マジセミ

SSO認証基盤を、IDaaSではなく「社内構築」するメリットと、その手法を解説

中～大規模・長期間の運用に適した「KAMOME SSO」説明会

KAMOME SSO

2022.10.04

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！

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数多く担当する。

2008年、かもめエンジニアリング社設立。
統合認証基盤やビッグデータ処理など、通信サービス事業向けのシステムで
多くの導入実績を上げつつ、2017年にはSSO分野で「KAMOME SSO」を提供開始。
SSOやID分野のセミナーで年間30回程度講師を担当。

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

2021年、テレワークのセキュリティ強化を推進するため、
ゼロトラスト接続サービス「Keygateway C1」を発表

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

オライリー・ジャパンより刊行の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。

「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
エイチ・シー・ネットワークス株式会社
FUJITSU
NTT AT
IP3

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/Keygateway（かもめSSO / キーゲートウェイ）

- **SSO認証サーバ「Keycloak」**
  OSSをベースに独自の機能をプラス、B2CからB2Bまでカバー
- 「Keygateway T1」
  SAML非対応の業務アプリをプライベートSaaS化するツール
- 「Keygateway C1」
  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

※　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）

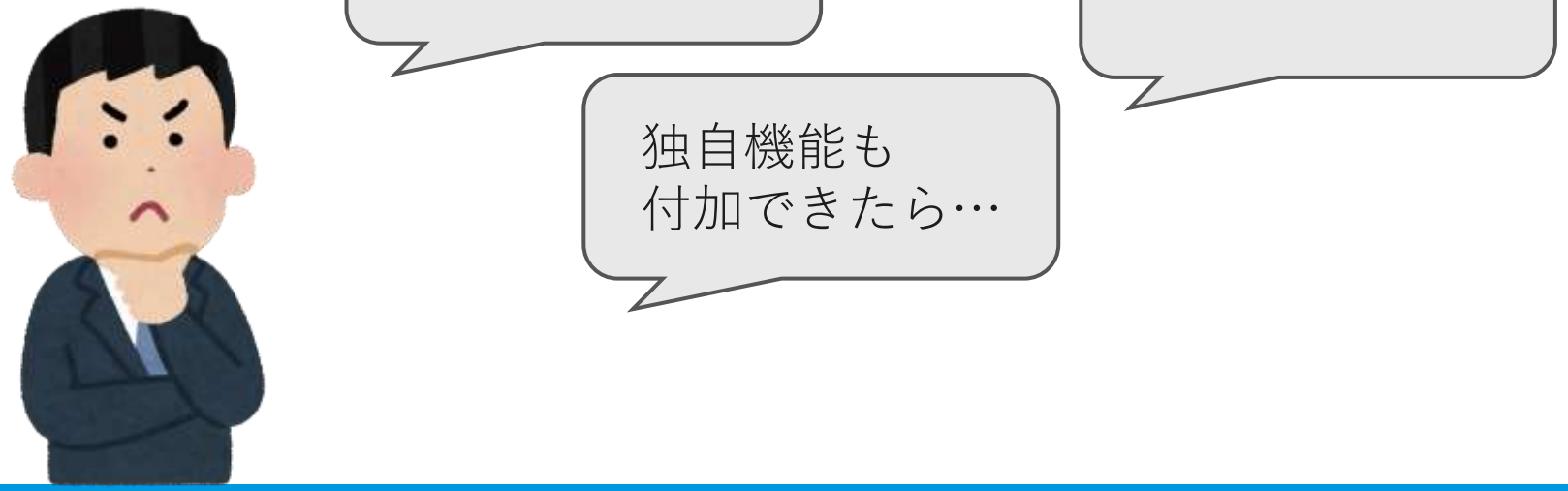
KAMOME Engineering

認証基盤と言えばIDaaS？

認証基盤と言えば IDaaS ？

KAMOME Engineering

「シングルサインオンを行う認証基盤として IDaaSは当社に適しているか？」



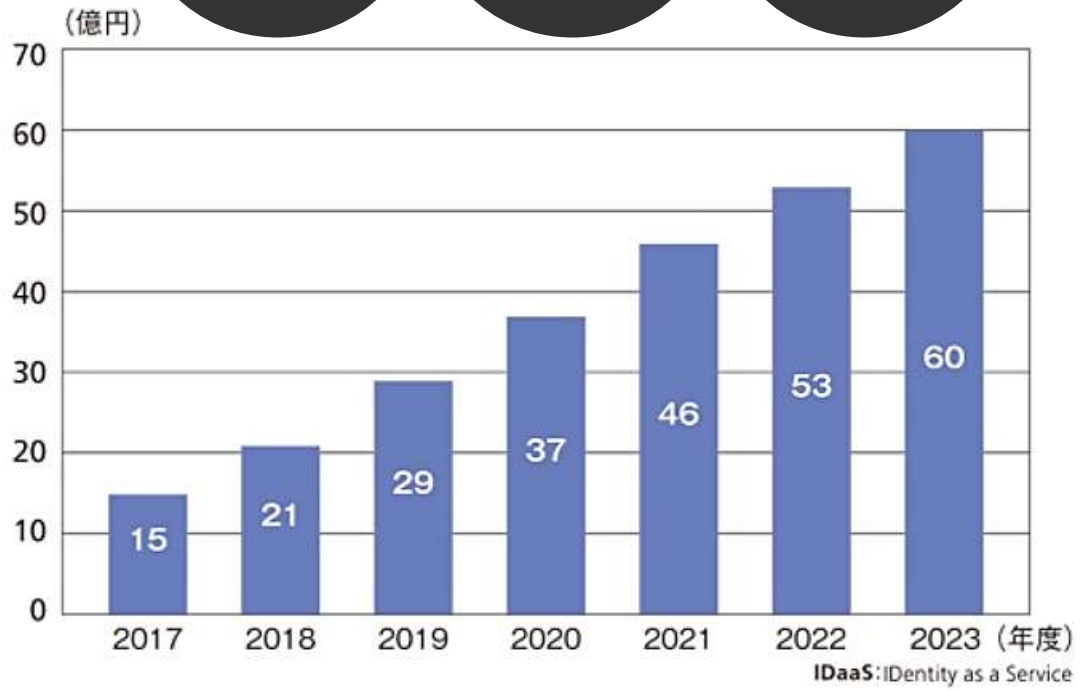
KAMOME Engineering

クラウドの普及と共に伸びるIDaaS

導入が早い

初期費用が安い

運用がラク



Azure Active Directory

onelogin

IIJiD

auth0

GMOトラスト・ログイン

HENNGE One

okta

2020年1月　ITR社調査レポート
「アイデンティティ・アクセス管理／個人認証型セキュリティ市場2021」
日経クロステック記事 https://xtech.nikkei.com/atcl/nxt/column/18/01615/033100001/ より引用

KAMOME Engineering

しかし、一定以上の規模で使い続けるには課題も。

課題 ❶

個々のシステムに
合わせ込んでくれない

「 機能 」

課題 ❷

利用者の増加につれて
確実に上昇する

「 コスト 」

KAMOME Engineering

個々のシステムへの合わせ込み

■ 自社システム向けに認証システムのほうを合わせられない

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

■ 対応が難しい認証方式も

- IDaaSは「SAML」「OpenID Connect」等のフェデレーションが得意
- フェデレーション対応していないシステムとの連携は、困難な場合も多い
  （ましてWebシステム以外は…）

SSOに巻き取れないシステムがあると
セキュリティ、利便性、ともに課題が残る

利用規模拡大に伴うトータルコスト

■ スモールスタートに適したIDaaS

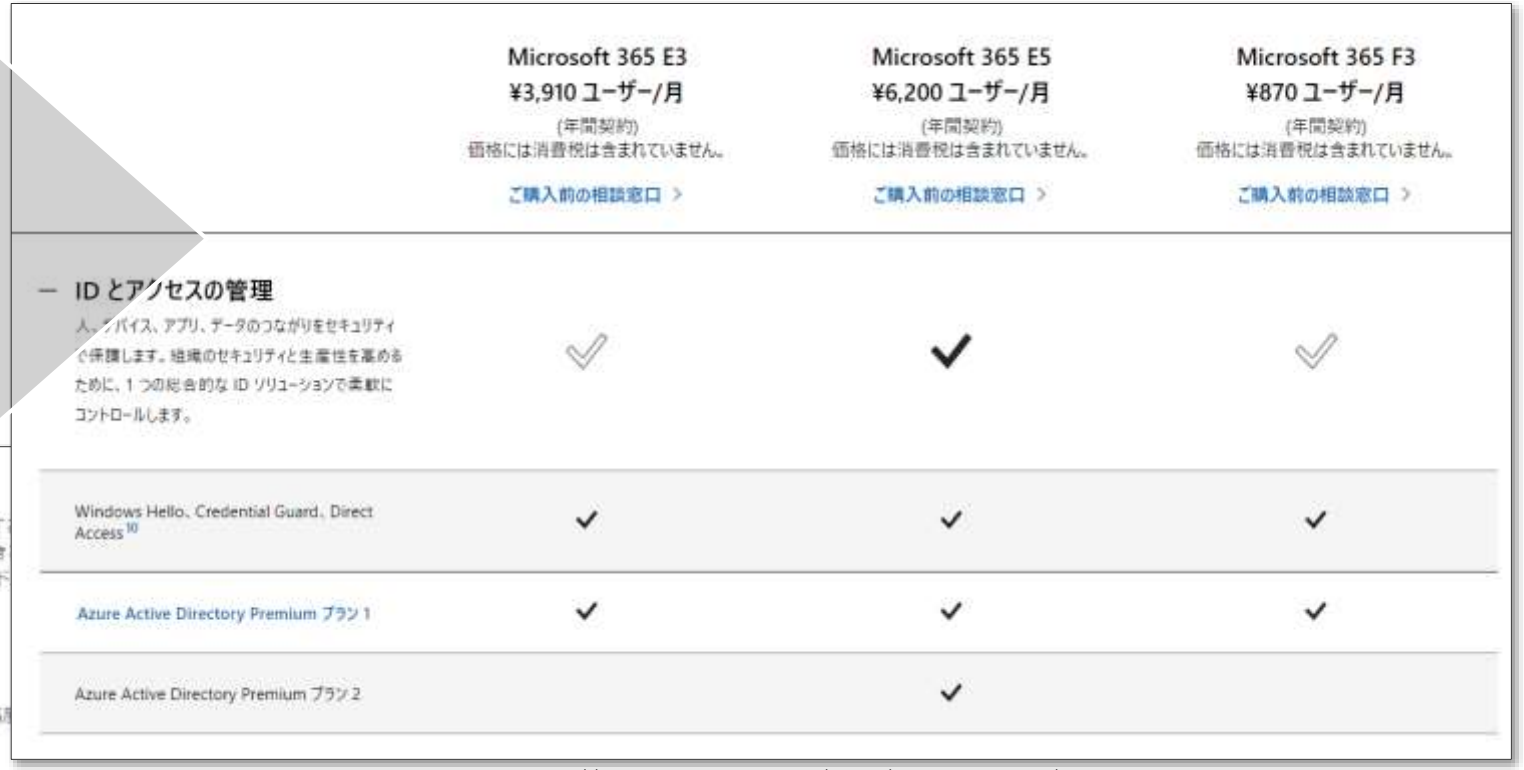
- 無償・割安プランがある
- ID数課金の他、フリーミアムモデルや認証数による従量課金を採用するIDaaSも
- 初期構築費用は抑制できる

