無線 LAN の技術とクラウドシフトの動向

Trends in Wireless LAN Technology and Cloud Shift

上　村　俊　貴

要　約　2019 年に Wi-Fi Alliance が Wi-Fi 6 の認定プログラムを開始した．Wi-Fi 6 の主要な技術として，セキュリティの向上，無線 LAN の高速化，遅延の低減，2.4GHz 帯の電波干渉軽減，省電力化といった技術が組み込まれている．これらの技術を使用することにより，安定した高速な通信を実現できる．本稿では，Wi-Fi 6 の理解を深めるとともに，シスコシステムズ合同会社の Meraki 製品を例として活用のポイントを挙げる．Meraki 製品では，SaaS 型の無線 LAN コントローラーや Wi-Fi 6 に対応したアクセスポイントを提供しており，設定変更，ステータス確認，トラブルシューティングなどをシンプルに行うことができる．また，クラウド管理型 IT ソリューションによる今後のクラウドシフトについて解説する．

Abstract　The Wi-Fi Alliance launched a Wi-Fi 6 certification program in 2019. Key technologies incorporated in Wi-Fi 6 include improved security, faster wireless LANs, decreased latency, reduction of interference in the 2.4 GHz band, and power savings. By using these technologies, stable and high-speed communication can be realized.

In this paper, we will deepen our understanding of Wi-Fi 6 and describe the advantages of using Cisco Meraki products as an example. Meraki provides SaaS-type wireless LAN controllers and Wi-Fi 6 certified access points, making it simple to change settings, check status, and troubleshoot. In addition, the future “cloud shift” with cloud-managed IT solutions is explained.

1. は　じ　め　に

2014 年に IEEE（米国電気電子学会）[1]が無線 LAN の規格である 802.11ax の検討を開始し，2019 年に Wi-Fi Alliance が Wi-Fi 6 の認定プログラムを開始した．Wi-Fi 6 では，無線 LAN の干渉軽減，無線 LAN 高速化技術，強固なセキュリティ，無線 LAN 接続時の低消費電力化などの技術が採用された．これらの技術により，今まで以上に高速で安定した無線 LAN 通信を行えるようになった．

2019 年末頃から Wi-Fi 6 に対応したノートパソコンやスマートフォンが販売開始され，徐々に普及し始めた．4K/8K の高画質な動画配信，テレプレゼンスによるオンライン会議，AR/VR といった大容量のデータ通信において，従来は有線 LAN を利用することが多くあったが，Wi-Fi 6 の普及に伴い，今後は無線 LAN を利用する機会が増加すると考えられる．

ネットワーク機器だけでなくトラブルシューティングに便利な製品や統合管理ソフトウエアなど取り扱う製品が多くなり，それぞれの製品の専門知識が求められる中，企業のネットワーク管理者が全ての機能を活用することは困難である．また，オンプレミス型のソフトウエア製品では，サーバーの設置場所や空調整備だけでなく，OS バージョンアップに伴う新機能搭載により，CPU やメモリーの増設や再構成を検討する場合がある．これらの課題を解決するク

ラウド管理型 IT ソリューションがある．インターネットに接続された環境であれば，いつでもどこからでも操作ができ，かつ柔軟なスケーリングにも対応できる．

本稿では，Wi-Fi 6 の理解を深めるとともに，シスコシステムズ合同会社（以下，シスコシステムズ社）[2]の Meraki 製品[3]を例として活用のポイントを挙げる．2 章で無線 LAN の規格と利用拡大，3 章で Wi-Fi 6 の技術紹介，4 章で無線 LAN 管理形態の変遷，5 章で Meraki 製品の概要と利活用の方法，6 章で無線 LAN 製品のクラウドシフトについて述べる．

なお，無線 LAN としては，Bluetooth や ZigBee などの狭い範囲の無線 PAN（Wireless Personal Area Network）もあるが，本稿では，Wi-Fi 技術を中核に無線 LAN として解説する．

2. 無線 LAN について

一般のオフィスでは，無線 LAN 経由でノートパソコンやタブレット端末を使用することが主流となり，座席のフリーアドレス化や会議室への移動が容易になった．

無線 LAN 端末が普及し始めた 2000 年代初頭，無線 LAN 機器が非常に高価であり 2.4GHz 帯をごく一部のユーザーが使用するのみであった．また，無線 LAN の電波が度々切断され，データ通信速度が遅くなることから，業務ではあまり利用されなかった．その後，2009 年に MIMO と呼ばれる技術を実装して低価格化を実現すると，次第に無線 LAN の業務利用が一般的になる．無線 LAN 端末が増加する一方で，2.4GHz 帯のチャネルが干渉し，データ通信が断続的になる問題が発生した．また，スマートフォンの普及と共に，無線 LAN を利用する端末がさらに増加したため，帯域が圧迫され全体のパフォーマンスが低下する問題が発生した．その対策として，チャネルボンディングと呼ばれる技術が登場し，理論上 600Mbps の速度へ向上した．しかし，チャネルボンディングにより 5GHz 帯の使用可能なチャネル数の減少と，各種レーダーとの干渉による DFS[*1] が問題になった．このように，無線 LAN の利用が増加することで様々な問題が発生し，その度に新たな技術が登場している．

