大手資材メーカーや大規模病院が実現した「脱VPN」の方法

ランサムウェア攻撃におけるVPNのリスクと、
KeygatewayC1による代替方法を解説

Keygateway C1

2024.11.25

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。

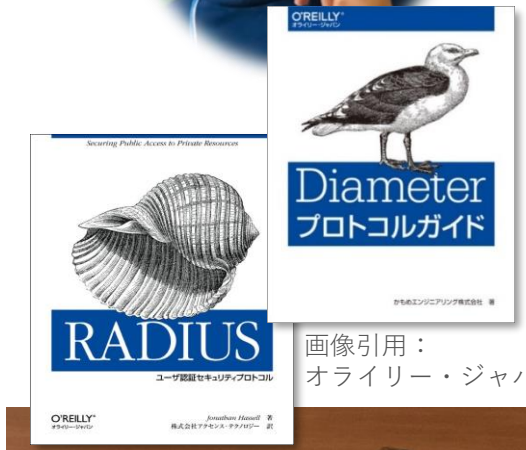
2017年、シングルサインオンシステム「KAMOME SSO」提供開始。

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）



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、時々マンガ。
最近のヒットは、何十度目かの再読　幸村　誠『プラネテス』。

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　KFEP（ケイフェップ）

特許取得

- 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）

- 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**

特許出願中

- 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）

特許取得

- 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）
- 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
- OEM提供先

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

KAMOME Engineering

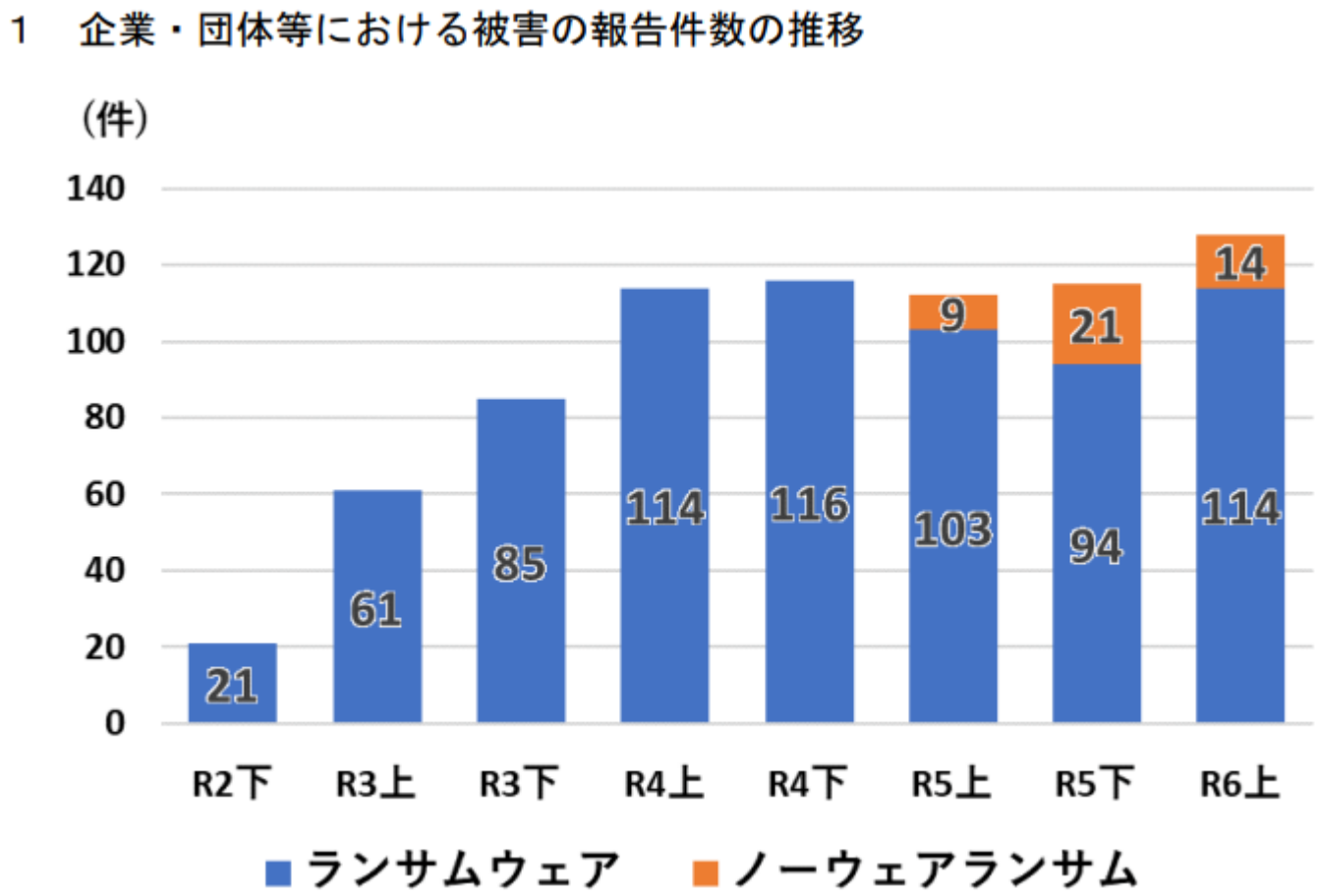
ランサムウェアによる被害の実態

感染の8割以上が「リモートアクセス経由」

KAMOME Engineering

被害は常態化している

警察庁『令和６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』より抜粋（一部画像加工）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf



※ ノーウェアランサム：
暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

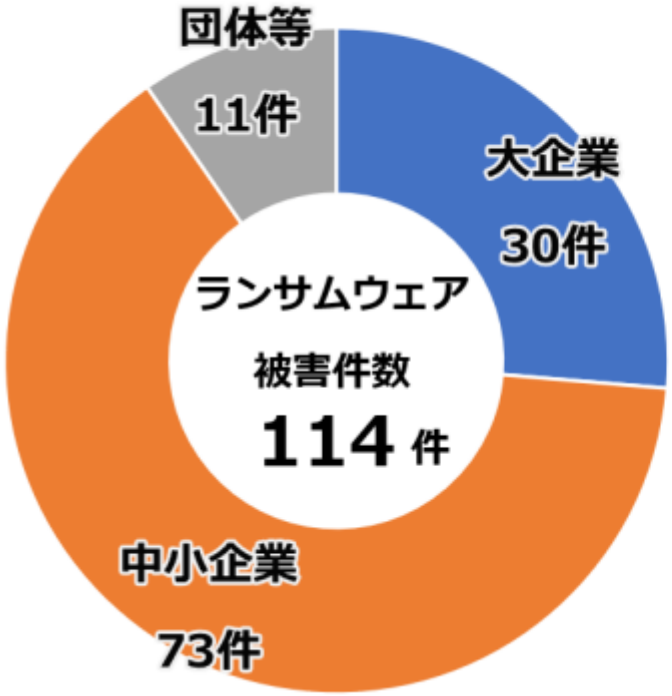
- 対策の必要性が繰り返し指摘されているにもかかわらず、**被害報告数は高止まり**状態
- 報告義務はないため、未報告の被害については不明
  - 特に中小企業の被害は報告されないケースも多いと考えられ、実際にはより多くの被害が発生しているはず

