

サイバーセキュリティとSASEとIPv6？

Nov. 2025

Nobuyuki Homma (nhomma@paloaltonetworks.com)

自己紹介

- 本間 庸之 (Nobuyuki Homma)
 - 1994年 Sierに入社
 - 2006年 L3屋さんに転職
 - 2014年 セキュリティ屋さんに転職(現在に至る)

まずはじめにおさらいを…

おさらい(その1)

ゼロトラストって？

- 最近巷でよく耳にする「ゼロトラスト」って？
 - 歴史；
 - 2009年にForrester Reserch社のアナリストのJohn Kindervag氏により提唱される
 - NIST(米国国立標準技術研究所)SP800-207が代表的な「ゼロトラスト」の定義
- ゼロトラストの基本原則
 - Verify Explicitly(常に検証)
 - ユーザのIDや, デバイスの状態, 位置情報, アクセス先アプリケーション等, すべての要素を基にアクセスする際, 都度, 検証
 - Least Privilege Access(最小権限アクセス)
 - ユーザやデバイスには, 必要最低限のリソースのみアクセスを許可
 - Assume Breach(侵害を前提)
 - 攻撃が既に内部に存在する前提で, ラテラルムーブメントと呼ばれる水平展開を防ぐよう設計

ゼロトラストって？

- 最近巷でよく耳にする「ゼロトラスト」って？

- 歴史；

- 2009年にForrester Reserch社のアナリストのJohn Kindervag氏により提唱される

- NIST(米国立標準技術研究所)SP800-207が代表的な「ゼロトラスト」の定義

- ゼロトラスト

- Verify E

- ユー

- Least Privilege Access(最小権限アクセス)

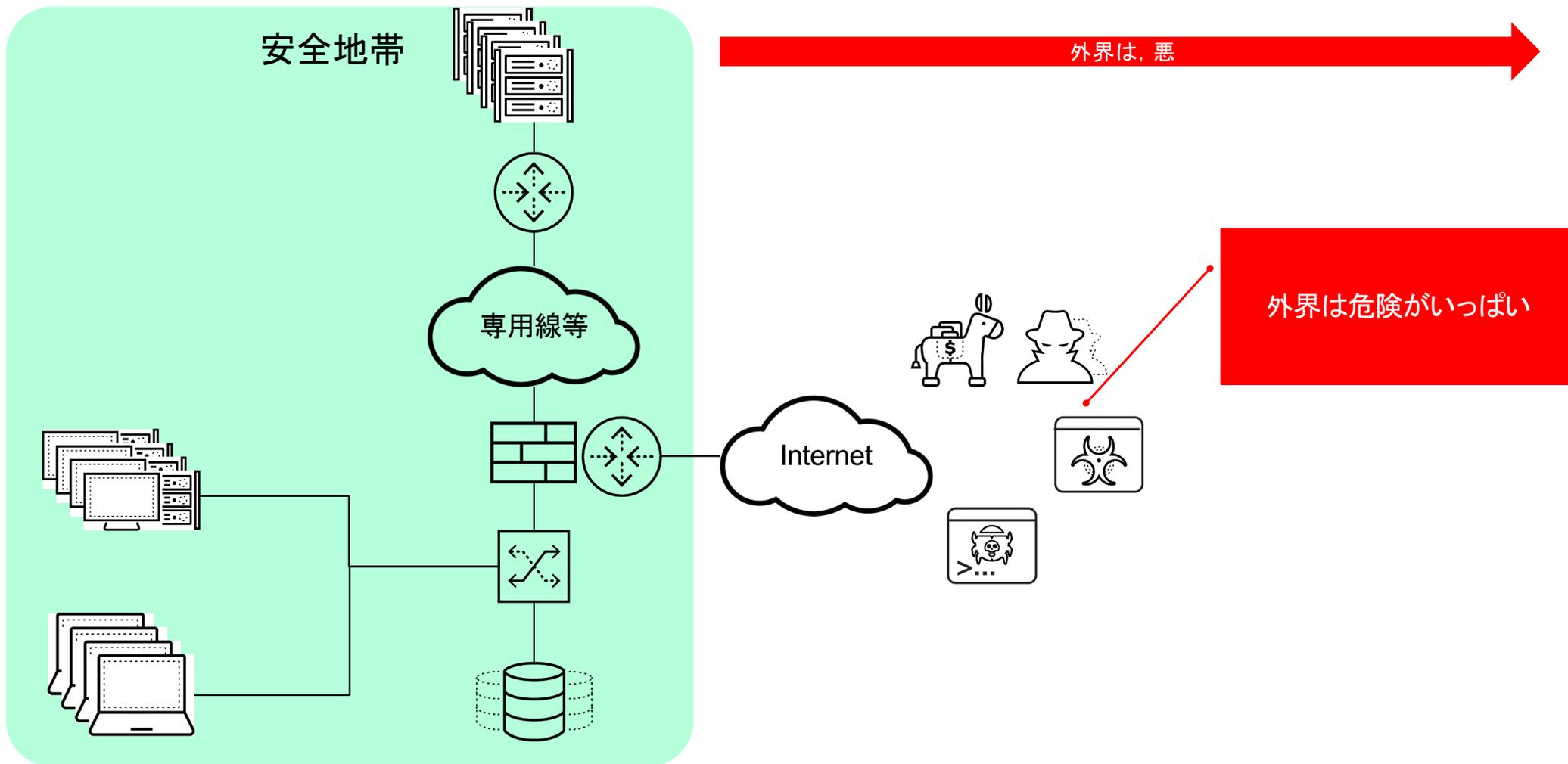
- ユーザやデバイスには、必要最低限のリソースのみアクセスを許可

- Assume Breach(侵害を前提)

