Wi-Fiの最新技術とマーケット動向

2018年11月28日

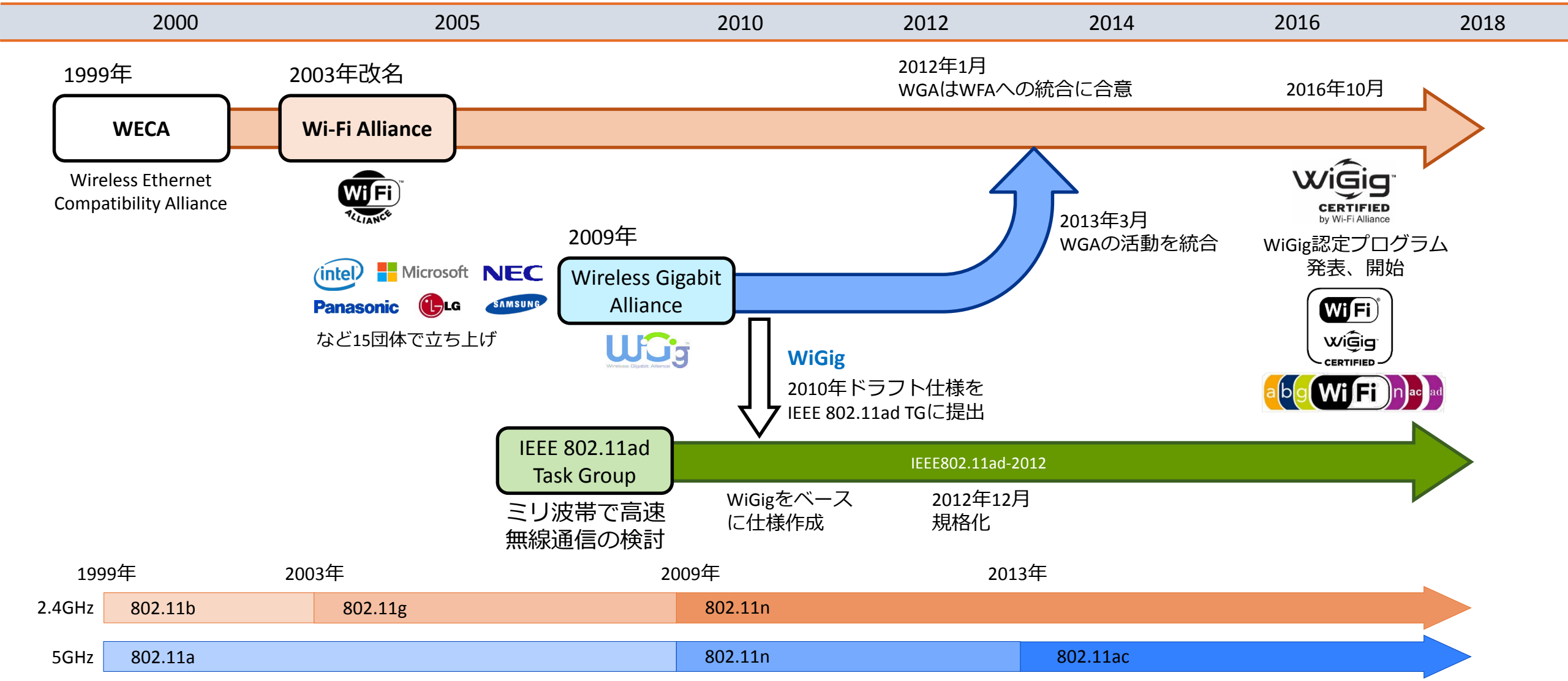
ラッカスネットワークス
テクニカルディレクター
小　宮　博　美

RUCKUS™
an ARRIS company

進化を続ける無線LAN規格

世代	規格名	利用周波数帯(Hz)	最高伝送レート	規格化	
1	802.11	2.4G	2M bps	1997年 6月	
2	802.11b	2.4G	11M bps	1999年 9月	
3	802.11a	5G	54M bps	1999年 9月	
3	802.11g	2.4G	54M bps	2003年 6月	
4	802.11n	2.4G 5G	600M bps	2009年 9月	Wi-Fi 4
5	802.11ad	60G	6,757M bps	2012年12月	
5	802.11ac	5G	6,933M bps	2013年12月	Wi-Fi 5
6	802.11ax	2.4G 5G	10,000M bps	2018年7月 ドラフト	Wi-Fi 6

802.11ad 標準化の流れ



IEEE 802.11ad / WiGig の特徴

- ミリ波帯の**60GHz**を利用
- 60GHz帯は免許不要の帯域で、全世界で利用可能（利用可能周波数範囲は国／地域で異なる）
- **2.16GHz**という非常に広いチャンネルでマルチギガビット／秒を実現
- IEEE802.11ad-2012ではMIMOは定義されていない
- 60GHzの電送波は直進性が高く、回り込みはほとんどない
- 60GHzの電送波は減衰しやすく、高速通信可能な距離は**10m程度**
- 遮へい物を透過しての通信は困難
- ビームフォーミングが仕様に取り込まれている
- 2018年10月末現在 12製品がWiGig CERTIFIED認定されている
- WiGig CERTFIED製品は、802.11adと802.11g/n（2.4GHz）、802.11ac（5GHz）間のシームレスな切り替えができる
- 802.11adと802.11a/b/g/n/ac間で互換性はない
- パソコンとディスプレイ間の映像転送などを主な用途と考えていた

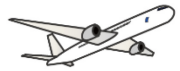
周波数帯ごとの主な用途と電波の特長

物質の電子を電離させることができない電磁波（非電離放射線）

（電離放射線）

物質の電子を電離させることができる電磁波

電波（電波法の定義）



- 船舶、航空機用ビーコン
- 電子タグ

長波 LF

- AMラジオ
- 船舶、航空機通信

中波 MF

- 船舶、航空機通信
- 短波放送
- 電子タグ
- アマチュア無線

短波 HF

- FM放送
- 防災行政無線
- 消防警察無線
- 航空管制通信

超短波 VHF

- 地デジ放送
- 携帯電話
- 無線LAN
- コードレス電話

極超短波 UHF

- マイクロ波中継
- 衛星通信・放送
- 電波天文
- 無線LAN

マイクロ波 SHF

WiGig

- 電波天文
- 衛星通信
- 衝突防止レーダ
- 無線LAN

ミリ波 EHF

可視光線

赤外線

紫外線

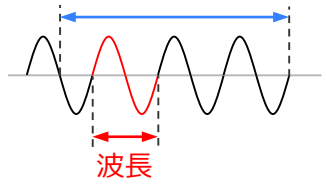
X線　γ線

周波数	3K Hz	10K Hz	30K Hz	300KHz	3MHz	30MHz	300MHz	3GHz	30GHz	300G Hz	3T Hz	3000THz
波　長	100 km	30 km	10 km	1 km	100 m	10 m	1 m	10 cm	1 cm	1mm	0.1mm	0.1μm

低　い　←　周　波　数　→　高　い

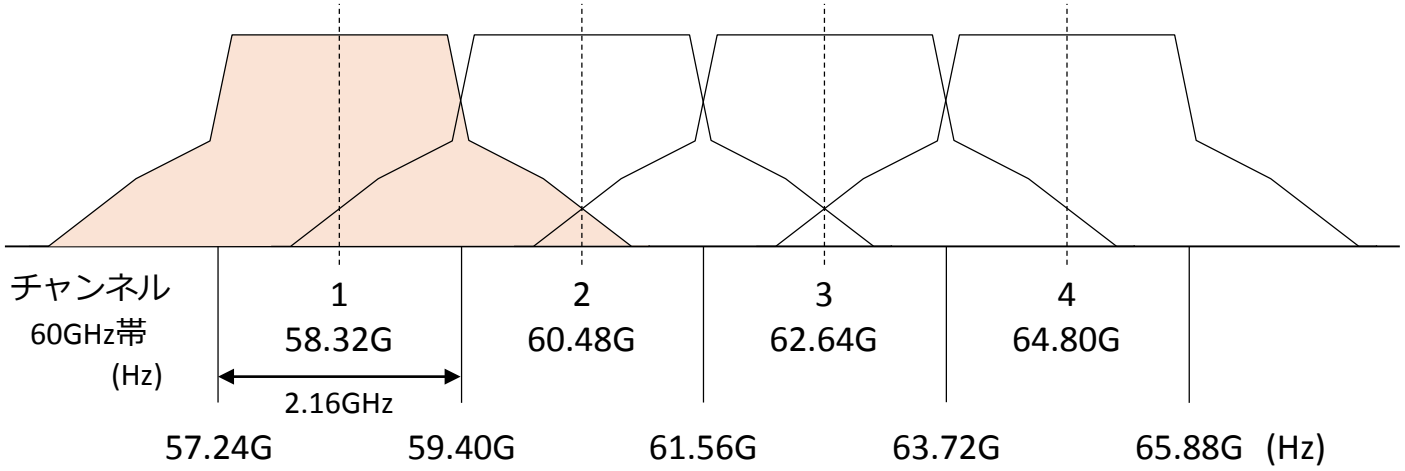
長　い　←　波　長　→　短　い

回り込む　←　電波の伝わり方　→　直進する

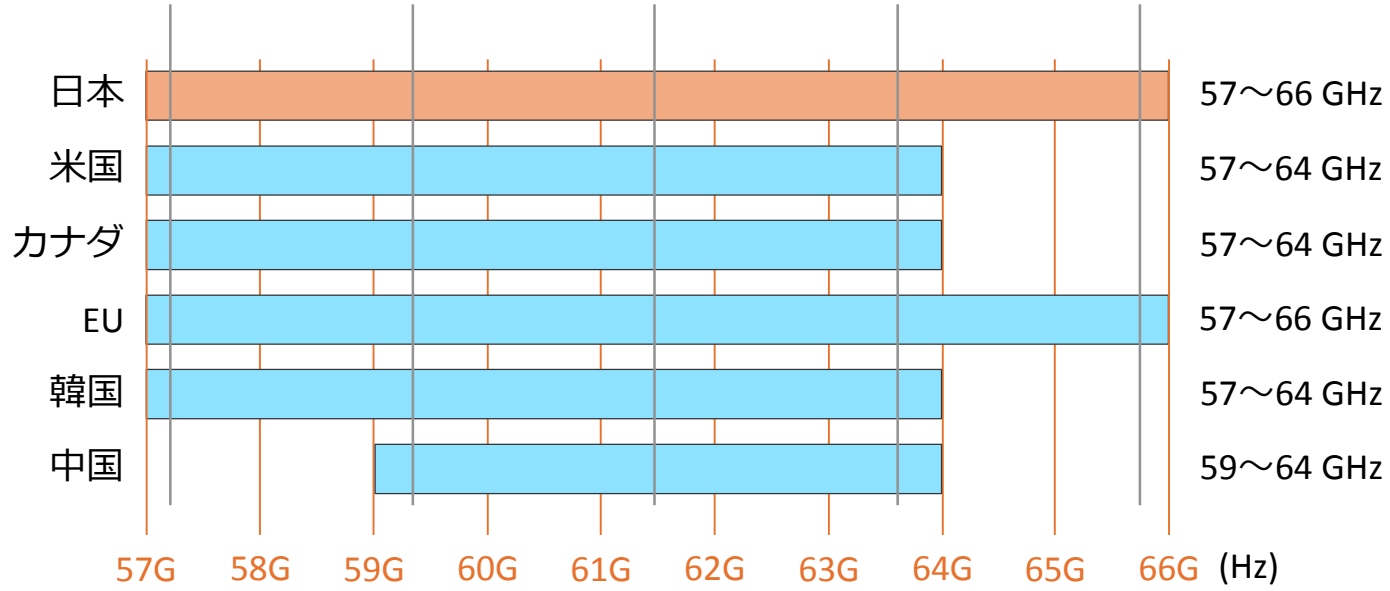


60GHz帯のチャンネル割り当て

802.11ad
チャンネル



各国の
周波数割り当て



60GHz帯無線システムの技術的条件

2015年11月　電波法施行規則の一部が改正

	60GHz帯小電力データ通信システム 10mW以下	60GHz帯小電力データ通信システム 10mW超え
周波数	57～66 GHz	57～66 GHz
単位チャンネル	規定なし	規定なし
無線チャンネル	規定なし	規定なし
空中線電力	10dBm以下	**10dBmを超え24dBm以下**
等価等方輻射電力	規定しない	**40dBm以下**
空中線利得	47dBi以下	**空中線電力10dBmを超える場合は最大方向10dBi以上**
変調方式	規定しない	規定しない
キャリアセンス	規定しない	**キャリアセンスによる干渉低減機能を有すること**
占有周波数帯域	**9GHz以下**	**9GHz以下**
不要発射の強度の許容値	**55.62GHz未満: -30dBm/MHz以下** **55.62～57GHz: -26dBm/MHz以下** **66～67.5GHz: -26dBm/MHz以下** **67.5GHz以上: -30dBm/MHz以下**	**55.62GHz未満: -30dBm/MHz以下** **55.62～57GHz: -26dBm/MHz以下** **66～67.5GHz: -26dBm/MHz以下** **67.5GHz以上: -30dBm/MHz以下**
空中線電力の許容偏差	上限50%、 下限70%	上限50%、 下限70%
周波数の許容偏差	指定周波数帯または±500ppm	**指定周波数帯または±20ppm**

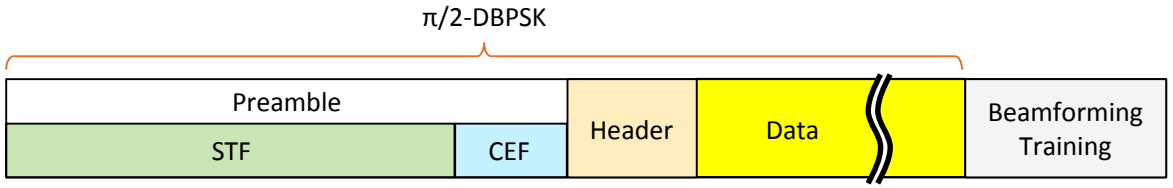
802.11ad modulation-code rate & Frame Type (Mandatory)

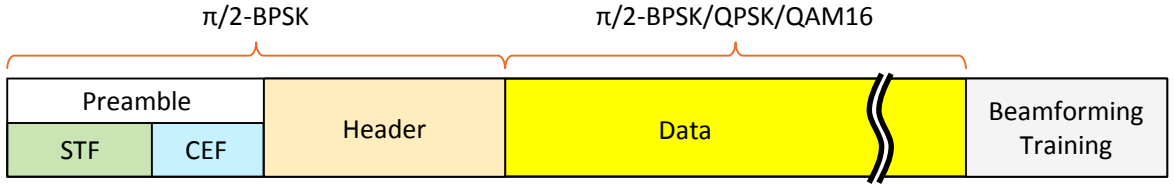
Modulation code rate for **control** PHY

MCS Index	Modulation	Code rate	Data rate (Mbps)
MCS-0	DBPSK	1/2	27.5

Modulation code rate for **Single Carrier** PHY

MCS Index	Modulation	N_{CBPS}	Repetition	Code rate	Data rate (Mbps)
MCS-1	π/2 BPSK	1	2	1/2	385
MCS-2	π/2 BPSK	1	1	1/2	770
MCS-3	π/2 BPSK	1	1	5/8	962.5
MCS-4	π/2 BPSK	1	1	3/4	1,155
MCS-5	π/2 BPSK	1	1	13/16	1,251.25
MCS-6	π/2 QPSK	2	1	1/2	1,540
MCS-7	π/2 QPSK	2	1	5/8	1,925
MCS-8	π/2 QPSK	2	1	3/4	2,310
MCS-9	π/2 QPSK	2	1	13/16	2,502.5
MCS-10	π/2 16QAM	4	1	1/2	3,080
MCS-11	π/2 16QAM	4	1	5/8	3,850
MCS-12	π/2 16QAM	4	1	3/4	4,620





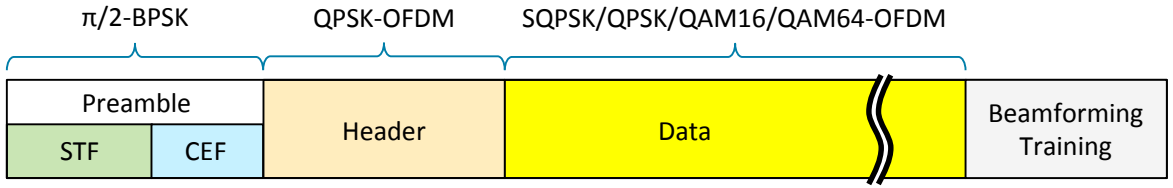
802.11ad modulation-code rate & Frame Type

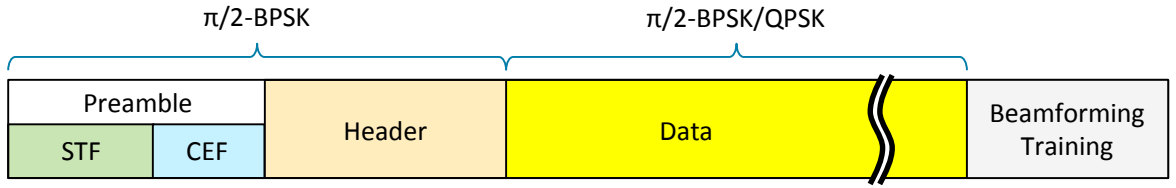
Modulation code rate for **OFDM** PHY

MCS Index	Modulation	Code rate	NBPSC	NCBPS	NDBPS	Data rate (Mbps)
MCS-13	SQPSK	1/2	1	336	168	693.00
MCS-14	SQPSK	5/8	1	336	210	866.25
MCS-15	QPSK	1/2	2	672	336	1,386.00
MCS-16	QPSK	5/8	2	672	420	1,732.50
MCS-17	QPSK	3/4	2	672	504	2,079.00
MCS-18	16-QAM	1/2	4	1,344	672	2,772.00
MCS-19	16-QAM	5/8	4	1,344	840	3,465.00
MCS-20	16-QAM	3/4	4	1,344	1,008	4,158.00
MCS-21	16-QAM	13/16	4	1,344	1,092	4,504.50
MCS-22	64-QAM	5/8	6	2,016	1,260	5,197.50
MCS-23	64-QAM	3/4	6	2,016	1,512	6,237.00
MCS-24	64-QAM	13/16	6	2,016	1,638	6,756.75

