

HPE Aruba Networking 最新キャンパスネットワークソリューションの ご紹介

日本ヒューレット・パッカード合同会社
Aruba事業統括本部 技術統括本部

Feb 20, 2024

Arubaのセキュリティ戦略

The screenshot shows a news article on the SDxCentral website. The article title is "HPE Aruba aims for one security policy for all network connections" by Nancy Liu, dated August 16, 2023. The article features a large image of an Aruba building with the text "a Hewlett Packard Enterprise company". A prominent banner at the top of the article reads "Unified SASE Award-winning SSE. Industry-leading SD-WAN. One single solution." with the HPE Aruba Networking logo. The article also includes a "Related Resources" section with links to "SASE vs. SD-WAN. Watch the Video" and "Get the New 2022 Gartner® Magic Quadrant™ for SD-WAN".

<https://www.sdxcentral.com/articles/news/hpe-aruba-aims-for-one-security-policy-for-all-network-connections/2023/08/>

HPE Arubaは全てのネットワーク接続に対して1つのセキュリティポリシーを目指します

ハイブリッド クラウドのネットワークを保護することは、これまで以上に重要になっています。そのため、HPE Aruba は セキュリティに重点を置き、すべての接続方法に **普遍的なセキュリティ ポリシーを提供すること**を目指しています。

「そして、私たちが提供しようとしているのは、**接続方法や移動先を問わず、適用される単一のセキュリティ ポリシーです**」と同氏は付け加えた。

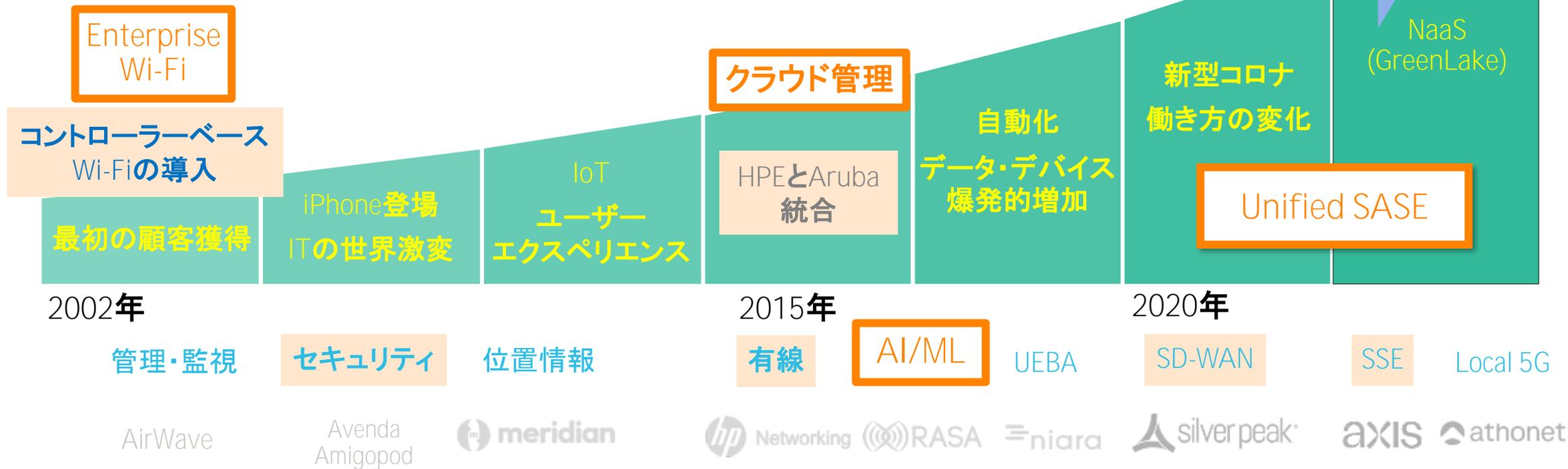
Aruba がこのビジョンを実現する方法の1つは、セキュア アクセス サービス エッジ (SASE) 製品を通じてです。

ベンダー統合のトレンドに乗って、HPE は Axis Security を買収し、**SD-WAN と SSE が単一のテクノロジー スタックに緊密に統合された統合 SASE ソリューションを提供しました**。この買収により、Aruba は「プラグ アンド プレイ」の細分化された SASE アプローチを提供できるようになり、企業顧客はネットワークとセキュリティ スタックを別のベンダーから調達するか、**Aruba 単独から調達するかを選択できるようになります**、と Aruba の最高セキュリティ責任者の Jon Green 氏は SDxCentral との以前のインタビューで述べました。

Arubaはどこから始まって、どこへ向かうのか

People move Network must follow

Mobile First Networking + Security First Networking



HPE Aruba Security First Networking

可視化

Shared
Visibility

ネットワーク全体での
可視化

ポリシー

Global
Policy

ポリシーの一元化

適用範囲

Edge-to-Cloud
Enforcement

全てのネットワークに
適用

運用

AI-Automated
Operations

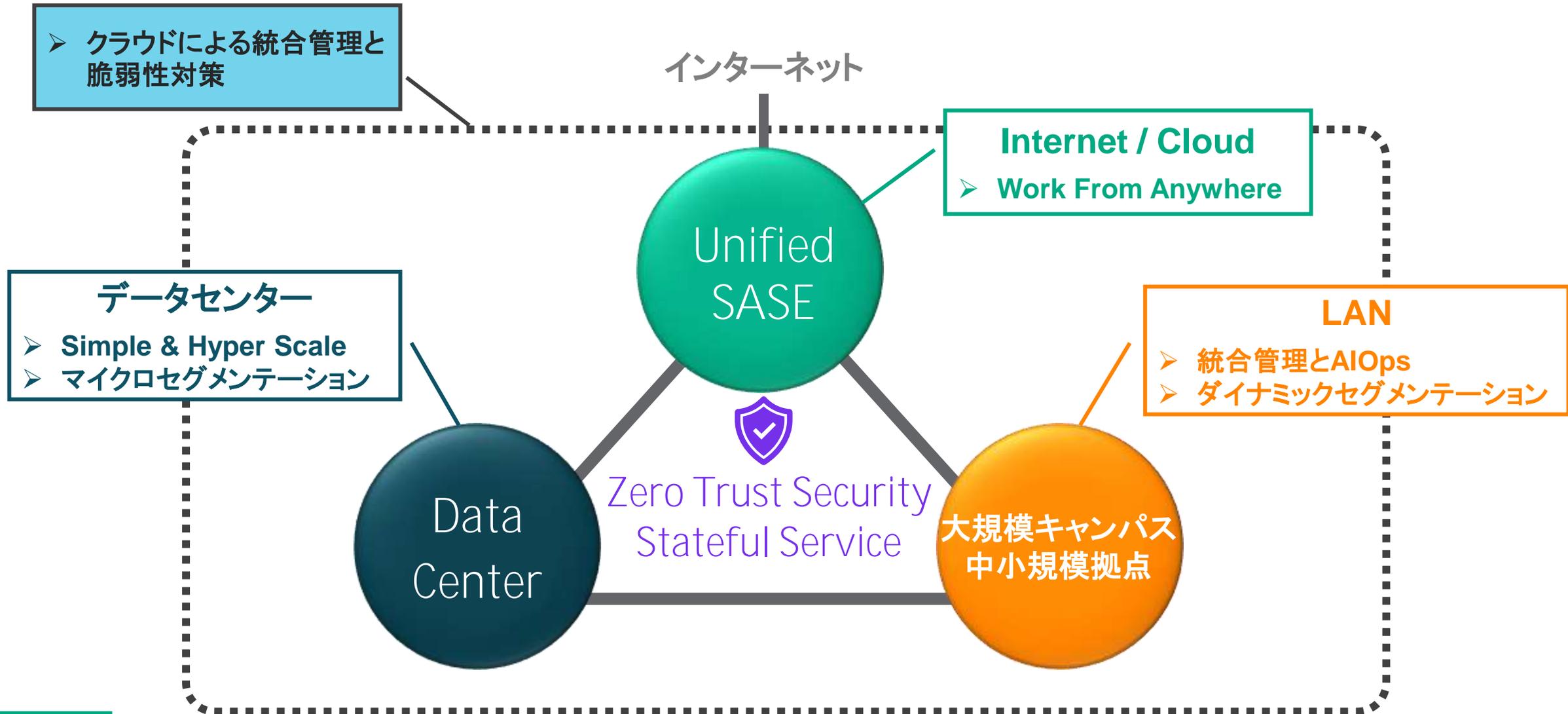
AIops による運用改善

Security First 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 Networking - 全方位ゼロトラスト



キャンパスネットワークにも最適 本当に使えるAI搭載クラウドネットワーク Aruba Central



キャンパスネットワークにおけるポイント

①ユニファイド インフラストラクチャ



シンプルに快適なネットワークを実現したい

②運用・管理性



運用負荷を下げたい
トラブルシューティングにか
かっている時間を減らして
いきたい

③セキュリティ



不正な端末を接続させたく
ない、LAN内のセキュリティを
向上させたい

キャンパスネットワークの課題を解決する Aruba Central AIを搭載したクラウドネットワークオーケストレーター

様々なNWをクラウドから管理



Deployment Flexibility



拡張性



AIによるNW分析・自動化



ゼロトラストセキュリティ



NW全体を一元管理



無線LANアクセスポイント

Wi-Fi 6E
屋内

ブランチオフィス向け

リモートAP
(AOS10 Only)

Wi-Fi 6E

Wi-Fi 6

Wi-Fi 6E

Wi-Fi 6



650 Series



630 Series



610 Series



600H Series



500H Series



605R Series



503R Series

<今後リリース予定>



550 Series



530 Series



510 Series



500 Series



503 Series



518 Series



580 Series



570 Series



560 Series

Wi-Fi 6
屋内

Wi-Fi 6
屋外向け

ゲートウェイ

Campus



7280

(AOS8) 2K AP / 32K Clients
 (AOS10) 8K Devices (AP) / 32K Clients
 100 Gbps, 80 Gbps (Encrypted)



7205

(AOS8) 256 AP / 8K Clients
 (AOS10) 1K Devices (AP) / 8K Clients
 12 Gbps, 5 Gbps (Encrypted)



7030

(AOS8) 64 AP / 4K Clients
 (AOS10) 256 Devices (AP) / 4K Clients
 8 Gbps, 2.6 Gbps (Encrypted)



7010

(AOS8) 32 AP / 2K Clients
 (AOS10) 128 Devices (AP) / 2K Clients
 8 Gbps, 2.6Gbps (Encrypted)

3rd Generation of Controllers



9240

9240 w/ Gold Capacity License
 (AOS8) 2K AP / 32K Clients
 (AOS10) In Development
 40 Gbps, 35 Gbps (Encrypted)

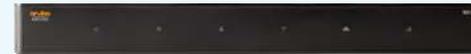
9240 w/ Silver Capacity License
 (AOS8) 1K AP / 24K Clients
 (AOS10) In Development
 30 Gbps, 30 Gbps (Encrypted)

9240 Base Model
 (AOS8) 512 AP / 16K Clients
 (AOS10) 4K Devices (AP) / 32K Clients
 20 Gbps, 20 Gbps (Encrypted)



9114 (AOS10 Only)

(AOS10) 4K Devices (AP) / 10K Clients
 20 Gbps, 20 Gbps (Encrypted)



9012

(AOS8) 32 AP / 2K Clients
 (AOS10) 256 Devices (AP) / 2K Clients
 4 Gbps, 3 Gbps (Encrypted)



