SASEとIPv6 ”If not IPv6, then what?”

- IPアドレスを考えなくて良いクラウド時代にIPを考える -

24 November 2021

Miya Kohno, Distinguished Systems Engineer, Cisco Systems

Abstract

この数年間で企業において、セキュリティ制御とネットワーク制御をクラウド化する「SASE (Secure Access Service Edge)」の検討が急速に進み、テレワーク化がこれを加速しています。企業はインフラの細かい設計や運用にとらわれることなく、アプリケーションの観点から、通信トラフィックやセキュリティ戦略を最適化できるようになります。

そのような中、最近北米の運用者コミュニティ(NANOG)のメーリングリストで、「If not IPv6, what? (IPv6でないとしたら何なのか?)」という議論が起こりました。IPv6対応ユーザーがOn the Internet (インターネット上のユーザー)であるのに対し、未対応のユーザーはAccess to the Internet (インターネットにアクセスするユーザー)としてインターネットからは実質分断されてしまうであろう、という意見が印象的でした。

本セッションのテーマは、IPアドレス設計などを考えなくて良くなるクラウド・ファースト、SASE時代に、IPv6のことも考えてみよう、というものです。よりビジネス中心・アプリケーション中心にシフトしながら、将来のインターネットとの良い関係を探るための、SASE設計上の考慮点を取り上げます。

自己紹介 --- 河野 美也 Miya Kohno

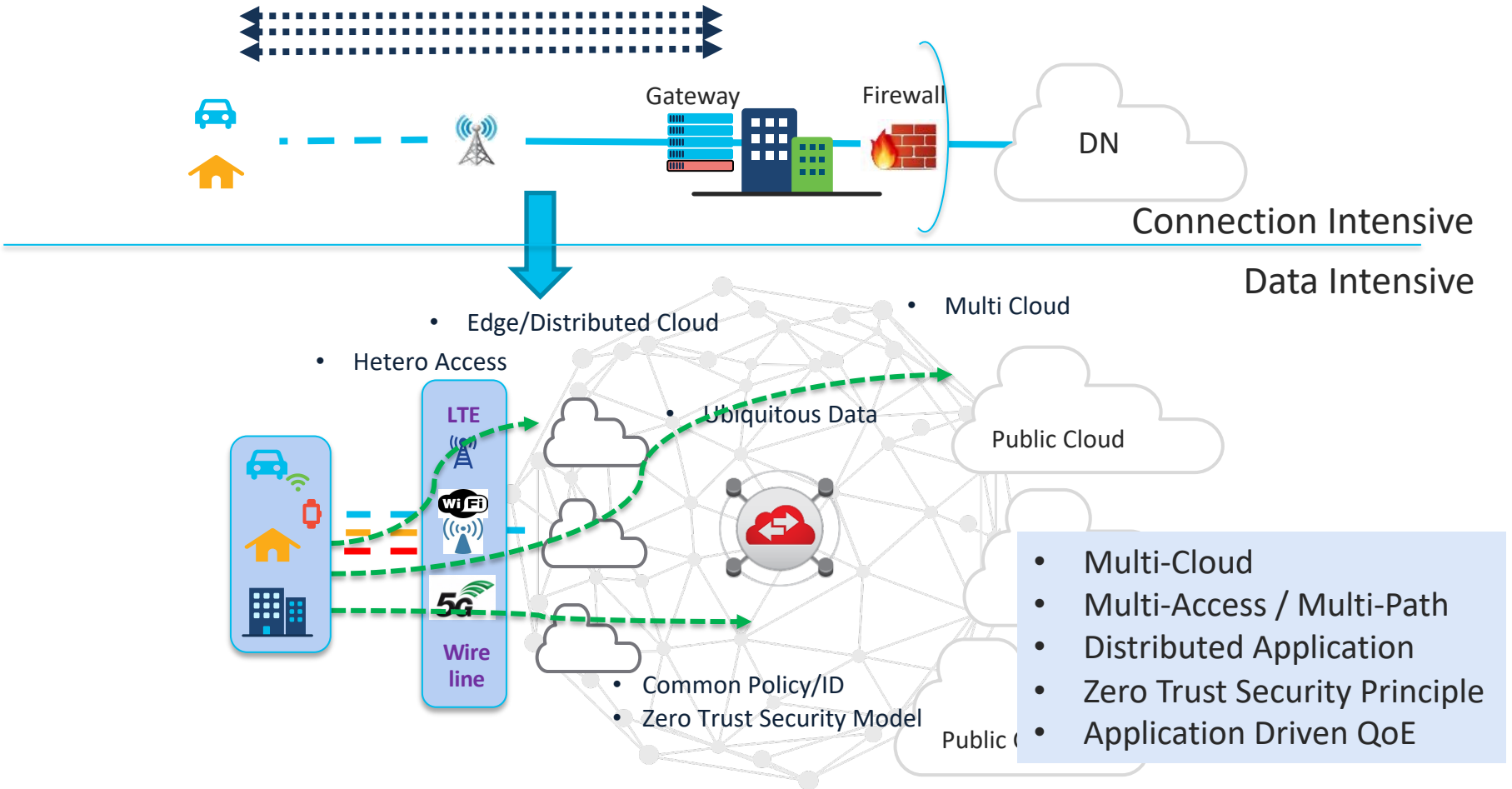
- ソフトウェア開発者 → ネットワーク技術者
- Distinguished Systems Architect @ Cisco Systems
- システム理論
  https://qiita.com/mkohno/items/ba8e207c225484814aff
- ネットワークアーキテクチャ考
  https://gblogs.cisco.com/jp/author/miyakohno/
- Twitter : mkohno
- ♬ Cellist

Team SRv6 !!

Agenda

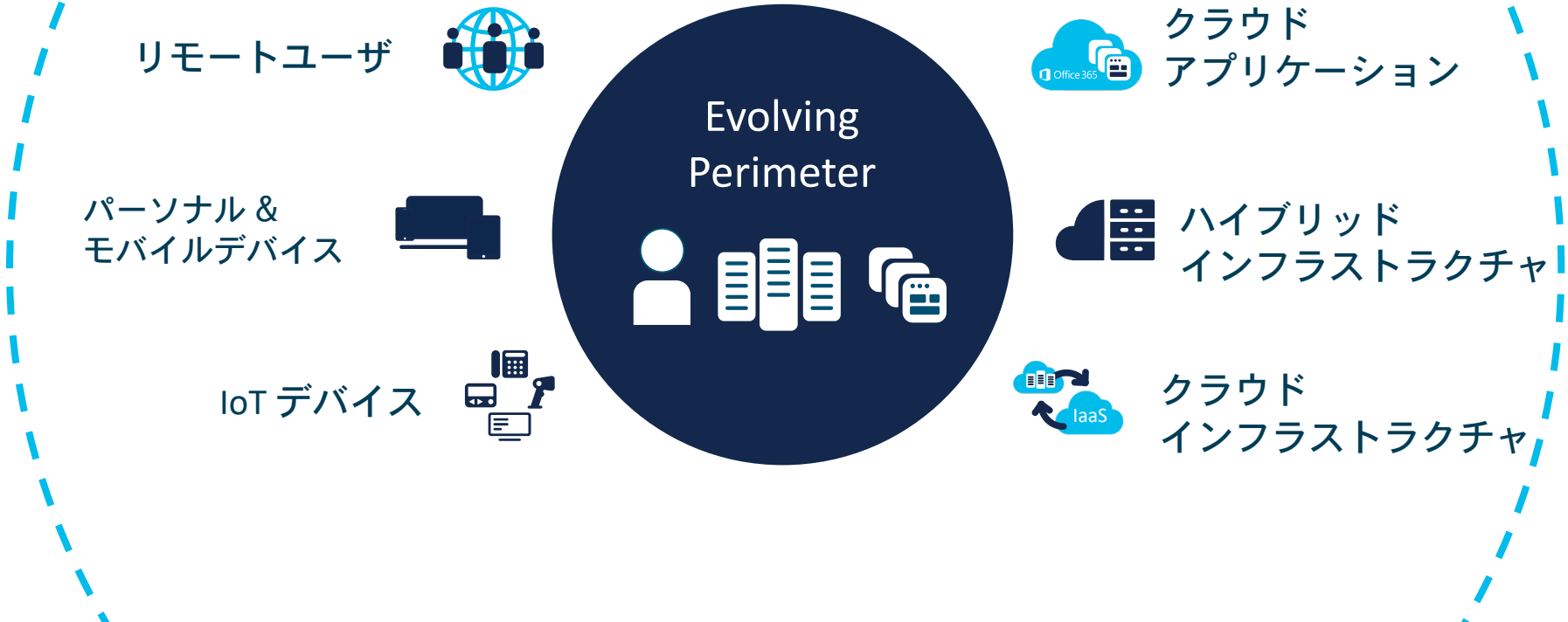
- *イマドキの企業ネットワーク*
- If not IPv6, then what? - IPv6やっぱり重要
- SASE と IPv6