「利用者数」「連携システム数」「MFA対応等のオプション機能」・・・
増加に比例してライセンス費用が上昇

課題❷　コスト

たとえばMS365の場合・・・

1,000ユーザーで
- 月額　　87万円　～　391万円
- 年額　1,044万円　～ 4,692万円



	Microsoft 365 E3 ¥3,910 ユーザー/月 (年間契約) 価格には消費税は含まれていません。 ご購入前の相談窓口 >	Microsoft 365 E5 ¥6,200 ユーザー/月 (年間契約) 価格には消費税は含まれていません。 ご購入前の相談窓口 >	Microsoft 365 F3 ¥870 ユーザー/月 (年間契約) 価格には消費税は含まれていません。 ご購入前の相談窓口 >
ID とアクセスの管理 人、デバイス、アプリ、データのつながりをセキュリティで保護します。組織のセキュリティと生産性を高めるために、1 つの総合的な ID ソリューションで柔軟にコントロールします。	✓	✓	✓
Windows Hello、Credential Guard、Direct Access[10]	✓	✓	✓
Azure Active Directory Premium プラン 1	✓	✓	✓
Azure Active Directory Premium プラン 2		✓	

https://www.microsoft.com/ja-jp/microsoft-365/compare-microsoft-365-enterprise-plans

Premium P1

Azure Active Directory Premium Edition は、より要求の厳しい ID およびアクセスの管理を必要とする組織を支援す
管理機能が追加され、ハイブリッド ユーザーがオンプレミスの機能とクラウドの機能にシームレスにアクセスでき
アプリケーション アクセス、セルフサービスの ID とアクセスの管理 (IAM)、セキュリティに関して、ハイブリッド
すべてが含まれています。

Premium P2

Azure Active Directory Premium P2 には、他のすべての Azure Active Directory エディションの全機能に加えて、高
れます。

Active Directory ドキュメントに記載されている各レベルの機能比較。

購入方法	Azure Premium P1	Azure Premium P2
Microsoft 担当者	Microsoft 365 に付属	Microsoft 365 に付属
オンライン	¥820.171 ユーザー/月*	¥1,230.256 ユーザー/月*

