COMMSCOPE®

Wi-Fi領域における規格

Internet Week 2019 S14 Wi-Fi 今昔物語

2019年11月28日

RUCKUS™

小宮　博美

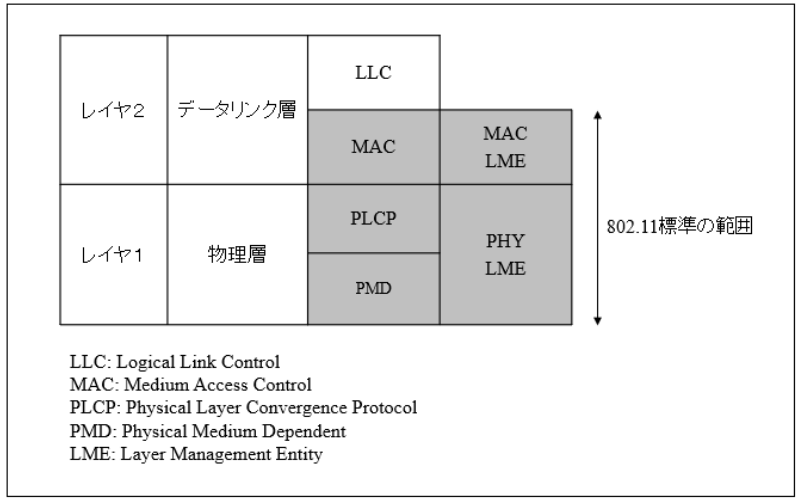
ラッカスネットワークス
テクニカルディレクター

進化を続ける無線LAN規格

世代	WFA呼称	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 5G 60G	2 Mbps	1997年 6月
2		802.11b	2.4G 5G 60G	11 Mbps	1999年 9月
3		802.11a	2.4G 5G 60G	54 Mbps	1999年 9月
3		802.11g	2.4G 5G 60G	54 Mbps	2003年 6月
4	Wi-Fi 4	802.11n	2.4G 5G 60G	600 Mbps	2009年 9月
5		802.11ad	2.4G 5G 60G	6,757 Mbps	2012年12月
5	Wi-Fi 5	802.11ac	2.4G 5G 60G	6,933 Mbps	2013年12月
6	Wi-Fi 6	802.11ax	2.4G 5G 60G	9,607 Mbps	2018年7月 ドラフト

‘97 802.11 無線 LAN 登場

- 1990 年に設立された IEEE *1 の 802委員会ワーキング・グループ 11が 1997 年に最初に無線 LAN の国際標準 IEEE 802.11 を策定
- 802.11 標準で規定された内容は、802.3 イーサネットと同様にデータリンク層の MAC *2 副層と物理層および、その管理機能
- MAC 副層のアクセス制御方式
  - ポーリング方式
  - CSMA/CA *3
- 物理層
  - 2.4 GHz 帯を利用した直接シーケンス・スペクトラム拡散方式 (DSSS *4)
  - 周波数ホッピング・スペクトラム拡散方式 (FHSS *5)
  - 赤外線通信方式
- 伝送レート：1, 2 Mbps
- 802.11 標準では速度は遅く、製品も限られていた



*1: Institute of Electrical and Electronics Engineers (米国電気電子技術者協会)
*2: Medium Access Control
*3: Carrier Sense Multiple Access with Collision Avoidance
*4: Direct Sequence Spread Spectrum
*5: Frequency Hopping Spread Spectrum

’99 802.11b – 2.4 GHz 帯で 11 Mbps へ高速化

- 802.11 標準との互換性を保ちながら伝送レートを 11 Mbps まで高速化した 802.11b が 1999 年に策定
- 物理層
  - 2.4GHz 帯に Intersil と Lucent Technologies が共同提案したCCK *1 方式を採用
- 伝送レート：1, 2, 5.5, 11 Mbps
- 暗号：WEP

- 家庭で常時接続のブロードバンド回線および、省スペース効果のあるノートＰＣの普及により、配線不要な無線 LAN の導入が家庭で進む
- 暗号化などセキュリティ面では十分とは言えないが、無線 LAN 製品の普及には貢献
- 100 Mbps のイーサネットが当たり前になった企業では、無線 LAN は遅く、不安定で安全ではないと考えられ、導入が進まない

*1: Complementary Code Keying

’99 802.11a – 5 GHz 帯を利用し最高 54 Mbps

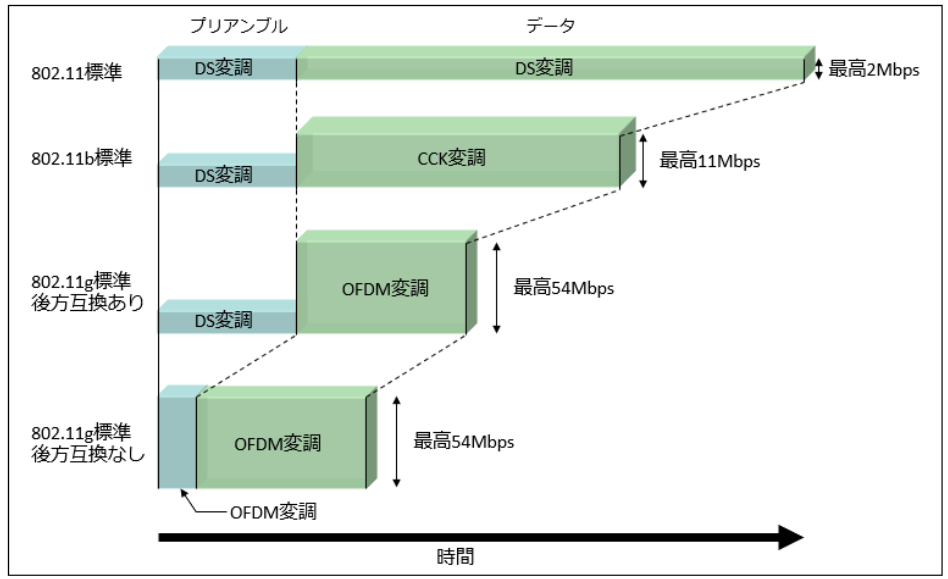
- 1997年に米国 FCC[*1] が 5GHz 帯の 300 MHz (5.15～5.35 GHz, 5.725～5.825 GHz) の帯域を開放したのに伴い、最高 54 Mbps の 802.11a が 1999 年に策定
- 物理層
  - NTTとLucent Technologiesが共同提案した直交周波数分割多重 (OFDM [*2])方式を採用
  - データを 48 の低速データ列に分割し、サブキャリアを用いて並列伝送
- 伝送レート：6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 暗号：WEP

