C6 ゼロトラストのその後とこの後
～アフターコロナの行先

株式会社エーピーコミュニケーションズ
島田 直人

2025/11/25 @Internet Week 2025

登壇者紹介

- 島田直人 Naoto Shimada
  - 株式会社エーピーコミュニケーションズ 所属
  - 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

- 株式会社エーピーコミュニケーションズ APCommunications
  - Palo Alto Networks 国内初のCPSP認定
  - Cisco セレクトデベロッパー、Zscaler DSA認定 など

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なく、
  各種機能の詳細な質問には回答できません

今回のゴール

- ゼロトラストとは？概要の再認識
- 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？
  押さえておきたい知識や心構えを押さえる

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

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

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

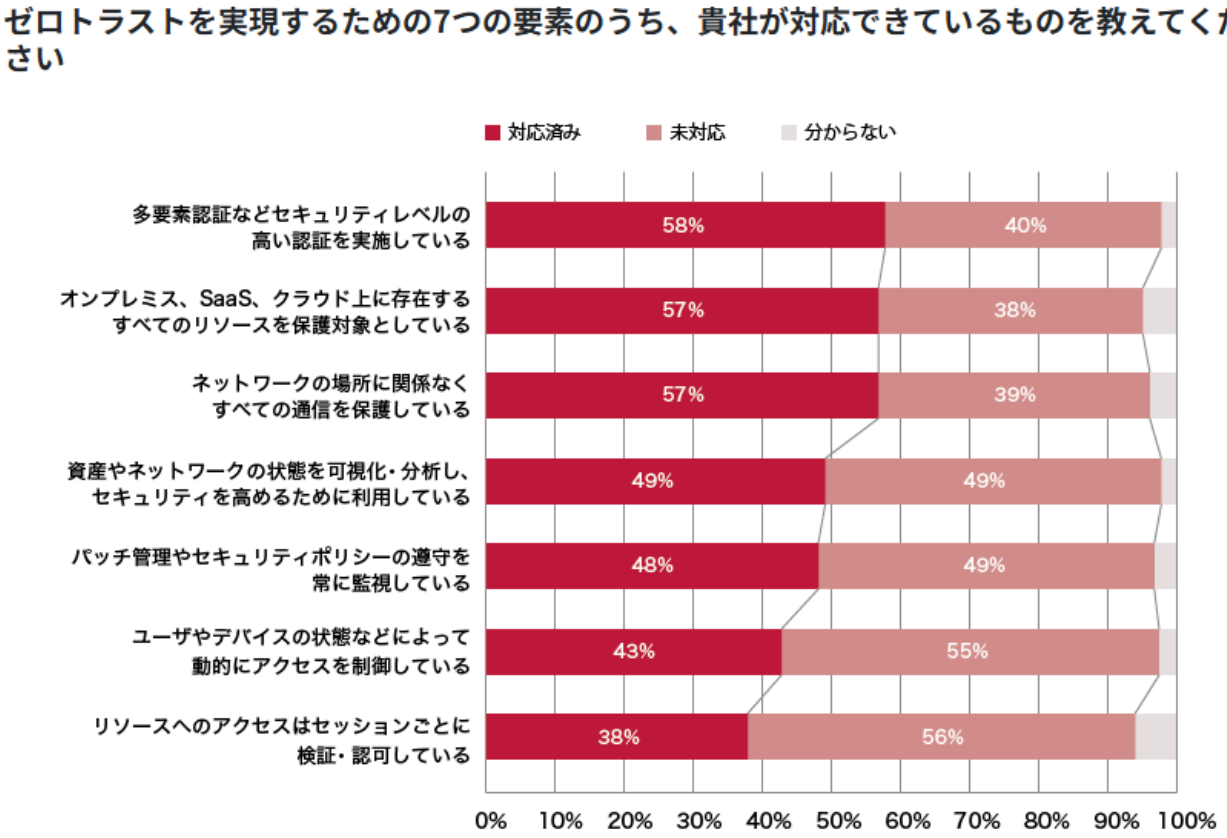
    https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf

