



# Arubaの快適な企業 Wi-Fiソリューション

ユニアデックス株式会社

---

# Aruba製品ラインナップ

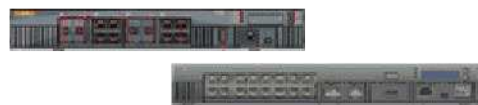
## ソフトウェア



## モビリティ・コントローラ



Aruba 7200



Aruba 7030/7010



Aruba 3000シリーズ



Aruba 7005

## インスタント



IAP-225



IAP-103

独立型・小規模向け

## アクセス・ポイント

屋外 AP



AP-224/225



AP-103



AP-275

RAP-155/P



AP-175P



RAP-3



AP-115/114 AP-204/205



AP-109/108

キャンパス AP

リモート AP

## モビリティスイッチ

S3500  
S2500  
S1500



PoE

10GE Uplink

Site-to-Site VPN

Aruba Stack

Role Base

# ■ Wi-Fiへの要件

## 安定性 + 高品質

多数の端末の同時接続が必要  
全てのユーザーが快適に利用できる必要がある

## 柔軟性・高可用性

Wi-Fiがプライマリネットワークになりつつあり、  
今まで以上の柔軟性、高可用性が必要

## セキュリティ

高いセキュリティレベルを維持したままでのBYOD、  
ゲストアクセスへの対応が必要

## ITスタッフ不足

常にWi-Fi専任スタッフがいるわけでは無いので、  
現地での対応は最小限に留める必要がある

# ■ Arubaが選ばれる4つの理由



**高機能コントローラで安定・快適なWi-Fiを提供**

## ClientMatch / ARM

業界初の高機能な負荷分散機能と、電波自動調整機能による安定したWi-Fiを提供



**導入規模に応じた柔軟なWi-Fiソリューション**

## コントローラ / RAP / IAP

ランチコントローラ、RAPやIAPなどネットワーク構成や拠点の規模に応じた柔軟なWi-Fiサービスの展開が可能



**認証 + ファイアウォール機能でセキュアなWi-Fi**

## Role Base

セキュアな802.1x認証と端末やユーザ情報に基づいたRole-Baseアクセス制御を実現



**セルフサービスでヘルプデスクの負荷削減**

## AirWave / IAP

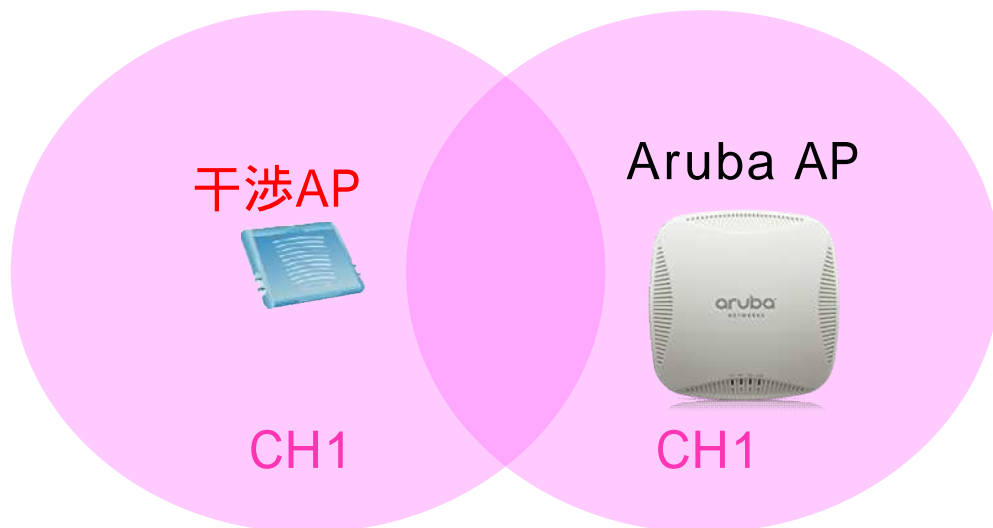
- AirWaveでAP設定の集中管理
- IAPはAP交換時の初期設定不要

# ■ インテリジェントな自動電波調整機能（ARM）

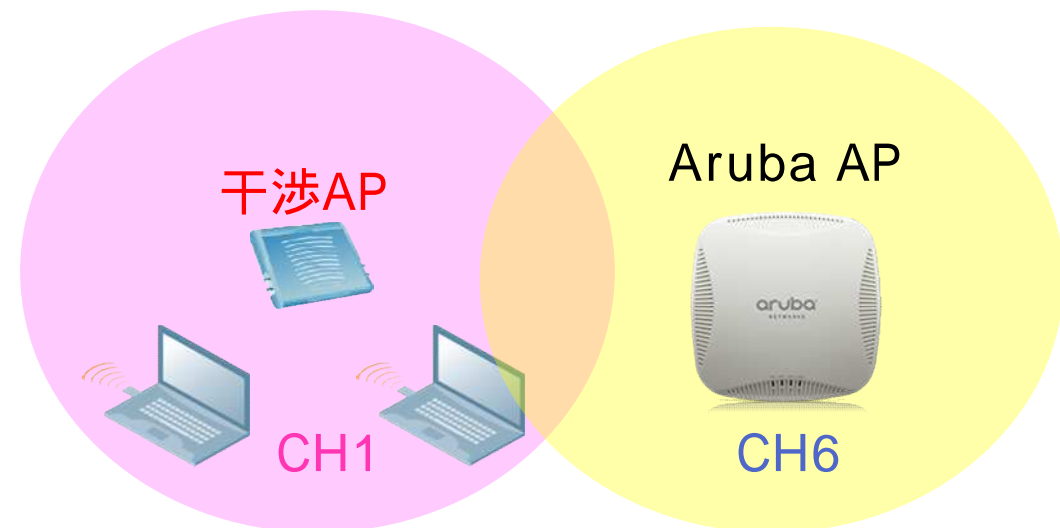
安定性

- いわゆる設定管理の一括化だけの機器は電波調整機能は無い
- Wi-Fiは干渉のパフォーマンス、安定性への影響が大きいため電波調整機能は必須
- ArubaのARM機能では、干渉波とそこでの通信状況を見てAPの電波チャンネルを自動変更

