Airheads Academy
これから始めるSASEとゼロトラスト

2024/7/26
日本ヒューレット・パッカード合同会社
Aruba事業統括本部

Agenda

- ゼロトラストとは？
- ゼロトラストが注目されている背景
- Arubaが提供する全方位ゼロトラスト
- SASEとは？

Agenda

- ゼロトラストとは？
- ゼロトラストが注目されている背景
- Arubaが提供する全方位ゼロトラスト
- SASEとは？

ZERO TRUST IS

- “ゼロトラストとは、NWが侵害されている場合であっても、情報システムやサービスにおいて、各要求を正確かつ最小権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体である”

NIST SP-800-207定義より

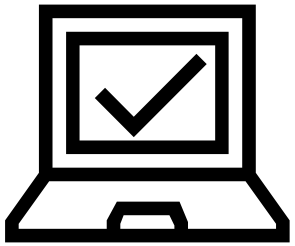
NIST：米国国立標準技術研究所

ゼロトラストアクセスの考え方

暗黙的なトラストゾーンを最小化/動的な認可ポリシー変更

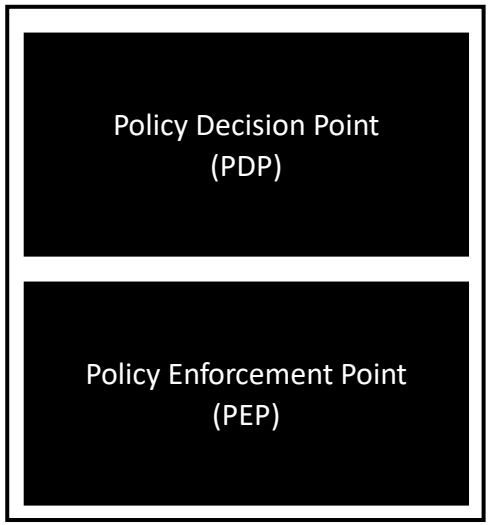
Subject/System

- PC
- Mobile
- アプリなど
- **攻撃者も含む**



Untrust Zone

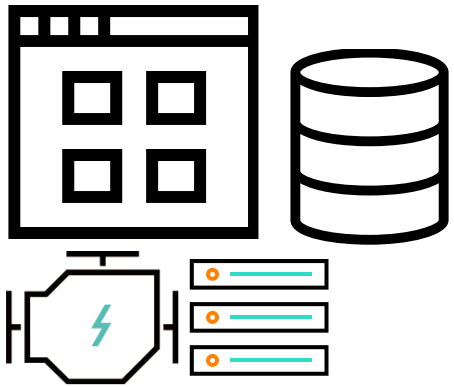
PEP/PDP



暗黙的な
Trust Zone

Resource

- コンピュータ
- データ
- IoTデバイス
- プリンターなど



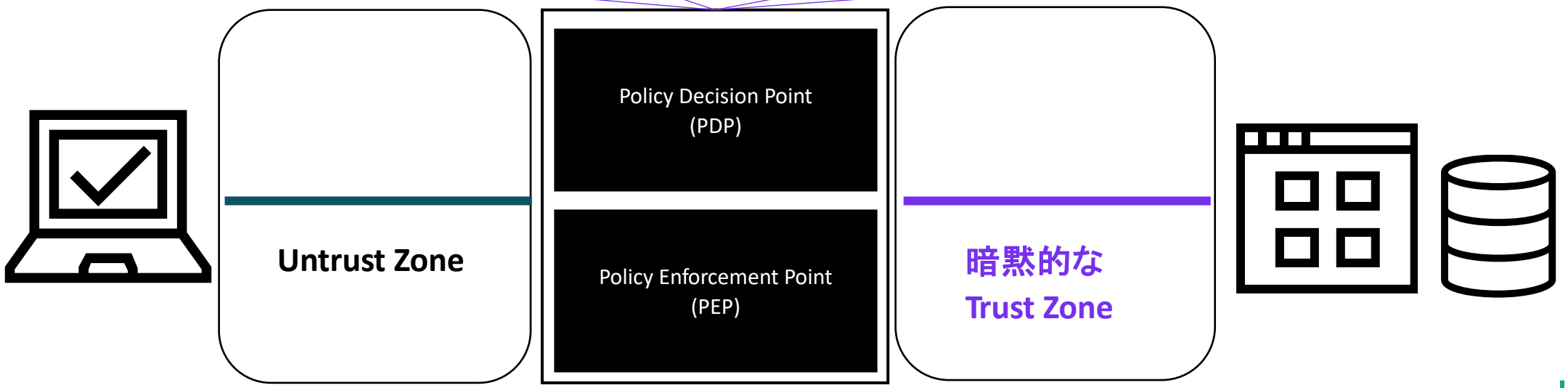
ゼロトラストアクセスの考え方

空港・搭乗時のたとえ

認証

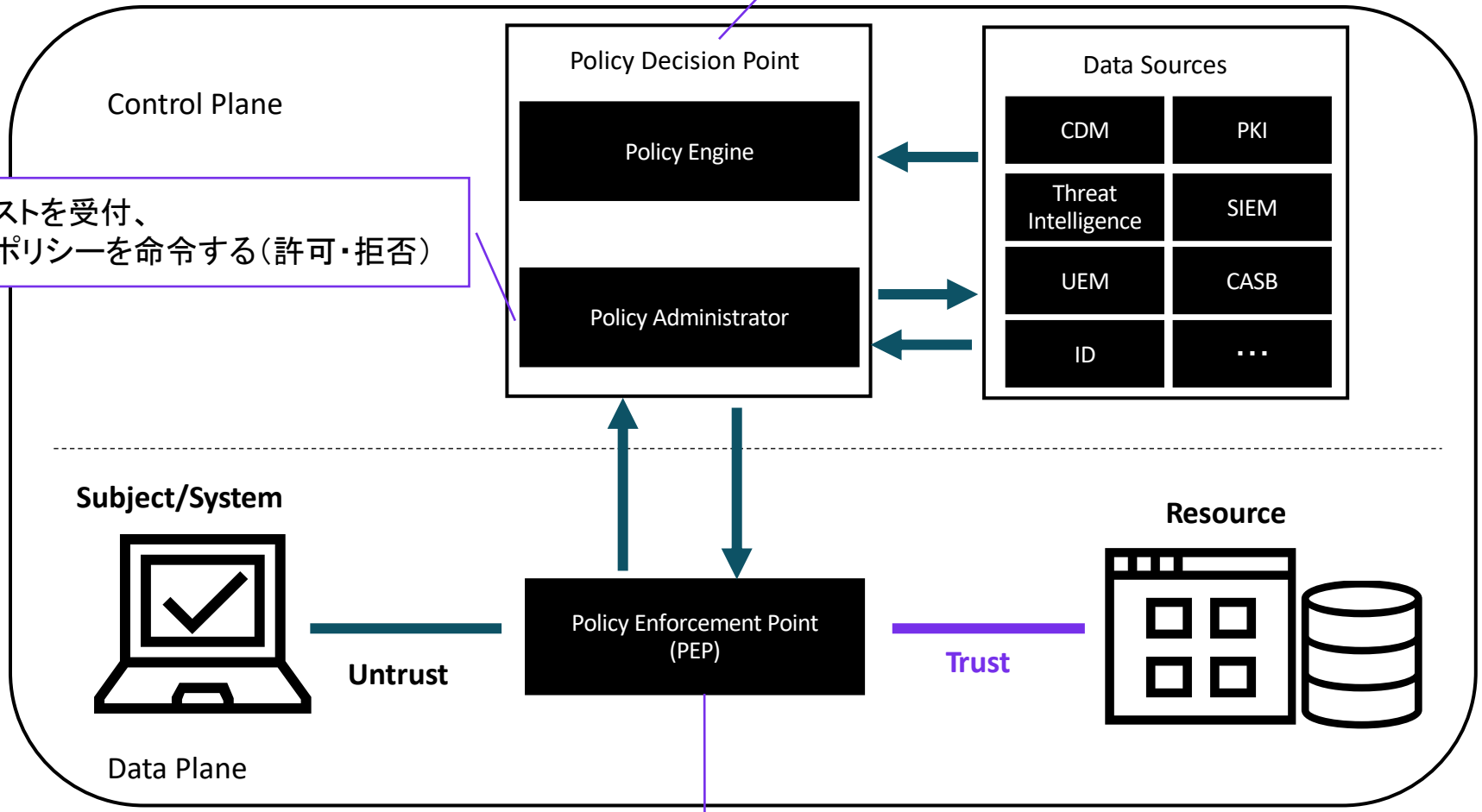
認可

最小権限



ゼロトラストの論理コンポーネント

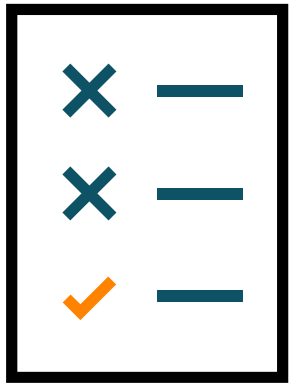
- リソースへのアクセス許可・拒否を決める
- リアルタイムに監視を行い、動的に認可ポリシーを変更する



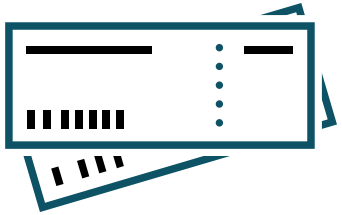
- PEPから認証リクエストを受付、
- PEPに対して、認可ポリシーを命令する（許可・拒否）

- 企業リソースへの接続を許可、監視、遮断する
- Policy Administratorに認証要求を送信する
- Policy Administratorから認可ポリシー更新を受け取る

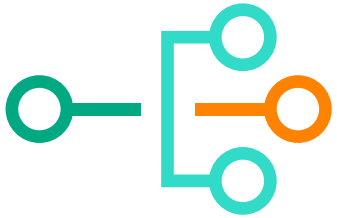
ゼロトラストの原則



常に認証認可する



最小アクセス権限



突破を想定し、監視
/動的に認可を変更

ゼロトラストの原則：Never Trust, Always Verify

信頼できる端末のみ許可

認証・認可、二要素認証を適切に行い、リソースへのアクセス権があるかを明示的に確認する

認証・認可＋二要素認証

最小限のアクセス

認証・認可を元に、必要十分なリソースへのアクセス権だけを与えるべく、**ロールベースアクセス制御（RBAC）**を行う

RBAC & ZTNA

脅威は既に侵入している

脅威の拡大を最小限に留めるべく、**セグメンテーション**を適切に行う。このセグメンテーションは脅威の侵害に対応（脅威を隔離）するため動的に行うことが求められる

ステートフルサービス

ゼロトラスト

- ✓ いつでも守る
- ✓ どこからでも守る
- ✓ どんなデバイスでも守る

Work Anytime

どの時間帯でも快適で安定したネットワークを提供

Work Anywhere

働く場所に関わらず、安全で安定したConnectivityを提供

Work from Any Device

PCと同様の設定が施された他デバイスを活用

Agenda

ゼロトラストとは？

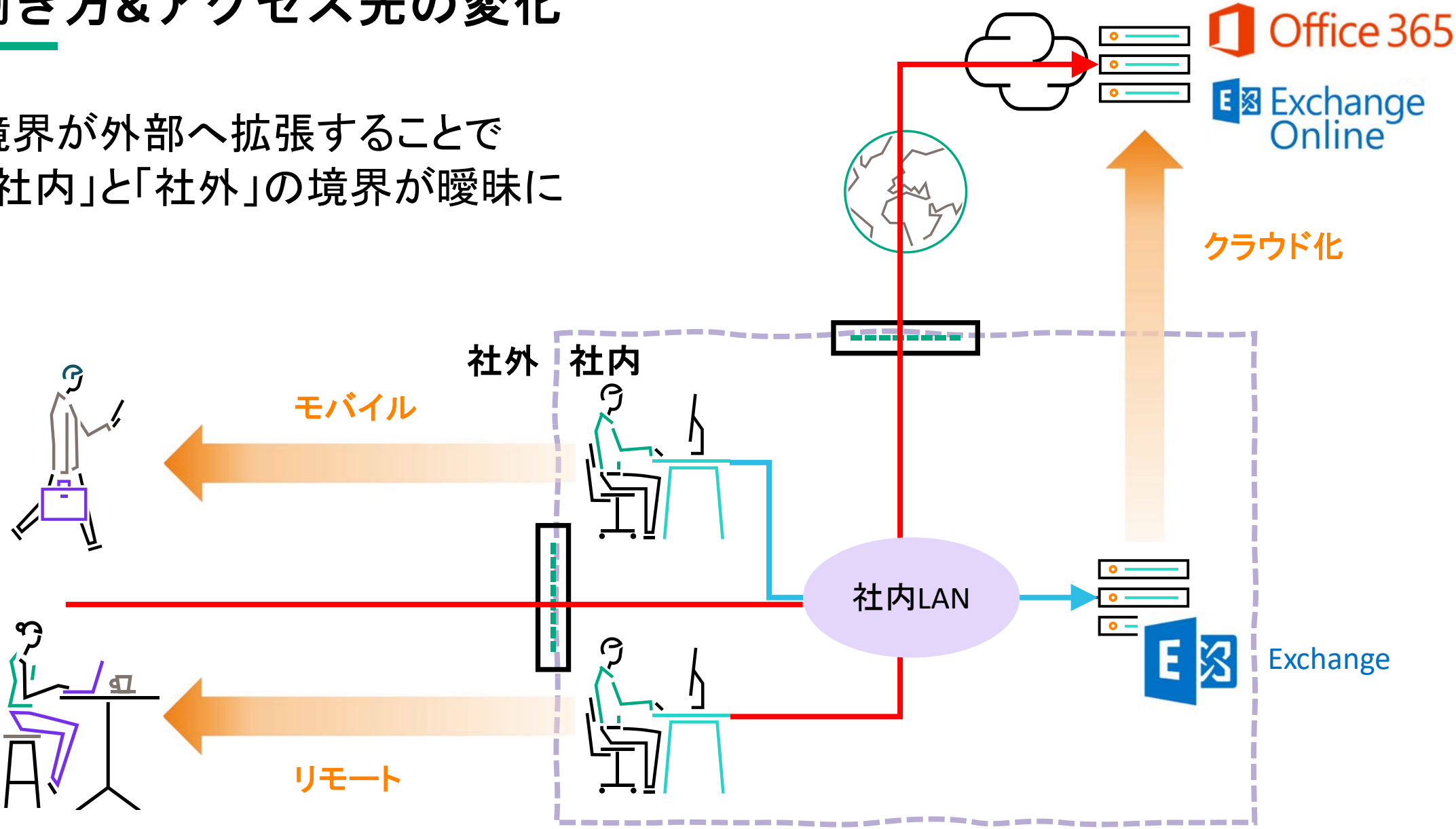
ゼロトラストが注目されている背景

Arubaが提供する全方位ゼロトラスト

SASEとは？

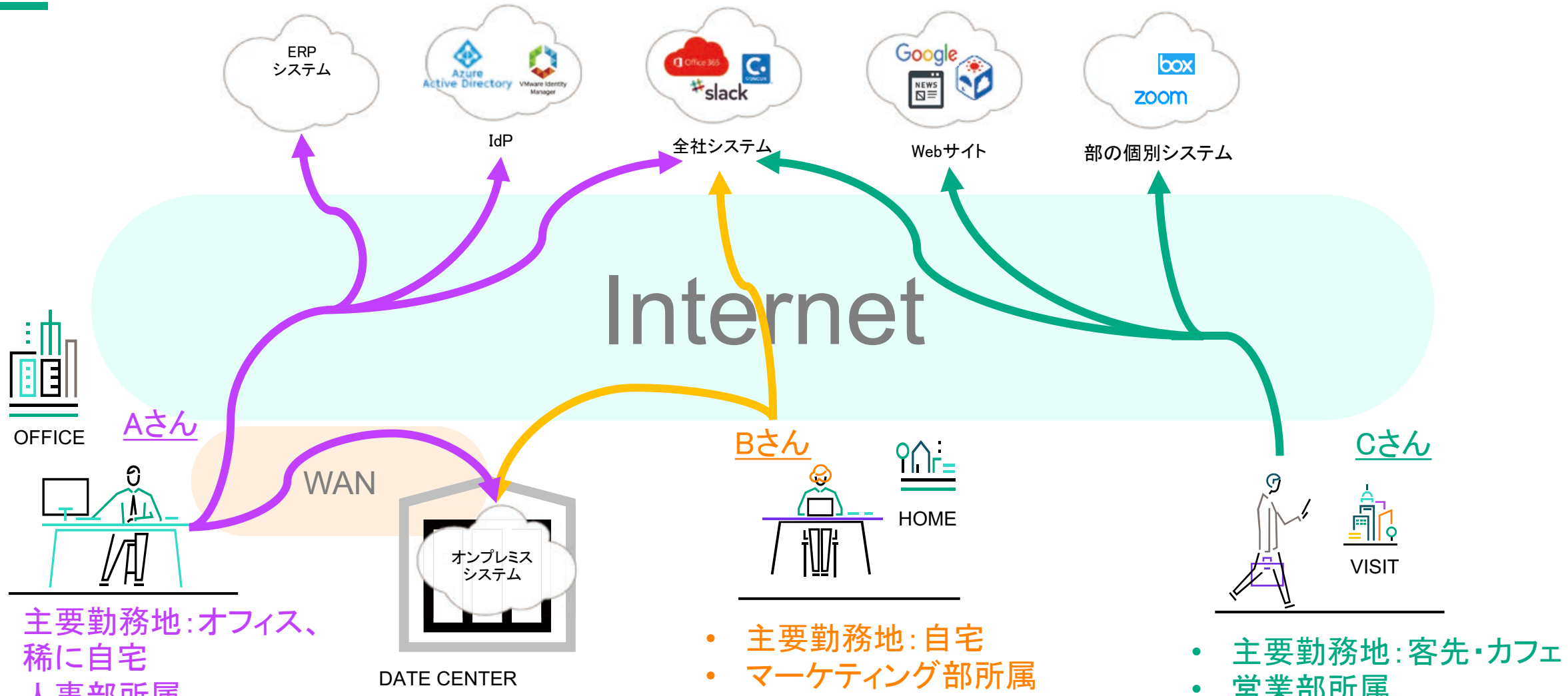
働き方&アクセス先の変化

境界が外部へ拡張することで
「社内」と「社外」の境界が曖昧に



働き方＆アクセス先の変化によってネットワークに起きていること

接続元・接続先双方の多様化



- 主要勤務地：オフィス、稀に自宅
- 人事部所属

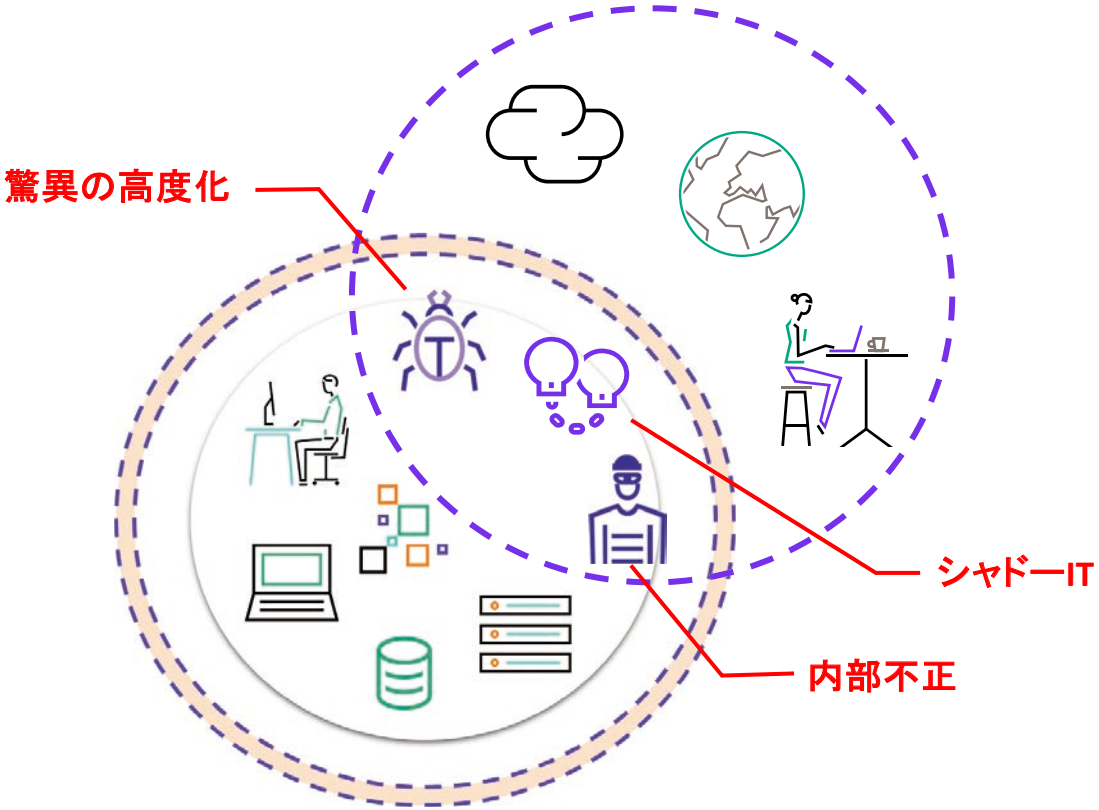
- 主要勤務地：自宅
- マーケティング部所属

- 主要勤務地：客先・カフェ
- 営業部所属

境界型セキュリティの弱点

従来の境界型セキュリティモデル

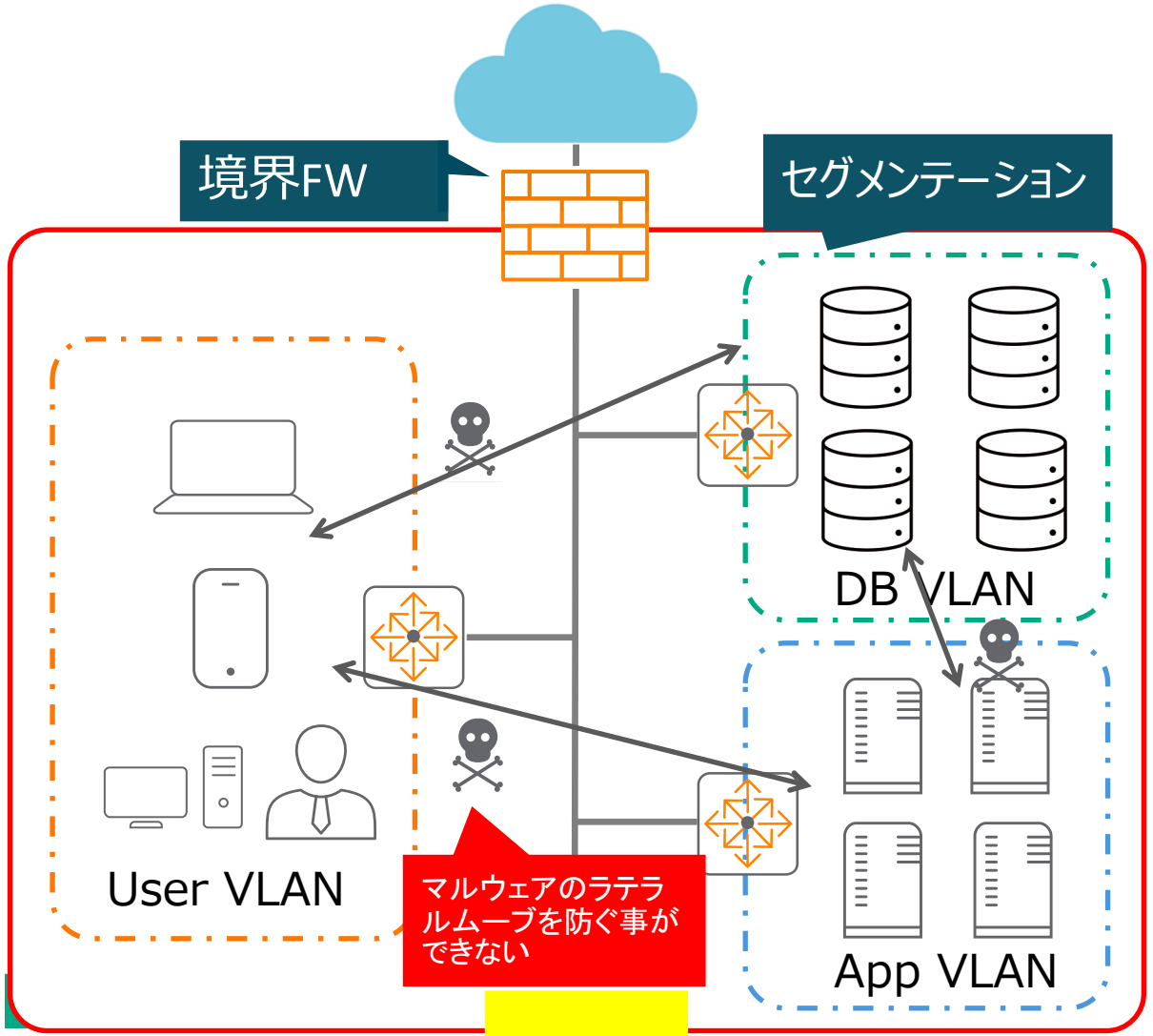
- 外部（インターネット）=信頼できない
- 内部（社内LAN）＝信頼できる
- 情報資産は企業内部に存在
- 従業員は信頼できる