Data Intensive Architecture



IT 環境の変化

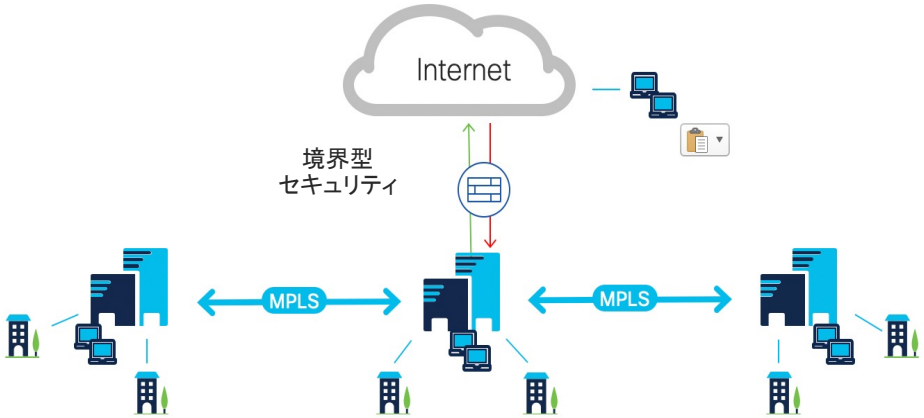
ユーザ、デバイス、アプリケーションの偏在



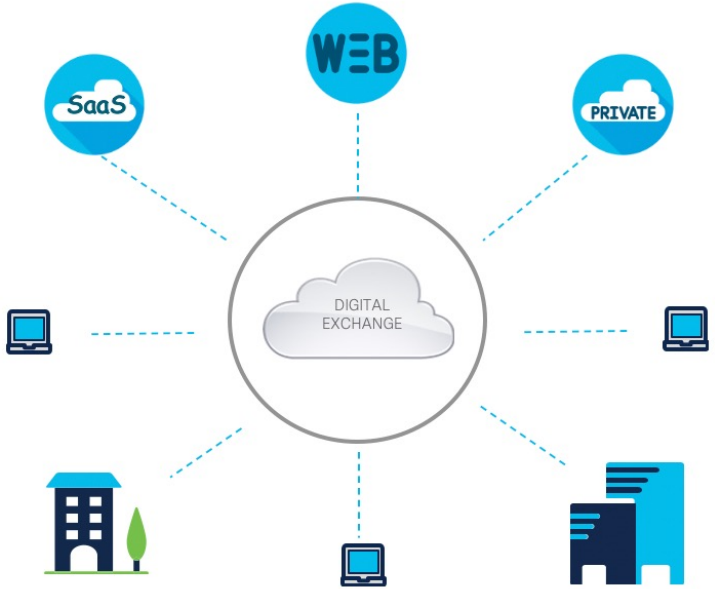
ネットワークの変革

Internet/Cloud は新たな「宇宙の中心」

DC-Centric

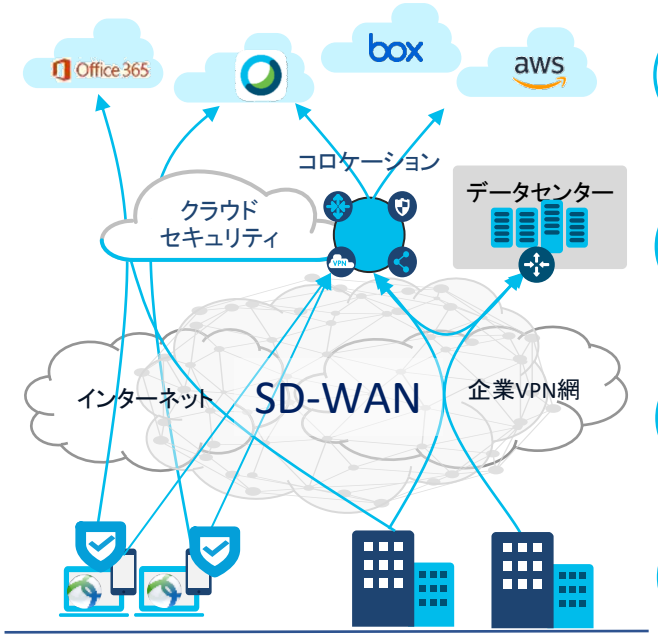


Internet/Cloud-Centric



イマドキの企業ネットワーク