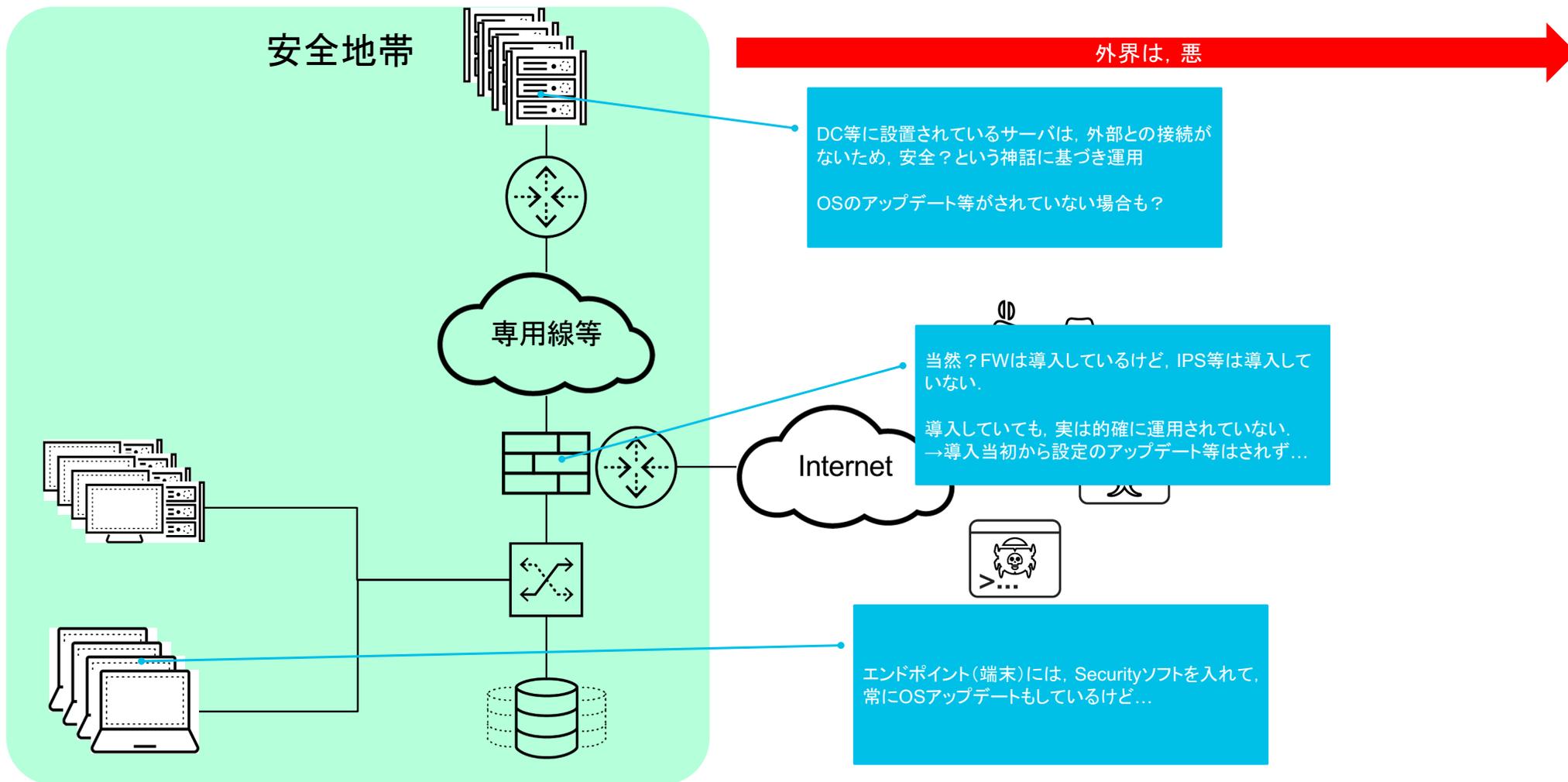
- 攻撃が既に内部に存在する前提で、ラテラルムーブメントと呼ばれる水平展開を防ぐよう設計

すごく、簡単に一言で表すと、
「何も、誰も、信じない」を前提としたセキュリティモデル

今までは...



でも、実際には…



なんで？

基本的には、内部に悪者は居ない. という性善説が前提

なんで？

加えて

なんで？

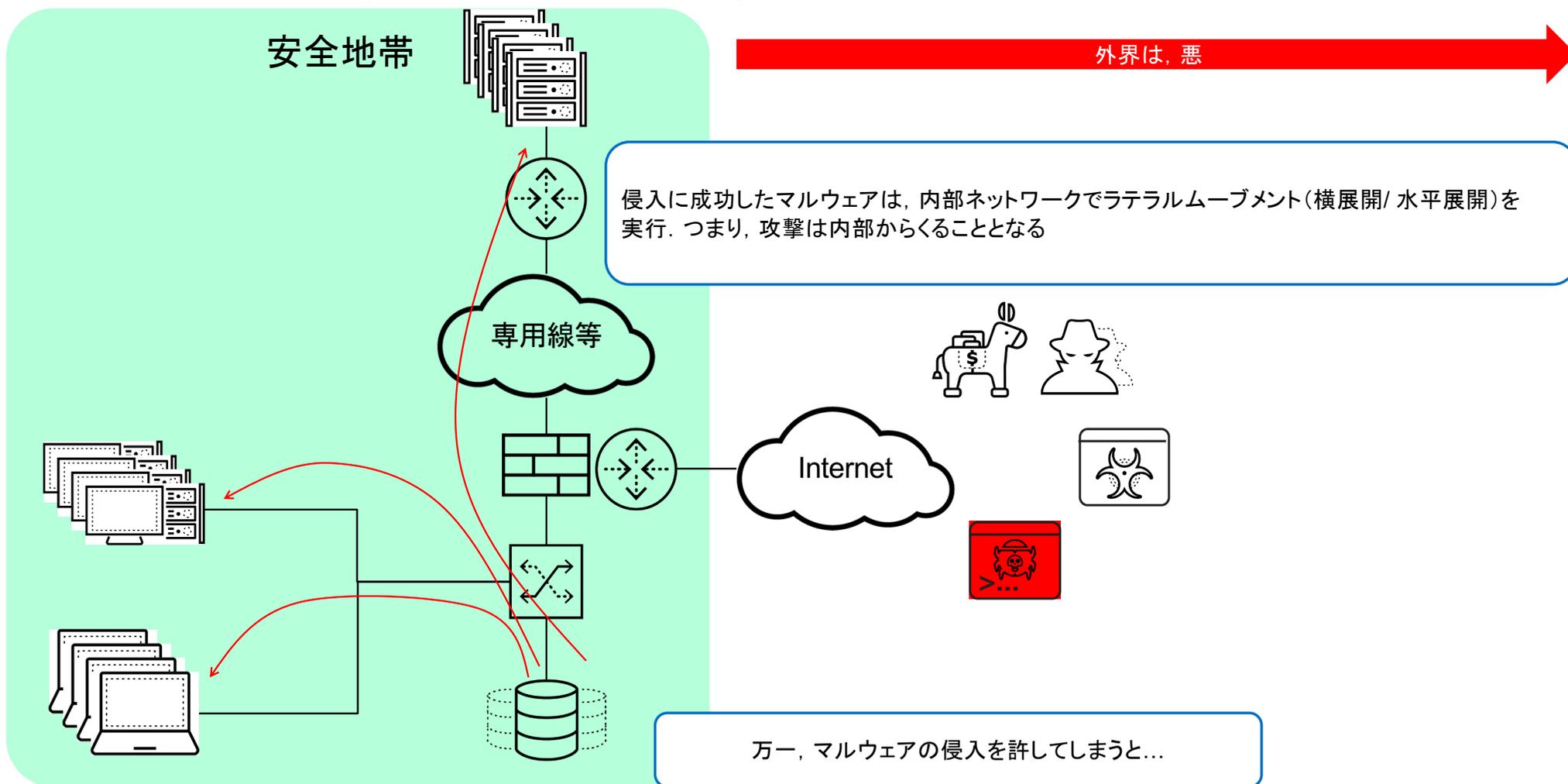
セキュリティ対策としてチャレンジした成功は、あまり評価されず、
失敗のときにマイナスの評価傾向が強い

なんで？

結果...

