

公衆無線LANセキュリティ分科会

公衆無線LANの環境整備の在り方

2017年11月24日

コーデンテクノインフォ株式会社

エブリセンスジャパン株式会社

IEEE802.11 TGai チェア 真野 浩

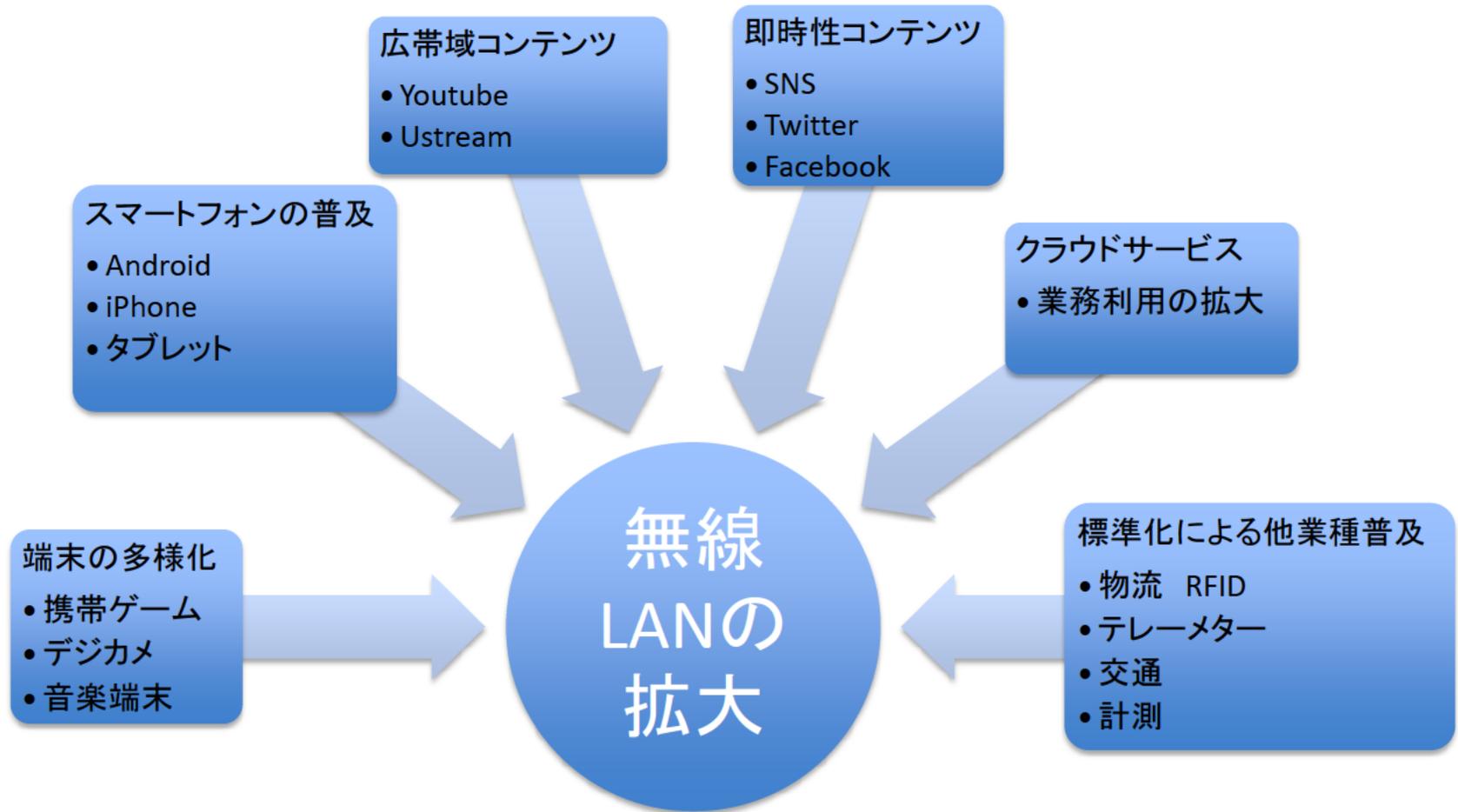
Agenda

- 無線LAN/Wi-Fiとは
- 無線LANの普及と利用範囲
- 無線LANの特長
- 無線LAN固有のセキュリティ課題
- 無線LANセキュリティ保護と対象
- 無線LANの導入での評価指針例
- 無線LANの最近の課題
- 無線LANの標準技術動向
- 無線LANの高密度環境での事例
- 最新業界動向
- まとめ

無線LAN/Wi-Fiとは

- IEEE802.11
 - 無線LANの世界標準規格。
 - IEEE802.11a/b/g + l, u 等で示される
 - 2.4GHz及び5GHzを使い、利用者に従事者免許が不要。
 - 非占有、専用電波を利用。
- Wi-Fi
 - Wi-Fi Allianceによって無線LAN機器間の相互接続性を認証されたことを示す名称。
 - Wi-Fi Allianceによって認定された機器には、Wi-Fiロゴの使用が許可されている。
- 公衆無線LAN
 - 飲食店やビルや商業施設、公共施設、電車内から電柱等に無線LAN基地局を設置し、インターネットサービスを提供する事業、またはサービスの総称。

