

中・大規模企業のSSO基盤

～相次ぐオンプレ版SSOツールのサポート終了にどう対応すべきか～



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、日本企業のID管理の課題を解決するため、Keyspider社を設立。

「クラウドID管理サービス Keyspider」の提供開始。

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。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が好き。

最近のヒットは、宮城谷昌光『公孫龍』 林譲治『知能侵蝕』



ID管理・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

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）
- 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

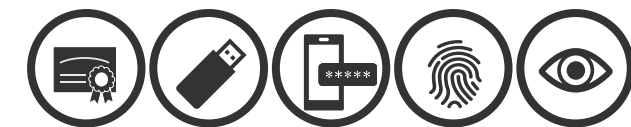
- IDaaSサービス 認証基盤
 - ・ 通信事業者 2,000社
- 社内業務アプリ SSOシステム
 - ・ 家電メーカー 7,000ユーザ
- 学内システム SSOシステム
 - ・ 大学 15,000ユーザ
- OEM提供先



※ 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)

認証基盤といえば IDaaS ?

MFA対応「必須化」「義務化」の流れが加速



<https://www.itmedia.co.jp/enterprise/articles/2401/05/news032.html>

<https://help.salesforce.com/s/articleView?id=000392813&type=1>

Help

製品 業種別ソリューション 事例 学習コンテンツ サポート 企業情報

ヘルプを検索

多要素認証 (MFA) への対応のお願い

公開日: 2023年7月31日

説明

お客様のデータの機密性、完全性、可用性は、お客様のビジネスにとって不可欠であり、Salesforce はお客様のデータの保護に真摯に取り組んでいます。4月に、多要素認証 (MFA) のような技術を駆使して最高水準のセキュリティを提供していく、という Salesforce のコミットメントについて再度お知らせしました。顧客データを守るパートナーとして、Salesforce は 2022 年 2 月 1 日より、Salesforce 製品クラスには MFA の使用を必須条件とすることを決定しました。MFA を使用するために追加の費用は不要です。

ITmedia エンタープライズ

記事一覧 | オルタナティブ・ブログ | 用語辞典

CIO・クラウド戦略 データドリブン経営 業務の自動化 **セキュリティ** DX×組織 中小企業IT

注目ワード エンタープライズAI サプライチェーン&ロジスティクス Web3

ITmedia エンタープライズ > セキュリティ > GitHubがまだ2FAを設定していないユーザーに通知メ...

セキュリティニュースアラート

GitHubがまだ2FAを設定していないユーザーに通知メール 期限迫るため急ぎ対処を

GitHubはサイバー攻撃対策としてユーザー設定しなければアカウントが制限される

2024年01月05日 07時00分 公開

TECH+ Powered by マイナビニュース

会員10万人突破 特別企画

検索する

企業IT テクノロジー 導入事例

ドコモビジネス PR Sky PR

Amazon Web Services(AWS)、2024年半ばから多要素認証 (MFA)が必須に

掲載日 2023/10/09 12:07

著者: 後藤大地

<https://news.mynavi.jp/techplus/article/20231009-2786679/>

Tableau Online

多要素認証必須化のご案内

ビデオを見る

日本経済新聞

朝刊・夕刊 LIVE Myニュース 日経会社情報

トップ 速報 オピニオン 経済 政治 ビジネス 金融 マーケット マネーのまなび テック 国際 スポーツ 社会・調査

クレカ決済、本人認証機能の導入義務化 24年度末までに

+フォローする

2023年1月20日 19:47

保存

経済産業省は20日、クレジットカードの不正利用防止に向けた対策をまとめた。カード発行会社や電子商取引 (EC) サイト事業者、カード利用者の本人確認のため「ワンタイムパスワード」や生体認証などの導入を義務づける。2024年度末を期

<https://www.nikkei.com/article/DGXZQOUA205F00Q3A120C2000000/>

MFA対応にも後押しされ、SSOは広く普及

※ Salesforceの場合

①

Salesforce MFA

Salesforce
のみ
MFA対応

Salesforceより無料で提供されるが…



引用 … <https://customersuccessjp.salesforce.com/l/220122/2021-09-02/26rt47>



②

MFA対応機能付きの シングルサインオン (SSO)

※ IDaaSの例

複数
システムの
認証一元化



※ SSOシステムには、オンプレミス製品（国内／海外）も多くあります

「オンプレミスのSSO製品がサポート終了してしまう」

急いで乗換え先を探さなくては…
やはり今ならIDaaSになるのかな？



「IDaaSは、自社の都合に合致しているだろうか」



利用者はかなり
多くなる見込み

使いたいMFA
あるだろうか？

クラウドサービスも
社内システムも

対象システムも
それなりに多い...