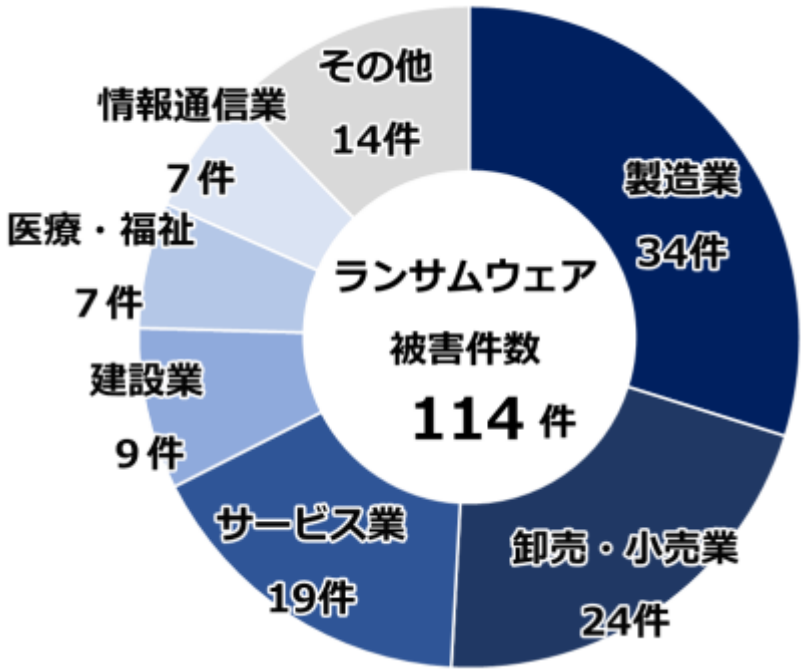
KAMOME Engineering

中小企業への広がりが進む、 業種は問わず

警察庁『令和６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』より抜粋（一部画像加工）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

３　被害企業・団体等の規模別／業種別報告件数





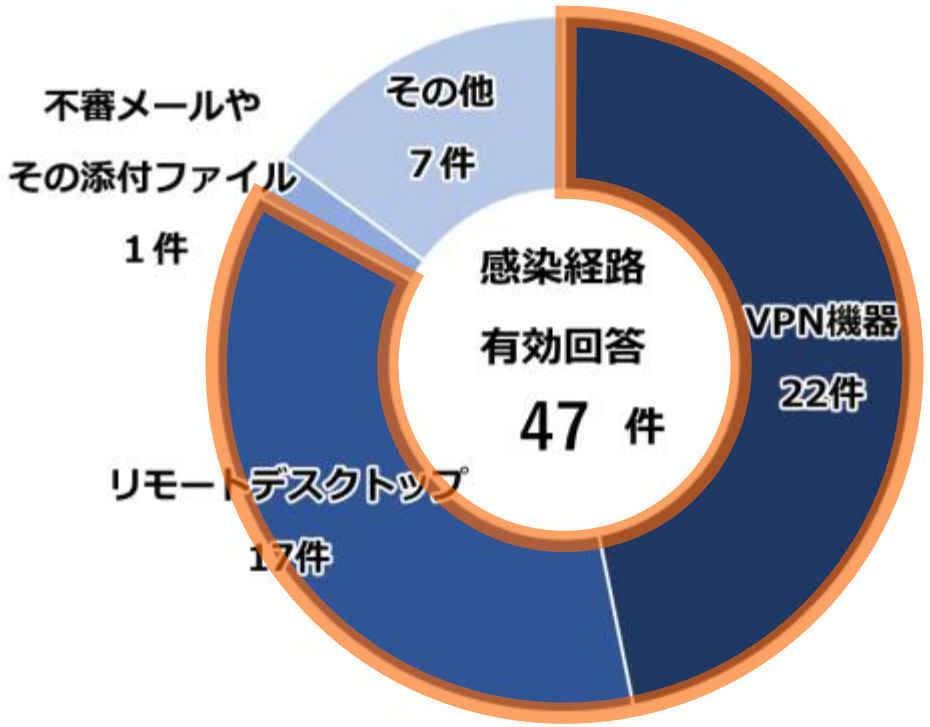
- **中小企業**の比率がさらに増加
  - 前年上半期　60件 58%
  - ➡ 今期　73件 64%
  - 身代金の獲得が比較的容易かつ短期間で可能と判断されている模様
- あらゆる業種がターゲットとなっている

KAMOME Engineering

感染経路 ＝ 圧倒的に「リモートアクセス」

警察庁『令和６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』より抜粋（一部画像加工）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

● 感染経路



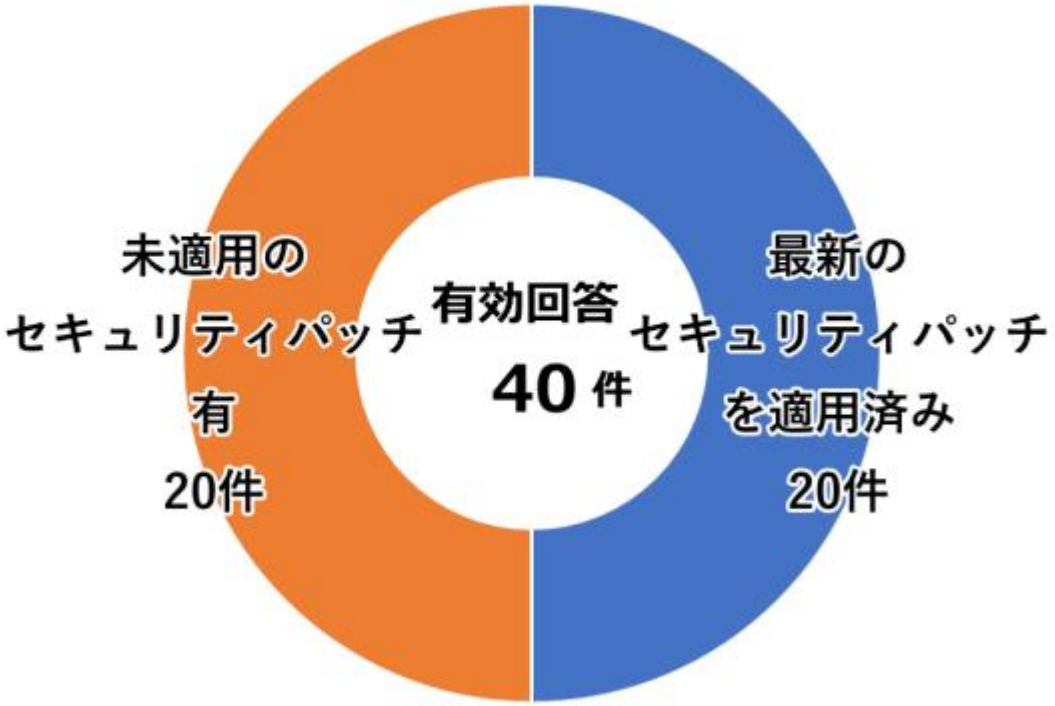
- リモートデスクトップ経由の被害が急増
  - 前年上半期　5件 10%
  - ➡ 今期　17件 36%
- VPN機器経由を含め **39件 83%が リモートアクセスの経路から** 侵入

