# 脱VPNへの一歩
## ～ZTNAの必要性と技術解説～

株式会社エーピーコミュニケーションズ

APCommunications

2023/11/21 InternetWeek2023（東京大学 伊藤謝恩ホール）

# Session 1

## ZTNA羅針盤
## ～攻撃対象領域の極小化の必要性とZTNAについて～

**山根 康裕（ やまね やすひろ ）**

**エンジニアリングマネージャ**

**年　齢：38歳**

**出身地：福岡県**

情報系専門学校を卒業後、2007年に新卒採用にてエーピーコミュニケーションズへ入社。

2012年に結婚&第一子誕生をきっかけに地元福岡へ転職。
転職後は大手ISPにて九州全域の顧客に手広く担当。

ゼロトラストの世界に興味を持ち、二年前にエーピーコミュニケーションズに出戻り、現在はゼロトラスト事業の責任者として活動中。

# Session 2

## ZTNA展開図
## ～Zero Trust Network Access技術解説～

**嘉藤 育宏 ( かとう やすひろ )**

**シニアプロフェッショナル**

**年　齢：45歳**

**出身地：宮城県(育ちは千葉県)**

2002年に新卒採用で富士通特機システム（現：富士通ディフェンス＆ナショナルセキュリティ株式会社）へ入社。

オープンプラットフォームのHW保守作業全般を経験し、運用監視/管理ソフトウェアの設計構築経験を積み、インフラ設計構築に従事。

2022年にゼロトラストの世界に引き込まれるように転職、エーピーコミュニケーションズに入社、現在はクラウドセキュリティを担当中。

Session 1

# ZTNA羅針盤
## ～攻撃対象領域の極小化の必要性とZTNAについて～

株式会社エーピーコミュニケーションズ
山根 康裕（y_yamane@ap-com.co.jp）

APCommunications

2023/11/21 InternetWeek2023（東京大学 伊藤謝恩ホール）

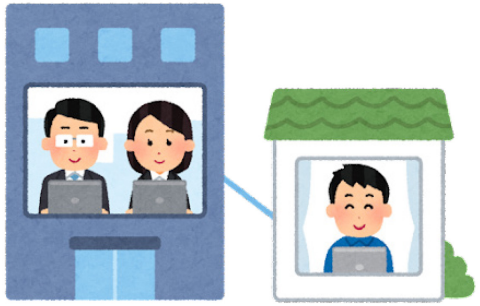
1. 脱VPNと言われている背景
2. VPNとは
3. VPNのどこに問題があるのか
4. ZTNA/SDPについて
5. ZTNA/SDPの技術について

