巷で噂のSASEって？

July. 2026

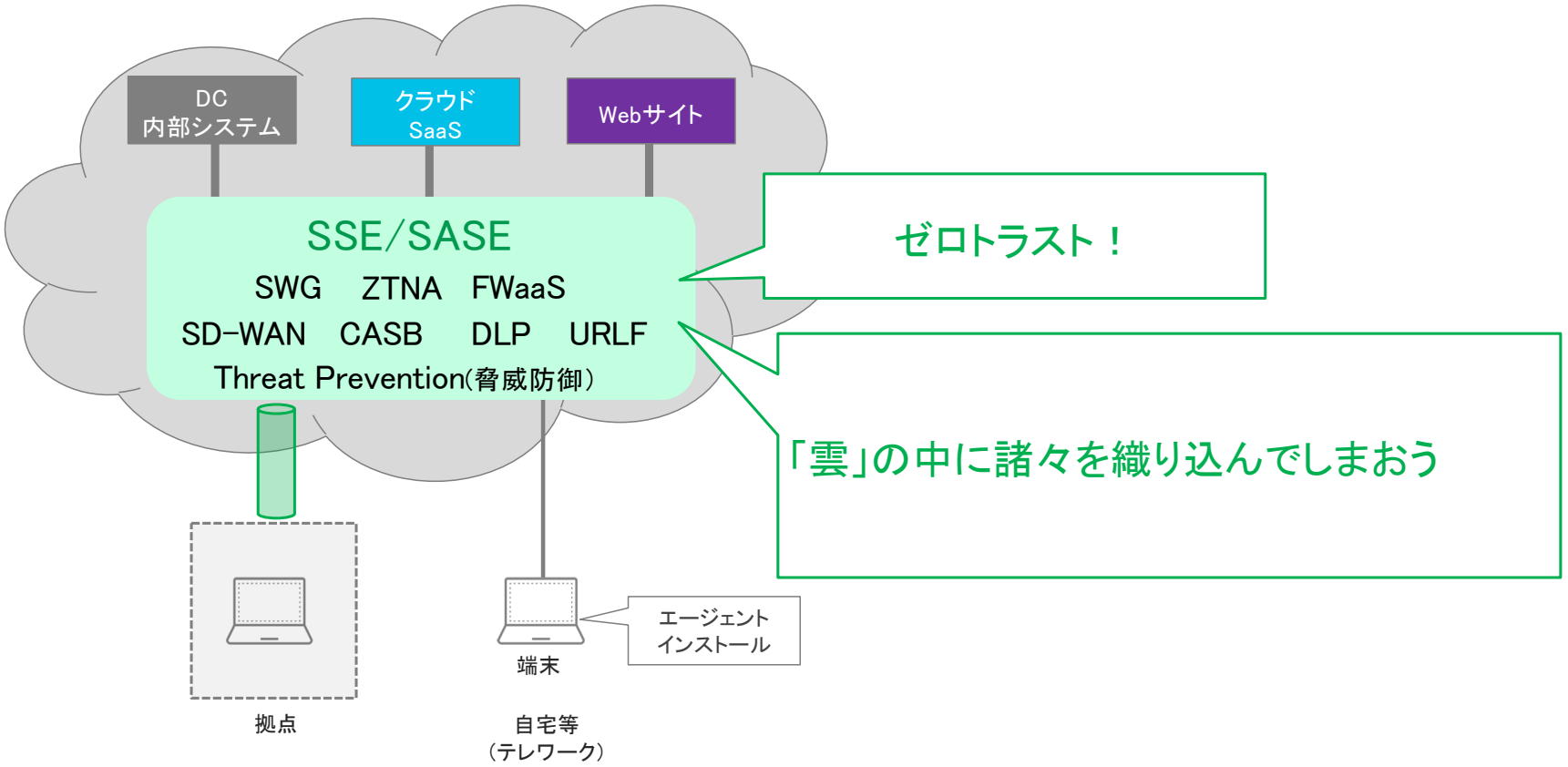
Nobuyuki Homma（nhomma@paloaltonetworks.com）