無線LANの拡大要因



全ての電子サービスに普及

政府行政サービス

- 公衆無線LAN、電子政府

医療

- 電子カルテ、院内通信

水道

- テレメータリング

物流

- RFID、テレメータリング、POS

情報通信

- 電気通信事業、公衆無線LAN

金融

- ネットバンキング、モバイルバンキング

航空

- ラウンジサービス、業務端末

鉄道

- 公衆無線LAN、業務端末

電力

- スマートグリッド

ガス

- テレメータリング

無線LANの特長



- 場所、端末、接続元、接続箇所の特定が困難
- インターネット上の全てのサイトに接続可能
- 誰でも使え、誰でも受信できて、誰でも電波を送受信できる

無線セキュリティ保護の対象

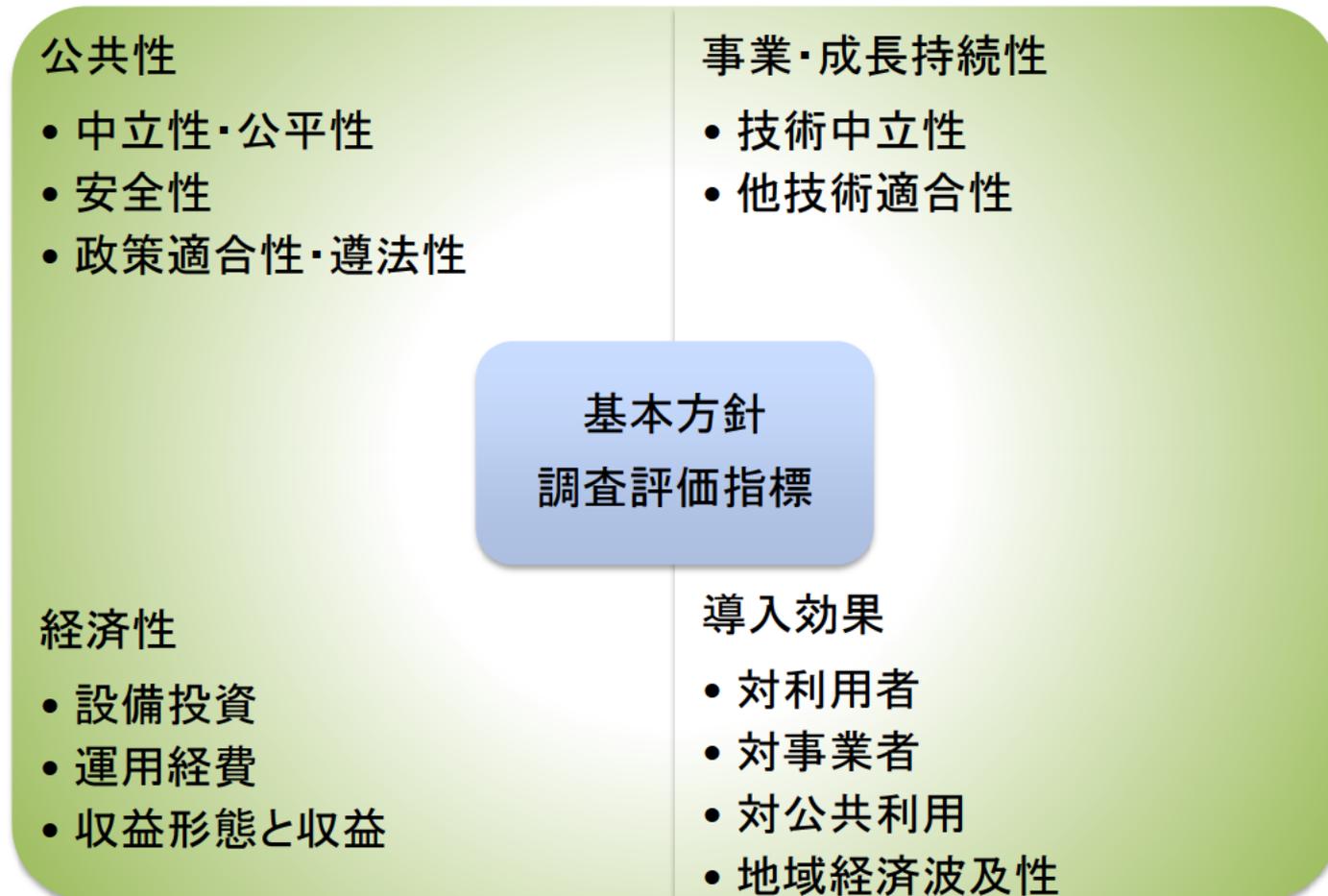
アタックの種類	被害者	対策	提供者責務
盗聴	無線LAN利用者	SSL/VPNの利用	利用者への告知責任
成り済ましアクセス	無線LAN利用者 インターネット側ホスト	WPA2以上の認証	利用者の確認 トレーサビリティ
偽基地局による 通信の搾取対策	無線LAN利用者	WPA2以上の認証	利用者への告知責任
電波による通信妨害	無線LAN利用者 運用者	ステルスID等	サービス品質

- 無線LANのセキュリティアタックは、利用者以外に**全てのネットワークサービスに影響**する。
- 機会提供者は、**利用者認証等のトレーサビリティが社会責務**
- テレメータリグ、IOTの普及にもとない、インターネットと接続される重要な社会インフラが増加しており、アタックによるサービスダウンの棄権性が存在。
- 1x 認証の採用が望ましい。**

基本的な導入評価指標の例

- 四つの評価指標。

- 無線LANは、共用電波(コモンズ)を利用することに留意。
- 既に、多数の民間/個人/公共利用が先行していることに留意



評価指標1 公共性

- 公共性

- 中立性・公平性

- 事業者に対する、中立性・公平性
 - 利用者に対して、中立性・公平性
 - 民業、官業の共存性
 - 公共利用の在り方

- 安全性

- 無線LAN、インターネットアクセスが内包するセキュリティに対する対応
 - 利用者の保護(情報盗聴、登録等個人情報保護、フィッシング対策等、ウィルス感染)
 - ネットワークの保護(不正アクセス、電波干渉保護を含む)
 - インターネットの保護(踏み台によるネットワークアタック対策等)
 - 緊急利用時の優先通信保護

- 政策適合性・遵法性

- 電波法
 - 電気通信事業法
 - 電気通信役務利用放送法
 - 個人情報保護
 - ホワイトスペース、コモンズ拡大などの電波政策との整合
 - コンテンツ、サービス倫理(コンテンツ提供の場合)

評価指標2 事業・成長持続性

- 公衆無線LANの提供＝通信事業の提供
 - 有償, 無償を問わず利用者に安定、継続的な提供
 - 技術要件、管理、運営体制の維持が必要。
- 技術中立性
 - 無線LANは、IEEE802.11/ Wi-Fi Alliance で標準化
 - フォーラム型標準
 - デファクトスタンダード
 - 技術革新が激しいため、機器のライフサイクルで更新発生
 - 技術選択は、供給側ではなく受益者が先導
- 他技術との融合性
 - 3G/LTE/5GとWi-Fiの連動が普及
 - IPv6の普及(IPv4アドレスの枯渇)

評価指標3 経済性

- 整備投資(CAPEX)
 - 機器投資
 - 置局費用(地権交渉～置局工事まで)
 - 上流回線等の導入費用
 - 認証等運用設備等の導入費用
- 運用経費(OPEX)
 - 基地局維持費用(機器保守費用、置局経費)
 - 上流回線運用費用
 - サーバー等運用費用
 - 障害対応費用(含むサポート)
 - 保守維持費用
- 収益形態と収益
 - 公衆無線LAN事業の収益構造の明確化
 - 接続料金収入
 - 関連事業収入
 - エリアポータルサイト
 - デジタルサイネージ

評価指標4 導入効果

住民並びに地域生活、地域産業を豊かにし、ユビキタス社会やICT社会としての利便性等にいかに寄与するか。

－ 対利用者(住民)

