

# 社内システムを 改修不要でプライベートSaaS化するには

SAML非対応でも、AzureADやIDaaSと連携して  
「認証統合 + AzureAD」の多要素認証対応



## 潮村 剛 (しおむら たけし)

1990年代半ば、食品メーカーからITベンチャーに飛び込む。  
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し鍛えられる。

2008年、かもめエンジニアリング社を設立。  
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、一般企業の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事業者を中心とした19社で「ゼロトラストアライアンス」を設立。

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)

趣味 料理と読書。歴史小説とSFが好き。



画像引用：  
オライリー・ジャパン



## 「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



Marubeni  
Network Solutions



エイチシーネットワークス株式会社



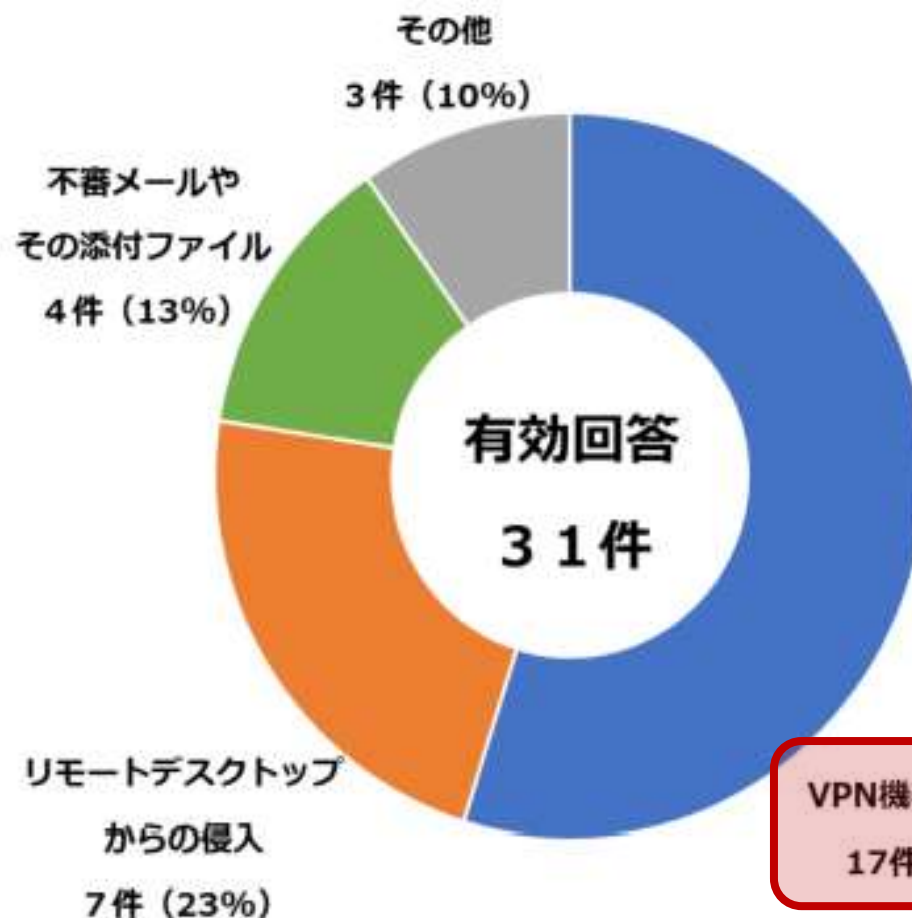
# VPNが抱える課題と、ゼロトラストモデル

## ランサムウェアの感染経路は 半数以上がVPN経由

警視庁 令和3年（2021年）9月発表  
「令和3年上半期におけるサイバー空間をめぐる  
脅威の情勢等について」より

引用：[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03\\_kami\\_cyber\\_jousei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf)

【図表7：感染経路】



VPNにある課題とは？  
どんな対策が？

VPN機器からの侵入  
17件 (55%)

