いま企業に求められる認証基盤とID管理

～ID連携技術によるクラウド、モバイル活用実現や、適切な権限管理の実現に向けて～

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
三田 善啓

自己紹介

三田 善啓

株式会社オージス総研

統合認証ソリューション担当部門　マネジャー

主戦場

統合認証基盤構築プロジェクトのマネジメント

自社商品（ThemiStruct）ソリューション開発

オージス総研について

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　中沢　正和
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	402.4億円（単体）　参考　733.2億円（グループ単純合計）(2018年度)
従業員数	1,439名（単体）　参考　3,456名（グループ合計）（2019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）

ダイバーシティ関連認定

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）
IdentityPlatform

APIエコノミー時代の
統合認証パッケージ

認証認可・アイデンティティ分野での取り組み

ロ OpenAMコンソーシアム　副会長

現在OpenAMがGitHubで公開しているOpenAMのソースコードは、オープンソース・ソリューション・テクノロジ株式会社と株式会社オージス総研のソースコードをマージしたものとなっており、脆弱性対策や機能拡張を共同で実施しています。

【OpenAMコンソーシアムがソースコード公開に至った狙い】
https://www.atmarkit.co.jp/ait/articles/1811/05/news006.html

<https://www.openam.jp/operation/operation_2018/2018-7-9-newsrelease.html>

ロ OpenID ファウンデーション・ジャパン会員

OpenID Japan

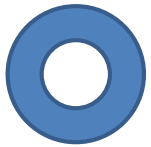
「統合認証基盤」を考える

セキュリティのための統合認証基盤

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

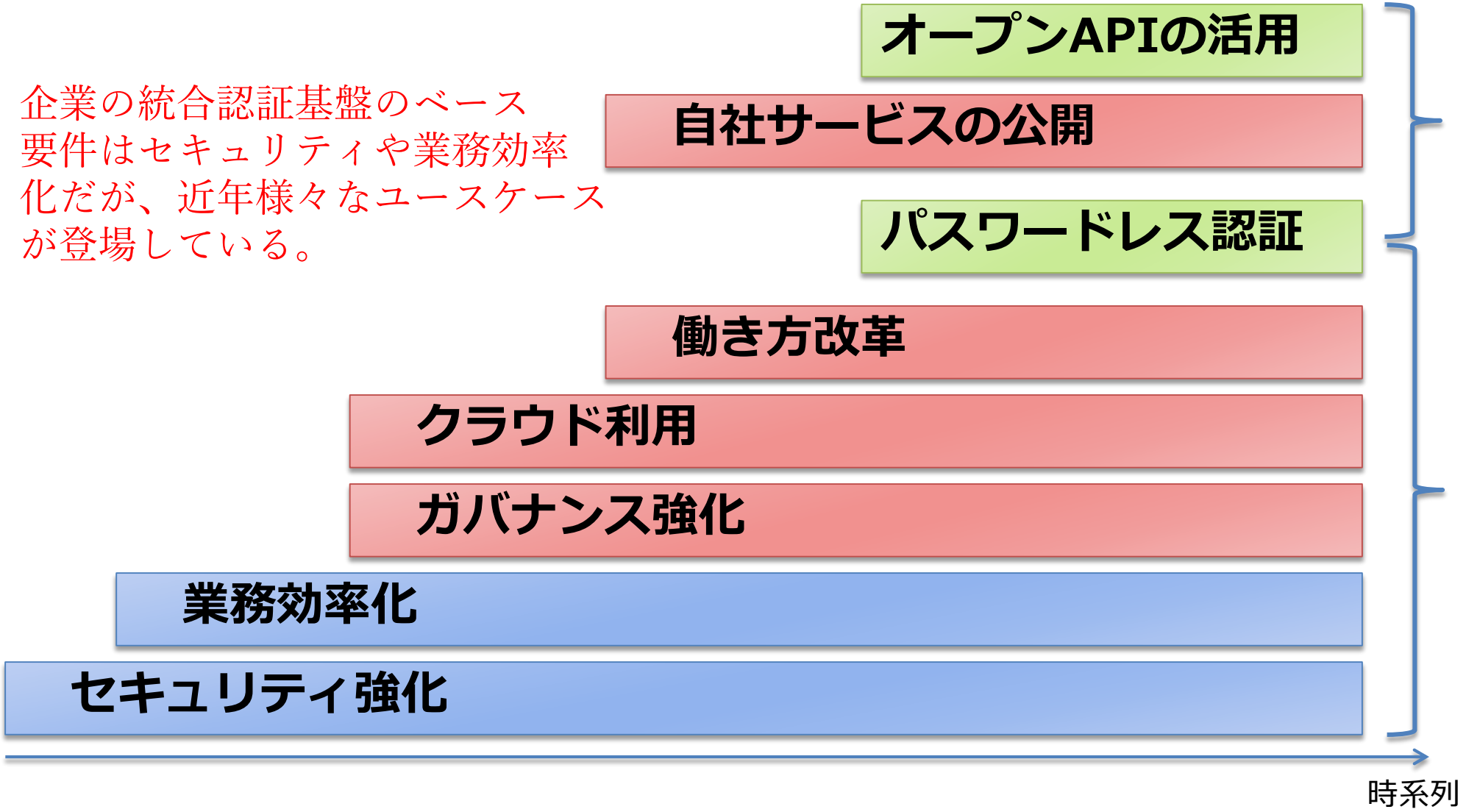
利用を制限するための統合認証基盤



クラウド、デバイス、サービスを活用してもらうための統合認証基盤

企業内の統合認証基盤のユースケース

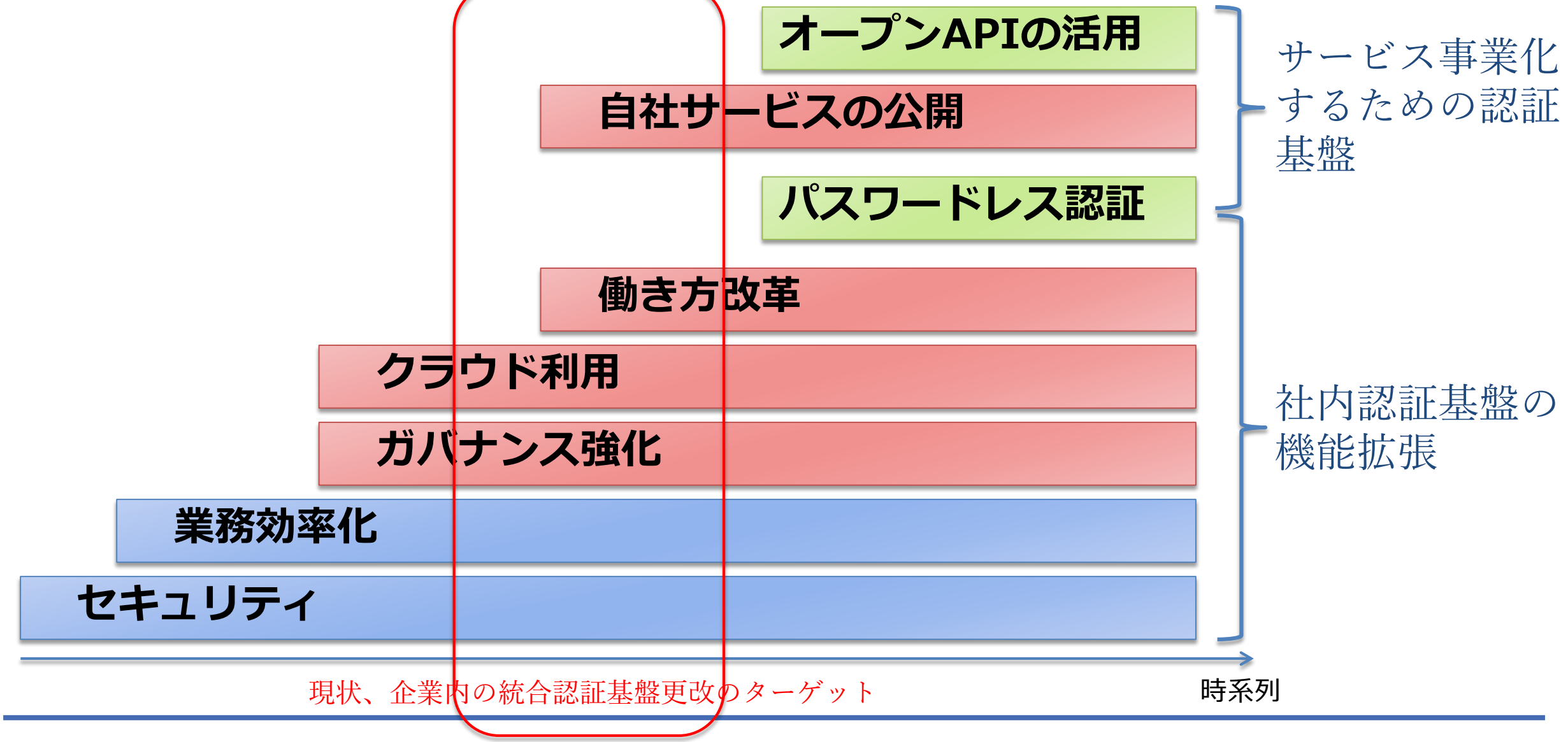
企業の統合認証基盤のベース
要件はセキュリティや業務効率化だが、近年様々なユースケースが登場している。



ユースケースの特徴（実現技術）

ユースケース	実現技術
オープンAPI活用	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（OAuth）
自社サービスの公開	多要素認証（OTP　クライアント証明書認証）による取引先の認証 認証連携（SAML　OpenID Connect）プロトコルによるログインの実装
パスワードレス認証	アプリ内にパスワード保存不要な安全な認証方式（FIDO2）
働き方改革	社外からのクラウド利用の制限。社外から利用時する場合の追加認証（OTP）の実施。社用端末の識別（クライアント証明書認証）。
クラウド利用	SaaSアプリケーションの認証連携（SAML　OpenID Connect）プロトコルを利用した認証一元化（Single Sign On）
ガバナンス強化	入社退社だけでなく人事異動に則した権限のタイムリーな付与（Roll Base Access Control）や、証跡追跡
業務効率化	ID登録の一元化や、IDプロビジョニング
セキュリティ強化	パスワードなどセキュリティポリシー統一と、認証一元化（Single Sign On）