- 住民が直接的に享受する利便性。

－ 対事業者

- 公衆無線LAN事業者やインターネット接続事業者、ASP等のサービス提供者が享受する導入効果。

－ 対公共利用

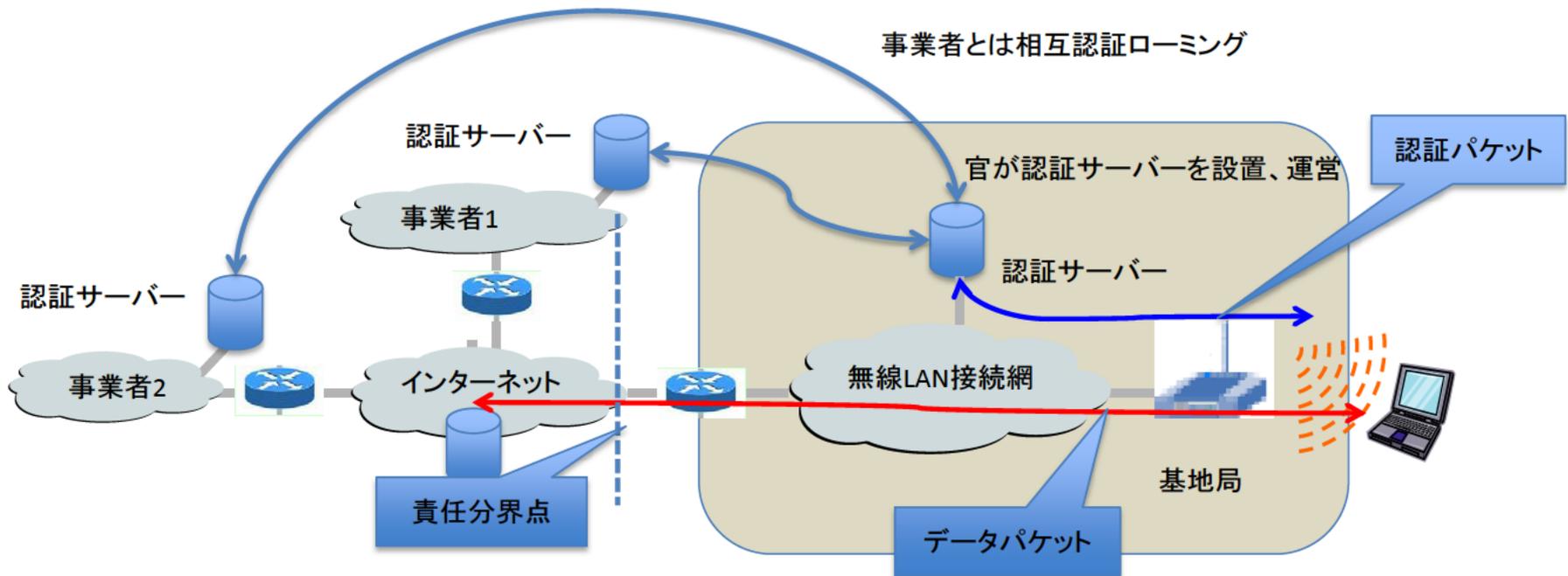
- 各種行政サービス、緊急通信等、行政自らが利用者として、公衆無線LANの整備によって得る効果
- 観光政策、広報戦略等の対外的利用、行政機関間のイントラ的利用、緊急通信網利用による効果。

－ 地域経済への波及性

- 観光、地域産業活性等、域内産業に対して、公衆無線LANの整備が与える導入効果。
- デジタルサイネージとの関連事業などによる、新規ビジネス創出効果。

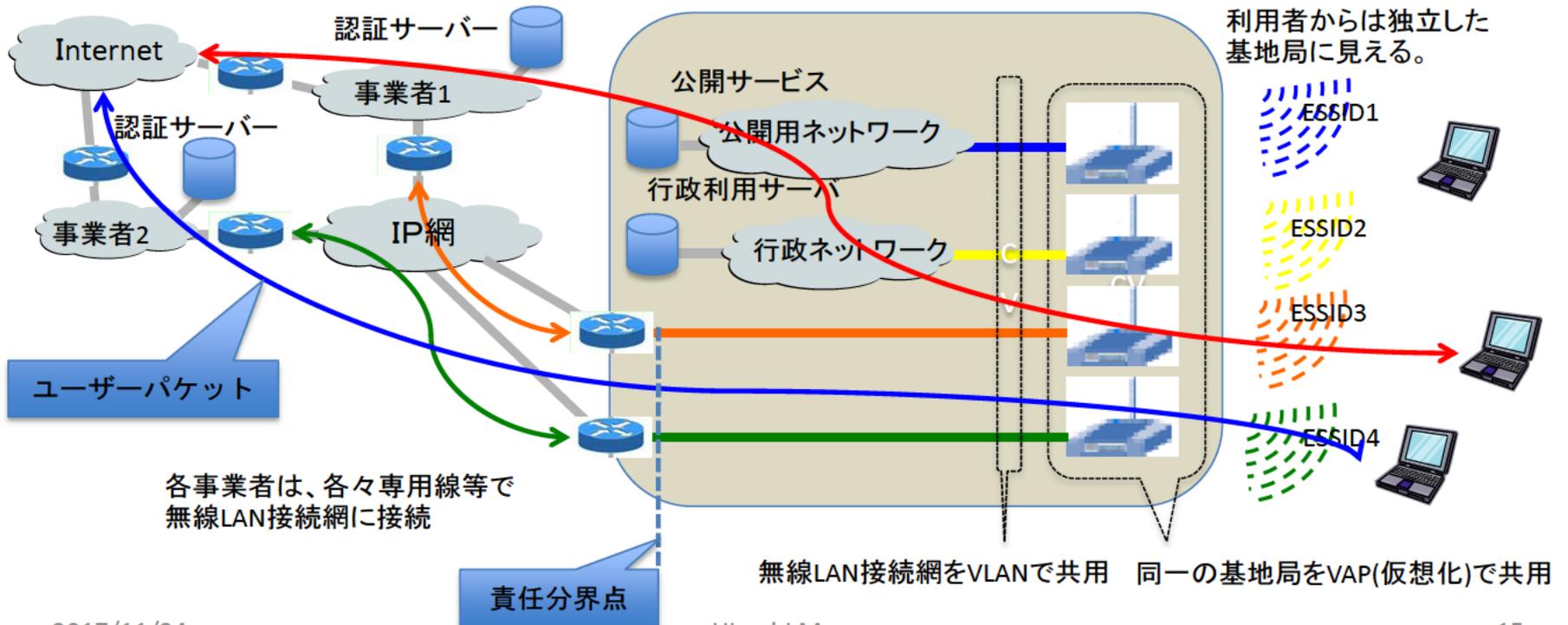
ローミング型

- 官設置の認証サーバーと事業者の認証サーバーで、ローミング
- 一次認証、セキュリティポリシーは、官が運用
- 事業者とのローミング方式等は、個別調整
- 利用者のトラフィックは、直接インターネットへ接続



バーチャル型

- VAP(仮想AP)とVLAN(仮想LAN)で、設備共用
- 各事業者は、専用線とルーターで、接続点まで接続
- 全てのユーザートラフィックは、事業者ネットワークにトンネリングされる
- 行政利用、公開サービスなどは、事業者ポリシーと分離して運用可能
- WEB認証は、公開用ネットワークなどに閉じる