* 年間契約

https://azure.microsoft.com/ja-jp/pricing/details/active-directory/

※　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

SSOを社内構築したら

KAMOME Engineering

メリット

自社の都合に合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

IDaaSの利用費用よりコスト削減可能

- 長期運用が前提ならばIDaaSよりコストメリットも

KAMOME Engineering

課題

■ 運用管理が必要

- 自社で運用やメンテナンスができるメンバーが必要

■ 導入期間が長い

- 運用開始まで6ヵ月～12ヵ月程度？

■ 初期費用が高額

- 構築費用 ＋ ライセンス費用　を合わせると
  初期投資が数千万円台後半以上必要なプロダクトも･･･

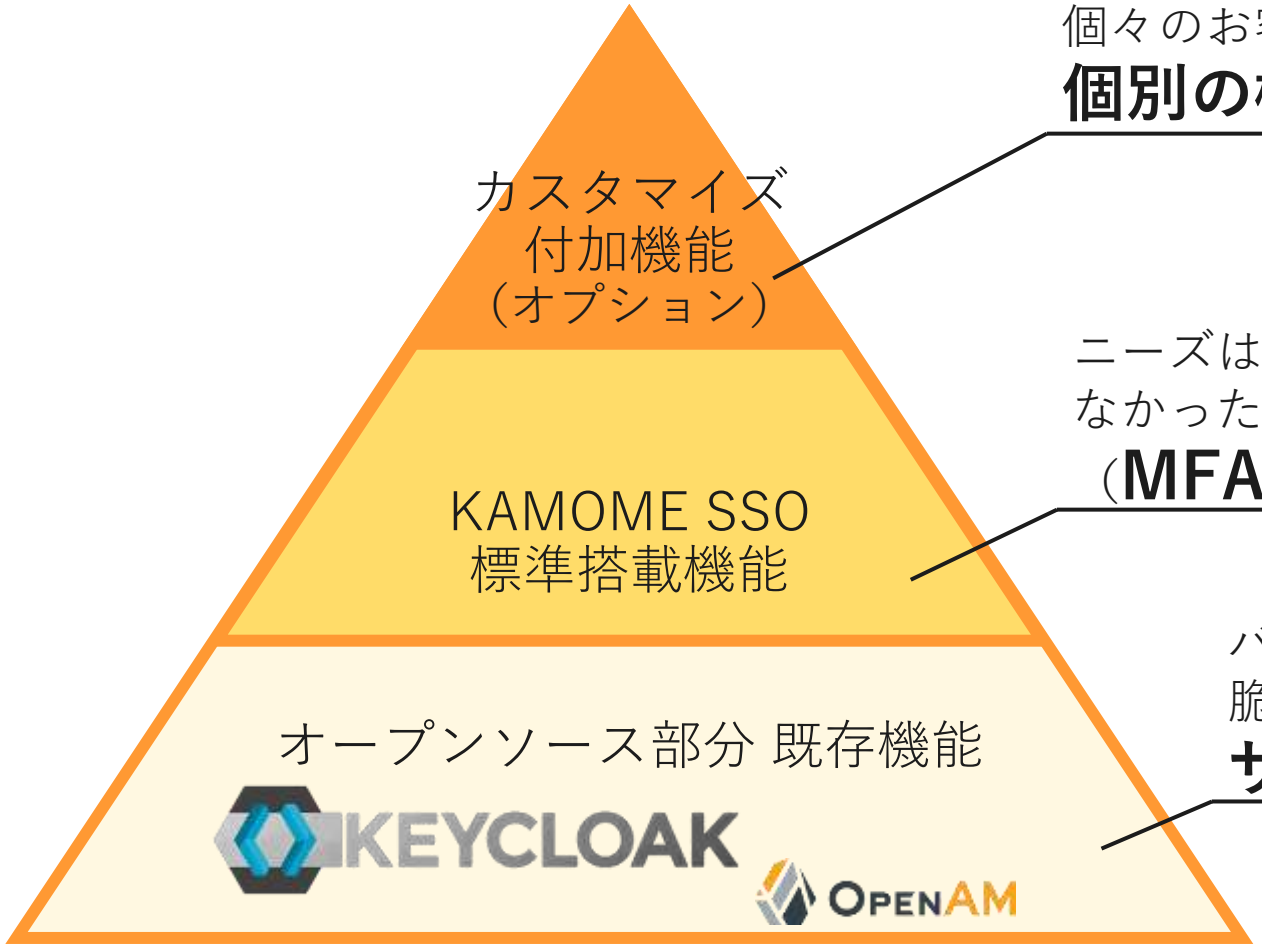
➡ 解決策があります

※　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

オンプレ×オープンソースベースのSSOシステム

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

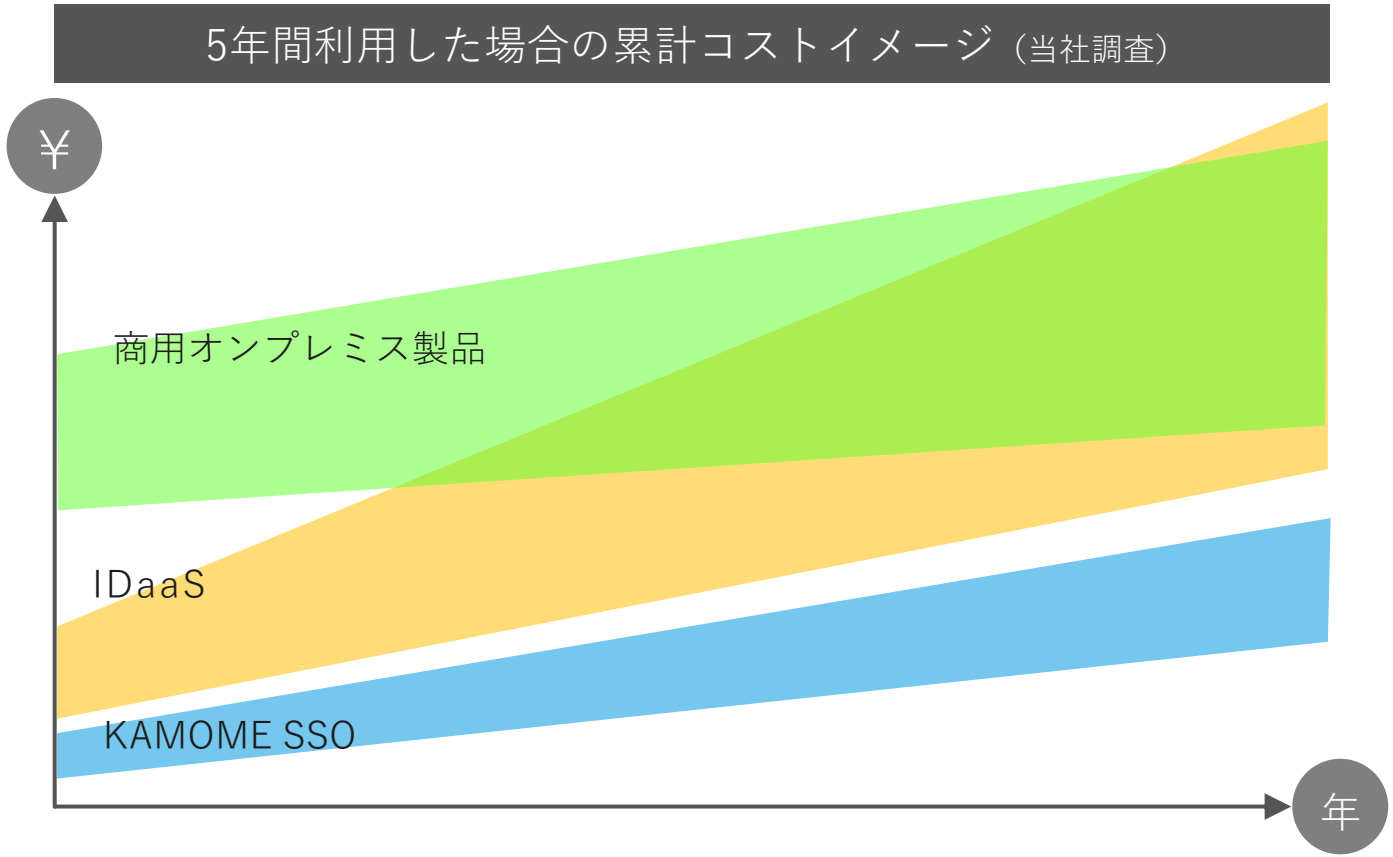
ニーズは多いがオープンソースに
なかった機能を独自に搭載
（**MFA認証**、**Bot対応**など）

