

# コンピュータ ネットワーク

Ethernet, 無線 LAN 編  
2011/10/19

## 前回の復習

- プロトコル
  - プロトコルとは
  - OSI 参照モデル
- Ethernet
  - イーサネットとは
  - イーサネットフレーム
  - MAC アドレス
  - CSMA/CD
  - 物理層とデータリンク層
  - Ethernet による通信
  - 全二重と半二重
  - リピータとスイッチ

## 本日の流れ

- Ethernet の仕組み
  - 伝送メディア
  - トロポジ
  - ループと障害
- 無線 LAN
  - 無線 LAN (WiFi) の仕組み
  - 無線 LAN のセキュリティ

## ETHERNET の仕組み



## ノードが通信を行うためのメディア

- 有線
  - 銅線 (\*メタルケーブル)
    - 同軸ケーブル
    - 平衡ケーブル
    - より対線
  - 光ファイバケーブル
- 無線(電波)
  - 携帯電話・PHS
  - WiMAX
  - LTE
  - Wireless LAN (WiFi)
  - 衛星通信
  - etc...

\*光ファイバケーブルに対して一般の銅線を用いたケーブルを区別するために使われることが多い呼称

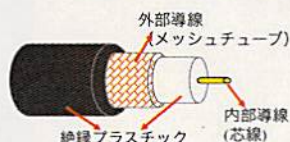
## 銅線メタルケーブルの特性

- メタルケーブルの減衰
  - 周波数が高くなるほど減衰する
  - 伝送距離が長くなるほど減衰する
- ノイズ(雑音)による減衰
  - ケーブルなどを流れる信号を歪ませる要素(電圧)
  - 外部からのノイズと内部のノイズ(電磁誘導など)



## 同軸ケーブル (coaxial cable)

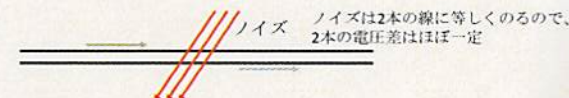
- 多重構造のケーブル
  - 芯線を絶縁プラスチック、メッシュチューブ、被覆で覆う
- 特徴
  - 外部への電磁波の漏れや外界からの影響を低減
    - 雷や工場用電源など強力な電気・電磁波の影響は受ける
  - 強く折り曲げてはいけない
  - 同軸ケーブルの種類やコネクタの形状が多様



コネクタだけでなく、異種ケーブル同士をつなぐ変換コネクタも豊富

## 平衡ケーブル

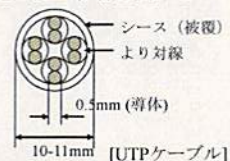
- 平衡
  - 2本のケーブル (e.x. TX+ TX-) について、抵抗などの条件が対等な場合、平衡であるという
- 平衡の特性
  - 外部からのノイズは両方の線に等しくのる (コモンモード)
  - ノイズによる影響を受けにくい





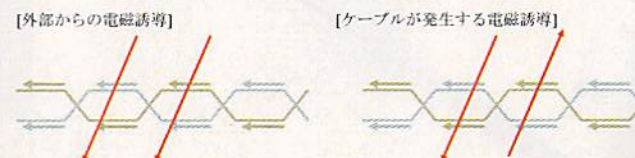
## ツイストペアケーブル

- 特徴
  - 対を構成する2本の芯線を均等によりわけすることで、雑音や漏話を低減
  - 折り曲げが可能で配線の自由度が高い
  - 雷や工場用電源など強力な電気・電磁波の影響を受ける
- UTP/STP
  - Unshielded Twisted Pair
    - インピーダンス100Ω
    - より対線の外がそのまま被覆
    - Ethernetの主流伝送メディア
  - Shielded Twisted Pair
    - インピーダンス150Ω
    - より対線と被覆の間にシールド（メッシュ状に編まれた導電対）



## ツイストペアケーブルのノイズ耐性

- 実用上最も平衡度が高いケーブル
  - より対によって高い平衡性
  - 外部からのノイズを打ち消す
  - ケーブル自体が発するノイズも打ち消す
  - ノイズに強いだけでなく、他のケーブルにノイズの影響を与えない



## ツイストペアケーブルのコネクタ

- 主なもの
  - RJ11 6極 電話用
  - RJ45 8極 LAN/ISDN用
  - RJ48 8極 ISDN新規格用
- ケーブル内の配線
  - ケーブルの色によって決まっている