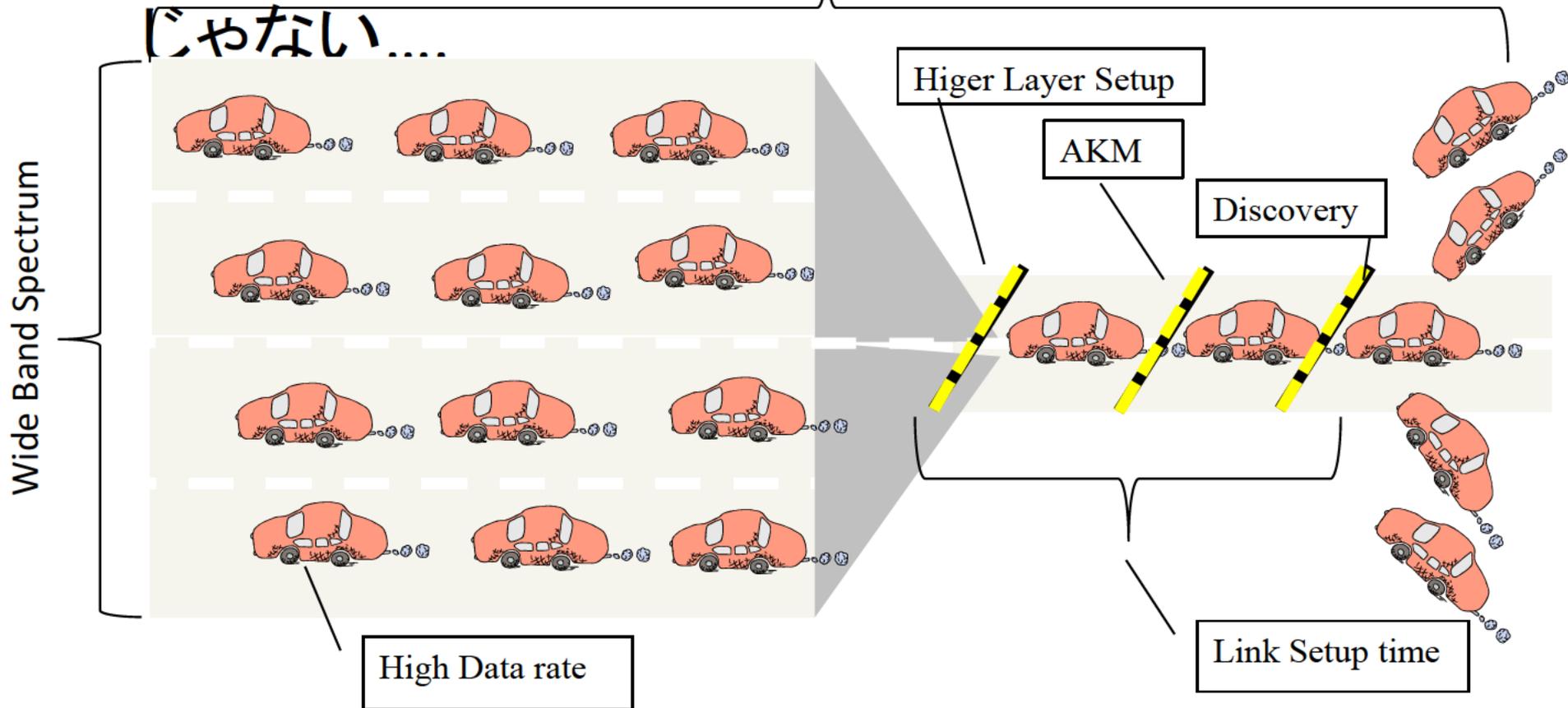
設置・運営費用の負担事例

- 設置費(CAPEX)
 - 機器費
 - 置局費
 - 地権交渉～置局工事
 - 上流回線等の導入
 - 認証等運用設備等導入
- 運用経費(OPEX)
 - 基地局維持費
 - 機器保守費用、置局経費
 - 上流回線運用費
 - 運用費
 - 障害対応、保守維持費

分担項目	IRU型	ローミング型	バーチャル型	備考
基地局 設置	官	官	官	基地局間接続網含む
基地局 運用	民	官	官	基地局間接続網含む
認証サーバー設置	官	官	民(複数)	
認証サーバー運用	民(単一)	官	民(複数)	
上流回線設置	官	官	民	
上流回線運用	民(単一)	官	民	
公共利用用認証サーバーは、いずれの場合も官が設置、運用。				

無線LANの乱立による非効率性

- つながりにくい、つながらない、希望したものじゃない....



公衆無線LANの現状 なぜ、つながりにくいのか？

- Time/Date: Around 18:00 / October 11(Tue), 2011
- Location: Shinjuku station (Keio line), Tokyo
- Monitoring CH: 6CH(2,437MHz)
- Monitoring period: 300 seconds (5 minutes)



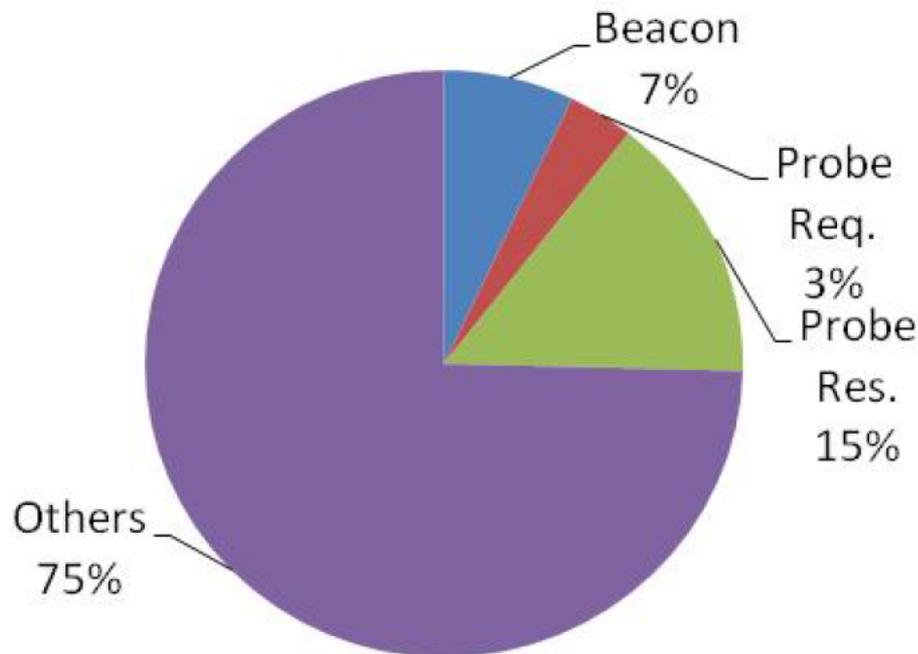
↑ Measured CH

<Equipment>

- Thinkpad X200
- Windows XP
- USB Wireless Monitor Adaptor (Air Pcap NX)
- Wireshark