内部は安全と思えば、少しでも運用も含めて楽チン

最近のサイバー攻撃の傾向と大きな被害



ゆえに...

安全地帯

侵入経路/アタックサーフェスの増加
サイバー攻撃の巧妙化
SSL暗号化通信

が界は、悪

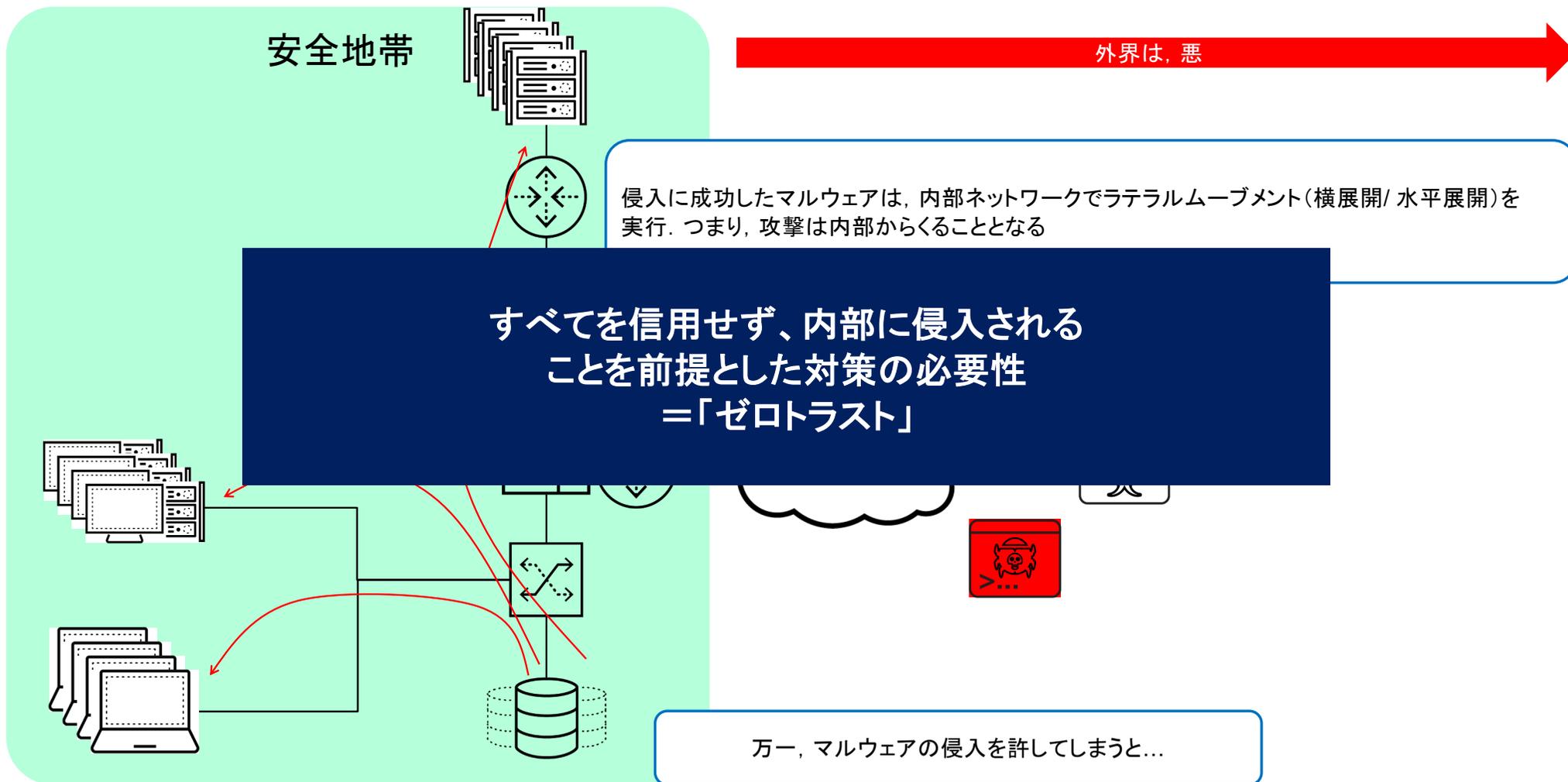
実行. つまり, 内部からくることとなる

ラルムーブメント(横展開/ 水平展開)を

境界面セキュリティモデルの限界

万一、マルウェアの侵入を許してしまうと...

ゆえに…



これを踏まえて おさらい(その2)

最近の出来事とネットワーク

- 一体, どうすれば???
- テレワークとクラウド中心のITインフラのトラフィック傾向を意識しないとね
 - DC回線増強や, ハードウェア設備の増強?
 - ハードウェアベースのインフラの場合, 5年後のトラフィックを見据えた機種選定?
 - リモートアクセス用VPN装置の脆弱性対策のための運用負担って???
 - 計画停電や, 障害時の業務の継続性も意識しないと…

最近の出来事とネットワーク

- 一体、どうすれば???
- テレワークとクラウド中心のITインフラのトラフィック傾向を意識しないとね
 - DC回線増強や、ハードウェア設備の増強?
 - ハードウェアベースのインフラの場合、5年後のトラフィックを見据えた機種選定?
 - リモートアクセス用VPN装置の増設は、増設しただけで運用負担が増える
 - 計画停電や、障害時の

ゼロトラストネットワークを作ろう！

最近の出来事とネットワーク

- 一体, どうすれば???
- テレワークとクラウド中心のITインフラのトラフィック傾向を意識しないとね
 - DC回線増強や, ハードウェア設備の増強?
 - ハードウェアベースのインフラの場合, 5年後のトラフィックを見据えた機種選定?
 - リモートアクセス用VPN装置の増強
 - 計画停電や, 障害時の

