

CIAM検討の際に留意したいポイント

～ 求められるSSO基盤の選び方 ～



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、シングルサインオンシステム「KAMOME SSO」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」提供開始。

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。理事。

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)

趣味 料理と読書。歴史小説とSF、時々マンガ。

最近のヒットは、マーサ・ウェルズ『システム・クラッシュ マーダーボット・ダイアリー』。



画像引用：
オライリー・ジャパン



ID管理・ユーザー認証分野を中心に展開

統合認証基盤システム ケイフェック KFEP

- 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

特許取得

RADIUS認証サーバ フルフレックスKG fullflex 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

特許取得

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

- SSO認証サーバ「KAMOME SSO」
オープンソースをベースに独自の機能付加、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に替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

特許出願中

ID管理クラウドサービス キースパイダー Keyspider

- 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）
- Entra ID（旧AzureAD）、Microsoft 365、Google Workspace、Salesforce、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

ID管理・ユーザー認証分野を中心に展開

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

etc.・・・

- OEM提供先



※ 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)

大規模Webサービス用認証基盤

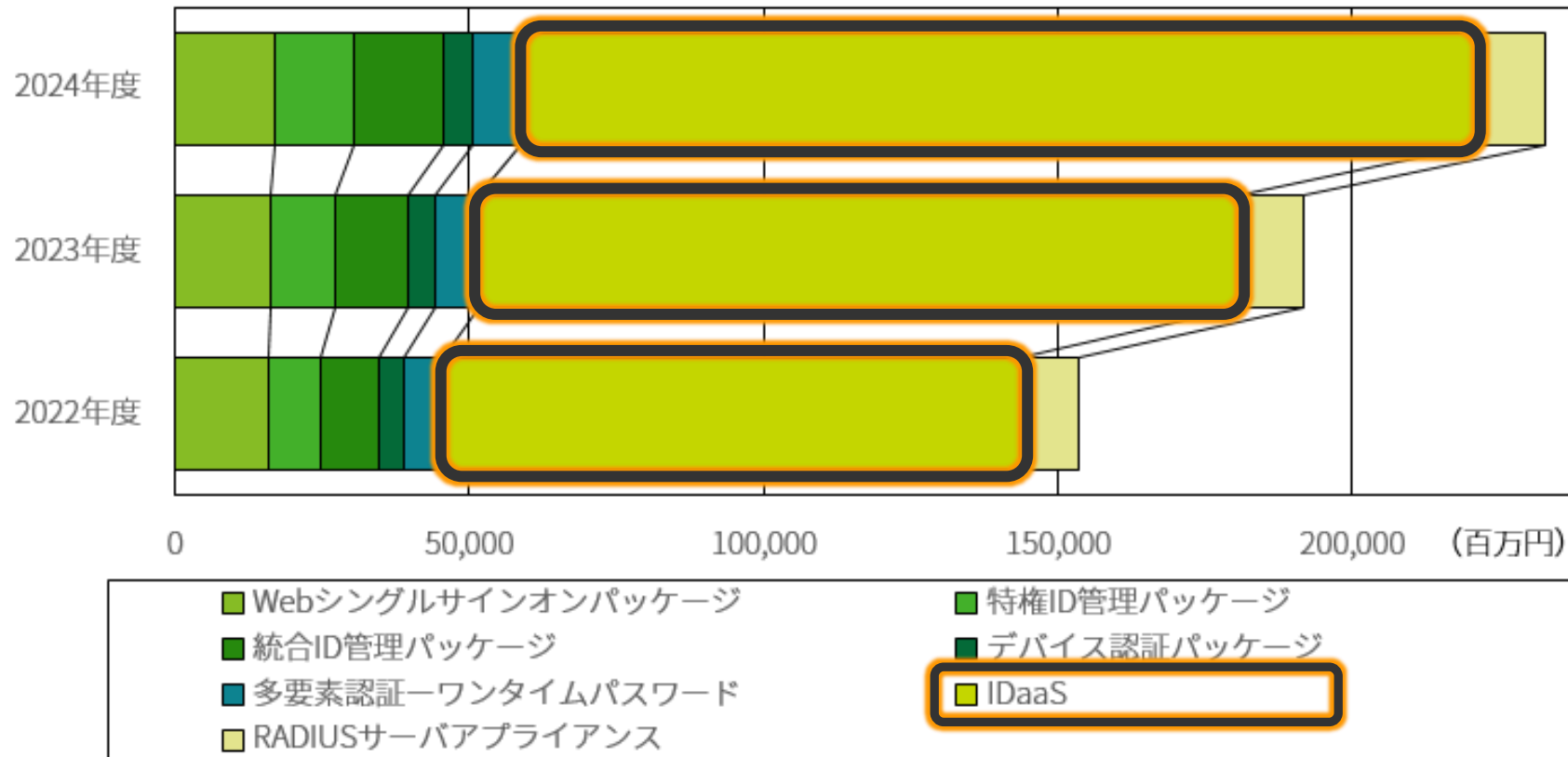
クラウドの普及と共に伸びるIDaaS

デロイト トーマツ ミック経済研究所

『個人認証・アクセス管理型セキュリティソリューション市場の現状と将来展望 2024年版』 2024年3月15日発刊 より

出典 … <https://mic-r.co.jp/mr/03050/>

■ 個人認証・アクセス管理型セキュリティソリューション市場の分野別規模推移



CIAM と EIAM の違い

	CIAM <u>Consumer</u> Identity and Access Management	EIAM <u>Enterprise</u> Identity and Access Management
利用者	会員、顧客	自社／グループ内従業員、取引先 など
一般的な規模	数千 ～ 数百万ユーザー	数百 ～ 数千ユーザー
主な対象システム	Web上で提供されるサービス	業務システム (SaaS等を含む)
ID登録	利用者自身による (ソーシャルログイン利用を含む)	人事DBなどから
目的	- 利便性向上、1to1マーケティング - 不正アクセス防止	- 不正アクセス防止 - 生産性向上
その他	MA／CRM 等との連携も重視される	ActiveDirectory、LDAP 等と 連携するケースも多い

