令和５年度　初級レベル

無線LAN基礎セミナー

オンラインセミナー
ウェビナー

一般社団法人情報通信設備協会
Information & Telecommunication Equipment Constructor's Association

V3.0

無線LAN基礎セミナーの内容

①無線LANの概要 (3P)

通信方式、規格、周波数帯、チャンネル、高速化技術、SSID

②技術編 (12P)

無線LANの電波干渉、ローミング、マルチSSID、WDS

③セキュリティ編 (19P)

暗号、認証

①無線LANの概要

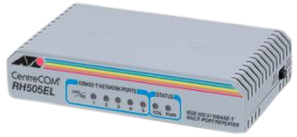
無線LANの通信方式

現在の有線Ethernetは、Full Duplex（全二重）通信が主流です

一方、無線LANのアクセス方式は、有線EthernetにおけるHalf Duplex（半二重）通信に似ています。複数端末が同時に送信することはできません
従って、端末数の増加に伴い、パフォーマンスは低下する傾向があります

無線LANはHalf Duplexで動作するHUB（リピーター）のネットワークと似ています

HUB（リピーター）：CSMA/CD



Carrier Sense Multiple Access with Collision Detect
（衝突検出機能付きキャリア感知多重アクセス）

パケットの衝突が前提となっており、「パケットの再送」が発生しやすい

無線LAN：CSMA/CA

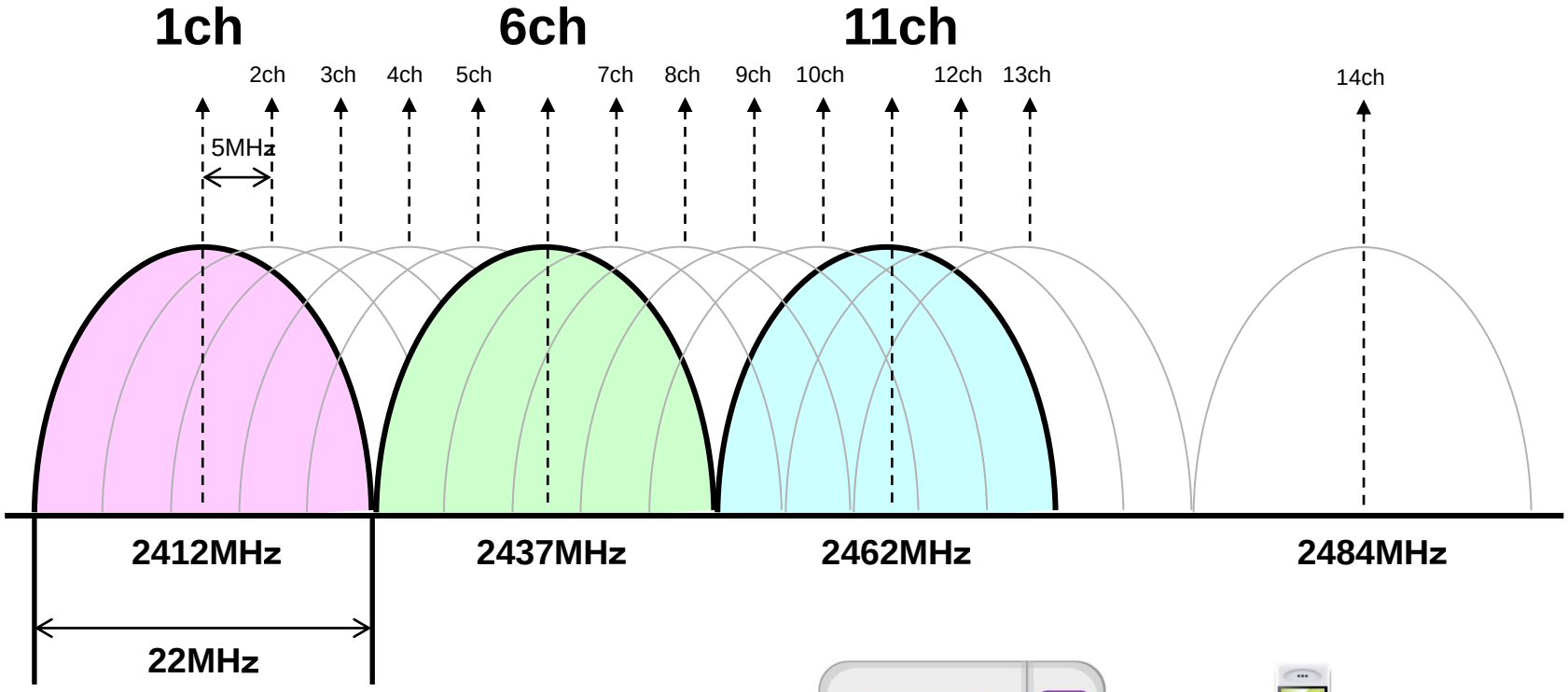
Carrier Sense Multiple Access with Collision Avoidance
（衝突回避機能付きキャリア感知多重アクセス）

パケットの衝突が発生しにくくなるシステムを取り入れています

無線LANのチャンネル（2.4GHz帯）

2.4GHzの周波数帯では、中心周波数が2412MHzから2484MHzまで、5MHz間隔でチャンネルが定められています。現在干渉なしで利用できるチャンネルは1ch・6ch・11chの計３チャンネルです。

