資料１-5

インターネットトラヒック研究会
～「新たな日常」におけるインターネットの品質確保に向けて～
説明資料

2020/12/1

アカマイ・テクノロジーズ合同会社
メディア プロダクト マネジメント部
シニア プロダクト マネージャー
伊藤 崇

マーケティング本部
シニア プロダクト マーケティング マネージャー
金子　春信（CCIE/CISSP）

アカマイの成り立ち

1995年： ティム・バーナーズ＝リー氏がインターネットの課題をMITで提唱
1996年： MIT 応用数学の教授 トム・レイトン(弊社CEO)がチームを編成
1997年：研究成果である効率的分散キャッシュ構成法を元に
MIT ビジネスコンテスト入賞
1998年： Akamai Technologies 設立

Massachusetts Institute of Technology

Akamai Edge プラットフォーム

325,000	1,500	4,100	136	1,000
サーバー	ネットワーク	ロケーション	国	都市

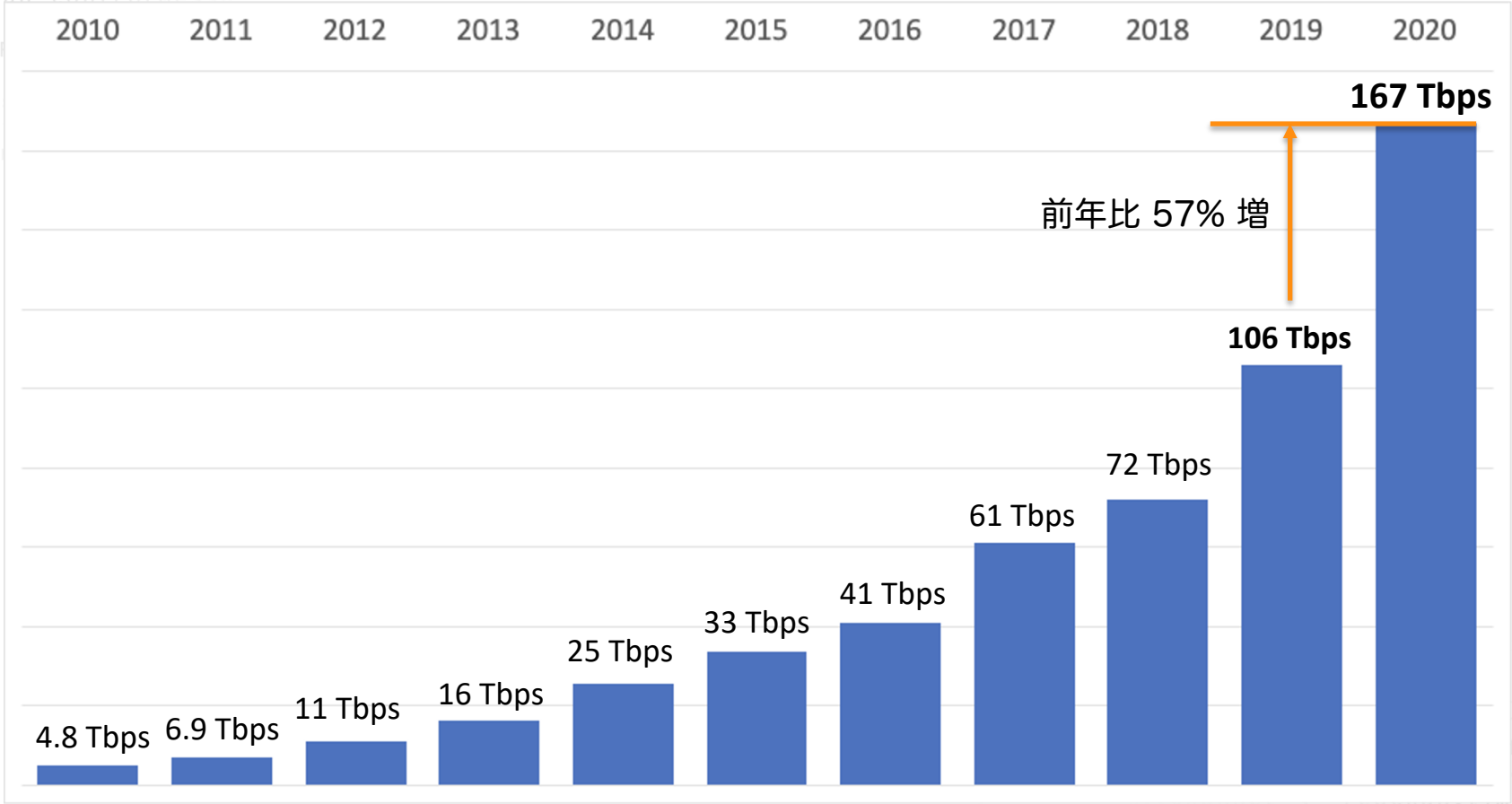
日々加速するトラフィック

1 秒あたり 5,600 万件のヒット数
1 日あたり 3 兆件以上の配信
1 秒あたり 120 テラビット以上

世界の主要ブランドからの信頼

Fortune 500 企業の半数以上
世界の大手 OTT サービス 68 社
ゲーム業界の上場グローバル企業トップ 25 社全て
グローバル通信事業者トップ 50 社すべて
世界各地の 500 を超える銀行