- 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

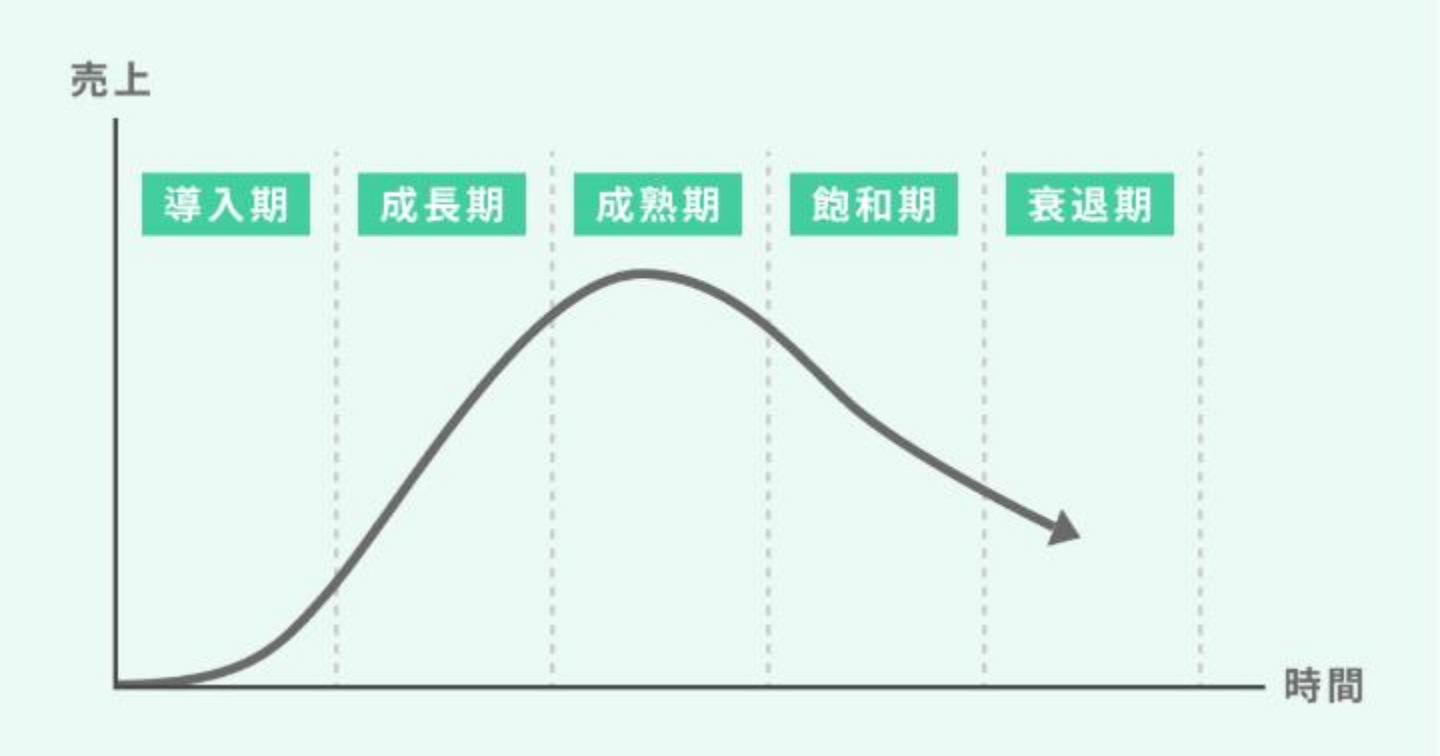
- ゼロトラストアーキテクチャの導入に向けて継続的に議論

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/

2025年現在

- 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

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...

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、2つを併せ持つサービス
  - 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