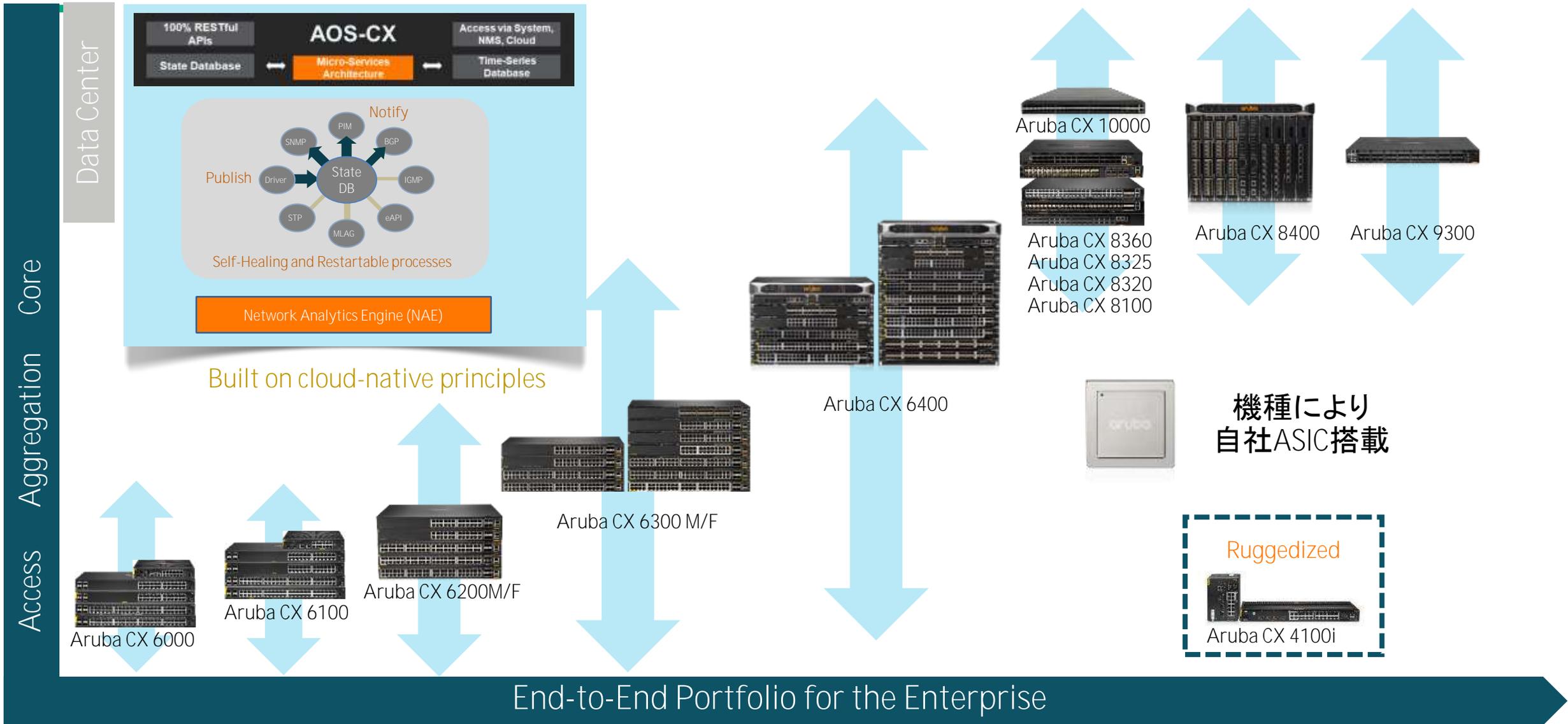
9004 / 9004-LTE

(AOS8) 32 AP / 2K Clients
 *Not applicable to 9004-LTE
 (AOS10) 128 Devices (AP) / 2K Clients
 4 Gbps, 3 Gbps (Encrypted)

4th Generation of Gateways

Aruba CX スイッチ

キャンパスエッジからデータセンターコアまでAruba Centalに対応



Aruba CXスイッチのポイント

コストと拡張性(柔軟性)での評価が高い

	機能面	コスト (製品)	コスト (メーカー保証、保守)	コスト (運用関連)	その他 (実績/シェア)	その他 (拡張性)
C社	○	× (サブスクリプション等で 長く使えば使う程コスト 増)	△	○ (既存運用ベースで 新モデル運用建付)	◎	○ (DNAのハードル高& オンプレ前提)
Aruba	○	◎ (本体安価+サブスクリ プション等も不要)	◎ (リミテッドライフタイム保 証と保守の選択)	△ (新運用建付が必要)	○	◎ (シンプルな実装&クラ ウド型管理への移行も 可能)

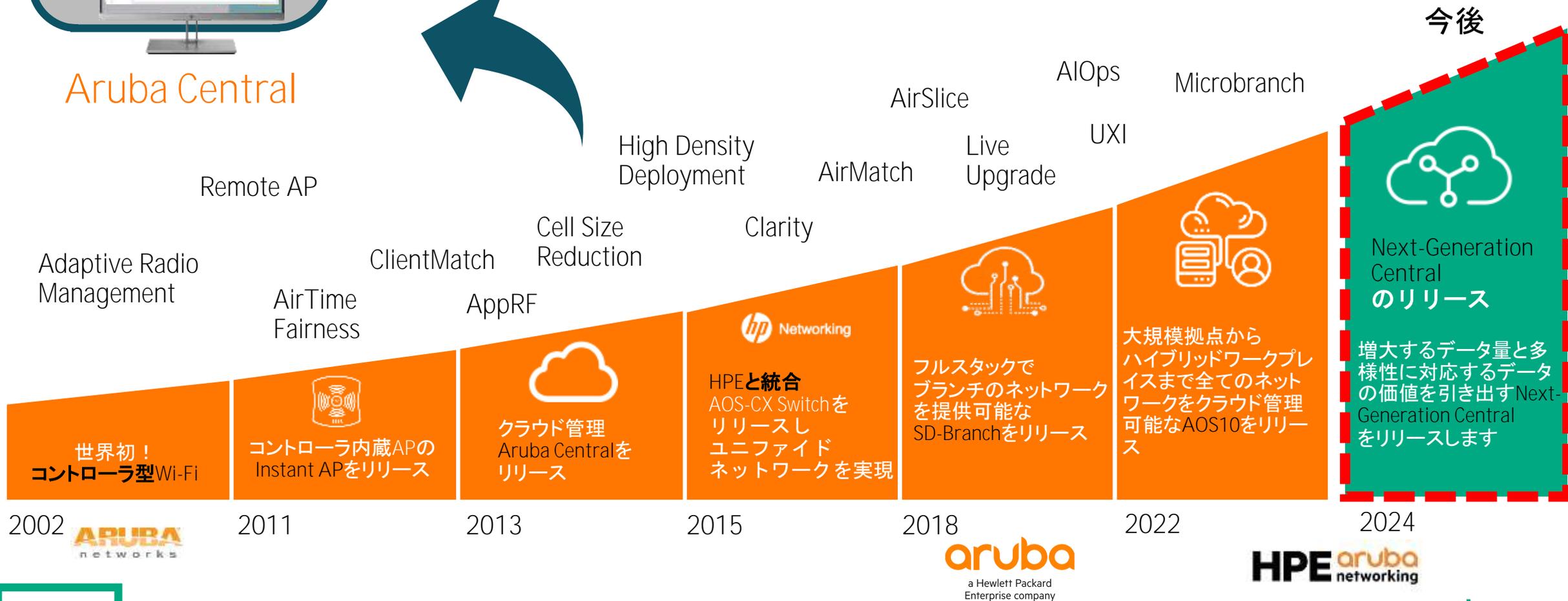
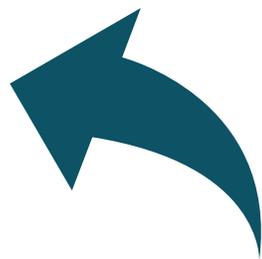
- 機能面 → C社と同等, シングルOSでエッジからデータセンターコアまでカバー
- コスト面(製品価格) → Aruba価格競争力あり、見積もりのBOMが圧倒的に少ない
- コスト面(ライセンス) → 基本的なL2/L3機能は全てライセンスフリー
- メーカー保証、保守 → 殆どの機種がリミテッドライフタイム保証(販売終了から5年間), メーカー保守/パートナー様保守もあり
- コスト面(運用関連) → 新しい管理に移行提案するチャンス
- 管理面 → HW交換無しでクラウド管理(Wi-Fiと一元管理)が実現できる

Aruba Centralの歴史を振り返る



Aruba Central

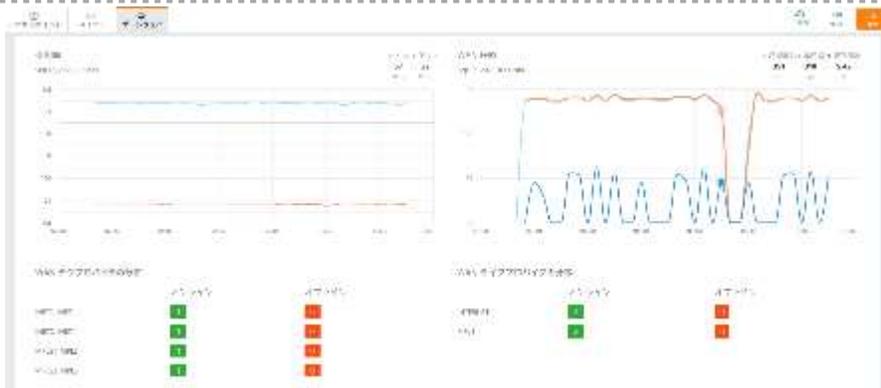
20年以上の経験とテクノロジー



Aruba Central 活用例 ～ネットワークを包括的に管理～

GUI上から一括設定

- 有線・無線・SD-WAN全て設定可能
- 設定はユーザフレンドリーなウィザード形式



ネットワークの可視化

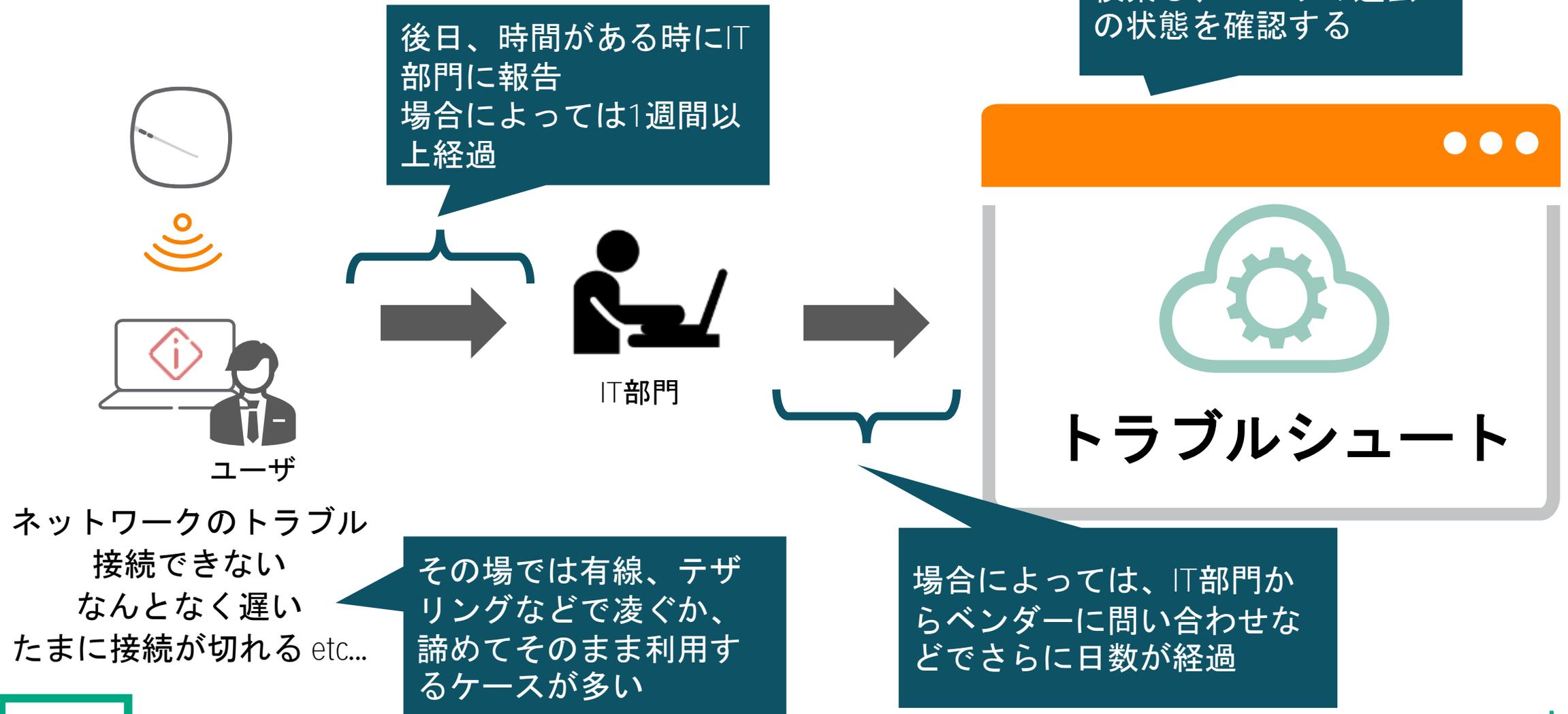
- ユーザ視点の電波品質を提示
- LAN、WANの通信状況を可視化
- クライアント・拠点毎の使用アプリケーションを可視化