干渉APにクライアントがない  
（実通信なし）

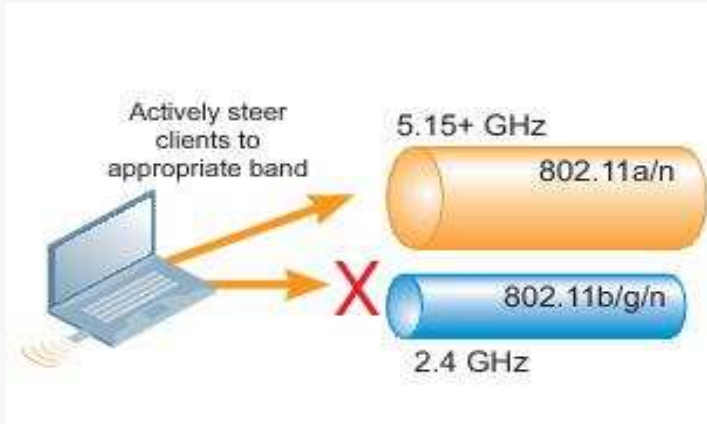


干渉APにクライアントがいる  
（実通信あり）

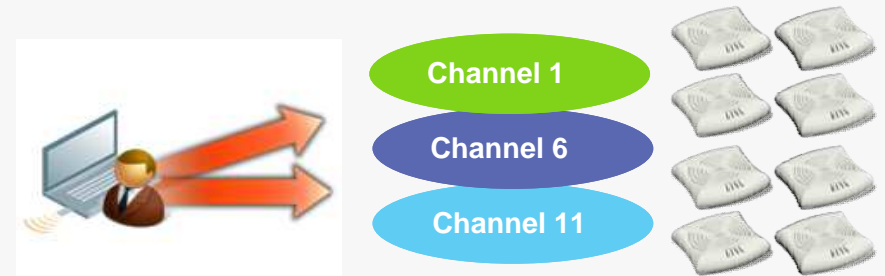




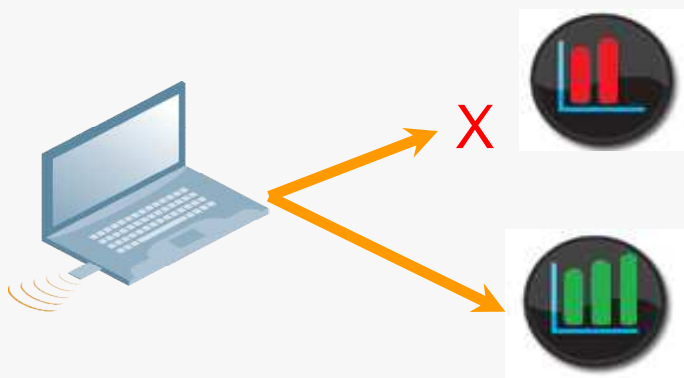
# ClientMatch : 業界初、様々な負荷分散機能を統合！



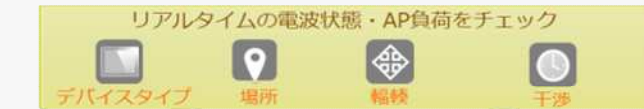
最適な周波数帯を選択



負荷の少ないChannelを選択



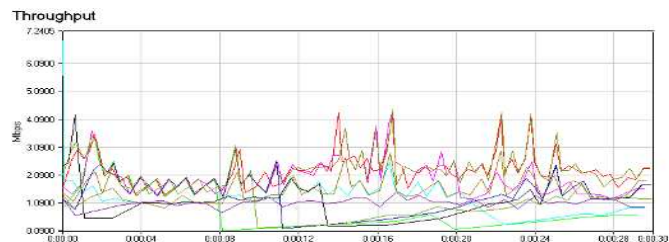
最適なアクセスポイント



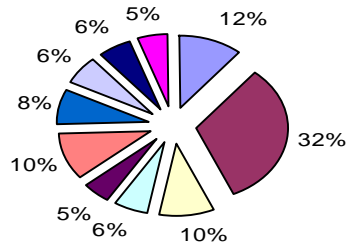
接続済みの端末も動的に移動

## AirTime Fairness : 無線リソースの最適分配機能

Air Time Fairnessなし



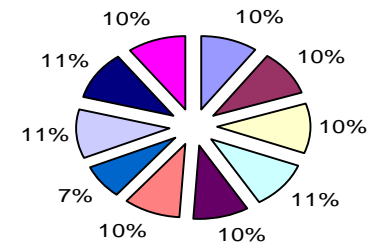
Per client throughput



Air Time Fairnessあり



Per client throughput



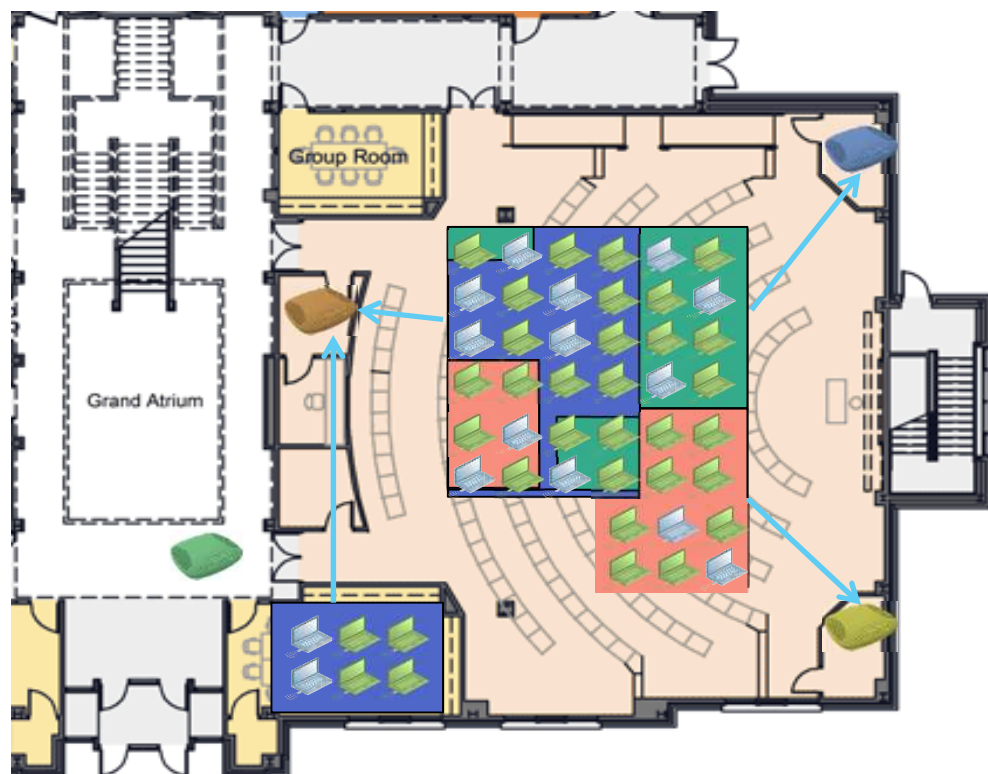
- 新旧様々な(11a/b/g/n/ac)端末の混在時に全てのクライアントで同じ量の通信をさせる
- 11nなど、高機能端末に優先して無線リソースを与えて無線リソースを有効活用する

# ClientMatchによる負荷分散

安定性

2.4 GHz  
5 GHz

## ClientMatch前



- 最適なAPに接続していない端末が多い
- 端末設定によっては、2.4GHzに偏ることもある

## ClientMatch後



- APに接続済みの端末も動的に最適なAPに再接続（ユーザは気が付かない）
- 5GHz帯を有効に利用



# ClientMatchの効果：スループットの比較

安定性

## ClientMatch無し

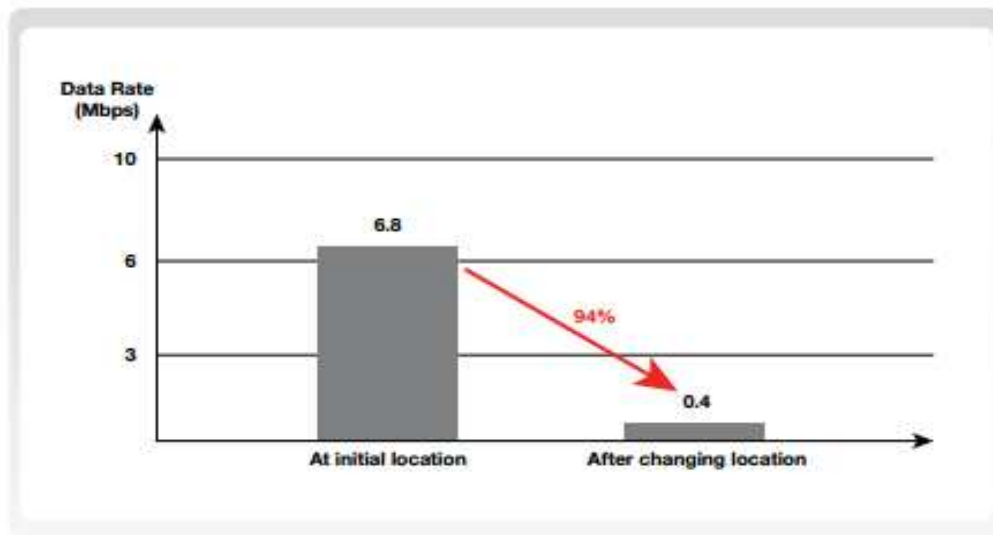


Chart 1. Samsung Galaxy tablet on Cisco Wi-Fi

## ClientMatch有り

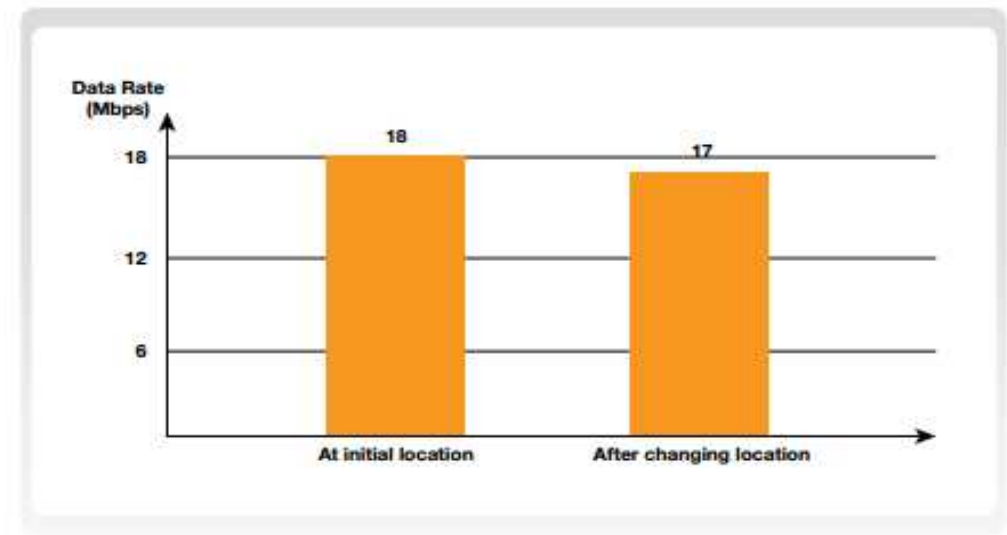


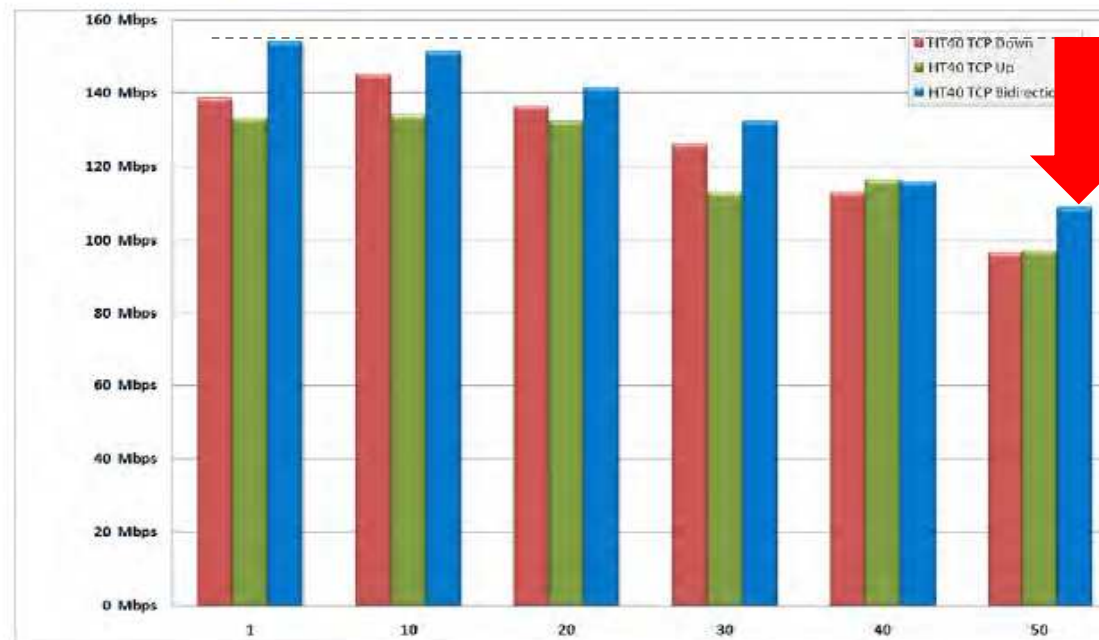
Chart 2. Samsung Galaxy tablet on Aruba Wi-Fi with ClientMatch

- AP4台に50台の端末を接続した試験結果
- ClientMatch無しだと負荷分散がうまくできず、一部の端末のパフォーマンス劣化が顕著になる

# ■ 負荷分散はなぜ重要か

- 同一AP（同一チャネル）への接続端末数が増加すると、パケットの衝突する確率が増加するため、チャネル利用効率が落ちる（APの処理能力とは別問題）
- チャネルあたり 50 台程度を超えると、スループット低下が顕著
- 某社のSingle Channelは論外