KAMOME Engineering

「パッチを当てていれば大丈夫」？

警察庁『令和６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』より抜粋（一部画像加工）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

- 侵入経路とされる機器のセキュリティパッチの適用状況



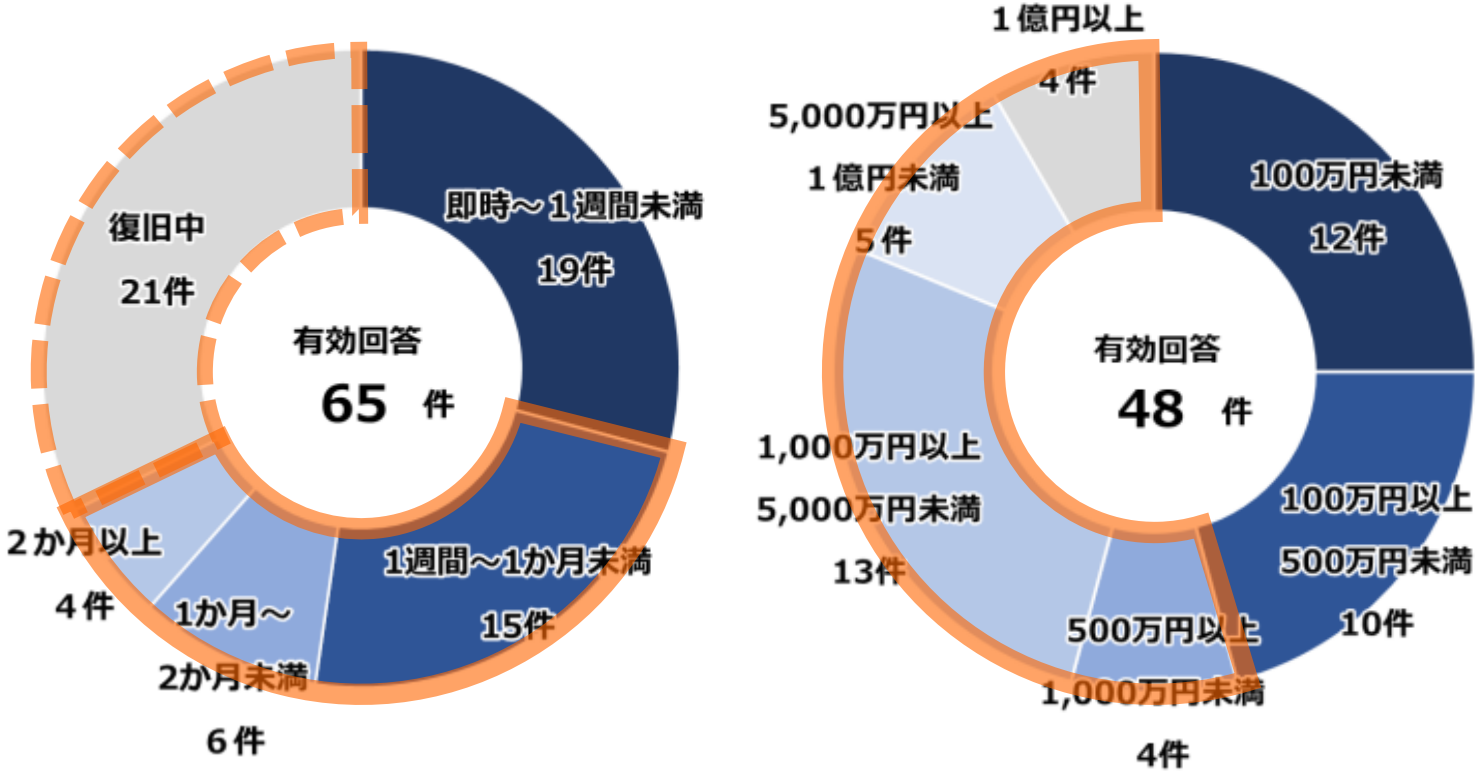
- 半数が、**セキュリティパッチを適用していた**にもかかわらず被害を受けた
- パッチ適用前に侵入されるケースも多い

KAMOME Engineering

事業への影響は大きい

警察庁『令和６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』より抜粋（一部画像加工）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

● 復旧等に要した期間／調査費用の総額



- **25件 38%** が、復旧等に**「1週間以上」**
  「復旧中」を含めると
  46件 71％
- **26件 54%** が、復旧等に**「500万円以上」**

