マジセミ

ZTNAと「KeygatewayC1」解説

～ ゼロトラストを取り入れたセキュリティ強化 ～

かもめエンジニアリング株式会社
潮村　剛

Keygateway

2023.01.26

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！

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

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。
最近のヒットは「プロジェクト・ヘイル・メアリー」

画像引用：
オライリー・ジャパン

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

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

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

※　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

ゼロトラストモデル
と
ZTNA

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

近年注目が高まった背景

- コロナ禍を通じ、リモートワークが定着（働き方の変化）
- 業務システム利用者の拡大（サプライチェーンの拡大）
- 業務システムのリフト・シフト化（クラウド環境・SaaS利用の促進）
- ランサムウェア攻撃・サプライチェーン攻撃の激化

「境界防御型」セキュリティの課題がクローズアップ

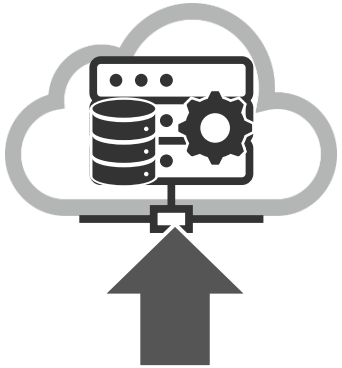
Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

業務システムの変化

ほぼ社内やデータセンターのみ

クラウドへの設置（IaaSへリフト）
クラウドサービス（SaaSへシフト）
の利用拡大



リフト

シフト

・しかし、すべてをシフトまで持って行けるわけではない
・一部の**自社システム**は残さざるを得ない
・**オンプレ**に残るものだってある

業務システムは、あちこちに分散される

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

※ 記載の他社サービス名およびロゴは、各社の商標または登録商標です。

KAMOME Engineering

利用者の利用環境の拡大

ほぼ社内のみ

→ **社内とリモートアクセスの併用へ拡大**

・リモートアクセスがレアケースではなくなった。
・**社内社外を問わず、どこからでも**接続される…

「安全な場所」によって情報資産を守ることは、ほぼ不可能

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

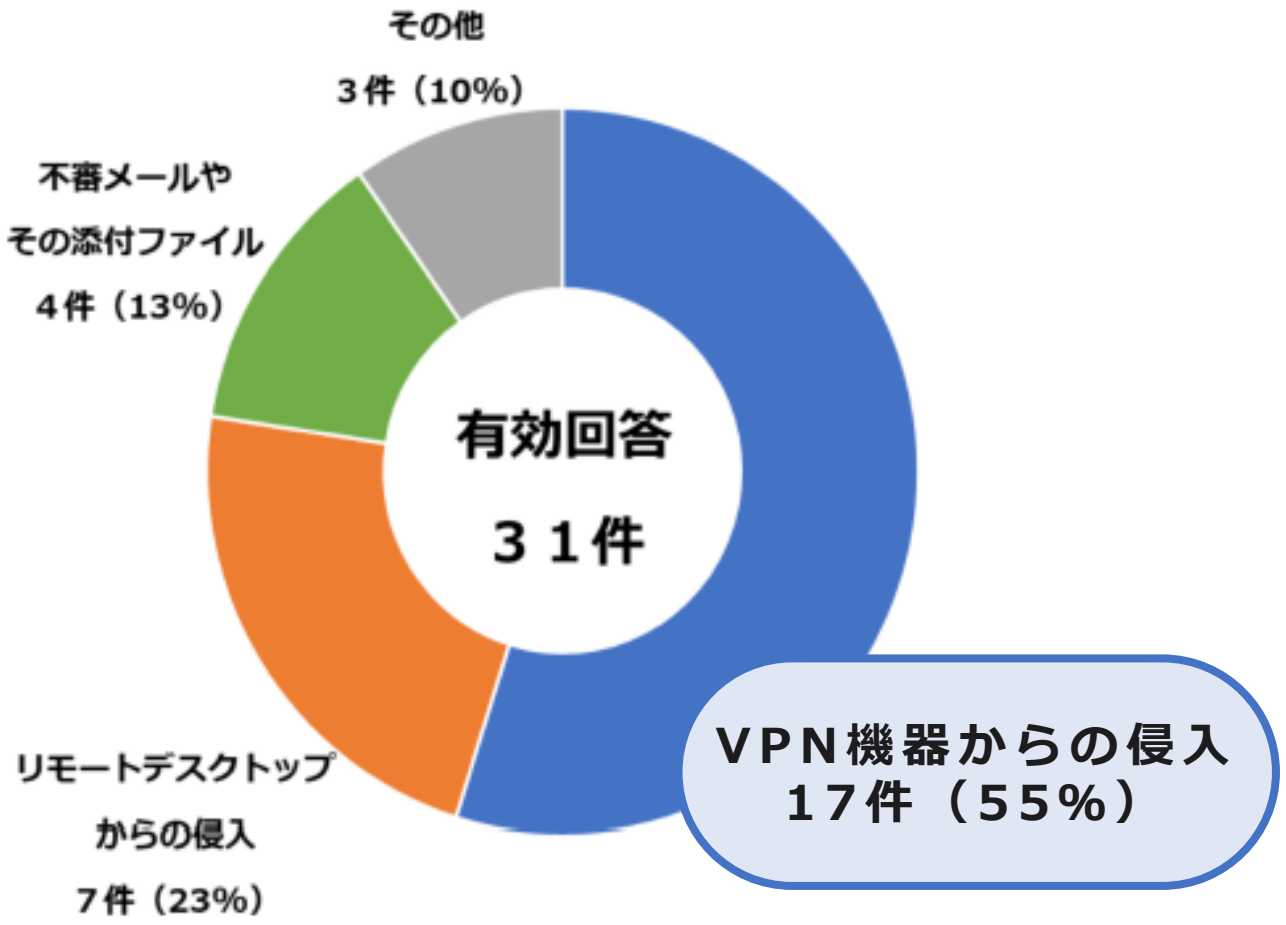
KAMOME Engineering

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

【図表７：感染経路】



Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