Figure 64 TCP HT40 Client Scaling Test (Aggregate Channel)



端末数が50台で  
スループットが  
30%低下

# ■ 最高性能の802.11ac AP

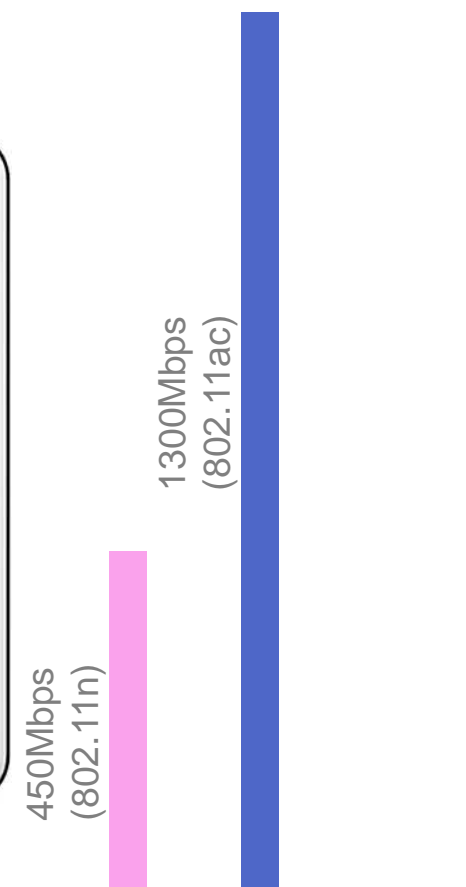
安定性

- これまでの801.11n APと比べてスループットが大幅に向上
- クライアントが帰属する推奨値もAP1台あたり100台程度に向上(radioあたり50台程度)  
これまでの802.11n APでは、AP1台あたり約50~60台程度が推奨値)

約3倍のスループット!



- 3x3:3デュアル・ラジオ
- 5GHz 11ac: **最大1.3Gbps**
- 2.4GHz 11n: 最大450Mbps
- 2x GEリンク・アグリゲーション
- 1Gbps以上のTCPスループットを実現
- PoE (802.3af) で動作可能  
フル機能の場合、PoE+ (802.3at)要



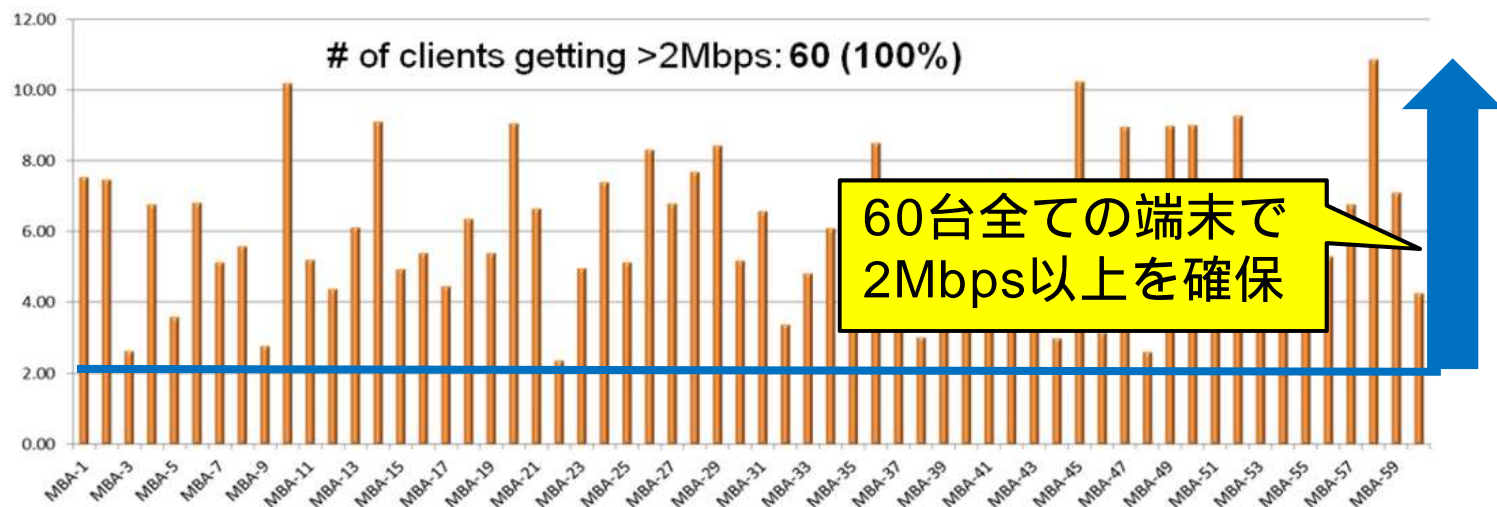
2013年6月にリリース済  
(既に国内でも多くの導入実績)

# ■ AP-220シリーズ： 端末60台接続時のパフォーマンステスト

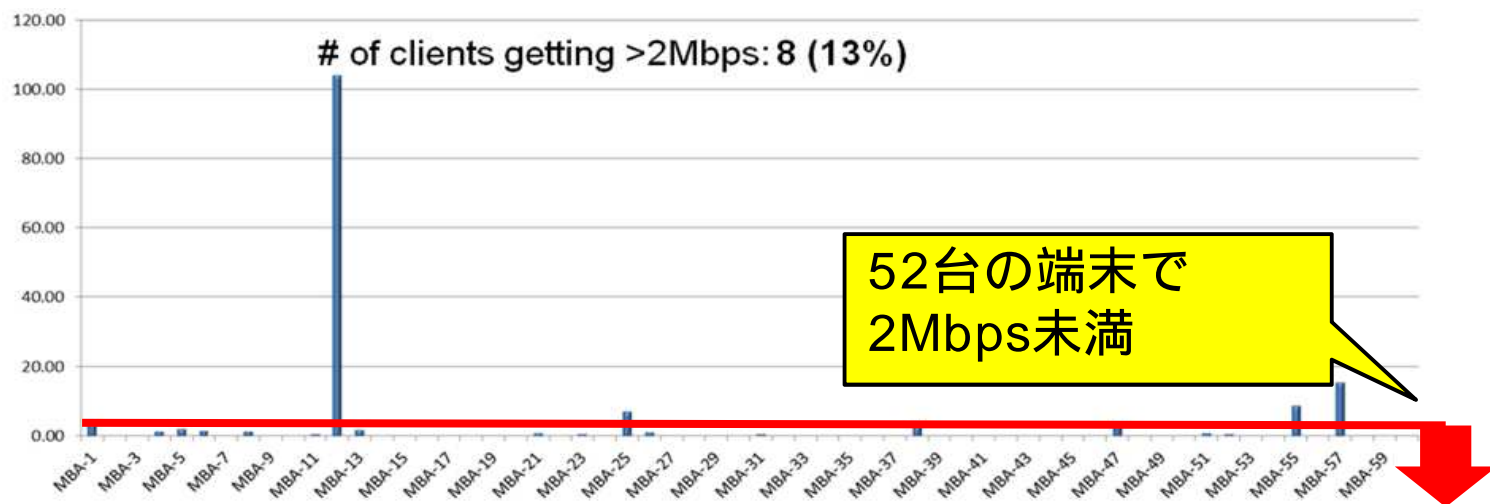


## TCPスループット試験比較（双方向:upstream/downstream）

Aruba AP225  
(AOS: 6.3.1.2)



他社の  
同クラス製品



# ■ AppRFによるアプリケーション 通信の最適化



クラウドおよび  
コラボレーション・アプリの可視  
化と制御  
(アプリ数1,500以上)

DPIを使用する次世代  
モビリティ  
ファイアウォール

3<sup>rd</sup> Party  
システムとも連携



SDN  
API



# MS Lyncの動的帯域制御概要



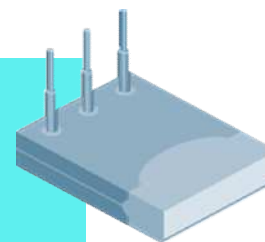
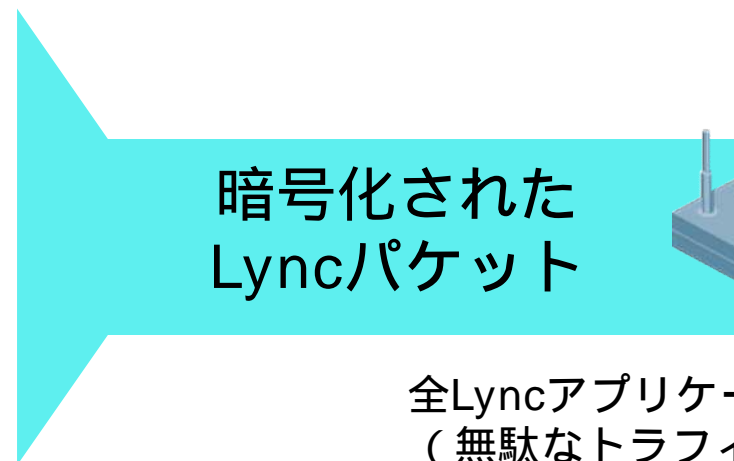
Lync Voice / Video / デスクトップ共有 / ファイル転送を識別して、優先制御出来る、**唯一のWi-Fi資格**を取得 (Microsoft Lync認定プログラム)

日本マイクロソフト 品川本社の無線LANインフラとしてアルバが採用！  
他社のソリューション



Microsoft Lync2013

- Voice (音声)
- Video (映像)
- デスクトップ共有
- ファイル転送
- インスタントメッセージ

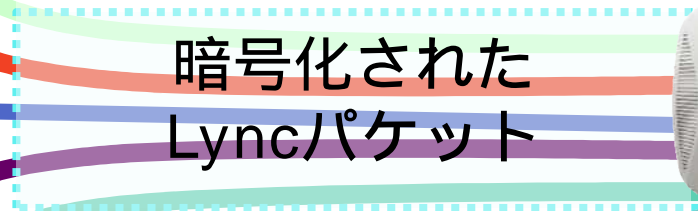


全Lyncアプリケーションを丸ごと優先処理  
(無駄なトラフィックも優先処理される)