＊IEEE802.11b利用の場合は14チャンネルだけ
中心周波数が離れていますので最大4チャンネル利用可能です。

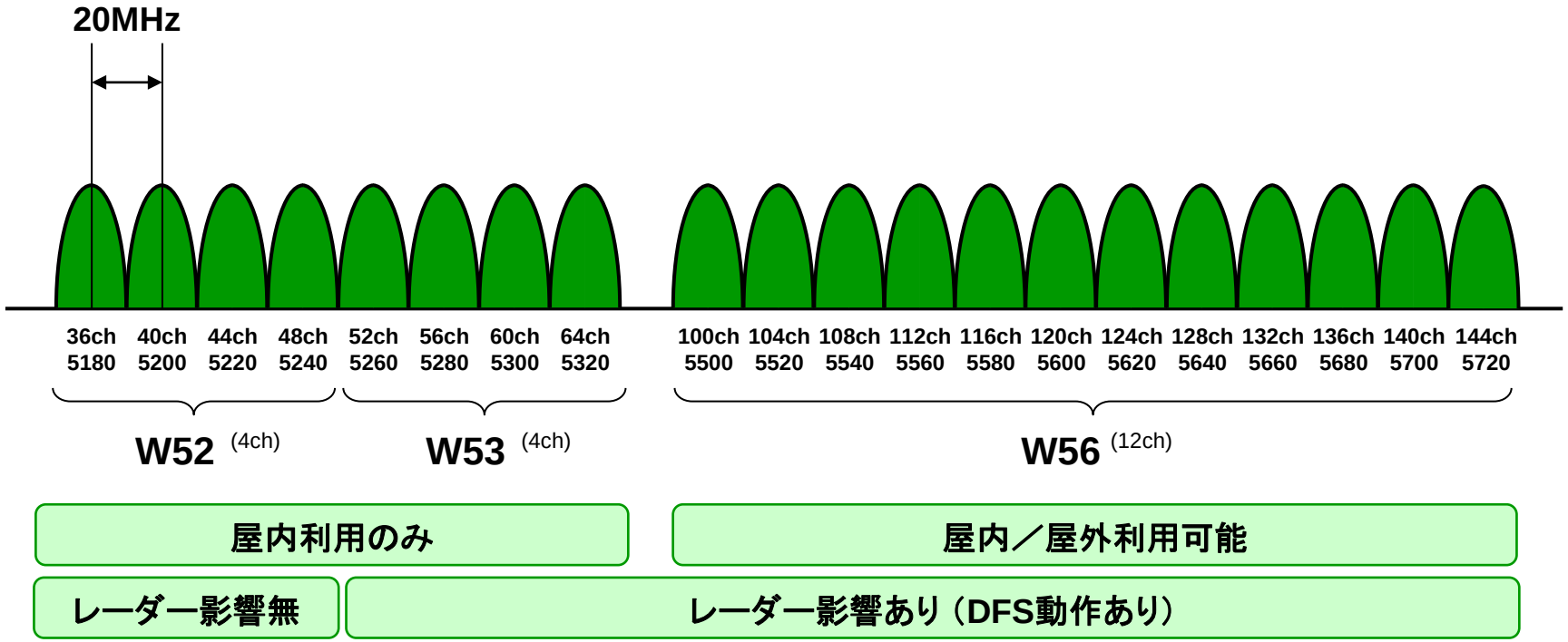


規格（モード）	伝送速度（理論値）
802.11b	最大11Mbps
802.11g	最大54Mbps
802.11n	最大600Mbps
802.11ax	最大9.6Gbps

電子レンジやコードレスフォンからの影響を受ける場合があります。

無線LANのチャンネル（5GHz帯）

5GHzの周波数帯は、20MHz間隔でチャンネルが定められています。2.4G帯とは異なり、隣接チャンネルを使用しても干渉がおこりません。



規格（モード）	伝送速度（理論値）
802.11a	最大54Mbps
802.11n	最大600Mbps
802.11ac	最大6.9Gbps
802.11ax	最大9.6Gbps

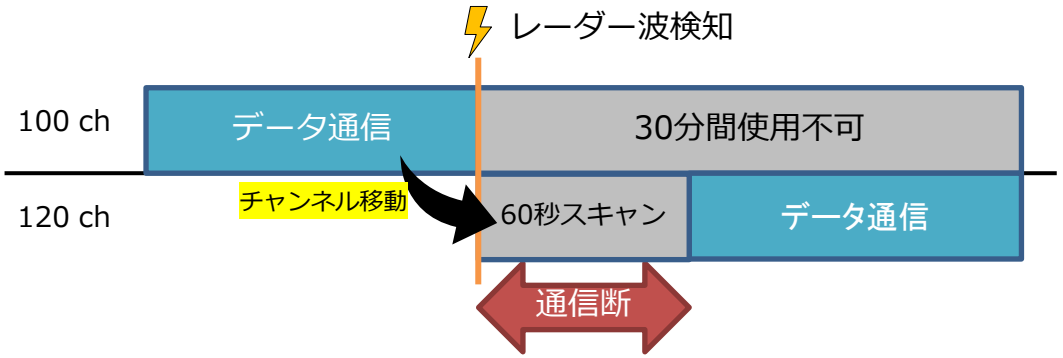
DFS（Dynamic Frequency Selection）について

無線APがDFSチャンネルを利用する場合は、そのチャンネルでレーダー波が検出されないことを60秒確認します。確認中は電波を送信できません。DFSチャンネル利用開始後も常時確認しており、レーダーを検出したら他のチャンネルに移動して、再度そのチャンネルでレーダー波が検出されないことを60秒間確認します。
なお、レーダー波を検出したAPはそのチャンネルを一定時間使用できなくなります。

Zero Wait DFS

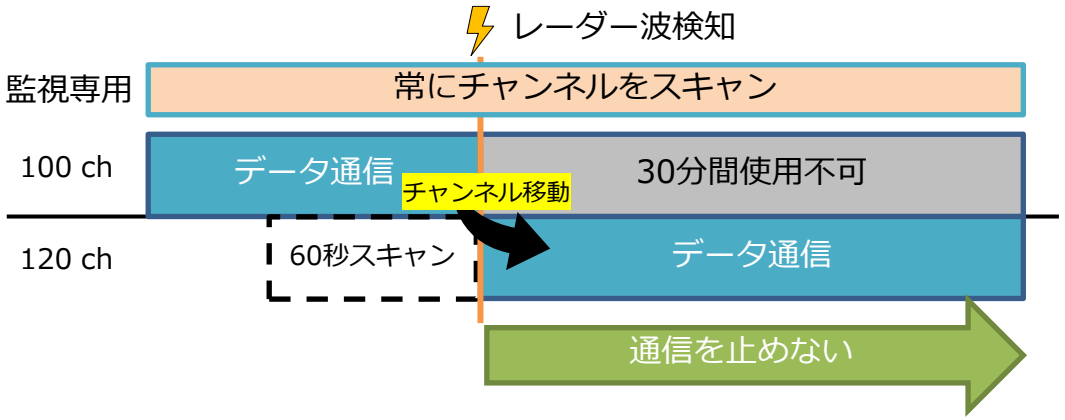
変更の候補となるチャンネルを常に監視を行い、レーダー波を検知した際にすぐにチャンネルを移動することで、通信を継続できる機能です。

従来のDFS



・DFS機能により気象レーダーなどのレーダ波を検知した場合、利用していたチャンネルの変更が必要となります。
・変更後のチャンネルにおいても、再度干渉しないかを確認するため、1分間おきにスキャンを実施する必要があり、この間は通信ができません。

Zero Wait DFS※



・変更の候補となるチャンネルを常に確認しておき、DFS機能のよりレーダー波などを検知した場合は即座に候補のチャンネルに切り替えを実施、通信を再開することが可能になります。