## 被害事例の代表格 (米コロニアル・パイプライン社)



引用：<https://www.nikkei.com/article/DGXZQOGN084D30Y1A500C2000000/>



引用：<https://jp.reuters.com/article/cyber-usa-pipelines-idJPKCN2DK2P3>



## 社内（境界内）ネットワークに一度入ってしまえば、すべてのシステムへアクセス可能

### ■ テレワーク用のPCのリスク

→ 安易なパスワードの流出から、乗っ取り、ウィルス汚染の危険性

### ■ VPNでは「ネットワークの入口」だけ認証

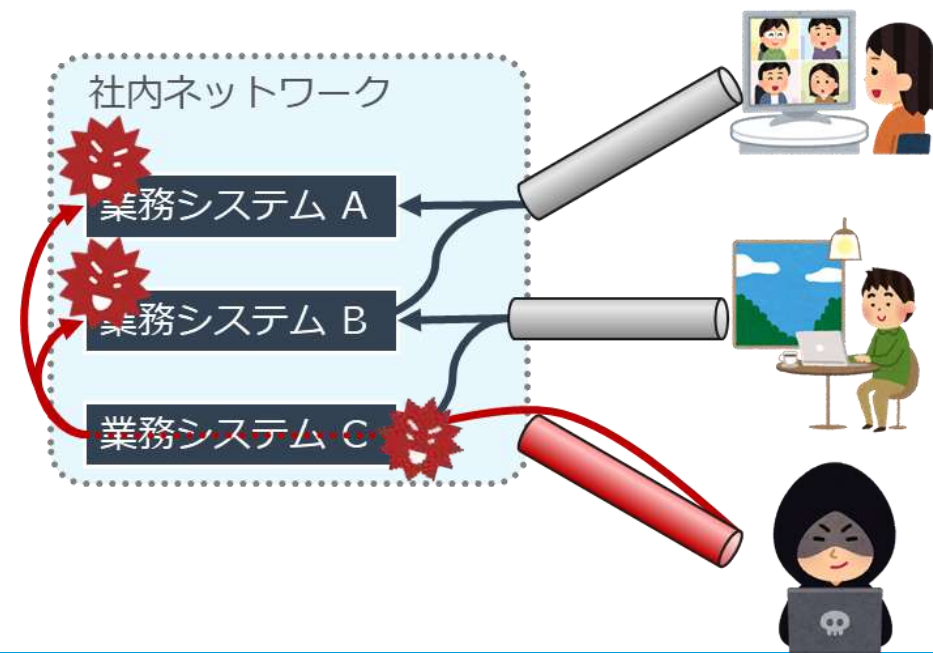
→ 各業務システムは守らない

### ■ 社内LAN内は行き来自由

→ 侵入されれば被害は全体へ

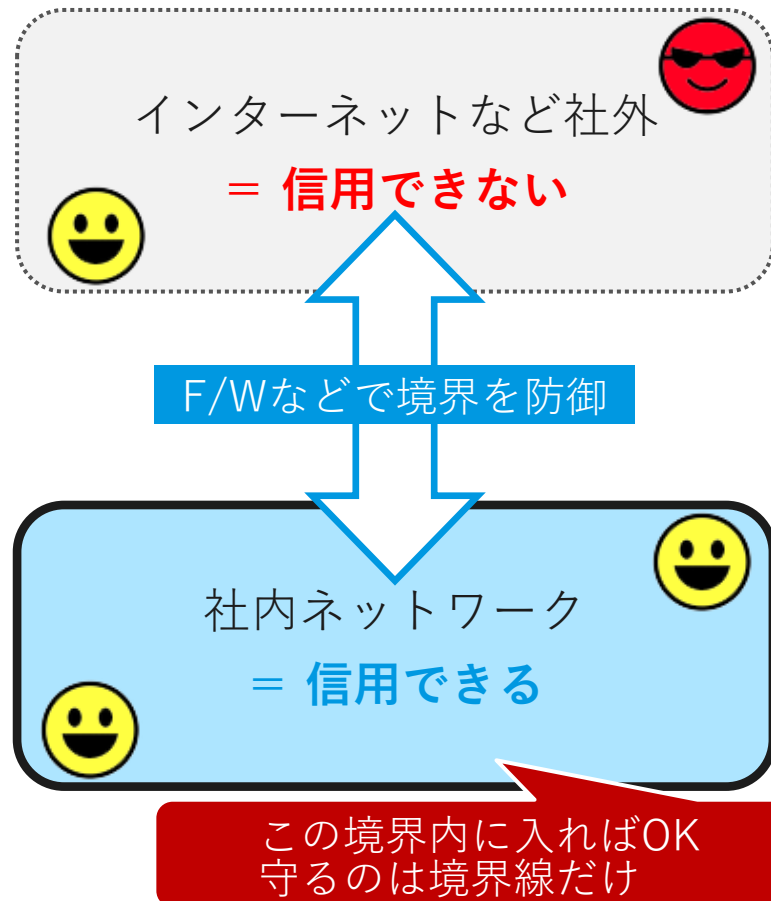
### ■ アクセスログはシステム毎に記録

→ 解析と追跡に時間がかかる



## VPNの課題 = 前提となる考え方「境界防御モデル」の限界

### VPNを利用した境界防御モデル

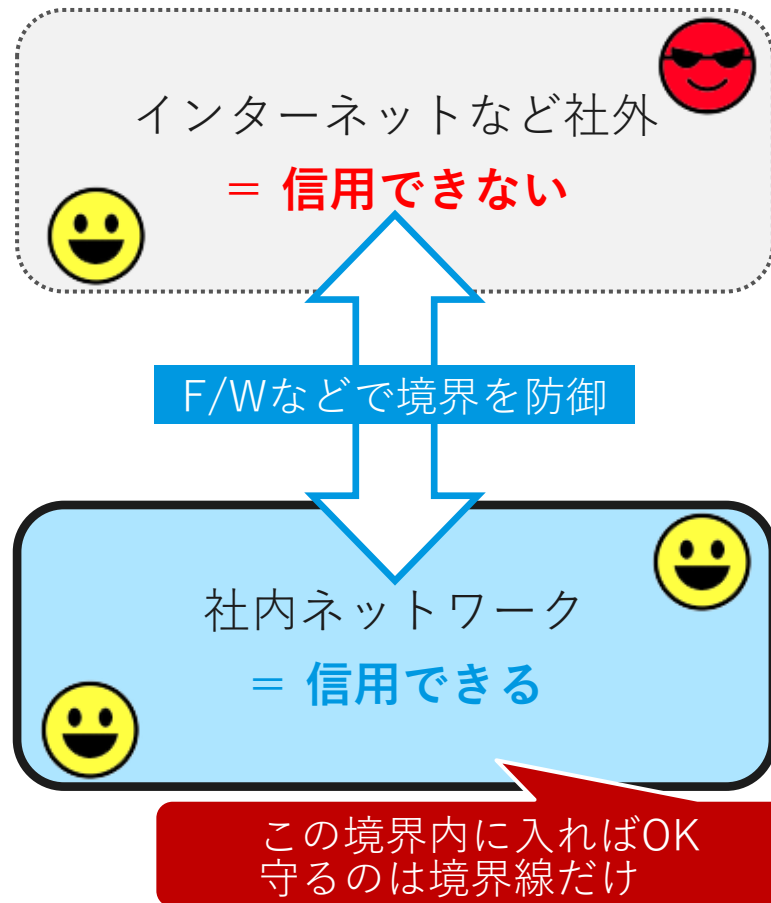


- SaaSの利用によって、情報資産がインターネット上に
- テレワークの普及により、インターネット上の端末から社内ネットワークへのアクセスが急増
- VPN (=社内ネットワークの拡張) が負荷に耐えられない
- VPNは社内ネットワークに一旦入ると、あとはアクセスし放題！ 危険
- 標的型攻撃や社内不正などが多発



