2014 年 9 月
IP 電話普及推進センタ

技術解説 第 9 回

『モバイルコミュニケーションを支える技術（2）』

無線 LAN は、電波を利用して通信を行うため特有の課題があります。
一つは他の電波との干渉による通信性能の劣化、そしてもう一つは無線 LAN の通信内容の盗聴・不正アクセスです。 今回はこれらの課題を解決する技術を紹介します。

電波干渉と置局設計

●無線 LAN と電波干渉

オフィス街や住宅密集地など多数のアクセスポイントが設置されるエリアでは通信速度が著しく低下することがあります。速度低下の原因の1つとして、無線通信する機器が電波を発生するため、そうした機器が近くにあると電波がお互いに影響し合ってしまう「電波干渉」が考えられます。

無線 LAN では、「電波干渉」による通信速度への影響を小さくして複数の機器が同時に通信できるように、利用する周波数帯域を分割する方法を採用しています。その分割した周波数帯域をチャネルと呼びます。

2.4GHz 帯の無線 LAN は、使用周波数が重なる複数のチャネルで同時に通信があることを意識せず複数のチャネルが重なり合う構成となっています。そのため、近くに存在するアクセスポイントが同じチャネル、又は重なり合うチャネルを使用すると電波干渉を起こしてしまいます。なお、5GHz 帯のチャネルは干渉が考慮されおり、同じチャネルが重ならなければ干渉はほとんど発生しません。

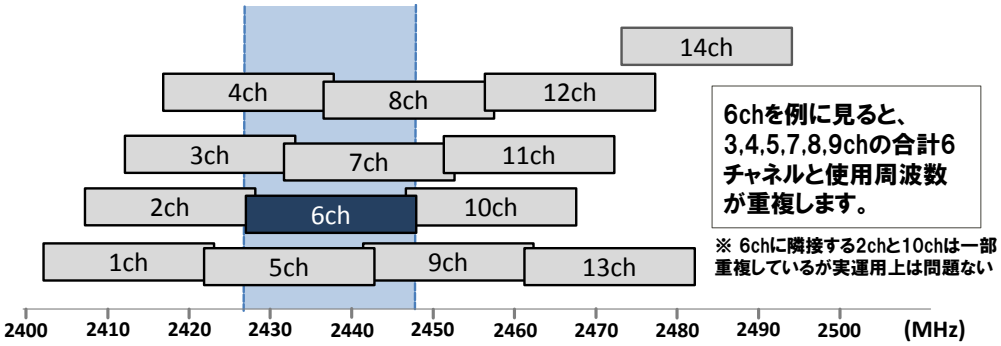

図 1：チャネル割り当て（2.4GHz）

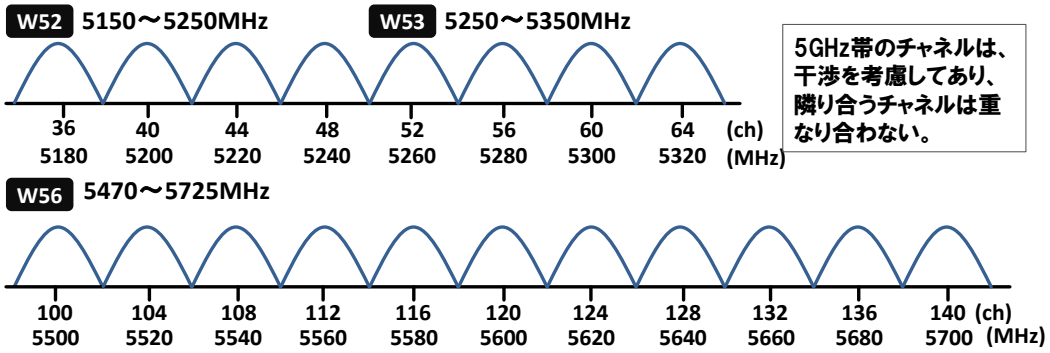

図 2： チャネル割り当て（5GHz）

●外来波との共存

2.4GHz 帯は無線 LAN 以外の機器でも無線免許なしに利用が可能な帯域であり多くの機器で利用されています。代表的な機器として、医療用装置、家庭用コードレス電話機、低周波治療器、アマチュア無線、電子レンジ、Bluetooth などがあり、これらが発する電波が、無線 LAN に影響を与える場合があります。

