C22 まるっとわかる！ゼロトラストとSASE

~ ゼロトラストの昨今 ~

島田 直人

2026/07/01 @Internet Week Showcase in Shizuoka

目次

- はじめに
- ゼロトラスト・SASEのおさらい
- ゼロトラストの話題が増えた「その後」
- ゼロトラストの「この後」
- おまけ

登壇者紹介

- 島田直人　Naoto Shimada
  - ゼロトラスト事業立ち上げメンバーとして3年前より現職へ
  - Zscaler ACE、FY25 BEST SALES ENGINEER AWARD など
  - CSAジャパン 個人会員

- とある会社
  - Palo Alto Networks 国内初のCPSP認定
  - Cisco セレクトデベロッパー

特記事項

- 発言は個人の見解に基づくものであり、
  所属組織を代表するものではありません

- 例示のため具体的な製品名を挙げることがありますが、
  特定製品の利用を奨励するものではございません

今回のゴール

- ゼロトラストとは？
  - 概要と必要な知識をいくｔかピックアップ
- コロナ禍に後押しされてゼロトラストは流行ったのか？を知る
- さらに今後はどのようになっていくのか？
  - 心構えを押さえる

はじめに

ゼロトラストが特に話題になって数年...

- ゼロトラスト化は進みましたか？
- 実はブームが去ってしまった？
- ゼロトラストしなくても良くなった？

アメリカの対応

- 2022年6月 アメリカ合衆国大統領府

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

政府機関のゼロトラスト化を要求

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

アメリカの対応

- 2025年1月 大統領令
  - Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity

(B) revise OMB Circular A-130 to be less technically prescriptive in key areas, where appropriate, to more clearly promote the adoption of evolving cybersecurity best practices across Federal systems, and to include migration to zero trust architectures and implementation of critical elements such as EDR capabilities, encryption, network segmentation, and phishing-resistant multi-factor authentication; and

ゼロトラストアーキテクチャへの移行に関する記述

https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/

国内の対応

- 2022年6月 デジタル庁
  - ゼロトラストアーキテクチャ適用方針 公開

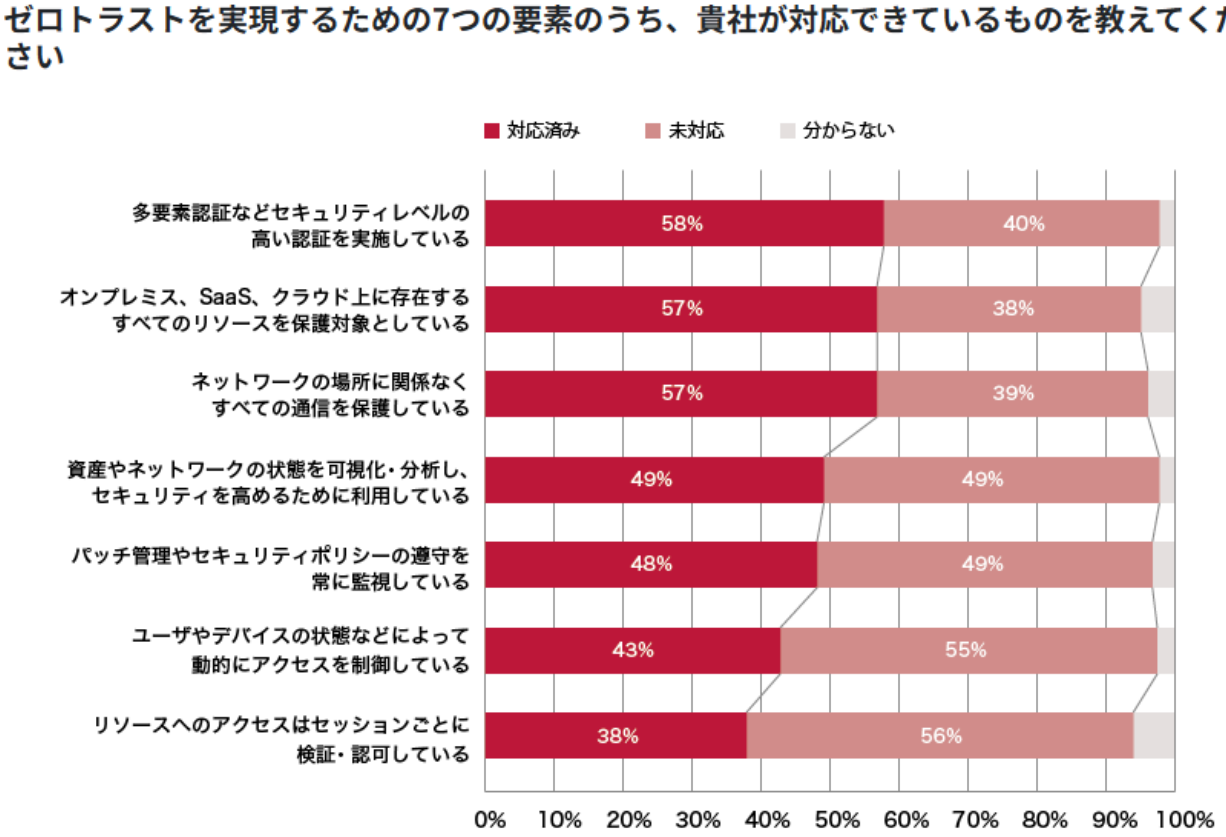
    https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf