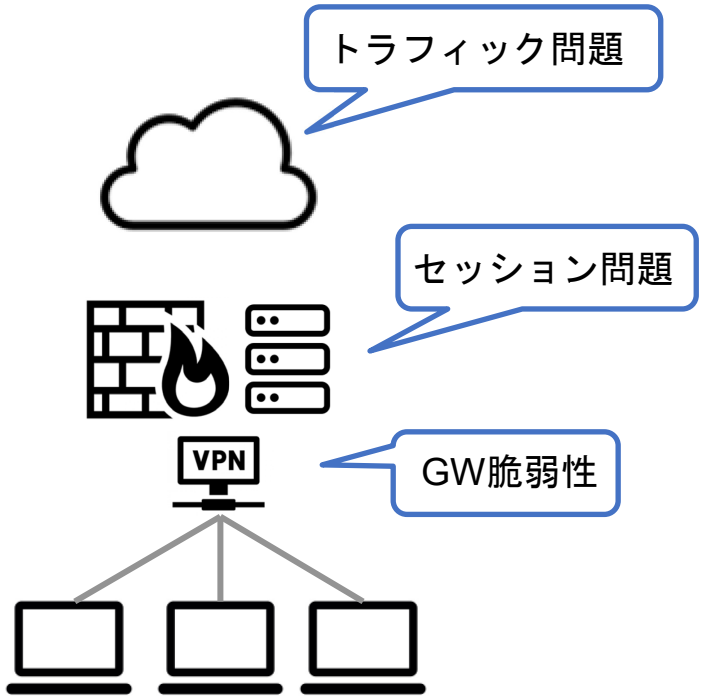
# 脱VPNといわれている背景

## ①コロナ禍でVPNにおける課題が露呈

COVID19パンデミック

リモートワーカーの増加

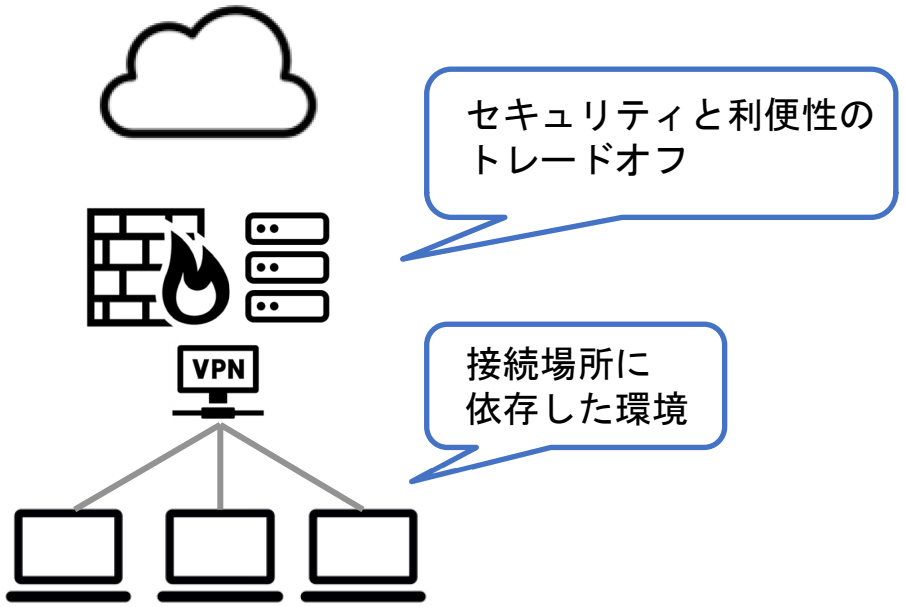




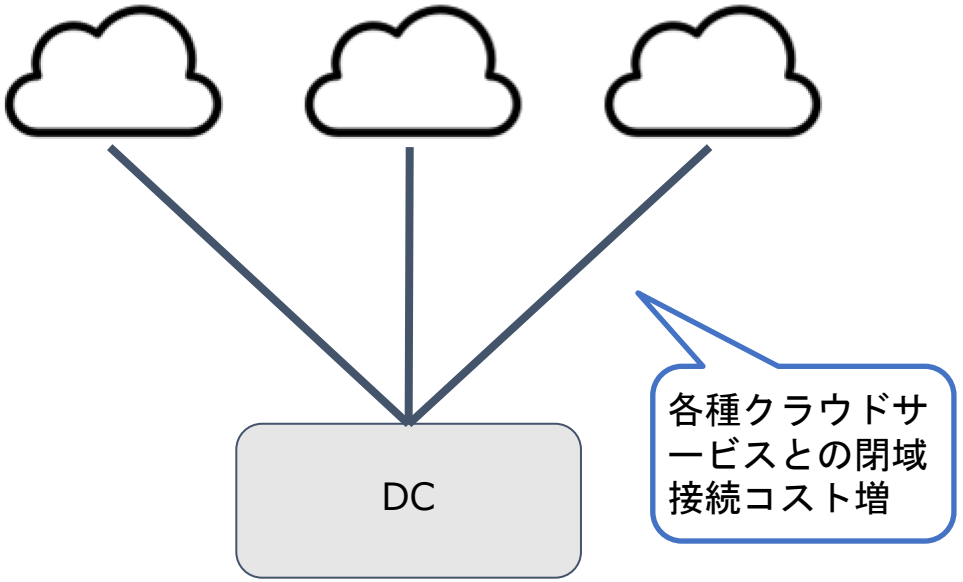

更に、半導体不足も重なり増強も間に合わず影響が業務に及ぶことも
ITインフラが最重要経営課題として扱われる状況へ

# 脱VPNといわれている背景

## ②クラウドサービスの普及とDX化




## ③コストの増大




VPN環境では場所に依存してしまい、セキュリティと利便性のトレードオフに
また、DCや閉域接続コストも増えていきトラフィック量が増えるほどコスト増に