また 5GHz 帯は日本国内では航空管制レーダーや衛星通信、気象レーダーで使用されています。無線 LAN はこれらに影響を与えないことを条件に利用が許可されています。5GHz 帯無線 LAN で利用する周波数帯域は図 2 に示す通り、W52,W53,W56 と呼ばれる 3 つの帯域となります。このうち W56 を除き屋外での使用が禁止されています。また気象レーダーと利用帯域が重なっている W53、W56 はレーダーの電波を監視し、干渉しないチャネルを選択する"DFS[1]"や干渉を防ぐために電波の出力を調整する"TPC[2]"の搭載が義務付けられています。

	2.4GHz帯 （IEEE802.11b/g/n）	5GHz帯（IEEE802.11a/n/ac）
電波特性	伝達距離が長い 回り込みやすい	伝達距離が短い 直進性が強い
チャネル構成	各チャネル間の重複あり 計13チャネル（11bのみ14）	各チャネルは重複なし 計19チャネル
周波数帯共有	ISMバンド（産業/科学/医療）、 アマチュア無線	気象/航空/船舶レーダー
屋外利用	全チャネルが可能	一部チャネルのみ可能

図 3： 2.4GHz 帯、5GHz 帯の特徴

●置局設計

企業内に無線 LAN を導入する際にはアクセスポイントを設置します。この設置場所を決めることを置局設計と呼びます。建物内の障害物の影響やアクセスポイント間や外来波の電波干渉の影響を考慮し、利用可能エリア、性能要件、運用条件を満たすように、アクセスポイントの設置場所、利用するチャネル、電波出力の組み合わせを決める置局設計が重要です。

置局設計では最初に電波調査（サイトサーベイ）を行います。電波調査は、外来波

1 Dynamic Frequency control System
2 Transmitter Power Control

（他の無線 LAN システムの電波）の調査やアクセスポイントの置局を決定するために必要な電波の特性、特にアクセスポイントを展開する社屋・フロアにおける電波状況・電波特性を得るために行います。ここで「見通しの空間における電波到達距離」「電波を遮断する障害物の情報」「社屋内における既存電波や干渉機器の情報」「隣接建物からの外来波」等の情報を採取して、置局設計に反映します。置局設計の際には、隣接する AP に同じチャネルを使用しない、使用エリアをカバーできるように AP を設置する、外来波を考慮してチャネル設計を行う、人の集まるエリアでは電波出力を抑えて AP を多く配置するなどの点に留意します。また運用開始後も環境は変化するため定期的に電波調査を行い、利用環境が最適になるように見直すことも重要です。