2. 1 無線 LAN の主な規格

無線 LAN の規格は IEEE[4]が策定しており，主に 802.11b（2.4GHz 帯．規格値 11Mbps），802.11a（5GHz 帯．規格値 54Mbps），802.11g（2.4GHz 帯．規格値 54Mbps），802.11n（2.4/5GHz 帯．規格値 600Mbps），802.11ac（5GHz 帯．規格値 6.9Gbps），802.11ax（2.4/5GHz 帯．規格値 9.6Gbps）が存在する．これらの規格について，2019 年に Wi-Fi Alliance（無線 LAN の普及や相互接続性を認定する業界団体）が新たな命名法を発表し，802.11ax を Wi-Fi 6，802.11n

表 1　無線 LAN の主な規格

規　格	概　　要	Wi-Fi Alliance の命名法
IEEE 802.11a	5GHz 帯で規格値 54Mbps を実現	—
IEEE 802.11b	2.4GHz 帯で規格値 11Mbps を実現	—
IEEE 802.11g	2.4GHz 帯で規格値 54Mbps を実現	—
IEEE 802.11n	2.4/5GHz 帯で規格値 600Mbps を実現	Wi-Fi 4
IEEE 802.11ac	5GHz 帯で規格値 6.9Gbps を実現	Wi-Fi 5
IEEE 802.11ax	2.4/5GHz 帯で規格値 9.6Gbps を実現	Wi-Fi 6

を Wi-Fi 4，802.11ac を Wi-Fi 5 とした．なお，これらの呼称は 802.11ax や Wi-Fi 6 など表記が異なるが，同じ技術を指している（表 1）．本稿では，Wi-Fi Alliance の命名法で表記する．

2. 2　拡大する無線 LAN への要求

様々なサービスを無線 LAN で利用したいという要求は，ますます増加している．オフィスでは無線 LAN を主流で利用し，有線 LAN が搭載されていないノートパソコンを使用する場合もある．教育現場では従来の教科書の代わりに無線 LAN に接続したタブレット端末を使用し，教材や動画を配信して利用している．今後は IoT デバイスの普及や，AI による自動化，リモート操作，テレプレゼンスなど大容量のデータを高速で利用することも求められるだろう．

2. 2. 1　様々なサービスと肥大化するデータ通信量

一般的な企業で業務に無線 LAN を利用する場合，シンクライアント，ビデオ会議，ドキュメント管理といったデータ通信を行う際の速度目安として，無線端末 1 台当たり，約 2Mbps のデータ通信速度が不可欠である．しかし，スタジアムのように高密度な環境において，より臨場感があり没入感を体感できるような，4K，8K といった高画質な動画データや，AR，VR といったコンテンツを取り扱いたいという期待が高まっている．大容量のデータをストレスなくスムーズに送受信するデータ通信速度としては，端末 1 台あたり，4K 動画では約 30 ～ 40Mbps，8K 動画では約 80 ～ 100Mbps になると考えられる[5]．

2. 2. 2　拡大する IoT 分野

ユーザー情報の活用や様々な規格の新規プロトコル出現，改変により，無線 LAN へ IoT デバイスを接続する環境が今後も増加するだろう．これらの IoT デバイスは，電池で稼働するものが多い．仮に，大量の IoT デバイスを所有している場合，電池を定期的に交換することは，管理やコスト面を考慮すると現実的ではない．IoT デバイスの設置後は，撤去するまで継続して使用できることが求められる．Cisco 2019 VNI（Visual Networking Index）によると，IoT 接続は，2022 年には全世界のすべての接続デバイス（285 億台）による接続の半数以上を占めると予測されている[6]．

2. 2. 3　ミッションクリティカルなサービスの利用

無線 LAN を用いたミッションクリティカルなサービスとして，ロボットによる倉庫の無人化，工場の省人化や遠隔監視，医療現場でのリモート手術などが挙げられ，今後サービス化されると考えられる．これらのサービスでは，低遅延で切断されることのない，大容量なデータ通信が求められる．

3.　Wi-Fi 6 の主要技術

Wi-Fi 6 の認定プログラムでは，セキュリティの向上，高速化，遅延の低減，電波干渉軽減，低消費電力化といった技術が搭載されている．Wi-Fi 5 と比較すると，データ通信速度の実測値では最大で 4 倍の速度を実現し，無線 LAN 端末を 2 ～ 4 倍の台数まで接続できる．これにより，無線 LAN 環境の全体パフォーマンスを向上させ，さらに安心して無線 LAN を利用できる．

3. 1　WPA3

Wi-Fi Alliance は，2018 年に個人および企業向けネットワークの保護機能を強化した次世代無線 LAN セキュリティ規格「Wi-Fi CERTIFIED WPA3」（WPA3）を発表した．WPA3 は，10 年以上に渡り広く採用されている WPA2 の後継機能であり，無線 LAN セキュリティの簡素化，さらに強固なデータの暗号化を実現する新機能を備えている．WPA3 対応無線 LAN は，最新のセキュリティ方式を採用し，ミッションクリティカルなネットワークへセキュリティが確保されたデータ通信を提供する．

WPA3 セキュリティ規格は，WPA3-Personal と WPA3-Enterprise の二つのモードがある．

1）WPA3-Personal
ユーザーの指定したパスワードが，一般的に推奨される強度に達していない場合においても，パスワードによる認証を提供する．WPA3 は，ユーザー確立プロトコルである SAE（同等性同時認証）を活用し，第三者によるパスワード推測からユーザーを保護する．