自己紹介

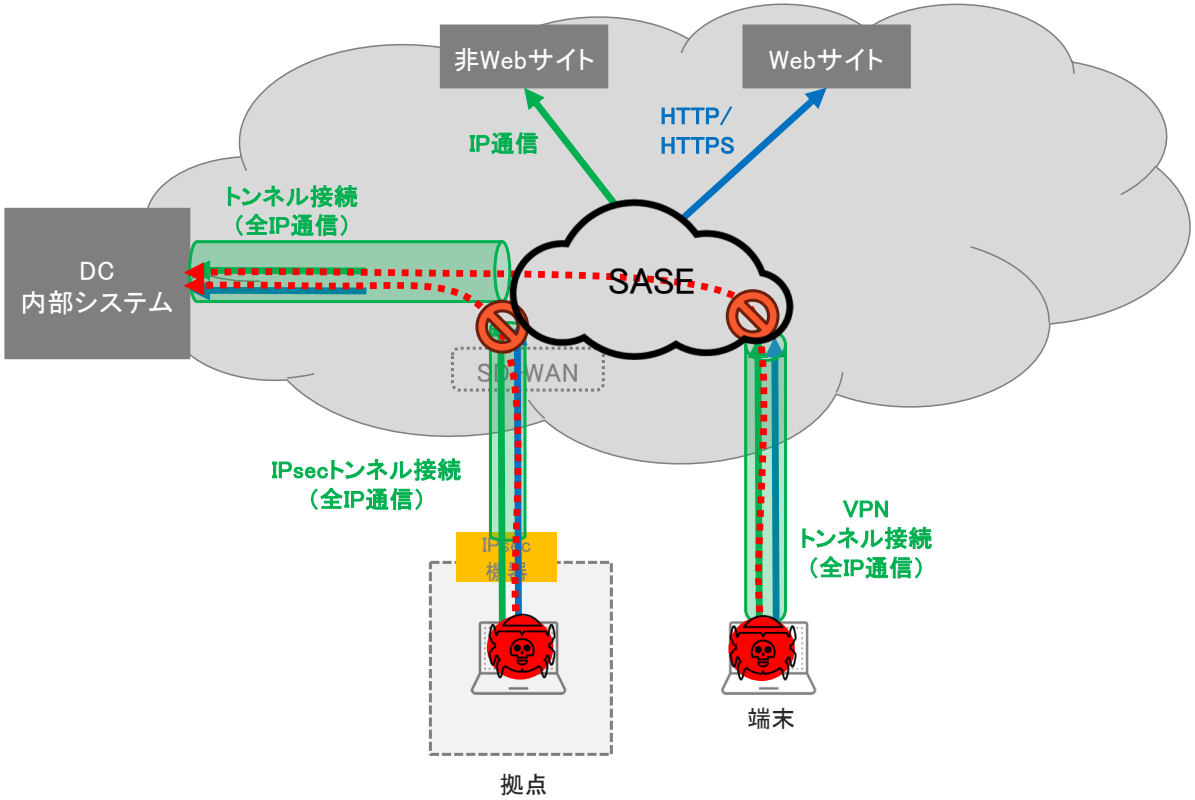
- 本間　庸之（Nobuyuki Homma）
  - 1994年　SIerに入社
  - 2006年　L3屋さんに転職
  - 2014年　セキュリティ屋さんに転職（現在に至る）