問題箇所の調査

- AIで問題箇所と解決方法を提示
- 様々なイベントの発生をメールやSlackに送信
- 定期レポートを作成し、社内報告に使用



トラブルシューティングのよくあるステップ



2002年からの多くのユーザ様での経験

“圧倒的に信頼性の高い”

AIと自動化

真に信頼できる分析



2.5M+
管理デバイス

230M+
クライアント

110K+
設定種別

30+
業種 (大規模～小規模まで)

AI Opsでトラブルシューティングと問題解決を改善

自動化によりMTTRが短縮、IT効率も向上

POWERFUL FEATURES

AI Search

自然言語検索で、必要な情報への迅速なアクセスとトラブルシューティング

Network Insights

プロアクティブなネットワーク異常検知と最適化

AI Assist

自動化されたAruba TACトラブルチケットの生成

Client Insights

正確なIoTプロファイリングによる容量計画とセキュリティポリシーの推進

Application Insights

自動化されたアプリケーションレベルのパフォーマンス監視

Wi-Fi, Wired, WAN Infrastructure:
設計、構築、トラブルシューティング、最適化

Security:
認証/認可、プロファイル

User:
アプリケーション / 接続性

POWERFUL RESULTS



Faster MTTR



63%

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



38%

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%削減

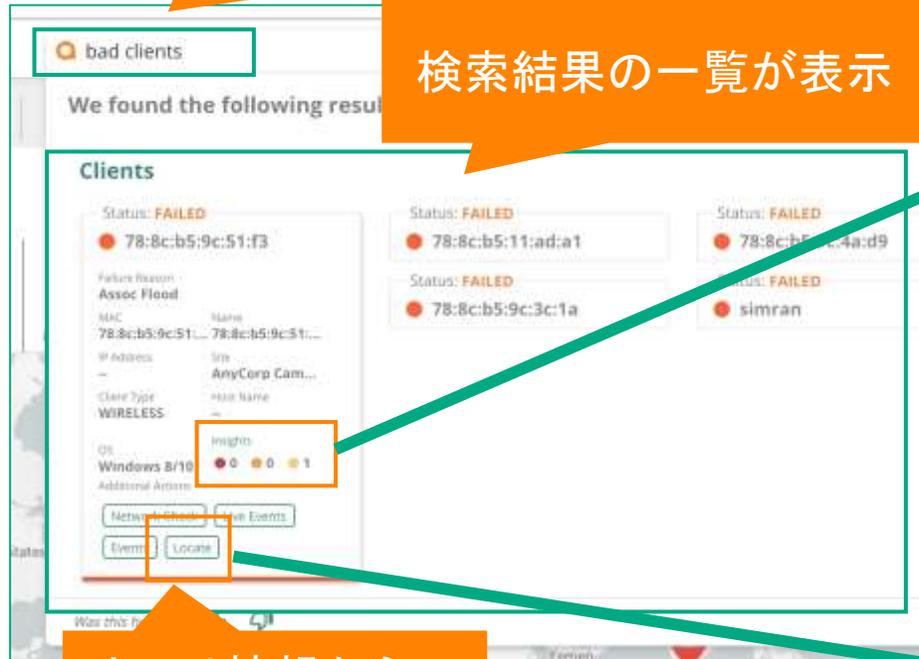
Confidential | Authorized

ArubaのAI Searchは知りたい情報を入力→項目をクリックするだけ

AI Insightのログと推奨事項を表示

知りたい情報を検索ボックスに入力

検索結果の一覧が表示



サマリ情報から
見たい項目を選択



クライアントの位置情報をMAPに表示



AI SearchでユーザーID検索

ユーザIDで検索

williamjones

We found the following results:

Clients

Name: williamjones@arub...
williamjones@arub...

MAC	IP Address
b4:4b:d6:23:a...	10.128.49.156
Status	Site
CONNECTED	Any Corp
Client Type	Host Name
WIRELESS	SJC-207

OS
Windows

Additional Actions
Network Check Live Events
Events Locate

すぐに概要を表示

クライアント詳細

データパス

クライアント

ユーザー名	クライアントタイプ	WLAN 割り当て	接続先
williamjones@arub...	Wireless	VLAN	アクセスポイント
AP ID	Any Corp Secure-SC	RADIUS	SSID
クライアントID	認証済み	認証サーバー	接続先
クライアント名	Computer	10.07.10.32	接続先
クライアント OS	Windows	Yes	接続先
クライアント ID	Aug 21, 2023, 14:32:21	接続先	接続先

ネットワーク

接続先

接続経路や詳細なアクセス情報を確認

インサイト

最大30日前までの傾向を確認できる

理由	推奨事項
クライアントは最適な AP を見つけられません	Enable 802.11n for SSID Any-Corp-Secure-SC [2 more]
見逃される理由	クライアントに最適な WLAN ドライバがあることを確認します [2 more]
認証サーバーが調子	RADIUS サーバーの CPU およびメモリ使用量を確認します [2 more]

ローミング (%) - 最近 1 週間

AIを使った原因と対策

最大30日前までの傾向を確認できる

Network InsightでAIが具体的な解決策まで提示

事象

アクセスポイントは5 GHzの高い使用率の影響を受けました

無線品質

解決策

(100%) 影響を受けたアクセスポイントラジオ、1 アクセスポイントラジオ...

理由

- APには未管理の近隣APが多すぎます
- APには管理対象の近隣APが多すぎます
- ビーコンを低データレートで送信
- SSIDが多すぎます

推奨事項

- 不正APをチェックして排除します。
- ARM設定でラジオの送信出力範囲を縮小します。
- レガシーデバイスを考慮しながらビーコンのデータレートを増加
- 周波数あたりのSSID数を4(最大)に減らします。

ラジオ - 最近1か月 - 比較先



アクセスポイント > AI

1

影響あり

クライアント > AI

2

影響あり

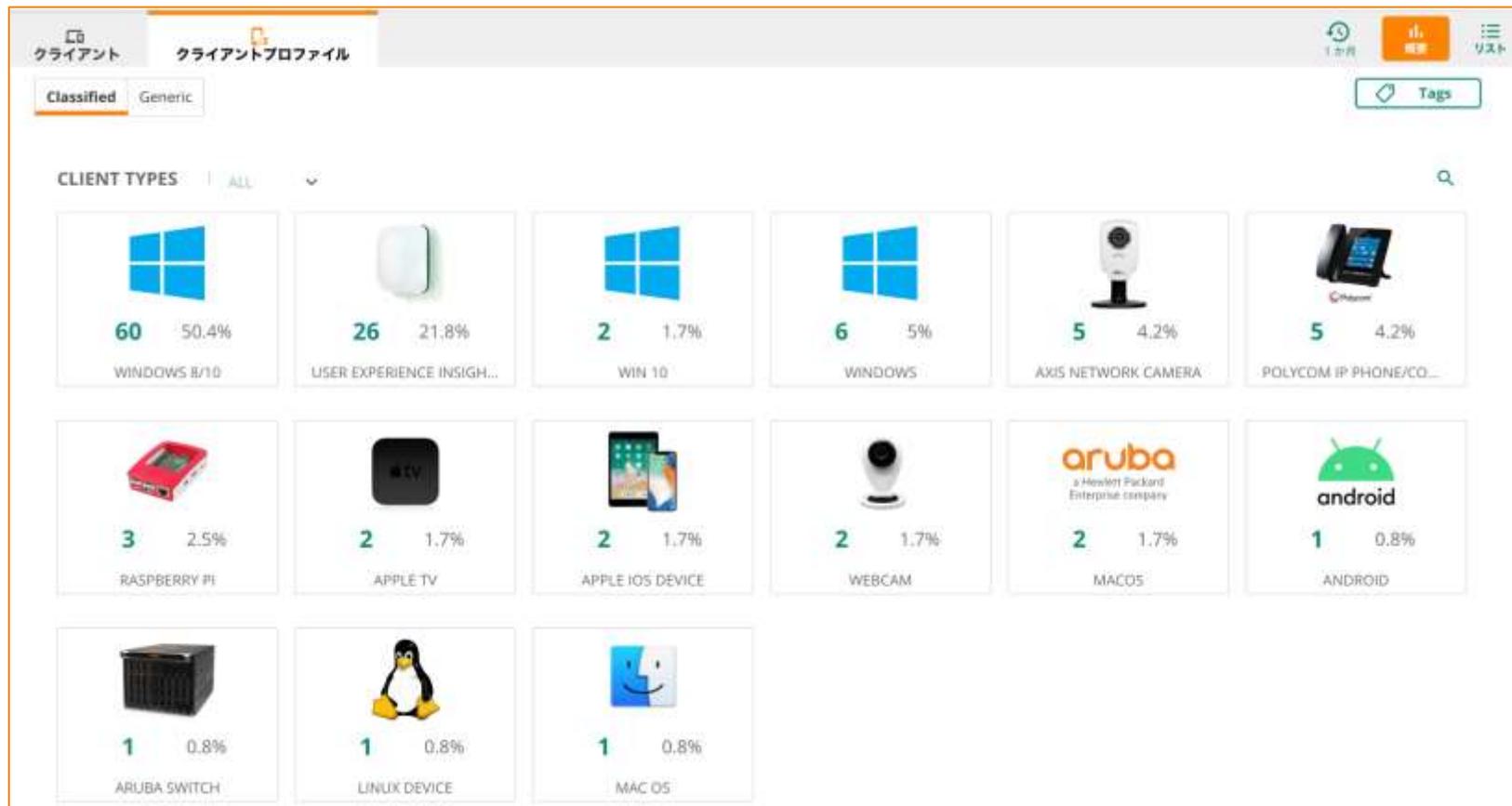
RF情報 > AI

1

影響を受けたチャネル

クラス(似たような他の環境)のベースラインと比べることで、自社の環境が他社と比べた時に異常なのか把握することができる

接続クライアントの情報を自動収集して可視化



クライアントプロフィール機能

- HTTP User Agent, DHCP Fingerprint, MAC OUI を使い接続クライアントを自動的に判別
- 判別した情報を元に通信のアクセス制御も可能

Aruba UXI (User Experience Insight) でネットワークアセスメント

Aruba UXIセンサーが端末としてネットワークに接続し、ネットワークの接続性やアプリケーションへの到達性などをモニタリングしてレポートします。

Aruba UXIセンサー

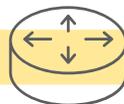


①Wi-Fiに接続



SSIDへ接続できる?
無線環境はどう?

②ネットワークチェック



認証できる?
DHCPやDNSは問題ない?

③アプリへの疎通チェック



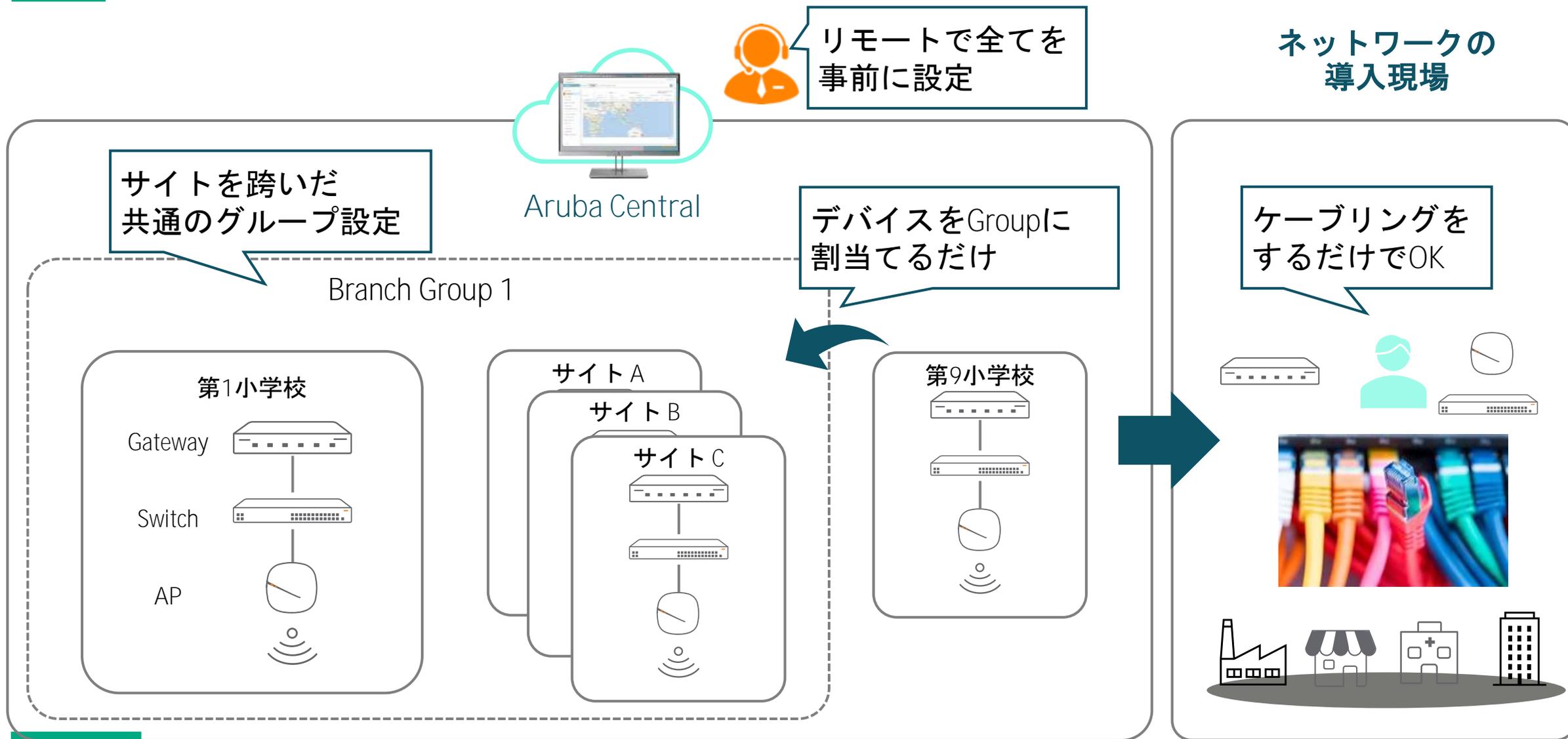
センターや内部サーバーへの疎通は?
クラウドアプリへの疎通は?
スループットは?