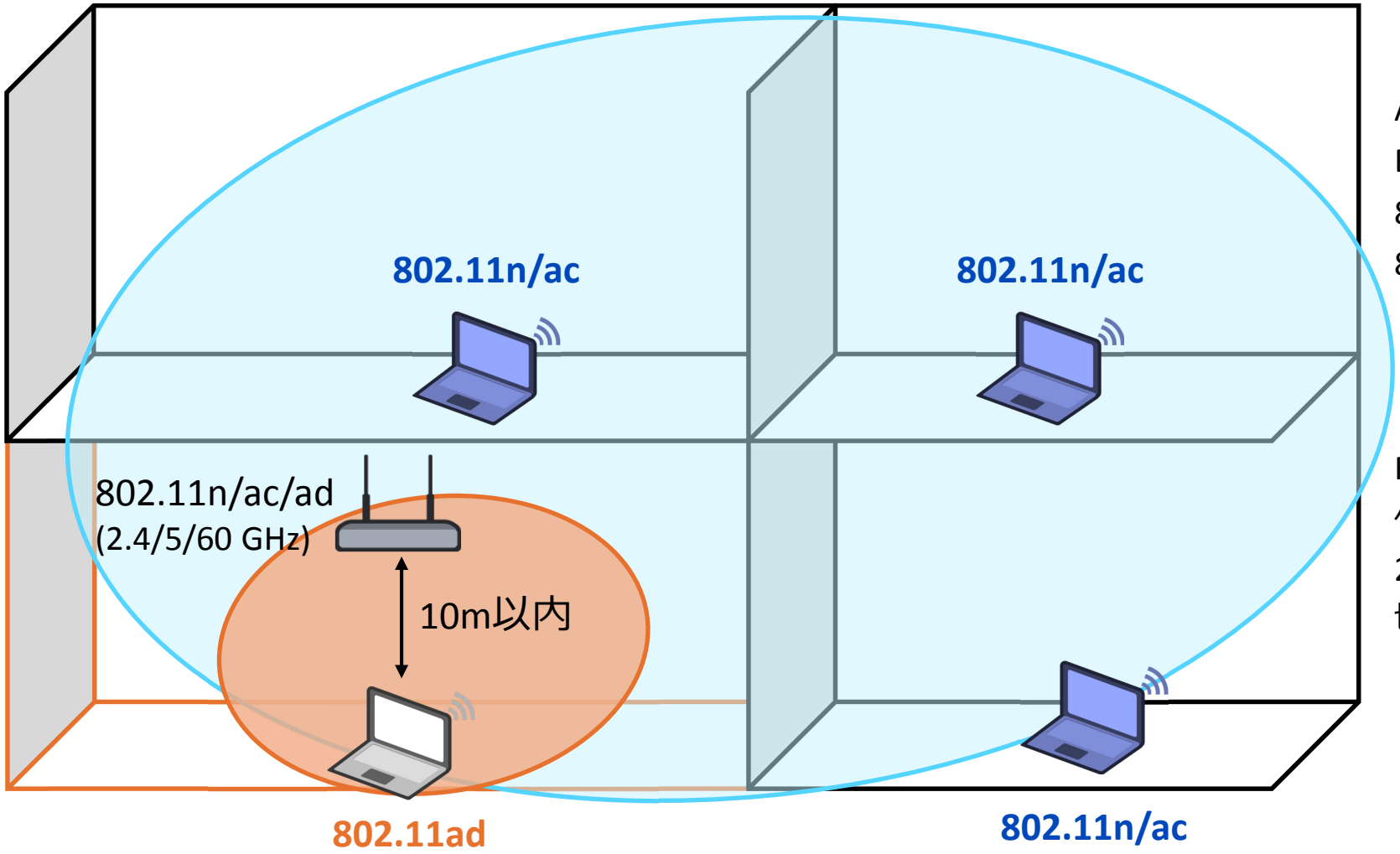
Modulation code rate for **Low Power Single carrier** PHY

MCS Index	Modulation	Effective Code rate	Coding Scheme	NCPB	Data rate (Mbps)
MCS-25	π/2 BPSK	13/28	RS(224,208)+Block code(16,8)	392	626
MCS-26	π/2 BPSK	13/21	RS(224,208)+Block code(12,8)	392	834
MCS-27	π/2 BPSK	52/63	RS(224,208)+SPC (9,8)	392	1,112
MCS-28	π/2 QPSK	13/28	RS(224,208)+Block code(16,8)	392	1,251
MCS-29	π/2 QPSK	13/21	RS(224,208)+Block code(12,8)	392	1,668
MCS-30	π/2 QPSK	52/63	RS(224,208)+SPC (9,8)	392	2,224
MCS-31	π/2 QPSK	13/14	RS(224,208)+Block code(8,8)	392	2,503



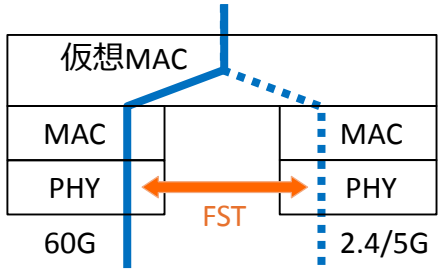


802.11adのカバレージ



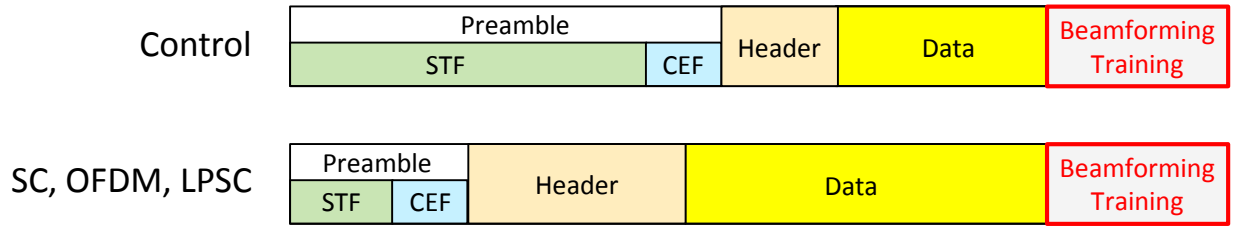
APが802.11n/ac/ad (2.4/5/60GHzのTri-Band)をサポートしていれば、802.11adでカバーできないエリアは802.11n/acでカバーされる

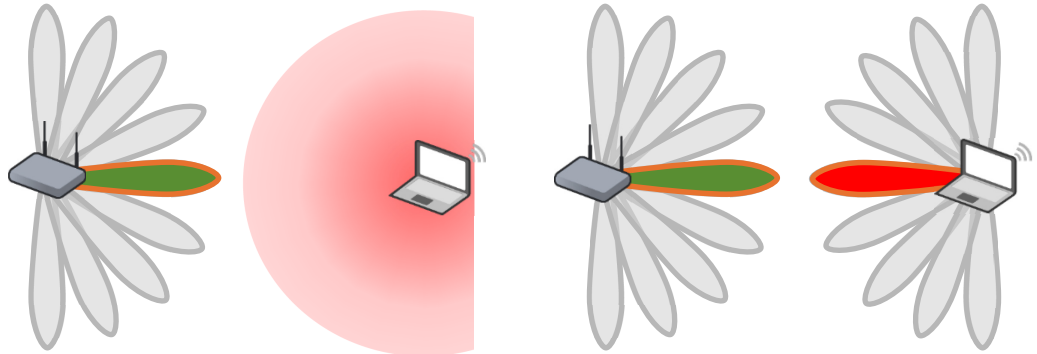
Fast Session Transfer (FST)
仮想MAC技術を利用し、60GHzと2.4/5GHzのPHY間のセッションを高速に切り替える



PHY Beamforming Training

- Beamformingを利用した送信はオプションだが、 Beamforming Training (BFT) プロトコルの実装は義務付けられている
- Sector Level Sweep (SLS) と Beam Refinement Protocol (BRP) の2つのフェーズ
- Sector Level Sweep
  - セクター（アンテナパターン）単位でパケットを送信し、受信デバイスはどのパケットが最高の品質だったかを通知し、おおよその方位を把握
  - 受信デバイスには、どのパケットが最高の品質だったかを通知する義務がある
- Beam Refinement Protocol
  - おおよそ把握した方位内で微調整

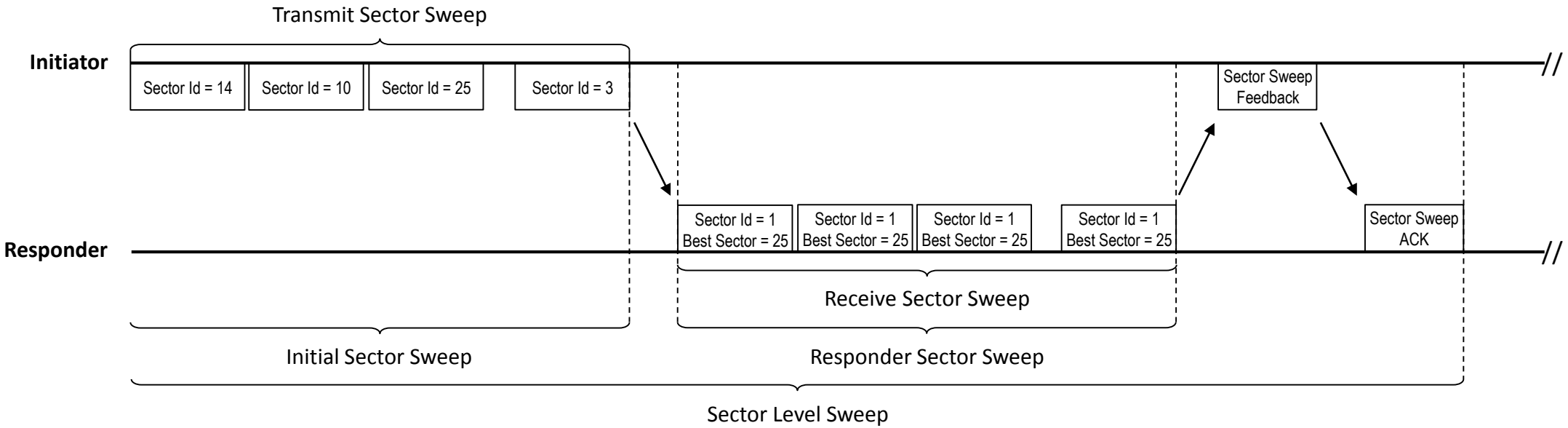


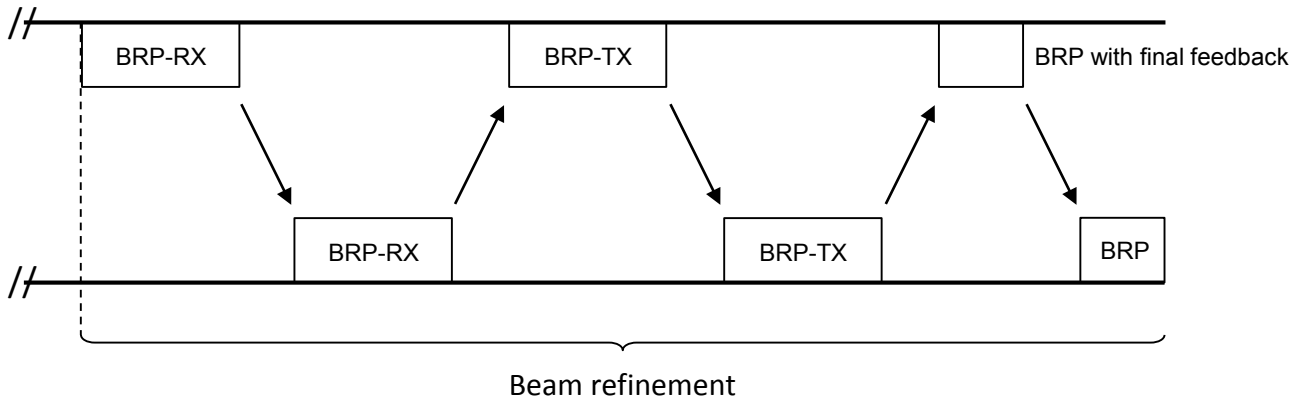


クライアントがBeamformingをサポートしていない場合

クライアントもBeamformingをサポートしている場合

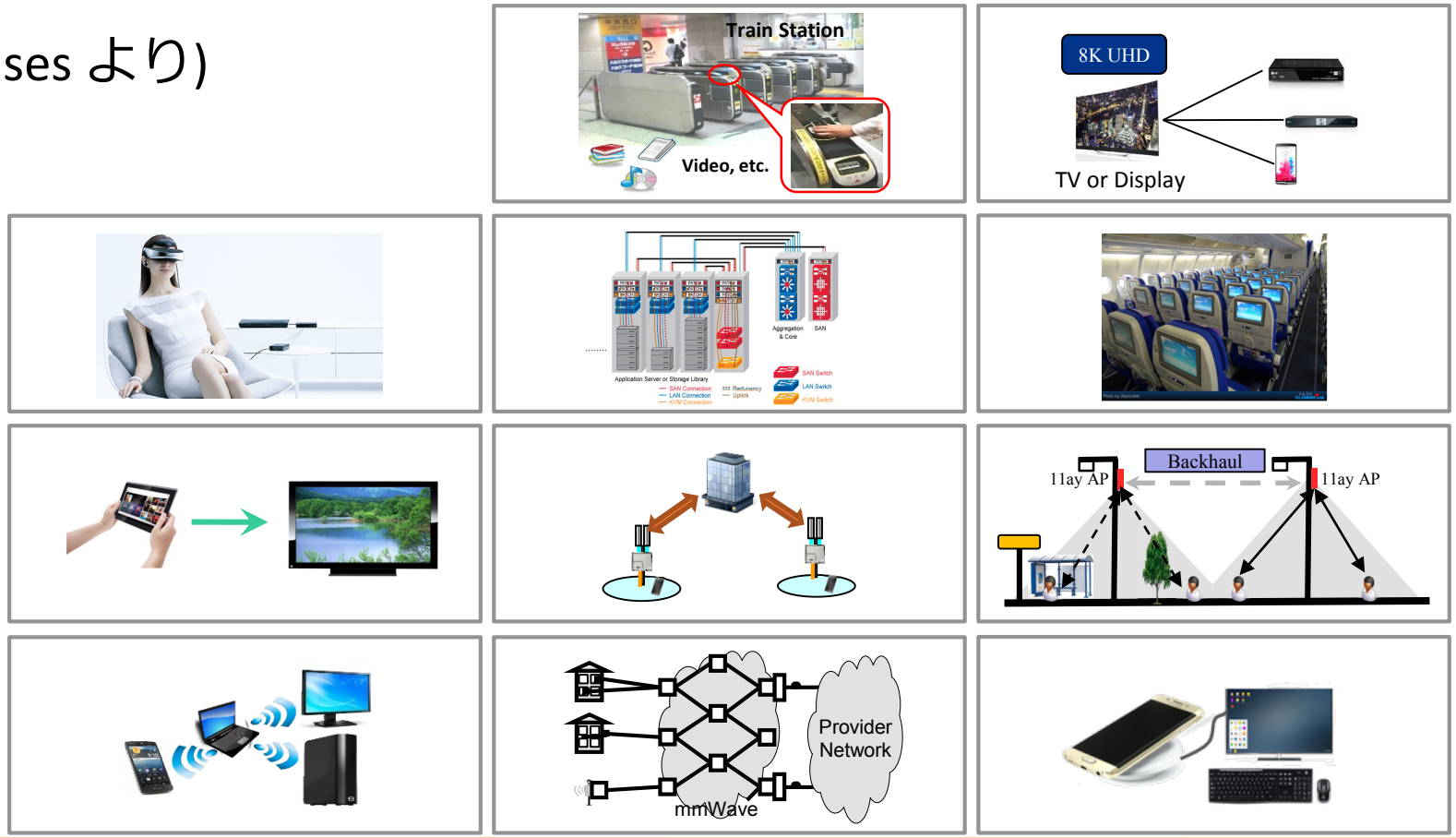
Beamforming Trainingの流れ



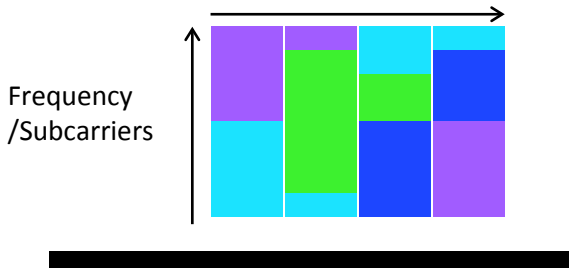


802.11ay 概要

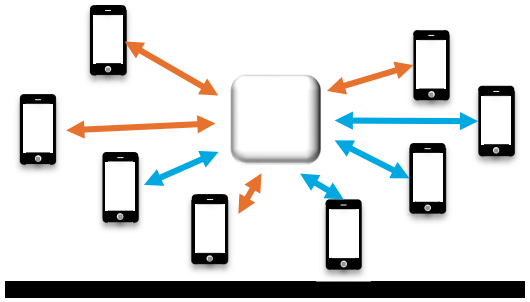
- 2015年 3月に Task Group (TG) となる
- 45GHz以上の周波数を利用して 20Gbps 以上での伝送を実現するのが目標
- 標準化作業中
- Use Cases (IEEE 802.11 TGay Use Cases より)
  - Ultra Short Range (USR) 通信
  - 8K UHDの無線伝送
  - AR/VR ヘッドセット
  - データセンター
  - ビデオ／多量データ配信／VoD
  - モバイルオフロード、MBO(Multi-Band Operation)
  - モバイルフロントホール
  - 無線バックホール
  - オフィスドッキング
  - ミリ波配信ネットワーク
  - USR無線ドッキング