時間占有率

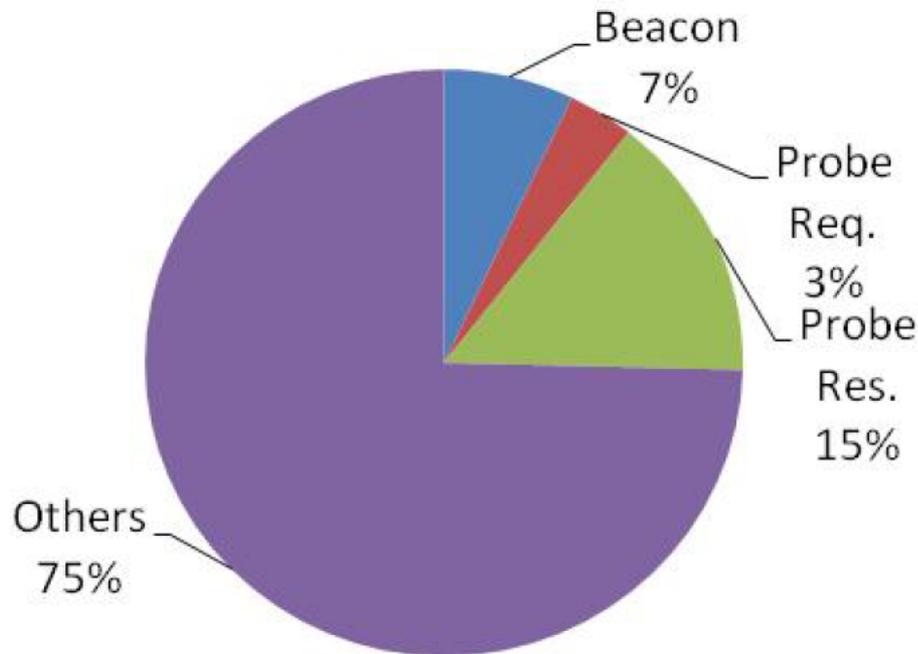
- 実に1/4の時間は、ビーコンとプローブパケットが消費している。



Packet type	Occupancy rate (%)	Occupied time (sec)
Beacon	7.06	21.17
Probe Req.	3.58	10.75
Probe Res.	14.74	44.22
Others	74.62	223.86
Total	100.00	300.00

時間占有率

- 実に1/4の時間は、ビーコンとプローブパッケージが消費している。



Packet type	Occupancy rate (%)	Occupied time (sec)
Beacon	7.06	21.17
Probe Req.	3.58	10.75
Probe Res.	14.74	44.22
Others	74.62	223.86
Total	100.00	300.00

Characterization of Rio Tinto Stadium Environment

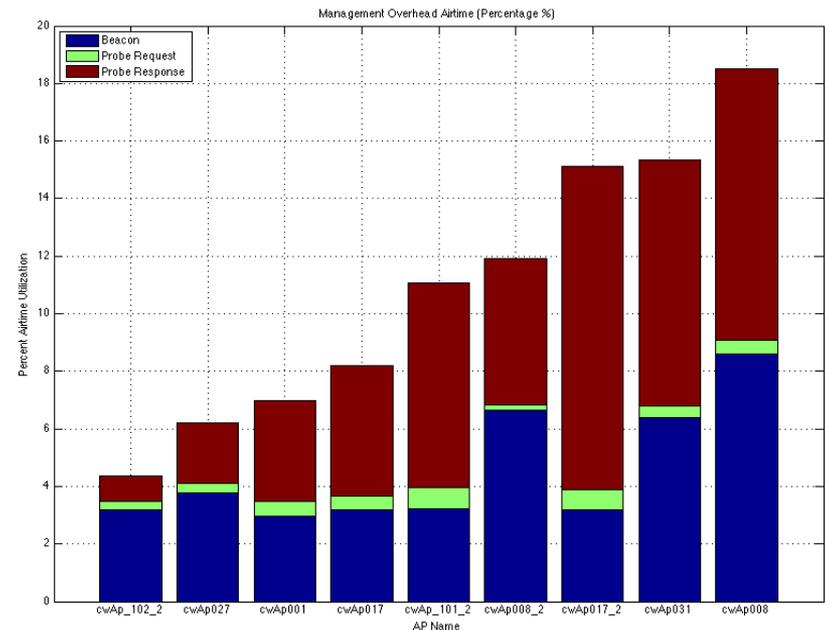


We analyze WiFi data sniffed in this environment and take it to be representative of a High Density WiFi installation.

- Salt Lake City Soccer Stadium
 - ~80APs in bowl
 - ~105APs total (for concessions and infrastructure)
 - ~20k seat capacity
 - ½ Full during testing -> ~10k clients

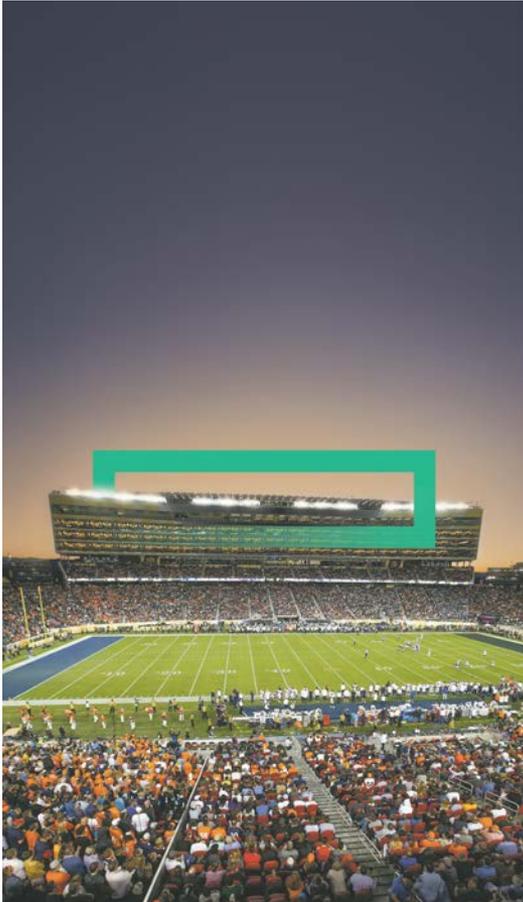
Airtime Utilization in High Density Environment

- Management Traffic can consume substantial amounts of airtime.
 - Beacons up to 8-9%
 - Probe Responses up to 9-10%
 - Probe Requests $\frac{1}{4}$ - $\frac{3}{4}$ %
- Utilization depends on AP placement
 - APs placed in the center of the stadium hear more clients and other APs.