KAMOME Engineering

システム自体への損害だけでなく…

被害総額「数十億円」におよぶケースもある

KAMOME Engineering

導入が広がる「ゼロトラスト」とZTNA

「中」と「外」を区別しないセキュリティ

KAMOME Engineering

「境界防御モデル」の限界 ➡ 実態と今後に適した進化へ

VPN等が前提とする境界防御モデル

クラウド上やSaaSへ
業務システムは拡大中

インターネットなど組織外
＝ **信用できない**

F/Wなどで境界を防御

組織内ネットワーク
＝ **信用できる**

この中なら
安全！

情報資産

境界内だけ守ればOK？
社外からはVPNでOK？

**セキュリティ
モデルも
進化が必要**

ゼロトラストモデル

インターネットなど組織外
＝ **信用できない**

**すべての
接続を検証**

情報資産

どこにあっても
守る対象は情報資産

組織内／組織外を問わず
同じ基準で常にチェック

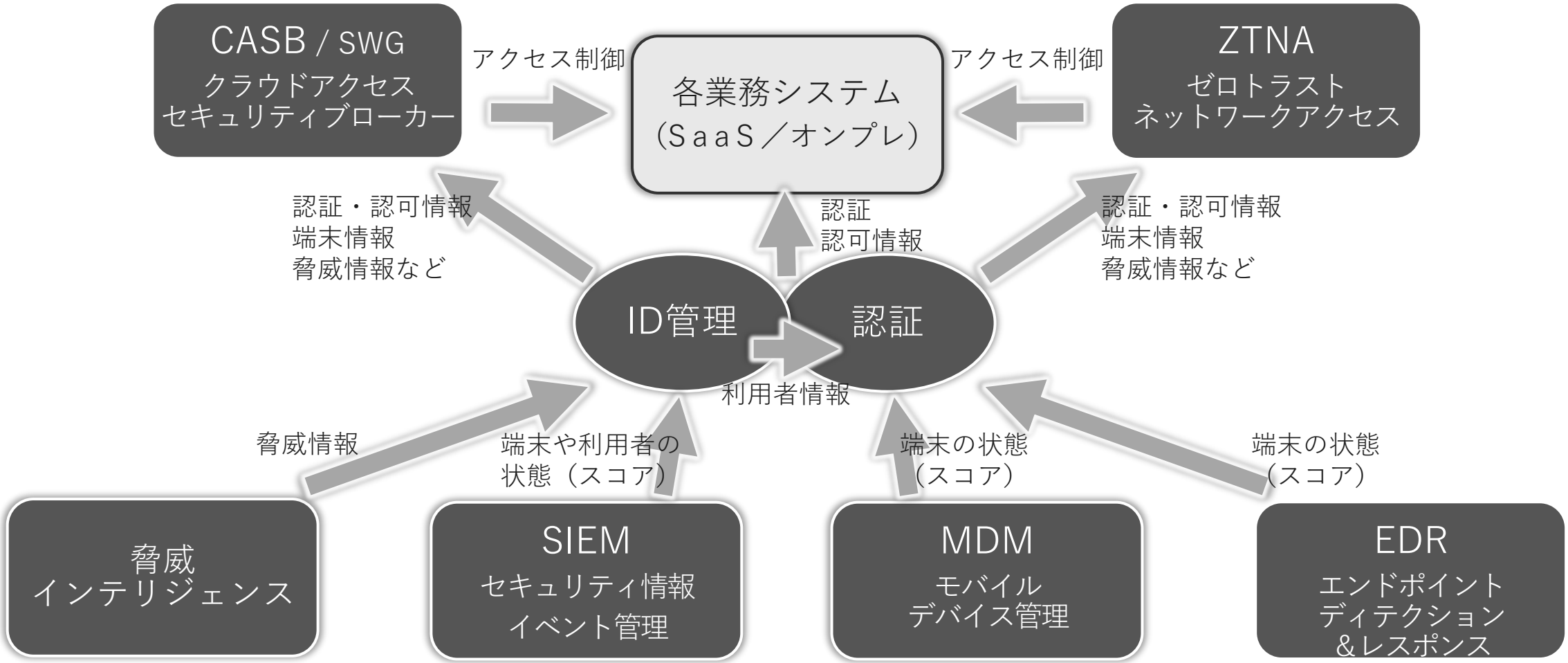
アクセス権の提供は
常に最小限度に限定

組織内ネットワーク
＝ **信用できない**

安全圏は
どこにもない

KAMOME Engineering

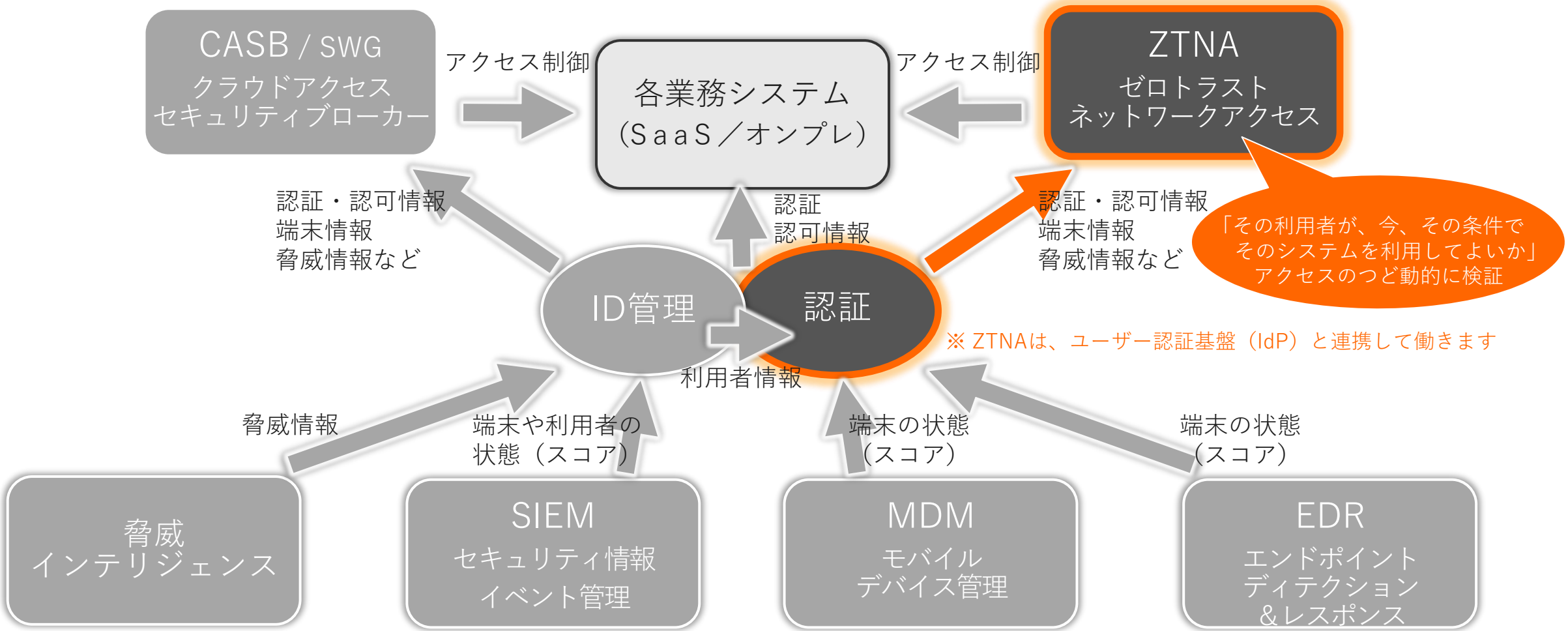
ゼロトラストモデルの主な構成



※　各要素の定義・分類・機能等は、ベンダー毎に少しずつ異なった状態であり、明確に定まってはいません。

KAMOME Engineering

ゼロトラストの中核を担うZTNA（Zero Trust Network Access）



※　各要素の定義・分類・機能等は、ベンダー毎に少しずつ異なった状態であり、明確に定まってはいません。

KAMOME Engineering

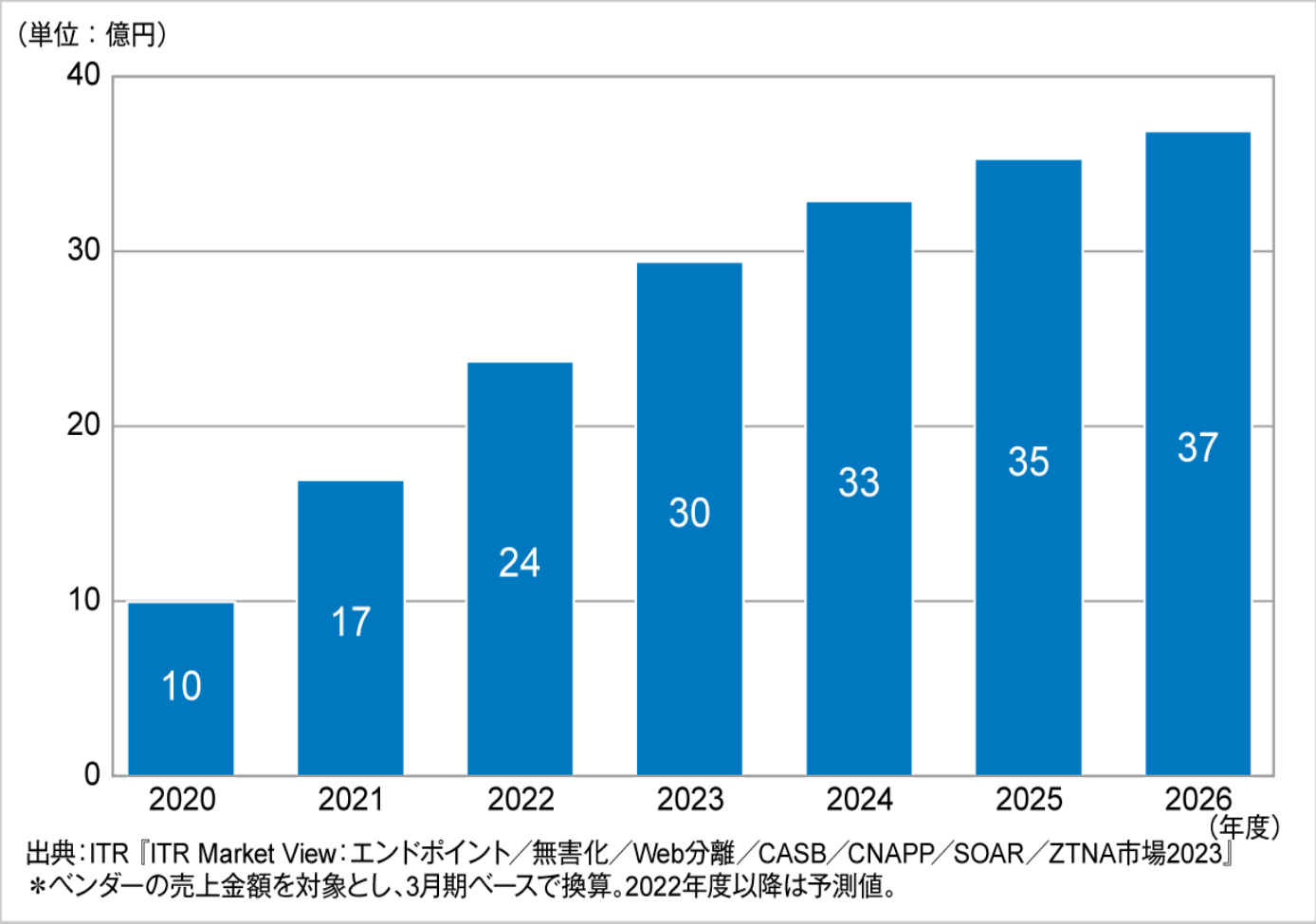
VPN等の代替となり、より強固なセキュリティのZTNA

	VPN／RDP	ZTNA
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	○ • ゼロトラストモデルを用いた接続コントロール