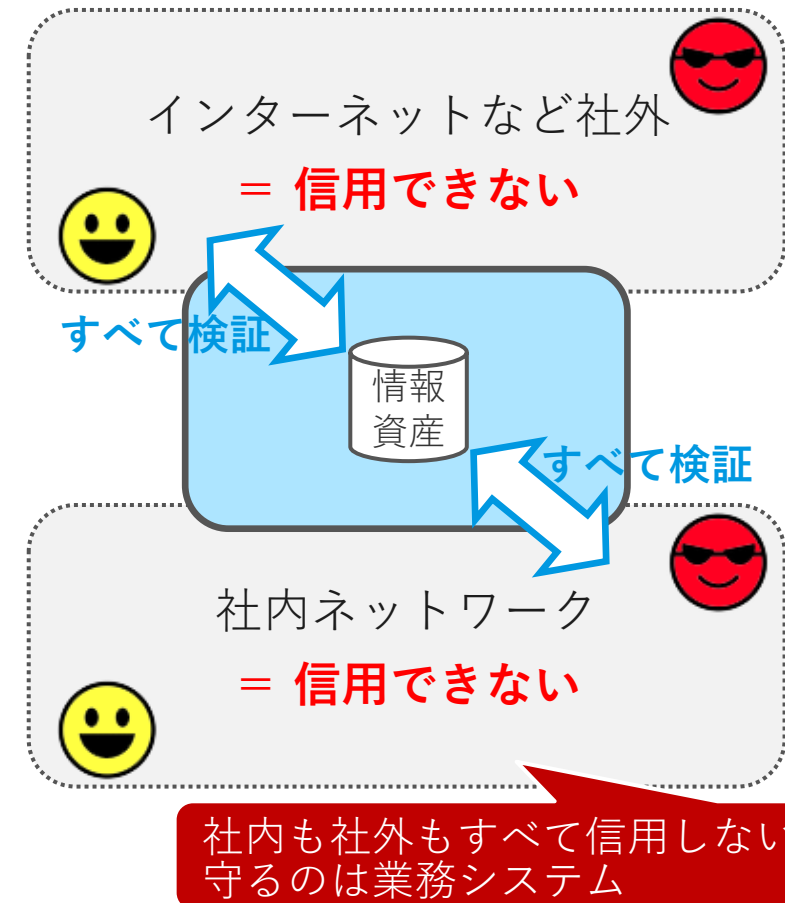
## 「境界防御モデル」の限界 → 新しい考え方へ進化

VPNを利用した境界防御モデル

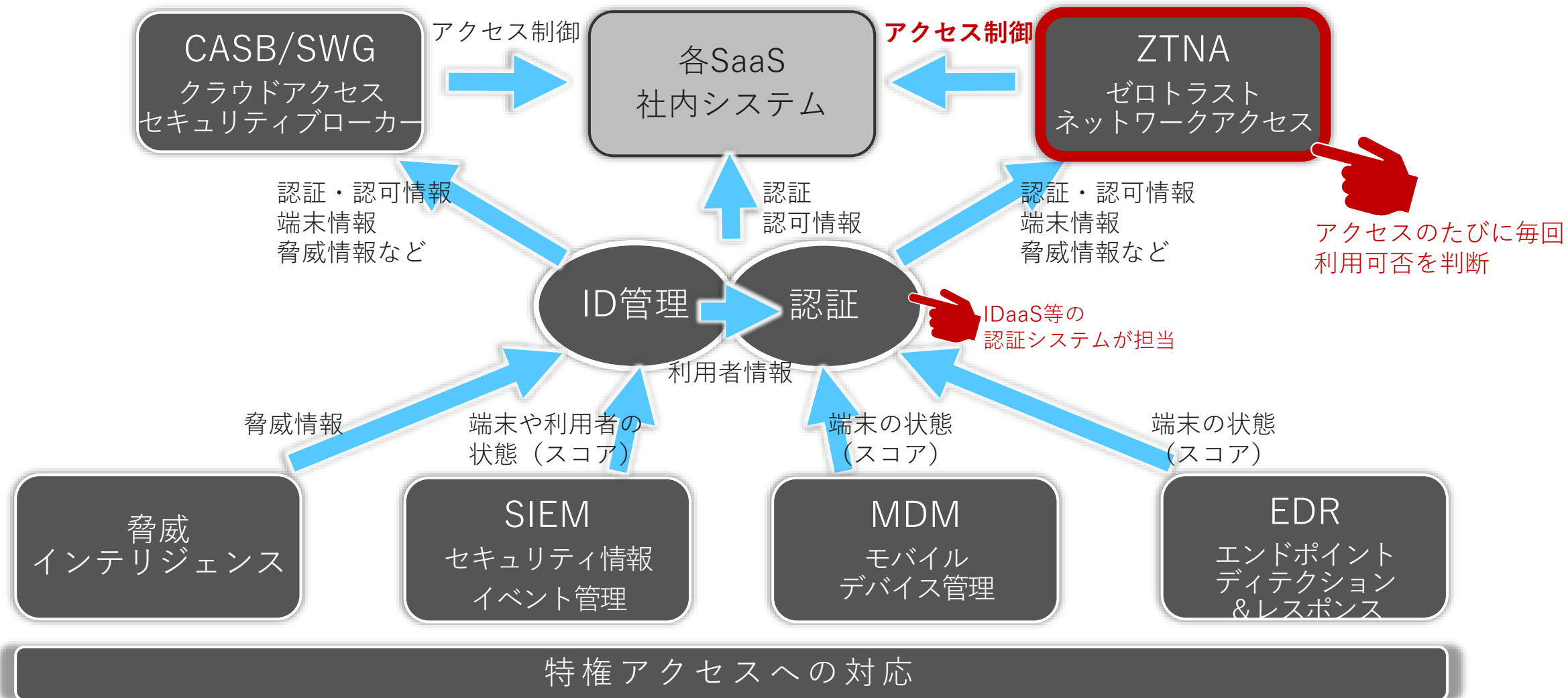


対象と  
考え方が  
進化

ゼロトラストモデル



※ 単一の製品で理想の「ゼロトラスト」が実現できるわけではありませんし、「完璧なゼロトラスト」は現時点では実現が難しいとも言われています。



※ 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)