IEEE 802.11ax 主要拡張機能

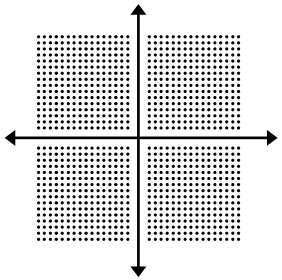


OFDMA

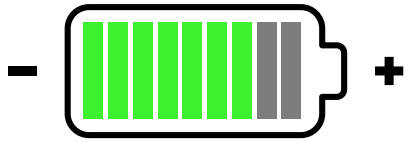


UL MU-MIMO

PHY/MAC 効率化



1024-QAM



省電力 効率化

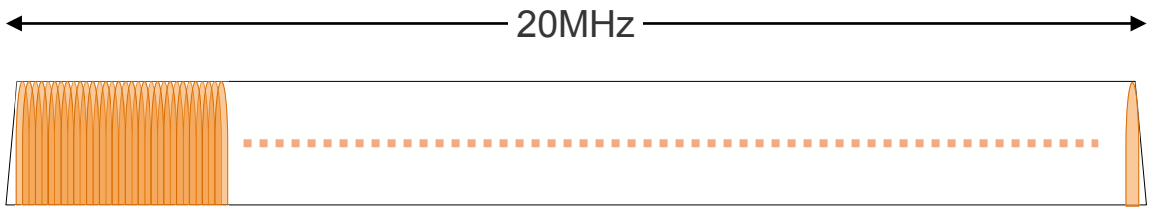
BSS Coloring

802.11a/b/g/n/acとの下位互換性を保ち
ユーザあたりの平均スループットを4倍以上にする

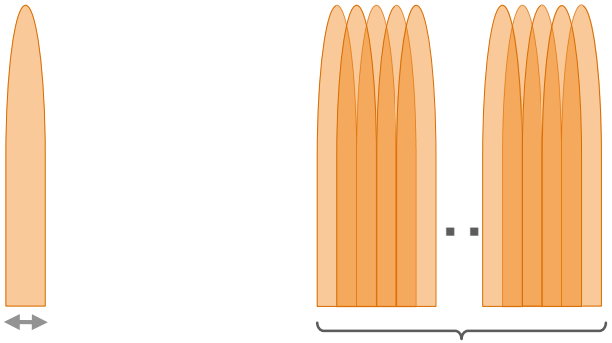
OFDMAでマルチユーザアクセス

- OFDMA（Orthogonal Frequency Division Multiple Access：直交周波数分割多元接続）
- 4G/LTEで利用されているOFDMAを採用
- 802.11acで取り入れたMU-MIMO（下り）に加え、上りでもマルチユーザアクセスを実現
- 伝送波をより細かな単位にして、複数のユーザのデータを同時に伝送できるようにデザインされている
- クライアント機器のアクセス権、送信タイミングはAPが集中制御

サブキャリア



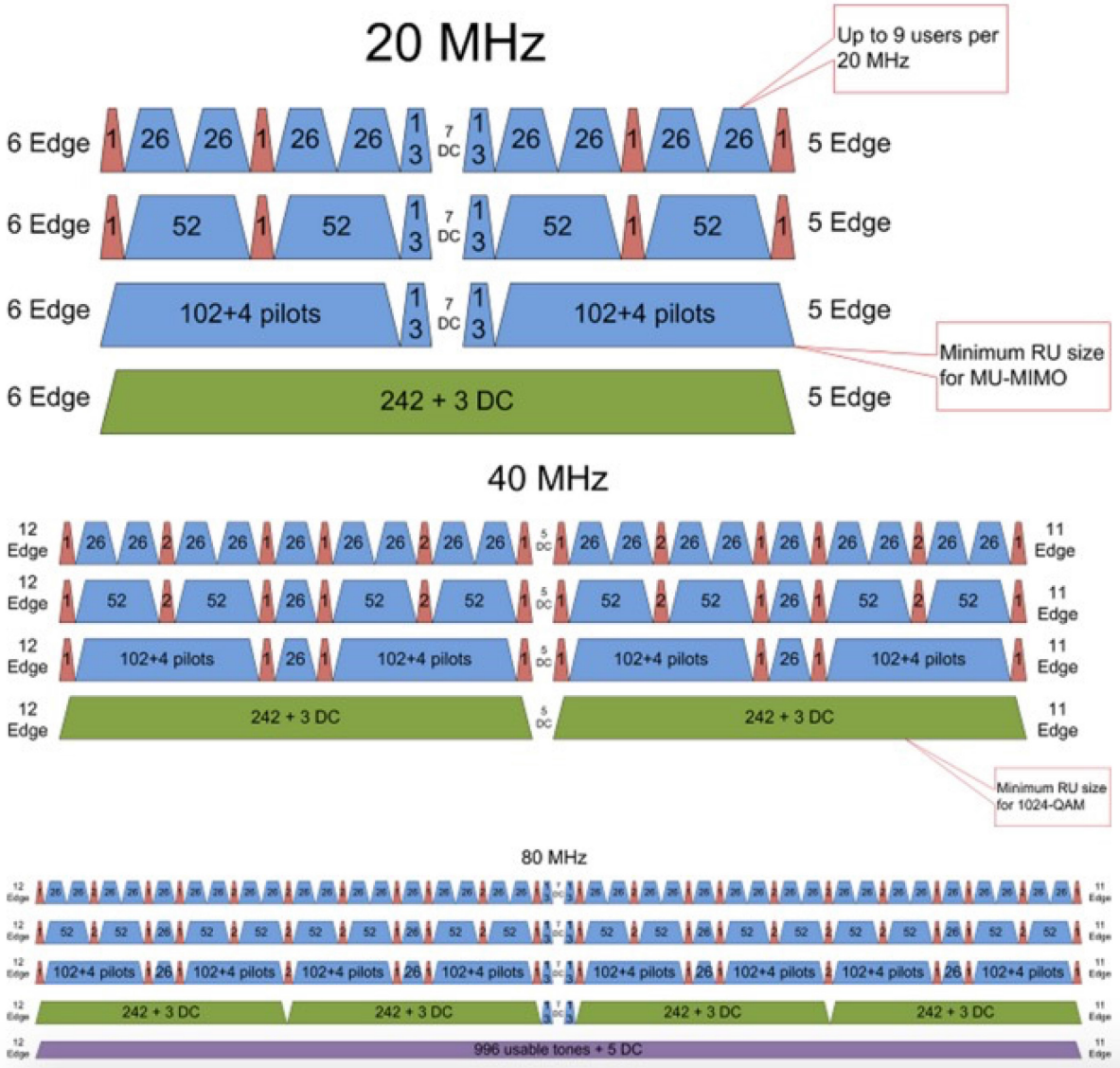
256 サブキャリア （20,000k / 78.125k = 256）



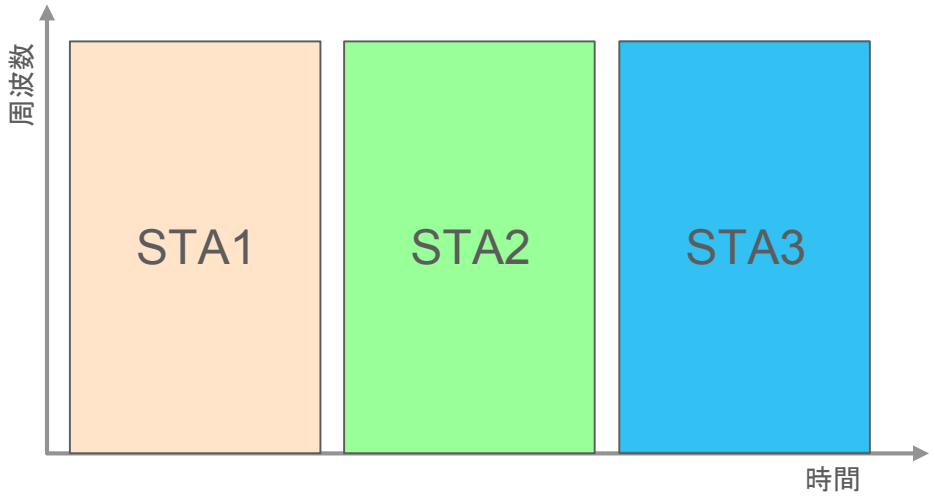
78.125kHz
サブキャリア

リソースユニット(RU)
サブキャリアをいくつか集めた単位
最低26サブキャリ

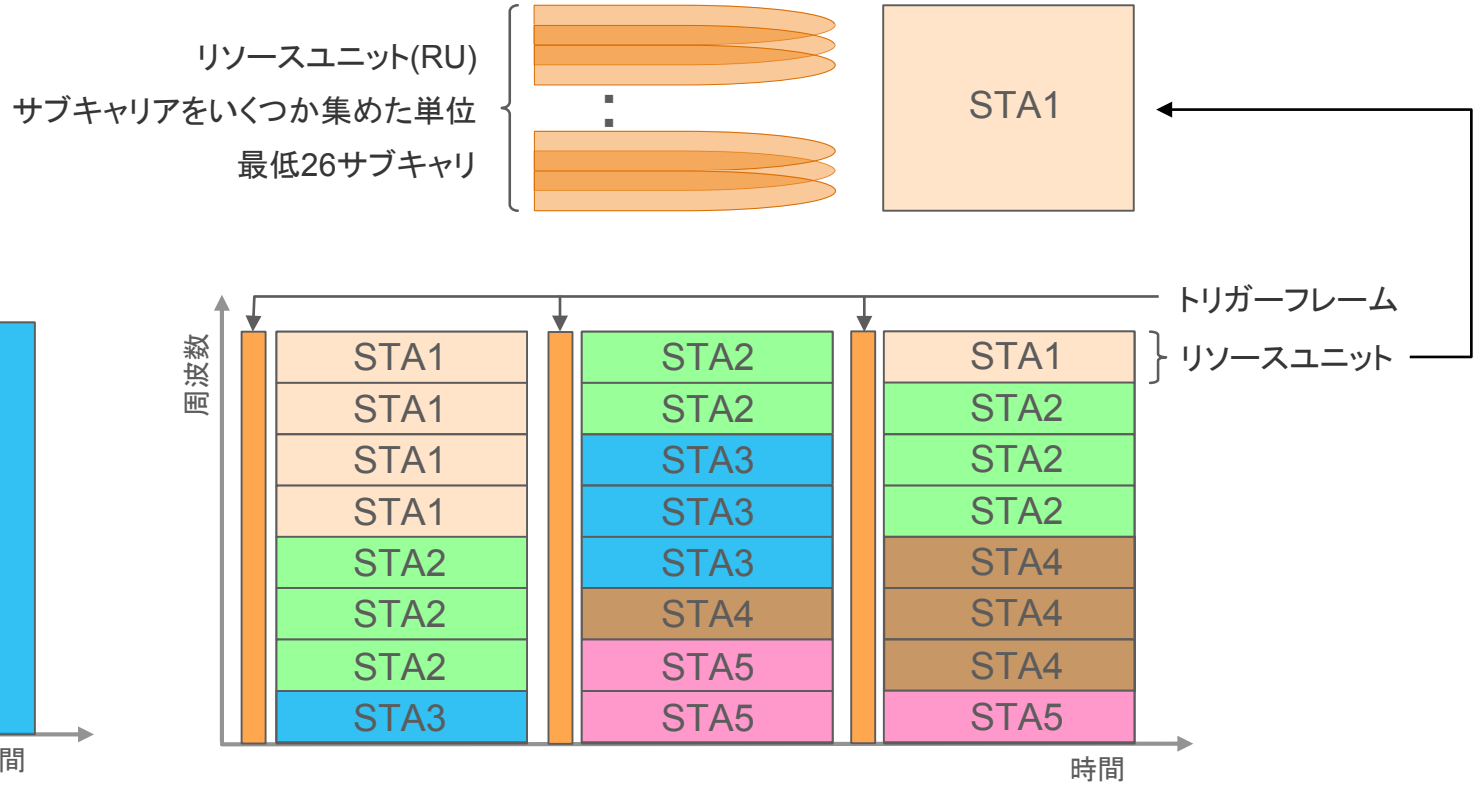
RUを最小単位（チャンネル）として扱う



上りマルチユーザアクセスを可能にする OFDMA



OFDM



OFDMA

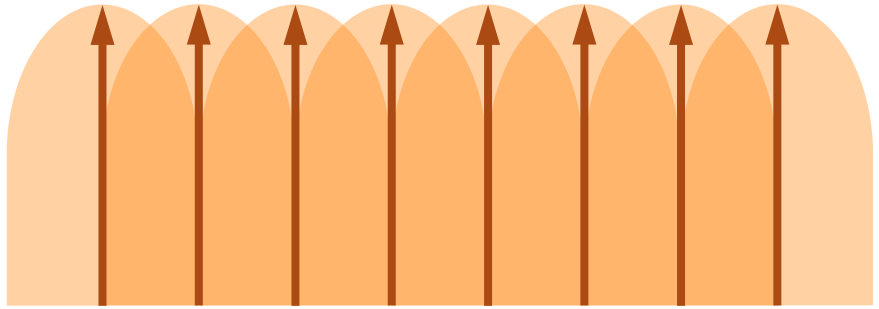
- RU単位で異なるユーザのデータを伝送することで、マルチユーザ アクセスを実現
- 送信タイミングはAPが制御

802.11ax – PHY/MAC 効率化

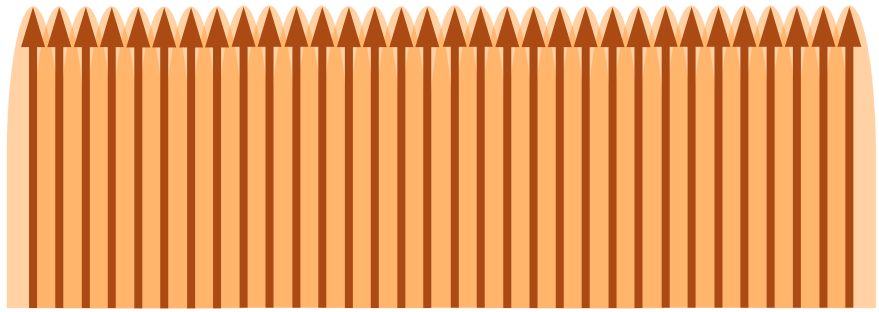
	802.11ac	802.11ax	
周波数帯	5 GHz	**2.4**, 5 GHz	2.4GHzも利用可能
チャンネル幅（ボンディング）	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	
FFTサイズ	64, 128, 256, 512	256, 512, 1024, 2048	
サブキャリア間隔	312.5 kHz	**78.125 kHz**	スペクトルの効率化でより多くのトーン／チャンネル
OFDMのシンボル長	3.2 µs + 0.8/0.4 µs CP	**12.8 µs + 0.8/1.6/3.2 µs CP**	オーバーヘッドを低減し、屋外での運用を支援
変調方式（最高次数）	256-QAM	**1024-QAM**	高次の変調方式でより高いデータレートを可能にする
データレート	433 Mbps (80 MHz, 1ss) 6,933 Mbps (160MHz, 8ss)	600.4 Mbps (80 MHz, 1ss) 9,607.8 Mbps (160MHz, 8ss)	

802.11ax – More Efficiency with Sub-Carrier Spacing

- 802.11axでは、以前の802.11仕様と比較し使用可能なデータトーンの数が4倍に増えるようにサブキャリア間隔が縮小された
- 利用可能なデータトーンが4倍に増加しかつ、変調方式が1024-QAMに増加すると、最大PHYレートが劇的に増加する
- より多くのデータトーンにより、OFDMAでの同時ユーザ（最大74人）のサポートを可能にする



