小規模な組織の「脱VPN」はどう実現すべきか？

過剰な機能を排し、KeygatewayC1でシンプル＆低コストに始める
安全なリモートアクセス

2025.08.19

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 … 「惑星カレスの魔女」ジェイムズ・H・シュミッツ著（創元SF文庫）

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）

- OSSをベースに独自の機能をプラス、B2CからB2Bまでカバーする SSO認証サーバ「**KAMOME SSO**」
- SAMLやOIDC非対応の業務Webアプリを改変不要でSSO環境に対応、SAML/OIDCアダプター「**Keygateway T1**」
- VPNに代わるゼロトラスト接続サービス「**Keygateway C1**」

特許取得

- 官公庁、金融機関、医療機関、通信事業者、ECサイト、エネルギー大手、製造大手、各種団体、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）
- Microsoft 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

主要実績

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 ➡ 20,000社へ拡張
- 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
- ゼロトラスト ID管理サービス
  - 総合電機メーカー　OEM提供
- OEM提供先

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

KAMOME Engineering

ランサムウェアによる被害の実態

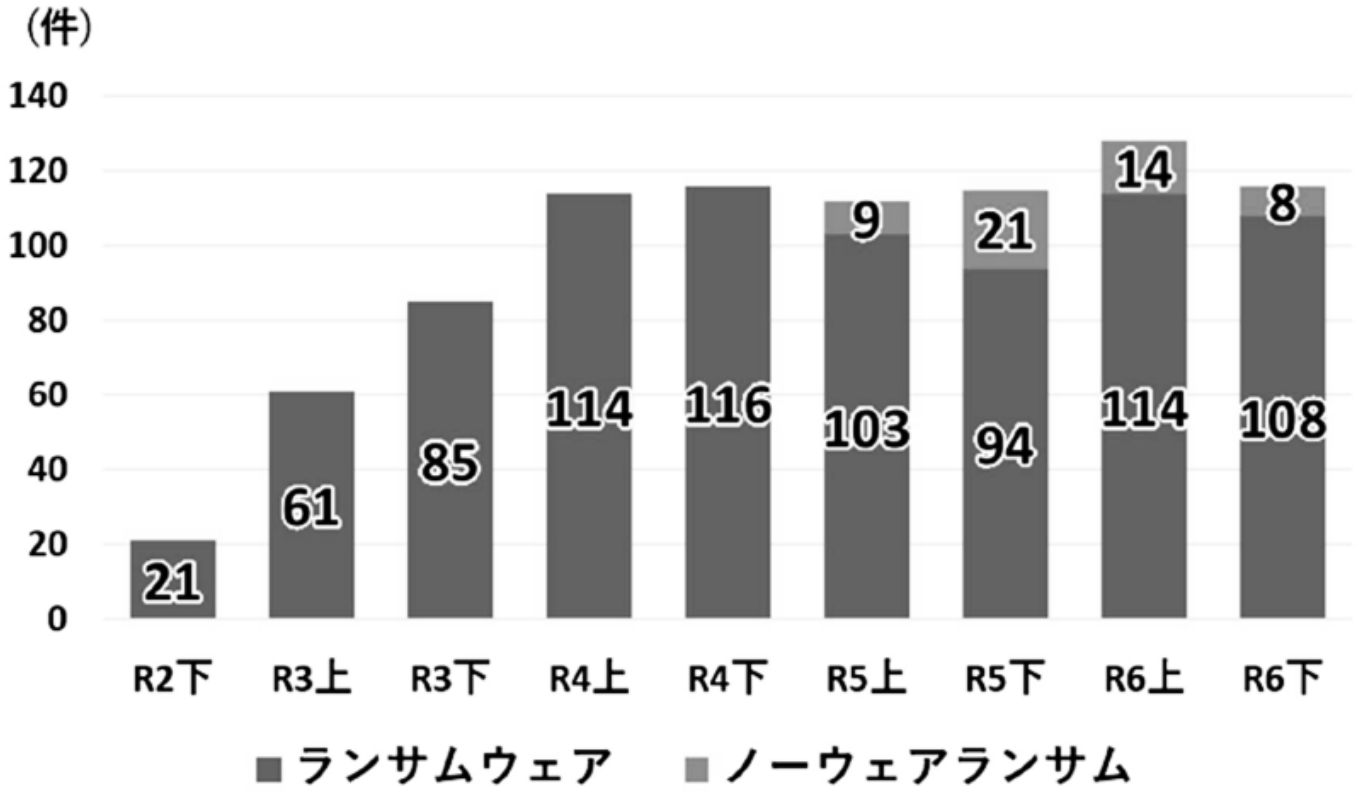
感染の8割以上が「リモートアクセス経由」

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/R6/R06_cyber_jousei.pdf

■　企業・団体等における被害の報告件数の推移



※ 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。

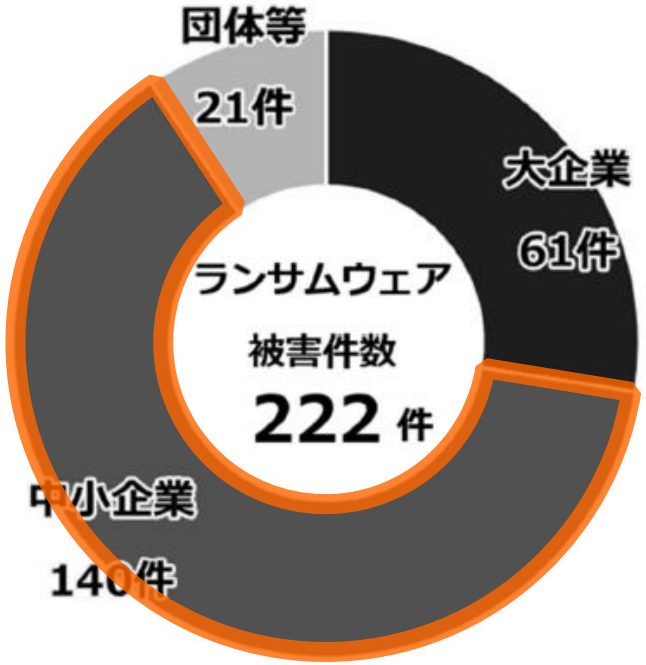
- 対策の必要性が繰り返し指摘されているにもかかわらず**被害報告数は高止まり**状態
- 報告義務はないため、未報告の被害については不明

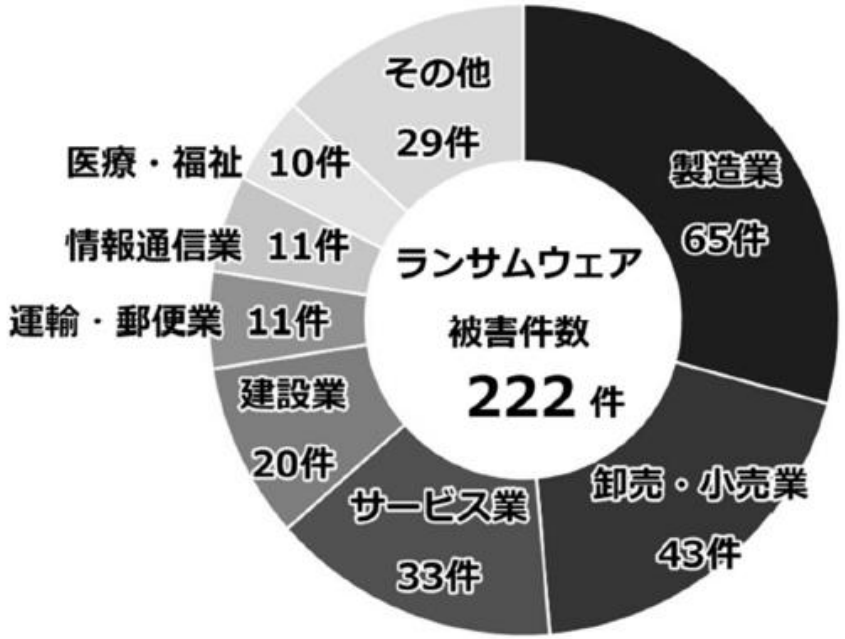
  特に中小企業の被害は報告されないケースも多いと考えられ、実際にはより多くの被害が発生しているはず

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/R6/R06_cyber_jousei.pdf

■ 被害企業・団体等の規模別／業種別報告件数





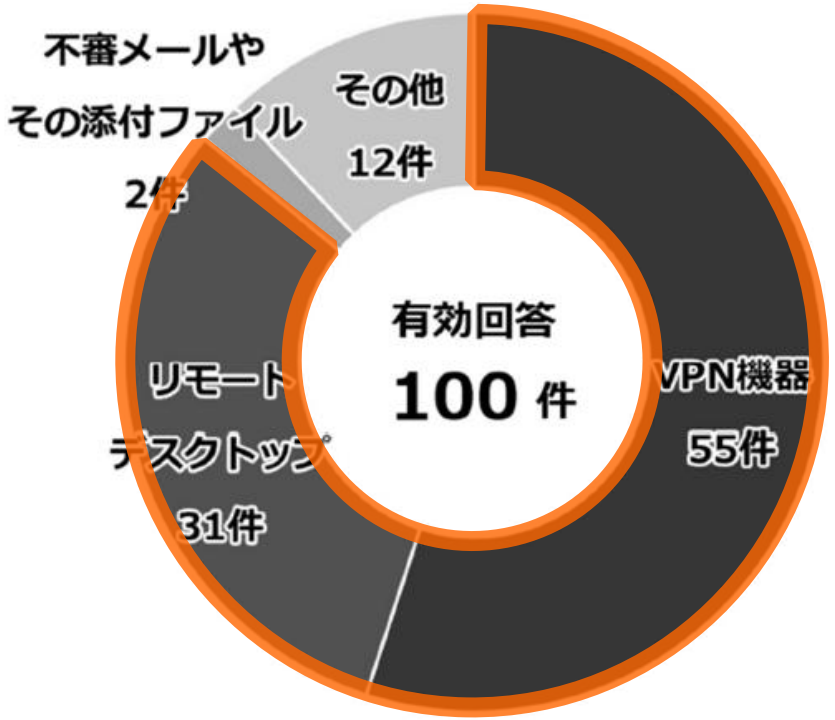
- **中小企業**の比率がさらに増加
  - 前期　102件　52%
  - ⇓
  - 今期　140件　63%
  - 身代金の獲得が、比較的容易 かつ 短期間で可能と判断されている模様
- **あらゆる業種**がターゲットに