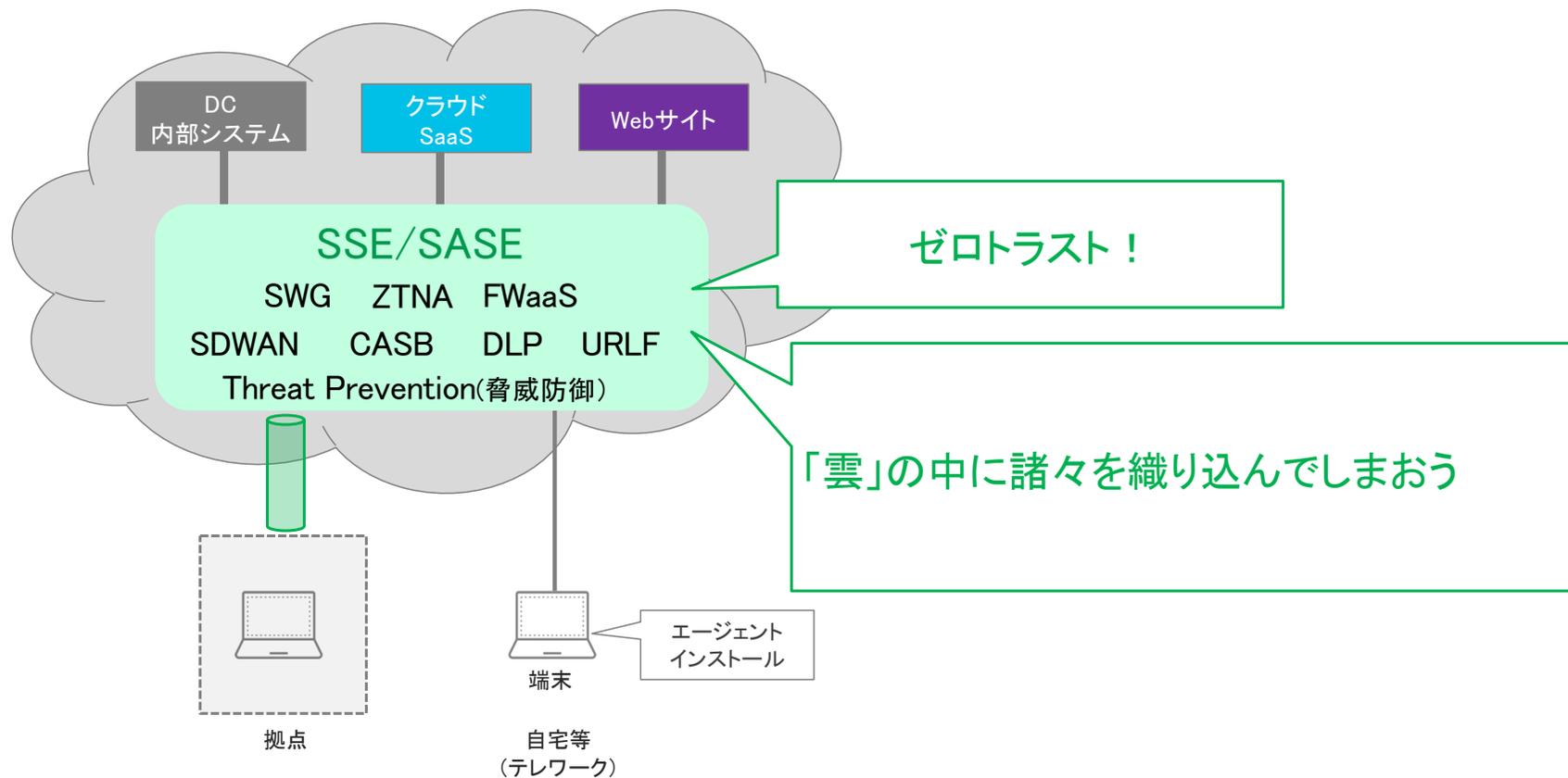
でも...
新型コロナウイルス蔓延...

最近の出来事とネットワーク

- 一体、どうすれば???
- テレワークとクラウド中心のITインフラのトラフィック傾向を意識しないとね
 - DC回線増強や、ハードウェア設備の増強?
 - ハードウェアベースのインフラの場合、5年後のトラフィックを見据えた機種選定?
 - リモートアクセス用VPN装置の増強は、増強は増強でいいけど、
 - 計画停電や、障害時の

テレワークを考慮しつつ、クラウドも意識しつつ...