- 802.11, 802.11b との互換性なし（互換性を考慮せず高速化を優先）
- 日本では 5.15～5.25GHz (J52) の 100MHz (4チャンネル) が屋内利用限定で無線LAN用に開放された
- 802.11a/5 GHz の無線チップ／モジュールの製造メーカーが限られていた（Atheros、NTT）
- 無線チップが限られていたため、当初は製品化も進まなかった

*1: Federal Communications Commission (連邦通信委員会)
*2: Orthogonal Frequency Division Multiplexing

’03 802.11g – 2.4 GHz 帯でも 54 Mbps を実現

- 2.4GHz帯で後方互換性を保ちながら 802.11a 同様の高速化を実現した 802.11g が 2003 年に策定
- 物理層
  - CCK方式に 802.11a で採用された OFDM を追加
  - 後方互換を維持するため、プリアンブル部分を DSSS 方式で伝送（このオーバーヘッドがパフォーマンスに影響を与える）
- 伝送レート：1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- 暗号：WEP



- 802.11b と同じ 2.4 GHz 帯を利用していることから、機器の802.11g 対応が迅速に行われると共に、低価格化も進み、無線 LAN 製品の利用が広まる
- 企業でも会議室など部分的ではあっても導入が始まる

’09 802.11n – 無線 LAN で 100 Mbps 以上の高速化

- 複数のアンテナで送受信を行う MIMO*1 と 2個のチャネルを束ねて利用するボンディング技術を取り入れ、最高伝送レート 600 Mbps の 802.11n が 2009 年に策定
- 物理層
  - 2.4 GHz, 5 GHz
  - OFDM
- 伝送レート：1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps, MCS インデックス
- 暗号：WEP, TKIP, AES

- 電波法の省令改正も行われ、多くのチャンネルの開放と40 MHz通信が可能になった
- 多くの技術が盛り込まれ、高速化、信頼性の向上、セキュリティの強化が実現し、企業の導入意欲が高まっていたこともあり、ドラフト段階から多くの製品が市場投入された
- クライアントデバイスの無線 LAN 対応が進むと共に、有線より安価に柔軟性のあるネットワークが構築できるようになる
- パブリック Wi-Fi サービスが本格的に始まる

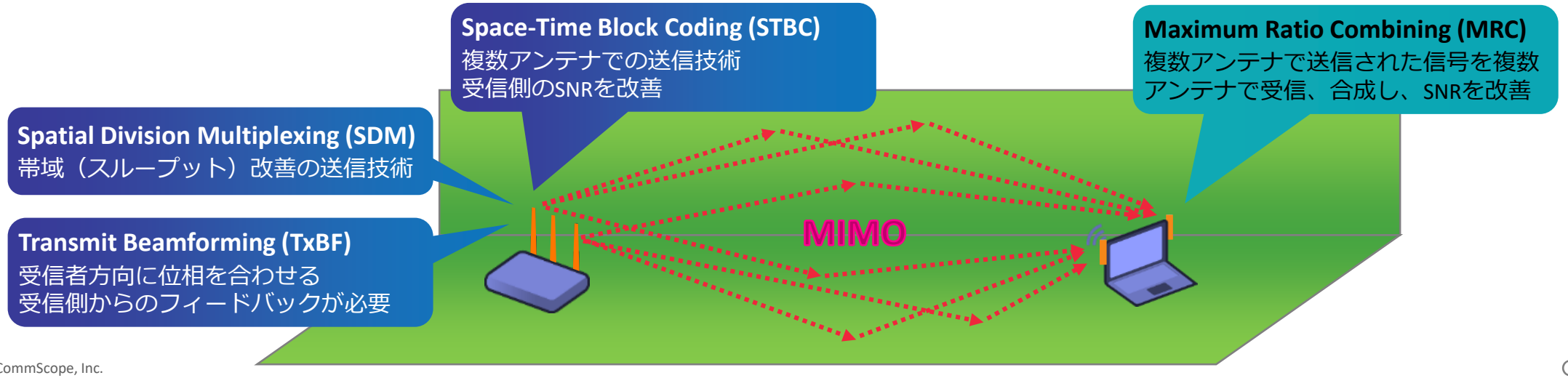
*1: Multiple Input Multiple Output

802.11n ハイライト

- 100Mbpsを超えるスループットを目的とし、それを最大伝送レート 600 Mbpsで実現
- 2.4G, 5G Hzの両帯域をサポート
- 変調方式に OFDM を採用し、後方互換性を確保
- MIMO を採用し、複数の空間ストリームでの送受信を行いスループットを向上
- MIMO は、接続安定性と到達距離も改善
- チャネルボンディングで利用帯域幅を増やし、伝送効率を向上
- オーバーヘッドを軽減するパケット集約機能と制御時間の短縮
- AES の採用で、脆弱性のある WEP, TKIP からの脱却