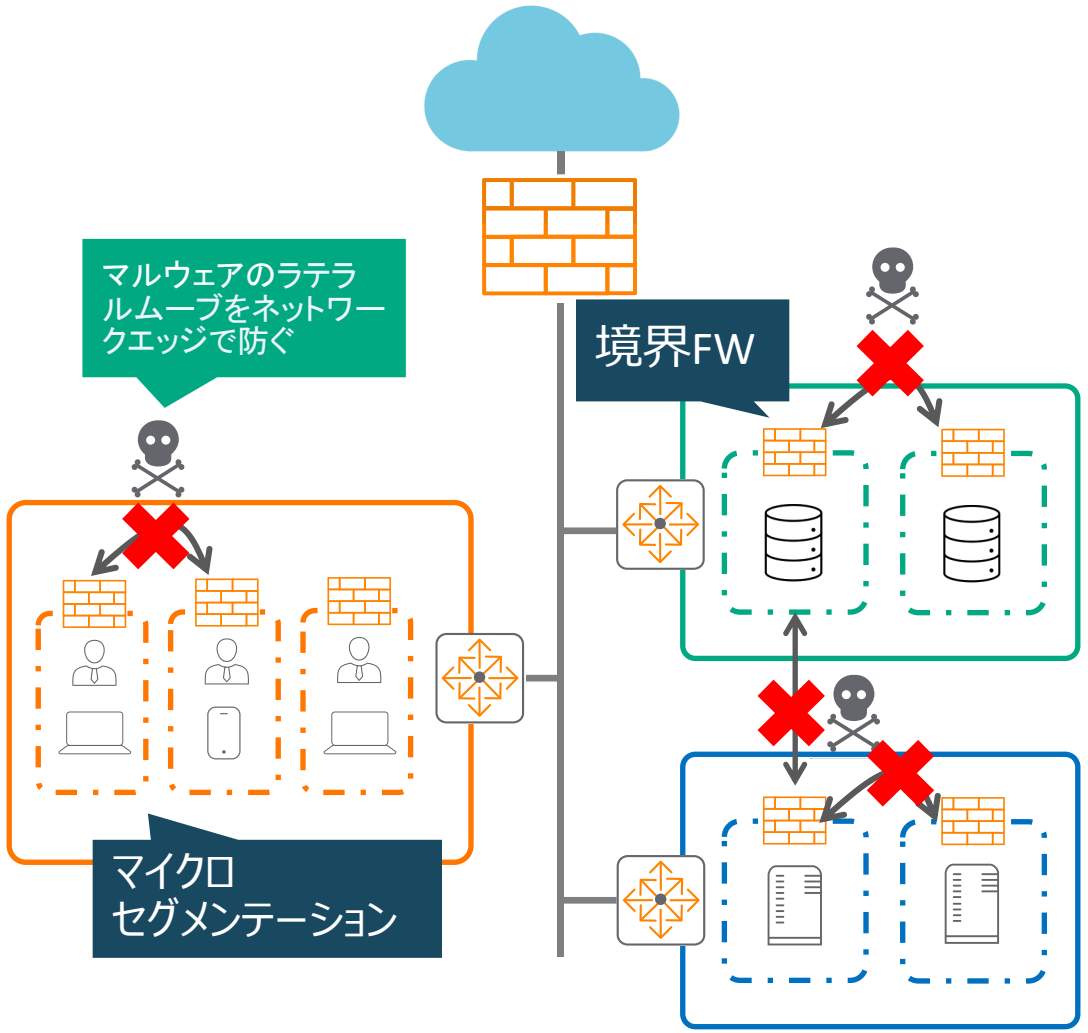
- 内部（社内LAN）の拡張によって境界の崩壊
- 情報資産は企業外部にも分散
- 高度化した脅威が境界を超える
- 従業員は信頼できない

ネットワークエッジでマルウェアのラテラルムーブを防ぐ

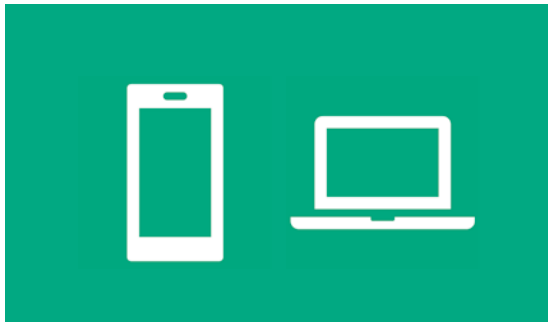
従来の境界型防御



Micro Perimeter & Micro Segmentation



ランサムウェアのターゲット



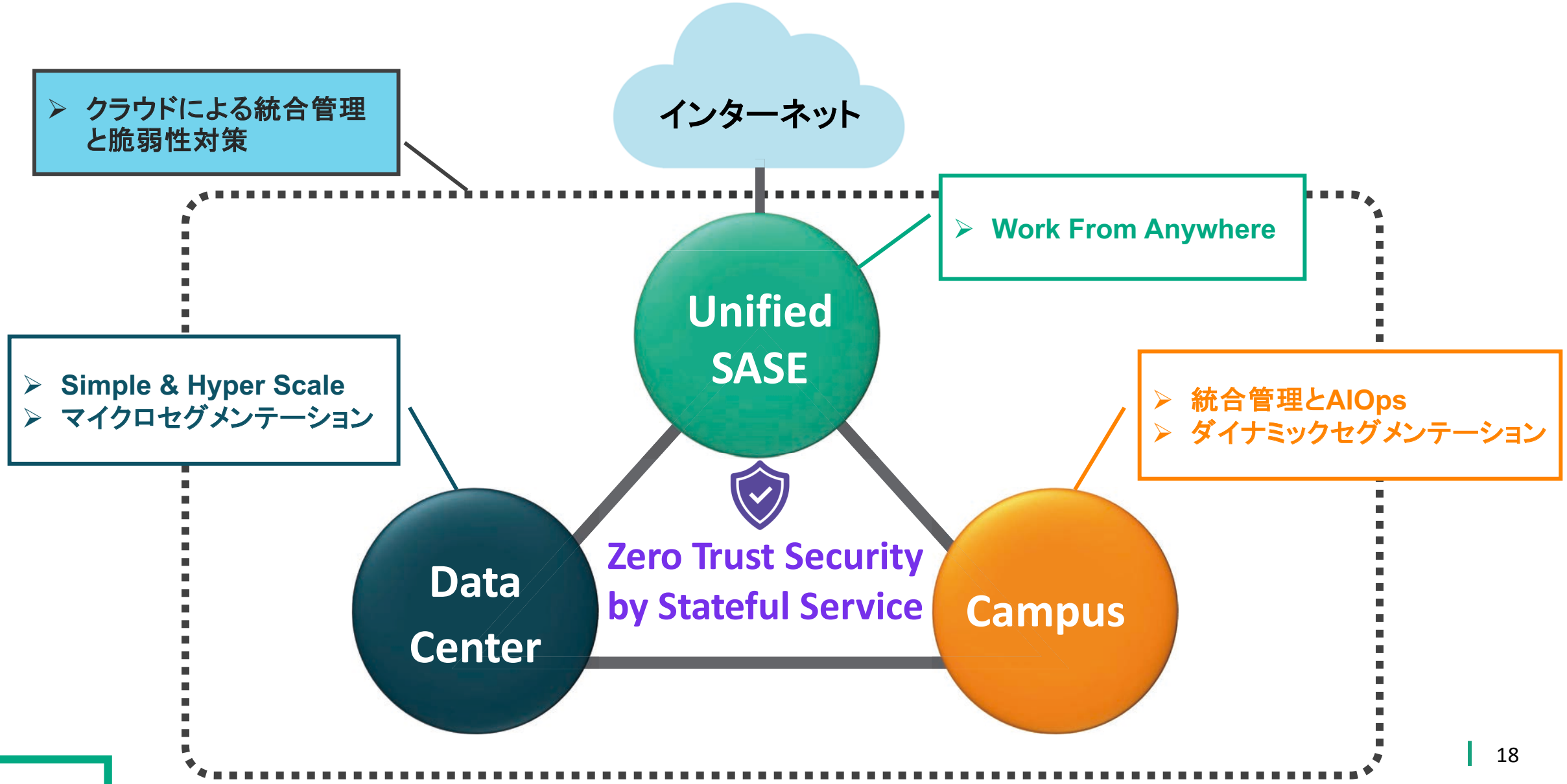
80 - 90%
はBYODや非管理端末

70%
は500人未満の組織

25%以上
が製造業や教育関連

Source : https://www.microsoft.com/ja-jp/security/security-insider/microsoft-digital-defense-report-2023

HPE Aruba Networking が実現する 全方位ゼロトラスト



Agenda

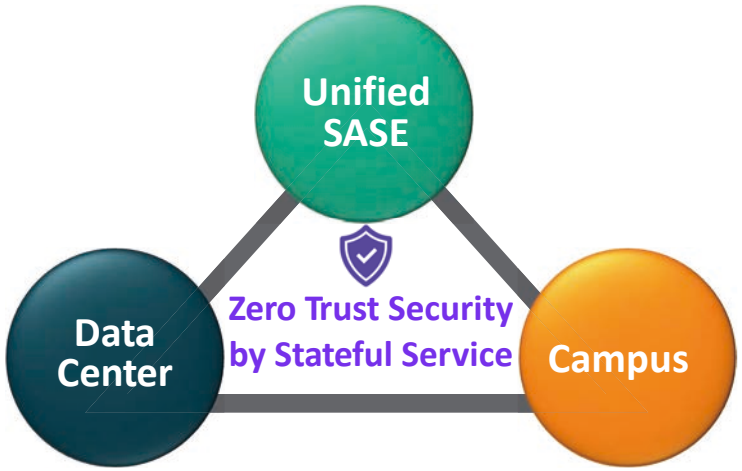
ゼロトラストとは？

ゼロトラストが注目されている背景

Arubaが提供する全方位ゼロトラスト

SASEとは？

HPE Aruba Security-First Networking のコンポーネント



Modern Cloud Security

- SSE : ZTNA, SWG, CASB, DEM
- 統合SSEプラットフォーム
- シンプルな管理UI

SD-WAN Modernization

- クラウド連携
- UTM + ルータ
- アプリケーションの最適化

SASE Initiative

- Unified SASE
- Work from Anywhere の実現

Data Center Network Modernization

- 運用の簡素化
- 800Gbpsのステートフルサービススイッチ
- Micro Segmentation

Campus Network Transformation

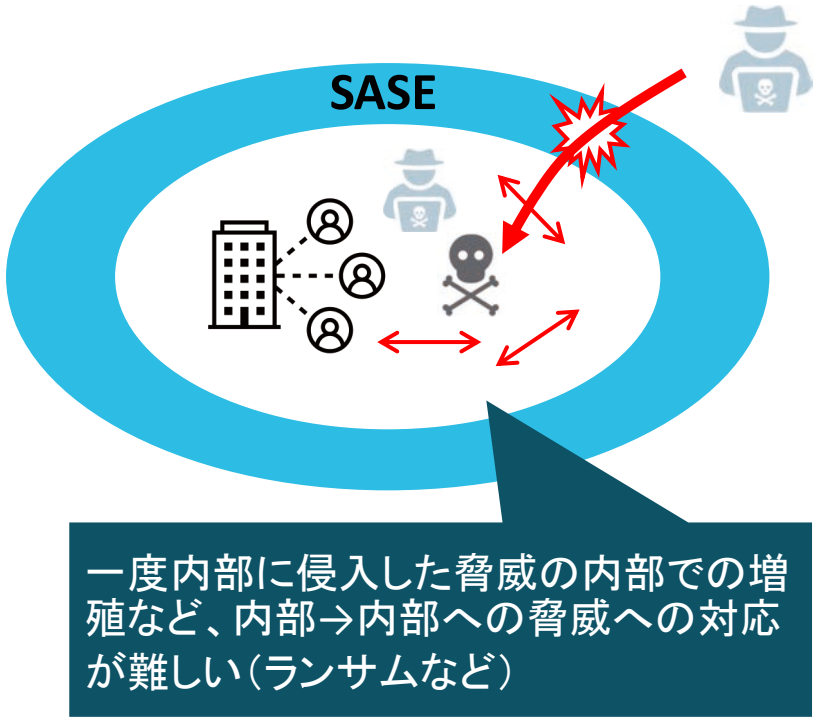
- Unified Infra
- Wi-Fi, Wired, IoTの最適なアクセス
- AIOps & Security

NAC-Driven Segmentation

- ロールベースポリシーの一元化
- Dynamic Segmentation

LANセキュリティの重要性：SASE だけではランサムに対応できない

Campus



SASEでカバーしている領域

Device セキュリティ
端末の不正なふるまいを阻止

- ゼロデイ攻撃で検知できなかったら？
- 対応していない端末は？

Gateway セキュリティ
外部からの攻撃を防御
内部から外部への不正通信を阻止

- 内部への侵入を許してしまったら？
- 直接内部へマルウェアを持ち込まれたら？

LANセキュリティ
内部、外部へのアクセス制御を定常的に実施
脅威が侵入してしまった時も被害を最小限に止める

- ネットワークセキュリティの最後の砦！

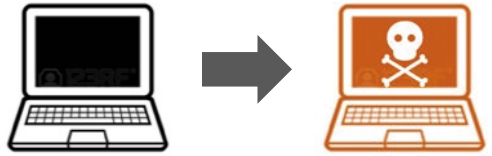
ネットワークのRBAC
Dynamic Segmentation

RBAC: Role-Based Access Control

LANセキュリティの課題

多種多様なユーザ・端末・
非管理端末がアクセス

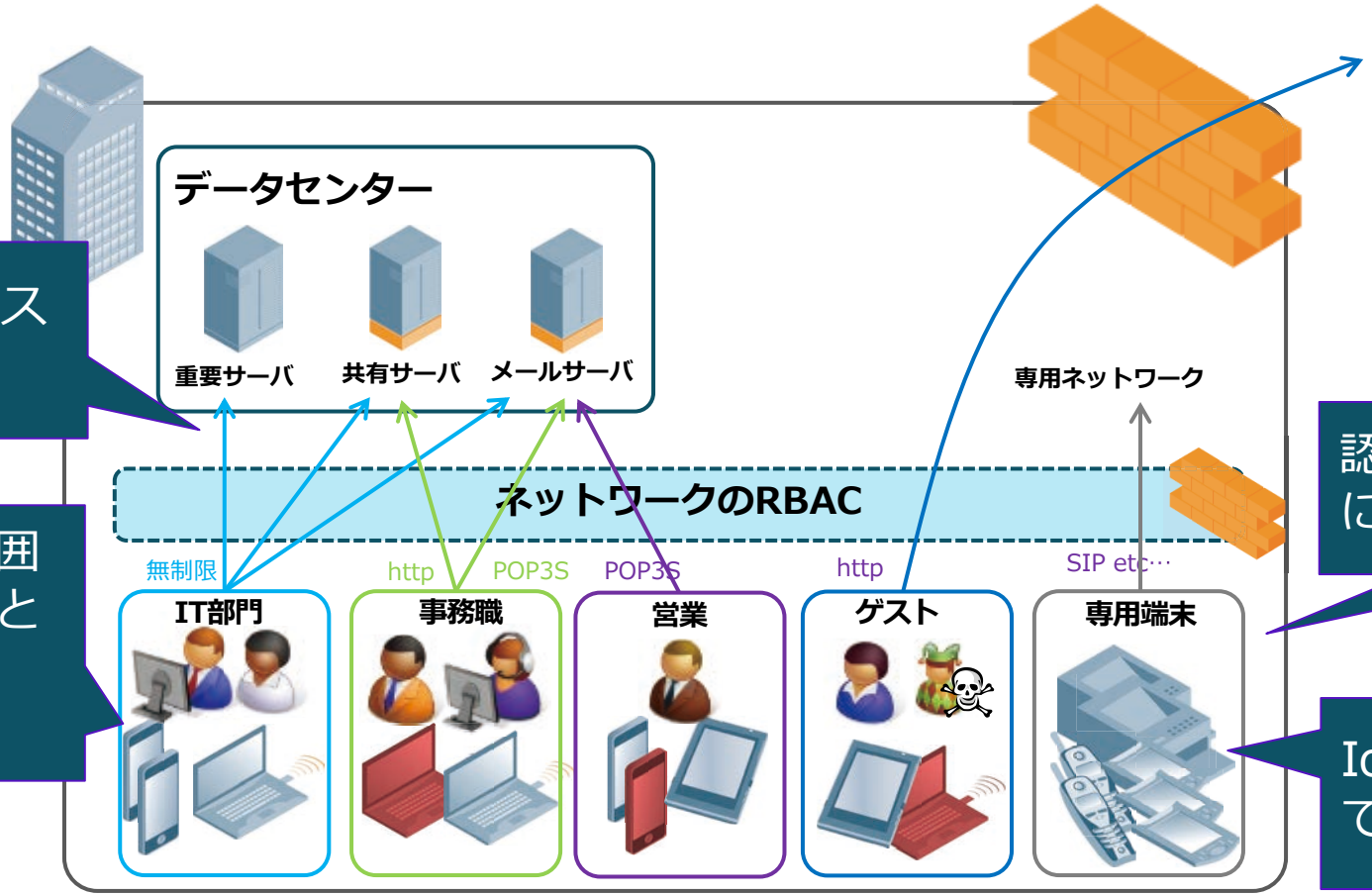
どのように識別するか？



端末の振る舞いによって
ステータスが変わる
（ランサム感染など）

接続後の端末への対処

ネットワークのRBAC



アクセス先のリソースとプロトコルを制限

脅威侵入時の影響範囲を最小限に留めることができる
＝**Segmentation**

認証・認可の情報を元にRoleを適用する

IoTなどIPで接続する全ての端末に適用が可能

ゼロトラストCampus LAN

Campus

Dynamic Segmentation

外部セキュリティ製品と連携することで、インシデント発生時に速やかに端末をネットワークから隔離する**動的なセグメンテーション（Dynamic Segmentation）**が可能

Notification

3rd Party Security Appliance

Policy Decision Point

ClearPass

RADIUS
Dynamic Authorization

アンダーレイはそのまま、**オーバーレイ**でゼロトラストネットワークを構築

Device/Role

- 管理PC
- BYOD
- IOT
- ゲスト

Access Switch

GRE Tunnel

GRE Tunnel

Access Point

Policy Enforcement Point

Mobility Gateway

ネットワークの
RBAC

Resource

Trusted

Untrusted

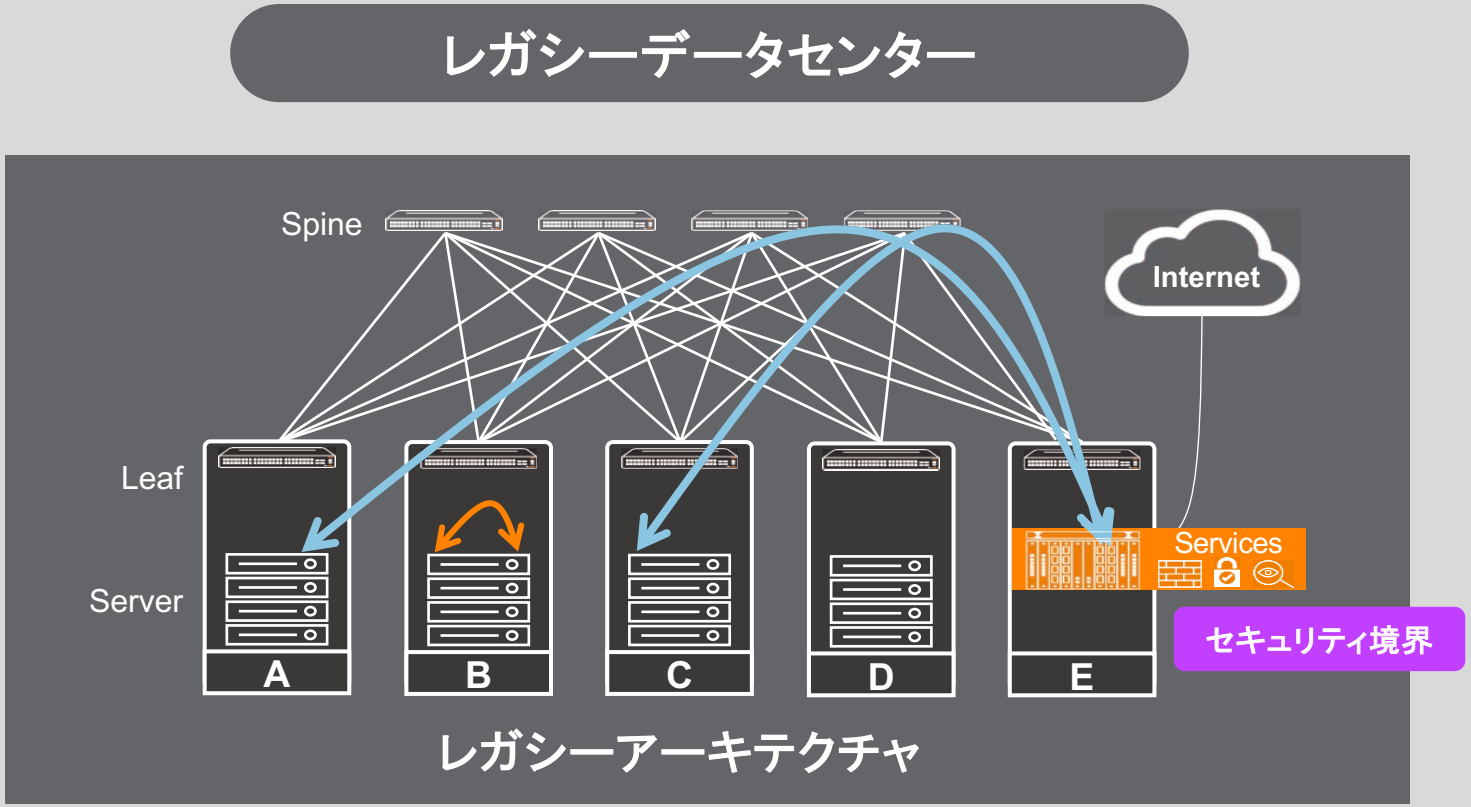
- SaaS
- 不審なサイト
- 社内サーバ
- 社内端末

ステートフルファイアウォール機能を兼ねているため、外部、内部から端末への不正アクセスをデフォルトでブロック

Micro Segmentation & Perimeter を実現

分散型アーキテクチャで実現するゼロトラストデータセンター

DC

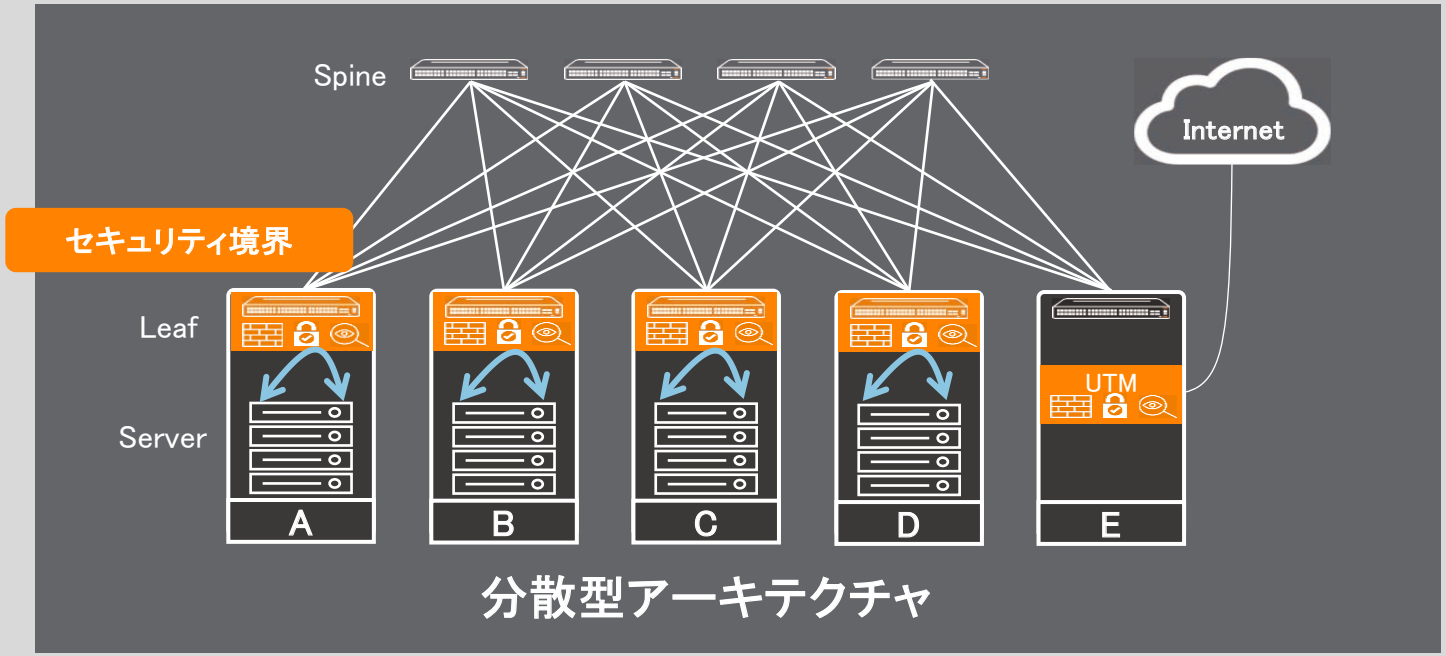


- シングルポイントでスループットが出ない
- 高性能ファイアウォールのため高コスト
- 結果的にマイクロセグメンテーションを未実装

分散型アーキテクチャで実現するゼロトラストデータセンター

DC

これからの分散型データセンター



- 分散型のため、スループットが劇的に向上
- スイッチと一体型でTCOを削減
- マイクロセグメンテーションを実装しゼロトラストを実現

Aruba CX 10000

HPE aruba networking + AMD PENSANDO

DPU1 (AMD PENSANDO) | CPU | DPU2 (AMD PENSANDO)