CIAMの中核は、ユーザー認証機能

■ シームレスなログイン環境を提供するSSO

- 複数サービスのユーザー認証を統合することで、顧客のスムーズな体験を実現

■ 多様な認証方式・手段への対応

- SAML、OpenID Connect 等のモダンな認証方式によるセキュリティ強化
- ワンタイムパスワード、生体認証、ソーシャルログイン 等を利用したセキュリティ強化

■ アクセスの記録

- 一元化された認証ログをもとに顧客行動を把握し、MAやCRMによるマーケティング施策に活用

■ 拡張性

- ユーザー数、対象サービス数、データ量 等の増加への柔軟な対応

CIAM選定のポイントは、ユーザー認証機能

特にCIAM選定の際に重視されるポイントは…

大規模ユーザに対して認証機能が提供できること

既存のサービスシステムと連携できること

「そのCIAMは、我が社に適しているだろうか」



対象サービスは
今後増やしていく予定

セキュリティ強化は
もちろん必須

コストを
どう弾き出せばいいのか

会員数の増加も
見込んでおく必要がある

社内システムの認証とは
規模が違いすぎる

大規模サービスの規模での利用には課題も

課題 ①

独自の付加機能・運用形態
MA等との連携…

「個別カスタマイズ」

課題 ②

会員や対象サービスの拡大に
比例して上昇する

「コスト」

独自の付加機能・運用形態、MA等との連携…

そのままでは接続できないサービスもある

運用中システムとの組み合わせや機能改修・付加など
こちらの要望には合わせてもらえない



会員や対象サービスの拡大に比例して上昇

初期コストは抑えられるし、
利用者が少ないうちは良かったのだが…

サービスは増やしていく上に、
MFA連携などのオプション積み上げもインパクト大

従量課金制のプランも検討してみたが、
予算化しづらくなるのがネック

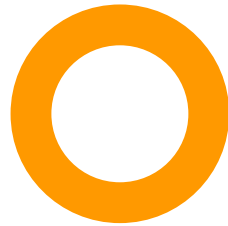


※ 講演中でも、思いついたご質問は随時「Q&A」へご入力ください。
(お答えは原則として最後にまとめさせていただきます)

オンプレミスで
自社導入するとしたら…？

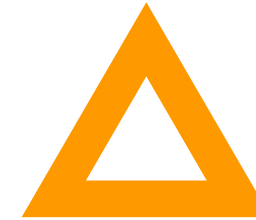
商用SSO製品（大規模向け）導入を検討

個別カスタマイズ



既存システムとの連携、機能付加など
自社に合わせた柔軟な構築が可能

コスト



長期ランニングコストは軽減できるが、
初期費用が非常に高額になる

構築費用 + ライセンス費用 合算で
数千万円後半～数億円台のプロダクトも…

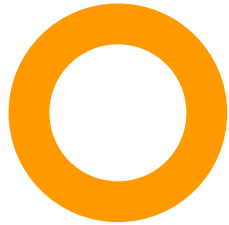
その他の課題



- 導入期間がやや長め … 運用開始まで、6ヵ月～12ヵ月程度？
- 自社内での運用が困難 … サポート費用に加え、継続的に運用要員の提供を受けるケースが多い
- 導入済み・運用中の場合、販売・サポートの終了が迫っているケースもある