2）WPA3-Enterprise
192 ビットの暗号強度を実現し，政府機関や金融機関のように機密データを扱う無線 LAN のデータ通信を保護する．WPA3 は，WPA2 対応の無線 LAN 端末との互換性を有する．

また，Wi-Fi Alliance は，新たなプログラム「Wi-Fi CERTIFIED Easy Connect」（Easy Connect）を発表した．このプログラムは，高度なセキュリティ基準を維持し，IoT デバイスのような，ディスプレイがない無線 LAN 端末も接続できる．Easy Connect と WPA3 を用いることにより，IoT デバイスはセキュリティが確保された環境で無線 LAN を利用できるようになる．

さらに，公共の場などで利用する公衆無線 LAN サービスに，新たなメリットを提供する認定プログラム「Wi-Fi CERTIFIED Enhanced Open」を発表した．これにより，オープンネットワークの利便性を維持し，公共の場で利用できるオープン認証（認証を伴わずインターネットへ接続させるサービス）など，ユーザー認証が望ましくない環境や，認証情報（パスワードなど）の提供が難しい環境においても，データ通信の暗号化ができるようになった．

3. 2　OFDMA

アクセスポイントと任意の無線 LAN 端末間で一定のデータ通信を行っている間に別の無線 LAN 端末から接続されると，データ通信の衝突が起きる．これを避けるため，Wi-Fi 5 で採用されていた OFDM（Orthogonal Frequency Division Multiplexing）では，データ通信制御により，1 台の端末とのみ通信する仕様であった．どの端末と通信するかをランダムに決定するため，無線 LAN 端末が多数存在する場合は待機状態の端末が多くなり非効率である．これにより，データ通信速度を保証することが困難となり，遅延やジッターなどが生じる．

Wi-Fi 6 の技術である OFDMA（Orthogonal Frequency Division Multiple Access，直交周波数分割多元接続）は，使用するチャネルをトーンと呼ばれる細かい帯域に分割することで，複数の無線 LAN 端末と同時に通信できる技術である[7]．トーンを 26，52，106，242，484，

996，2x996 のいずれかにグループ化したものがリソースユニットであり，これを無線 LAN 端末に割り当てる．利用できる最大リソースユニット数は，一つのリソースユニットが 26 トーンの場合，帯域幅 20MHz では 9 個であり，帯域幅 160MHz では 74 個となる（表 2）．

表 2　OFDMA で利用できる最大リソースユニット数

リソースユニットの種類	帯域幅			
	20MHz	40MHz	80MHz	160MHz
26 トーン	9	18	37	74
52 トーン	4	8	16	32
106 トーン	2	4	8	16
242 トーン	1	2	4	8
484 トーン	—	1	2	4
996 トーン	—	—	1	2
2x996 トーン	—	—	—	1

Wi-Fi 5 では同時に通信できる端末数が 1 台だったのに対して，Wi-Fi 6 では，リソースユニットの割り当てにより複数の端末で同時に通信できる．また，無線 LAN 端末からアクセスポイント（アップリンク），アクセスポイントから無線 LAN 端末（ダウンリンク）の双方向通信で，それぞれの端末と同時に通信できる．例えば，ある瞬間の 20MHz において，26 トーンのリソースユニットが 3 個，52 トーンのリソースユニットが 1 個，106 トーンのリソースユニットが 1 個割り当てられる場合は，同時に 5 台の端末が通信できる（図 1）．

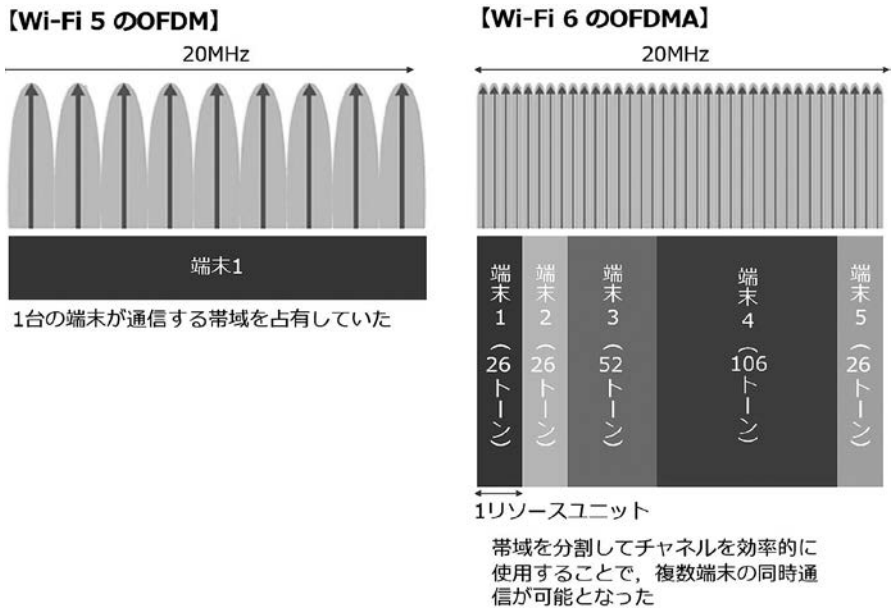

図 1　20MHz における OFDM と OFDMA の比較

3. 3　1024QAM

無線LANにおける最大のデータ通信速度は，チャネル帯域幅，密度，空間ストリーム数，オーバーヘッドの四つの要因により決定する．Wi-Fi 6では，1024QAMの変調方式を採用することにより，オーバーヘッドが大幅に改善した．Wi-Fi 5で採用されている256QAMと比較すると，Wi-Fi 6の1024QAMでは，最大速度が理論上4倍に増えている．ただし，256QAMよりもノイズの影響を受けやすいという特性があるため，Wi-Fi 6の1024QAMの変調方式は，8本の送受信アンテナを用いることでこの欠点を補っている．8本のアンテナが，広いカバレッジエリアでは無線LAN通信の連続性を担保してデータ通信速度の揺らぎを補正し，狭いカバレッジでは通信速度を大幅に向上させる．