クラウドのダッシュボードで見える化
レポートिंग
(Wi-FiまたはLTEで情報をアップロード)

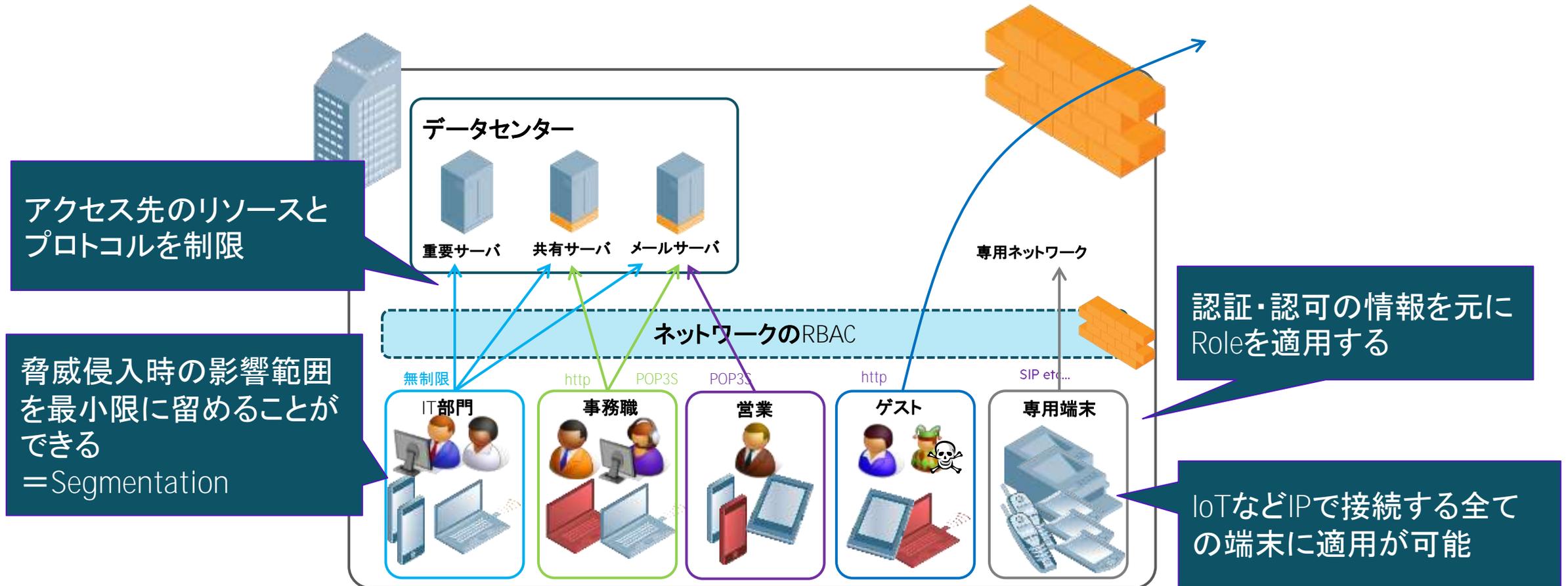


Wi-Fi 6E対応のセンサーが新登場
Aruba User Experience Insight G6E sensor

Aruba CentralのZTP (ゼロタッチプロビジョニング)



[セキュリティ] ネットワークのロールベースアクセス制御



Arubaはゼロトラストに通じるイントラネットセキュリティを昔から提供

Arubaのユーザーロール

User Roleとは

- ポリシーとセキュリティのシンプルな集まり
 - VLAN, QoS, レートリミット, MTU, PoE プライオリティ, STP ポート設定
- Aruba製品に20年以上存在
Aruba AP上に繋がっていれば、User Roleを使っています!

User Roleの適用方法

- 認証と認可に基づく適用(Zero Trust的な考えにも通じる)
- User Roleは端末が認証されると動的に適用される
- 動的だけでなく、静的にも適用可能

利点

- ロール設定に基づいたポリシーを適用
- スイッチではACL, レートリミット, QoSなどをアクセスポートに事前設定不要
- 物理ポートではなく端末に紐付ける

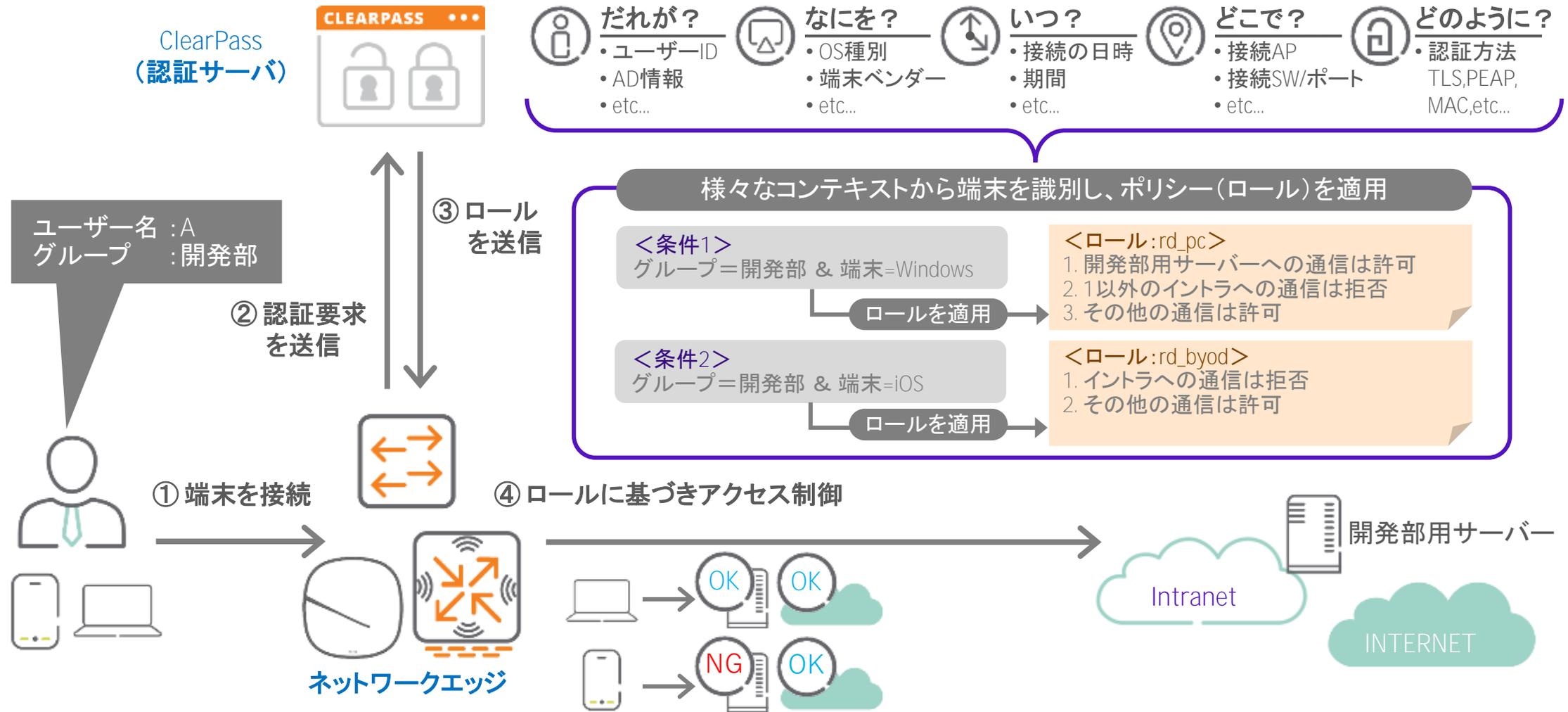


```
aaa authentication port-access dot1x authenticator
radius server-group ClearPass
enable

aaa authentication port-access mac-auth
radius server-group ClearPass
enable

interface 1/1/1-1/1/48
aaa authentication port-access dot1x authenticator
max-eapol-requests 1
max-retries 1
enable
aaa authentication port-access mac-auth
enable
```

