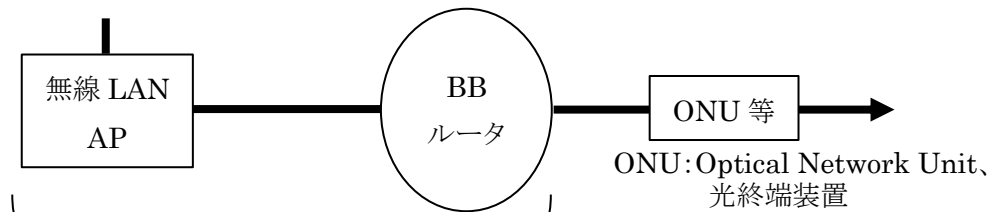


情報処理概論

無線 LAN アクセスポイント(以下、AP)



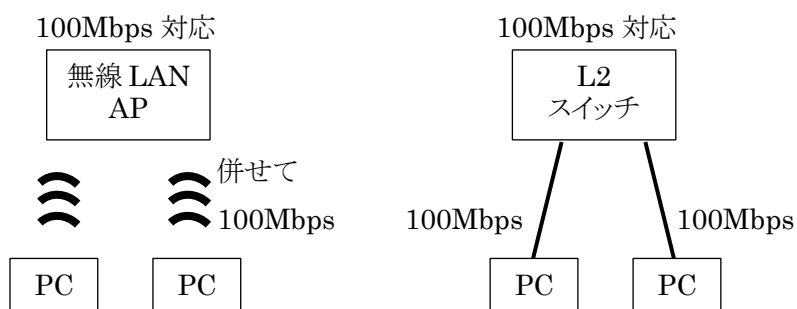
家庭向け等では一体化された製品が多い(企業等では独立した AP も)

通信方法

一般的には AP(親機)と端末(子機、PC 等)の通信(インフラストラクチャモード) 端末同士、AP 同士の直接通信も可能だが、ここでは省略

CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)方式 通信可能となったら、ランダムな時間待ってから通信

無線 LAN では一時に 1 つの通信だけ、L2 スイッチを使う場合は同時並行可



距離が遠くなると低速に



無線 LAN の規格

IEEE (The Institute of Electrical and Electronics Engineers) の 802.11 部会で規格策定

規格	周波数	最大速度
IEEE 802.11b	2.4GHz 帯	11Mbps
IEEE 802.11g	2.4GHz 帯	54Mbps
IEEE 802.11a	5GHz 帯	54Mbps
IEEE 802.11n	2.4GHz 帯、 5GHz 帯	600Mbps
IEEE 802.11ac	5GHz 帯	6.9Gbps

シングルバンド (b g n)

2.4GHz 帯だけを利用

デュアルバンド (a b g n)