また，ガードインターバル[*2]は，Wi-Fi 5が0.4μs，0.8μsのいずれかであるのに対して，Wi-Fi 6では，0.8μs，1.6μs，3.2μsのいずれかとなる．ガードインターバルを長くすることにより，アクセスポイントから離れたIoT端末や屋外で無線LANを利用する場合など，長距離における複数経路の耐性が向上する．

3. 4　MU-MIMO

Wi-Fi 6におけるMU-MIMOの仕様では，ビームフォーミングも引き続きサポートする．Wi-Fi 5では最大4台（4空間ストリーム）の無線LAN端末までの同時通信に対し，Wi-Fi 6では最大8台（8空間ストリーム）まで拡張された．

また，Wi-Fi 5では，同時送信がアクセスポイントから複数の無線LAN端末への一方向（ダウンリンク）のみで，無線LAN端末からアクセスポイントへの送信は1度に1台のみ利用できる仕様であった．一方Wi-Fi 6では，アクセスポイントから複数の無線LAN端末へ同時に

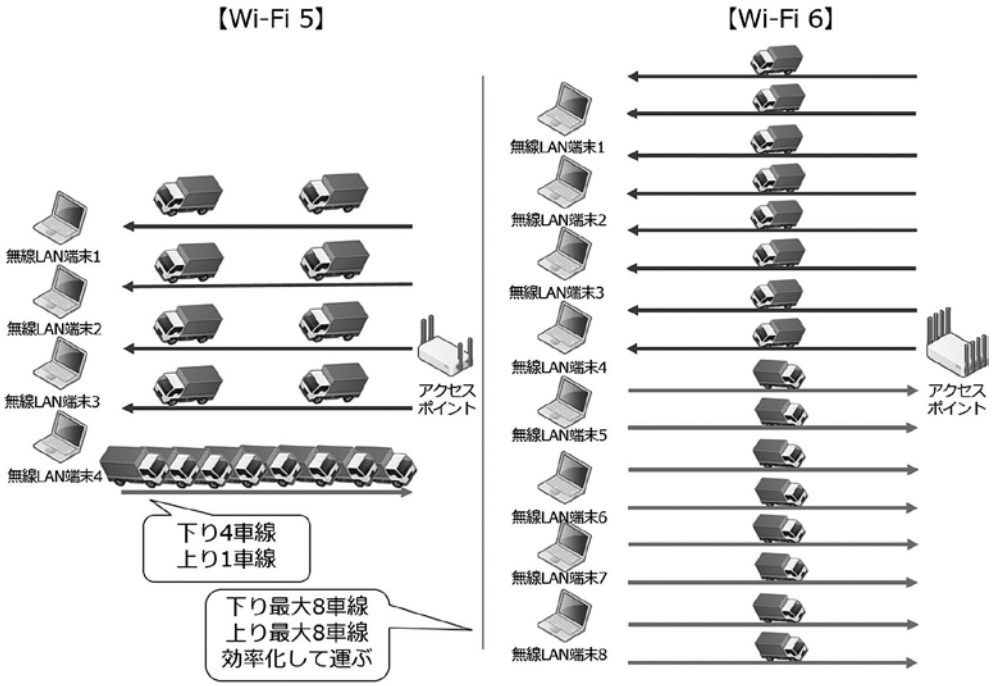

図2　Wi-Fi 5とWi-Fi 6のMU-MIMO比較

データを送信できるだけでなく，複数の無線 LAN 端末からアクセスポイント（アップリンク）へも同時に送信できる，Uplink MU-MIMO 機能が追加されている．OFDMA と MU-MIMO の技術を組み合わせることにより，最大 8 台分の空間ストリームを各無線 LAN 端末に割り当てられる（図 2）．これは，アクセスポイントと無線 LAN 端末のデータ通信をスケジューリングする動作であり，結果的にデータ通信の高速化を実現した．

3. 5　BSS Coloring

無線 LAN を同じ場所で複数台利用した場合，チャネルを共有するため，干渉することが課題となっている．BSS（Basic Service Set）Color は，同じチャネルの BSS を区別するものである．BSS Coloring では，同一チャネルを使用するアクセスポイントが付近に存在する場合，BSS Color により，どのアクセスポイントへ接続中であるか識別する．つまり，同一チャネルかつ異なる BSS Color では，CSMA/CA の制御を除外することで，通信効率を向上させ，電波の干渉を軽減する（図 3）．BSS Coloring は 5GHz 帯も使用できるが，チャネル数の少ない 2.4GHz 帯で，より効果を発揮すると考えられる．