Trident-3 ASIC

ステートフルF/W
DDoS対策
暗号化

Agenda

ゼロトラストとは？

ゼロトラストが注目されている背景

Arubaが提供する全方位ゼロトラスト

SASEとは？

SASEの構成要素　　SASE= SD-WAN + SSE

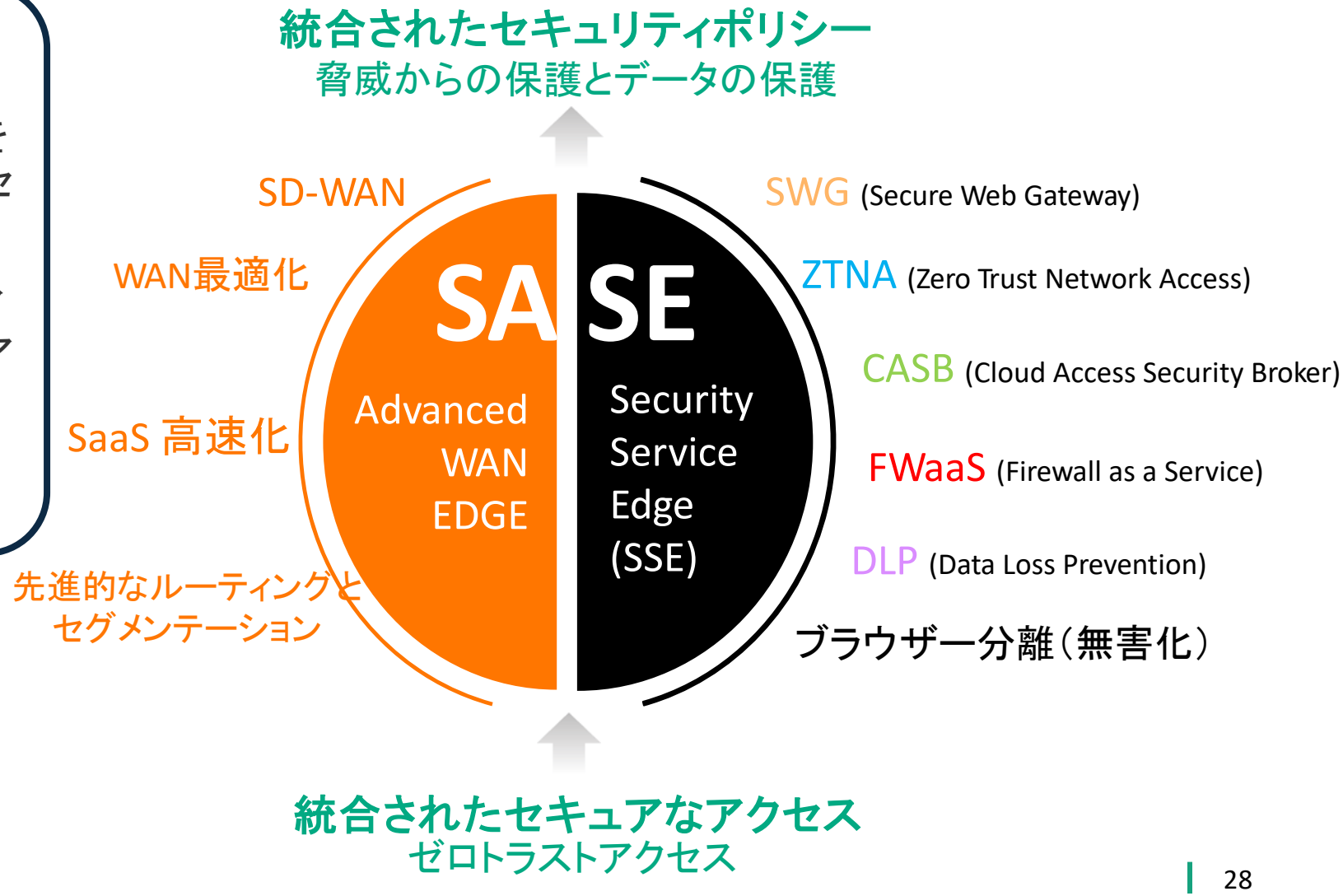
SASEとは？

Secure Access Service Edge

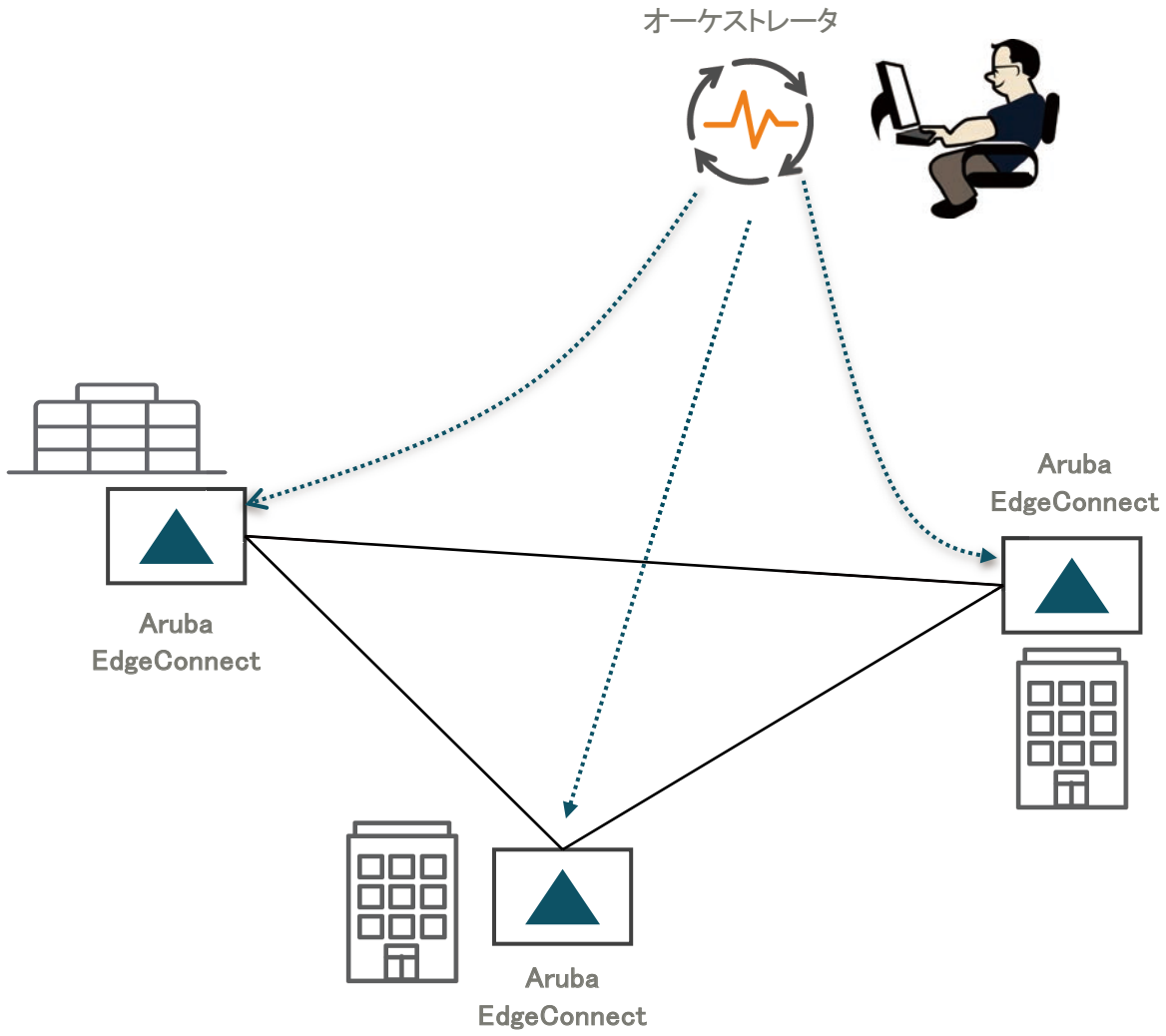
SASEは、SD-WAN/SWG/CASB/NGFW/ZTNAを含む、サービスとしての統合ネットワークとセキュリティ機能。

SASEは主にサービスとして提供され、デバイスやユーザのアイデンティティに基づき、リアルタイムのコンテキストとセキュリティポリシーを組み合わせたゼロトラストアクセスを可能にします。

SASEはゼロトラストの概念を実現するためのフレームワーク



SD-WANとは？



SD-WAN = Software Defined WAN

ソフトウェアによる制御でWAN(広域ネットワーク)を動的／柔軟に管理、運用する技術

オーケストレータと呼ばれる管理ソフトウェアで地理的に分散したネットワーク機器を集中的に管理する

- 設定をオーケストレータで集中的に行うため、各ルータで矛盾のないように一貫性をもった状態で設定の維持／管理が可能
- 簡単にIPSecによるVPNを構成できるルータ
- PBR機能を強化したルータ

SSE (Security Service Edge) が提供する主要な機能

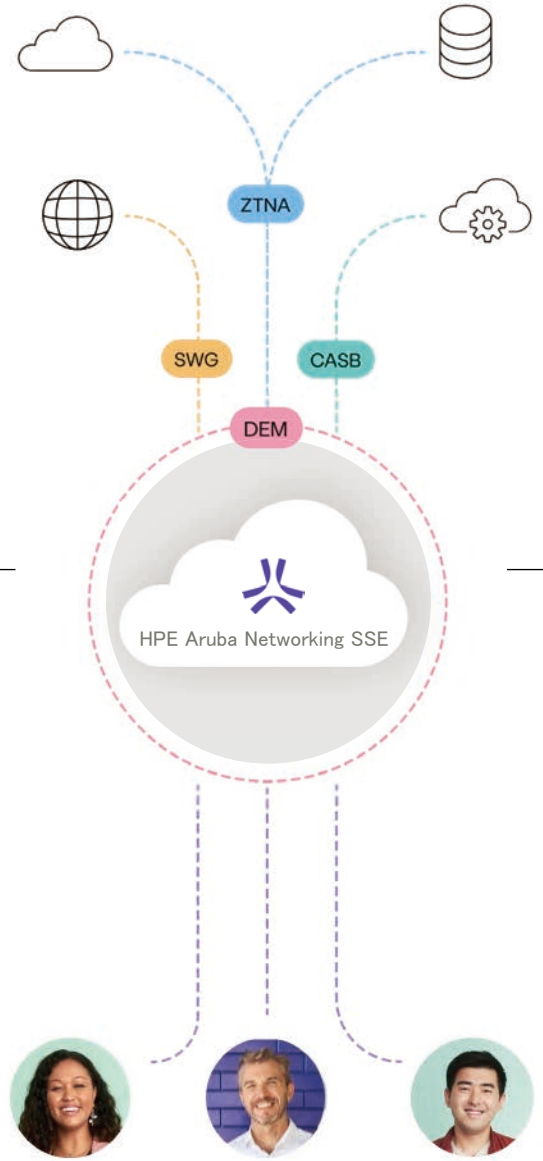
ZTNA

エージェントの有無に関わらずデータセンタ、パブリッククラウドのアプリケーションに対してセキュアなリモートアクセスを提供
例：VPN/VDI のリプレイス

SWG

インターネットへアクセスを制御し、悪意のあるサイトから保護

例：URL filtering ギャンブル/マルウェア、DNS control, SSL inspection for マルウェア



CASB

セキュアなSaaSアクセスを実現し、データ損失から保護を行います

例：SalesForce/Sharepoint/BoxなどのSaaSアプリケーションへのアクセス、Upload/Downloadの制御

DEM

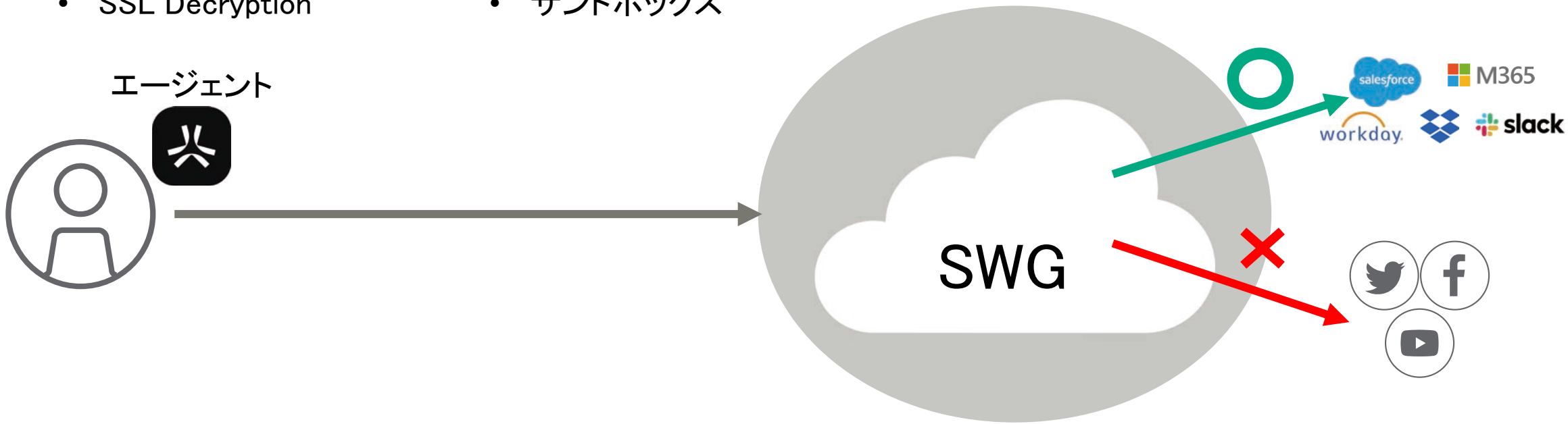
ユーザ通信のパフォーマンスを観測し、アクセスに関する問題をトラブルシュート

例：プライベート/インターネット宛通信に対するレイテンシーを計測

Secure Web Gateway（SWG）とは

全てのWeb/インターネット宛通信を分析しクライアント発の通信を検査し、定義したポリシーに従って
通信を許可・拒否するWebセキュリティのソリューション

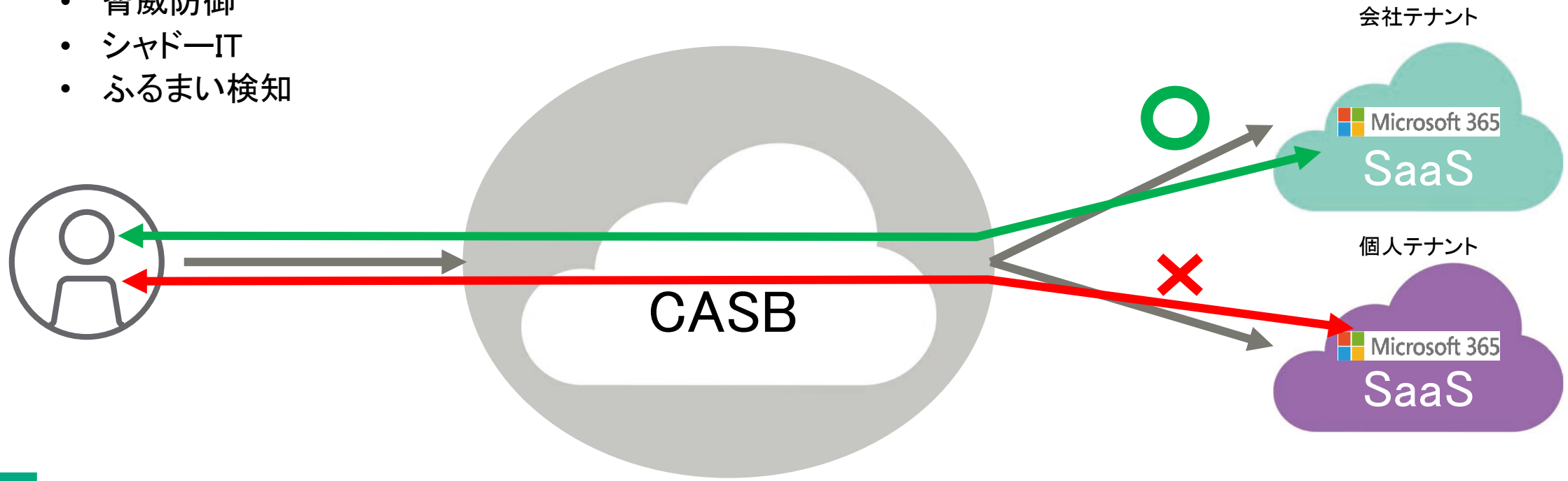
- URLフィルタリング
- コンテンツフィルタリング
- SSL Decryption
- Web分離
- アンチウィルス
- サンドボックス



CASB（Cloud Access Security Broker）とは

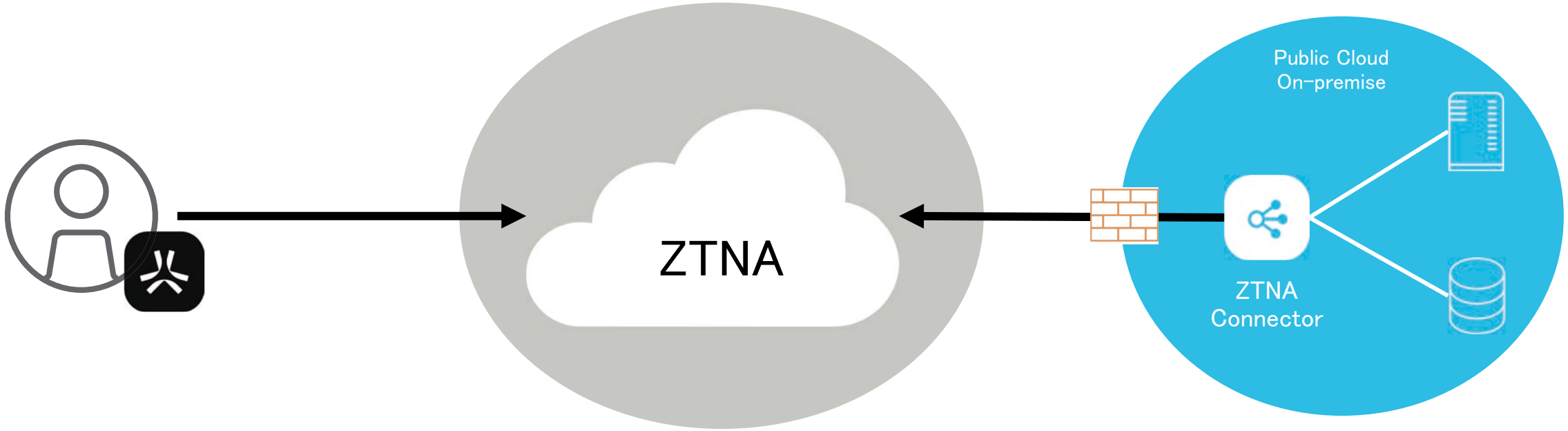
ユーザとクラウドサービスの間に制御箇所を設けて利用状況の可視化・制御を可能にするソリューション。
SWG+CASBと一緒に利用することがとても多い

- SaaSアプリケーションの可視化
- データセキュリティ
- 脅威防御
- シャドーIT
- ふるまい検知



ZTNA (Zero Trust Network Access) ≒ Remote Access

ZTNAの場合、クラウドがHubとなりクライアントの通信をZTNA Connectorへ中継するような仕組みになります。
AgentとConnectorがSSEとセッションを確立し、確立したセッションを介して到達性を確保します。



