The way forward

HPE aruba networking

Security-First AI-Powered Networking

昨今の共通する優先事項

場所を問わないExperienceの重要性

Apps

トランザクション、ソーシャル
コラボレーション、コミュニケーション

People

従業員、請負業者、ゲスト、
患者、パートナー

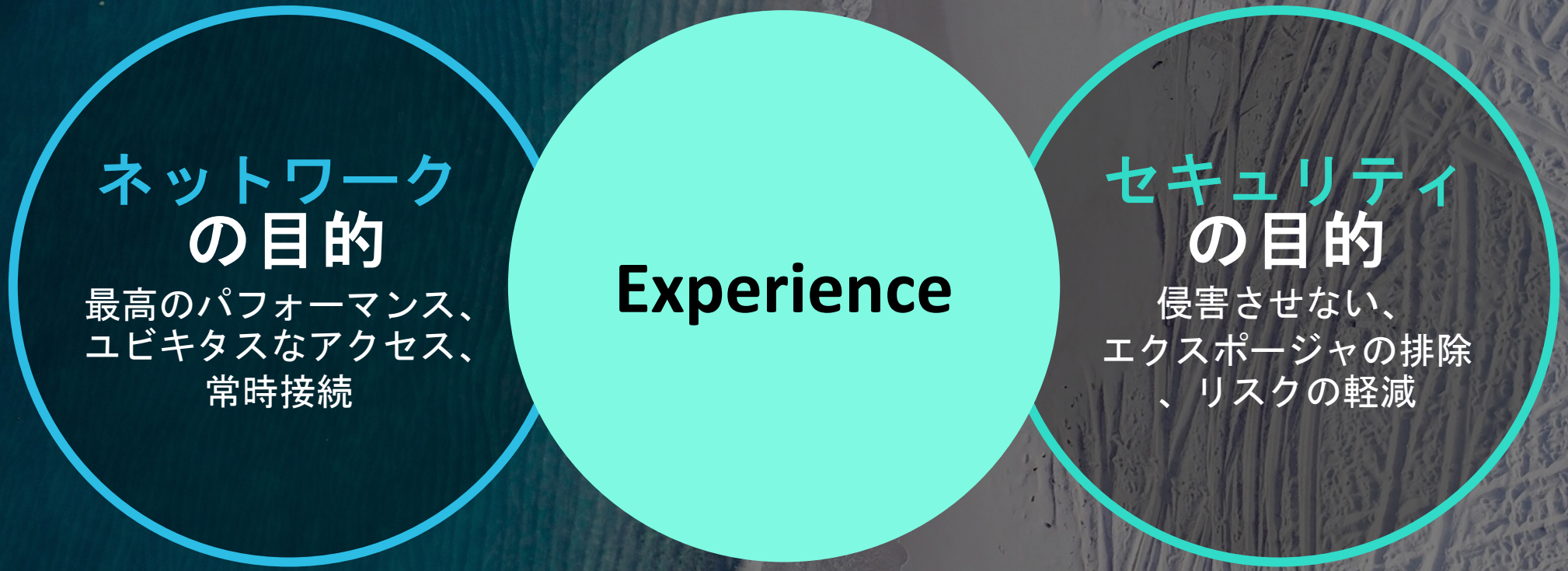
Things

カメラ、センサー、POS、
産業機械、医療機器

セキュアな接続は差別化されたExperienceの実現に不可欠

従業員の生産性の向上 | お客様の心をつかむ | 複数事業者間の信頼関係構築 | 産業効率を最適化

ビジネスは選択を余儀なくされる



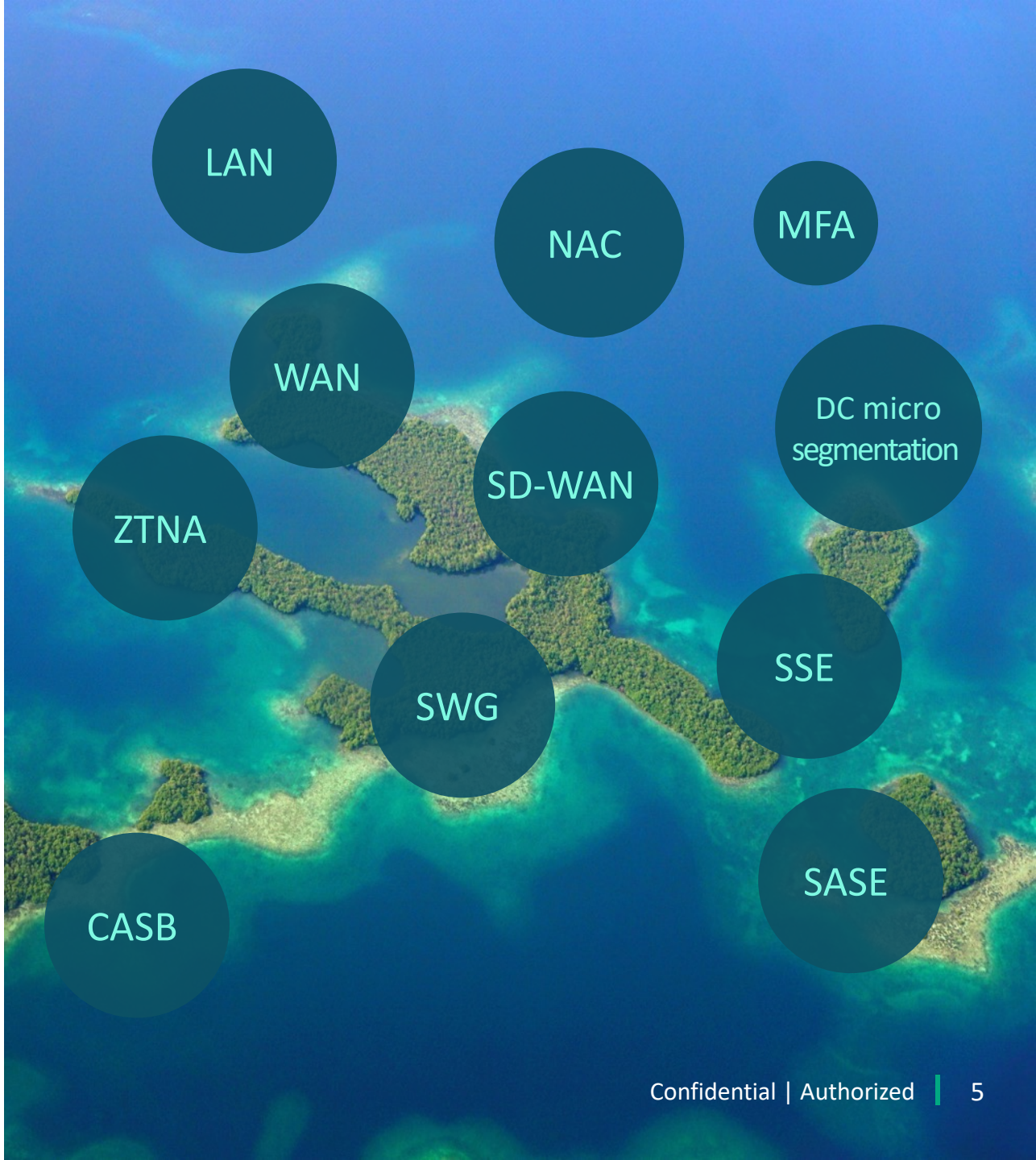
IT責任者は両者のバランスを取ろうとする

ネットワークの方向性	vs	セキュリティの方向性
アクセスの快適性		妥協のない安全性
ユーザの利便性		都度検証による信頼性
新ビジネス展開の迅速性		セキュリティリスクの低減

Patchwork complexity

しかし、
ネットワーキングと
セキュリティのイノベーションの島々で
ゼロトラストの原則を
適用することは難しい。

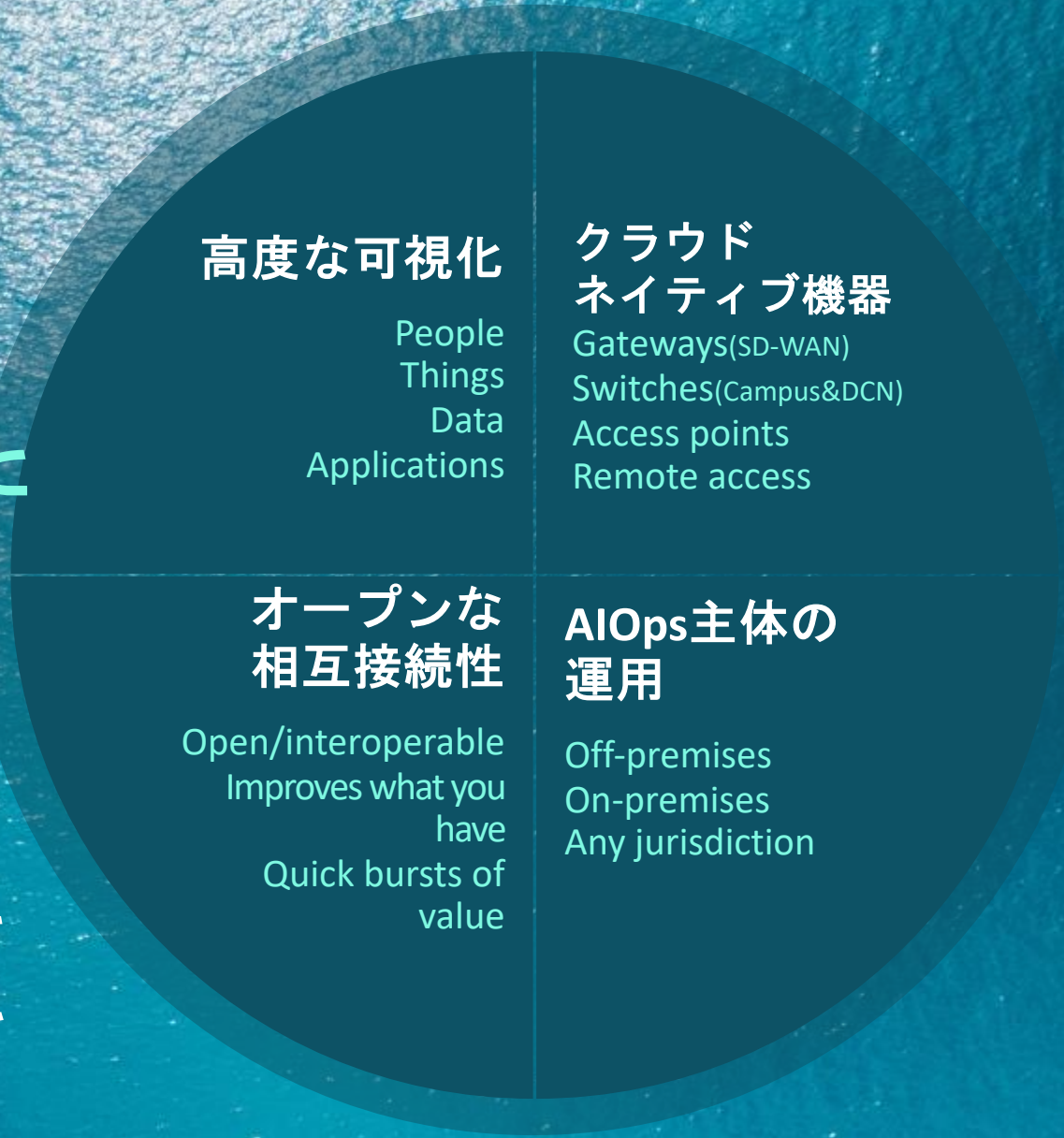
- サイロ化し、複雑さを増す
- 死角や隙間が残る
- IT全体をカバーすることはない



What’s needed

この複雑さの解決には Security-firstを前提とした ネットワークプラットフォームが必要

あらゆるネットワークにおいて本質的にゼロトラストの原則を実現すること



Our differentiators

Security-First Networkingが実現する価値

可視化の共有	グローバル ポリシー	Edge-to-Cloud エンフォース メント	AIによる自動 オペレーション
Common truth	Policies that follow you	Access Points. Switches, Gateways, Cloud	Manage at scale

Security-First AI-Powered Networking

セキュリティ対策を初めからネットワーク設計に組み込むことでユーザ利便性を下げない

Security-First AI-Powered Networking フレームワーク

人・モノ	アクセス形態	ロケーション	ネットワーク領域 セキュリティポリシー	SSEクラウド セキュリティ	データ及び アプリケーション
			Access Points Microbranch Gateway SD-Branch Gateway SD-WAN Gateway CX Switches Data Center with CX10K top of rack		

Security-First AI-Powered Networking:			
セキュリティ対策を初めからネットワーク設計に組み込むことでユーザ利便性を下げない			
可視化の共有	グローバルポリシー	Edge-to-Cloud エンフォースメント	AIによる自動 オペレーション

Security-First AI-Powered Networking を始めるには？

クラウド セキュリティ

- ZTNA：ユーザー体験とセキュリティを両立するリモートアクセス、VPNからのリプレース
- SWG：Webトラフィックに対する脅威からの保護やURLフィルタリングの実施
- CASB：SaaSアプリに対するデータの監視と制御を行い企業ポリシーの管理と徹底
- 統合されたシンプルなSSE

WANエッジの モダナイゼーション

- クラウドファーストを念頭に置いたWAN エッジ
- 拠点のファイアウォールとルーターをリプレース
- IoTデバイスなど全てのデバイスを制御対象にし、アプリのパフォーマンス向上とセキュリティも確保