前半のセッションを踏まえて…

SASE？SSE？クラウドソリューション



SASEというものは…

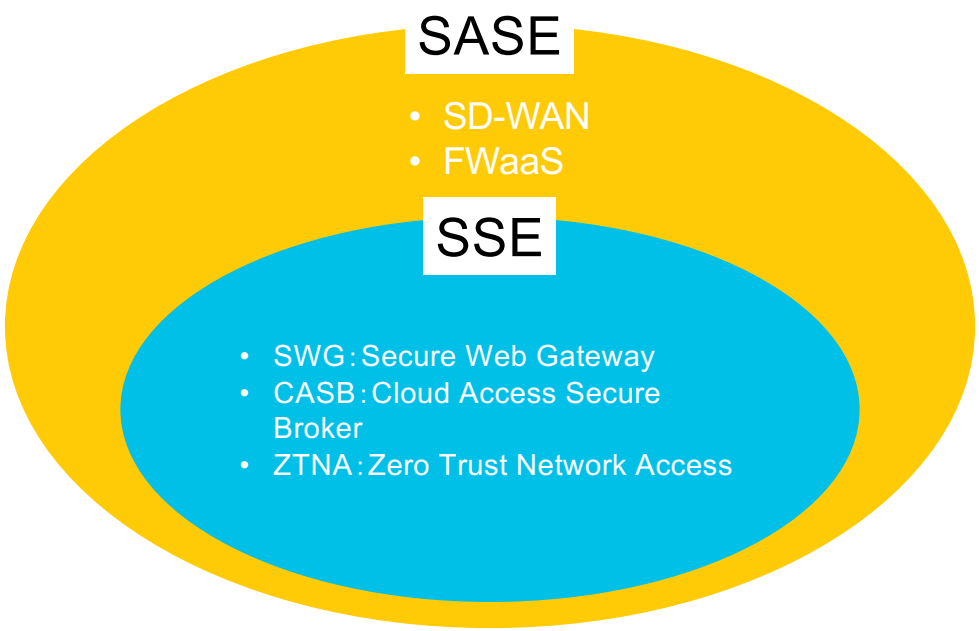


SASEとSSEの定義（違い）

- SASEとSSEの違いって？
  - SASE： Secure Access Service Edge
  - SSE： Security Service Edge

主な違いは？

カバーする「範囲」



SASEとSSEの定義（違い）2

特徴	SASE	SSE
定義	ネットワークとセキュリティを統合した包括的なプラットフォーム	SASEのセキュリティコンポーネントのみを抽出したもの
主な機能	セキュリティ機能； SWG，ZTNA，CASB，FWaaS ネットワーク機能； SD-WAN，WAN最適化，QoS	セキュリティ機能； SWG，ZTNA，CASB，FWaaS
対象レイヤ	Layer3からLayer7	主にLayer7を中心としたプロキシベース
代表的な製品例	Cato Networks，Palo Alto Networks	Zscaler，Netskope

- 主な相違点
  - WAN機能（SD-WAN）の有無
    - SASE：SD-WAN等のネットワーク機能が含まれているため，拠点間通信や，既存の閉域網の置き換えが可能
    - SSE：ネットワーク機能が含まれないため，別途WAN環境を維持/ 構築する必要あり
  - プロトコル対応
    - SASE：アプリケーション互換が高く，非Webプロトコルを含む，すべてのトラフィックを一環して保護
    - SSE：Proxyベースとなるため，特定のアプリケーション/ プロトコルの保護．（コネクタ等の利用でその制約を解除可能）
  - 運用面
    - SASEは，単一ベンダにてネットワークとセキュリティの両方が提供されるため，単一のコンソール，エージェント，ポリシーモデルで運用可能