1. 脱VPNと言われている背景
2. VPNについて
3. VPNのどこに問題があるのか
4. ZTNA/SDPについて
5. ZTNA/SDPの技術について

# VPNについて

## VPNを大きく大別すると4つに分けられる

### IP-VPN

通信事業者のプライベートIP網内で、MPLSを採用したVPN

### インターネットVPN

インターネットなどの公衆網を利用し、セキュリティプロトコルを使って実現するVPN
(例)IPsec-VPN,SSL-VPN

### 広域イーサネット

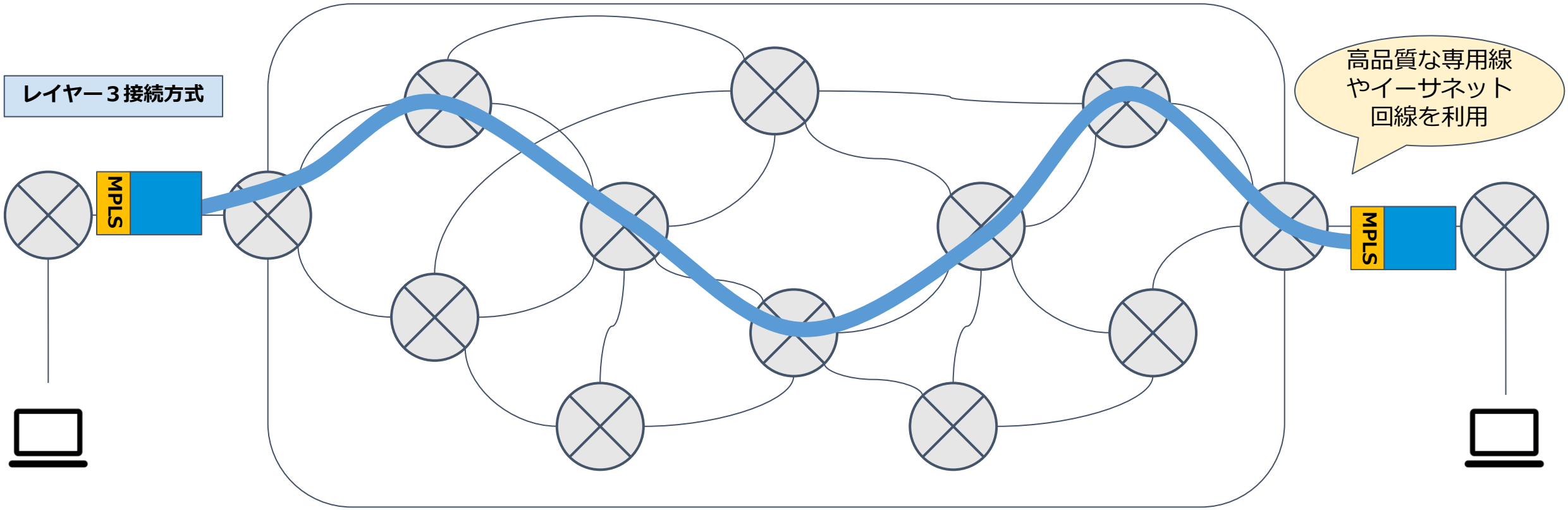
イーサネットによるローカルエリアネットワーク(LAN)を地理的に広域化したもの

### エントリーVPN

比較的安価なブロードバンド回線を用いて閉域IP網へ接続するVPN