企業内の統合認証基盤のユースケース



「統合認証基盤」ユースケース
適正な認証 を考えてみる

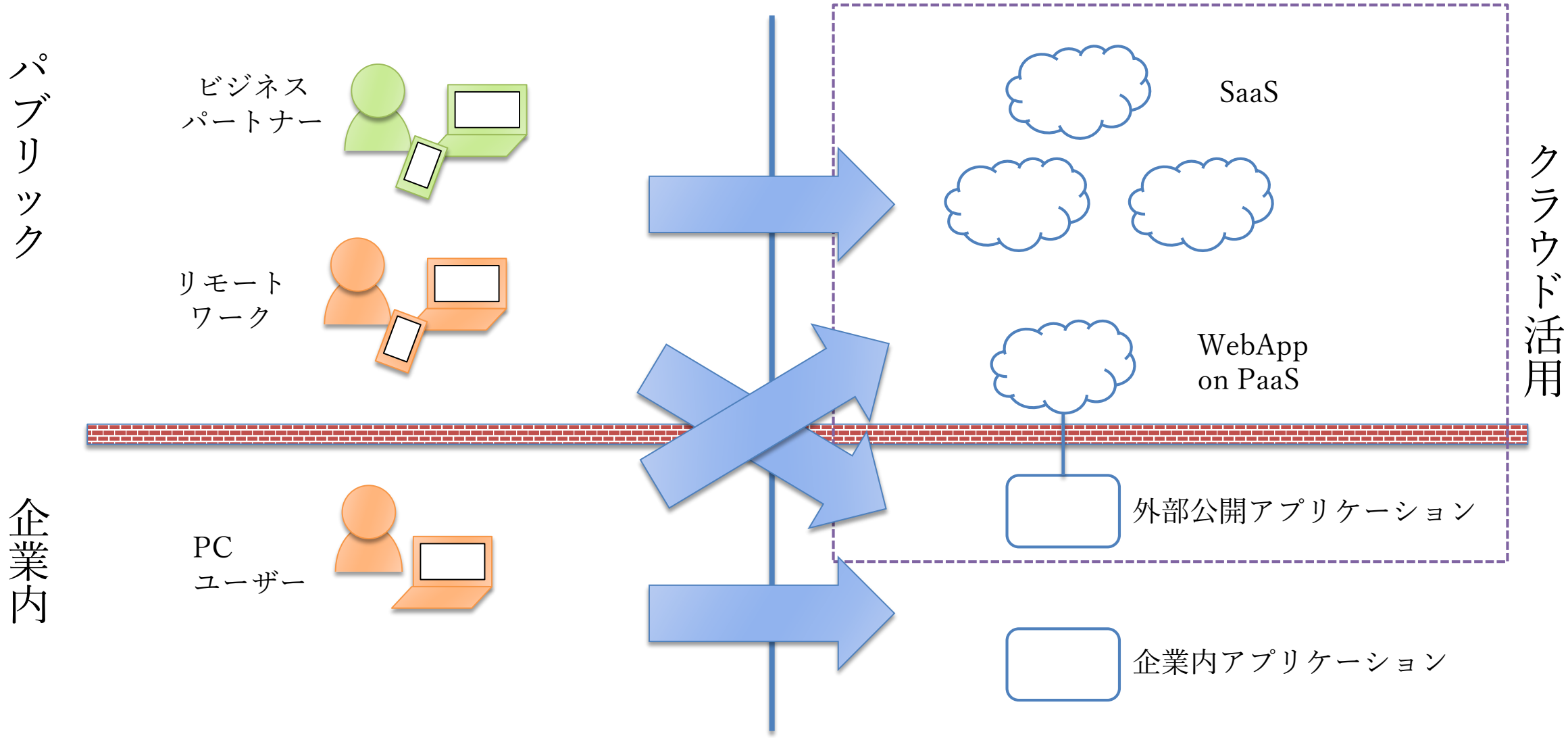
ユースケースの特徴（実現技術）

ユースケース	実現技術
オープンAPI活用	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（OAuth）
自社サービスの公開	多要素認証（OTP　クライアント証明書認証）による取引先の認証 認証連携（SAML　OpenID Connect）プロトコルによるログインの実装
パスワードレス認証	アプリ内にパスワード保存不要な安全な認証方式（FIDO2）
働き方改革	社外からのクラウド利用の制限。社外から利用時する場合の追加認証（OTP）の実施。社用端末の識別（クライアント証明書認証）。
クラウド利用	SaaSアプリケーションの認証連携（SAML　OpenID Connect）プロトコルを利用した認証一元化（Single Sign On）
ガバナンス強化	入社退社だけでなく人事異動に則した権限のタイムリーな付与（Roll Base Access Control）や、証跡追跡
業務効率化	ID登録の一元化や、IDプロビジョニング
セキュリティ強化	パスワードなどセキュリティポリシー統一と、認証一元化（Single Sign On）

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 だけでなく 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
- **自社サービス公開による事業化**
  - ビジネスパートナーのシステム利用へ

業務向けIT活用の世界観



認証基盤で対応しておくべきこと、など

ロ 状況に応じた認証方式の選択

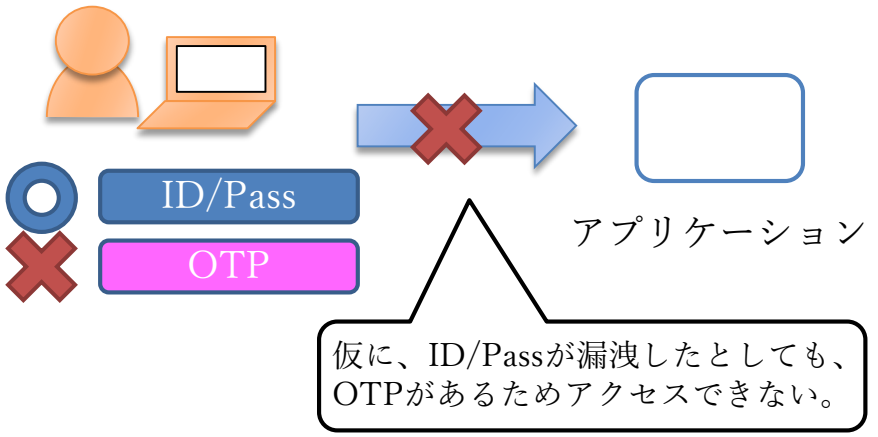
- 社内からのアクセスに対する認証なのか、社外からのアクセスに対する認証なのか？
- 人（不正ログインユーザー）に対してセキュリティ強化したいのか、モノ（管理外デバイスへ情報漏洩）に対してセキュリティ強化したいのか？

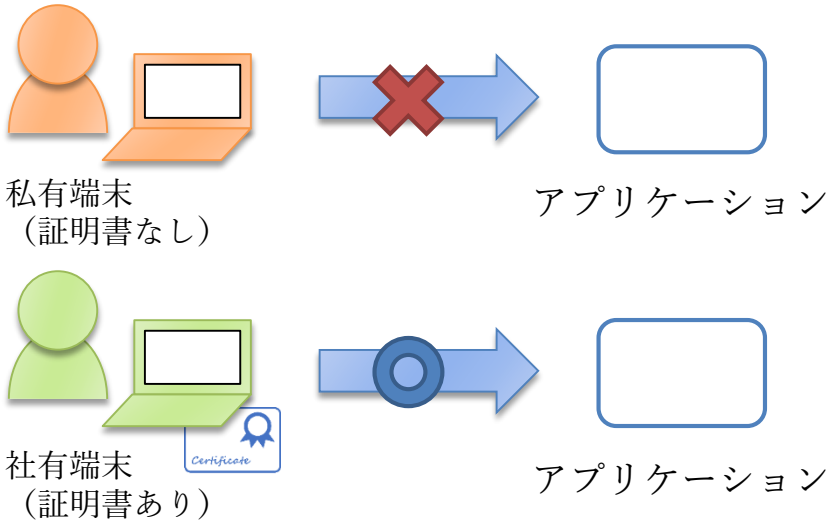
ロ ID連携技術への対応

- SaaSのアプリケーションを自社認証基盤経由で利用したい（自社認証基盤を経由せずWeb上でSaaSアプリケーションにログインさせたくない）。
- 自社のサービスをWeb公開するにあたり、取引先からID連携プロトコルに対応していることを求められる。

