マジセミ

B2B SaaSベンダーの認証の課題

MFA対応、自社サービスのSAML/OIDC対応、
お客様企業のAzureAD/IDaaSとの認証連携

2023.11.07

かもめエンジニアリング株式会社

KAMOME Engineering
日本でいちばん仕事が大好きなチームです！

はじめに

2019年、私たちは
「オンプレの社内システムを巻き取ってSSOしたい」というニーズへ向けて
Keygatewayの提供を開始しました。

しかし、当初想定したニーズとは異なる別のお問合せやご商談をいただくケースも増えています。

それが今回ご案内する、
BtoB向けSaaSベンダーさんのための
「自社提供サービスのフェデレーション（SAML／OpenID Connect）対応」です。

このセミナーをさまざまな手段でご覧になる方々のご参考になれば、幸いです。

スピーカー紹介

KAMOME Engineering

潮村 剛 （しおむら たけし）

1990年代半ば、食品メーカーからITベンチャーに。
国内の主要通信サービス事業者を中心に認証系システム案件を担当。

2008年、かもめエンジニアリング社を設立。
通信サービス事業向け統合認証基盤やビッグデータ処理のシステムの導入実績多数。

2017年、SSO分野で「KAMOME SSO」シリーズの提供開始。

2019年、「クラウドID管理サービス　Keyspider」の提供開始。
日本企業のID管理の課題を解決するため、Keyspider社を設立。

2021年、「ゼロトラスト接続サービス　KeygatewayC1」発表
日本企業のテレワーク環境のセキュリティ強化を推進。

2022年、「ゼロトラストアライアンス・ジャパン」、ITベンダーやSI事業者19社で設立。
日本企業へのゼロトラストセキュリティの普及を目的。

SSOやID分野のセミナーで年間30回程度講師を担当。
オライリー・ジャパン社刊行IT技術書籍のプロデュース。
　『RADIUS – ユーザ認証セキュリティプロトコル』（2003年）
　『Diameter プロトコルガイド』（2015年）

画像引用：
オライリー・ジャパン

趣味　料理と読書。歴史小説とSFが好き。
最近のヒットは『ミッキー7』

ID管理・認証分野を中心に展開

統合認証基盤システム　KFEP（ケイフェップ）

- 複数サービスの 「認証・認可」システムを統合、システム規模を最大93%削減の実績
- 運用コストを最大96%削減の実績
- 単一障害点が存在せず、運用SLA向上に貢献
- 通信事業者250ライセンス以上、エンタープライズ約4,000ライセンスの採用実績

認証システム　KAMOME SSO（かもめ SSO）/ Keygateway（キーゲートウェイ）

- **「KAMOME SSO」**
  オープンソース「Keycloak」 をベースに独自の機能をプラス、B2CからB2Bまでカバー
- **「KeygatewayT1」**
  SAML非対応の業務アプリをプライベートSaaS化するツール
- 「KeygatewayC1」
  VPNに代わるゼロトラスト接続サービス

官公庁、金融機関、通信事業者、ECサイト、エネルギー大手、製造大手、教育機関など、幅広い業種と規模での採用実績

RADIUS認証サーバ　fullflex KG（フルフレックスKG）

- インターネット創成期からネットワーク認証を支える、導入実績国内No.1の信頼のブランド
- 単一障害点が存在せず、運用SLA向上に貢献
- WebGUIで運用状態の確認、ログの検索も実現
- 認証拠点の統合に最適なマルチテナント対応

ID管理クラウドサービス　Keyspider（キースパイダー）

- 企業内のユーザー情報、権限情報を統合的に管理できる、ID管理クラウドサービス（SaaS）
- AzureAD、Office365、Salesforce、Google WORKS、BOX、さらに国産のクラウドサービスやオンプレの社内システムとも簡単にID連携
- 独自のセキュア通信機能で、オンプレの社内システムとも安全に連携。日本特有の人事処理にも対応

「ユーザーの認証・認可」「ID管理」を中心としたチーム

通信キャリア向け 大規模認証システム

- 携帯電話サービス 基幹認証システム
  - 国内通信事業者　4,500万ユーザ
- 企業顧客向けVPNサービス 認証基盤
  - 国内総合電機メーカー　100万ユーザ
- 社内LANアクセス　認証基盤
  - 国内大手移動体通信事業者　20万ユーザ
- Webフィルタリングサービス
  - 認証エンジンセキュリティベンダー OEM提供

etc.・・・

エンタープライズ市場向け シングルサインオン（SSO） & ID管理システム

- IDaaSサービス 認証基盤
  - 通信事業者　2,000社
- 社内業務アプリ SSOシステム
  - 家電メーカー　7,000ユーザ
- 学内システム SSOシステム
  - 大学　15,000ユーザ
- OEM提供先

株式会社 スタイルズ　FUJITSU　Marubeni Network Solutions　NTT AT　HCNET エイチ・シー・ネットワークス株式会社　IP3

※　講演中でも、思いついたご質問は随時「Q&A」へご入力ください。
（お答えは原則として最後にまとめさせていただきます）

KAMOME Engineering

SaaSベンダーさまの最近の課題について

SaaSベンダーさまの最近の課題について

KAMOME Engineering

当社で伺っている課題には、一定のパターンがあります

- 複数サービスを展開して、顧客企業1社当たりの売上を増大したい
- できれば利用者数の多い（大口の）顧客企業を獲得したい
- 他社サービスとの連携を図って新規顧客の流入を促進したい