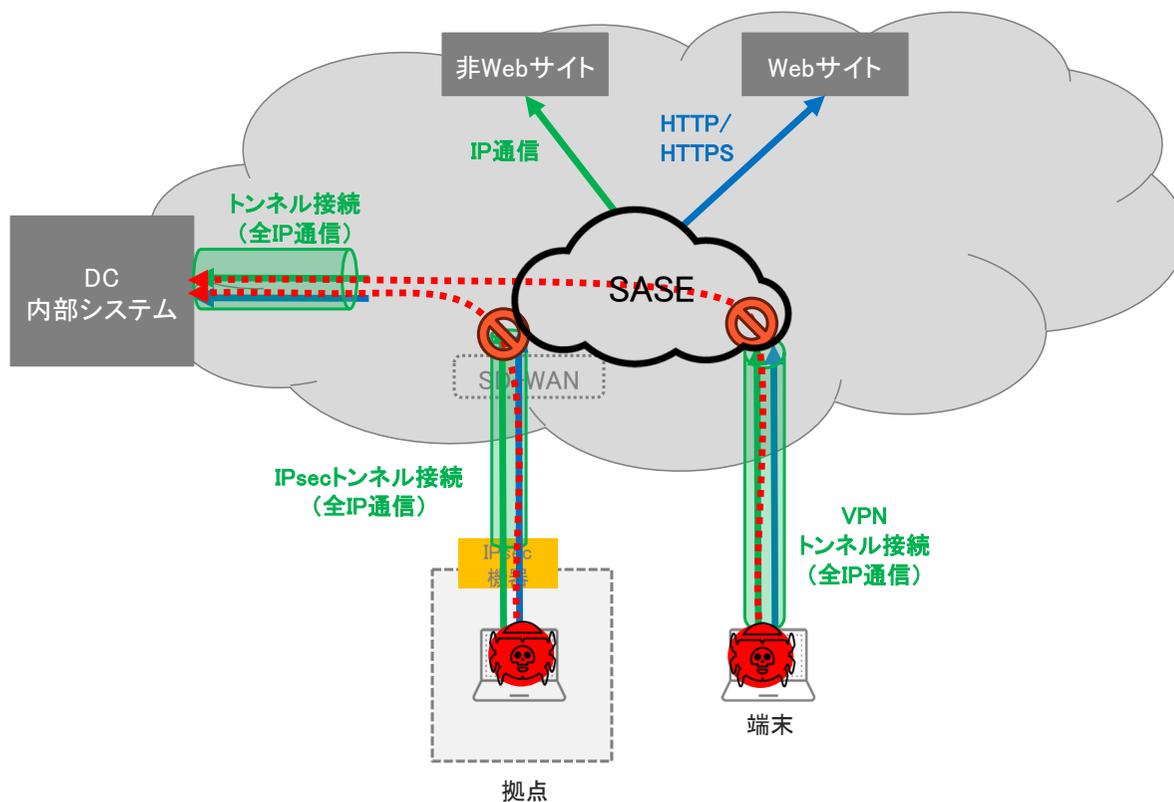
SSE ? SASE ? クラウドソリューション



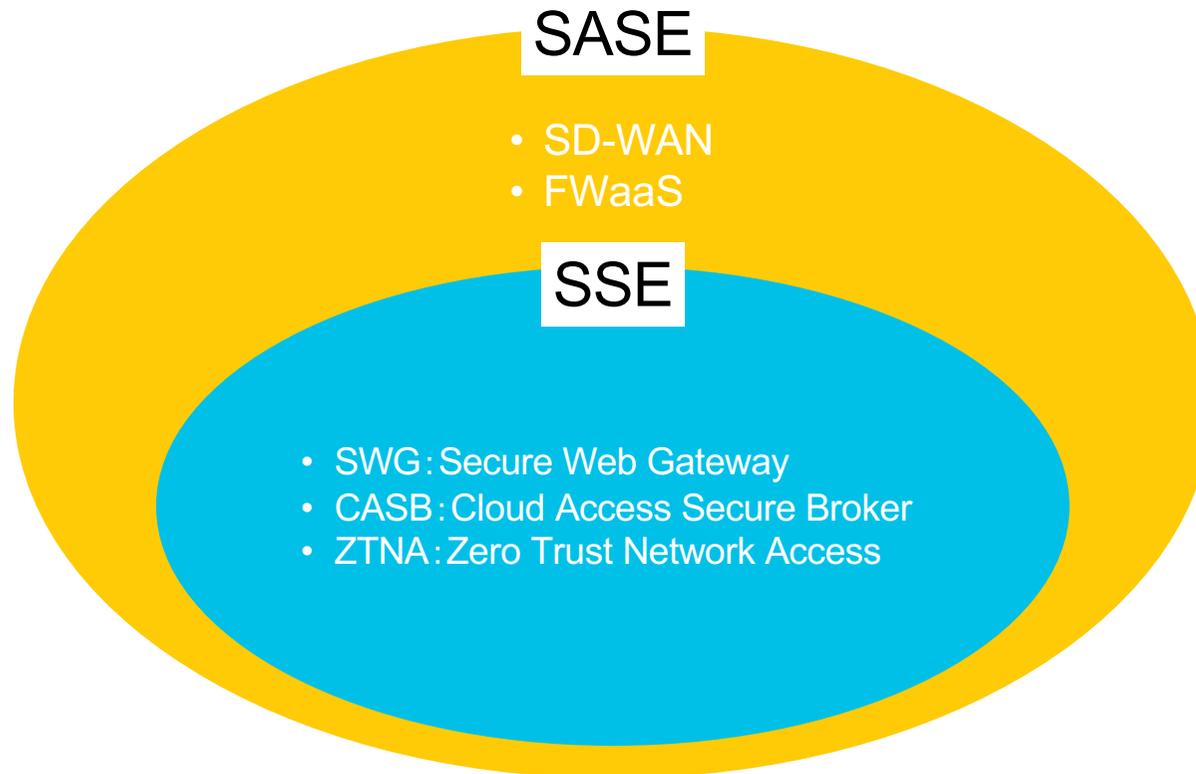
SASEというものは…

アーキテクチャ

インターネットアクセスと内部アクセスの仕組み



言葉の定義？ SSE vs. SASE



SASE = SSE + WAN (SD-WAN/ FWaaS/ Routing)

言葉の定義？機能

機能一覧	機能概要
SWG (Secure Web Gateway)	インターネットに対するWebアクセスに対して、主にプロキシの仕組みを利用してアクセス制御する機能。一般的にURLフィルタリング、各種脅威防御機能、CASB機能やDLP機能を提供
ZTNA (Zero Trust Network Access)	ゼロトラストの概念に基づいて、認証/認可に基づくアプリケーションに対するアクセス制御機能 また、デバイス状態の継続的や場所/時間帯等に基づいたきめ細やかな動的アクセス制御機能を提供
FWaaS	TCP/UDPセッションベースでステートフルにアクセス制御するファイアウォール機能
URLフィルタリング	Web通信に対してカテゴリベースやホワイトリスト/ブラックリストベースでのアクセス制御機能
脅威防御	ポリシー的に許可された通信に対する、IPS/脆弱性防御やアンチウィルス機能。 サンドボックス機能やDNSセキュリティなどの機能を提供しているサービスもあり
CASB (Cloud Access Security Broker)	インターネット上のSaaSに対するアクセス制御する機能。 ファイルの送受信やテナント制御などSaaSに特化したポリシーベースのアクセス制御機能 SaaSに対するリスクベースの情報提供やリスクベースでのアクセス制御可能
DLP (Data Loss Prevention)	外部へ送出するファイルやデータ内に個人情報が含まれるかを検査し、DLPポリシーに該当した場合通信の遮断もしくはログ生成させる機能 指定した特定キーワードの検知に加え、データベースでの日本人の名前/住所やマイナンバーなどの検知にも対応
SSL復号	SSLで暗号化されたWeb通信をリアルタイムで復号し、通信内容を検査する機能
アプリケーション識別	許可された通信に対してアプリケーションを識別し、可視化する機能

ここから本題

IPv6とセキュリティ

- よく耳にする(した)お話し
 - IPv6化すると、セキュリティ強度があがる？
 - 「IPv6ってIPSec使ってるからv4より安全だよな？」という議論はあったものの、v4/ v6どちらもIPSec使える
 - IPv6は、v4より危険？
 - 不正RAとか、end-end通信が基本なので、外から丸見え問題とか…の議論も昔あったり…

IPv6とセキュリティ

- よく耳にする(した)お話し
 - IPv6化すると、セキュリティ強度があがる？
 - 「IPv6ってIPSec使ってるからv4より安全だよな？」という議論はあったものの、v4/ v6どちらもIPSec使える
 - IPv6は、v4より危険？
 - 不正RAとか、end-end通信が

特定の視点で見れば、その視点での議論は大事

IPv6とセキュリティ(つづき)

- セキュリティ強度があがる？さがる？
 - 答え : v4と大差ない.
 - 様々なリスクは同じ(Eg. 不正なWiFiへの誘導とか?). いずれにしても, セキュリティ対策を講じないといけないので, 違いはない.
 - v4だと, NATで見えないけど…
 - 最近では, v6は外から入れなくなってる. v4もv6も突破されるリスクは同じ.