VPN経由による被害事例

引用：https://www.nikkei.com/article/DGXZQOFD0119F0R00C22A3000000/?unlock=1

日本経済新聞　お申込み

トップ　朝刊・夕刊　LIVE　Myニュース

トヨタ工場停止、部品会社がランサムウエア被害と発表

中部　＋フォローする

引用：https://toyokeizai.net/articles/-/538803

東洋経済 TOYOKEIZAI ONLINE　▶お知らせ　【無料エリア拡大中】シキホー！Mineで納得就活

3月20日（日）　週刊東洋経済プラス | 四季報オンライン |

トップ　新型コロナ　ビジネス　政治・経済　マーケット　キャリア・教育　ライフ

自動車最前線 ▶ 経営

デンソー、今度はドイツでサイバー攻撃の受難

2021年末に受けた不正アクセスとの関連は不明

2022/03/14

ツイート　一覧　B! 0　印刷

メニュー　キーワードで検索　日経XTECH

IT　電機　自動車

トヨタ取引先の小島プレス工業がマルウエア感染公表、ランサムウエア攻撃の可能性大

島津 忠承　日経クロステック

2022.03.01

引用：https://xtech.nikkei.com/atcl/nxt/news/18/12332/

メディア　ITmedia NEWS

カテゴリー：速報　連載　業界動向　セキュリティ　クリエイター　社会とIT

特集：AI・ロボット　クラウド　SaaSビジネス　SaaSの選び方　量子コンピュータ

ITmedia NEWS > セキュリティ > 大阪・病院サイバー攻撃の侵入口業者、徳島の被害病...

SECURITY HOT TOPICS

大阪・病院サイバー攻撃の侵入口業者、徳島の被害病院と同一のVPN利用

2022年11月08日 09時00分 公開

印刷　49

PR モジュラモノリス | マイクロサービスの自律性との両立

PR デジタルサイネージで商品の売り上げが3倍以上に!?

身代金要求型ウイルス「ランサムウエア」

バー攻撃でシステム障害が続く大阪急性期・

（大阪市住吉区）は11月7日、完全復旧を

引用：https://www.itmedia.co.jp/news/articles/2211/08/news073.html

メニュー　キーワードで検索　日経XTECH

IT　電機　自動車

piyokangoの週刊システムトラブル　＋連載をフォロー

ランサムウエア被害の日本盛が調査報告、脆弱性があるVPN装置からの不正侵入だった

piyokango　セキュリティーリサーチャー

2022.11.01

引用：https://xtech.nikkei.com/atcl/nxt/column/18/00598/070100188/

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

VPN経由による被害事例（米コロニアル・パイプライン社）

日本経済新聞

トップ　朝刊・夕刊　LIVE

米最大の石油パイプライン停止　サイバー攻撃で

北米　＋ フォローする

2021年5月8日 23:17 (2021年5月9日 6:05更新)

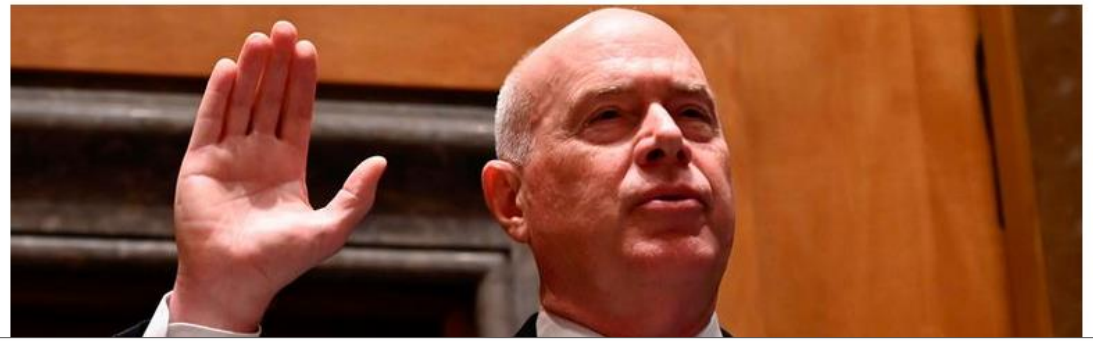
引用：https://www.nikkei.com/article/DGXZQOGN084D30Y1A500C2000000/