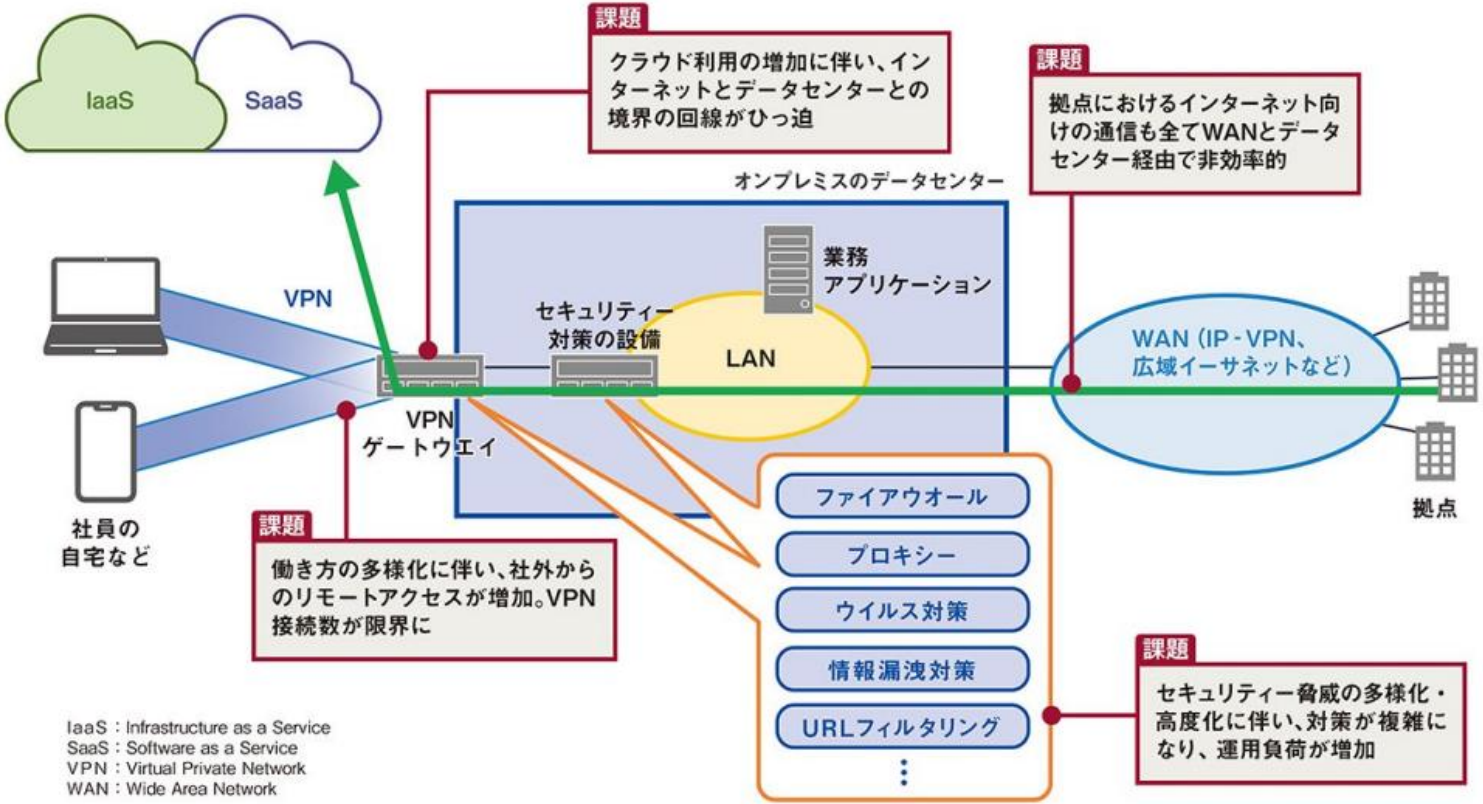
SSE

- Secure Service Edge
- Gartner社より、SASEの2年後 2021年に提唱

- SASEのうち、SD-WANを中心とする
  ネットワークの部分がオミットされたサービス

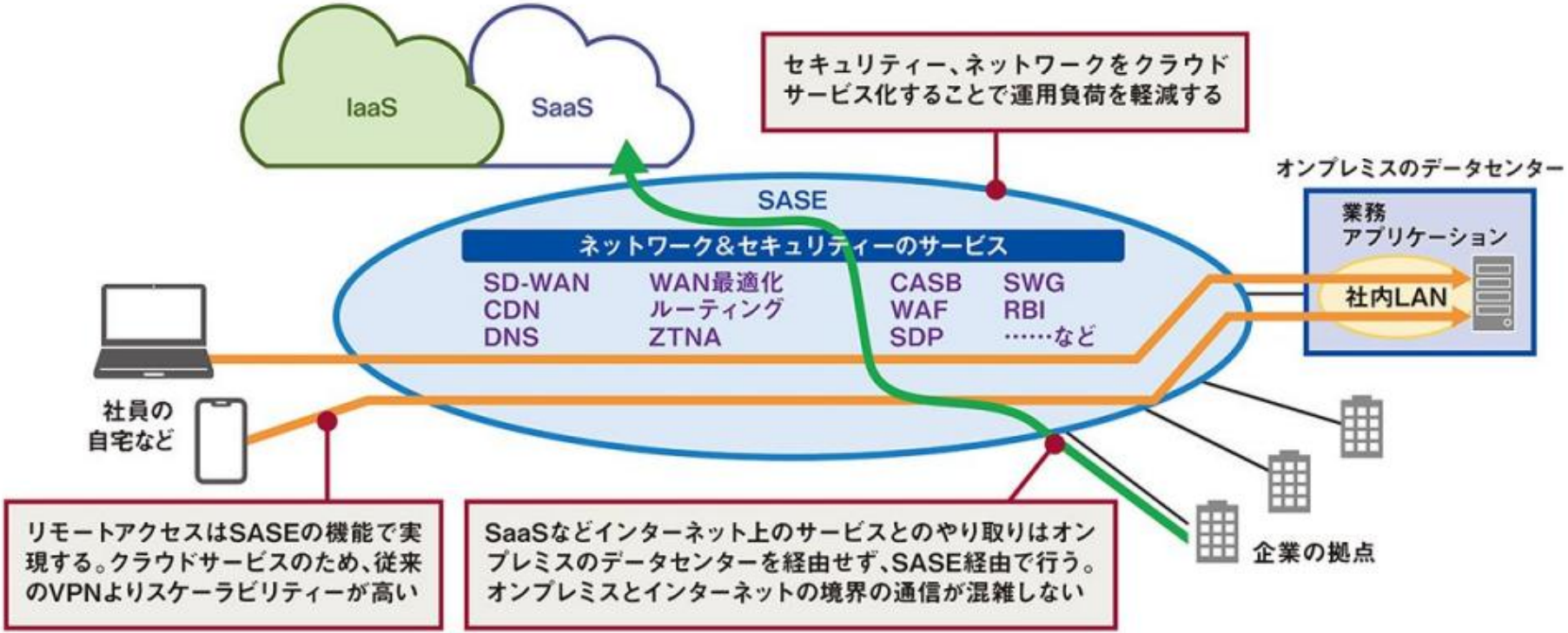
- 主な構成要素
  - SWG
  - CASB
  - FWaaS
  - ZTNA
  - ~~SD-WAN~~

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)