管理者の負荷軽減	△ • 機器の管理・入替 • 帯域・帯域コストの管理 • ばらばらに出力されるログ	○ • VPN機器の管理・入替不要 • 帯域・帯域コストの管理不要 • 統合されたアクセスログ
利用者の負荷軽減	△ • 各システム個別のID/PW（自己管理）	○ • SSOにより認証自動化されPW管理不要

KAMOME Engineering

境界防御モデル ➡ ZTNA の移行は進行している

ITR Market View（2023年6月）



出典：ITR『ITR Market View：エンドポイント／無害化／Web分離／CASB／CNAPP／SOAR／ZTNA市場2023』
＊ベンダーの売上金額を対象とし、3月期ベースで換算。2022年度以降は予測値。

メディア @IT atmarkIT

「今後はVPNに代わってZTNAが主流になる」

企業システムのクラウドシフトとテレワークの定着に伴い、従来の「境界型防御セキュリティ」を見直し、ZTNAの導入を検討する企業が増えている。

「ゼロトラストセキュリティ」という概念が定着したことや、VPN機器の脆弱（ぜいじゃく）性を突いた攻撃が起きていることなどの要因からZTNAへの注目が高まっており、市場が大きく成長しているという。

ITRの藤 俊満氏（コンサルティング・フェロー）は、「自宅などからVPNを使用して社内ネットワークにログインし、クラウドサービスを使用するというやり方では、同時ログイン数の制限があったり、レスポンスが遅くなったりする問題がある。ZTNAであればその問題を解決できるため、今後はVPNに代わってZTNAが主流になるだろう」と述べている。

ITRは、2021～2026年度の年平均成長率（CAGR）を16.8%と見込み、2026年度の市場規模は37億円に達すると予測している。

引用 …https://atmarkit.itmedia.co.jp/ait/articles/2306/16/news046.html（画像一部加工）

KAMOME Engineering

大手資材メーカーの事例

ZTNAソリューション

Keygateway C1

KAMOME Engineering

お客様の概要

企業規模	国内 約10支店、工場等 約10拠点
従業員数	1,500 ～ 2,000人規模 （単体）
リモート業務利用者数	6,000 ユーザー （各種スタッフ含む）
接続先システム	約 40 システム