## Arubaのソリューション

高優先 ↑  
低優先 ↓

- Voice (音声)
- Video (映像)
- デスクトップ共有
- ファイル転送
- インスタントメッセージ



各Lyncアプリケーション毎にパケットを優先制御

# ■ アルバは2つのLyncソリューションを有する



Microsoft Lync2013

## Lync ALG (SDN API) Lync serverに専用PlugIn要



## Lync (Media Classification)



# Lync SDN API vs MediaClassification



Feature	Media Classification	SDN API
WMM/DSCP値のマーキング / リマーキング	✓	✓
Lync voice/videoを自動的に識別し有線制御	✓	✓
Office365 Lync トラフィックの優先制御	✓	
100台以上のコントローラ環境に適応した拡張性	✓	
LyncサーバにPlugIn不要	✓	
Lync デスクトップシェアリング、ファイル転送を自動的に識別し、優先制御		✓
MOSの算出		✓
UCCスコアの算出 ( Real-time call quality analysis )		✓
UCCスコアとWi-Fi環境を元にしたCall qualityの算出		✓
UCC ダッシュボードの利用		✓
AirWaveのFloor plan上にLync クライアントの健康状態を表示		✓
100%のLync トラフィックを識別 / 制御出来る精度		✓

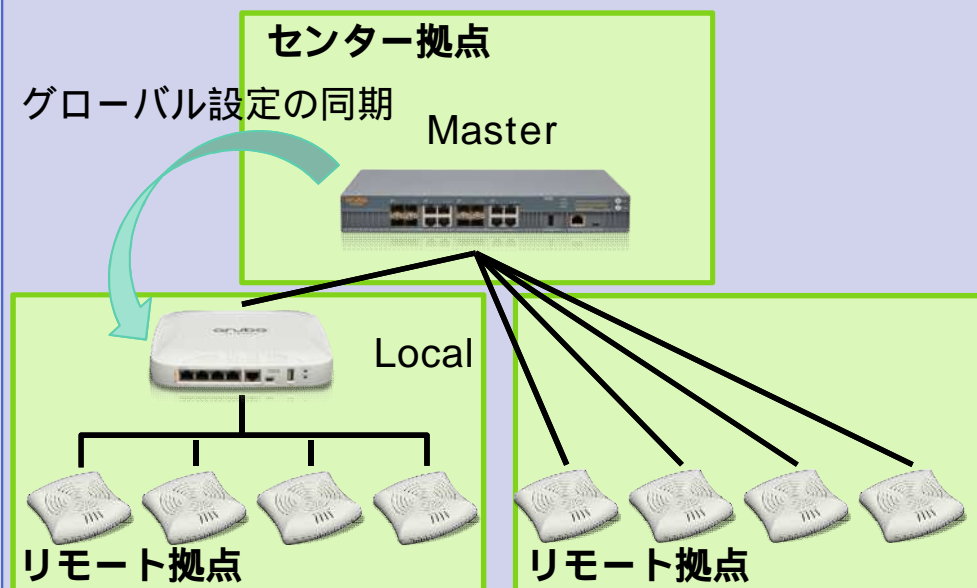


# ■ Arubaの柔軟な拠点へのWi-Fi展開方法



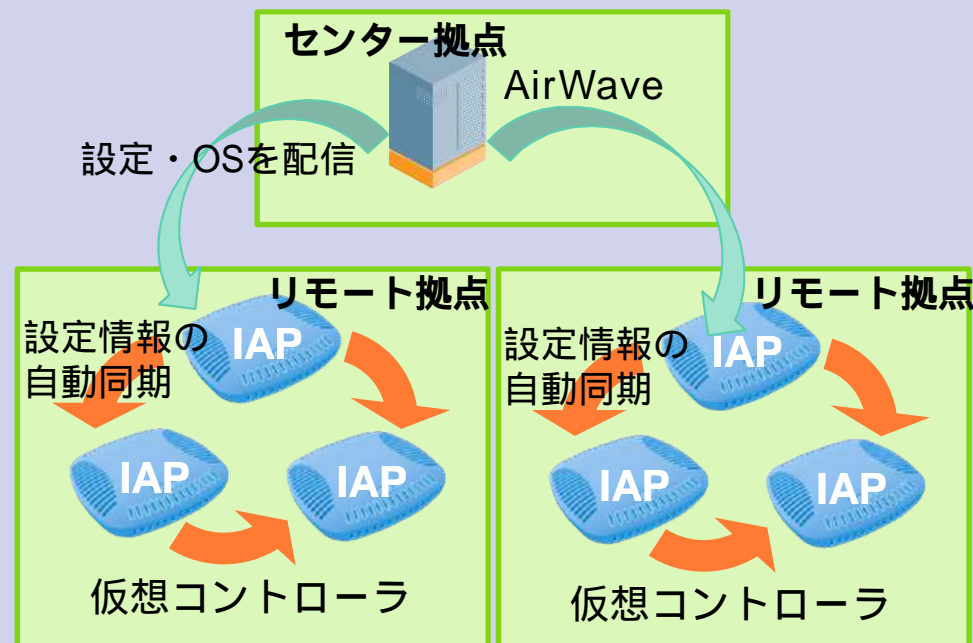
## ブランチコントローラ、RAPブによる拠点Wi-Fiの展開

- 大規模展開へ対応する拡張性
- 複数コントローラ構成における集中管理構成
- トラフィックは、トンネルモードによるセンター集中化、ブリッジモードによる分散型が可能

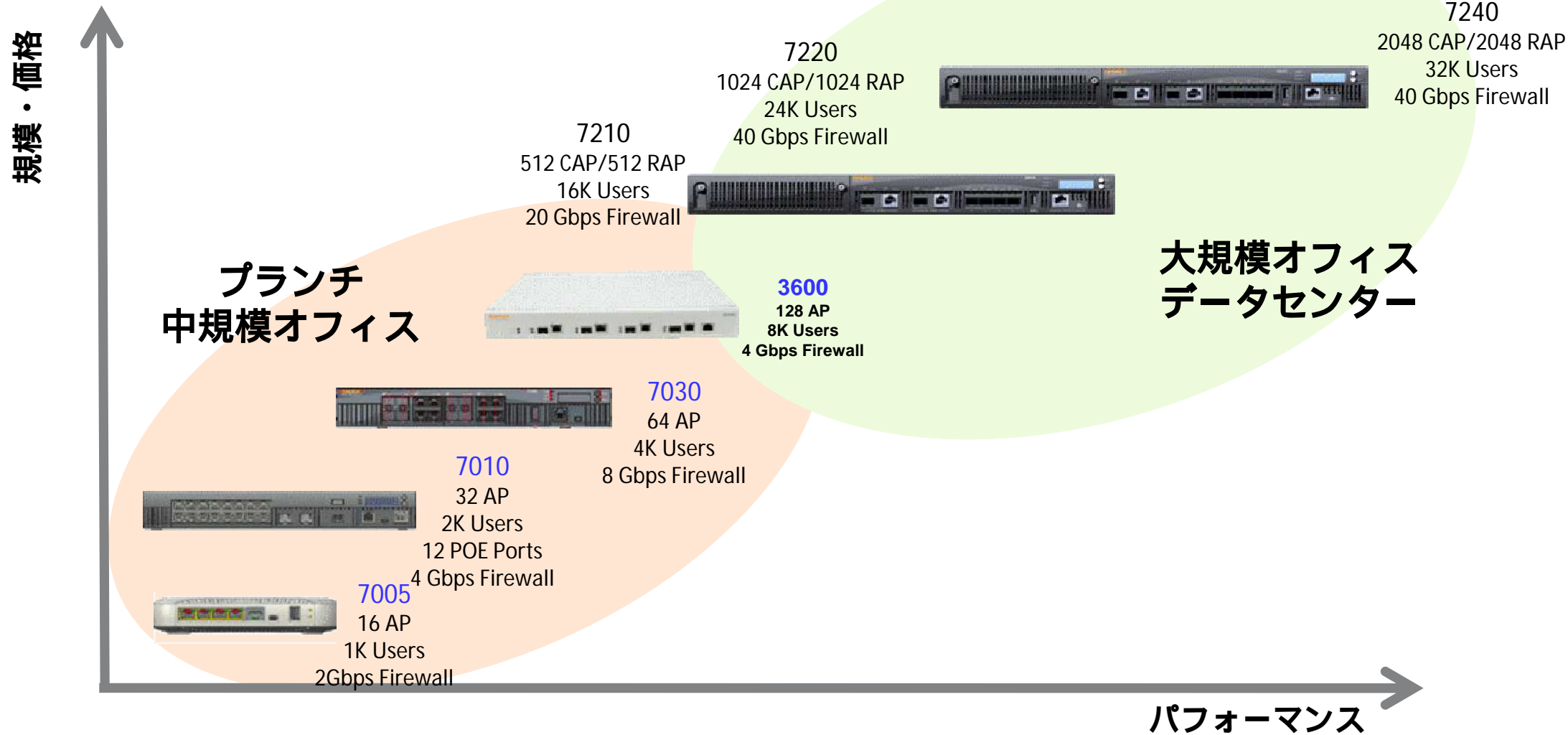


## Instant APによる物理コントローラレスのWi-Fi展開

- 拠点毎の仮想コントローラ
- ウィザードによる簡単設定（完全日本語化）
- コントローラ型APにアップグレードが可能
- 複数の仮想コントローラはAirWaveで統合管理