利便性の向上、連携インターフェース　が必要

KAMOME Engineering

課題を解決する方法は、、

自社提供サービス共通の
認証基盤を整備

» **シングルサインオン（SSO）化**
MFAにも対応して利用者認証を一元化

顧客企業のサービスの一部とする
（顧客認証基盤と連携）

汎用的・標準的な
連携インターフェースの整備

» **グローバル／モダンな認証方式の導入**

※　講演中でも、思いついたご質問は随時「Q&A」へご入力ください。
（お答えは原則として最後にまとめさせていただきます）

KAMOME Engineering

自社提供サービス共通の認証基盤を整備

➡ シングルサインオン（SSO）化

～　自社構築を検討する際のご参考として　～

KAMOME Engineering

「IDaaSでよいのでは？」 ➡ 検討を進めると現れる課題

課題 ❶

個々のシステムに
合わせ込んでくれない

「 機能 」

- IDaaSは一般的に個別対応はしてくれない
- SDK組み込み型もバリエーション次第

課題 ❷

利用者・サービスの
拡大につれて
確実に上昇する

「 コスト 」

- 「利用者数」「連携システム数」
「MFA対応等のオプション機能」 ・・・

要望に比例してライセンス費用の上昇も

KAMOME Engineering

メリット

■ 自社の都合に合わせた導入や運用が可能

- メンテナンスのタイミング、機能の改修や追加なども可能