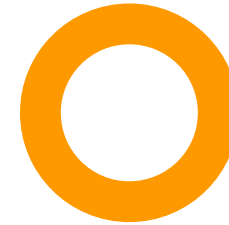
オープンソースによる構築を検討

個別カスタマイズ



既存システムとの連携、機能付加など
自社に合わせた柔軟な構築が可能

コスト



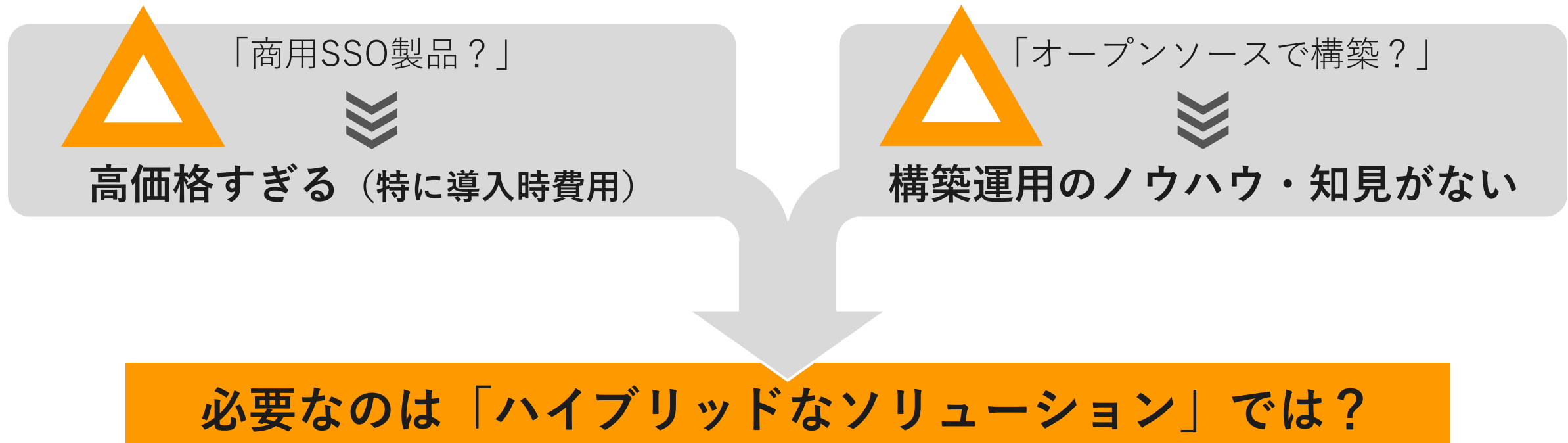
初期費用・ランニングコストともに大幅軽減
が可能

しかし！



構築・運用や脆弱性対応の「ノウハウ」や「知見」が必要

導入の検討

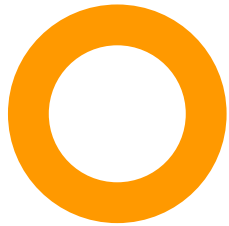


- 自社に必要な機能がある
- コストパフォーマンスが良い（導入時、運用時どちらも）
- 国内から専門家によるサポートが受けられる
- 導入期間は短めがいい



商用製品やオープンソースの課題を解決します

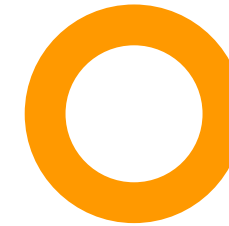
個別カスタマイズ



既存システムとの連携、機能付加など
自社に合わせた柔軟な構築が可能

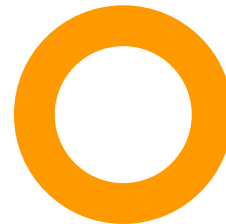
※ フェデレーション非対応システムとの連携を可能にする
「Keygateway」についても後述します