SASE イニシアティブ

- ユーザーにとって快適なハイブリッドワーク環境を提供
- SD-WANとSSEをシングルベンダーで実現

キャンパス ネットワークの変革

- ユニファイドインフラストラクチャー
- 全てのユーザーとデバイスための最先端のネットワーク提供
- AI活用を駆使したネットワークとセキュリティの運用の変革

データセンター ネットワーク モダナイゼーション

- AFCによる設定の合理化と簡素化
- DPU対応スイッチを活用した分散型アーキテクチャ

AFC: Aruba Fabric Composer
DPU: Data Processing Unit

NACドリブン セグメンテーション

- 一元化されたロールベースのポリシーを適用
- 一貫した(有線/無線、WANネットワーク)に対するダイナミックなポリシー適用

NAC: Network Access Control

Hewlett Packard Enterprise

あらゆる場所やデバイスから高速・安全に接続、最新ネットワーク環境の作り方

日本ヒューレット・パッカード合同会社
Aruba事業統括本部　第一技術部　部長
池田　豊

2024年2月20日

Security-First AI-Powered Networking

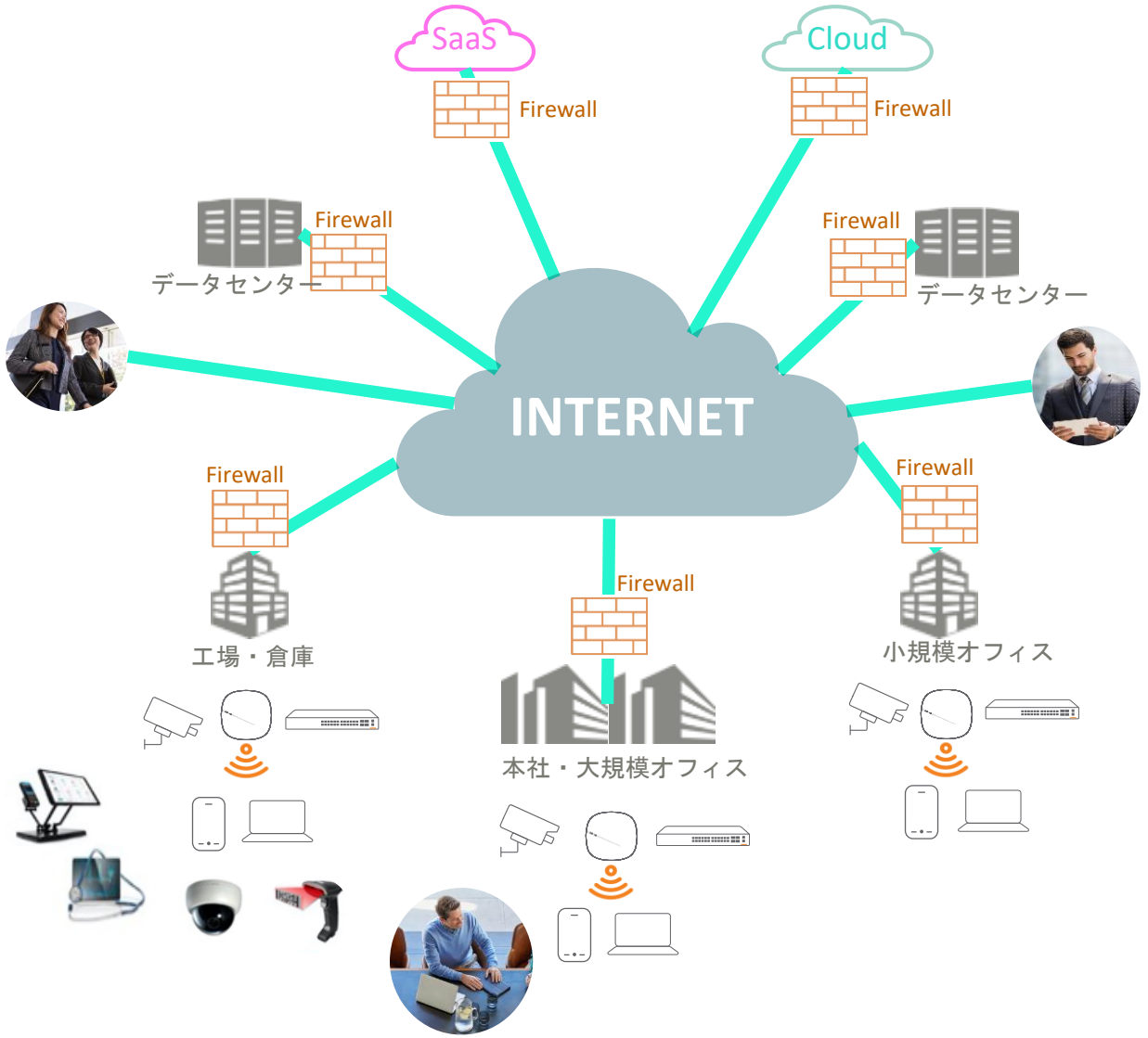
MISSION

ネットワーク領域における
アタックサーフェス(攻撃対象領域)を低減させること

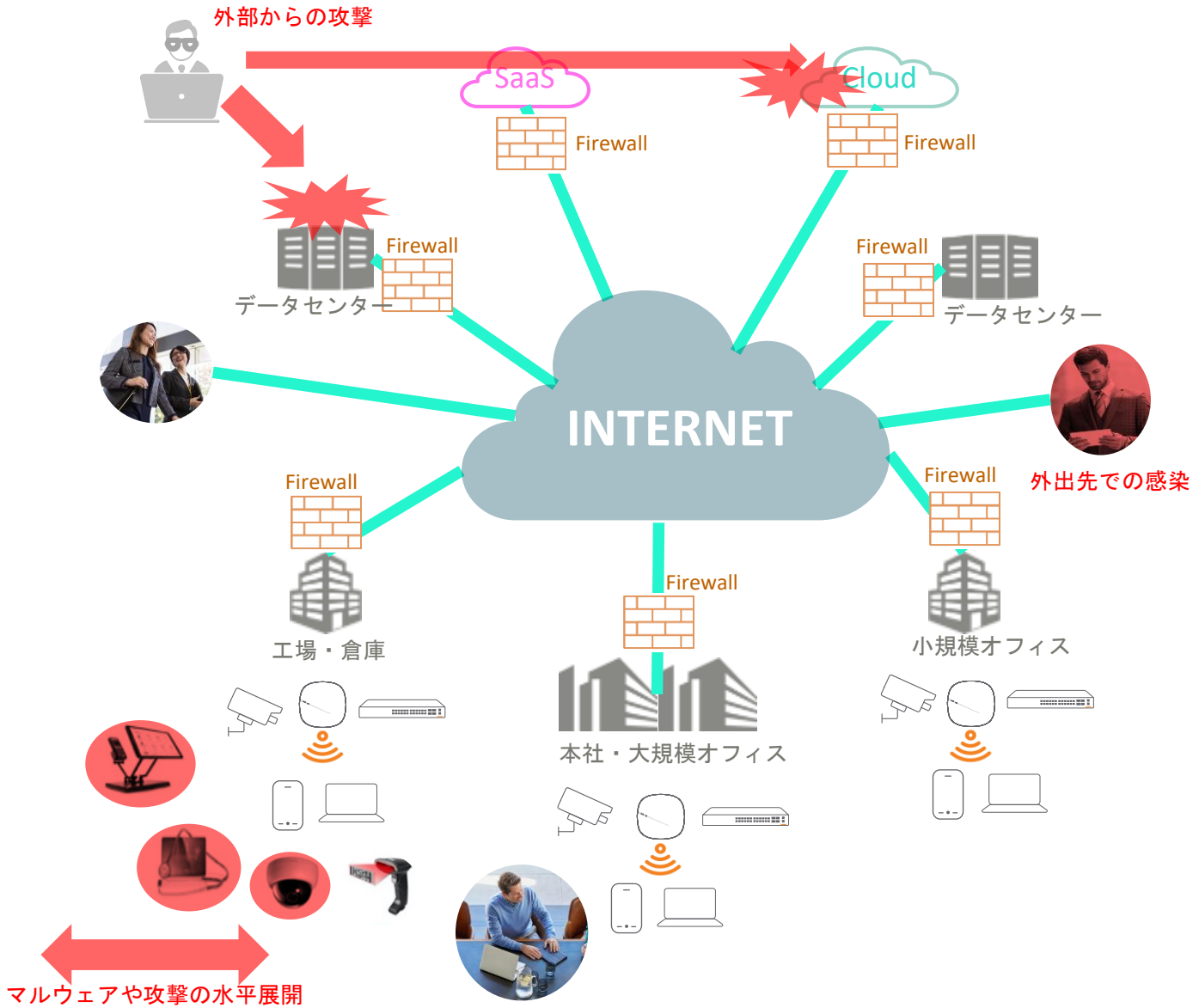
本セッションのポイント

- 外部からの対策
- 内部からの対策
- HPEが目指す企業ネットワークのTOBE像

現在の社内ネットワークはインターネット中心の分散型アーキテクチャモデル

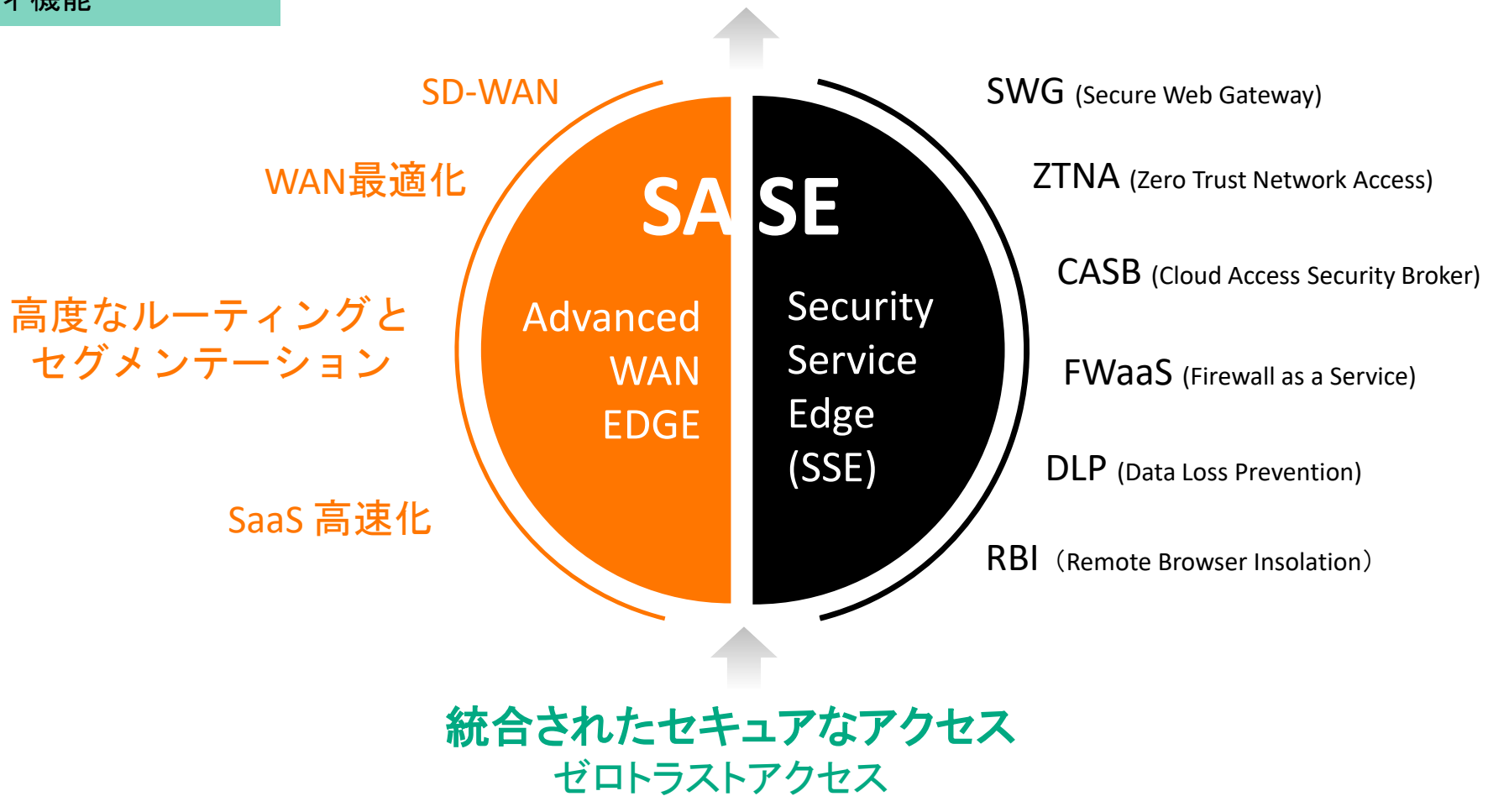


インターネット中心のアーキテクチャはゼロトラストが原則



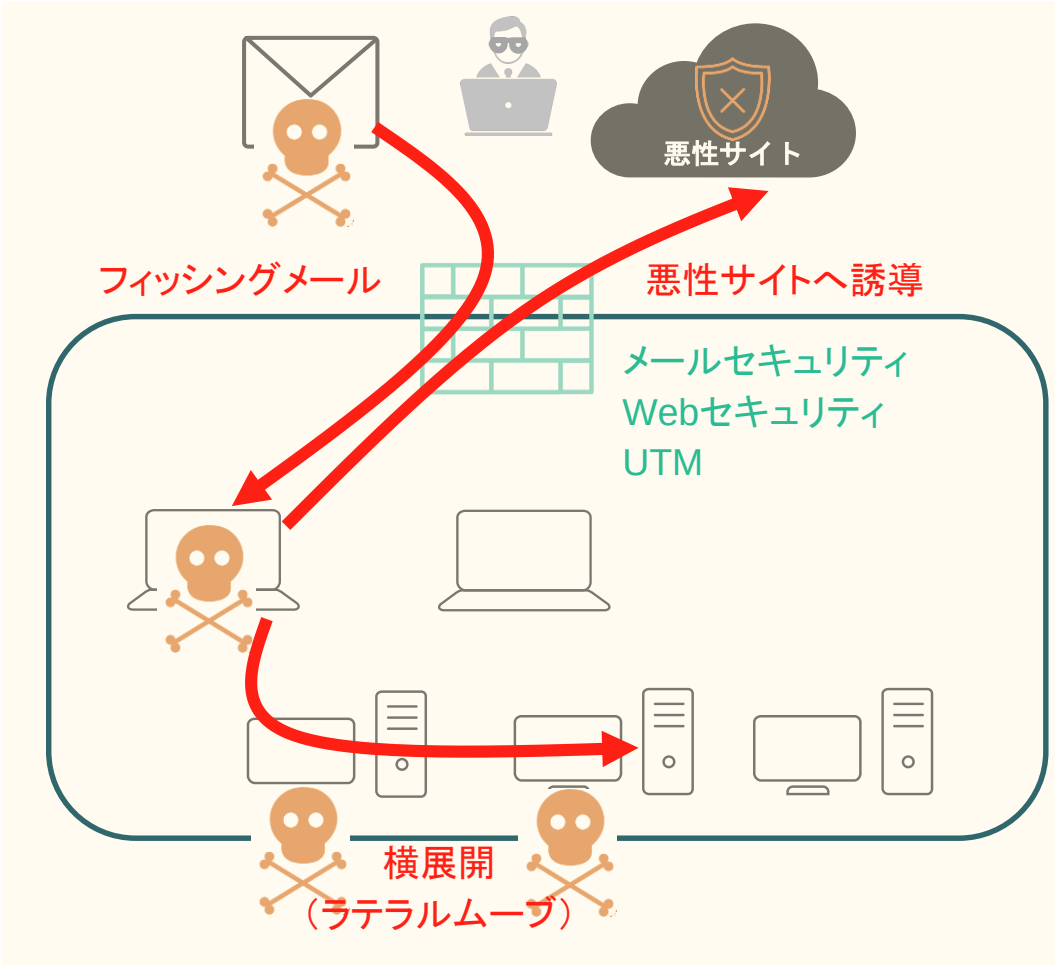
多くの企業ではゼロトラストネットワーク構築のため、SASE実装の検討が進む

SASE (Secure Access Service Edge)
Gartnerが提唱するサービスとしての