SASEの特長

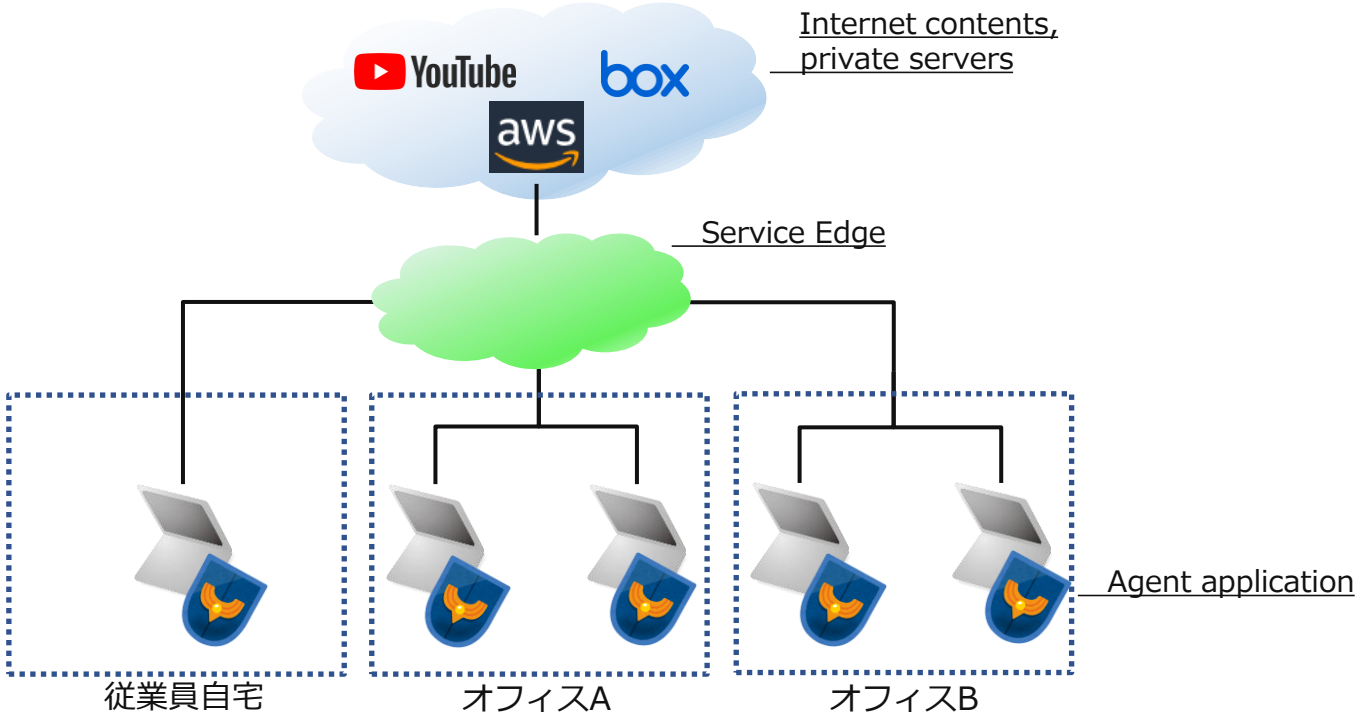


CASB：Cloud Access Security Broker
CDN：Content Delivery Network
DNS：Domain Name System
RBI：Remote Browser Isolation
SASE：Secure Access Service Edge
SDP：Software Defined Perimeter
SWG：Secure Web Gateway
WAF：Web Application Firewall
ZTNA：Zero Trust Network Access

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)