【効果】
・5GHzの通信を最大限に利用することができ、チャンネル設計の幅が広がり無線LANの設計がより柔軟になります。

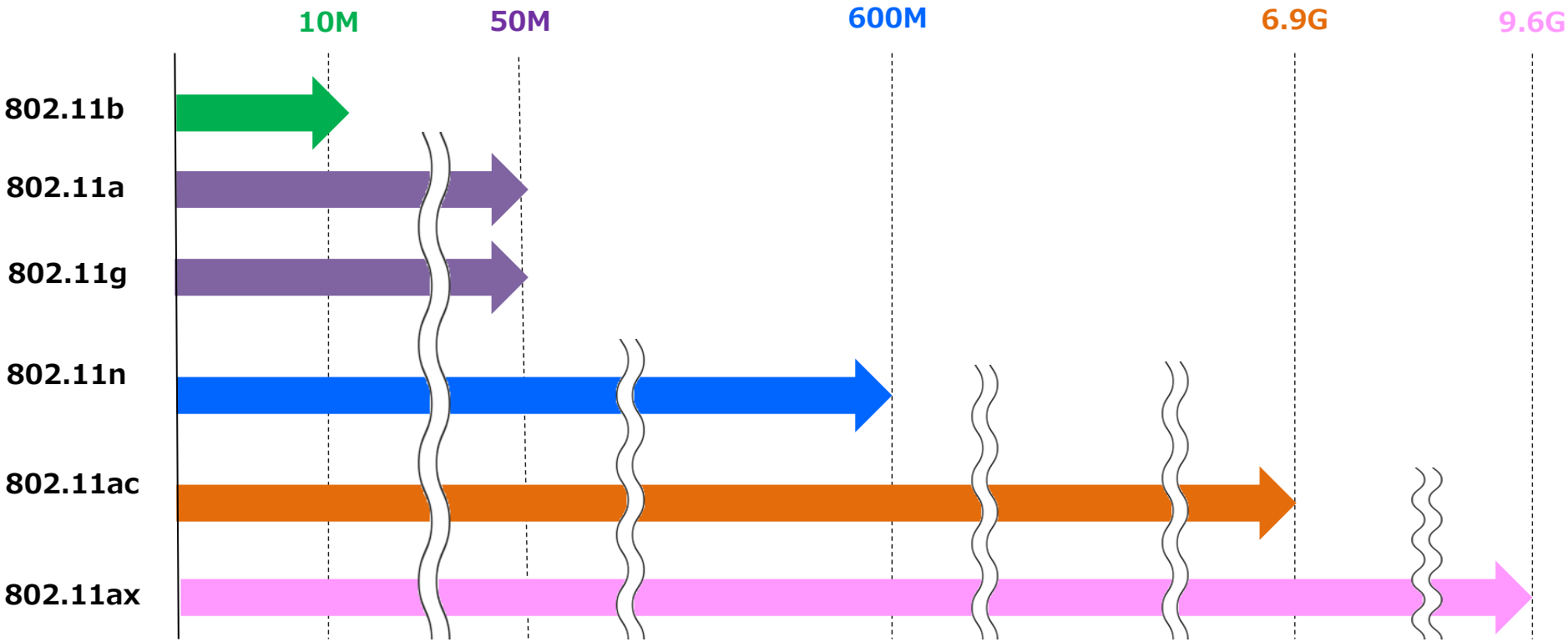
※ 対象機種：AT-TQ6702 GEN2、AT-TQ6602 GEN2、AT-TQm6702 GEN2、AT-TQm6602 GEN2
サポートするファームウェアのバージョン： 8.0.1-1.1以降

無線規格

無線LANは規格によって通信速度が異なります。

無線LANの通信速度は、無線アクセスポイントの電波強度に左右されますが、その電波強度は「無線アクセスポイントと無線端末との通信距離」や「無線アクセスポイントと無線端末の間に介在する障害物の有無とその材質」によって左右されます。

IEEE802.11b/a/g/n/acが現在の無線LANで使用される主な規格ですが、最近ではIEEE802.11ax規格を実装した無線アクセスポイントも存在します。



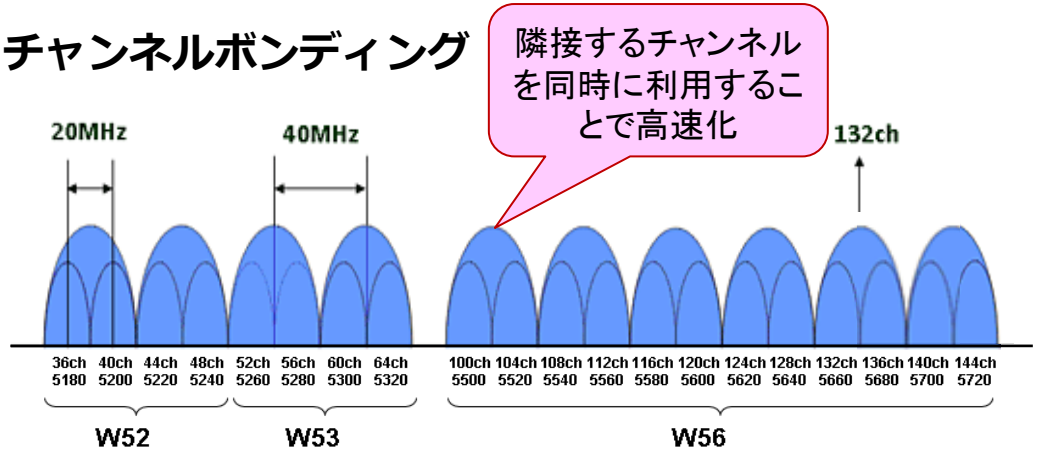
（注）上記は規格上の伝送速度（理論値）です。

高速化技術（11n/11ac/11ax）

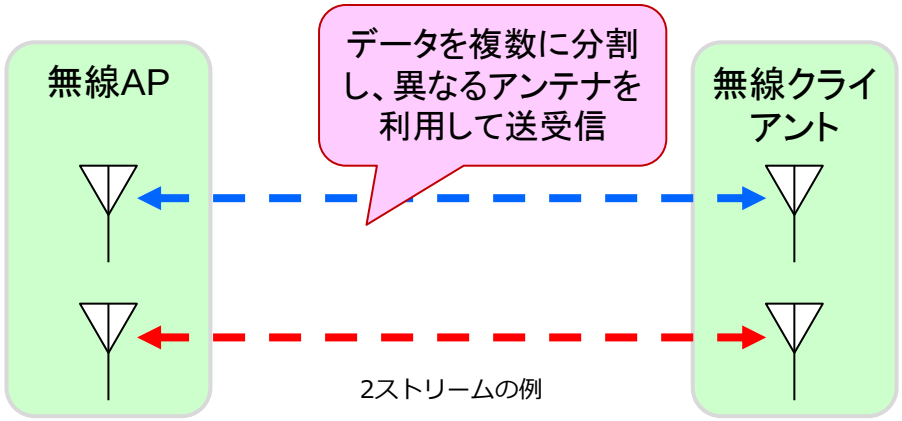
東名高速道路は輸送量拡大のためにどのような手段を用いたでしょうか
- 車線数の拡大
- 第2東名の建設

無線の高速化技術も同様です

・**チャンネルボンディング**



・**ストリーム多重（MIMO）**



11ac

	20 MHz	40 MHz	80 MHz	160 MHz
1ストリーム	86.7 Mbps	200 Mbps	433 Mbps	867 Mbps
2ストリーム	173.3 Mbps	400 Mbps	867 Mbps	1.73 Gbps
3ストリーム	288.9 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps
4ストリーム	346.7 Mbps	800 Mbps	1.7 Gbps	3.47 Gbps
8ストリーム	693.3 Mbps	1.6 Gbps	3.4 Gbps	6.93 Gbps