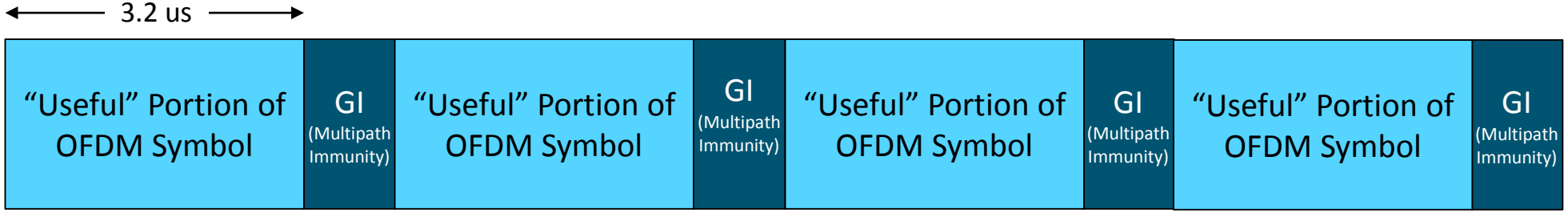
サブキャリア間隔　312.5 kHz



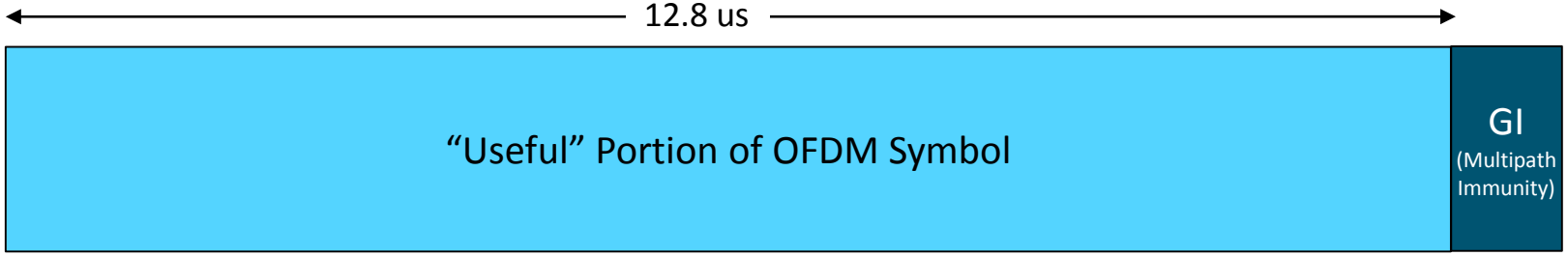
サブキャリア間隔　78.125 kHz

802.11ax – 長い OFDM シンボル

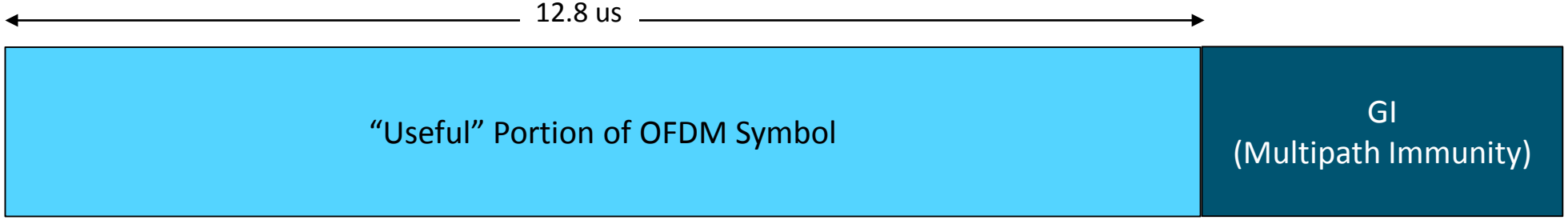
11g/n/ac の OFDM シンボル



11ax の OFDM シンボル（屋内：GI オーバーヘッドの減少でスループットは向上）



11ax の OFDM シンボル（屋外：長いGIによるマルチパスへの耐性を向上)



802.11ax – MAC/PHY 効率化

	802.11a/g	802.11n/ac	802.11ax
トーン数 (20MHz)	64	64	256
サブキャリア間隔	20MHz/64 = 312.5KHz	20MHz/64 = 312.5KHz	20MHz/256 = 78.125KHz
データ サブキャリア	48	52	234
効率性	**75%**	**81%**	**91%**
OFDM シンボル	3.2us	3.2us	12.8us
ガード インターバル	0.8us	0.4, 0.8us	0.8, 1.6, 3.2us
シンボル タイム	4.0us	3.6, 4.0us	13.6, 14.4, 16.0us
効率性	**80%**	**89%, 80%**	**94%, 89%, 80%**

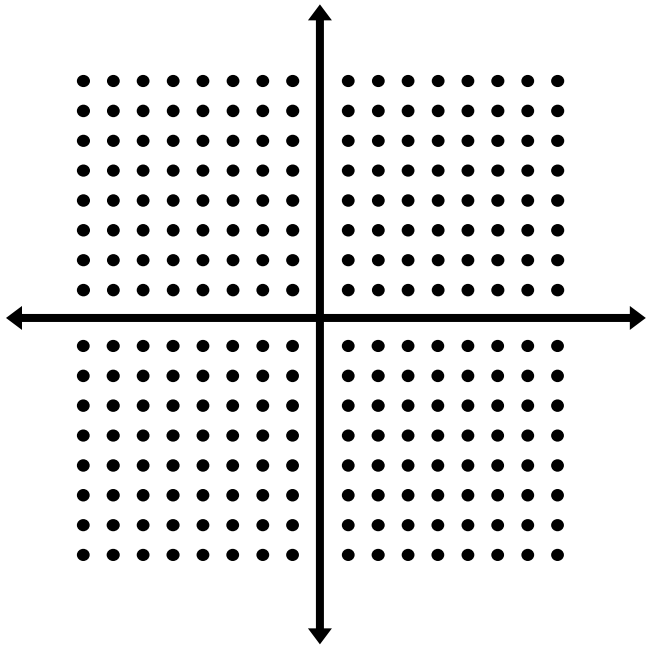
PHY-レベルの
効率性を向上

11n/ac より ～17% 効率的

11a/g より ～40% 効率的

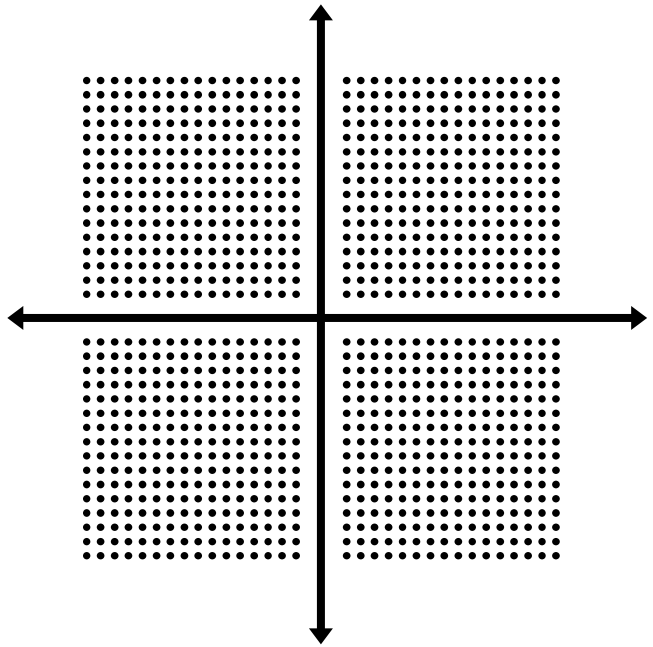
802.11ax – 1024-QAM

信号空間ダイヤグラム



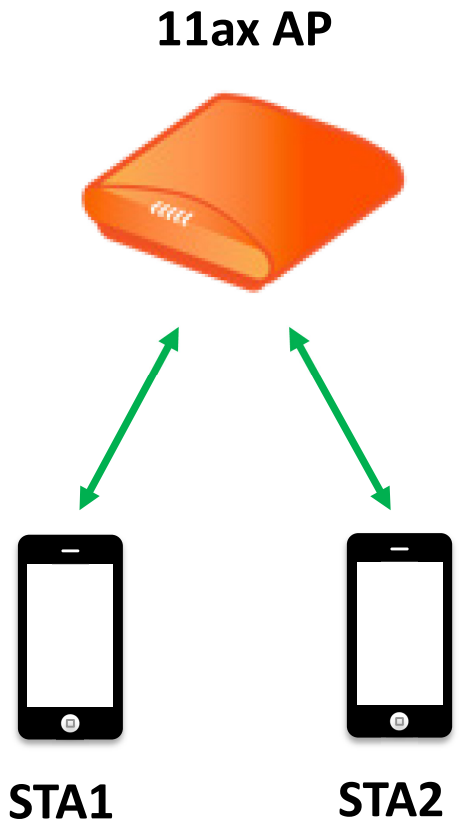
256-QAM
11ac

25%
データレート向上

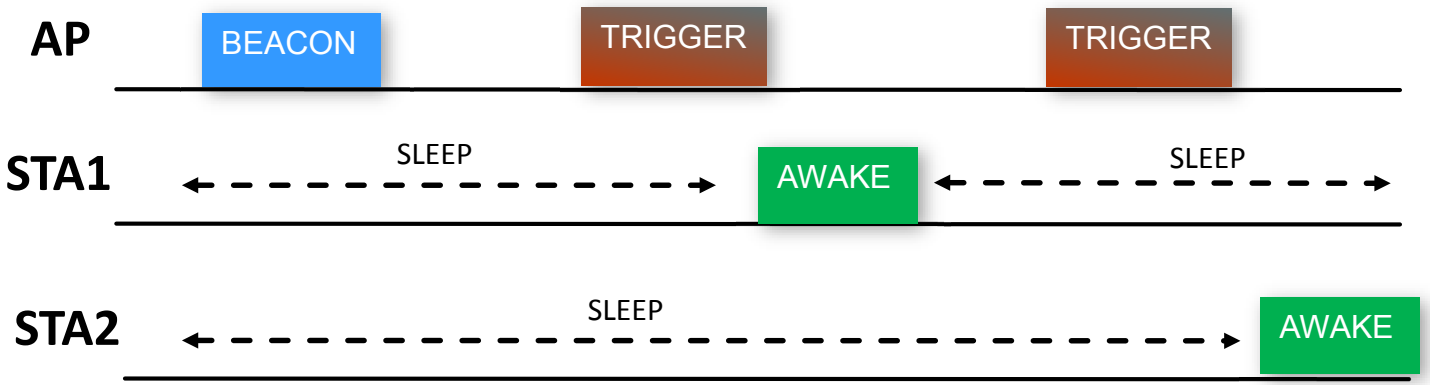


1024-QAM
11ax

802.11ax – 電力の効率化



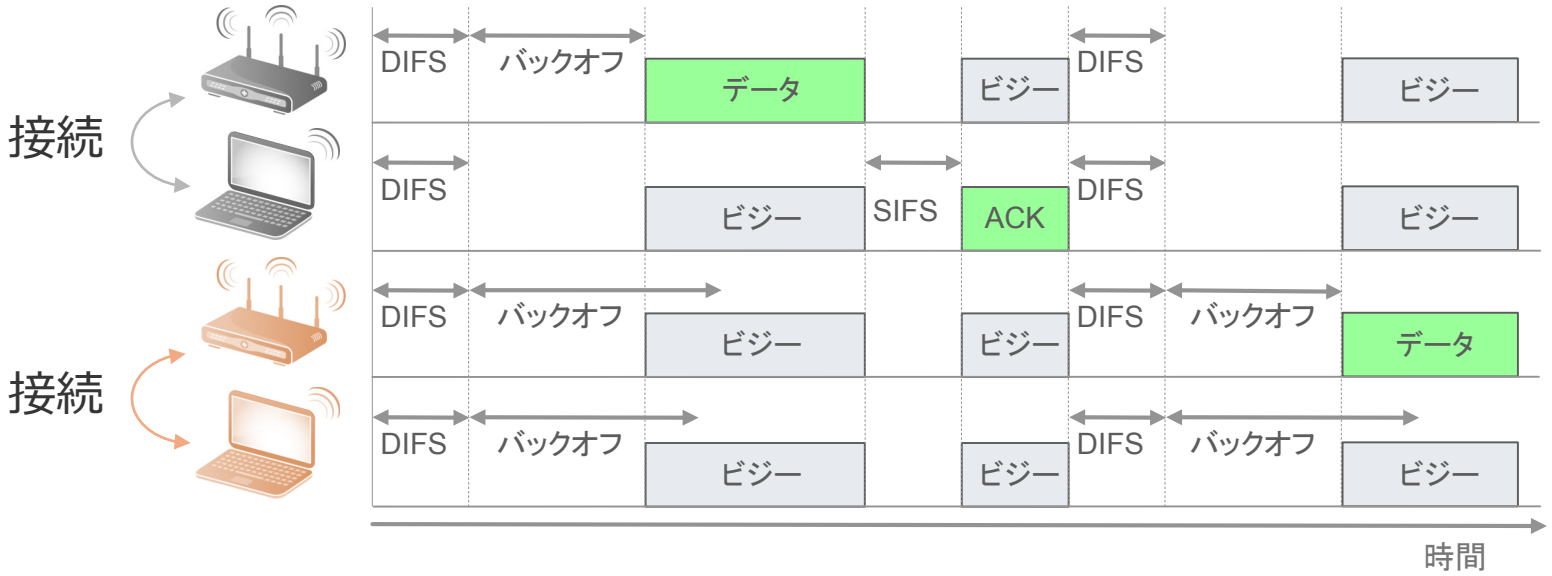
目標待ち時間



- AP – クライアント間で起き上がる時間をネゴシエーション
- AP は TWT (Target Wake Time)を利用し、クライアントデバイス間の空中での競合を避ける
- スケジュールされたスリープと起き上がり時間は、クライアントにとって効率的な電力利用を可能にする

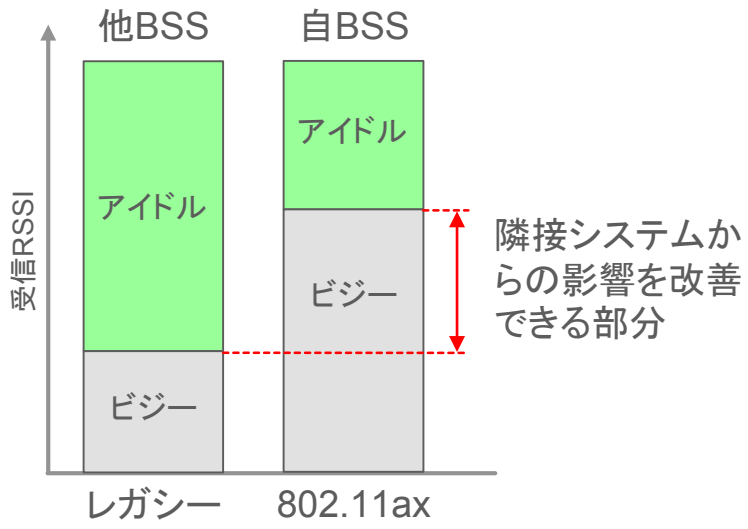
802.11a/b/g/n/acでの干渉回避方式

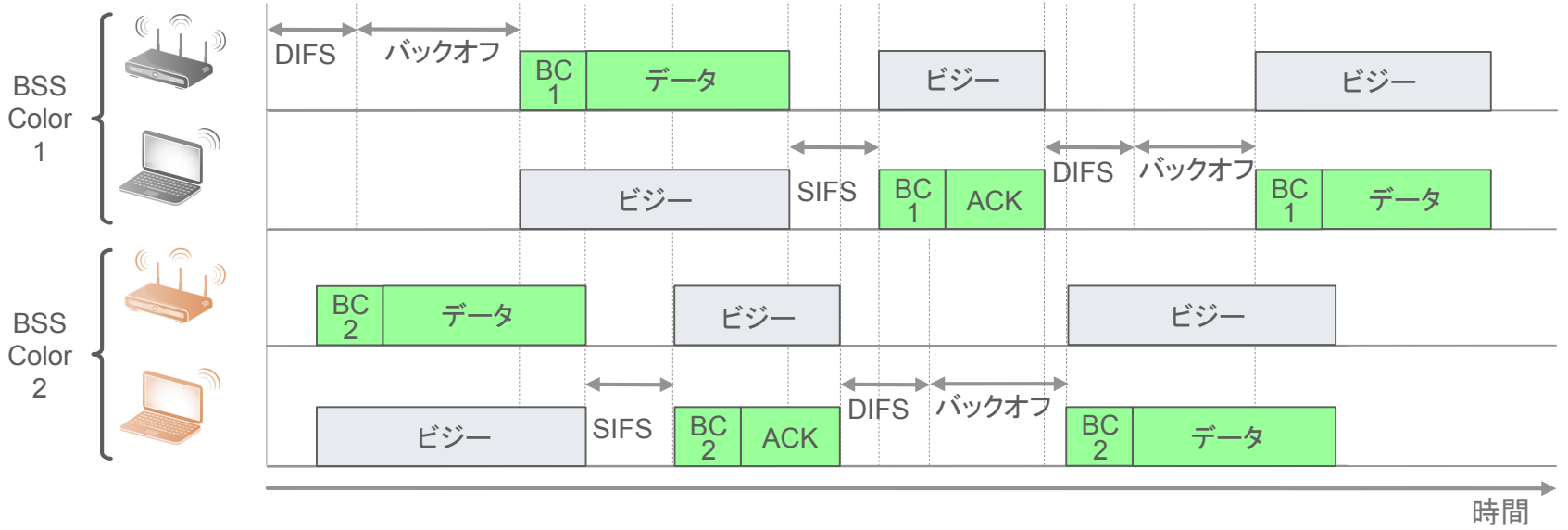
- これまでの干渉回避方式はCSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
- CSMA/CAでは、同一チャンネルを共有している機器で1台だけが送信できる
- AP(BSS)が複数あっても条件は同じ
- エリア内のAP/クライアント密度が増加すると、無線帯域の利用効率が悪化し、遅い、切れるなどの問題が出始める



高密度環境を実現するBSS Coloring

- プリアンブル内に”BSS Color”というフィールドを追加し、自BSSの通信か他BSSの通信かを明確にする
- 他BSSのフレームに対しては、高めのしきい値でビジーと判定し、自BSSの通信をなるべく継続できるようにする