KAMOME Engineering

お問い合わせの概要

利用中のSSOシステムが更改となり、それには **Entra ID**（**旧AzureAD**）の採用が決まった

リモートアクセスには**キャリアのVPNを利用中**だが、
セキュリティ上の課題が大きい上に、**回線がビジー**な問題も抱えている

VPNの替わりとなる、 Entra ID と連携できるソリューションを探している

稼働中のオンプレミス業務システムは Entra ID でSSOできないことも課題

KAMOME Engineering

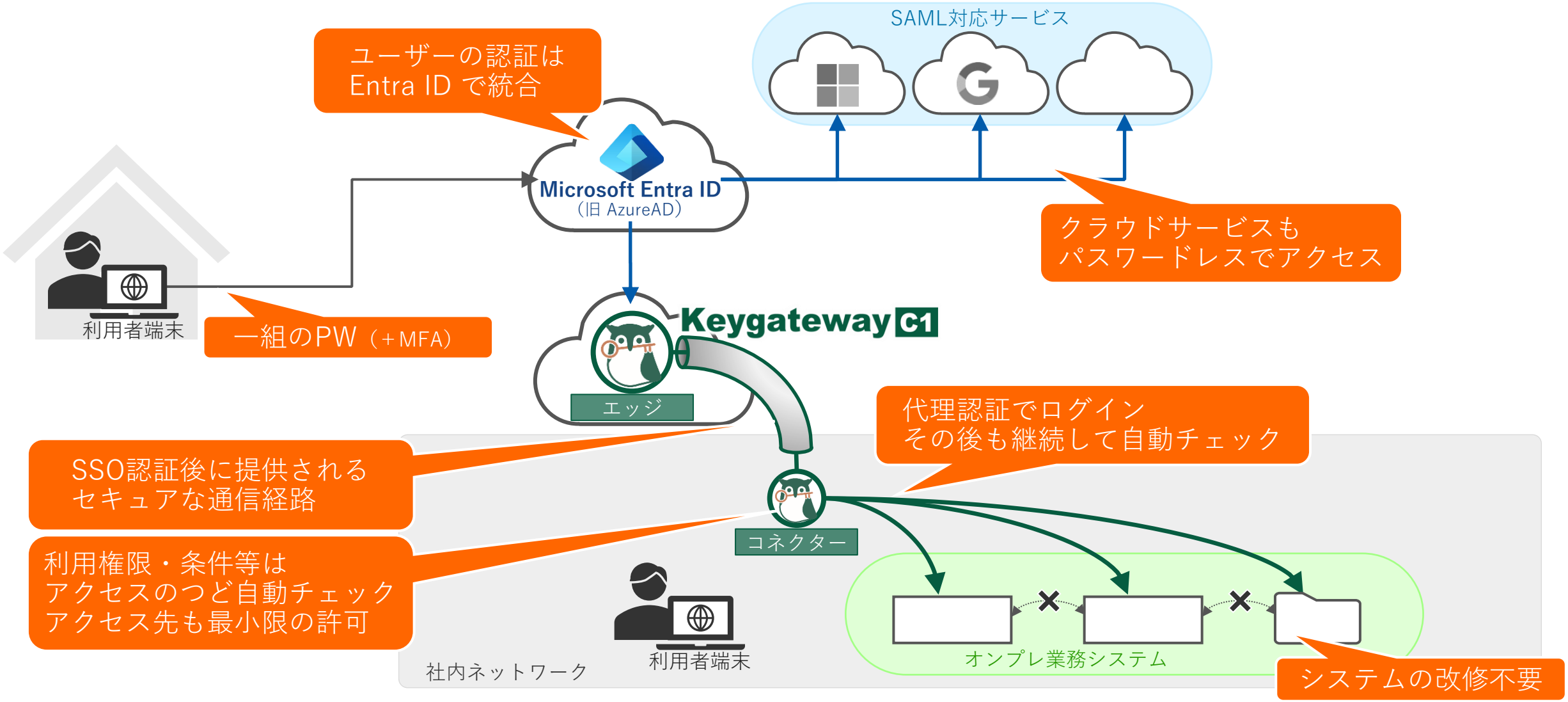
主なご要望と、それに対する解決案

- **VPNの廃止**
  - ➡ ZTNAソリューションを導入
  - ➡ 認証基盤である Entra ID と連携

- **セキュリティの強化**
  - ➡ ZTNAによるユーザ単位・システム単位で動的なアクセス制御を実現

KAMOME Engineering

ご提案の構成概要



KAMOME Engineering

お客様ご選定の主なポイント

- 「Entra ID との連携実績が豊富なことで、有力候補となった」
- 「同じくZTNAソリューションである Entra Private Access と KeygatewayC1 で
  それぞれ数ヵ月ずつPoCを行い比較検討した結果、
  最終的に処理の速さ（体感としては2倍程度）が決め手となった」
- 「社内からもSSOは使用できる必要があり、その解決方法も優れていた」
- 「さらに、自社運用担当者へのスキルトランスファーに
  積極対応してくれたことも大きかった」

KAMOME Engineering

大規模総合病院の事例

ZTNAソリューション

Keygateway C1

KAMOME Engineering

お客様の概要

病院規模	病床数 … 数百床
院内スタッフ	～ 1,000名
リモート業務利用者数	数百名
接続先システム	クラウドサービス　数件 院内オンプレシステム　数件　（一部リモートデスクトップ使用）

KAMOME Engineering

お問い合わせの概要

リモート業務にVPNを利用していたが、セキュリティリスクが問題視されたため**遠隔診断などの運用をいったん停止**した

結果として**医療提供に一部遅延**も発生しているため、できるだけ早く再開させたい

VPNよりも安全性の高いリモートアクセス手段を、まず早急に確保する必要がある

一部に**リモートデスクトップ**を使用しているので、それも含めたセキュリティ向上を図りたい

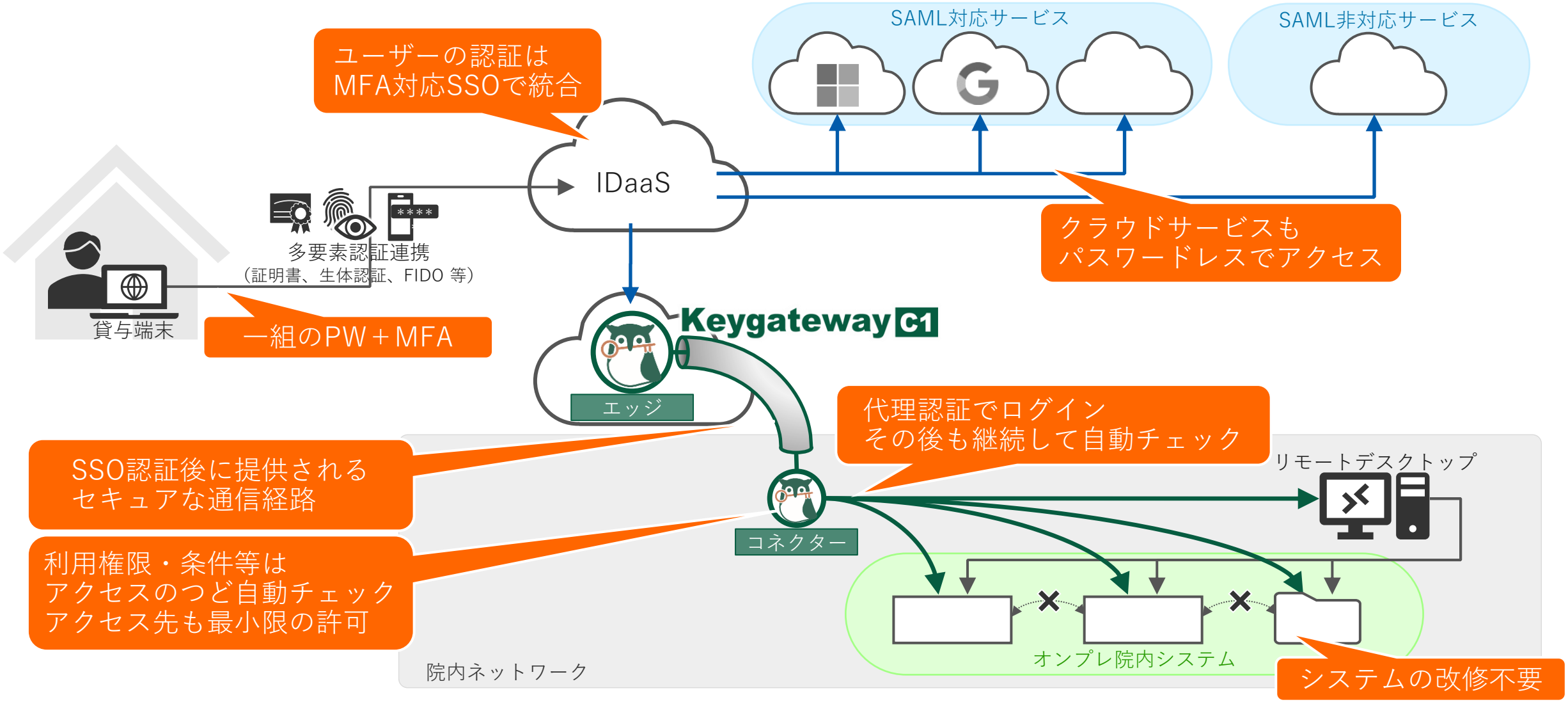
KAMOME Engineering

主なご要望と、それに対する解決案

- **VPNの廃止**
  - ➡ ZTNAソリューションを導入
  - ➡ 認証基盤である IDaaS と連携
- **セキュリティの強化**
  - ➡ IDaaSによるシングルサインオン（SSO）環境の導入
  - ➡ 多要素認証（MFA）対応も実現（証明書、ワンタイムパスワード 等）
  - ➡ ZTNAによるユーザ単位・システム単位で動的なアクセス制御を実現

KAMOME Engineering

ご提案の構成概要



KAMOME Engineering

お客様ご選定の主なポイント

- 「KeygatewayC1は、シンプルにVPNの代替となるソリューションが欲しいというニーズに合っていた」
- 「比較検討した競合のZTNAサービスは、オーバースペックであり、高価格すぎた」
- 「別途検討中のID管理ソリューションも含め、連携実績があるものを一括して提供してもらえるのは有難い」
（多数のベンダーから別々に導入するのは結構大変）