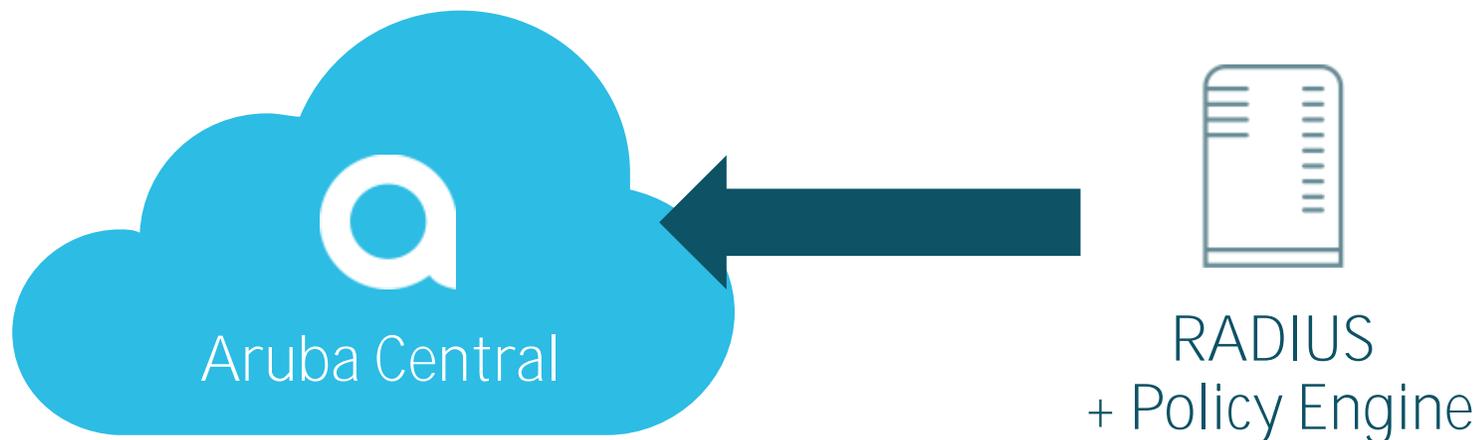
ユーザーロールの適用方法①: Aruba ClearPass



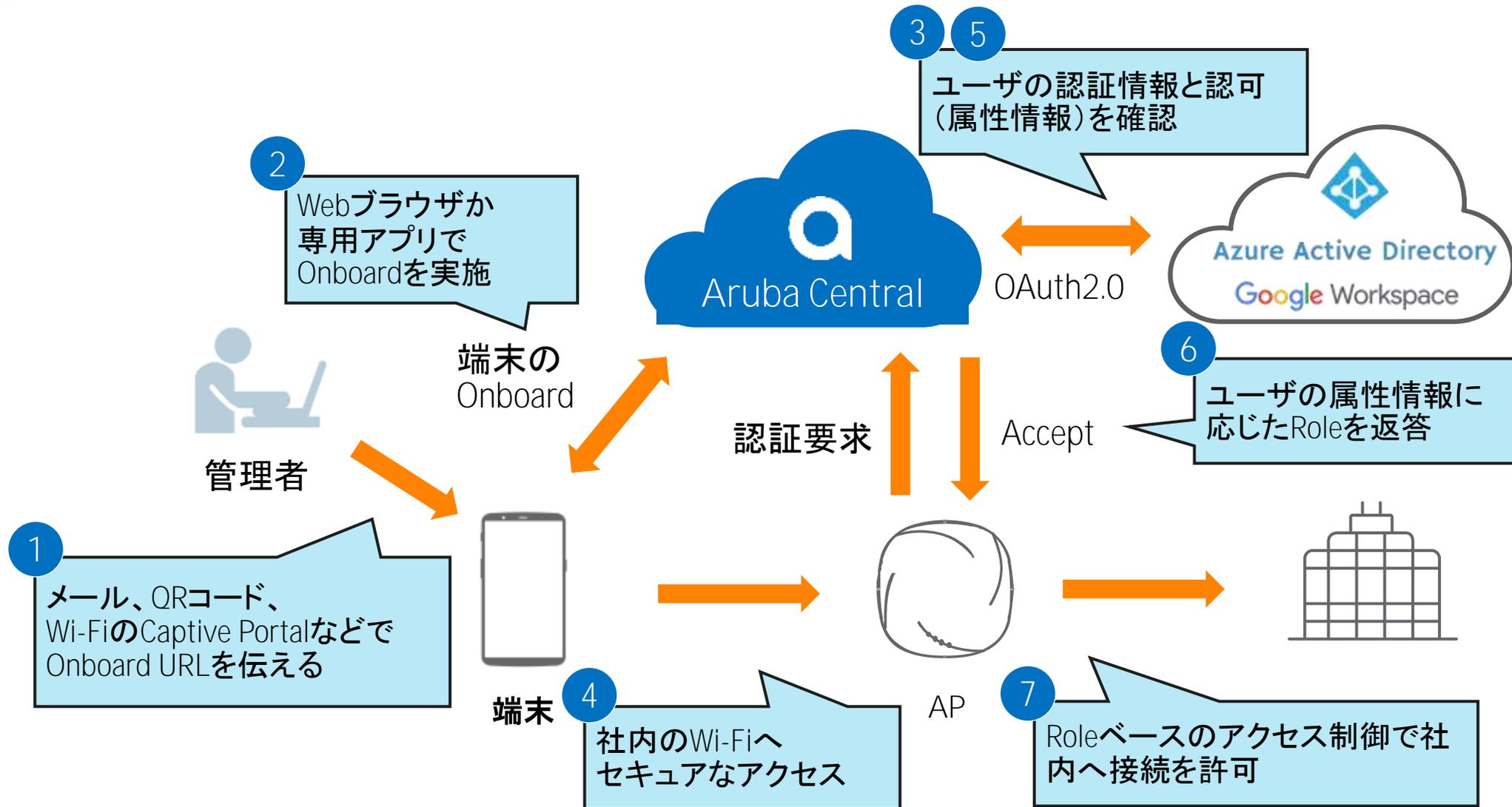
ユーザーロールの適用方法②: Cloud Auth

※Cloud Auth ≠ ClearPass

- ✓ Aruba Central 上で提供するRADIUSサーバ+ポリシーエンジン
- ✓ 802.1X(EAP-TLS)とMAC認証に対応
- ✓ 802.1Xの認証ソースはMS Entra ID(旧Azure AD)とGoogle Workspaceに対応
- ✓ 端末のプロビジョニング (Onboard) 機能も提供 (App or Web)
- ✓ MAC認証はCentralにMACアドレスを登録 (CSVでインポート可, 最大5万MAC)
- ✓ リリース時の機能は全てAP Foundationに含まれる



ユーザーロールの適用方法②: Cloud Auth 802.1Xのフロー



ユーザーロールの適用方法③: Aruba Central NetConductor

Role to Roleでのポリシーを適用



Aruba Central
Role-based Security Policies

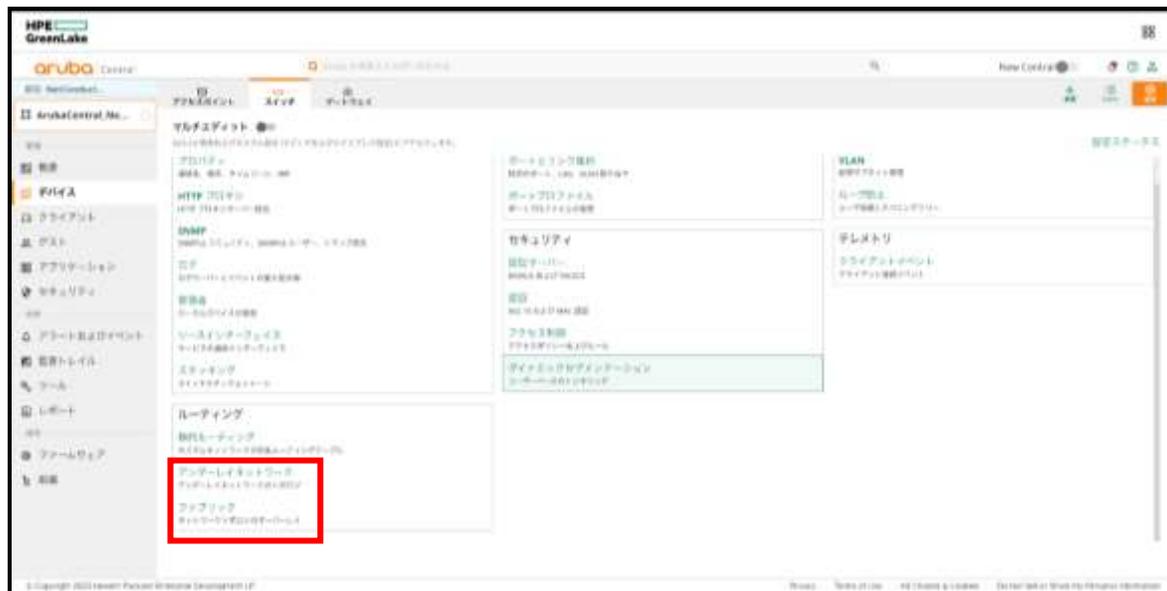
	IP Camera	Printers	Media Sensor	Smart Building	Doctor	HR
IP Camera	✗	✗	✗	✓	✗	✗
Printers	✗	✓	✗	✗	✓	✗
Media Sensor	✗	✗	✗	✓	✗	✗
Smart Building	✗	✗	✓	✓	✗	✗
Doctor	✗	✗	✗	✗	✓	✓
HR	✗	✗	✗	✗	✓	✓

Assign Permissions
Assign permissions for source role CorpPC

DESTINATION ROLES (7)		
Name	Allow Source to Destination	Allow Destination to Source
BYOD Guest	<input type="checkbox"/>	<input type="checkbox"/>
BYOD Laptop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CorpPC (self)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Printer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Cancel Assign

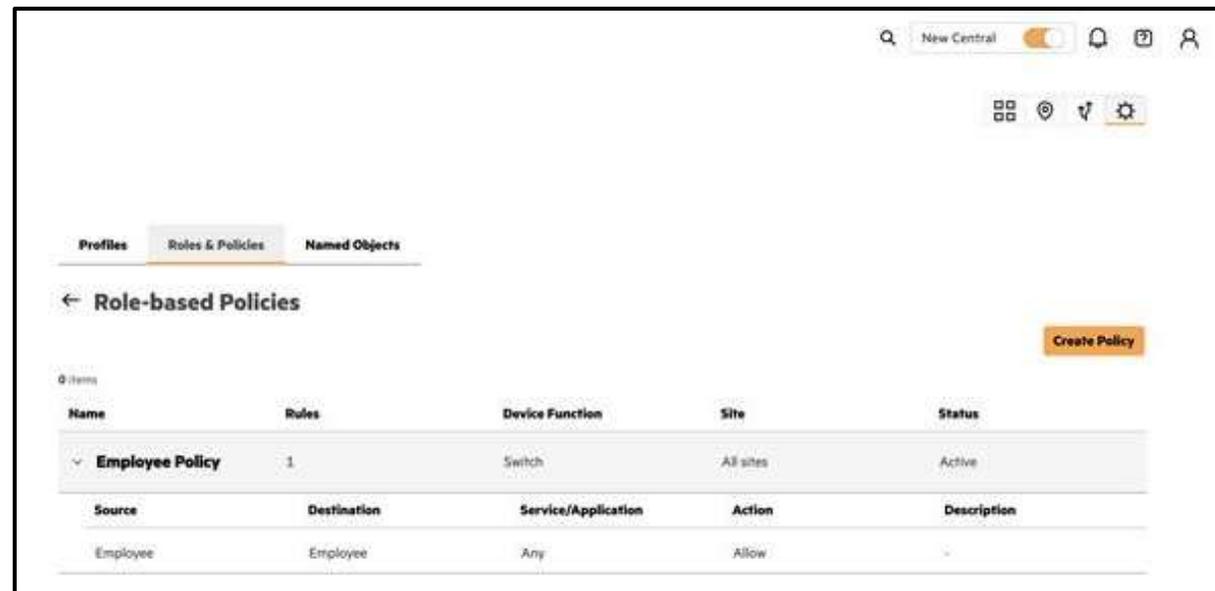
[ご参考] Aruba Central NetConductorでできること



Central NetConductor Fabric Wizard

複雑なCLIを利用しないで、OSPFを利用したアンダーレイ・ネットワークやVXLANのオーバーレイネットワークが構成可能。

3階層のキャンパスネットワークとスパイン-リーフのデータセンターネットワーク構成に対応



大規模なセキュリティポリシーの適用

Global Policy Managerを利用して、様々なデバイスのRoleとPolicyによるGBPの定義が可能

通信制御で利用していたACLなどの利用が不要

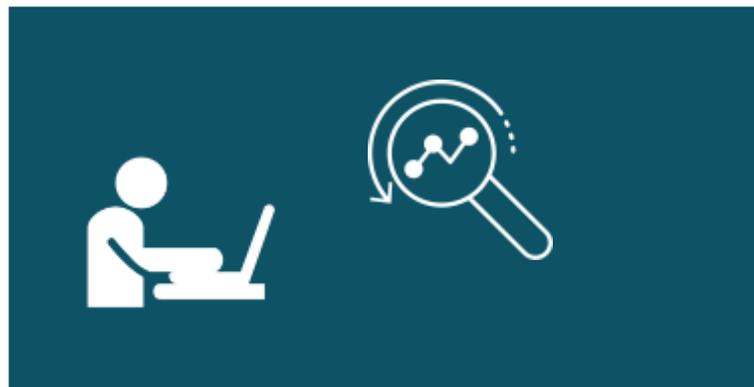
他社よりイイ！

Aruba Centralの**良い点**とAruba**無線の実力**



安定・快適なネットワークに必要な要素

可視化



- AIを使った自動解析と問題点の可視化と対応策の提示ができるか
- 直感的な操作で問題までたどり着くことができるか
- ネットワークの利用状況（負荷状況）、接続端末の可視化ができるか

調査力



- 自動解析だけで原因が不明瞭な場合に、トラブルシューティングする手段を保持しているか
(詳細なログ、リアルタイムログの確認、パケットキャプチャ等)

対応力



- 見つけた問題点を設定変更で解決することができるか
- ネットワーク、Wi-Fiの機能で問題が発生しない、発生しにくいようにすることができるか

ArubaはAI分析の結果から対策までを提示できる



ArubaのNetwork Insightは問題の原因と対策、設定ポイントまでを提示

他社ソリューションは、問題の原因までは特定出来るが、対策が不明瞭の場合が多い。
また想定される根本原因も1つのみ。

Feature	Aruba Central	他社 Cloudソリューション	他社 Cloud ソリューション
統計の保存期間	✓ 3時間、1日、1週間、1ヶ月	× 30日間	× 1週間
解決されたユースケース	AI インサイト: 40 を超えるユースケース ✓ Foundationサブスクリプションで大体のユースケースをサポート ✓ RF エクセレンス	同様の機能はありません × オンデマンドで推奨事項を実行する × 問題のある AP またはクライアントを詳しく調べて根本原因を知る	AI アクション: <20 のユースケース × AI には AI用のサブスクリプションが必要です × RF アクションは2つだけ
異常検出	はい: 一部の AI インサイトのみ ✓ サイト内の会社のベースライン ✓ ピア比較によるクラスベースライン	はい: ✓ 接続グラフ - ネットワークごとの6週間のデータの自動ベースライン ✓ 貴社のようなネットワークからの推奨でのピア比較	はい: 接続のみ × 異常なスパイク検出、ベースライン計算の詳細なし × ピア比較はありません