状況に応じた認証方式の選択

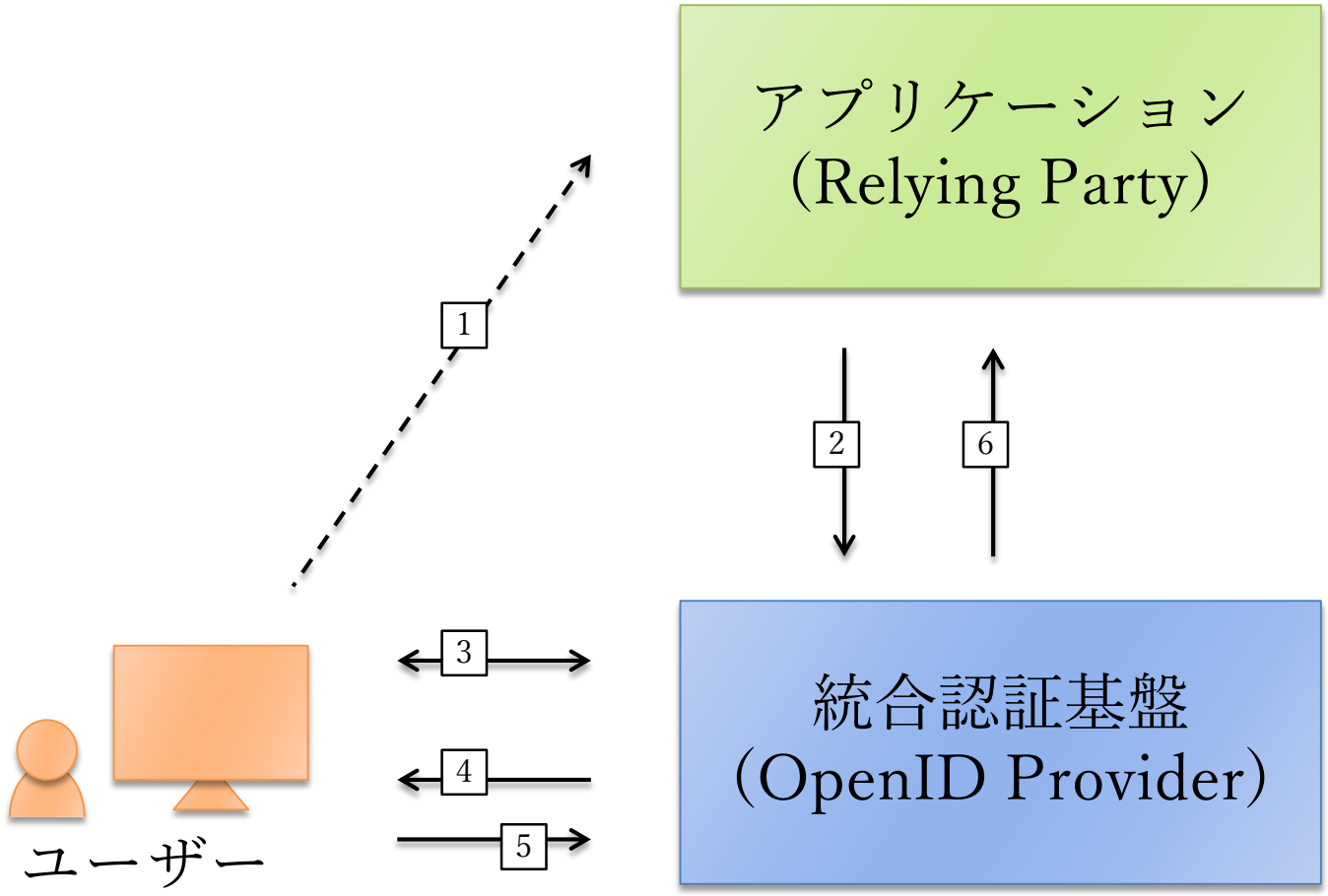
- **ID・パスワード認証 + OTP（FIDO）**
  - 人（ユーザー）に対する認証強化
  - パスワードの他に、ユーザー本人を特定（あるいは本人しか知りえない情報）する情報を利用して認証する
- **ID・パスワード認証 + クライアント証明書**
  - モノ（デバイス）に対する認証強化。
  - クライアント証明書を導入した会社支給端末のみアクセスを許可することで、私有端末に情報漏洩させない。
- **上記の組み合わせもOK**





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。

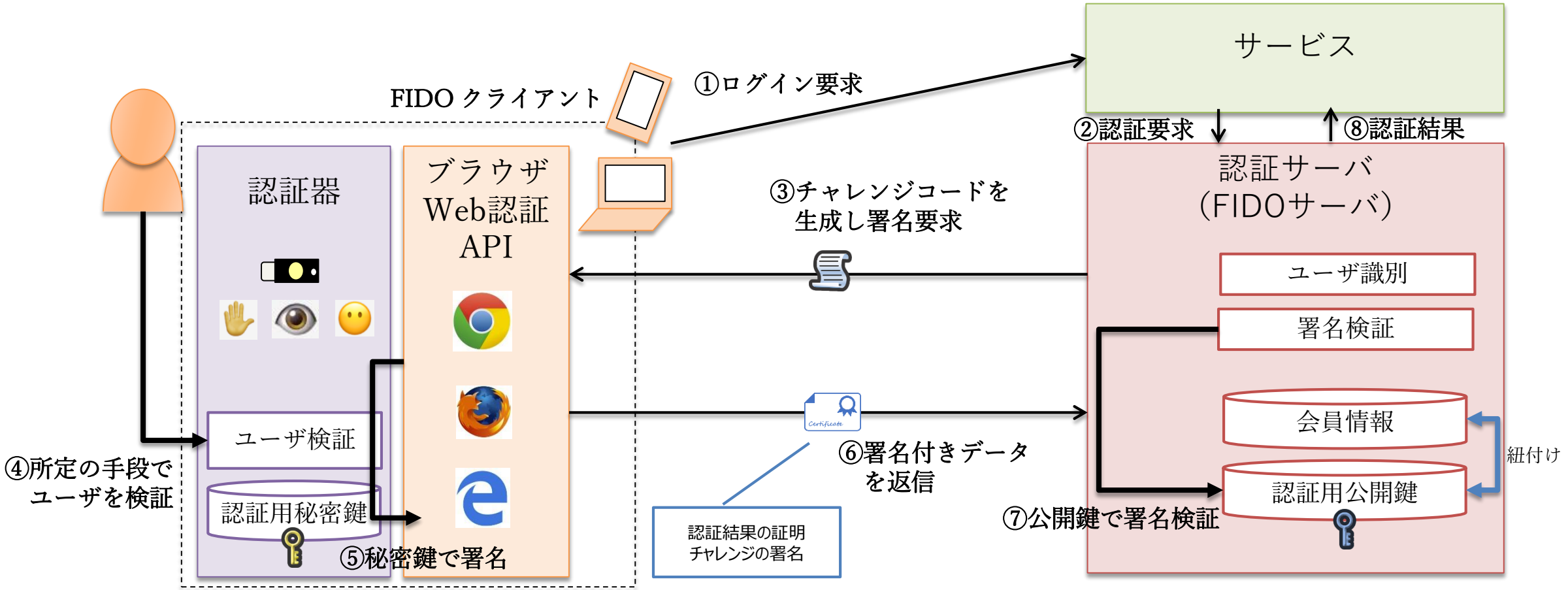
ユースケースの特徴（実現技術）

ユースケース	実現技術・特徴
オープンAPI活用	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（OAuth）
自社サービスの公開	多要素認証（OTP　クライアント証明書認証）による取引先の認証 認証連携（SAML　OpenID Connect）プロトコルによるログインの実装
パスワードレス認証	アプリ内にパスワード保存不要な安全な認証方式（FIDO2）
働き方改革	社外からのクラウド利用の制限。社外から利用時する場合の追加認証（OTP）の実施。社用端末の識別（クライアント証明書認証）。
クラウド利用	SaaSアプリケーションの認証連携（SAML　OpenID Connect）プロトコルを利用した認証一元化（Single Sign On）
ガバナンス強化	入社退社だけでなく人事異動に則した権限のタイムリーな付与（Roll Base Access Control）や、証跡追跡
業務効率化	ID登録の一元化や、IDプロビジョニング
セキュリティ強化	パスワードなどセキュリティポリシー統一と、認証一元化（Single Sign On）