- 2024年6月 デジタル庁
  - 国・地方ネットワークの将来像及び実現シナリオに関する検討会

    https://www.digital.go.jp/councils/local-goverments-network

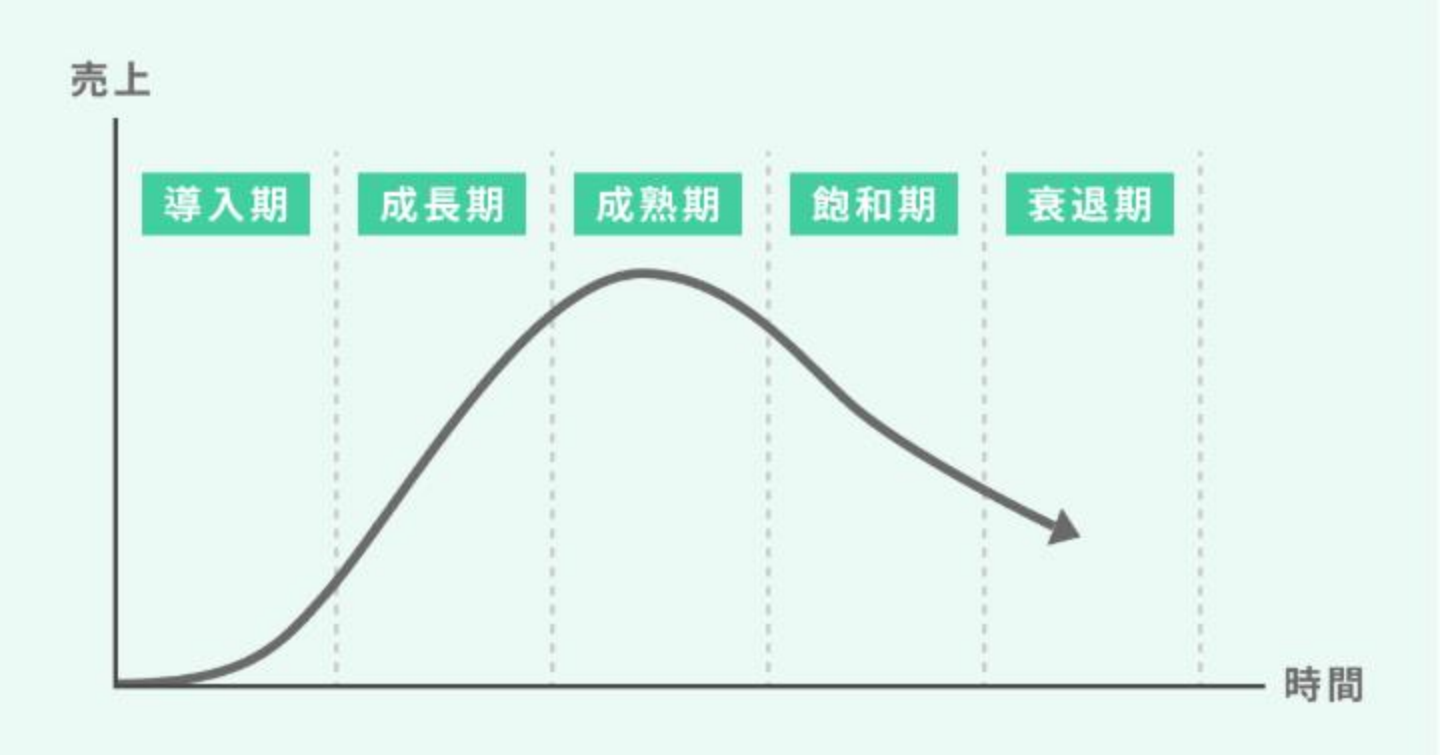
- ゼロトラストアーキテクチャの導入に向けて**継続的に議論**

国内の対応



引用：【ゼロトラスト実態調査】5割がすでに一部対応済。認証強化の実施が最多、今後の課題はアクセス制御
IIJメールマガジンの読者に対するWebアンケート（2024年7月24日～7月31日, 情報システム部門 n=347）
https://ent.iij.ad.jp/articles/8369/

国内の対応



引用：プロダクトライフサイクルとは？意味や段階を徹底解説 https://backlog.com/ja/blog/what-is-the-product-life-cycle/

2026年現在 まとめ

- アメリカでは先行してゼロトラストを推進
- 日本国内でも、省庁のみならず大手企業が着々と導入
  - コロナ禍のリモートワーク需要も後押し
- 中小企業も追従して導入を検討
- ゼロトラストは前ほど騒がれなくなったものの、
  依然として検討・導入が進んでいる状況

ゼロトラスト・SASEのおさらい

ゼロトラスト

- Forrester Research社のJohn Kindervag氏より**2010年**に提唱
  - 実際の製品や導入する会社が出てくるのはまだ先のこと
- 「信頼せず、常に検証する (Never trust, always verify)」
  - 盲目的な信頼の従来型モデルでは防げない事例が増加...
- 概念を表す言葉であり、製品そのものではない
  - ゼロトラストモデル、ゼロトラスト化という言い方になる
  - それでもゼロトラスト製品とは言ったりするけど...

ゼロトラスト 7つの原則

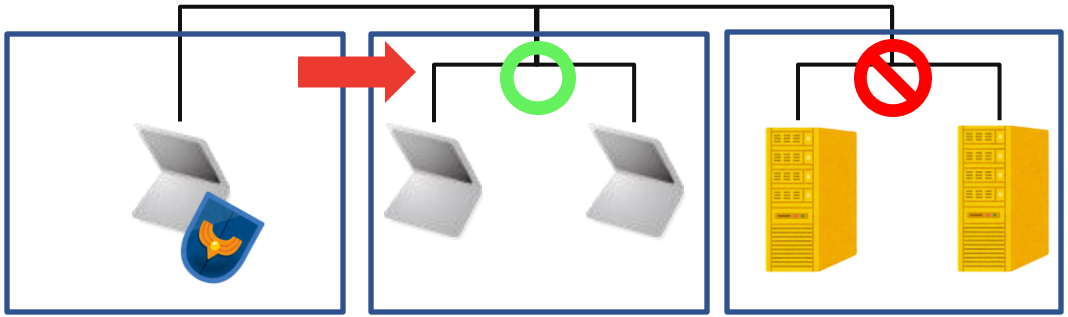
- NIST SP 800-207 Zero Trust Architecture より
  1. データソースとコンピュータサービスは、全てリソースと見なす
  2. ネットワークの場所に関係なく、通信は全て保護される
  3. 組織のリソースへのアクセスは、全て個別のセッションごとに許可される
  4. リソースへのアクセスは動的なポリシーによって決定される
  5. 組織が保有するデバイスは、全て正しくセキュリティが保たれているように継続的に監視する
  6. リソースの認証と認可は、全てアクセスが許可される前に動的かつ厳密に実施される
  7. 資産・ネットワーク・通信の状態について可能な限り多くの情報を収集し、セキュリティを高めるために利用する

常に検証 + 最小限の権限 を実現する

- SDP/ZTNA、micro segmentation
  - 簡単に言うと
    「ネットワークへの接続認証が通れば、その先は全て認可」
    だったものを
    「各アプリケーションごとの認可レベルで制御」していく