## VPNに替わるZTNAサービス

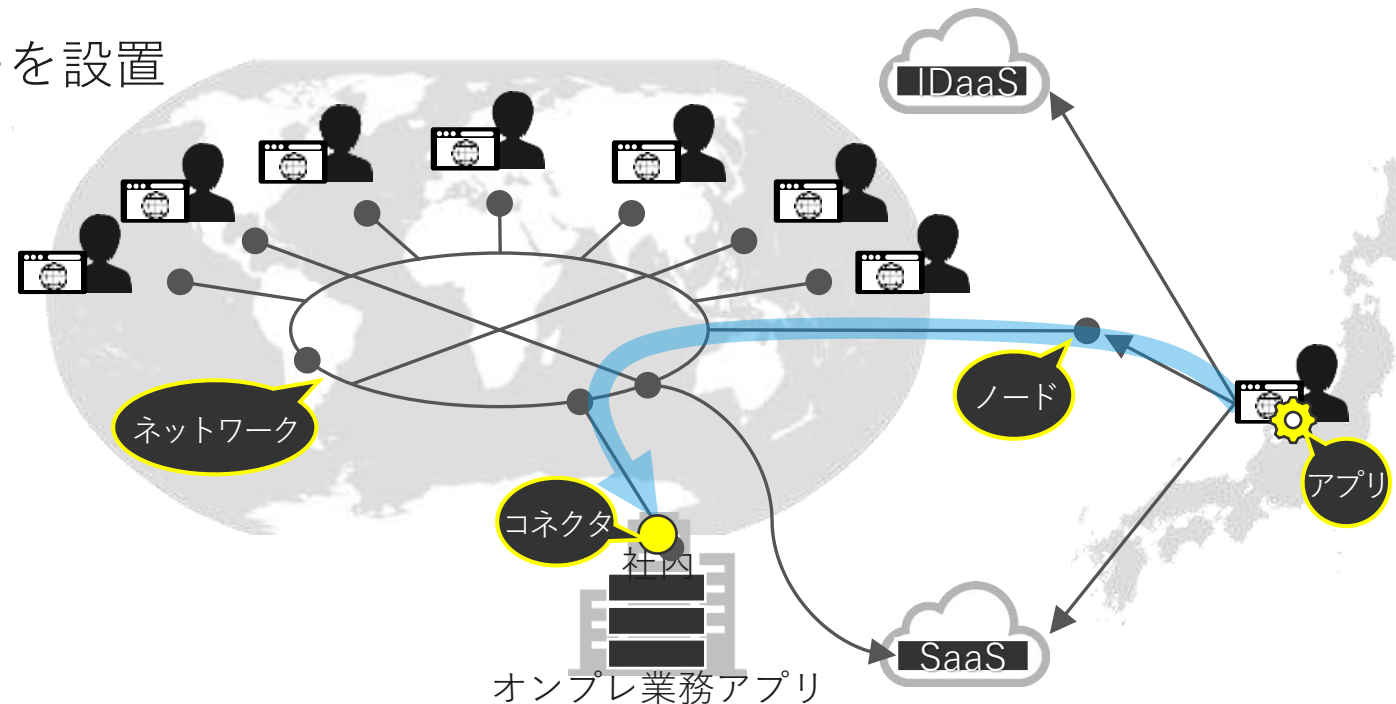
## ZTNAサービスの概要

- ネットワークの内外を問わず、全てのアクセスを毎回チェックし、接続の可否を動的に判断するものです。
- オンプレミスの業務アプリも、SaaSと同様のアクセス制御が可能になります。
- IDaaS等の認証システム（IdP）と連携して動作します。

## 世界中に拠点を持つグローバル企業向き

### ■ 世界中にノード（アクセスポイント）を多数設置

- 最寄りのノードに接続し、独自ネットワークを経由し社内へアクセス
- ユーザー認証は独自基盤かIDaaSを利用
- 端末にアプリ導入、社内にコネクターを設置

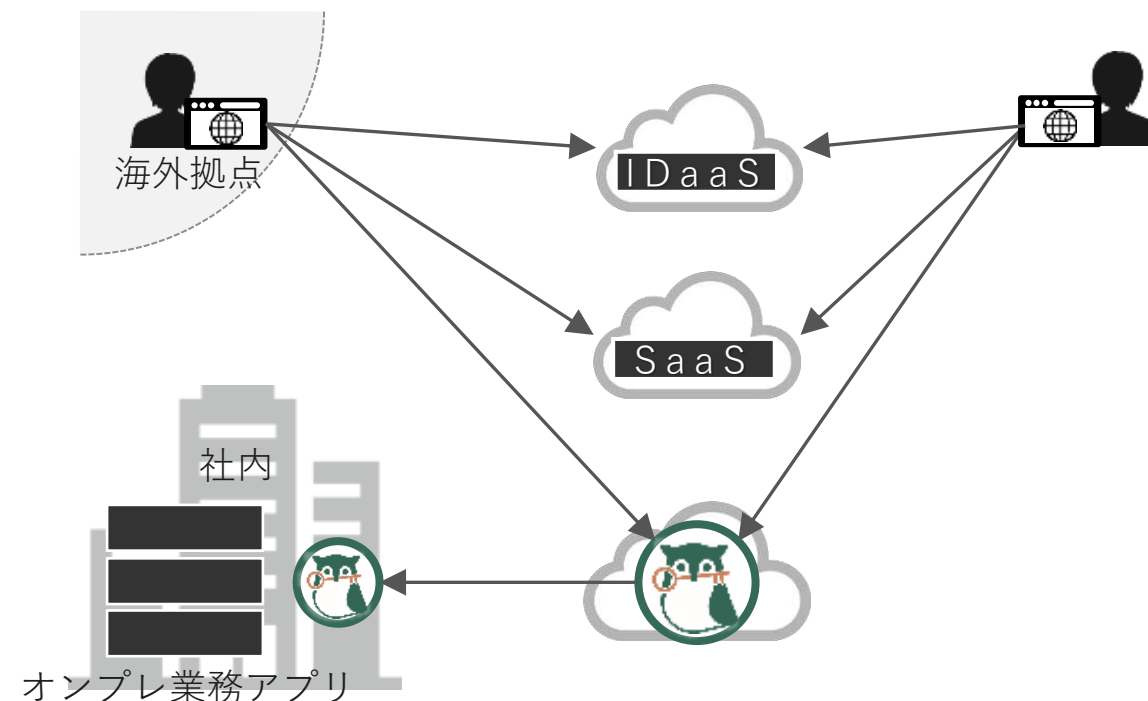


そんなに大規模でなくていいんだけど...