アカマイ上でのピークトラフィックの推移 (グローバル)



インターネット品質確保に向けた取り組み

1、分散配信による、ISP・キャリア間のトラフィック軽減と大規模配信の実現

参考資料

・2018/03/27 放送コンテンツの製作・流通の促進等に関する検討委員会（第12回）

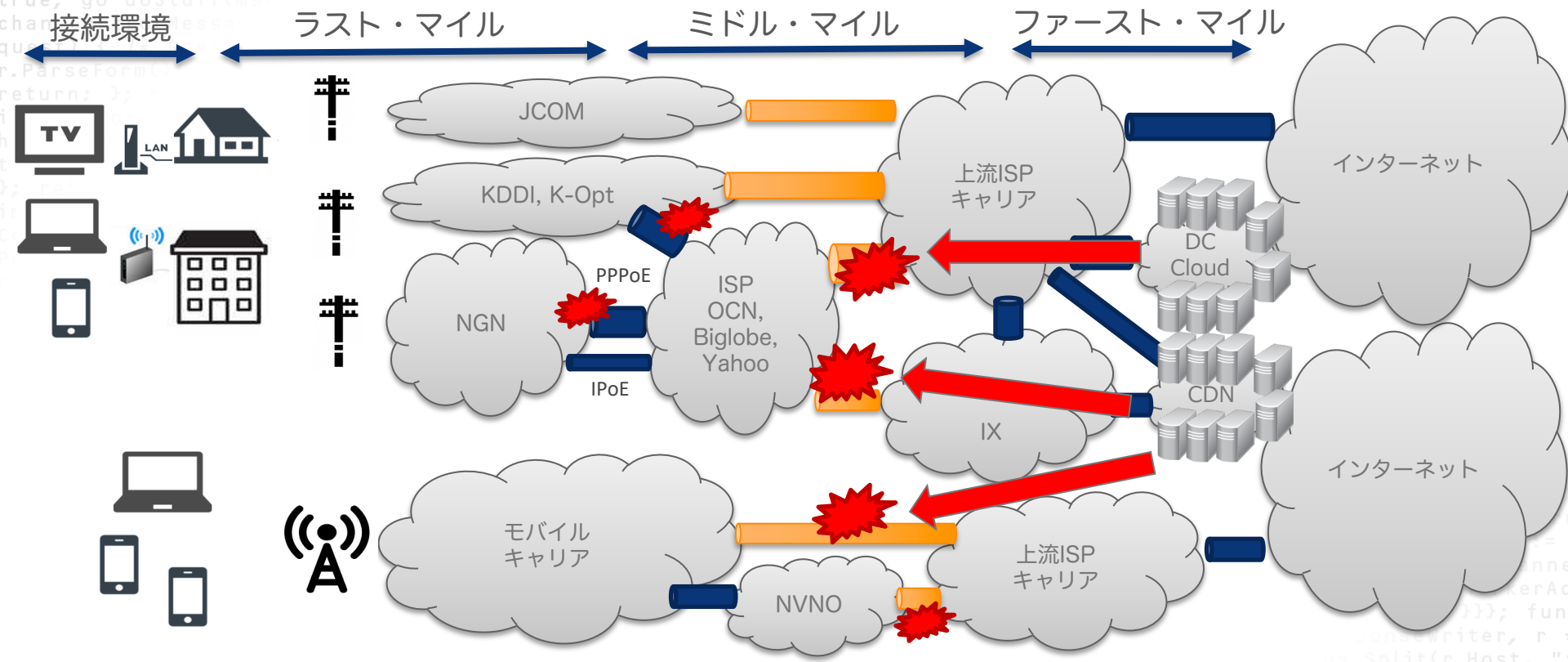
https://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/bunkakai/02ryutsu04_04000130.html

・2018/12/19 ネットワーク中立性に関する研究会（第5回）

https://www.soumu.go.jp/main_sosiki/kenkyu/network_churitsu/02kiban04_04000240.html