進化を続ける無線LAN（Wi-Fi）規格

	802.11 (Legacy)	802.11b (Legacy)	802.11a (Legacy)	802.11g (Legacy)	802.11n (HT)	802.11ac (VHT)	802.11ax (HE)
規格化年	1997	1999	1999	2003	2009	2014	2019 (見込み)
帯域	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	**2.4/5 GHz**
チャンネル幅	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
最高 PHY レート	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	**9.6 Gbps**
帯域あたりの効率	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	**62.5 bps/Hz**
最大空間ストリーム	1	1	1	1	4	8	8
最大MU 空間ストリーム数	NA	NA	NA	NA	NA	4 (DL only)	**8 (UL & DL)**
変調方式	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	**OFDMA**
最大コンスタレーション／コードレート	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	**1024-QAM**, 5/6
最大OFDMトーン	NA	NA	64	64	128	512	**2048**
サブキャリスペース	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	**78.125 kHz**

WPA2の弱点

- 2017年10月にWPA2の脆弱性 KRACKs (Key Reinstallation AttaCK) が公開された
  - 単一の方法ではなく 複数の方法がある
  - 4 way handshakeで 同じパケットを再送する欠点を利用し 暗号化通信の解読を可能にする
  - 電波の届く範囲で 特定のクライアントを狙う必要がある
  - 既に修正ソフトウェアが配布されている
  - 現実的には非常に困難で 実害の報告は聞いていない
- 辞書攻撃 (Dictionary attack) 可能
  - WPA2ではパスフレーズ (Passphrase) を何度でも入力できてしまう
  - 偶然がない限り 非常に長い時間を要する
  - 電波の届く範囲で 長い時間攻撃し続ける必要がある
  - エンタープライズモードを利用すれば回避できる

- WPA2 のリリースは 2004年9月で、既に14年が経過している。3DES同様、セキュリティー的にはそろそろマイグレーションしていいころ

Wi-Fi Alliance®
Wi-Fiセキュリティ規格 「Wi-Fi CERTIFIED WPA3™」を発表

https://www.wi-fi.org/ja/news-events/newsroom/wi-fi-alliance-wi-fi-wi-fi-certified-wpa3

2018年6月25日

パーソナル／エンタープライズネットワーク向けの次世代Wi-Fi®セキュリティ規格

Wi-Fi Alliance®は、個人および企業向けネットワークのWi-Fi保護機能を強化した次世代Wi-Fi®セキュリティ規格「Wi-Fi CERTIFIED WPA3™」を発表しました。WPA3は、10年以上にわたって広く採用されているWPA2™の後継であり、Wi-Fiセキュリティの簡素化や、よりレジリエントな認証、さらに強固な機密データの暗号化を実現する新機能を備えています。Wi-Fi業界がWPA3セキュリティ規格に移行する中、WPA2デバイスの相互運用性とセキュリティは引き続き確保し続けます。

WPA3 概要

WPA3 は、WPA2の幅広い普及と成功を基盤に、Wi-Fi セキュリティ設定の簡素化と Wi-Fi ネットワーク セキュリティの保護の強化を実現する一連の機能を提供する

- **WPA3-Personal Mode**
  - SAE (Simultaneous Authentication of Equals, 同等性同時認証) を使用して、より耐性の高いパスワードベースの認証を提供し、第三者によるパスワード推測の攻撃に対してユーザーに強力なセキュリティ保護を提供
- **WPA3-Enterprise 192-bit Mode**
  - WPA3-Enterprise の 192ビットセキュリティにより、政府、防衛などの強固なセキュリティが必要な環境に推奨される暗号強度の最新版を提供
- **WPA3-Transition Mode**
  - WPA3 は WPA2 との下位互換性を維持し、相互運用をサポートする

WPA3-Personal

- WPA3-Personalは、 SAE (同等性同時認証) を使用した保護が強化されたパスワードベースの認証で、 PSK の WPA2-Personal に置き換わる
- SAEはIEEE 802.11仕様に基づいている
  - Section 12.4.1: SAEは、ゼロ知識証明 (zero-knowledge proof) に基づくパスワード認証された鍵交換であるDragonflyの変種
- 業界標準の楕円曲線暗号(Elliptic Curve Cryptography)を使用
- 推奨される強度に達していない「低い乱雑さ(entropy) 」のパスワードでも、「高い乱雑さ」のセキュリティを提供する
- パスワードの強度への依存を減らし、覚えにくい複雑なパスワードを生成するユーザの負担を軽減
- 鍵交換プロトコル中にパスワードが決して共有されない
- SAEでは認証の成否を送り合わないため、ランダムなパスワード攻撃が成功したかを判断するのが難しく、辞書攻撃に高い耐性を持つ

WPA3-Enterprise 192-bit Mode

- WPA3-Enterprise の 192ビットの暗号強度は、政府機関や金融などの機密データが送信されるネットワークのセキュリティを強化する
- Wi-Fi Alliance の 192ビット セキュリティスイートは、米国政府仕様に基づいており、機密性の高いネットワーク用の一貫した暗号化ツールセットを確立している
- 192ビットのセキュリティスイートには、以下が含まれる：
  - 認証付き暗号化のための GCMP-256 (256-bit Galois/Counter Mode Protocol)
  - 鍵導出と鍵の確認のための 384-bit HMAC (Hashed Message Authentication Mode), HMAC-SHA384 (Secure Hash Algorithm)
  - 鍵確立と認証にECDH (Elliptic Curve Diffie-Hellman) 交換と 384ビットの楕円曲線を使用する ECDSA (Elliptic Curve Digital Signature Algorithm)
  - 非対称暗号とデジタル署名のためのRSAの鍵長は 3kビット以上
  - 堅牢な管理フレーム保護のためのBIP-GMAC-256 (Broadcast/Multicast Integrity Protocol Galois Message Authentication Code)
- WPA3-Enterpriseの192ビットセキュリティにより、暗号化ツールの適切な組み合わせが使用され、WPA3ネットワーク内の一貫したセキュリティのベースラインが設定される

WPA3-Transition Mode（移行モード）

- WPA3対応ネットワークは、 WPA3-Transition Modeを使用してレガシーWPA2クライアントを引き続きサポートする
- WPA3-Personal、 WPA3-Enterprise 共に下位互換性が考慮されている
- WPA3-Enterpriseの移行モードでは、 WPA2対応デバイスは暗号化アルゴリズムとして使用できるのはAESのみ

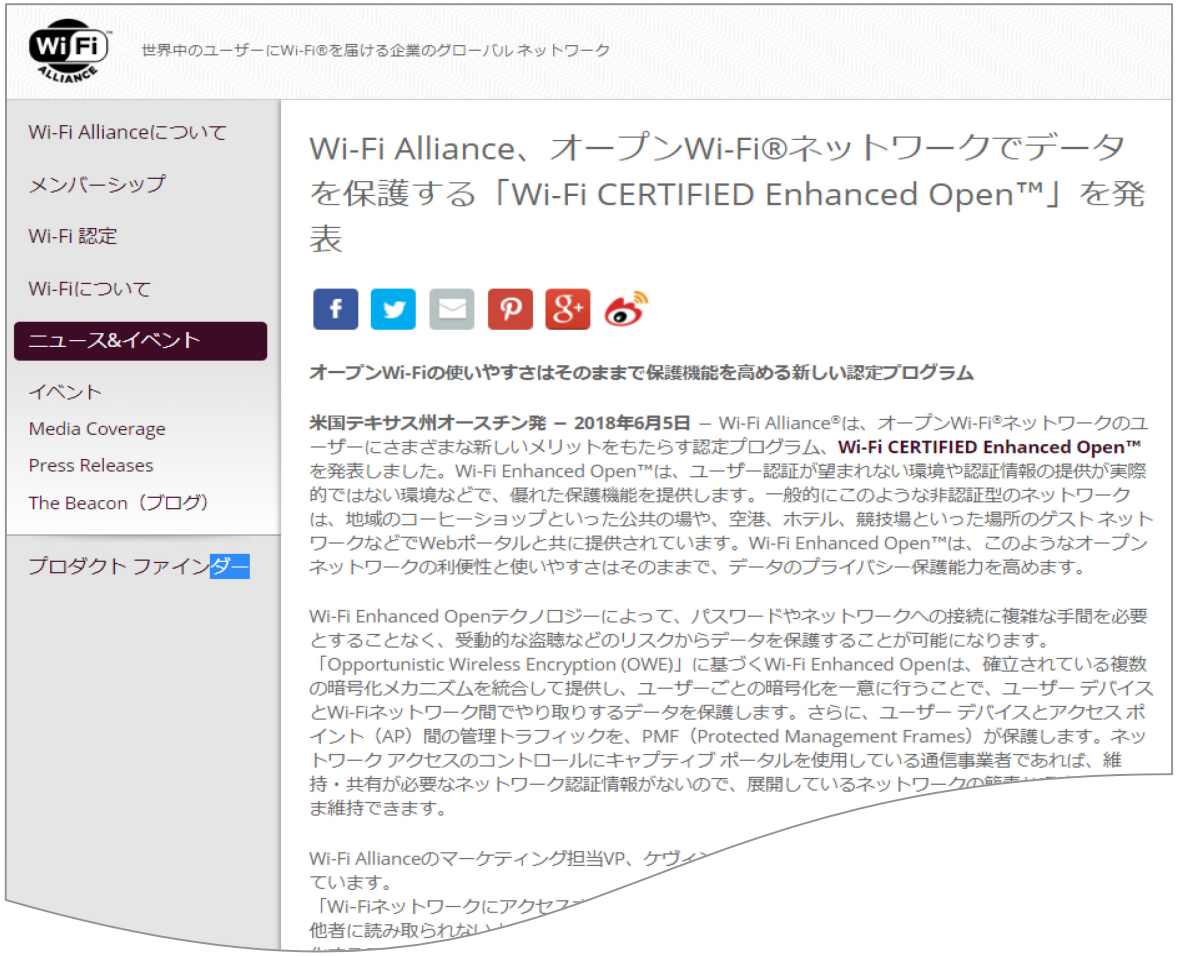
下位互換性を維持しながら WPA3 を導入

- WPA3は、 Wi-Fi CERTIFIEDデバイスのオプション認証
- WPA2は引き続きすべてのWi-Fi CERTIFIEDデバイスの必須セキュリティ認証
- WPA3の市場導入が進むと、WPA3は最終的にすべてのWi-Fi CERTIFIEDデバイスの必須のセキュリティ認証になる
- WFAは、2018年末ごろからWPA3対応製品の出荷が始まり、2019年末ごろから製品出荷が本格化すると予測している
  - 2018年10月末時点で、WFA で CERTIFIED されているのは 12 製品

- WPA3専用ネットワークでは、最新のセキュリティ方法を使用し、従来のプロトコルであるWEPとTKIPは利用できない
- WPA3では、WPA3-PersonalおよびWPA3-Enterpriseネットワークに保護された管理フレーム（PMF: Protected Management Frames）を使用する必要がある

Wi-Fi Alliance、オープンWi-Fi®ネットワークでデータを保護する「Wi-Fi CERTIFIED Enhanced Open™」を発表

https://www.wi-fi.org/ja/news-events/newsroom/wi-fi-alliance-wi-fi-wi-fi-certified-enhanced-open



世界中のユーザーにWi-Fi®を届ける企業のグローバル ネットワーク

Wi-Fi Allianceについて
メンバーシップ
Wi-Fi 認定
Wi-Fiについて
ニュース&イベント
イベント
Media Coverage
Press Releases
The Beacon（ブログ）
プロダクト ファインダー

Wi-Fi Alliance、オープンWi-Fi®ネットワークでデータを保護する「Wi-Fi CERTIFIED Enhanced Open™」を発表

オープンWi-Fiの使いやすさはそのままで保護機能を高める新しい認定プログラム

米国テキサス州オースチン発 – 2018年6月5日 – Wi-Fi Alliance®は、オープンWi-Fi®ネットワークのユーザーにさまざまな新しいメリットをもたらす認定プログラム、**Wi-Fi CERTIFIED Enhanced Open™**を発表しました。Wi-Fi Enhanced Open™は、ユーザー認証が望まれない環境や認証情報の提供が実際的ではない環境などで、優れた保護機能を提供します。一般的にこのような非認証型のネットワークは、地域のコーヒーショップといった公共の場や、空港、ホテル、競技場といった場所のゲスト ネットワークなどでWebポータルと共に提供されています。Wi-Fi Enhanced Open™は、このようなオープン ネットワークの利便性と使いやすさはそのままで、データのプライバシー保護能力を高めます。

Wi-Fi Enhanced Openテクノロジーによって、パスワードやネットワークへの接続に複雑な手間を必要とすることなく、受動的な盗聴などのリスクからデータを保護することが可能になります。「Opportunistic Wireless Encryption (OWE)」に基づくWi-Fi Enhanced Openは、確立されている複数の暗号化メカニズムを統合して提供し、ユーザーごとの暗号化を一意に行うことで、ユーザー デバイスとWi-Fiネットワーク間でやり取りするデータを保護します。さらに、ユーザー デバイスとアクセス ポイント（AP）間の管理トラフィックを、PMF（Protected Management Frames）が保護します。ネットワーク アクセスのコントロールにキャプティブ ポータルを使用している通信事業者であれば、維持・共有が必要なネットワーク認証情報がないので、展開しているネットワークの管理…ま維持できます。

Wi-Fi Allianceのマーケティング担当VP、ケヴィ…ています。
「Wi-Fiネットワークにアクセス…
他者に読み取られない…

2018年6月5日

オープンWi-Fiの使いやすさはそのままで保護機能を高める新しい認定プログラム

Wi-Fi Enhanced Open™は、ユーザー認証が望まれない環境や認証情報の提供が実際的ではない環境などで、優れた保護機能を提供します。一般的にこのような非認証型のネットワークは、地域のコーヒーショップといった公共の場や、空港、ホテル、競技場といった場所のゲストネットワークなどでWebポータルと共に提供されています。Wi-Fi Enhanced Open™は、このようなオープン ネットワークの利便性と使いやすさはそのままで、データのプライバシー保護能力を高めます。

Wi-Fi CERTIFIED Enhanced Open

- オープンネットワークにおけるデータの保護が目的
- Opportunistic Wireless Encrypt (OWE) を利用
- 認証やパスワードの入力などを行わずにデータの暗号化を行い、盗聴からデータを保護
- 複数の暗号化の仕組みを統合して、クライアントごとに異なる暗号化通信を行う
- 鍵交換には、SSL/TLSと同じ Diffie-Hellman (ECDH) を使用
- 管理フレームは PMF で暗号化
- 既存ネットワークとの相互運用性も考慮されている
- なりすましに対する対策は考慮されていない

WPA3と合わせて Wi-Fi Easy Connect を発表

https://www.wi-fi.org/ja/discover-wi-fi/wi-fi-easy-connect

Wi-Fi®デバイスのシンプルでセキュアな接続を実現

Wi-Fi CERTIFIED Easy Connect™は、最高のセキュリティ標準を実装しながら、Wi-Fi®ネットワークへのデバイス接続時の複雑さを軽減するとともに質の高いユーザー エクスペリエンスを提供します。Wi-Fi CERTIFIED Easy Connectによって、便利なユーザー インターフェイスのないデバイスまでも含めて、製品のQRコードを読み取るだけというシンプルな作業でWi-Fi ネットワークを利用することが可能になります。

Wi-Fi Easy Connect

- ディスプレイなどを持たない機器を容易に無線LANに接続
- スマートフォンなどのカメラでQRコードを読み取り、APに登録することで接続が可能になる
- QRコードに公開鍵などが埋め込まれているが、各機器とのみ通信できる仕組みになっている

WFAの発表スライドより

1. 専用アプリをインストールしたコンフィグレータでAPのQRコードを読み込み、APに接続
2. コンフィグレータが接続したいクライアントのQRコードを読み込み、APに登録
3. APに登録された情報を基にAPとクライアントがネゴシエーションを行い、接続が完了