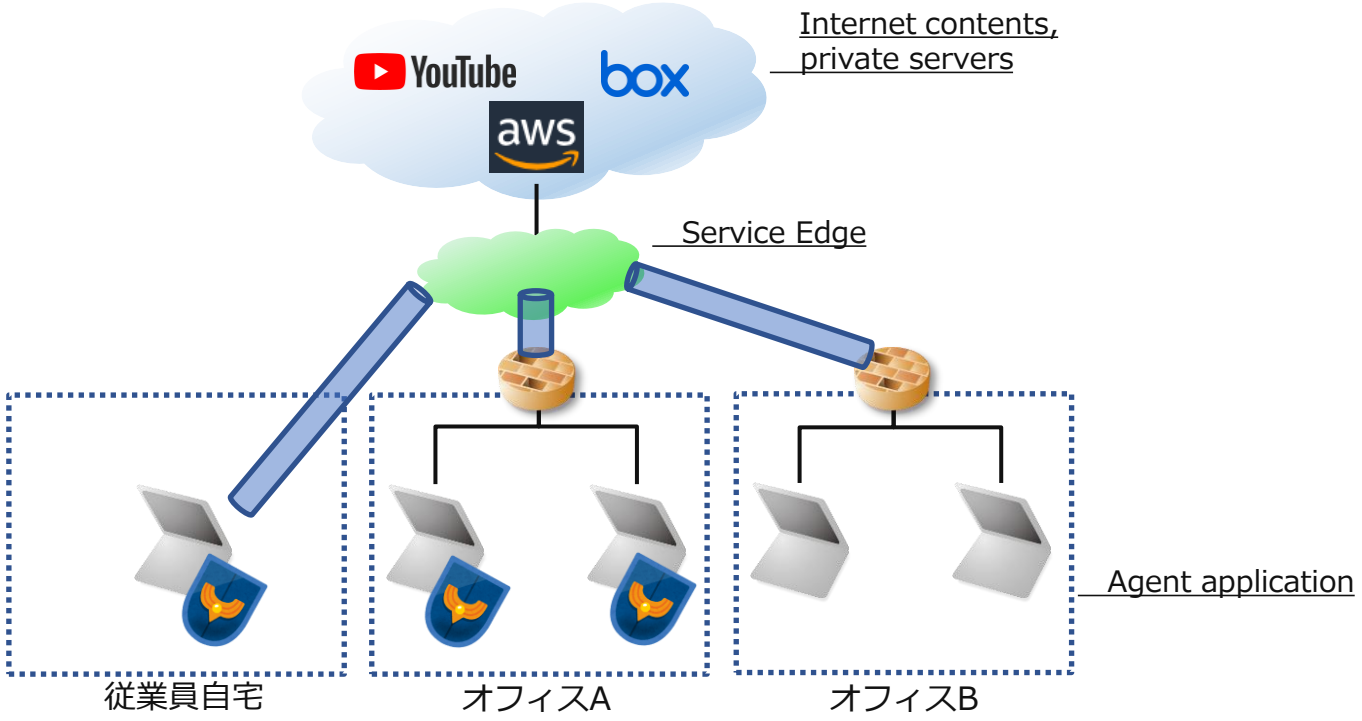
クラウドプロキシ型の特徴

- クライアントの通信をサービスエッジで一度終端する
  - 既存ネットワークへの依存度が低い一方、拠点間通信の制御は不得手



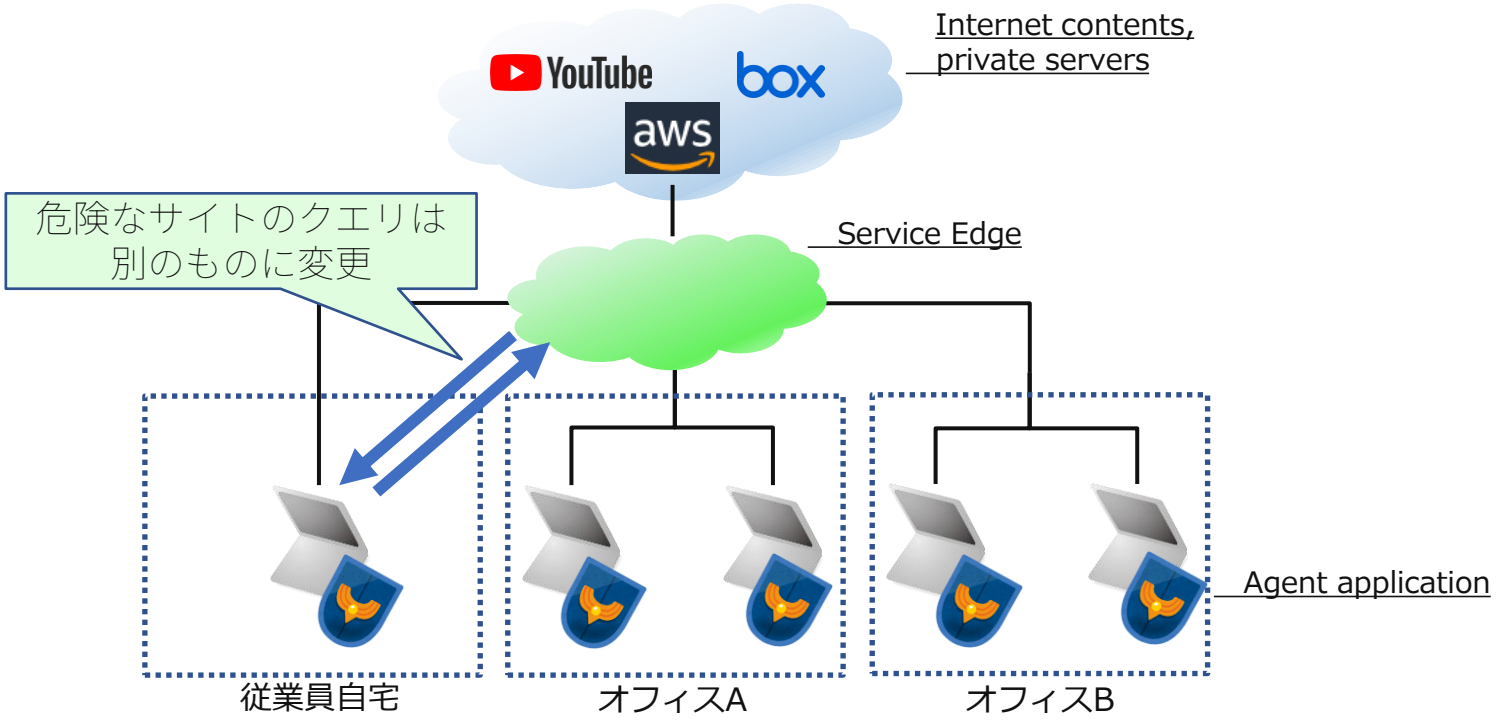
ネットワーク型の特徴

- クライアントの通信経路上にサービスエッジが存在
  - 既存ネットワーク機器からの移行が楽



DNS型の特徴

- クライアントからのDNSリクエストに対するクエリで制御



ゼロトラストの話題が増えた「その後」

SASE・SSEを導入してめでたしめでたし。

- かと思いきや…

SASE・SSE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