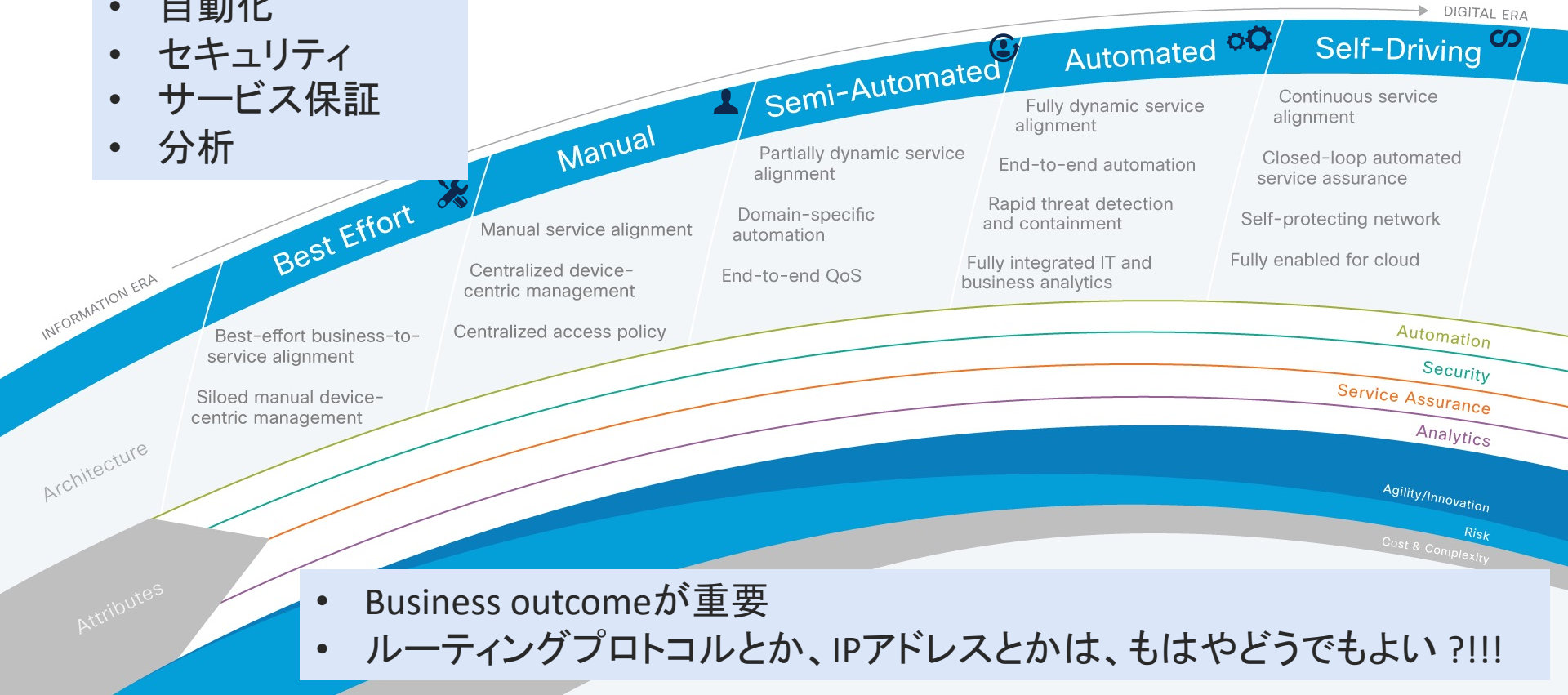
Intent Based Network Architecture



- インテントベース
- マルチアクセス
- マルチクラウド
- ゼロトラスト

Digital Readiness Model（情報時代からディジタル時代へ）

- 自動化
- セキュリティ
- サービス保証
- 分析

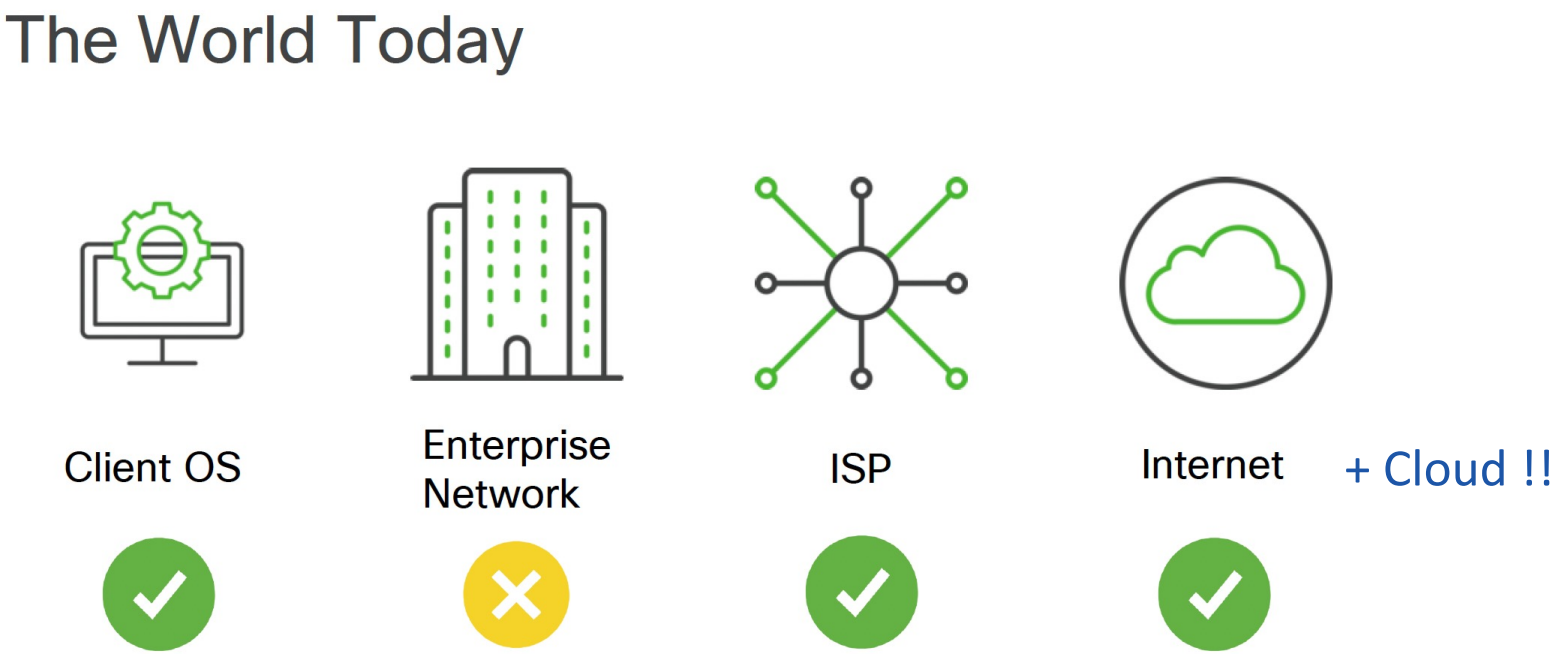


- Business outcomeが重要
- ルーティングプロトコルとか、IPアドレスとかは、もはやどうでもよい ?!!!