統合ネットワークとセキュリティ機能



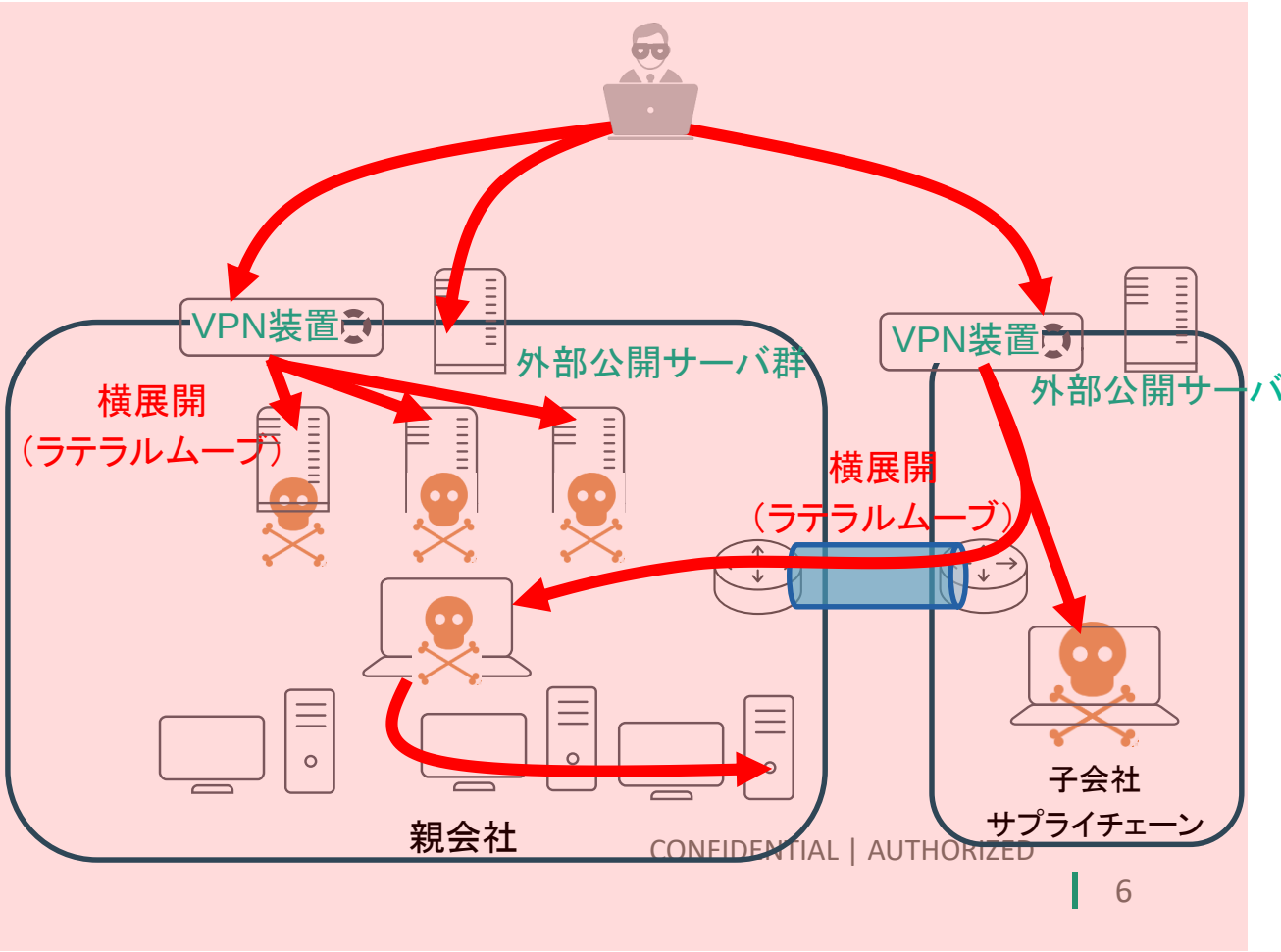
昨今、ランサムウェア攻撃侵入経路の多様化が課題

従来の主な侵入・感染方法



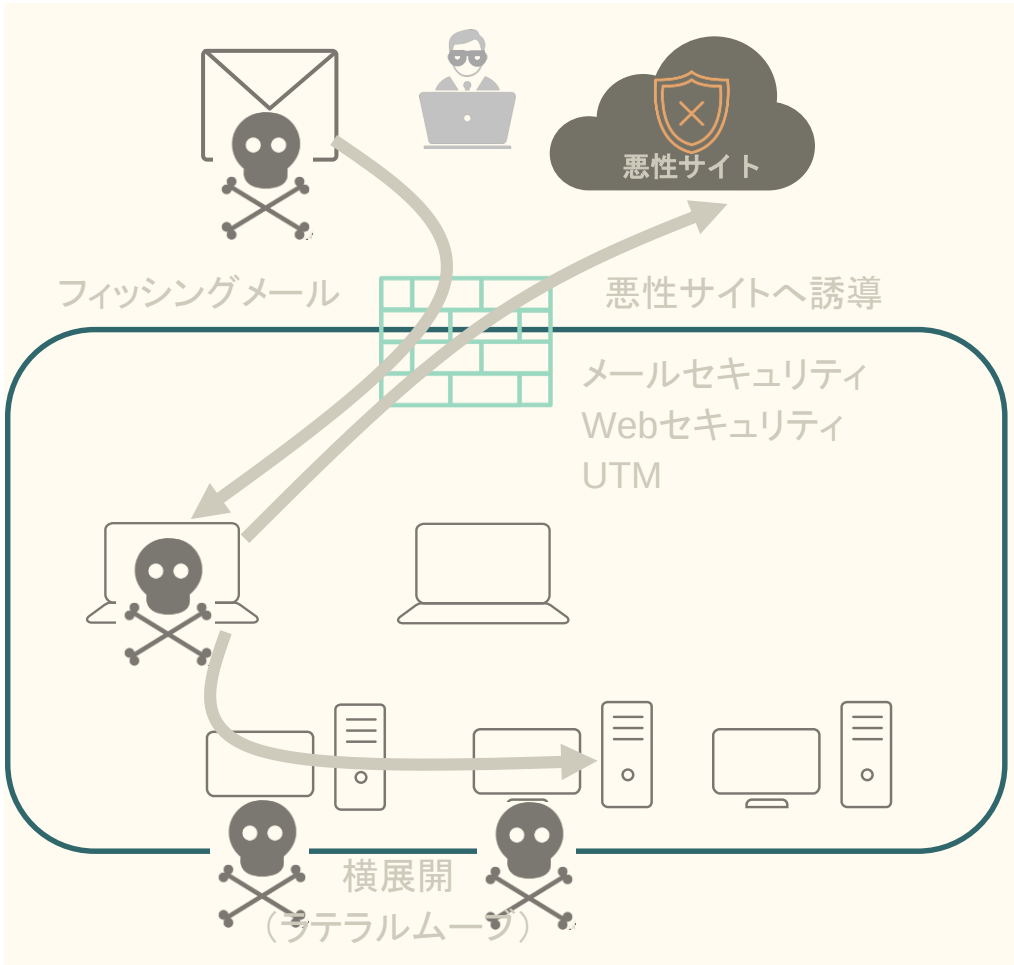
＋

最近の侵入・感染方法



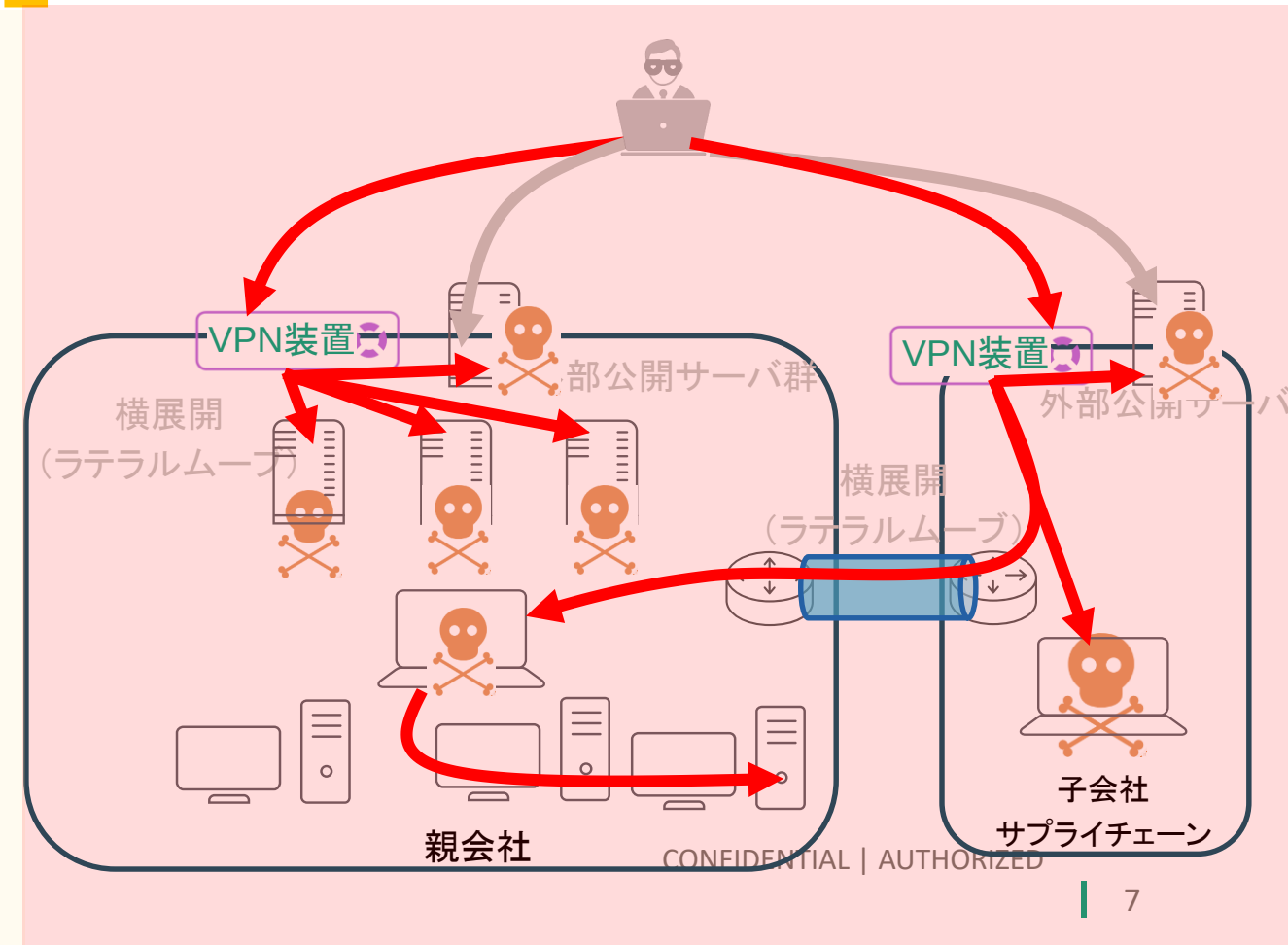
VPN装置が攻撃対象及び攻撃起点

従来の主な侵入・感染方法



＋

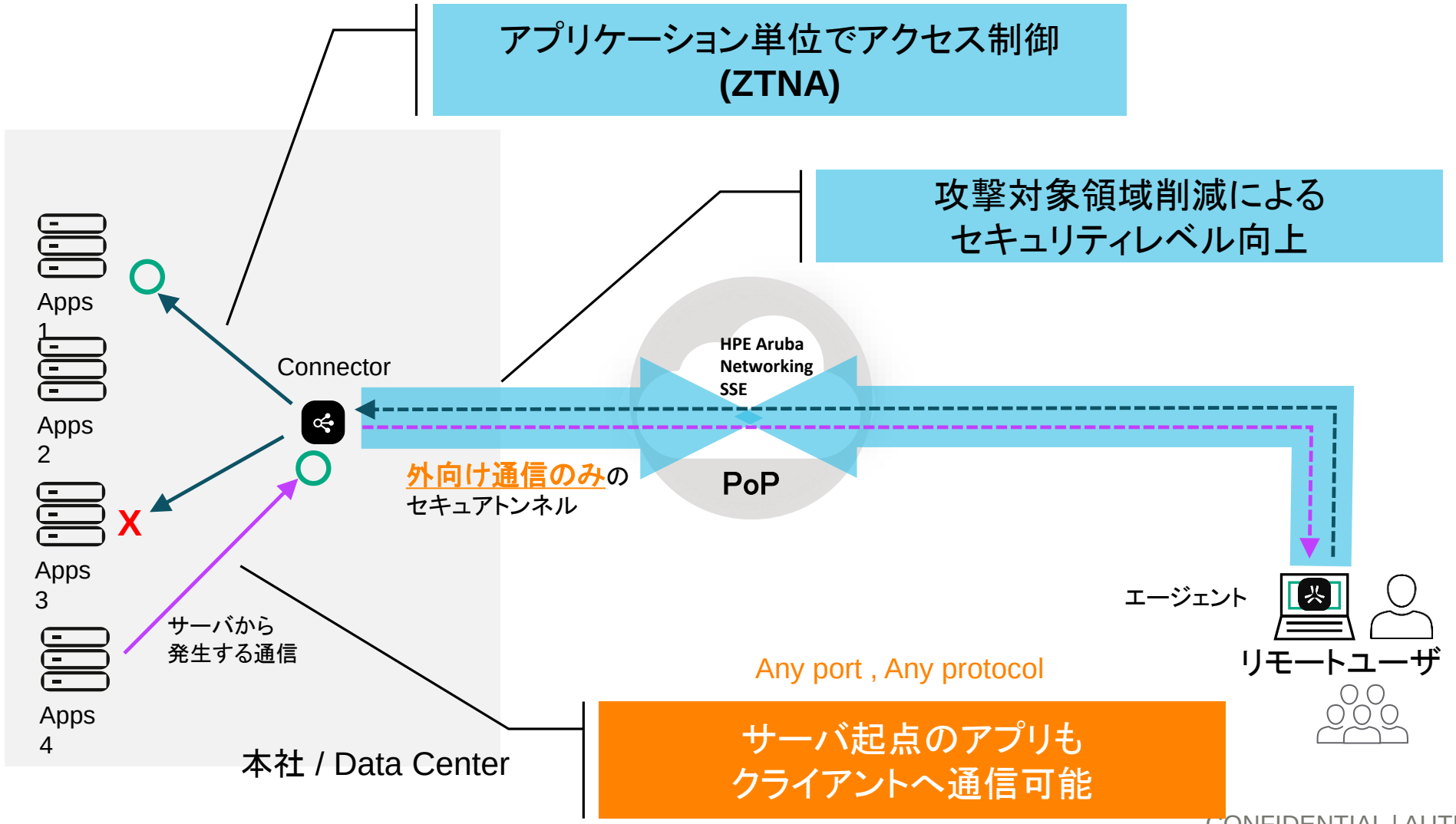
最近の侵入・感染方法



外部からのアタックサーフェス対策
VPN → ZTNA

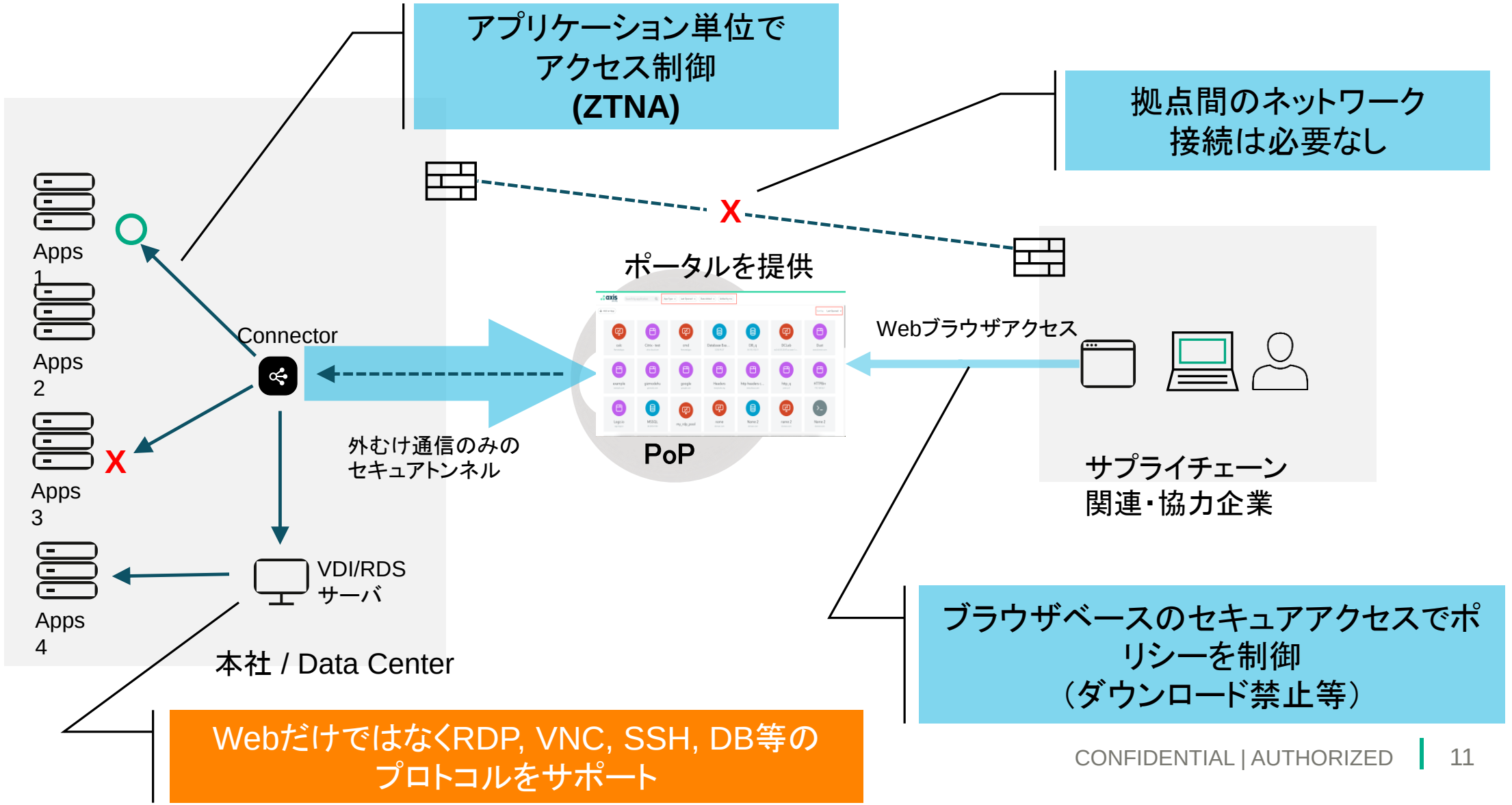
SASEコンポーネントの一部であるZTNA
なぜ普及が進まない？

HPE Aruba Netwroking SSE（ZTNA）は従来のZTNA課題を解決



買収先企業、協力会社、関係会社からも安全なアクセス

エージェントがインストールできない環境にエージェントレスZTNA



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

CASB

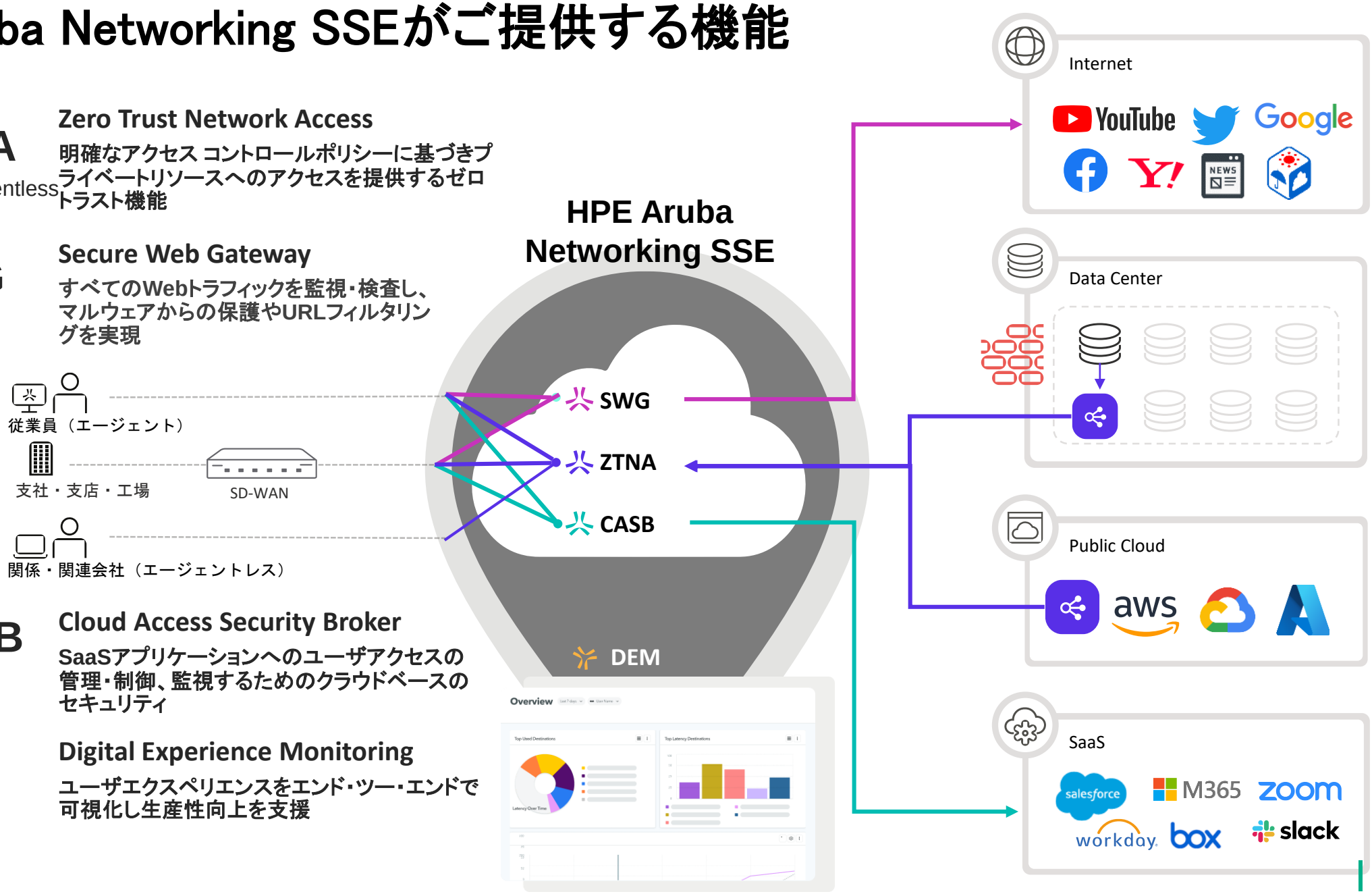
Cloud Access Security Broker

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

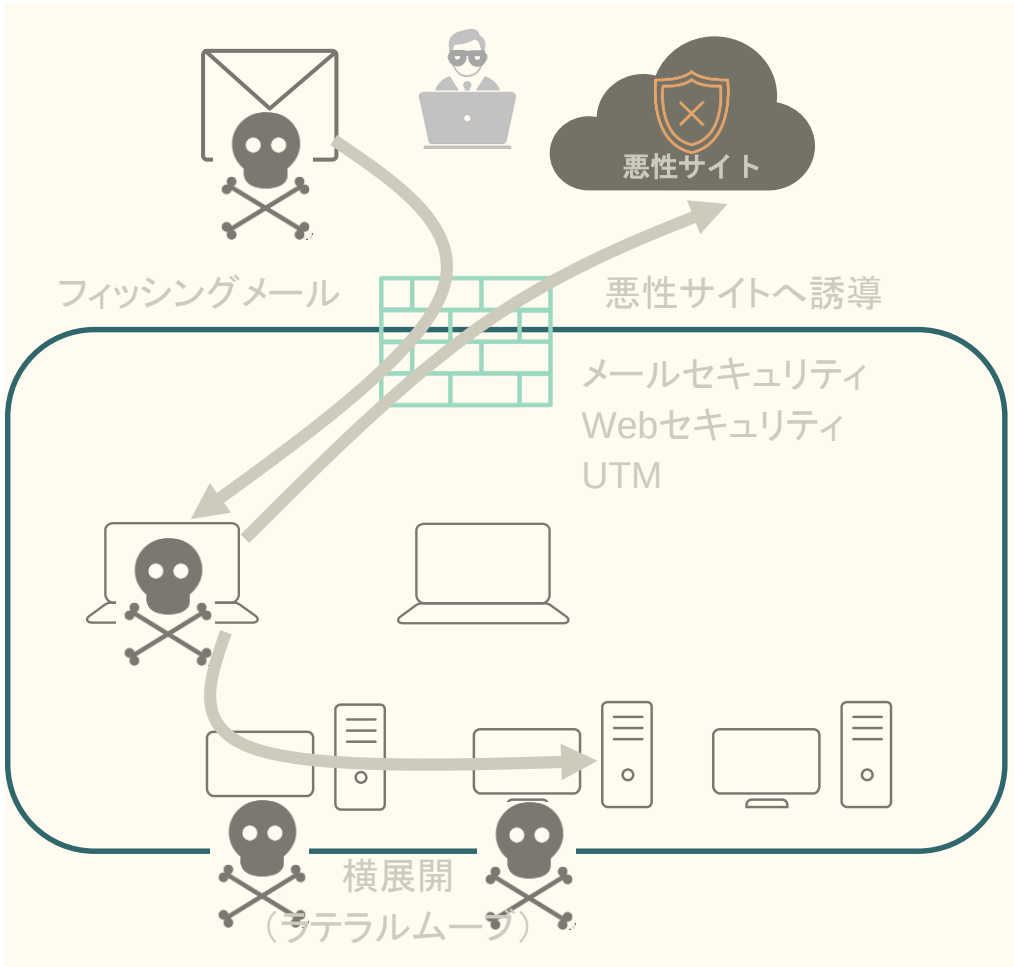
ユーザエクスペリエンスをエンド・ツー・エンドで可視化し生産性向上を支援



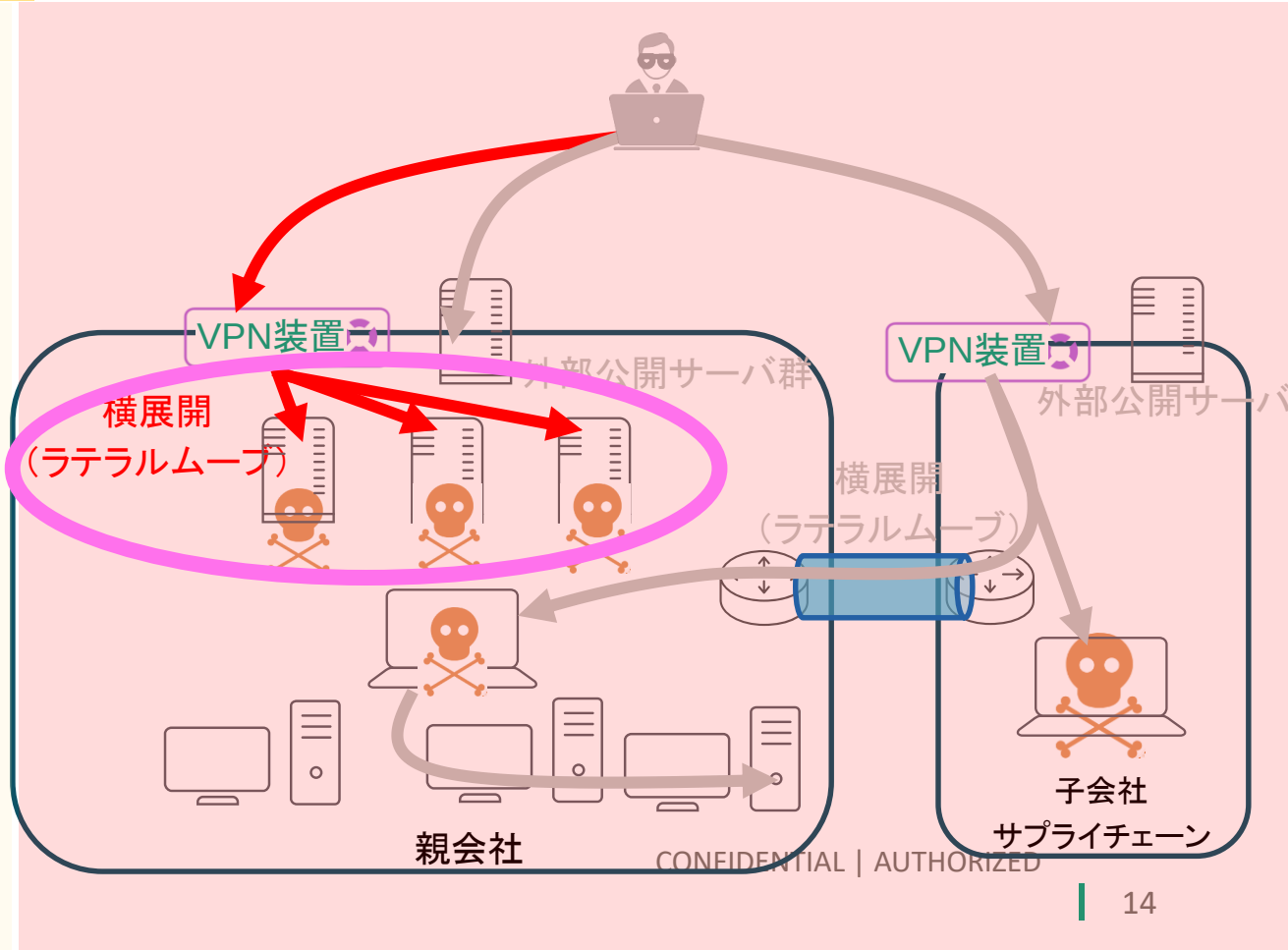

VPN環境は
まだ排除できない

VPN装置が攻撃起点となると、脆弱なサーバーファーム（DMZ）

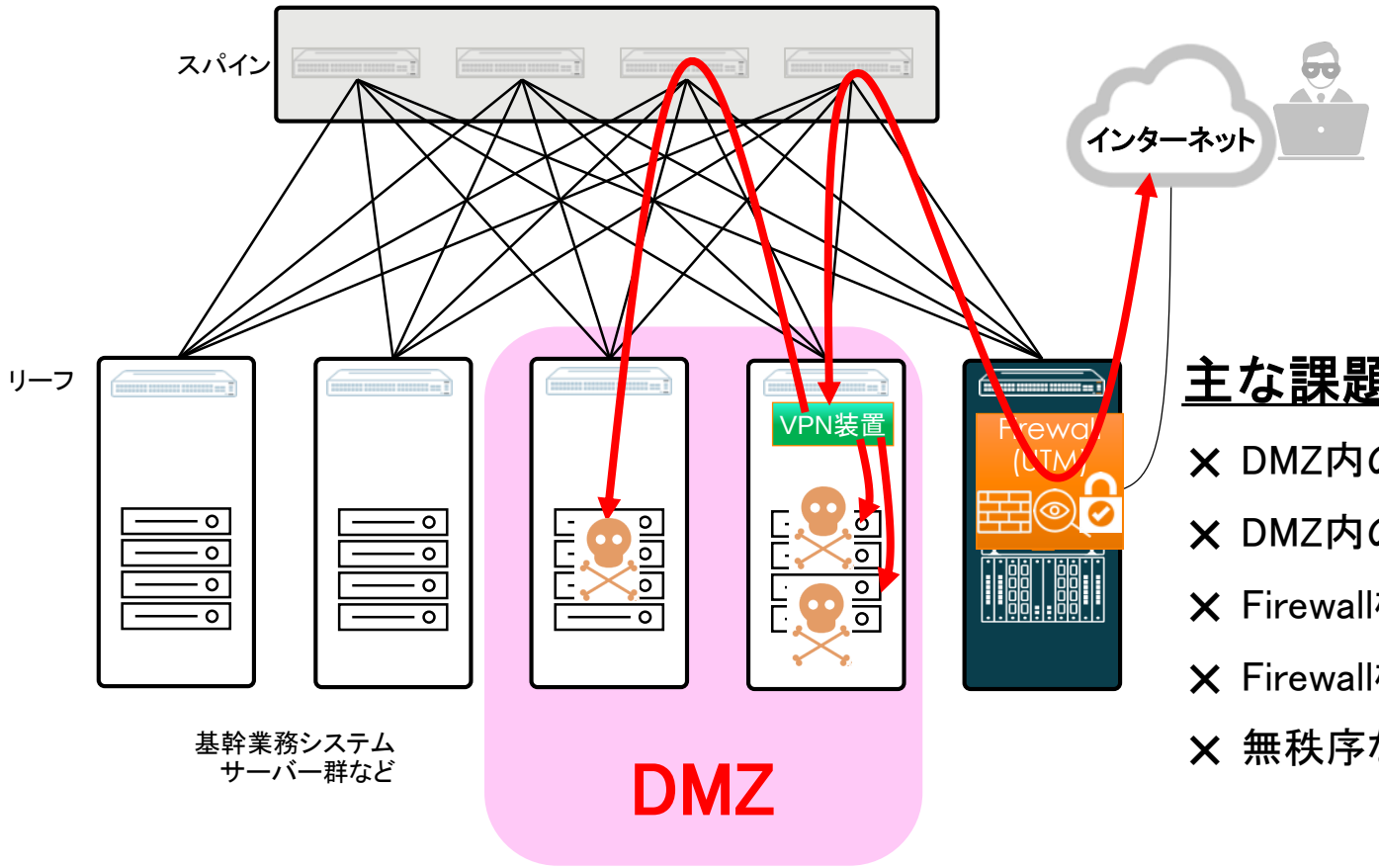
従来の主な侵入・感染方法



現在の侵入・感染方法



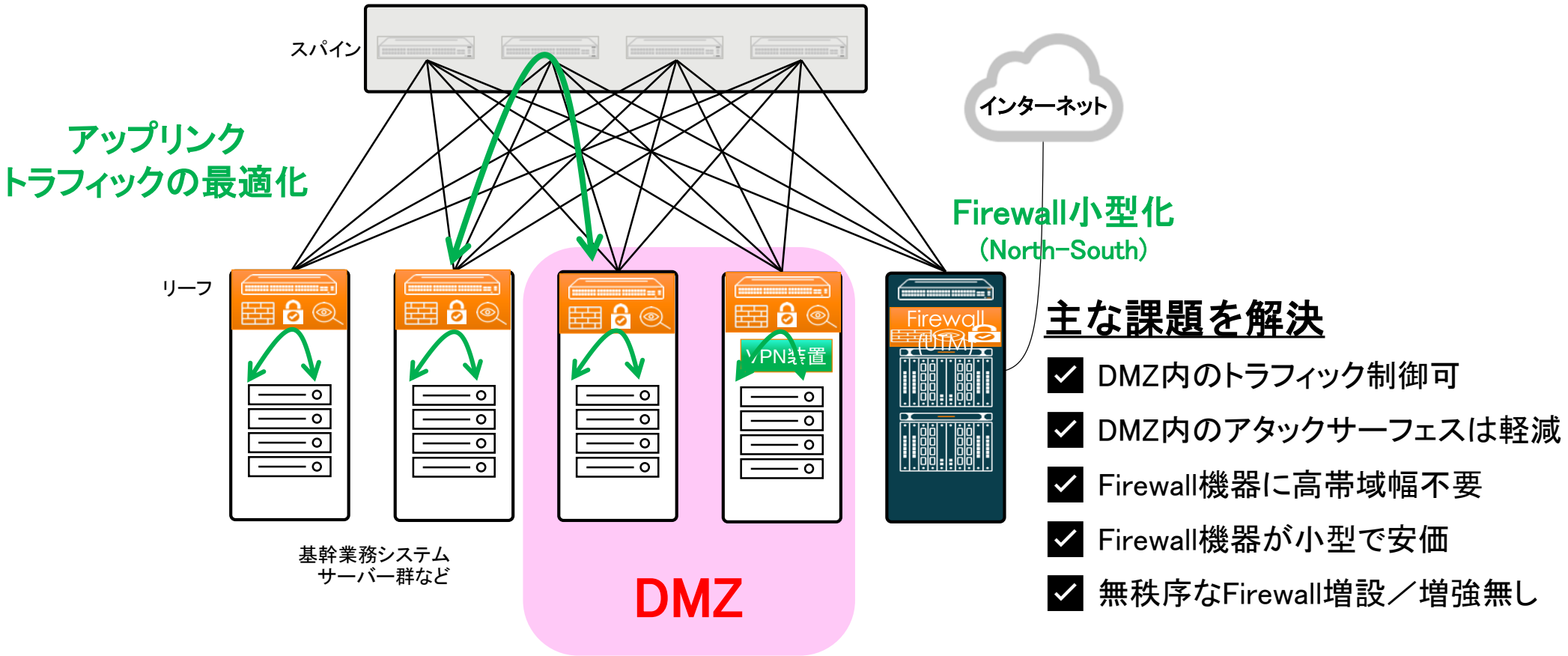
DMZ内はフラットなネットワーク構成が多く、攻撃が横展開されやすい