言葉の定義？機能

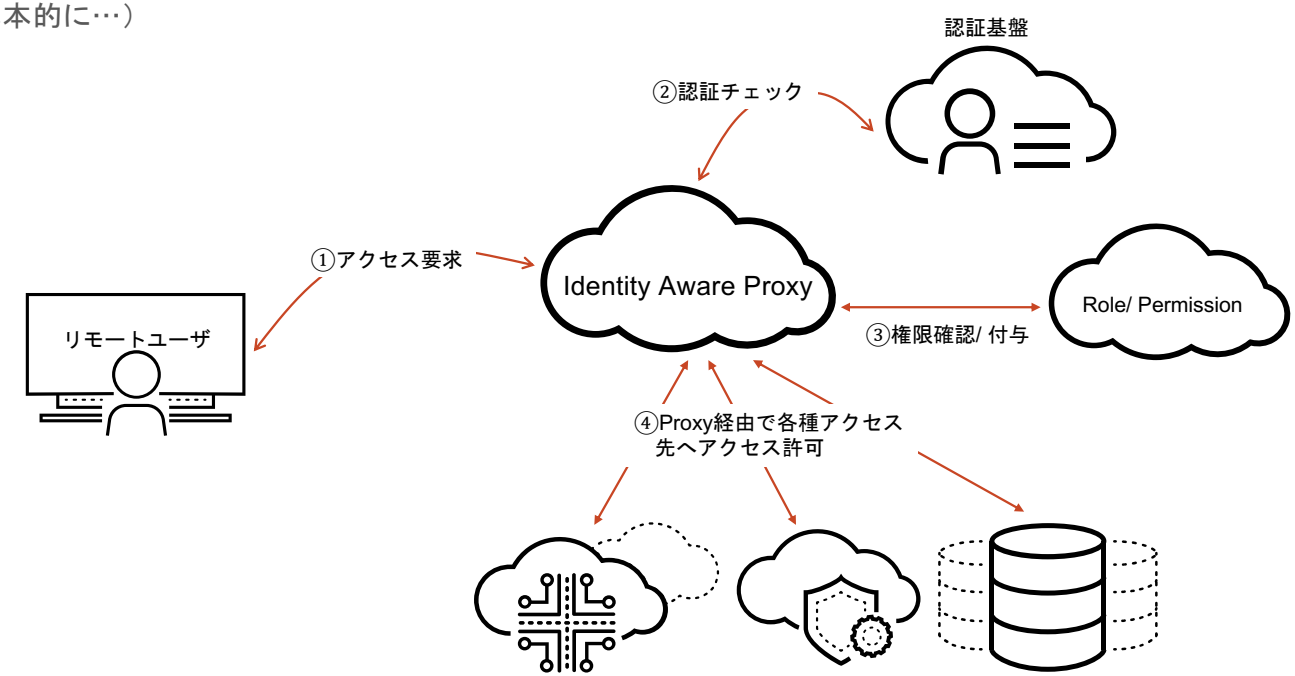
機能一覧	機能概要
SWG (Secure Web Gateway)	インターネットに対するWebアクセスに対して，主にプロキシの仕組みを利用してアクセス制御する機能. 一般的にURLフィルタリング，各種脅威防御機能，CASB機能やDLP機能を提供
ZTNA (Zero Trust Network Access)	ゼロトラストの概念に基づいて，認証/認可に基づくアプリケーションに対するアクセス制御機能 また，デバイス状態の継続的や場所/ 時間帯等に基づいたきめ細やかな動的アクセス制御機能を提供
FWaaS	TCP/UDPセッションベースでステートフルにアクセス制御するファイアウォール機能
URL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