## 日本国内を主要拠点とする企業・団体向き

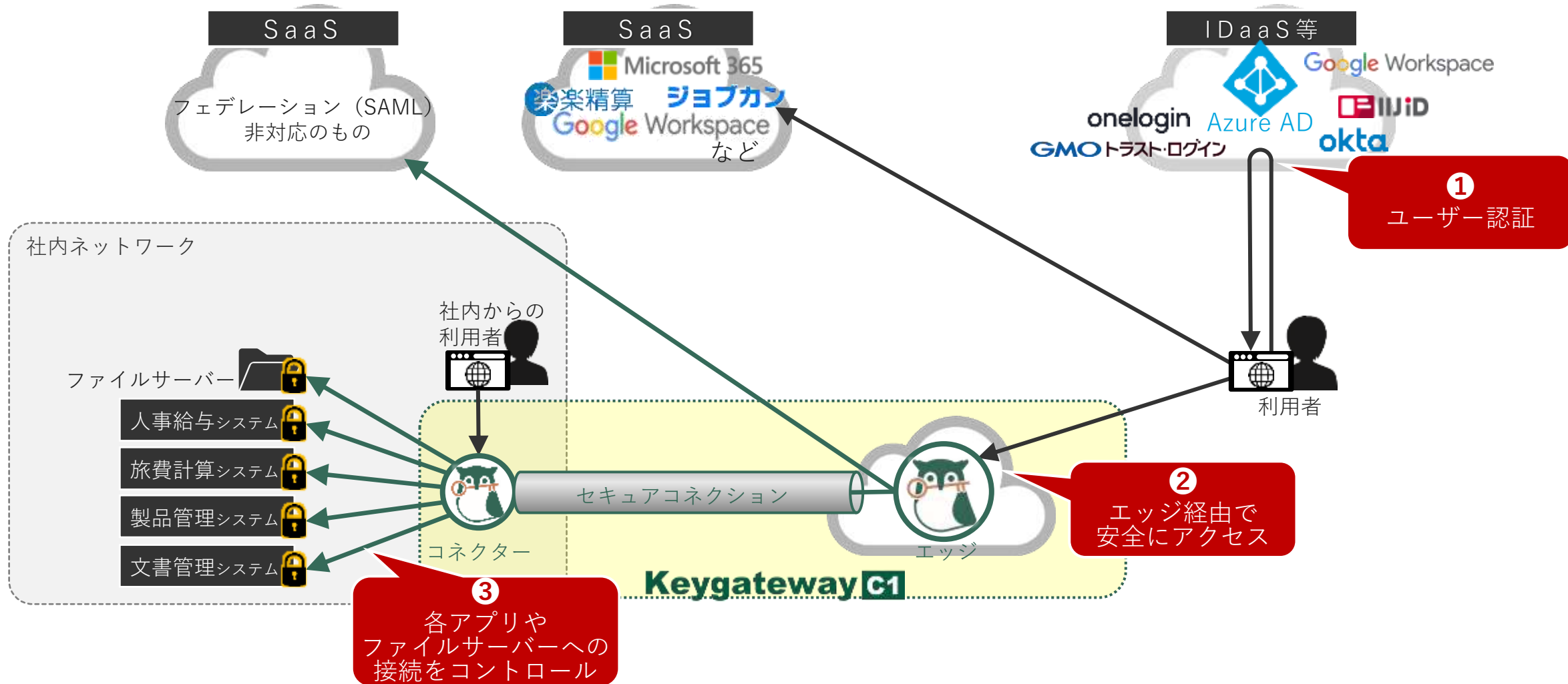
### ■ 日本企業に必要な機能をシンプルに実現

- 国内のノード（エッジ）に接続、社内までアクセス
- ユーザー認証はIDaaSを利用
- 日本企業が必要とする機能を装備（順次増強中）
- 端末用アプリ原則不要（一部機能利用時のみ必要）
- 社内にコネクタを設置





# ゼロトラストを導入して、社内システムをプライベートSaaS化



## 日本発、国内企業向けZTNAサービス

1

**VPNの代替**として利用でき

さらに便利です

2

VPNよりも**強固なセキュリティ**で

社内システムを守ります

(IDaaS等との連携によりMFAにも対応)

3

クラウドサービスだけでなく

**社内システムのアクセス制御も統合し**

利用者や管理者の負荷を大幅に低減します

4

運用負荷の低い

**クラウドサービス**で提供します

## VPN利用の場合

セキュリティリスク低減

- △ • いったん侵入されたら自由に活動されてしまう

管理者の負荷軽減

- △ • クライアントツール管理
- △ • ばらばらに出力されるログ

利用者の負荷軽減

- △ • 各システム個別のID/PW (自己管理)

運用コスト抑制

- △ • 回線や帯域の増強
- △ • 機器の入替、メンテナンス

 **Keygateway C1**

- • ゼロトラストモデルを用いた接続コントロール

- • クライアントツール不要
- • 統合されたアクセスログ

- • SSOにより認証自動化されPW管理不要

- • クラウドサービス利用料のみ (初期構築費用は別途)

## ユーザー情報管理

Keygateway Version: 1.0.0

検索対象テナント: [選択] | ユーザーID: [検索] | 表示件数: 20 件

管理対象情報

- ログ検索
- 管理者情報
- ユーザー情報
- テナント

## 管理者情報管理

Keygateway Version: 1.0.0

テナント名: [管理用テナント] | テナントID: keygateway

管理者追加

ID	管理者ID	管理者名	作成日時	更新日時	処理
1	admin@keygateway.jp	かもめ管理者	2022/03/29 14:01:58	2022/03/29 14:01:59	変更 削除

## アクセスログ検索

Keygateway

検索対象テナント: [選択]