REUTERS　マーケット　外為　株式市場　ニュース　ビデオ　その他

テクノロジー　2021年6月9日 / 7:32 午前 / 9ヶ月前更新

コロニアル、ハッカー集団に1段階認証破られ侵入許す＝ＣＥＯ

ロイター編集　1 分で読む



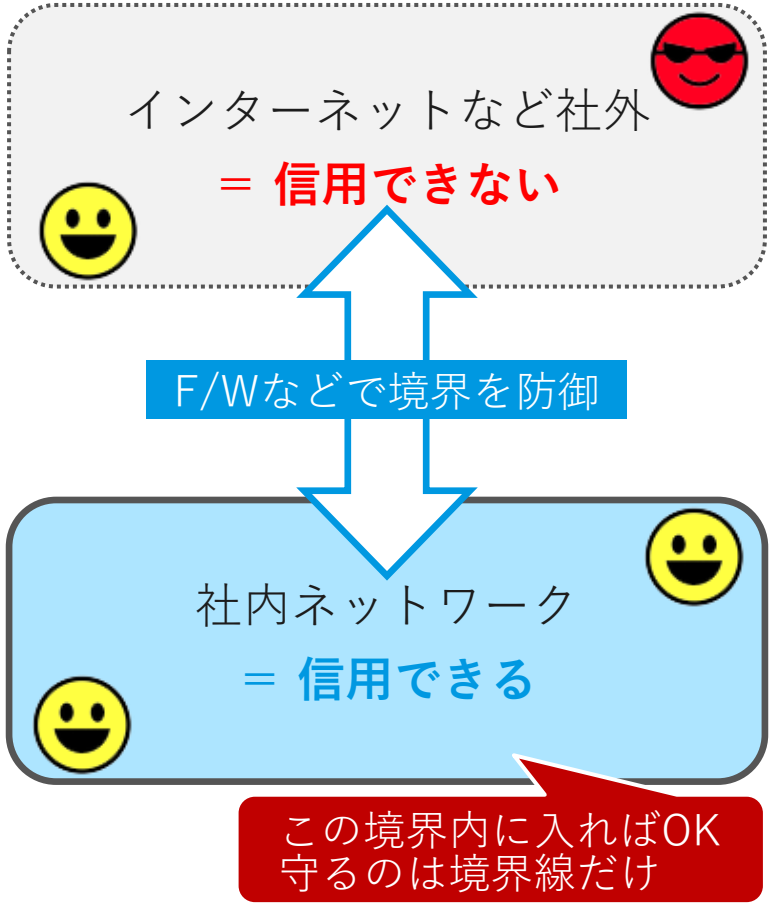
引用：https://jp.reuters.com/article/cyber-usa-pipelines-idJPKCN2DK2P3