IEEE802.11の高密度環境での実現事例の現状

Actual use case of IEEE802.11 in High Dense area



- The result was an awesome fan experience. Working with Aruba, a Hewlett Packard Enterprise company, event organizers were able to deliver for the big game. A wireless network of over **1,300 Wi-Fi access points** and **1,200 Bluetooth beacons** allowed the **70,000 plus fans** in the stadium to find their seats, send thousands of selfies and even order food to their seats over the network. It's exactly what you'd expect from a global leader in wireless networking—hosting the world in the heart of Silicon Valley. To see how your business can change the game with Aruba, visit us at hpe.com/gamechanger
- © Copyright 2016 Hewlett Packard Enterprise Development LP. © Copyright 2016 Levi's® Stadium. All Rights Reserved.

Super Bowl 50 use case

High Density Wi-Fi Design: How to Deliver 10 TB of Fan Wi-Fi at the Big Game

Total Data Transferred on Wi-Fi
10TB+

Beats Every Past Big Game by 60%+

Unique Wi-Fi Users
28.6K
40% of Attendance

Beats Every Past Big Game

Concurrent Wi-Fi Users
20K+
28% of Attendance

Big Game and Venue Record

Continuous Wi-Fi Bandwidth > 3Gbps
4h 0m

New league record!

Average Data Consumed per Fan
370MB

54% higher than 2014 Big Game

The first Big Game to Deliver Indoor Navigation

Stadium App

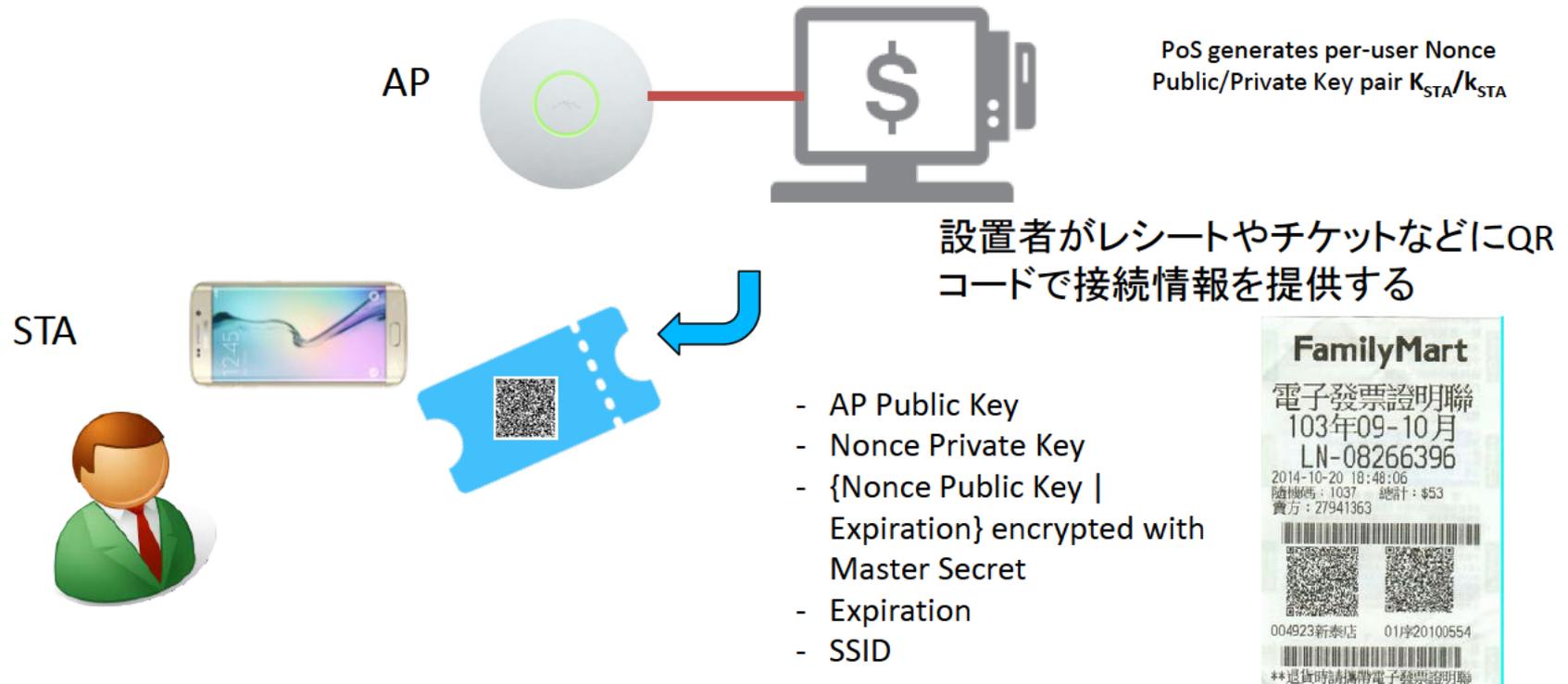
業界動向(Wi-Fi Alliance)

● 認識されている課題

- WPA2/.1xの導入には、運営者に相応のシステム構築が必要

● 課題解決

- 簡便でセキュリティを確保できる手法の提案と要件整理



Next generation Wi-Fi connectivity



Prepared for Hiroshi Mano
November 2017

Topics

- Wi-Fi Alliance[®] overview
- Wi-Fi[®] industry update
- Wi-Fi programs benefiting the next generation networks
- Wi-Fi CERTIFIED Vantage[™]
- Upcoming Wi-Fi capabilities

Wi-Fi Alliance overview



The worldwide network of companies that brings you Wi-Fi



*Effective
collaboration*

*Diverse ecosystem:
800+ companies*



*Wi-Fi CERTIFIED™
evolution*

*Driving
industry growth*

An aerial photograph of a vast body of water, likely a bay or a large lake, with several small islands scattered across the surface. In the background, a range of mountains is visible under a sky filled with soft, white clouds. The overall color palette is muted, with blues, greys, and whites.

***Wi-Fi Alliance Vision:
Connecting everyone and
everything, everywhere***



Wi-Fi Alliance members collaborate to...