IPv6特有の攻撃

- その昔, 不正RAを使った盗聴はあった
 - ただ…
 - v4のDHCP問題におけるDHCP Snoopingと, v6の不正RA問題におけるRA Guardと大差ナシ

つまり…

サイバーセキュリティ視点では, IPバージョンによる攻撃の差異はない
(と考えて良い)

SASEの方式

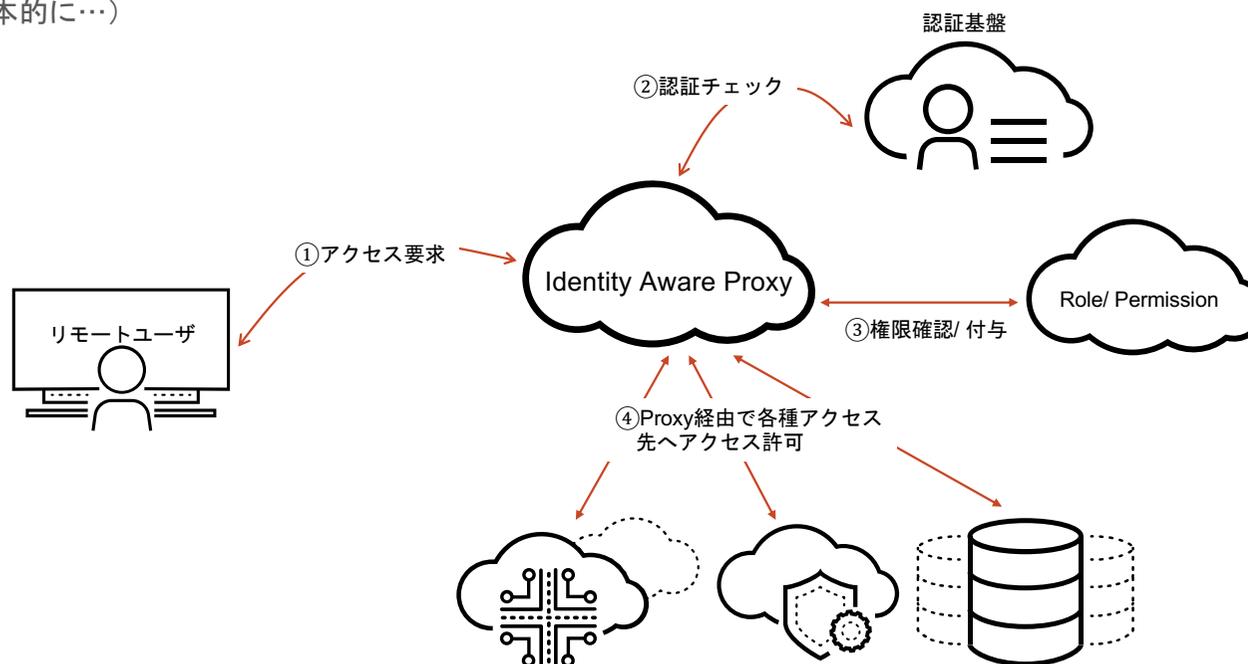
SASEを紐解いてみる

*1: IAPやSDPはZTNAを実現する技術の選択肢のため、
広義では、IAP/SDPの2つに分けられる
ここでは、やや定義が異なるが、敢えてZTNAを分けている

- (敢えての *1) 大きく3つの方式に分類できる

- IAP (Identity Aware Proxy) 方式

- Cloud Proxyでアクセス先への通信を仲介し、IDの認証・認可を通過したあとにアクセス制御が可能
- エージェントレス型(基本的に…)



SASEを紐解いてみる(その2)

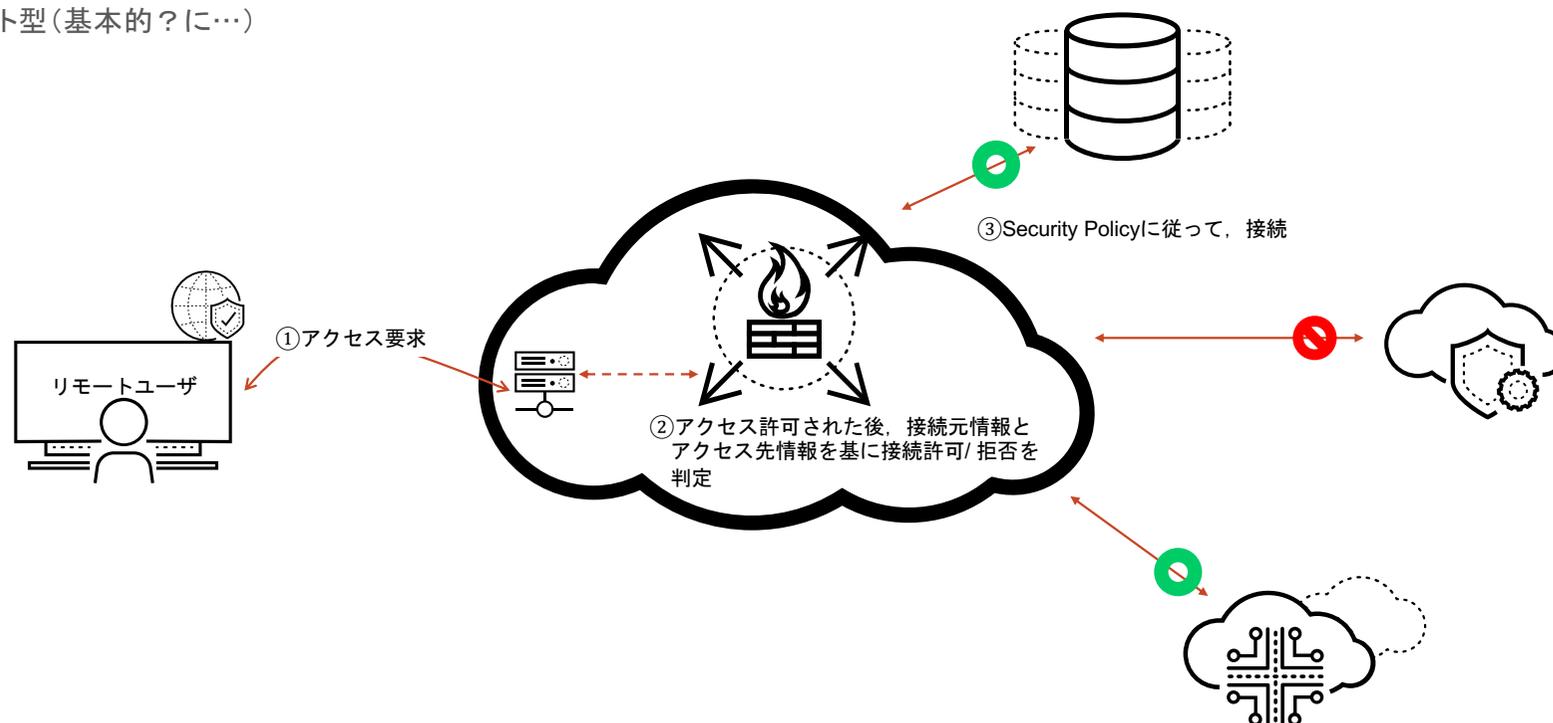
- SDP (Software Defined Perimeter) 方式
 - 認証後、接続許可/ 拒否の判断をし、アクセス許可先へ直接接続を提供
 - エージェント型(基本的に…)