パスワードレス認証

FIDO2

- 公開鍵認証方式を応用してオンライン経由で認証を行う仕組み（≠生体認証、パスワードレス）



パスワードレス認証

FIDO2の特徴

- 認証サーバにパスワード情報や生体情報を保持する必要がない
- パスワード情報や生体情報がネットワーク上を流れない
- 上記情報がないため、認証サーバが狙われない、不正ログインできない
- FIDO対応のブラウザと認証器を持つデバイスがあれば多要素認証が簡単に実現できる
- パスワードを使わず認証することもでき、パスワード管理から解放される
- FIDO2対応のUSBやBluetooth、NFCの外部認証器を利用することもできる

「統合認証基盤」ユースケース
適正なアクセス管理 を考えてみる

ユースケースの特徴（実現技術）

ユースケース	実現技術・特徴
オープンAPI活用	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（OAuth）
自社サービスの公開	多要素認証（OTP　クライアント証明書認証）による取引先の認証 認証連携（SAML　OpenID Connect）プロトコルによるログインの実装
パスワードレス認証	アプリ内にパスワード保存不要な安全な認証方式（FIDO2）
働き方改革	社外からのクラウド利用の制限。社外から利用時する場合の追加認証（OTP）の実施。社用端末の識別（クライアント証明書認証）。
クラウド利用	SaaSアプリケーションの認証連携（SAML　OpenID Connect）プロトコルを利用した認証一元化（Single Sign On）
ガバナンス強化	入社退社だけでなく人事異動に則した権限のタイムリーな付与（Roll Base Access Control）や、証跡追跡
業務効率化	ID登録の一元化や、IDプロビジョニング
セキュリティ強化	パスワードなどセキュリティポリシー統一と、認証一元化（Single Sign On）