- ✓ インターネットに晒す必要無
- ✓ DDoS/脆弱性の対処も必要無
- ✓ トラフィック量が増加したらオートスケーリング

コンテキストに基づいたアクセス制御

認証ソース

グループ	接続元	時間帯
正社員	どこでも	いつでも
協力会社	日本国内のみ	日中帯のみ

正社員

協力会社

- エージェントインストール
- ディスク暗号化
- OSアップデート適用
- Firewall
- EDRのインストール状況

貸与PC

ZTNA
社内アクセス

全てのリソースに
アクセス許可

私用端末

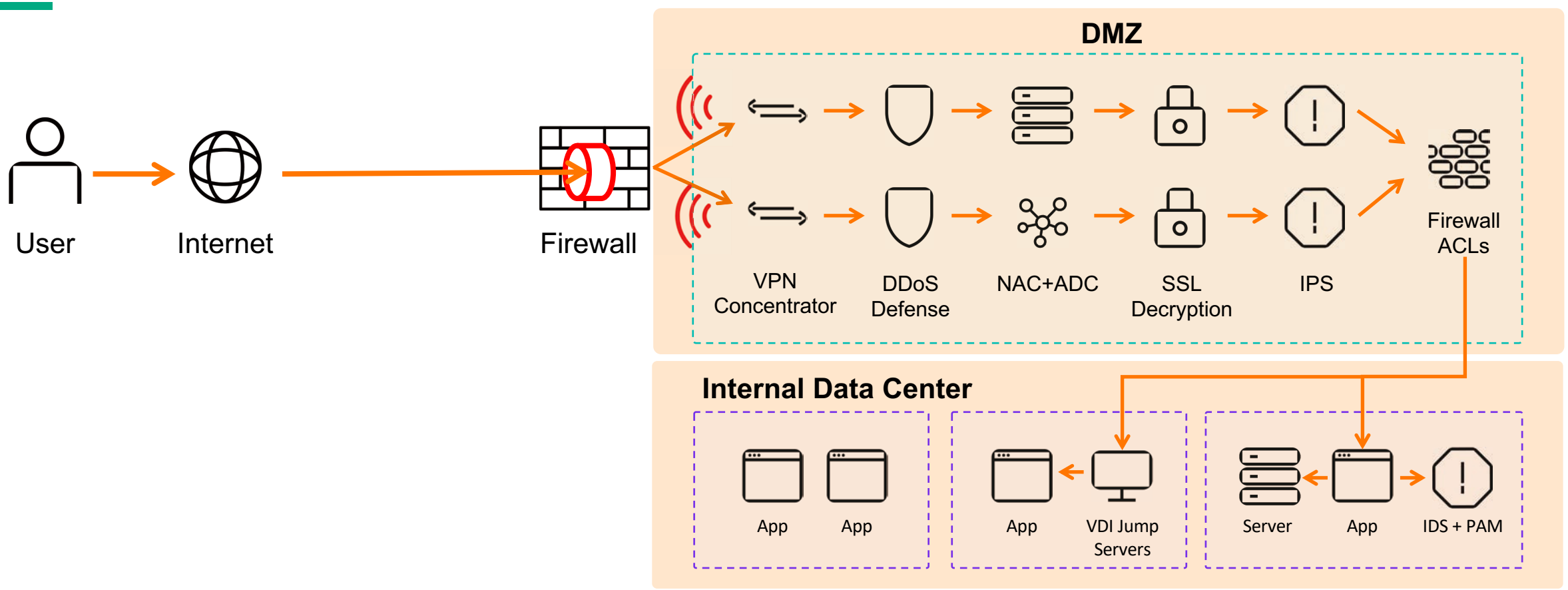
限定的なZTNA
社内アクセス

Web Appのみ

- ディスク暗号化
- OSアップデート適用
- Firewall

VPNが持つセキュリティリスク

SASE



攻撃対象になりやすい

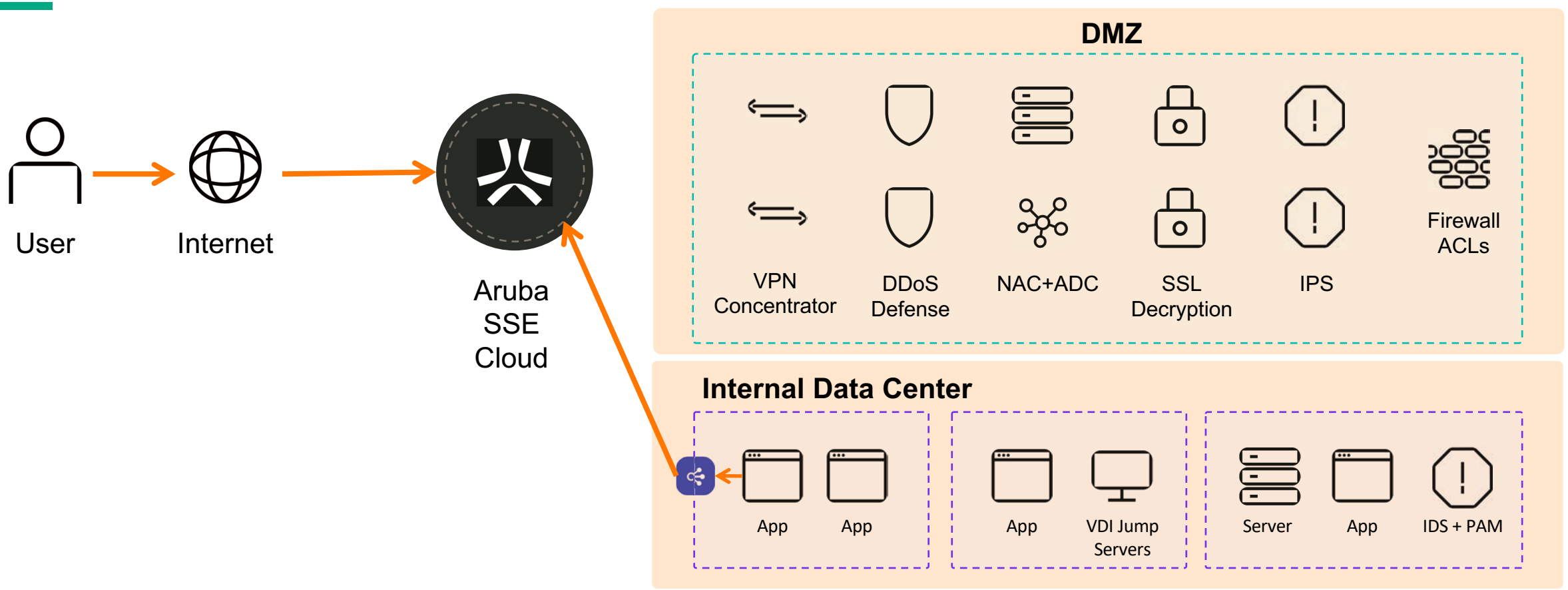
- IPアドレスを公開している
- Inbound 通信を許可
- VPN終端装置の脆弱性対策

アプリ単位の制御が未実装

- 不正アクセスされると、内部でラテラルムーブが容易に

ZTNAでセキュリティリスクを回避

SASE



攻撃対象が無い

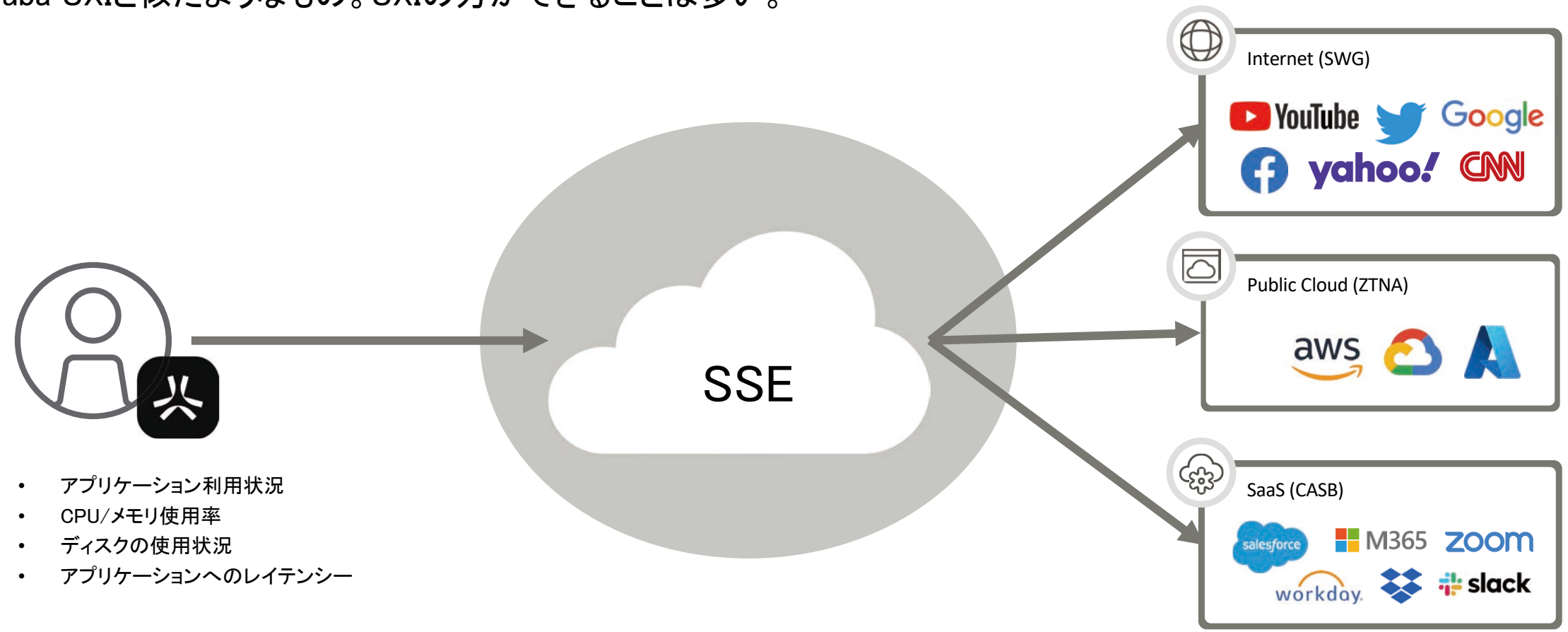
- IPアドレスは公開不要
- Inbound通信が不要
- 脆弱性対策はクラウドが実施

アプリ単位のアクセス

- アプリ単位、プロトコル単位でのアクセス制御

Digital Experience Monitoring (DEM)

Agentがインストールされたユーザ端末の状況をクラウドからモニタリング可能なツール
※Aruba UXIと似たようなもの。UXIの方ができることは多い。

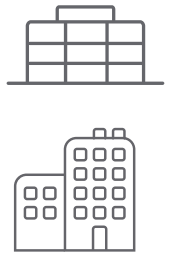


- アプリケーション利用状況
- CPU/メモリ使用率
- ディスクの使用状況
- アプリケーションへのレイテンシー

SD-WAN、SSE単体では接続性とセキュリティを実現できない

Secure SD-WAN

拠点間接続を簡単に
エラー補正可能なルーティング
Next Generation Firewall
Advanced Segmentation
高度な可視性

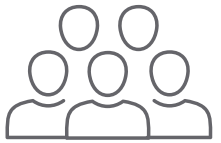


拠点を接続する
ネットワークの進化と
セキュリティ機能を提供

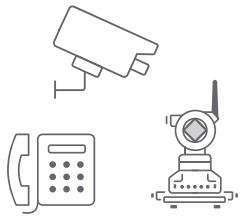
課題:ユーザ保護
ユーザに対する
エンドポイント接続と
セキュリティ機能が不足

Security Service Edge (SSE)

Cloud Access Security Broker(CASB)
Secure Web Gateway(SWG)
Zero Trust Network Access(ZTNA)
Data Loss対策(DLP)
ランサムウェア対策



ユーザがアプリケーション
へ安全に接続するための
セキュリティ機能を
提供



課題:ポリシーの一元化
オンプレミスデバイスを
保護する機能不足

SASEにより相互補完し、次世代のネットワークとセキュリティを実現

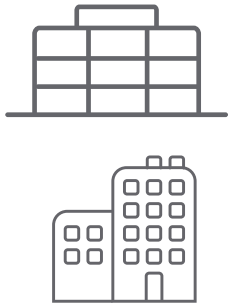
Secure SD-WAN

拠点間接続を簡単に
エラー補正可能なルーティング
Next Generation Firewall
Advanced Segmentation
高度な可視性

Security Service Edge (SSE)

Cloud Access Security Broker(CASB)
Secure Web Gateway(SWG)
Zero Trust Network Access(ZTNA)
Data Loss対策(DLP)
ランサムウェア対策

Secure Access Service Edge (SASE)

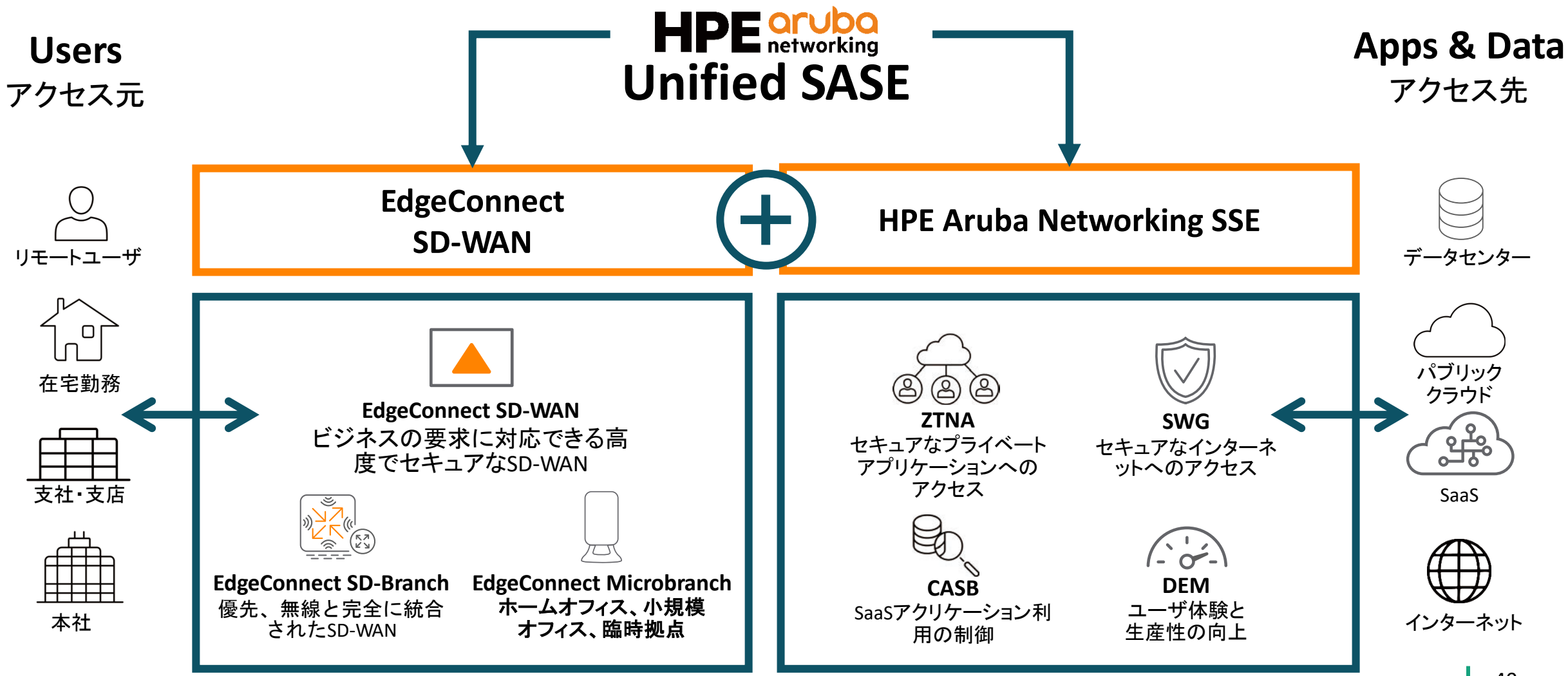


拠点間、データセンター
クラウドへの接続とコストを
最適化し、トラフィックを自
動でSSEにルーティングす
ることでセキュリティ確保

ネットワーク全体で
ゼロトラストを実現し
全てのユーザ・デバイスを
安全に接続

HPE Aruba Networking Unified SASE

業界をリードするEdgeConnect SD-WANと次世代SSEをSASEとしてご提供

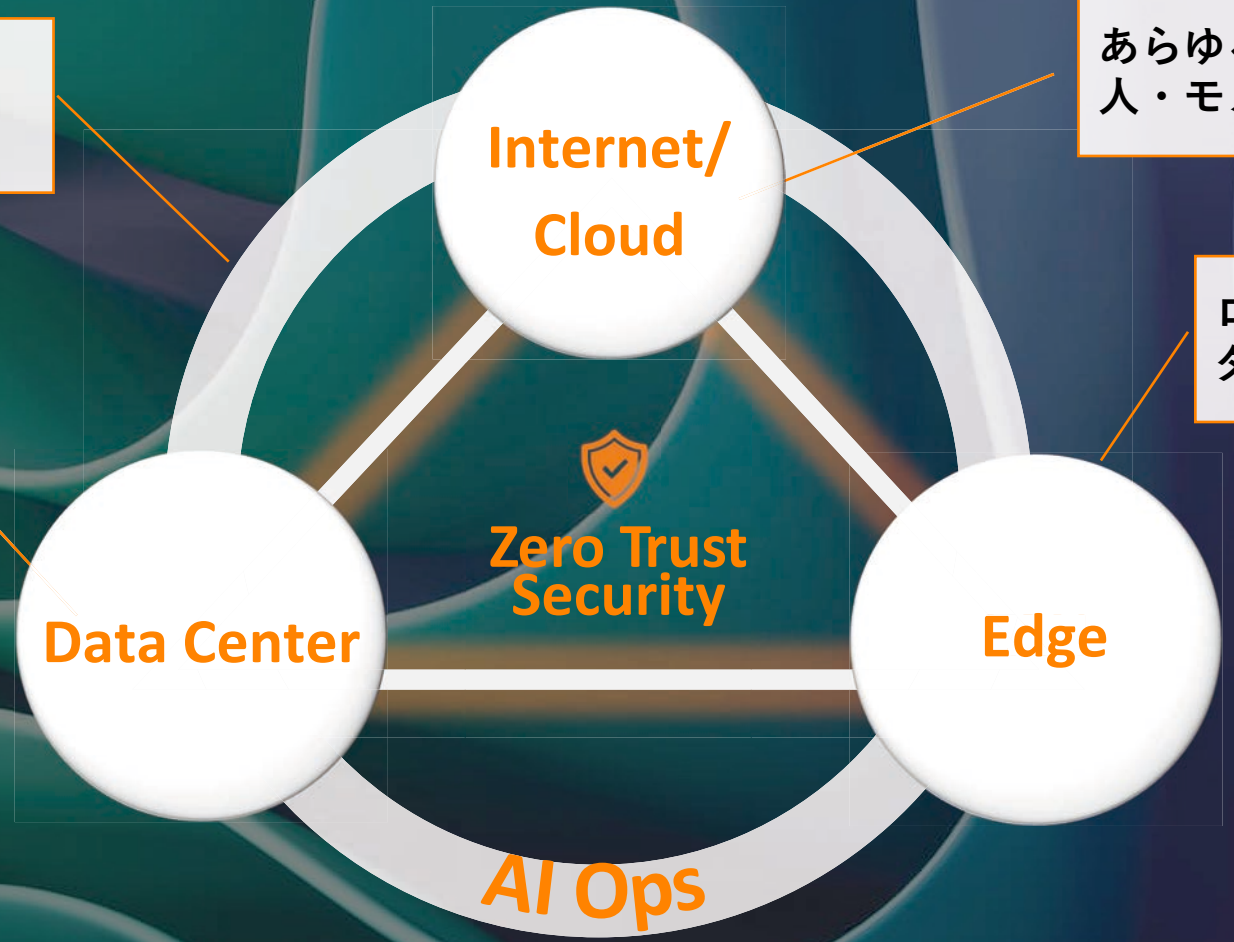


Security-First, AI-Powered Networking

セキュリティが導くコネクティビティの未来

クラウドベースのAIOps
コントロールと脆弱性対策

シンプルかつスケーラブルな
マイクロセグメンテーション



あらゆる場所からの接続
人・モノ・アプリを柔軟かつ安全に接続

ロールベースのアクセス制御
ダイナミックセグメンテーション


HPE aruba networking
Security-First Networking

Hewlett Packard
Enterprise

Airheadsアカデミー:
HPE Aruba Networking SSEのご紹介

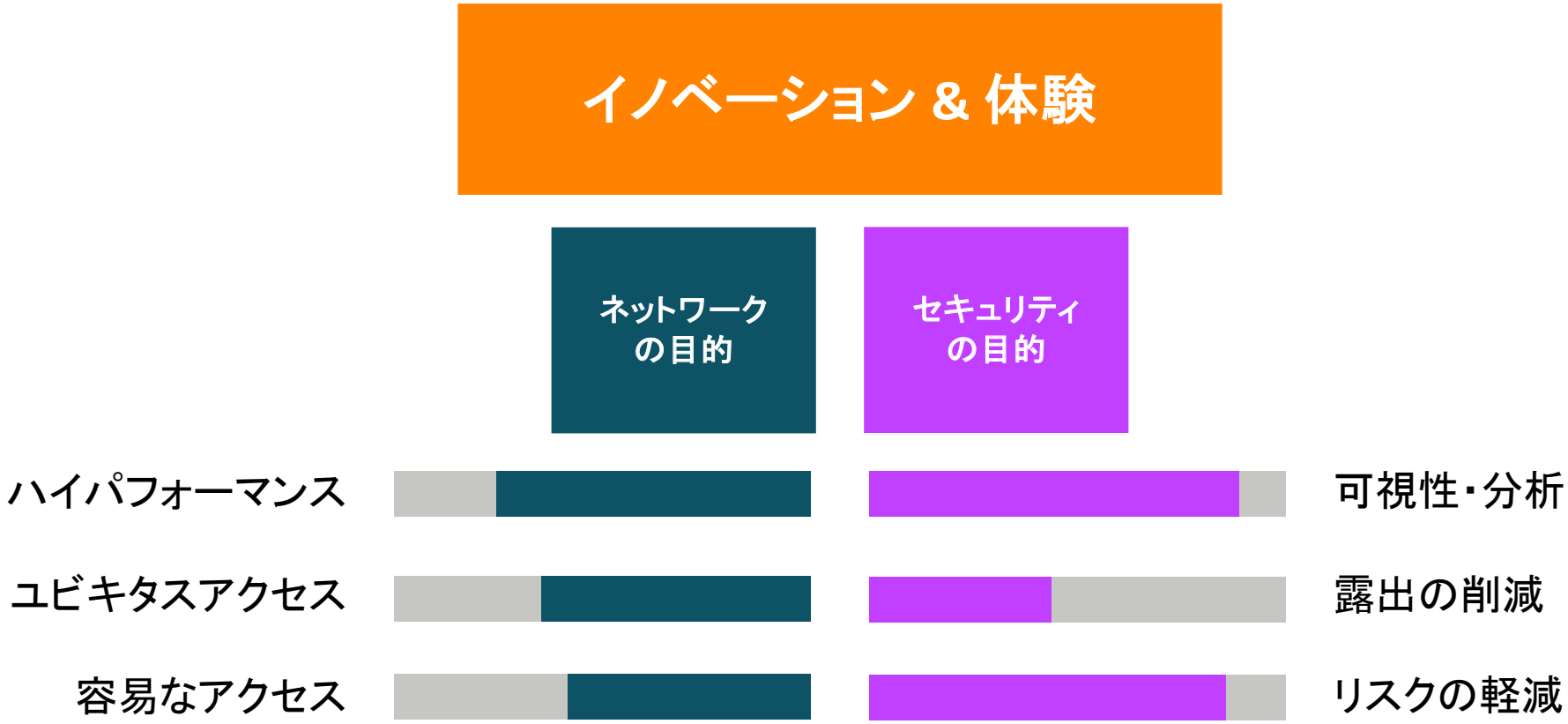
2024年7月26日

Hiroki.Sakabe@hpe.com

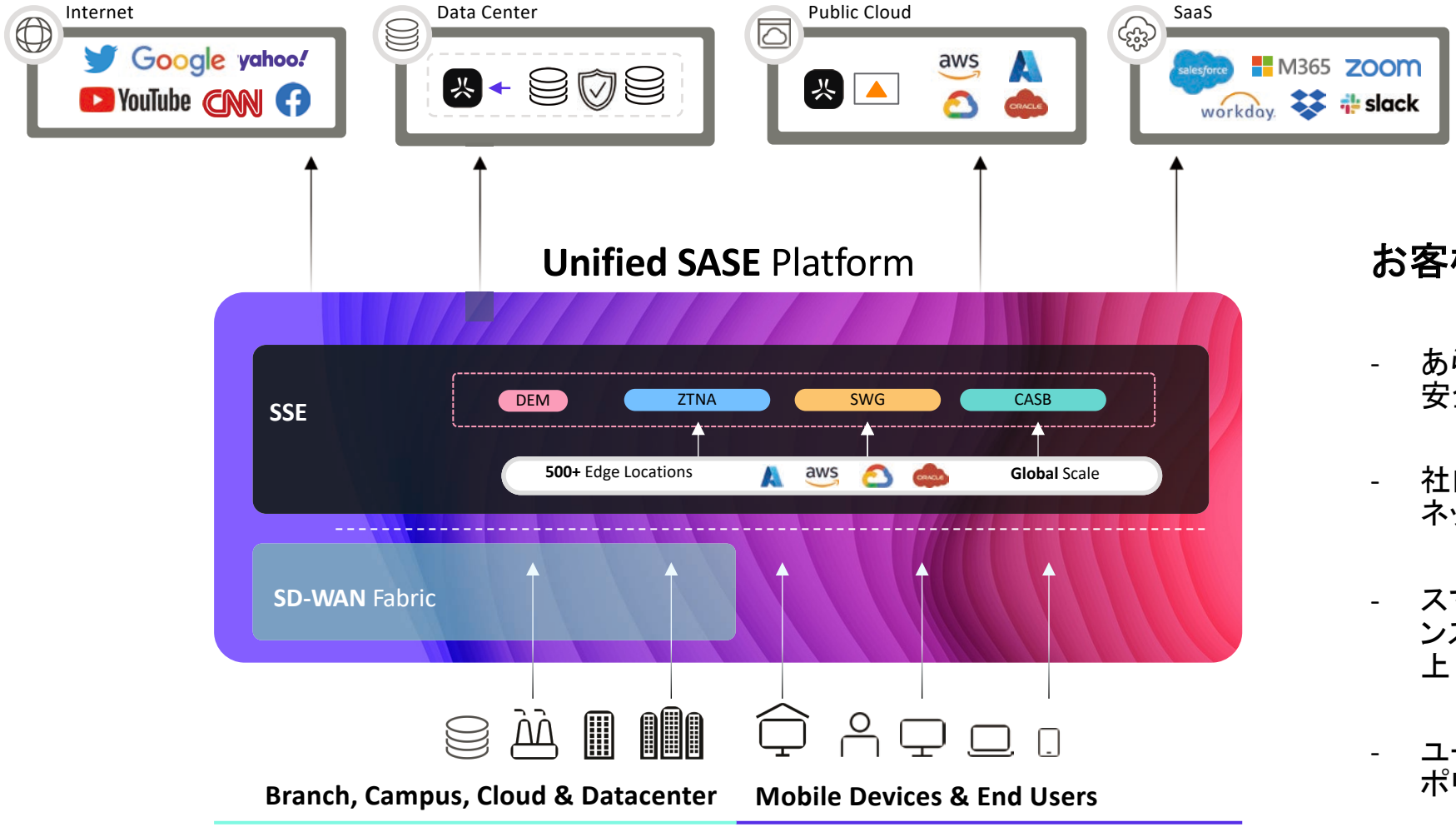
Next Stage :