最大伝送速度（理論値）

11ax

	20 MHz	40 MHz	80 MHz	160 MHz
1ストリーム	143.4 Mbps	286.8 Mbps	600.5 Mbps	1.2 Gbps
2ストリーム	286.8 Mbps	573.5 Mbps	1.2 Gbps	2.4 Gbps
3ストリーム	430.1 Mbps	860.3 Mbps	1.8 Gbps	3.6 Gbps
4ストリーム	573.5 Mbps	1.14 Gbps	2.4 Gbps	4.8 Gbps
8ストリーム	1.1 Gbps	2.3 Gbps	4.8 Gbps	9.6 Gbps

最大伝送速度（理論値）

(注) 上表は、規格で制定されている最大伝送速度（理論値）です。
市場製品には上表の全ての機能が実装されている訳ではありません。

IEEE802.11ac Wave1/Wave2

- IEEE802.11ac では、搭載している技術によって、第1世代（Wave1：ウェイブワン）と第2 世代（Wave2：ウェイブツー）に分かれます

- 11ac の技術をフルに活用することで、規格上の理論値である最大通信速度、6.93Gbps となります

技術	Wave1	Wave2
最大通信速度	1.3Gbps	6.93Gbps
最大チャンネルボンディング幅	80MHz	160MHz
空間ストリーム数	最大 3	最大 8
MIMO	Single User MIMO	Multi User MIMO

NOTE

Multi User MIMOを利用するには、無線LANアクセスポイントがWave2に対応し、かつ無線端末が　Multi User MIMOの機能を実装している必要があります。

【Wave2 Multi User MIMOの効果】

- **無線LAN の通信待ち時間が短縮され、効率的な通信が可能となります**
- **スマホやタブレットなど複数の端末を接続した時に速度低下を防ぐ**

メリットがあります

無線LANの接続名（SSID）

パソコンやスマートフォンからWi-Fiに接続しようとする時、接続先のネットワーク名が表示されますネットワーク名とは、無線アクセスポイントが電波につける名前です。一般的にSSID (Service Set IDentifier)* と呼ばれます

・ESSID (Extended SSID)と呼ばれることもあります

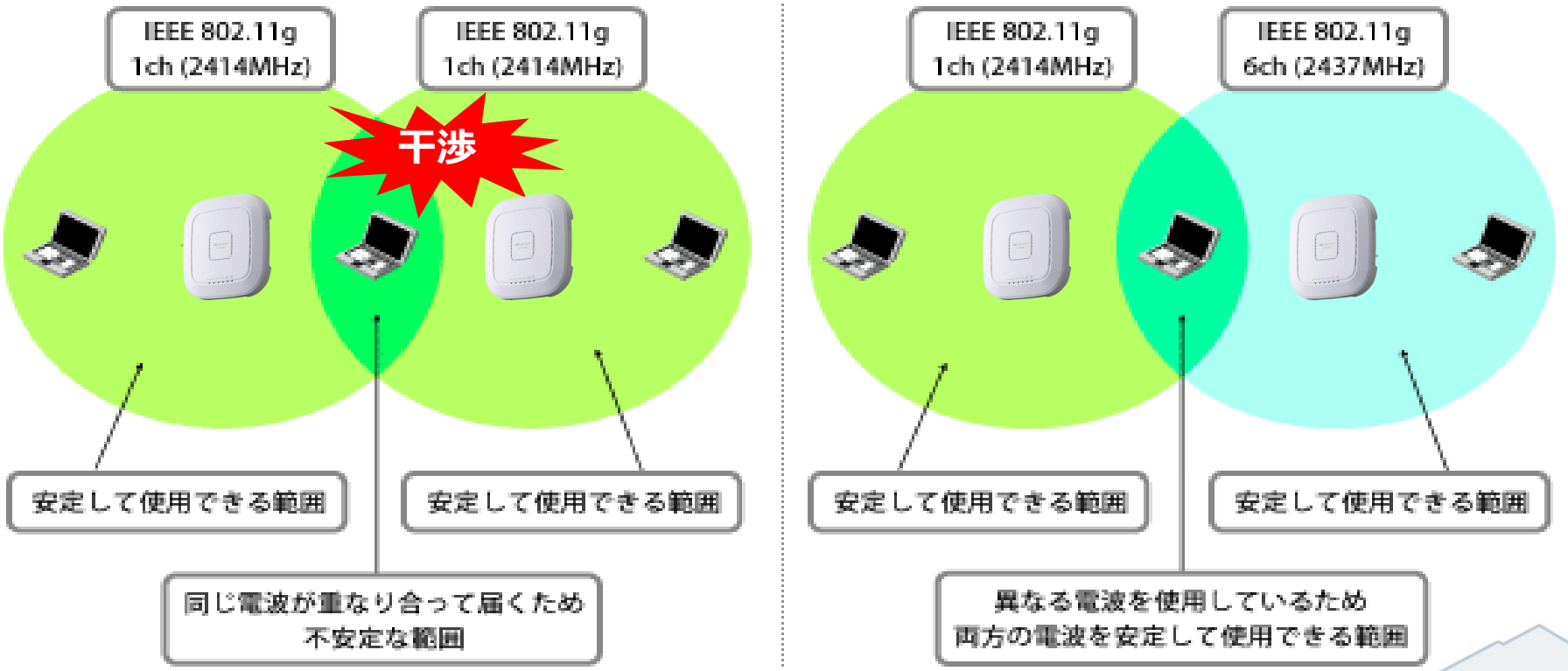
・SSID名は通常1～32文字の半角英数記号で表します

無線APは自分が提供する電波を、定期的に自己紹介しています
これを「ビーコンの送信」と言いますビーコンの中身はSSID名や通信モードなどの情報を含んでいます

②技術編

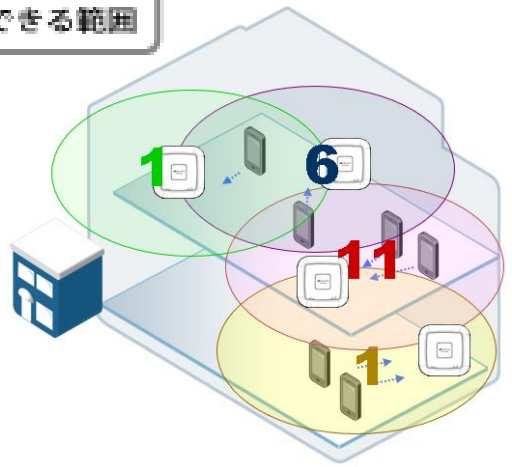
無線LANの電波干渉

無線LANで使用する電波は、チャンネル(CH)と呼ぶ周波数帯に分割されています
周波数が干渉する電波同士がぶつかると、通信速度が低下する等、問題となる場合があります



■設計例

- APの電波が互いに届かない場合は同じCHを設定可能
  (図では1ch設定部位が該当)
- APの電波が互いに届く場所では重複しないCHを設定する
- APを密に配置する必要が有る場合は、電波出力を弱くしたり
  CH重複を認識の上で設定する