コスト



初期導入費用 + サブスクリプションライセンス費用
初期費用・ランニングコストの大幅軽減を実現

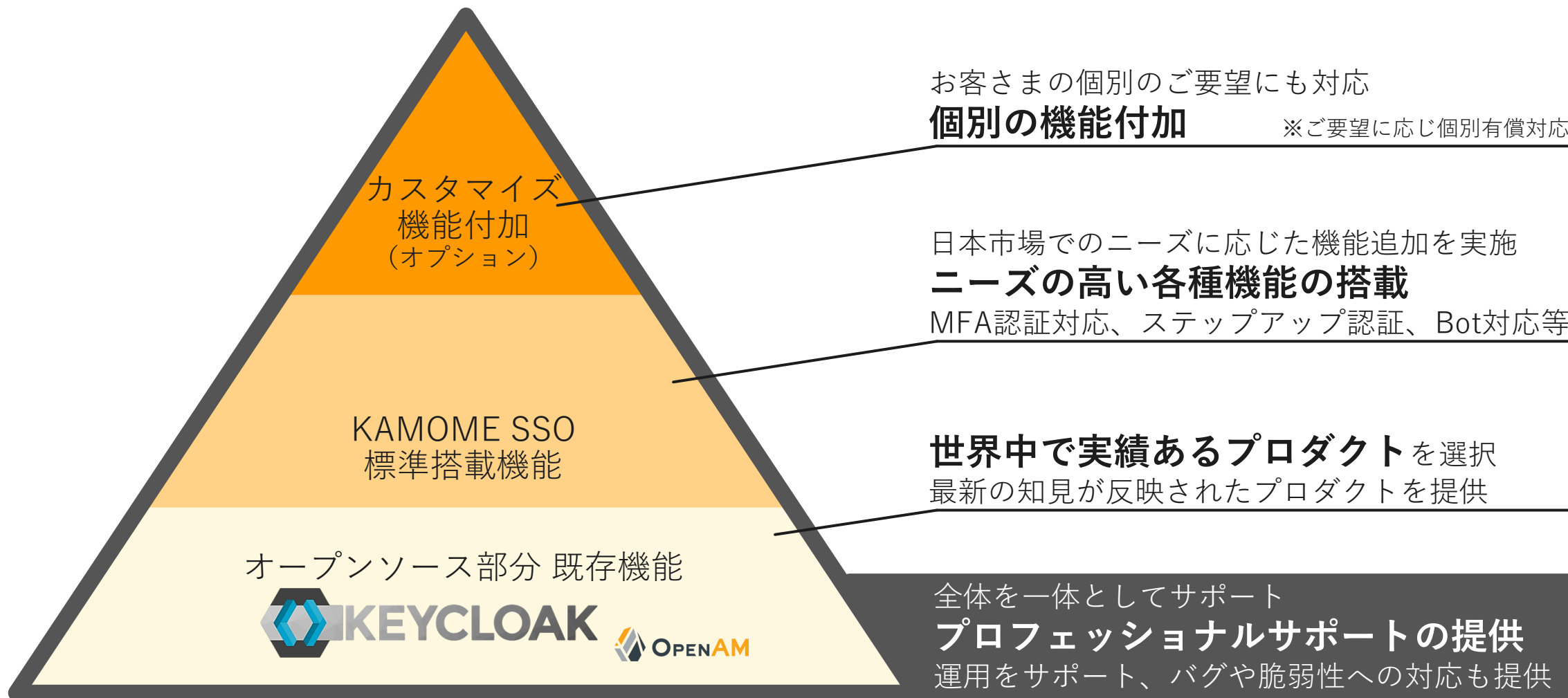
導入や運用の技術的サポート



実績豊富な「認証システムのエキスパート」による、
国内からのサポート提供

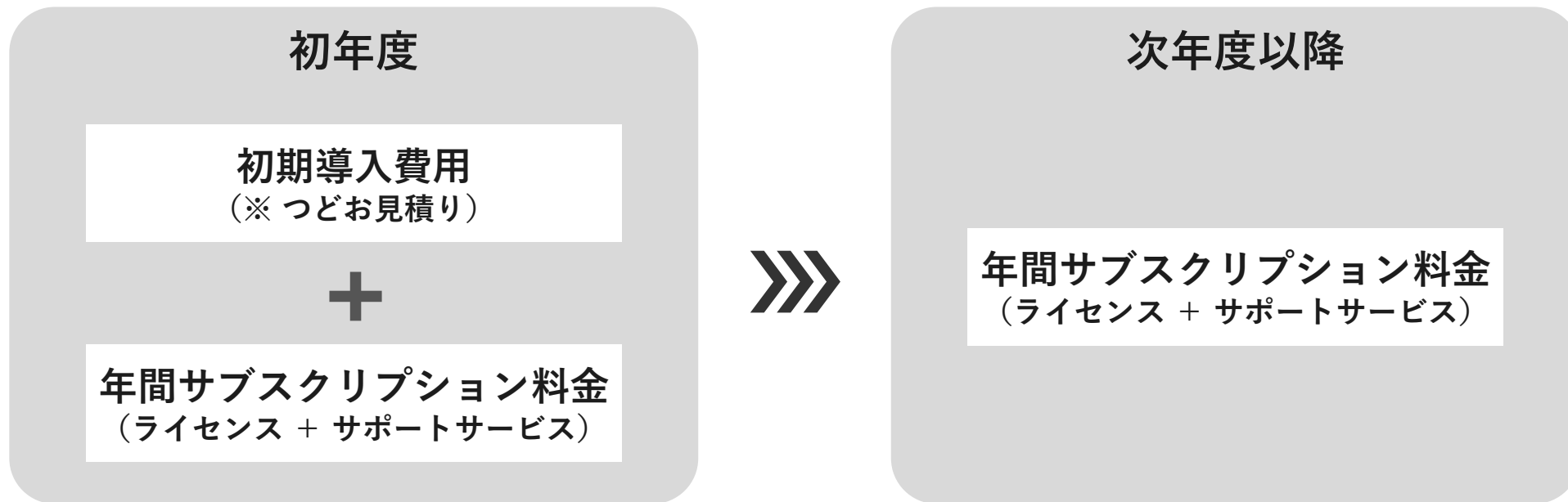


概要





料金体系

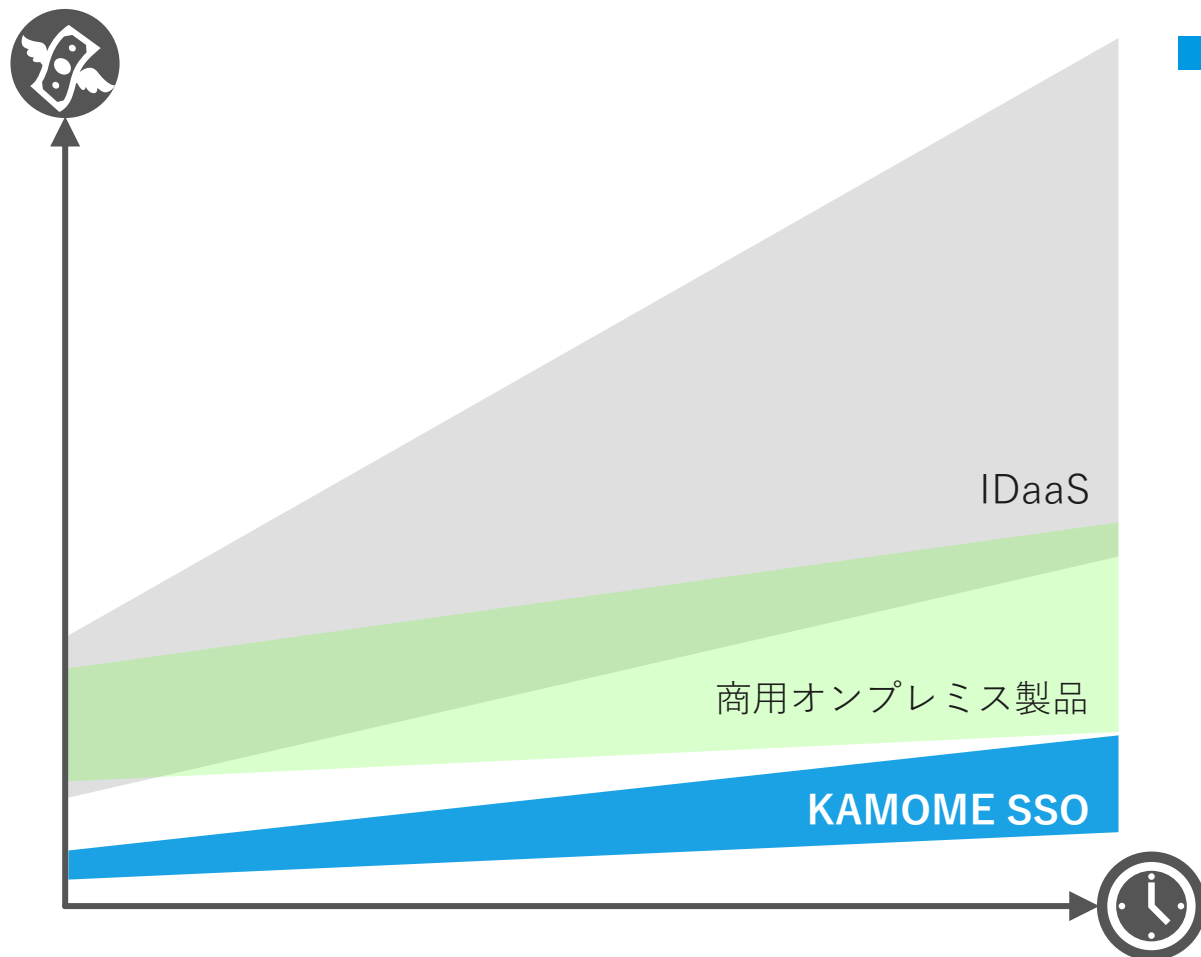


- 利用者ID数単位ではない → **利用者が増加しても金額へ直接影響なし**
- 認証要求数などによる従量課金ではない → **必要な年間費用が明確で予算化しやすい**



圧倒的なコストパフォーマンス

5年間利用した場合の累計コストイメージ（当社調査による）



■ 累計コストイメージ

「10万ユーザー」「5年間利用」のケース（当社調査による）

- IDaaS … 4.5億 ～ 42.7億円 程度
- 商用オンプレミス製品 … 1.5億 ～ 5.7億円 程度
- KAMOME SSO … 0.7億 ～ 1.5億円 程度

KAMOME SSOは、100万ユーザー規模でも他製品ほどの費用上昇はありません。

利用者が多いほど、利用期間が長いほど、コストメリットは高くなります。

※ 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)