主な課題

- ✕ DMZ内のトラフィック制御不可
- ✕ DMZ内のアタックサーフェスは軽減不可
- ✕ Firewall機器に高帯域幅が必要
- ✕ Firewall機器が大型で高額
- ✕ 無秩序なFirewall増設／増強

DC内のアタックサーフェスを軽減するには、リーフ（もしくはToR）スイッチでステートフルファイヤーウォール機能を実装すること



主な課題を解決

- ✓ DMZ内のトラフィック制御可
- ✓ DMZ内のアタックサーフェスは軽減
- ✓ Firewall機器に高帯域幅不要
- ✓ Firewall機器が小型で安価
- ✓ 無秩序なFirewall増設／増強無し

CX10000はDPU搭載の分散サービススイッチ

DCNのセキュリティサービスを簡素化、トラフィック最適化、高い拡張性を提供

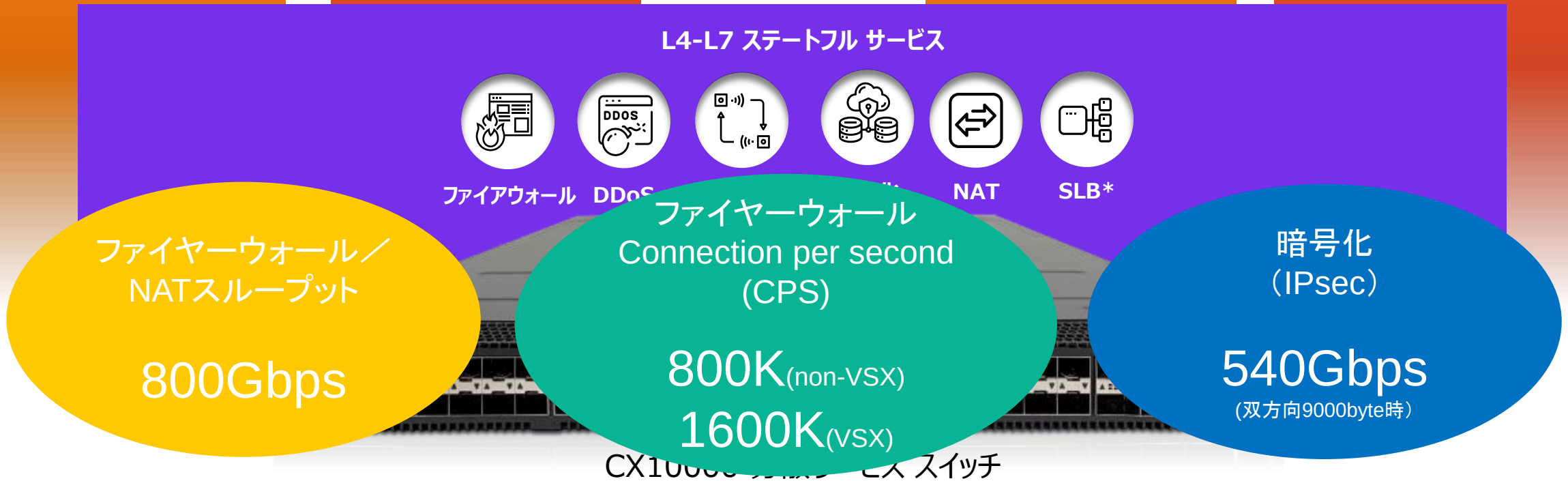
新しいカテゴリ
分散サービス スイッチ

ゼロトラストをネットワーク
サーバーエッジに拡張
ワークロード/アプリの近く
にファイアウォール

AMD PENSANDO

帯域幅を最適化し、ネット
ワーク/セキュリティのプ
ロビジョニングを簡素化

拡張性とパフォーマン
スの大幅な向上、
TCO の削減

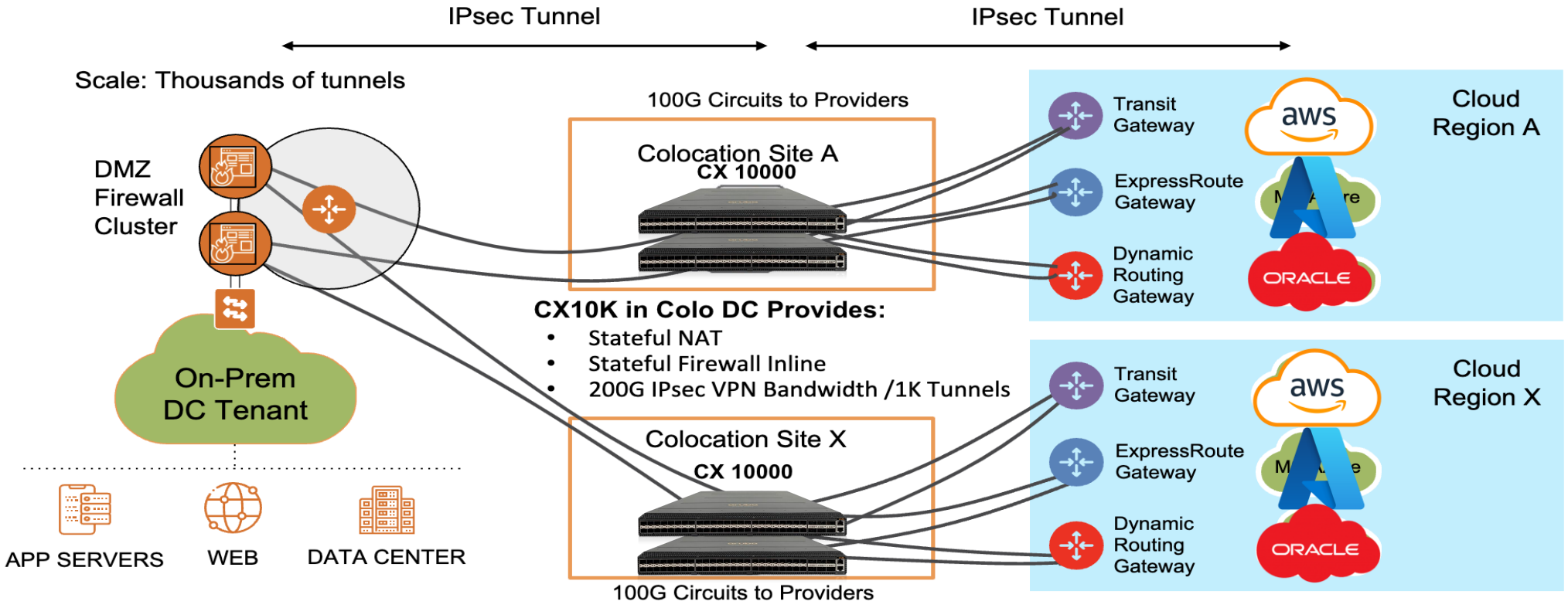


CX10000 分散サービス スイッチ
Aruba AOS-CX オペレーティング システム
3.2Tbps、48x 10/25G & 6x 100G フルプロトコルスタック、拡張性のある集中管理

*Requires future software release.

CX10000もう一つの使用例

複数DCとコロケーションエッジをマルチクラウドへセキュアに相互接続



複数のDC ロケーションを安全に相互接続

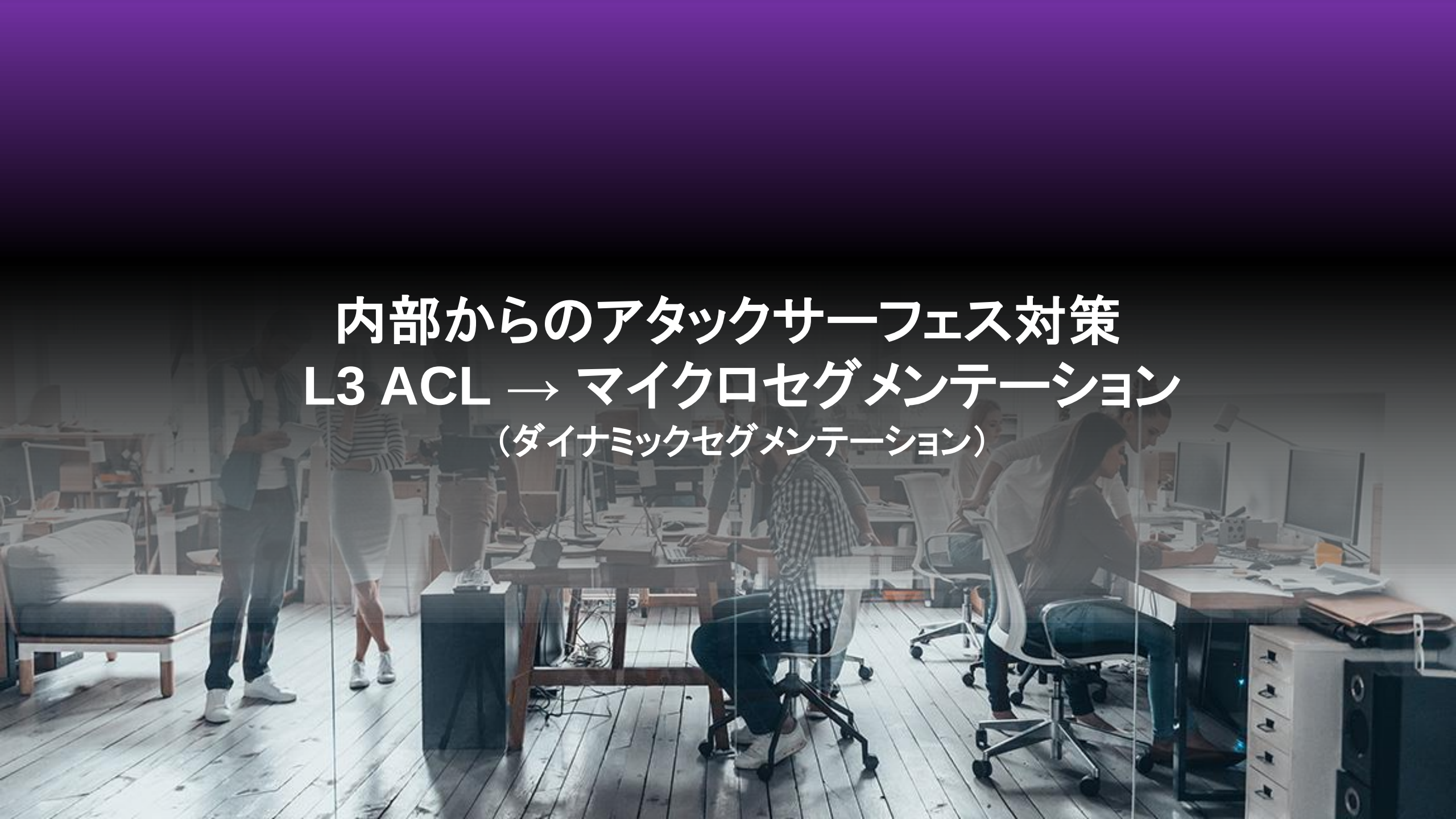
200G IPsec暗号化 | ルーティング | ファイアウォール | NAT

TCOを75%以上削減、影響範囲を極小化、プロバイダを介したHAを実現

事例:

200台を超えるCX10Kを対象としたTier 2 MSPプロジェクト:
5 年間で FW/IPsec のコストを 1億ドル削減 !!