Address obstacles to market growth

Develop Wi-Fi technologies

Define a Wi-Fi roadmap

Ensure Wi-Fi interoperability

Advocate globally for spectrum

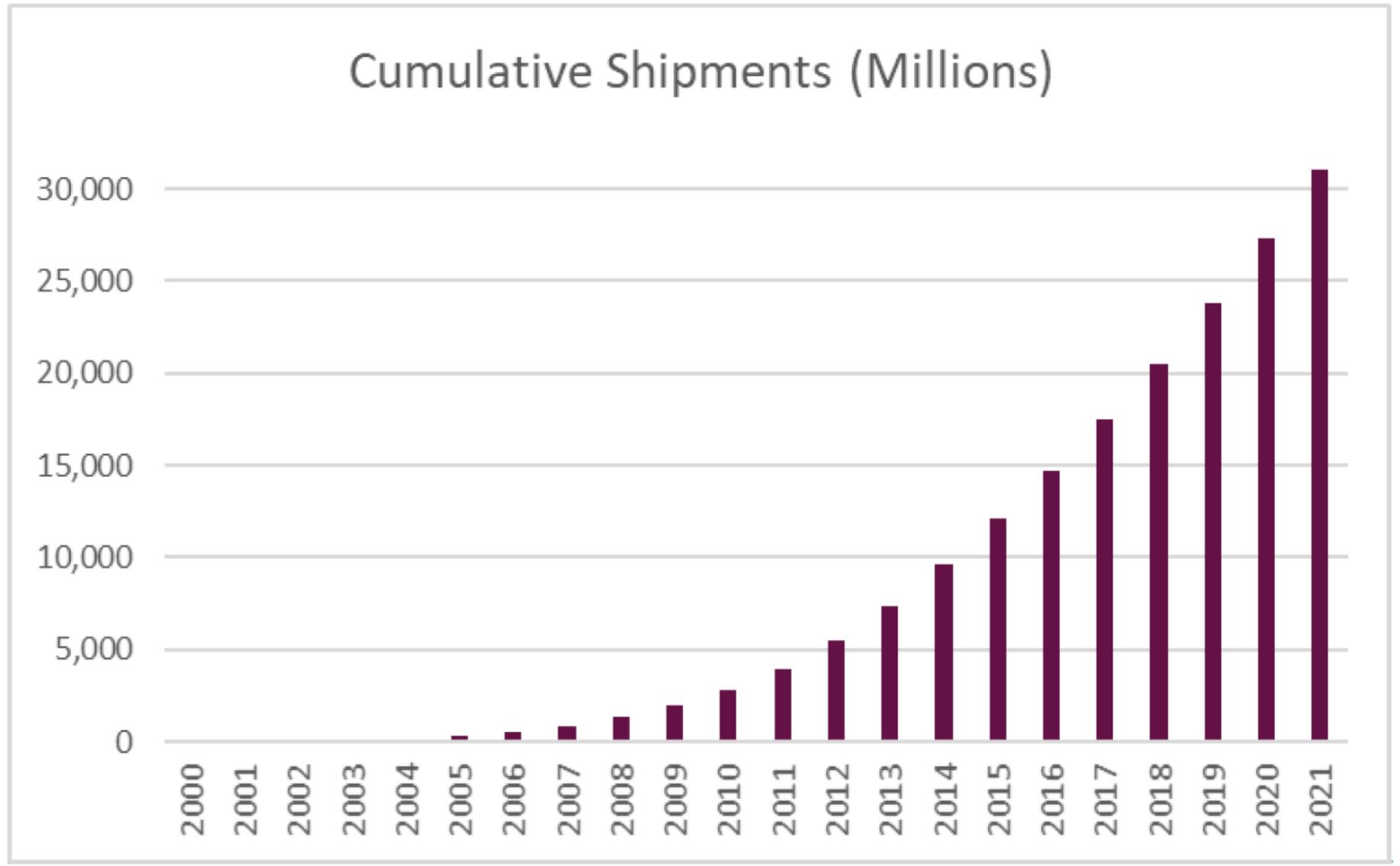


Wi-Fi industry update



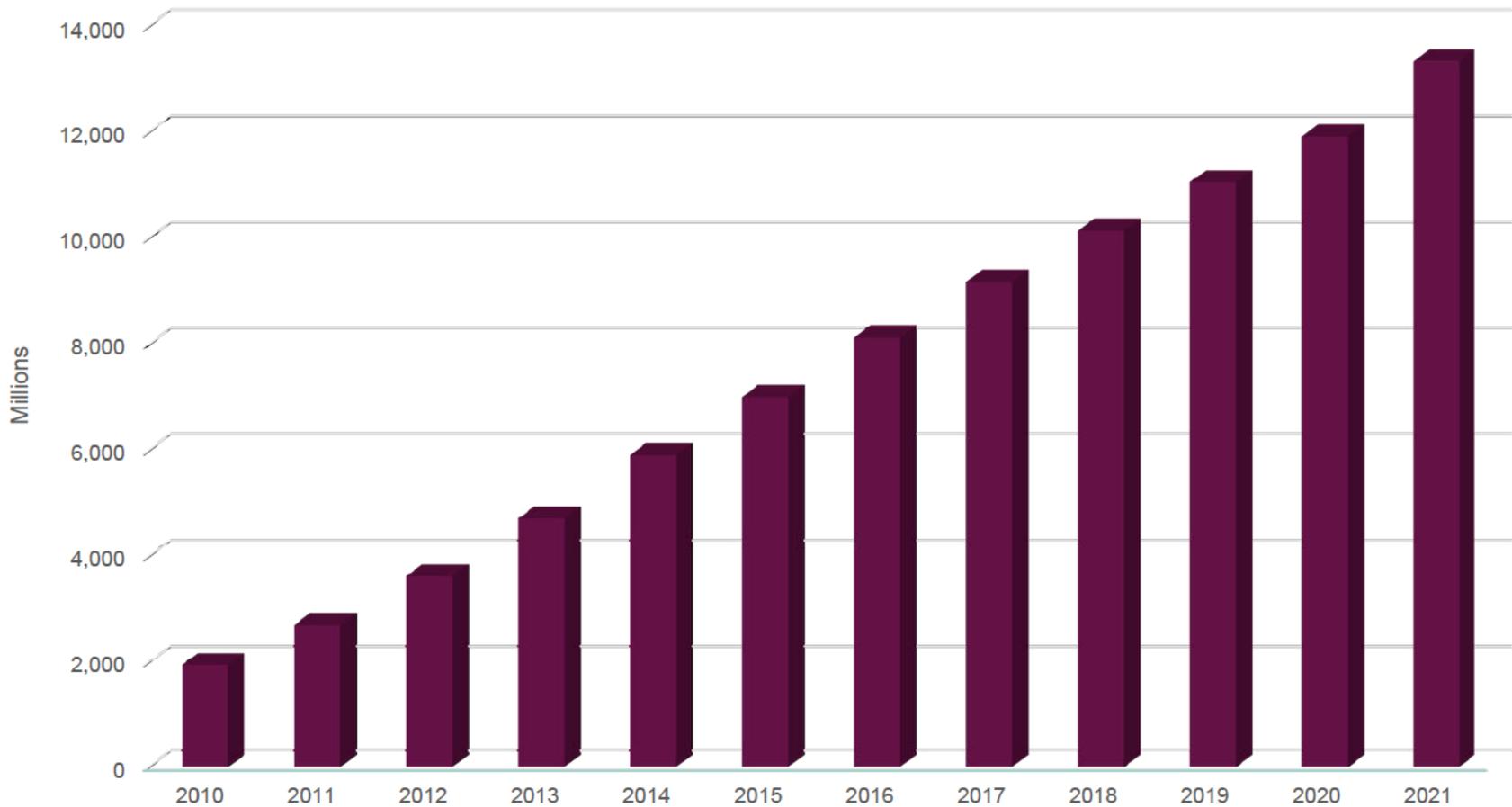


Cumulative Wi-Fi shipments by year



Wi-Fi installed base

Wi-Fi® Device Installed Base
ABI Research, January 2017



Wi-Fi is one of the greatest success stories of the high tech era



- Eight billion devices in use
- Three billion shipments a year
- Continued innovation
- Carries more than half of all internet traffic
- [End user affinity](#)