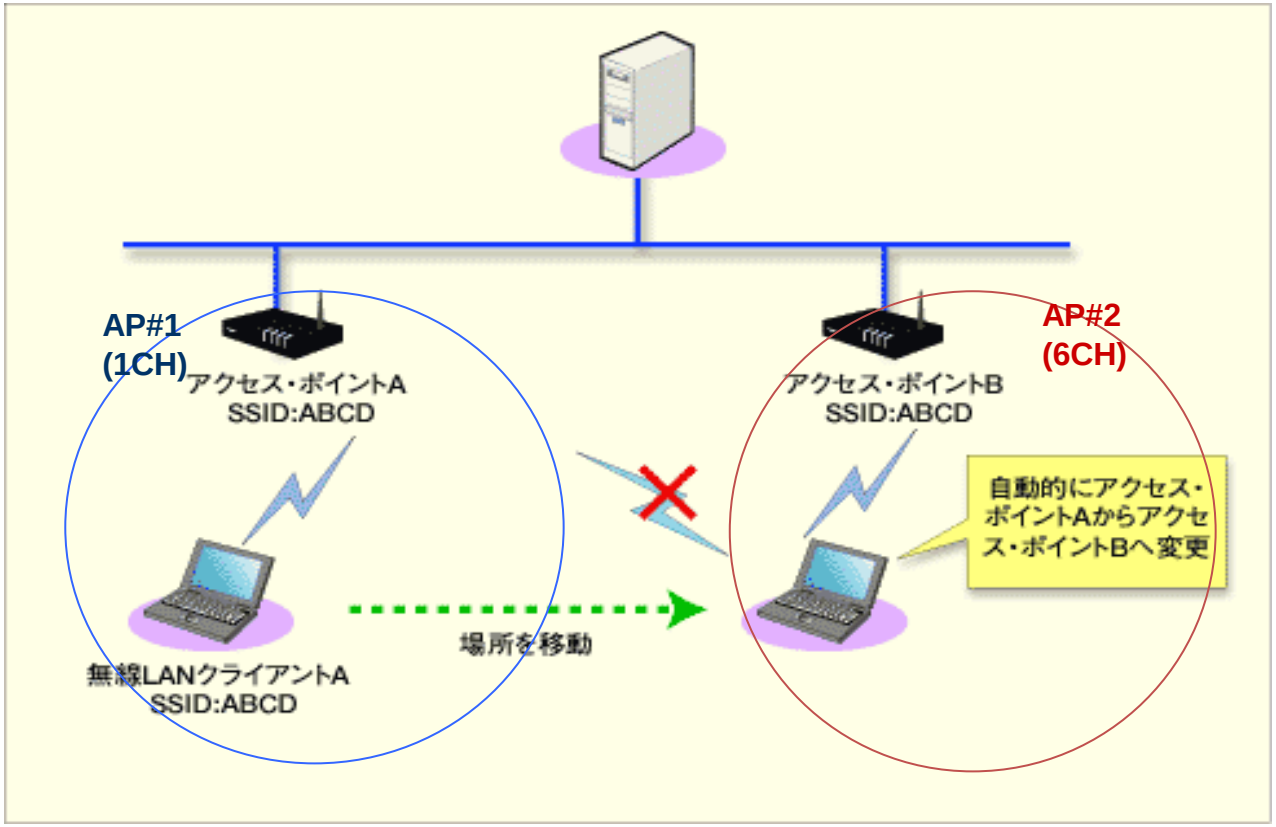


ローミング

ローミングとは

あるAPに接続していたクライアントが移動したなどで、APとの接続性が弱くなる、または切れた際に、同じSSIDをもつ異なるAPに接続を切替える一連の動作をローミングと言います（クライアント側で提供される機能です）

- 一般的に全く通信が途切れることなく、ローミングすることはできません（瞬断する）
- 通信速度が下がっても、最初に接続したAPとの通信が維持されている限り、他のAPへのローミングは行われません



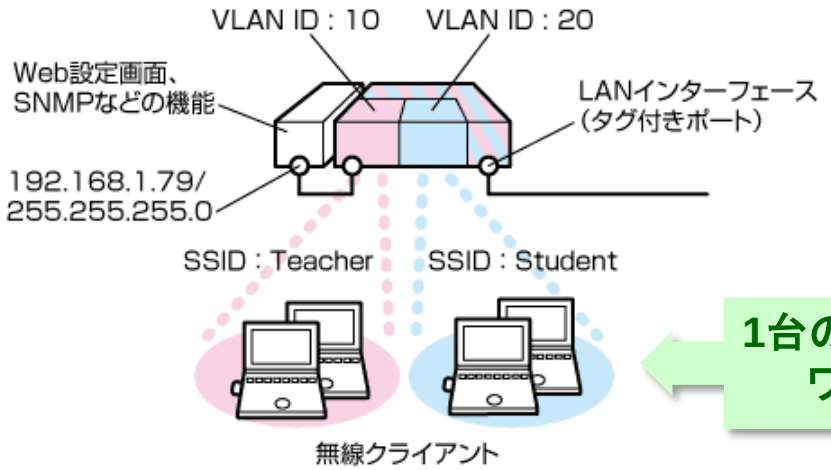
マルチSSID（VAP）

1台のアクセスポイントを複数のアクセスポイントのように動作させる機能、それがマルチSSIDです。一般的にはVAP (Virtual Access Point) と呼ばれます

◆複数VLANを1台のAPに収容

例えば、学校内ネットワークで、「教師用」、「生徒用」などというように複数のVLANを持つネットワークに対して無線クライアントを接続する場合を考えてみます
VAPに対応する無線APであれば、先生は「教師用」のSSIDに接続し、生徒は「生徒用」のSSIDに接続します各々の通信は有線側でVLANのタグ付きフレームとなります