アクセス管理とは

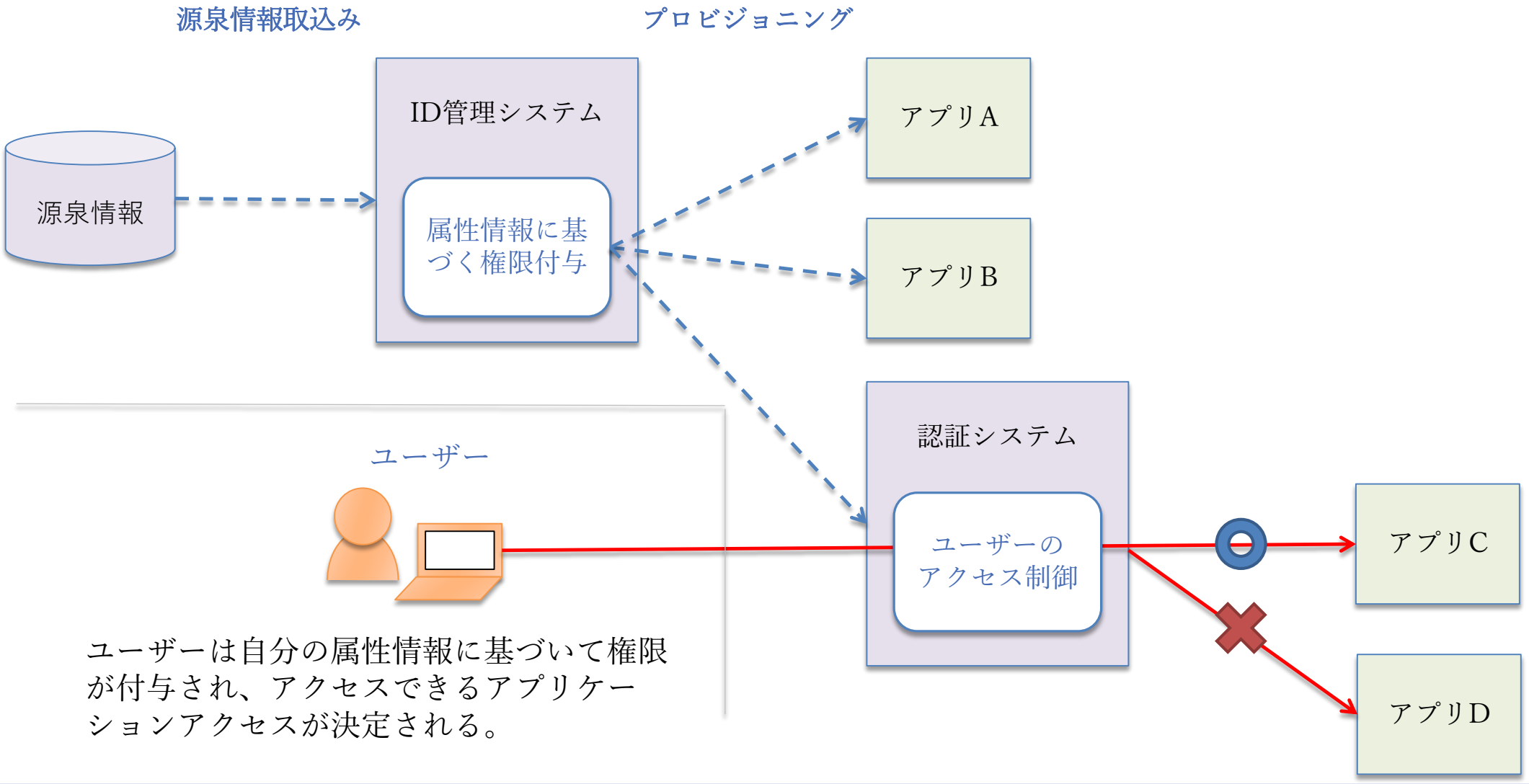
□ 統合認証基盤　何を”統合”しているのか

- 認証システム　　IDの利用正当性を確認する。
- ID管理システム　　IDのライフサイクルに従って情報正当性を保証する。

アクセス管理　認証システム＋ID管理システムでなければ実現できない

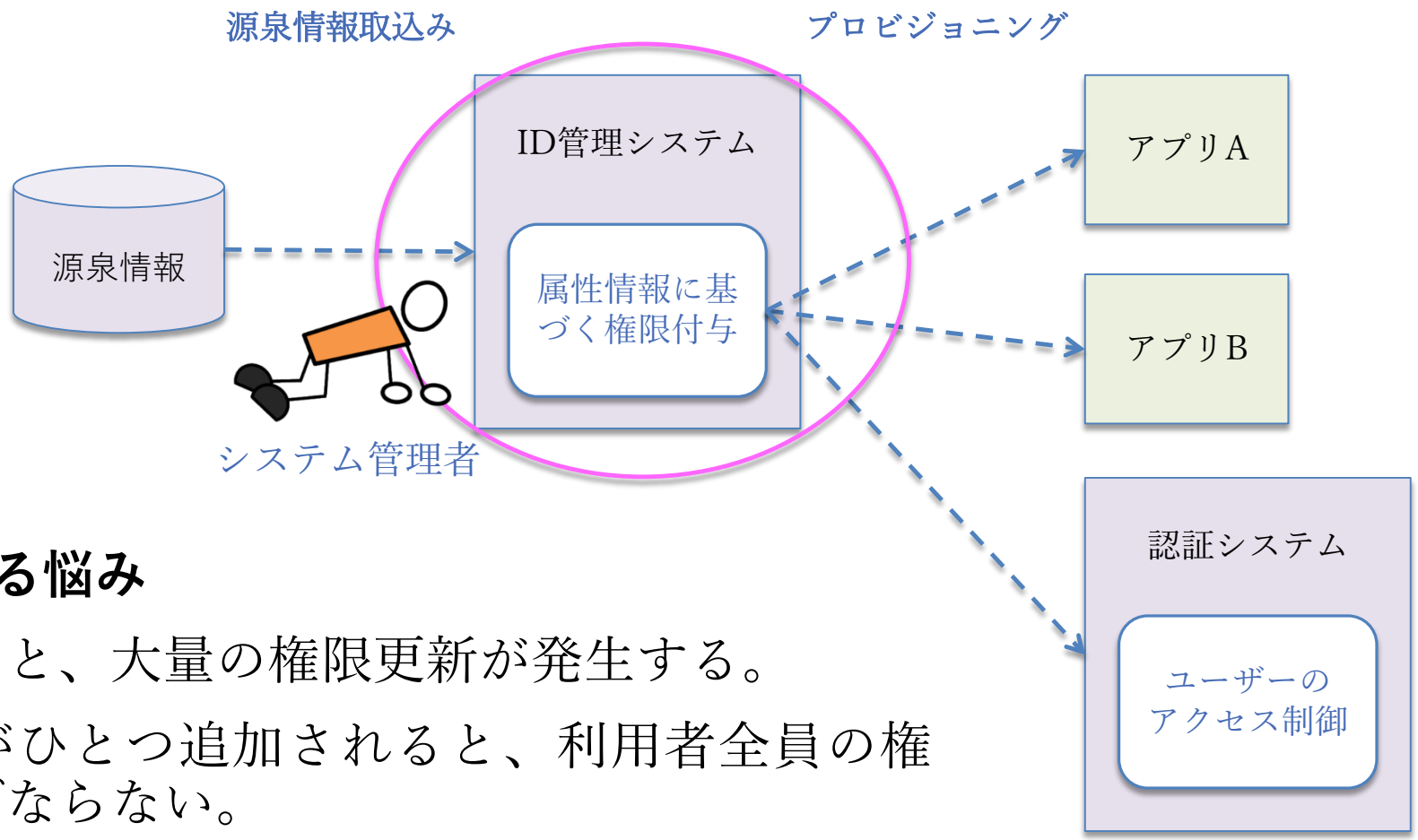
ID管理システムによって、付与されたアクセス権限に従って、認証システムはIDのアクセス制御を実施する。