コスト、5年間の
総額はどの位？

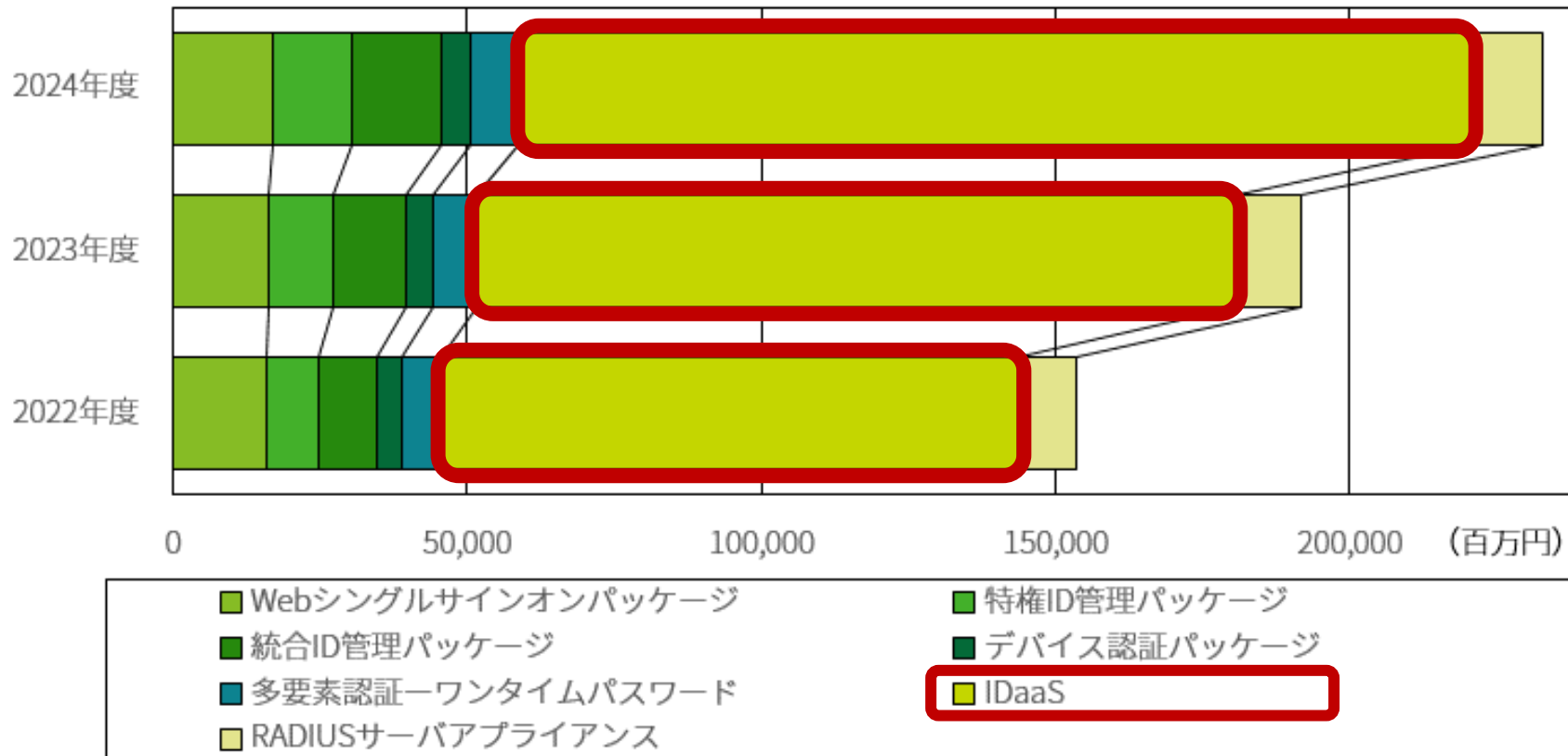
クラウドの普及と共に伸びるIDaaS

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



しかし、一定以上の規模で使い続けるには課題も

課題 ①

対象者やプランの拡大で
上昇してゆく

「コスト」

課題 ②

ハイブリッド環境での
運用で対応必須となる

「既存システム」

利用対象拡大に伴うトータルコスト

■ 「同一プラン加入」や「比較的少人数」ではメリット大

- オフィススイートプラン内包のIdP機能を活用、追加コスト不要でメリット大
- 比較的少人数の場合、IDaaSサービスは5年間総コスト面でもメリット大
- 低コストの機能限定プランや、認証数での従量課金制のIDaaSサービスも
- 初期導入費用が抑制可能なケースも



「対象者の範囲を拡大」「MFA等のオプション機能の追加」...