AIで検知出来るトラブル比較

他社のCloud管理ソリューションはAIOPSに優れていると言われますが。。。

使用事例	Aruba Central	他社 Cloud ソリューション	他社 Cloud ソリューション
デュアルバンド対応クライアントは主に 2.4 GHz 帯域を使用しました	✓	いいえ	いいえ
低いSNR	✓	手動閾値アラート	✓- カバレッジホール経由
帯域幅の使用量が多い	いいえ	手動閾値アラート	いいえ
802.1X 認証の失敗率が高い	✓	スマートしきい値アラート	✓
高頻度のキー交換の失敗	✓	いいえ - 暗黙的な認証失敗	いいえ - 暗黙的な認証失敗
高 DHCP 障害	✓	スマートしきい値アラート	✓
高度な関連付けの失敗	✓	スマートしきい値アラート	いいえ
キャプティブポータルの障害	✓	いいえ	いいえ
ARP障害	いいえ	いいえ	✓
DNSの問題	✓	スマートしきい値アラート	✓
Mac 認証の失敗	✓	いいえ - 暗黙的な認証失敗	いいえ - 暗黙的な認証失敗
Wi-Fi に影響を与える屋外クライアント	✓	いいえ	いいえ
カバレッジホールの検出	✓	いいえ	✓
ローミング数が多い	✓	いいえ	いいえ
ローミング時の遅延が大きい	✓	いいえ	いいえ

Cloudとの接続が切れてもローカルでステータスを確認可能

Aruba

他社

```
Aruba-AP# show ap debug cloud-server

IAP mgmt mode           :athena-mgmt
cloud config recvd      :TRUE
state diff              :disable
Device Cert status      :SUCCESS
Cert Verify             :enable
Domain Name Verify      :enable
CoP Mode Enabled        :FALSE
First Primary CoP Server :None
Second Primary CoP Server :None
Backup CoP Server       :None
Device info send        :SUCCESS
Aruba-AP#
Aruba-AP# ping google.com
Press 'q' to abort.
PING 142.250.76.142 (142.250.76.142): 56 data bytes
64 bytes from 142.250.76.142: icmp_seq=0 ttl=57 time=3.5 ms
```

- コンソールアクセスが無いので、APがCloudに接続できない場合のステータスを全てLEDで表示
- LED機能は豊富だが、あまりに複雑で解読が困難

- Cloudと接続が切れた場合も、コンソール、SSHでAPにアクセスし、ネットワークの接続性、Cloud接続のステータスをローカルで確認することができる

Arubaは標準ライセンスで豊富なレポート機能を提供します

1 か月を超えるレポートには追加料金がかかります

Feature	Aruba Central	他社 Cloudソリューション	他社 Cloud ソリューション
間隔	<ul style="list-style-type: none"> ✓ 1年間のワイヤレス概要 ✓ 最長3ヶ月のレポート期間 	<ul style="list-style-type: none"> ✓ 6ヶ月 	ネットワーク分析を使用すると <ul style="list-style-type: none"> × 30日間 × 最長1年間のプレミアム Analytics サブスクリプションが必要です
取得された合計統計情報	<ul style="list-style-type: none"> ✓ 21種類、100以上のアイテムをキャプチャ 	<ul style="list-style-type: none"> × 17個のアイテム 	<ul style="list-style-type: none"> × 30個のアイテム
トップエントリー	<ul style="list-style-type: none"> ✓ 10、25、40 アイテム 	<ul style="list-style-type: none"> ✓ 上位 50 アイテム 	<ul style="list-style-type: none"> × 上位 5 項目のみ
アラート	はい: 電子メールと Webhook 通知 <ul style="list-style-type: none"> ✓ 100以上のアラートタイプ ✓ カスタマイズ可能な重大度 	はい: 電子メールと Webhook 通知 <ul style="list-style-type: none"> ✓ 接続に失敗したクライアントに対するスマートしきい値 × 30種類のアラート × カスタマイズできない重大度 	はい: 電子メールと Webhook 通知 <ul style="list-style-type: none"> × 50のアラートタイプ × カスタマイズできない重大度

Arubaは標準のFoundationライセンスのみコスト的にも有利です

Aruba Centralは、CPU が 70% を超えた場合に重大度の重大度アラートが送信されるなどの細かい設定が可能

他社には、ゲスト、RAPIDS、セキュリティコンプライアンスレポートなどの徹底的なレポートがありません。

他社には、ゲスト、RAPIDS、セキュリティコンプライアンスレポートなどの徹底的なレポートがありません。

対応策とWi-Fi機能が圧倒的に豊富なAruba

Aruba

ローミング関連

高速ローミング

Opportunistic Key Caching (OKC):

802.11r:

802.11k:

RRM サイレント IE:

802.11v:

ClientMatch, 負荷分散

クライアント制御

バンドステアリングモード: 5GHz を優先

エアタイムフェアネスモード: デフォルトアクセス

ClientMatch:

ClientMatch の計算間隔: 3 秒

ClientMatch のネイバーマッチング: 60 %

ClientMatch のしきい値: 123

マルチキャスト最適化機能

ブロードキャスト/マルチキャスト

ブロードキャストフィルタ: 無効

DTIM 間隔: 1 ビーコン

マルチキャスト送信最適化:

ダイナミックマルチキャスト最適化 (DMO):

DMO チャネル使用量のしきい値: 90 %

Probe, Auth Request 閾値

ローカルプローブ要求のしきい値: 自動 ← 手動 0

認証要求の最小 SNR: Automatic ← Manual 0

無通信状態の請求へ deauth を送信:

WMM (Wireless QoS)

Wi-Fi マルチメディア

	シェア	DSCP マッピング
バックグラウンド WMM シェア	0 %	
ベストエフォート WMM シェア	0 %	
ビデオ WMM シェア	0 %	
音声 WMM シェア	0 %	

あくまで一例で
他にも多数存在

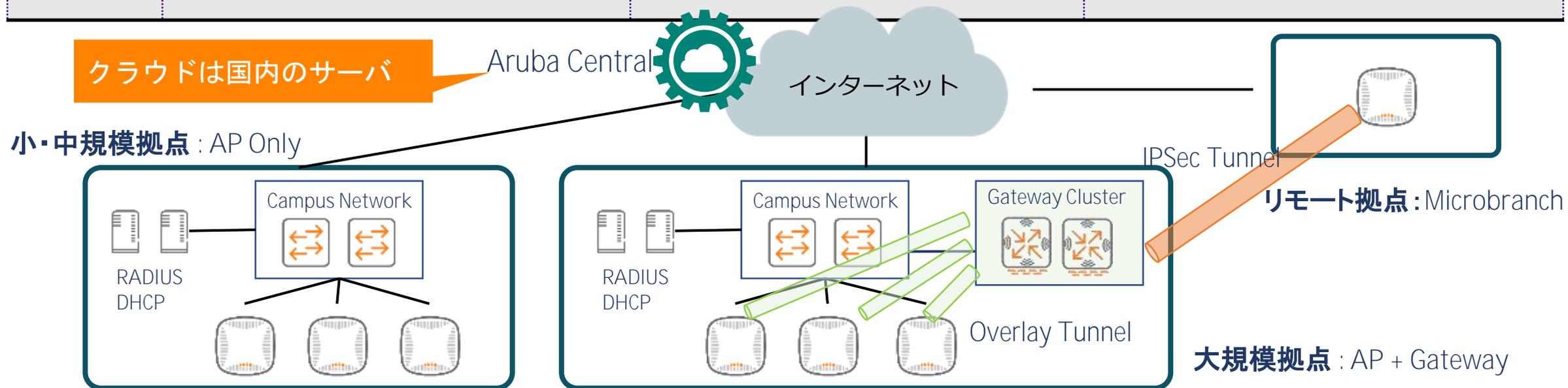
他社

- 基本的な機能、設定変更が可能な項目がほとんどないので、問題を可視化した後の対応策を取ることが困難

- ネットワークの問題解決のための対応策、機能が豊富
- 何か困った時になんとかなるのはAruba

意外と盲点になるスケーラビリティ

Feature	Aruba Central	他社 Cloudソリューション	他社 Cloud ソリューション
規模	<ul style="list-style-type: none"> ✓ AP単体での導入の場合 最大500のAP(同一VLAN) 最大5,000のクライアント(同一VLAN) ✓ Gateway導入の場合(9240 Cluster構成) 最大8KのAP 最大128Kのクライアント 	<ul style="list-style-type: none"> ✗ サイト/ネットワークあたり最大 800 台のデバイス ✗ 組織ごとに最大1000 のネットワーク ✗ 組織ごとに最大20,000 台のデバイス 	<ul style="list-style-type: none"> ✗ 2,000端末以上は、Edgeの導入を推奨 ✗ Edgeソリューション: 500AP/5,000クライアント



Arubaは大規模にも対応し、柔軟な構成パターンが可能！

キャンパスネットワーク向け無線LANの進化

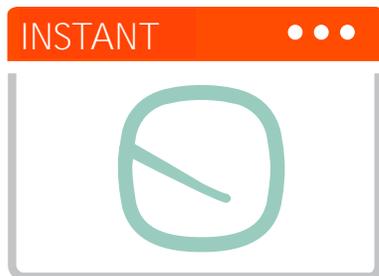
ArubaOS10



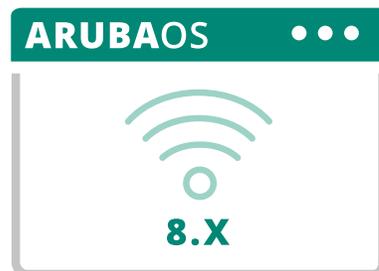
ArubaOS 10 (AOS10)

IAP, コントローラー, SD-BranchのOSを統合した
ユニファイドオペレーティングシステム

Aruba Instant AP (コント
ローラーレスAP)