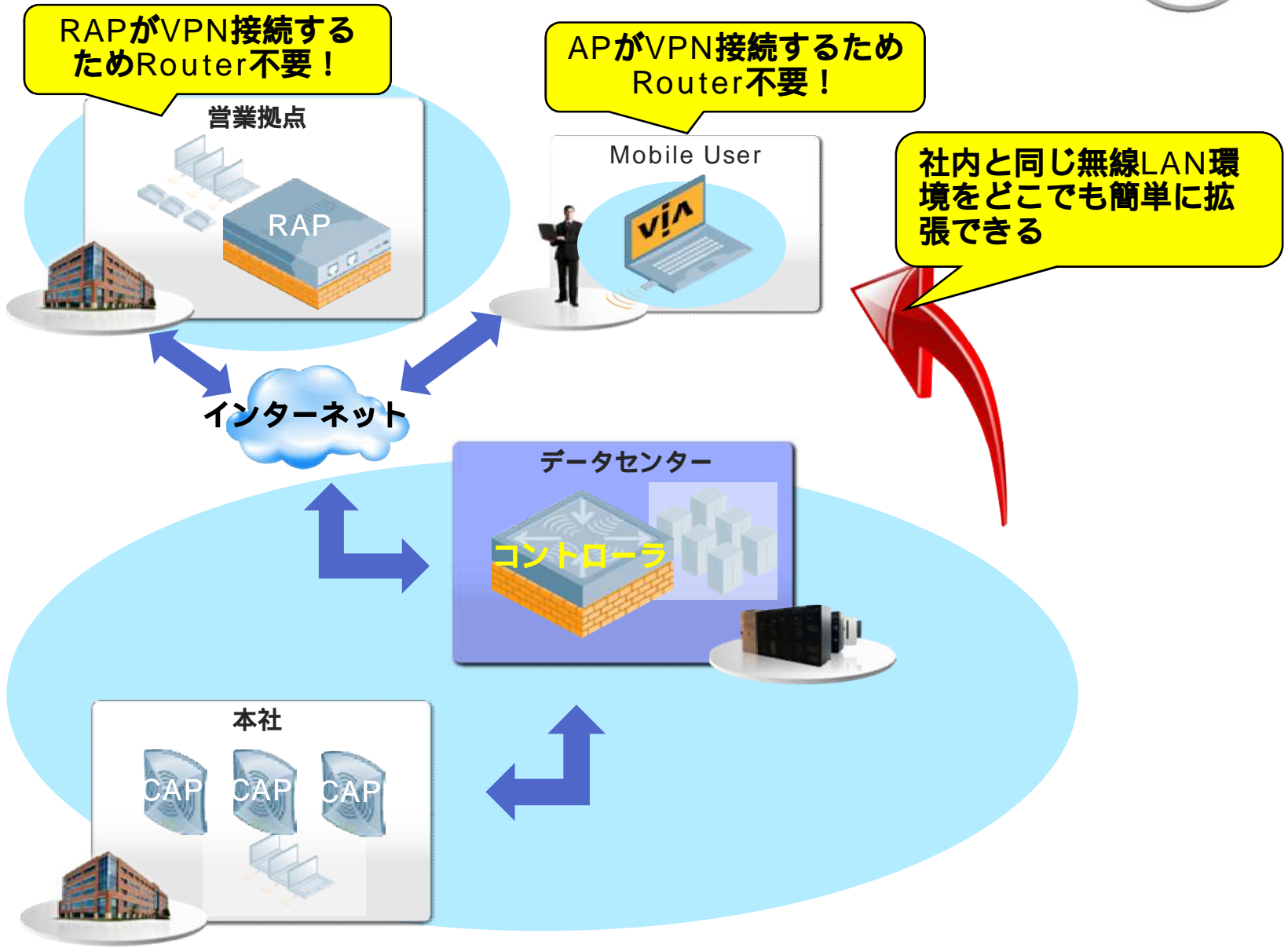
# ■ 規模に応じたコントローラ



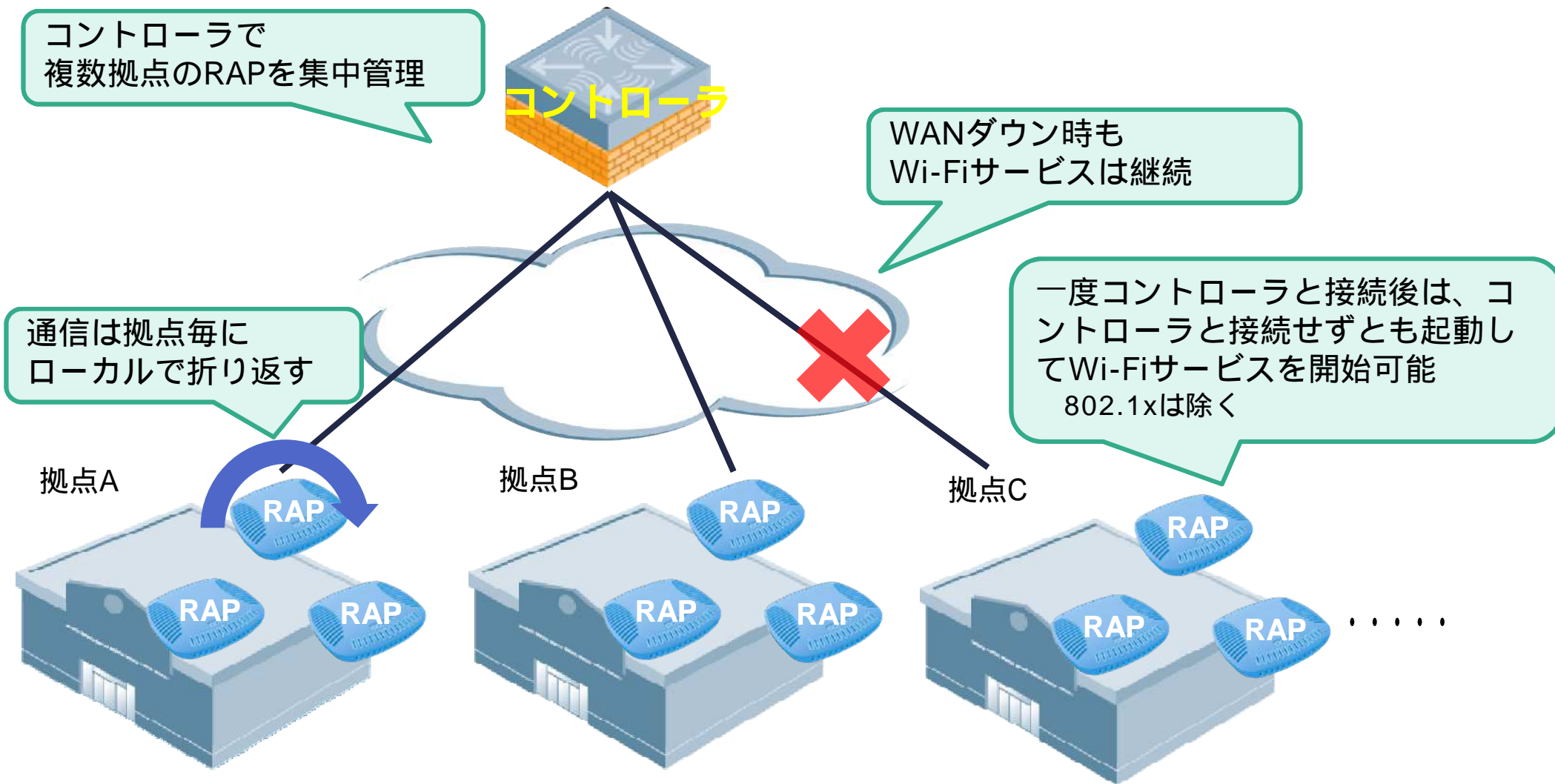


# Remote AP (RAP) で、 様々な拠点への容易なWi-Fi展開

有線ポート付のRAPもあるため、SOHOや新拠点立ち上げ時、災害時の在宅勤務など、様々な状況に応じてネットワークを展開可能！



# WANダウン時もWi-Fiサービスを継続Remote AP Bridgeモード



# IAPを使った分散型アーキテクチャ

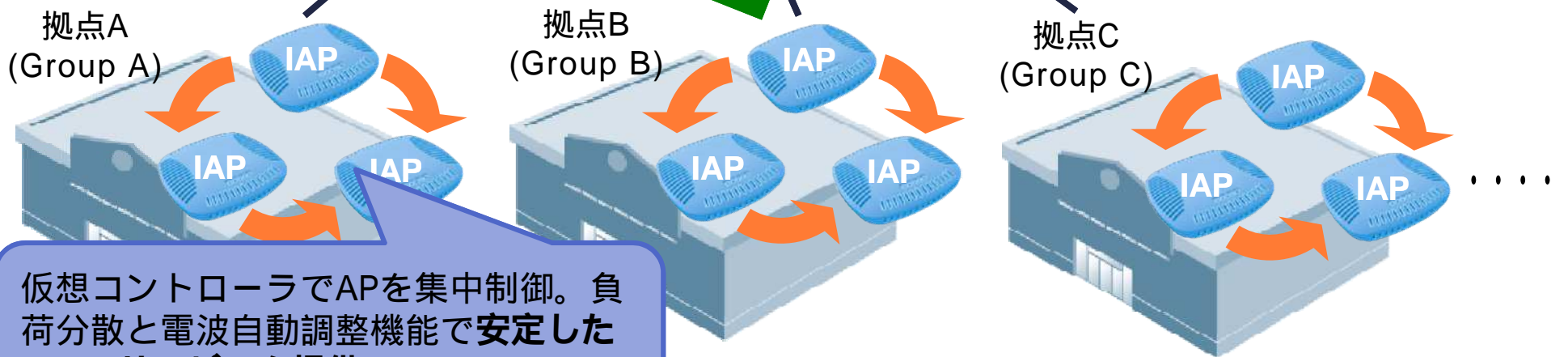


- ・ 拠点Aの設定 (Group A)
  - ・ 拠点Bの設定 (Group B)
  - ・ 拠点Cの設定 (Group C)
- \* 全拠点を同じ設定にしたり、複数拠点を同じグループにしたりすることも可能。

管理サーバ  
(AirWave)

設定やソフトウェアバージョン、障害時の対応などはAirWaveで集中管理が可能

学校毎に独立した仮想コントローラで動作するため、WAN障害時もWi-Fiサービスを継続できる



仮想コントローラでAPを集中制御。負荷分散と電波自動調整機能で安定したWi-Fiサービスを提供

# IAP : 1台からでも使える企業Wi-Fi ~導入規模に応じた無線LAN展開を実現~



Instant Access Point  
(IAP)