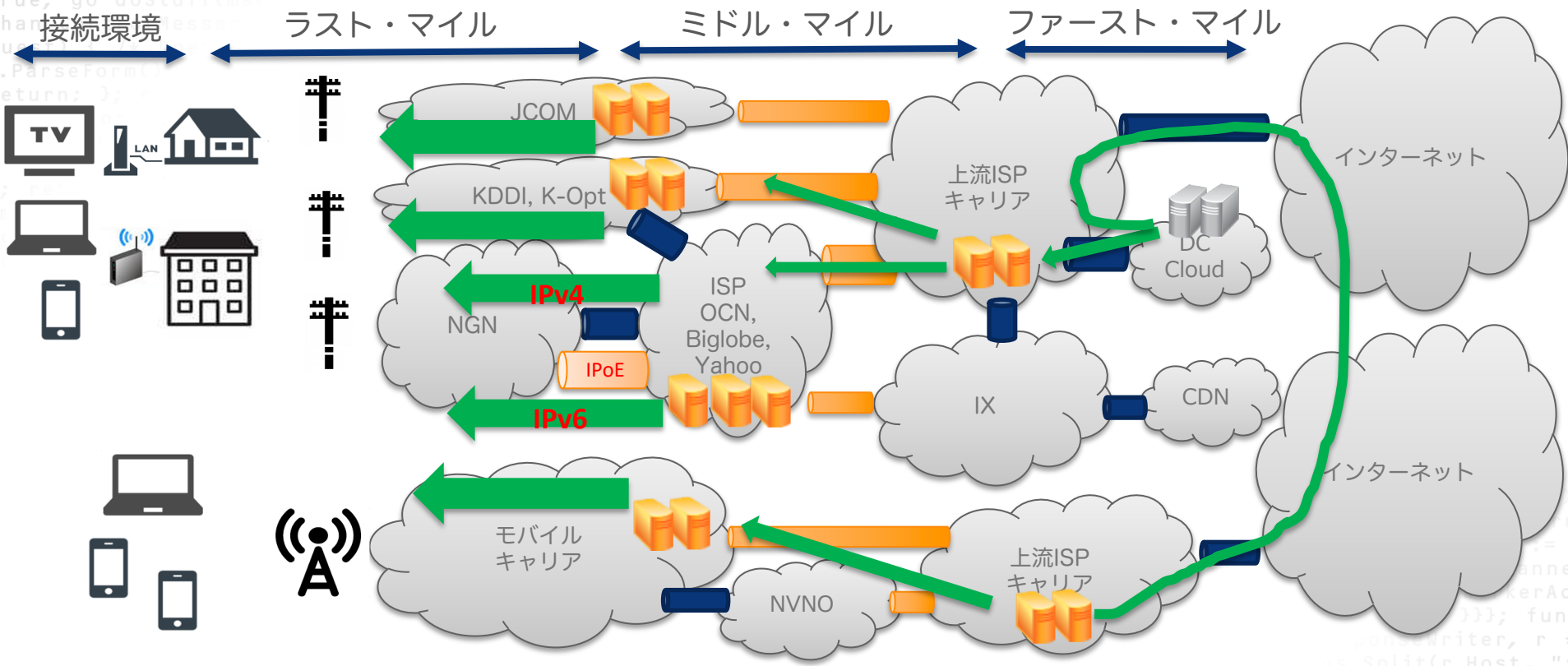
2、在宅勤務における、業務用インターネット通信品質向上

トラフィック増の課題 (混雑するポイント)



トラフィックが増大し、配信元サーバーがネットワークの上流にある場合、ミドルマイルでの混雑が発生し、また近年では、ラストマイルとの接続ポイントでも混雑が頻繁に発生している

アカマイの取組み (分散配信 + IPv4 IPv6 配信)