VAPによるVLANの分割例



1台のAPで複数の無線ネットワークを収容できます

ポイント！

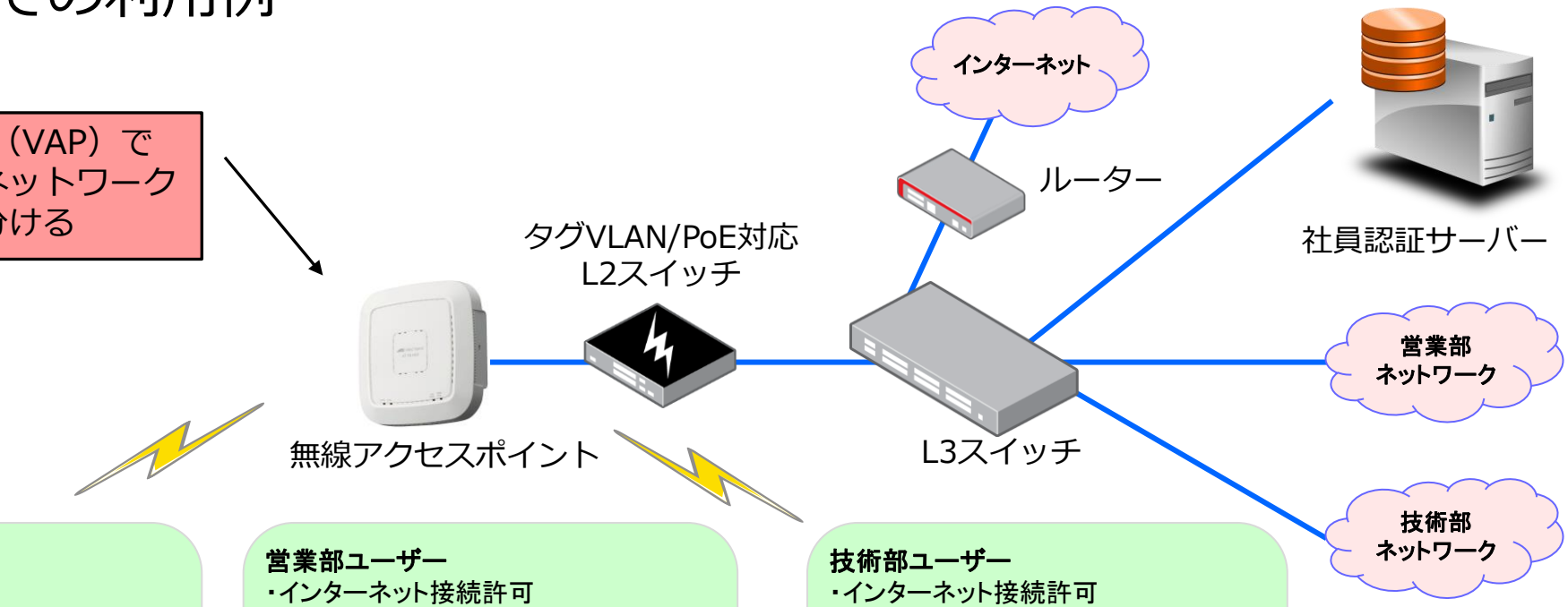
必要以上にVAPを増やすと、無線通信のパフォーマンスが低下することがあります

VAPを増やす → **ビーコンが増える** → **通信帯域を圧迫する**

マルチSSIDを使ったネットワーク例

オフィスでの利用例

マルチSSID（VAP）で
無線端末のネットワーク
グループを分ける



ゲストユーザー
・インターネット接続許可
・通信はゲスト認証と暗号化の必要あり
・社内LANへの侵入不可
・802.11n (2.4G)で接続

SSID: guest

営業部ユーザー
・インターネット接続許可
・通信は社員認証と暗号化の必要あり
・営業部ネットワーク参照可能
・802.11ac で接続

SSID: eigyou

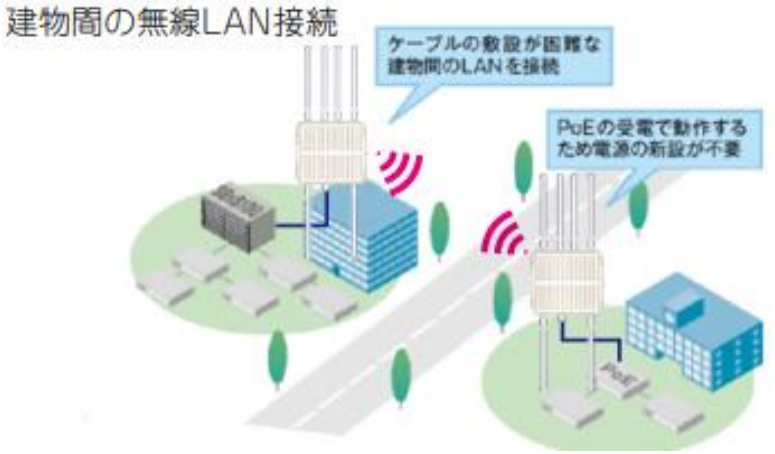
技術部ユーザー
・インターネット接続許可
・通信は社員認証と暗号化の必要あり
・技術部ネットワーク参照可能
・802.11ac で接続

SSID: gijyutu

学校や病院、公共施設などのネットワークでも、同様に構成することが可能です

無線AP同士の接続（WDS）

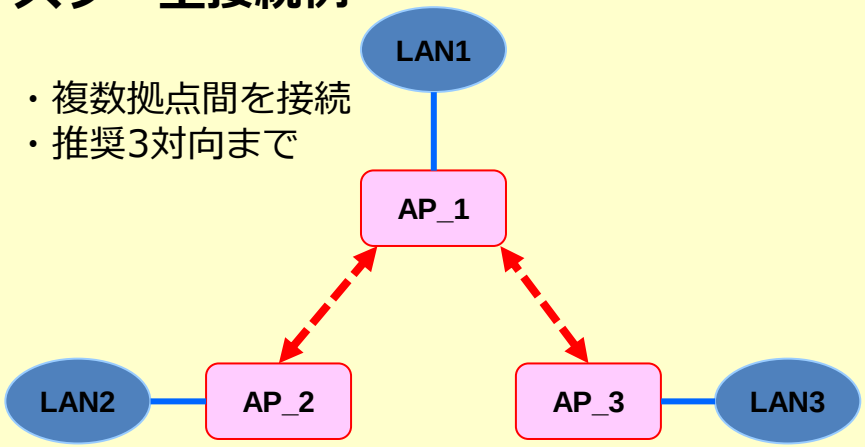
有線LANの一部区間を無線化したい場合や、無線のエリア拡張を行いたい場合などは、無線アクセスポイント同士を対向接続することで対応できますこのような接続形態をWDS (Wireless Distribution System) 接続と言います