[T568B]

ストレートケーブル



## UTPケーブル結線

- TIA/EIA-T568A と TIA/EIA-T568B
  - ピン番号：引っかけが無い側から見て一番左が1
  - ハブから90m以下
  - どちらを使っても良い
- クロス
  - 10/100 の場合
  - T568A ↔ T568B

ピン番号	T568A	T568B
1	白/緑	白/橙
2	緑	橙
3	白/橙	白/緑
4	青	青
5	白/青	白/青
6	橙	緑
7	白/茶	白/茶
8	茶	茶

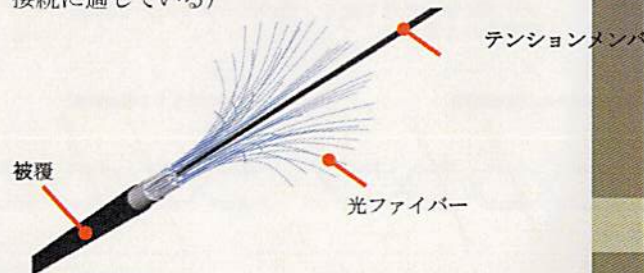




## 光ファイバー

### 特徴と構造

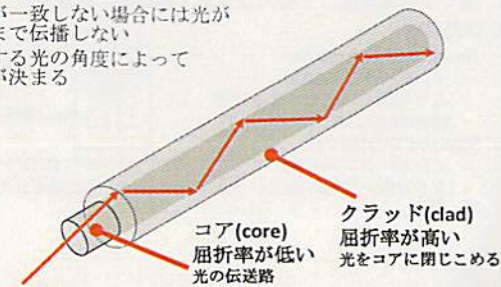
- 信号の周波数がかかなり高くなるまで損失は一定
- 電磁誘導などの電磁障害の影響を受けない  
(雷の影響、長距離での減衰が少ないなど屋外間接続に適している)



©情報機器と情報社会のしくみ素材集  
Source: <http://kyoiku-gakka.u-sacred-heart.ac.jp/youhou-kiki/1704/1704-A.jpg>

## 光ファイバーの伝播の原理

- コアとクラッドは光の屈折率が異なる
- 光はコアとクラッドの境界で全反射を繰り返す
- 反射光同士の干渉により、位相が一致する場合には光が遠くまで伝播する
  - 位相が一致しない場合には光が遠くまで伝播しない
- 入射する光の角度によって位相が決まる



## SMF/MMF

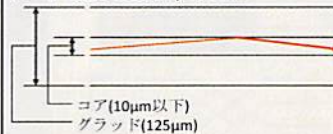
### SMF (single mode fiber)

- 伝播モードが1つ
- 中長距離用
- ATM/SONET/WDMなどで使用

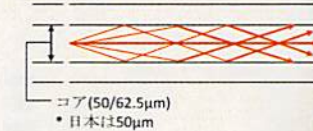
### MMF (multi mode fiber)

- 伝播モードが複数
- 短距離用
- LANではMMFが一般的
- 比較的安価

[SMF] 波長 1310nm / 1550nm



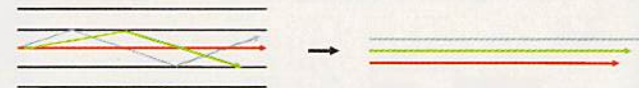
[MMF] 波長 850nm / 1310nm



※コアの直径が小さいほうがモードは少なくなる (開口数)

## SMFとMMFの特性

- SMFの方が長距離に使える
  - MMFはモードが多くあり、光路差がある (モード分散)
  - SMFはモードがひとつしかないので、光路差がない



同じ長さのファイバでも、モードによって光の到達距離が違う



## 光ファイバの減衰

- 光がパワーを失うことで減衰
  - 散乱
    - ファイバーの不完全性、基本的構造による損失
    - 波長の4乗に逆比例
  - 吸収
    - ファイバーの不純物が光エネルギーを吸収
  - 低損失の波長領域（ウインドウ）の存在
    - 820-850nm / 1300nm / 1550nm