日時: [年][月][日] [時][分] から [年][月][日] [時][分] まで

アクセス元IP: IPv4形式で指定してください。 (192.0.2.0) | ユーザーID: 半角英数字記号で入力してください。 (abc/12)

トランザクションID: 半角英数字記号で入力してください。 (abc/12) | メッセージ種別: [選択]

認可結果: [選択] | HTTPステータスコード: [選択]

HTTPメソッド: [選択] | アクセス先URL: [検索]

ポリシー名: [選択] | 認可理由: [選択]

表示件数: 20 件

日時 | アクセス元IP | ユーザーID | トランザクションID | メッセージ種別 | 認可結果 | ポリシー名 | 認可理由 | HTTPステータスコード | HTTPメソッド | コンテンツ表 | アクセス先URL

※ 予告なく変更する場合があります

「ファイルサーバーには  
対応していませんか？」



**Webアプリ以外にも  
対象システムを拡大中**

- 第一弾：  
**ファイルサーバー対応**
- 今後対応予定：  
クラサバ型業務アプリ  
Windowsアプリ  
VDI 等

「ZTNAサービスでは、  
Webプロキシを  
越えられないようで…」



**独自機能を付加し、  
Webプロキシ経由の接続可能**

- ZTNAの導入を断念していた  
お客さまでも採用
- i-FILTERやFortiGateなど  
主要製品で実績

「最初の導入の際は  
手伝ってもらえますか？」



**技術サポート提供**

- お客さま側のツール  
（コネクタ）等の構築を  
提供可能です
- 構築を自社のビジネスと  
されたいSI事業者さまに  
スキトラも積極的に提供中





全体的にサクサク動いて**動作が早い**と感じた。代理認証ももたつかない印象で、社内でも好評です。

【情報通信業、3,000名、セキュリティシステム担当】

最初に某海外ベンダのサービスを検証したが、**Webプロキシを経由**する必須条件がクリアできず、採用を断念。Keygateway C1 は**連携テストをすぐ共同で実施**でき、条件もクリアできることが確認できて助かりました。**スキルトランスファー**にも積極的で、これから提案する先の幅が広がりました。ファイルサーバー連携機能も期待しています。

【システムインテグレータ、顧客提案担当SE】

AzureAD Application Proxyと比較検討した。Keygateway C1の方が業務アプリにログインするまでの時間が速く、**体感で1/2程度**。お客さまの評価も高く、選定の決め手になった。

【製造業、2,500名、情報セキュリティ担当】

当時未実装だった機能を要望したが、ロードマップに反映し実装してくれた。実装の途中で**トライアル環境を積極的に提供**してくれ、社内への説明に役立った。

【建設業、800名、情報システム担当】

海外ベンダーのサービスを検討していたが、高価すぎて断念。Keygateway C1 は**実質1/3以下の価格**で、**サポートが国内から**提供という点も安心材料だった。今後のSMBプランにも期待。