内部からのアタックサーフェス対策
L3 ACL → マイクロセグメンテーション
（ダイナミックセグメンテーション）



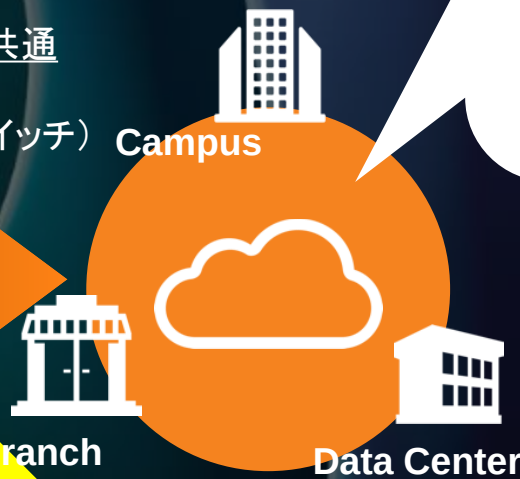
一般的な社内ネットワークセキュリティの課題は「認証後」

無線LAN
・暗号化（WPA2-AES）

有線LAN
・ポートセキュリティなど

無線・有線LAN共通
・802.1x(証明書認証)
・MACアドレス認証

無線・有線LAN共通
・VLAN境界型
ACL制御（L3スイッチ）



認証後、従業員の端末は社内自由にアクセスできる場合が多く、

ゼロトラスト原則のネットワーク設計でない

エンドポイント及び認証や暗号化に関しては、頻繁に設計アップデートが行われ、十分に対策済

過去10年以上、設計がアップデートされていない

なぜ、キャンパス内マイクロセグメンテーションの普及が進まない？

米国国立標準技術研究所（NIST）の発表したサイバーセキュリティフレームワーク（CSF）でも、ゼロトラストアーキテクチャを構築する上での必要なアプローチの1つとして、マイクロセグメンテーションを利用することが明記されている。日本でも、政府情報システムのためのセキュリティ評価制度（ISMAP）にて、マイクロセグメンテーションがゼロトラストの要素と記載されている。

とは言っても…

EDR+SWGがある
から大丈夫

単純に面倒

ポリシーの
ライフサイクル管理が大変

そもそも
ポリシー定義できない

自分の負荷が増えるだけ

Micro-Segmentation実装検討の進め方

#1. エージェント導入できない脆弱なデバイス（プリンタ、IP電話、IoTデバイスなど）への適用を想定する

#2. デバイスが送信するトラフィックの可視化

#3. マクロでポリシーを考え（マイクロではない）、大雑把なポリシーグループを作り、適用する

#4. 運用の中で、マクロからマイクロへのポリシー移行を進め、一定のライフサイクルを確立

#5. 業務用PCなど、他デバイスのポリシーグループを作り、同様にマクロからマイクロポリシーへ段階的に適用を進める

Micro-Segmentation実装検討の進め方

#1. エージェント導入できない脆弱なデバイス（プリンタ、IP電話、IoTデバイスなど）への適用を想定する

#2. デバイスが送信するトラフィックの可視化

#3. マクロでポリシーを考え（マイクロではない）、大雑把なポリシーグループを作り、適用する

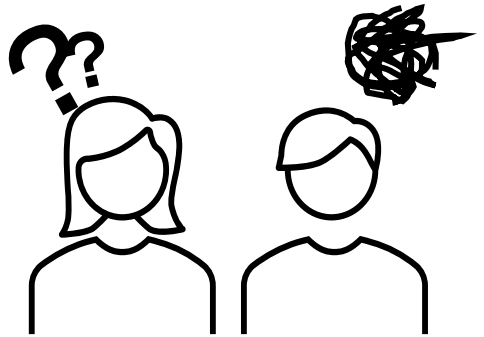
#4. 運用の中で、マクロからマイクロへのポリシー移行を進め、一定のライフサイクルを確立

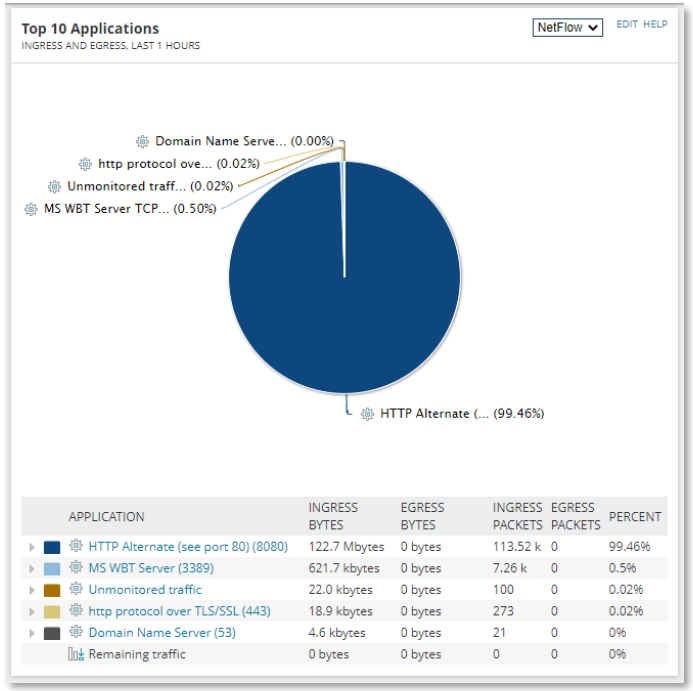
#5. 業務用PCなど、他デバイスのポリシーグループを作り、同様にマクロからマイクロポリシーへ段階的に適用を進める

現在もログやフローデータは集めてるが、あまり活用されてない

主にトラブルシューティング時に利用

・ポートのトラフィック量のみ監視
・Syslogサーバーにイベントログ送付のみ
・sFlow/NetFlowデータではHTTPSなど詳細な
アプリケーション情報が不明
・端末情報はIPアドレスとMACアドレスのみ

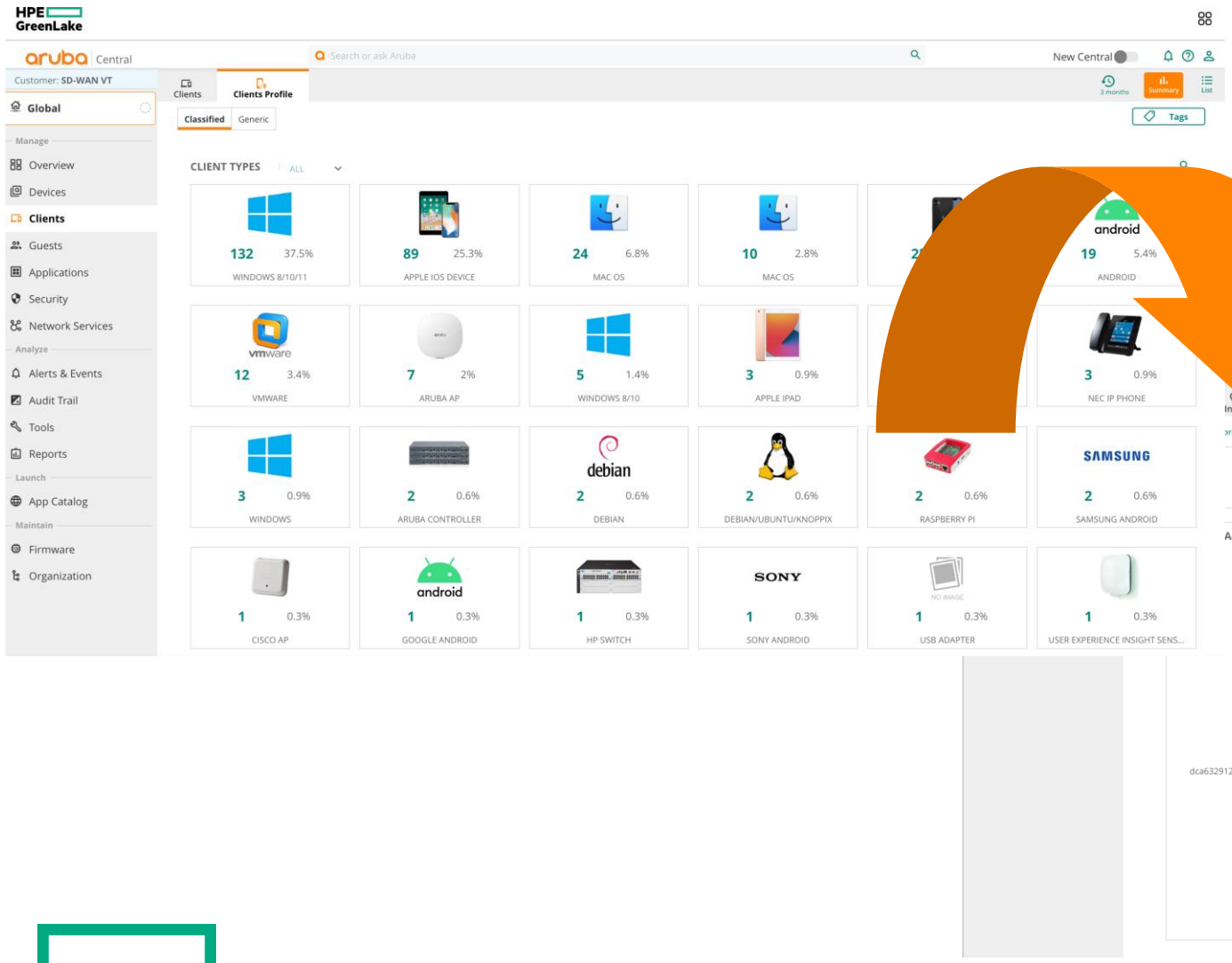




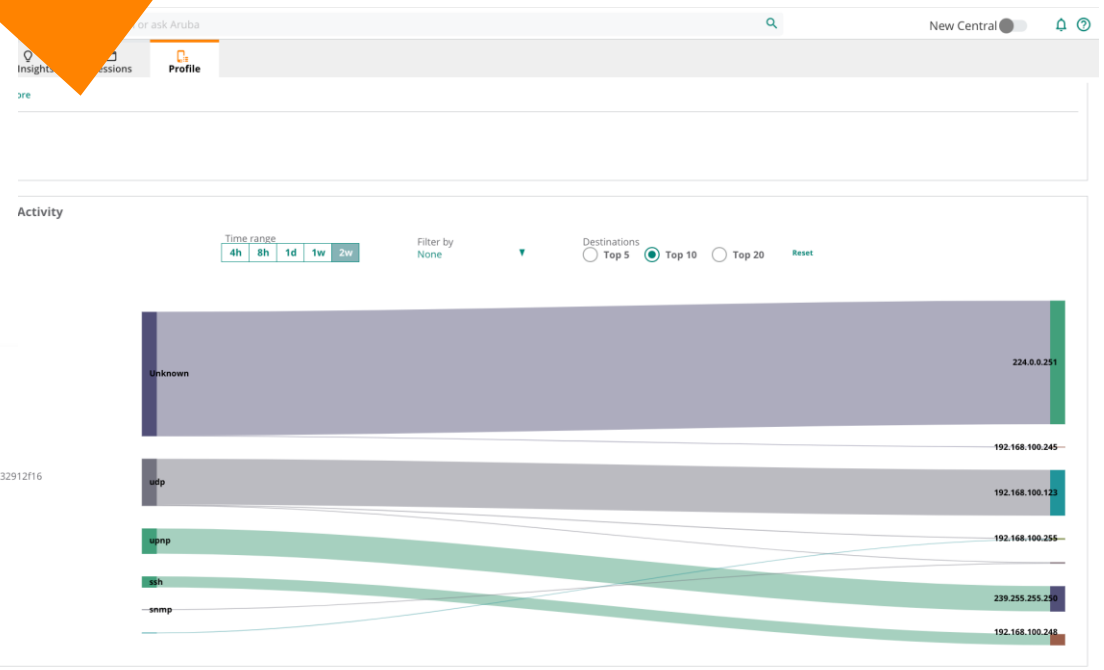
一般的なFlow情報の可視性

ポリシー設計に役立つ可視性が必要

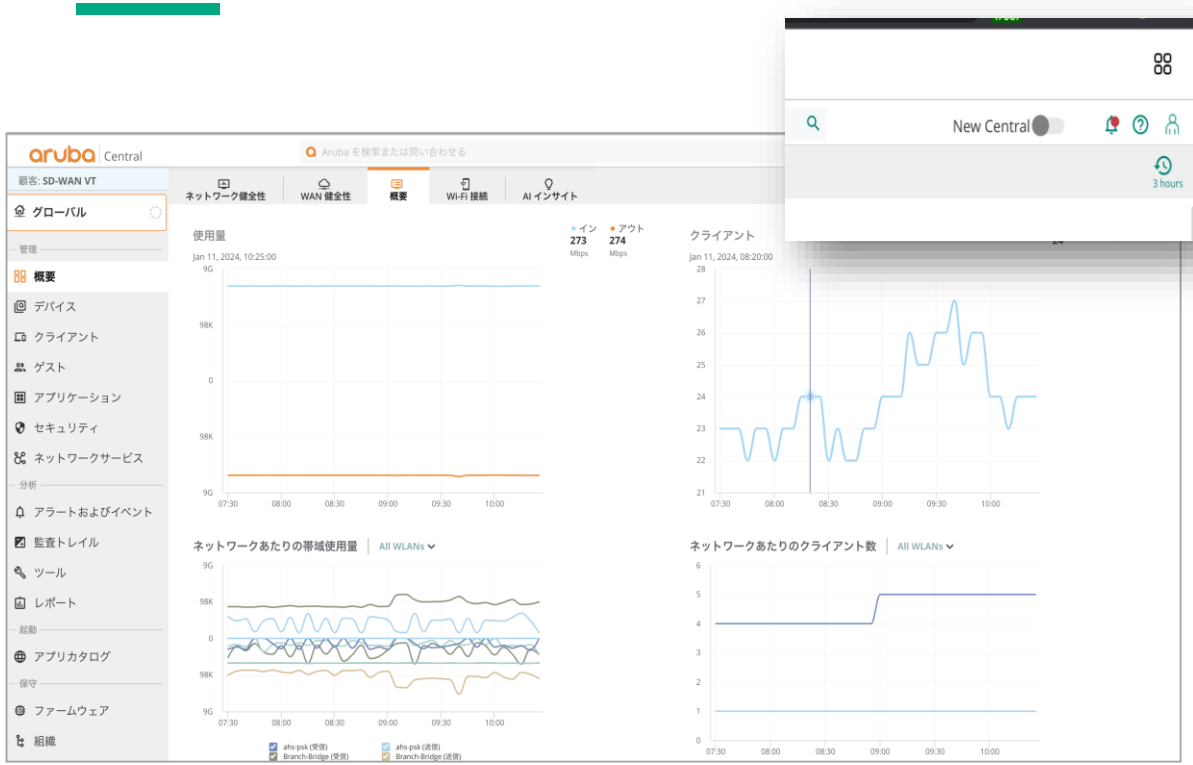
Centralなら有線・無線デバイスをAIで自動特定 (※Gateway構成、有線LANはUBT利用を想定)
トラフィックトレンドも一目でわかる



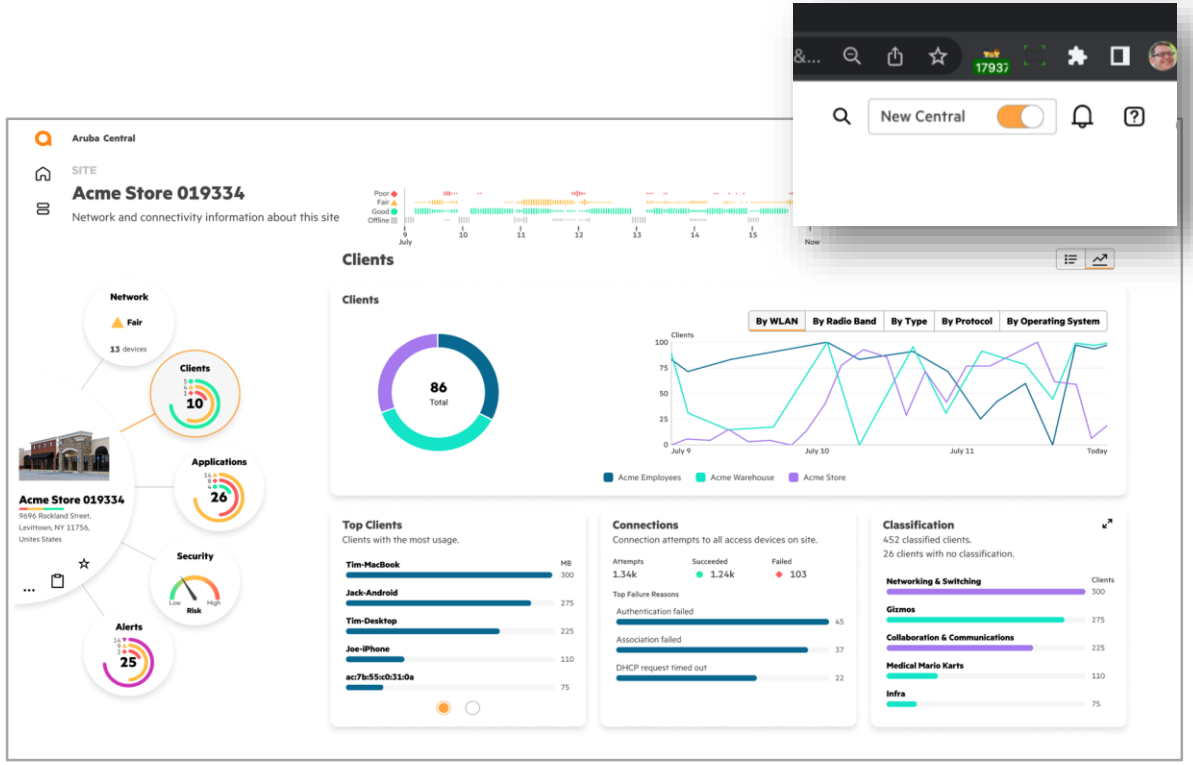
検出した接続デバイスをクリック（例えば、Raspberry Pi）
ポリシー設計に必要なトラフィック内容を可視化



2024年、Next-Generation HPE Aruba Networking Centralへ



現Central



新Central

Next-Generation HPE Aruba Networking Centralのご紹介

主な新機能

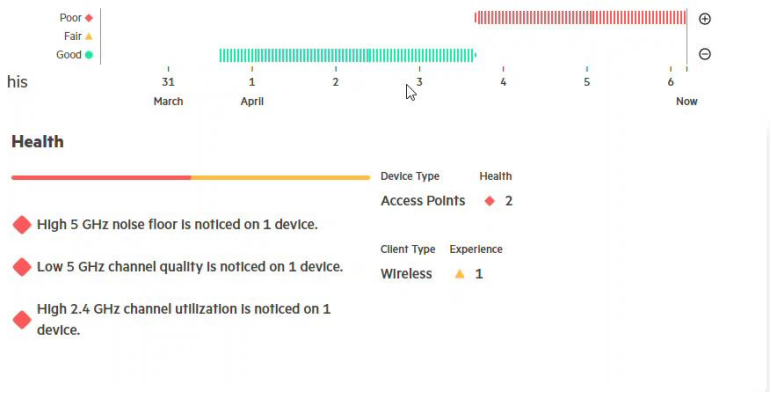
「ソーラーシステム」ビュー

ネットワークナビゲーションの変革

- 複雑なネットワークをより適切に表現する **Entity-centric** なビュー
- 直感的なナビゲーションにより マニュアル作業による見落としの軽減、**問題の早期発見**を可能にする
- ブレンドされた様々な指標により問題の切り分け間違いや追加の確認作業を軽減

業界初の「ネットワーク・タイムトラベル」

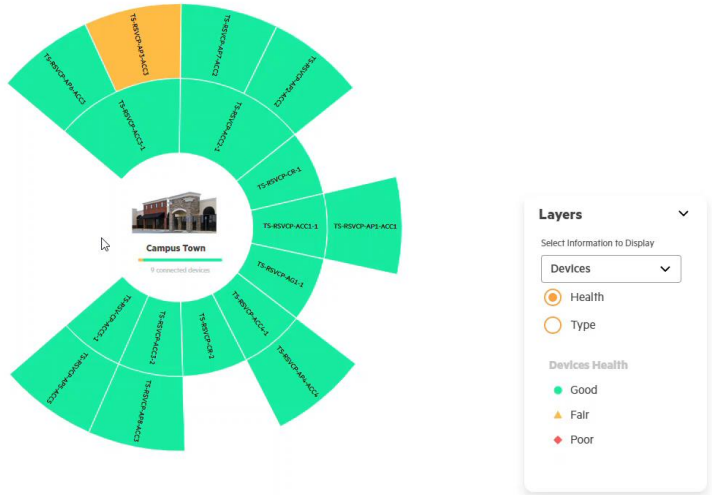
パケットキャプチャを超える機能



- 「**Point in time (特定の時点)**」での全体のスナップショット
- パケットキャプチャによる手動解析を超えるより細かい調査・確認が可能
- **最大7日間、1分単位**で時間を遡ることができます。