## 電波

- 特徴
  - ケーブルが不要で設置が比較的容易
  - 他の機器からの干渉を受けやすい
    - ※無線LANと電子レンジなど
  - 周波数が高くなると
    - データの送出速度を高められる
    - 直進性が高くなり、遮蔽物の影響を受けやすい
      - 例) 大雨が降ると衛星放送が見づらくなる
  - 免許が必要な設備も
    - 衛星回線の送信局



## トポロジー

- イーサネットによるネットワークは基本的に循環の無いグラフ構造にて構築される
- ルータ(中継機)にてネットワークが区切られる



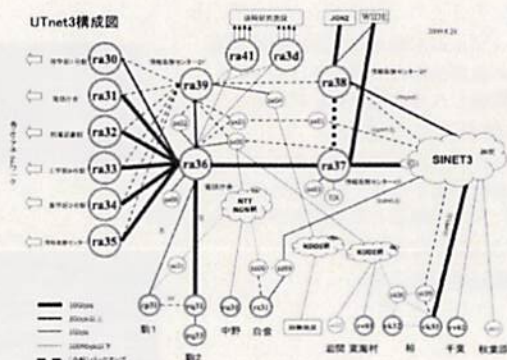
## MAC address / IP address

- 通信先は常に IP address によって指定される
- ARP/NDP によって IP address → MAC address 変換が行われる





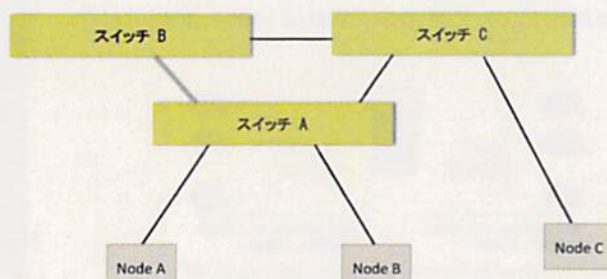
## 東京大学のネットワーク構成



## ループの弊害

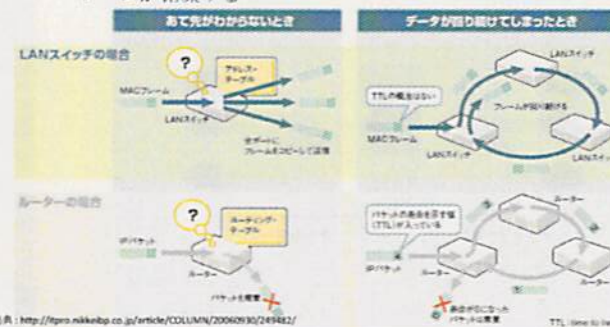
- ループが発生すると、フレームは同じ場所を堂々めぐり
  - トポロジによっては重複するパケットが増殖する場合も
- ループフレームは消えない
  - ブロードキャストストームの発生
  - IPにはTTLがあるが、Ethernetにはない
  - ブリッジの負荷が高くなり、フォワーディングできなくなる
  - ネットワークに接続した機器が動作が極端に遅くなる

## ループ構成とは



## ループの概念

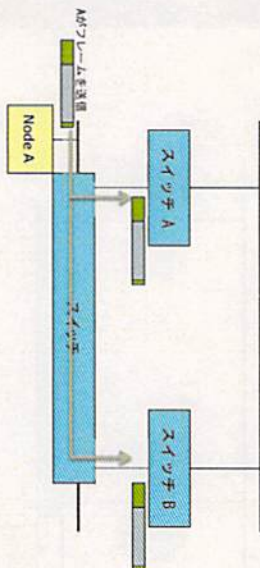
- ルータにてネットワークが区切られる
- 同一ネットワーク内にループが存在するとイーサネットフレームが循環する



出典: <http://pro.nikkeitp.co.jp/article/COLUMN/2006/09/26/4482/>

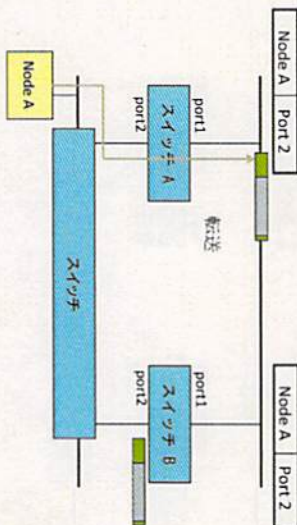
## ルーティング(1/7)