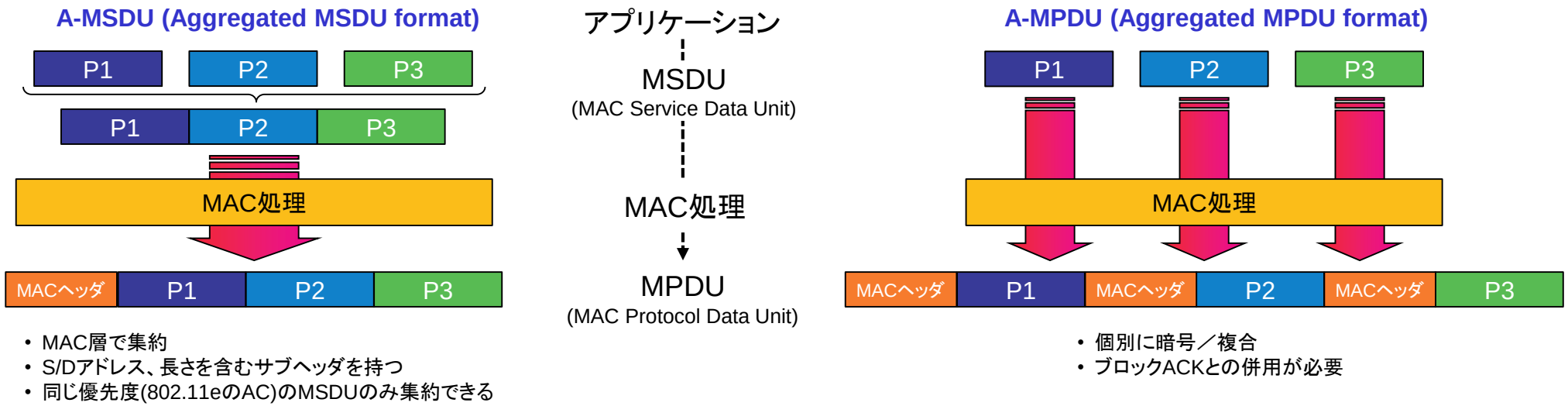
802.11nで採用された技術：MIMO

- Multiple Input Multiple Output： 複数のアンテナで送受信を行う技術
- m x n (m: 送信アンテナ数、 n: 受信アンテナ数)
- 802.11n では 2x1 から 4x4 まで定義されている
- 2本以上のアンテナで異なる空間ストリームを送信し 2本以上のアンテナで高度な信号処理を行って受信
- 高速化と共に安定性と耐障害性を実現し、電波の到達距離も延長
- 反射信号の利用も可能なので、802.11a/g ではカバーしづらかった物陰にも強い
- 802.11n(MIMO) APとレガシー 802.11a/g クライアント間通信のスループットも最大 30% の向上が見込める



802.11nで採用された技術：パケット集約

- 複数のデータ・パケットを 1個の 802.11フレームで伝送する技術
- 802.11ヘッダーとACKのオーバーヘッド、送信権の取得回数、衝突を削減し伝送効率を向上
- A-MSDUとA-MPDU
- ブロックACK（複数パケット分のACKを１つに集約、802.11e に規定あり）
  - 11a/b/gでは、パケットとACKは1：1
- ファイル転送などのアプリケーションには有効だが、音声のようにリアルタイム性が高いアプリケーションには不向き
  - パケット間隔が広がる場合も発生し、遅延によって音声品質が劣化する

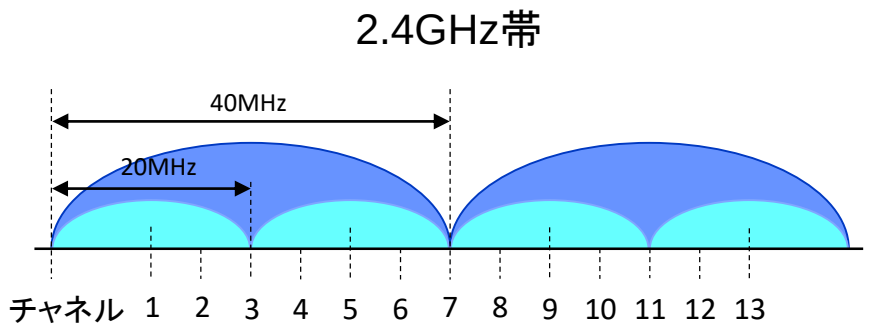


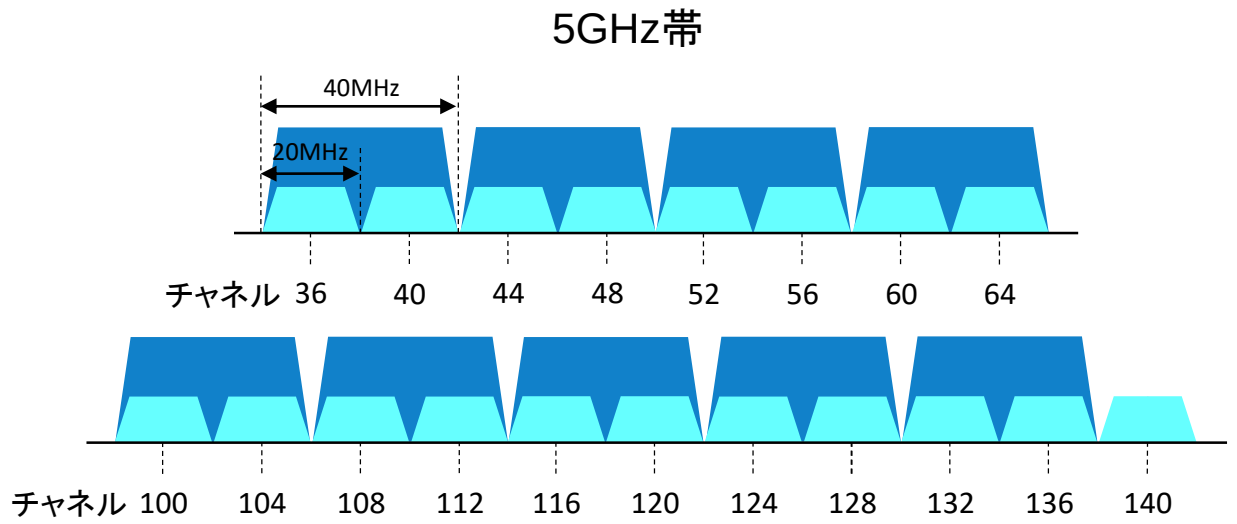
- MAC層で集約
- S/Dアドレス、長さを含むサブヘッダを持つ
- 同じ優先度(802.11eのAC)のMSDUのみ集約できる