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

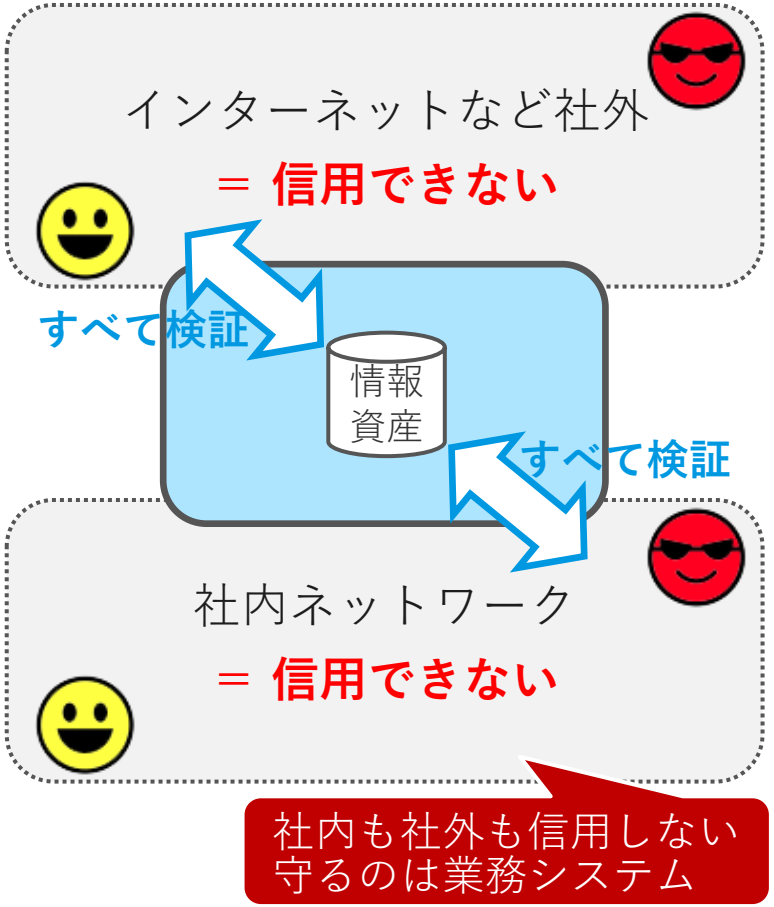
「境界防御モデル」の限界 ➡ 新しい考え方へ進化

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



Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

ZTNAの役割

ゼロトラストネットワークの7原則

❶ すべてのデータソースと処理サービスを「リソース」と考える

❷ ネットワークの場所に関係なくすべての通信が保護される

❸ リソースへのアクセスはセッションごとに許可される

❹ リソースへのアクセスは動的なポリシーによって決定される

❺ 組織に関連する機器は、可能な限り安全を保てるよう継続的に監視する

❻ リソースの認証と認可は動的に実施され、許可する前に厳密に適用される

❼ ネットワークインフラとコミュニケーションの現状をできる限り収集する

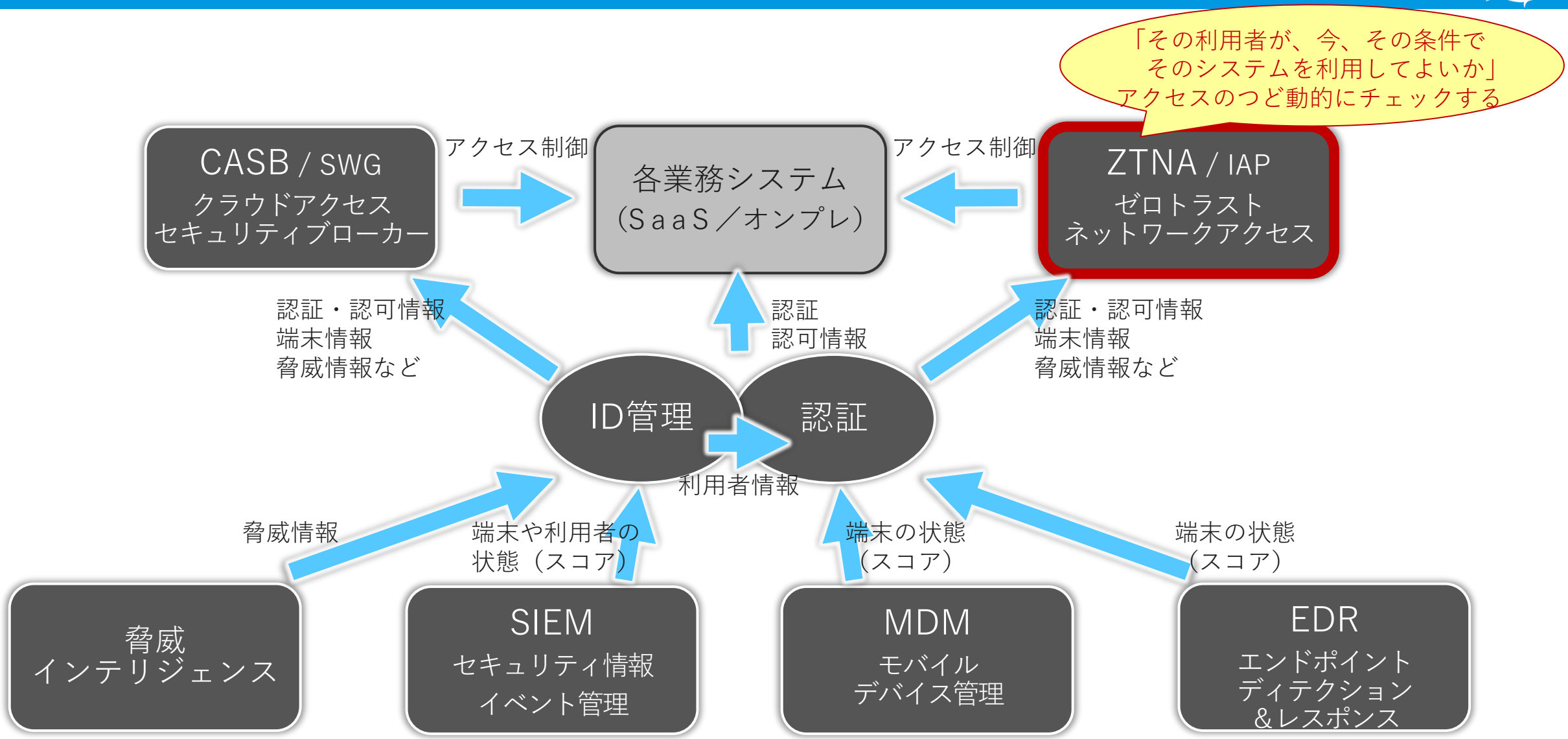
米国国立標準技術研究所（NIST） 2020年8月公開
「Special Publication（SP）800-207 ゼロトラスト・アーキテクチャ」より

… 特にZTNAの役割に関する部分

基本は
「デバイスがリソースにアクセスする際に、そのつど利用可否を判定する」こと

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

ゼロトラストモデル と ZTNA



※ 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。
※ 本セッションでは、一般的に「IAP型ZTNA」と呼ばれるものをご説明します。

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

一般的なVPNとの比較

	VPN	ZTNA / IAP
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	△ • VPN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