1. あるセグメントに、2台のスイッチがいたとする。  
ノードAが送信したフレームは両方のスイッチで受信される



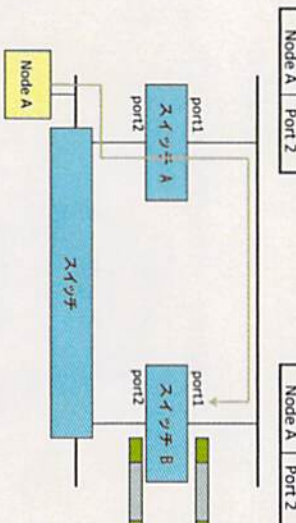
## ルーティング(2/7)

2. スイッチA,BはノードAがポート2の先にいると学習。  
その後、先にグリッパAがスイッチBにフレームを送る。



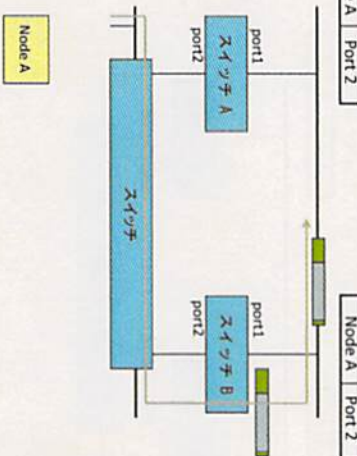
## ルーティング(3/7)

3. スイッチBがスイッチAからフレームを受信する。ただし、受信しただけでまだ転送は行っていない。キャプチャも変更なし。



## ルーティング(4/7)

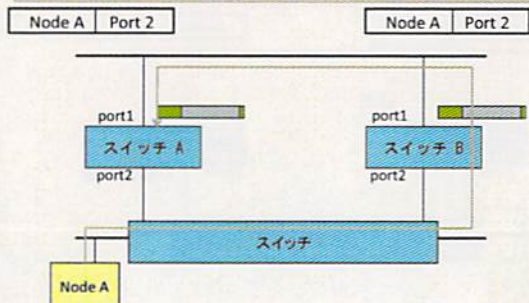
4. スイッチBがノードAから受信したフレームをスイッチAに転送。





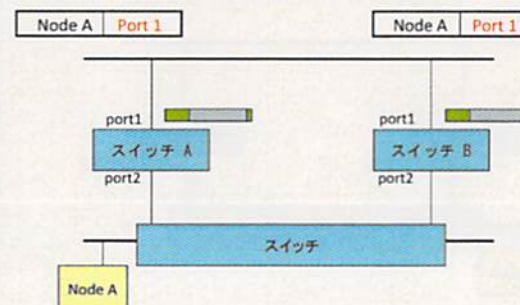
## ループ(5/7)

5. スイッチAはスイッチBが転送したフレームを受信



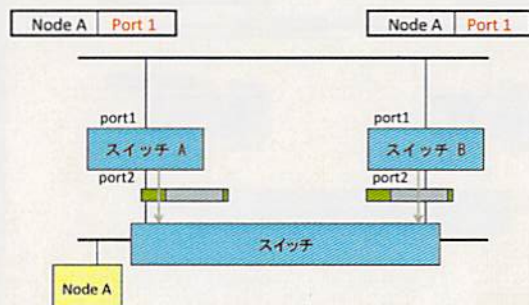
## ループ(6/7)

6. スイッチA、Bはお互いから受信したフレームの処理を開始。ノードAは port 1 に移動したと学習し、キャッシュを更新



## ループ(7/7)

7. ノードAはポート1の先に存在するとキャッシュされているため、ブリッジA、BはLAN1へフレームを転送する



## Spanning Tree Protocol

- IEEE 802.1d
- ループ回避アルゴリズム
- フレームフォワード用のツリーを作ることで、送受信すべきポートを制限
- ツリーの形成は、根(root)側から葉(leaf)側に向かって行われる

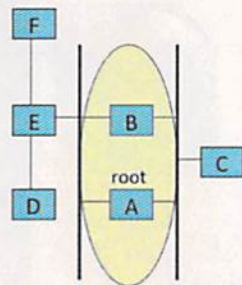


出典: <http://pro.nikkeibp.co.jp/article/COLUMN/2006/09/30/249482/>



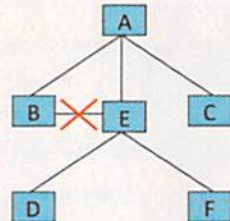
## Spanning Tree

実際のトポロジ(ネットワーク構成)