- 個別に暗号／複合
- ブロックACKとの併用が必要

802.11nで採用された技術：チャネル・ボンディング

- 隣接する2個のチャネルを使用し 40MHz の帯域で伝送を行う
- 利用する帯域幅を増やすことで伝送効率を向上
- 2倍の帯域幅を利用すると、伝送レートもほぼ 2倍になる
- 電波法では 40MHz での無線LAN通信が認められていなかったが、2007年6月の電波法の一部改正で利用可能になった
- 2.4GHz はチャネル数が少ないので、現実的には 5GHz向け





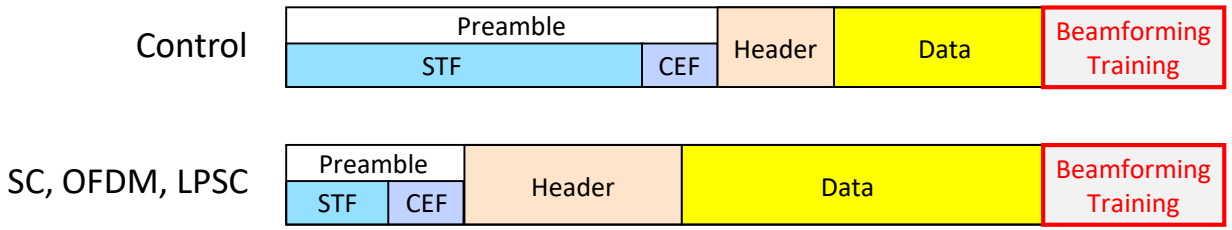
’12 802.11ad – 60 GHz 帯の広帯域を使った大容量通信

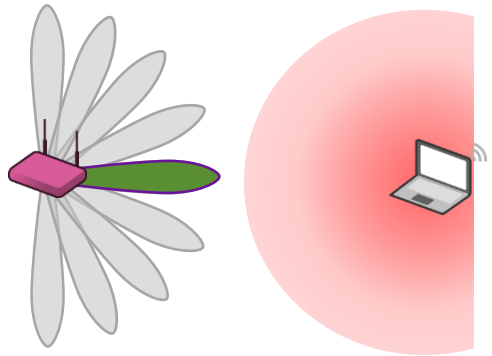
- 映像伝送を主な用途とした近距離、大容量通信のためのミリ波の 60 GHz 帯を利用した 802.11ad が2012 年に策定
- 物理層
  - 60 GHz
  - Control, Single Carrier, OFDM, Low Power Single Carrier PHY
- 伝送レート：各 PHY で異なる MCS インデックス (最高 6,757 Mbps)
- 暗号：AES-CCMP/GCMP

- 60 GHz 帯は免許不要な帯域で、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）
- 2.16 GHz という非常に広い帯域を利用した伝送で マルチギガビット／秒 を実現
- 60 GHz の電送波は直進性が高く、減衰しやすい。そのため、回り込みはほとんどなく、高速通信可能な距離は 10m 程度
- MIMO は定義されていないが、ビームフォーミングは仕様に取り込まれている
- 802.11a/b/g/n/ac と互換性はないが、シームレスな切り替え方式は規定されている

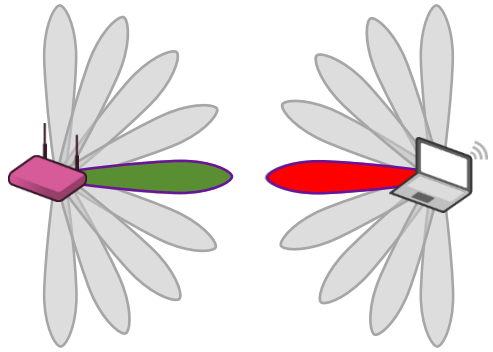
802.11adで採用された技術：PHY Beamforming Training

- 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

’13 802.11ac – 無線 LAN で 1 Gbps 越えのスループット

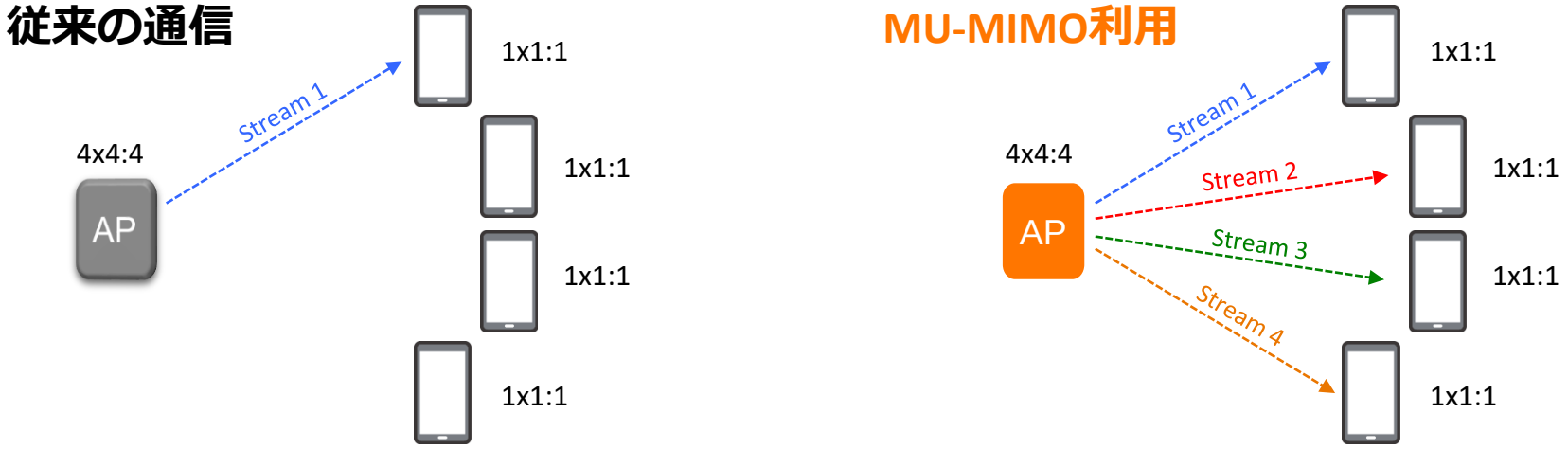
- より効率的な変調方式と広帯域を使い、最高伝送レート 6,933 Mbps の 802.11ac が 2013 年に策定
- 物理層
  - 5 GHz
  - OFDM
- 伝送レート：簡素化された MCS インデックス
- 暗号：AES