※通信品質はベストエフォート

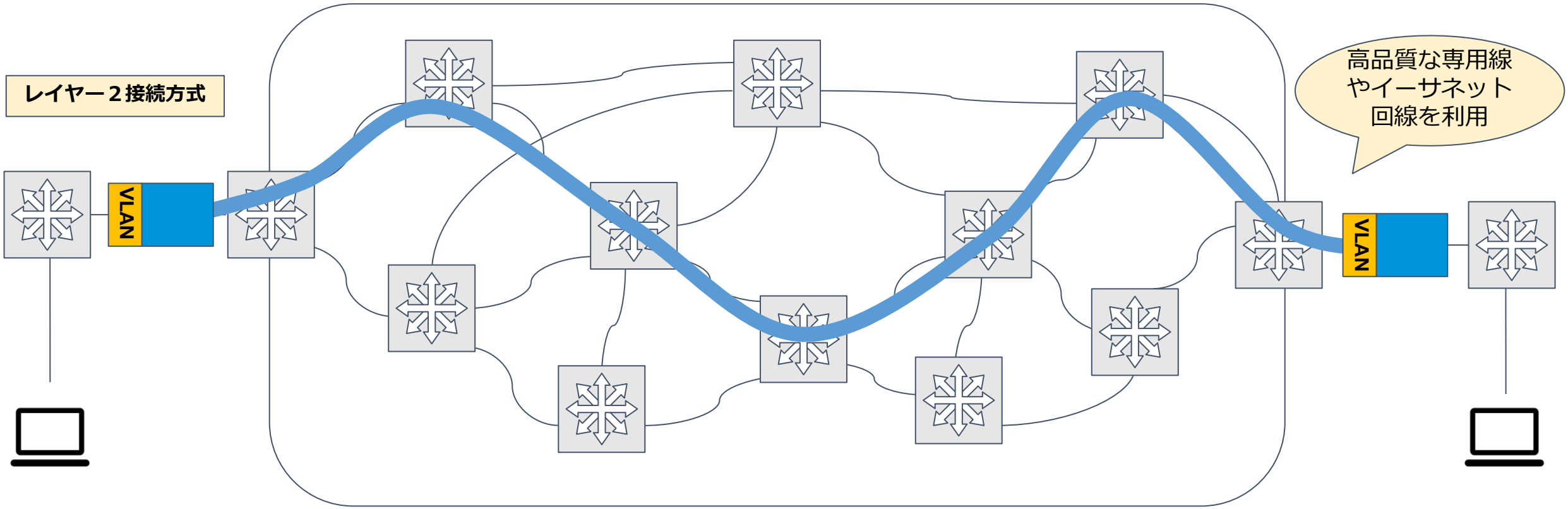
# IP-VPN

通信事業者のプライベートIP網内で、MPLSを採用したVPN



# 広域イーサネット

イーサネットによるローカルエリアネットワーク(LAN)を地理的に広域化したもの
様々なプロトコルにも対応

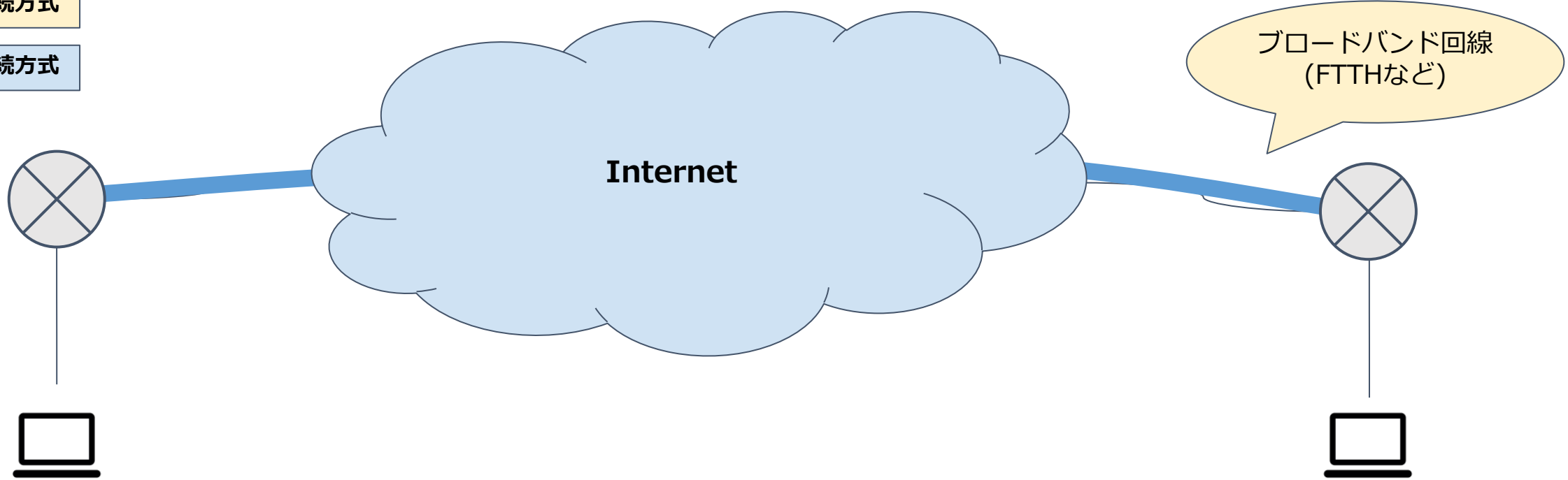


# インターネットVPN

インターネットなどの公衆網を利用し、セキュリティプロトコルを使って実現するVPN
(例)IPsec-VPN,SSL-VPN

**レイヤー２接続方式**

**レイヤー３接続方式**

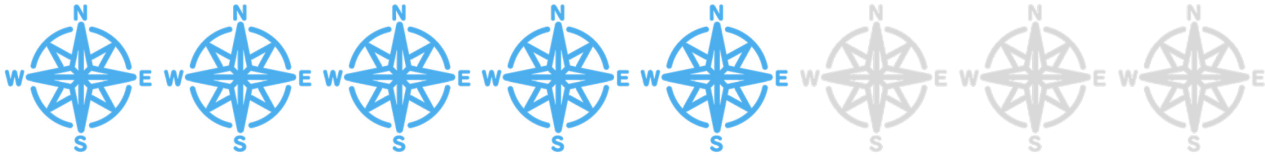