2.4GHz 帯と 5GHz 帯の両方を利用

利用周波数による違い

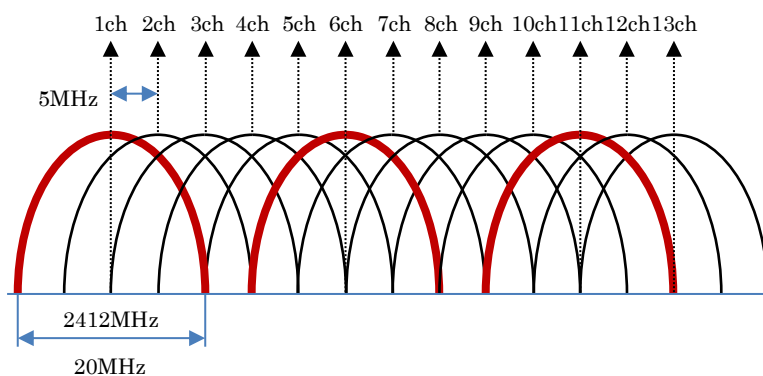
2.4GHz 帯の方がカバーするエリアは広い

利用周波数による違い

2.4GHz 帯 電子レンジ、Bluetooth など

5GHz 帯 船舶用気象レーダー など（屋外利用の制約も）

2.4GHz 帯チャンネル分布



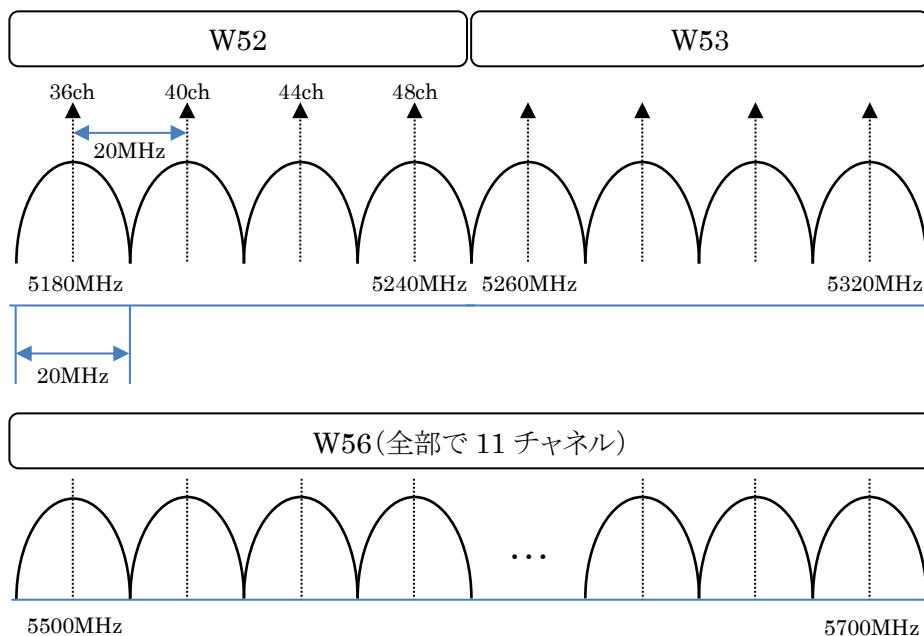
1つの AP は 1つのチャンネルを利用

同じチャンネルを使う別の AP があると ⇒ CSMA/CA が働き、速度低下

隣接するチャンネルを使う AP があると ⇒ CSMA/CA が働かず、電波干渉

こうした電波干渉を防ぐため、2.4GHz 帯では 1ch、6ch、11ch だけを利用することが多い

5GHz 帯チャンネル分布



5GHz 帯では

チャンネル数は 19 (2.4GHz 帯は 13)

各チャンネルは重ならない (隣接するチャンネルでは電波干渉が発生したという実験結果も)

11n の高速化技術

変調方式の改良、MIMO、チャンネルボンディング

これらを利用するには、AP、無線 LAN アダプタの双方が対応している必要有
カタログ上の最高速度はこれらが全て使えた時

変調方式(情報をどのように電波に変換するか)の改良

11n では 1 つのチャンネルで通信できる情報量を 1.4 倍に

MIMO (Multiple Input Multiple Output)

複数のアンテナを使い、複数の情報を同時に送受信

アンテナ数は 1、2、3、4 (基本はアンテナ数に応じ、速度は 2 倍、3 倍、4 倍)

チャンネルボンディング

20MHz 幅のチャンネル 2 つを使い、40MHz 幅で通信

5GHz 帯ならば隣接する 2 つのチャンネル (9 つ使える)

2.4GHz 帯では、最大 2 つ (利用できない機器も多い)

11ac(5GHz 帯だけを使用)

変調方式の改良(1.3 倍)、MIMO 4 ⇒ 8、

チャンネルボンディング 40MHz 幅 ⇒ 80 及び 160MHz 幅

11ax(2018 年リリース予定)

最大速度 9.6Gbps(11ac の 1.5 倍)

それよりもスループット(実行速度)の向上を目指す(4 倍以上)

無線 LAN 利用上の注意

他人が勝手に利用したり、通信内容を見られてしまう場合も

⇒ 通信を暗号化すると共に、他人が使えないように

暗号化

WEP(Wired Equivalent Privacy) ただし、その気になれば解読可能

新しい暗号化法 TKIP、AES、EPA

強い順に並べると、EPA、AES、TKIP、WEP

Wi-Fi (Wireless Fidelity)

無線 LAN の業界団体(Wi-Fi Alliance)により無線 LAN 機器間の相互接続性を認証されていることを示す(Wi-Fi CERTIFIED)。



WPA (Wi-Fi Protected Access)

Wi-Fi Alliance が定めたセキュリティに関する規格

WPA と WPA2(WPA2 の方が強力)

WPA、WPA2 には個人向けの PSK(パーソナルモード)と企業向けの Enterprise

PSK を利用するときには、事前に 8~63 文字の文字列(パスフレーズ)を設定する。

(パスフレーズには 20 文字以上の十分に予測困難な文字列を利用すること)

WPA/WPA2 の暗号化方式には TKIP と AES

TKIP は破られる可能性があり、可能ならば WPA2(AES)、それが無理ならば WPA(AES)

2006 年 3 月以降は WPA2 を利用できないと Wi-Fi CERTIFIED が付けられない