SASEの方式

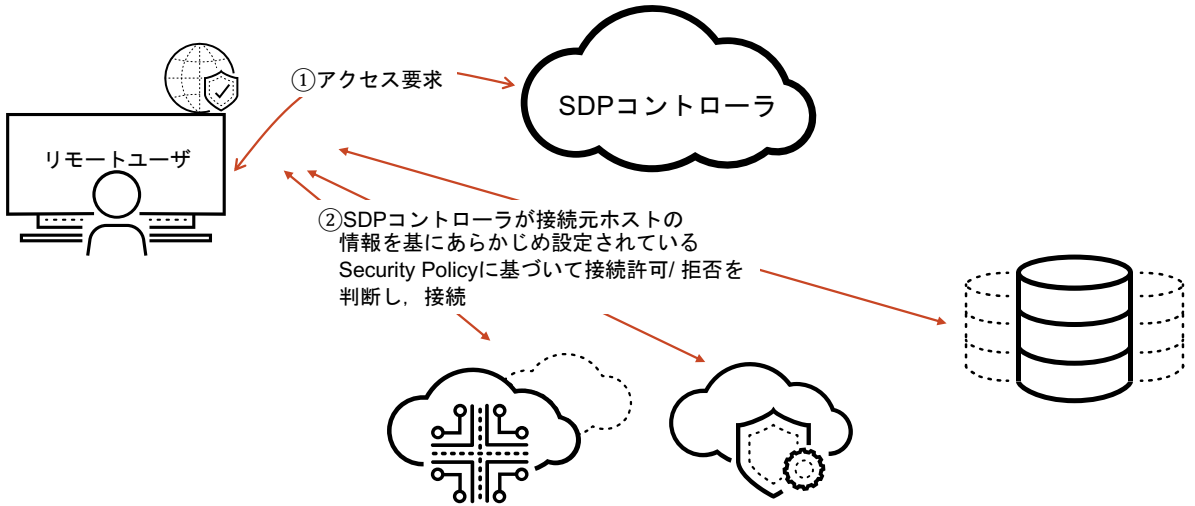
SASEを紐解いてみる

- 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…）



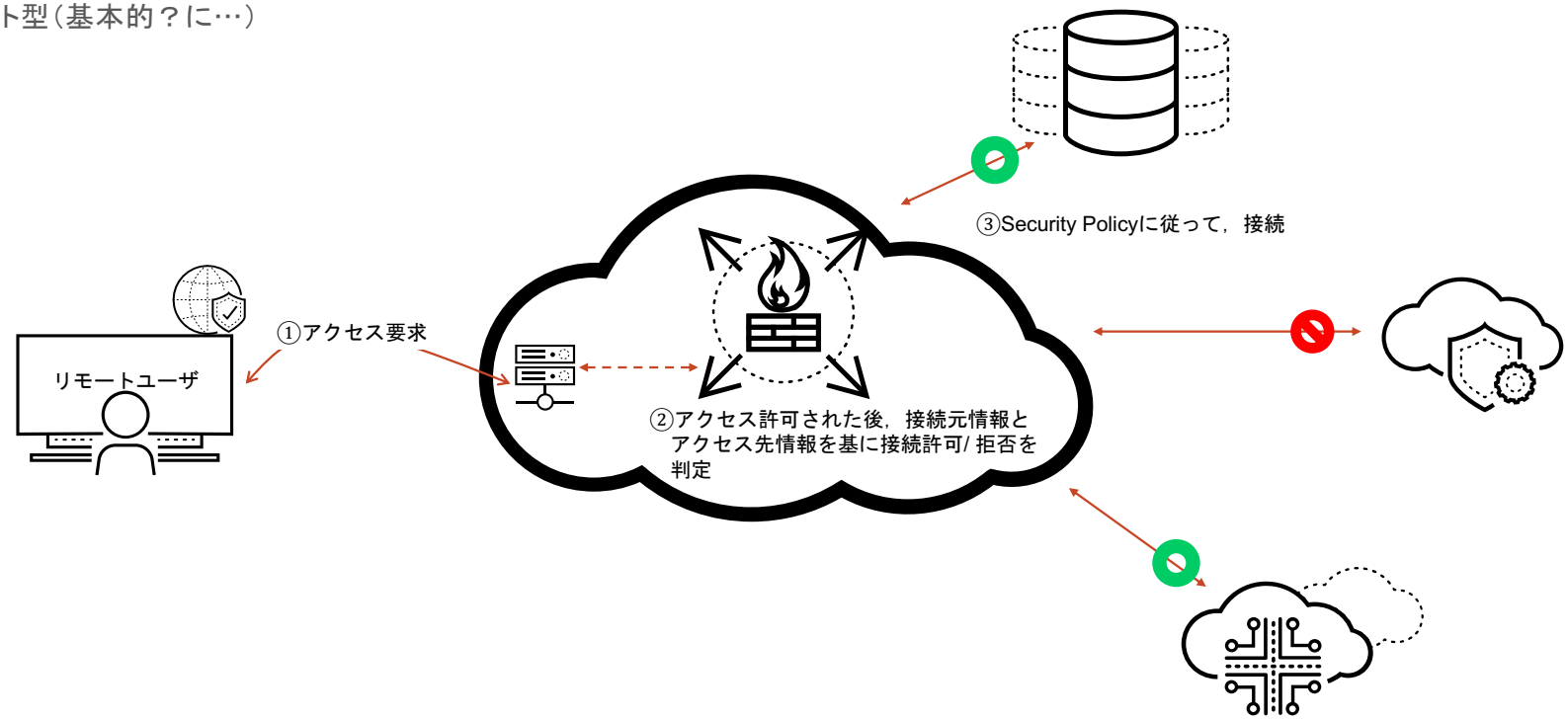
SASEを紐解いてみる（その2）

- 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）

- VPN + ZTNA技術のHybrid方式
  - ユーザ認証情報でVPN接続後，セキュリティポリシ（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. Hybrid

- 結局，どの方式が良いんだっけ？
  - IAP方式
    - ユーザ認証と認可をリクエストごとに実施
    - MFA（Multi
  - SDP方式 = V
    - 認証タイミ
      - 要は，
        続を確
  - Hybrid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

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…

各方式を理解し，ユースケースに応じて適切な方式を検討する必要がある

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？により適する方法が異なる　とか…

個々にネットワーク接

IAP vs. SDP vs. Hybrid比較表

特徴	IAP	SDP	Hybrid
制御範囲	基本的にWebトラフィックのみ	全IP通信（アプリケーション単位）	全IP通信（全ポート/ プロトコル）
ユーザ/ アプリケーション単位のアクセス制御	○	○	○
隠蔽性	アプリの公開FQDNのみ公開	リソースを動的に隠蔽	アプリケーション/ IPの隠蔽
SSL複合	○ （IAPのクラウドにて実行）	△ （SDPアクセスゲートウェイでSSL復号機能に対応しているSSE/SASEあり）	○
非Web通信のアクセス制御	X	○	○
デバイス検疫/ 動的ポリシ	X（対応しているものもあり）	○	○
エージェント	必須ではない	必要	必要
ドメインログオン	X	△（対応しているものもあり）	○
運用面（トラブルシューティング）	△	X	○