【医薬系、50名、経営企画部門】





※ 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・利用の事例



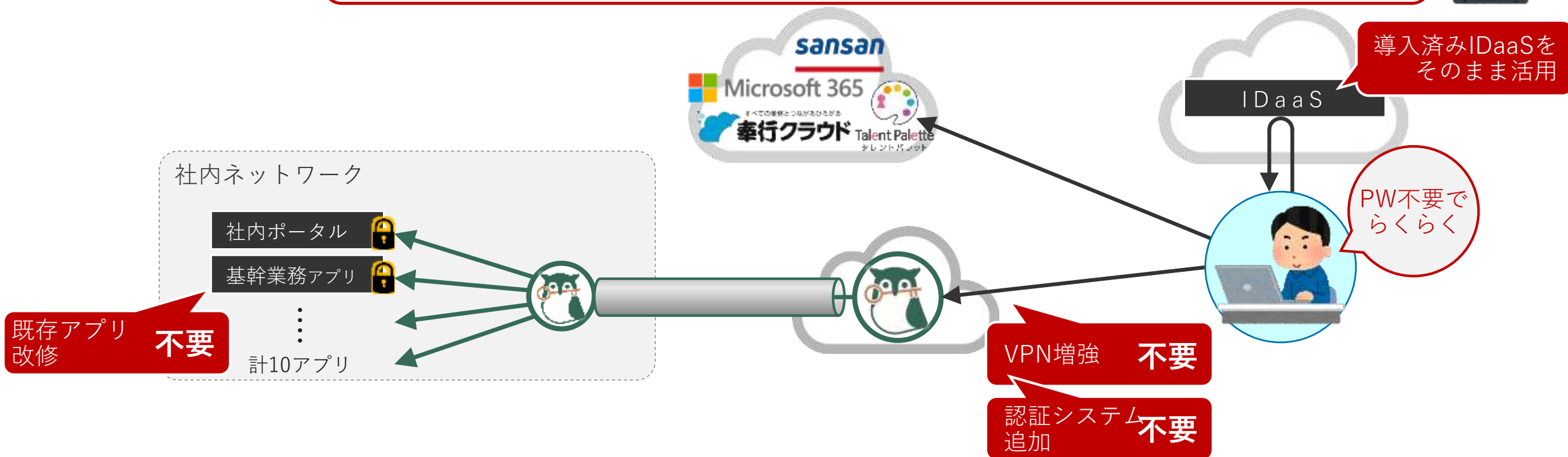
## ① 不動産業（利用者数：約200名）



- 社内ネットワーク上の業務アプリは、VPNを利用して接続していた。
- テレワークが増えた現在、ID/パスワードを各自で管理させるのはハイリスクだ…



- Keygateway C1 導入で、**利用者個人によるパスワード管理が不要**になりセキュリティが向上できた



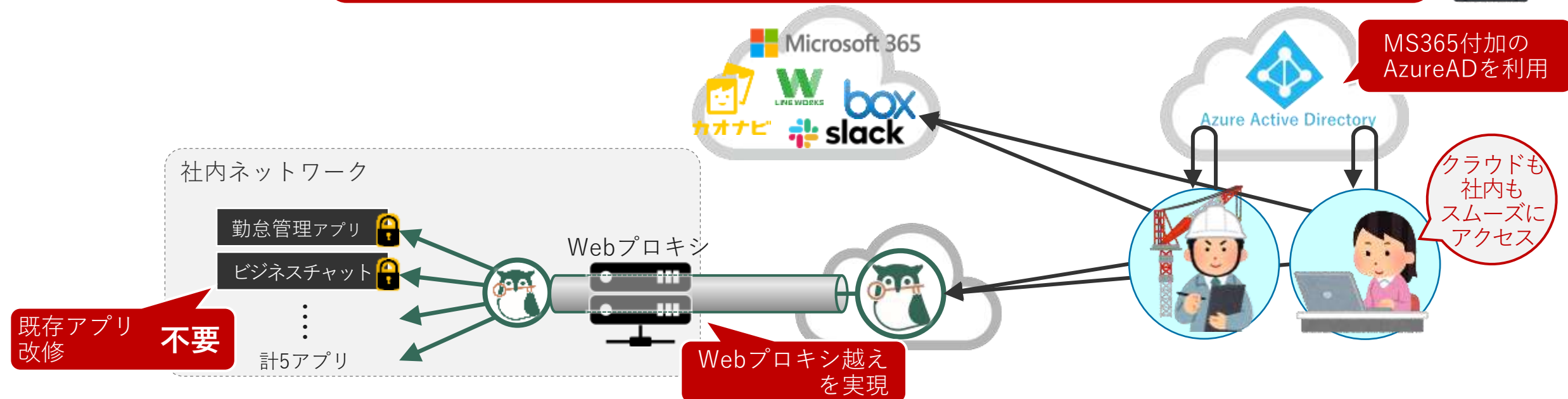
## ② 建築・土木業（利用者数：約800名）



- ZTNAサービスを利用したいが、Webプロキシを超えられないようで、導入は断念するしかないか…。



- Keygateway C1 は、**Webプロキシを経由した接続**も可能だったので支障なく導入できた。



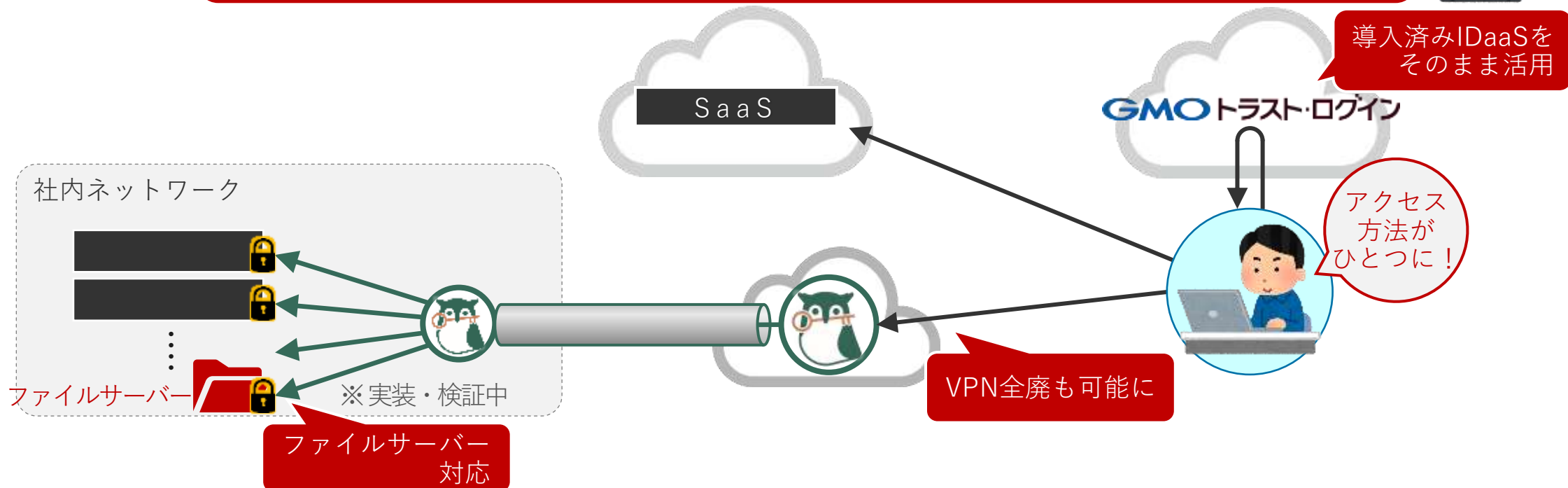
### ③ 通信事業者（利用者数：約3,000名）



- 機密性の高いデータが多く入ったファイルサーバーをSSOから除外したくないが、ZTNAサービスの連携対象はWebアプリ限定ばかりだったので困った…。



- Keygateway C1 は、**ファイルサーバーへの接続もカバー**されるので、全面導入を前提に現在PoC中。




# 導入検討のための情報





名称・詳細つき比較表も個別にご提供できます (お問い合わせください)

