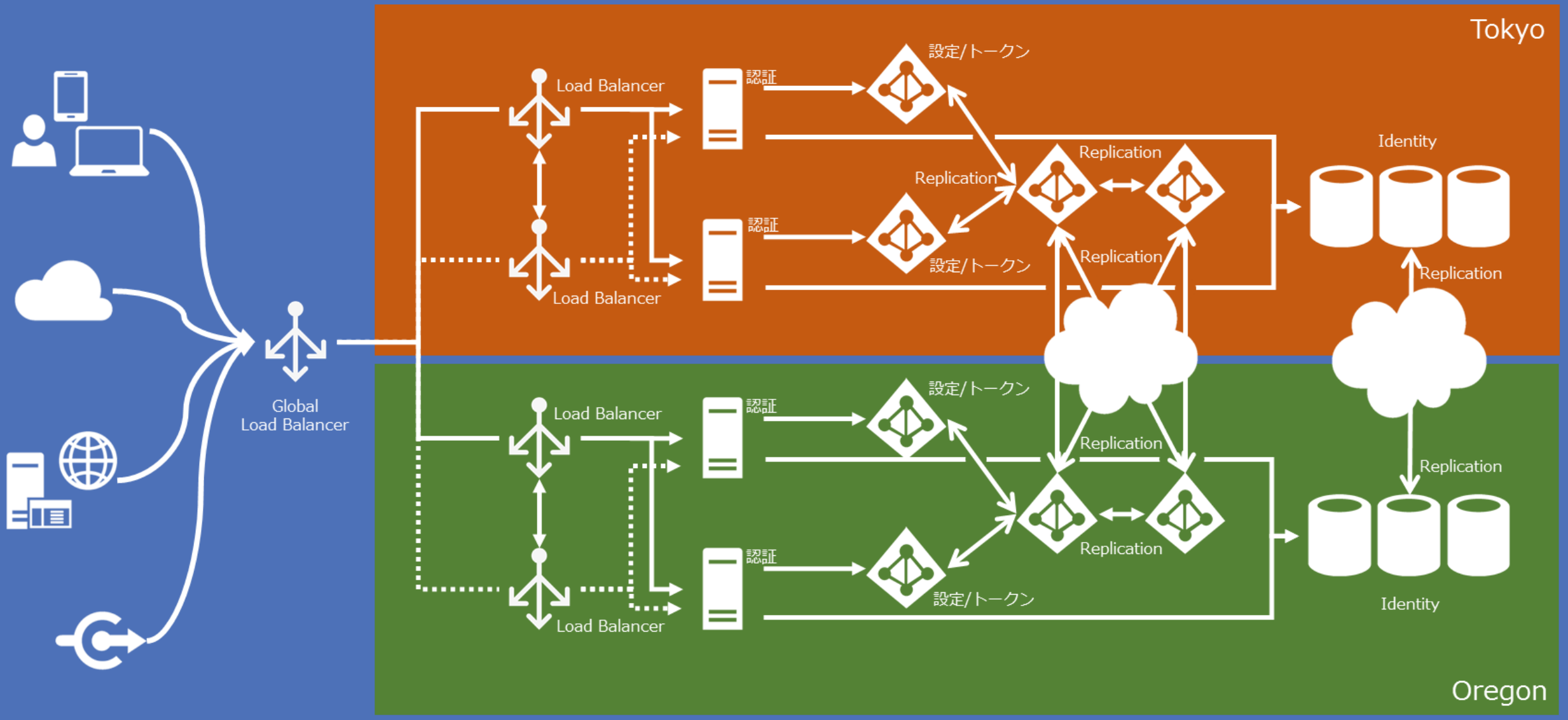
システム停止を回避

- 認証基盤役割の増加に伴い、システム停止や遅延による機会損失が大きくなり、事業継続性や機会損失回避など可用性要求のレベルが格段にUPした

スピードスタート・スモールスタート

- 短期間でビジネスをスタートさせたり、事業規模に応じてスタート、柔軟にスケールできる必要がある

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。



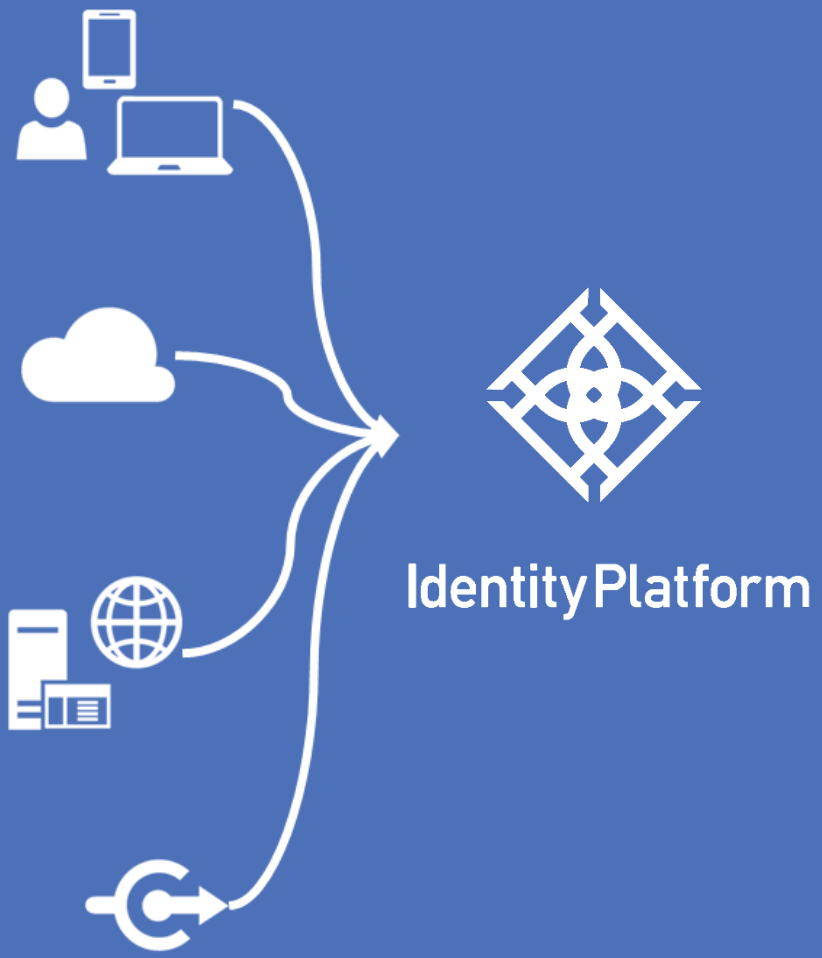
当社のアプローチ

ThemiStruct テミストラクト

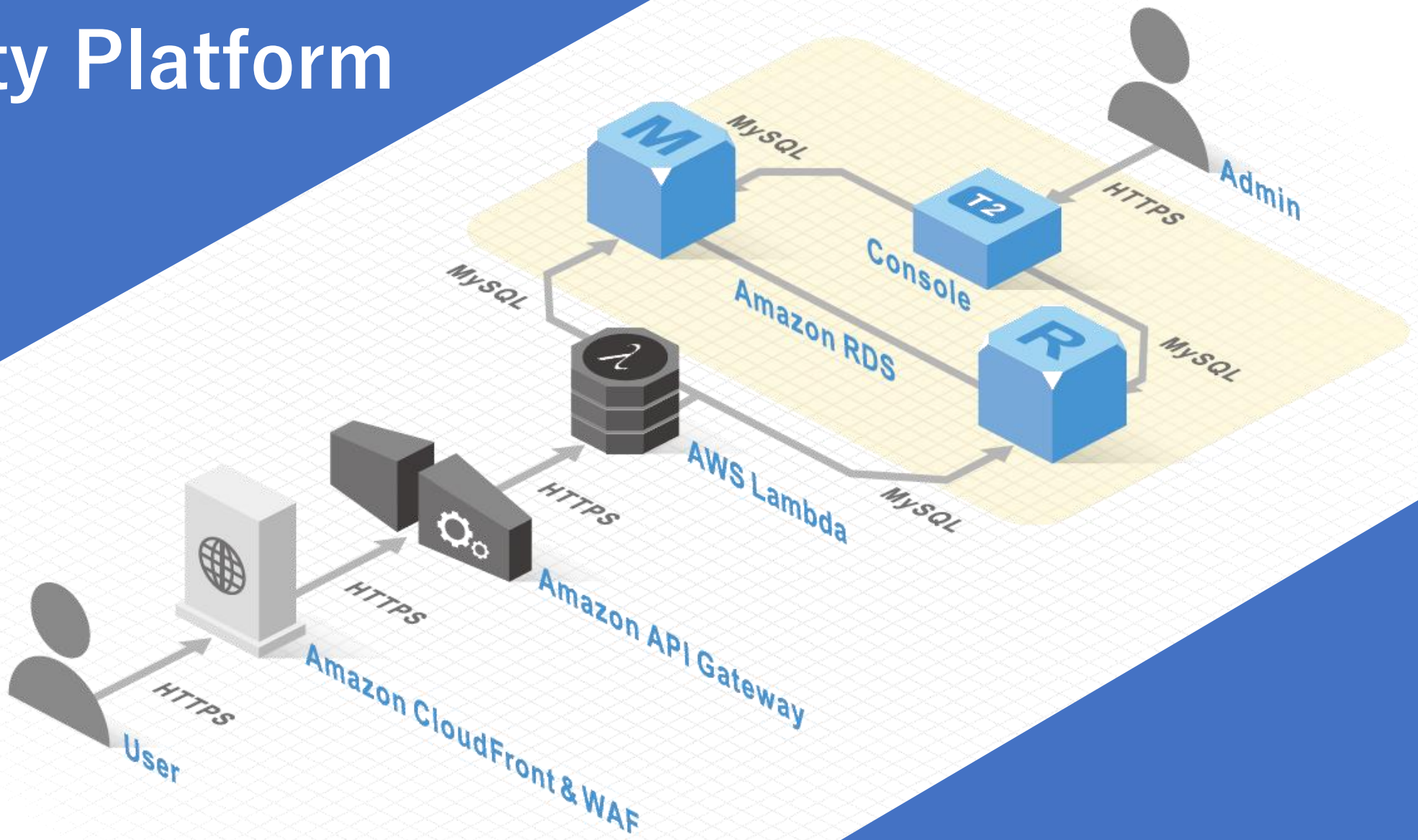
IdentityPlatform AWS対応版

- ✓ AWSのPaaS上で動く
  アイデンティティ連携基盤
- ✓ ≠OpenAM、OpenIDM
- ✓ ≠IDaaS
- ✓ オージス総研自社商品