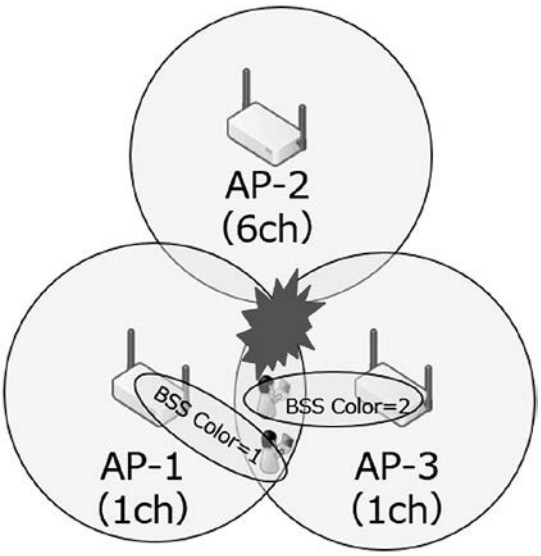

図 3　BSS Coloring による干渉の軽減

3. 6　TWT

スマートフォンなどの端末では，Wi-Fi 5 において U-APSD（Unscheduled Automatic Power Save Delivery）または WMM-PS（Wi-Fi Multi Media Power Save）と呼ばれる無線省電力機能が組み込まれている．この機能に対応した無線 LAN 端末は，アクセスポイントから常にデータを送信させるのではなく，無線 LAN 端末へのデータ通信をバッファリングさせる．代わりに，アクセスポイントは，TIM（Traffic Indication Message）を使用し，無線 LAN に接続された全端末において，データ通信の使用有無を確認するため，定期的に起動時間トリガーを送信する．無線 LAN 端末は，起動時間トリガーを必ず受信して，常時バックグラウンドで無線 LAN 機能を動作させるため，IoT デバイスでの使用には向いていなかった．

Wi-Fi 6 では，TWT（Target-Wakeup Time）と呼ばれる新たな省電力機能が採用された．TWT を有効にすることで，アクセスポイントと無線 LAN 端末のスリープ間隔を個別にスケジュールし，アクセスポイントからの起動時間トリガーにより起動する．これにより，無線 LAN 利用時の大幅な省電力化を実現した．

4. 無線 LAN の運用管理

無線 LAN の運用管理は，アクセスポイント，コントローラー，統合管理ソフトウエア，認証サーバーなどのネットワーク機器の管理だけでなく，レイアウト変更に伴うアクセスポイントの配置検討，認証で使用する証明書，OS バージョン，設定変更，トラブルシューティングおよびメンテナンスなどがある．本章では，無線 LAN の運用管理で特徴的なアクセスポイントの管理方式，無線 LAN のトラブル，課題について記載する。

4. 1　アクセスポイント管理方式

アクセスポイントの管理は，無線 LAN コントローラーを自社に設置し管理するオンプレミス型と，無線 LAN コントローラーを持たずメーカーが提供する SaaS 型のサービスを利用するクラウド型がある．

1）オンプレミス型自律管理方式
アクセスポイントの設定を 1 台ごとに管理する方式である．主に自宅など管理するアクセスポイントの台数が少ない場合に利用される．

2）オンプレミス型集中管理方式
管理したい拠点や組織ごとに無線 LAN コントローラーを設置し，アクセスポイントの設定を一元管理する方式である．物理的にセキュリティが確保されたネットワークを構築できる．無線 LAN 端末をインターネットに接続せず，社内のシステムのみを無線経由で利用したい場合には有効である．

3）クラウド型集中管理方式
無線 LAN コントローラーの機能をクラウド上に集約し，アクセスポイントの設定をクラウド上に保存し管理する方式である．柔軟なスケーリングや設定の一元管理，OS バージョンアップの自動化などができる．また，インターネットにアクセスできる環境であれば，社外のどこからでも管理画面にアクセスして，ステータス確認やトラブルシューティングなどを容易に行うことができる．

4. 2　無線 LAN で発生するトラブル

物理的に目視できる有線 LAN と比べると，無線 LAN を利用する場合は，目に見えない電波環境などトラブル原因の特定が困難になることが多い．これは全てのアクセスポイント管理方式において同様である．トラブルシューティングを行うには，無線 LAN コントローラー側の調査だけでなく，実際に無線 LAN 端末を利用するユーザー側の状況も調査しなければならない．

トラブルの要因として，ノートパソコンやハンディ端末，スマートフォン，IP 電話など，端末ごとに仕様が異なること，端末を持ち移動することでローミングが発生して接続するアクセスポイントが適切に切り替わらないことなどが考えられる．これらのトラブルシューティン

グを行う場合，端末を特定するための確認事項が多く，状況を把握して解決するまでに時間を要する．このような，無線 LAN でよく発生する 3 種類のトラブル事例とその解決策を以下に記載する．

4. 2. 1　無線 LAN へ接続不可

無線 LAN へ接続不可な場合，接続可能な SSID 一覧に表示されない，接続ボタンを押しても接続中の状態から進まない，何度も認証失敗の画面が表示されるなどの問題が発生する．

ノートパソコンやスマートフォンなどの無線 LAN 端末は，インターネットに接続するまでに以下の五つのステップをクリアしていく．トラブルシューティングの際は，どのステップで問題が発生しているのかを確認し，それぞれの項目に適した対策を行う．