Wi-Fiに求められるもの

厳しい環境であっても、アプリケーションとサービスに対し

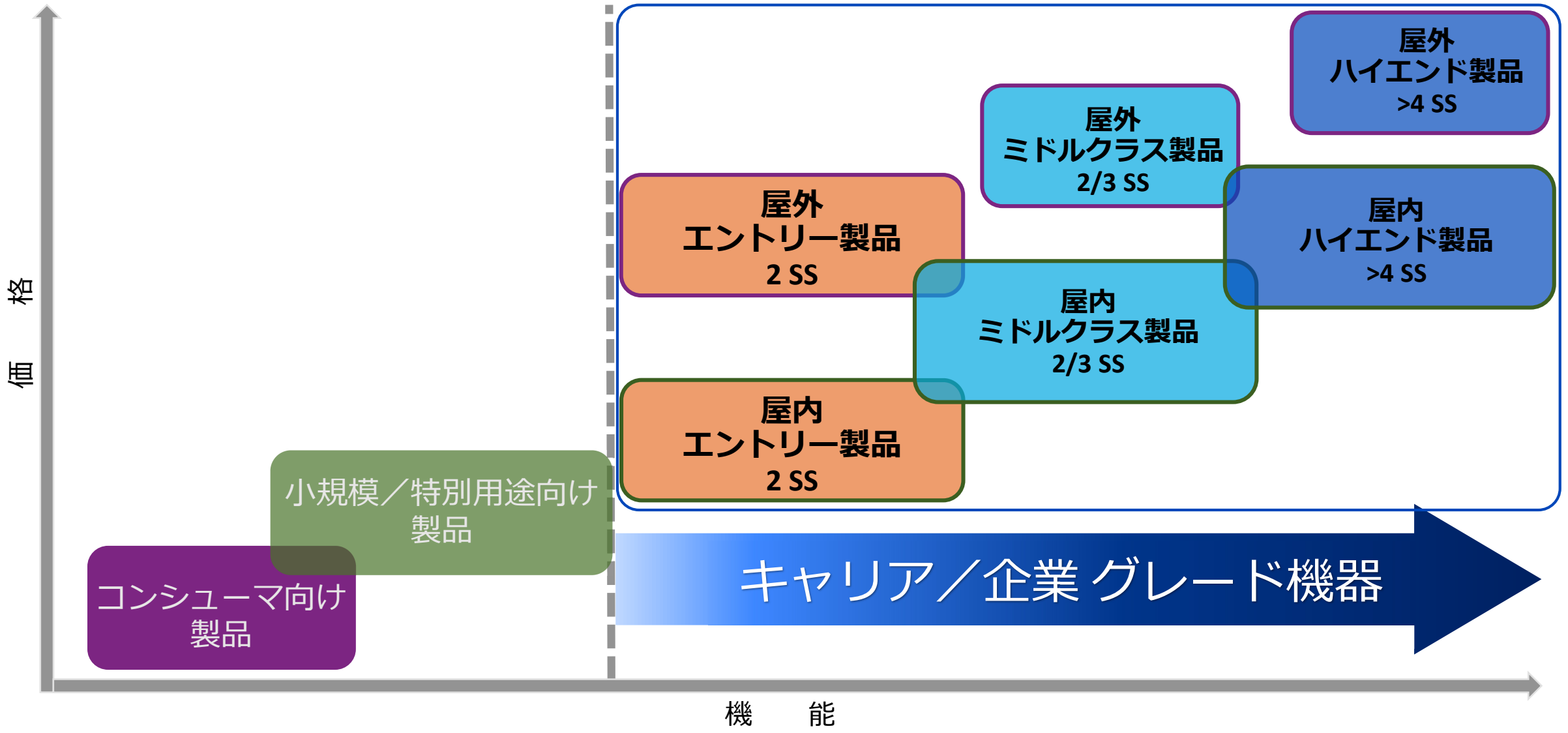
高性能で安全で信頼性の高いWi-Fiアクセスが求められている

教　育	ホ　テ　ル	通信事業者	集 合 住 宅	シティWi-Fi	公 共 施 設






企業の Wi-Fi には企業向け製品が必要



マルチメディア アプリケーション

Voice over WLAN

ビデオ会議／カンファレンス

映像／ビデオサーベイランス

電子ブック／電子教科書

高密度AP環境で動画の配信：関東第一高等学校 様

導入のポイント

- アクセスポイントを高密度で設置しても少ない干渉
  - 高密度環境においても干渉が少い
  - 40 ～ 50 台のクライアントの同時アクセスが安定していた
  - スループットを維持し、快適な通信環境の構築が可能
- 通信容量に応じ、自動でクライアントを割り振るインテリジェンス

お客様担当者の言葉

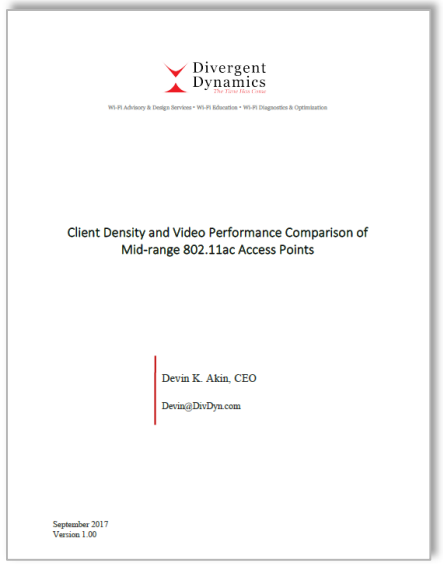
「ラッカスの製品は、学校特有の環境に合致していました。企業だと、ネットワークに接続しないで書類を作成したり、打ち合わせなどパソコンを使わない業務も多いので、同時アクセスはあまり問題になりませんが、学校では**40 ～50人**による**同時アクセス**、しかも**動画**等容量が大きいコンテンツへのアクセスが発生します。そのため、アクセスポイントは全ての教室と公共スペースに**2台ずつ設置**していますが、これだけの台数を導入しても**干渉が起きないのはラッカスだけ**でした。それどころか、同時接続するユーザーを2台のアクセスポイントに自動で割り振ってくれるため、アクセススピードも落ちません。」

Divergent Dynamicsによるテストレポート

Divergent Dynamics
The Time Has Come

ダイバージェントダイナミクスは、スタジアム、アリーナ、コンベンションセンター、展示会、病院、学校などの高密度で複雑な環境でのWi-Fi設計とパフォーマンスの最適化に重点を置く、ベテランが経営する先進的なWi-Fiのスペシャリストです。
世界クラスのWi-Fiトレーニングサービスも提供します。

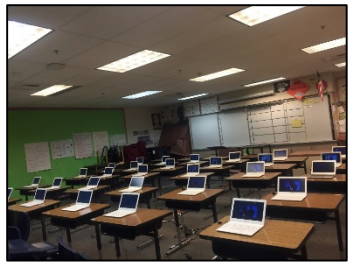
http://divdyn.com/


Divergent Dynamics

Client Density and Video Performance Comparison of Mid-range 802.11ac Access Points

Devin K. Akin, CEO
Devin@DivDyn.com

September 2017
Version 1.00



http://divdyn.com/docs/WiFi-vendor-video-stress-test.pdf

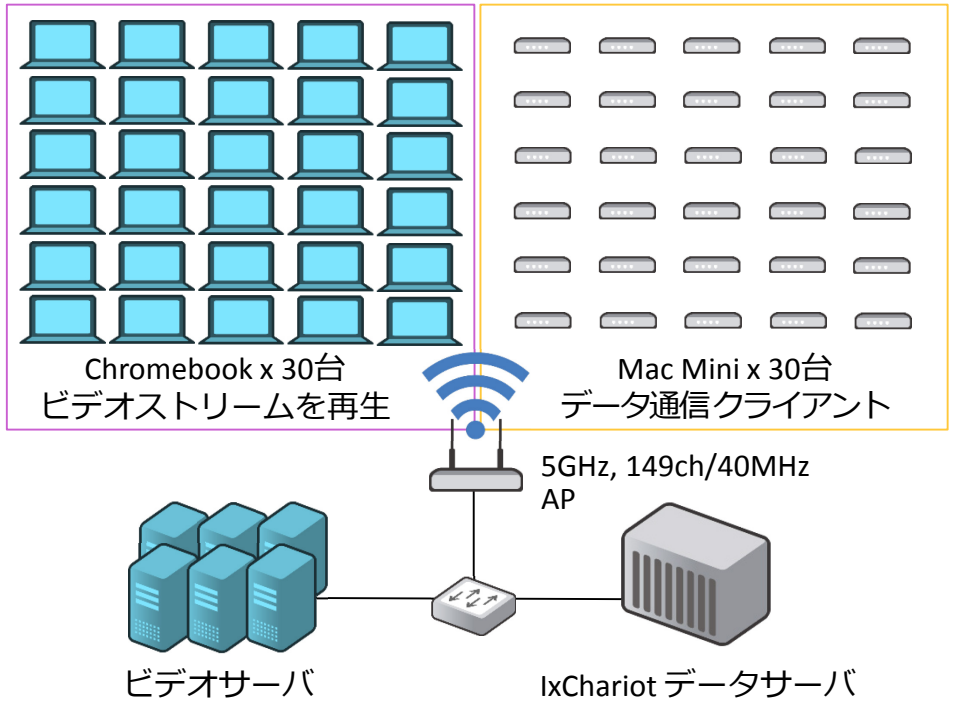
5社のミドルクラス 802.11ac Wavw 2 APを用いて、クライアント密度とビデオパフォーマンスの比較を行った試験のレポート
（2017年9月）

試験対象アクセスポイント

ベンダー	AP/コントローラ	ソフトウェアバージョン	MIMOタイプ
Ruckus	R610 with SZ100	3.5.0.0.832	3x3:3 11ac
Aruba	AP-305 with 7205	6.5.1.2	3x3:3 11ac
Aerohive	AP250	HiveOS 8.0rl build-161337	3x3:3 11ac
Meraki/Cisco	MR42	Cloud	3x3:3 11ac
Cisco	1850i with 5508	8.3.102.0	4x4:4 11ac

実環境で利用されているミドルクラスの 802.11ac Wave2 3x3:3 AP 製品を選択
メーカーから 3x3:3 の製品を入手できなかった場合は、次の上位モデルを選択

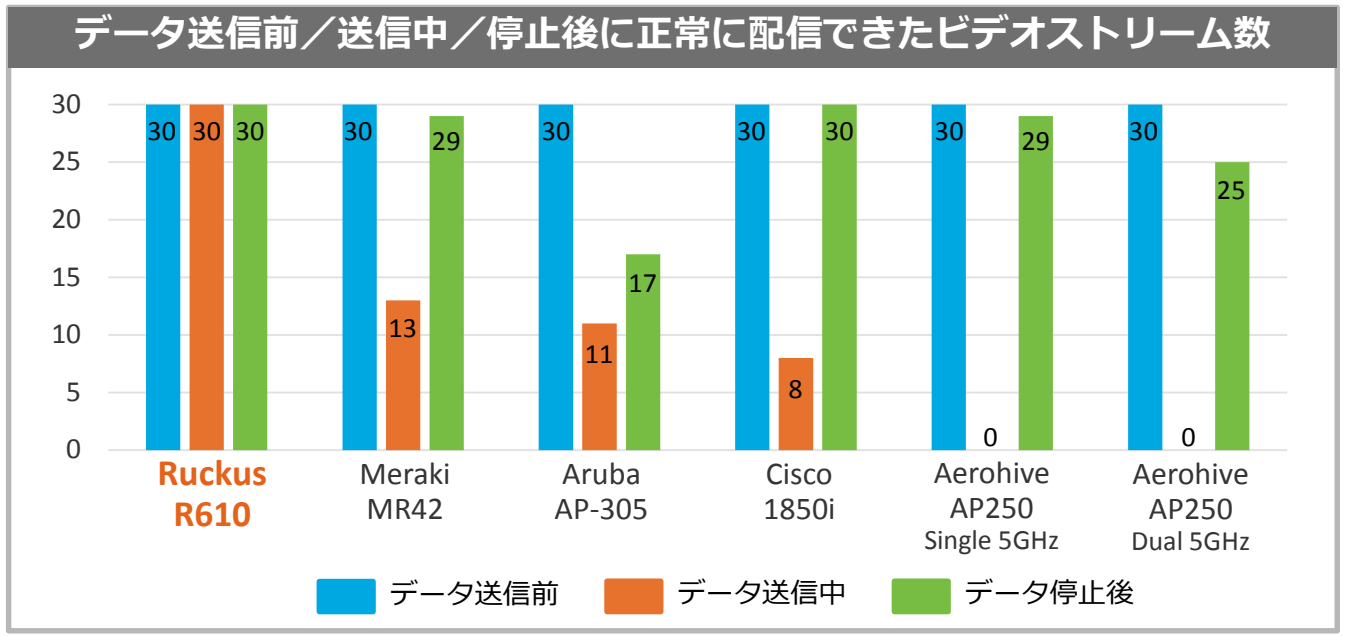
30ビデオクライアント & 30データクライアント

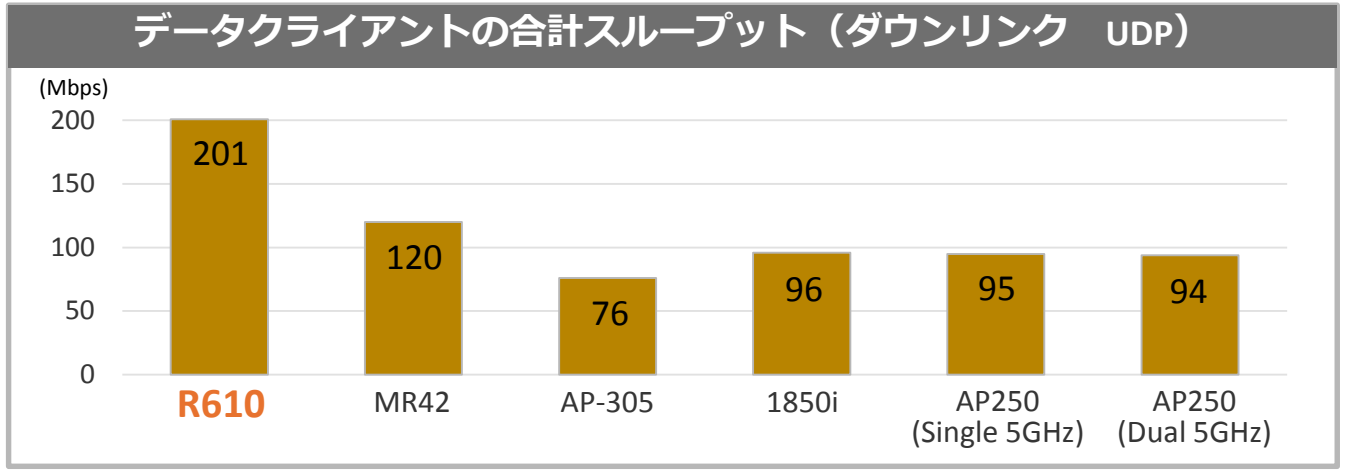


テスト手順：

1. Chromebook 30台でビデオを手動で起動
2. 全てのビデオが起動してから1分後に、隣の部屋に設置されているMac Mini 30台へデータ送信を開始。データ送信中に正常に配信出来ているビデオストリーム数をカウント
3. Mac Mini 30台のデータ送信停止し、再スタートしたものも含めてビデオストリーム数をカウント

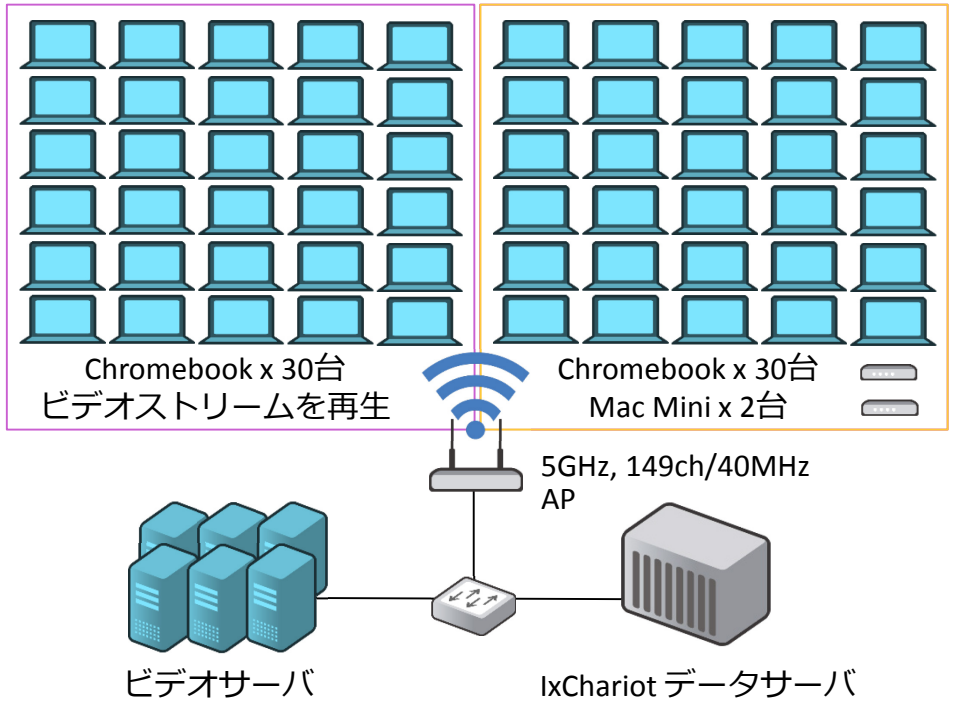
＊同じテストを3回繰り返す





Source: Client Density and Video Performance Comparison of Mid-range 802.11ac Access Points by Devin K. Akin