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

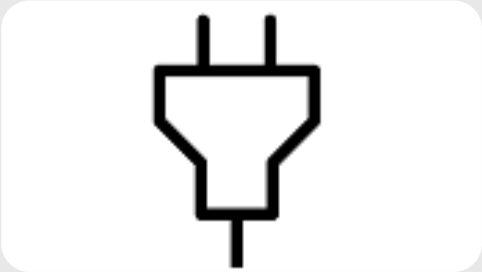
構成要素（IAP型の場合）

エッジ ／ IAP（Identity Aware Proxy）

- 利用者⇔アプリケーション（接続先システム）の通信を仲介し、アクセスをコントロールする
- パブリックな場所（≒Web上）に置かれる

IdP（Identify Provider） ／ IAM（Identity and Access Management）

- 利用者が誰であるかの認証を行う
- IDaaSを利用する場合が多い
  （オンプレミスSSO基盤でも可）



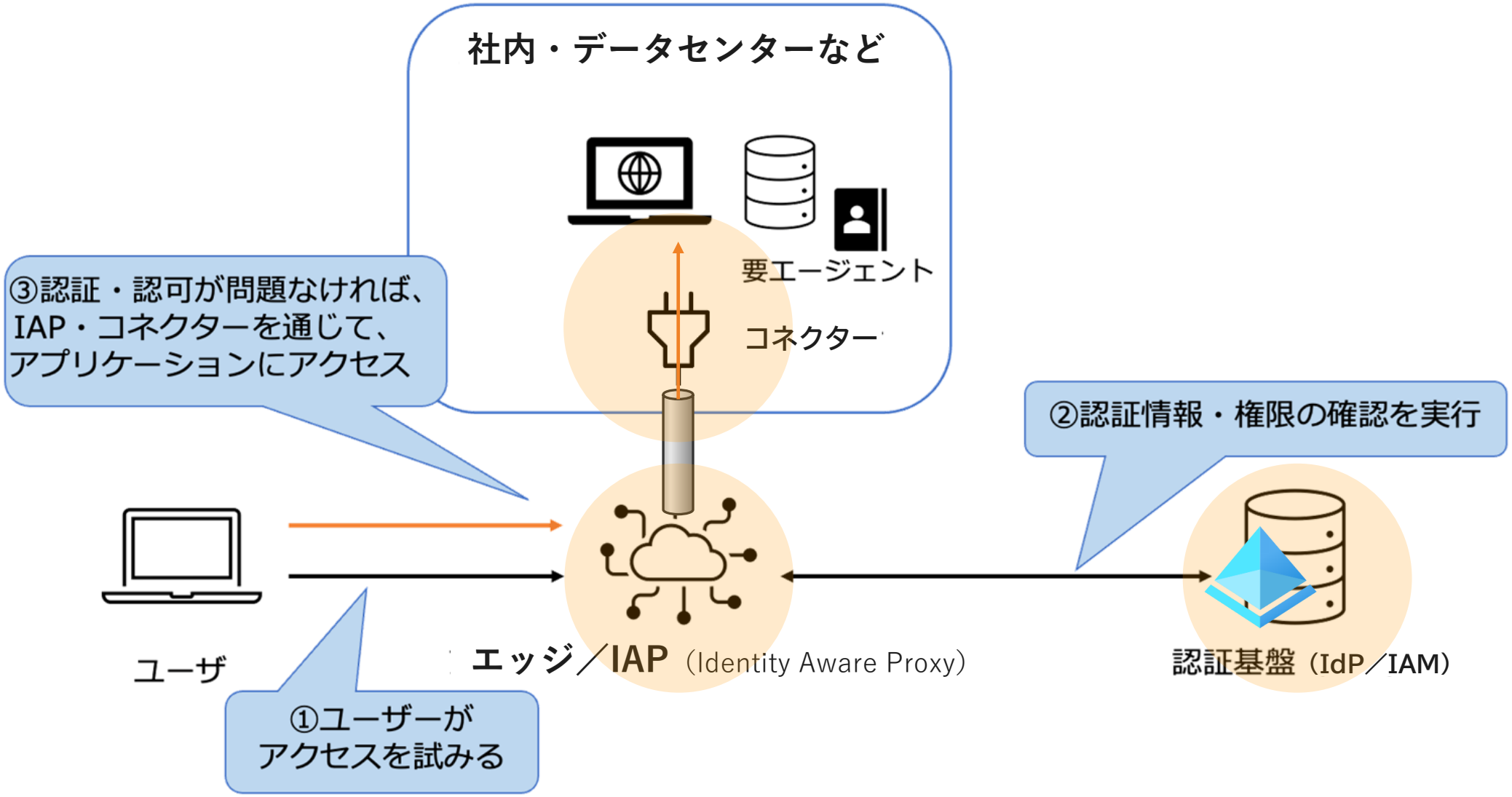
コネクター

- アプリケーション（接続先システム）がオンプレミスにある場合に必要
- IAPとアプリケーションの間に置かれる
  （データセンター内や社内LAN環境のアプリを利用したい場合は、アプリと直接通信できる場所）
- IAP⇔コネクター間の通信は暗号化される