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



KAMOME SSO主要機能

認証機能	SAML対応	○	
	OpenIDConnect対応	○	
	Oauth対応	○	
	エージェント方式による認証	○	接続先アプリケーションにエージェントツール要
	多要素認証対応 クライアント証明書による認証	○	
	多要素認証対応 ワンタイムパスワード認証	○ TOTP/HOTP	検証確認済み： ・Google Authenticator（Google製） ・FreeOTP Authenticator（RedHat製）
	多要素認証対応 ワンタイムパスワード認証（メールベース）	○	KAMOME SSO独自機能
	多要素認証対応 FIDO2対応	○	
	LDAP連携	○	
	Active Directory連携	○	
	Desktop SSO	○	Active Directoryを利用してWindowsログオンと連携
	リスクベース認証 ・認証失敗回数チェック ・最終ログインからの経過時間チェック ・IPアドレス履歴チェック ・IPアドレスによるアクセス制限 ・過去にログインした事があるブラウザかチェック	○	KAMOME SSO独自機能
	reCAPTCHA（Bot対応）	○	KAMOME SSO独自機能
	その他の認証モジュール対応	外部RDB対応 （予定）	
認可機能	サイトごとのアクセス制限	○ （予定）	KAMOME SSO独自機能 SAMLベース
管理機能	アカウントロック	○	所定回数のログイン失敗でロック
	認証ログ出力	○	
	Web GUI	○	
	GUIへの自社ロゴ表示	有償オプション	
その他、お客さま要望によるカスタマイズ		有償オプション	

❶ 地域インフラ提供会社【顧客数：単体約40万】

課題・要望

- グループ含めた複数の提供サービスでID/PWがバラバラになっており、顧客の利便性が図れない
- 利用状況の把握・通知のデジタル化が必要になったのを機に、まとめてSSO化したい
- ソーシャルログインやMFA対応も導入したい

IDaaSを検討

- @100円だとしても 4,000万円／月
- MAUベースのものは費用が予測できず予算化困難
- ユニバーサルサービスとしてのサービス提供
  ＝利用者へ転嫁できないコスト

自社構築を検討

- 商用アプリもコスト高（初期費用で数億円）

オープンソースなら安い？

- しかし自社ではサポートできない

オープンソースベースのプロダクト

KAMOME SSO

必要な機能を満たし、コストも抑制

※ 対象サービスにはフェデレーション非対応のものもあるため、
併せて「Keygateway T1」も採用　【後述】

② BtoBサービス提供会社【顧客数：約1,000社 10万アカウント】

課題・要望

- 他社サービスとの連携が必要になった
- 利用者の利便性とセキュリティ確保の観点から、認証連携（ OpenID Connect）を希望

コストの問題

- IDaaSは、導入コストは抑えられるが利用費用が利用者数に比例して上がり、予算化が困難
- 顧客に転嫁は受け入れられにくいが、自社で負担するのも難しい

オープン性・専門性の問題

- 技術的にブラックボックスなプロダクトやサービスは望ましくなく、自社でも把握可能であって欲しい
- 認証系のノウハウを持ってないため、この分野に強く知見と実績あるベンダーと組みたい