# エントリーVPN

比較的安価なブロードバンド回線を用いて閉域IP網へ接続するVPN
※通信品質はベストエフォート

1. 脱VPNと言われている背景
2. VPNについて
3. VPNのどこに問題があるのか
4. ZTNA/SDPについて
5. ZTNA/SDPの技術について

# VPNのどこに問題があるのか



IP-VPN、広域イーサネット、エントリーVPNは外部からのアクセスに対して強固である一方、内部犯行や別の経路から内部に侵入された場合は、**水平方向の攻撃に対して非常に弱い**

**IP-VPN**

**広域イーサネット**

**エントリーVPN**

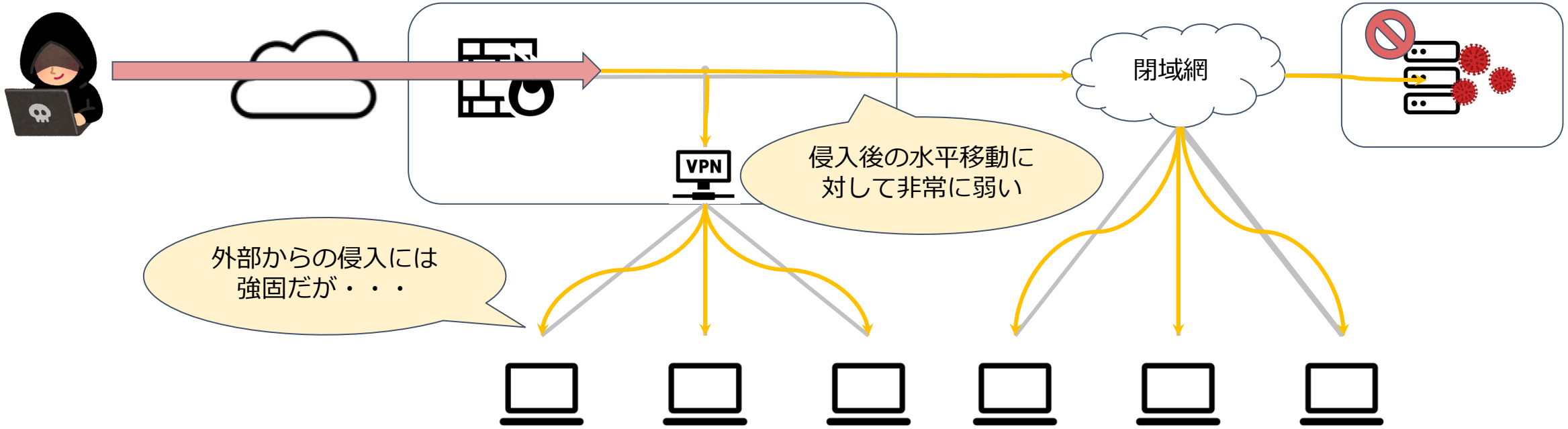
GW側ではグローバルIPアドレスを保持し、待ち受けポートを開けている状況
**攻撃対象領域を保持**