ネットワーク下流からの分散配信と、IPv4 v6 の両方式を使って配信を行うことで、
ミドルマイルと、アクセス網への混在を回避し、大規模配信を実現

緊急事態宣言に伴う在宅勤務急増で見えた課題

企業の課題
※本日の議題

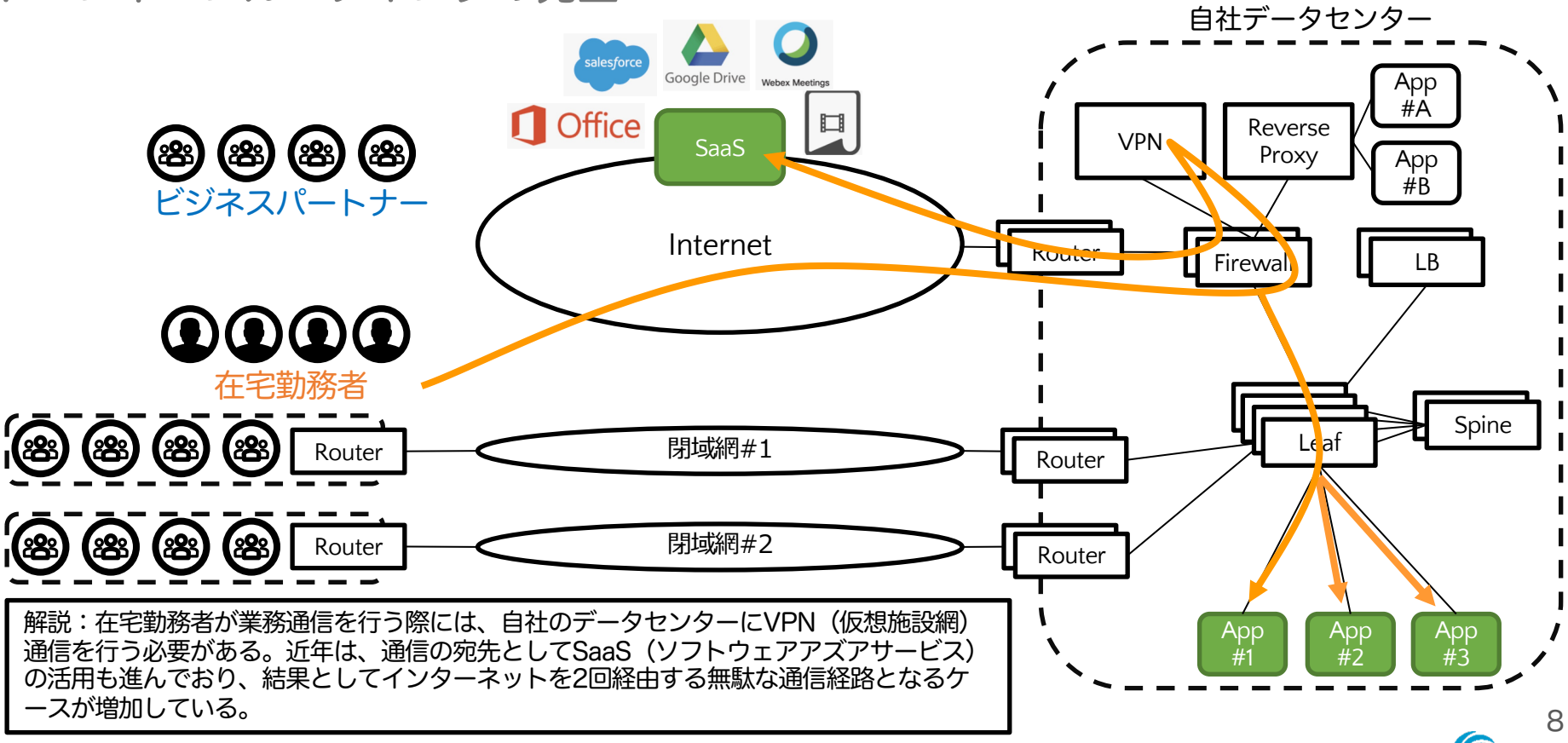
- インターネット回線輻輳
- VPN機器処理能力不足（又はライセンス不足）
- 高度化するサイバー攻撃への対策