SASEとIPv6

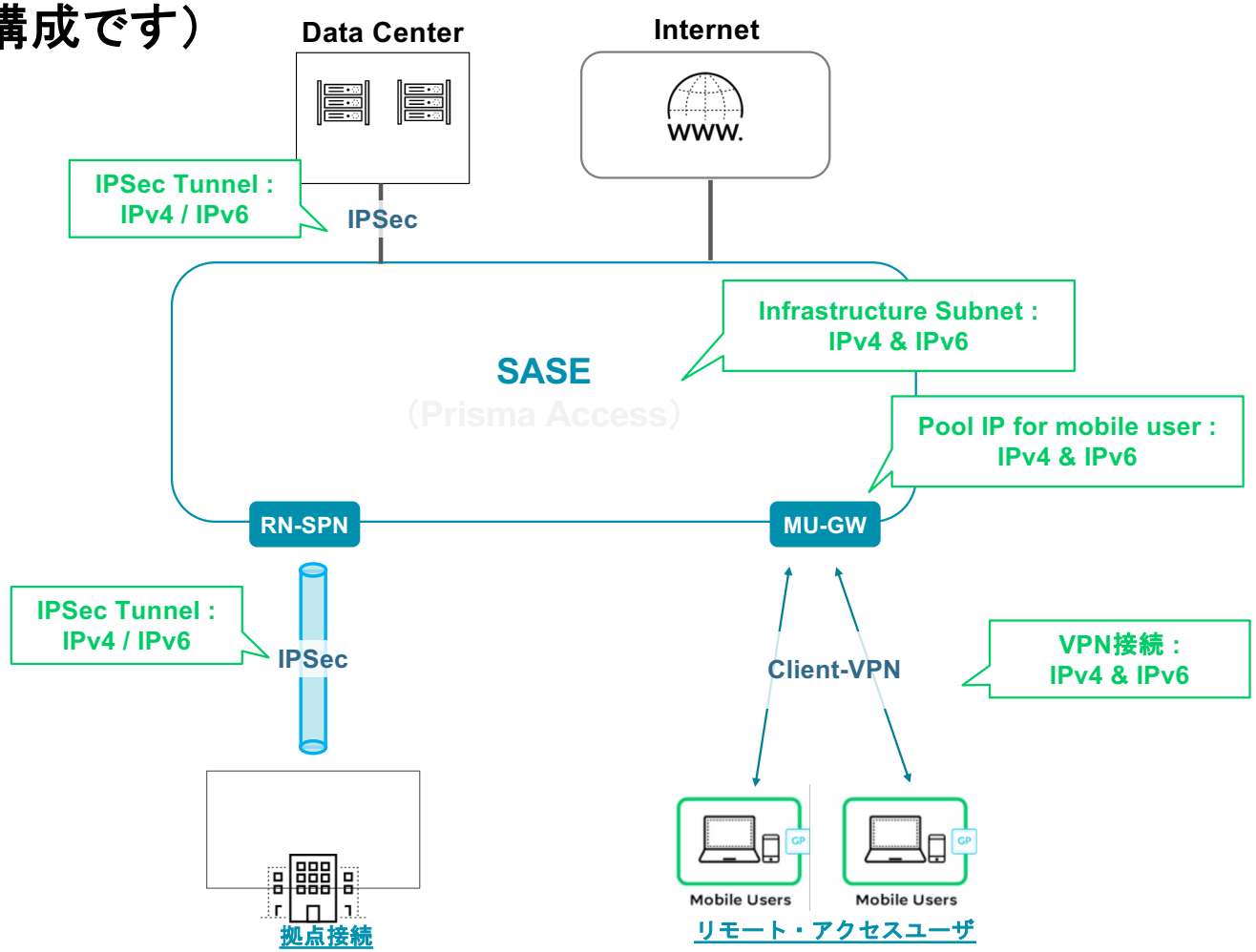
巷のSASEは，IPv6に対応している？

- 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？（ウチも？）

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	○	–	○	–	–	–	Google Public DNS（64）
Dual Stack	Dual Stack(IPv6)	○	○	○	○	NAT64	NPTv6	
IPv6	Dual Stack(IPv6)	○（DNS64/ NAT64）	○	○（DNS64/ NAT64）	○	NAT64	NPTv6	