Mobility Conductor,
Mobility Controllerとコ
ントローラーベース
AP



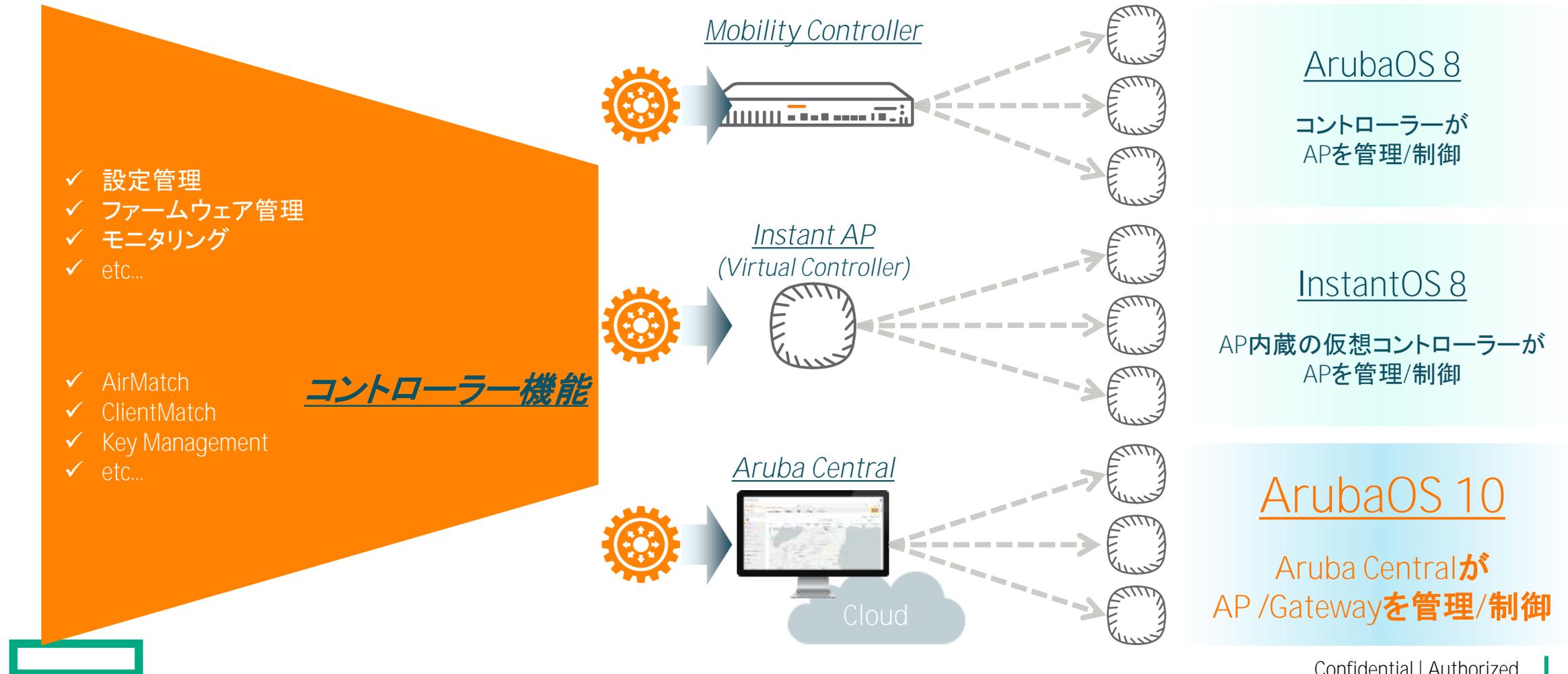
ブランチ及びヘッド
エンドゲートウェイ



* IAP, AOS8もご選択いただけます

AOS10 : Aruba Centralによる新しいアーキテクチャ

無線LANのコントローラー機能を”Aruba Central”に移行した新しいArubaOS



ArubaOS 8

コントローラーが
APを管理/制御

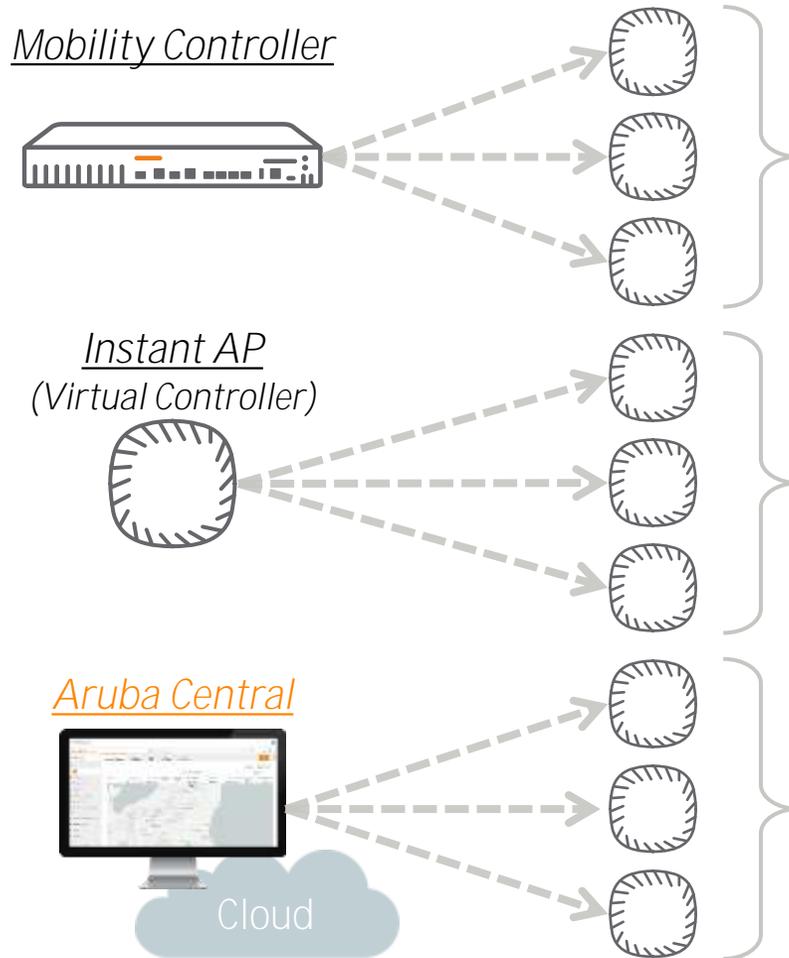
InstantOS 8

AP内蔵の仮想コントローラーが
APを管理/制御

ArubaOS 10

Aruba Centralが
AP /Gatewayを管理/制御

AOS10と従来のコントローラー/IAPの比較 - 拡張性



ArubaOS 8

管理可能なAP数/クライアント数は
コントローラーのモデルに依存

→ **最大管理数を超える
APの増設時には
コントローラーの増設/変更が必要**

InstantOS 8

管理可能なAP数/クライアント数は
約100AP/約2,000クライアント

→ **最大管理数を超える
APの増設時には
IAPクラスタの分割が必要**

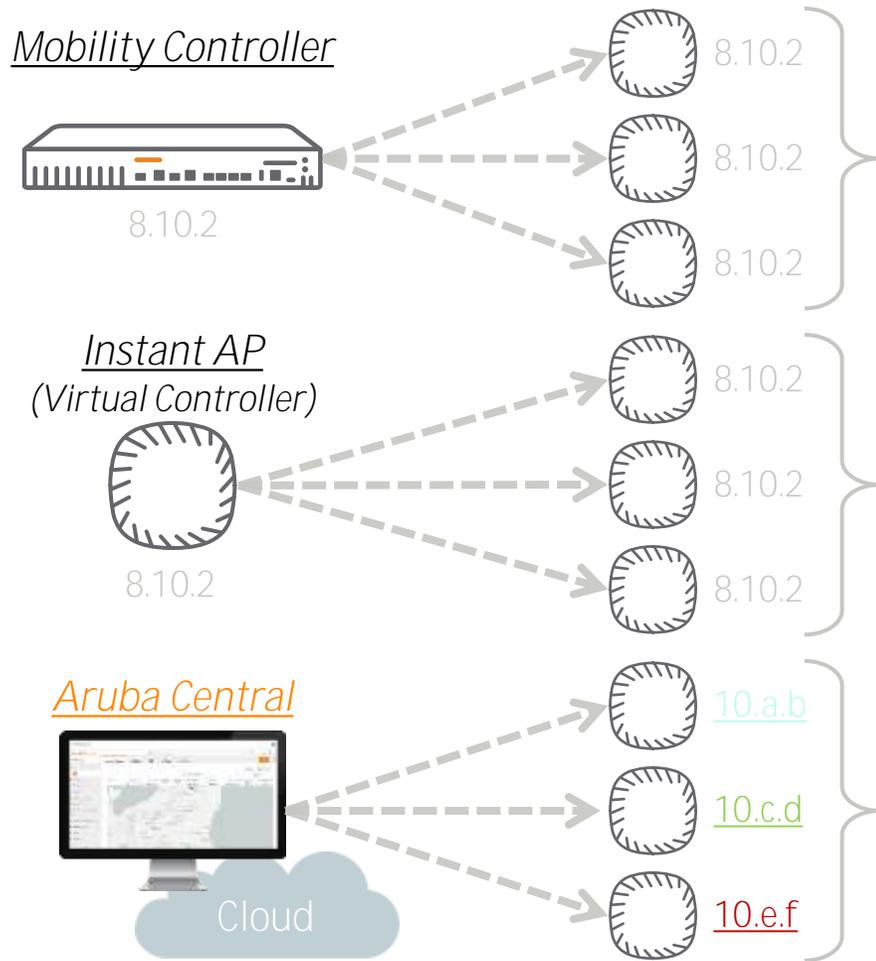
ArubaOS 10

管理可能なAP数/クライアント数に
制限なし

→ **AP増設時の
考慮は不要**



AOS10と従来のコントローラー/IAPの比較 - 管理性



ArubaOS 8

同じコントローラー管理下の
全APが同じバージョン

アップグレードは全APが対象

- ✓ サポート終了時
- ✓ 不具合の修正時
- ✓ サポート・バージョンが新しいAPの導入時

InstantOS 8

同じ仮想コントローラー管理下の
全APが同じバージョン

アップグレードは全APが対象

- ✓ サポート終了時
- ✓ 不具合の修正時
- ✓ サポート・バージョンが新しいAPの導入時

ArubaOS 10

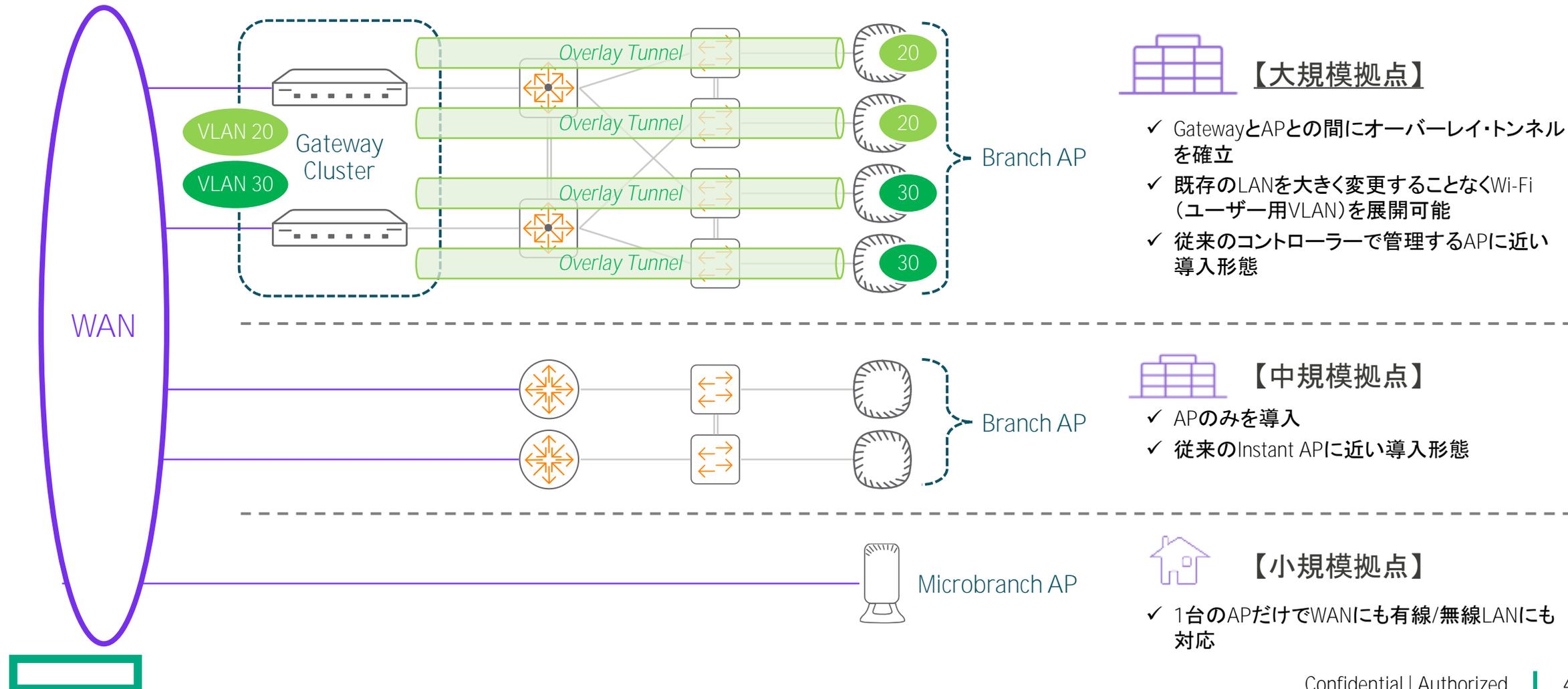
サポート中のバージョンであれば
制限なし

アップグレードは一括/個別で可能

- ✓ サポート終了時は、一部のAPで安定稼働を確認後、全APを一括でアップグレード
- ✓ 不具合の修正時は、対象APのみを個別にアップグレード
- ✓ サポート・バージョンが新しいAPの導入時のアップグレードは不要