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/R6/R06_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

前期	21件	18%
⇓		
今期	31件	31%

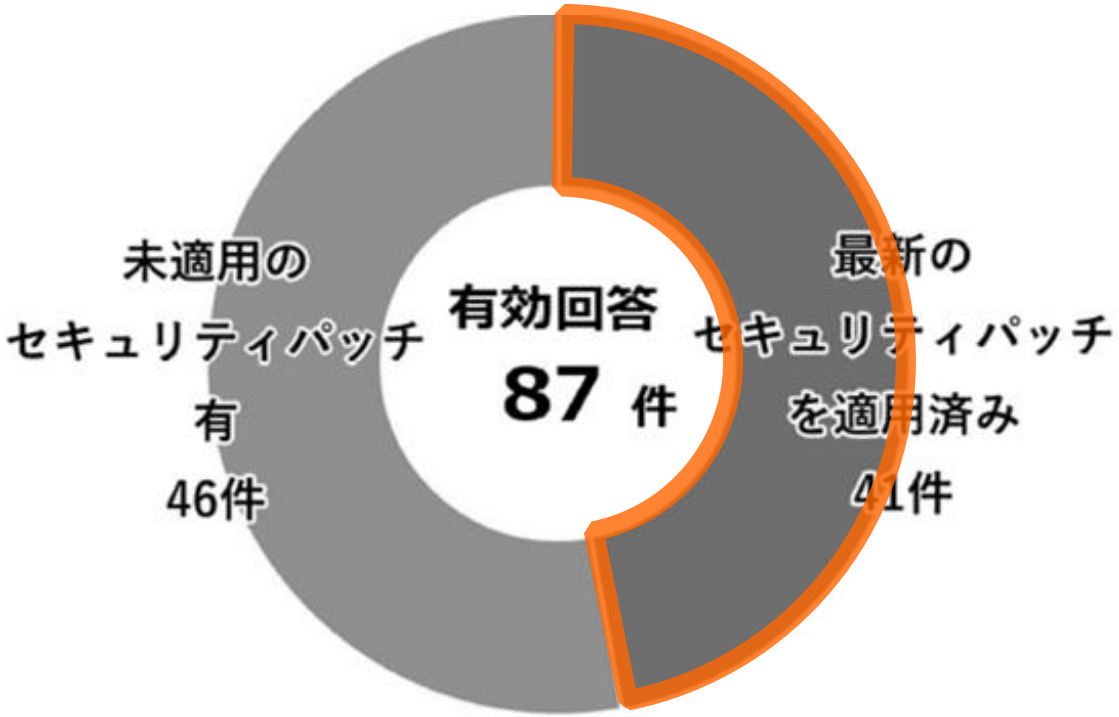
- VPN機器経由を含め
86件 86％が
リモートアクセス経路から
侵入

KAMOME Engineering

「対策していれば大丈夫」？

警察庁『令和６年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/R6/R06_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**



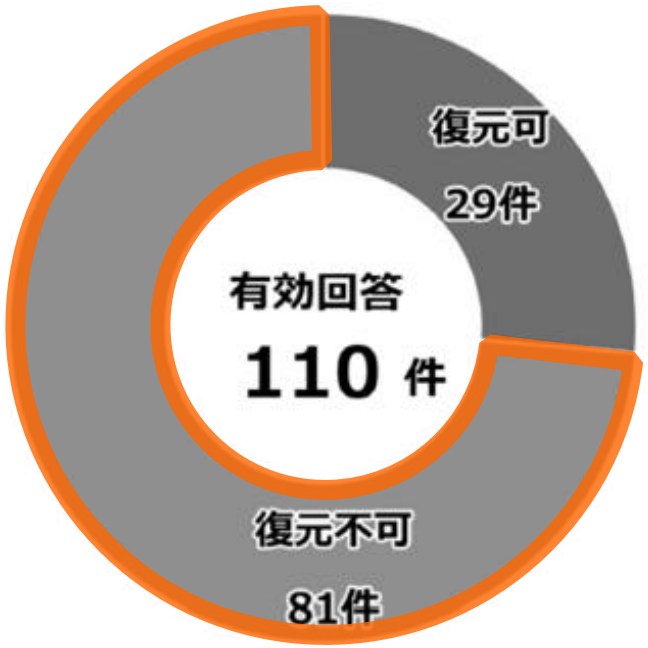
- 半数近くが、**最新のセキュリティパッチを適用**していたにもかかわらず被害を受けた
- パッチ適用前に侵入されるケースも多い