	海外ブランド サービス A	海外ブランド サービス B	海外ブランド プロダクト C	かもめエンジニアリング 
主な対象	海外拠点多い グローバル企業	海外拠点多い グローバル企業	同社オフィススイートクラウドサービスを利用中の企業	<b>100ID</b> ~規模の、 国内を主な拠点とする組織
コスト	<ul style="list-style-type: none"> <li>● 初期費用は別途</li> <li>● 利用費用 (年間) 1IDあたり 1万円以上</li> </ul>	<ul style="list-style-type: none"> <li>● 初期費用は別途</li> <li>● 利用費用 (年間) 1IDあたり 2万円以上</li> </ul>	<ul style="list-style-type: none"> <li>● 初期費用は別途</li> <li>● 利用費用は対象プランによる</li> <li>※プランによりSLA設定無し</li> <li>※自社設備として運用のため、ベンダ以外にSI事業者からの有償サポートが必要なケースも</li> </ul>	<ul style="list-style-type: none"> <li>● 初期費用は別途</li> <li>● 利用費用は他社サービスの 1/4 ~ 1/3 程度以下 (ボリュームディスカウントあり)</li> <li>● サポートは国内で提供</li> <li>● <b>10ID~100ID規模の SMB向けメニューも準備中</b></li> </ul>
機能等	<ul style="list-style-type: none"> <li>● 世界各国にノード設置</li> <li>● ノードから社内NWまでセキュアな通信</li> <li>● 端末アプリ/Webブラウザ (利用範囲限定)</li> <li>● 認証の自動化機能無し</li> <li>● 認証は独自基盤か IDaaS (海外IDaaS)</li> <li>● 社内からのアクセスは別サービスを組合せ</li> </ul>	<ul style="list-style-type: none"> <li>● 世界各国にノード設置</li> <li>● ノードから社内NWまでセキュアな通信</li> <li>● 端末アプリ</li> <li>● 認証の自動化機能予定</li> <li>● 認証は独自基盤か IDaaS (海外IDaaS)</li> <li>● 社内からのアクセスは範囲外</li> </ul>	<ul style="list-style-type: none"> <li>● 自社設備として導入・運用が必要</li> <li>● 認証の自動化機能あり</li> <li>● 社内システムの認証にADを利用</li> <li>● 構築・運用を担当可能なSI事業者が少ない</li> <li>● 社内からのアクセスは利用不可</li> </ul>	<ul style="list-style-type: none"> <li>● 認証の自動化機能あり</li> <li>● エッジ-社内NWでセキュアな通信</li> <li>● 認証はIDaaS (国内で利用可能な全てのIDaaSに対応)</li> <li>● 国内で利用するIDaaSと連携可能</li> <li>● 端末用アプリ不要</li> <li>● 社内からのアクセスにも利用可能</li> <li>● <b>ファイルサーバー対応</b></li> <li>● <b>Web Proxy経由アクセス対応</b></li> </ul>





詳細別途個別にご案内できます (お問い合わせください)

No.	名称	状況
01	AWS Single Sign-On	OK
02	AzureAD	OK
03	CloudGate UNO	OK
04	CloudLink	OK
05	Google Workspace	OK
06	HENNGE ONE	検証中
07	Keycloak	OK
08	Nextset	検証中
09	Okta	OK
10	Onelogin	OK
11	OpenAM	OK
12	TrustLogin	OK
	: (随時検証中)	

※ 2022.04現在。SAML / OpenID Connect に対応したIdPであれば基本的に連携可能です。



No.	名称	種別	方式	状況
01	ADPS	SaaS	FORM認証	連携OK
02	aipo	SaaS	FORM認証	連携OK
03	Alfresco	オンプレ	ヘッダ認証	連携OK
04	Apace Guacamole	オンプレ	FORM認証	連携NG
05	ATLISSIAN	SaaS	FORM認証	検証中
06	Backlog	SaaS	FORM認証	連携OK
07	Box	SaaS	FORM認証	連携OK
08	COMPANY Talent Management	オンプレ	FORM認証	連携OK
09	cybozu.com Store	SaaS	FORM認証	連携OK
10	DataDelivery	オンプレ	FORM認証	検証予定
11	desknet's NEO	SaaS	FORM認証	連携OK
12	desknet's NEO パッケージ版	オンプレ	FORM認証	連携OK
13	Eight	SaaS	FORM認証	連携OK
14	FileBlog	SaaS	FORM認証	連携OK
15	GitLab	SaaS	FORM認証	連携OK
16	GRANDIT	オンプレ	FORM認証	連携OK
17	Jenkins	オンプレ	FORM認証	連携OK
18	Knowledge	SaaS	FORM認証	連携OK

No.	名称	種別	方式	状況
19	Money Forward ID	SaaS	FORM認証	連携OK
20	Monitorix	オンプレ	BASIC認証	連携OK
21	Office365	SaaS	FORM認証	検証中
22	Redmine	オンプレ	FORM認証	連携OK
23	Salesforce	SaaS	FORM認証	連携OK
24	TimePro-VG	オンプレ	FORM認証	連携OK
25	TimePro-XG	オンプレ	FORM認証	連携OK
26	Trello	SaaS	FORM認証	検証中
27	Voice Reader	SaaS	FORM認証	連携OK
28	WordPress	オンプレ	FORM認証	連携OK
29	Zabbix	オンプレ	FORM認証	連携OK
30	クラウドサイン	SaaS	FORM認証	連携OK
31	サイボウズ	オンプレ	FORM認証	連携OK
32	サイボウズのクラウド基盤	SaaS	FORM認証	連携OK
33	ジョブカン	SaaS	FORM認証	連携OK
34	楽楽精算	SaaS	FORM認証	連携OK
35	勤革時	SaaS	FORM認証	連携OK

※ 2022.03現在。  
 連携先システムの仕様により、一部に機能制限が生じる場合もあります。



## 自社のアプリに適用可能か、ご自身で簡単に確認が可能

Step ①  
ブラウザの準備

Firefoxの場合

2022.01  
Copyright©2021-2022 KAMOME Engineering, Inc. All rights reserved.

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変なチームです！



既存アプリのベンダーさんにいちいち確認しなくても大丈夫ですね！

# まとめ

- ✓ VPNの最も大きな課題に、セキュリティが挙げられます。
- ✓ 「すべてを信用しない」ゼロトラストモデルの導入により、ネットワークのセキュリティを向上できます。
- ✓ 利用者からのアクセスを動的に制御するZTNAサービスは、VPNの代替として利用でき、さらに高いセキュリティを実現します。
- ✓ 「Keygateway C1」は、さまざまな規模の日本企業に適したZTNAサービスです。
- ✓ **IDaaSも含めた総合的なソリューションについては、この後のスタイルズ様のセッションをご覧ください。**



# ありがとうございました



ゼロトラストやユーザー認証関連のWebセミナーを開催（月2～3回程度）  
さまざまな立場の方にご参加いただいております。



オライリー・ジャパン社より出版。  
当社 および 当社メンバーが、執筆・翻訳に携わりました。



ブログ記事をアップしています。あわせてご参照ください。  
「ZTNAとは何か?」「AzureADプラン比較」 など

<https://solution.kamome-e.com/blog/>



## ■ 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](mailto: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好きなおチームです！