〝認証・認可のエキスパート〟が提供

KAMOME SSO

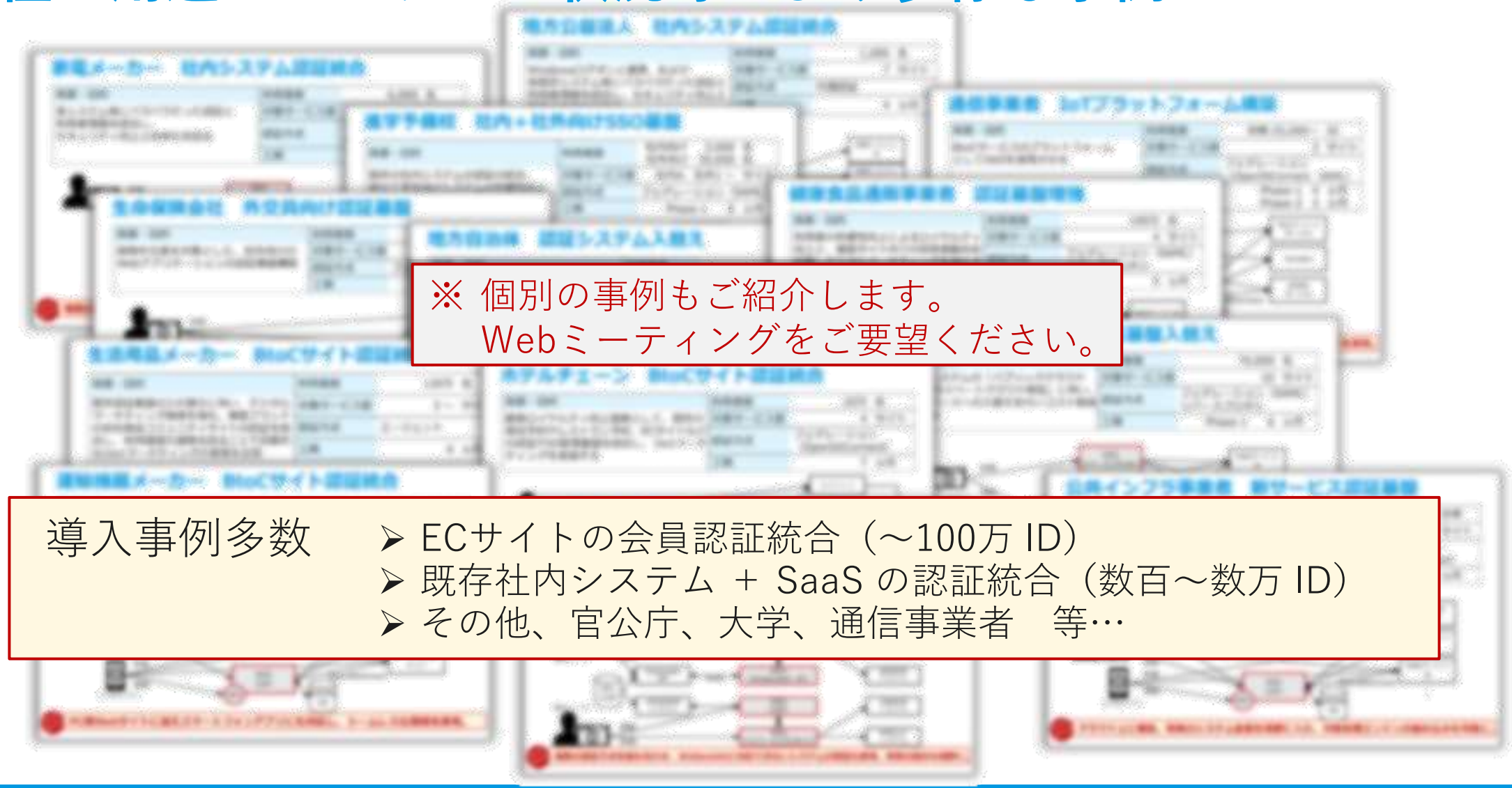
コスト抑制しつつ、さまざまなご要望に柔軟対応

KAMOME SSO 事例より

	保険会社 外交員用Webアプリケーション認証統合	地方自治体 認証システム入替え	運輸事業者 サービス認証基盤入替え	大手SI事業者 ポータルサイト連携
利用者数	約100,000	約5,000	約70,000	当初 約600 （最大数万想定）
接続先システム数	4	10	10	3
認証方式	SAML（フェデレーション）	SAML（フェデレーション） 代理認証【※】	SAML（フェデレーション） リバースプロキシ【※】	SAML（フェデレーション）
特長・付加機能	• 利用者によるパスワード変更用画面など付加	• ソーシャルネットワークとの相互認証 • 多要素認証との連携	• スマートフォンからの利用を想定したAPIも提供	• IPアドレスによる接続制限 • 多要素認証との連携
工期（試験期間含む）	4ヵ月	5ヵ月	6ヵ月	6ヵ月