Security-first, AI-powered Networking

ネットワーク vs セキュリティ



HPE Arubaはネットワークとセキュリティ技術を統合しシンプルに



お客様へご提供する価値:

- あらゆるアプリケーションへの安全なアクセス
- 社内、支店、データセンターのネットワークを近代化
- スマートルーティングとエクスペリエンスモニタリングによる生産性の向上
- ユーザとデバイスに対するポリシー管理の簡素化

HPE Aruba Networking SSEがご提供する機能

ZTNA
Agent/Agentless

Zero Trust Network Access
明確なアクセス コントロールポリシーに基づき
プライベートリソースへのアクセスを提供するゼロトラスト機能

SWG

Secure Web Gateway
すべてのWebトラフィックを監視・検査し、
マルウェアからの保護やURLフィルタリングを実現

Employee access to resources

Branch user & server access

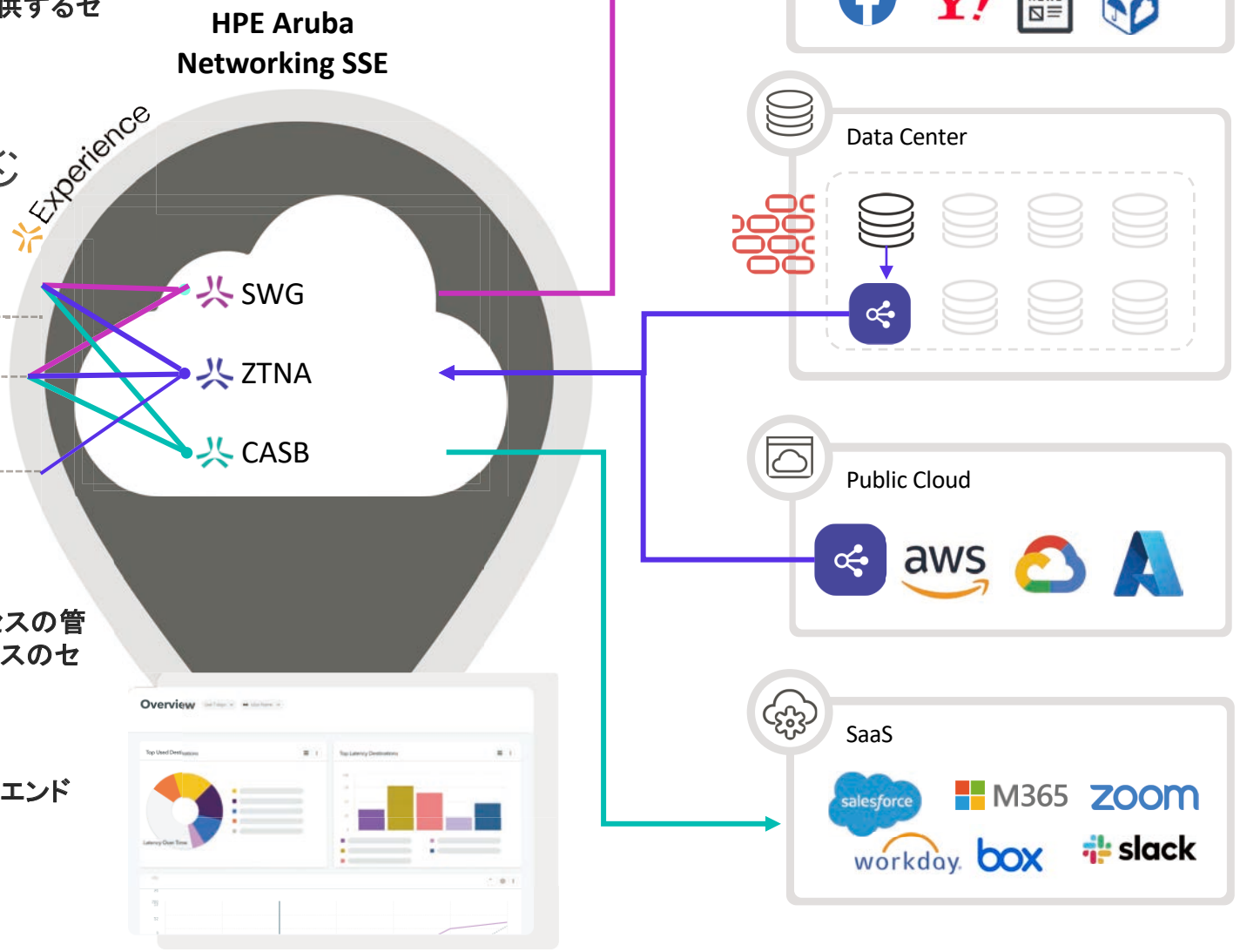
Third-party access

CASB

Cloud Access Security Broker
SaaSアプリケーションへのユーザアクセスの管理・制御、監視するためのクラウドベースのセキュリティ

DEM

Digital Experience Monitoring
ユーザエクスペリエンスをエンド・ツー・エンドで可視化し生産性向上を支援



HPE Networking SSEの特徴と強み

HPE Aruba Networking SSE概要

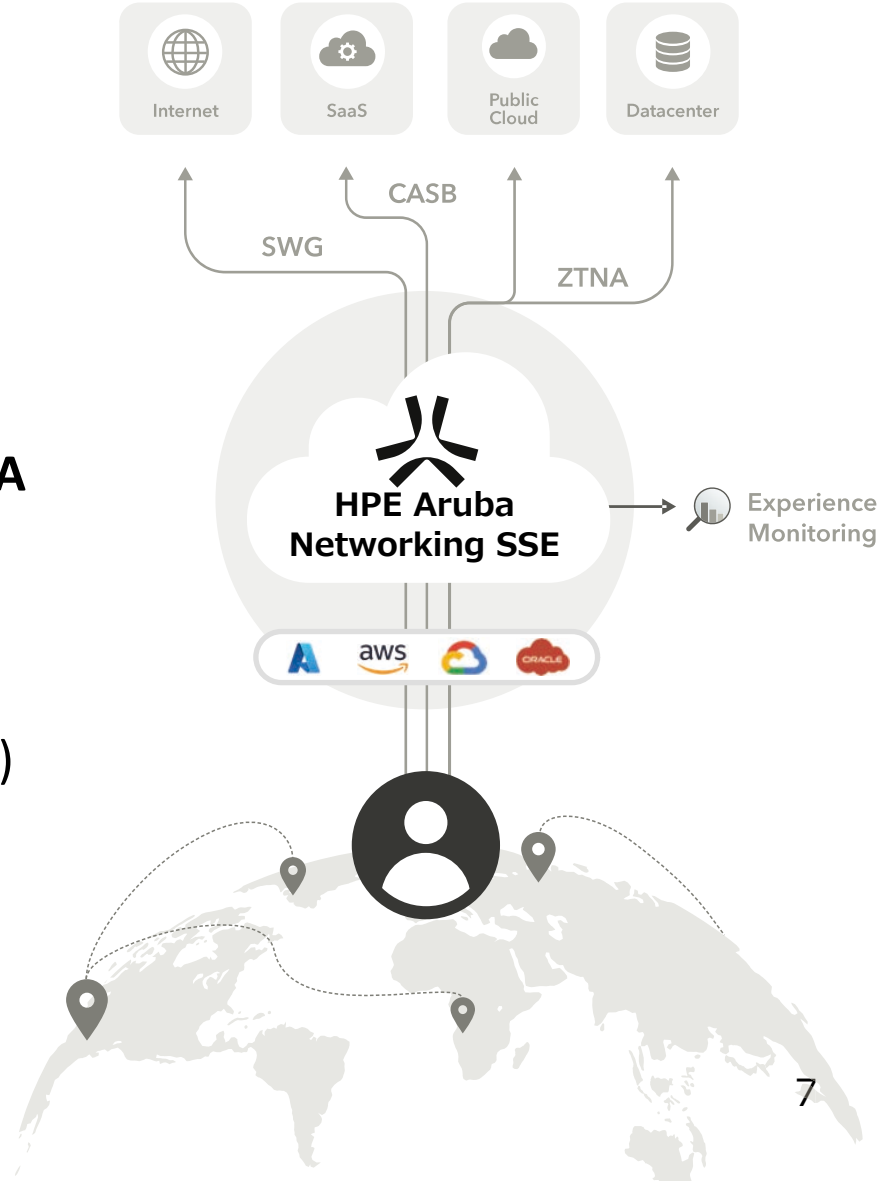
クラウドネイティブアーキテクチャのSSE (Security Service Edge)プラットフォーム

SSE (Security Service Edge)ソリューション

従業員に安全なアクセス環境を提供する
クラウドセキュリティサービス

特徴

- ✓ ビジネスアプリケーションへの安全なアクセスを実現する**ZTNA** (Zero Trust Network Access)に強みを持つ
- ✓ 従業員のインターネットへの安全なアクセスを提供する **SWG**(Secure Web Gateway)
- ✓ SaaSのアクセスを制御する**CASB**(Cloud Access Security Broker)も提供



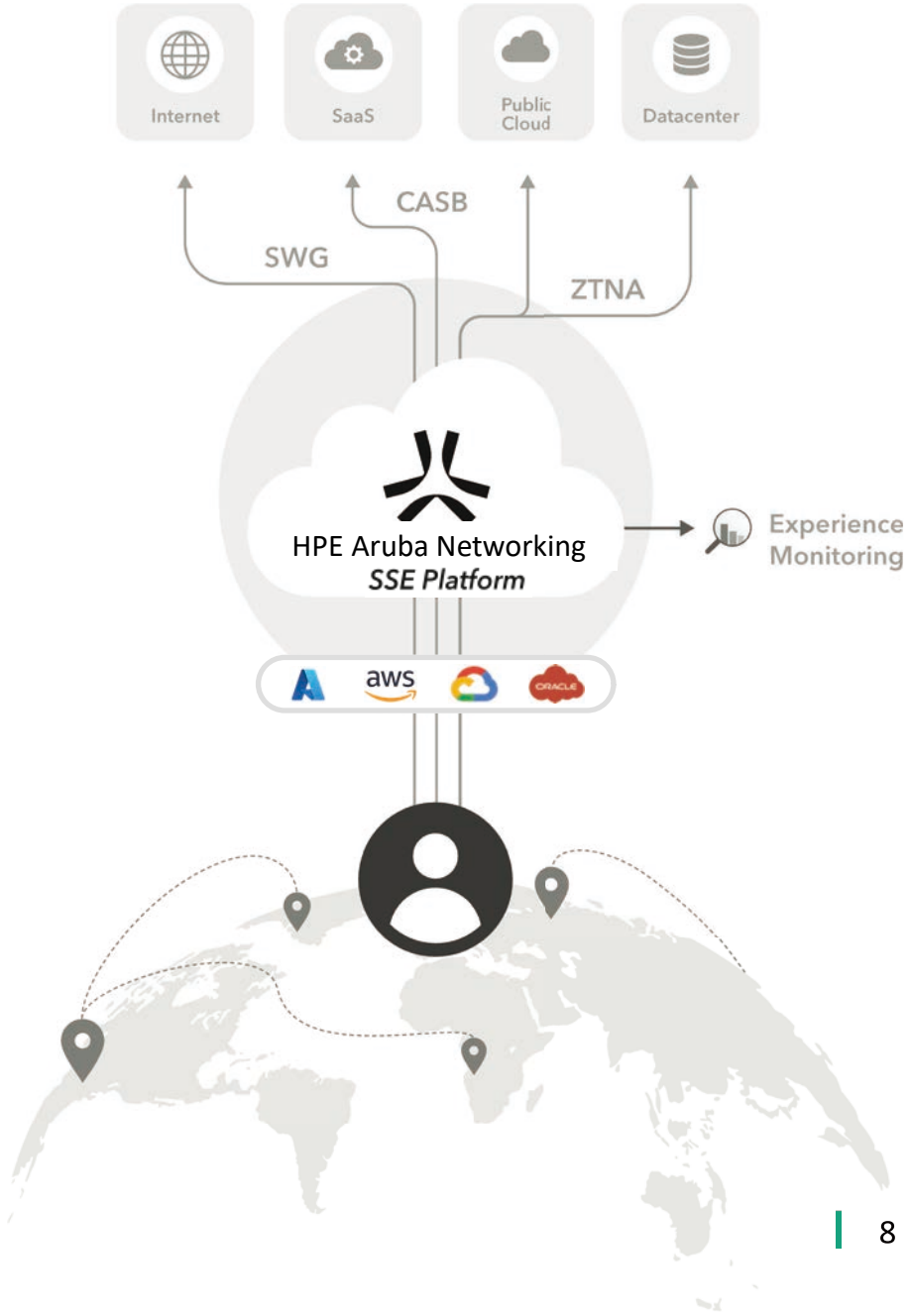
HPE Aruba Networking SSE の強み

統合アクセスプラットフォームとして開発・展開（One UI, One Platform）
（バラバラの製品の寄せ集めではない）

ポリシーとトラフィックの制御をシンプルに管理
（インターネットやSaaSだけではなく、SSH, RDP, VOIP, AS400, ICMPいった様々なプロトコルに対応）

AWS, Azure, Google and Oracleのクラウドバックボーンを介してアクセスを最適化
（クラウドネイティブで高い冗長性と拡張性を提供）

エージェント及びエージェントレスをサポートし、ユーザがセキュアにリソースにアクセス可能
（サプライチェーンや関連企業の協業が容易に）



統一されたシンプルな管理(管理面の向上)

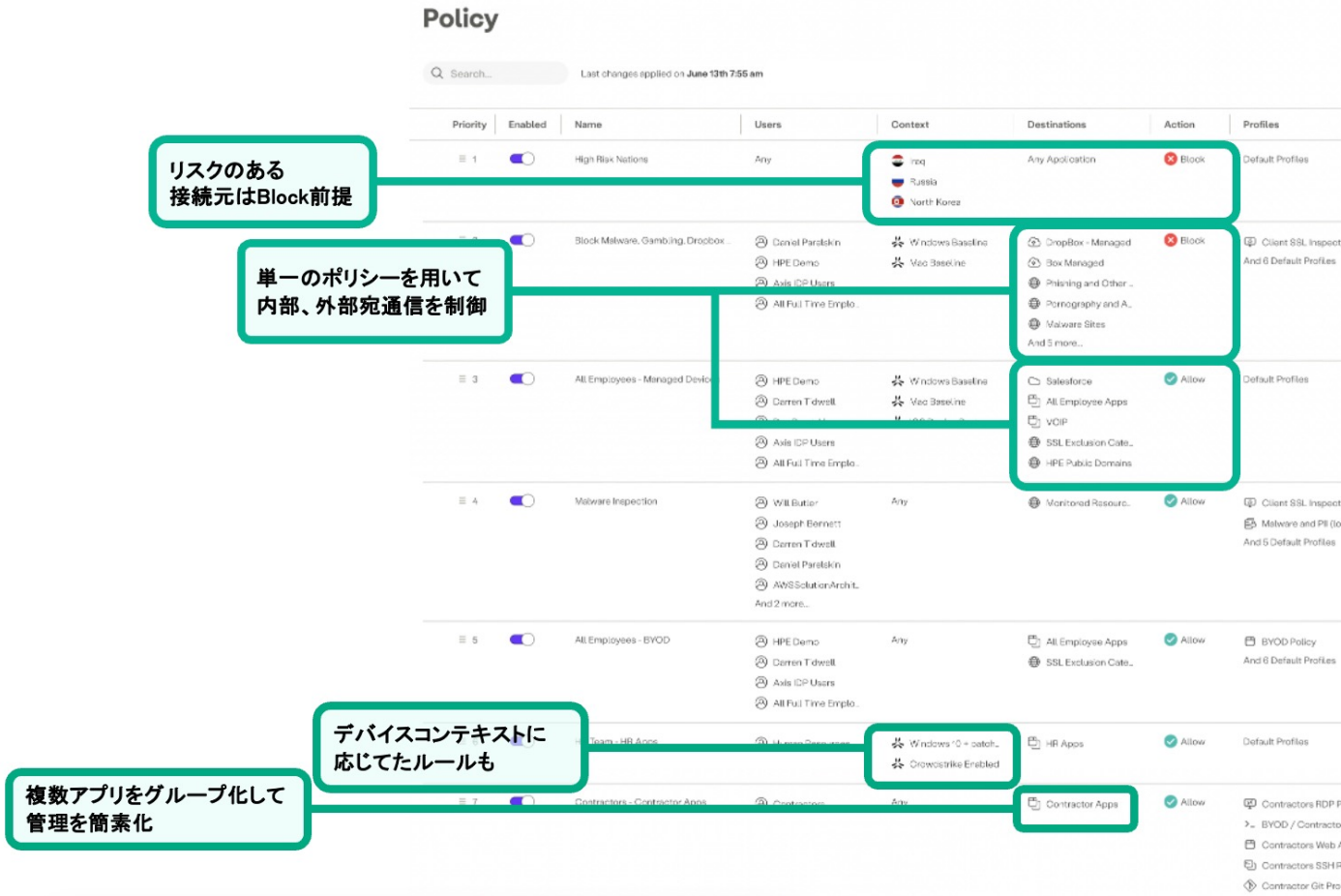
ZTNAもSSE機能の１つとして提供され
クラウドコンソールを通じて制御が可能です。

ただし、SSEソリューションの多くは、機能を追加開発や
買収することで寄せ合わせ構成されており、プラットフォームやコンソールが異なりシンプル化とは言えない場合も・・・

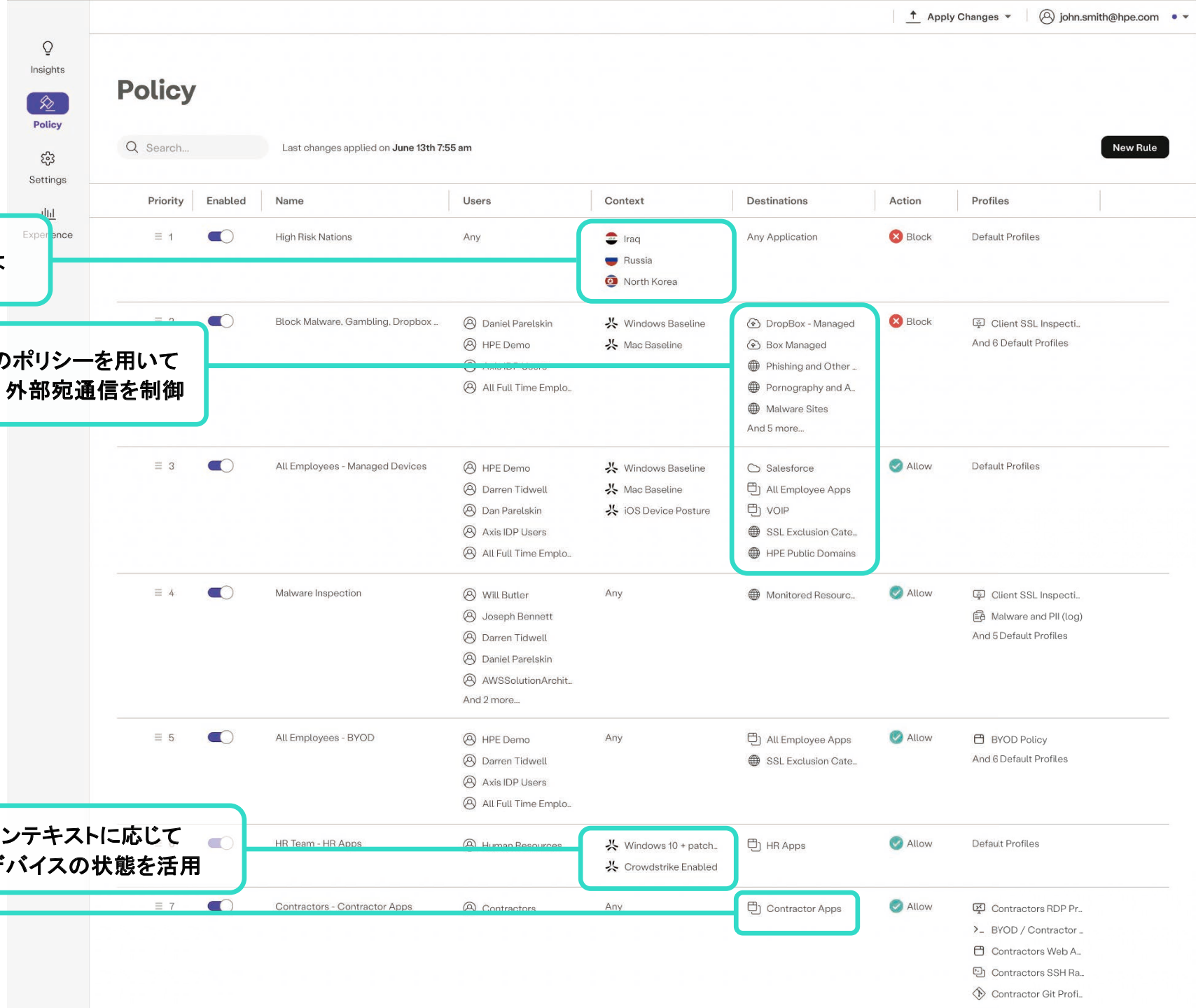
HPE Aruba Networking SSEは
管理性にこだわりシンプルな運用性を提供！

- **統合アクセスプラットフォーム**
  として開発・展開（One UI, One Platform）
  （バラバラの製品の寄せ集めではない）
- **ポリシーとトラフィックの制御をシンプルに管理**
  （インターネットやSaaSだけではなく、SSH, RDP, VOIP, AS400, ICMPいった様々なプロトコルに対応）