「サンバーストトポロジー」ビュー

パワフルでスケーラブルなビジュアライゼーション

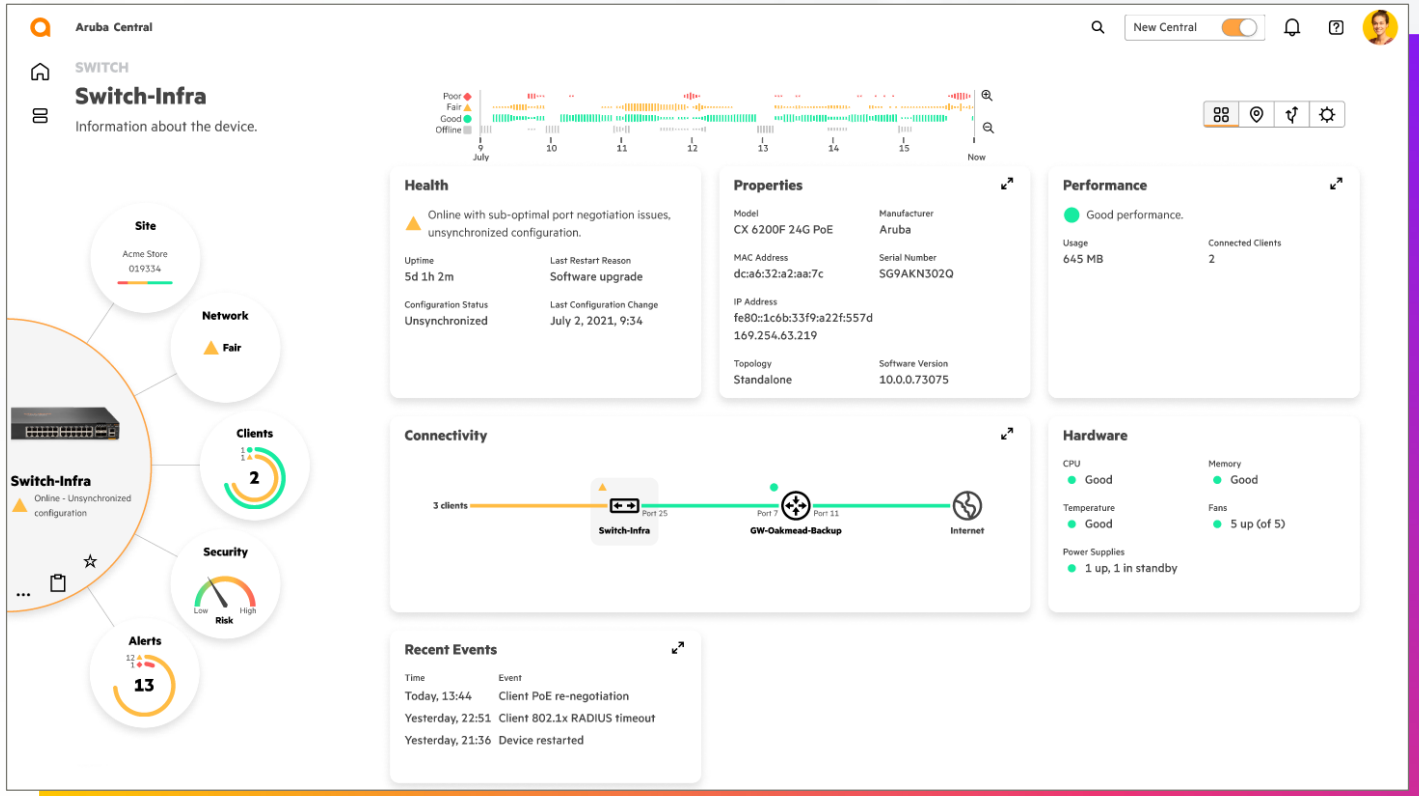


- 物理的/論理的ネットワーク接続を直感的に視覚化
- 従来の一画面でのノード/リンク表示数を大幅に超え、大規模なネットワークの可視化を変革
- コンテキストフィルタと参照ポイントの変更機能

真のネットワーク・イノベーションに向けたコミットメント

Next-Generation Central Cloud Management

AI powered, operator centric experience

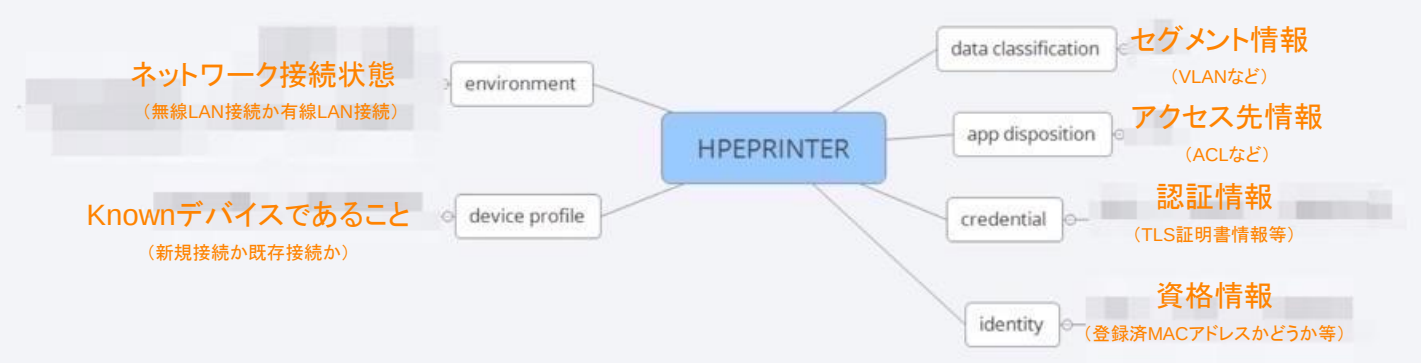


- **相関関係にあるネットワークコンテキストをフルスタックで可視化**
  クライアント、有線、無線、WAN、セキュリティ、アプリケーションをEdge-to-Cloudで可視化
- **現在起きている問題、解決済みの問題を見やすく**
  AI InsightのAlertを大幅強化、サイト階層毎の閾値設定
- **グローバルな多次元AI/MLモデル**
  ピアグループと自動ベースラインを使用したトレーニング
- **インテリジェント・オートメーション**
  ビジネス・インテントベース運用

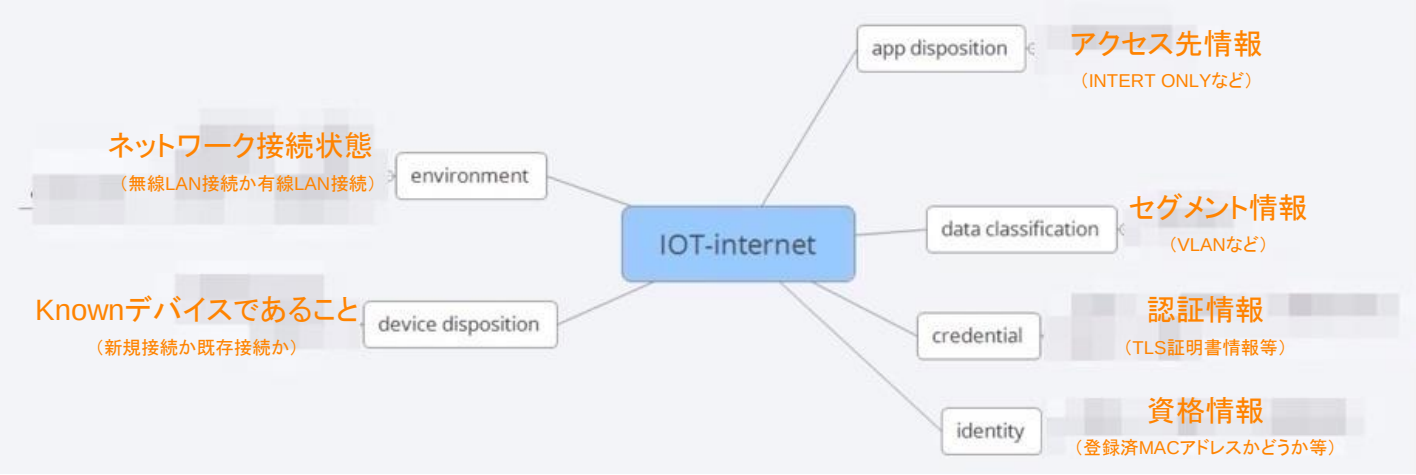
HPE社内のマイクロセグメンテーションポリシー例

社内プリンターとIoT端末用ポリシー

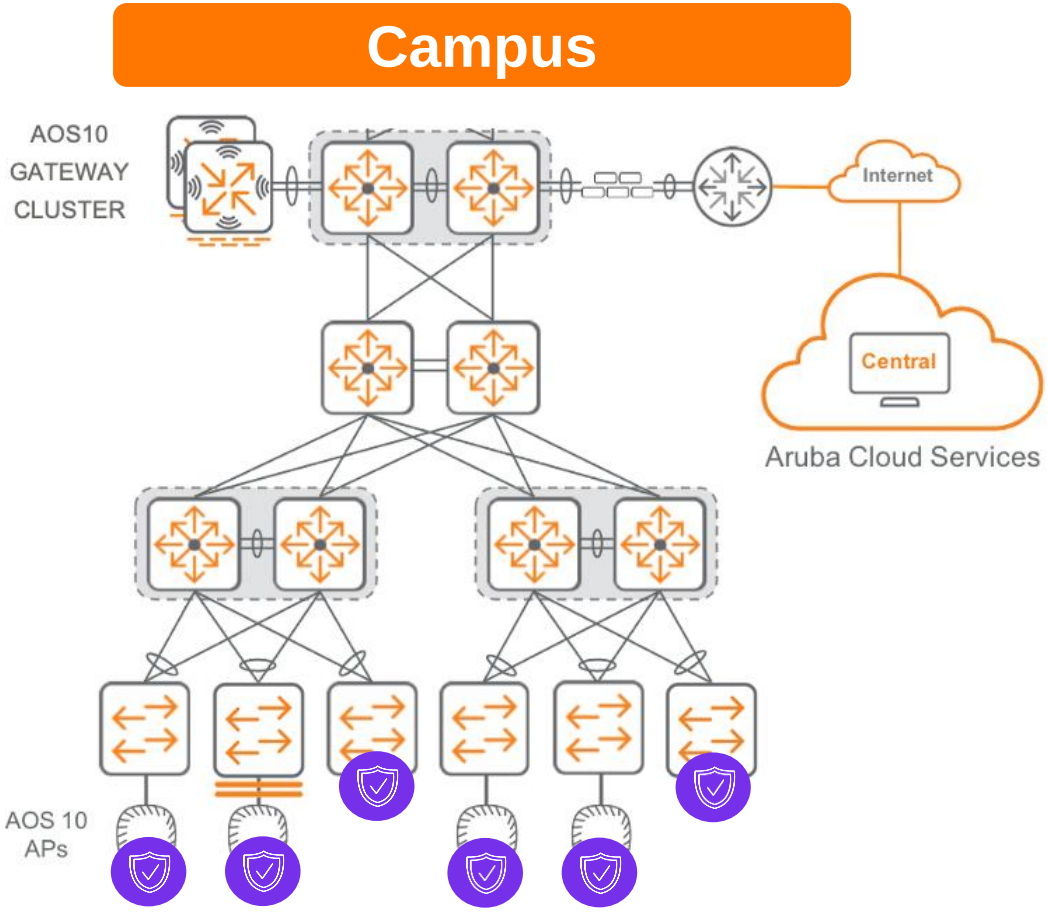
社内プリンター



IoT端末（Internet接続要）



内部からのアタックサーフェス対策
アクセス制御含めたポリシー・エンフォースメントポイント



セキュリティ観点で
Wi-Fiについても少し

Wi-Fi6E移行とWPA3の実装

ポイント

- WPA3により、デフォルトで100%暗号化
  - ✓ アイデンティティ確認の前に、プライバシー優先設計
  - ✓ 暗号化されたウォール・ガーデン、キャプティブ・ポータル
- 無線LAN環境におけるアタックサーフェスの最小化
  - ✓ 保護された管理フレームが必須となり、認証解除攻撃を防止
  - ✓ 辞書攻撃や総当たり攻撃は不可
  - ✓ 中間者攻撃による通信の盗聴・改ざん不可
- 無線LANシステム単体でセキュリティを向上
- 6GHz運用によって、Wi-Fi7に対応するネットワークの将来性

AP-600シリーズ

Coming soon！

Wi Fi 7

最適なWi-Fi6E移行とWPA3の実装方法は？(３つのオプション)

- 既存APの一部で試験的にWPA3とOWE（Enhanced Open） 新規SSIDを有効化
  - ✓ WPA3移行を容易にするため、事前に接続性を確認

- 周波数帯毎（2.4GHz / 5GHz / 6GHz）にSSIDを分ける
  - ✓ 5GHz帯へのフォールバックを許容する
  - ✓ 6GHz対応APの設置間隔次第で、ローミング課題を考慮
  - ✓ Appleデバイスは互換性向上のため、5GHz帯利用に誘導するかもしれない（ポップアップメッセージ）

- 全面的にWi-Fi6E AP導入して、既存SSIDに6GHz帯を追加
  - ✓ WPA3トランジションモードを有効化し、一定期間のフォールバック想定も一案

AP-600シリーズ

Coming soon！

Wi Fi 7

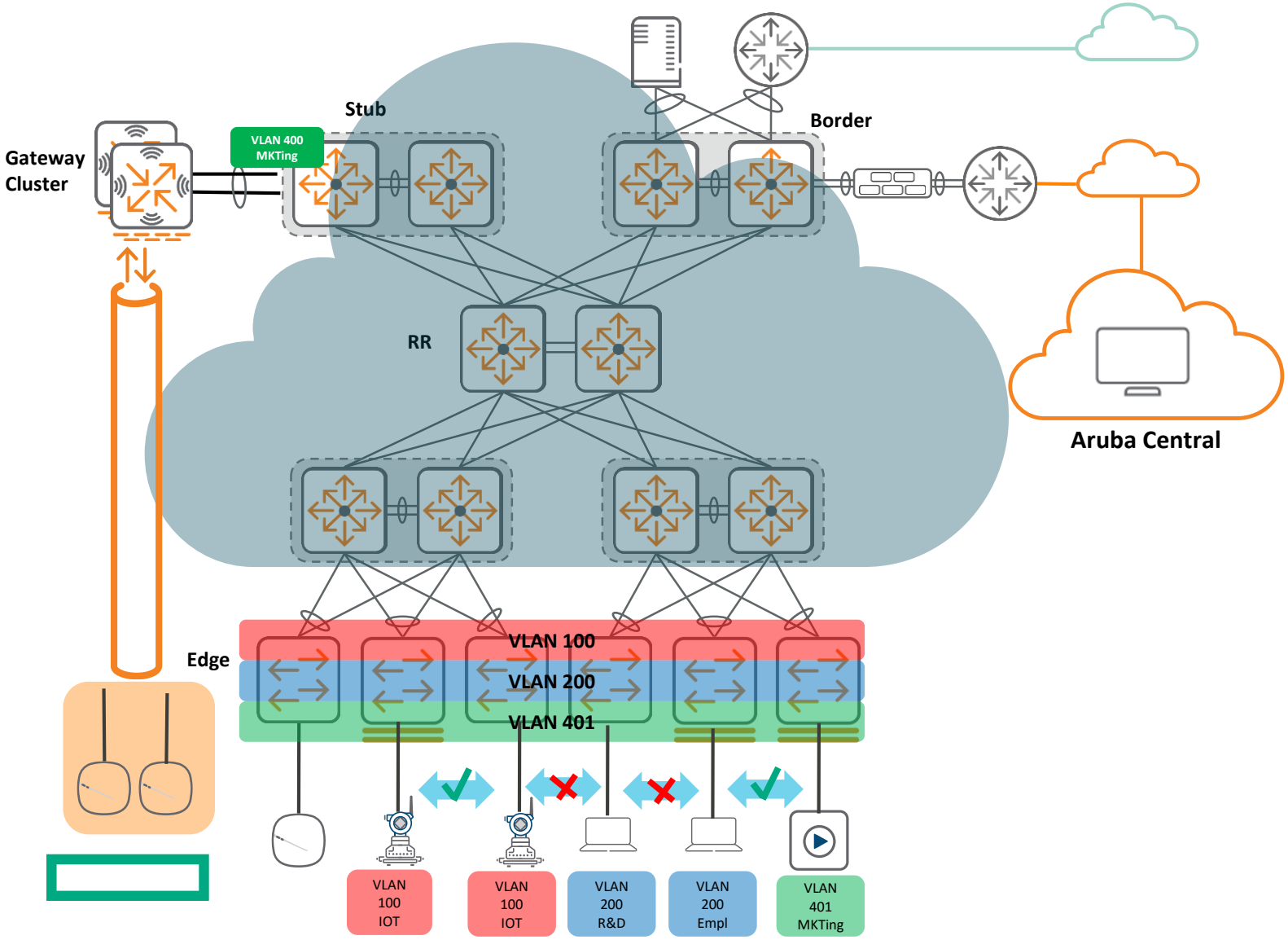
Security-First AI-Powered Networking

ネットワーク領域におけるアタックサーフェス(攻撃対象領域)を低減

今後を見据えたHPE Aruba NetworkingのTOBE像

Aruba Central NetConductor

グローバル規模で自動化されたキャンパスファブリック



NETWORK ORCHESTRATION

ネットワーク全体をウィザード形式の自動化
ワークフローで複雑なファブリック構成の展開を簡素化

ZERO TRUST FABRIC

中央集約型もしくは分散型EVPN-VLANファブリックを
クラウドネイティブなCXスイッチとCentralで構築

GLOBAL POLICY ENFORCEMENT

グローバル規模のポリシー及びマイクロ
セグメンテーションを設計。Role-to-Roleで抽象j化

AI NETWORKING

生成AI、LLMを実装した次世代ネットワーク運用

	Camera	Surveillance Headend	Bldg. Maint.	Smart Building	Doctor	Medical Alpps
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
Bldg. Maint.	✗	✗	✗	✓	✗	✗
Smart Building	✗	✗	✓	✓	✗	✗
Doctor	✗	✗	✗	✗	✗	✓
Medical Apps	✗	✗	✗	✗	✓	✓