**インターネットVPN**

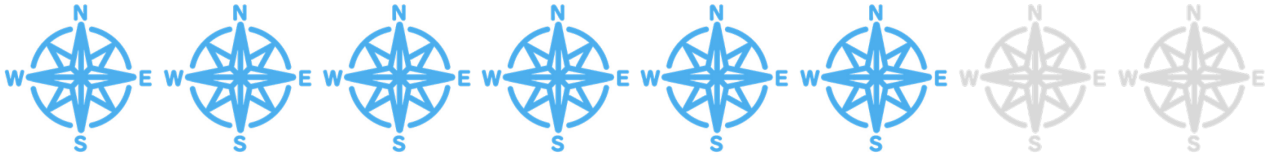
# ラテラルムーブメント(水平移動)とは

攻撃者がネットワークに侵入した後に、ユーザリソース(資産)にアクセスするために使用する一連の手法

情報収集 → 偵察 → 初期侵入 → 防御回避 → 内部侵入 → 内部偵察 → 内部調査 → 情報搾取 → 痕跡消去



# VPNのどこに問題があるのか



IP-VPN、広域イーサネット、エントリーVPNは外部からのアクセスに対して強固である。

一方、内部犯行や別の経路から内部に侵入された場合は、通信に対して認証を行わないため、**水平方向の攻撃に対して非常に弱い**

**IP-VPN**

**広域イーサネット**

**エントリーVPN**

GW側ではグローバルIPアドレスを保持し、待ち受けポートを開けている状況**(攻撃対象領域を保持)**

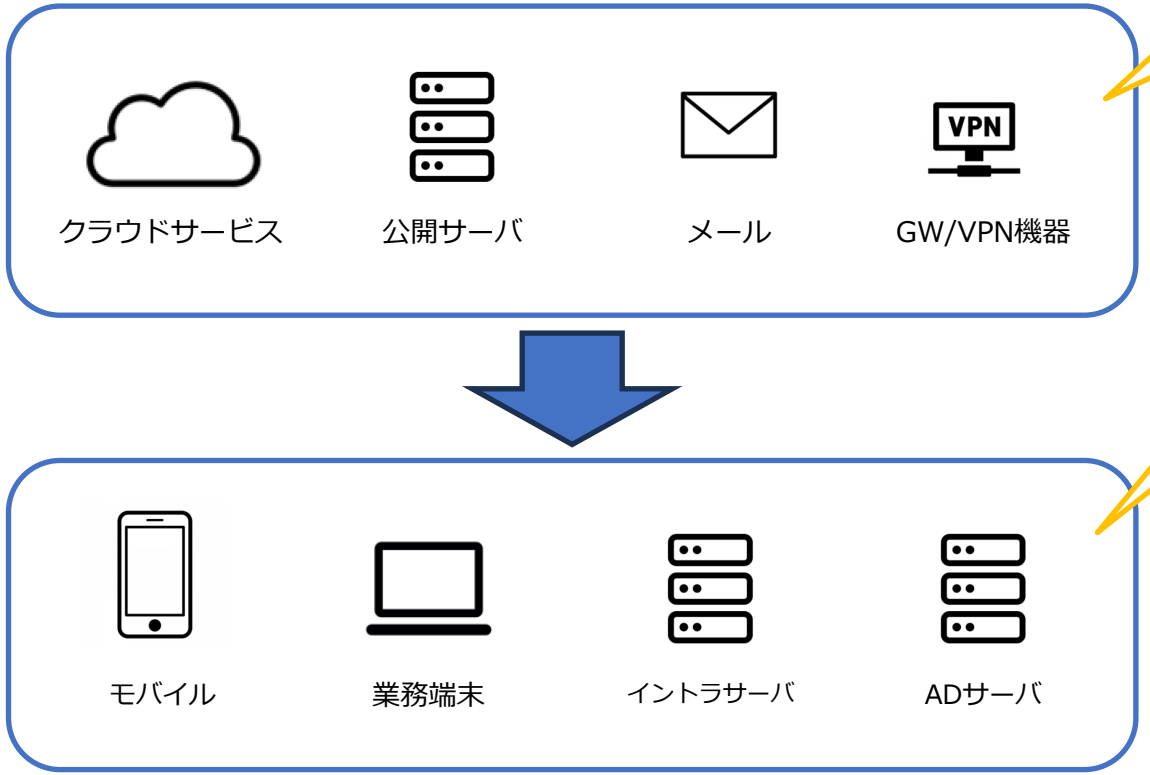
一度認証を許可した通信はどの送信先に対してもアクセス可能な状況

**インターネットVPN**

# 攻撃対象領域(アタックサーフェス)とは

認証されていないユーザーがある環境に対して、攻撃を仕掛けることができるポイントの集合を表す。

(例)




グローバルIPアドレスやドメインなど外部からアクセス可能なポイントは全て攻撃対象領域となる

セキュリティが不十分な場合はここから内部に侵入されるリスクが生じる

間接的に被害を受ける可能性がある社内システムも同様に対象となる

外部からアクセスされる可能性のある攻撃対象領域を極小化していくことが重要!!

下記のような攻撃を受ける標的となる要素も対象

- グローバルIPアドレス
- ドメイン
- アカウント
- メールアドレス
- DNSレコード
- SSL証明書
- API
- トークン
- 脆弱性
- コンフィグ

etc…

1. 脱VPNと言われている背景
2. VPNについて
3. VPNのどこに問題があるのか
4. ZTNA/SDPについて
5. ZTNA/SDPの技術について

# ZTNA/SDPについて

## ZTNA/SDPとは

➡レガシーなVPNに代わる次世代アクセスサービス

### ユーザ認証

アプリケーションアクセスをネットワークと完全に分離し、認証された承認済みのユーザのみに特定アプリケーションへのアクセスを許可します。