■ 既存の運用リソースを有効活用可能

- 運用中のインフラを活用した導入、統合した運用も可能

■ ランニングコストの大幅軽減

- 長期運用を前提とすると、IDaaSに比べてトータルコストは大幅減も可能

KAMOME Engineering

課題

ノウハウや知見が必要

- 自社で運用やメンテナンスができる要員が必要

導入期間が長め

- サービス事業者の場合、運用開始まで 6ヵ月～12ヵ月程度？
  （要件定義など含む）

初期導入時の費用が高額

- 構築費用 ＋ ライセンス費用　合算で
  初期投資が数千万円台のプロダクトも･･･

KAMOME Engineering

導入の検討

「商用のSSO製品？」

高価格すぎる

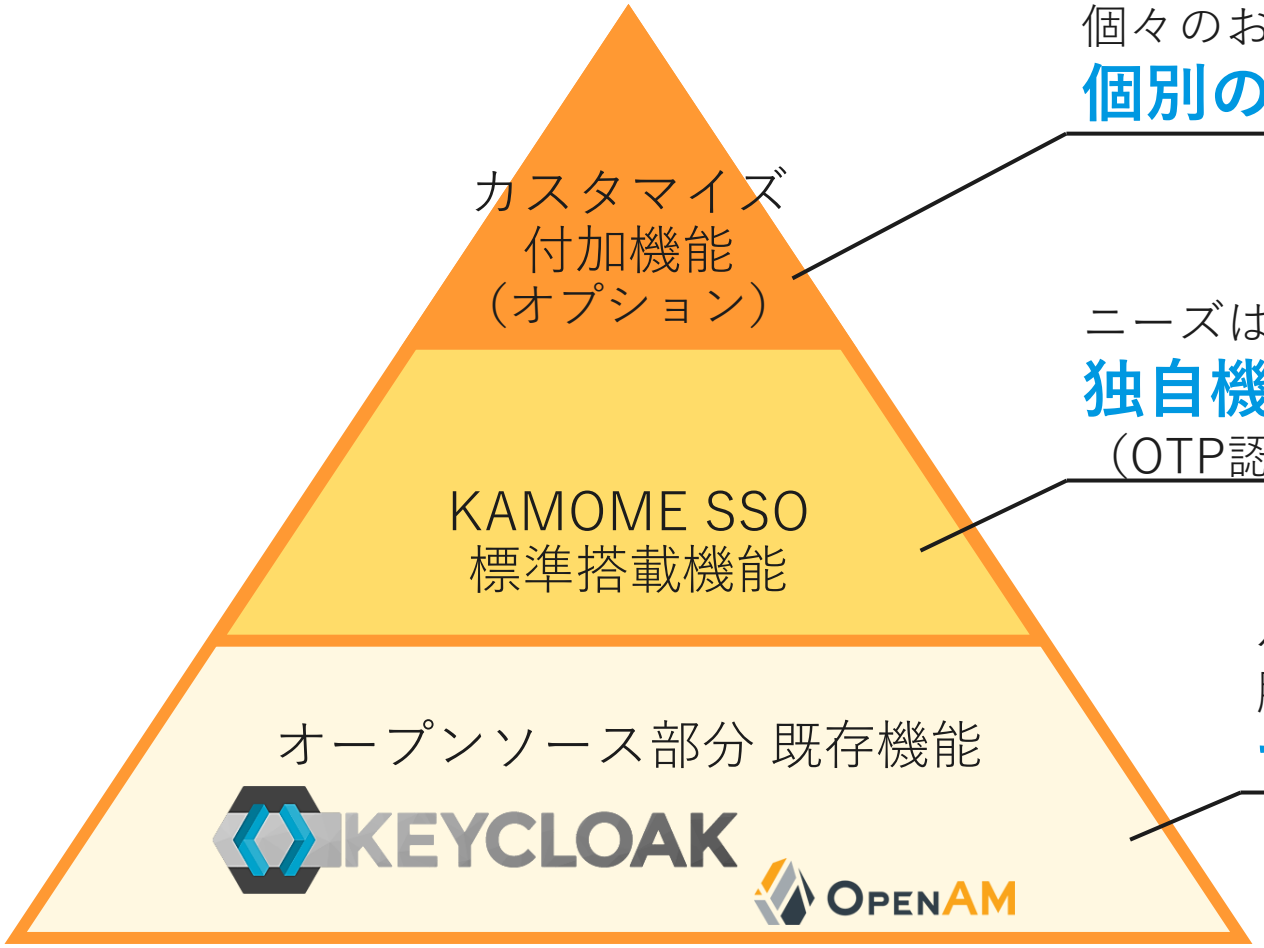
「オープンソースで導入？」

ノウハウや知見が無い

「ハイブリッドなソリューションがあればいいのでは」

- 必要な機能がある
- 国内でプロからのサポートがある
- 導入期間は短めがいい
- コストパフォーマンスもよい

オープンソースベースのSSO認証システム



個々のお客さまのご要望に応じた
個別の機能付加も可能

※ご要望に応じて見積

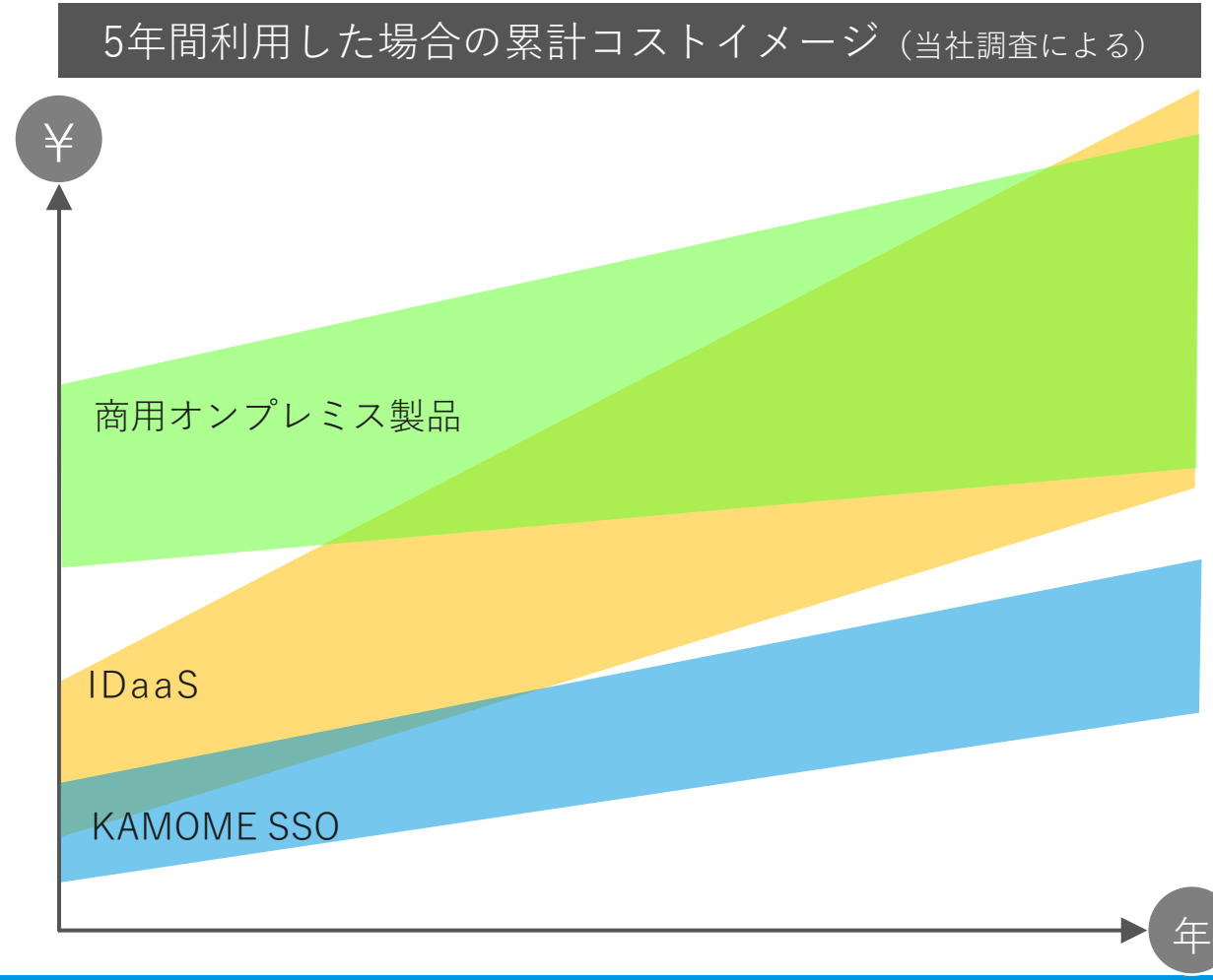
ニーズは多いがオープンソースになかった
独自機能を搭載
（OTP認証対応、リスクベース認証、Bot対応など）