【※】 Keycloakベースの場合は、別途「Keygateway」との併用が必要

業種・用途・システムの状況等により多様な事例



※ 個別の事例もご紹介します。
Webミーティングをご要望ください。

導入事例多数

- ECサイトの会員認証統合（～100万 ID）
- 既存社内システム ＋ SaaS の認証統合（数百～数万 ID）
- その他、官公庁、大学、通信事業者　等…

ライセンス・料金の体系

システムの規模に応じた一律の利用料金体系

- ライセンス＋サポートサービスを、サブスクリプションスタイルで提供

利用者ID数単位ではない

➡ 利用者が増加しても金額は変更なし

認証要求数などによる従量課金ではない

➡ 必要な年間費用が明確で予算化しやすい

料金イメージ

「3,000ユーザー」「接続システム数15個」のケース

- IDaaSの場合　…　一般的に 1,000万円超（年額）
- **KAMOME SSO の場合 …　IDaaSの1/3程度（年額）＋ 初期導入費用**

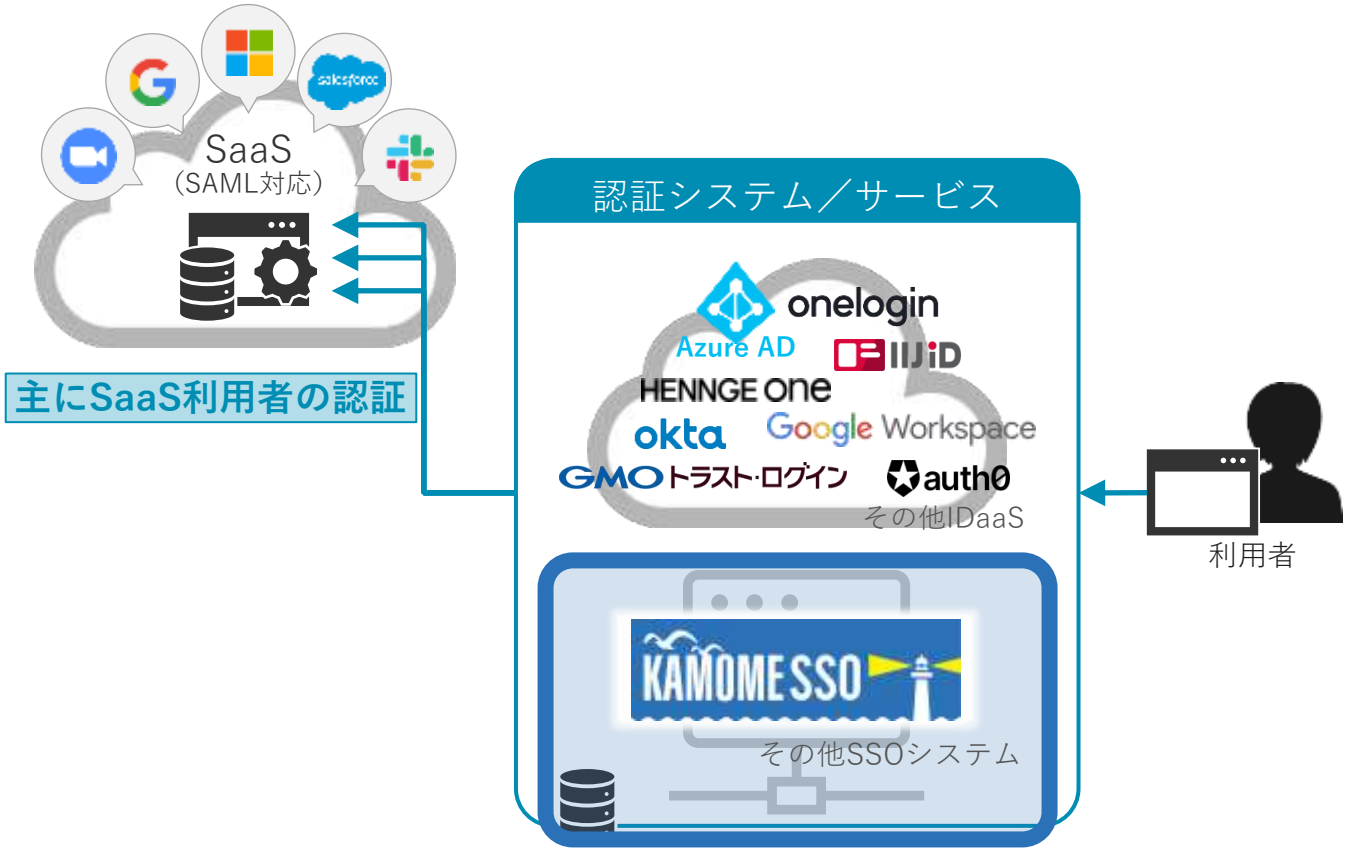
※　講演中でも、思いついたご質問は随時「Q&A」へご入力ください。
（お答えは原則として最後にまとめさせていただきます）