ループが発生する

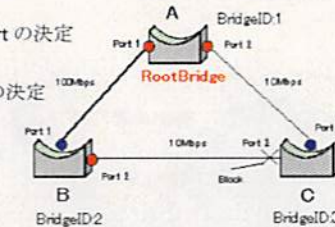
論理的なツリー



B <-> Eのリンクをツリーに含めないことでループ回避

## Spanning Tree の動作

1. Root Bridge の決定
2. Root Port の決定
3. Designated Port の決定
4. Blocked Port の決定



● DP (Designated Port)  
● RP (Root Port)

出典: <http://www.it-study.com/network/spanningtree.htm>

## Rapid Spanning Tree Protocol

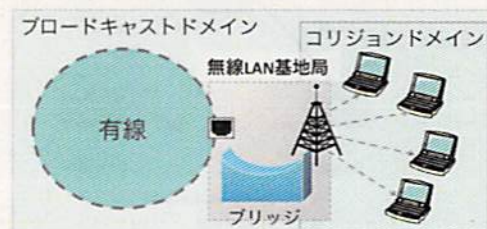
- IEEE802.1w
- Spanning Treeの再構築にかかる時間を短縮
  - トポロジ変更をBridge間のHandshakeで行う
  - リンクの状態をより短時間で検知する
- ポートの役割を追加
  - Alternate Port
  - Backup Port

無線LAN

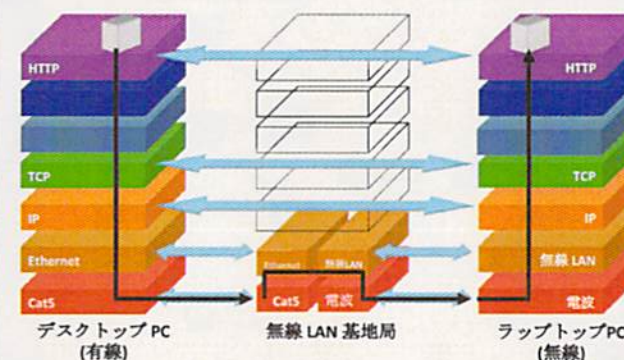


## 無線LAN基地局の動作

- 有線/無線間はブリッジとして動作
- 無線区間は実質リピータ
- 電波はどこへ飛ぶか細かくコントロールできない
  - 想定外の場所で受信できてしまう
  - 電波漏洩

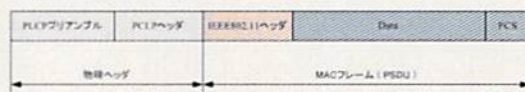


## データリンク層としての無線LAN



## 無線 LAN フレーム (1)

IEEE802.11 フレームフォーマット

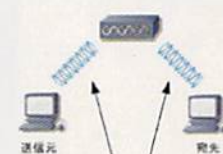


IEEE802.11 フレームフォーマット

出典: <http://www.infraexpert.com/study/wireless7.html>

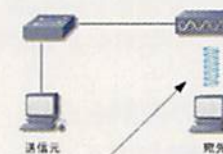
## 無線 LAN フレーム (2)

① 無線機器 → 無線機器への通信



Address1 宛先MAC	Address2 送信元MAC	Address3 BSSID	Address4 -
-------------------	--------------------	-------------------	---------------

② 有線機器 → 無線機器への通信

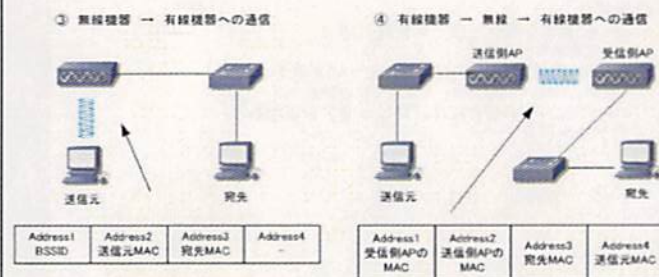


Address1 宛先MAC	Address2 BSSID	Address3 送信元MAC	Address4 -
-------------------	-------------------	--------------------	---------------