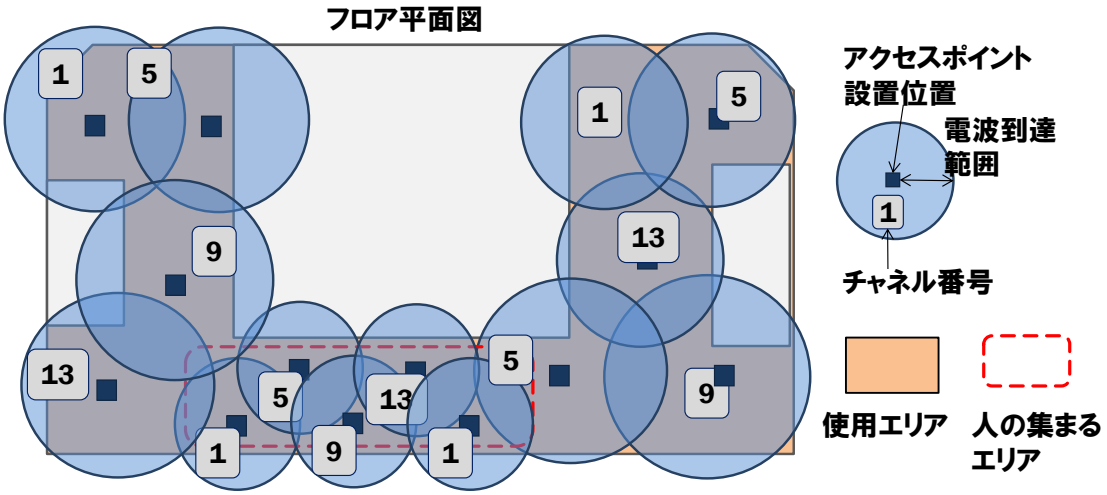

図 4：置局設計のイメージ

無線 LAN のセキュリティ

●セキュリティ対策の必要性

無線 LAN はケーブル工事を伴う有線 LAN のような制約に縛られることなく利用することができ利便性がありますが、逆に第三者による盗聴、不正アクセスの試みにも気づき難いというリスクがあり、十分なセキュリティ対策が必要です。

●盗聴対策（通信の暗号化）

無線 LAN では、アクセスポイントと端末の通信内容を電波の届く範囲であれば第三者から傍受され、通信内容を解析される危険性があります。電波を傍受されることを防ぐのは建物の入退場管理や建物からの電波漏洩を防ぐなどの総合的な対策が必要ですが、通信内容の解析を防ぐためには無線 LAN の通信内容の暗号化が有効です。

無線 LAN の暗号化方式には、図 5 のような種類があります。

WEP 方式は無線 LAN 規格策定の初期からの方式ですが、現在では家庭用の PC でも数分で解読できるなどセキュリティ面の問題が指摘されています。

WEP の脆弱性が指摘されたため IEEE は、より強固な無線 LAN のセキュリティ規格 802.11i の検討を行いました。策定途中に暫定的なセキュリティ強化方式として公開されたのが WPA です。WPA は WEP 対応の無線 LAN 機器のハードウエアを交換することなくファームウエア、ドライバなどのソフトウエアバージョンアップで対応できることが特徴です。

そして 2004 年に策定された 802.11i の仕様を実装したものが WPA2 です。企業用途としては WPA2 を使用することが現在一般的です。

方式	説明
WEP	RC4と呼ばれる暗号化アルゴリズムを使った共有鍵暗号化方式。初期の無線LAN標準暗号化方式として採用されたが、解読手法が広く出回るなど深刻な脆弱性が明らかとなっている。
WPA	業界団体Wi-Fi Allianceが制定したセキュリティ方式。 パケットごとに暗号鍵を変更するTKIP方式によりWEPの脆弱性を改善。
WPA2	業界団体Wi-Fi Allianceが制定したセキュリティ方式。WPAとほぼ同じセキュリティ方式。暗号化方式に米国政府の標準暗号であるAESを採用し、WPAに比べ安全性を高めている。

図 5： 無線 LAN の暗号化方式

●不正アクセス対策（アクセス認証）

第三者からの不正アクセスを防ぐために、無線 LAN にはアクセス認証の仕組みが規定されています。

一つはアクセスポイントと無線 LAN 端末の間にパスワードを設定する PSK 方式[3]です。この方式は追加の認証装置が不要であり導入が容易です。一方企業で利用する場合には、アクセスポイント毎にパスワード設定する必要があること、共通のパスワードを利用することなどから利用者の特定が困難であること、パスワード漏洩時にすべてのアクセスポイント・無線 LAN 端末でパスワードを変更する必要があるなど運用の課題があります。

もう一つの方式は EAP 方式[4]（IEEE802.1X 方式）です。この方式では無線 LAN 端末のアクセス認証はアクセスポイントではなく、認証サーバにて行われます。EAP 方式では利用者の特定ができ、また認証はパスワードだけではなく IC カードなど電子証明書などを用いる厳格な方法をとることができます。

まとめ

このように、通信速度とセキュリティの課題を解決する技術が無線 LAN の利用を支えています。

---

[3] Pre-Shared Key(事前共有鍵)

[4] Extensible Authentication Protocol（拡張認証プロトコル）