- 2014 年の Wave 1、2017 年の Wave 2 の 2 ステップで導入
- 2013 年 3 月に 11ac 導入に向けた電波法の改正が行われ、広帯域を使った伝送が可能となった
- MU-MIMO *1 の導入
- クライアントー AP 間の伝送レートは飛躍的に向上したが、11n で実用性のあるスループットを得られていたため、当初の 11ac への移行はスローペース
- 標準では 8 空間ストリームまで規定されているが、4 空間ストリームを超える製品はほとんどなく、市場のクライアントは 2 空間ストリーム製品が主流

*1: Multi-User Multiple Input Multiple Output

802.11ac ハイライト

- 対象帯域は 5GHz のみで完全後方互換
- 全てのフレームを A-MPDU に統一
- より効率的な 256-QAM の採用で、伝送レートを 33% 向上
- チャネルボンディングに 80/160/80+80 MHz を追加
- MIMO の対象アンテナ数を 8 個まで増加させ、最大空間ストリームを 8 に拡張
- 最大 4 台のクライアントへ同時に送信を可能にした下り MU-MIMO



802.11ax – 伝送の最適化で総スループットを向上

- ユーザあたりのスループットを 4 倍以上にすることを目標に、 802.11ax の標準化が進められ、2018 年 7 月にドラフト化、標準化完了は 2020 年中旬の見込み
- 物理層
  - 2.4 GHz, 5 GHz
  - OFDM, OFDMA *1
- 伝送レート：簡素化された MCS インデックス
- 暗号：AES

- 11ac と同様に 2ステップ（Wave 1/2?）での導入が見込まれている
- 11ax 導入に向けた電波法の改正は 2019 年 7 月に行われた
- 無線 LAN クライアントの密度が非常に高くなっている現在、無線環境の利用効率を向上し、エリア全体でのスループット向上が期待されている
- iPhone 11 が 11ax をサポートしたことにより、他製品の追随と導入の加速が見込まれる

*1: Orthogonal Frequency Division Multiple Access

802.11ax ハイライト

- 2.4G, 5G Hz の双方が利用可能で、後方互換
- LTE で利用されている OFDMA の採用
- 下りに加え、上り MU-MIMO を追加
- FFT サイズ、サブキャリア間隔、OFDM シンボル長に変更を加え、PHY/MACの効率化
- 1024-QAM 追加で伝送効率を 25% 向上
- 効率的な省電力 - Target Wake Time
- 高密度環境を可能にする BSS Coloring
- Wi-Fi Alliance の認定は、2 ステップで考えられている

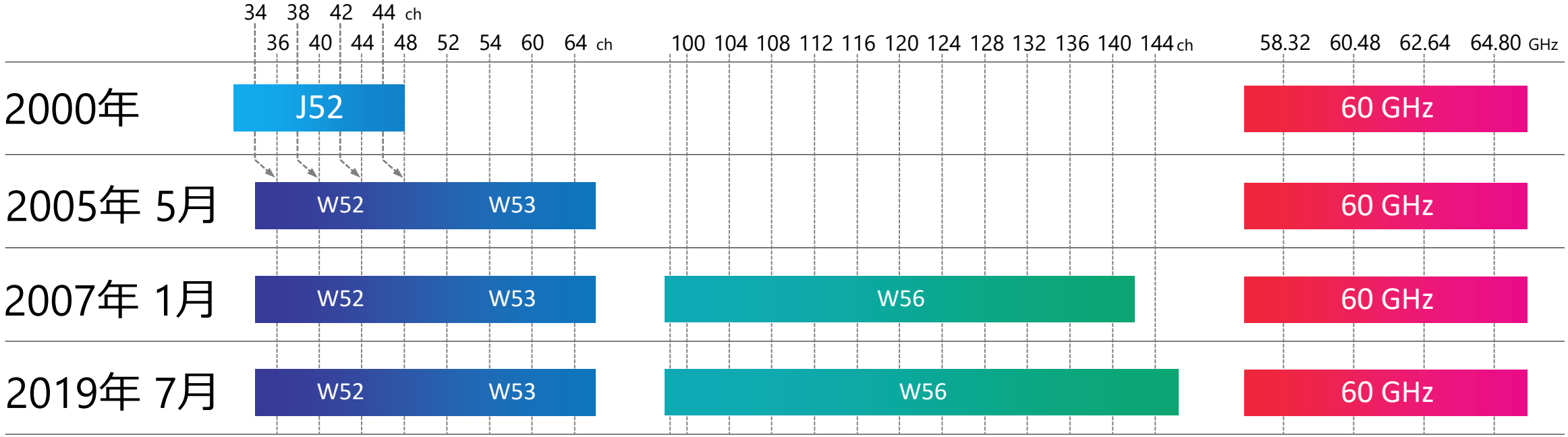
Spec 1	Spec 2
DL and UL OFDMA	UL MU-MIMO
DL MU-MIMO	Spatial re-use
BSS coloring	160 MHz
Target Wake Time	Long Range 802.11ax
20 MHz Only	**6 GHz** *1

*1: 5.925 GHz – 7.125 GHz (1.2 GHz) のアンライセンスバンド

日本の法整備の流れ

1992年12月	「小電力データ通信システム」として、初めて 2.4 GHz 帯 (2,471～2,497MHz) 無線LANを導入
1999年10月	802.11b導入に向けた改正
2000年 3月	802.11a導入に向けた改正 屋内用 5.2 GHz帯 (5,150～5,250 MHz) を開放
2001年 9月	802.11g導入に向けた改正
2005年 5月	802.11a拡張向け改正 日本独自のJ52 (34,38, 42,46 ch)を国際的なW52 (36,40,44,48 ch)に変更 W53 (52,56,60,64 ch)を新たに追加、開放
2007年 1月	屋外で利用可能な 5GHz帯のW56 (100,104,108,112,116,120,124,128,132,136,140 ch)を追加、開放
2007年 6月	802.11n導入に向けた改正
2008年 5月	J52からW52への変更に伴い、クライアントデバイスに認められていた経過措置が終了し、J52対応製品の製造が不可となる
2013年 3月	802.11ac導入に向けた改正
2018年 6月	登録局制度の下で5.2 GHz 帯無線 LAN の屋外利用を可能にし、同時に高出力化（仰角 8 度未満で最大EIRP 1 W）を実現
2019年 7月	802.11ax導入に向けた改正 W56に144 chを追加、開放