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

構成要素（IAP型の場合）



Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

※　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）

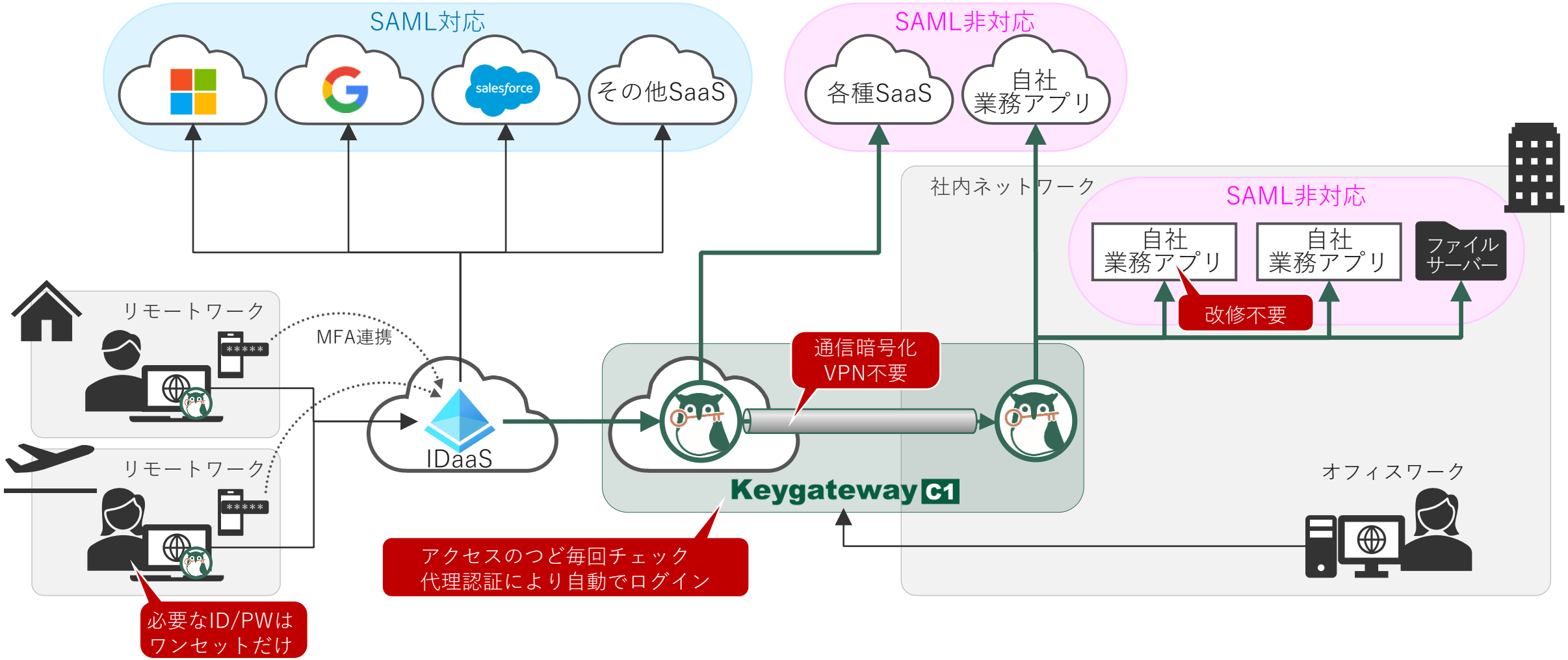
KAMOME Engineering

ゼロトラストを取り入れてセキュリティを強化する
クラウド接続サービス

Keygateway C1

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

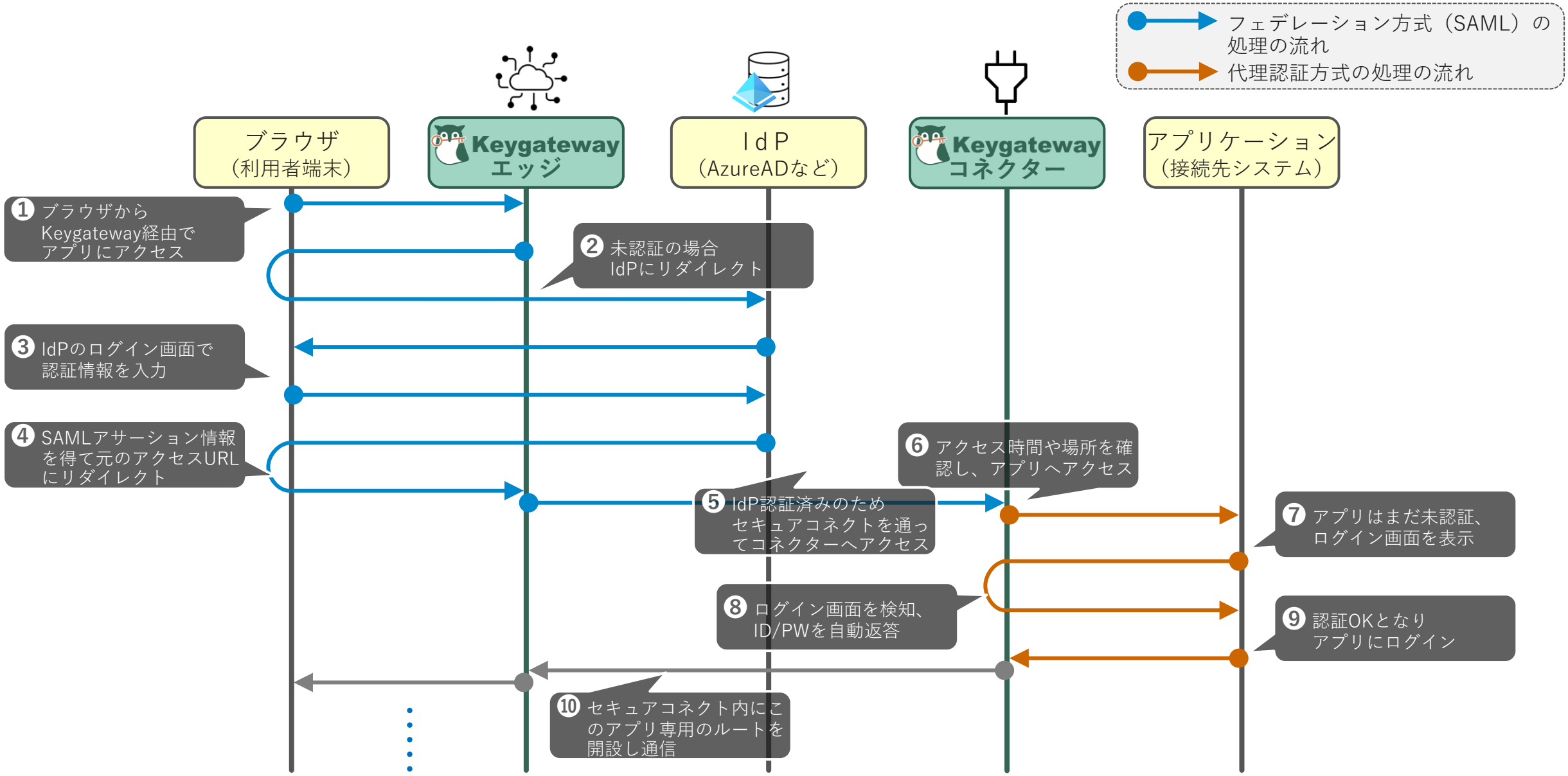
IdP（SSOシステム）と連携し、さらに安全なアクセス経路を提供



Copyright©2022 KAMOME Engineering, Inc. All rights reserved.
※ 記載の他社サービス名およびロゴは、各社の商標または登録商標です。 ※ 概念図であり、実際の通信の流れとは異なります