SAML/OpenID Connect 非対応の システムとの連携

サービス事業者さまから寄せられる、もうひとつの課題

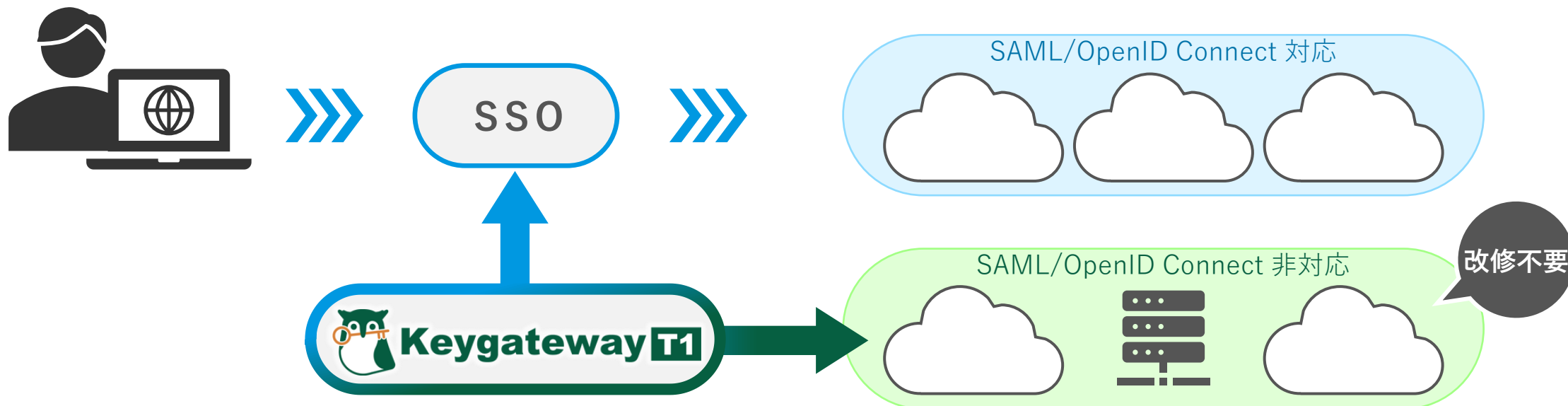


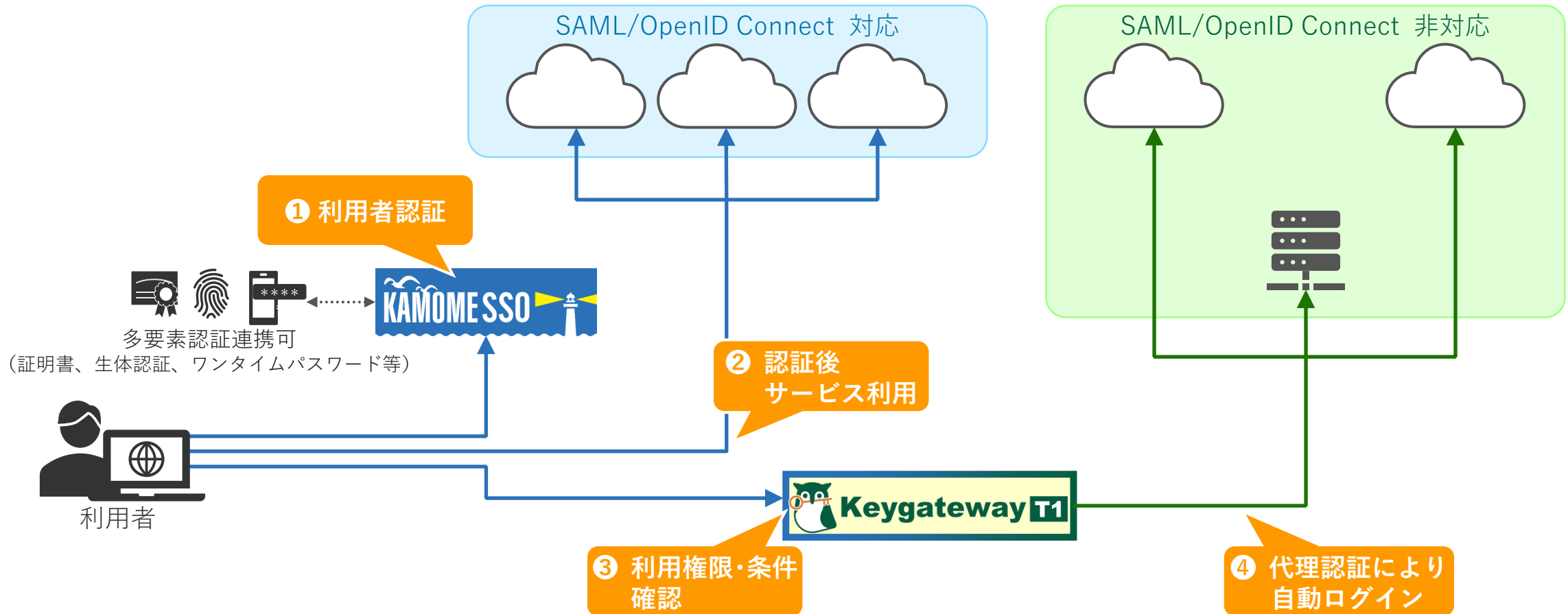
レガシーな
サービスシステムも運用中…



■ SSOシステムとサービスシステムを“橋渡し”

- 組み合わせにより、さらに一体化したSSOを実現





「ユーザー認証の一元化」が実現します。

※ 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)

導入事例の一部をご紹介します

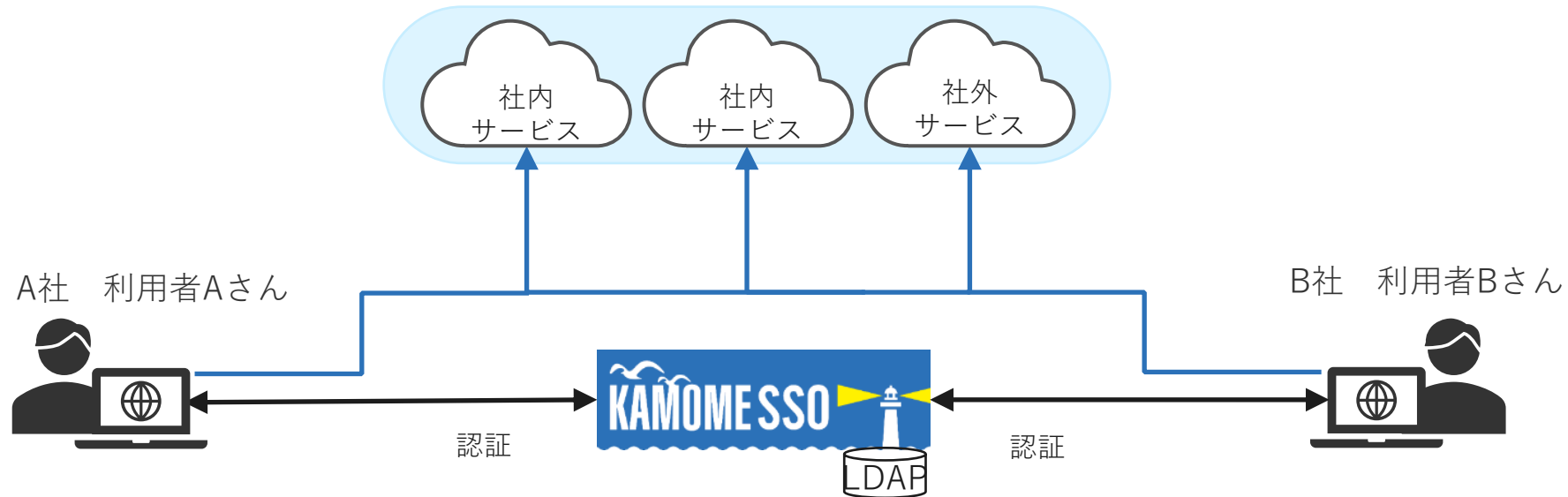


社内・社外サービスを連携させてプラットフォームを構築中だが、OpenID Connectによる認証方式が必要。
また、ログイン画面はサービスに合わせてカスタマイズしたい。