- ライセンス不要
- コントローラ型APと同価格
- パーチャルコントローラ
  - APに**コントローラ機能**を内蔵
  - AP1台から使える
  - 電波干渉を防ぐ電波自動調整機能
  - ステートフル ファイアウォール
  - 不正 AP 検出
  - 音声と動画に対するステートフルQoS
- ウィザードによる簡単設定 (完全日本語化)
- コントローラ型APにアップグレードが可能



1~数十台



数十~数百台



数百台~

# ■完全日本語対応、シンプルな設定画面



APUBA networks Virtual Controller Ins

1 ネットワーク

名前 クライアント  
instant 1  
→ 新規

Instant-C1:A5:6B

情報

名前: Instant-C1:A5:6B  
国コード: US  
仮想コントローラ IP: 0.0.0.0  
AirWave IP: 0.0.0.0  
周波数帯: すべて  
マスター: 192.168.21.252  
OpenDNS status: Not connected  
Uplink type: Ethernet  
Uplink status: Up

新しいネットワーク ヘルプ

1 基本情報 2 VLAN 3 セキュリティ 4 アクセス

基本情報

名前 (SSID): an-iap

主な用途:  従業員  音声  ゲスト

コンテンツフィルタリング: 無効

ステルスモード:

詳細オプションを表示

次へ キャンセル

検索

ネットワーク アクセスポイント  
ant 6c:f3:7f:c1:a5:6b

モニタリング 0 alerts IDS 設定

利用率のトレンド

クライアント

スループット (bps)

1M 100K 10K 0 100 10K 1M

21:45 21:50

— アウト — イン

Ja

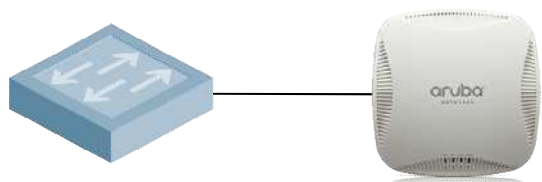
AirWave ステータス: 未設定 | 今すぐ設定

一時停止

# ■ 設定もシンプル



スイッチ (ネットワーク)へIAP  
を接続して起動



接続、起動！

- 起動後、“Instant”というSSIDを自動でふく
- 最初に立ち上がったAPが仮想コントローラとして動作



PCでInstant SSIDへ接続し、ブラウザを立ち上げGUIアクセス

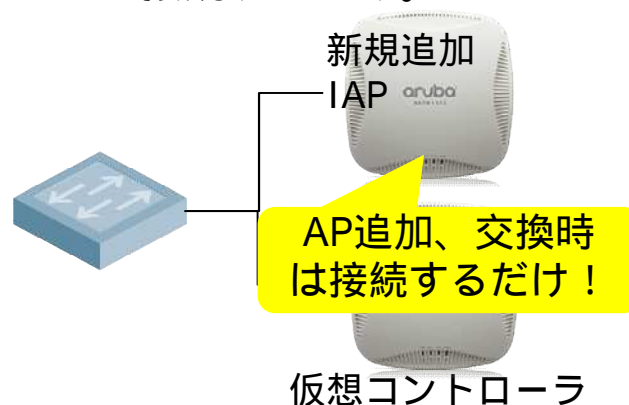


- GUIで簡単にWLANを設定
- 基本設定もシンプルで簡単

ウィザードに形式で、画面に沿って設定していくだけ

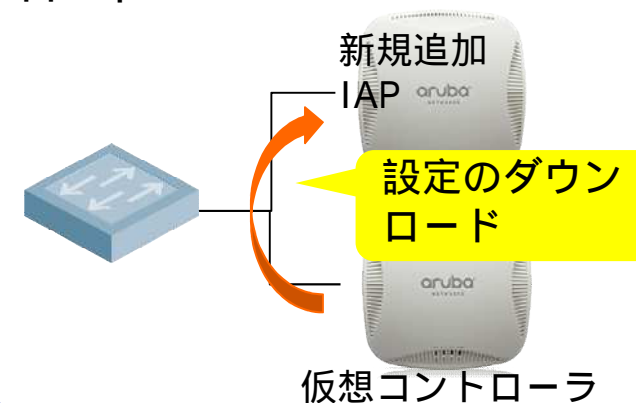


APの追加は同じL2ネットワークへAPを接続するだけ。



AP追加、交換時は接続するだけ！

追加APは自動的に設定をダウンロード

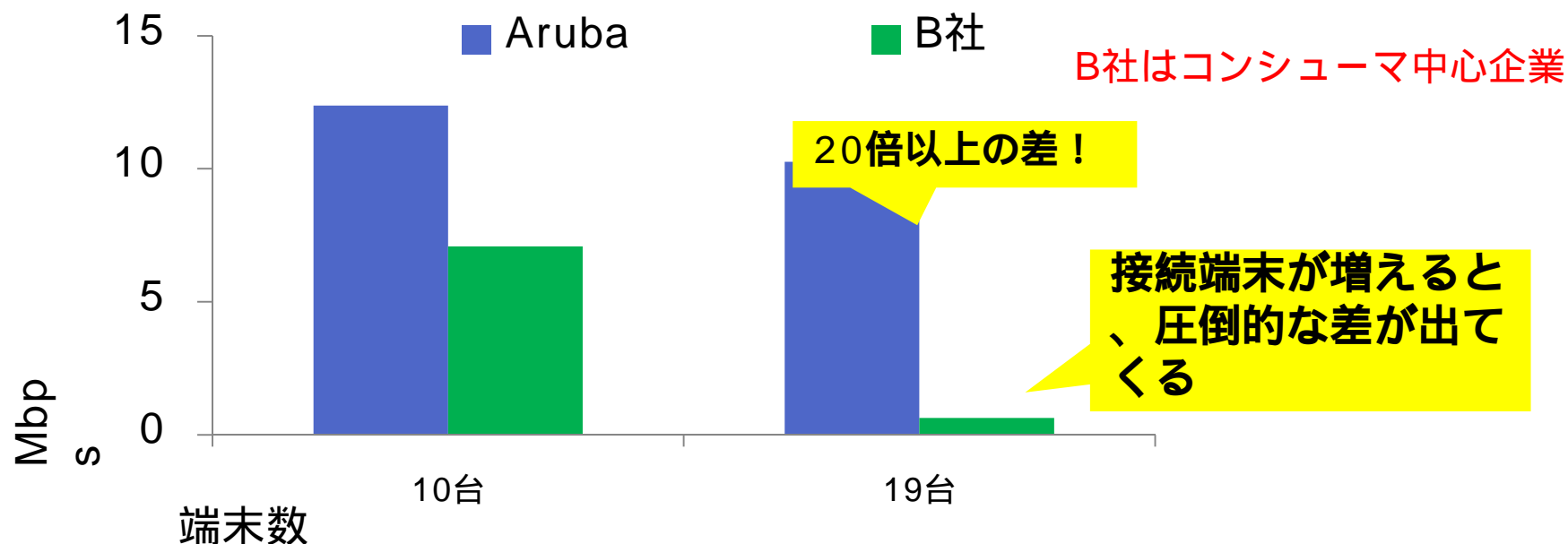


設定のダウンロード



# ■ コンシューマ製品との違い

試験内容：複数端末が同時にhttpでファイルダウンロードを実施  
結果：（以下は1端末当りの平均スループット）



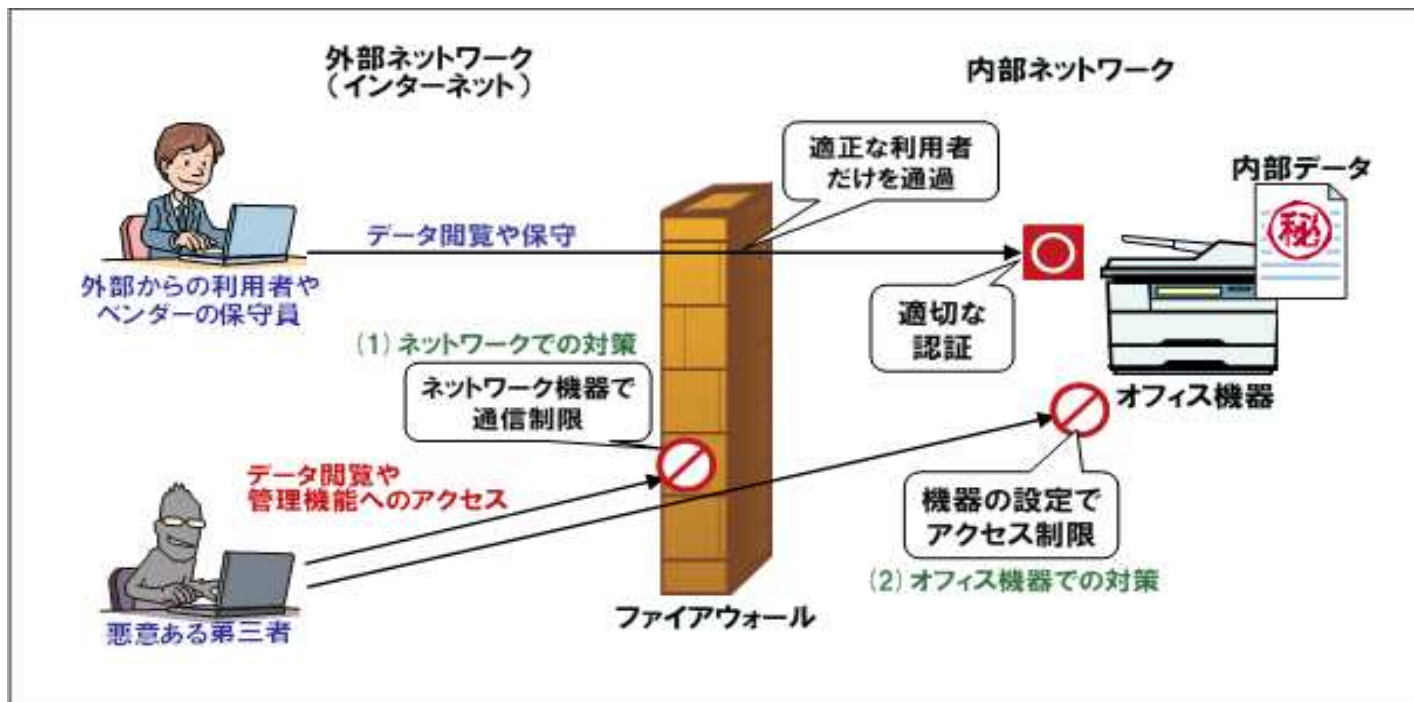
- コンシューマ製品は接続端末数は数台が限度
- 企業利用はエンタープライズ製品を選ぶ必要がある