バグの修正、機能改修、
脆弱性への対応 等
サポートサービスの提供

オンプレミス構築のメリットに加え・・・

■ 初期＆運用コストを大幅に軽減

- 利用者が多いほど差は明らか
- 長期運用が前提の場合、特に効果大



利用イメージ

KAMOME Engineering

課題を満たすための基盤

自社提供サービス共通の
認証基盤を整備

» **シングルサインオン（SSO）化**
MFAにも対応して利用者認証を一元化

顧客企業のサービスの一部とする
（顧客認証基盤と連携）

汎用的・標準的な
連携インターフェースの整備

» **グローバル／モダンな**
認証方式の導入

本日の本題

※　講演中でも、思いついたご質問は随時「Q&A」へご入力ください。
（お答えは原則として最後にまとめさせていただきます）

KAMOME Engineering

グローバル／モダンな認証方式の導入

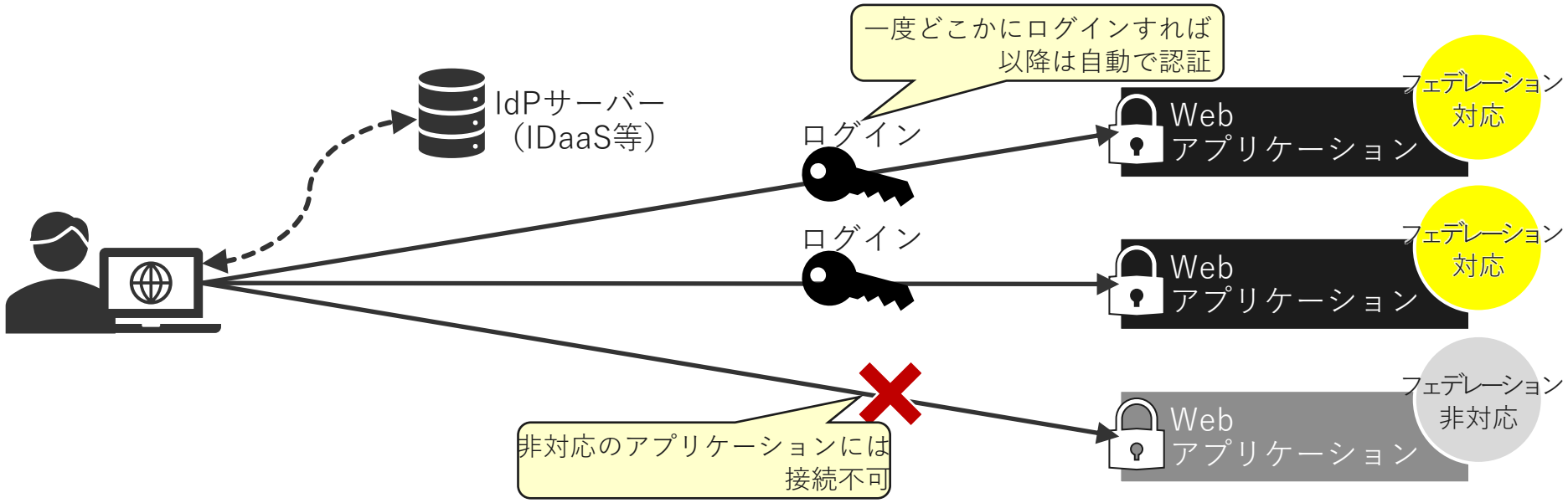
～ SaaSの「フェデレーション対応」 ～

KAMOME Engineering

SaaS利用時の認証方式のグローバルスタンダード

- ✓ 対応しているアプリが対象なら、アプリ改修不要、エージェント不要
- ✓ 多要素認証、ソーシャルログイン 等との連携が容易
- ✓ 協業などのための認証連携が容易
- ✓ 特にSaaSの利用者認証に多く利用されている

SAML v2.0 OpenID Connect OAUTH 2

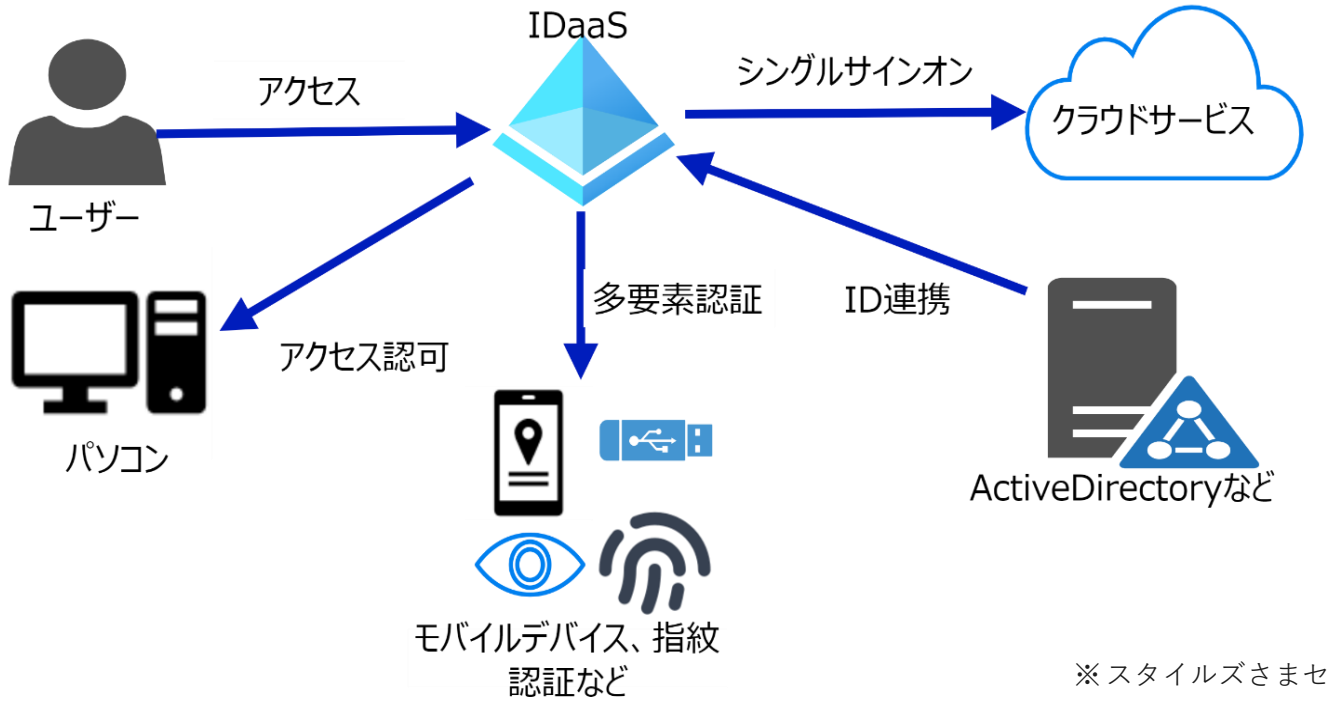


しかし、すべてのSaaSがフェデレーションに対応できているわけではない

KAMOME Engineering

SaaSの顧客となる企業にとっては…

- ✓ IDaaSによるSSO導入が進んでいる
- ✓ AzureADにオプション付加された機能を使って、IDaaSと同様のSSO基盤を構築する企業も増加
- ✓ ほぼすべてのケースで、フェデレーション方式が使われている



※スタイルズさまセミナー資料より引用

「採用するSaaSは、フェデレーション対応のものにそろえたい」

KAMOME Engineering

寄せられたご要望の例

■ SaaSベンダー側の課題

- **提供サービスが増える**ため、
  サービスの利用者アカウントをSSO化により統一して利便性向上を図りたい
- 提供サービスの会員向けに設置している**ポータルサイトをうまく活用**したい
- 自社サービスのSSOシステムと顧客企業のSSOシステムを連携させ、
  大手企業の採用を実現させたい
- 既存のサービスシステムを顧客企業のSSOシステムとフェデレーション連携させたいが、
  改修や既存方式との併存も必要
- ばらばらだった認証方式をグローバル標準に揃え、
  他社サービスとの協業や相互乗り入れを図れるしくみにしたい