アクセス管理とは



ユーザーは自分の属性情報に基づいて権限が付与され、アクセスできるアプリケーションアクセスが決定される。

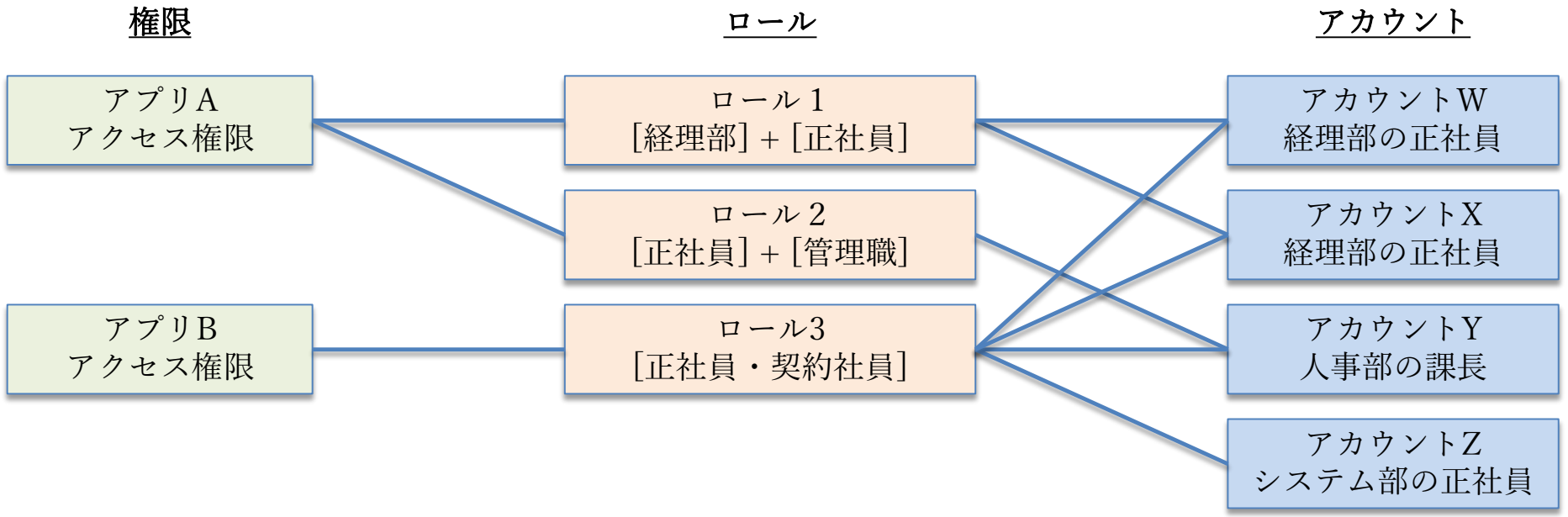
ロールベースアクセス管理



ロ システム管理者が抱える悩み

- 大型人事異動があると、大量の権限更新が発生する。
- アプリケーションがひとつ追加されると、利用者全員の権限を更新しなければならない。
- グループ会社の増減や統廃合で、権限付与やり直し。