KAMOME Engineering

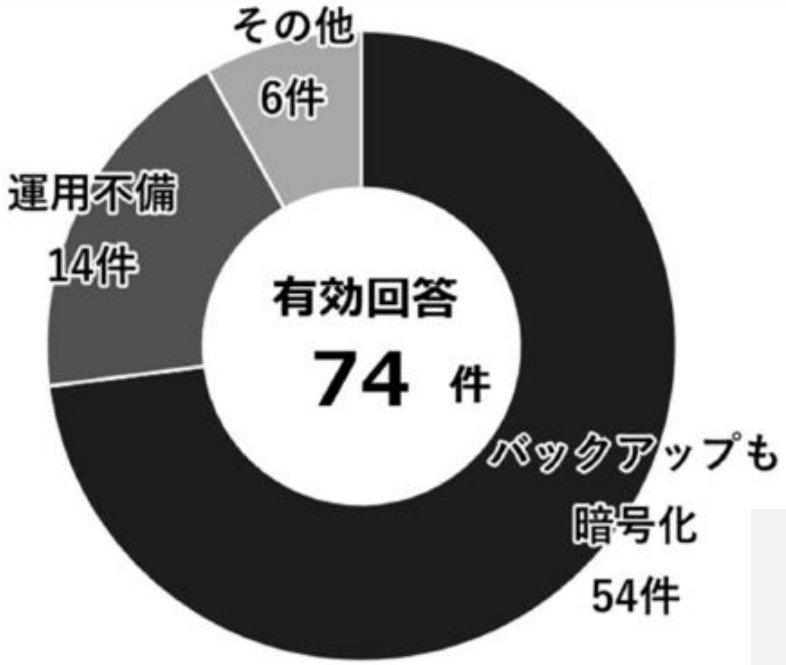
「対策していれば大丈夫」？

警察庁『令和６年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/R6/R06_cyber_jousei.pdf

■ バックアップからの復元結果



■ バックアップから復元できなかった理由



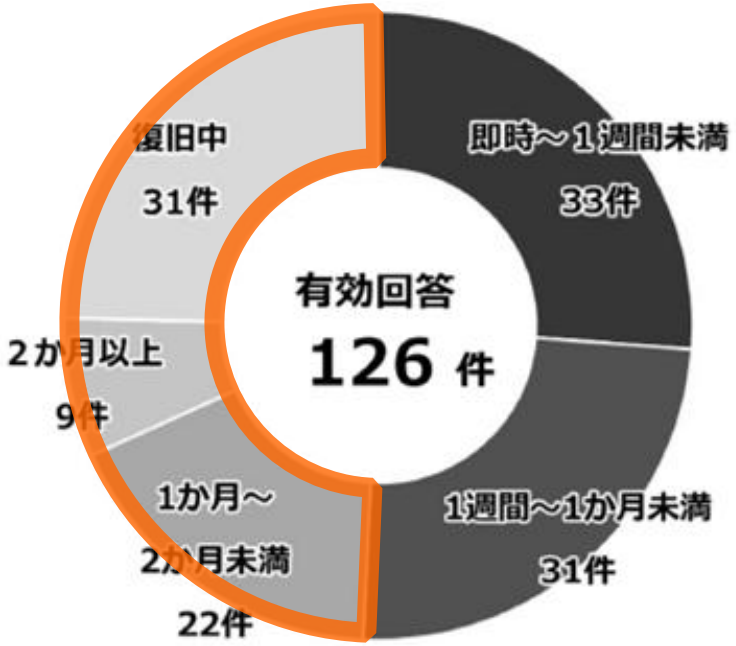
- 81件 74% が、
  バックアップから復元不可
- 侵入者は、
  バックアップやログも
  攻撃対象とし、復元を妨害する

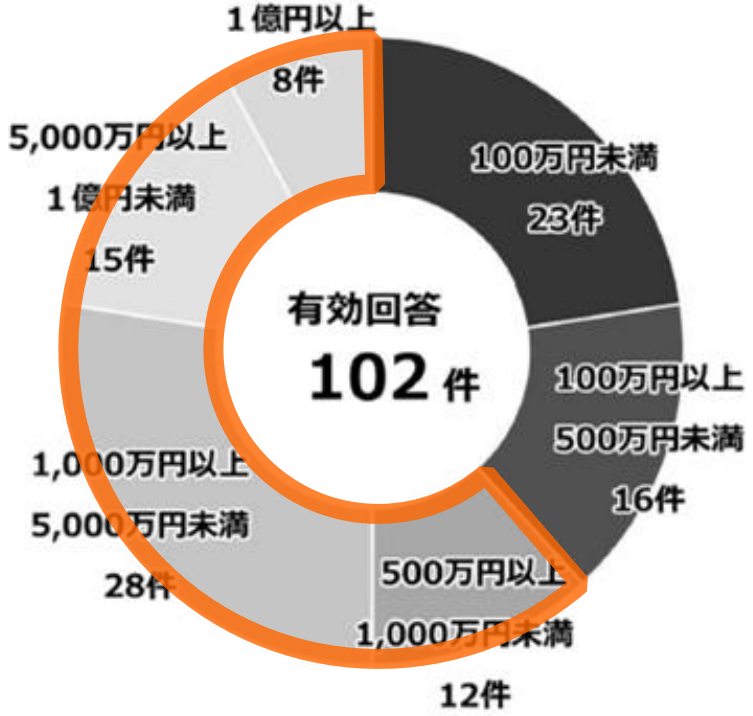
KAMOME Engineering

事業への影響は大きい

警察庁『令和６年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/R6/R06_cyber_jousei.pdf

■ 復旧等に費やした期間／調査費用の総額





- 62件 49% が、復旧等に
  「1ヵ月以上（または復旧中）」
- 63件 62% が、
  「500万円以上」の費用を
  要している
  ※ 調査・復旧部分のみ