AI X CLOUD NATIVE
NETWORKING


THANK YOU

Hewlett Packard Enterprise

SASE構築して終わり?! ゼロトラストセキュリティ運用の複雑性と最適化の勘所

日本ヒューレット・パッカード合同会社
ハイブリッドソリューションズ事業統括
横山博樹

2024年2月20日

企業のインフラに大きな変化の波が

クラウドサービスの利用拡大

- オンプレミスからクラウドへ
- 企業ネットワークの境界が曖昧に

モバイルデバイスの普及

- 外から企業リソースにアクセス
- デバイス接続先セキュリティも重要

IoTデバイスの普及

- ネットワーク接続IoTデバイス増
- 攻撃対象へのリスク大

攻撃手法の巧妙化・洗練化

- 高価値データがオンラインに存在
- 攻撃者の技術力向上・洗練化

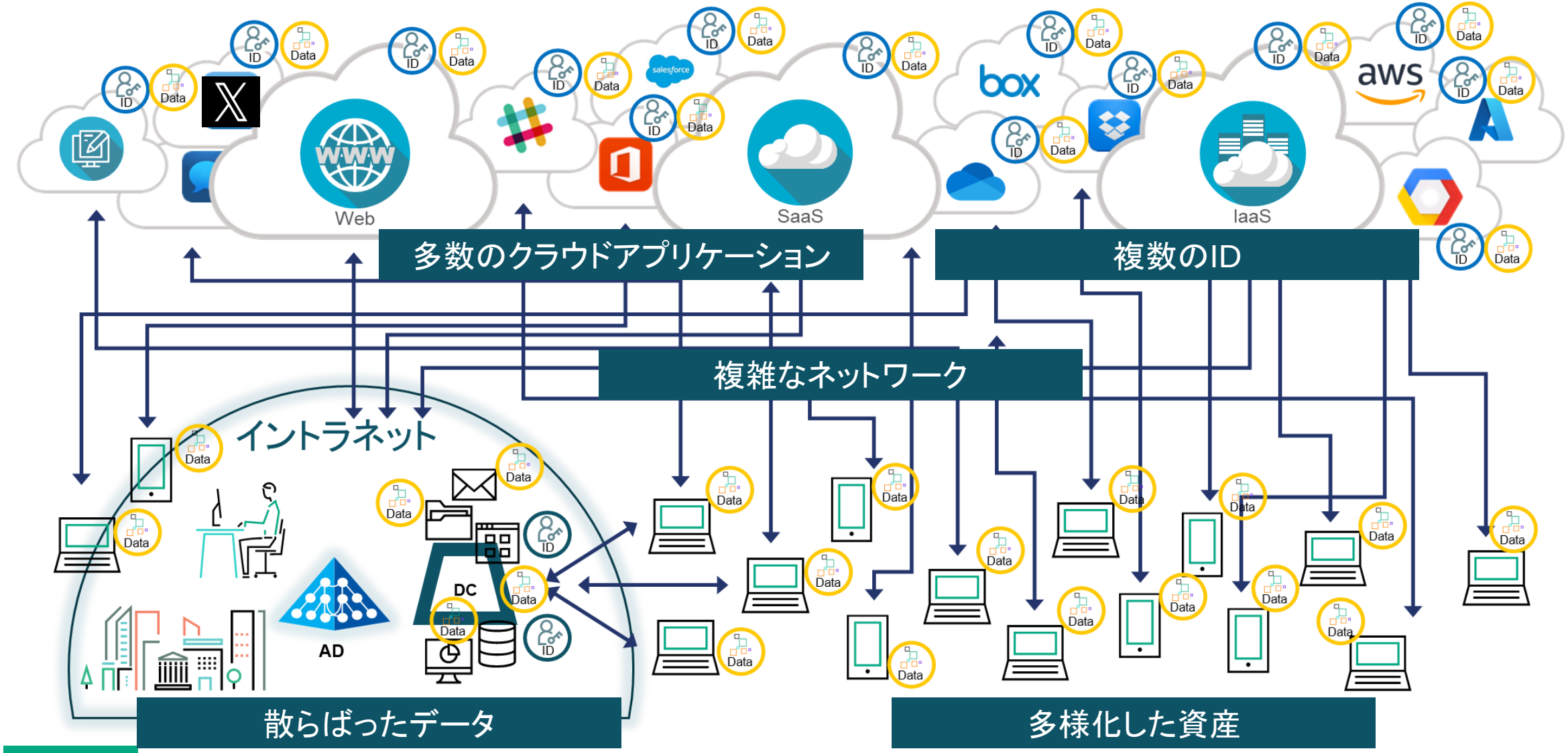
従業員の意図しない行動

- 人的ミスでマルウェア感染も
- 故意のデータ持ち出しも

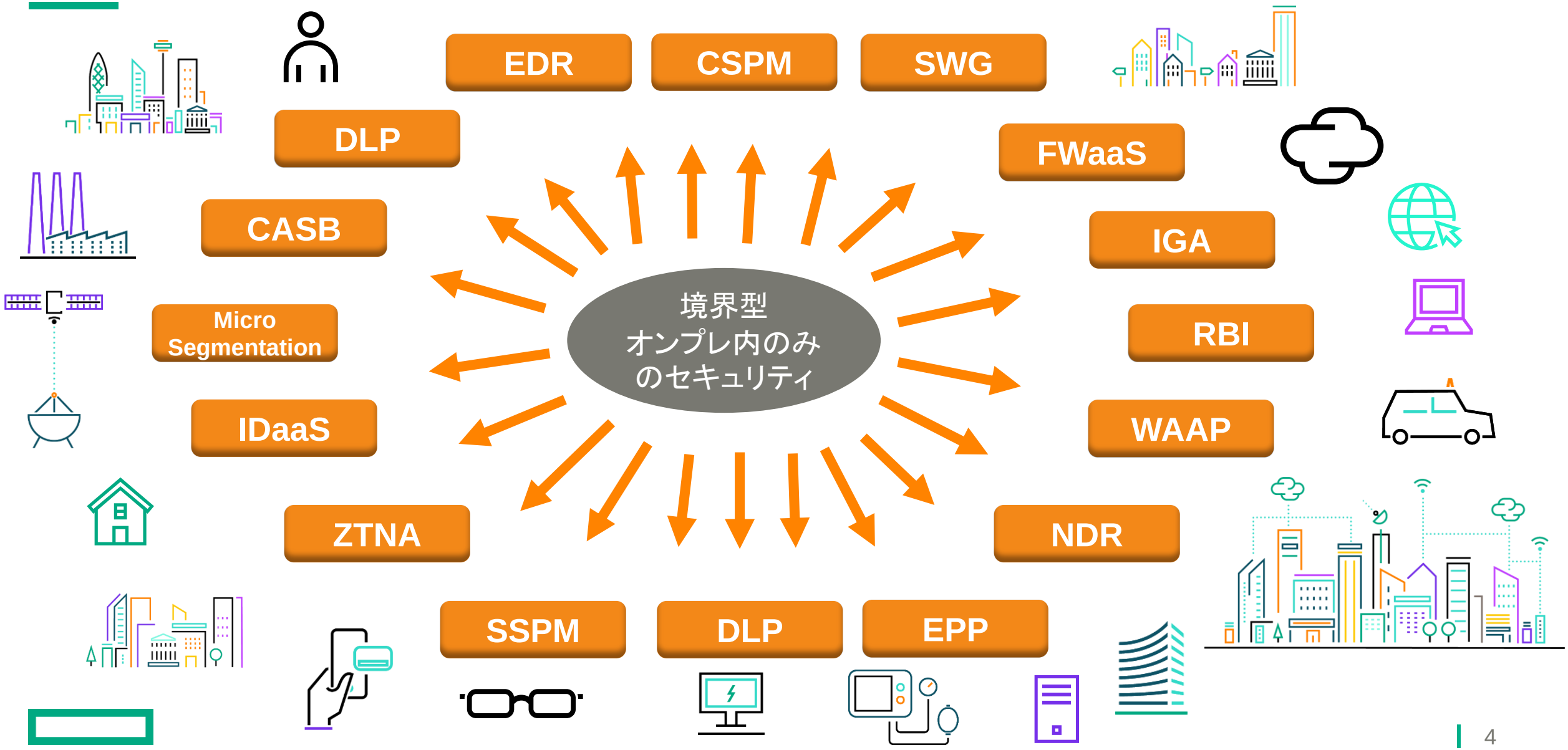
通信経路の複雑化

- 通信経路が複雑化
- 境界の外側からの攻撃が増加

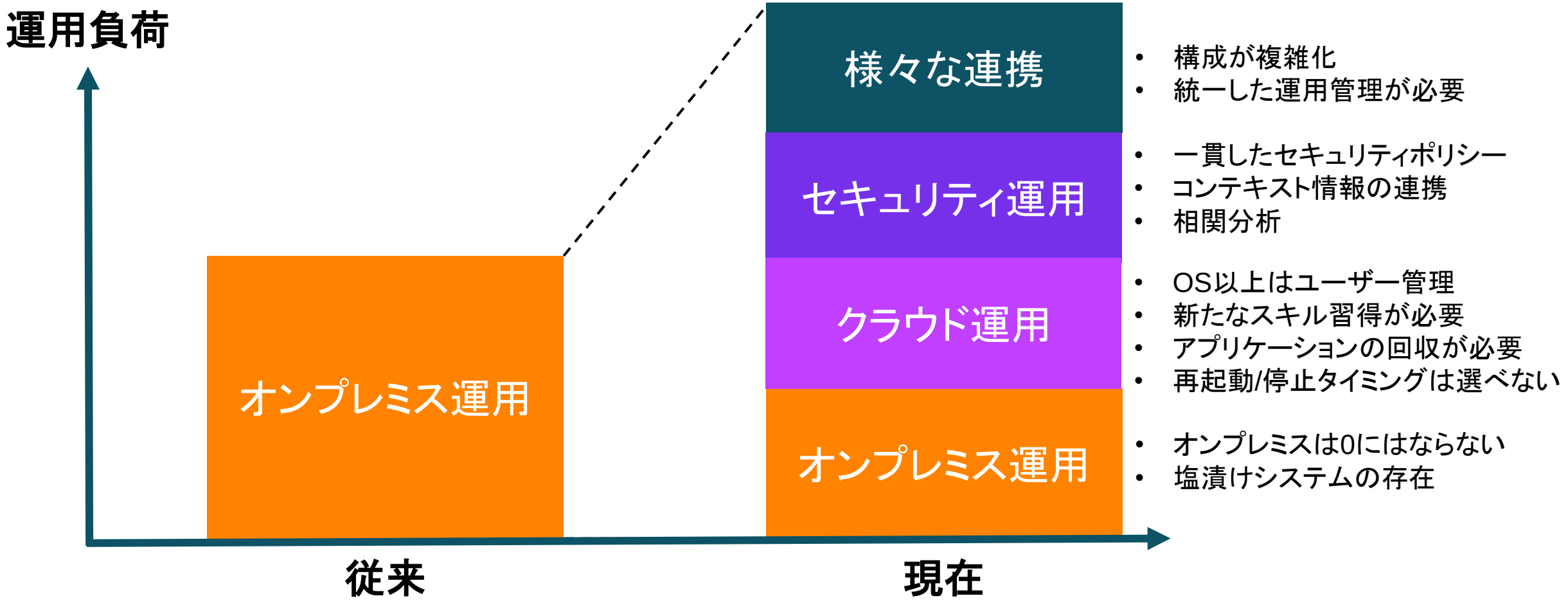
広がる世界による分散化



ゼロトラスト導入によって起こるセキュリティエンフォースメントポイントの分散



しかし分散された環境の運用は一筋縄ではいかない

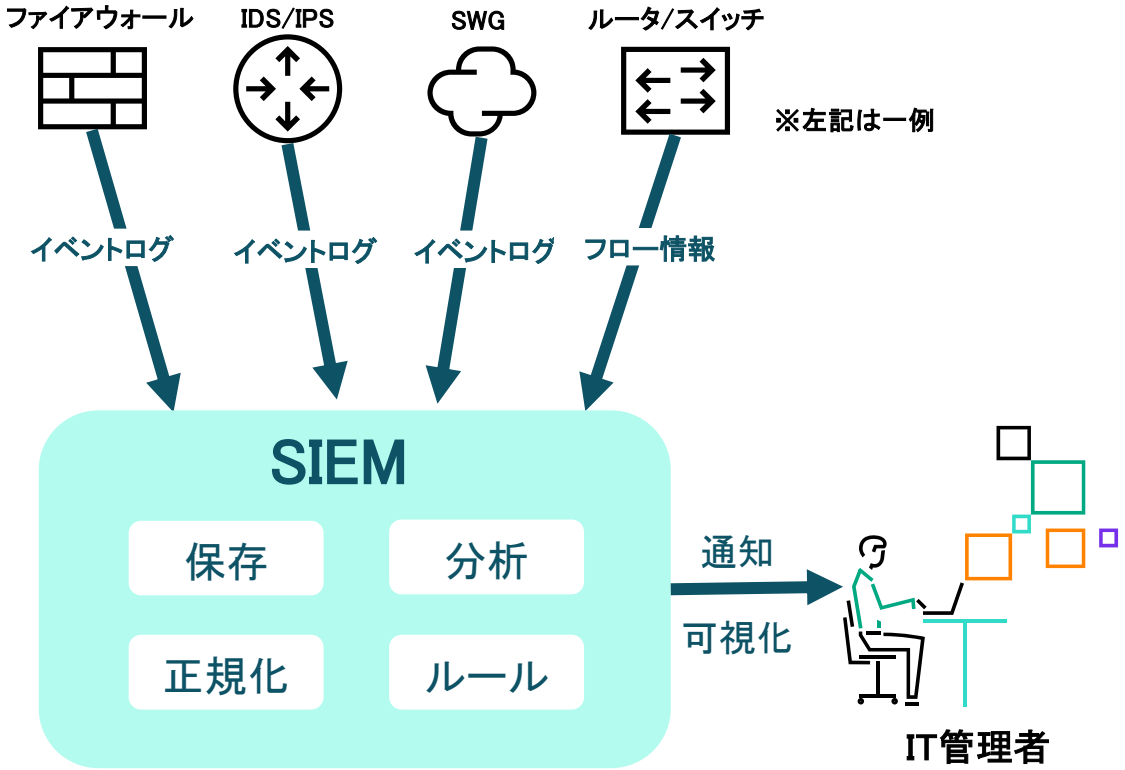


今後も運用環境は動的に広がっていくため、リソース不足問題はより深刻化

ゼロトラストセキュリティの分散に伴うログ運用の課題

ログまみれで、大切なユーザの状況や環境把握ができない

統合的に管理・分析するSIEMはもちろん必要だが…



課題① システム環境の複雑化・多様化

- より広範囲からより多くのデータを収集する必要が出てきた
- 収集対象の範囲が広がることは、運用コストの上昇にもつながる

課題② 膨大なログ

- 管理対象デバイスのセキュリティ／ネットワーク機器、認証サーバなどが生成するログ情報は、1日あたりテラバイトに達することもある

課題③ 工数管理

- 複数のログを相関分析して脅威を早期に検知するためには高度なデータ解析スキルが求められることもあり、管理工数も膨れ上がる

課題④ 「未知の脅威」「内部不正対策」に弱み

- 人的に定義したルールに基づくため、頻繁にルールの更新等のメンテナンスが必要となる上、未知の攻撃手法には対応できない
- 振る舞いの多様化による、統一的な判定基準の難化により、誤検知や見落としが多くなり、適切な予兆検知には結びつかない

運用効率化のために導入したSIEMが運用の手間に

SOCベンダーに依頼しても…

- SOCベンダーだけだと定型化された製品に基づくSOCに絞った運用しか出来ない
- 基本SOCは検知したアラートを報告するまでの作業で、それ以降は運用で対応が必要
- スキャンをかける等のオペレーションも基本運用側で対応が必要
- SOCベンダーは日本語レポートしか出ないが、横断的に見るには英語も必要
- SOCはEDR等エージェントが入っていることが前提であり、エージェントが入っていない未管理端末の管理等、IT資産管理としての運用も残ってしまう

SOCベンダーだけでは解決が難しいケースもある

ゼロトラストセキュリティのエンフォースメントポイント分散における3つの課題

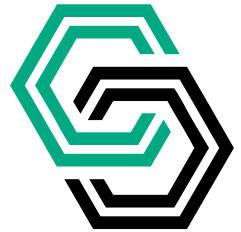
運用工数の増大

- 複数製品の管理や運用により運用工数やコストが肥大化
- セキュリティ製品の棚卸しに苦労する
- 属人化しやすくなる
- 人材不足、スキルセット不足

一貫性の欠如

- 製品ごとに異なるセキュリティポリシー・不整合
- カバーできていないセキュリティ機能の発生
- 複数製品によるセキュリティ機能の重複の発生
- セキュリティイベントの追跡が困難に