- 利用者数 10万アカウント ～ (最大100万)
- 対象サービス数 3
- 工期 3ヵ月



今後見込まれる利用者拡大や
提携サービスの増加に対応するため
必要機能のカスタマイズを実施



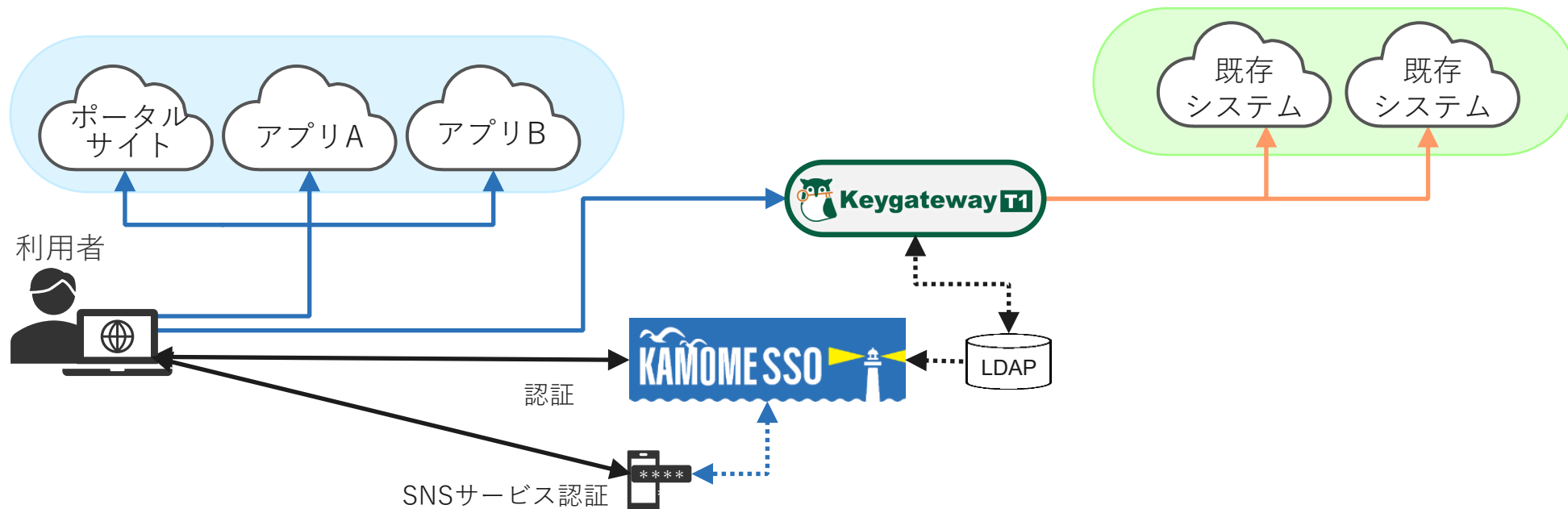


提供中のサービスの認証がバラバラ。
利用者の利便性を上げるとともに、今後のサービス拡充に向けて
利用率を向上させたい。
ただし運用コストはできる限り抑えたい。

- 利用者数 100万アカウント ~
- 対象サービス数 12
- 工期 3ヵ月



既存システムを巻き取り
運用コスト95%削減して実現
多要素認証やリスクベース認証も導入し、
不正アクセスを防止



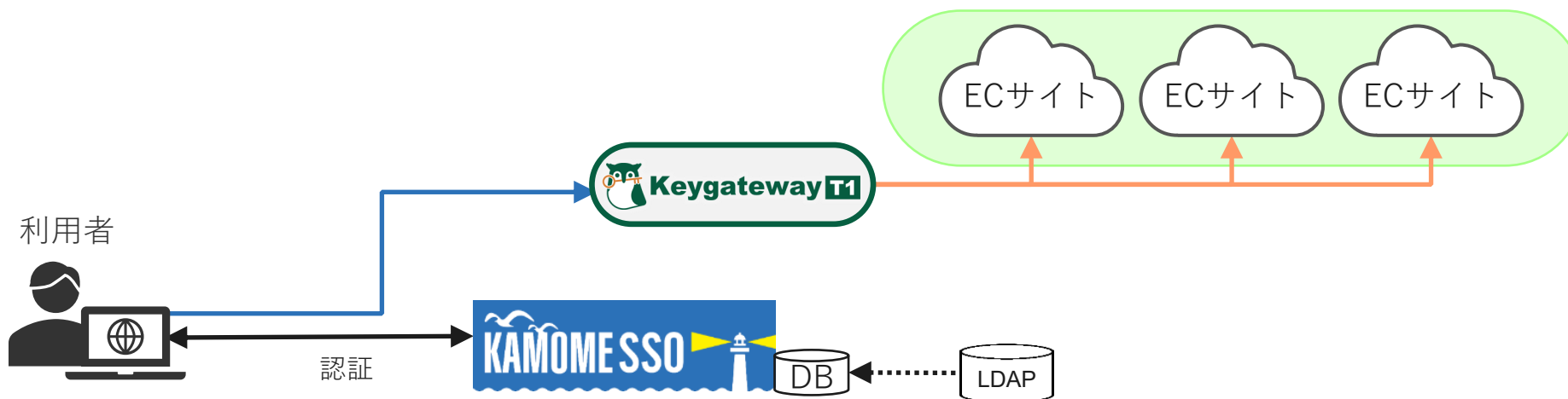


利用者の利便性向上と併せ、
複数サイト内での利用者動向を把握し、デジタルマーケティングの
強化を図りたい。

- 利用者数 100万アカウント～
- 対象サービス数 4
- 工期 5ヵ月



ログイン状態を
購入ページ前後で2段階に分ける機能を付加し
利用者のロイヤルティ向上を実現





新オプション「マネージドサービスプラン」

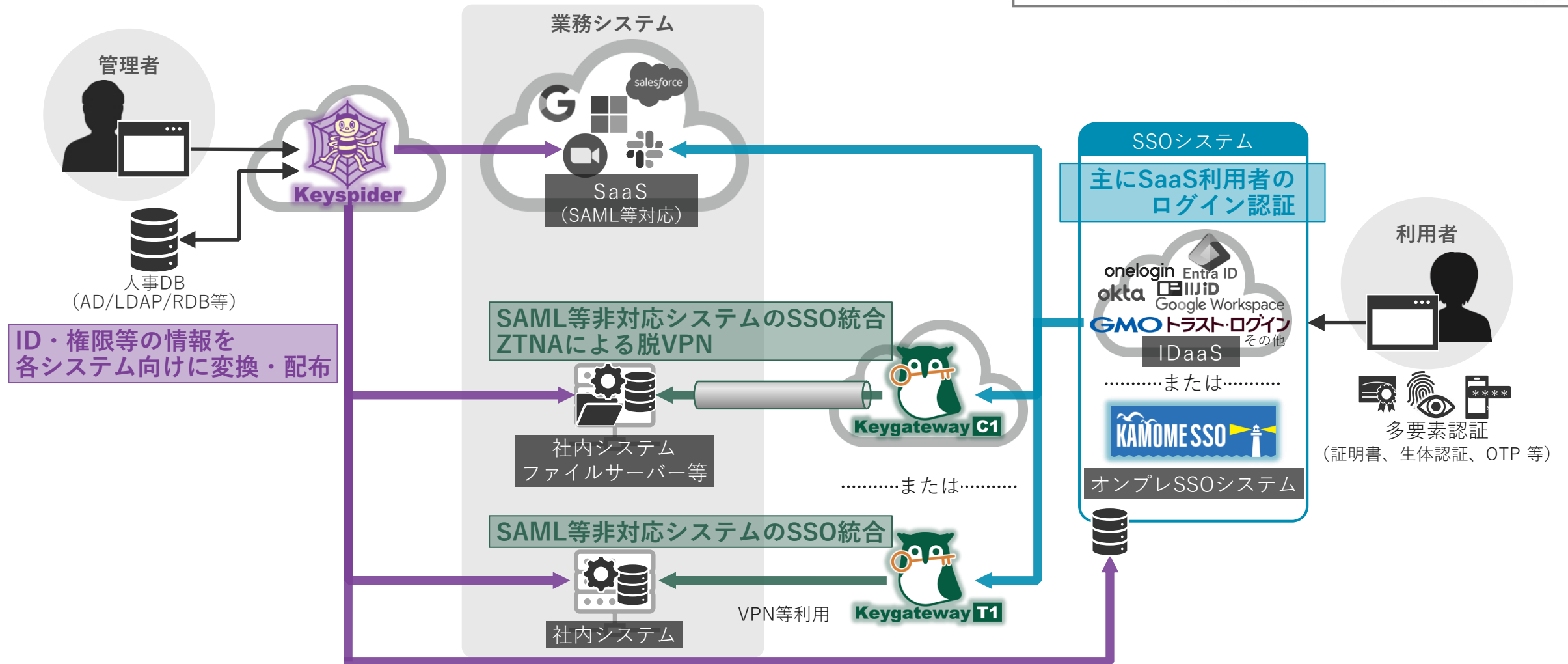
オンプレミスと同様の
柔軟性・使い勝手を
クラウドで

サーバーやOSなどの
管理は不要

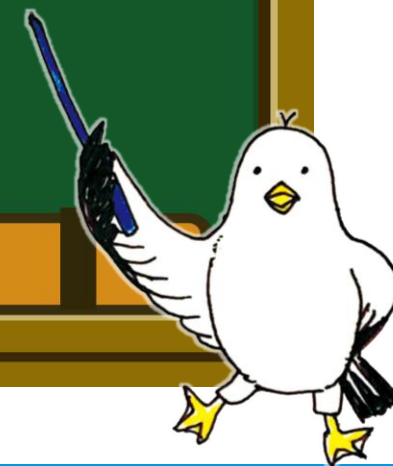
「KAMOME SSOの運用負荷を軽減させてIDaaSのように使いたい」