# ■ 最近のセキュリティ脅威事例



2013年11月、国立大学をはじめとする複数の大学の複合機からの個人情報を含む情報漏えいが報じられたことを受けて独立行政法人情報処理推進機構（IPA）が注意喚起のためプレス発表した

## 複合機等のオフィス機器をインターネットに接続する際の注意点



Source : IPA

<http://www.ipa.go.jp/about/press/20131108.html>

# ■境界内のセキュリティ脅威事例



- テレビや冷蔵庫などスマート家電から大量不正メール送信（2014年1月）  
<http://www.proofpoint.com/about-us/press-releases/01162014.php>
- Androidを乗っ取ってボットネットを構築する凶悪な「Obad（オーバッド）」（2013年6月）  
[http://www.securelist.com/en/blog/8131/Obad\\_a\\_Trojan\\_now\\_being\\_distributed\\_via\\_mobile\\_botnets](http://www.securelist.com/en/blog/8131/Obad_a_Trojan_now_being_distributed_via_mobile_botnets)

## 外部は堅牢だが、内部はもろい

“クリティカルなリソースをネットワークの内側から攻撃する戦略が例外ではなく、当たり前になりつつあることを示しており、組織は境界だけでなく内部のトラフィックについても脅威がないかどうか漢詩する必要に迫られることとなります。”

Palo Alto Networks

“アプリケーションの使用および脅威分析レポート

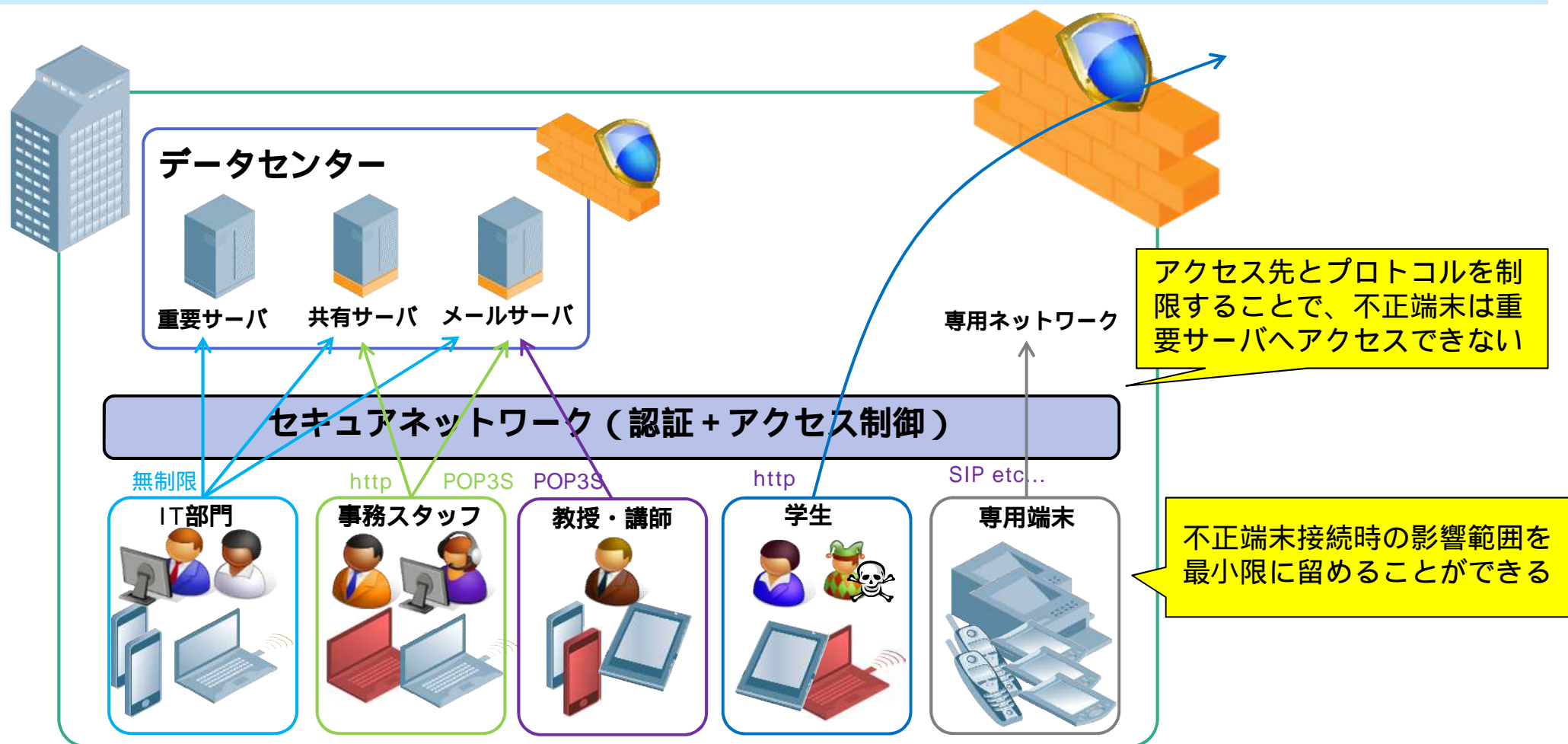
企業におけるアプリケーションの使用とそれに伴う脅威の分析

第10版、2013年2月” より抜粋

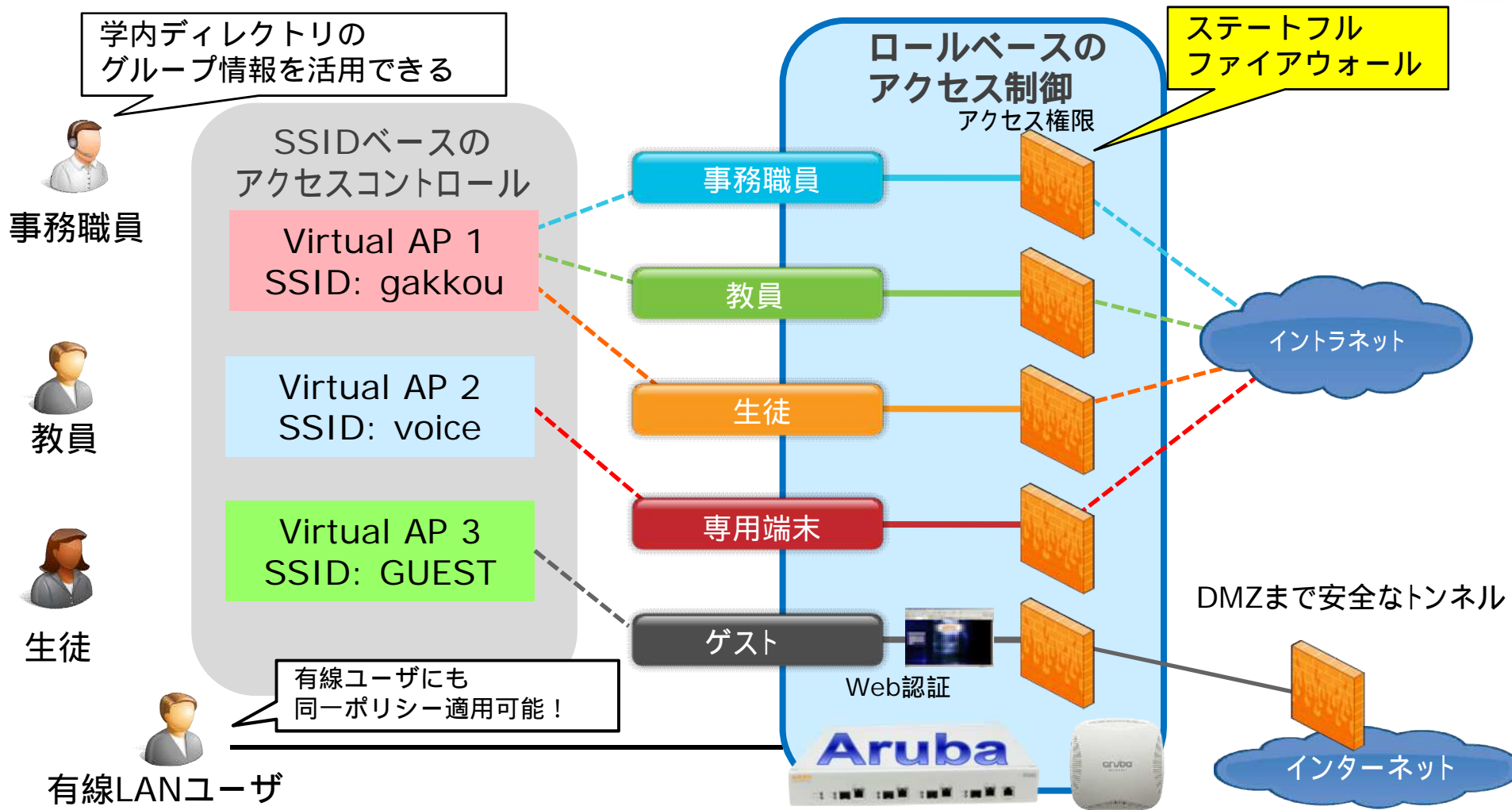
# LAN内のアクセス制御の実装イメージ



**認証**：誰が、どの端末で、どこからアクセスしているかをネットワークが識別  
**アクセス制御**：ユーザ、端末毎に**必要最小限の宛先だけ**にアクセスを許可



# ArubaのRoleベースのアクセス制御



学内ディレクトリと連携しRole (ユーザグループ) 毎のアクセス制御を簡単に実現  
もちろんユーザがどこに移動しても、同じポリシーでのアクセス制御が可能

# ■ ファイアウォールの活用例： 簡単なWindows XP・ゲーム機対策ネットワーク

- Aruba Controllerは**ファイアウォールを内蔵**しており、Role Base のアクセス制御が可能
- DHCPのFingerprintを使い、端末のOSを識別し、OS毎にRoleを割当てることが可能
- Windows XPだけ学内ネットワークにアクセスさせないネットワークを容易に構築できる
- ゲーム機などを繋がせないようにすることも可能