KAMOME Engineering

システム自体への損害だけでなく…

- 取引先／クレーム対応
- 対応スタッフの疲弊
- 逸失利益
- 損害賠償責任
- 行政への対応

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（ゼロトラストネットワークアクセス）

「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

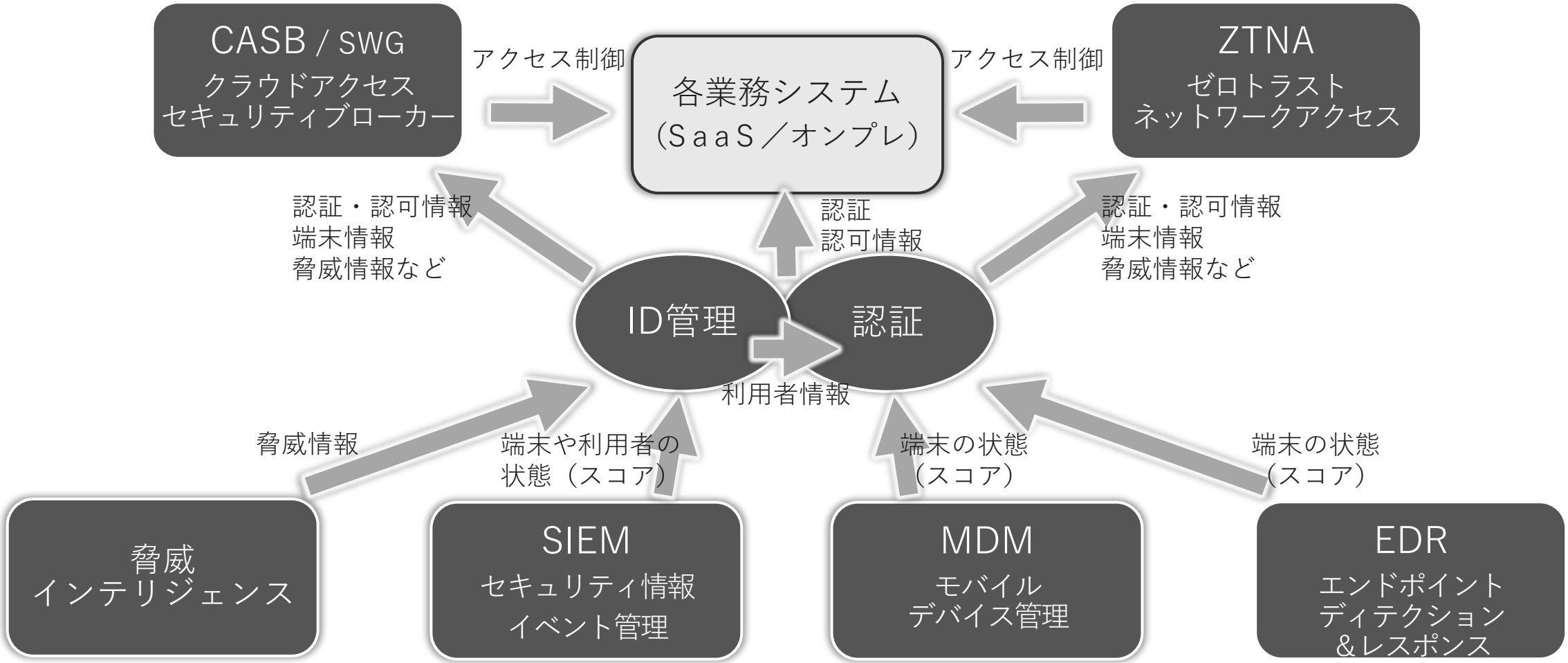
アクセス権の提供は
常に最小限度に限定

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

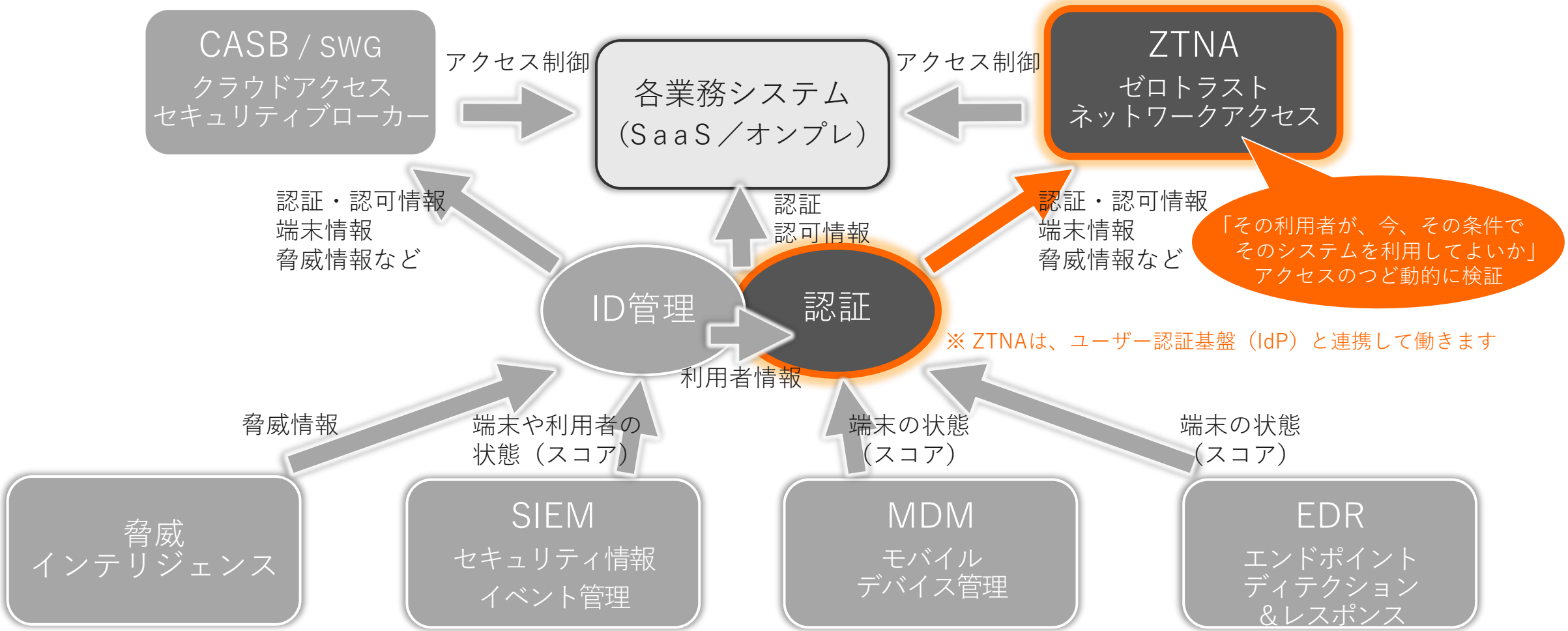