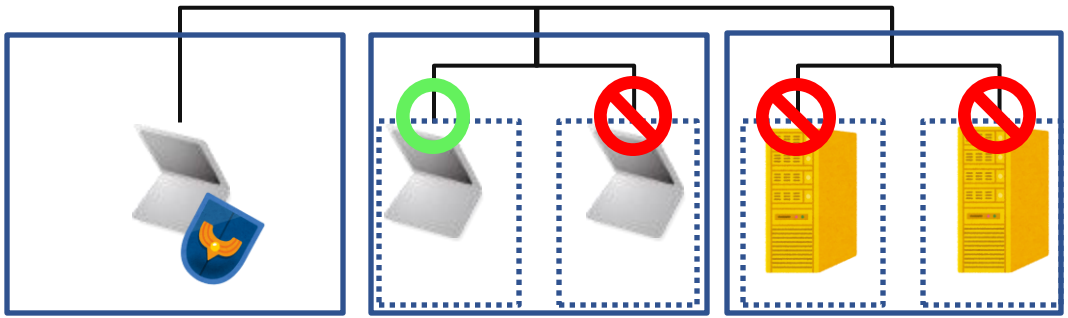
常に検証 + 最小限の権限 を実現する

- micro segmentation
  - 「ネットワークにさえ接続できれば、その後の通信は自由」では侵入後の攻撃に無抵抗になってしまう
  - ラテラルムーブメント (水平展開、水平方向への攻撃)



常に検証 + 最小限の権限 を実現する

- micro segmentation
  - 権限を最小限にすることで、水平展開による被害も抑制



常に検証 + 最小限の権限 を実現する

- 従来
  - VPNの接続情報を知っていれば、誰でもそのネットワークに入れる
- ZTNA
  - 特定のユーザー、部署、場所、時間帯、その他任意のSAML属性など
  - アプリケーションの TCP/UDP port xx のみ
- 詳細なモニタリングが可能な製品もあるが、干渉に注意
  - 例：FTPなど、ポートの待ち受けが発生するプロトコルでは
    ヘルスチェックの通信が先に到達することでポートが閉じてしまう

SASE

- Secure Access Service Edge
- Gartner社より**2019年**に提唱

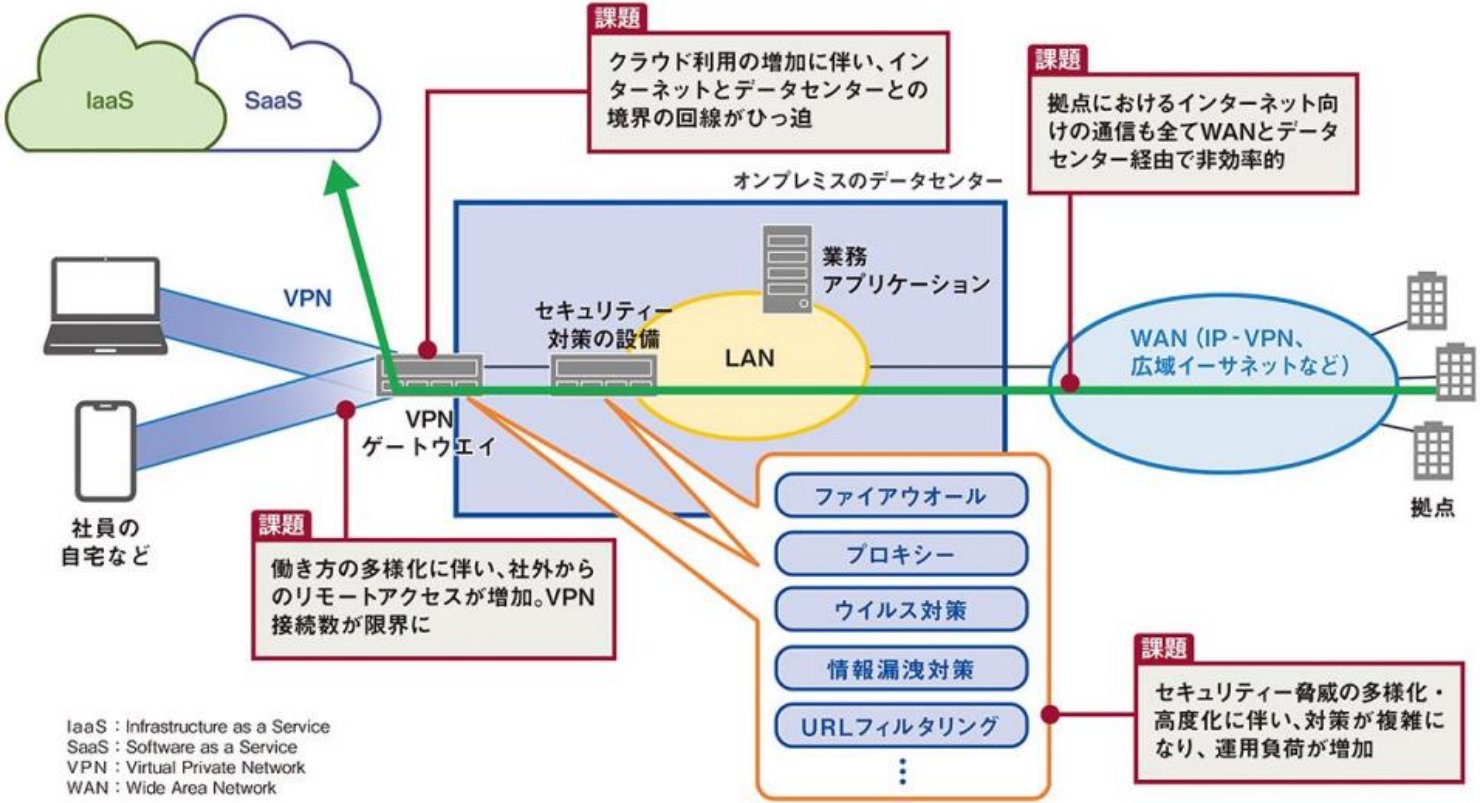
- **セキュリティ**と**ネットワーク**を併せ持つクラウドサービス
  - 今やこの2つは切っても切れない関係