KAMOME Engineering

寄せられたご要望の例

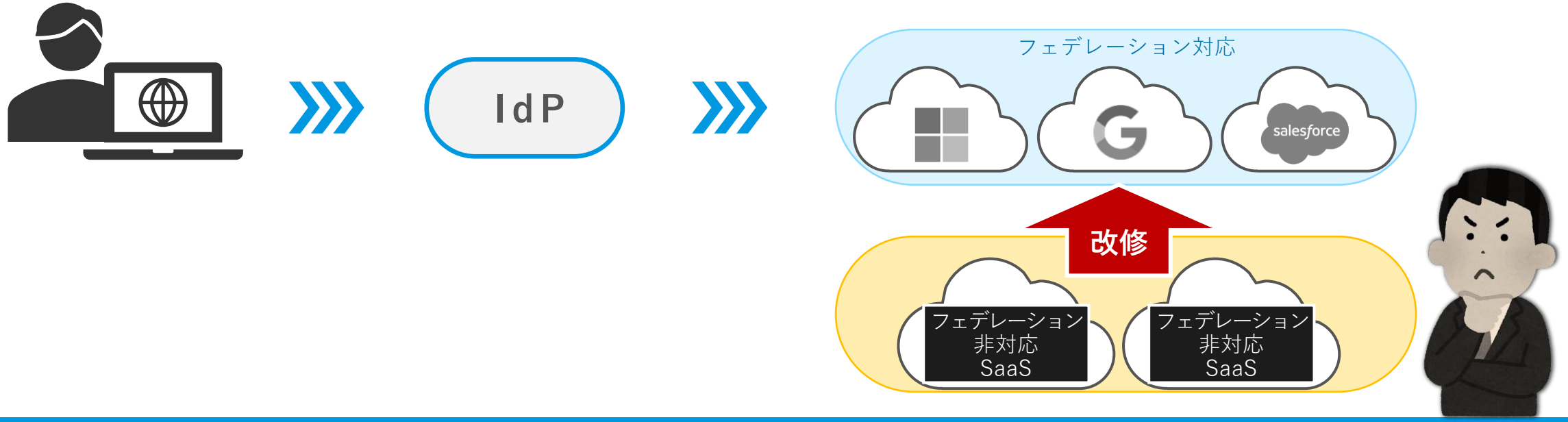
■ 顧客企業側の課題 （フェデレーション対応SaaSにまとめたい理由）

- 利用者個人に**パスワード管理**をまかせたくない
- SSO対象外の業務システムがあると、**SSOの導入効果**がじゅうぶんに得られない
- SSO化で各業務システムの**認証ログを一元化**して、内部監査やIT統制への対応を行いたい

KAMOME Engineering

選択肢❶　改修

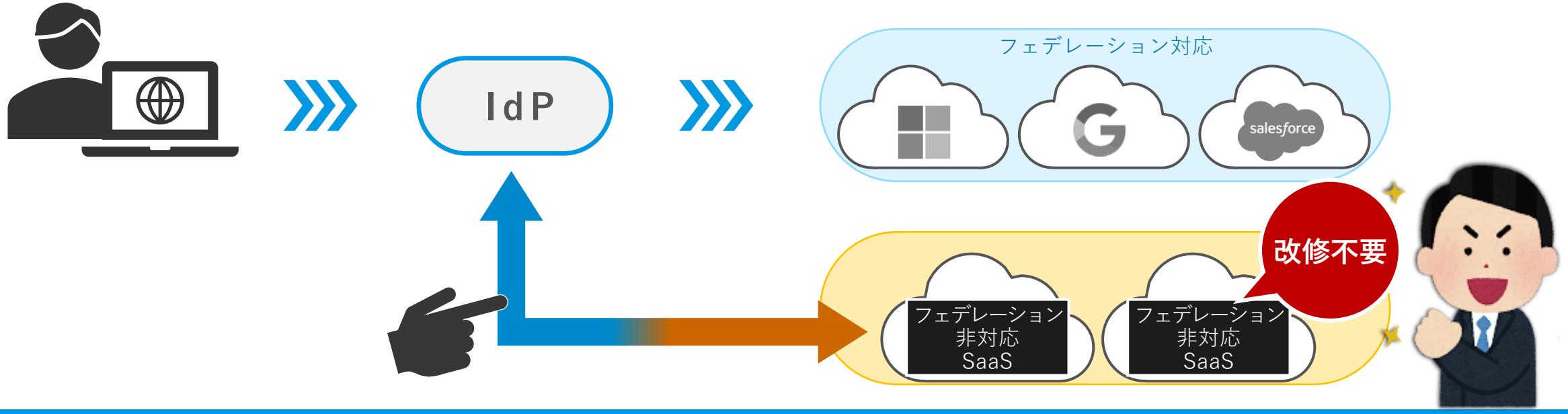
- すべてのサービスシステムを改修する
  ➡ **手間**と**コスト**と**知見**が必要
- 一度にフェデレーション対応への移行は難しく、移行期間が必要
  ➡ **利用者への周知や利便性の確保**が難しい