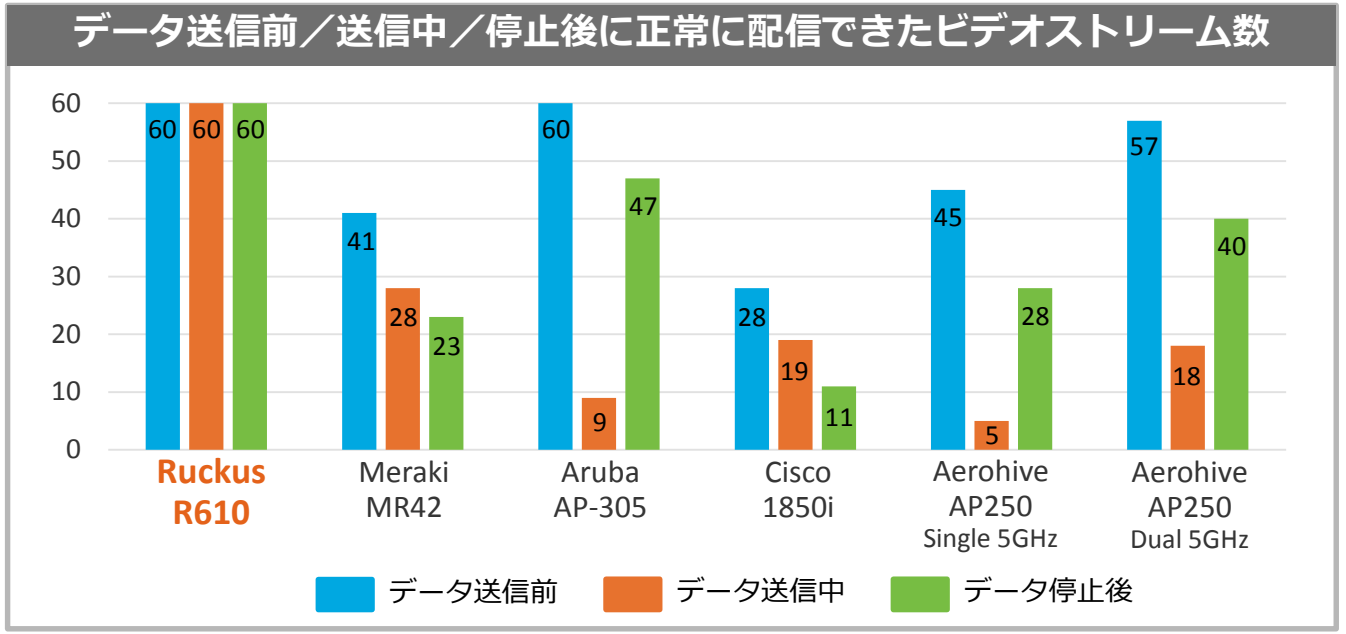
60ビデオクライアント & 2データクライアント

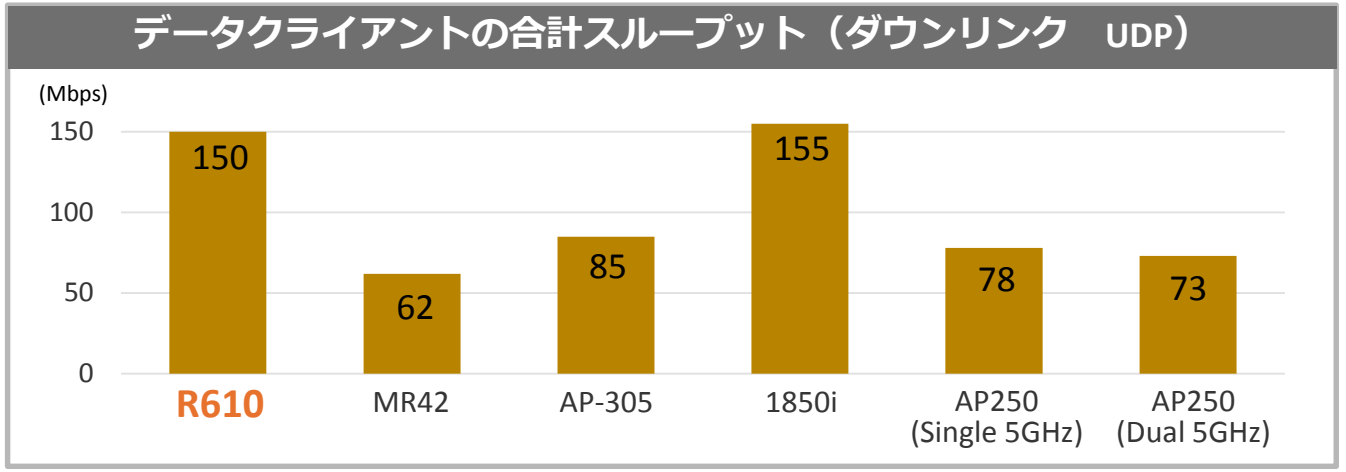


テスト手順：

1. Chromebook 60台でビデオを手動で起動
2. 全てのビデオが起動してから1分後に、Mac Mini 2台へデータ送信を開始。データ送信中に正常に配信出来ているビデオストリーム数をカウント
3. Mac Mini 2台のデータ送信停止し、再スタートしたものも含めてビデオストリーム数をカウント

＊同じテストを3回繰り返す





Source: Client Density and Video Performance Comparison of Mid-range 802.11ac Access Points by Devin K. Akin

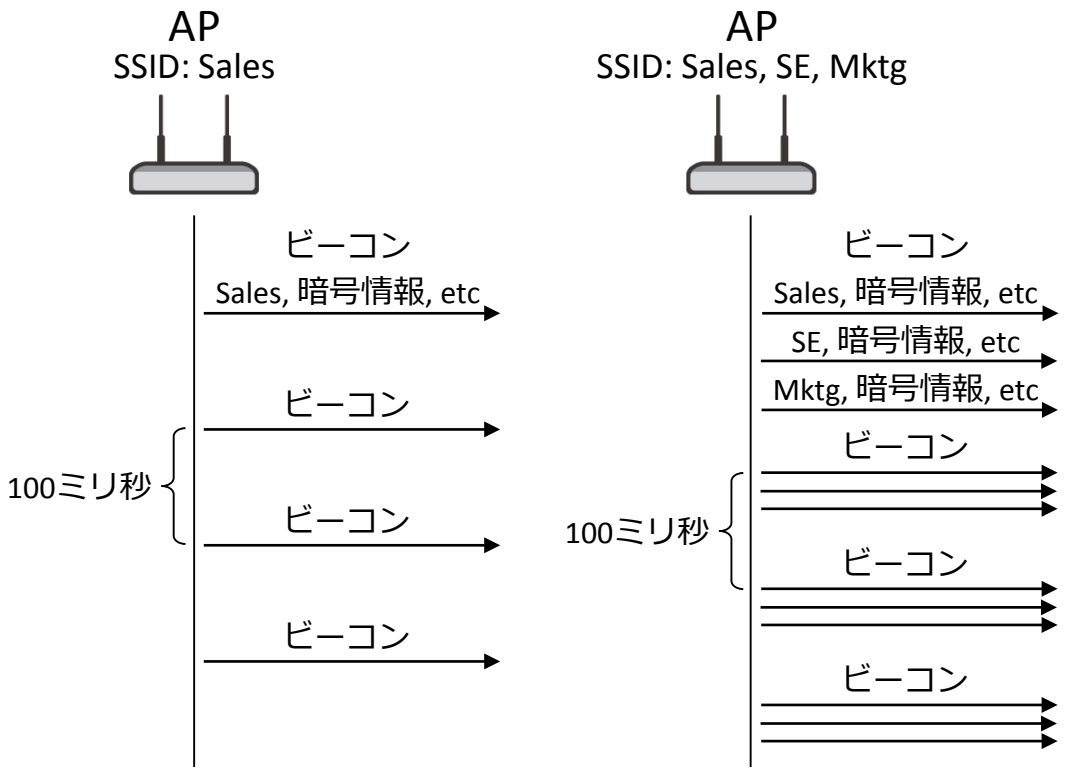
公衆 Wi-Fi に求められる要素

- 限られた設置条件で；
  - 希望エリアに対し100%のカバレージ
  - 高いスループット
  - ノイズに影響されない安定性
- 多数のAPを一元管理
- どんなクライアントでもつながる

無線LANで常に送信されている管理フレーム

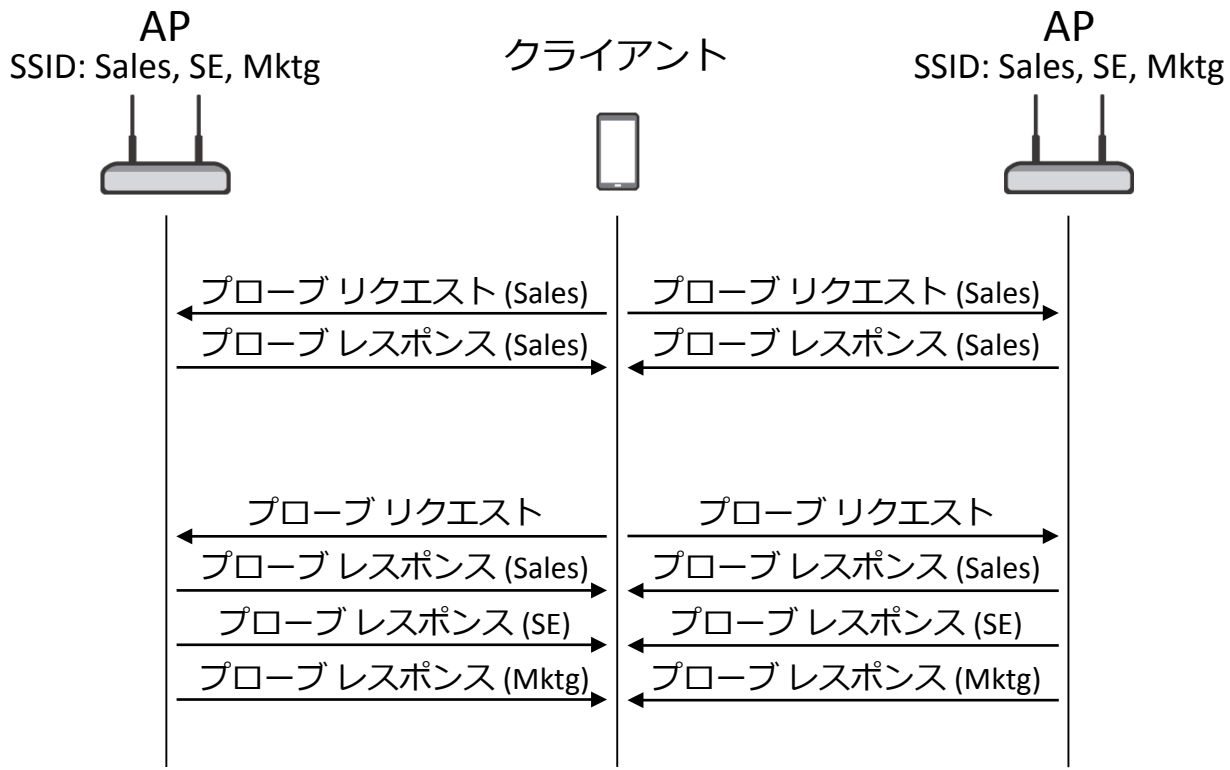
ビーコン（Beacon）

- APはSSIDや接続条件などの情報を含むフレーム
- APは一定間隔（通常100ミリ秒毎）でビーコンを送信し続ける
- 複数のSSIDをサービスしているAPは、SSID単位でビーコンを送信



プローブ リクエスト／レスポンス（Probe Request/Response）

- クライアントが接続したいSSIDをサービスしているかAPに問い合わせる
- 周囲のAPでサービスされているSSIDを問い合わせる
- 全てのチャンネルで行われる

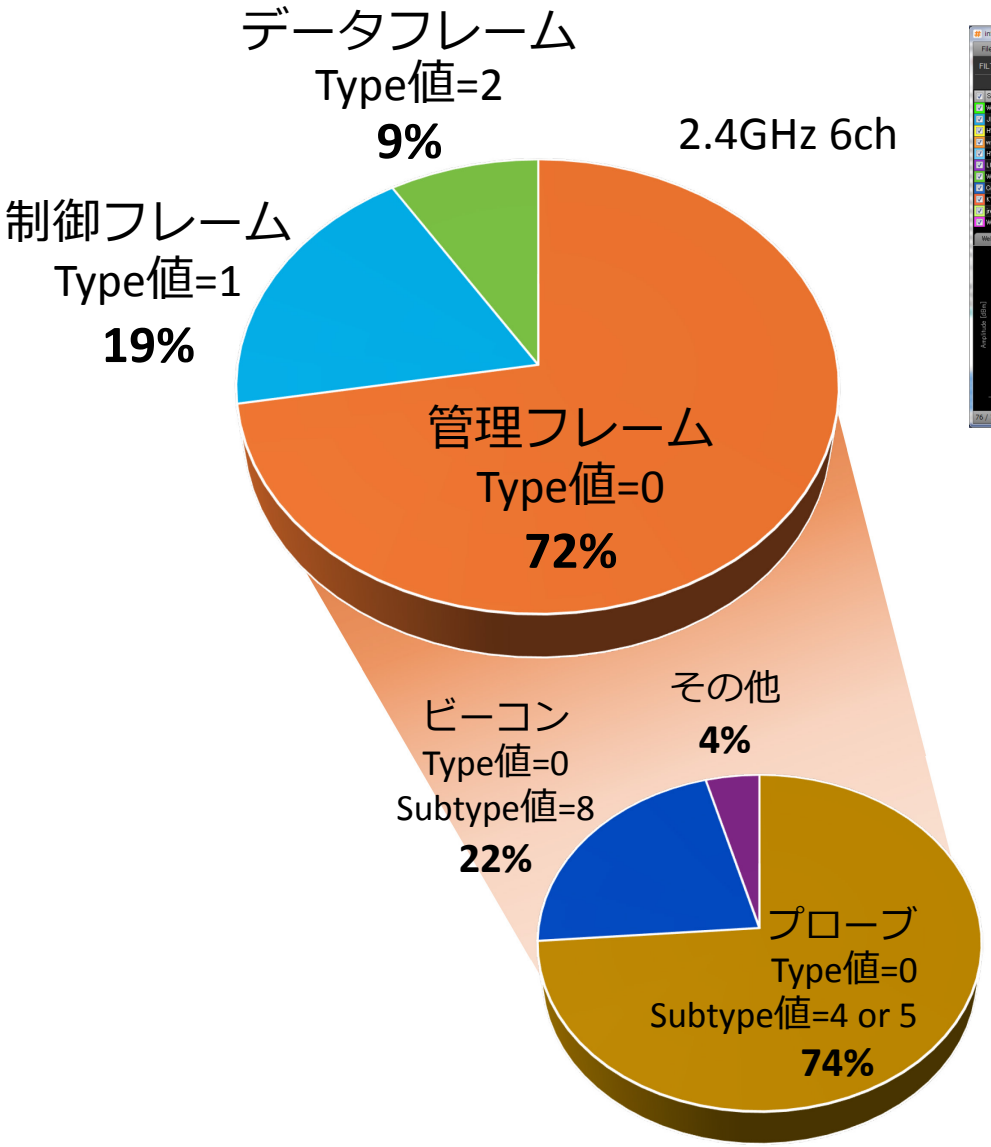


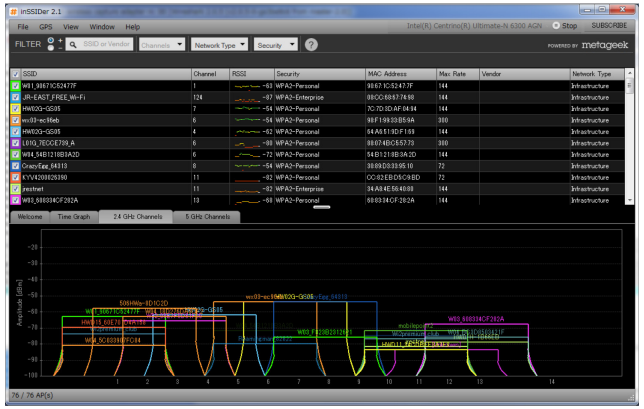
管理フレームの増大はスループットに影響あり

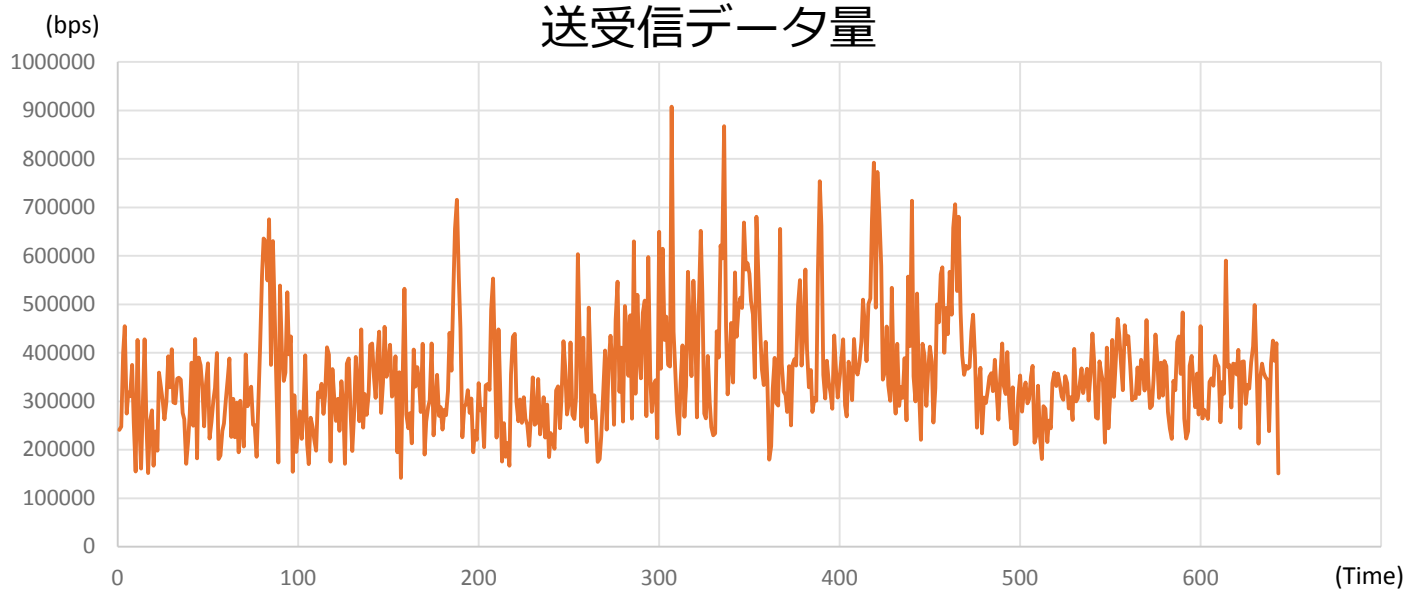
- SSIDを複数設定することで管理フレームも増加
- 無線LANクライアントデバイス数が増加し、管理フレームによるエアータイムの圧迫が深刻
- 通常、管理フレームは低い送信レートを利用が利用され、遠くまで届き影響範囲が大きい
- 一般的な無線LAN機器の受信感度
  - 2.4 GHz　1 Mbps: -95 dBm, 2 Mbps: -93 dBm, 6 Mbpa: -91 dBm
  - 5 GHz　　6 Mbps: -92 dBm
  - “**通信できる**”エリアと電波が“**届く**”エリアは違う