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。



ThemiStruct Identity Platform



AWSマネージドサービスを使い安全な認証基盤を短時間で

CloudFront, API Gateway, Lambda, RDS, CloudWatch, …

✓ **サーバーレス**	個々のサーバーの管理が不要
✓ **高いスケーラビリティ**	アクセス量予測、事前リソース確保、 事前の設備投資が不要
✓ **十分な可用性**	複雑な設計、膨大なテストからの開放
✓ **豊富なセキュリティオプション**	AWS WAF, AWS Shield, … などを 組み合わせて安全対策を強化
✓ **使えるモニタリング機能**	ダッシュボード、ログ管理、通知の 仕組みを簡単に構築

OpenID Certified になりました。

ThemiStruct テミストラクト
Identity Platform AWS対応版

http://openid.net/certification/

オージス総研の ThemiStruct Identity Platform は OpenID Connect™ プロトコルの OP Basic, OP Implicit, OP Config の3つのプロファイルに適合した OpenID Certified™ 実装です。

そして...

ビジネスの「デジタル変容」が必要な時代

認証基盤エンジニアは「Identity Professional」への
変容が求められています

オージス総研では
Identity Professional の育成の
取り組みを始めています

まとめ

まとめ

- 認証基盤のユースケースが広がってきた。デジタルビジネスに対応できる認証基盤構築のニーズが高まる。
- 認証だけではなく、利用者のアイデンティティを管理、提供するプラットフォームが必要となる。
- アイデンティティ連携技術の標準化、製品・サービスへの実装は急速に進行中。標準に適合して、相互接続性を高める。
- ThemiStructソリューションは ThemiStruct Identity Platform をラインアップに加え、皆さまのビジネスをサポート。