KAMOME Engineering

選択肢❷　IdPとサービスシステムを〝橋渡し〟

- SSOシステム（IdP）とサービスシステムをSAMLで連携させ、
  サービスシステムからの認証要求にはユーザに代わって回答するしくみ



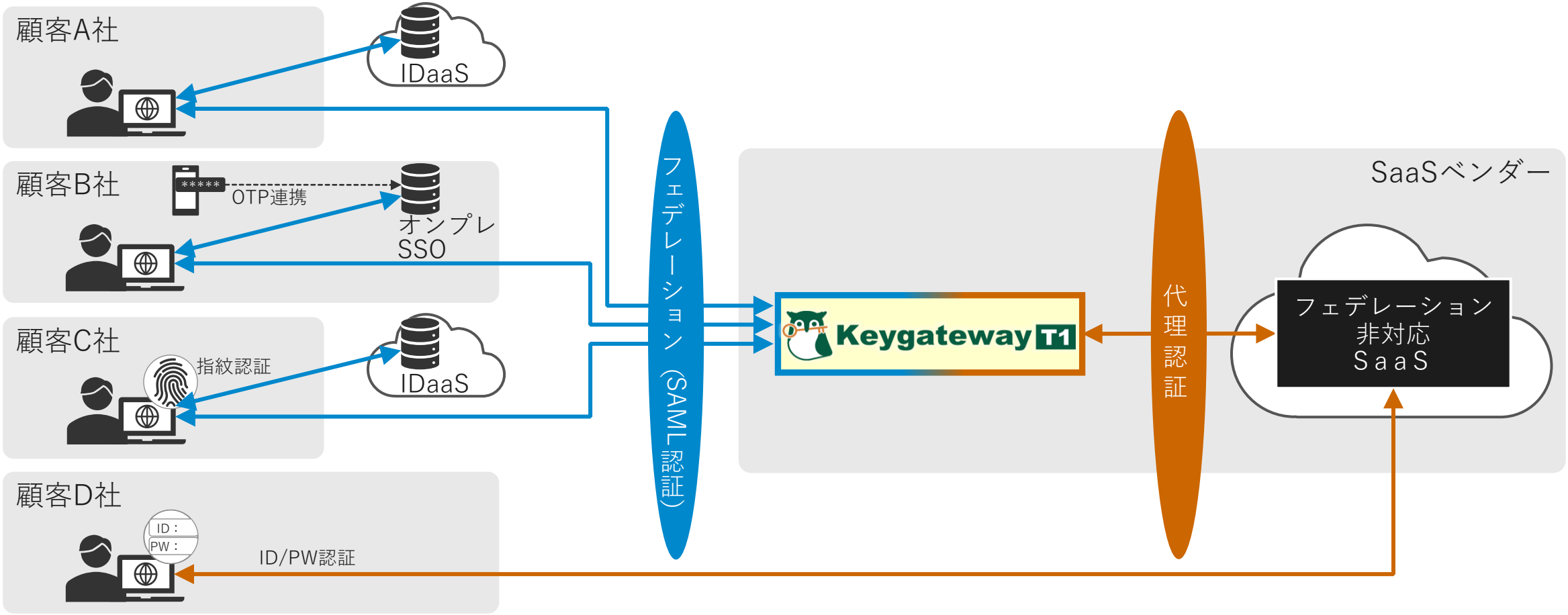
※　講演中でも、思いついたご質問は随時「Q&A」へご入力ください。
（お答えは原則として最後にまとめさせていただきます）

KAMOME Engineering

IdPとサービスシステムを〝橋渡し〟

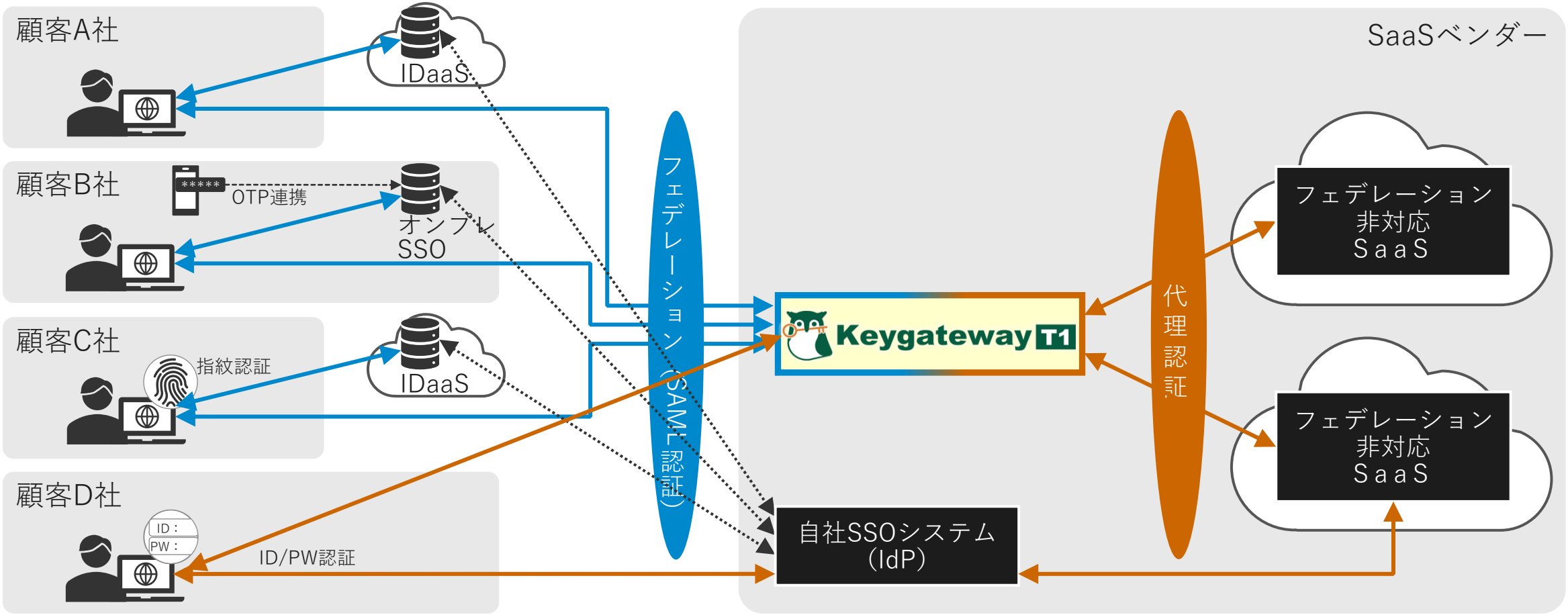
構成イメージ -1

顧客側のIdPを利用するケース



構成イメージ -2

顧客側とSaaSベンダー側のIdPが連携するケース



特長・利点

豊富な連携実績

国内で利用されている主要IDaaSの他、商用SSO製品やSSO向けオープンソースとも**広い連携実績**があります。

使い勝手向上

顧客企業　…　**自社システムの一部のような使い勝手**でSaaSを利用できます。
利用者　…　個別のパスワード管理から解放されます。

改修が不要

既存のサービスシステムにも、顧客企業側にも、
フェデレーション対応のための改修は不要です。

さらに、こんな特長・利点も、、

顧客企業へのアプローチ強化	フェデレーション対応サービスと同様に扱えるため、**採用のハードル**が下がります。
連携先増加の対応が容易	IdPやサービスシステムの連携をKeygatewayT1が担うため、**サービスや顧客の拡張・拡大などへの対応**が容易になります。
多様なサービスに対応	**ID体系やパスワードが異なる**複数のサービスにも対応可能です。
端末用ソフト不要	利用者端末（PC）に、**端末用アプリやエージェントツール等は不要**です。
OpenID Connectにも対応	**SAML**の他、BtoCサービスに多く使われる **OpenID Connect** にも対応しています。