トータルコストの確認が必要



Microsoft365サービスでの価格例 (2024.03現在)

1,000ユーザーの場合…

- 月額 100万円 ~ 713万円
- 年額 1,200万円 ~ 8,556万円

▼ ID およびアクセス管理

1つのIDプラットフォームでセキュリティを強化し、アクセスをシンプルにし、スマートなポリシーを設定することができます。

資格情報の紛失や盗難が原因の侵害から組織を守ることができます

Microsoft Advanced Threat Analytics で攻撃タイムラインを簡潔にリアルタイムで把握できます¹⁶

Windows Hello for Business を使用してノート PC、タブレット、デバイス、アプリにすばやくサインインできます

Microsoft 365 E3

¥4,500 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。

Microsoft 365 E5

¥7,130 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。

Microsoft 365 F3

¥1,000 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。

プラン 1

プラン 2

プラン 1

✓

✓

✓

✓

✓

✓

✓

✓

引用 … <https://www.microsoft.com/ja-jp/microsoft-365/enterprise/microsoft365-plans-and-pricing> (一部画像加工)

クラウドサービス以外の業務システムへの対応

■ 認証方式への対応が難しい業務システムも

- IDaaSは「SAML」「OpenID Connect」等のフェデレーション方式が基本
- フェデレーション方式に対応できないシステムとの連携は困難な場合も多い（Webシステム以外やファイルサーバなどはさらに対応が難しい）



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



※ 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)

自社専用システムを検討するとしたら…？

メリット

■ 自社の都合に合わせた機能や運用が可能

- 既存業務システムの巻き取りで、セキュリティと利便性を大幅に向上
- 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

- 運用中のインフラを活用した導入、統合した運用も可能
- 既存業務システム含めた全体の運用負荷を削減

■ 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



課題 【商用製品の場合】

■ 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～数億円台のプロダクトも…

■ 導入期間がやや長め

- 運用開始まで、4ヵ月～6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



課題【オープンソースの場合】

■ 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

■ 導入期間が少し長め

- 運用開始まで、2ヵ月～4ヵ月程度？

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

※ 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)

自社専用のSSOシステムの導入



+



世界中で実績のあるOSSを選択 + 日本でニーズの高い機能を追加

全体を一体としてサポート

プロフェッショナルサポートの提供

お客さまの個別のご要望にも対応

個別の機能付加

※ご要望に応じ個別有償対応

カスタマイズ
機能付加
(オプション)