## DHCP Fingerprintの例：

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3084686370636420342E302E3135
BlackBerry	Option 60	30426D61636B4265727279
Windows 7/ Vista Desktop	Option 55	37010f03062c2e2ff1f2179f92b
Windows XP(SP3, Home, Professional)	Option 55	37010f03062c2e2ff1f21f92b
Windows Mobile	Option 60	3c4d6963728f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OSX	Option 55	370103060f775ffc2c2e2f

# Wi-Fiの認証方式の特徴



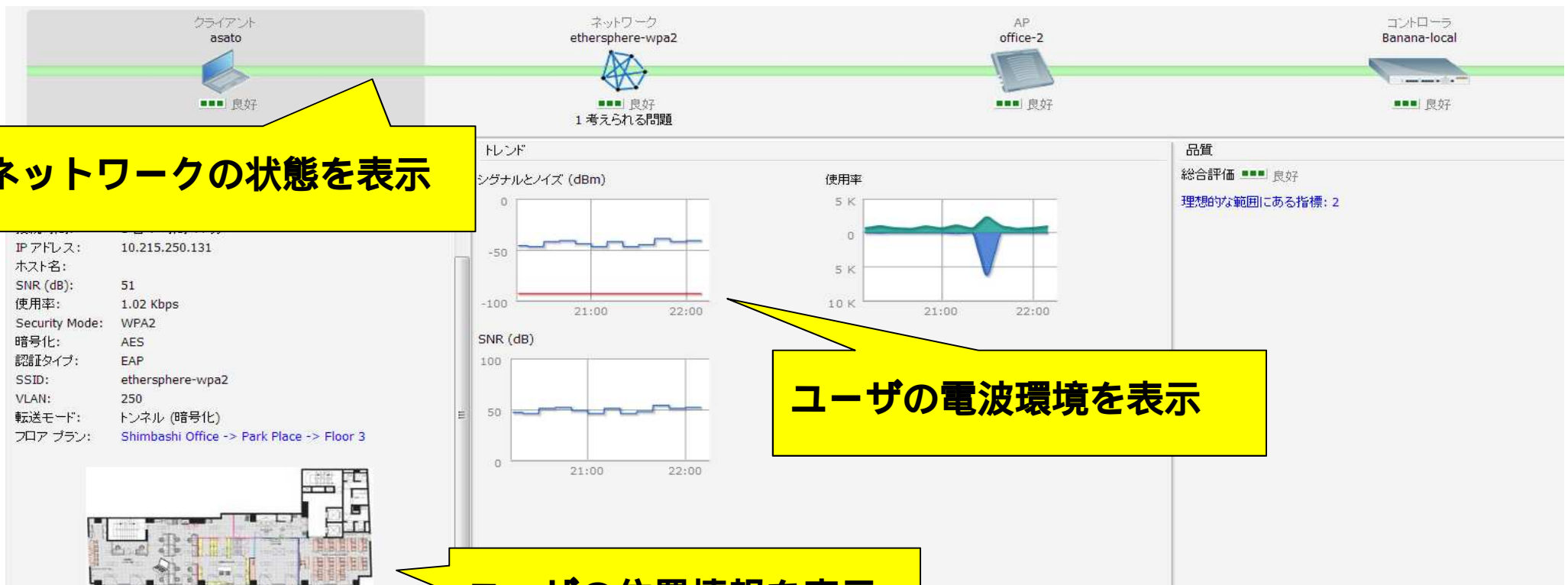
種類	認証対象	実装	セキュリティ	特徴
PSK	共有鍵 認証では無い	易	低	共有鍵が漏洩したら不正アクセスだけでなく、暗号化トラフィックも簡単に解読されてしまう 鍵変更時に全てのユーザに通知しないといけない
MAC 認証	MACアドレス	中	中 暗号化は無い	無線クライアントの認証機能がない場合に利用 MACアドレスは簡単に偽造できる
Web 認証	ユーザ名・パスワード	中	中 暗号化は無い	ブラウザができれば端末は問わない
802.1x EAP-PEAP	サーバ証明書・ ユーザ名・パスワード	中	高	比較的手軽に利用が可能だが、端末が対応している必要がある。
802.1x EAP-TLS	サーバ証明書 クライアント証明書	難	高	無線クライアントに証明書のインストールが必要。証明書/CAのための追加費用が必要 証明書インストール後はユーザはWi-Fiに接続するだけ

- 盗聴されない安全なWi-Fiには802.1xが必須
- ユーザの利便性を取ると、クライアント証明書を使ったEAP-TLSが望ましい

# AirWave統合監視システムによる ネットワークサービスの状態を「見える化」



- ユーザに提供しているネットワークサービスがどうなっているかを一括表示、確認することが可能に
- 一目で問題箇所がわかり迅速なトラブルシューティングを実現！



ネットワークの状態を表示

ユーザの電波環境を表示

ユーザの位置情報を表示



# 統合監視システム活用例 ～障害時の対応～



## ユーザを検索

- ユーザから通信障害の連絡を受ける
- ユーザ (or 端末) を検索し一覧から選択する

検索BoxにユーザID、又はMACアドレスを入力

検索結果の一覧を表示

名前	MACアドレス	IPアドレス	デバイスタイプ	AP	接続時間	モード	フロアプラン
sato	18:00:20:07:07:18		Android	server-room	16日 6時間 16分	1.1n 2.4 GHz	
sato	44:6D:57:3D:0C:07		Windows 7	office-1	30日 15時間 12分 9秒	1.1n 5 GHz (80)	
sato	7C:01:C3:85:86:2E		Apple Mac	office-2	1日 17時間 2分	1.1n 5 GHz (80)	

## ネットワークの状態を確認

- 経路上のネットワーク機器に問題が無いか一気通貫で確認
- 電波状況もグラフで確認
- 電波が弱ければMAPを確認

問題機器があれば赤く表示される

受信電波が弱いので、クライアントの位置を確認してみる

## 問題箇所を調査

- MAP上で端末がどのAPに繋がっているか一目で確認

近くのAPに繋がっていないことがすぐ分かる  
ローミング閾値を要調整

# 統合監視システム活用例 ～日常監視、レポート～



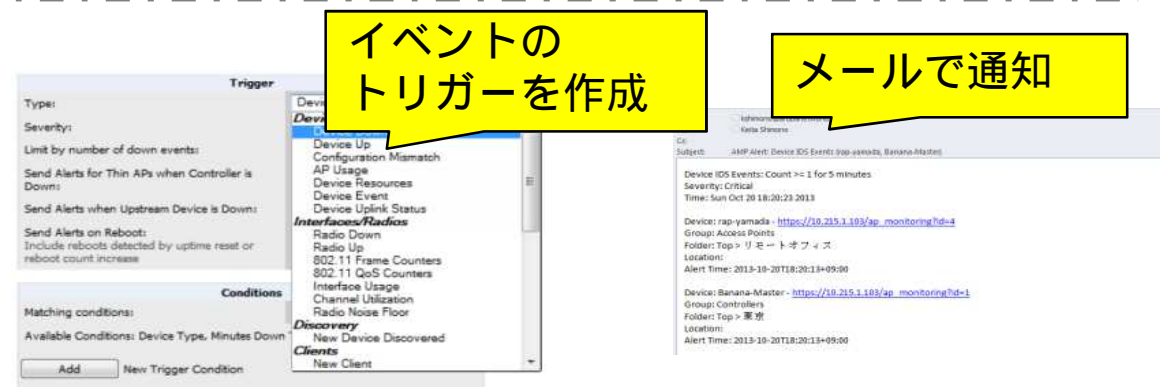
## 問題箇所の調査

- 全ユーザの電波環境、パフォーマンス状況を確認。数値の低いユーザがいれば詳細を確認
- ネットワークの傾向調査等で問題箇所があれば詳細を確認



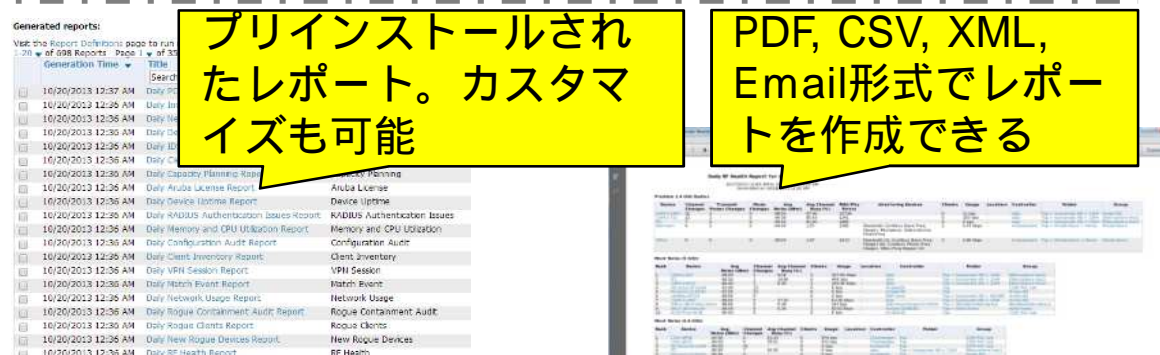
## イベント発生時にメールで通知

- 様々なイベント（デバイスダウン、不正APの検知等）の発生をトリガーにメールで管理者に通知
- メール内のリンクをクリックし、詳細を調査



## 管理状況の定期レポートを作成

- 定期レポートを作成し、社内報告に活用



# ■ AppRFによるアプリケーション通信の最適化

クラウドおよび  
コラボレーション・アプリの可視  
化と制御  
(アプリ数1,500以上)

DPIを使用する次世代  
モビリティ  
ファイアウォール

3<sup>rd</sup> Party  
システムとも連携



SDN  
API





**UNIADDEX**  
YOUR ICT FORCE