ゼロトラストモデルの主な構成



※　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

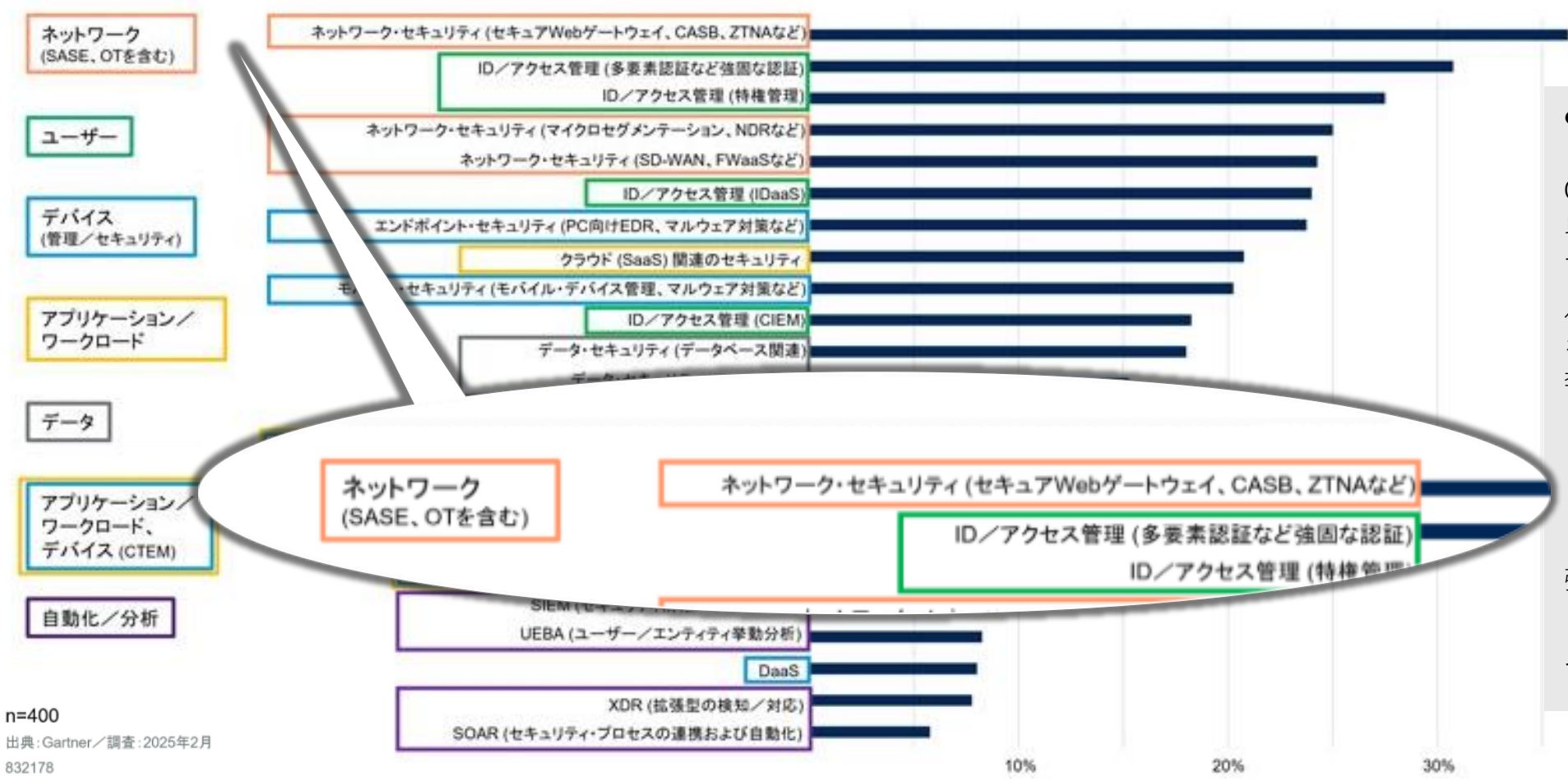
VPN等の代替となり、より強固なセキュリティのZTNA

	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 ➡ ゼロトラストネットワーク の移行が加速

ガートナージャパン発表　ゼロトラストの最新トレンド より（2025年5月）（一部画像加工）
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20250508-zero-trust