WDSによる接続と、無線クライアントの接続サービスを同時に提供することも可能です。この場合は異なる周波数帯で提供されることをお勧めいたします

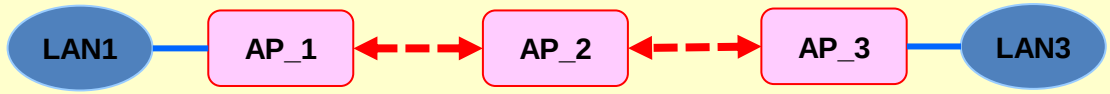
スター型接続例

・複数拠点間を接続
・推奨3対向まで



多段接続例

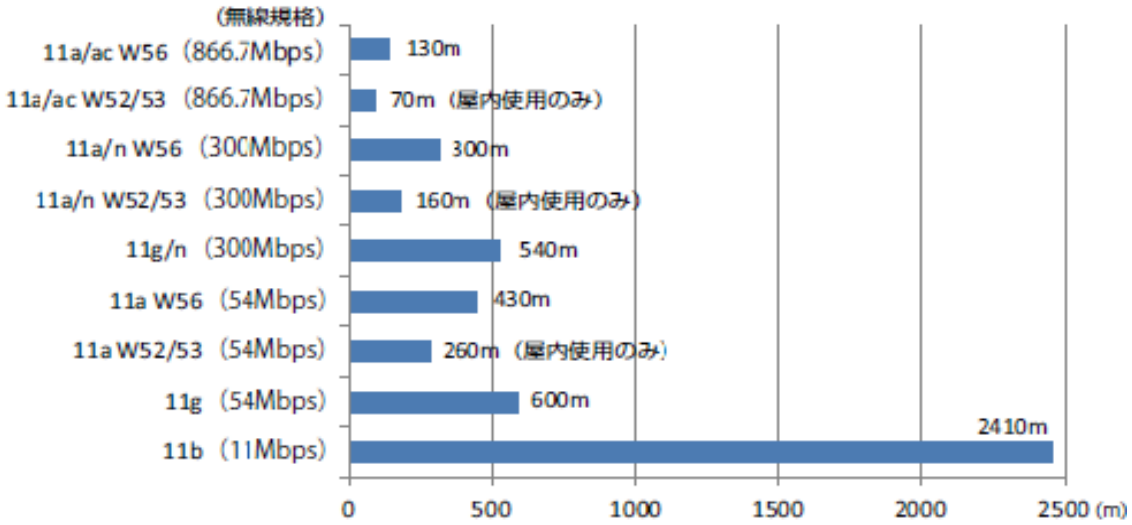
・エリア拡張時に有効
・最大2段（中継1回）まで



パフォーマンスが要求されるケースでは、1対向でご利用ください

通信速度と距離の関係

WDS利用時の通信速度と伝送距離（理論値）



無線LANの通信距離を検討する上でポイントになるのは

・無線規格（通信速度、周波数:802.11b/a/g/n/ac）
・環境（屋内/屋外、見通し、APの地上高など）

※1.上記データは、当社の屋外モデル「TQ5403e」を2台対向でWDS接続した場合の理論値です。
実際に設置された環境などにより実測値は異なりますので事前検証が必要になります。

■通信速度
低速の規格であるほど、長距離の通信が可能（11bは長距離向き）

■周波数帯
2.4GHz帯は5GHz帯と比較して障害物に強く、距離を伸ばしやすい（ただし干渉が無いこと）

■屋内/屋外
屋内はマルチパス(※2)が発生しやすく、距離を伸ばすことが難しい

■見通し
障害物がある場合、金属やコンクリートは電波が通り抜けにくい

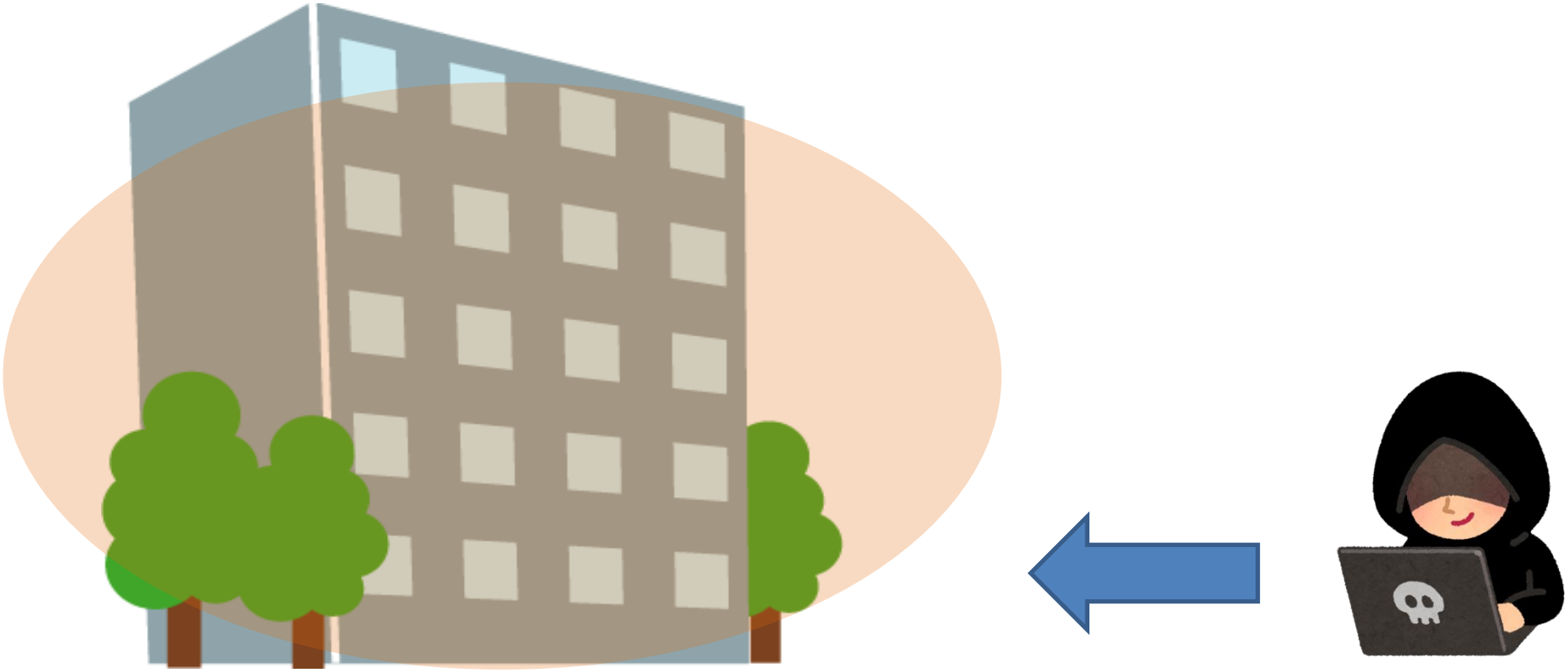
■アクセスポイントの地上高
地面に近いとマルチパス(※2)が発生しやすい

※2.マルチパスとは、壁や天井などで反射した電波が複数の経路をとおって受信側に届く現象です。
マルチパスが発生すると発信した電波にノイズが生じたりして正確に電波を受信できないことがあります。