サービス提供者の課題
※参考※

- リモートアクセスサービス基盤ひっ迫
  - サービス利用急増による接続困難
  - セキュリティ問題からのサービス終了

在宅勤務者の通信非効率化の課題

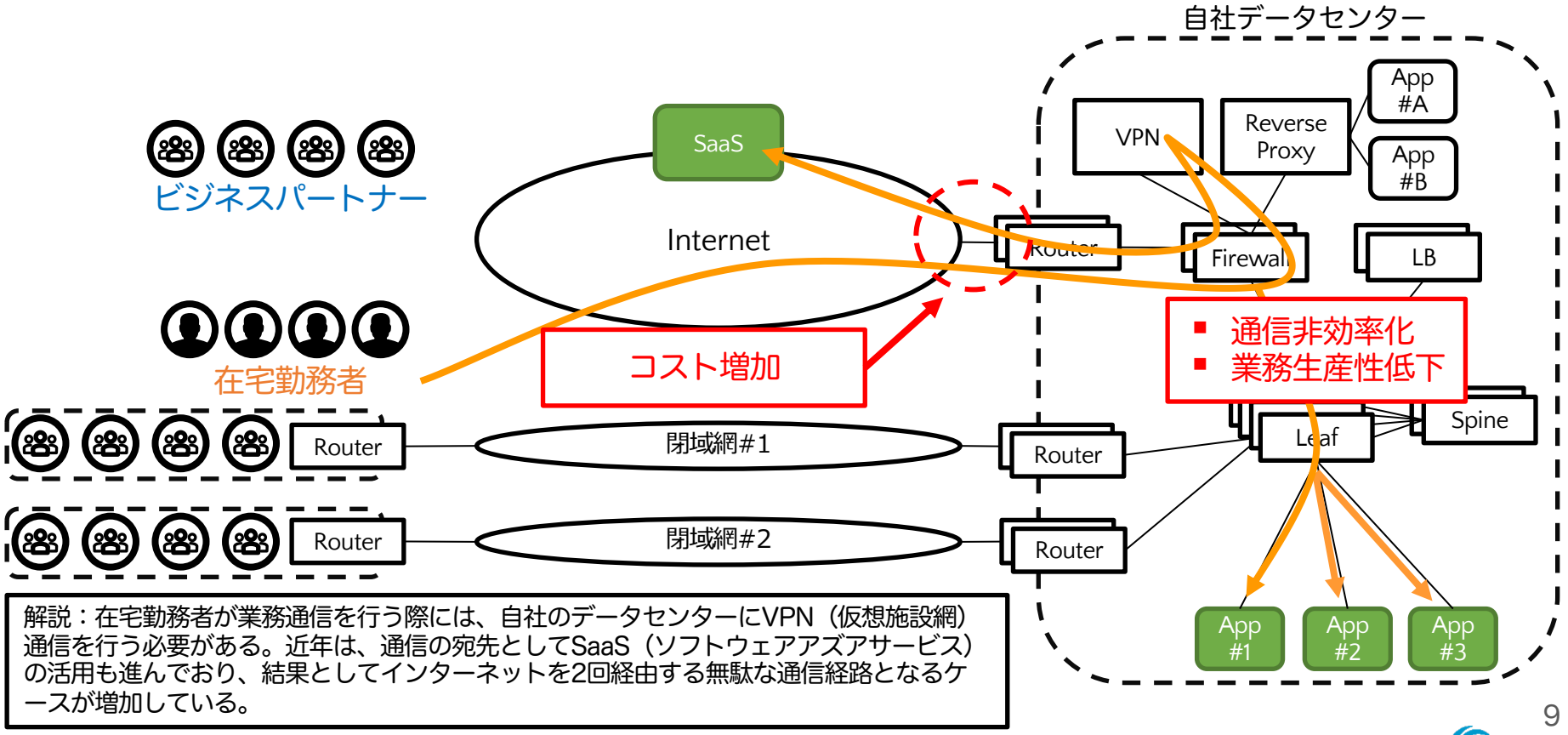
トロンボーンルーティングの発生



解説：在宅勤務者が業務通信を行う際には、自社のデータセンターにVPN（仮想施設網）通信を行う必要がある。近年は、通信の宛先としてSaaS（ソフトウェアアズアサービス）の活用も進んでおり、結果としてインターネットを2回経由する無駄な通信経路となるケースが増加している。

在宅勤務者の通信非効率化の課題

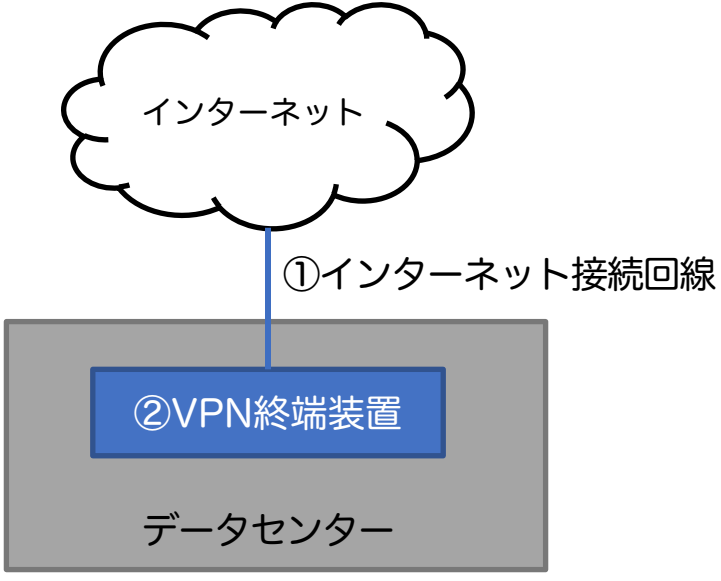
トロンボーンルーティングの発生



解説：在宅勤務者が業務通信を行う際には、自社のデータセンターにVPN（仮想施設網）通信を行う必要がある。近年は、通信の宛先としてSaaS（ソフトウェアアズアサービス）の活用も進んでおり、結果としてインターネットを2回経由する無駄な通信経路となるケースが増加している。