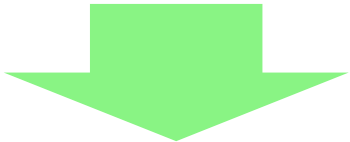
エンジニア不足・ナレッジ不足

- 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

エンジニア不足・ナレッジ不足

- 流行を後ろ盾に押し売りするベンダー
  - 売るだけ売って、PM・エンジニアが見つからないまま案件スタート
  - ベストプラクティスや気を付けるべき設定なども知らぬまま、数年経った今でも放置されていたり
  - 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



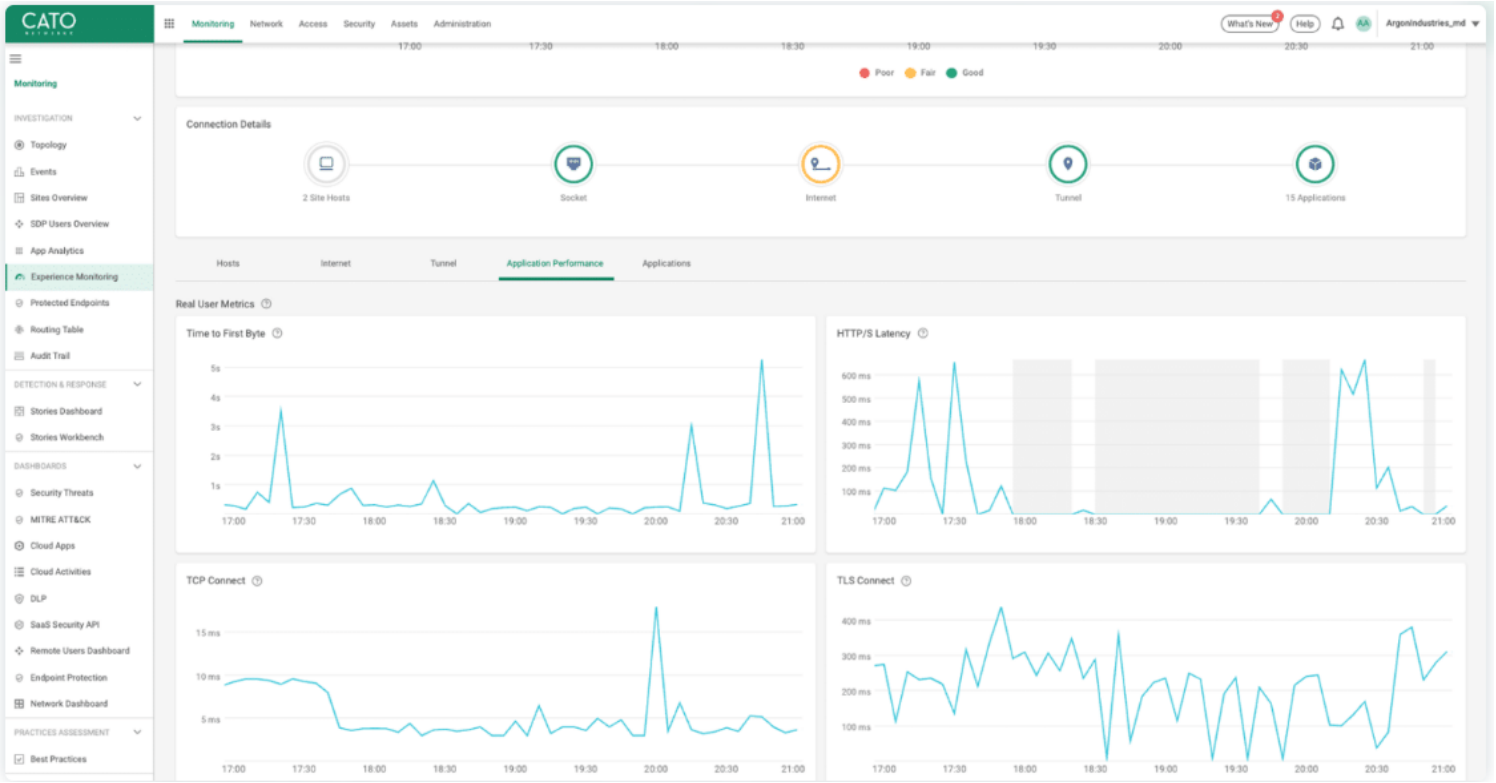
- PoCの時点で十分に検証を行い不安な点を洗い出し、メーカーのウェビナーなども活用して自社で学習していくか、リソース・実績が確かなベンダーを頼りましょう