AOS10の柔軟性

- 小規模拠点から大規模拠点までをカバーする柔軟なアーキテクチャー



AOS10: APのみを導入

導入 ターゲット

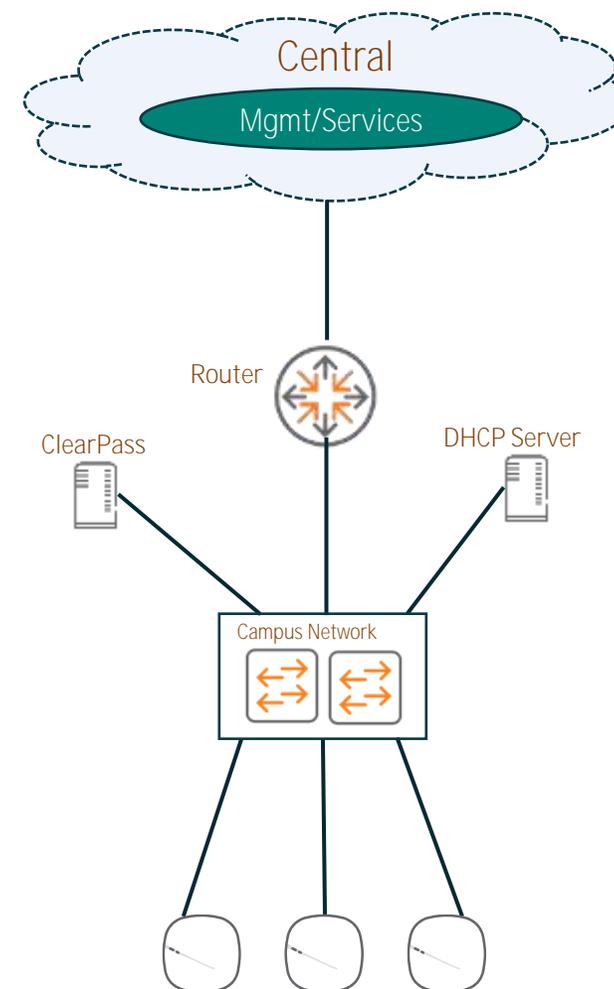
- 小～中規模キャンパス
- 拠点分散のエンタープライズ
- 分散拠点
- 1ローミングドメイン(1管理VLAN, 1クライアントVLAN)でmax 500AP/5000client目安

AOS10での ポイント

- すべてのAPがスタンドアロンで動作し、Centralから制御
- APがAuthenticatorになる
- マルチバージョンで動作可能
- AirMatch, Live Upgrade, UCC, AirGroup, ローミング(ClientMatch)

IAP導入と 同じポイント

- ユーザーVLANはAPで設定し、トラフィックはAPでブリッジされる
- APが接続されるスイッチのポートはTrunkポート
- Firewallポリシー適用はAPで行われる



AOS10: ゲートウェイと一緒に導入

導入 ターゲット

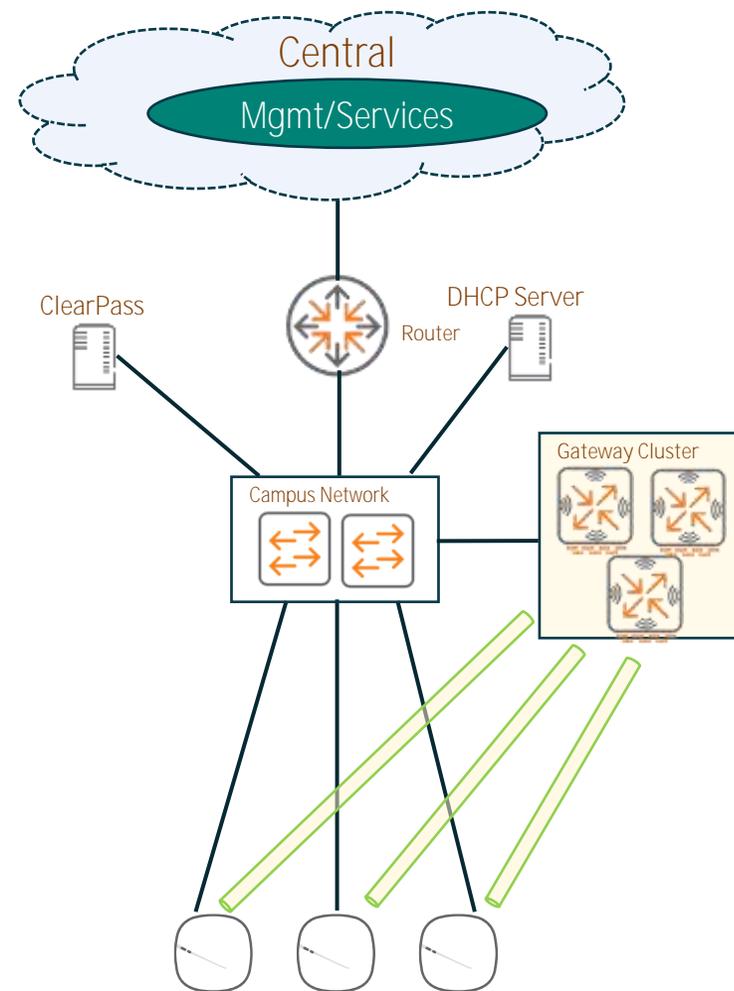
- 中～大規模エンタープライズキャンパス
- 拠点分散の大規模エンタープライズ
- SD-Branch (SD-WAN)

セキュリティ & ポリシー

- ユーザートラフィックのトンネリング
- WLANのセグメンテーション
- 集中型のVLANやブロードキャストトラフィック管理
- 異なるサブネット内のローミング
- 集中型の高度なポリシー適用
- 無線LAN/有線LANに対し一貫したポリシー適用

機能

- ダイナミックRADIUSプロキシ
- モビリティ
- Microbranch
- MultiZone
- SD-Branch (SD-WAN)



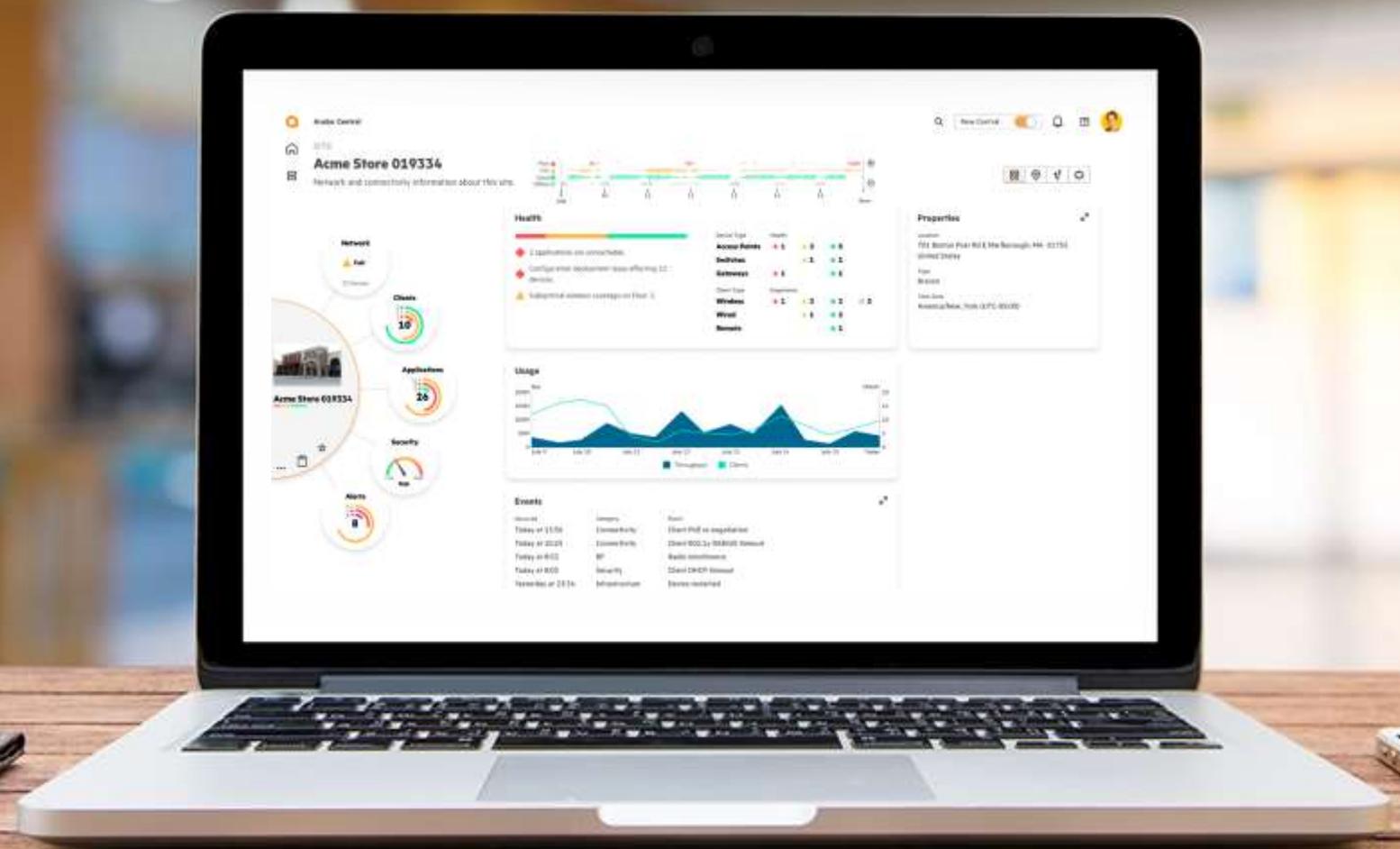
Aruba Centralの進化

Next Generation Aruba Central



new

進化を遂げるCentral Next-Generation Central



Next-Generation Central **ダッシュボード**



Next-Generation Centralの主な機能-1



「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



Next-Generation Centralの主な機能-2



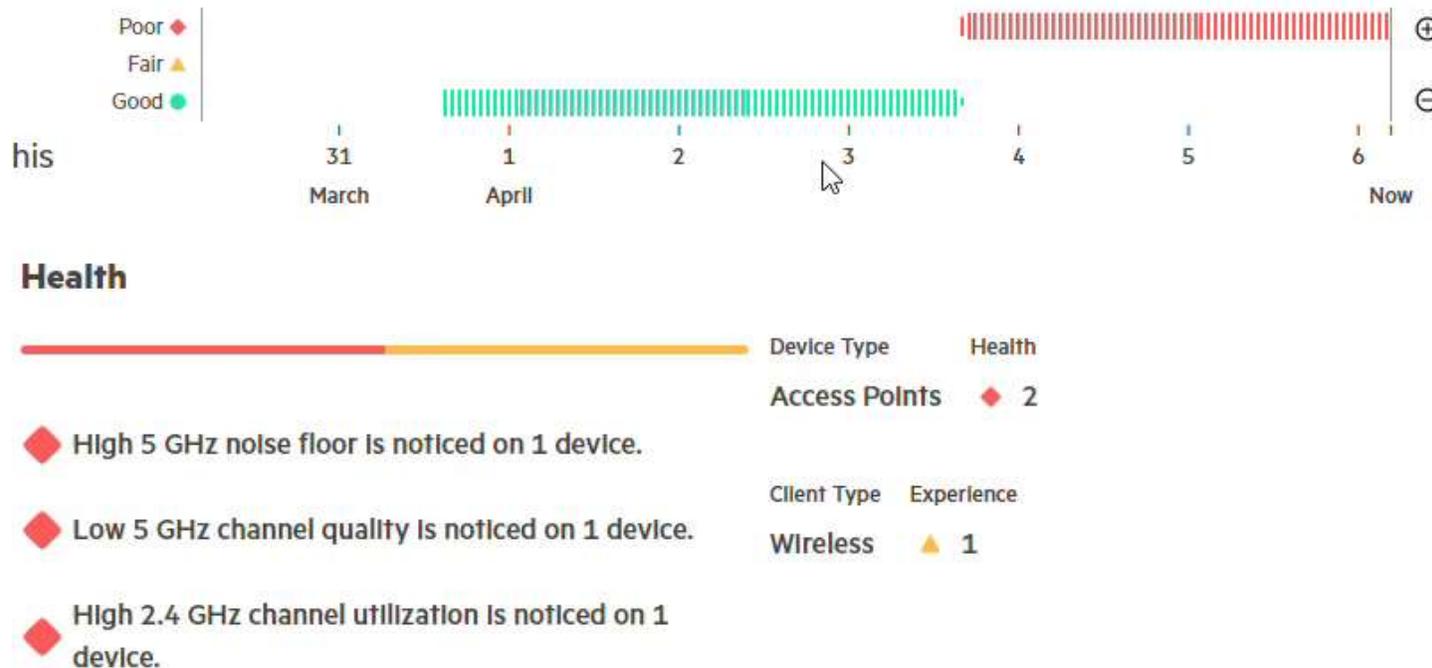
業界初の「ネットワーク・タイムトラベル」

パケットキャプチャを超える新機能



直感的な
データビュー

- 「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。



Next-Generation Centralの主な機能-3

- 「サンバースト・トポロジー」ビュー



Thank you!