Wi-Fi CERTIFIED programs for next generation connectivity



Wi-Fi CERTIFIED™ ac

State of the art Wi-Fi performance, capacity, and efficiency

- Evolutionary throughput improvements with wave 2 features
- MU-MIMO: simultaneous communication among devices improves efficiency, capacity, and throughput
- 160 MHz operation doubles speeds for data intensive applications



Wi-Fi CERTIFIED WiGig™

High-performance Wi-Fi at 60 GHz

- Multi-gigabit capability for line-of-sight applications requiring high throughput
- Entertainment: Download HD movies in seconds; provide immersive AR/VR experiences
- Metropolitan backhaul: Bring core functionality for outdoor devices with 60 GHz infrastructure
- Public kiosks: Enable customers to obtain products or services quickly and securely over Wi-Fi



Wi-Fi CERTIFIED TimeSync™

Precisely synchronized audio, video, and data

- Sub-microsecond synchronization among multiple Wi-Fi devices
- Accurate representation of audio, video, or data
- In-room multichannel audio and video capabilities
- Infrastructure and peer-to-peer modes



Wi-Fi CERTIFIED Miracast™

Easy-to-use, multi-vendor content display

- High-resolution multimedia content display between devices
- Eliminates need for cables without sacrificing quality
- Supports high-definition (HD) and 4K Ultra HD formats
- Operates through existing Wi-Fi networks or leverages peer-to-peer connection through [Wi-Fi Direct](#)
- More than [7000 devices](#) certified



Power saving features

Power efficient Wi-Fi enhancements for IoT and power sensitive applications

- Longer sleep periods reduce connectivity requirements
- Address resolution enhancements limit communications frequency
- Target market segments include smart home, smart city, industrial and healthcare



Wi-Fi CERTIFIED Vantage™ for managed networks



Wi-Fi CERTIFIED Vantage™

Elevated experience in Wi-Fi networks

- Designates devices that provide the best experience in managed networks
- Users will have better experience in stadiums, airports, train stations, hotels, and homes
- Aggregates advanced features of [Wi-Fi CERTIFIED Passpoint®](#), [Wi-Fi CERTIFIED™ ac](#), [Wi-Fi CERTIFIED Agile Multiband™](#), and [Wi-Fi CERTIFIED Optimized Connectivity™](#)
- Improves network resource management and seamless roaming
- Enables [“neutral host”](#) deployments



[Wi-Fi Vantage™ highlights](#)

Wi-Fi Vantage™ improves resource management and user experiences in managed networks



High performance,
dual-band operation

Secure, light-touch authentication

Wi-Fi Vantage™

Efficient use of spectrum,
smart steering

Improved roaming,
efficient transmissions

*Wi-Fi Vantage advances are based on
three pillars to deliver enhanced
managed network capabilities:
mobility, manageability, and performance*

Wi-Fi Vantage brings common approach to deliver quality experience in carrier networks



Mobility

Steering and transition mechanisms bring seamless user experience:

- Accessing networks
- Inter-network roaming
- Transitioning to and from Wi-Fi to cellular networks

Technologies:

Wi-Fi Agile Multiband
Wi-Fi Optimized
Connectivity

Manageability

Better understanding of network environment and:

- Allocation of resources
- Provisioning
- Authentication
- Intra-network roaming

Technologies:

Wi-Fi Agile Multiband
Wi-Fi Optimized Connectivity
Passpoint

Performance

High level performance in very dense environments:

- MU-MIMO
- Higher data rates
- Dual-band capability

Technologies:

Wi-Fi CERTIFIED ac

Wi-Fi CERTIFIED Passpoint®

Streamlined network access in hotspots

- Seamless “in-pocket” connectivity
- Secure connection via industry-standard security protections
- Standards-based offload and Wi-Fi roaming on billions of smartphones and Wi-Fi-only devices
- Foundational to Next Generation Hotspot roaming: supported by 40+ operators worldwide. Rollouts in EU, APAC, Americas
- Nearly 2000 Passpoint certified devices: view notable products [here](#)



Wi-Fi CERTIFIED Agile Multiband™

Wi-Fi that ensures quality connections by responding to changing conditions

- Dynamic monitoring evaluates the best connection possible
- Intelligent steering uses the best band, channel, or AP to balance traffic or meet network needs
- Fast transitions improve experience with latency-sensitive applications such as voice or video



[Wi-Fi Agile Multiband highlights](#)

Wi-Fi CERTIFIED Optimized Connectivity

Enhanced network connectivity when roaming

- Optimized discovery brings faster network and AP discovery; metrics aid in network selection
- Optimized authentication (FILS Authentication) delivers faster initial authentication and IP layer connectivity
- Efficient transmissions result from reduced management frames, allowing devices to spend less time exchanging management information



Upcoming Wi-Fi capabilities



Device provisioning

A simple and secure way to configure Wi-Fi devices

- For IoT and smart home devices without a user interface
- Simplifies the process of adding devices to a secure Wi-Fi network through use of **QR codes or NFC**
- Supports legacy devices
- Based on Device Provisioning Protocol (DPP) technology



Generational security enhancements coming soon

Next generation Wi-Fi security coming in 2018

- Brings advanced cryptographic algorithms and addresses risky user behavior
- Supports open, personal, and enterprise scenarios
- Wi-Fi security as a “system”
- Decisively moves the industry away from outdated technologies
- Built for quantum computing era



Security enhancements overview by network type



1. **For open networks**, such as coffee shops: delivers user based per-link encryption
 2. **For personal networks**, such as homes: stronger authentication and encryption processes
 3. **For enterprise networks**: cutting edge cryptographic strength with NSA's Suite B
- No impact or learning curve for the end user



Wi-Fi CERTIFIED ax

Made for a new era of extremely demanding Wi-Fi

- Enhancements
 - Better coverage, more density, increased capacity
 - Improved performance at the edge, even among overlapping networks
 - Enhanced power efficiency
 - Latest security (WPA3)
- New protocols and mechanisms such as
 - Resource scheduling OFDMA
 - UL MU-MIMO
 - Dual carrier modulation
 - 1024 QAM
- 2.4GHz and 5GHz operation with backward compatibility

Wi-Fi: cornerstone of connected life now, and into the future



- For much of the world, Wi-Fi defines the network at home, work, school
- Wi-Fi devices and applications will continue to diversify
- We are working on a range of capabilities to delight our users
- Manufacturers can rely on Wi-Fi CERTIFIED™ products to deliver great connectivity for next generation experiences





Thank you!

Get involved in Wi-Fi Alliance

www.wi-fi.org

membership@wi-fi.org

+1 512 498 9434



ご清聴ありがとうございました。