- ガートナージャパン社プレスリリースより引用

Gartnerは、2025年2月に国内の従業員500人以上の組織を対象に実施したユーザー調査において、
「『ゼロトラスト』として見直し／強化したセキュリティ領域」
を尋ねました。その結果、上位3つに挙げられた対策は、

「ネットワーク・セキュリティ（セキュアWebゲートウェイ、CASB、ZTNAなど）」、

「ID／アクセス管理 (多要素認証など強固な認証)」、

「ID／アクセス管理 (特権管理)」

でした。

Gartner

ZTNAを簡単に利用するには、どうすれば…？

海外グローバルベンダーが提供している
ZTNAサービスもありますが…

でも、あれほどハイスペックなものを求めている
わけじゃないんですよね

ランニングコストも高額だし、
初期構築費用がかさむと、なおハードル高くて…

必要な機能に絞って小さく始める「脱VPN」の需要が増えています

ZTNAを簡単に利用するには、どうすれば…？

数万ユーザーの大規模向けにも採用されていますが、
ここでは、**300ユーザーまでの中小規模向け** に特化してご紹介します。

KAMOME Engineering

中小規模「脱VPN」のユースケース

ゼロトラスト接続サービス
Keygateway C1

KAMOME Engineering

よくあるお問い合わせの概要

リモートアクセスにはSSL-VPNを利用中だが、
セキュリティ上の課題があるため安全性の高い代替手段を探している

IDaaS（IdP）は導入済み／導入予定
（Entra ID 、HENNGE One 、Onelogin 、Okta 、GMOトラスト・ログイン 等）

社内閉域網内には、オンプレ業務システムやファイルサーバーがあるが、
これらがSSOできないことも課題

いくつか問い合わせてみたが、
我が社には規模とコストインパクトが大きすぎる

KAMOME Engineering

当社からのご提案

Keygateway C1

リモートアクセスにはSSL-VPNを利用中だが、
セキュリティ上の課題があるため安全性の高い代替手段を探している

IDaaS（IdP）は導入済み／導入予定
（Entra ID 、HENNGE One 、Onelogin 、Okta 、GMOトラスト・ログイン 等）

社内閉域網内には、オンプレ業務システムやファイルサーバーがあるが、
これらがSSOできないことも課題

いくつか問い合わせてみたが、
我が社には規模とコストインパクトが大きすぎる

→ IDaaSと連携する
ZTNAソリューションの導入

→ SSO環境への適用

→ 小規模でも現実的なコスト体系

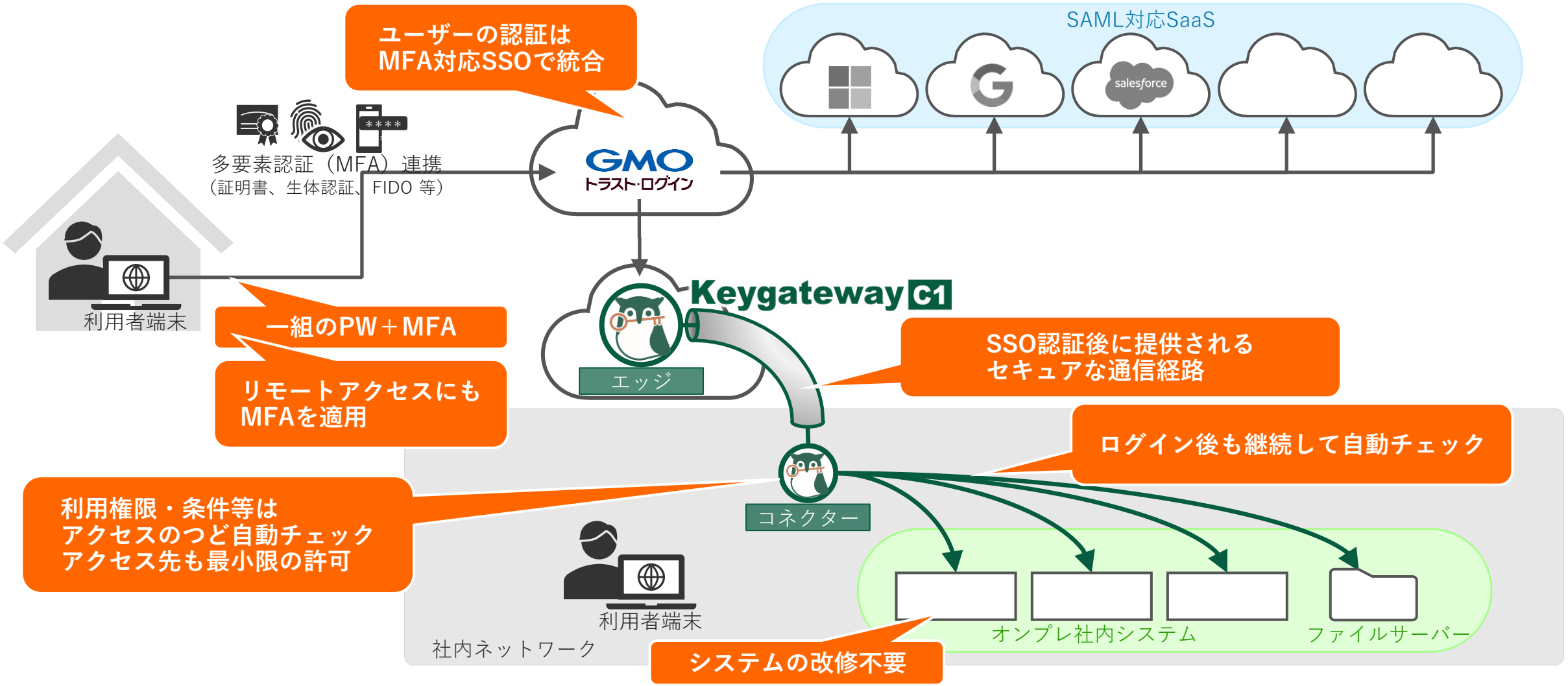
KAMOME Engineering

代表的な要件例

従業員数	約　200名		
IDaaS	導入済み （GMOトラスト・ログイン）		
接続先システム	IDaaSでSSO	・SaaS（SAML対応）	5件
	IDaaSでSSO困難	・社内オンプレシステム（Webアプリ）	3件
		・ファイルサーバー	1件
多要素認証	あり（証明書、ワンタイムパスワード 等）		

KAMOME Engineering

Keygateway C1 ご提案例の構成概要



新たに中小規模向けプランをご用意しました

KAMOME Engineering

Keygateway C1 「SMBプラン（仮称）」