Keygateway C1 シーケンス図

KAMOME Engineering



Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

KAMOME Engineering

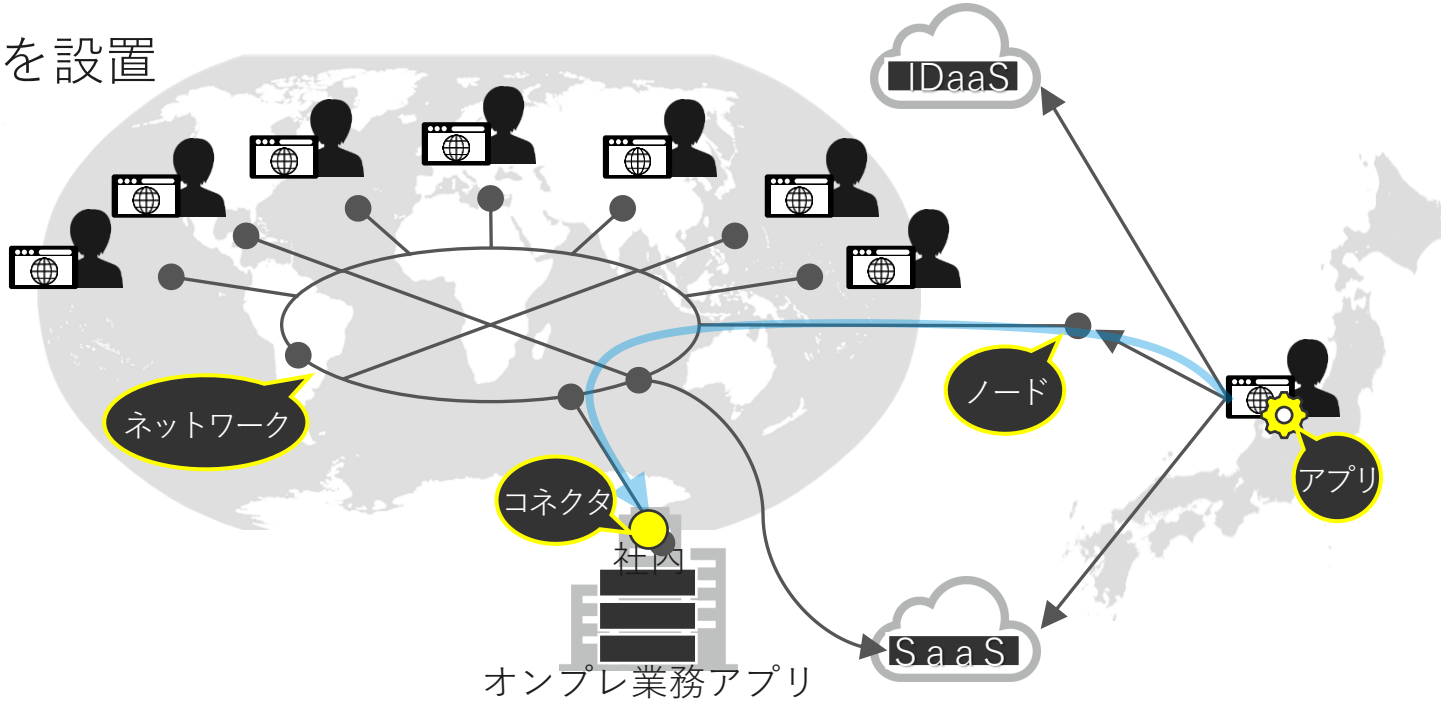
多くは、世界中に拠点を持つグローバル企業向き

■ 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

■ 大手ベンダーより提供多数

BeyondCorp
BeyondCorp Enterprise
zscaler
netskope
PRISMA ACCESS BY PALO ALTO NETWORKS
Azure Active Directory



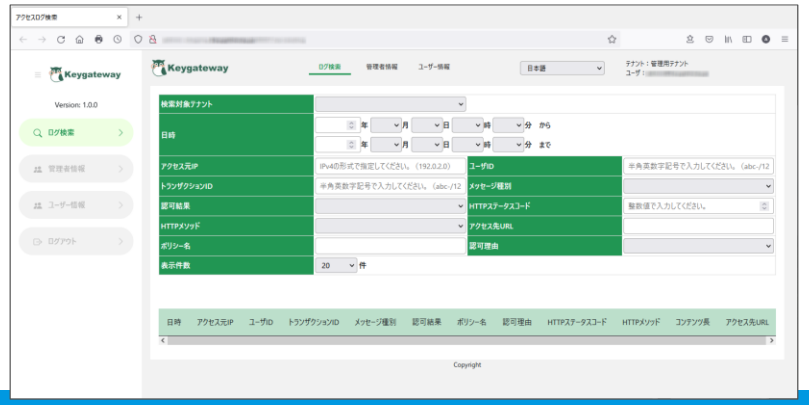
Copyright©2022 KAMOME Engineering, Inc. All rights reserved.
※ 記載の他社サービス名およびロゴは、各社の商標または登録商標です。