複雑性の増加



- 設定・管理がより困難に
- 構成エラー等の脆弱性を生み出す原因に
- 必要な情報がすぐに見つからない
- 攻撃の発見や対応が遅れる

ゼロトラストの運用を最適化するための3つの視点

Right Mix Operation
次世代セキュリティ運用

Human

ヒューマン　必要とされるヒトの介在
コンピューテーション的なアプローチ

Data

網羅的なデータ収集と管理
機械化・自動化

① HPE Managed Services: ハイブリッドクラウド運用支援サービス

OpsRamp
a Hewlett Packard Enterprise company

AIOps

HPE Managed Services

クラウドならではの「責任共有モデル」をベースに HPE の
プロプロフェッショナルがインフラストラクチャを運用管理

お客様は **クラウドネイティブ** などの
アプリケーションサービスに専念できる

Global Capability & Best Practice
世界10ヶ国で提供するITオペレーションセンター
（日本にも設置）

HPE GreenLake Edge-to-Cloud Platform

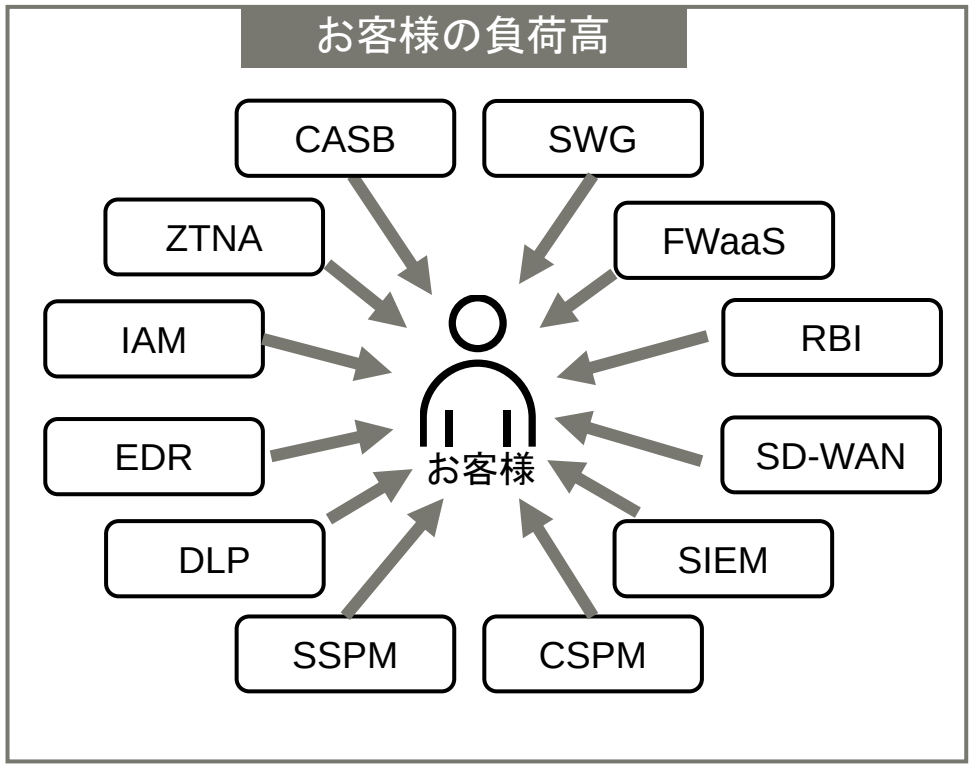
（GUI / API 統合インターフェイス）

セルフサービスポータル / 自動化
/ マーケットプレイス / ハイブリッドクラウドコスト分析

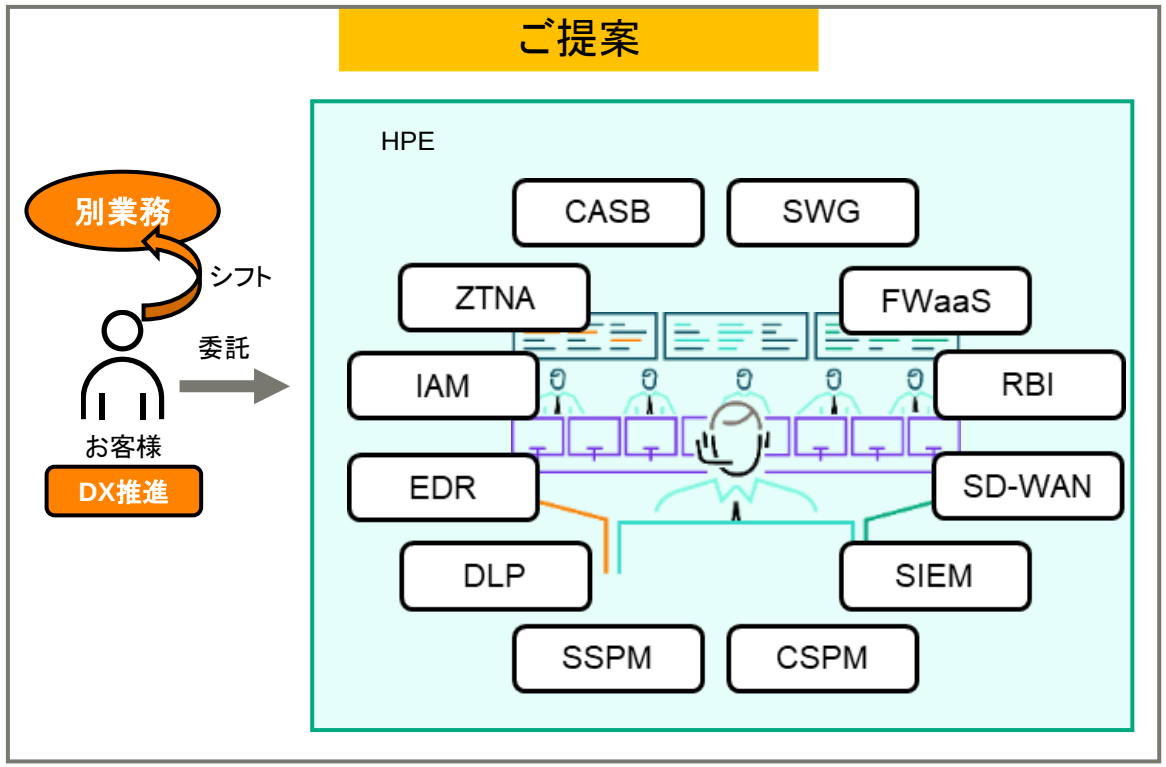
AIOps、自動化を用い、複雑なハイブリッドクラウド環境をHPEが運用管理

① HPE Managed Services: ゼロトラスト運用支援サービス紹介

様々な機能理解の必要性



ゼロトラストの全方位的な運用支援



一部機能だけでなく、ゼロトラストの全方位的な支援でお客様の負荷を低減

① HPE Managed Services: ITOCが提供する運用サービス内容

グローバルで多様なシステム環境のマネジメント実績

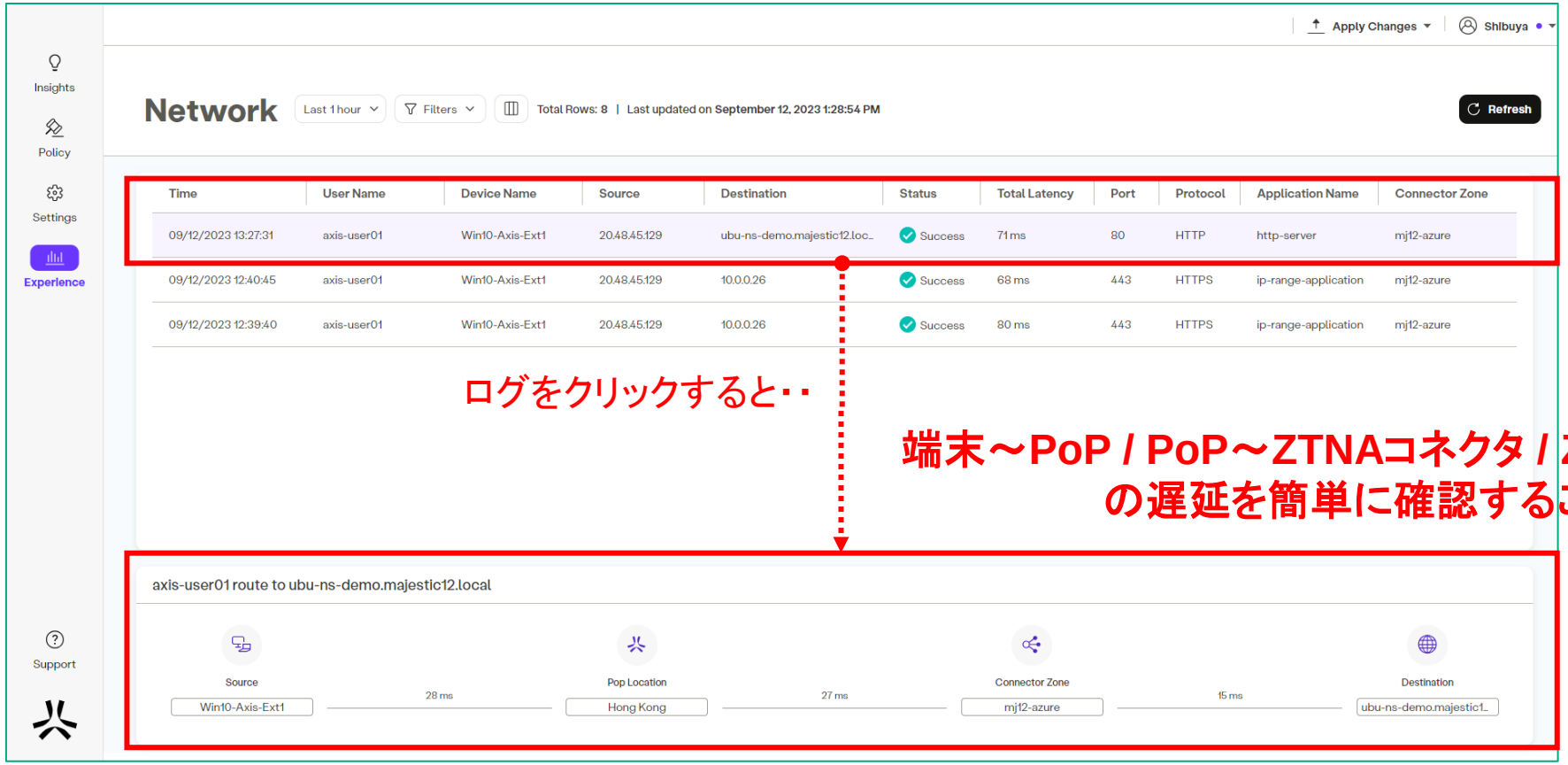
業界アプリケーションプラットフォーム	VDI	SAPおよびSAP HANA	ML/AI	M365	Zero Trust
データ保護	コンテナ	データベース	ビッグデータ	HPC	パブリッククラウド	仮想VM
コンピュート	ハイパーコンバージド	ネットワーキング	ベアメタル	ストレージ	などなど・・・

その他カスタム要件にも柔軟に対応が可能です

多種多様な領域に対応することで、お客様の運用負荷を軽減、IT運用の最適化を実現

② プラットフォームとして、あらゆるデータを収集できる環境づくり

HPE Aruba Networking SSE: DEM機能でユーザ状況を把握し、1つの指標として扱うことも重要



ユーザエクスペリエンスをEnd to Endで可視化し、障害の前兆を迅速に把握

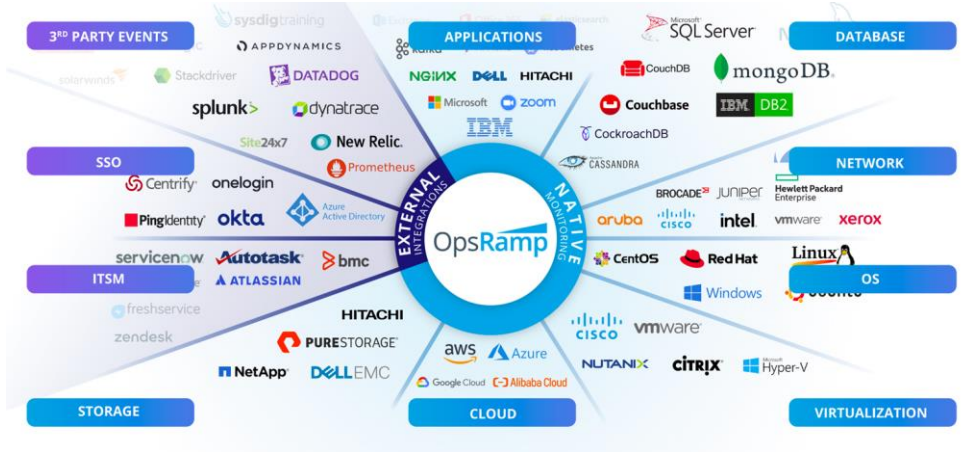
③ HPEのポートフォリオにAIOpsのリーディングベンダーがJoin

OpsRamp
a Hewlett Packard Enterprise company

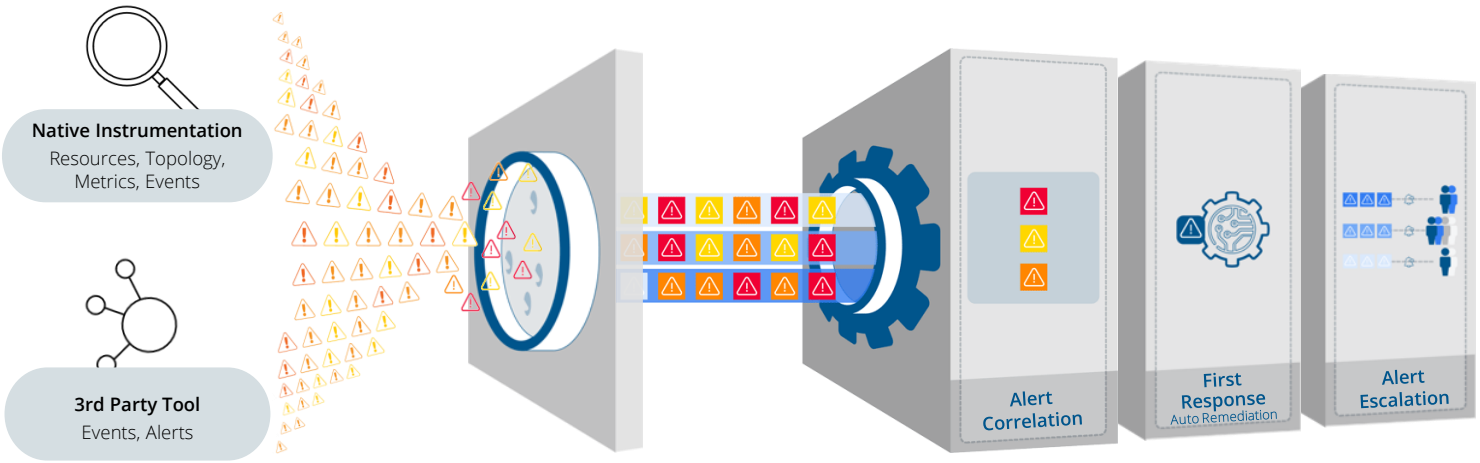
サイロな情報の一元化

イベント＆インシデント管理

自動化による自律型運用管理



ディスカバリーとモニタリング



アラート相関による
ノイズ削減

インテリジェント
オートメーション

HPE Managed ServiceはOpsRampでの運用を標準搭載

③ OpsRampによるお客様の成果

100%

自動検出とオブザーバビリティの指標によるハイブリッドIT環境全体の可視化

30%

IT運用の効率化
自動化とポリシーベースのテンプレートによる改善

95%

AIOpsを活用したイベント相関によるアラートノイズとアラーム低減

50%

AIOpsを活用したイベント相関によるMTTDとMTTRの短縮

" 新しく改善されたコマンドセンターは、私たちがビジネスに提供できる価値を変えました。”

- Epsilon

③ AIOps機能・運用管理ツール連携

Aruba Central HPE aruba networking

OpsRamp
a Hewlett Packard Enterprise company

Red Hat Ansible Automation Platform

servicenow

HPE Managed Servicesではグローバル100名体制で
ツールの開発、連携、自動化を促進

③ Aruba Central: AIOpsによるトラブルシューティングの改善

信頼性向上のための3つのポイント

問題発生を防止する	問題を早期に解決する	情報を迅速に把握する
AI Insights	**AI Assist**	※ 現在、英語のみに対応 **AI Search**
AIを活用した分析によって 問題が顕在化する前に 推奨される対策や設定を提示	パケット・キャプチャやログを 障害発生時に自動的に取得 障害対応の時間を短縮	自然言語での検索によって 多種多様な情報の中から 必要な情報に迅速にアクセス

パワフルな結果

Faster MTTR

調査対象の顧客のうち、ネットワークやユーザーの問題を**50%以上早く解決**

Fewer Support Tickets

調査対象の顧客のうち、ITトラブルチケットを少なくとも**50%以上削減**

HPE Managed Servicesによるゼロトラストセキュリティ運用事例

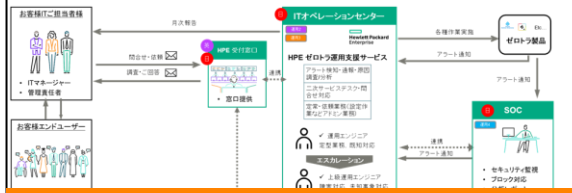
製造業　グローバルゼロトラスト基盤

顧客ビジネス概要＆課題

日々報道されるサイバー攻撃によるセキュリティリスクが高まる中、従来の境界型では限界を感じていた。特に日系企業にとって狙われやすい、サプライチェーンへの攻撃への対策の必要性がある一方、新規開発によるサプライチェーンは日々拡大しており、セキュリティリスクへの対策が急務となった。

◆顧客が抱えていた課題

- セキュリティ対策ツールや環境が各拠点で異なっている
- 現行のやり方では、ガバナンスの統制やセキュリティレベルの底上げに限界がある
- 海外とのコミュニケーションで時間を要しゼロデイ攻撃に対応出来ない
- 海外拠点における脆弱性に特に不安である
- セキュリティ対応とともにコミュニケーション基盤として連携が可能な基盤の導入が必要



顧客のチャレンジ

- ゼロトラストネットワークの考えを取り入れた、クラウドセキュリティを活用した海外ITインフラのセキュア化
- 人材不足の中での海外グループ拠点含めた新たなテクノロジー基盤の導入

HPE運用範囲

- 製品イベントの監視や各種製品の問い合わせ対応・維持管理を実施
- セキュリティログを常時監視・相関分析による予兆検知やリアルタイムのインシデント対応を実施
- 上記サービスを提供するための日本語・英語受付窓口機能の提供

Prisma Access　AzureAD　Intune　Exchange Online　Teams　SharePoint Online　OneDrive　Ivanti

ビジネスベネフィット

- 日本国内本社による海外グループ拠点内ITインフラセキュリティの一括管理
- M&A等新たな拠点追加時の迅速な展開可能な基盤の獲得

保険業　グローバルセキュリティ基盤

お客様のビジネスニーズとITの課題、背景

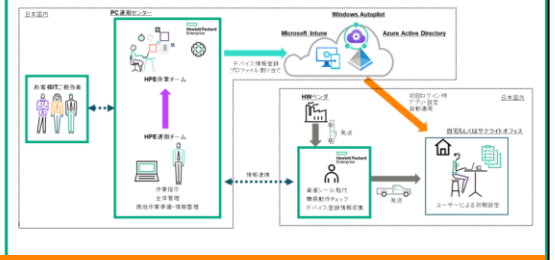
セキュリティ強化施策とし、海外現地オンプレミス機器のクラウド化とクラウドサービスによる端末管理の実現が急務

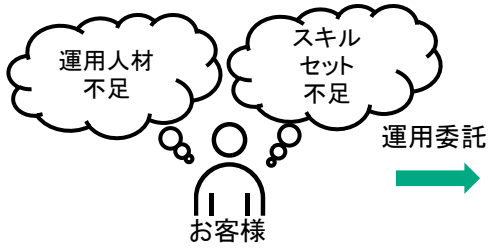
サービスサマリーとHPE訴求ポイント

- 日本から海外拠点への訪問はせずにリモートでの情報連携のみでのゼロタッチキッティング展開&運用の実現
- 納期問題など発生する様々な課題に対する、多言語での現地とのやり取りと課題解決
- 構築と運用チームが密接に連携したワンストップ体制
- 海外におけるPC・NW機器調達から配布作業まで、日本国内での契約と集中管理（お客様自身での現地調達機器も存在）
- デバイスを紛失した場合緊急依頼を受けてアカウントロックをかけてクラウド環境への接続させない管理の実現

ビジネスベネフィット

HPE提供運用ソリューション全体図





最新テクノロジーに追従する
エンジニアスキルセット

グローバル・国内問わず
多拠点での全体最適化

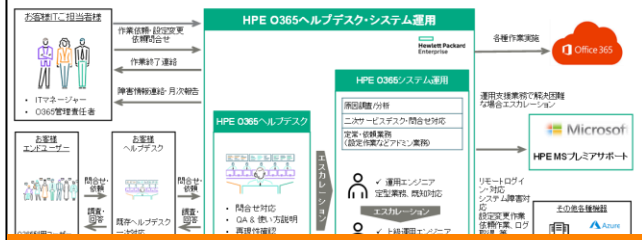
Hewlett Packard Enterprise

お客様は運用開始後、新たなDX化を推進

製造業　グローバルコミュニケーション基盤

お客様のビジネスニーズとITの課題、背景

ITプラットフォームが統合されていないグローバル組織間のコミュニケーション、ドキュメント共有、会議、チームワークに関する非常に非効率的な作業シーンの改善を目的に、プラットフォームのグローバル共通化を検討。M365環境の知見を持ちグローバル視点で支援が可能な運用チームの必要性。



HPEのソリューション

- O365利用者向けグローバルヘルプデスク(日本語・英語・中国語)の提供とO365システム運用の提供。
- ファーストステップとして日本本社10,000人に対する運用支援体制を確立。その後、海外向けに要件・体制拡充が必要となる部分を、グローバルと相互に認識あわせしながら海外向け運用体制への拡張。
- Exchange Online、Teams、Intune、OneDrive等各種Microsoftソリューションにプルーフポイント等関連システムまで包括的にサポート。
- 構築と運用チームが密接に連携しあうことで、構築チームによる段階的な拡張リリースに合わせ、運用も段階的に組込み拡張を実施。
- 要件が未確定な中で半年後のカットオーバーが必達であり、デリバリーと提案を日々繰り返しながら運用カットオーバーを半年で実現。
- HPE MSプレミアサポートによる支援も提供。Microsoft社へのエスカレーションにおいて通常有償でのサポートが必要となる状況下であっても、本サポートにより継続調査回答を実施。お客様環境に特化した複雑で難しい問題にたいしてもワークアラウンドや根本原因の調査を実施し解決策を提供。

ビジネスベネフィット

- ビジネススピードの向上。

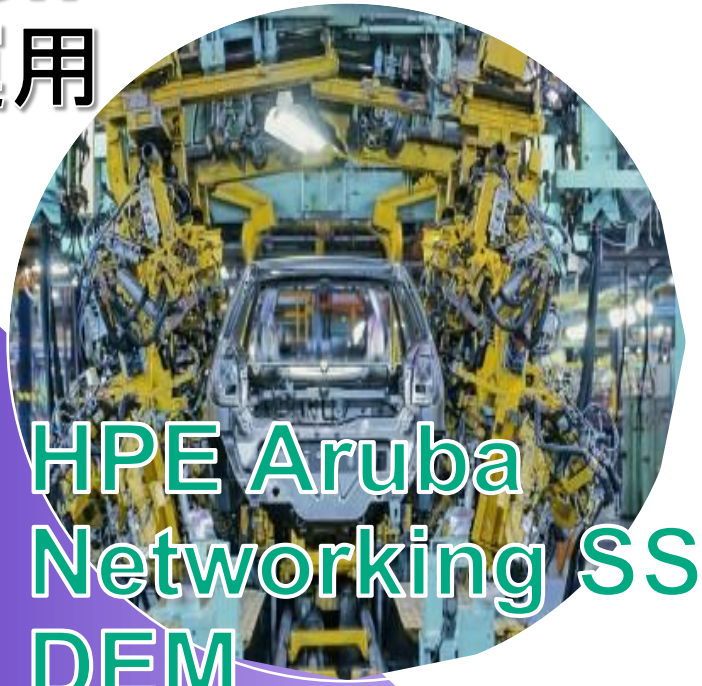
新しいテクノロジーや全体最適が図れる運用者のスキルセット

まとめ:最適なリソース、製品、AIを駆使し、ゼロトラスト環境を適切に運用

Right Mix Operation
次世代セキュリティ運用

HPE Managed Services

OpsRamp
Aruba AIOps



HPE Aruba Networking SSE
DEM

Human

ヒューマン　必要とされるヒトの介在

コンピューテーション的なアプローチ

Data

網羅的なデータ収集と管理

機械化・自動化

THANK YOU

hiroki.yokoyama@hpe.com