従業員規模	300名以下	※ 従業員総数が多い組織で 「KeygatewayC1の利用者が 従業員の一部 かつ 300名以下」 となる場合は別途ご相談ください
接続先システム数	計 5件以下	※ Webアプリ、クラサバアプリ、ファイルサーバー 等 ※ 原則として当社検証済みのものに限ります （未検証のものについては別途ご相談ください）
連携IDaaS	当社にて接続検証済みのもの　1件	
初回契約期間	3年間	※ 4年目以降は、同条件で1年単位の更新が可能です
費用	初期費用	150万円
	サブスクリプション　100 ID まで	15万円 ／月
	サブスクリプション　200 ID まで	20万円 ／月
	サブスクリプション　300 ID まで	25万円 ／月

連携システム検証状況

接続先システム（オンプレミスのみ抽出）

No.	名称
01	ADManager Plus Web UI
02	ADSelfService Plus Web UI
03	Alfresco
04	Apace Guacamole
05	COMPANY Talent Management
06	DataDelivery
07	desknet's NEO V6.0 R1.1
08	Dr.SUM
09	ExchangeUSE バージョン:11.2.30
10	GRANDIT
11	Jenkins
12	LiveU
13	Mattermost

No.	名称
14	Monitorix
15	PHPQUERY2
16	Redmine
17	Report Viewer II
18	SAP BusinessObjects BI4.3
19	STRAMMIC
20	TimePro-VG
21	TimePro-XG
22	WordPress
23	X-point v2.7
24	Zabbix
25	サイボウズ
26	プリザンター

連携IdP（IDaaSなど）

※ SAML、OpenID Connect、OAuth 対応IdPは基本的に可

No.	名称
01	AWS Single Sign-on
02	Microsoft Entra ID
03	CloudGate UNO
04	CloudLink
05	GMOトラスト・ログイン
06	Google Workspace
07	HENNGE One
08	KAMOME SSO
09	Keycloak
10	Nextset
11	Okta
12	Onelogin
13	OpenAM

2025.07 現在（随時追加検証中）

※ 接続先システムの仕様により、一部に機能制限等が生じる場合もあります。　※ 試用版・デモサイトにて行った検証も含まれます。

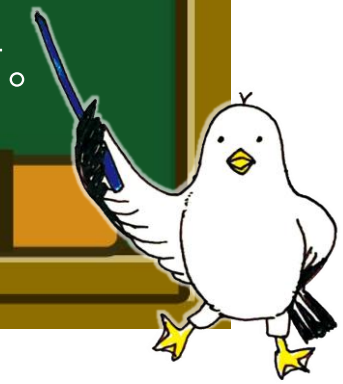
導入の主要ポイント

- 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環境へ適用させるため、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。
- SMBプラン（仮称）のご利用により、コストパフォーマンスも格段に向上。

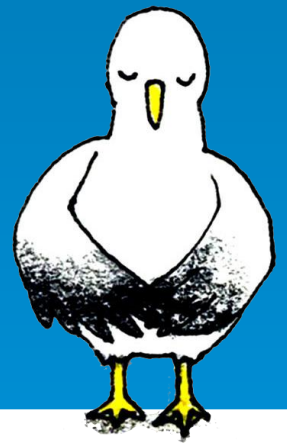
まとめ

KAMOME Engineering

- 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。中小規模でも導入しやすい「SMBプラン（仮称）」もご用意しました。
- 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！