- 主な構成要素
  - SWG
  - CASB
  - FWaaS
  - ZTNA
  - SD-WAN

機能や機能群(製品)そのものを表す言葉

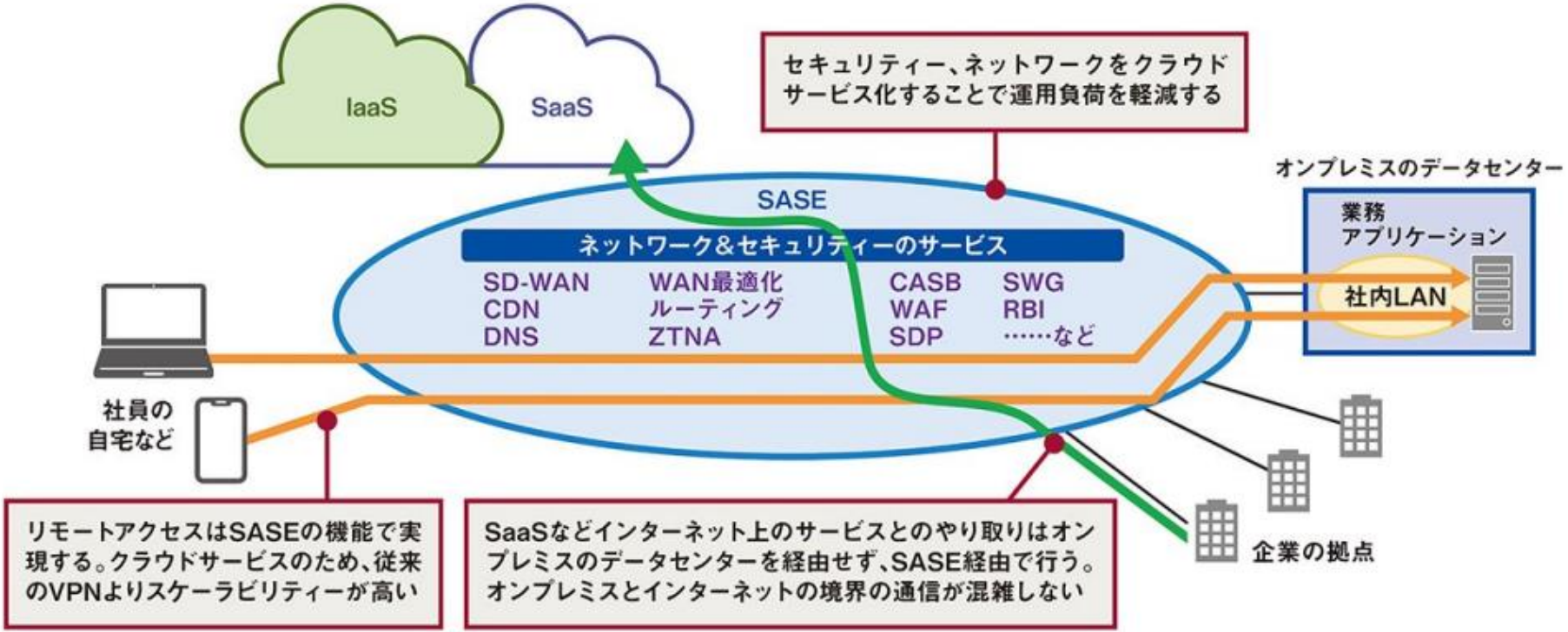
SASEの具体例は次のセクションにて！

従来の境界防御の課題



引用：すべてわかるゼロトラスト大全(日経クロステック, 2020)

ゼロトラストを実現するSASEの特長



CASB：Cloud Access Security Broker
CDN：Content Delivery Network
DNS：Domain Name System
RBI：Remote Browser Isolation
SASE：Secure Access Service Edge
SDP：Software Defined Perimeter
SWG：Secure Web Gateway
WAF：Web Application Firewall
ZTNA：Zero Trust Network Access

引用：すべてわかるゼロトラスト大全(日経クロステック, 2020)

ゼロトラストの今

ゼロトラスト製品を導入してめでたしめでたし。

- かと思いきや...

ゼロトラスト製品を導入してめでたしめでたし？

- 需要急増によるエンジニア不足
- 導入するベンダー、ユーザー双方のナレッジ不足

エンジニア不足・ナレッジ不足

- コストやスペックなどの都合で、今まで使えていなかったSSL Inspectionなどの機能に関する検討不足
  - 使ってみるとページの表示が崩れてしまう
  - 会社全体に影響を与えたくないからOFFにしてしまう

- でも、ONにしないとほとんど意味がない

SSL Inspection

- 暗号化されたトラフィックを復号して検査すること
  - SSLよりTLSの方が後継、未だにSSLの方でも呼ばれる

- 近年ではほとんどのWeb通信がHTTPSであり、
  悪性の高いサイトでももちろんHTTPS対応しているため、
  これをしないとほとんど**何も見えない・防げない**
  - 単なるURL(SNI)のフィルタリング以上の
    細かい制御要件を満たすためには、復号が必要不可欠

- 通信の途中で復号→再暗号化する、という点だけ見ると
  攻撃者が行う Man In The Middle攻撃と同じ
  - ブラウザによってはこれを検知して警告する

SSL Inspection

- 例えばクラウドプロキシ型の製品であれば、
  その製品の証明書を端末にインストール

- 実際にブラウジングすると、元々とは異なる証明書が見える

SSL Inspection

- 高速に処理しないとトラフィックが停滞することから、
  高いマシンスペックが要求される
  - ゼロトラスト化すればサービス側で処理される構成になるので、
    スペック問題からは解放

- ページの表示が崩れるといったトラブルが起こりやすく、
  除外対応に追われたり、導入を躊躇されたり...