Agenda

- イマドキの企業ネットワーク
- *If not IPv6, then what? - IPv6 やっぱり重要*
- SASE と IPv6

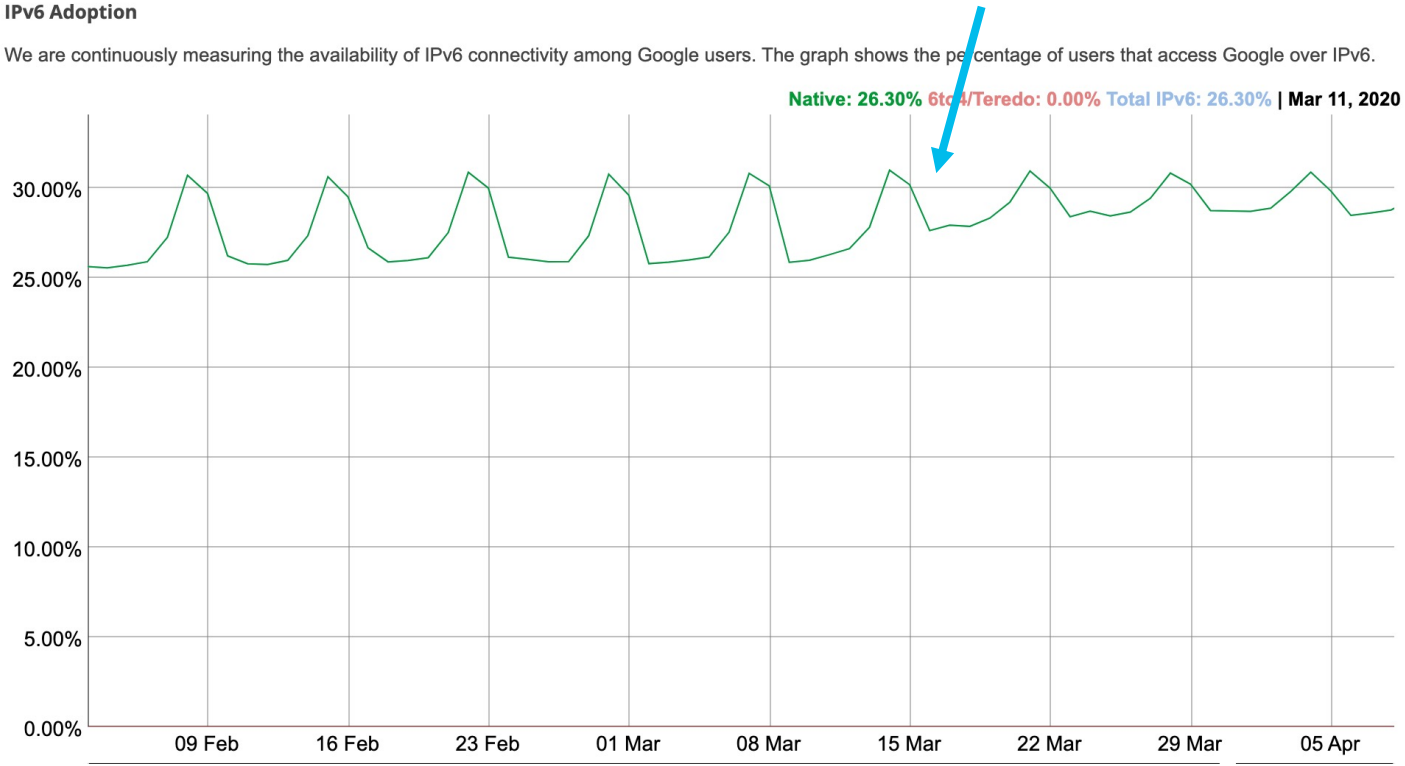
企業ネットワークにおける IPv6 導入



Source : Cisco Meraki

最近の IPv6 動向

- 企業よりも家庭でのIPv6普及が進んでいることが、Hybrid Workで顕著に示された

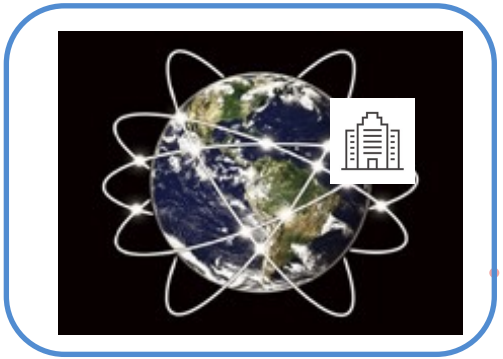


https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

If not IPv6, what? 「IPv6でなければ何なのか?」

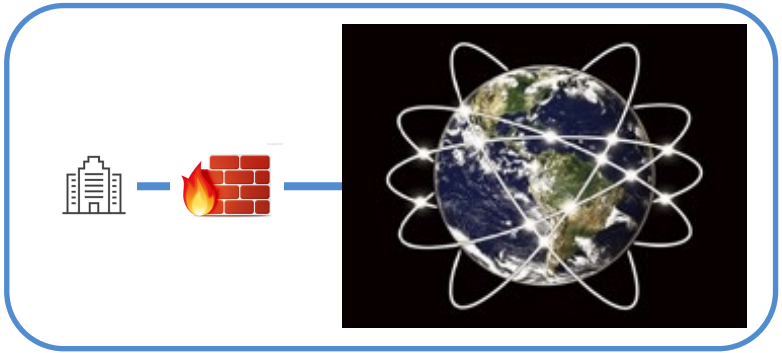
NANOG (北米ネットワークオペレータグループ) のMailing Listより (2021年9月)

We are heading into a world where Internet is going to be bifurcated with "/on/ the Internet" (with globally routed IP address(es)) or "/access/ /to/ the Internet" (with one or more layers of CGN).



OR

インターネットは、(グローバルアドレスにより)「インターネット上にいる」という状態と、(1つ以上のキャリアグレードNATの層により)「インターネットへのアクセスを持つ」という状態に二分される世界に向かっている。



https://mailman.nanog.org/pipermail/nanog/2021-September/215059.html

IPv6 やっぱり重要 – IoT普及の可能性

IoT システムの特徴

- 低消費電力エッジデバイス / 分散型エッジコンピュート
- IoT サブネットのスケーリング（数万台規模）
- 展開のしやすさ＋コスト＋規模 → 無線通信

  → デバイスのモビリティ、ドメイン内でのリナンバリングの回避
- 決定的なアドレスの存在 / 位置情報

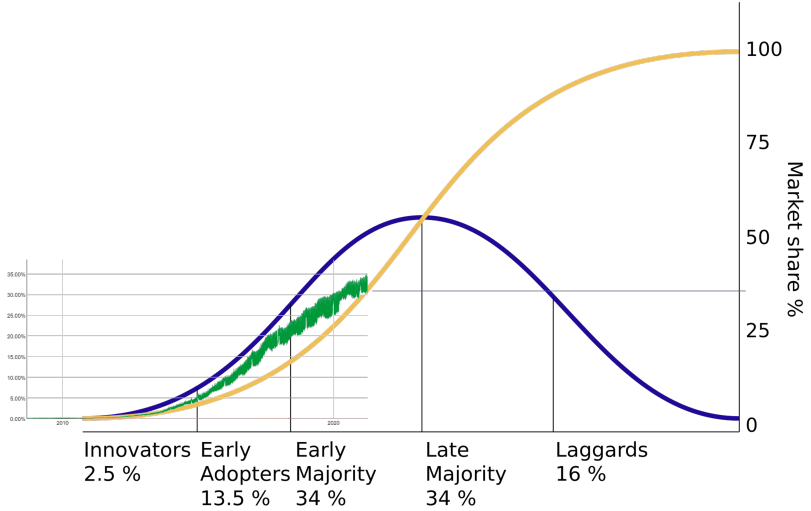
- “Don’t Forget IPv6 When Considering an SD-WAN”
  - IoT + IPv6 + SD-WAN

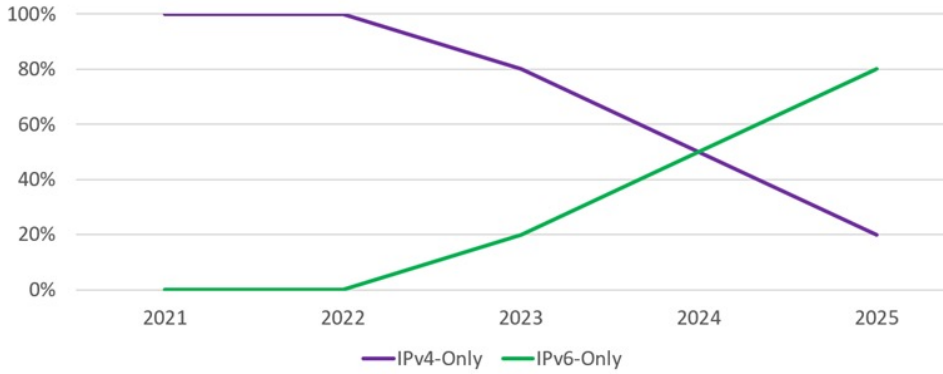
https://www.sdxcentral.com/articles/contributed/dont-forget-ipv6-when-considering-sd-wan/2017/04/

IPv6 やっぱり重要 – 長期的には IPv6-only へ

- “Dualstack where you can, Tunnel where you must” から
- “IPv6-only where you can, Dualstack where you must” へ