シンプルで統一された管理コンソールのポリシー設定



HPE Aruba Networking SSE ポリシー設定イメージ



悪意のある宛先の通信はBlock

単一のポリシーを用いて内部、外部宛通信を制御

コンテキストに応じてデバイスの状態を活用

複数のアプリはタグを用いて簡素化

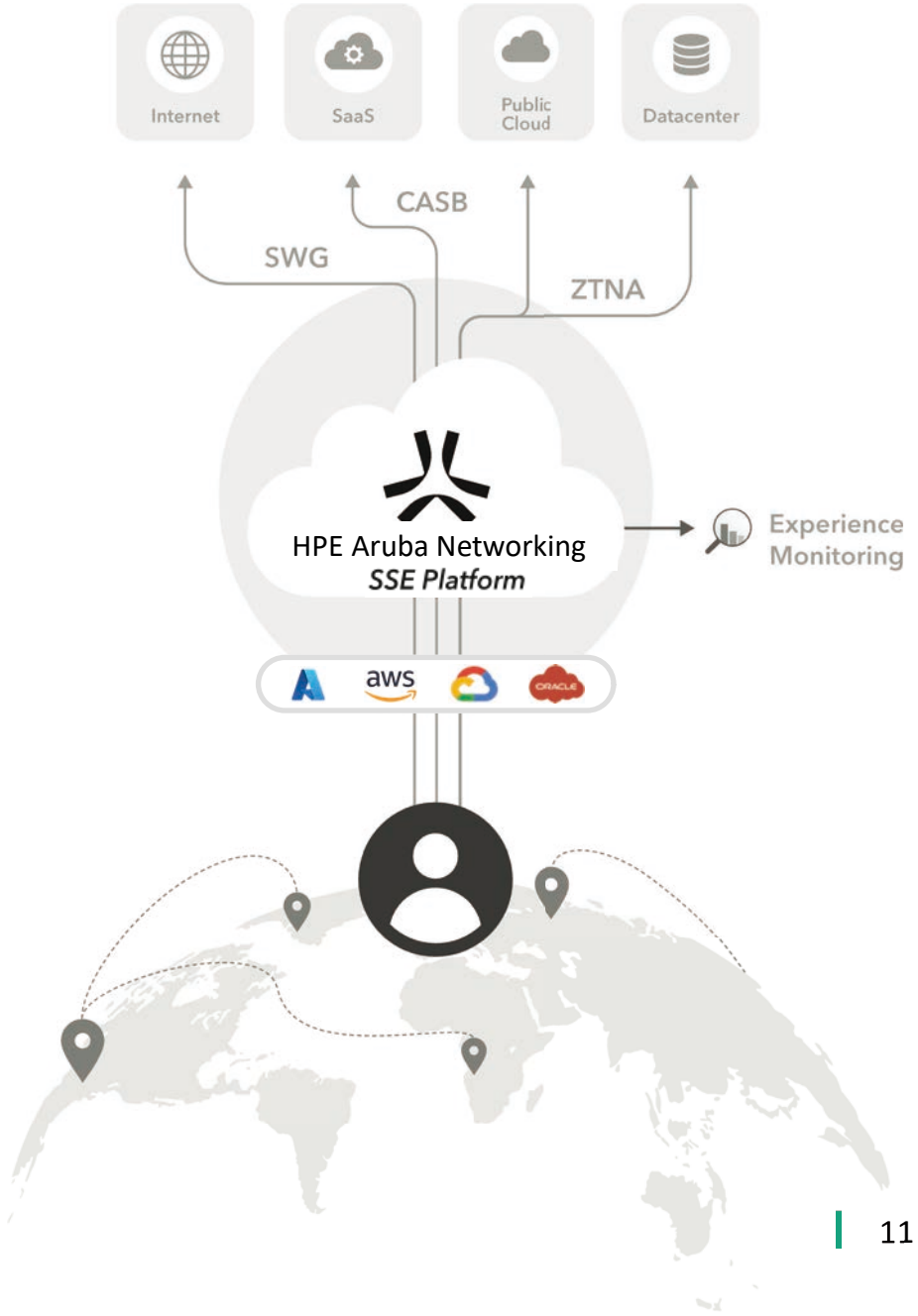
HPE Aruba Networking SSE の強み

統合アクセスプラットフォーム
として開発・展開（One UI, One Platform）
（バラバラの製品の寄せ集めではない）

ポリシーとトラフィックの制御を
シンプルに管理
（インターネットやSaaSだけではなく、SSH, RDP, VOIP, AS400, ICMPいった様々なプロトコルに対応）

AWS, Azure, Google and Oracleのクラウド
バックボーンを介してアクセスを最適化
（クラウドネイティブで高い冗長性と拡張性を提供）

エージェント及びエージェントレスをサポ
ートし、ユーザがセキュアにリソースにア
クセス可能
（サプライチェーンや関連企業の協業が容易に）



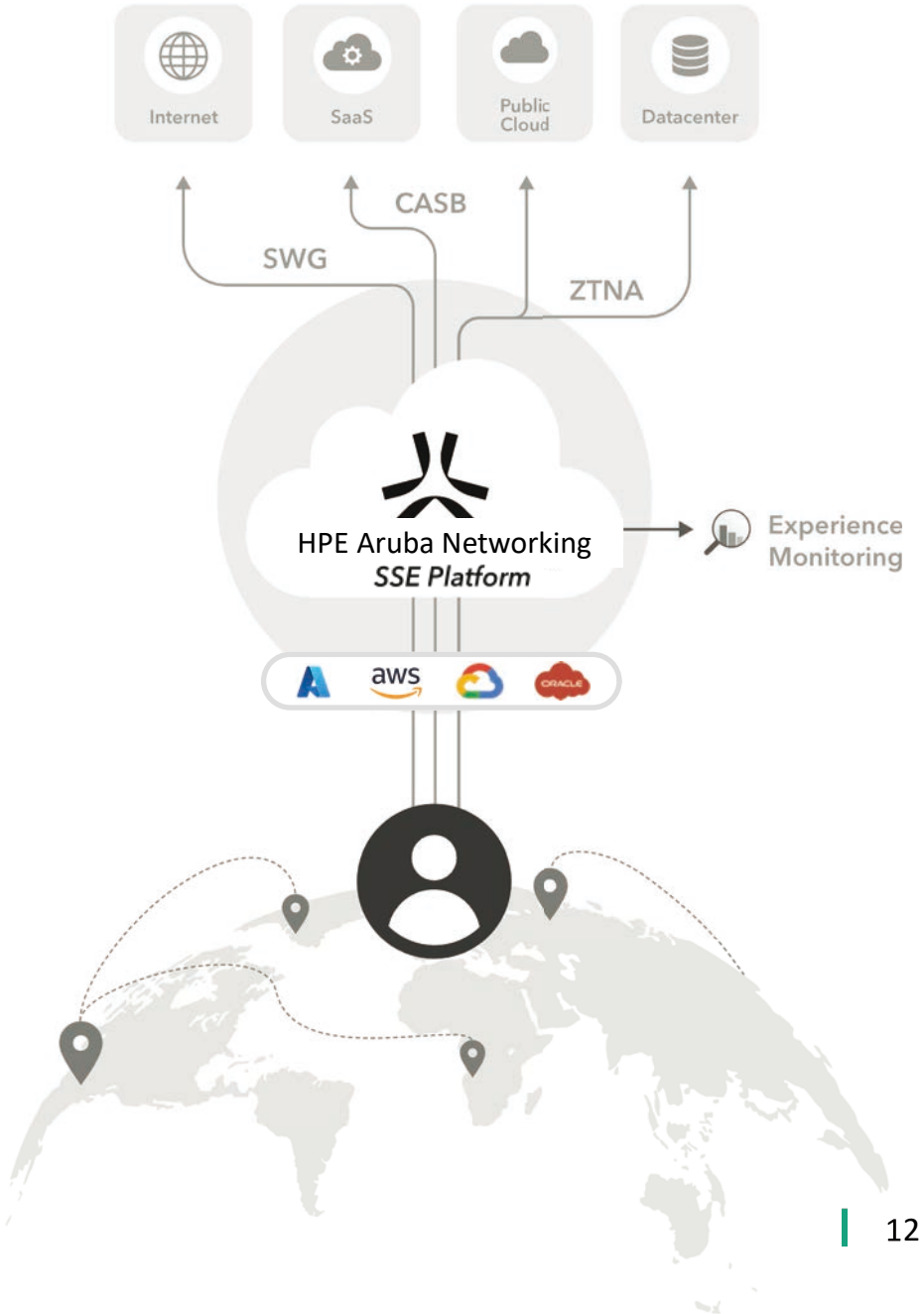
サービスの柔軟性

SSEは機能としてクラウドサービスとして提供されます。
必要に応じてリソースを迅速にスケールしお客様に継続した機能を提供します。
お客様運用などのオンプレミス型のにおいては、新しいハードウェアの購入・追加が必要があり、スケーリングには時間とコストがかかりましたが、この負担からお客様を解放します。

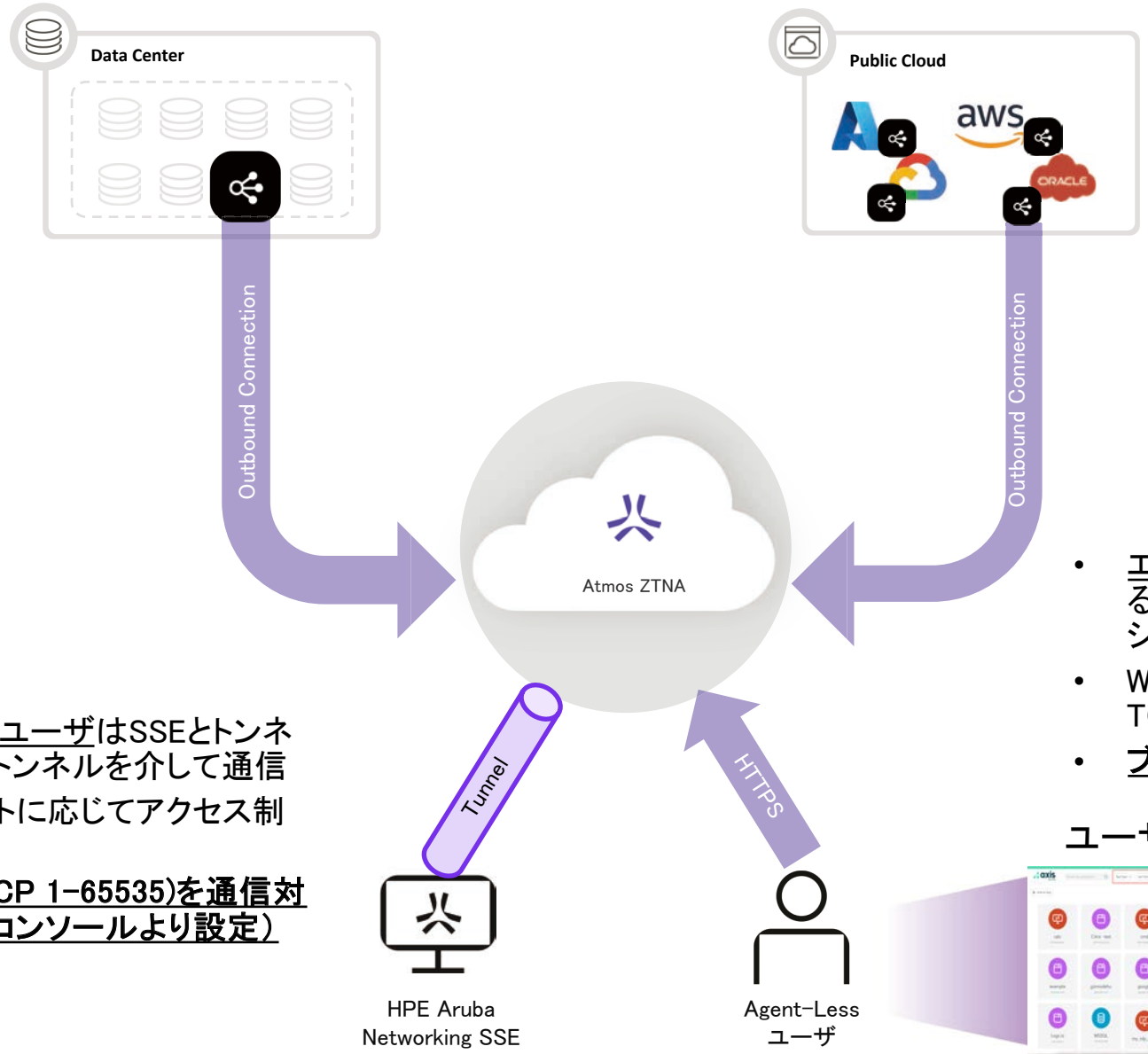
ただし、自社DCにてサービスを提供している製品も多く、
拡張にはオンプレと同じように時間がかかる場合も・・・

HPE Aruba Networking SSEは
クラウドネイティブなアーキテクチャで先進的なサービス展開

- **AWS, Azure, Google and Oracleのクラウドバックボーンを介してアクセスを最適化**
  （クラウドネイティブでアジリティを確保し、高い冗長性と拡張性を提供）



ZTNA (Zero Trust Network Access)



アプリケーション側

- ZTNAのために利用するために専用のHWアプライアンスは不要（Connectorと呼ぶVMの配置が必要）
- アプリケーション単位でアクセス
- プライベートアプリケーションへのユーザのアクティビティも追跡可能（リモートアクセスしたユーザが実行したコマンドなど）
- **ConnectorにPublic-IPは不要**

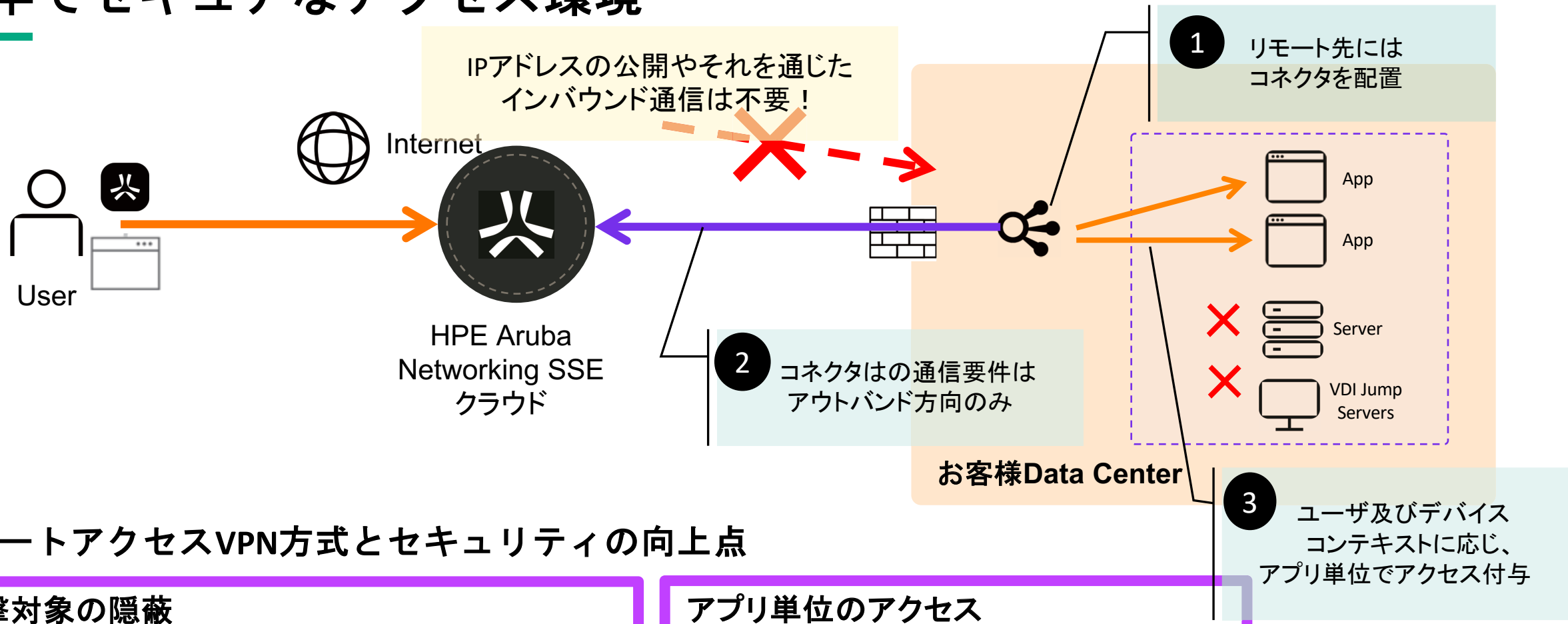
クライアント側

- エージェントデバイス/ユーザはSSEとトンネルを形成し、確立したトンネルを介して通信
- デバイスのコンテキストに応じてアクセス制御が可能
- **全てのポート(TCP/UCP 1-65535)を通信対象として制御が可能(コンソールより設定)**

- エージェントレス/ユーザはクラウドが提供するユーザポータル通じて、ZTNAアプリケーションアクセスを提供
- Webだけでなく、SSH、RDPなど業務で必要なTCPプロトコルをサポート
- **ブラウザベースで専用ソフトウェア不要**

ユーザ毎にポータルを提供

堅牢でセキュアなアクセス環境



リモートアクセスVPN方式とセキュリティの向上点

攻撃対象の隠蔽
- IPアドレスの公開不要
- インバウンド通信が不要（コネクタからAxisクラウドに対するアウトバウンドのみ）
- 脆弱性対策はクラウドサービスとして提供