- 過去のJANOGなどでも議論
  - JANOG45 そろそろSSL通信に本気出して向き合ってみる
    - 証明書配布や除外などの運用負荷、パフォーマンスの問題

SSL Inspection

- Certificate pinning
  - ブラウザなどの各アプリケーションに証明書をピン留め
  - これと異なる証明書が提示された場合、その通信を拒否する

  - MITM攻撃を防ぐために発案された
  - OSのアップデートといったクリティカルな通信に影響する

  - 各メーカーは、インスペクション除外推奨リストを定義
  - それでも、対応しきれていないものは自分たちで対処

- ゼロトラストは「信頼せず、常に検証する」
  →でも、**除けておいた方が良いものもある**

SSL Inspection

- SSL Inspectionのために、各メーカーはQUICのブロックを推奨

- Cato

https://support.catonetworks.com/hc/en-us/articles/360004274777-Internet-and-WAN-Firewall-Policies-Best-Practices

- Netskope

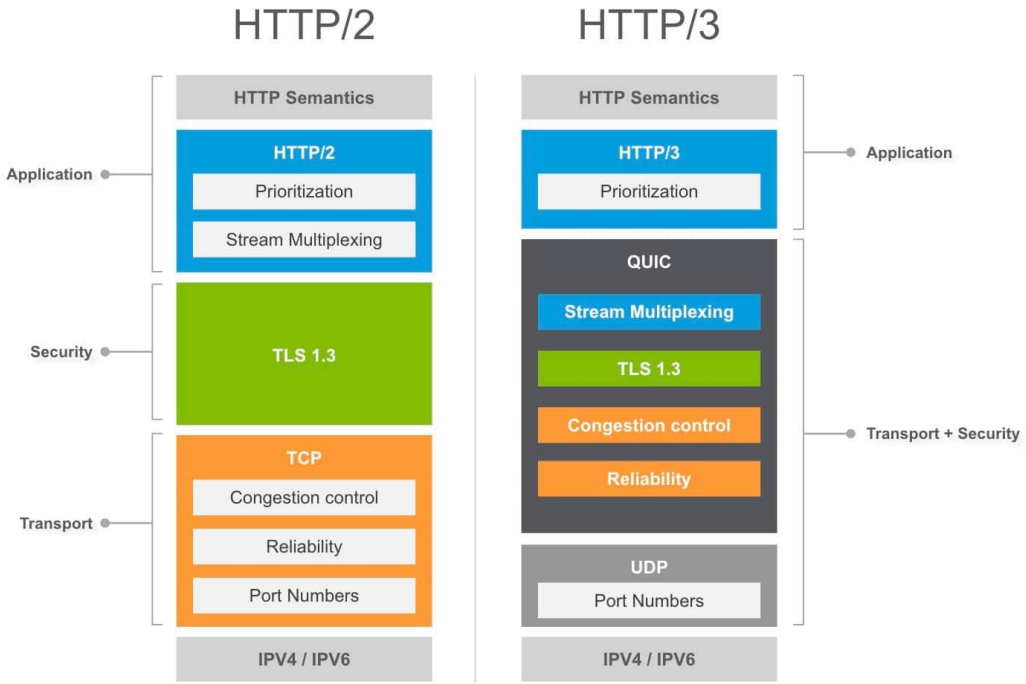
https://community.netskope.com/next-gen-swg-2/a-quic-primer-to-how-netskope-handles-the-quick-udp-internet-connections-protocol-928?utm_source=chatgpt.com

- FortiSASE

https://docs.fortinet.com/document/fortisase/25.1.51/administration-guide/219936/blocking-quic

SSL Inspection

- そもそもSSL InspectionはTLS(TCP)が対象
  - QUICはL4の一部まで暗号化されている



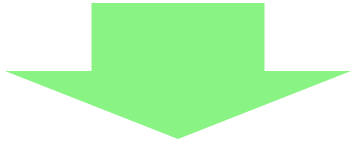
引用：HTTP/3 を使用し、高速で信頼性が高く安全な Web 体験を提供
https://www.akamai.com/ja/blog/performance/deliver-fast-reliable-secure-web-experiences-http3

SSL Inspection

- JANOG49 QUICについて話そう
  - 最終手段：本当にUDP443を塞いでいいの？
  - 「やったら負け」
- Internet Week とある美味しいお弁当をいただけるセッション
  - HTTPSレコードが活用されるはずが...
- サービス側で止めるより、ブラウザで止めてしまった方が良い
  - フォールバックするよりは、元から使わせない
- 時代と逆行してしまうけど致し方なし？
  - QUIC Inspection を実装する製品が出てくるという噂も

エンジニア不足・ナレッジ不足

- 流行を後ろ盾に押し売りされすぎた？
  - PM・エンジニアが見つからない...
  - 数年経っても基本設定だけで放置されていたり
  - ライセンスは数年一括で売れるが、その後のケアはやりたくない



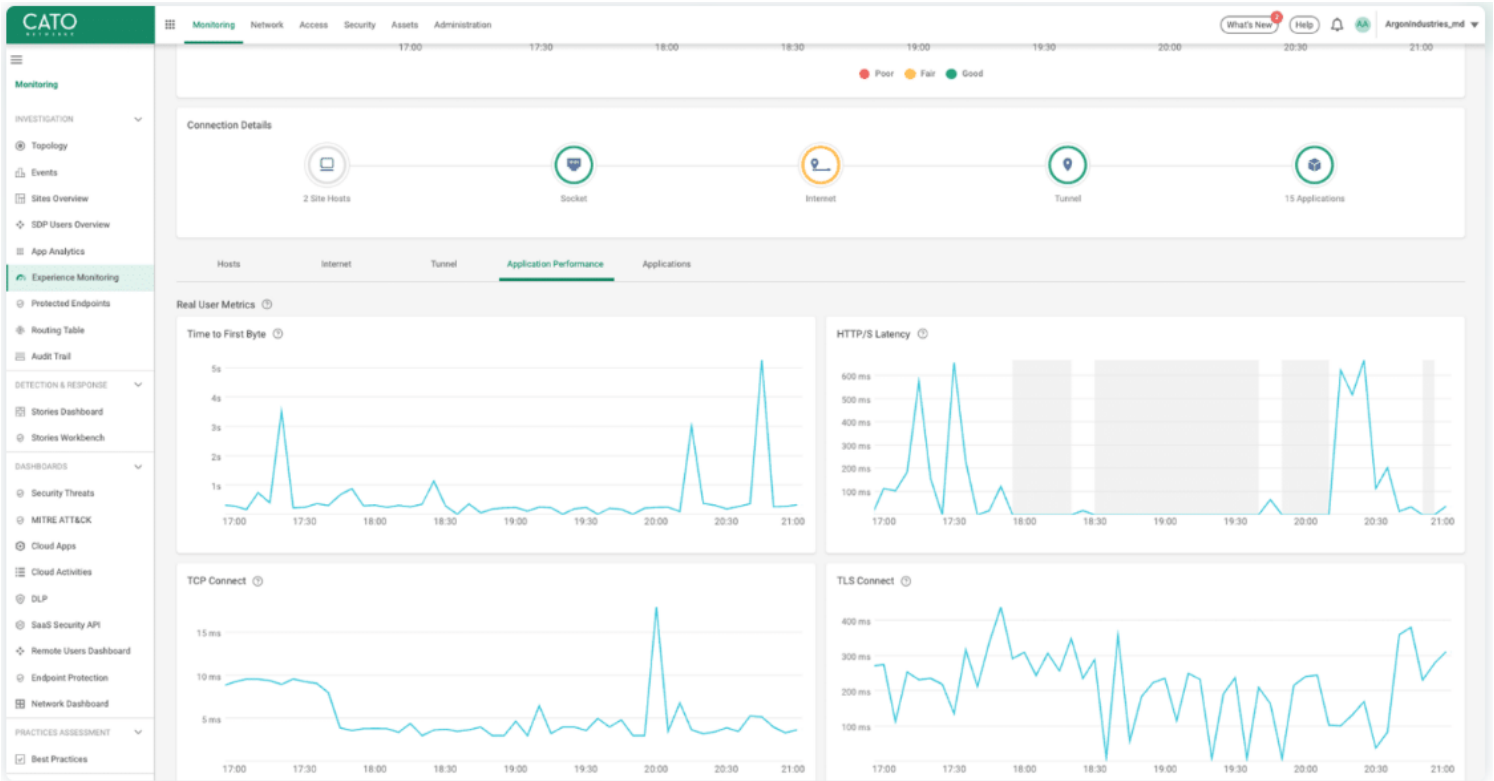
- PoCの時点で十分に検証を行い不安な点を洗い出し、
  メーカーのウェビナーなども活用して自社で学習していくか、
  リソース・実績が確かなベンダーを頼りましょう