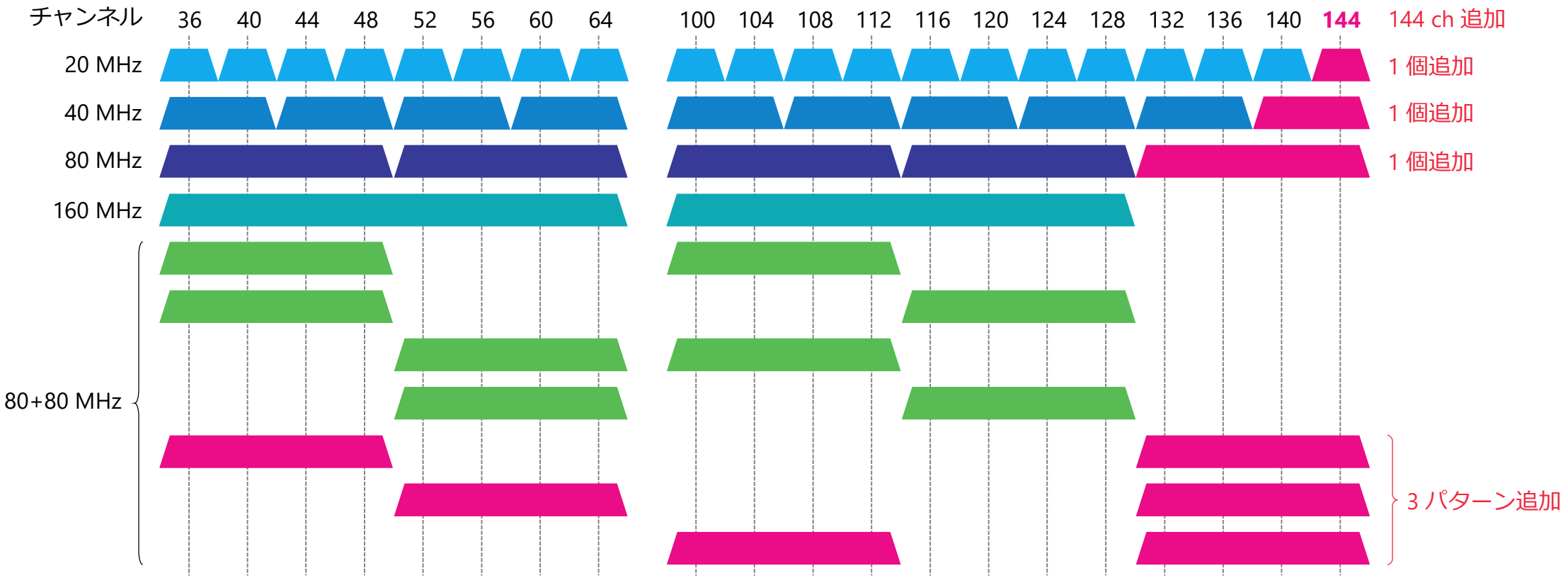
5G / 60G Hz帯 チャンネル解放推移



- 5GHz 帯無線LANに利用できる周波数は、当初日本独自の J52 で 国外製品との互換性がなかった
- 2005 年に省令改正され、国際標準のチャンネルを利用するようになるが、以前の製品との互換性はない。同時に W53 も利用可能になる
- 無線 LAN の普及が進み、2007 年に W56 も利用可能となる
- 144 ch も利用可能とし、大容量通信に有用なチャンネルボンディングの運用性を高める