大別すると、3つのモデルに分けられます。

❶ サービスサイトの利用者向け認証基盤を構築

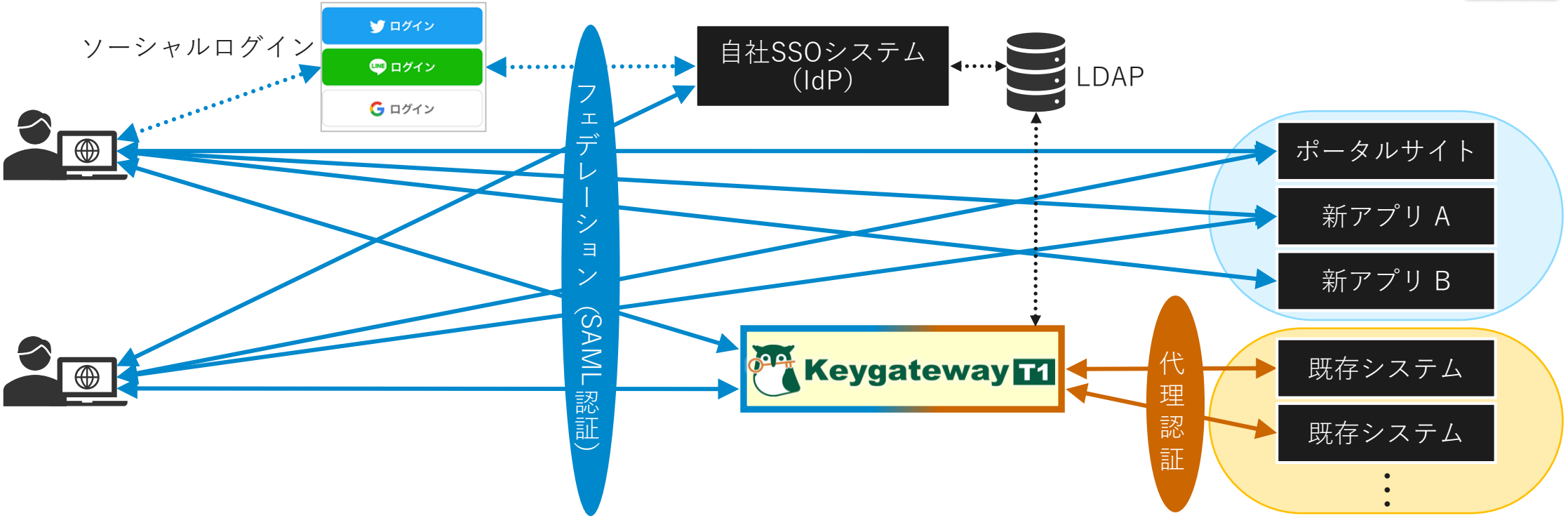
❷ フェデレーション対応していない自社クラウドサービスを
フェデレーション認証可能に

❸ 自社認証システムと顧客企業の認証システムの連携（❶＋❷）

それぞれについて、具体的な事例を見ていきましょう。

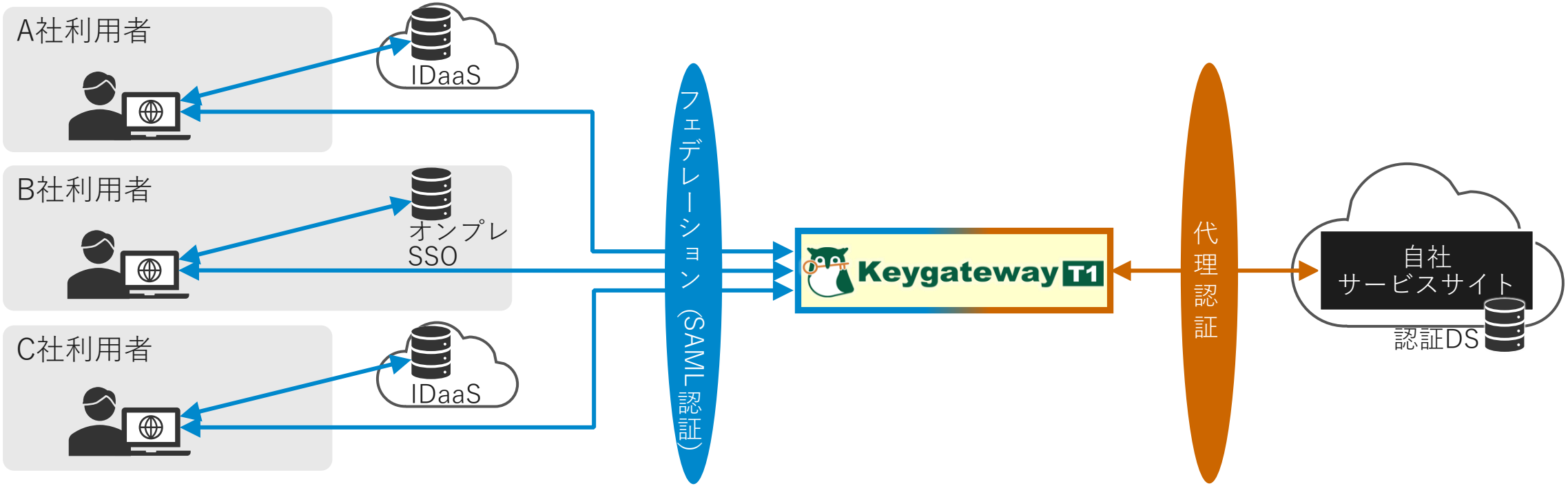
自社サービスサイトの利用者向け認証基盤を構築

- 提供中サービスの認証がバラバラになっており、利用者にとって不便だったが、KeygatewayT1を導入することにより、認証が一元化して利便性が大幅に向上した
- 多数の非SAML対応サービスの対応に莫大な改修コストと長期間の工期がかかる見込みだったが、KeygatewayT1を導入することで、コストも導入期間も削減できた