アプリ単位のアクセス
- ユーザ、デバイス単位からアプリ単位、プロトコル単位でのきめ細やかなアクセス制御

ZTNA（エージェント）

デモクライアント
（Windows）

User

Internet

HPE Aruba
Networking SSE
クラウド

コネクタ:
内部のアプリケーションに接続できる
ネットワーク内に配置し、リモートからのアクセスを
仲介するデバイス

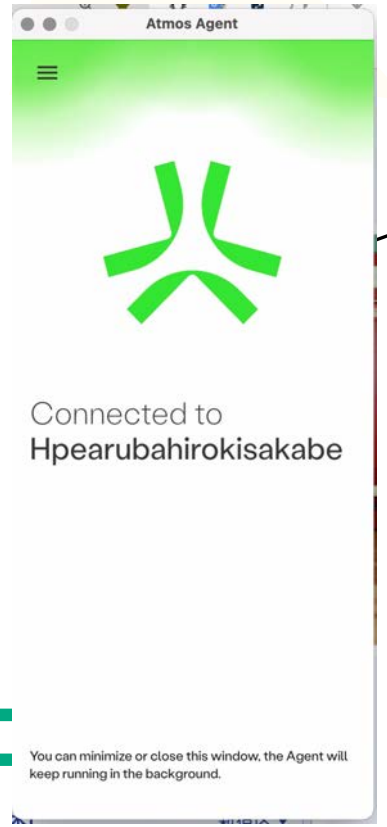
App

App

Server

VDI Jump
Servers

Lab



SSE エージェント
ユーザーごとに提供され
るポータルサービス

15

ZTNA（エージェントレス）

デモクライアント
（Windows）

User

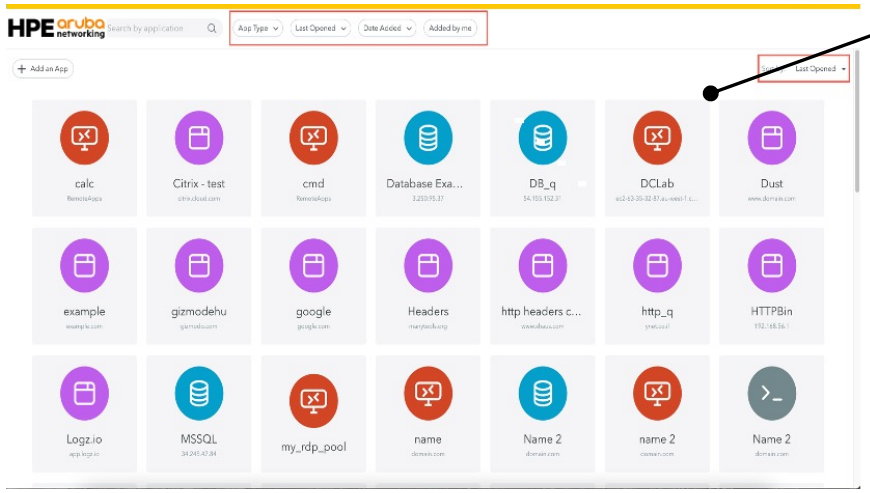
Internet

HPE Aruba
Networking SSE
クラウド

コネクタ:
内部のアプリケーションに接続できる
ネットワーク内に配置し、リモートからのアクセスを
仲介するデバイス

App
App
Server
VDI Jump
Servers

Lab



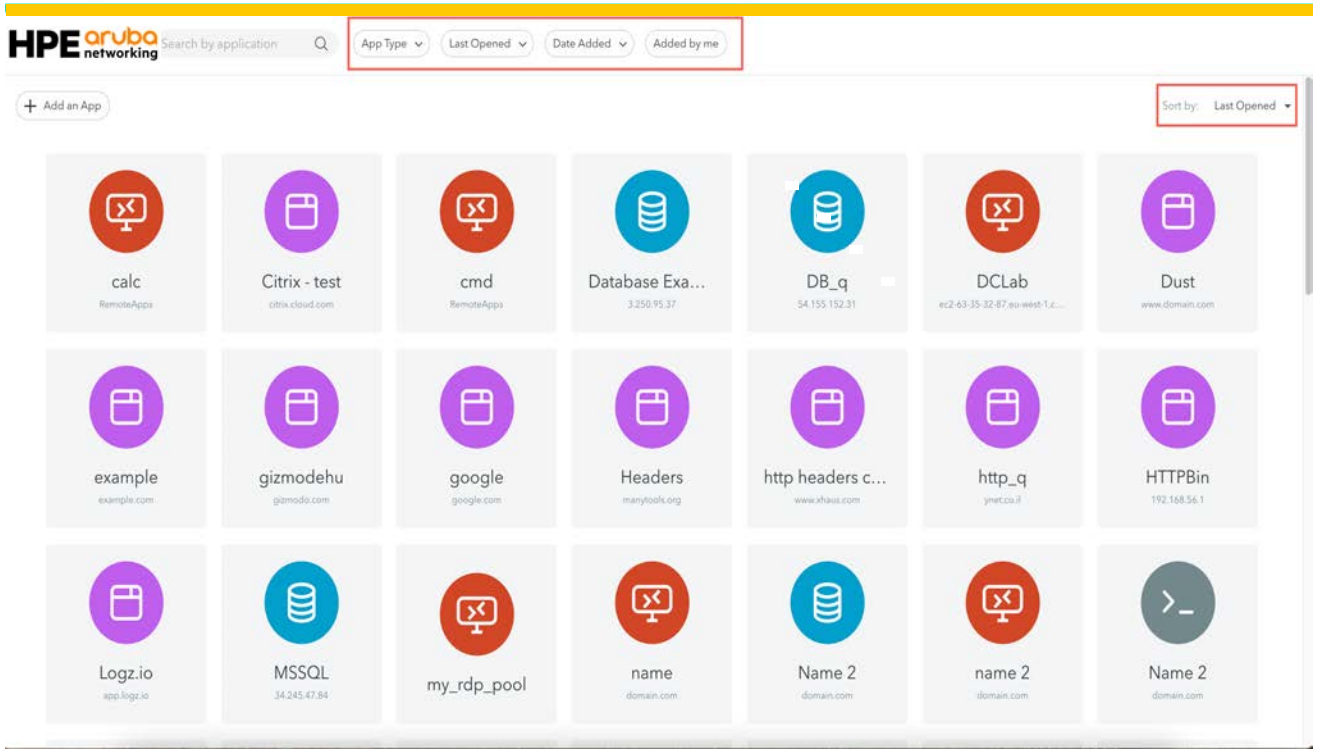
User Portal
ユーザーごとに提供されるポータルサービス

16

エージェントレスZTNA？

- ユーザ毎にポータルを自動で提供し、ポータルを通じてブラウザベースによるアプリケーションの利用を提供
- SSHやRDPなどはネイティブアプリによる接続も提供

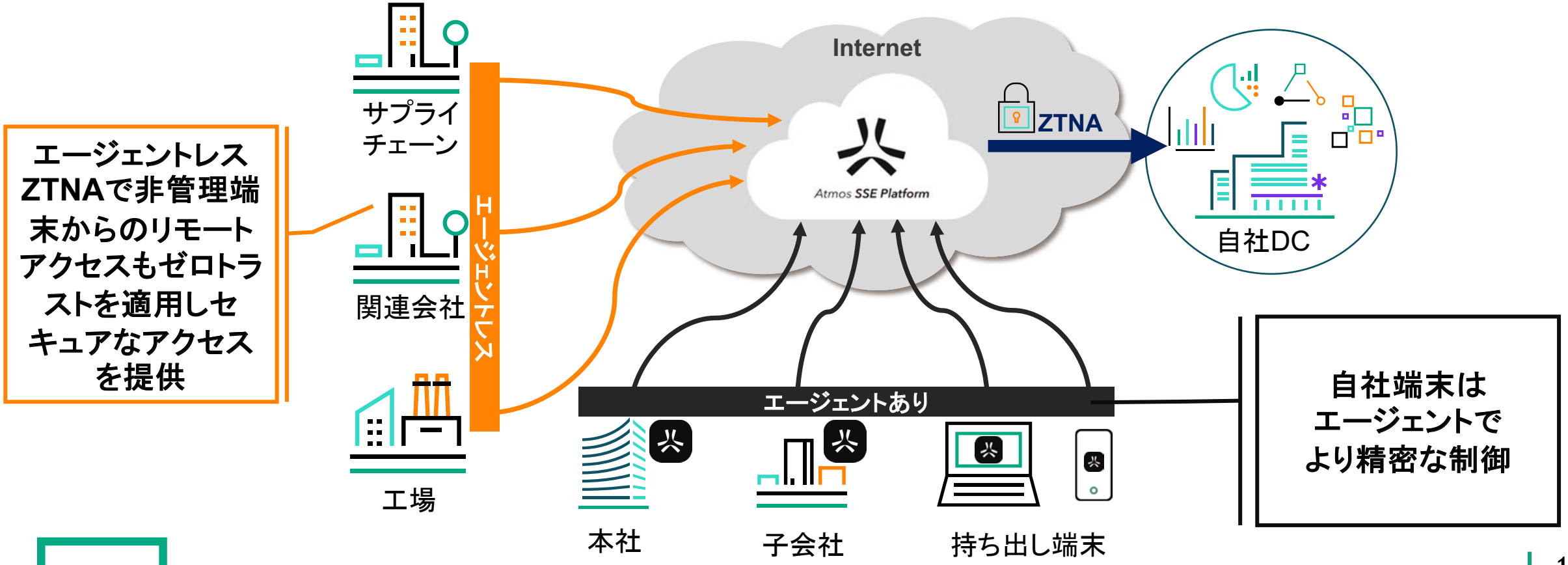
ユーザ毎にWebポータルを提供



エージェントレスZTNAの利用例
関係会社やサプライチェーンにもゼロトラストを適用

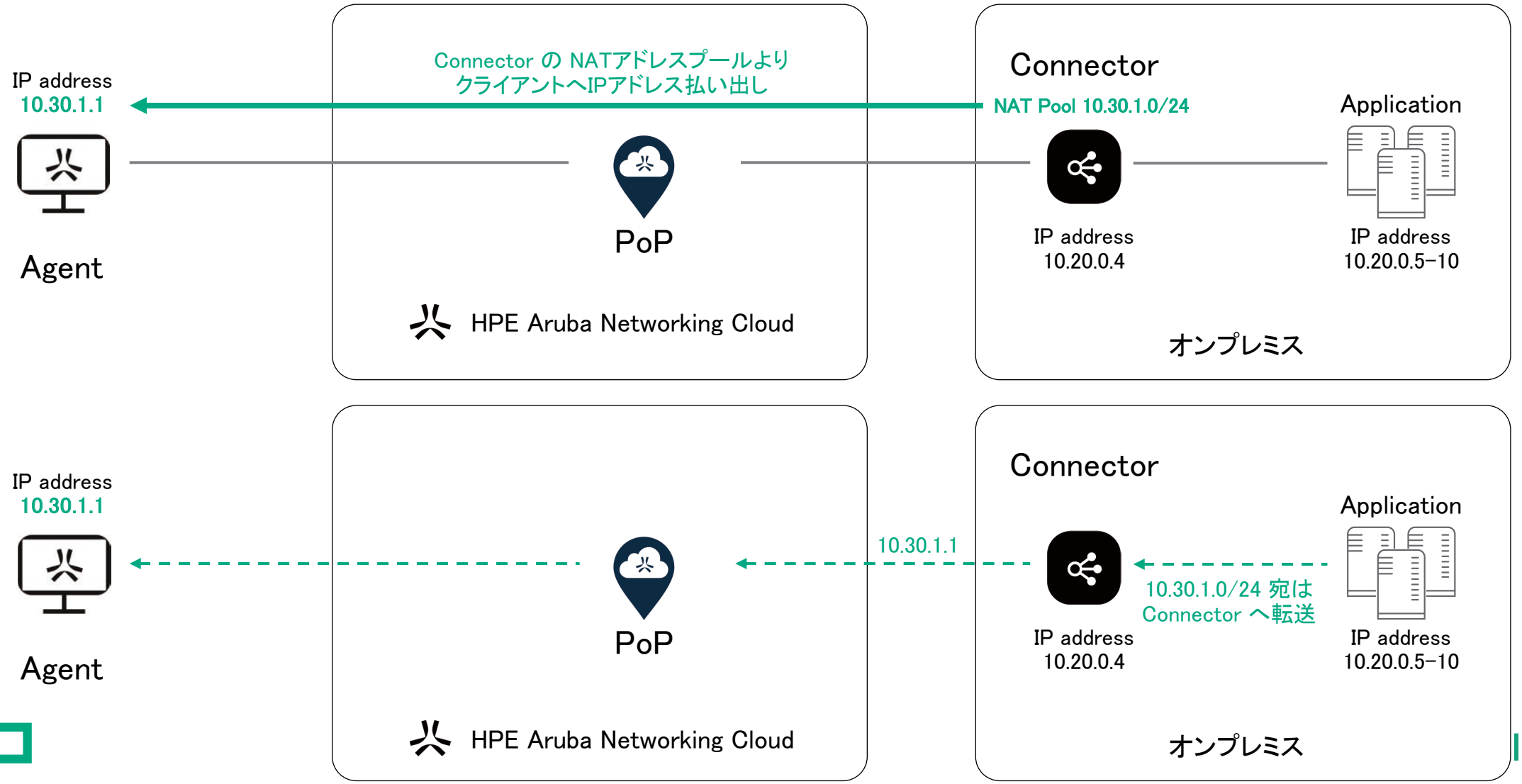
いままでの課題

自社管理ができないので、サプライチェーンや関連会社の端末への
エージェントインストールは難しいが、自社アプリへのアクセスが必要



パッチ配信などにもサーバ発通信にも対応可能

サーバ発で行う通信もConnector経由で到達性を確保



Thank you

HPE Aruba SASEソリューション

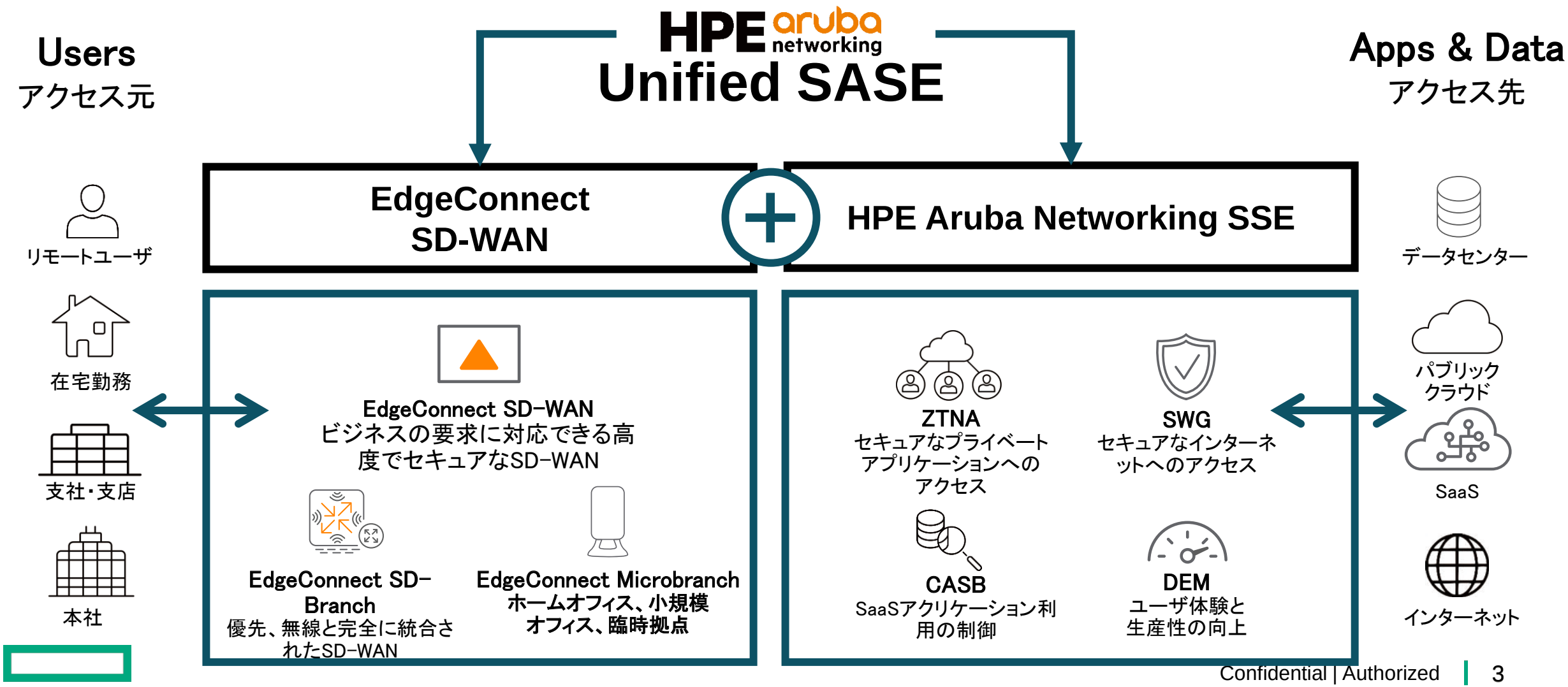
横山晴庸 (Haruyasu.Yokoyama@hpe.com)

Jul-26-2024

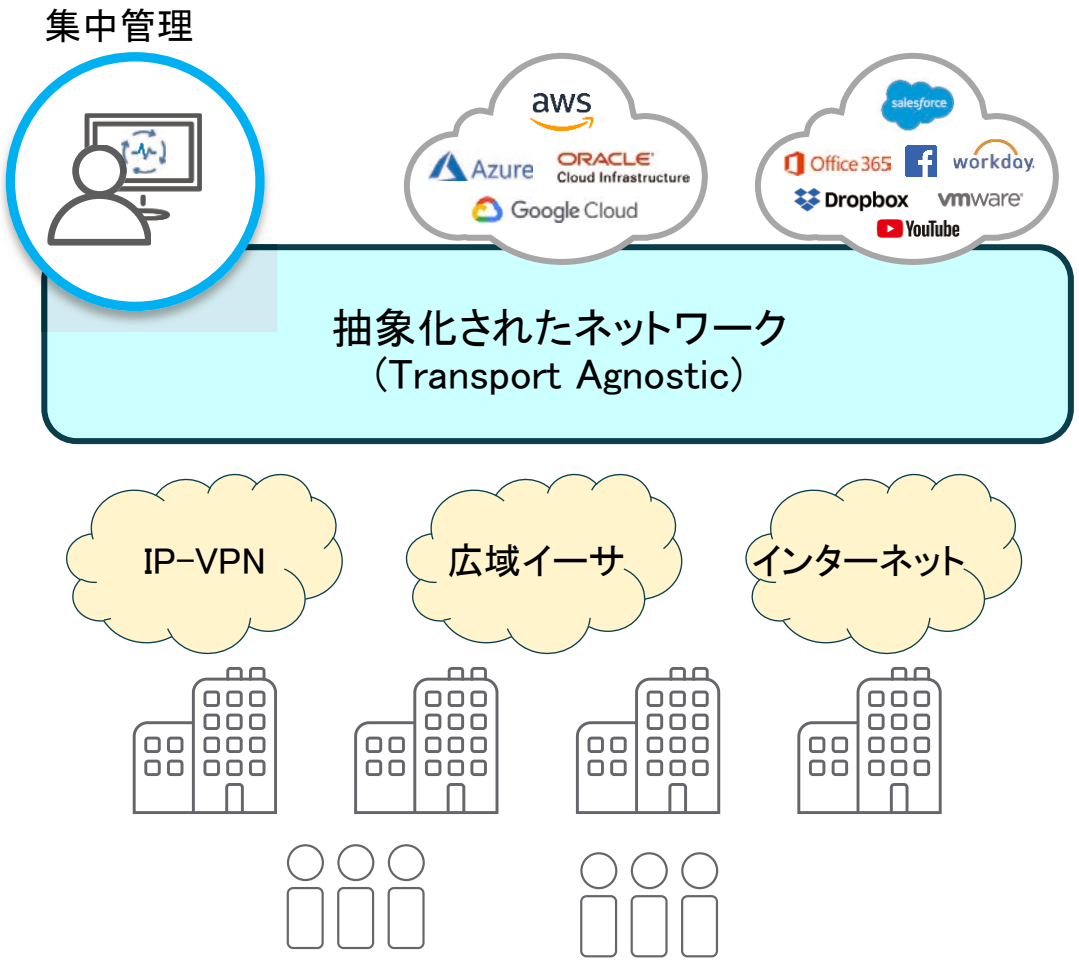
Agenda

- ArubaのSASEソリューション
- SASEの動向
- SASE導入時の注意点

HPE Aruba Networking Unified SASE
業界をリードするEdgeConnect SD-WANと次世代SSEをSASEとしてご提供



SASEへの期待



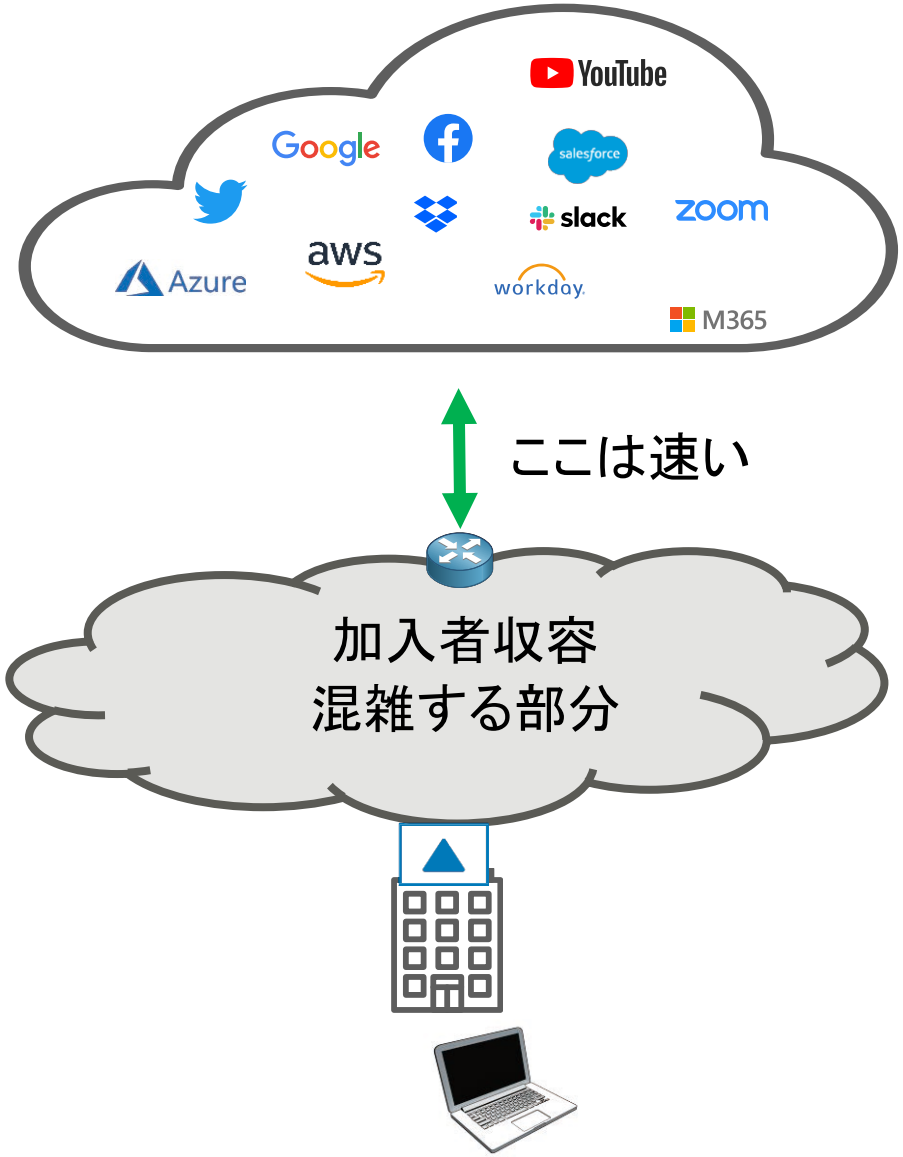
- 集中管理で容易に設定変更をできること、変化に強いネットワーク
- 不十分なパフォーマンスや不具合にはすぐに気づけること
- 廉価で短納期な回線を束ねて広帯域を得る、簡単に通信を強化できること
- FECやWAN高速化機能による高パフォーマンスの拠点間通信
- 各アプリケーションの優先順位に応じて、回線の使い分けや適切な帯域の割り当てができること
- クラウドアクセス(SaaS, IaaS)の最適化
- 安全なインターネットアクセスの提供(クラウドセキュリティ連携)
- セグメント化されて、セキュリティ事故があっても被害が局所化されること

クラウドアクセスの最適化を考える

SASEはセキュリティを維持しながら快適なネットワーク利用を提供するための手段

- 日本のネットワーク事情を考慮
  - 混雑している箇所を如何に速く抜けられるか
- SaaSアクセスのパフォーマンスを定量的に監視
  - 継続的に計測可能な手段があるのが望ましい

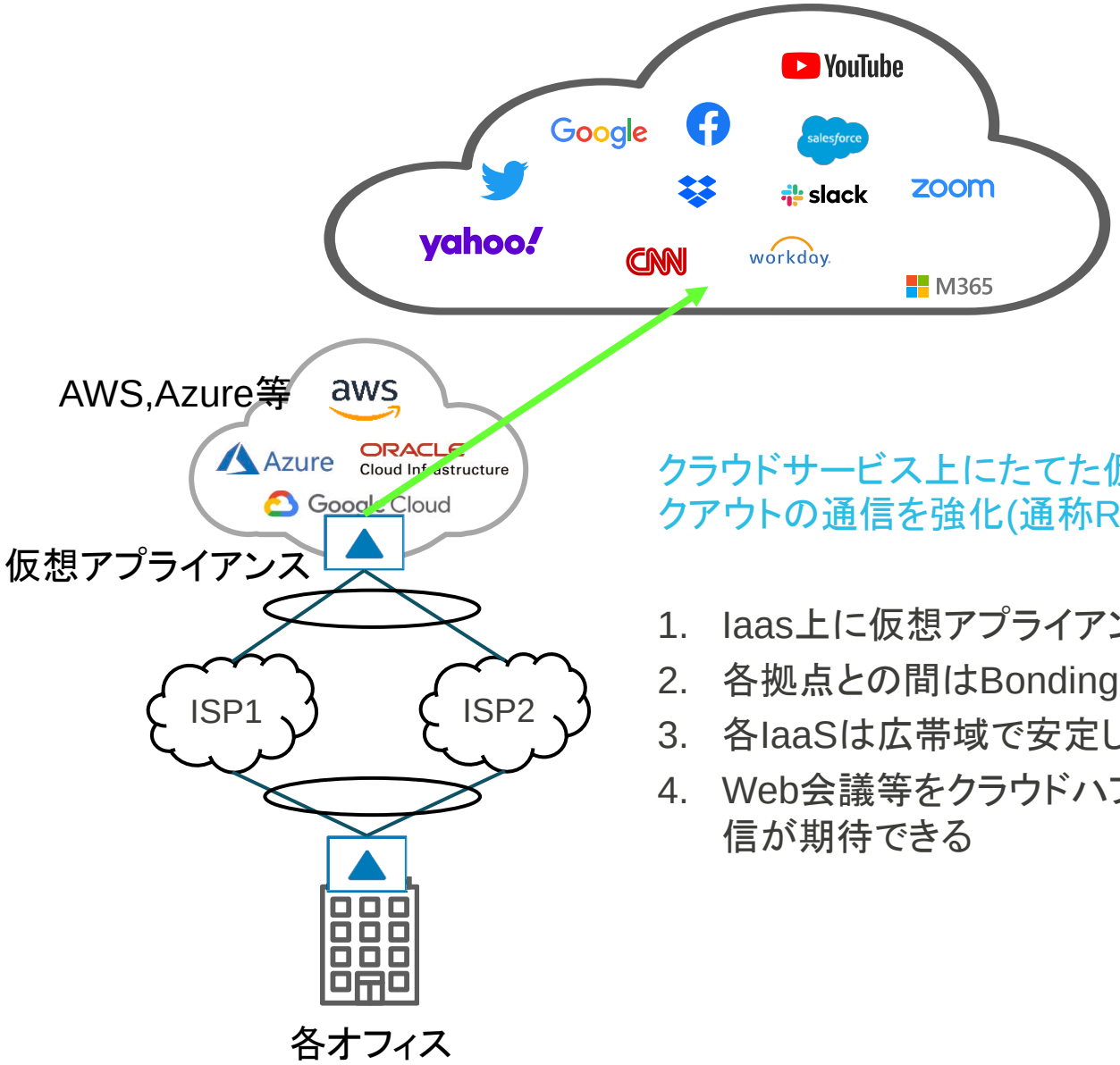
日本のインターネット



日本のネットワーク

- アクセス部分が混雑する。
- 国土が狭いので、最終の宛先(クラウドサービス)までの距離は近く、混雑した部分を抜けられればそこから先は速い

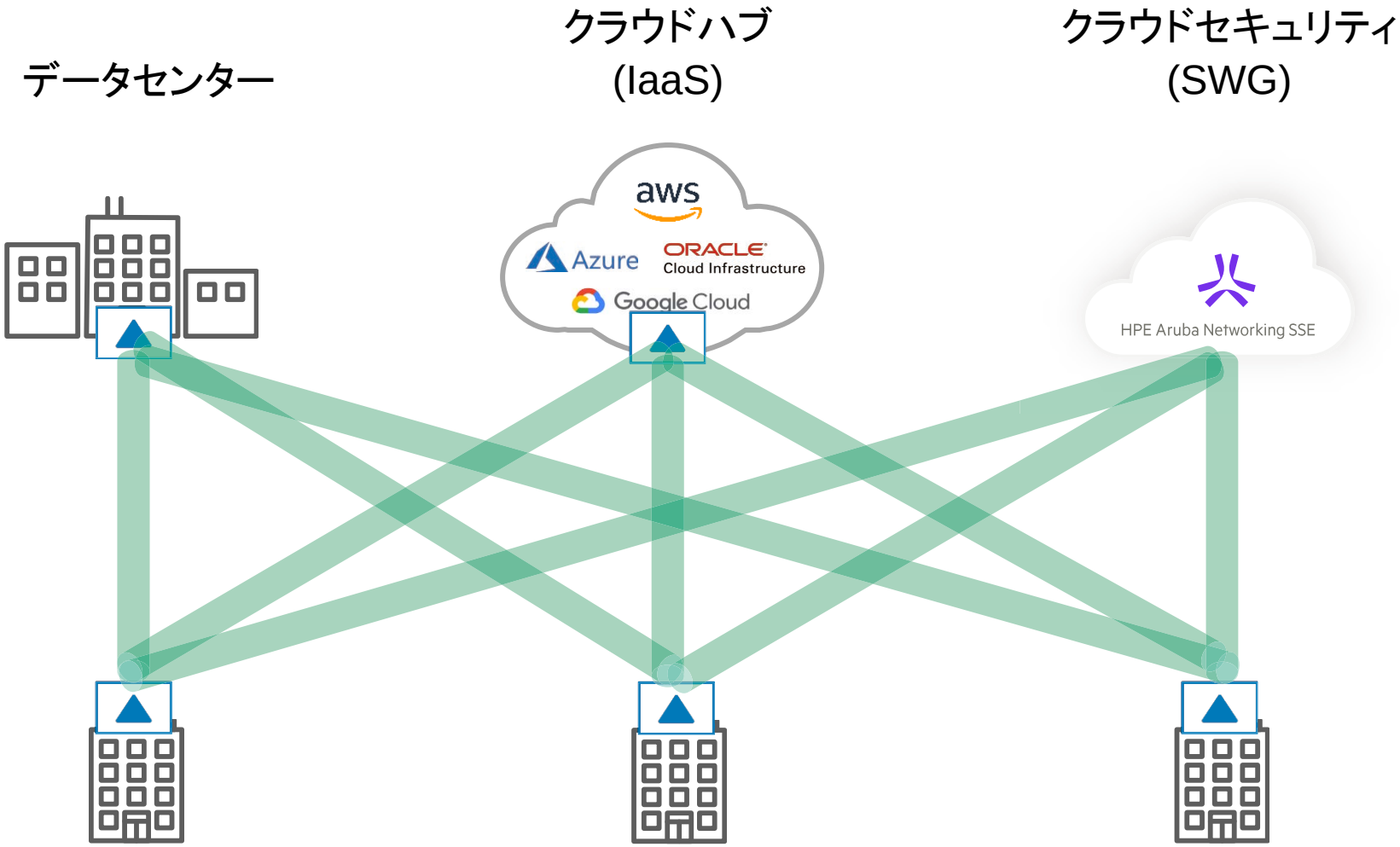
クラウドハブを使った混雑箇所の通信品質強化
- Ruggedized First Mile -