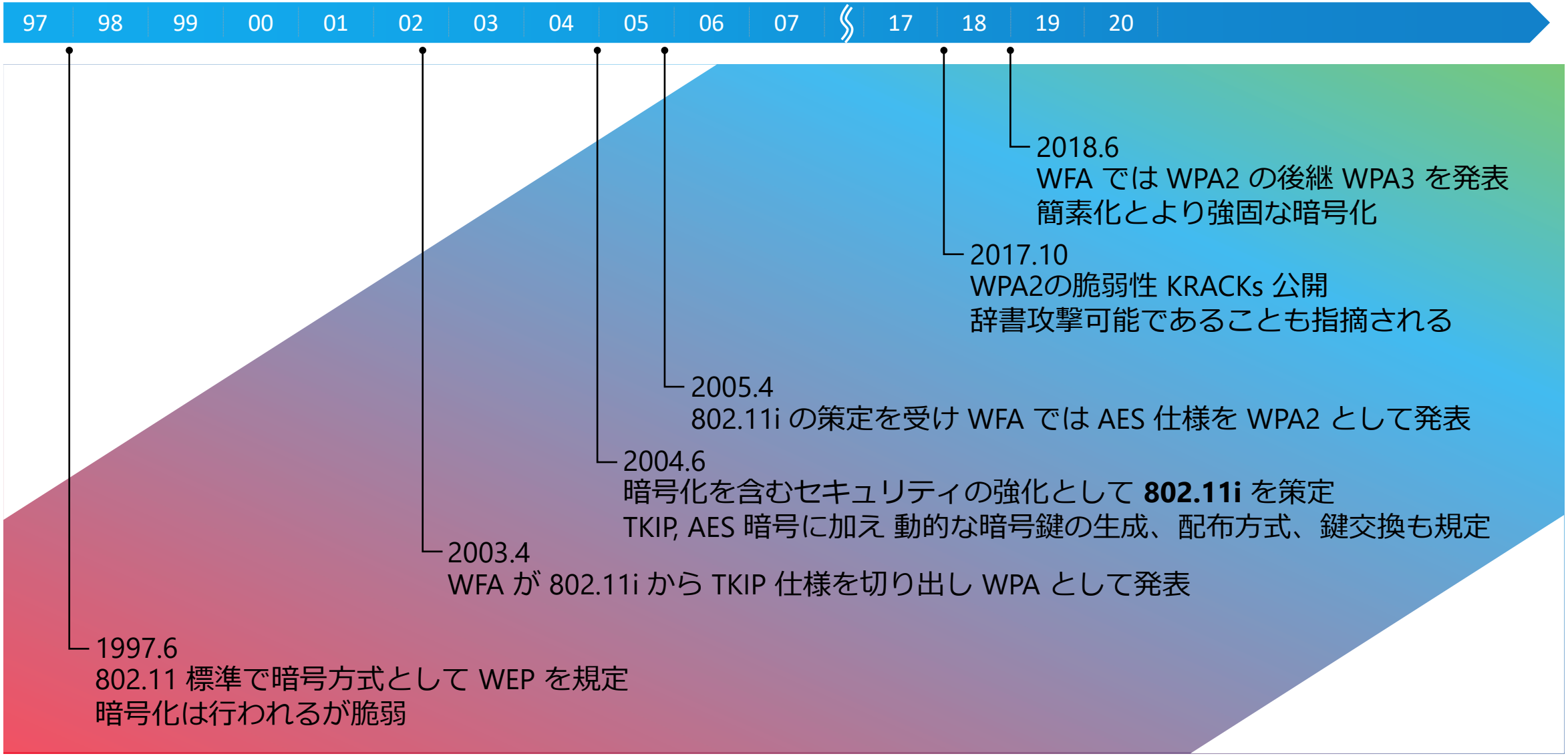
144 ch を解放する効果

- 20MHz幅の144chを開放することで、40MHzチャネル1個、80MHzチャネル1個、80+80MHzチャネル3パターンを追加することが可能



COMMSCOPE

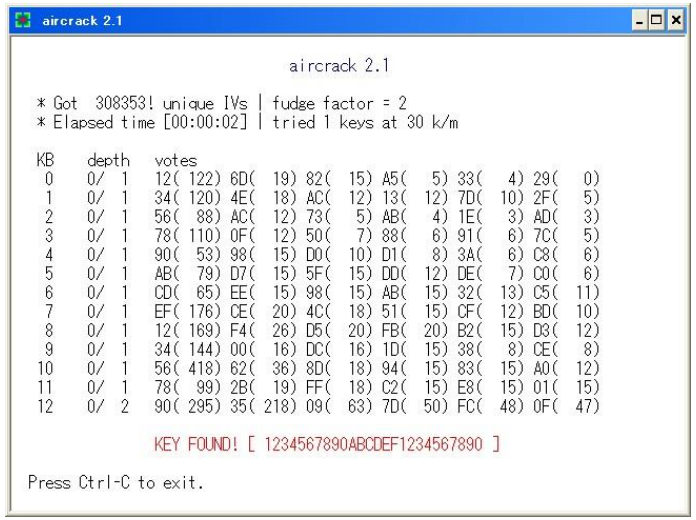
Wi-Fi セキュリティの進化



WEP の脆弱性

- 802.11 では WEP 鍵の配送方法が規定されていない
  - 全ての機器に同一の鍵を事前に設定しておかなければならない
  - 管理を徹底しなければならない鍵を全てのユーザが知っているということになる
  - 鍵の変更も全ての機器で同時に設定変更をしなければならない
- 暗号アルゴリズムに RC4 (Rivest Cipher 4) を利用している
  - 1バイト単位で簡易な暗号化を行なうブロック暗号アルゴリズム
  - 簡易な暗号アルゴリズムと 40/104 ビットの鍵の短さが弱点
  - ある程度の暗号化されたパケットを収集すれば解読できる

WEPでは、入力された40ビットまたは、104ビットの鍵に24ビットのIV(Initialization Vector: 初期化ベクタ)を加え拡張鍵を作成する。平文1バイトに対し作成された拡張鍵から1バイトが抽出され、排他的論理和を実行し暗号文1バイトが完成する。あとはこの作業を繰り返し、暗号文を完成する。完成した暗号文は、IVと共に送信される。WEPで暗号化する範囲には既知の情報が多く存在するIPヘッダも含まれるため、IPヘッダの情報と暗号化した結果が判れば逆算して鍵を求められる。残りの問題は鍵の配列だが、特定のIV(Weak IV)で特定の場所の鍵が使われる可能性が高いということが判明していて、このWeak IVをいくつか集めれば最初の1バイト目から順に鍵を解読することができる。実際、クラック・ツールを使い300,000程度のパケットを収集し、約2秒で104ビットの鍵の解読に成功。



恒久対策にはならない TKIP

- 一時鍵を用いて鍵混合を2段階行い、パケットごとに異なる鍵で暗号化されるように工夫
- WEP で脆弱とされた IV も倍の長さの 48 ビットに拡張
- Weak IVを使わない工夫も実装
- 既存の機器がファームウェアの更新のみで対応できるよう考慮し、暗号アルゴリズムは WEP と同じ RC4 を利用

- TKIPは WEP の脆弱性を補っているが、暗号アルゴリズムが RC4 で弱く、解読されるリスクは残る
- WEP があまりに脆弱だったため、AES が規格で取り入れられるまでの暫定措置

暗号アルゴリズムを一新した安心の AES

- AES *1 は、ホァン・ダーメン (Joan Daemen) 氏とフィンセント・ライメン (Vincent Rijmen) 氏が開発した暗号アルゴリズム ラインデール (Rijndael) を採用した新たな暗号化方式
- 米商務省技術標準局 (NIST) がこれまで利用してきた DES *2 に変わる新しい標準暗号化方式として採用
- AES は DES を強化した 3DES より安全と言われている
- 鍵長によって処理の段階数が異なる
  - 128ビットの鍵長では、10 段階の処理
  - 192ビットの鍵長では、12 段階の処理
  - 256ビットの鍵長では、14 段階の処理
- AESでは比較的軽い処理を 1 段階とし、同じ処理を n 回繰り返す
- 通常では暗号化のための処理を多くすると、計算処理が重くなるが、AESは安全性に加え、高速処理可能なところも高く評価されている
- 現時点では解読されたことが無く安全