導入の主要ポイント

- 境界防御型のリモートアクセスを廃止してゼロトラスト化することで、
機密性の高い情報資産をより強力に守れます。
- 既存社内システムもまとめてSSO化するため、利便性や生産性が向上します。
- 認証基盤を整備することで、今後のシステム拡充を容易にします。
- かもめエンジニアリングが提供する、国産のクラウドサービスです。
設置場所やサポート等も、すべて国内で完結します。
- グローバルベンダーから提供される大規模なサービスと比較して、
コストパフォーマンスが格段に良いです。

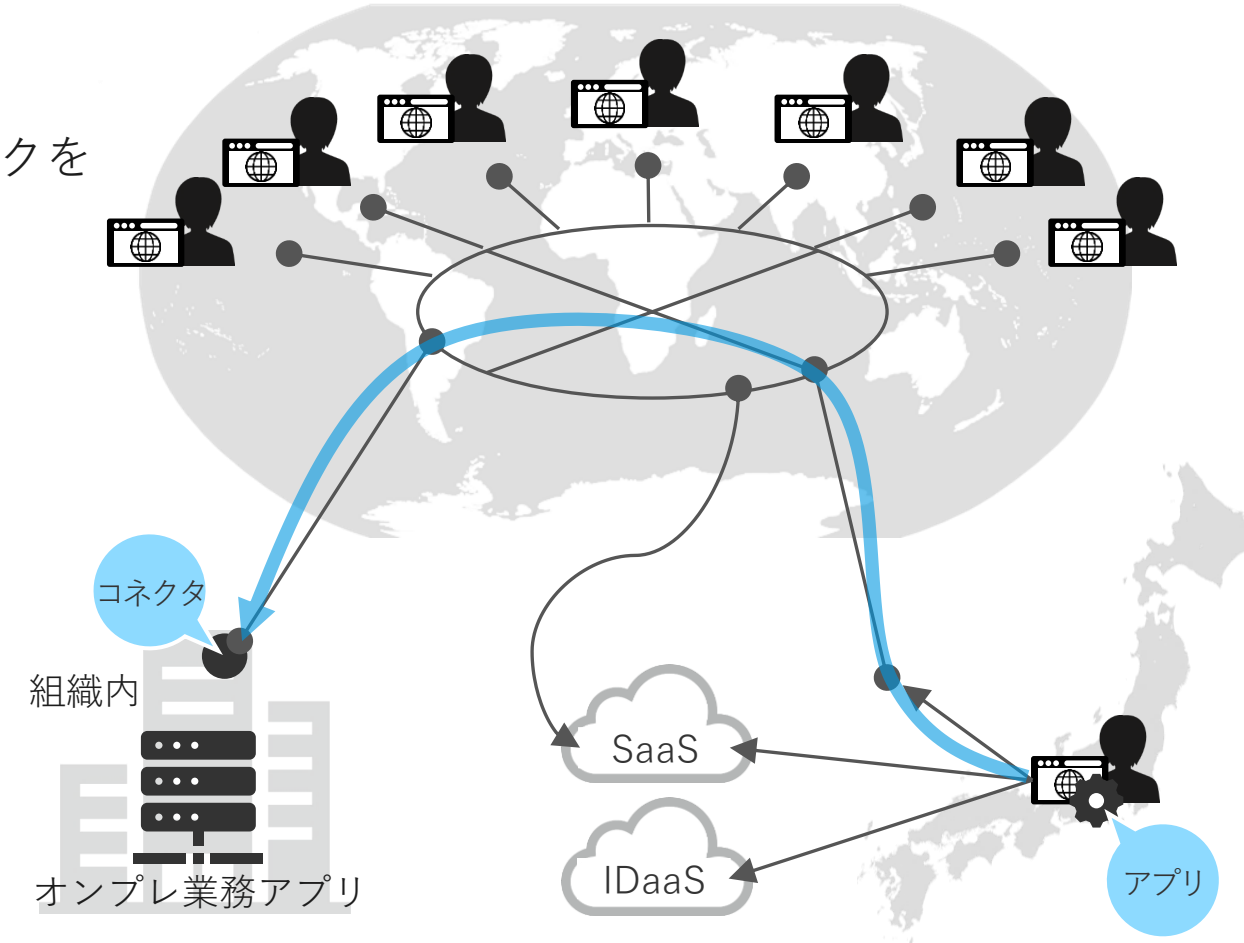
【参考】グローバルベンダーのZTNAサービス（構成イメージ）

KAMOME Engineering

世界中にアクセスポイントを多数設置

- 最寄りのアクセスポイントに接続、独自ネットワークを経由して組織内までセキュアな経路を提供
- ユーザー認証は、独自基盤またはIDaaSを利用
- 端末にアプリ導入、社内にコネクターを設置
- 多機能、大規模、高価格