1）SSID の発見
企業向けの SSID は，一覧に表示されないようセキュリティの設定をしている場合があり，その場合は設定を手動で入力する．手動で設定しても接続不可な場合は，SSID を公開設定にするか，OS や無線 LAN ドライバーのアップデート等で対策できる．

2）無線 LAN への接続
端末が無線 LAN への接続に失敗する場合，電波が弱く接続しにくいことや，接続台数の上限設定によりアクセスポイントが接続を拒否していることなどが考えられる．電波が弱い場合は，アクセスポイントを増設して対策する．上限設定により接続不可な場合は，設定の見直し，もしくは高密度な環境に対応したアクセスポイントへの更改を検討する．

3）認証
無線 LAN への接続を試みると，ユーザー名やパスワードの入力を要求されるが，入力しても失敗する，もしくは認証画面が表示されず認証失敗と表示されることなどが考えられる．パスワード等の入力ミスであれば，正しく入力することで改善するが，それでも接続不可な場合は無線 LAN と認証サーバーの設定を見直す．

4）IP アドレスの取得
ネットワークに接続するためには IP アドレスを取得する．無線 LAN の場合，多くは DHCP サーバーからアドレスを取得するが，接続する端末の台数が多く，DHCP サーバーが払い出しできる上限に達している場合は，DHCP アドレスの払い出し期間を見直すことやセグメンテーション（ネットワークの分割）など設計を見直す．

5）名前解決
インターネット上の多くのサービスは，IP アドレスだけでなく FQDN（完全修飾ドメイン）で提供されており，名前解決（FQDN と IP アドレスの紐づけ）を行うために DNS サーバーを設置する．IP アドレスは取得できるがインターネットに接続不可な場合は，DNS サーバーと問題なく通信できることを確認する．

4. 2. 2　無線 LAN への接続が解除される

無線 LAN に接続していた端末が接続を解除される場合，電波に関する問題が発生している

可能性が高い．例えば，各種レーダーと電波干渉することによる電波の停止，電波強度が不十分な環境での利用，障害物による電波の乱れなどが考えられる．

これらの問題が頻繁に発生する場合は無線 LAN 環境を見直す．例えば，空港や停泊場など各種レーダーと電波干渉が発生しやすい場所の場合，DFS の考慮が不要なチャネル設計にするといった対策が有効である．電波が弱い場合や障害物により電波の乱れが発生する場合は，アクセスポイントの台数を増やすことで，物理的な電波の到達範囲を広げ，接続性を確保することができる．

4. 2. 3　無線 LAN の速度が遅い

無線 LAN の速度が遅い場合，インターネットの Web ページ表示に時間がかかる，ファイルダウンロード，アップロードに時間がかかるなどの問題が発生する．その原因は，無線 LAN へ接続する端末の増加，取り扱うデータの大容量化，無線 LAN 端末が距離の遠いアクセスポイントに接続しデータレートが低い状態で通信を行っていることが考えられる．

無線 LAN を利用する端末の増加や取り扱うデータの大容量化については，高密度な環境に適したアクセスポイントを選定し環境を構築する．現在では，ノートパソコン，タブレット，スマートフォンなど，1 人あたり 2 台，3 台と接続することが多くなり，今後は IoT 端末の接続が増加することを考慮すると，より高密度な環境に適した設計が求められる．

無線 LAN の特性上，低いデータレートで接続する無線 LAN 端末が 1 台でもあると，高いデータレートで接続する他の端末も含め，全体のデータ通信速度が遅くなるという性質がある．そのため，無線 LAN 端末が，距離の遠いアクセスポイントに接続し続ける場合は，無線 LAN のローミング設定を見直すとよい．例えば，電波強度がある一定の閾値を割ったら他のアクセスポイントに接続させるなどが有効である．もしくは，Air Time Fairness[*3] と呼ばれる技術を使用することにより，Wi-Fi 4 に対応した端末と Wi-Fi 6 に対応した端末を同時に使用する場合でも，それぞれの規格に合った速度となるよう，データ通信の時間を均等に分配することができる．この機能を使用することで，古い規格の端末が存在している環境においても，無線 LAN 全体のパフォーマンスを向上できる．

4. 3　運用管理の課題

無線 LAN の運用管理では，取り扱う製品が多くそれぞれの専門知識が求められ，ネットワーク管理者が全ての機能を活用することは困難である．また，オンプレミス型の製品では，サーバーの設置と構成を検討する場合がある．これらの煩雑な課題を解決する製品として，いつでもどこからでも操作ができ，かつ柔軟なスケーリングにも対応できるクラウド管理型 IT ソリューションがある．

5.　クラウド管理型 IT ソリューション

クラウド管理型 IT ソリューションは，無線 LAN コントローラーの機能を SaaS としてメーカーより提供されており，顧客はサービスをサブスクリプション形式で購入して利用する．物理的な無線 LAN コントローラーが不要なため，イニシャルコストを抑えることができる．また，オンプレミス型の製品では提供されていない，トラブルシューティングのためのツールが標準で用意されていることや，視認性に優れているといった利点がある．その反面，クラウド