エンジニア不足・ナレッジ不足

- 接続が遅い、できないといった問題発生時、
  確認ポイントが増えてどこに原因があるのかの究明が困難に
  - 既存の自社ネットワーク
  - **SASE** New!
  - **リモートワーク環境** New!

エンジニア不足・ナレッジ不足

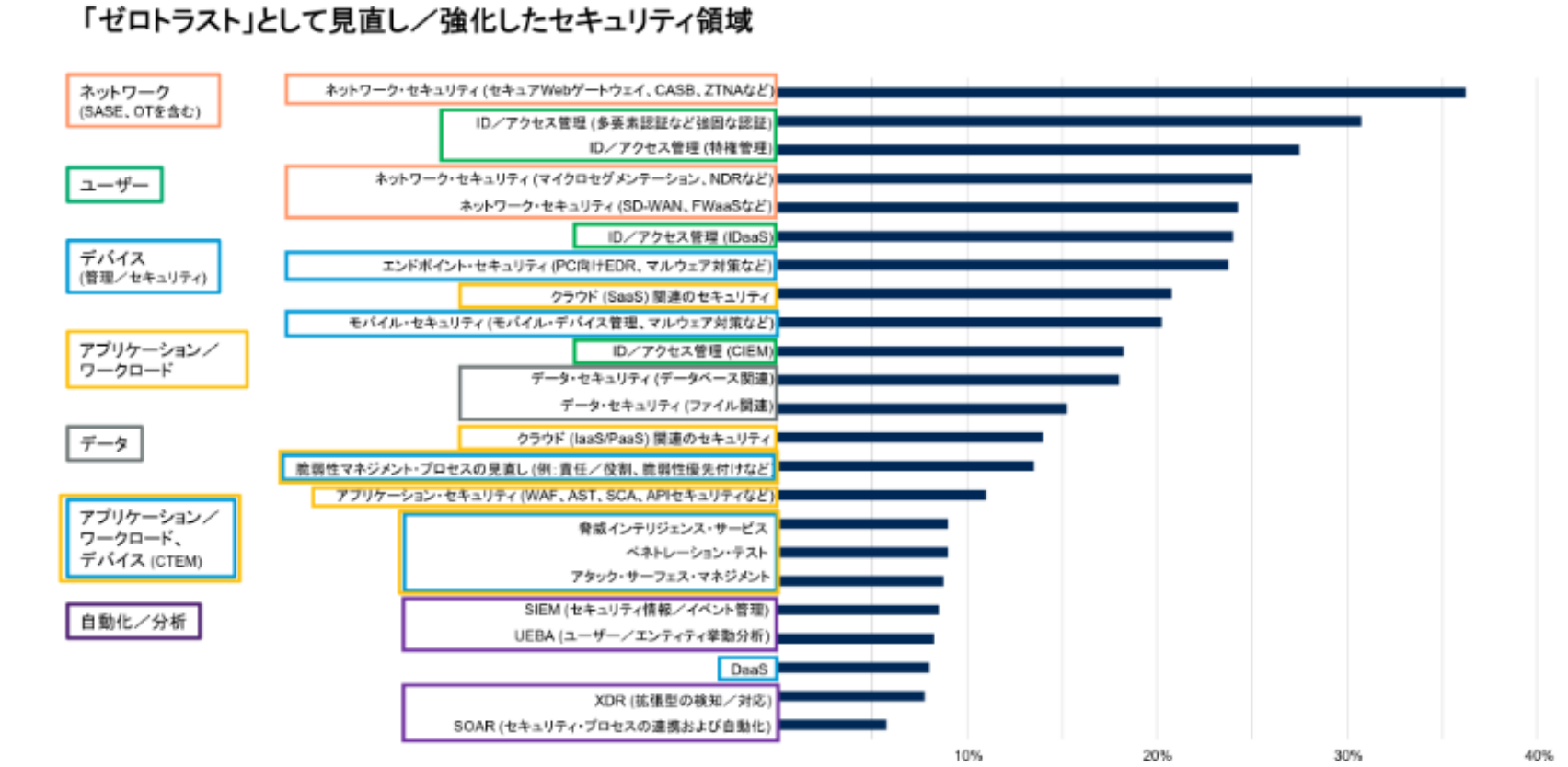
- デジタルエクスペリエンスのモニタリング機能を備える製品も



引用：Cato DEM https://www.catonetworks.com/ja/platform/digital-experience-monitoring-dem/