  目標はIPv6 の普及ではない。設計や運用、エンジニアリングの簡素化のために IPv6-only を目指すべき。

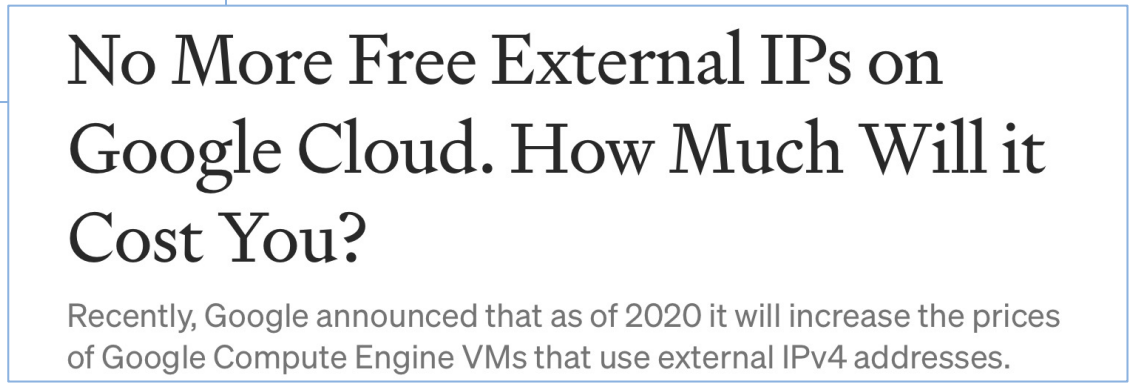




https://blogs.infoblox.com/ipv6-coe/ipv6-only-where-you-can-dual-stack-where-you-must/
https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

クラウドにおける IPv6 動向

https://d1.awsstatic.com/whitepapers/IPv6-on-AWS.pdf



https://blog.doit-intl.com/gcp-announces-no-more-free-external-ips-estimate-your-future-costs-11bd3a8193cc

クラウドにおける IPv6 動向

IPv6 導入戦略 : Motivationによって異なる

Private IPv4の不足

- IPv6-only VPCとIPv6-onlyサブネットをクラウド上のネットワークのセグメントとして作成する
- セグメント間のルーティングを設定し、IPv6-onlyノードが他のIPv6-onlyノードと通信できるようにしする
- NAT64やデュアルスタックロードバランサーなど、IPv6とIPv4の相互運用レイヤーを提供する

Public IPv4の不足

- デュアルスタックのVPCとサブネットを作成する（ロードバランサーやエッジサービスなどのサービスをデュアルスタックモードで設定し、対応するDNSレコードをクラウド上に作成する）
- オプションとして、専用のIPv4-onlyまたはIPv6-onlyのデプロイメントにおいて、IPv4とIPv6用に別々のエンドポイントを提供する

IPv6-only NWとの相互接続

- デュアルスタックVPCを作成し、それらを使ってNAT46の 相互運用レイヤをホストする（完全なデュアルスタックの採用は現実的ではない場合が多いので、相互運用性のあるレイヤを提供することが望ましい）

IPv6 endpointを必須要件に

- 「Public IPv4の不足」と同等

Source - https://d1.awsstatic.com/whitepapers/IPv6-on-AWS.pdf

クラウドにおける IPv6 動向

モード

- IPv4 only mode
  IPv4で通信できるが、IPv6ノードと通信する場合は、相互運用性レイヤが必要
- IPv6 only mode
  IPv6で通信できるが、IPv4ノードと通信する場合は、相互運用性レイヤが必要
- Dual Stack mode
  IPv4とIPv6の両方で通信可能。相互運用性レイヤの必要なし

アドレス割り当て

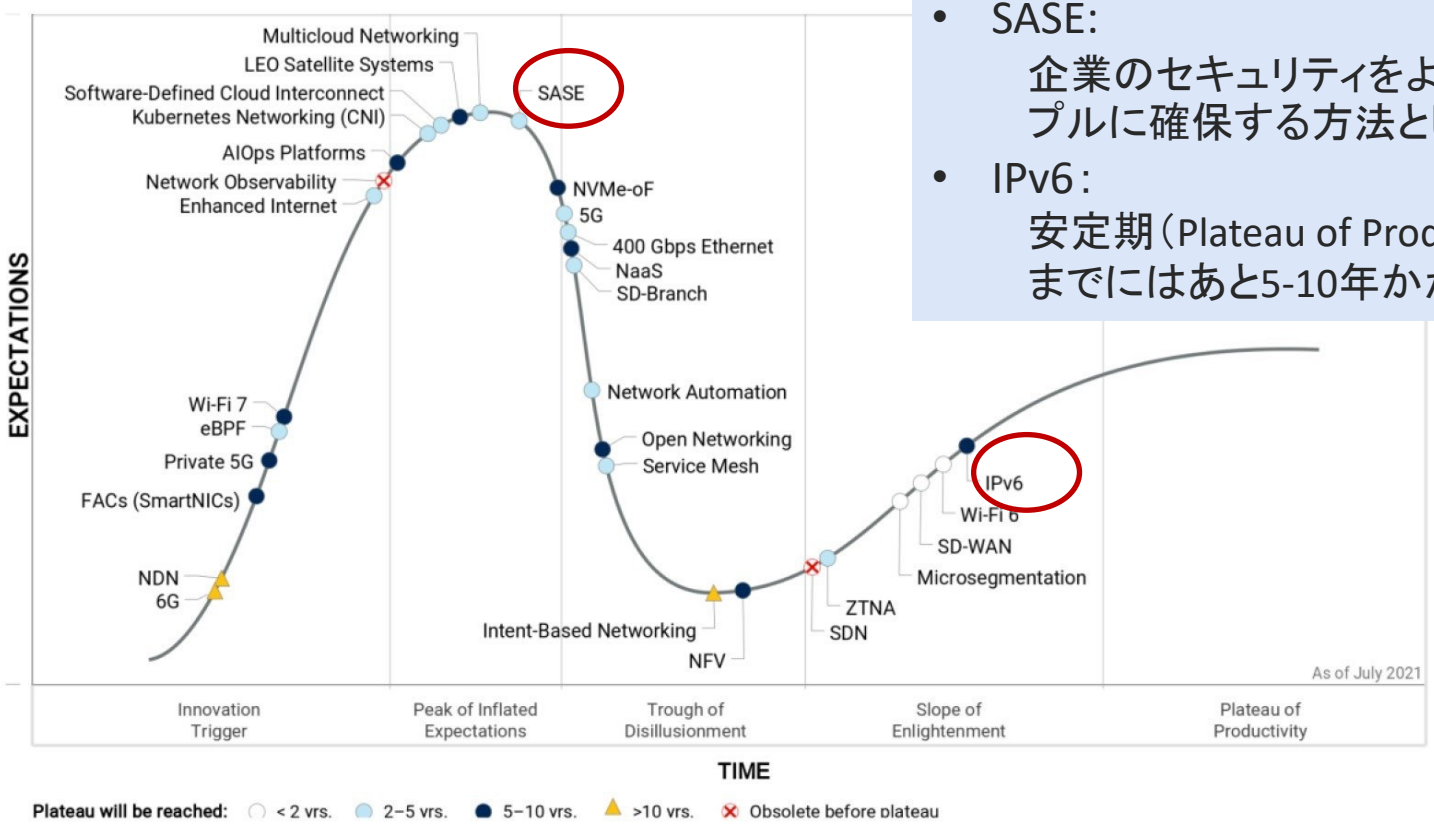
- Cloud
  クラウドが持つアドレスブロックから割り当てる
- BYOIPv6 (Bring your own IPv6)
  企業側が取得したアドレスブロックから割り当てる