上に全ての機能が集約しているため，インターネットへの常時接続が必須となっている．

本章では，ネットワーク製品をクラウド上で一元管理できる製品である，シスコシステムズ社の Meraki 製品について記載する．

5. 1　Meraki 製品

Meraki 製品は，セキュリティアプライアンス，スイッチ，アクセスポイント，監視カメラといったネットワーク機器の設定を全てクラウド上に保存し，日本語に対応した Web ブラウザ経由で GUI 操作ができるクラウド管理型 IT ソリューションである．Meraki 製品は他のオンプレミス製品と異なり，CLI のコマンド操作が不要で専用のコマンドを覚えなくてもよい．今までネットワーク製品を担当したことがない場合も，直感的な操作ができる利点がある．

オンプレミス型の製品では，導入後は設定変更や OS バージョンアップ等を行っておらず，複数の脆弱性が存在する状態で使用している場合も少なくない．これは，OS をバージョンアップする度に，影響範囲や手順の確認に時間と費用を要し，迅速な対応が困難である場合が多いためである．Meraki 製品を使用すると，OS のバージョンアップ自動化，リモートでのトラブルシューティングに適した機能の使用，複数拠点の設定情報の一元管理などができるようになる．

さらに，クラウド上にログを保存する機能，認証機能，可視化機能，無線 LAN 端末の分析機能，リモートトラブルシューティング機能が標準で搭載されている．これらの機能を用いることで，他にサーバーなどの機器を調達しなくても，最新の機能を最新のセキュリティパッチが適用された状態で使用できる．クラウド製品の特性上，常時インターネットへの接続が必須となっているが，無線 LAN のデータ通信はクラウド上を経由せず，LAN 内で利用できる仕様となっている．アクセスポイントから Meraki クラウド宛の通信は管理データ通信のみとなっており，そのデータ通信も暗号化されているため安心して利用することができる．

5. 2　Meraki 無線 LAN の主な特徴

Meraki 製品にはセキュリティアプライアンスやスイッチ，監視カメラの製品も存在するが，本節ではアクセスポイントの機能のみにフォーカスして記載する．無線 LAN は，用途ごとに SSID を作成する場合が多い．例えば，社員が利用する SSID と，来客者向けの SSID など．別々の SSID において，無線 LAN 端末間の通信は一般的に ACL（Access Control Lists）で制御するが，Meraki 製品では，社内ネットワーク宛の通信を拒否する設定項目が用意されており，一箇所の設定変更で社員と来客者の通信を遮断する機能が備わっている．

来客者向けの SSID は，ホテルや空港など公共の場でよく用いられ，Web 認証の機能を有している．無線 LAN を利用するユーザーは，登録したメールアドレス宛に送られてくる認証リンクをクリックすると，インターネットに接続できる仕様である．この Web 認証は，メールアドレスで登録する方法以外にも，Google の G Suite や Facebook のサービスと認証連携することで，インターネットに接続する方法が存在する．これらの認証連携により Meraki の管理者は，無線 LAN を利用するユーザーの情報（性別や年代など）を取得することができ，その情報を分析する機能も備わっている．例えば，こうしたユーザー情報を API 連携することにより，無線 LAN を利用する年代や性別ごとに，近隣の観光地，飲食店，お土産情報など有益な情報を通知し，さらにマーケティングにも活用できる．

5. 2. 1　Wi-Fi 6 対応アクセスポイント

Meraki 製品では，2020 年初頭に Wi-Fi 6 の機能を実装したアクセスポイントが複数リリースされている．これらは，数人から十数人など少人数の利用に特化した製品や，高密度な環境に対応した製品など，顧客のニーズに合わせたラインナップを取り揃えている．無線 LAN 端末が Wi-Fi 6 に対応することで，Wi-Fi 6 の機能を利用できるようになる．

5. 2. 2　ゼロタッチプロビジョニング

オンプレミス型の製品では，購入したアクセスポイントを一度開封し，無線 LAN コントローラーへ接続するための設定を事前に施した後，設置することが一般的である．このため，拠点が多くなるに連れて展開に時間を要し，設定ミスやトラブルがあった場合などは現地での切り分け作業が必須となっている．一方，Meraki 製品では，工場出荷時の設定にて DHCP サーバーから IP アドレスを取得し，自動的に Meraki クラウドへ接続後，OS を最新の安定バージョンへアップグレードする．したがって，購入した製品を直接設置する場所へ送付し，LAN ケーブルを接続することで使用できる状態となる．

このように，アクセスポイント本体に事前の設定が不要な状態で設置できることを，ゼロタッチプロビジョニングと呼ぶ．ただし，事前にクラウド上でアクセスポイントのシリアル番号を無線 LAN コントローラーに登録しなければならない．アクセスポイントがインターネットに接続後，クラウド上で設定した SSID や電波の設定が自動的に適用される．これにより，複数の拠点へアクセスポイントを導入したい場合には，速やかに展開することができる．

5. 2. 3　リモートトラブルシューティング

無線 LAN で問題が発生した場合，速やかな解決が求められる．無線 LAN 端末がインターネットに接続するまで，4. 2. 1 項で述べたとおり，五つのステップを通過する．Meraki 製品では，このステップのどこに問題が発生しているのかを確認する機能が搭載されている（図4）．