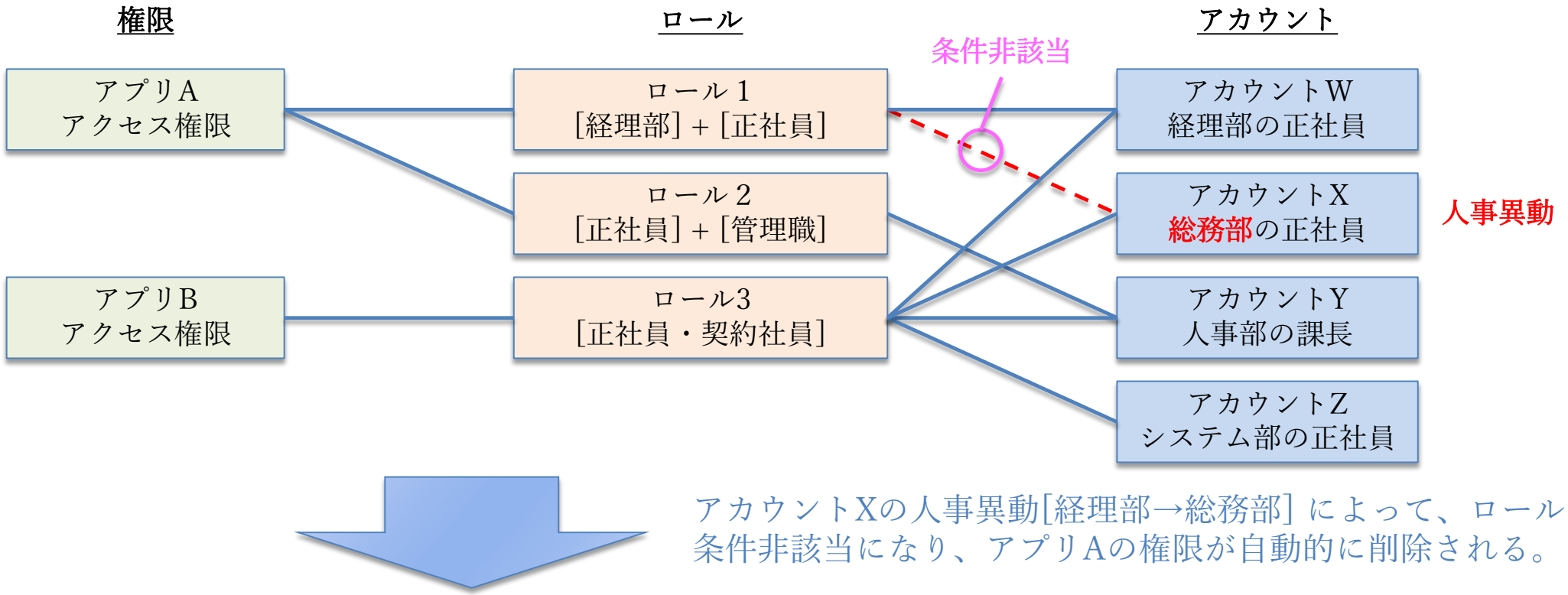
ロールベースアクセス管理



ロールベースアクセス管理の考え方

- 権限をアカウントを直接紐付けずに、特定のアカウント属性の値を条件とするロールと紐付けする。
- 人事異動などアカウント属性の変更があった場合、ロールが自動的に付与・削除され、権限の付与・削除も自動的に行われる。

ロールベースアクセス管理



アカウントXの人事異動[経理部→総務部] によって、ロール１が条件非該当になり、アプリAの権限が自動的に削除される。

ロールによる権限の自動反映

- 人事異動によるアカウント属性変更を自動的に反映することで、システム管理者が抱える悩みを解消できる。

ユースケースの特徴（実現技術）

ユースケース	実現技術・特徴
オープンAPI活用	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（OAuth）
自社サービスの公開	多要素認証（OTP　クライアント証明書認証）による取引先の認証 認証連携（SAML　OpenID Connect）プロトコルによるログインの実装
パスワードレス認証	アプリ内にパスワード保存不要な安全な認証方式（FIDO2）
働き方改革	社外からのクラウド利用の制限。社外から利用時する場合の追加認証（OTP）の実施。社用端末の識別（クライアント証明書認証）。
クラウド利用	SaaSアプリケーションの認証連携（SAML　OpenID Connect）プロトコルを利用した認証一元化（Single Sign On）
ガバナンス強化	入社退社だけでなく人事異動に則した権限のタイムリーな付与（Roll Base Access Control）や、証跡追跡
業務効率化	ID登録の一元化や、IDプロビジョニング
セキュリティ強化	パスワードなどセキュリティポリシー統一と、認証一元化（Single Sign On）