そんなお声にお応えして、「マネージドサービスプラン」を
販売開始しました。

お問い合わせも多くいただいております。
ご要望いただきましたら、個別ミーティングにて詳しくご案内差し上げます。

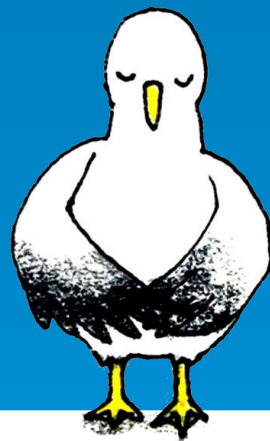
トータルな課題解決を提供しています



- 大規模向けのユーザー認証基盤の最も重要なポイントは、「大規模ユーザに対して認証機能が提供できる」「既存のサービスシステムと連携できる」の二点です。
- IDaaSはすぐれたサービスですが、大規模向けに利用するには「個別カスタマイズ」「コスト」という課題があります。
- 「KAMOME SSO」は、利用者数による料金体系ではなく、自社都合に合わせたカスタマイズ、専門家によるサポート提供、トータルコストの抑制を実現します。
- SAML/OpenID Connect に非対応のシステムとも連携させたい場合には、「KAMOME SSO」と「KeygatewayT1」のセットが有効です。
- 「KAMOME SSO」には、クラウド環境への導入・設置～管理運用までを提供するマネージドサービスオプションが近日付加されます。
- 「KAMOME SSO」「KeygatewayT1」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から提供されます。



ありがとうございました



■ 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大好きなチームです！