インターネット回線とVPN終端装置

双方に考慮が必要



①インターネット接続回線

- 通信事業者との帯域増強契約
- 新規回線引き込み工事

②VPN終端装置

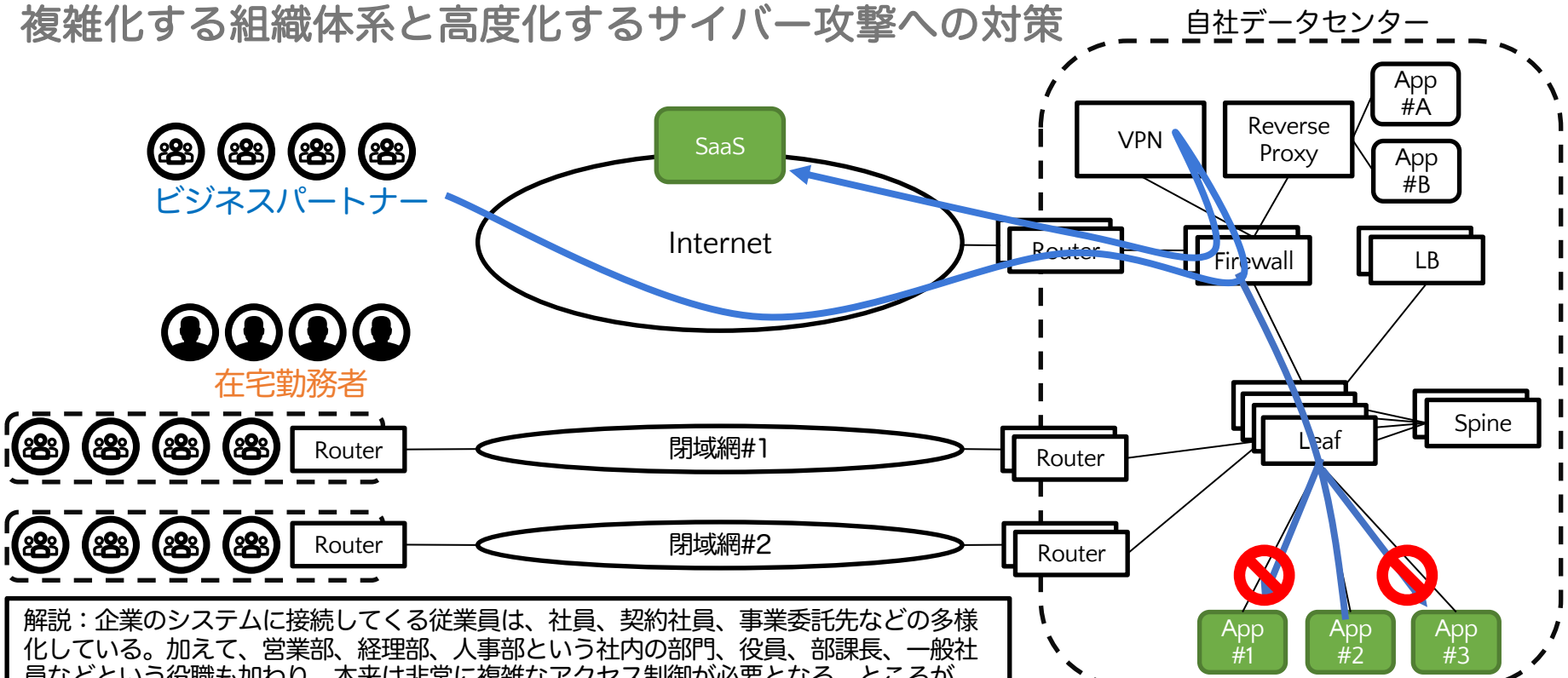
- 接続ライセンス追加購入
- 装置の買い替え
- 装置の買い足し

いずれも時間と予算がかかる

※緊急事態宣言下では、機器の不足により調達期間も長期化。その間の事業継続性が脅かされた。

アクセス制御の課題

複雑化する組織体系と高度化するサイバー攻撃への対策



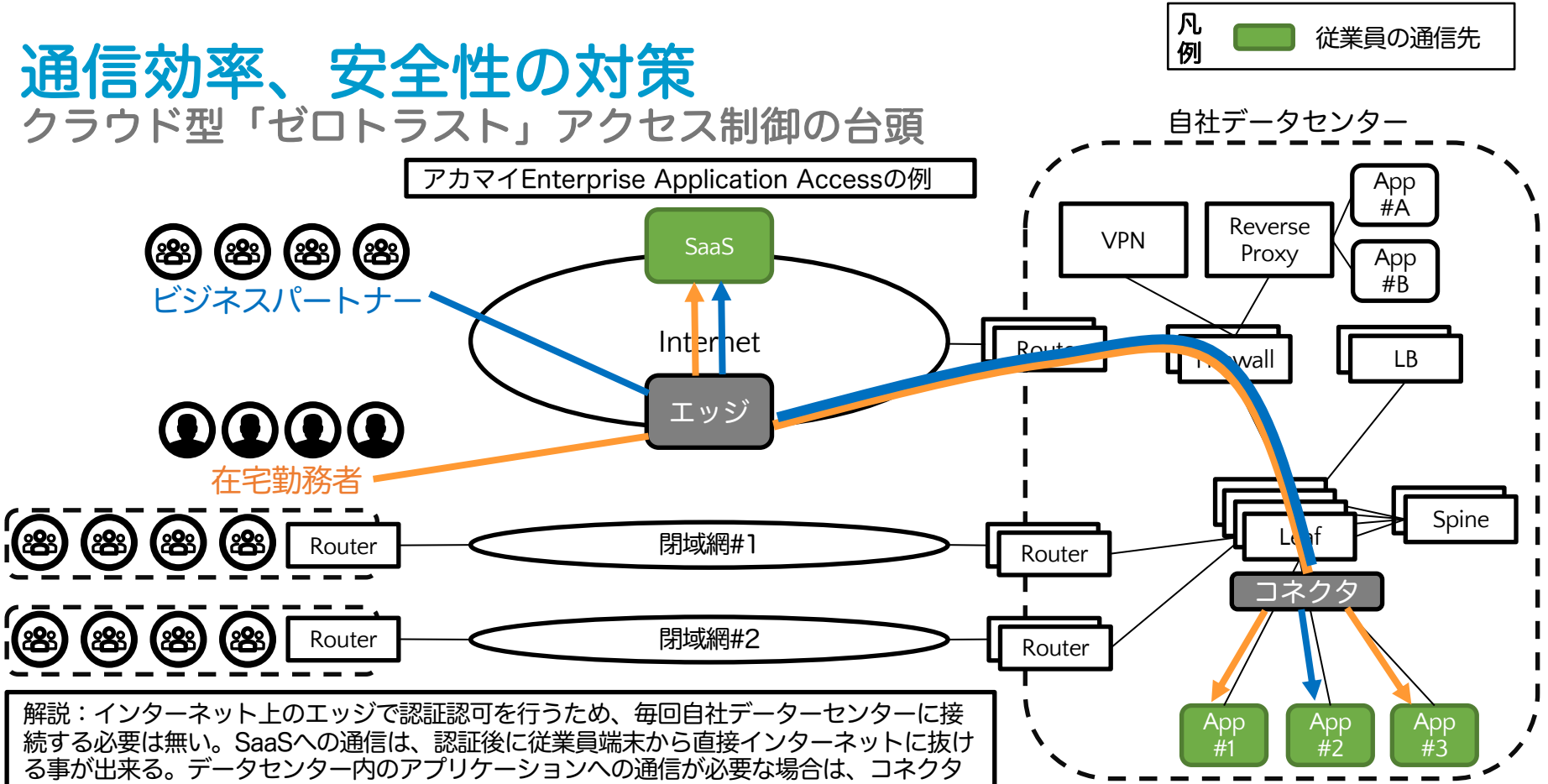
解説：企業のシステムに接続してくる従業員は、社員、契約社員、事業委託先などの多様化している。加えて、営業部、経理部、人事部という社内の部門、役員、部課長、一般社員などという役職も加わり、本来は非常に複雑なアクセス制御が必要となる。ところが、ネットワーク層では、到達性を優先する設計が多く、在宅勤務者の増加が、攻撃面の増加となっているケースも多い。対策として、接続時の認証認可を強める必要がある。