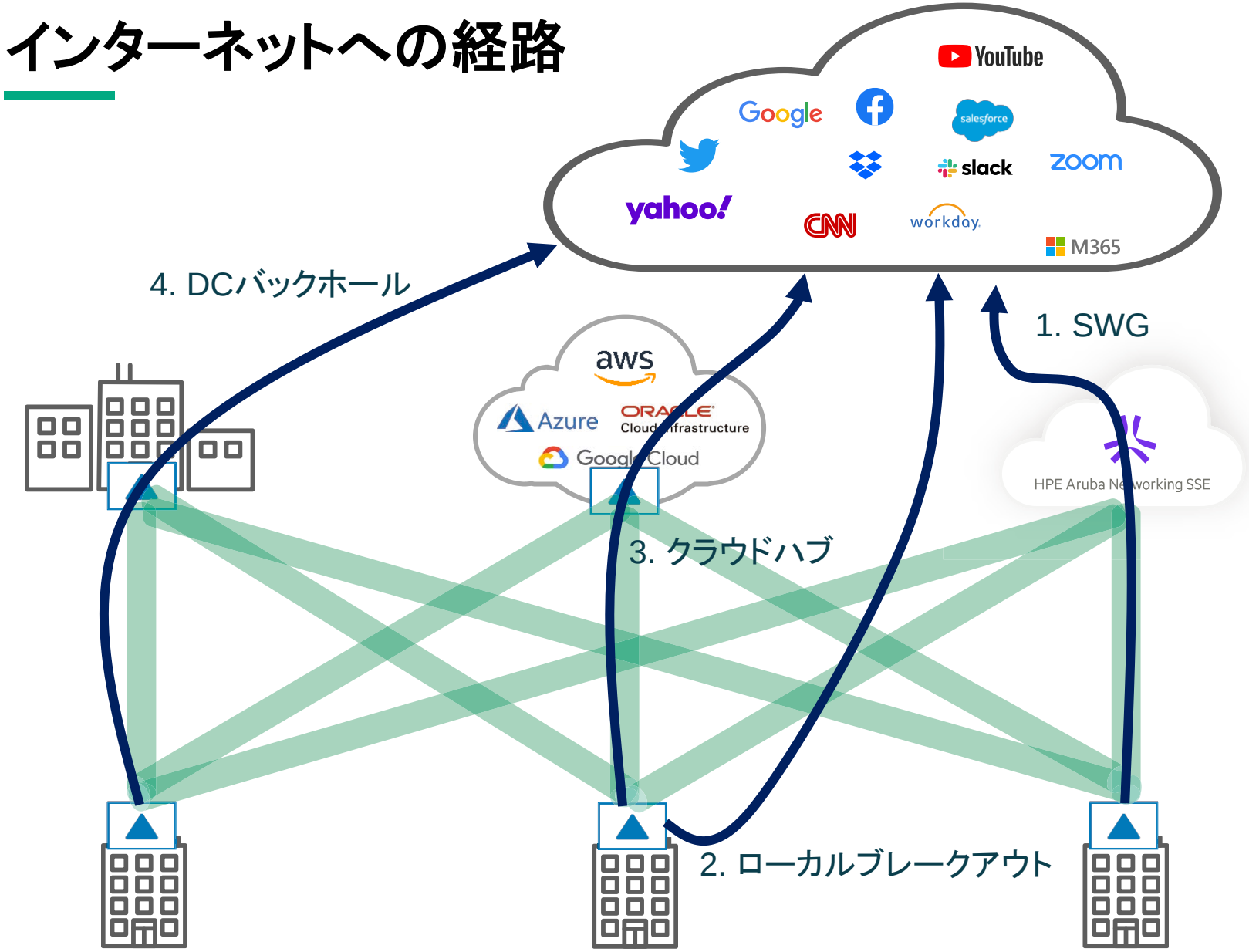
クラウドサービス上にたてた仮想アプライアンスを利用してローカルブレークアウトの通信を強化(通称Ruggedized First Mile)

1. Iaas上に仮想アプライアンスを用意(クラウドハブ)
2. 各拠点との間はBondingを利用して接続、拠点とIaaS間の通信を強化
3. 各IaaSは広帯域で安定した回線を保持
4. Web会議等をクラウドハブ経由で送信する事により高速で安定した通信が期待できる

SASE


データセンター
クラウドハブ
(IaaS)
クラウドセキュリティ
(SWG)
aws
Azure
ORACLE
Cloud Infrastructure
Google Cloud
HPE Aruba Networking SSE
各オフィス拠点／工場

インターネットへの経路



経路の選択肢

1. SWG (SASE)
2. ローカルブレークアウト
3. クラウドハブ
4. DCバックホール

通信種別の分類

- 信頼できる宛先
- SWGに送っても意味のない通信種別
- SWGで精査させたい宛先

勘案する要素

- スループット、レスポンス速度
- セキュリティ
- 回線コスト
- SWGコスト(ライセンス帯域)

適用例

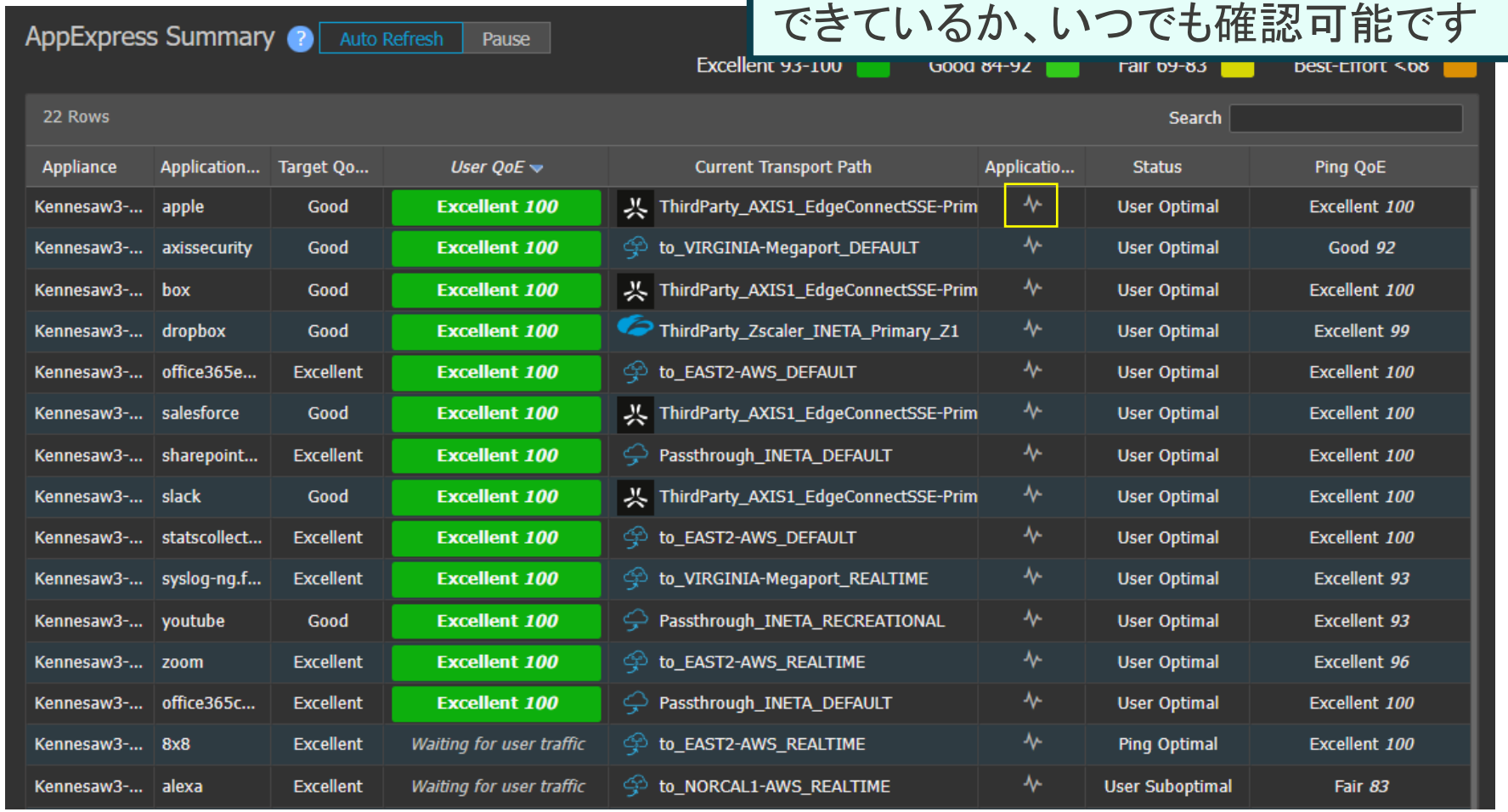
通信の種別毎にインターネット宛ての最適な経路を選択するように構成する

通信種別の分類	通信種別の例	経路	注記
信頼できる通信先	M365, Salesforce, Boxなど ビデオ会議等のメディア通信	ローカルブレークアウト クラウドハブ	DCバックホールはバックアップ
SWGに送る意味のない通信	公開鍵ピニングされているアプリケーション(復号できない) SWGのAgentからの通信 (SWG宛てのトンネルを通すとライセンス上損になる)	ローカルブレークアウト クラウドハブ	DCバックホールはバックアップ
SWGで精査したい宛先	上記以外	SWG宛てトンネル	

アプリケーションレスポンスの継続監視

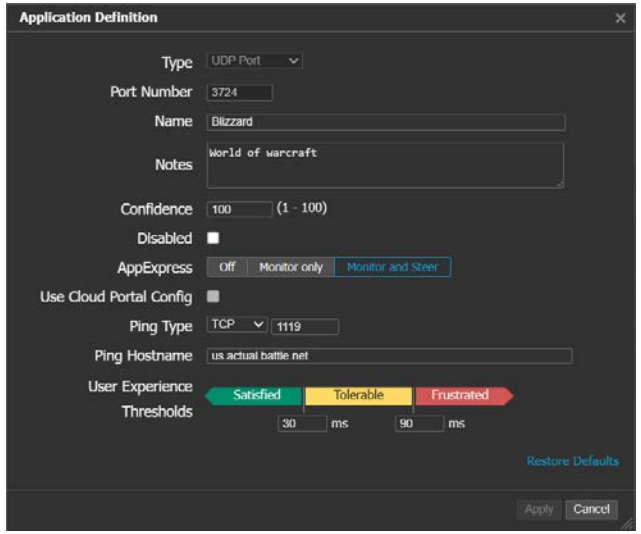
重要なSaaSへのアクセス速度を定量的に評価

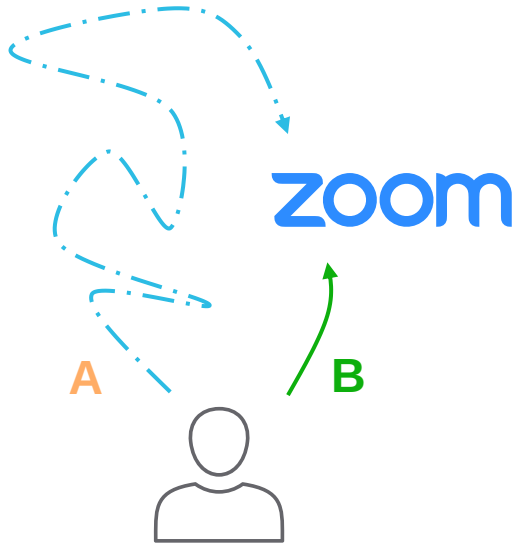
主要なアプリケーションに良好なパフォーマンスでアクセスできているか、いつでも確認可能です



Appliance	Application...	Target Qo...	User QoE	Current Transport Path	Applicatio...	Status	Ping QoE
Kennesaw3-...	apple	Good	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Prim		User Optimal	Excellent 100
Kennesaw3-...	axissecurity	Good	Excellent 100	to_VIRGINIA-Megaport_DEFAULT		User Optimal	Good 92
Kennesaw3-...	box	Good	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Prim		User Optimal	Excellent 100
Kennesaw3-...	dropbox	Good	Excellent 100	ThirdParty_Zscaler_INETA_Primary_Z1		User Optimal	Excellent 99
Kennesaw3-...	office365e...	Excellent	Excellent 100	to_EAST2-AWS_DEFAULT		User Optimal	Excellent 100
Kennesaw3-...	salesforce	Good	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Prim		User Optimal	Excellent 100
Kennesaw3-...	sharepoint...	Excellent	Excellent 100	Passthrough_INETA_DEFAULT		User Optimal	Excellent 100
Kennesaw3-...	slack	Good	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Prim		User Optimal	Excellent 100
Kennesaw3-...	statscollect...	Excellent	Excellent 100	to_EAST2-AWS_DEFAULT		User Optimal	Excellent 100
Kennesaw3-...	syslog-ng.f...	Excellent	Excellent 100	to_VIRGINIA-Megaport_REALTIME		User Optimal	Excellent 93
Kennesaw3-...	youtube	Good	Excellent 100	Passthrough_INETA_RECREATIONAL		User Optimal	Excellent 93
Kennesaw3-...	zoom	Excellent	Excellent 100	to_EAST2-AWS_REALTIME		User Optimal	Excellent 96
Kennesaw3-...	office365c...	Excellent	Excellent 100	Passthrough_INETA_DEFAULT		User Optimal	Excellent 100
Kennesaw3-...	8x8	Excellent	Waiting for user traffic	to_EAST2-AWS_REALTIME		Ping Optimal	Excellent 100
Kennesaw3-...	alexa	Excellent	Waiting for user traffic	to_NORCAL1-AWS_REALTIME		User Suboptimal	Fair 83

主要アプリケーションのレスポンス時間監視





Appliance	Application	User QoE	Current Transport Path
Kennesaw3-Po...	apple	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Primary_INETB
Kennesaw3-Po...	axissecurity	Excellent 100	to_VIRGINIA-Megaport_DEFAULT
Kennesaw3-Po...	box	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Primary_INETA
Kennesaw3-Po...	dropbox	Excellent 100	ThirdParty_Zscaler_INETA_Primary_Z1
Kennesaw3-Po...	salesforce	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Primary_INETA
Kennesaw3-Po...	sharepointon...	Excellent 100	Passthrough_INETA_DEFAULT
Kennesaw3-Po...	slack	Excellent 100	ThirdParty_AXIS1_EdgeConnectSSE-Primary_INETA
Kennesaw3-Po...	statscollector	Excellent 100	to_EAST2-AWS_DEFAULT
Kennesaw3-Po...	syslog-ng.fiv...	Excellent 100	to_VIRGINIA-Megaport_REALTIME
Kennesaw3-Po...	youtube	Excellent 100	Passthrough_INETA_RECREATIONAL
Kennesaw3-Po...	zoom	Excellent 100	to_EAST2-AWS_REALTIME
Kennesaw3-Po...	office365co...	Excellent 100	Passthrough_INETA_DEFAULT
Kennesaw3-Po...	alexa	Excellent 100	Passthrough_INETA_REALTIME
Kennesaw3-Po...	office365exc...	Waiting for user traffic	to_EAST2-AWS_DEFAULT
Kennesaw3-Po...	8x8	Waiting for user traffic	to_DESMOINES-Azure_REALTIME

Application Monitoring

監視対象のアプリケーションを選択
評価レベルの閾値を指定

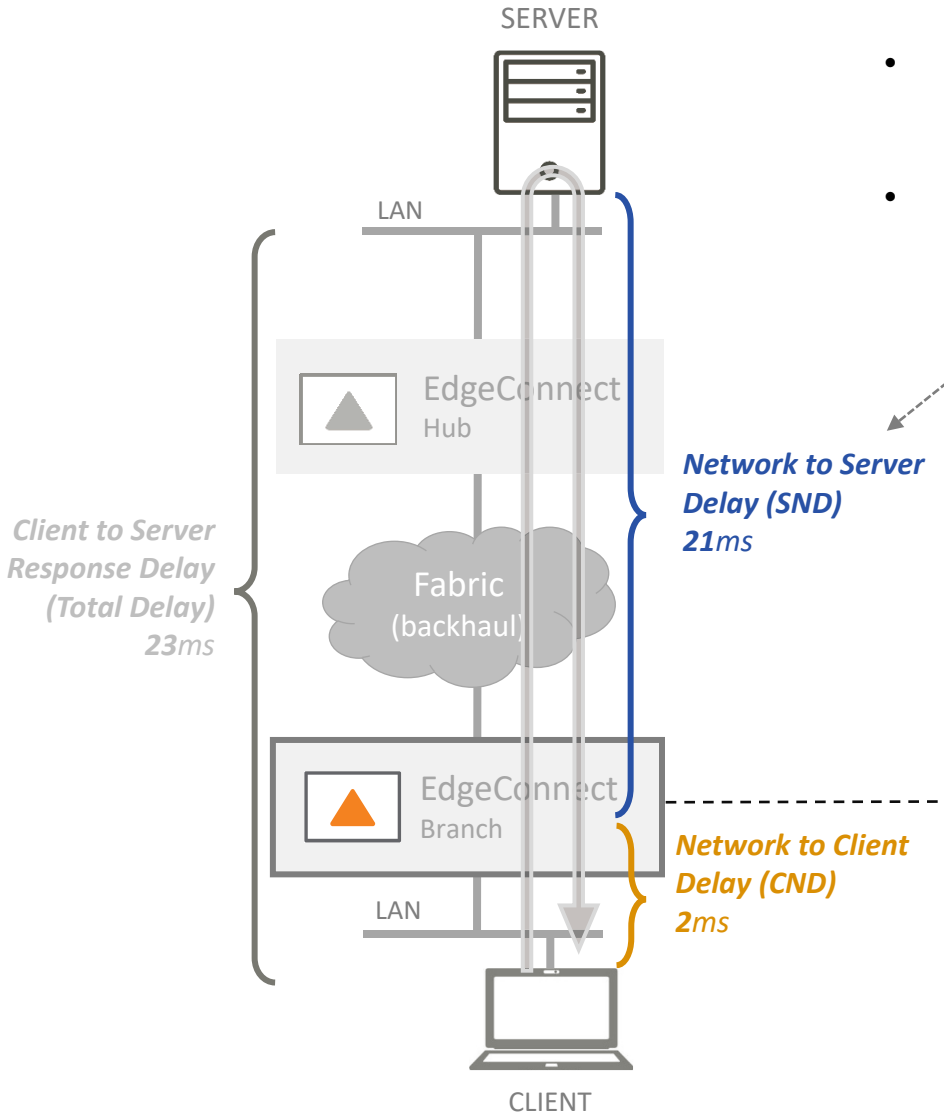
Optimized Routing

複数の経路がある場合、よりレスポンスの良い経路を選択

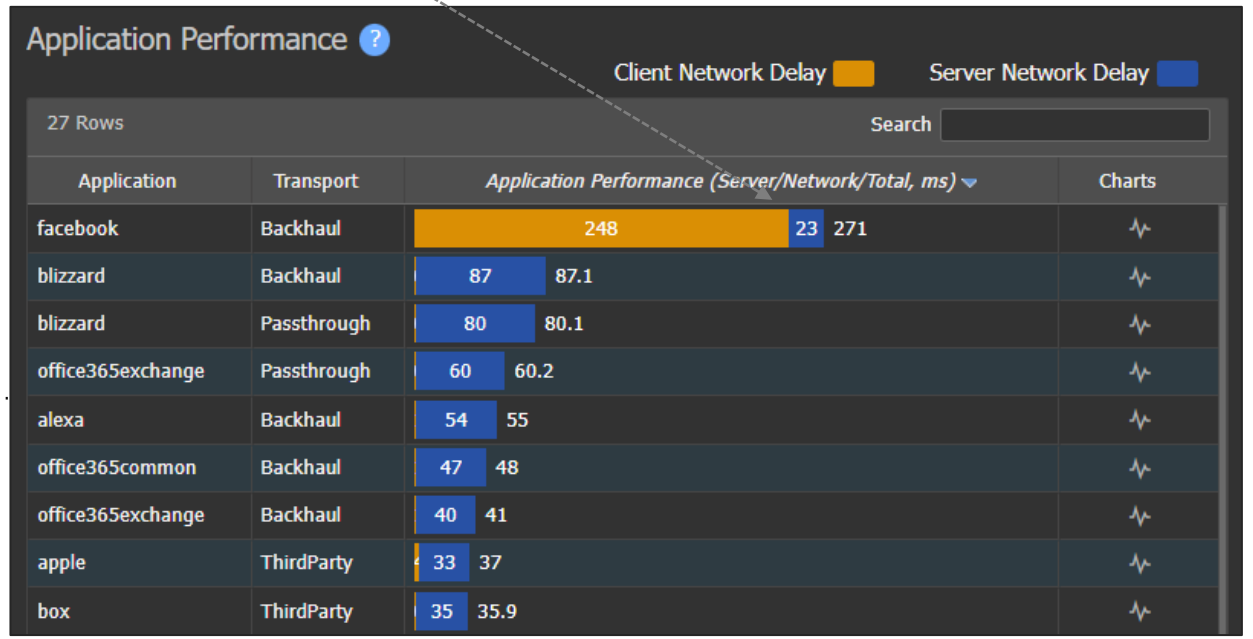
Performance Reporting

レスポンスの良否を継続的に監視して
アプリケーション毎に評価値一覧化

アプリケーションのレスポンスの計測



- LAN内から外部にアクセスする通信を計測
  クライアント側EdgeConnectからサーバーにアクセスした際のレスポンスを計測して比較、良好な通信パスを選択する
- 各区間の遅延時間を一覧にして表示



Application	Transport	Application Performance (Server/Network/Total, ms)	Charts
facebook	Backhaul	248 23 271	
blizzard	Backhaul	87 87.1	
blizzard	Passthrough	80 80.1	
office365exchange	Passthrough	60 60.2	
alexa	Backhaul	54 55	
office365common	Backhaul	47 48	
office365exchange	Backhaul	40 41	
apple	ThirdParty	33 37	
box	ThirdParty	35 35.9	

導入時の注意点

1	移行計画は重視	• 既存のネットワークを止めずにどう移行していくかは重要です • 機能、価格だけでなく移行のしやすさも評価ポイントです
2	運用負荷も要考慮	• バージョンアップ頻度等の運用負荷も製品選定時に考慮しましょう
3	POCで確認	• 同じ機能でも設定イメージには大きな差があります • 少なくとも2～3製品程度は実機で評価する事をお奨めします

Thank you

Sase-Japan@hpe.com