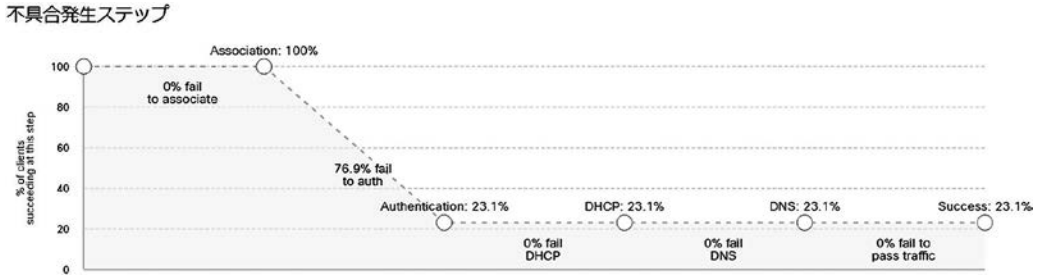

図 4　無線 LAN の不具合発生ステップ確認画面

この機能では，インターネットへ接続するまでに通過するステップのうち，問題がある部分の失敗率（0% fail＝問題がない状態）を表示している．無線 LAN 利用者から無線 LAN への接続に問題があるという連絡を受けた場合，管理者はこの機能を使用することで，原因を即座に特定して解決することができる．

6. クラウドシフトへのアプローチ

これまでの無線 LAN 製品は，実績が豊富であり，確立した運用スキームを用いることができるオンプレミス型が主流であった．また，クラウド型製品がセキュリティの都合により使用できない場合など，オンプレミス型を選択する顧客は今後も少なからず存在すると考えられる．

クラウド型製品では，人事異動やレイアウト変更によるネットワークの設定変更が頻繁に発生する場合でも，統合管理されたクラウド上の一つのシステムにより変更できる．また，クラウド型製品の中には，自動で OS バージョンを最新にアップデートする製品も存在する．これらの利用により，運用の負荷が高い企業においては，負荷軽減やコスト削減が図れる．

無線 LAN のトラブルシューティングに関しても，既に障害ステップを特定する機能が搭載されているものもあり，今後は問題の解決まで自動化されることで，運用負荷がより軽減されると考えられる．例えば，API を利用することで他社製品のネットワーク機器，サーバーなど機種を問わず障害解決までを行う仕組みなどが挙げられる．これらの利用により，運用の負荷が高い企業においては，負荷軽減やコスト削減が図れる．

無線 LAN 製品において，クラウド型製品はリリース後の歴史が浅く，一部の機能が未実装なものも存在する．しかし機能の充足により，クラウド型製品に対する懸念が一層減少していき，サーバーやソフトウエア製品だけでなく，無線 LAN コントローラーもクラウド型製品への移行が加速するであろう．

7. お　わ　り　に

Wi-Fi 6 や，クラウド管理型 IT ソリューションの最新の機能を使って，無線 LAN をシンプルに運用管理できることを記載した．Wi-Fi 6 に対応したノートパソコンやスマートフォンは 2019 年末頃に登場しており，今後は標準的にこの技術が使用されると考えられるため，企業の無線 LAN を更改する際は Wi-Fi 6 に対応した製品を選択すべきである．

2021 年には，Wi-Fi 6E と呼ばれる新たな技術が登場する予定である．5GHz 帯において 80MHz や 160MHz のチャネルボンディングの場合は，チャネル数が減少するため使用が困難である．Wi-Fi 6E では，6GHz 帯の使用によりこの問題を解決することが期待される．Wi-Fi 6E に加え，その他無線 LAN の新たな技術も含め，今後の動向を注視していきたい．

最後に，本稿を執筆するにあたりご支援いただいた皆様に心より感謝申し上げます．

＊ 1　Dynamic Frequency Selection の略称．公共で使用するレーダー等の電波とアクセスポイントの電波が干渉する場合，アクセスポイントの電波を停止し干渉しないチャネルへ切り替える機能．
＊ 2　電波が反射，透過することにより端末まで複数経路で届く際に発生する問題を回避する機能．
＊ 3　802.11g など以前使用されていた規格の端末が無線 LAN の通信を占有し，他の端末も含め全体のパフォーマンスが低下する問題を解決する機能．

参考文献
［1］ Wi-Fi Alliance，https://www.wi-fi.org/
［2］ シスコシステムズ，https://www.cisco.com/
［3］ Cisco Meraki，https://meraki.cisco.com/
［4］ IEEE802，https://www.ieee802.org/
［5］ 4K・8K 時代に向けたケーブルテレビの映像配信の在り方に関する研究会，総務省，2018 年 4 月，https://www.soumu.go.jp/main_content/000548317.pdf，P45
［6］ Cisco Visual Networking Index（VNI）：予測とトレンド，2017 ～ 2022 年ホワイト

ペーパー，シスコシステムズ，2020年6月，https://www.cisco.com/c/ja_jp/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html
［7］ Wi-Biz 通信 Vol.45，一般社団法人無線 LAN ビジネス推進連絡会，2019年7月，https://www.wlan-business.org/archives/23683

※ 上記参考文献に含まれる URL のリンク先は，2020年10月12日時点での存在を確認.

執筆者紹介 上 村 俊 貴（Toshiki Kamimura）
2015年ユニアデックス(株)入社．無線 LAN 製品主管部として従事．主に，無線 LAN コントローラーや Meraki 製品の拡販業務に取り組む．2016年に Certified Meraki Networking Associate（CMNA），2020年に Cisco Certified Network Professional Wireless（CCNP Wireless）を取得.