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製品 New!
  - リモートワーク環境 New!

エンジニア不足・ナレッジ不足

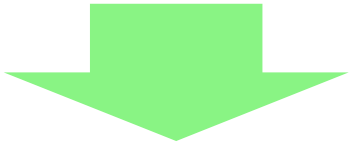
- デジタルエクスペリエンスのモニタリング機能を備える製品も



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

エンジニア不足・ナレッジ不足

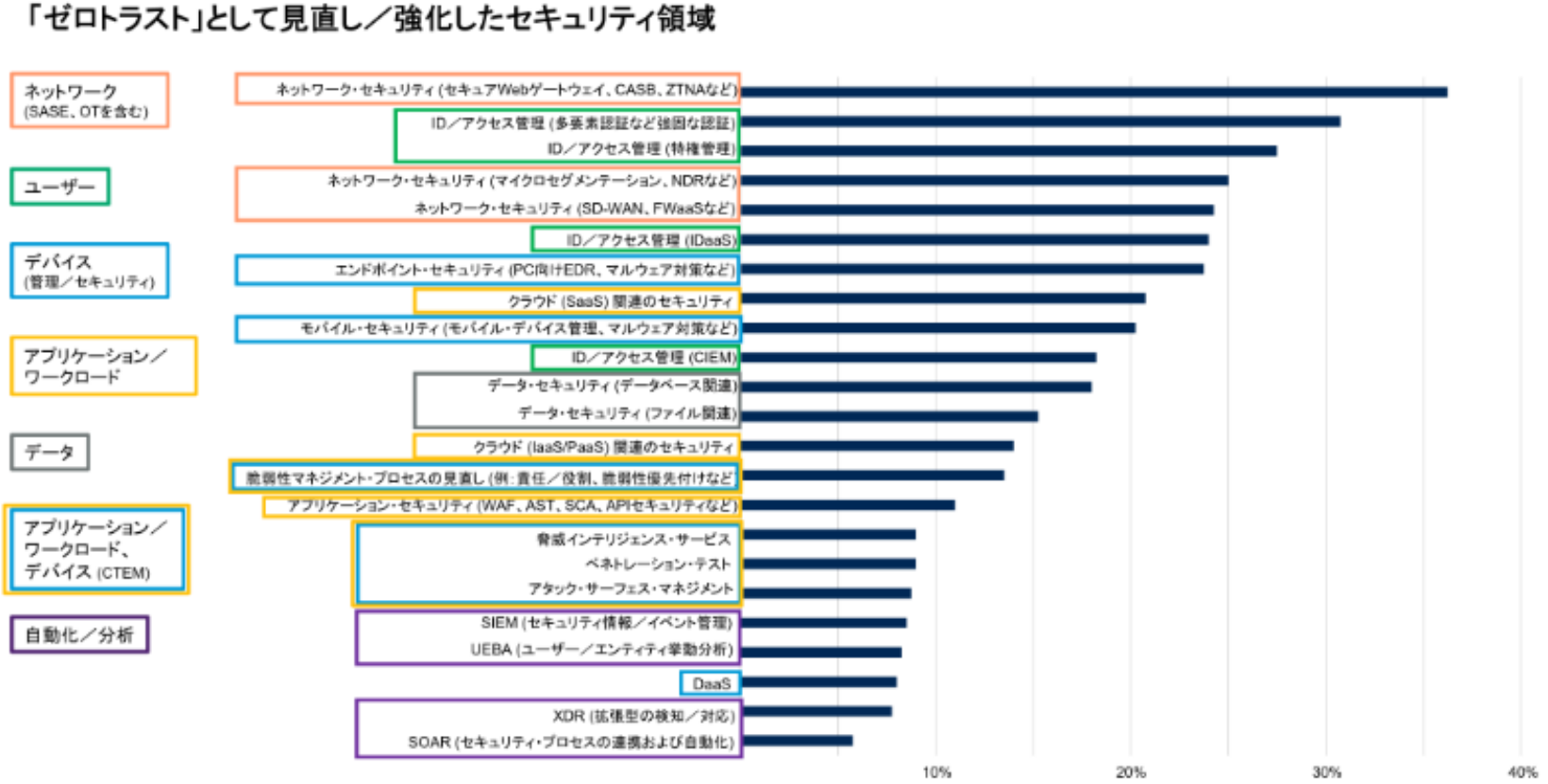
- ネットワーク・セキュリティで部門が分かれている会社では、
  どちらが対応するのかの押し付け合いや、
  予算が取れない、片方の理解が得られないなんてことも…