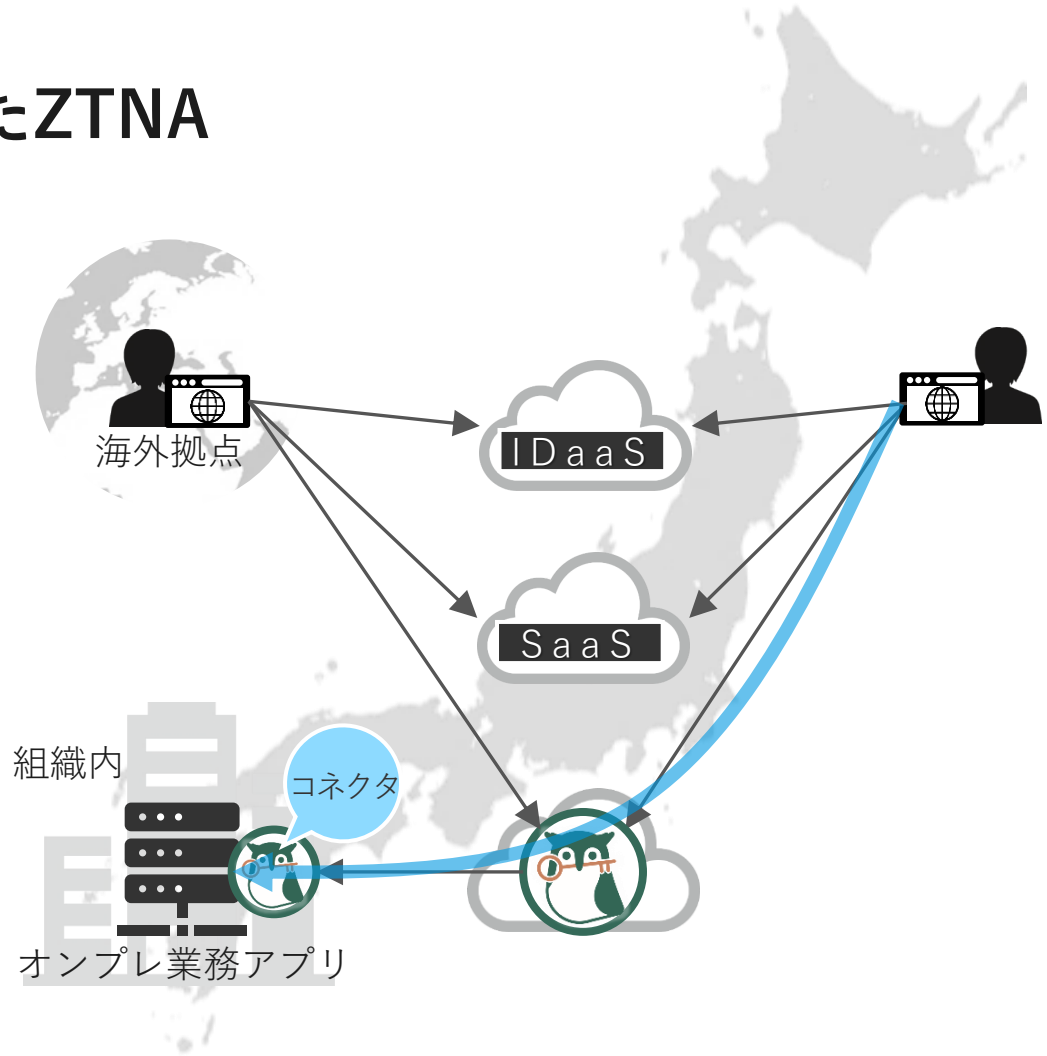
世界中に拠点があるグローバル企業向き



ゼロトラスト接続サービス
Keygateway C1

日本企業に必要な機能をシンプルに実現したZTNA

- 国内のアクセスポイント（エッジ）に接続、組織内まで
  セキュアな経路を提供
- ユーザー認証は、IDaaSを利用
- 端末のアプリ不要（接続先がWebアプリの場合）
  組織内にコネクター設置
- 最小限のアクセス権限を提供するほか、場所や時間帯での
  アクセス制限も可能

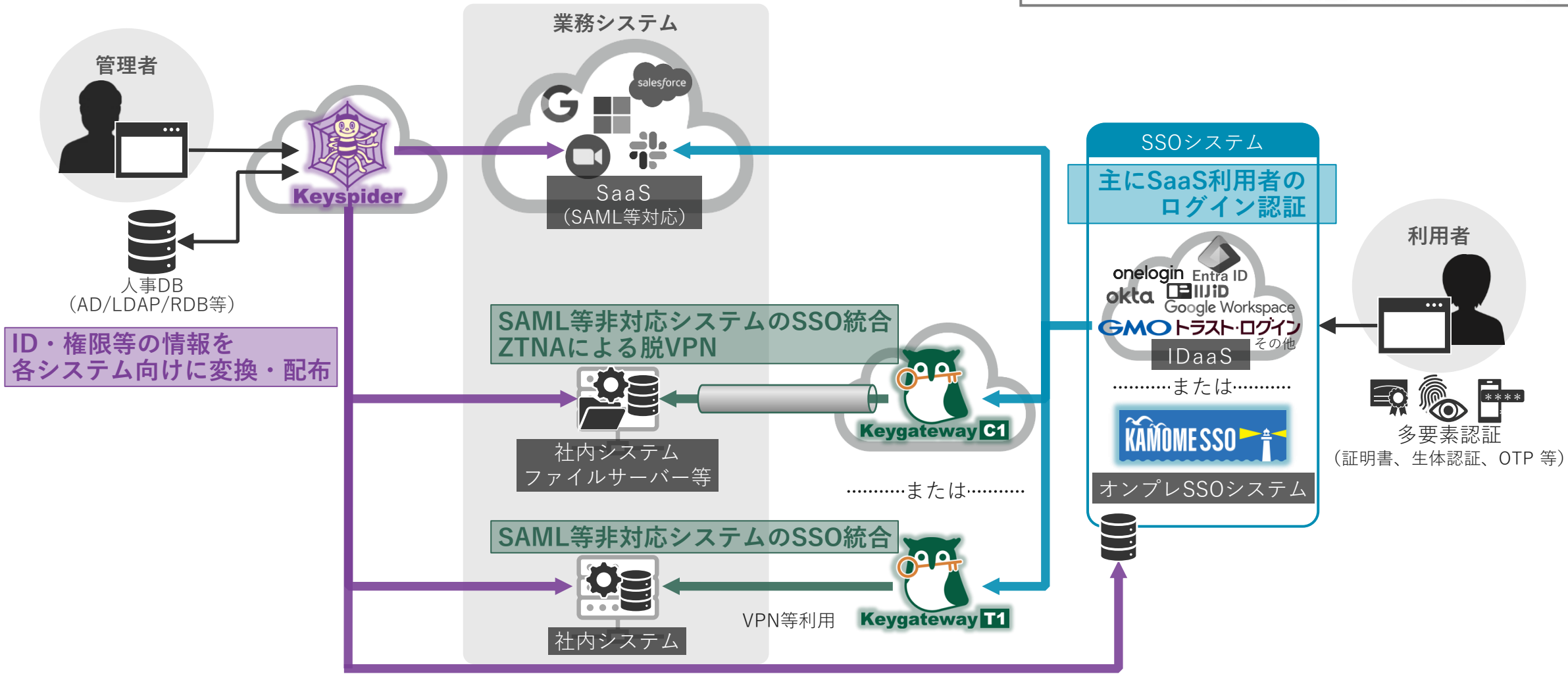


日本国内を主要拠点とする法人・団体向き

KAMOME Engineering

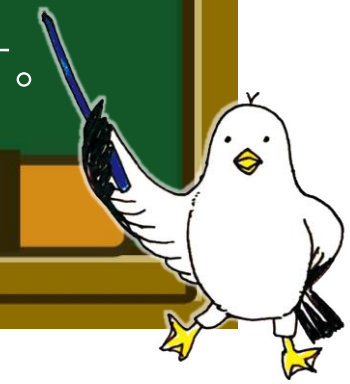
トータルな課題解決を提供しています

KAMOME SSO　Keygateway C1　Keygateway T1　Keyspider

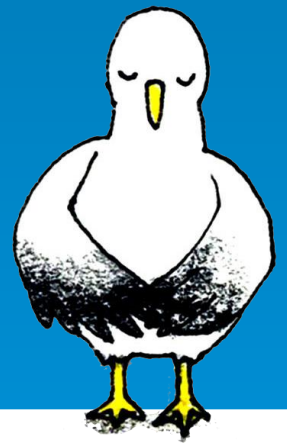


まとめ

- VPNなどのリモートアクセス経路を主な侵入路とした ランサムウェア攻撃は減少の気配を見せておらず、被害は深刻な状態が続いています。
- VPNなどの境界防御モデルにはセキュリティ上の課題が指摘されており、それに替わるリモートアクセス手段としてZTNA（ゼロトラストネットワークアクセス）の導入が進んでいます。
- ゼロトラストはハードルが高いと思われがちですが、コストパフォーマンスの高いミニマムなソリューションもあります。
- 「KeygatewayC1」で脱VPNを実現し、情報資産のセキュリティを高めましょう。
- ユーザー認証分野に多くの実績を持つかもめエンジニアリングよりご提供します。
- **個別のWebミーティングを設定します。ぜひご要望ください。**



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が大好きなチームです！