KAMOME Engineering

SSOだけではない

ID管理 ～ 利用者認証・認可 のトータルソリューション

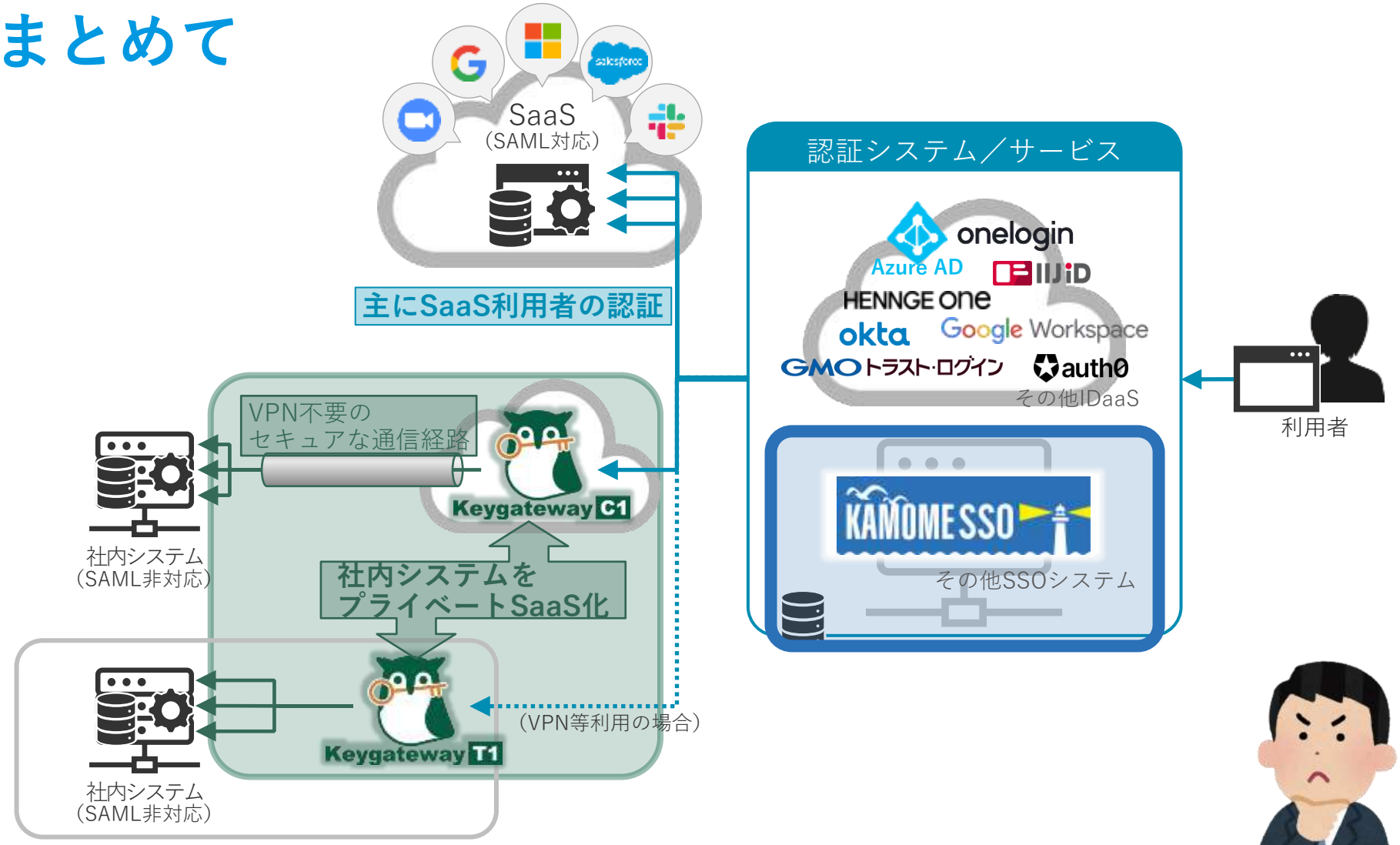
主にSaaS利用者の認証



業務システムはSaaS以外にもあるのだが…？

KAMOME Engineering

社内システムもまとめて認証一元化

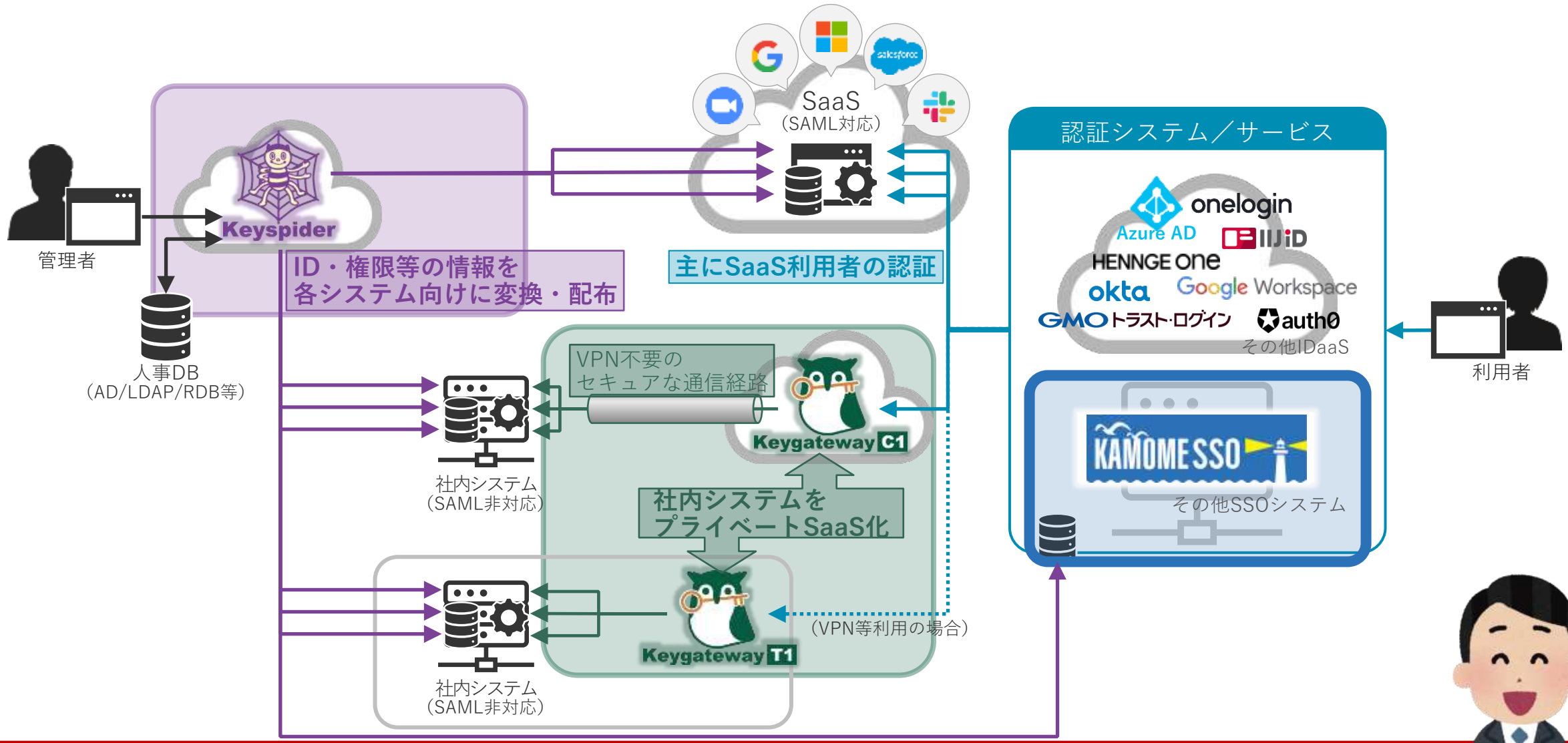


さらに…

すべてのシステムへID・権限情報を適切に反映させるには…？

ID管理 ～ 利用者認証・認可 のトータルソリューション

KAMOME Engineering



メンテナンスの抜け漏れも防ぎ、トータルな接続制御でセキュリティ向上

まとめ

- IDaaSは、スモールスタートには非常に便利ですが、
  規模や利用形態によっては適さない場合もあります。
- 自社システムへの合わせ込み、コストの抑制が可能な、
  オープンソースベースの「KAMOME SSO」があります。
- 「KAMOME SSO」は、ユーザー認証分野で多くの実績と知見を持つ
  かもめエンジニアリングが提供しています。
- オンプレ等の自社システムへの安全な接続には「Keygateway」
  ID・権限情報の管理には「Keyspider」もご検討ください。

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！