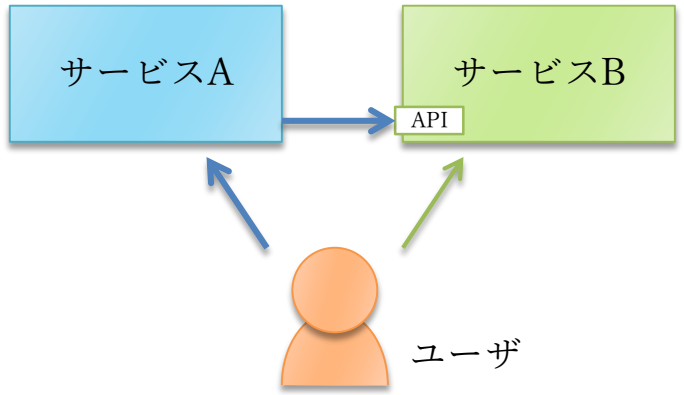
オープンAPIの活用

ロ ユーザはサービスAに対して、別のサービスBに保管されているリソースに対して何らかのアクセスを行う権限を与えたい

- ユーザ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 OAuth 2.0

- ユーザ の同意に基づき、ユーザ 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



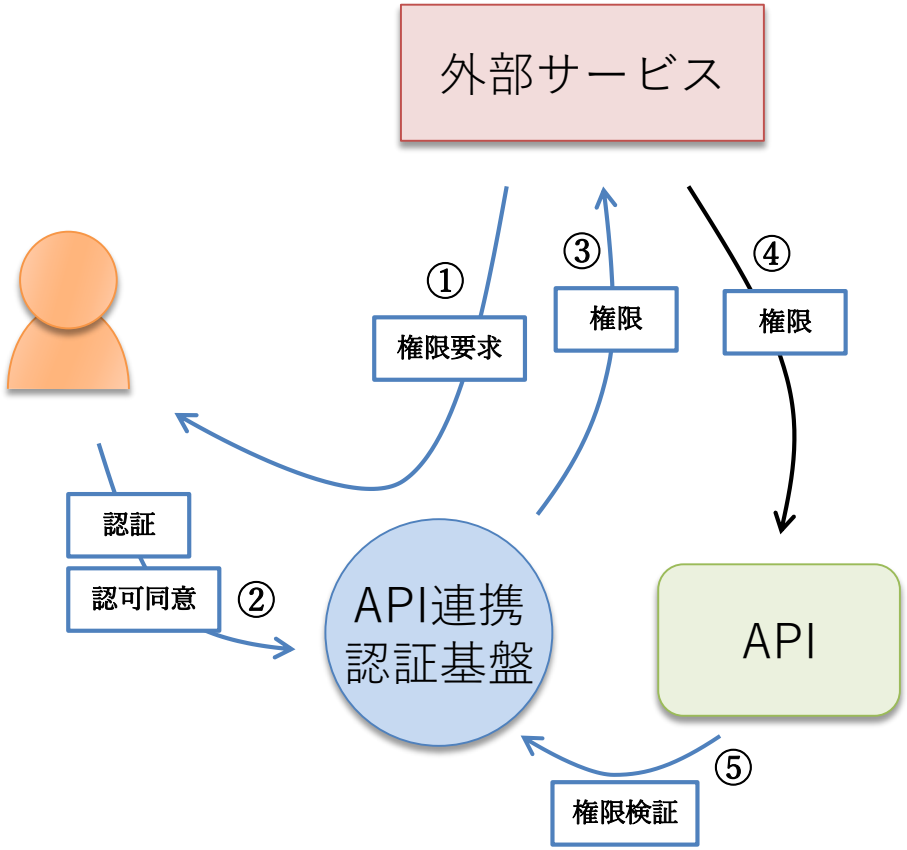
API連携認証基盤

- OAuth 2.0を利用するには「認可サーバ」の機能が必要
- 認可（アクセス権の委譲）の前提としてユーザが適切な方法で認証されている必要がある

- オープンAPIを提供するためには、API利用者の認証・認可ができる仕組みを構築しないといけない（API連携認証基盤）
  - ユーザを認証する機能（OpenID Connectなどが別途必要）
  - OAuth2.0 認可サーバの機能

API連携認証基盤

- 外部サービスへのAPI提供するための安全な認証機能の実現
- 再ログインを伴わない安全なサービス利用継続の実現
- サービス利用可能なプラットフォームの拡充
- 利用者の同意に基づくAPI提供・アクセス許可の実現
- APIアクセス可能なクライアントの制限、アクセス権の適用



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

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

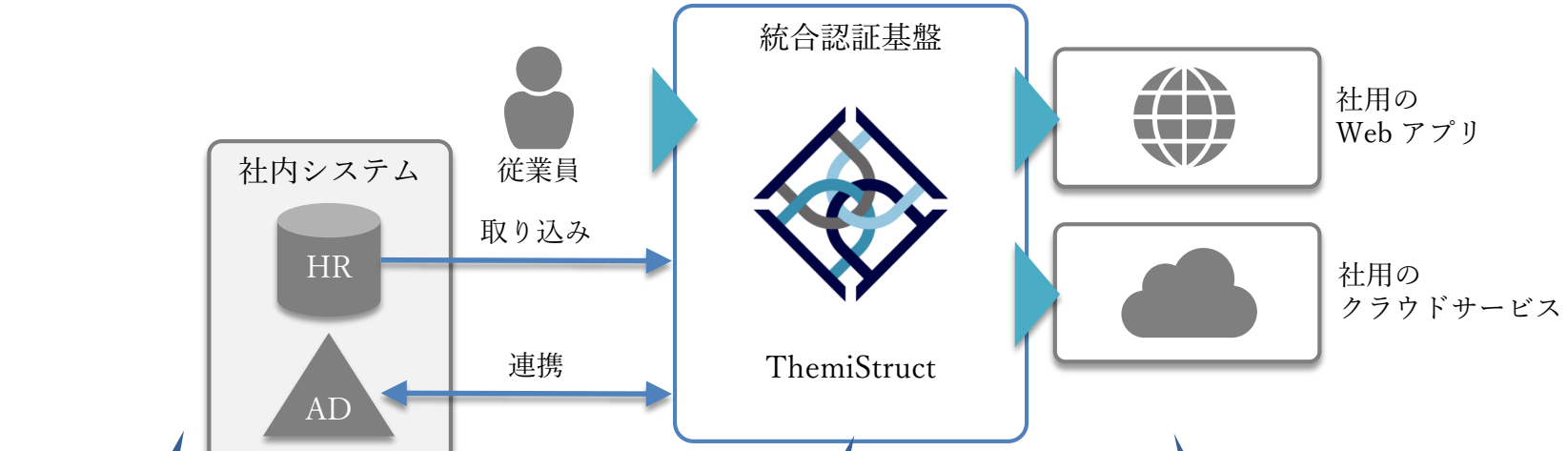
ThemiStruct-MONITOR

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

ThemiStruct を『統合認証基盤』に活用

ThemiStruct を『統合認証基盤』に活用した場合、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社内システムと連携することでガバナンス強化を実現します。



ガバナンス強化

人事システムやADとの連携で、適切なIDライフサイクル管理を実現します。

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。

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　(OpenAM)

ThemiStruct-IDM　ID管理ソリューション　(OpenIDM)

ThemiStruct-CM　電子証明書発行・管理 ソリューション　(EJBCA)

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

オープンソースベース商品

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

ThemiStruct　オープンソースベース商品　特徴

ThemiStruct は企業（エンタープライズ）がOSS（オープンソースソフトウェア）を利用するうえで不安を抱く、変化拡大する業務へ柔軟に対応するための機能拡張や、確実な保守サービスを提供することにより、安心して統合認証基盤に活用いただけます。

ロ　オープンソースに足りない機能を追加

- クラウドサービスとの連携、多要素認証、モバイル環境への対応、認証・認可機能の拡張など、オープンソースに足りない機能を独自に開発しています。また、管理ツールやインタフェースの追加・改良により、システムの運用で課題となるユーザビリティの改善を図っています。

ロ　安心のサポート

- パッチ適用やバグフィックスなどソースコードレベルでの安定稼働に向けた検証を行いソフトウェア品質の向上を図っています。また、独自に追加したログ収集モジュールや国内の開発拠点との連携などにより安心・確実・迅速な課題解決が可能です。

ロ　高い費用対効果

- 開発、ステージング、本番など稼働環境単位での価格設定のため、ユーザ数の増加による費用の発生がありません。

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

自社オリジナル商品

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

ThemiStruct Identity Platform 自社オリジナル商品　特徴

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の展開や従業員向けにアプリケーションの展開に必要となる、共通ID基盤の構築に活用いただけます。

□　API連携認証基盤としての機能を提供

- Fintech、IoTなどで対応が必要となるAPI公開に必要な認証システムとして利用いただけます。また、金融向けを中心に検討・策定が進められている技術標準やベストプラクティスにも継続的に適合しています。

□　短期導入と高可用性

- 専用インストーラーで、短時間でスケーラブル、高可用な認証基盤を立上げることができます。また、サービスをオンライン状態でソフトウェアアップデートを行なう機能を提供しています。

□　高い費用対効果

- 利用者数に応じてエディションを用意しており小規模利用時にもライセンス負荷を抑えることが可能となっています。さらに、オージス総研がワンストップで提供する高品質のサポートやオプションによる追加課金の最小化など、優れた費用対効果を発揮します。

まとめ

まとめ

- 統合認証のユースケースは、クラウドやモバイルなどのIT活用によって、時代とともに変化し、かつ重要度を増している。
- IT活用に合わせ、企業内の統合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。
- 当社では統合認証ソリューションとして、ThemiStruct シリーズを提供。それらを組み合わせて統合認証基盤だけでなく、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