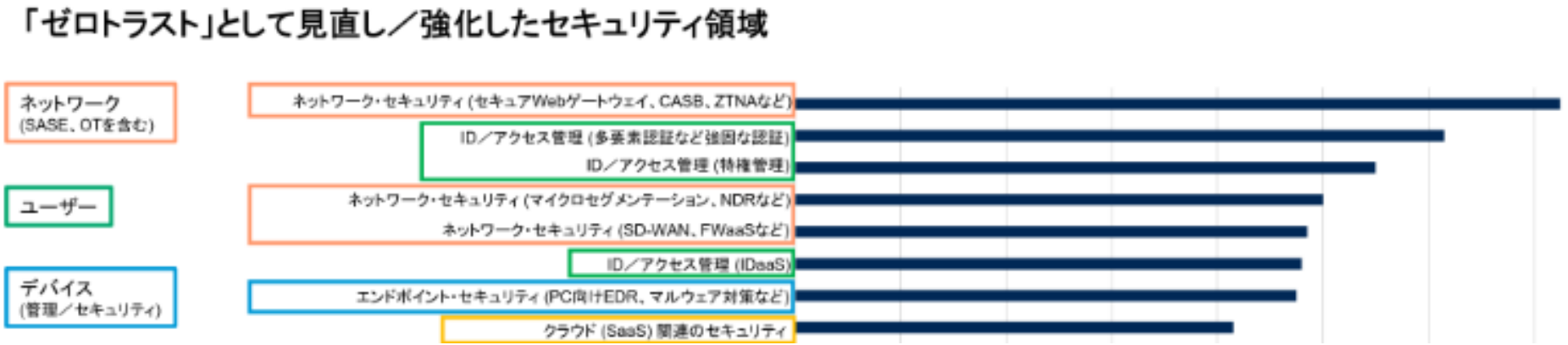
ゼロトラストの未来

このまま進んでいくのか？



引用：Gartner、ゼロトラストの最新トレンドを発表 (2025年2月, 情報システム部門 n=400)
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20250508-zero-trust

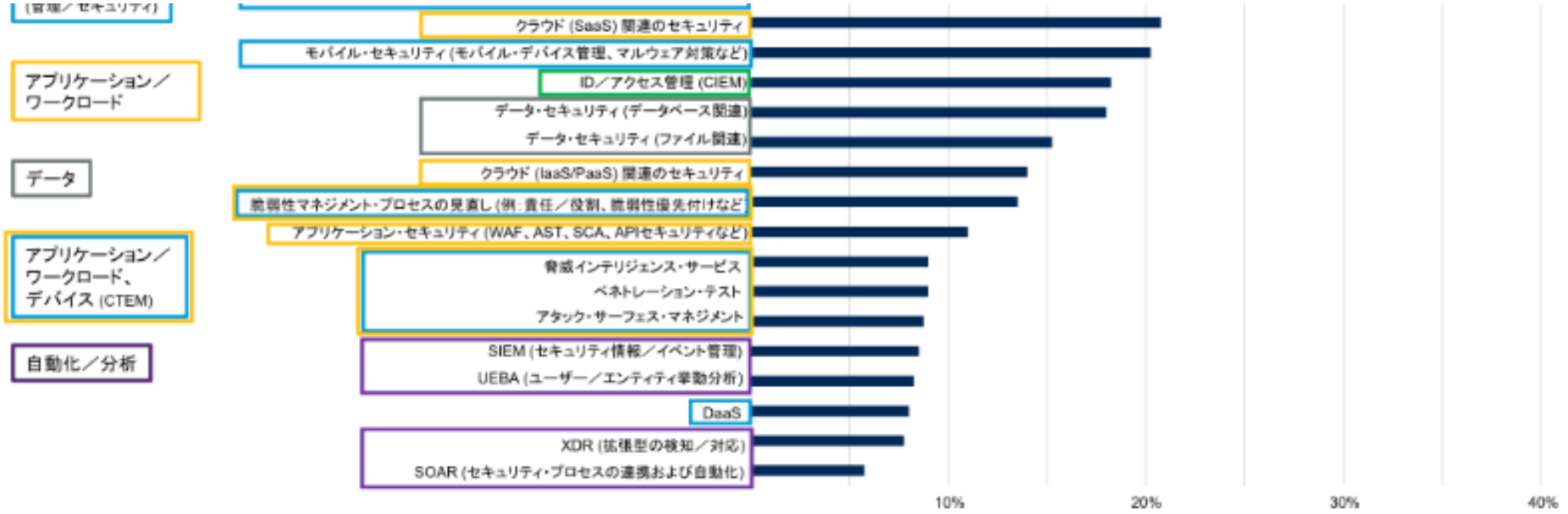
このまま進んでいくのか？



- ネットワーク、認証、エンドポイントなどの見直し・強化は比較的な順調な傾向にある

引用：Gartner、ゼロトラストの最新トレンドを発表 (2025年2月, 情報システム部門 n=400)
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20250508-zero-trust

このまま進んでいくのか？



- データセキュリティ、自動化・分析などはこれから伸びるか、そこまで進まない可能性も

引用：Gartner、ゼロトラストの最新トレンドを発表 (2025年2月, 情報システム部門 n=400)
https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20250508-zero-trust