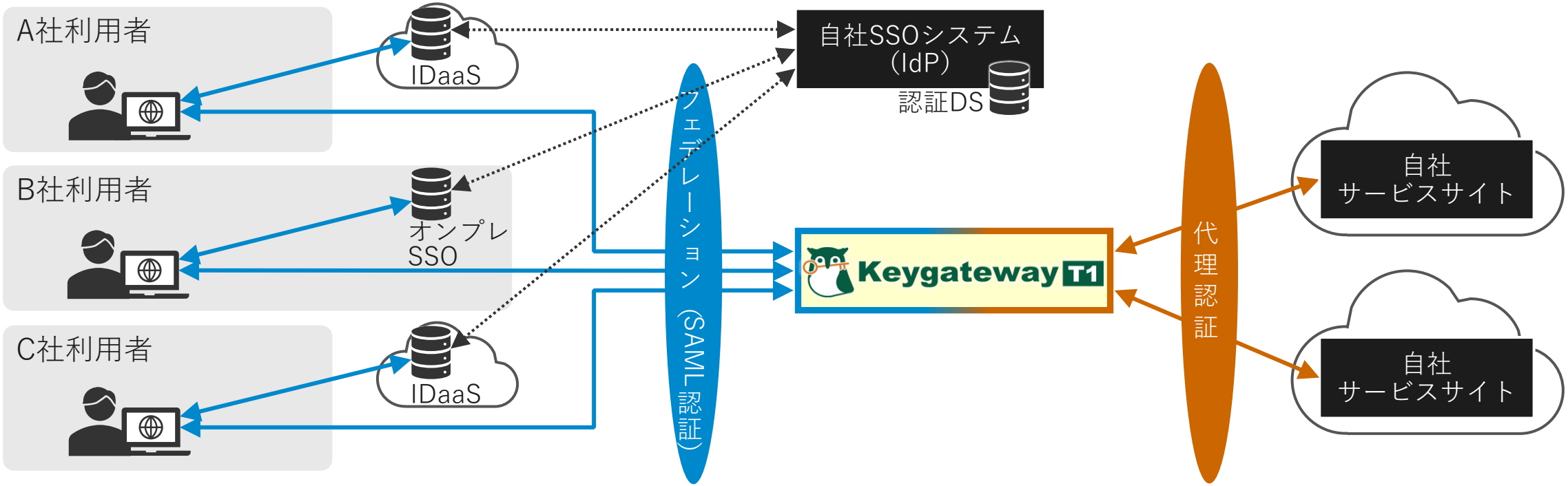
自社クラウドサービスをフェデレーション認証可能に

- 自社クラウドサービスを改修せず、顧客ごとのIdPに対応できるようになった
- 顧客利用者はパスワードレスで利用できるようになり、満足度アップ
- 自社にSSO環境を導入済みの大手企業にもアプローチがしやすくなった
- 既存のログイン環境とも共存できるため、既存顧客の使い勝手もそのまま維持



自社認証システムと顧客企業の認証システムの連携

- 顧客利用者は自社のSSOでログインすれば利用可能となり、利便性が大きく向上
- 自社認証システムと顧客企業の認証システムが連携することで、
  複数のサービスサイトの設定追加や変更が不要となり、運用への影響範囲を極小に抑制
- 自社のSSOを使用する利用者とも併存でき、顧客の状況に合わせた導入提案が可能に



導入までの基本的な流れ

ご提案（0.5ケ月～）

導入（0.5～4ケ月）

稼働後

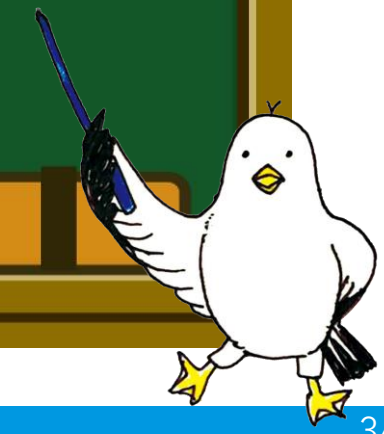
お問い合わせ → ご要望のヒアリング → 概算お見積り提示 → ご発注 → 要件定義 → 設計・構築 → 納品・ご検収 → サービスご利用開始 → サポートサービス開始

最短1.5ヶ月～で導入可能です
※システム数などによる

まとめ

KAMOME Engineering

- SaaSベンダーには、
  複数サービス展開、**顧客企業システム化**、**他社協業** 等の課題があります。
- 課題の解決の一助として、**認証基盤の整備** が有効です。
- **SaaSのフェデレーション対応**により、
  ・顧客企業の認証システム（IDaaSやAzureAD等）
  ・他社サービスの認証システム
  と容易に連携が可能になります。
- 「KeygatewayT1」は、**サービスシステムの改修不要**で
  フェデレーション対応を可能にし、手間とコストを抑制します。



ありがとうございました

セキュリティの土台は、まず「IDの適切な管理」から ――

ID管理クラウドサービス「Keyspider」

「業務システムはSaaSだけじゃない」社内システムも含めた安全な認証統合を実現

ゼロトラスト接続サービス「KeygatewayC1」

■ **お問い合わせ先**

- かもめインサイドセールスチーム　i-sales@kamome-e.com
- お問い合わせフォーム　https://solution.kamome-e.com/contact/

かもめエンジニアリング株式会社

KAMOME Engineering
日本でいちばん仕事が大好きなチームです！