すごく乱暴にまとめると…

SASEへの接続は，IPv4/ v6どちらでも待ち受けているため，自由に接続してきて構わない
（あくまでもウチの構成です）

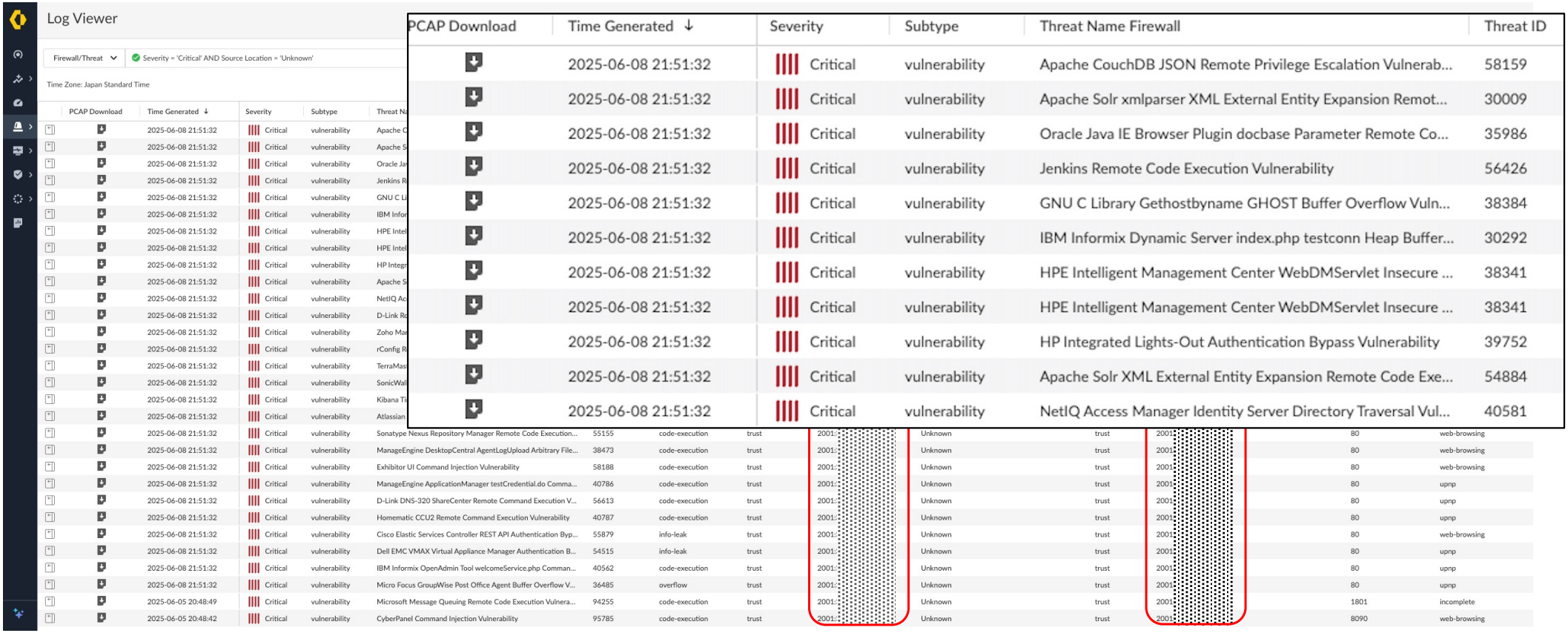
まとめ

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
    - だからと言って，IPレイヤでのセキュリティ対策は不要というわけではなく，v4/ v6どちらにおいてもIPレイヤでのセキュリティ対策は必要
    - 加えて，上位レイヤは，SASEで…
- （今流行りの）SASEとの接続
  - SASEとSSEの違いを理解して，必要な機能/ 方式を選択すべき
  - 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）



NIST サイバーセキュリティフレームワークと各領域に求められるセキュリティ

	エンドポイント		ネットワーク			クラウド		アイデンティティ	AI Apps
	サーバー	クライアントPC スマートデバイス	ユーザー	データセンター	拠点 (オフィス/店舗/工場...)	SaaS	IaaS/PaaS		
統制 Govern									
特定 Identify	各種テスト/ アセスメント	攻撃面管理 ASM	脆弱性管理 Vul. Mgmt	資産管理 Asset Mgmt		態勢管理 SSPM / DSPM / CSPM		特権管理 PAM	AI-SPM Red Teaming
防御/阻止 Protect	端末制御	メール セキュリティ	セキュア ブラウザ	リモート アクセス	NGFW / UTM	API CASB	CWP CNS CIEM コードセキュリティ	ID/アクセス管理 IAM	AI Runtime AI Agent
	EPP		SSE / SASE ZTNA / SWG / CASB/DLP			DLP			
分析/検知 Detect	EDR		NDR			CDR		ITDR	AIDR
	XDR								
	セキュリティ情報イベント管理 SIEM					振る舞い分析 UEBA			
調査/対応 Respond 復旧 Recover	セキュリティ運用オーケストレーション＆自動化 SOAR						脅威インテリジェンス管理 TIM		
外部サービス	各種監視・SOCサービス								
体制	端末/サーバ担当		NW担当			クラウド担当			インフラ担当

質疑応答/ ディスカッション