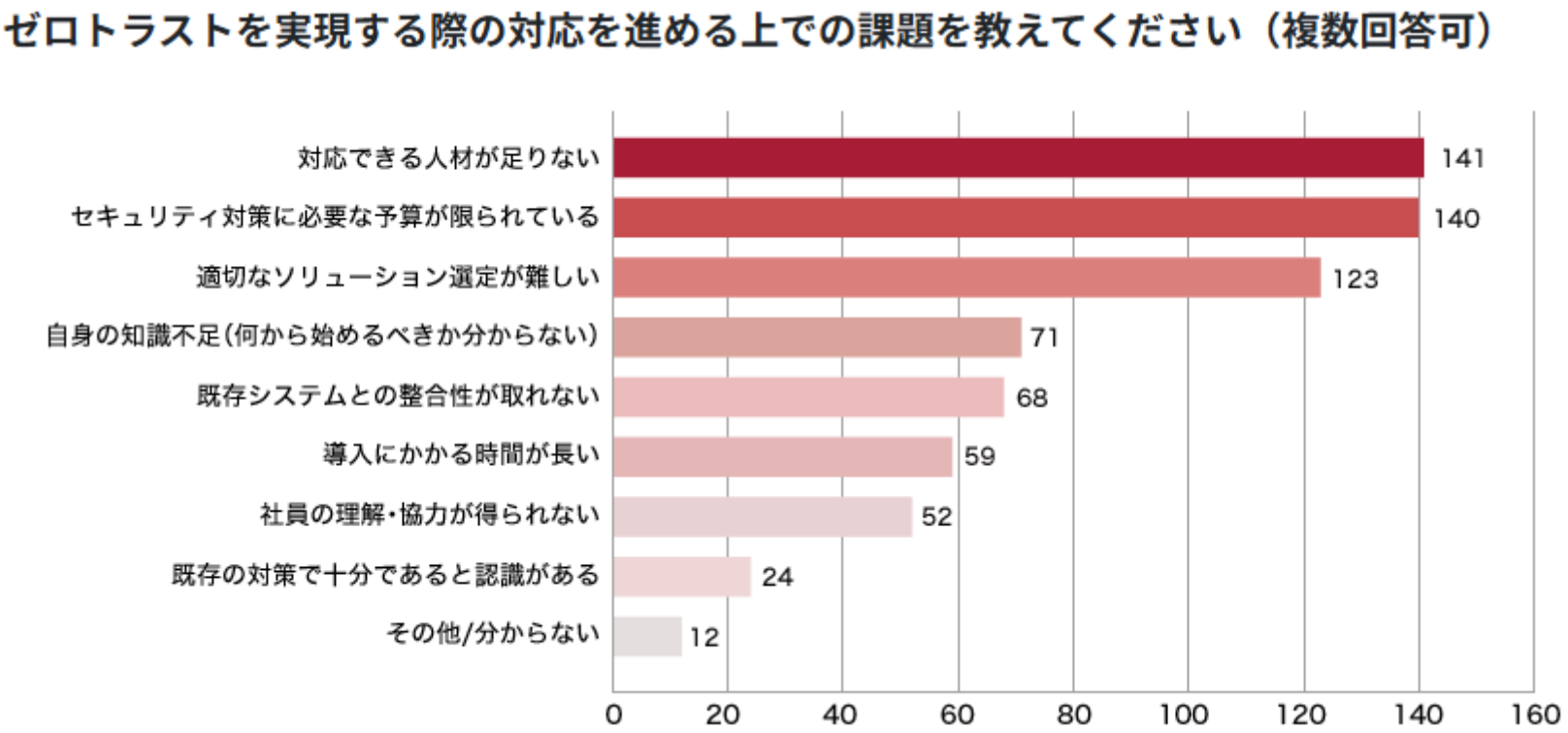
この後の課題

- 2028年までに 30% もの企業がゼロトラスト化の取り組みを放棄してしまう、との予想も

- 原因はやっぱり...
  - 複雑さ
  - 統合の欠如
  - 文化的な抵抗
  - 制限されたベンダーの価値

- Predicts 2025: Scaling Zero-Trust Technology and Resilience
  March 2025, Gartner社 https://www.gartner.com/en/documents/6283983

この後の課題



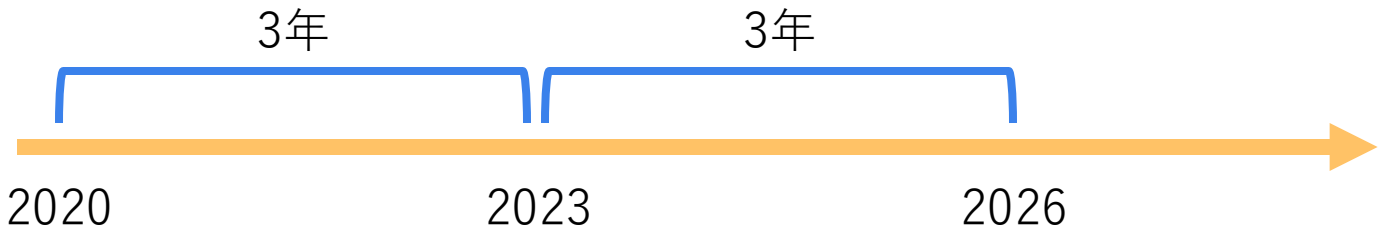
引用：【ゼロトラスト実態調査】5割がすでに一部対応済。認証強化の実施が最多、今後の課題はアクセス制御
IIJメールマガジンの読者に対するWebアンケート（2024年7月24日～7月31日, 情報システム部門 n=347）
https://ent.iij.ad.jp/articles/8369/

アフターコロナも課題がいっぱい

- リモートワークが受け入れられ、オフィスやデータセンターに依存しないネットワーク・セキュリティもスタンダードに
- 依然として解消されない人材不足
- ライセンス更改・機器ライフサイクルに伴う鞍替え
- CASB、DLPなど今まで未導入だった分野のナレッジ不足
- 導入したまま放置、あるだけで使われない多種多様な機能

ライセンス更新・機器ライフサイクルに伴う鞍替え

- コロナ禍から6年ほど経過
  - 3〜5年の年月は、ちょうどライセンス更新や機器ライフサイクルに伴うリプレースの周期と重なる



- 思ったよりも導入が進まなかった、ベンダーの対応が悪いなど様々な理由で**製品・ベンダーの鞍替えが進行中**
  - ライセンスを購入したがアプリの展開すらままならなかった、保守も契約したがあまり使っていないのでお金だけ払っているなど

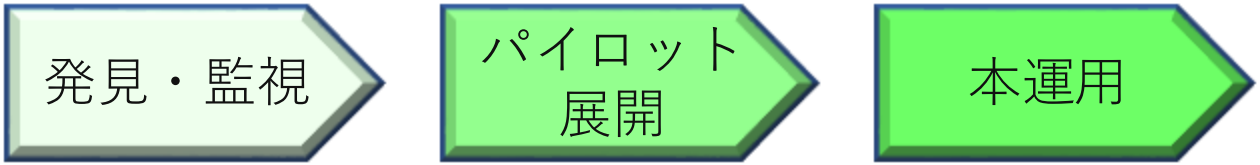
未導入だった分野のナレッジ不足

- Webアクセスなどの標準的な制御の次にニーズがあるのが、SaaSやデータ(CASBやDLP)などのセキュリティ機能
  - やはり必要な通信を止めてしまったり、クレームが来るのが怖い、大変→やらないの流れに陥りがち

- でも、ライセンスは買ってあったりする

未導入だった分野のナレッジ不足

- 止める・止めないの二択だけはないという意識が必要
- 段階的にアプローチしていきましょう



- まずは許可したまま発見・監視する
- 次に方針を決定する、パイロット展開で始めてみる
- そして本運用開始、チューニングしながら理想に近づけていく