Source - https://d1.awsstatic.com/whitepapers/IPv6-on-AWS.pdf

Agenda

- イマドキの企業ネットワーク
- If not IPv6, then what? - IPv6やっぱり重要
- *SASE とIPv6*

Gartner Hype Curve – 企業ネットワーキング



- SASE:
  企業のセキュリティをより迅速かつシンプルに確保する方法として期待大
- IPv6:
  安定期（Plateau of Productivity）に至るまでにはあと5-10年かかる

https://regmedia.co.uk/2021/07/15/screenshot_gartner_hype_cycle_for_enterprise_networking_2021.jpg

これまでの IPv6 導入ガイドライン

RFC7381 (Oct. 2014)
「企業IPv6導入ガイドライン」

準備と調査

External Phase

Internal Phase

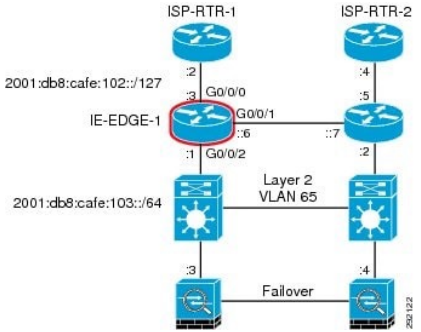
IPv6-only

Deploying IPv6 in the Internet Edge (Dec. 2011)
「インターネットエッジにおけるIPv6導入」

Core to Edge

Edge to Core

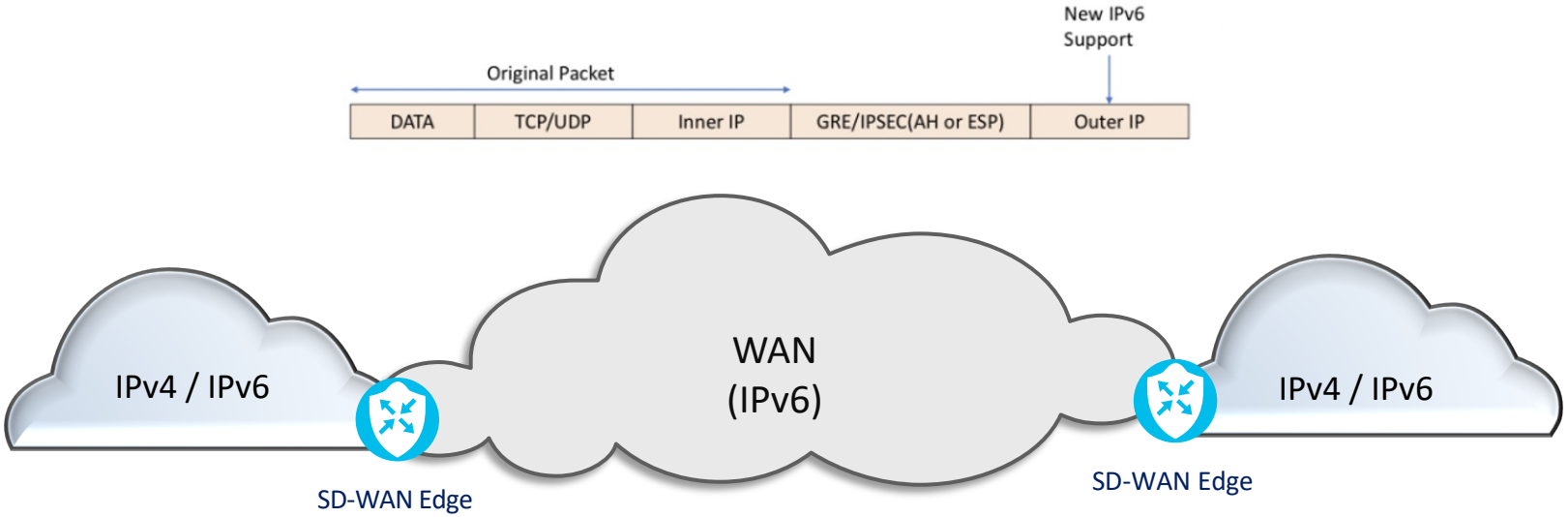
Internet Edge Only



https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Internet_Edge/InternetEdgeIPv6.html

SD-WAN + IPv6 underlay

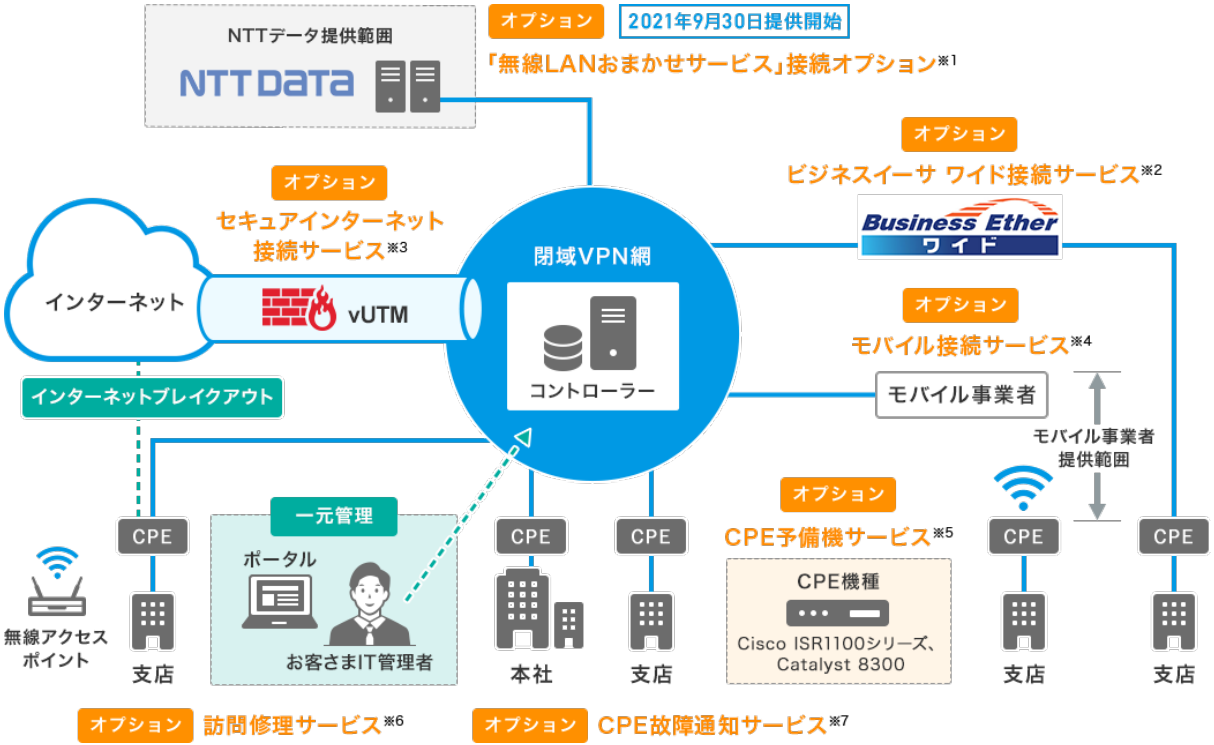
- GREまたはIPSecをサポート



- NAT traversalの問題なし
- Agile, Simple !