出典: <http://www.infraexpert.com/study/wireless7.html>



## 無線 LAN フレーム (3)



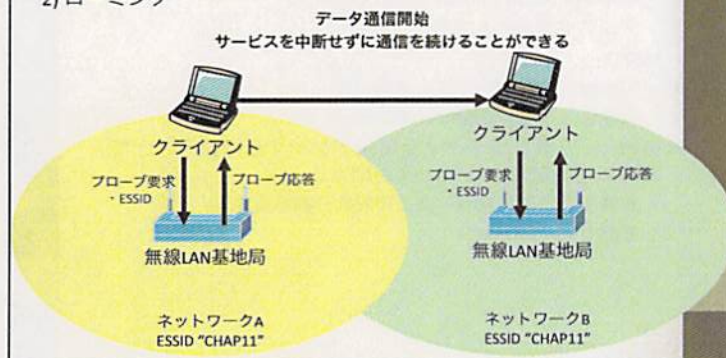
出典: <http://www.infocart.com/technology/wireless2.html>

## ESSID (Extended Service Set Identifier)

- 無線LANにおけるネットワークの識別子
  - アクセスポイントと無線LANユニットのESSIDが一致した場合、データの送受信が可能
  - セキュリティ機能ではない
- "ANY" 指定することで、全てのESSIDが利用できる
- ESSID ブロードキャスト
  - 無線LAN基地局が周囲にESSIDを送信
  - ブロードキャストの無効化(closed network)
    - ESSIDを知っている人しか容易に接続できなくなる
    - ただし、通信を傍受すればすぐにESSIDわかるため、他の方法との併用が必須

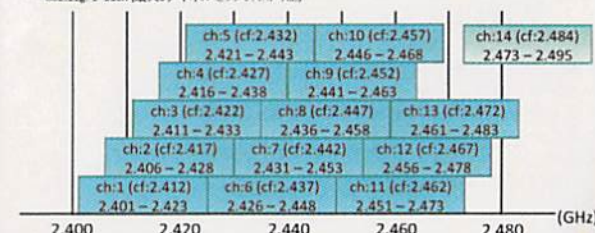
## 無線LANのローミング

- クライアントとAP間の認証とアソシエーション
- ローミング



## 2.4GHz帯無線LANのチャンネル割り当て

- 国内規格ARIB STD-T66, STD-T33
  - チャンネルごとの中心周波数...5MHz毎
  - 1chあたりの占有周波数...22MHz
- 隣接する基地局同士は4チャンネル以上離す
- 利用可能なチャンネル
  - 802.11b: 1~14ch (最大4チャンネルを同時利用可能)
  - 802.11g: 1~11ch (最大3チャンネルを同時利用可能)





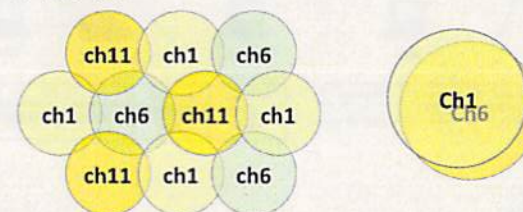
## 5GHz帯無線LANのチャンネル割り当て

5160MHz	5170MHz(34ch)	5170MHz	5180MHz(36ch)
5180MHz	5190MHz(38ch)	5190MHz	5200MHz(40ch)
5200MHz	5210MHz(42ch)	5210MHz	5220MHz(44ch)
5220MHz	5230MHz(46ch)	5230MHz	5240MHz(48ch)
5240MHz		5250MHz	5260MHz(52ch)
		5270MHz	5280MHz(56ch)
		5290MHz	5300MHz(60ch)
		5310MHz	5320MHz(64ch)
		5330MHz	

従来チャンネル(日本仕様)      新チャンネル(欧米と共通)  
日本では2005年5月以降採用

## 無線LAN基地局の設置(1/2)

- ・ 設置場所
  - ・ 高い位置に設置するほど広範囲に届く
  - ・ 電波漏洩も考慮
- ・ 一つの基地局がカバーする範囲(セル)を考える
  - ・ 同じSSIDを用い、ローミングで広範囲をカバー
- ・ ユーザ数が多い場合には、同じエリアを異なるチャンネルでカバー