*1: Advanced Encryption Standard
*2: Data Encryption Standard

Wi-Fi セキュリティを強固にした 802.11i

- 家庭や小規模オフィスでの利用を考慮した Home Mode と企業利用の Enterprise Mode
- Home Mode
  - 事前に鍵を設定しておくPSK (Pre-Shared Key：共有鍵) 方式を利用
  - 802.1x フレームワークは利用しない簡易な方式
- Enterprise Mode
  - LAN 接続時の認証として考えられていた 802.1x 規格を拡張し Wi-Fi 用として利用
  - 802.1x の認証、暗号鍵の生成、配布、ローテーションも規定
  - 暗号には TKIP と AES が規定されたが、現在では AES のみ利用
  - 暗号に加え、改ざん検出プロトコル CCMP *1 の実装も義務付けられている
  - CBC-MAC *2 でメッセージの完全性を確認する MIC *3 を算出し、電子署名を行う
  - CCMPでは、パケット番号を含むヘッダー情報も改ざん検出に利用し、同じデータを繰り返し送信しても、MICが異なるように考慮されている
    - 暗号化されたパケットを盗聴し、送信者になりすまして受信者に再度送ってもパケット番号が合わないため破棄される

*1: Counter mode with CBC-MAC Protocol
*2: Cipher Block Chaining Message Authentication Code
*3: Message Integrity Check

WPA2 の弱点

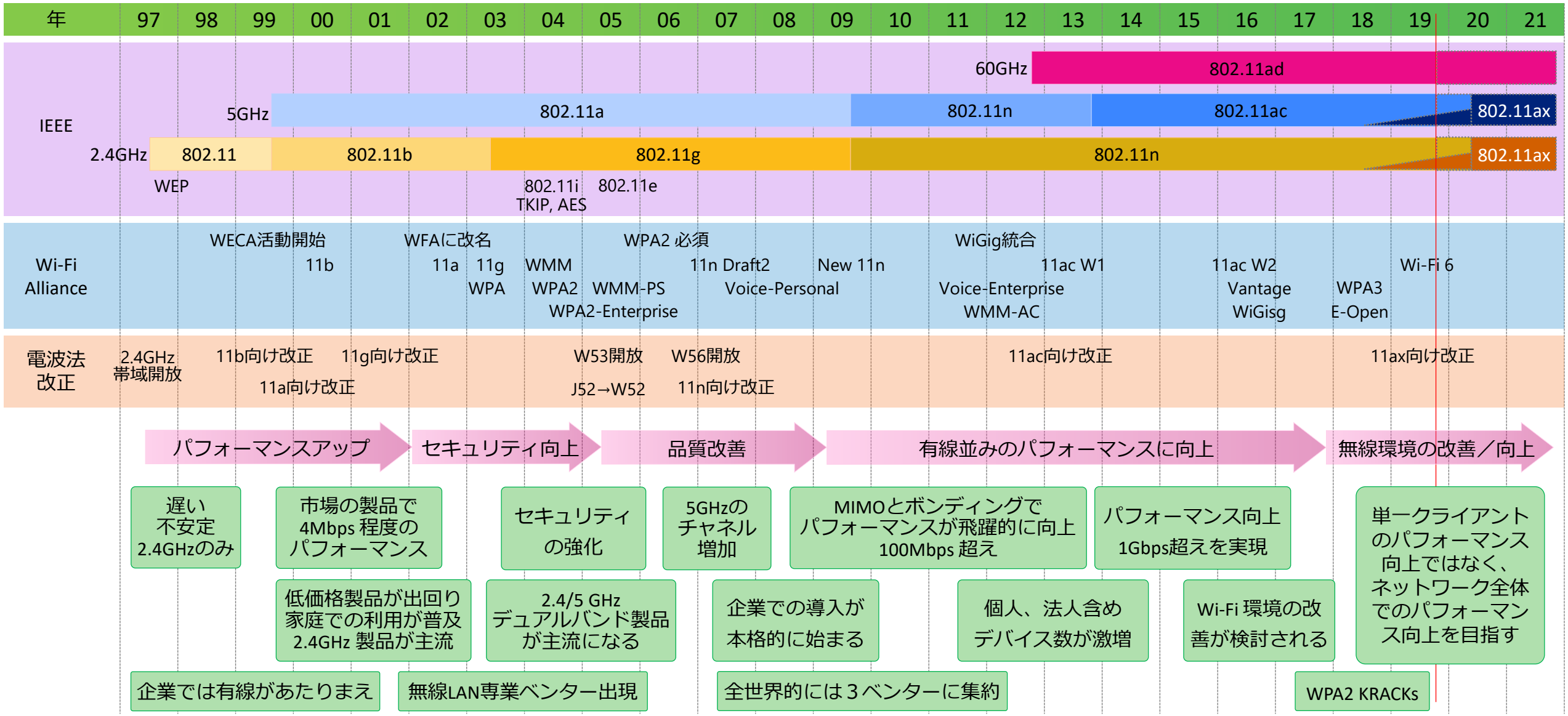
- 2017年10月に WPA2 の脆弱性 KRACKs (Key Reinstallation Attack) が公開された
  - 単一の方法ではなく 複数の方法がある
  - 4 way handshakeで 同じパケットを再送する欠点を利用し 暗号化通信の解読を可能にする
  - 電波の届く範囲で 特定のクライアントを狙う必要がある
  - 既に修正ソフトウェアが配布されている
  - 現実的には非常に困難で 実害の報告は聞いていない
- 辞書攻撃 (Dictionary attack) 可能
  - WPA2ではパスフレーズ (Passphrase) を何度でも入力できてしまう
  - 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

セキュリティ機能をより進化させた WPA3

- 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

Wi-Fi の歴史 まとめ



COMMSCOPE

COMMSCOPE®

Thank You