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

参考資料

統合認証ソリューション ThemiStruct

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 AWS対応版

クラウド、IoT時代の
“All in one”
認証プラットフォーム

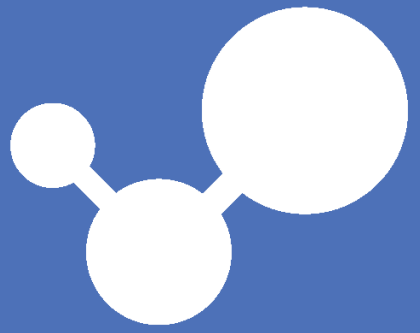
ThemiStruct Identity Platform

ThemiStruct テミストラクト
Identity Platform AWS対応版

- ✓ AWSのPaaS上で動く
  アイデンティティ連携基盤
- ✓ ≠OpenAM、OpenIDM
- ✓ ≠IDaaS
- ✓ オージス総研自社商品

あなたの Identity Platform が すぐ構築可能

アイデンティティ連携



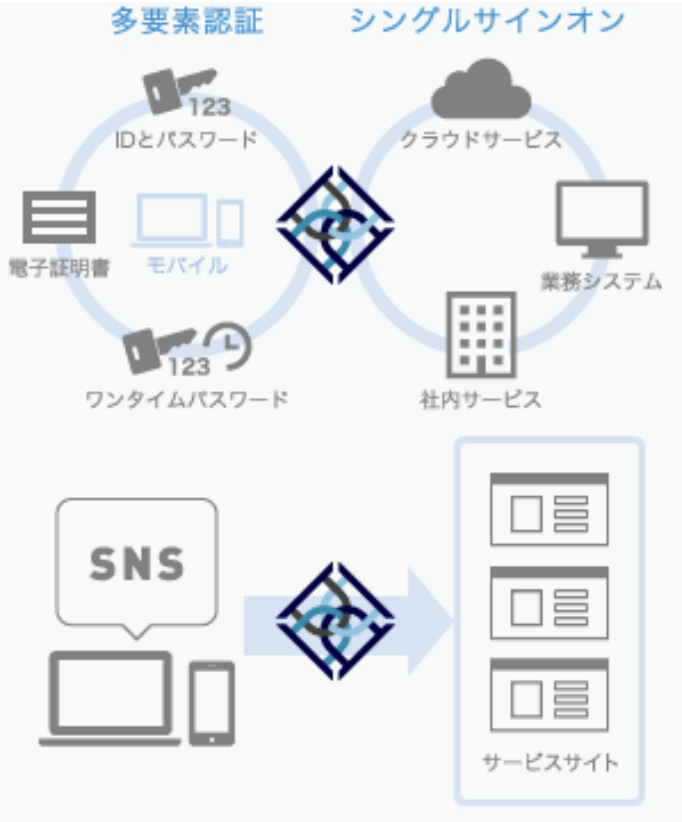
事業成長や突発的アクセスに 合わせたスケーリング

アクセスセキュリティ強化

ThemiStruct Identity Platform の特徴 (1)

認証システムの短期導入が可能

ThemiStruct Identity Platform はクラウド上に設置され、短期間で従業員、カスタマー、ビジネスパートナーに認証サービスを提供できます。また、APIを利用し既設サイトへの組み込みも容易です。



ログインを1回に、認証方法も組合せ自由

ThemiStruct Identity Platform に一度ログインを行うことで、ユーザーが利用したい各サイトへシングルサインオンすることができます。 その際のログインではIDとパスワードによる認証だけでなく、ワンタイムパスワード・電子証明書、指静脈情報などを利用することができます。また利用システムごとの設定により、各サイトやコンテンツのセキュリティ、ユーザビリティ要件に応じた認証を行うことができます。

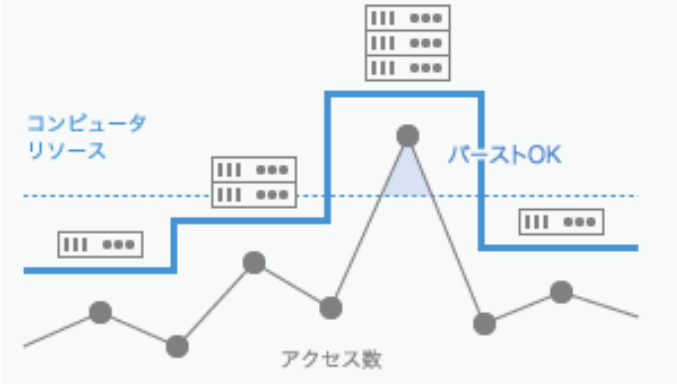
ユーザー登録のハードルを下げ、新規ユーザー登録率をアップ

FacebookやGoogleなどのユーザーが普段使っているSNSやWebサービスのアカウントを利用して、気軽にユーザー登録が可能です。サイトへの新規ユーザー登録率、ユーザビリティ、コンバージョン率を向上させます。ユーザー自身による登録や、管理者による一括登録も可能です。

ThemiStruct Identity Platform の特徴 (2)

各システムへ必要なときに、必要な情報を連携できます

ThemiStruct Identity Platform から各システムへ必要なタイミングで、必要なユーザー情報を連携することができます。各システムでユーザー情報の管理が不要になります。



事業成長に合わせたスケーリング、突発的アクセス集中への対応

サーバレスアーキテクチャにより、事業環境の変化や突発的アクセス集中に合わせて、自由にかつ自動でコンピュータリソースの拡張・縮小を行えます。