例：App#2しか業務で利用しないが、App#1やApp#3へ到達可能な構成が広く利用されている

Akamai

通信効率、安全性の対策

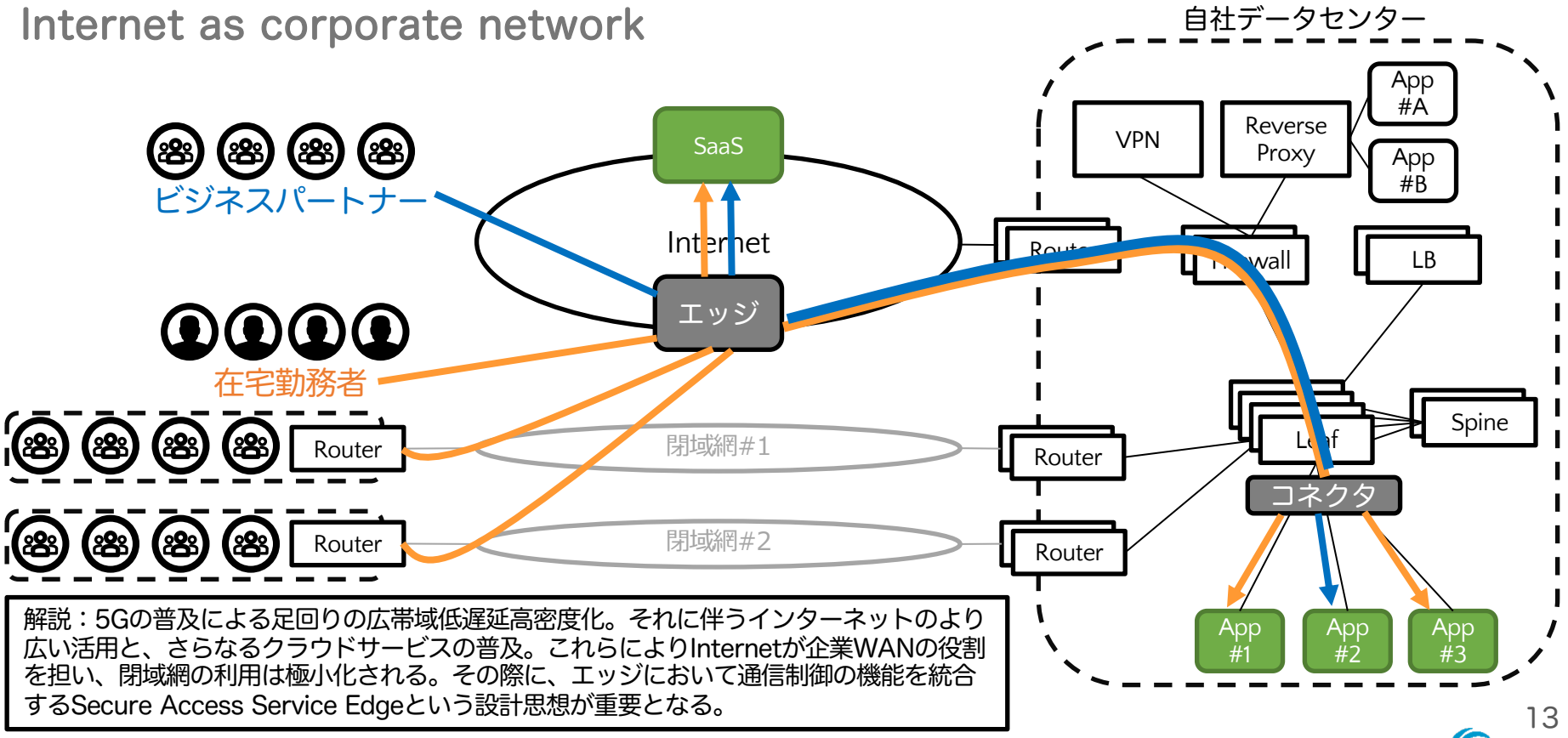
クラウド型「ゼロトラスト」アクセス制御の台頭



解説：インターネット上のエッジで認証認可を行うため、毎回自社データーセンターに接続する必要は無い。SaaSへの通信は、認証後に従業員端末から直接インターネットに抜ける事が出来る。データセンター内のアプリケーションへの通信が必要な場合は、コネクタを通してTLSによって暗号化された秘匿性の高い通信を行う。加えて認可管理が行われるため、不要なアプリケーションへの到達は出来ない。この認可が、サイバー攻撃において行われるラテラルムーブメント（水平移動）を防ぐ事に繋がる。