SASEを紐解いてみる(その3)

○ ZTNA(Zero Trust Network Access)方式

- ユーザ認証情報と、そのRole/ 行動等を基に、認証後のユーザへアクセス許可/拒否を動的に提供
- エージェント型(基本的?に…)



IAP vs. SDP vs. ZTNA

- 結局, どの方式が良いんだっけ?
 - SDP方式 = VPN方式と捉えられがちだけど…
 - 認証タイミングと認証要素でVPN方式とは大きく異なる
 - 要は, ユーザ環境は常に変化している(はず), なので, アクセスの都度, ユーザ単位にアクセス許可/拒否を判定し, 個々にネットワーク接続を確立
 - IAP方式
 - ユーザ認証と認可をリクエストごとに実施
 - MFA (Multi Factor Authentication: 他要素認証) と組み合わせることで強固なセキュリティを提供
 - ZTNA方式
 - ユーザ認証後, 必要なデータ, アプリケーションのみへの最小限のアクセス権限を提供

IAP vs. SDP vs. ZTNA

- 結局, どの方式が良いんだっけ?

- SDP方式 = VPN方式と捉えられがちだけど...

- 認証タイミングと認証要素でVPN方式とは大きく異なる

- 要は, 接続を確

いま在籍している会社の立場的には色々と言いたいけど...

個々にネットワーク接

- IAP方式

- ユーザ認証
- MFA (Multi

IAP/ SDP/ ZTNAどれが優れているか? は, 正直優劣は決めづらい
一般論としては, Webアプリで完結するか? BYODをどの程度認めてやるか? により適する方が異なる とか...