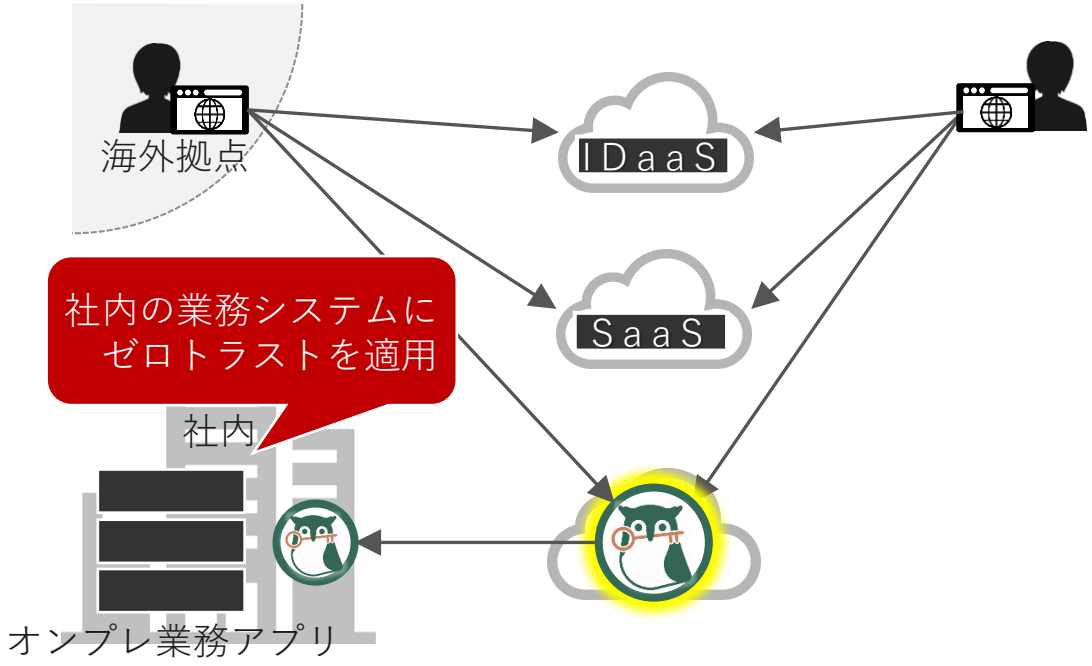
KAMOME Engineering

ゼロトラスト接続サービス
Keygateway C1 ➡ 国内メインの企業・団体向き

■ 日本企業に必要な機能をシンプルに実現したZTNA

- 国内のノード（エッジ）に接続、社内までアクセス
- ユーザ認証はIDaaSを利用
- 日本企業が必要とする機能を装備（さらに順次増強中）
- 端末用ツール原則不要（※）、社内にコネクター設置
  ※ 一部機能利用時のみ必要
- 日本語管理画面





Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

グローバルベンダーによるZTNAサービスとの比較（当社調査）

KAMOME Engineering

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 Keygateway C1
主な対象	海外拠点が多い グローバル企業	海外拠点が多い 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	**100ID** ～規模の、 国内を主な拠点とする組織
コスト	● 初期費用は別途 ● 利用費用（年間） 1IDあたり 1万円以上	● 初期費用は別途 ● 利用費用（年間） 1IDあたり 2万円以上	● 初期費用は別途 ● 利用費用は対象プランによる ※プランによりSLA設定無し ※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	● 初期費用は別途 ● 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） ● サポートは国内で提供
機能等	● 世界各国にノード設置 ● ノードから社内NWまでセキュアな通信 ● 端末アプリ／Webブラウザ（利用範囲限定） ● 認証の自動化機能無し ● 認証は独自基盤かIDaaS（海外IDaaS） ● 社内からのアクセスは別サービスを組合せ	● 世界各国にノード設置 ● ノードから社内NWまでセキュアな通信 ● 端末アプリ ● 認証の自動化機能予定 ● 認証は独自基盤かIDaaS（海外IDaaS） ● 社内からのアクセスは範囲外	● 自社設備として導入・運用が必要 ● 認証の自動化機能あり ● 社内システムの認証にADを利用 ● 構築・運用を担当可能なSI事業者が少ない ● 社内からのアクセスは利用不可	● 認証の自動化機能あり ● エッジ-社内NWでセキュアな通信 ● 認証はIDaaS （国内で利用可能な全てのIDaaSに対応） ● 端末用アプリ または Webブラウザ（利用範囲限定） **● 社内からのアクセスにも利用可能** **● ファイルサーバへ対応（2022春）** **● Web Proxy経由アクセス対応**

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

部分導入 ➡ 対象の拡大　も容易です

部署・事業所ごとに	属性・雇用形態ごとに	役職ごとに	勤務形態ごとに
例 「機密性の高い情報を扱う部門から先に」	例 「関係会社など外部スタッフのアクセス管理強化を」	例 「権限の大きな役職者を優先したい」	例 「まずはリモートワーカーを対象に」

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

まとめ

- ZTNAは、ゼロトラストモデルの中核となる
  「アクセスのつど、利用の可否を動的に判断する」
  という役割を担います。
- ZTNAの利用により、
  「VPNの代替」かつ「VPNより強固」な通信手段が得られます。
- かもめエンジニアリングの KeygatewayC1 は、
  AzureADなどのIdPと連携してZTNAを実現する
  日本国内企業向けの接続サービスです。

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

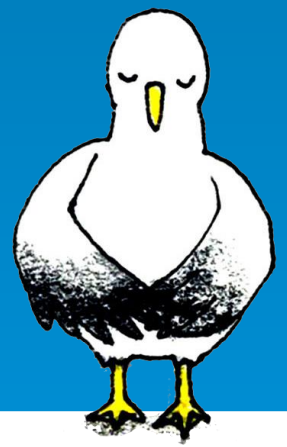
皆さまへのお願い

- **アンケートへのご回答を、ぜひお願いいたします。**
- 本日以降、主催者（かもめエンジニアリング）よりご連絡を差し上げます。
  連絡手段等についてご希望がおありの方は、その旨ご回答ください。
  - 「メールのみOK」「電話は10～12時が都合よい」　など
- さらに詳しいご説明や課題のヒアリングなどのため、
  ぜひWebミーティングをご要望ください。
  - スタイルズ社とのミーティングご要望についても、いったん当社でお預かりいたします。
- 具体的検討がおありの場合は、
  理由や状況について、お差し支えない範囲で具体的にご教示ください。

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！

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.

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！

Copyright©2022 KAMOME Engineering, Inc. All rights reserved.