- 管理フレームの量を低減することもWi-Fi Allianceなどで検討されている

サンプルデータ：東京駅構内の無線環境



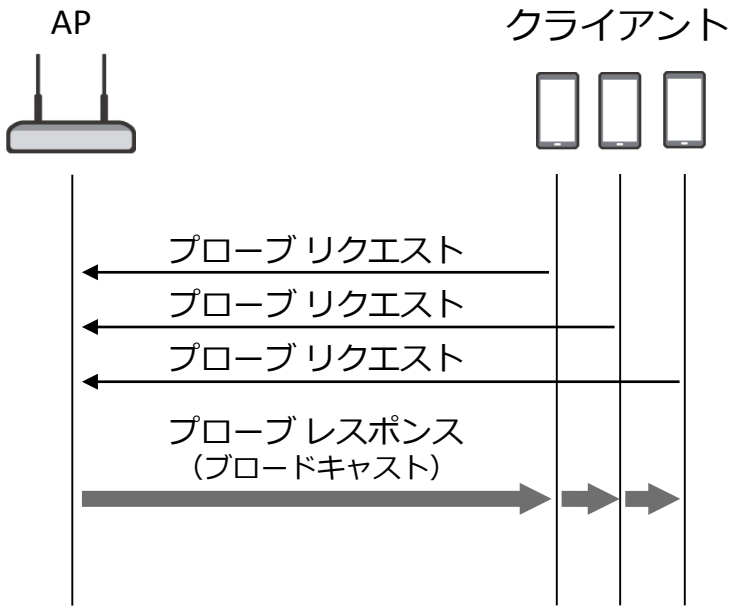




Wi-Fi Alliance Wi-Fi Vantage で無線環境の最適化

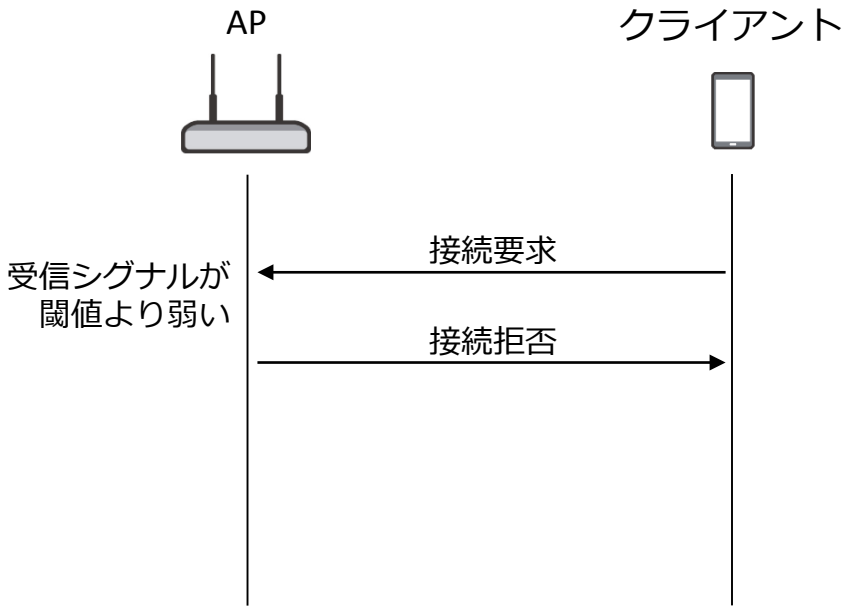
ブロードキャスト プローブ レスポンス

- Wi-Fi Vantage の機能のひとつ
- 複数のプローブリクエストに対し、レスポンスをブロードキャストの一回にする

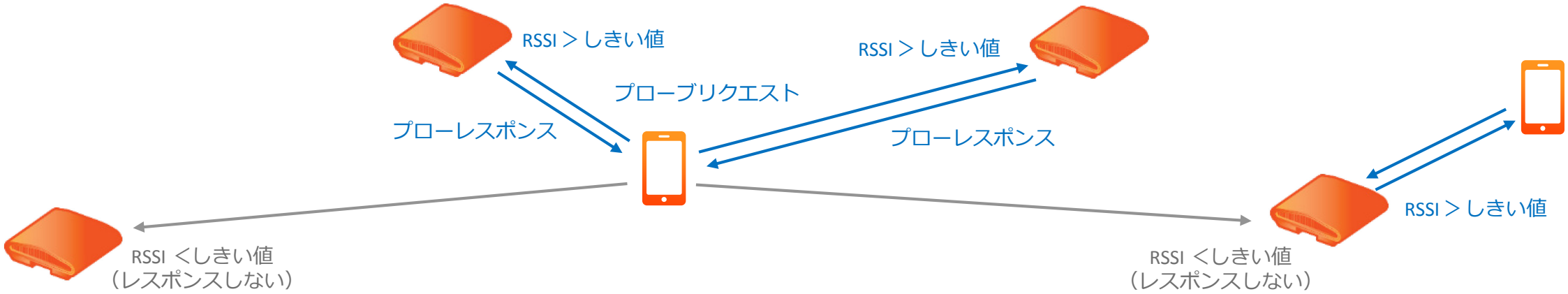


シグナルの強度で接続の可否を判断

- Wi-Fi Vantage の機能のひとつ
- クライアントから受信した接続要求フレームのシグナルの強さに応じて可否を判断
- シグナルの弱いクライアントが接続され、低速での通信や再送によって全体のパフォーマンスが低下することを回避

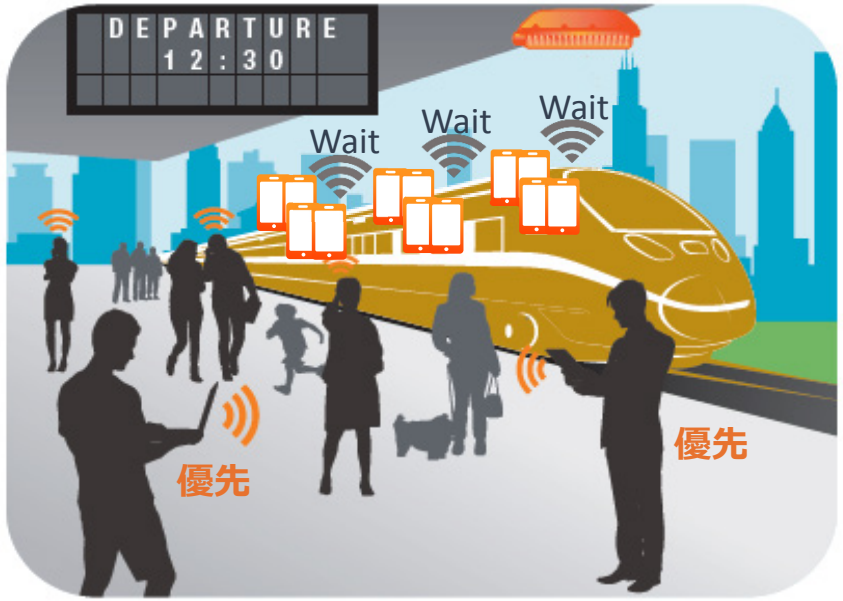


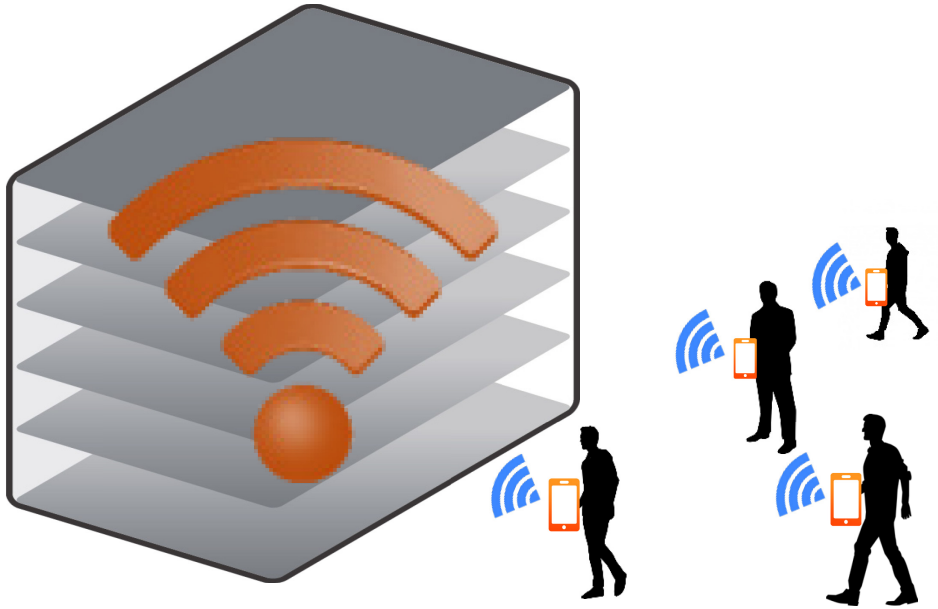
無線環境の混雑を回避し高スループットを維持



- 効率的な資源利用を実現するため信号が弱いプローブリクエストにはレスポンスしない
- データレートが低い機器との通信を行わず利用中ユーザのパフォーマンスを劣化させない
- クライアント負荷分散とは異なり 資源の有効利用が第一目的
- WLAN/SSID単位で設定可能

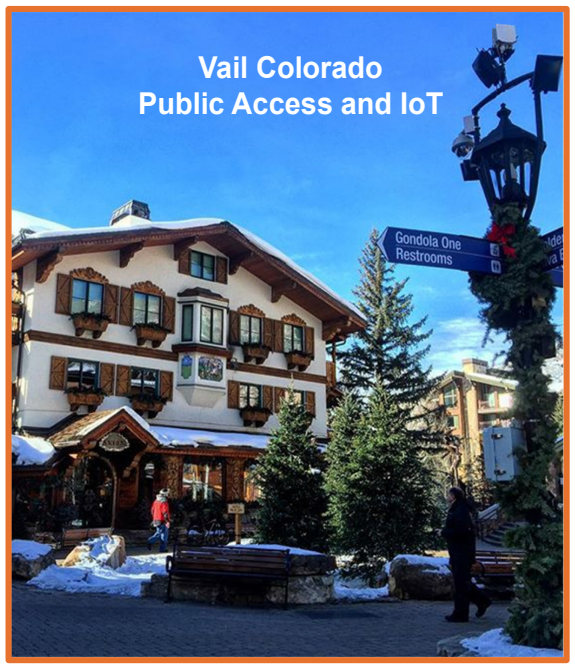
一時的なクライアントの制御





- タイマーを設定しWi-Fiクライアントの接続を制御
  - プローブリクエストに応答しない
  - 接続要求に応答しない／拒否する
- 不必要なプローブリクエストには応答しない
- 不意な接続を減らすことで切り替えのオーバヘッドをなくし、AP利用者のスループットを維持

City Wi-Fi
Wi-Fi はあらゆる都市で利用されている



カリフォルニア州　サンノゼ

要　求: 街全体をカバーし 大容量で拡張性のある屋内／屋外のキャリアークラスのWi-Fiが必要

ソリューション： Ruckusを標準化し 350 以上の AP を設置

CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

コンベンションセンター

サンノゼ国際空港

ダウンタウンのFree Wi-Fi

パーキングメーターシステム

ビデオ監視システム

公共の安全 - IP ビデオ と ビデオ分析

ソリューションフォーカス：

セキュリティ、交通、駐車などのためにビデオカメラを簡単に導入する

解決できる問題：

- より多くのIPビデオを展開したいと思っているが、各カメラに光ファイバー/同軸バックホールを敷設するのはとても高価で煩雑
- 深刻な渋滞問題があり、どのようにトラフィックや駐車を管理すればよいのか？
- 買い物客が駐車しやすくするために、駐車管理をどのように改善できるか？

AP + IoT ゲートウェイ

デバイス

Bluetooth
Wi Fi
Z-WAVE
LoRa

IoT LAN のコンポーネント

アクセス
ポイント

+

IoT
モジュール

WLAN
コントローラ

+

IoT
コントローラ

API

IoT 管理システム

スマート ホテル ルーム

ASSA ABLOY　ドアロックベンダー

スマート ドア ロック システムを導入したおかげで、簡単にかつ安全にルームキーを配布

チェックイン時、もうフロントで長蛇の列を待つ必要が無くなった不正侵入時、アラームも発報

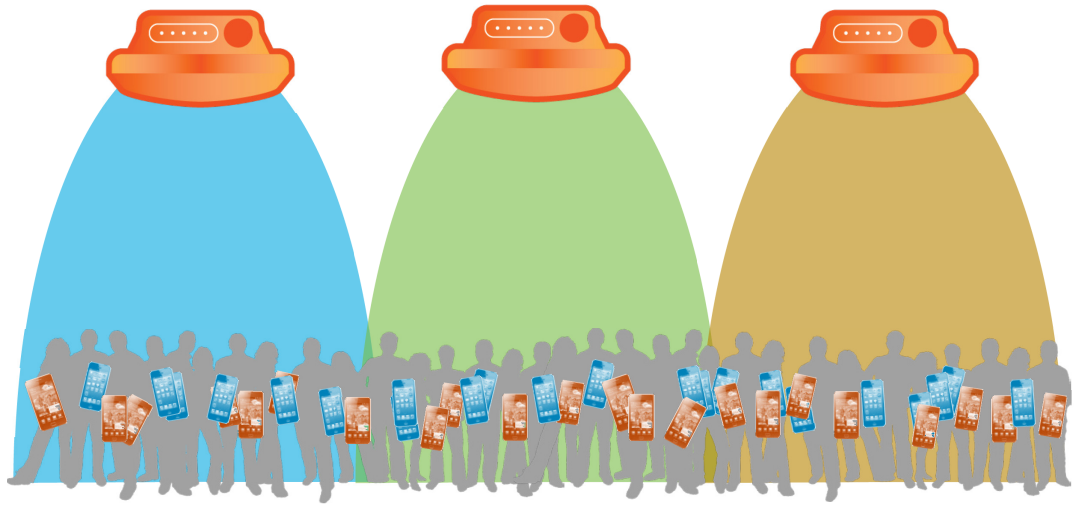
照明制御

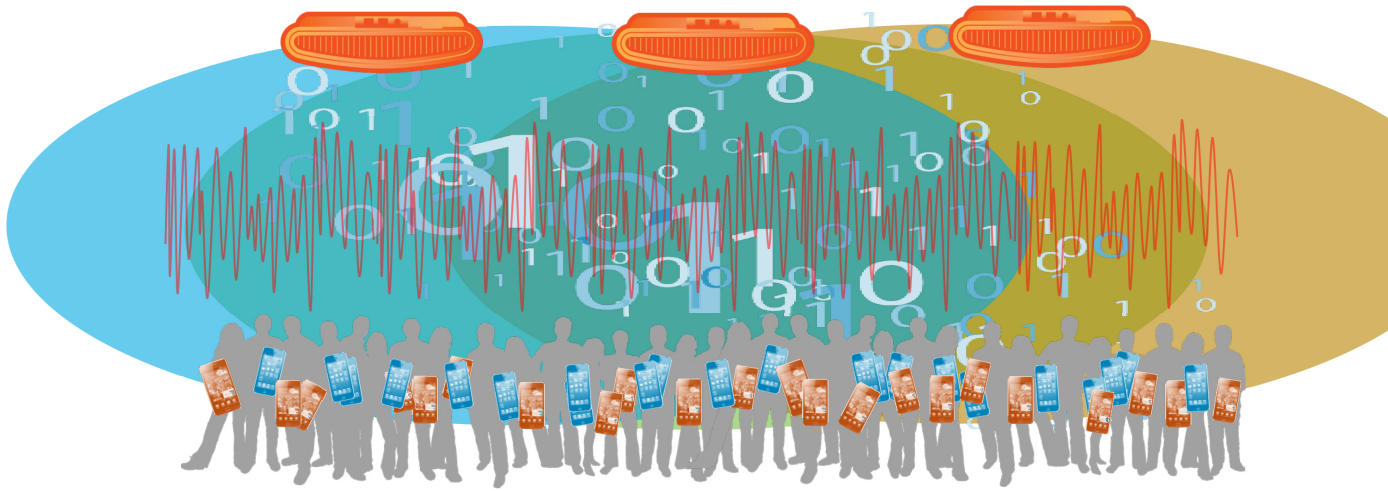
空調制御

ドアロック

AP + IoT

高密度環境で必要な要素





- 高密度環境ではセクターアンテナを利用し、管理フレームなど無線環境を分割
- プローブリクエストなどの管理フレームだけでなく、ユーザのデータフレームも無線環境として分割され、通信待ちのビジーを低減
- 無線LAN環境としての最適化と全体スループットの向上

FIFA World Cup & Rio Olympics　ブラジル

Maracanã
（マラカナン）
Rio de Janeiro

- 席数　76,000 席
- 設置AP数　217 台
- 30,000ユーザ
- 最大同時アクセス　11,000ユーザ
- ピークスループット　1Gbps

Estadio Nacional
（ナシオナル）
Brasilia

席数：71,000 席　設置AP数：217 台

Arena Fonte Nova
（フォンチ・ノヴァ）
Salvador

席数：50,433 席　設置AP数：151 台

Arena Pantanal
（アレーナ・パンタナール）
Cuiaba

席数：43,600 席　設置AP数：134 台

U2 コンサート

850GB
トラフィック

4,000
クライアント

1.6Mbps
2.4GHzの最低スピード

Thank You