次世代、エッジが全ての執行点となる

Internet as corporate network



解説：5Gの普及による足回りの広帯域低遅延高密度化。それに伴うインターネットのより広い活用と、さらなるクラウドサービスの普及。これらによりInternetが企業WANの役割を担い、閉域網の利用は極小化される。その際に、エッジにおいて通信制御の機能を統合するSecure Access Service Edgeという設計思想が重要となる。

アカマイの提言

企業で起きた課題

- インターネット回線ひっ迫
- VPN機器処理のひっ迫
  - ハードウェア性能
  - 同時接続ライセンス

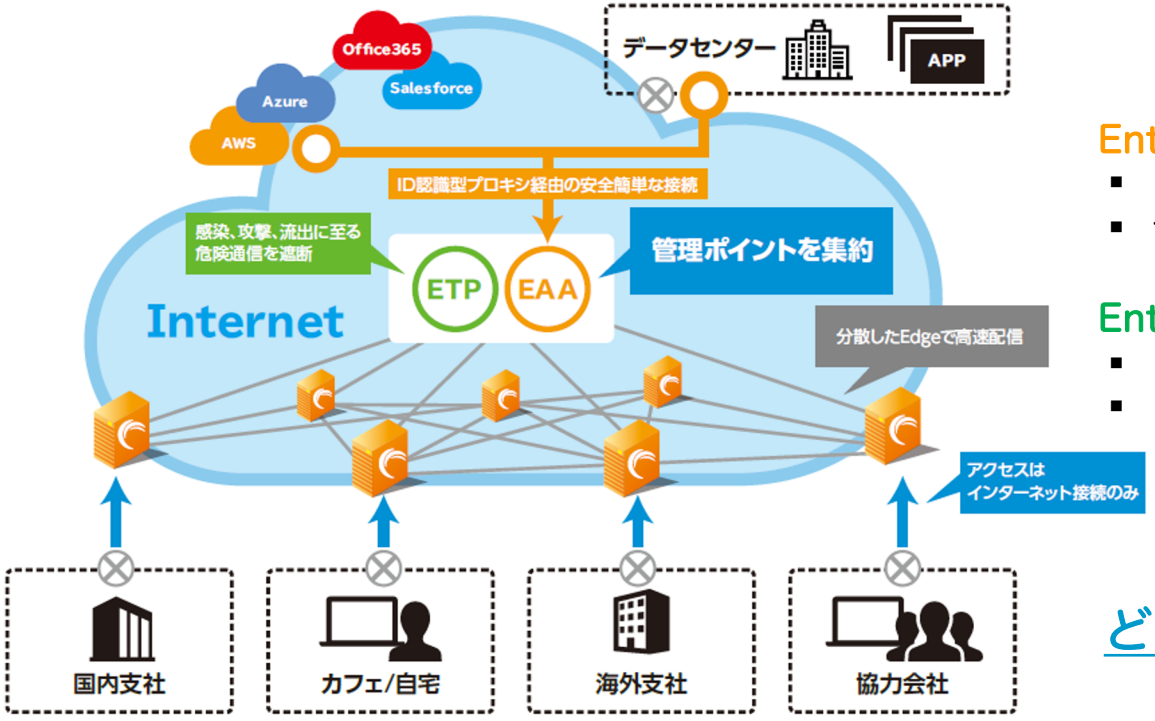
↓

上述の通り、クラウド型によって、通信経路の効率化と調達コストの最小化を行う。併せて、攻撃面増加を防ぐため、IAAAとネットワーク接続の統合を行う。リモートアクセスVPNは15年以上にわたって企業で利用されている技術であり安定性は高いが、既に多くの企業ではセキュリティ面で課題視され始めている。今回の在宅勤務急増に併せて、ゼロトラスト型アクセスソリューションの採用を検討する事が有効だ。その際には、中期的なSASEへの移行も考慮にいれ、エッジ上での実装を考慮に入れる事が望ましい。

参考資料

アカマイのエンタープライズ・ソリューション

https://www.akamai.com/jp/ja/solutions/security/zero-trust-security-model.jsp



Enterprise Application Accessの価値
- クラウドによる拡張性/柔軟性
- ゼロトラスト型のアクセス制御

Enterprise Threat Protectorの価値
- クラウドによる拡張性/柔軟性
- フィッシング、ランサムウェア対策

どこからでも検査して安全にする