SD-WAN + IPv6 underlay 事例

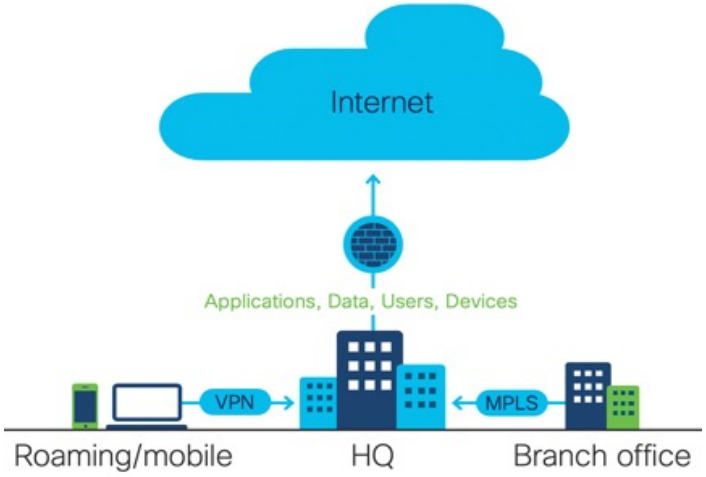
NTT東日本 Managed SD-WAN サービス



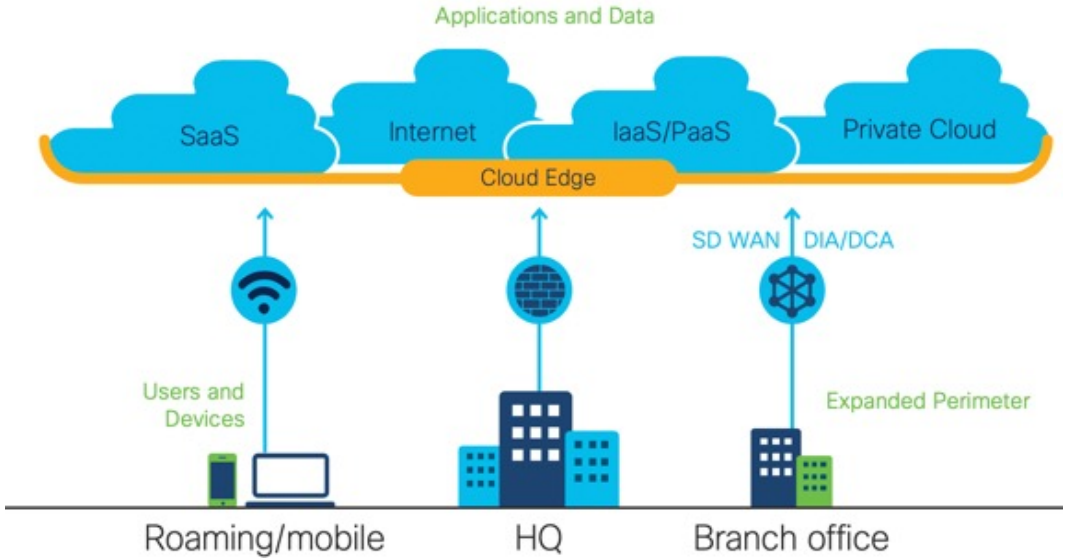
https://business.ntt-east.co.jp/service/sd-wan/

そしてSASE

Connect it + Secure it



企業に割当てられたIPv6(PI)アドレス



プロバイダーAから割当てられたIPv6(PA)アドレス

NAT66!

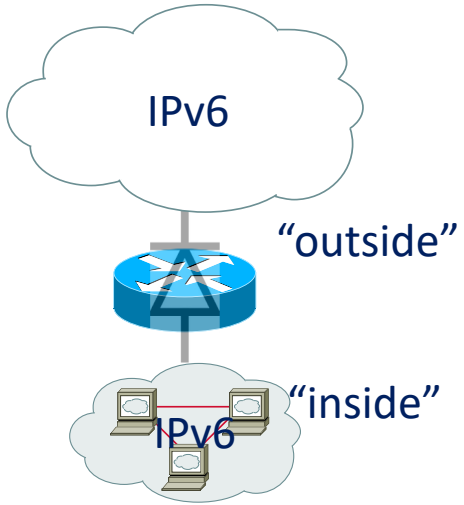
プロバイダーBから割当てられたIPv6(PA)アドレス

企業に割当てられたIPv6(PI)アドレス

PI : Provider Independent
PA : Provider Aggregatable

NAT66

- RFC 6296 - IPv6-to-IPv6 Network Prefix Translation
  - RFC 2993 - Architectural Implications of NAT では非推奨だったが必要性に応じるために、できるだけ害の少ない方法を標準化
  - アドレスの独立性(Address independence)を提供
  - 内部から外部へのみセッションを開始する
  - Firewall とは異なる



ゼロトラストアーキテクチャ(ZTA)と IPv6

“By providing end-to-end network paths and better support of microsegmentation, the transition to IPv6 only is going to be a key component of ZTA—zero trust architecture—which is one of the key pillars in the executive order”

-- Deputy Federal Chief Information Officer Maria Roat

「エンド・ツー・エンドのネットワークパスを提供し、マイクロセグメンテーションをより良くサポートすることにより、IPv6-onlyへの移行は、大統領令の重要な柱の一つであるZTA（ゼロ・トラスト・アーキテクチャ）の重要な構成要素となる」

--連邦政府副最高情報責任者 Maria Roat氏

https://www.nextgov.com/cybersecurity/2021/06/officials-federal-shift-ipv6-brings-new-cybersecurity-options-and-risks/174781/