日本市場でのニーズに応じた機能追加を実施

ニーズの高い各種機能の搭載

MFA認証対応、ステップアップ認証、Bot対応等

KAMOME SSO
標準搭載機能

オープンソース部分 既存機能



KEYCLOAK



OPENAM

世界中で実績あるプロダクトを選択

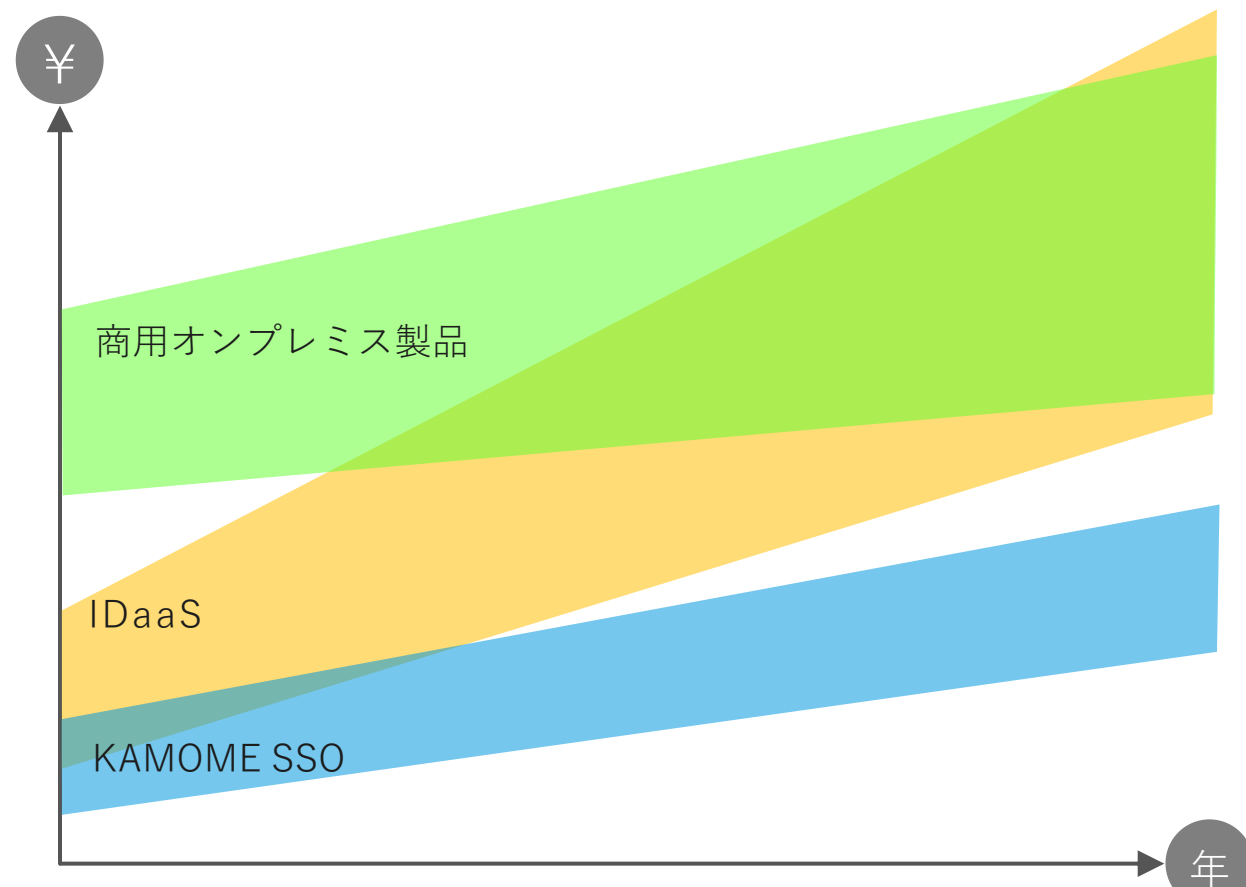
バグ修正や機能改修、脆弱性対応等も付加

自社専用システムのメリットに加え・・・

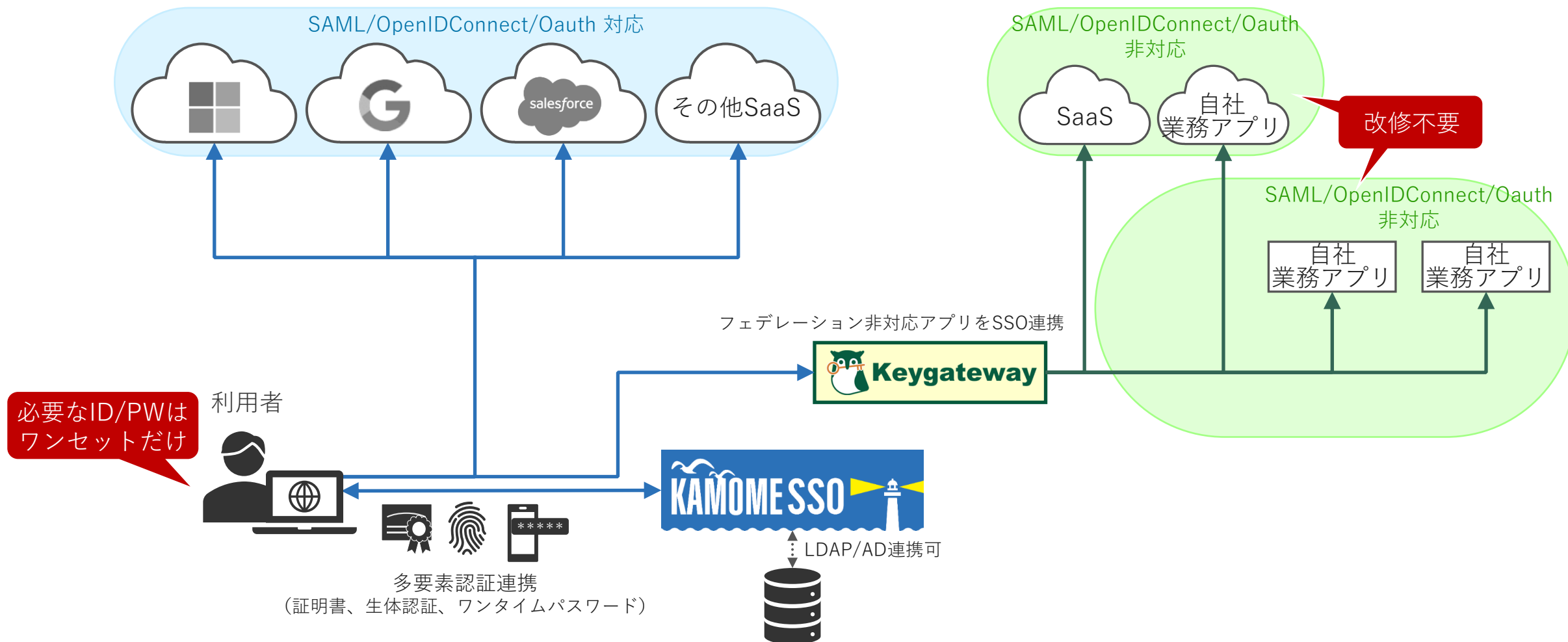
■ 初期&運用コストを大幅に軽減

- 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

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）



フェデレーション非対応のシステムも統合したSSOを実現



① 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



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、「Keygateway T1」を付加して採用



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、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



コスト抑制しつつ、さまざまなご要望に柔軟対応



業種・用途・システムの状況等により多様な事例

	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 [※ Keygateway併用]	SAML (フェデレーション) リバースプロキシ [※ Keygateway併用]	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

- その他…
- 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…

認証機能	SAML対応	○	
	OpenID Connect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
	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)
	ワンタイムパスワード認証 (メールベース)	○	KAMOME SSO独自機能
	FIDO2対応	○	
	LDAP連携	○	
	Active Directory連携	○	
認可機能	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