- ネットワークとセキュリティ、どちらにも感度の高い
  エンジニアを育てましょう、送り出しましょう
  - 例えばInternet Weekとか。

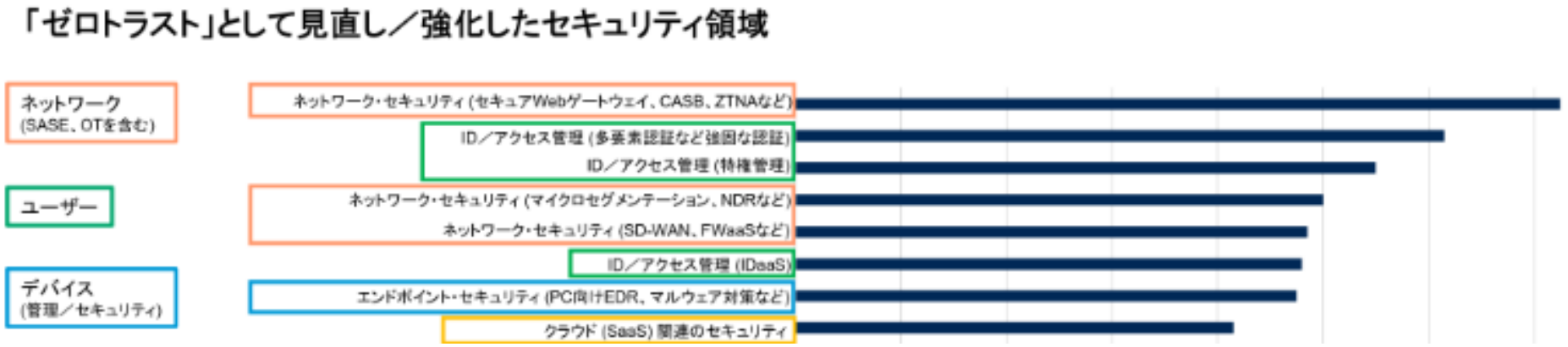
ゼロトラストの「この後」

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

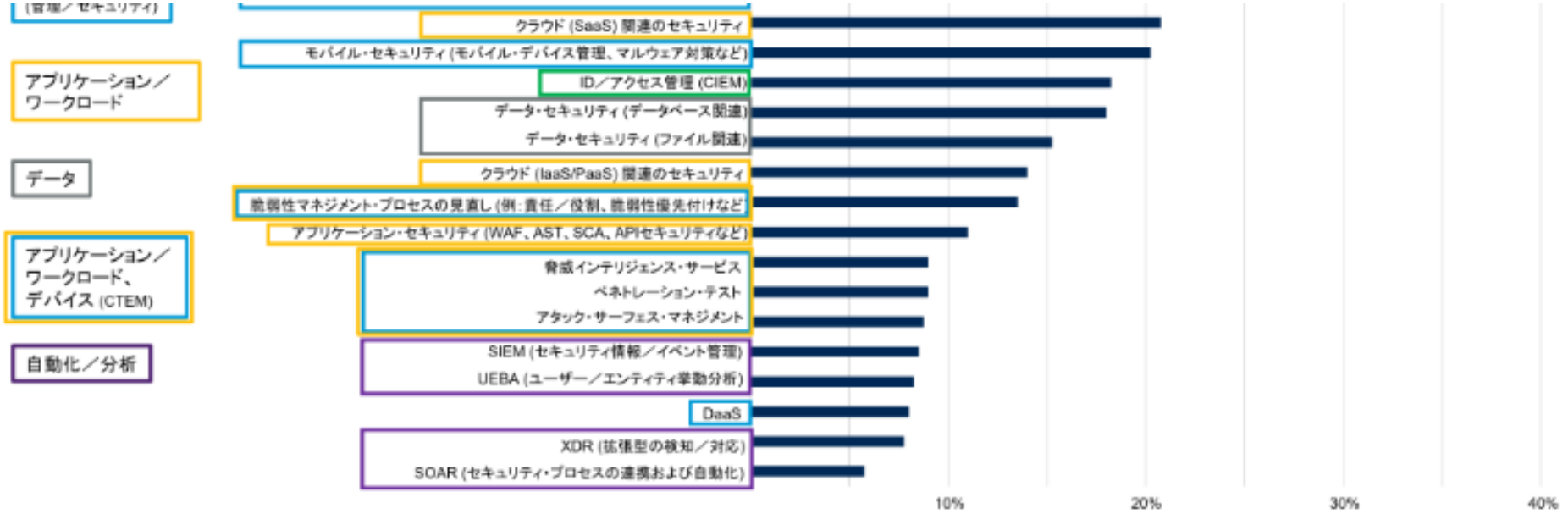
このまま進んでいくのか？



- 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

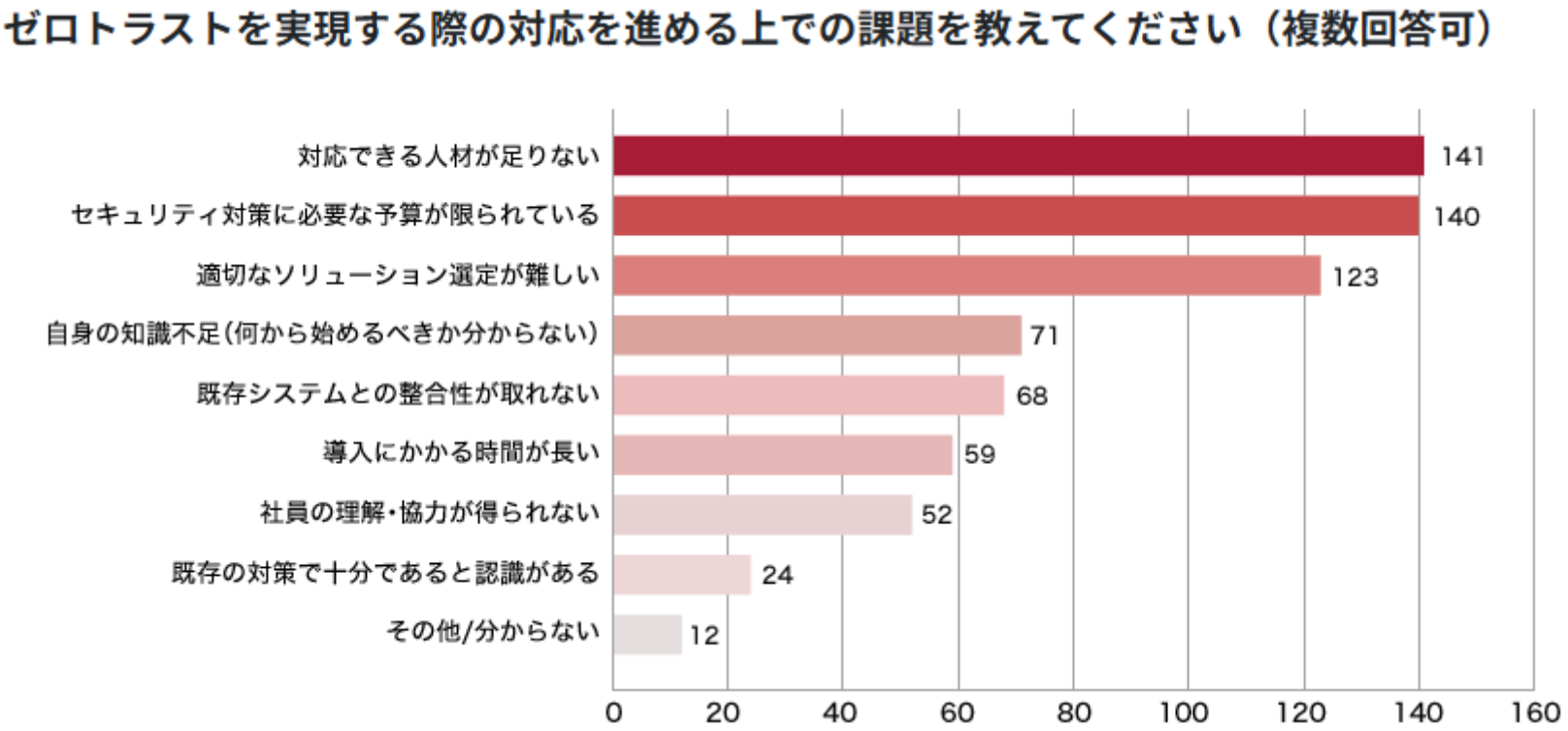
このまま進んでいくのか？



- 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



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/

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

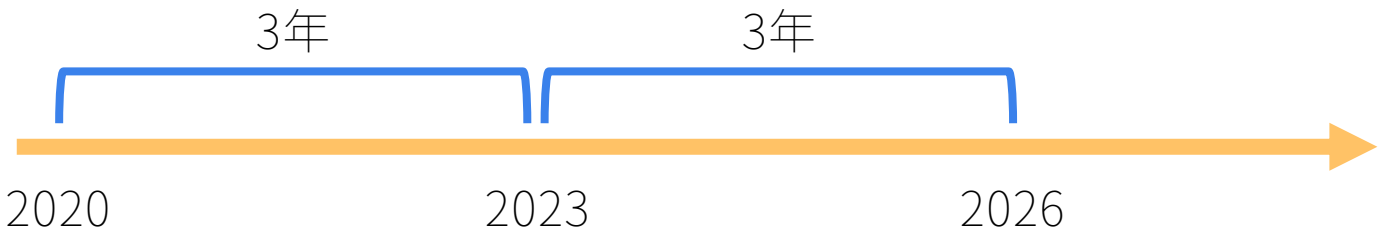
- Predicts 2025: Scaling Zero-Trust Technology and Resilience
  March 2025, Gartner社 https://www.gartner.com/en/documents/6283983

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5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

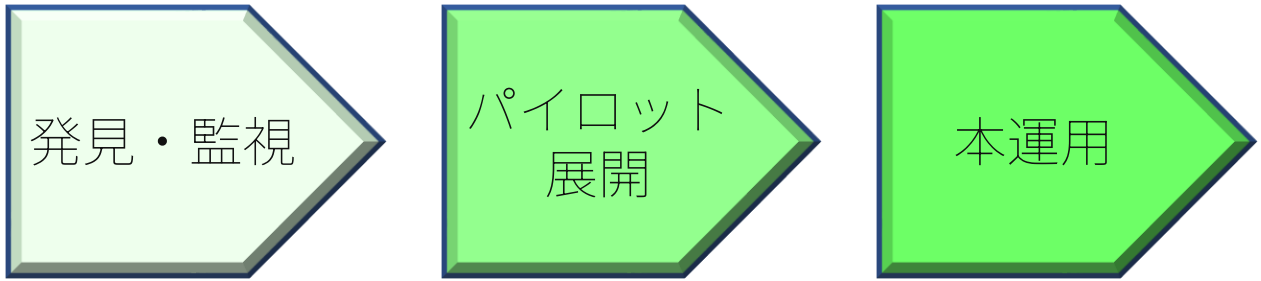
未導入だった分野のナレッジ不足

- 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、データセキュリティ(CASBやDLP)などの機能
  - 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

押さえておきたいこと
(講演にて)