ゼロトラストアーキテクチャの必要性

デジタル化を取り巻く環境の変化

サイバーセキュリティの課題

在宅勤務で
サイバー攻撃が
600%に急上昇*1

実際のインシデントの**50%**が
放置されている*2

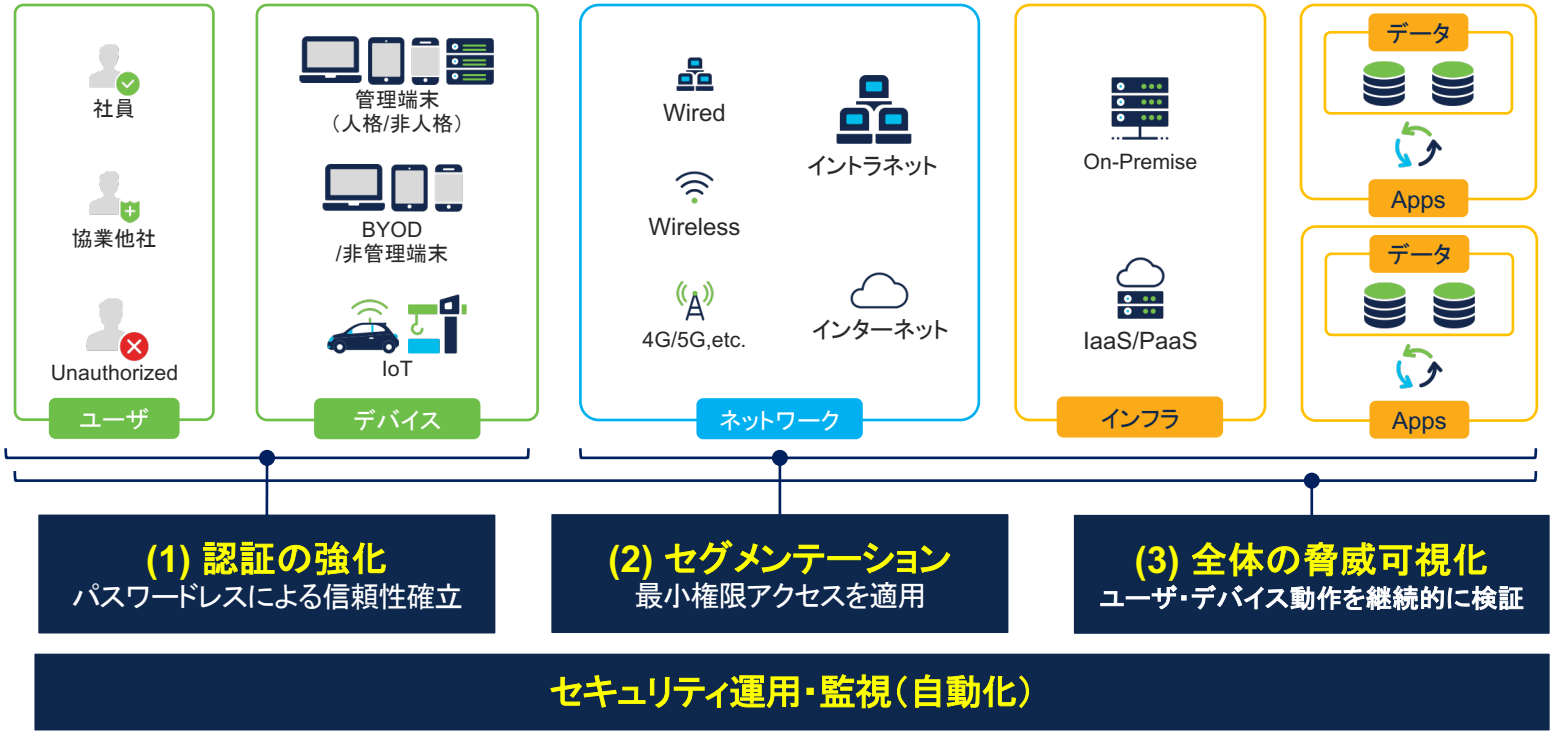
多要素認証(MFA)を
使用している組織
は **27%** に過ぎない
*2

不正侵入の**81%**以
上はID/パスワード
の漏洩や弱いパス
ワードが原因*3

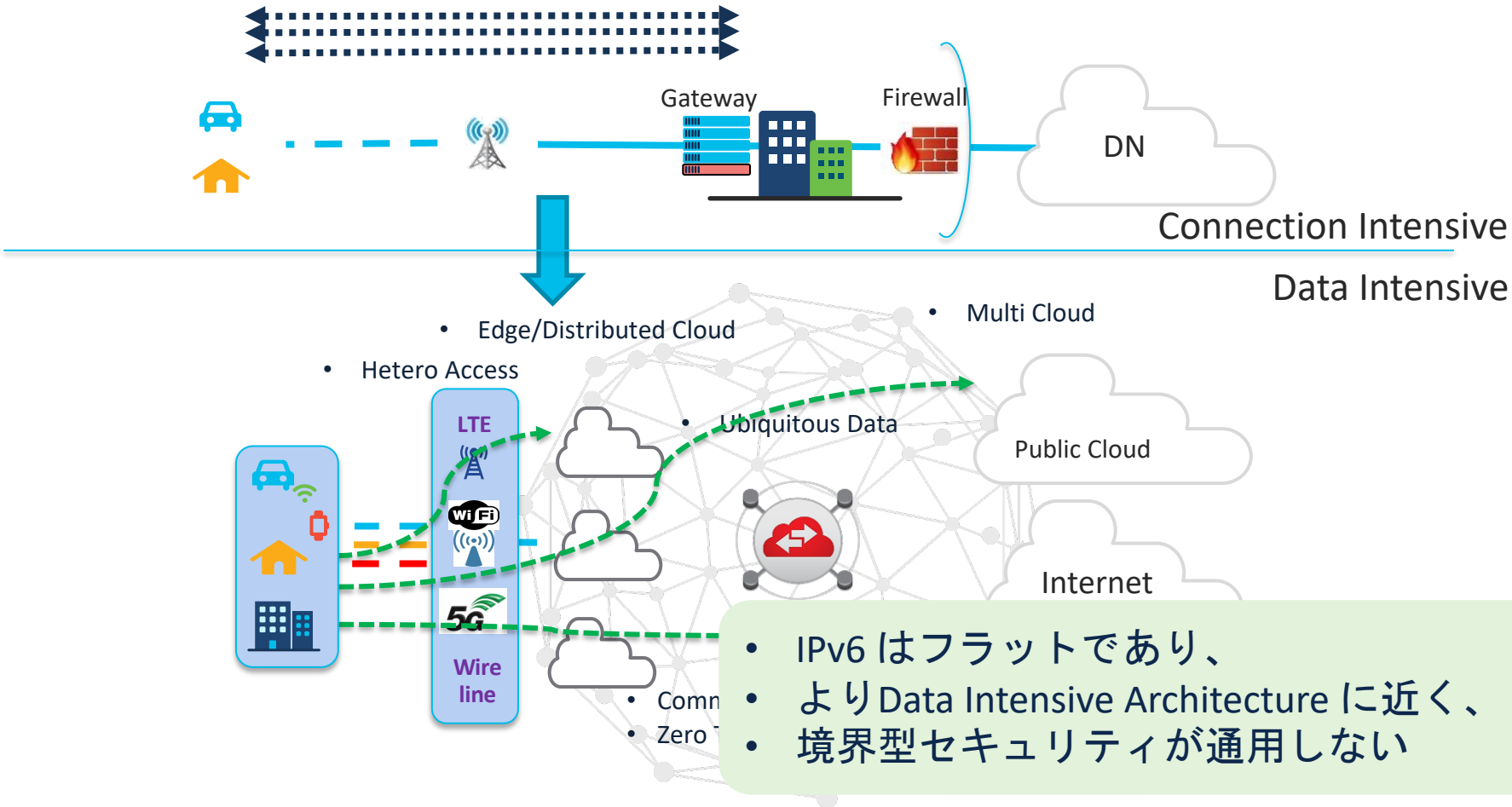
*1: Scott Galloway; MacAfee Report; Cisco; Zoom; Press Search; Cisco Analysis
*2:シスコ サイバーセキュリティ レポート シリーズ 2020
*3: Verizon Data Breach Report

ゼロトラストプラットフォームとは

誰もが、どこからでも、安全、便利、快適にネットワークにつながるために、認証強化、セグメンテーション、全体の脅威可視化、そして運用・監視の自動化を提供する



IPv6 と Data Intensive Architecture と ZTA



まとめ

- 現在の企業ネットワーク設計は、Outcome First, Cloud First が基本となり、ルーティングプロトコルや IP アドレスなどのことは考えなくても良い時代とも言える
- しかし、インターネットへの接続性に制限を持たせないために、また、将来性やシンプルさ、そしてディジタル時代のIoTアプリケーションのために、IPv6は重要である
- SD-WANやSASEは、これまでの境界(Perimeter)の概念を覆し、システム設計とセキュリティ設計を効率化、シンプル化する
- ゼロトラストアーキテクチャ(ZTA)を包含したSASEは、IPv6と親和性が高い
- クラウド時代にこそ、“Security by Design” と共に “IPv6 by Design” を実践したい


CISCO