管理機能	その他の認証モジュール対応	外部RDB対応 (予定)	
	サイトごとのアクセス制限	○ (予定)	KAMOME SSO独自機能 SAMLベース
	アカウントロック	○	所定回数のログイン失敗でロック
その他	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	

初期導入費用 + サブスクリプションライセンス

■ 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**



用途・導入形態によって
バリエーションがあります。
詳細はぜひご相談ください。

※ 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)

中～大規模社内利用 / SaaSの運用性を向上させる
関連ソリューションのご案内

「ID情報の管理を自動化したい」

利用者のID管理はセキュリティの基礎。

常に変動するID情報は迅速的確なメンテナンスが必要だが
システムの数も増えてなかなか大変・・・



各システムへID・権限情報を一括反映
国産ID管理クラウドサービス



Keyspider

「業務システムへのリモートアクセス、そろそろ脱VPNしたい」

フェデレーション非対応システムも巻き取ってSSO。

さらに、VPNを廃止してゼロトラストモデルを取り入れたい…



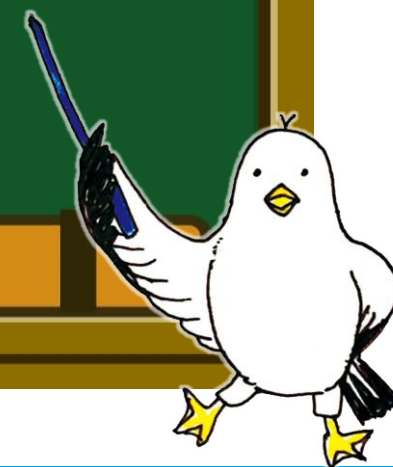
ZTNA (ゼロトラストネットワークアクセス) サービスで
セキュリティ強化 と 脱VPNを可能に



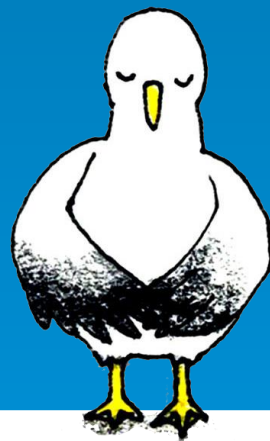
Keygateway C1

ファイルサーバー、クラサバ型アプリへの接続も対応
さらにRDP対応も進行中

- IDaaSは、導入しやすいサービスであり広く普及しつつありますが、利用の規模や形態によっては適さない場合もあります。
- オープンソースベースの「KAMOME SSO」は、自社都合に合わせた運用とトータルコストの抑制に役立ちます。
- フェデレーション非対応のシステムとも連携させたい場合には、「KAMOME SSO」と「Keygateway」の併用が有効です。
- 「KAMOME SSO」「Keygateway」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。
- ID・権限情報の管理には、ID管理クラウドサービス「Keyspider」
ゼロトラストを取り入れた脱VPNには「KeygatewayC1」もご検討ください。



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！