③セキュリティ編

電波は外に漏れます！

社内ネットワークの有線LANポートへのアクセスは、機器を社外から接続されない位置に設置して防止しますが、無線LANの電波は社外に漏れてしまいます



電波が漏れるとどのようなリスクがあるでしょうか？

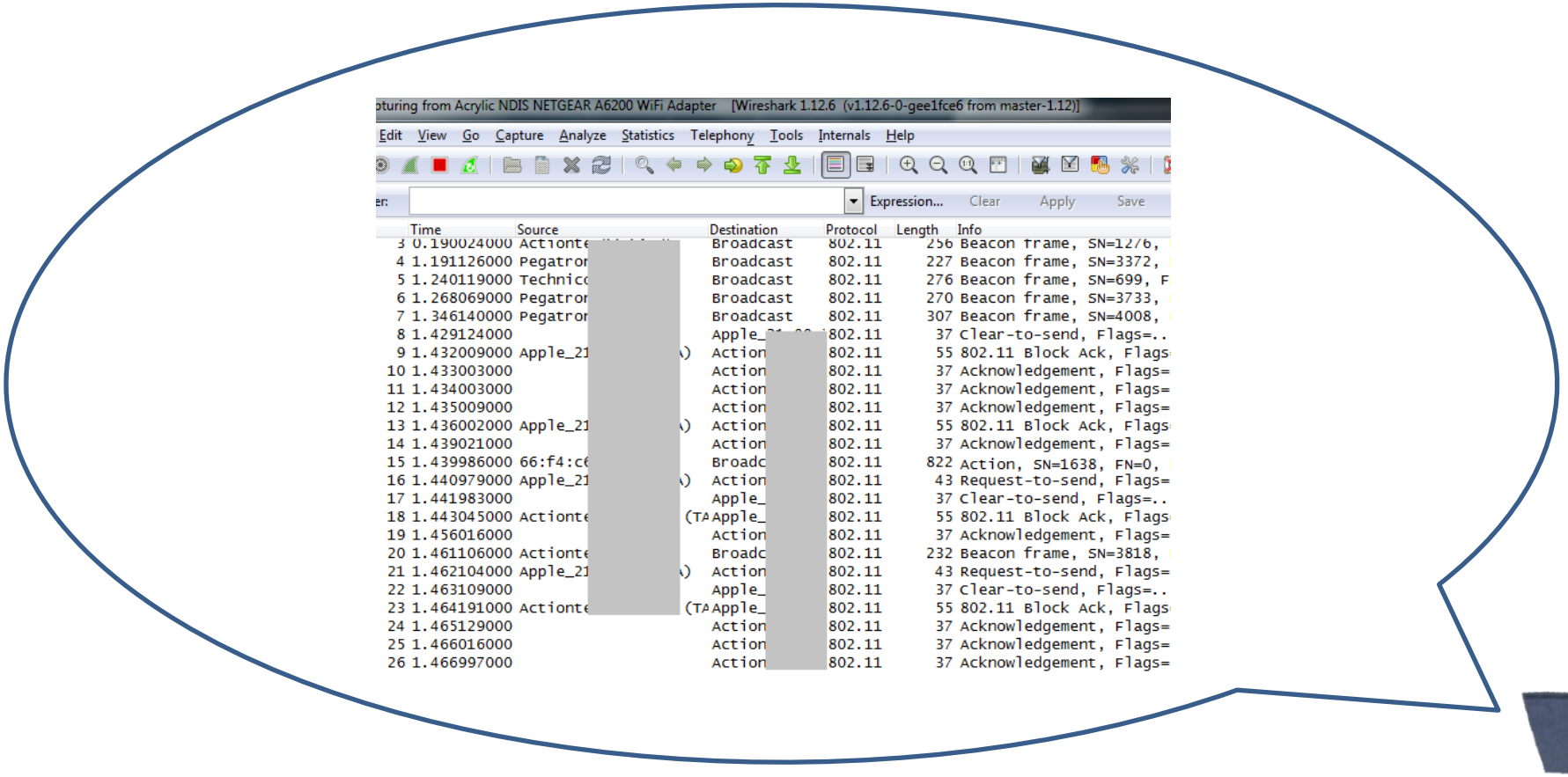
セキュリティ対策のない無線ネットワークでは

- 誰でも接続できてしまいます

  利用者の利便性は良い反面、悪意のユーザーに対する強力な対策が必要となります

- 誰でも傍受できてしまいます

  メール内容、Web閲覧状況などは簡単に盗み見することができます



安全で安心な通信を提供するために

認証と暗号化

- 有線LANでは「ケーブルを接続する」というアクションが、ある意味でセキュリティの一つになっています。無線LANでこれに相当するセキュリティを確保するために「認証」が必要です。
- 有線LANで通信の傍受は困難ですが、無線LANでは誰でも容易に行うことができます。傍受を防ぐためには通信を暗号化する必要があります。

セキュリティの種類	暗号化	認証	キー	MFP*
スタティックWEP	WEP（RC4）		64bit or 128bit	-
ダイナミックWEP(IEEE802.1X)	WEP（RC4）	RADIUS		-
WPA-パーソナル	TKIP (RC4)	○	半角英数記号 (8 - 63)	-
WPA2-パーソナル	CCMP(AES)	○	半角英数記号 (8 - 63)	○
WPA3-パーソナル	CCMP(AES)	○	半角英数記号 (8 - 63)	○(必須)
WPA-エンタープライズ	TKIP (RC4)	RADIUS		-
WPA2-エンタープライズ	CCMP (AES)	RADIUS		○
WPA3-エンタープライズ	GCMP(AES)	RADIUS		○(必須)

【暗号方式の強度について】
GCMP > CCMP > TKIP > WEP
となります。
WEPには脆弱性があります。利用は推奨できません。

*MFP (Management Frame Protection :管理フレーム保護)
無線APと無線端末間で送受信する管理フレームを暗号化によって保護し、セキュリティを確保します。管理フレームを保護することで、無線LANネットワークを狙った不正アクセスや攻撃を防御します。
無線アクセスポイント、無線端末ともに対応している必要があります。

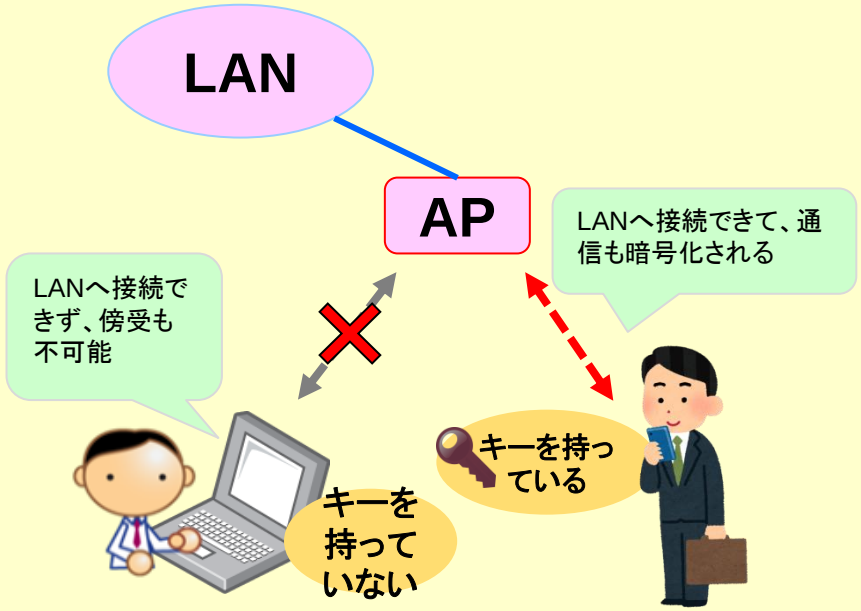
無線のセキュリティ構築イメージ

サービスの提供形態や規模によってセキュリティの種類を選択いただけます。

WPA2/3-パーソナル

WPA2-PSKやWPA3-SAEとも呼ばれます。
接続を許可したいクライアントに対しては、WPA2では事前共有キー（PSK）で、WPA3では同等性同時認証（SAE）により鍵交換をします。

無線アクセスポイントの設定のみで認証と暗号化を行えますので、手軽にセキュリティを確保できます。



WPA2/3-エンタープライズ

認証用にRADIUSサーバーを使用します。
例えばRADIUSサーバーに登録されているユーザーのみをLANへ接続できるように設定可能です。

無線アクセスポイントにはRADIUSサーバー情報を設定するだけで詳細なユーザー管理を行うことができます。
WPA3では192ビットの暗号強度を実現しています。