### アウトバウンド通信

アウトバウンド方向のみの通信を確立することで、IPを隠蔽し、ダークネットを形成する。

### アプリアクセス制御・認可

ユーザ承認後の通信は特定アプリケーションへのアクセスを1対1で許可し、その他セグメンテーションへのアクセスを禁止する。

### End-to-Endの暗号化通信

ネットワーク中心のアプローチから脱却し、MPLSからインターネットを中心とした新たな企業ネットワークを形成する。

# 機能面におけるVPNとの比較

| 項目 | VPN | ZTNA |
|---|---|---|
| 攻撃対象領域 | VPN、FQDN、待ち受けポートなどGWを狙った攻撃が可能 | 基本的にアウトバウンド通信方向のみ |
| ユーザ認証 | ユーザIDとパスワード認証のみ | IdPとの連携など、様々なユーザ認証方式が利用可能 |
| ラテラルムーブメント防止 | 侵入後抑止不可 | 抑止可能 |
| アクセス範囲 | 全てのネットワークアクセスを許可 | マイクロセグメンテーションの考えに基づいた必要単位でアクセスを制御 |
| 信頼スコア管理 | 実装なし | 信頼スコアに伴いアクセス制限レベルを変更 |

# ZTNAのメリットとデメリット

| メリット | デメリット |
| --- | --- |
| セキュリティ機能の向上 | ログインの負担 |
| 最適なアクセス | 適切な運用設計が重要となる |
| 最小権限でのアクセス | |
| 高度化したユーザ認証 | |
| 信頼性評価機能 | |
| スケーラビリティーの向上 | |
| BYODの推進 | |

1. 脱VPNと言われている背景
2. VPNについて
3. VPNのどこに問題があるのか
4. ZTNA/SDPについて
5. ZTNA/SDPの技術について

# Session 2

## ZTNA展開図
## ～Zero Trust Network Access技術解説～

**嘉藤 育宏 ( かとう やすひろ )**

**シニアプロフェッショナル**

**年　齢：45歳**

**出身地：宮城県(育ちは千葉県)**

Session 2

# ZTNA展開図
## ～Zero Trust Network Access技術解説～

株式会社エーピーコミュニケーションズ
嘉藤 育宏（ya_kato@ap-com.co.jp）

APCommunications