- ZTNA方式

- ユーザ認証後, 必要なデータ, アプリケーションのみへの最小限のアクセス権限を提供

SASEとIPv6

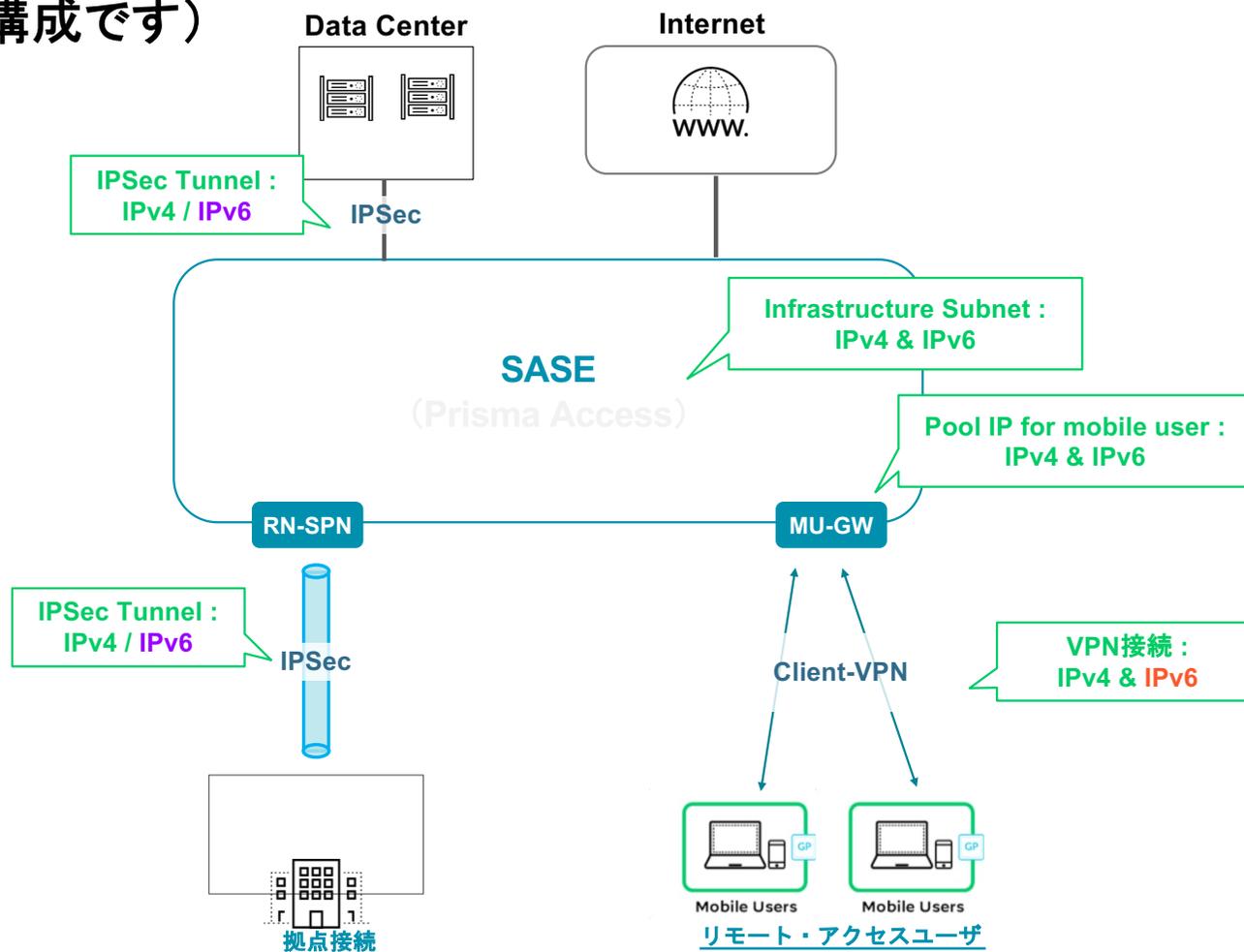
巷のSASEは、IPv6に対応している？

- 結論 : 「多くのベンダで、IPv6対応しています」
 - しかし、SASEは、前述の通り、実現方式は各社独自. このため、各社独自でサポート
 - なので、もしかしたらIPv6未サポートなSASEベンダもあるかも？
 - 制限事項があるかも？（うちも？）

どのようにサポートしている？

- 各社独自でのサポートとなるため、個々に詳細把握はしていませんが、ちなみにウチだと…
 - まずは、「IPv6を使うよ」という(Enable)設定をしないとダメ
 - リモート・アクセス(モバイルユーザ)
 - エージェントにてIPv6を利用するか否かを決定し、v6にてSASEへ接続
 - DNS64/ NAT64(相手側が未サポートの場合)
 - データセンタ接続/ インターネット接続
 - インターネット/ SaaSのEgress

どんな構成？（あくまでもウチの構成です）



互換性マトリックスで表すと…

端末のIP Version	エージェントのIP Version	Internet Destination Gateway - Internet		Private App Access		NAT Gateway - Internet		Default DNS
		IPv4	IPv6	IPv4	IPv6	IPv6 → IPv4	IPv6 → IPv6	
IPv4	IPv4	○	—	○	—	NAT64	NPTv6	Google Public DNS (64)
Dual Stack	Dual Stack(IPv6)	○	○	○	○	NAT64	NPTv6	
IPv6	Dual Stack(IPv6)	○ (DNS64/ NAT64)	○	○ (DNS64/ NAT64)	○	NAT64	NPTv6	

まとめ

まとめ

- サイバー攻撃
 - IP versionによる攻撃の差異は、ほとんどない。つまり、IPv4だから、安全。IPv6だから、危険。またはその逆。という差異はない。
 - つまり、同じようにゼロトラストの概念に基づき、セキュリティ対策は必要
- (今流行りの)SASEとの接続
 - 各社実装の違いはあれど、概ねIPv6を収容する機能はサポート済み
 - SASEを使って、安全なIPv6ライフを？
 - ただし、SASEと言っても、各社機能はまちまち。必要なセキュリティ機能と、IPv6収容とをチェックしよう

おまけ

IPv6トラフィックは、どう見える？（これもウチの場合です）

Log Viewer

Firewall/Threat Severity = 'Critical' AND Source Location = 'Unknown'

Time Zone: Japan Standard Time

PCAP Download	Time Generated ↓	Severity	Subtype	Threat Name Firewall	Threat ID								
	2025-06-08 21:51:32	Critical	vulnerability	Apache CouchDB JSON Remote Privilege Escalation Vulnerab...	58159								
	2025-06-08 21:51:32	Critical	vulnerability	Apache Solr xmlparser XML External Entity Expansion Remot...	30009								
	2025-06-08 21:51:32	Critical	vulnerability	Oracle Java IE Browser Plugin docbase Parameter Remote Co...	35986								
	2025-06-08 21:51:32	Critical	vulnerability	Jenkins Remote Code Execution Vulnerability	56426								
	2025-06-08 21:51:32	Critical	vulnerability	GNU C Library Gethostbyname GHOST Buffer Overflow Vuln...	38384								
	2025-06-08 21:51:32	Critical	vulnerability	IBM Informix Dynamic Server index.php testconn Heap Buffer...	30292								
	2025-06-08 21:51:32	Critical	vulnerability	HPE Intelligent Management Center WebDMServlet Insecure ...	38341								
	2025-06-08 21:51:32	Critical	vulnerability	HPE Intelligent Management Center WebDMServlet Insecure ...	38341								
	2025-06-08 21:51:32	Critical	vulnerability	HP Integrated Lights-Out Authentication Bypass Vulnerability	39752								
	2025-06-08 21:51:32	Critical	vulnerability	Apache Solr XML External Entity Expansion Remote Code Exe...	54884								
	2025-06-08 21:51:32	Critical	vulnerability	NetIQ Access Manager Identity Server Directory Traversal Vul...	40581								
	2025-06-08 21:51:32	Critical	vulnerability	Exhibitor UI Command Injection Vulnerability	58188	code-execution	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	web-browsing
	2025-06-08 21:51:32	Critical	vulnerability	ManageEngine ApplicationManager testCredential.do Comma...	40786	code-execution	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	upnp
	2025-06-08 21:51:32	Critical	vulnerability	D-Link DNS-320 ShareCenter Remote Command Execution V...	56613	code-execution	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	upnp
	2025-06-08 21:51:32	Critical	vulnerability	Homematic CCU2 Remote Command Execution Vulnerability	40787	code-execution	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	upnp
	2025-06-08 21:51:32	Critical	vulnerability	Cisco Elastic Services Controller REST API Authentication Byp...	55879	info-leak	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	web-browsing
	2025-06-08 21:51:32	Critical	vulnerability	Dell EMC VMAX Virtual Appliance Manager Authentication B...	54515	info-leak	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	upnp
	2025-06-08 21:51:32	Critical	vulnerability	IBM Informix OpenAdmin Tool welcomeService.php Comman...	40562	code-execution	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	upnp
	2025-06-08 21:51:32	Critical	vulnerability	Micro Focus GroupWise Post Office Agent Buffer Overflow V...	36485	overflow	trust	2001:3a80:1804:101	Unknown	trust	2001:3a80:1804:101	80	upnp
	2025-06-05 20:48:49	Critical	vulnerability	Microsoft Message Queuing Remote Code Execution Vulnera...	94255	code-execution	trust	2001:3a80:1805:28	Unknown	trust	2001:3a80:1805:28	1801	incomplete
	2025-06-05 20:48:42	Critical	vulnerability	CyberPanel Command Injection Vulnerability	95785	code-execution	trust	2001:3a80:1805:3c	Unknown	trust	2001:3a80:1805:3c	8090	web-browsing