## 無線LAN基地局の設置(2/2)

- ・ 周波数帯
  - ・ 2.4GHz帯 (802.11b/g)
    - ・ 干渉を起こしやすいが、障害物に強い
    - ・ 隣接する基地局のチャンネルが4以上離すのが望ましい
    - ・ 論理最大速度: 11Mbps / 54Mbps
  - ・ 5GHz帯 (802.11a)
    - ・ 直進性が高い
    - ・ 速度や安定性が高い
    - ・ 隣接する基地局では隣接するチャンネルを利用可能
    - ・ 論理最大速度: 54Mbps
- ・ 近隣に無線LAN基地局がある場合
  - ・ マンションやアパートなど
  - ・ チャンネルの重複、隣接(2.4GHz帯の場合)に注意
  - ・ 電子レンジ、業務用冷蔵庫
- ・ 互換性
  - ・ 11aと11b/gには互換性がない

## 最新の無線 LAN

- ・ IEEE 802.11n
  - ・ MIMO (Multiple Input Multiple Output)
  - ・ デュアルチャンネル技術
- ・ MIMO
  - ・ 2.4GHz / 5GHz どちらにも適用可能
  - ・ 論理最大速度: 300Mbps (600Mbps)
- ・ 複数の送信用アンテナ / 受信用アンテナを用いることで同時に送受信できるデータが増大
  - ・ 空間多重技術 (OFDM - 直交周波数分割多重方式)
  - ・ 変調方式 - 16QAM

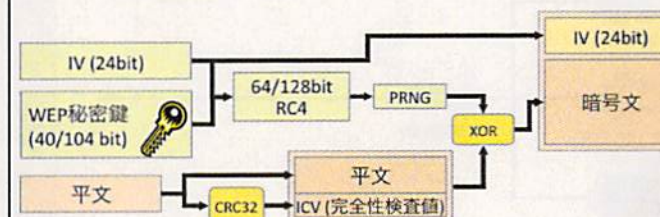


## 無線LANに対するセキュリティ上の脅威

- 盗聴
  - 暗号化されていないトラフィックをそのまま盗聴
  - WEPの解読
- ネットワークへの侵入
  - 電波漏洩
  - 認証機構の不備
- 偽APの設置
  - トラップ
  - Man-in-the-middleアタック
- DoS攻撃
  - 妨害電波
  - アソシエーション切断

## WEP (Wired Equivalent Privacy)

- 無線通信における暗号化技術
  - 秘密鍵暗号方式を利用: RC4アルゴリズム
    - 規格策定当時の米国の暗号輸出規制の関係
  - 鍵長は64bit, 128bit
    - 秘密鍵は40bit, 104bitのデータサイズ
- WEPとパフォーマンス
  - 以前に出荷されていた基地局ではWEPを有効化するとスループットが低下する製品が多かった

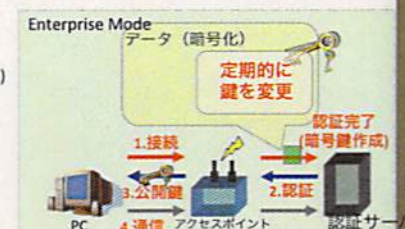


## WEPの脆弱性

- WEPには設計上の脆弱性が発見されている
  - Initialization Vector(初期化ベクタ)がわずか24bit
    - 同一IVを利用し続ける実装も
  - 64(40)bit WEP: 1時間以内に解読されるケースもある
    - 極めて危険
  - 最近の研究では 10秒程度で解読可能
- WEPの脆弱性を攻撃するツールが存在
  - なお、2004年5月の電波法及び有線電気通信法の一部を改正する法律で「暗号通信復元罪」が新設された
- WEP自体は利用しないよりは利用した方がよい
  - ただし128(104)bitを利用すること

## 802.11i (WPA)

- 暗号化方式: TKIP/AES
- TKIP(Temporal Key Integrity Protocol)
  - WEPの脆弱性を改善
    - IVを48bitに拡張
    - 一定時間毎に鍵を更新
- Home Mode (WPA Personal)
  - アクセスポイントとクライアントに共有鍵(PSK: Pre-Shared Key)を設定
  - 認証サーバが不要
- Enterprise Mode (WPA Enterprise)
  - 認証にIEEE 802.1xを利用
  - 認証サーバが必要
- WPA2
  - 暗号化に AES (Advanced Encryption Standard) を採用





## MACアドレスフィルタリング

